เอกสารประกอบการสอน

สาขาวิชาคณิตศาสตร์

NUMBER ทฤษฎีจำนวน THEORY

วิชญาพร จันทะนัน

คณะวิทยาศาสตร์

มหาวิทยาลัยราชภัฏบุรีรัมย์

2564

เอกสารประกอบการสอน
รายวิชา ทฤษฎีจำนวน

วิชญาพร จันทะนัน

คณะวิทยาศาสตร์
มหาวิทยาลัยราชภัฏบุรีรัมย์
2564

เอกสารประกอบการสอน
รายวิชา ทฤษฎีจำนวน

วิชญาพร จันทะนัน
วท.ม. (คณิตศาสตร์)

คณะวิทยาศาสตร์
มหาวิทยาลัยราชภัฏบุรีรัมย์
2564

คำนำ

วิทยาศาสตร์และเทคโนโลยีเป็นเครื่องมือที่สำคัญในการพัฒนาประเทศในโลกยุคปัจจุบัน ความรู้พื้นฐานทางด้านคณิตศาสตร์เป็นสิ่งจำเป็นอย่างยิ่ง ทั้งต่อการพัฒนาทางด้านวิทยาศาสตร์และเทคโนโลยี ทฤษฎีจำนวนนับเป็นศาสตร์ในสาขาคณิตศาสตร์เก่าแก่ที่สุดและได้ถูกพัฒนาขึ้นมาเรื่อย ๆ โดยนักคณิตศาสตร์รุ่นต่อ ๆ มา พยายามตอบปัญหาที่นักคณิตศาสตร์รุ่นก่อนยังหาคำตอบไม่ได้ ทำให้เกิดแนวคิดใหม่ ๆ

เนื้อหาทางด้านทฤษฎีจำนวนได้รับการนำไปประยุกต์ใช้ในด้านต่าง ๆ มากมาย เช่น ทฤษฎีรหัส การพัฒนาของขั้นตอนวิธีในการสั่งงานของคอมพิวเตอร์ การกำหนดแถบรหัสสินค้า การกำหนดการออกแบบชุดของเลขรหัสของบัตรเครดิตต่าง ๆ ตลอดจนใช้เป็นกฎเกณฑ์ในการออกบัตรประจำตัวประชาชนของบางประเทศ

เอกสารประกอบการสอนวิชาทฤษฎีจำนวนเล่มนี้ได้บรรจุเนื้อหาเพียงพอในการใช้เป็นแนวทางศึกษาในวิชาทฤษฎีจำนวน ซึ่งเนื้อหาประกอบด้วย ความรู้เบื้องต้น การหารลงตัว จำนวนเฉพาะ สมภาค ฟังก์ชันเลขคณิต สมการไดโอแฟนไทด์ ทฤษฎีบทเศษเหลือ รากปฐมฐาน ดรรชนีและกฎภาวะส่วนกลับกำลังสอง นอกจากนี้แล้วก็จะมีแบบฝึกหัดท้ายบทของแต่ละบทซึ่งมีความสำคัญในการทำความเข้าใจในเนื้อหาที่ได้เรียนในแต่ละหัวข้อ เป็นการตรวจสอบความเข้าใจในหัวข้อต่าง ๆ ในบทนั้น ๆ แบบฝึกหัดมีความหลากหลายทั้งยากและง่าย เพื่อพัฒนาความคิดและเป็นพื้นฐานที่ดีในการเรียนคณิตศาสตร์ต่อไป

วิชญาพร จันทะนัน
มีนาคม 2564

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

แผนบริหารการสอนตามกรอบมาตรฐานอุดมศึกษา (TQF)

ชื่อสถาบันอุดมศึกษา : มหาวิทยาลัยราชภัฏบุรีรัมย์
คณะ / สาขาวิชา : คณะวิทยาศาสตร์ สาขาวิชาคณิตศาสตร์

หมวดที่ 1 ข้อมูลทั่วไป

1. รหัสและชื่อรายวิชา 4092202 **:** ทฤษฎีจำนวน
2. จำนวนหน่วยกิต 3(3-0-6)
3. หลักสูตร **ชื่อหลักสูตรที่ใช้รายวิชานี้** วิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ **ประเภทของรายวิชา** วิชาเฉพาะด้าน
4. อาจารย์ผู้สอน อาจารย์วิชญาพร จันทะนัน
5. ภาคการศึกษา / ชั้นปีที่เรียน ภาคการศึกษาที่ 1/2563 นักศึกษาชั้นปีที่ 3 Sec.01
6. รายวิชาที่ต้องเรียนมาก่อน (Pre – requisite) -
7. รายวิชาที่ต้องเรียนพร้อมกัน (Co – requisite) -
8. สถานที่เรียน สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏบุรีรัมย์
9. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด ไม่มี

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายรายวิชา เพื่อให้นักศึกษามีความรู้ความเข้าใจได้เกี่ยวกับ สมบัติของจำนวนเต็ม การหารลงตัว จำนวนเฉพาะ สมภาคระบบส่วนตกค้าง สมภาคกำลังสอง ส่วนตกค้างกำลังสอง สมการไดโอแฟนไทน์ ฟังก์ชันออยเลอร์-ฟี สัญลักษณ์ของเลอจองด์ บทตั้งของเกาส์ สัญลักษณ์ของยาโคบี เป็นต้น และสามารถนำความรู้ไปใช้ในการศึกษาต่อระดับที่สูงขึ้นได้
2. **วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา** (สำหรับการปรับปรุงในภาคการศึกษาถัดไป) ไม่มี

หมวดที่ 3 ลักษณะและการดำเนินการ

1. คำอธิบายรายวิชา

การหารลงตัว จำนวนเฉพาะ สมภาค ระบบส่วนตกค้าง สมภาคกำลังสอง ส่วนตกค้างกำลังสอง สมการไดโอแฟนไทน์ ฟังก์ชันออยเลอร์-ฟี สัญลักษณ์ของเลอจองด์ บทตั้งของเกาส์ สัญลักษณ์ของยาโคบี

2. จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

บรรยาย	สอนเสริม	การฝึกปฏิบัติ/งานภาคสนาม/การฝึกงาน	การศึกษาด้วยตนเอง
21 ชั่วโมงต่อภาคการศึกษา	-	มี 21 ชั่วโมงต่อภาคการศึกษา	5 ชั่วโมงต่อสัปดาห์

3. จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาแก่นักศึกษาเป็นรายบุคคล

- อาจารย์จัดเวลาให้คำปรึกษาเป็นรายบุคคล/กลุ่มตามต้องการได้ตลอด 24 ชั่วโมง โดยใช้ E-Mail หรือ Social Network เป็นช่องทางการติดต่อ

หมวดที่ 4 การพัฒนาการเรียนรู้ของนักศึกษา

1. คุณธรรม จริยธรรม

1.1 คุณธรรม จริยธรรมที่ต้องพัฒนา

ตัวอย่าง พัฒนาผู้เรียนตามคุณลักษณะของหลักสูตรดังนี้

- ตระหนักในคุณค่าและคุณธรรม จริยธรรม เสียสละ และซื่อสัตย์สุจริต
- มีวินัย ตรงต่อเวลา และมีความรับผิดชอบต่อตนเองและสังคม
- มีภาวะความเป็นผู้นำและผู้ตาม สามารถทำงานเป็นทีมและสามารถแก้ไขปัญหา ความขัดแย้ง และลำดับความสำคัญของปัญหาได้

1.2 วิธีการสอน

- บรรยายพร้อมยกตัวอย่าง
- ทำแบบฝึกหัดในชั้นเรียน
- นำเสนอแบบฝึกหัดหน้าชั้นเรียน

1.3 วิธีการประเมินผล

- ประเมินผลพฤติกรรมการเข้าห้องเรียน
- ประเมินผลการร่วมกิจกรรมในชั้นเรียน
- ประเมินผลการส่งงานที่ได้รับมอบหมายตามเวลา
- ความตั้งใจ
- ความตรงต่อเวลา

2. ความรู้

2.1 ความรู้ที่ต้องได้รับ

มีความรู้ความเข้าใจเกี่ยวกับ สมบัติของจำนวนเต็ม การหารลงตัว จำนวนเฉพาะ สมภาค ระบบส่วนตกค้าง สมภาคกำลังสอง ส่วนตกค้างกำลังสอง สมการไดโอแฟนไทน์ ฟังก์ชันออยเลอร์-ฟี สัญลักษณ์ของเลอจองด์ บทตั้งของเกาส์ สัญลักษณ์ของยาโคบี

2.2 วิธีการสอน

ตัวอย่าง

- ศึกษาเอกสารประกอบการสอน
- บรรยาย
- แก้โจทย์ปัญหาในชั้นเรียน
- สนทนาซักถาม
- ทำแบบฝึกหัดตามใบงาน

- นำเสนอแบบฝึกหัดหน้าชั้นเรียน

2.3 วิธีการประเมินผล

ตัวอย่าง - ทดสอบย่อย
- สนทนาซักถาม
- การนำเสนองาน
- สอบกลางภาค
- สอบปลายภาค

3.1 ทักษะทางปัญญาที่ต้องพัฒนา

พัฒนาความสามารถในการคิดอย่างเป็นระบบ มีการวิเคราะห์ ปฏิบัติ และสามารถแก้ไขปัญหาอย่างชาญฉลาดและสร้างสรรค์

3.2 วิธีการสอน

ตัวอย่าง - มอบหมายงานให้ทำแล้วเสนอผลการศึกษา
- อภิปรายภายในชั้นเรียน

3.3 วิธีการประเมินผล

ตัวอย่าง - ประเมินผลจากชิ้นงาน
- สอบกลางภาคและปลายภาค

4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ

4.1 ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบที่ต้องพัฒนา

ตัวอย่าง - การสร้างสัมพันธภาพระหว่างผู้เรียนด้วยกัน
- ความเป็นผู้นำและผู้ตามในการทำงานเป็นทีม
- การพึ่งตนเองโดยการเรียนรู้ด้วยตนเอง และมีความรับผิดชอบทำงานที่ได้รับมอบหมายให้ครบถ้วนตามกำหนดเวลา

4.2 วิธีการสอน

ตัวอย่าง - การทำงานเป็นกลุ่ม การปฏิบัติหน้าที่และความรับผิดชอบในกลุ่ม
- การแลกเปลี่ยนเรียนรู้ และแลกเปลี่ยนข้อมูลระหว่างกลุ่ม
- การปฏิบัติงานเป็นรายบุคคล
- การนำเสนอผลงาน

4.3 วิธีการประเมินผล

- ประเมินผลพฤติกรรมการทำงานเป็นกลุ่ม

5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ

5.1 ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสารและการใช้เทคโนโลยีสารสนเทศที่ต้องพัฒนา

- สามารถวิเคราะห์ปัญหาวางแผน เพื่อแก้โจทย์ปัญหาเกี่ยวกับจำนวนได้

5.2 วิธีการสอน

ตัวอย่าง - การศึกษาค้นคว้าด้วยตนเองจากแหล่งเรียนรู้ออนไลน์และสื่ออิเล็กทรอนิกส์
- การนำเสนอผลงานด้วยวาจาประกอบสื่ออิเล็กทรอนิกส์
- การส่งผลงาน การตรวจสอบผลงาน และการแก้ไขผลงานทางอีเมล์

5.3 วิธีการประเมินผล

ตัวอย่าง - ประเมินผลจากการส่งข้อมูล ชิ้นงาน
- ประเมินผลจากการนำเสนอผลงาน

หมวดที่ 5 แผนการสอนและการประเมินผลการเรียนรู้

1. แผนการสอน								
สัปดาห์ที่	**หัวข้อ/รายละเอียด**	**จำนวนชั่วโมง/ผู้สอน**	**กิจกรรมการเรียนการสอน /สื่อที่ใช้**	**การพัฒนาการเรียนรู้ของนักศึกษา**				
				1	2	3	4	5
1	ชี้แจงรายละเอียดแนวทางการเรียนการสอน เกณฑ์การวัดผลการเรียน (Outline) กำหนดข้อตกลงเบื้องต้น ความรู้เบื้องต้นเกี่ยวกับระบบจำนวนเต็มและหลักการจัดอันดับอย่างดี	3	- บรรยาย / PPT - ปฏิบัติ - แบ่งกลุ่มทำแบบฝึกหัด	✓	✓	✓	✓	✓
2	หลักอุปนัยเชิงคณิตศาสตร์และวิธี สูจน์แบบอุปนัยเชิงคณิตศาสตร์	3	- บรรยาย / PPT - นำเสนอแบบฝึกหัด		✓	✓		✓
3	ขั้นตอนวิธีการหาร นิยามการหารลงตัว สมบัติเบื้องต้นของการหารลงตัว	3	- บรรยาย / PPT - แบ่งกลุ่มทำแบบฝึกหัด		✓	✓		✓
4	ตัวหารร่วมมาก ขั้นตอนวิธีแบบยุคลิด ตัวคูณร่วมน้อย	3	- บรรยาย / PPT - นำเสนอแบบฝึกหัด		✓	✓		✓
5	นิยามของจำนวนเฉพาะ ทฤษฎีหลักมูลของเลขคณิต	3	- บรรยาย / PPT - ทำแบบฝึกหัด		✓	✓		✓
6	การค้นหาจำนวนเฉพาะ ทฤษฎีที่สำคัญของจำนวนเฉพาะ	3	- บรรยาย / PPT - ทำแบบฝึกหัด		✓	✓		✓
7	นิยามและสมบัติพื้นฐานของสมภาค	3	- บรรยาย / PPT - นำเสนอแบบฝึกหัด		✓	✓		✓
8	นิยามและสมบัติพื้นฐานของสมการสมภาค สมภาคเชิงเส้น ทฤษฎีบทเศษเหลือของจีน ทฤษฎีบทของแฟร์มาต์และออยเลอร์		-					
9	สอบกลางภาค	2.00						
10	นิยามและสมบัติพื้นฐานของสมภาค	3	- บรรยาย / PPT		✓	✓		✓
11	สมการไดโอแฟนไทป์ ทฤษฎีบทเศษเหลือของจีน	3	- บรรยาย / PPT - ทำแบบฝึกหัด		✓	✓		✓
12	ระบบส่วนตกค้าง ฟังก์ชันออยเลอร์-ฟี	3	- บรรยาย / PPT - ทำแบบฝึกหัด		✓	✓		✓
13	รากปฐมฐาน อันดับของจำนวนเต็ม	3	- บรรยาย / PPT - นำเสนอแบบฝึกหัด		✓	✓		✓
14	จำนวนเต็มที่มีรากปฐมฐาน ส่วนตกค้างกำลัง	3	- บรรยาย / PPT - ทำใบงาน		✓	✓		✓
15	สมภาคกำลังสอง	3	- บรรยาย / PPT		✓	✓		✓

1. แผนการสอน								
สัปดาห์ที่	**หัวข้อ/รายละเอียด**	**จำนวนชั่วโมง/ผู้สอน**	**กิจกรรมการเรียนการสอน /สื่อที่ใช้**	**การพัฒนาการเรียนรู้ของนักศึกษา**				
				1	2	3	4	5
	สัญลักษณ์ของเลอจองด์ บทตั้งของเกาส์		- ทำใบงาน					
16	กฎภาวะส่วนกลับกำลังสอง	3	- บรรยาย / PPT - แบ่งกลุ่มทำแบบฝึกหัด		✓	✓		✓
17	สัญลักษณ์ยาโคบี	3	- บรรยาย / PPT - นำเสนอแบบฝึกหัด	✓	✓	✓	✓	✓
18	สอบปลายภาค	2.00						
	รวม	**56**	**ชั่วโมง**					

หมายเหตุ การพัฒนาการเรียนรู้ของนักศึกษา

1 = คุณธรรม จริยธรรมที่ต้องพัฒนา

2 = ความรู้

3 = ทักษะทางปัญญา

4 = ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ

5 = ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ

2. แผนประเมินผลการเรียนรู้			
ลำดับที่	**วิธีการประเมิน**	**สัปดาห์ที่ประเมิน**	**สัดส่วนของการประเมิน**
1	- การสอบกลางภาค	9	40%
	- การสอบปลายภาค	18	40%
2	- การส่งงานตามที่ มอบหมาย	ตลอดภาคการศึกษา, 16	10%
3	- การเข้าชั้นเรียน - การมีส่วนร่วม อภิปราย เสนอความคิดเห็นในชั้นเรียน	ตลอดภาคการศึกษา	10%
		รวม	100%

หมวดที่ 6 ทรัพยากรการเรียนการสอน

1. เอกสารและตำราหลัก

ณรงค์ ปั้นนิ่ม. ทฤษฎีจำนวน. กรุงเทพ ฯ: สำนักพิมพ์ภูมิบัณฑิต, 2545.

2. เอกสาร แหล่งเรียนรู้และข้อมูลแนะนำ

นิตติยา ปภาพจน์. ทฤษฎีจำนวน. กรุงเทพ ฯ: เอกสารประกอบการสอน มหาวิทยาลัยหอการค้าไทย, 2545.

อัจฉรา หาญชูวงศ์. ทฤษฎีจำนวน. กรุงเทพ ฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2542.

หมวดที่ 7 การประเมินผลและปรับปรุงการดำเนินการของรายวิชา

1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา

การประเมินประสิทธิผลในรายวิชาโดยนักศึกษา ได้นำแนวคิดและความเห็นจากนักศึกษาจาก

- การสนทนากลุ่มระหว่างผู้สอนและผู้เรียน
- การสังเกตพฤติกรรมของผู้เรียน
- แบบประเมินผู้สอน

2. กลยุทธ์การประเมินการสอน

ตัวอย่าง - ผลการสอน การดำเนินการจัดการเรียนการสอนที่สอดคล้องกับแผนบริหารการสอน

- แบบประเมินผลการสอนที่เน้นผู้เรียนเป็นสำคัญ
- ผลสัมฤทธิ์ทางการเรียน

3. การปรับปรุงการสอน

ไม่มี

แผนบริหารการสอนประจำบทที่ 1

เนื้อหาประจำบท

1. วิวัฒนาการของวิชาทฤษฎีจำนวน
2. เซตเบื้องต้น
3. การพิสูจน์เบื้องต้น
    3.1 การพิสูจน์ข้อความแบบมีเงื่อนไข
    3.2 การพิสูจน์โดยแจกแจงกรณี
    3.3 การพิสูจน์ข้อความแบบผันกลับได้
    3.4 การพิสูจน์โดยวิธีขัดแย้ง
    3.5 การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว
    3.6 การพิสูจน์โดยกลักอุปนัยเชิงคณิตศาสตร์
4. สมบัติจำนวนเต็ม
    4.1 ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม

วัตถุประสงค์เชิงพฤติกรรม

1. อธิบายวิวัฒนาการของวิชาทฤษฎีจำนวน
2. บอกความหมายของเซต และเขียนแสดงเซตตามวิธีต่าง ๆ ได้
3. พิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็มได้
4. พิสูจน์และบอกสมบัติของจำนวนเต็มได้
5. ประยุกต์ใช้ความรู้ในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 วิวัฒนาการของวิชาทฤษฎีจำนวน
    1.2 เซตเบื้องต้น
    1.3 การพิสูจน์เบื้องต้น
    1.4 สมบัติจำนวนเต็ม
    1.5 ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอนและตำราต่าง ๆ ที่เกี่ยวข้อง
2. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 1
ความรู้พื้นฐาน

นพพร ธนะชัยขันธ์ (2543 : 7-8) ได้กล่าวถึงประวัติของทฤษฎีจำนวนโดยมีวัตถุประสงค์เพื่อให้ผู้อ่านได้ทราบถึงความเป็นมาเกี่ยวกับทฤษฎีจำนวนไว้ว่า

ทฤษฎีจำนวน (number theory) เป็นสาขาหนึ่งของคณิตศาสตร์ ส่วนใหญ่จะเกี่ยวข้องกับการศึกษาสมบัติของจำนวนนับ (counting number)

$$1, 2, 3, 4, 5, 6, 7, 8, 9, ...$$

เราอาจเรียกจำนวนนี้ว่าจำนวนธรรมชาติ (natural number) หรือจำนวนเต็มบวก (positive integer) ก็ได้ ซึ่งถือว่าเป็นจำนวนที่มนุษย์สร้างขึ้นเป็นชุดแรก เราจะเห็นว่ามนุษย์มีความยุ่งยากในการดำรงชีวิตเป็นอย่างมาก ถ้าไม่มีความสามารถในการนับ จากหลักฐานทางประวัติศาสตร์พบว่าเมื่อประมาณ 3,500 ปีก่อนศริสต์ศักราช ชาวสุเมเรียน (Sumerian) ได้ประดิษฐ์ปฏิทินขึ้นโดยพัฒนามาจากรูปแบบบางอย่างทางเลขคณิต และต่อมาประมาณ 2,500 ปีก่อนคริสต์ศักราช ชาวสุเมเรียนยังได้คิดระบบจำนวนโดยใช้เลขฐาน จนกระทั่งมาถึงยุคบาบิโลเนีย ชาวบาบิโลเนียมีทักษะทางการคำนวณมากขึ้น โดยดูได้จากหลักฐานการค้นพบก้อนดินเหนียวของชาวบาบิโลเนียที่สร้างขึ้นเมื่อประมาณ 2,000 ปีก่อนคริสต์ศักราชมาแล้ว

ต่อมาเมื่อมนุษย์มีความเจริญมากขึ้นก็ได้พยายามคิดค้นและพัฒนาเกี่ยวกับสมบัติของจำนวนขึ้นเรื่อย ๆ โดยระยะเริ่มแรกยังมีเหตุผลของความเชื่อและโชคลางเข้ามาเกี่ยวข้อง เช่น จำนวน $3, 7, 11$ และ 13 เป็นต้น มีหลักฐานเชื่อได้ว่าก่อนที่มนุษย์จะศึกษาเกี่ยวกับจำนวนนั้นมนุษย์ได้อาศัยจำนวนในการจดบันทึกเหตุการณ์ต่าง ๆ และบันทึกในการค้าขายแลกเปลี่ยนสิ่งของกันมาเป็นเวลานานกว่า 4,000 ปีมาแล้ว

ชาวกรีกนับเป็นชนกลุ่มแรกที่เริ่มศึกษาเกี่ยวกับจำนวนเต็ม ประมาณ 600 ปีก่อนคริสต์ศักราช ปีทาโกรัส (Pythagoras) และศิษย์ได้ศึกษาจำนวนเต็มบวก โดยการจำแนกจำนวนเต็มบวกออกเป็น 4 กลุ่ม คือ

> จำนวนคู่ (even number) : $2, 4, 6, 8, 10, 12, 14, 16, \ldots$
> จำนวนคี่ (odd number) : $1, 3, 5, 7, 9, 11, 13, 15, \ldots$
> จำนวนเฉพาะ (prime number) : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$
> จำนวนประกอบ (composite number) : $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots$

การนับจำนวนเป็นสิ่งที่อยู่คู่กับมนุษยชาติมาช้านาน การพยายามทำความเข้าใจเกี่ยวกับจำนวนของมนุษย์จึงเกิดขึ้นเพื่อนำไปใช้ประโยชน์ในด้านต่าง ๆ จนเกิดเป็นการศึกษาสมบัติของจำนวนเหล่านั้นเรื่อยมา อันเป็นที่มาของสาขาหนึ่งทางคณิตศาสตร์คือ “ทฤษฎีจำนวน” (number theory) การมองเห็นวิวัฒนาการของวิชาทฤษฎีจำนวนนับเป็นพื้นฐานความรู้เพื่อให้รู้จักวิชานี้ ซึ่งจะกล่าวถึงเป็นส่วนแรก ก่อนจะกล่าวถึงเซตเบื้องต้น การพิสูจน์เบื้องต้น สมบัติจำนวนเต็ม และข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม เนื่องจากในขอบข่ายการศึกษาทฤษฎีจำนวน จะจำกัดเฉพาะจำนวนเต็มเท่านั้น และการเข้าใจสมบัติที่เกี่ยวกับจำนวนเต็มจะเป็นเครื่องมือสำคัญในการพิสูจน์สมบัติต่าง ๆ ที่เกี่ยวข้องต่อไป

1.1 วิวัฒนาการของวิชาทฤษฎีจำนวน

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์ (2552 : 1) ได้กล่าวว่า ทฤษฎีจำนวน เป็นสาขาวิชาหนึ่งในคณิตศาสตร์ซึ่งศึกษาเกี่ยวกับสมบัติของจำนวนโดยเน้นที่สมบัติของจำนวนเต็มและจำนวนนับ เนื่องจากจำนวนนับเป็นจำนวนชนิดแรก ๆ ที่มนุษย์รู้จัก จึงไม่น่าแปลกใจที่มนุษย์สนใจศึกษาจำนวนเหล่านี้ในแง่มุมต่าง ๆ อย่างกว้างขวาง และมีผู้ยกย่องไว้ว่า "วิชาทฤษฎีจำนวนเปรียบเสมือนราชินีแห่งคณิตศาสตร์ (Number theory is the queen of mathematics)" ตามคำกล่าวของนักคณิตศาสตร์ผู้มีชื่อเสียงนามว่า คาร์ล ฟรีดริช เกาส์ (Carl Fridrich Gauss 1777-1855)

ทฤษฎีจำนวนมีความเก่าแก่ย้อนกลับไปกว่า 2,500 ปีซึ่งนับว่าเป็นศาสตร์ที่มีความเก่าแก่ที่สุดก็ว่าได้ ผู้บุกเบิกวิชานี้ คือ พีทาโกรัส (Pythagoras 569-500 ปีก่อนคริสต์ศักราช) โดยเขาพยายามอธิบายจักรวาลและสรรพสิ่งรอบตัวว่าคือจำนวน จนก่อกำเนิดเป็นสำนักคิดอันรวบรวมผู้คนที่เชื่อเหมือนพีทาโกรัสไว้ด้วยกัน โดยมีปรัชญาสำคัญว่า "ทุกสิ่งทุกอย่างคือจำนวน" จากการรวมเป็นสำนักคิดนี้เองทำให้ค้นพบสมบัติพิเศษเกี่ยวกับจำนวนมากมาย เช่น จำนวนมิตรภาพ (amicable numbers) ซึ่งผลบวกของตัวหารแท้ของจำนวนหนึ่งจะเท่ากับผลบวกของตัวหารแท้อีกจำนวนหนึ่ง ในสมัยของพีทาโกรัสพบจำนวนมิตรภาพคู่แรกคือ 284 และ 220 ตัวหารแท้ของ 284 คือ $1, 2, 4, 71$ และ 142 จะได้ว่า

$$1 + 2 + 4 + 71 + 142 = 220$$

ตัวหารแท้ของ 220 คือ $1, 2, 4, 5, 10, 11, 20, 22, 44, 55$ และ 110 จะได้ว่า

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

ผู้ที่เชื่อโชคลางจะจารึกตัวเลขลงในเครื่องรางของขลัง โดยเชื่อว่าคนคู่ใดห้อยของขลังที่จารึกตัวเลขดังกล่าวจะเป็นมิตรแท้ต่อกัน (สมวงษ์ แปลงสพโชค. 2549 : 3, จารุวรรณ สิงห์ม่วง. 2011 : 80) การบุกเบิกเรื่องจำนวนมิตรภาพข้างต้นเป็นพื้นฐานให้เกิดการค้นพบจำนวนมิตรภาพอื่น ๆ อีกมากมายตามมา ดังตัวอย่างตามตารางต่อไปนี้

ปีที่ค้นพบ	ผู้ค้นพบ	จำนวนมิตรภาพ
ค.ศ. 1636	Pierre De Fermat (1601-1665)	$17,296$ และ $18,416$
ค.ศ. 1686	Rene Descartes (1596-1650)	$9,363,584$ และ $9,437,056$
ค.ศ. 1830	Adrien Marie Legendre (1752-1833)	$2,172,649,216$ และ $8,520,191$
ค.ศ. 1866	Nicolo Painini ชาวอิตาลีอายุ 16 ปี	$1,184$ และ $1,210$

ตารางที่ 1.1 แสดงตัวอย่างจำนวนมิตรภาพและผู้ค้นพบ
ที่มา : ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์ (2552 : 2)

กระทั่งในปัจจุบันคอมพิวเตอร์สามารถคำนวณจำนวนมิตรภาพได้มากกว่า 1,000 ล้านคู่ ซึ่งเห็นได้ชัดว่ารากฐานของการคำนวณจำนวนดังกล่าวนี้มีมากกว่าสองพันปีแล้ว

ในยุคของพีทาโกรัส ได้ค้นพบจำนวนที่มีความมหัศจรรย์อีกจำนวนหนึ่งคือ จำนวนสมบูรณ์ (perfect number) เหตุที่เรียกเช่นนี้ เพราะเป็นจำนวนที่เท่ากับผลบวกของตัวหารแท้ของจำนวนนั้น เช่น 6 มีตัวหารแท้คือ $1, 2$ และ 3 ผลบวกเท่ากับ 6 ก่อนที่จะเกิดการค้นพบจำนวนสมบูรณ์อีกสองจำนวนต่อมาคือ 28 และ 496 กระทั่งในปี ค.ศ. 2016 ได้พบทั้งหมด 49 จำนวน

ยุคสำคัญของการศึกษาทฤษฎีจำนวนสมัยต่อมาเกิดขึ้นราว 300 ปีก่อนคริสตกาล เมื่อยุคลิดแห่งอเล็กซานเดรีย (Euclic of Alexandria 450-380 ปีก่อนคริสต์ศักราช) ได้ตีพิมพ์หนังสืออิลิเมนต์จำนวน 13 เล่ม โดยมีหนังสือ 3 เล่มในชุดนั้นกล่าวถึงเรื่องราวเกี่ยวกับทฤษฎีจำนวน ได้แก่ จำนวนคู่ จำนวนคี่และจำนวนเฉพาะ ขั้นตอนวิธีแบบยุคลิด ตัวหารร่วมมาก ตัวคูณรวมน้อย และทฤษฎีบทที่ว่าจำนวนเฉพาะมีจำนวนเป็นอนันต์

สมัยกรีกยังมีนักคณิตศาสตร์อีกคนที่สำคัญคือ ดีโอฟานโตสแห่งอเล็กซานเดรีย (Diophantus of Alexandria) ซึ่งมีชีวิตอยู่ในช่วง 250 ปีก่อนคริสตกาล ได้ตีพิมพ์หนังสือ 13 เล่ม เนื้อหาในหนังสือชุดนี้ได้เรียบเรียงวิธีการแก้สมการทางพีชคณิตและปัญหาต่าง ๆ ผลงานสำคัญของดีโอฟานโตส คือ สมการพีชคณิตที่มีคำตอบเป็นจำนวนเต็มเรียกว่า **สมการไดโอแฟนไทน์ (Diophantine equation)** ตัวอย่างเช่น สมการพีทาโกรัส $x^2 + y^2 = z^2$ อันกลายเป็นรากฐานของการศึกษาทฤษฎีจำนวนในปัจจุบัน

แม้การศึกษาทฤษฎีจำนวนจะมีมาตั้งแต่สมัยกรีก หากการสิ้นสุดอารยธรรมกรีกโรมันต่อด้วยการเข้าสู่ยุคกลางของยุโรปทำให้เกิดการชะงักงันทางการศึกษาดังกล่าว เนื่องจากองค์ความรู้จากคริสตศาสนาได้กลายเป็นศูนย์กลางในการอธิบายสรรพสิ่งรอบตัวแทน จนกระทั่งเข้าสู่ยุคฟื้นฟูศิลปวิทยาการ (Renaissance) ราวคริสตศตวรรษที่ 14-17 ได้มีการฟื้นฟูวิทยาการสมัยกรีกโรมันขึ้นมาอีกครั้ง ช่วงเวลานี้เองที่เป็นจุดเริ่มต้นของทฤษฎีจำนวนสมัยปัจจุบัน เริ่มโดยนักคณิตศาสตร์ชาวฝรั่งเศสชื่อว่า ปีแยร์ เดอ แฟร์มาต์ (Pierre de Fermat 1601-1665) เขาได้ทำการศึกษางานของดีโอฟานโตสและเป็นคนที่ได้พบสมบัติของจำนวนเต็มอีกมากมาย โดยเฉพาะการคาดการณ์ว่าสมการ $x^2 + y^2 = z^2$ ไม่มีคำตอบเป็นจำนวนเต็มที่ไม่ใช่ศูนย์เมื่อ เป็นจำนวนเต็มที่มากกว่า แม้ขณะนั้นเขาสามารถพิสูจน์ได้เพียงกรณีที่ $n = 3$ เท่านั้น หากต่อมานักคณิตศาสตร์รุ่นหลังได้พยายามพิสูจน์ต่อจนสำเร็จ และตั้งชื่อว่า “ทฤษฎีบทสุดท้ายของแฟร์มาต์” เพื่อเป็นเกียรติพร้อมยกย่องแฟร์มาต์ว่าเป็นบิดาของทฤษฎีจำนวนสมัยใหม่

ทฤษฎีจำนวนของแฟร์มาต์ได้ส่งอิทธิพลต่อนักทฤษฎีจำนวนคนสำคัญอีกคน คือ เกาส์ ซึ่งได้ตีพิมพ์หนังสือ Disquistiones Arithmeticae ในปี 1801 เนื้อหาเกี่ยวกับการพิสูจน์อย่างเป็นระบบ ก่อนพัฒนาต่อมาเป็นสมบัติของจำนวนเฉพาะอันเป็นการวางรากฐานเกี่ยวกับทฤษฎีจำนวนไว้อย่างมั่นคง

จากการศึกษาวิชาทฤษฎีจำนวนหลายพันปีเห็นได้ว่า มีหัวข้อเกี่ยวกับจำนวนให้ขบคิดมากมายหัวข้อในการศึกษาบางประการต้องใช้เวลานานกว่าจะได้รับการแก้ไข บางครั้งต้องผ่านการพิสูจน์ซ้ำแล้วซ้ำเล่า หากพิจารณาว่าประเด็นใดเป็นสิ่งที่นักคณิตศาสตร์ให้ความสนใจอย่างยิ่งคงไม่พ้นเรื่องจำนวนเฉพาะ เหตุผลประการแรก คือการตรวจสอบว่าจำนวนใดเป็นจำนวนเฉพาะไม่ใช่เรื่องง่ายดายนัก ถ้าจำนวนนั้นเป็นจำนวนขนาดใหญ่ เช่น 10,006,721 แต่ปัญหานี้ในปัจจุบันเราสามารถตรวจสอบโดยใช้คอมพิวเตอร์พบว่า 10,006,721 เป็นจำนวนเฉพาะตัวที่ 664,999 เหตุผลอีกประการหนึ่ง คือมีสูตรทั่วไปในการหาจำนวนเฉพาะตัวที่ n หรือไม่ หลายศตวรรษมาแล้วเชื่อว่า $n^2 + n + 41$ เป็นจำนวนเฉพาะสูตรนี้เป็นจริงเพียง 40 จำนวนเรียงติดกันคือ $n = 0, 1, 2, ..., 39$ ทั้งนี้ ข้อเสนอของแฟร์มาต์ในการหาจำนวนเฉพาะคือ $F_n = 2^{2^n} + 1$ เป็นจำนวนเฉพาะสำหรับทุกจำนวนเต็ม $n \geq 0$ ต่อมาพบว่า $n = 5$ ไม่เป็นจำนวนเฉพาะเนื่องจาก 641 เป็นตัวประกอบของ F_5 พบโดยออยเลอร์ (Leonhard Euler ค.ศ. 1707-1783) เรียก F_n ว่า**จำนวนแฟร์มาต์ (Fermat number)** ในกรณีที่เป็นจำนวนเฉพาะเรียกว่า **จำนวนเฉพาะแฟร์มาต์ (Fermat prime)**

ปัญหาเกี่ยวกับจำนวนเฉพาะที่สนใจเรื่องหนึ่งก็คือ จำนวนเฉพาะคู่แฝด (twin prime) คือจำนวนเต็ม p และ $p + 2$ เป็นจำนวนเฉพาะทั้งคู่ เช่น 5 และ $7, 11$ และ $13, 17$ และ $19, 29$ และ 31 เป็นต้น มีจำนวนเฉพาะคู่แฝดไม่จำกัดจำนวนใช่หรือไม่ โดยใช้เครื่องคอมพิวเตอร์ตรวจสอบพบว่ามีจำนวนเฉพาะคู่แฝดที่น้อยกว่า $30,000,000$ มีทั้งหมด $152,892$ คู่

ทั้งหมดนี้เป็นเพียงจุดสนใจส่วนหนึ่งในวิชาทฤษฎีจำนวนเท่านั้น ยังมีสิ่งที่น่าสนใจอีกมากมายและยังคงมีปัญหาที่ยังไม่สามารถหาคำตอบได้ (unsolved problem) ให้ได้ขบคิด สิ่งนี้เป็นความท้าท้ายและอาจก่อให้เกิดองค์ความรู้ใหม่ ๆ ตามมาได้

1.2 เซตเบื้องต้น

เซต (Set) เป็นคำอนิยาม หมายถึง คำที่ต้องยอมรับกันในเบื้องต้นว่าไม่สามารถให้ความหมายที่รัดกุมได้ คำว่าเซตจึงหมายถึงกลุ่มของสิ่งของต่าง ๆ เมื่อกล่าวถึงกลุ่มใดแล้วจะสามารถบอกได้แน่นอนว่าสิ่งใดอยู่ในกลุ่มและสิ่งใดอยู่นอกกลุ่ม เรียกสิ่งต่าง ๆ ที่อยู่ในเซตว่า **สมาชิก (element)**(Pual Glendinning. 2012 : 48)

สำหรับเซตที่ไม่มีสมาชิกเขียนแทนด้วย $\varnothing$ เรียกว่า เซตว่าง (empty set) ถ้า a เป็นสมาชิกของเซต A เขียนแทนด้วย $a \in A$ และถ้า a ไม่เป็นสมาชิกของเซต A เขียนแทนด้วย $a \notin A$ เช่น $A = \{1, 2, 3\}$ จะได้ว่า $1 \in A$ แต่ $4 \notin A$ เป็นต้น การเขียนเซตประกอบด้วย 2 วิธีคือ วิธีแจกแจงสมาชิก และวิธีบอกเงื่อนไขของสมาชิก

1. วิธีแจกแจงสมาชิก (Tubular form) การเขียนเซตแบบแจกแจงสมาชิก คือการเขียนเซตโดยเขียนสมาชิกลงในเครื่องหมายวงเล็บปีกกา $\{\}$ และใช้เครื่องหมายจุลภาค $(,)$ คั่นระหว่างสมาชิกแต่ละตัว ตัวอย่างเช่น $\{1, 2, 3\}$ และ $\{a, b, c\}$ เป็นต้น

ตัวอย่าง 1.2.1

จงเขียนเซตต่อไปนี้แบบแจกแจงสมาชิก
(1) A เป็นเซตของเดือนที่ลงท้ายด้วย “ยน”
(2) B เป็นเซตของจำนวนเต็มบวกที่น้อยกว่า 200
(3) C เป็นเซตของจำนวนเต็มบวกที่เป็นจำนวนคู่

วิธีทำ (1) $A = \{$เมษายน, มิถุนายน, กันยายน, พฤศจิกายน$\}$
(2) $B = \{1, 2, 3, \ldots, 199\}$
(3) $C = \{2, 4, 6, 8, 10, \ldots\}$

ตัวอย่าง 1.2.2

จงเขียนเซตต่อไปนี้แบบแจกแจงสมาชิก
(1) $H = \{x \mid x$ เป็นจำนวนเต็ม และ $x^2 - 3x + 2 = 0\}$
(2) $I = \{x \mid x$ เป็นจำนวนเต็ม$\}$
(3) $J = \{x \mid x$ เป็นจำนวนเต็ม ที่อยู่ระหว่าง 1 กับ 2$\}$

วิธีทำ (1) $H = \{1, 2\}$
(2) $I = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
(3) $J = \varnothing$

2. วิธีบอกเงื่อนไขของสมาชิก (Set builder form) การเขียนเซตแบบบอกเงื่อนไขประกอบด้วย 2 ส่วน ส่วนแรกหมายถึงสมาชิก และส่วนที่สองคือเงื่อนไขของสมาชิก โดยมีเครื่องหมาย “|” หรือ “:” หรือ “;” คั่นระหว่างสองส่วนนั้น ซึ่งในที่นี้มักใช้เครื่องหมาย “|” และจะอ่านเครื่องหมาย “|” ว่า “ซึ่ง” หรือ “ที่” หรือ “โดยที่” (ช่อเอื้อง อุทิตะสาร. 2562 : 45, มานัส บุญยัง. 2532 : 3)

$$A = \{\text{สมาชิก} \mid \text{เงื่อนไขของสมาชิก}\}$$

ตัวอย่างเช่น $A = \{x \mid x$ เป็นจำนวนเต็มบวกที่น้อยกว่า $5\}$ หมายถึง เซต A คือเซตของ x โดยที่ x เป็นจำนวนเต็มบวกที่น้อยกว่า 5 และเขียนแจกแจงสมาชิกได้เป็น $A = \{1, 2, 3, 4\}$

ตัวอย่าง 1.2.3

จงเขียนเซตต่อไปนี้แบบบอกเงื่อนไขของสมาชิก

(1) $L = \{1, 4, 9, 16, 25\}$

(2) $M = \{$สีแดง, สีขาว, สีน้ำเงิน$\}$

(3) $N = \{\ \}$

วิธีทำ (1) $L = \{x^2 \mid x$ เป็นจำนวนเต็มบวก และ $x^2 \leq 25\}$

(2) $M = \{x \mid x$ เป็นสีของธงชาติไทย$\}$

(3) $N = \{x \mid x$ เป็นเดือนที่มี 25 วัน$\}$

สับเซต (Subset)

สำหรับเซต A ที่มีสมาชิกทุกตัวอยู่ในเซต B จะกล่าวว่า A เป็น **สับเซต (Subset)** ของ B เขียนแทนด้วย $A \subseteq B$

ดังนั้น ถ้ามีสมาชิกอย่างน้อยหนึ่งตัวที่เป็นสมาชิกของ A แต่ไม่เป็นสมาชิกของ B ก็จะกล่าวว่า เซต A ไม่เป็นสับเซตของ B เขียนแทนด้วยสัญลักษณ์ $A \not\subseteq B$ ในเบื้องต้นเพื่อให้ง่ายต่อการนำไปใช้ กำหนดสัญลักษณ์ดังนี้

$\mathbb{C}$ แทนเซตของจำนวนเชิงซ้อน	$\mathbb{Z}$ แทนเซตของจำนวนเต็ม
$\mathbb{R}$ แทนเซตของจำนวนจริง	$\mathbb{N}$ แทนเซตของจำนวนนับ

ตัวอย่าง 1.2.4

ถ้า $A = \{2\}, B = \{0, 1, 2\}, C = \{2, 4, 6\}$ และ $D = \mathbb{N}$ แล้วจะได้ว่า

(1) $A \subseteq A$	(2) $A \subseteq B$	(3) $A \subseteq C$	(4) $A \subseteq D$
(5) $B \not\subseteq A$	(6) $B \subseteq B$	(7) $B \not\subseteq C$	(8) $B \not\subseteq D$
(9) $C \not\subseteq A$	(10) $C \not\subseteq B$	(11) $C \subseteq C$	(12) $C \subseteq D$
(13) $D \not\subseteq A$	(14) $D \not\subseteq B$	(15) $D \not\subseteq C$	(16) $D \not\subseteq D$

เอกภพสัมพัทธ์ (universe) คือเซตที่ถูกกำหนดขึ้นโดยมีข้อตกลงว่า จะกล่าวถึงสิ่งที่เป็นสมาชิกของเซตนี้เท่านั้น และนิยมใช้ $\mathcal{U}$ แทนเอกภพสัมพัทธ์ เมื่อให้ A และ B เป็นเซตในเอกภพสัมพัทธ์ $\mathcal{U}$ นิยามการดำเนินการบนเซตดังต่อไปนี้

การดำเนินการบนเซต

ยูเนียน (union)	$A \cup B = \{x \mid x \in A$ หรือ $x \in B\}$
อินเตอร์เซกชัน (intersection)	$A \cap B = \{x \mid x \in A$ และ $x \in B\}$
ผลต่าง (difference)	$A \setminus B = A - B = \{x \mid x \in A$ และ $x \notin B\}$
ส่วนเติมเต็ม (complement)	$A^{\complement} = \{x \mid x \in \mathcal{U}$ และ $x \notin A\}$

ในกรณีที่ทราบจำนวนสมาชิกของเซต A เขียน $|A|$ แทนจำนวนสมาชิกของ A และได้ว่า

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A| = |\mathcal{U}| - |A^{\complement}|$$

เมื่อ A และ B เป็นเซตที่ทราบจำนวนสมาชิกแน่ชัด เป็นเซตในเอกภพสัมพัทธ์ $\mathcal{U}$

ตัวอย่าง 1.2.5

ให้ $\mathcal{U}$ เป็นเซตของจำนวนเต็มลบ

$$A = \{x \mid x^2 = 4\}$$

หมายถึง A เป็นเซตของจำนวนเต็มลบที่ยกกำลังสองแล้วเท่ากับ 4 หรือ $A = \{-2\}$

ตัวอย่าง 1.2.6

กำหนดให้ $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ และให้ $A = \{1, 3, 6, 9\}, B = \{1, 4, 8\}, C = \{3\}$ และ $D = \{1, 3\}$ จงหา $(B \setminus A) \cup (C^{\complement} \cap D)$

วิธีทำ หาสมาชิกของแต่ละเซตโดยเริ่มทำในวงเล็บก่อน ดังนี้

$B \setminus A = \{4, 8\}$
$C^{\complement} = \{1, 2, 4, 5, 6, 7, 8, 9\}$
$C^{\complement} \cap D = \{1\}$
ดังนั้น $(B \setminus A) \cup (C^{\complement} \cap D) = \{1, 4, 8\}$

ตัวอย่าง 1.2.7

จากการสำรวจนักศึกษากลุ่มหนึ่งจำนวนทั้งหมด 30 คน พบว่า มี 20 คน ชอบเรียนวิชาแคลคูลัส และมี 25 คน ชอบเรียนวิชาทฤษฎีจำนวน อยากทราบว่านักศึกษาที่ชอบเรียนทั้งสองวิชามีทั้งหมดกี่คน

วิธีทำ ให้ A แทน เซตของนักศึกษาที่ชอบเรียนวิชาแคลคูลัส
และ B แทน เซตของนักศึกษาที่ชอบเรียนวิชาทฤษฎีจำนวน
จะได้ว่า $|\mathcal{U}| = 30, |A| = 20$ และ $|B| = 25$
จาก $|A \cup B| = |A| + |B| - |A \cap B|$
จะได้ว่า $30 = 20 + 25 - |A \cap B|$

$$|A \cap B| = 45 - 30 = 15$$

ดังนั้น นักศึกษาที่ชอบเรียนทั้งสองวิชามีทั้งหมด 15 คน

1.3 การพิสูจน์เบื้องต้น

ในหัวข้อนี้เราจะกล่าวถึงพื้นฐานทางตรรกศาสตร์และระเบียบวิธีการพิสูจน์เบื้องต้น เพื่อนำไปใช้เป็นเครื่องมือในการศึกษาทฤษฎีจำนวนในบทต่อ ๆ ไป เริ่มต้นด้วยประโยคหรือข้อความที่น่าสนใจทางคณิตศาสตร์เป็นข้อความที่เราตัดสินใจได้ว่า ต้องเป็นจริงหรือเป็นเท็จอย่างใดอย่างหนึ่งเท่านั้น จะเป็นทั้งสองอย่างไม่ได้ กล่าวคือถ้าข้อความใดไม่เป็นจริงแล้วข้อความนั้นต้องเป็นเท็จ ในนัยกลับกัน ถ้าข้อความใดไม่เป็นเท็จแล้วข้อความนั้นต้องเป็นจริง เรียกข้อความหรือประโยคเหล่านั้นว่า **ประพจน์ (proposition)** และมีตัวเชื่อมประพจน์ 4 ชนิดคือ (พัฒนี อุดมกะวานิช. 2559 : 2)

1. และ เขียนแทนด้วย $\wedge$
2. หรือ เขียนแทนด้วย $\vee$
3. ถ้า...แล้ว เขียนแทนด้วย $\rightarrow$
4. ก็ต่อเมื่อ เขียนแทนด้วย $\leftrightarrow$

สรุปค่าความจริงในแต่ละกรณีตามตารางต่อไปนี้ เมื่อ p และ q เป็นประพจน์ และ T แทนค่าความจริงเป็นจริง F แทนค่าความจริงเป็นเท็จ

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	F	T	F	F
F	F	F	F	T	T

ตารางที่ 1.2 แสดงค่าความจริงของประพจน์ที่ถูกเชื่อมทั้ง 4 แบบ

ต่อไปนี้จะกล่าวถึง **นิเสธของประพจน์ (negation of proposition)** หมายถึงประพจน์ที่มีค่าความจริงตรงข้ามกับประพจน์นั้น ให้ p เป็นประพจน์ แล้วนิเสธของประพจน์ของ p เขียนแทนด้วย $\sim p$ แสดงค่าความจริงได้ดังตารางต่อไปนี้

p	$\sim p$
T	F
F	T

ตารางที่ 1.3 แสดงค่าความจริงของ $\sim p$

สองประพจน์มีความหมายเดียวกันในทางตรรกศาสตร์จะเรียกว่า **สมมูลกันเชิงตรรกศาสตร์ (logically equivalent)** หรือกล่าวคือ ประพจน์ p **สมมูล (equivalent)** กับ q เขียนแทนด้วย $p \equiv q$ ก็ต่อเมื่อประพจน์ทั้งสองมีค่าความจริงเหมือนกันทุกกรณี ตัวอย่างเช่น

$$p \rightarrow q \equiv \sim q \rightarrow \sim p \quad \text{และ} \quad p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

เรียกว่า**กฎแย้งสลับที่ (contrapositive law)**

ประพจน์ที่มีรูปแบบที่มีค่าความจริงเป็นจริงเสมอเรียกว่า **สัจนิรันดร์ (tautology)** และเรียกนิเสธของสัจนิรันดร์ว่า **ข้อความขัดแย้ง (contradiction)** ตัวอย่างเช่น $\sim p \vee p$ และ $p \rightarrow p \vee p$ เป็นสัจนิรันดร์ และ $\sim p \wedge p$ เป็นข้อความขัดแย้ง

ให้ p แทนประพจน์ $x > 2$ เมื่อ $x \in \{1, 2, 3, 4\}$ พิจารณาค่าความจริงดังตาราง

x	$p : x > 2$	ค่าความจริง
1	$1 > 2$	F
2	$2 > 2$	F
3	$3 > 2$	T
4	$4 > 2$	T

ตารางที่ 1.4 แสดงค่าความจริงของ $p(x)$

จากตารางจะเห็นได้ว่าค่าความจริงของประพจน์ p เปลี่ยนไปตามค่า x นิยมใช้ $p(x)$ แทนประพจน์ p และเรียก $\{1,2,3,4\}$ ว่า**เอกภพสัมพัทธ์ (universe)** นิยมเขียนแทนด้วย $\mathcal{U}$ เมื่อกล่าวว่า

"มี x ใน $\mathcal{U}$ ที่สอดคล้อง $p(x)$"

ประพจน์นี้มีค่าความจริงเป็นจริงเพราะว่ามี $x = 3$ ซึ่งทำให้ $p(3)$ มีค่าความจริงเป็นจริง เขียนแทนคำว่า "มี" ด้วย $\exists$ ดังนั้นเขียนประพจน์ดังกล่าวได้เป็น $\exists x \in \mathcal{U}, p(x)$ ในทำนองเดียวกัน ถ้ากล่าวว่า

"ทุก ๆ x ใน $\mathcal{U}$ ที่สอดคล้อง $p(x)$"

ประพจน์นี้มีค่าความจริงเป็นเท็จ เพราะว่ามี $x = 1$ ที่ทำให้ $p(1)$ มีค่าความจริงเป็นเท็จ จะเขียนแทนคำว่า "ทุก ๆ" ด้วย $\forall$ ดังนั้นเขียนประพจน์ดังกล่าวได้เป็น $\forall x \in \mathcal{U},\ p(x)$ เรียก 2 สัญลักษณ์ดังกล่าวว่า **ตัวบ่งปริมาณ (quantifier)**

หลายครั้งมักจะพบประพจน์ที่ซับซ้อนมากขึ้นเช่น "มีจำนวนเต็มจำนวนหนึ่งซึ่งบวกกับทุกจำนวนเต็มแล้วเท่ากับศูนย์" เขียนสัญลักษณ์ได้เป็น

$$\exists x \in \mathbb{Z}\ \ \forall y \in \mathbb{Z},\ x + y = 0$$

ประพจน์ลักษณะนี้กล่าวได้ว่ามีตัวบ่งปริมาณ 2 ตัว

ต่อมาจะกล่าวถึงการหานิเสธของประพจน์ที่มีตัวบ่งประมาณ เช่น "ไม่มีจำนวนเต็ม x ที่สอดคล้อง $x^2 + x + 1 = 0$" เขียนเป็นสัญลักษณ์คือ

$$\sim \exists x \in \mathbb{Z},\ x^2 + x + 1 = 0$$

หมายถึง "ทุกจำนวนเต็ม x จะสอดคล้อง $x^2 + x + 1 \neq 0$" เขียนเป็นสัญลักษณ์คือ

$$\forall x \in \mathbb{Z},\ x^2 + x + 1 \neq 0$$

สรุปได้ดังนี้ ให้ $\mathcal{U}$ เป็นเอกภพสัมพัทธ์ของประพจน์ $p(x)$ นิเสธของตัวบ่งปริมาณนิยามโดย

นิเสธของ $\forall x \in \mathcal{U}, p(x)$ คือ $\sim \forall x \in \mathcal{U}, p(x) \equiv \exists x \in \mathcal{U}, \sim p(x)$
นิเสธของ $\exists x \in \mathcal{U}, p(x)$ คือ $\sim \exists x \in \mathcal{U}, p(x) \equiv \forall x \in \mathcal{U}, \sim p(x)$

ในหัวข้อนี้ผู้เขียนจะมีการนำเสนอวิธีการพิสูจน์ไว้ทั้งหมด 6 วิธี ประกอบไปด้วย

1. การพิสูจน์ข้อความแบบมีเงื่อนไข
2. การพิสูจน์โดยแจกแจงกรณี
3. การพิสูจน์ข้อความแบบผันกลับได้
4. การพิสูจน์โดยวิธีขัดแย้ง
5. การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว
6. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

1.3.1 การพิสูจน์ข้อความแบบมีเงื่อนไข

การพิสูจน์ข้อความที่อยู่ในรูปแบบมีเงื่อนไข $p \to q$ เรียกวิธีการพิสูจน์แบบนี้ว่า **การพิสูจน์ข้อความแบบมีเงื่อนไข (proof of conditional statements)** เราต้องการแสดงว่าข้อความ $p \to q$ เป็นจริงทุก ๆ กรณีหรือเป็นสัจนิรันดร์ นั่นคือแสดงว่าถ้า p เป็นจริง แล้ว q เป็นจริงเสมอ เขียนเป็นโครงพิสูจน์ได้ดังนี้

การพิสูจน์

สมมติ p เป็นจริง
$\vdots$
ดังนั้น q เป็นจริง (ข้อสรุป)

□

เราจะเรียกวิธีนี้ว่า**การพิสูจน์โดยวิธีตรง (direct proof)** นิยมใช้เครื่องหมาย □ วางไว้บรรทัดสุดท้ายเพื่อบอกว่าจบการพิสูจน์ ในส่วนที่ว่างเว้นไว้คือส่วนที่จะเติมรายละเอียดให้สมบูรณ์อาจจะได้จากนิยาม ทฤษฎีบทที่พิสูจน์มาก่อนหน้า หรือสัจพจน์ เพื่อให้นำไปสู่ข้อสรุปอย่างเป็นเหตุเป็นผลกัน เมื่อพิสูจน์โดยวิธีตรงไม่ได้เราจะใช้สมมูลที่ว่า $p \to q \equiv \sim q \to \sim p$ เราเรียกว่า **การพิสูจน์โดยวิธีการแย้งสลับที่ (contrapositive proof)** มีโครงการพิสูจน์ดังนี้

การพิสูจน์

สมมติ $\sim q$ เป็นจริง
$\vdots$
ดังนั้น $\sim p$ เป็นจริง

□

ก่อนจะได้ศึกษาตัวอย่างการพิสูจน์นั้น ผู้เขียนจะให้บทนิยามที่ต้องใช้ในการพิสูจน์ก่อนดังต่อไปนี้ (ธนัชยศ จำปาหวาย. 2559 : 7)

บทนิยาม 1.3.1

จำนวนคู่ (even number) คือจำนวนเต็มที่หารด้วยสองลงตัว หรือเราจะกล่าวว่า a เป็นจำนวนคู่ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k$ และ**จำนวนคี่ (odd number)** คือจำนวนเต็มที่ไม่ใช่จำนวนคู่ หรือเราจะกล่าวว่า a เป็นจำนวนคี่ ถ้ามีจำนวนเต็ม k ซึ่ง $a = 2k + 1$

ตัวอย่าง 1.3.1

จงพิสูจน์ว่า “ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่”

แนวคิด เขียนเป็นสัญลักษณ์จะได้เป็น

$$\forall n \in \mathbb{Z}, n \text{ เป็นจำนวนคู่ } \to n^2 \text{ เป็นจำนวนคู่}$$

มีโครงการพิสูจน์ดังนี้

การพิสูจน์

สมมติ n เป็นจำนวนคู่
$\vdots$
ดังนั้น n^2 เป็นจำนวนคู่

□

การพิสูจน์ ให้ n เป็นจำนวนเต็มใด ๆ สมมติว่า n เป็นจำนวนคู่ โดยบทนิยาม 1.3.1 จะได้ว่ามีจำนวนเต็ม k

ซึ่ง $n = 2k$ แล้วจะได้ว่า

$$n^2 = (2k)^2 = 4k^2 = 2\left(2k^2\right)$$

ให้ $p = 2k^2$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น p เป็นจำนวนเต็ม นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $n^2 = 2p$ จากบทนิยาม 1.3.1 สรุปได้ว่า n^2 เป็นจำนวนคู่ □

ตัวอย่าง 1.3.2

จงพิสูจน์ว่า "ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่"

แนวคิด เขียนเป็นสัญลักษณ์จะได้เป็น

$$\forall n \in \mathbb{Z}, n^2 \text{ เป็นจำนวนคู่ } \rightarrow n \text{ เป็นจำนวนคู่}$$

เราจะพิสูจน์โดยวิธีแย้งสลับที่ ดังนั้นเราจะทำการพิสูจน์ข้อความต่อไปนี้

$$\forall n \in \mathbb{Z}, n \text{ เป็นจำนวนคี่ } \rightarrow n^2 \text{ เป็นจำนวนคี่}$$

การพิสูจน์ ให้ n เป็นจำนวนเต็มใด ๆ สมมติว่า n เป็นจำนวนคี่ โดยบทนิยาม 1.3.1 จะได้ว่ามีจำนวนเต็ม k ซึ่ง $n = 2k + 1$ แล้วจะได้ว่า

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1$$

ให้ $p = 2k^2 + 2k$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น p เป็นจำนวนเต็ม นั่นคือมีจำนวนเต็ม p ซึ่งทำให้ $n^2 = 2p + 1$ จากบทนิยาม 1.3.1 สรุปได้ว่า n^2 เป็นจำนวนคี่ □

ตัวอย่าง 1.3.3

จงพิสูจน์ว่า "ถ้า a เป็นจำนวนคู่ แล้ว $a + 4$ เป็นจำนวนคู่"

การพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ สมมติว่า a เป็นจำนวนคู่
โดยบทนิยาม 1.3.1 จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k$ แล้วจะได้ว่า

$$a + 4 = (2k) + 4 = 2k + 4 = 2(k + 2)$$

เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น $k + 2$ เป็นจำนวนเต็ม
จากบทนิยาม 1.3.1 สรุปได้ว่า $a + 4$ เป็นจำนวนคู่ □

ตัวอย่าง 1.3.4

จงพิสูจน์ว่า "ถ้า ab เป็นจำนวนคู่ แล้ว a เป็นจำนวนคู่ หรือ b เป็นจำนวนคู่"

การพิสูจน์ ให้ a, b เป็นจำนวนเต็มใด ๆ สมมติว่า a และ b เป็นจำนวนคี่
โดยบทนิยาม 1.3.1 จะได้ว่ามีจำนวนเต็ม m, n ซึ่ง $a = 2m + 1$ และ $b = 2n + 1$
จะได้ว่า

$$ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$$

เนื่องจาก m, n เป็นจำนวนเต็ม ดังนั้น $2mn + m + n$ เป็นจำนวนเต็ม
จากบทนิยาม 1.3.1 สรุปได้ว่า ab เป็นจำนวนคี่ □

1.3.2 การพิสูจน์โดยแจกแจงกรณี

การพิสูจน์ข้อความในรูปแบบ $(p \vee q) \to r$ เนื่องจาก

$$(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$$

ต้องพิสูจน์ว่าทั้ง 2 กรณีเป็นจริงคือ

การพิสูจน์ กรณีที่ 1 $p \to r$

สมมติ p เป็นจริง
$\vdots$
ดังนั้น r เป็นจริง

กรณีที่ 2 $q \to r$

สมมติ q เป็นจริง
$\vdots$
ดังนั้น r เป็นจริง

□

เราเรียกว่า**การพิสูจน์โดยแจกแจงกรณี (poof by cases)**

ตัวอย่าง 1.3.5

จงพิสูจน์ว่า “ถ้า a เป็นจำนวนคู่ หรือ a เป็นจำนวนคี่ แล้ว $a^2 + a$ เป็นจำนวนคู่”

แนวคิด เขียนเป็นสัญลักษณ์จะได้เป็น

$$\forall n \in \mathbb{Z}, (a \text{ เป็นจำนวนคู่ } \vee \ a \text{ เป็นจำนวนคี่}) \to a^2 + a \text{ เป็นจำนวนคู่}$$

การพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ
กรณีที่ 1 สมมติว่า a เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k$ แล้ว

$$a^2 + a = (2k)^2 + 2k = 4k^2 + 2k = 2\left(2k^2 + k\right)$$

เนื่องจาก k เป็นจำนวนเต็ม ดังนั้น $2k^2 + k$ เป็นจำนวนเต็ม สรุปได้ว่า $a^2 + a$ เป็นจำนวนคู่
กรณีที่ 2 สมมติว่า a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม c ซึ่ง $a = 2c + 1$ แล้ว

$$a^2 + a = (2c+1)^2 + (2c+1) = 4c^2 + 4c + 1 + 2c + 1 = 2\left(2c^2 + 3c + 1\right)$$

เนื่องจาก c เป็นจำนวนเต็ม ดังนั้น $2c^2 + 3c + 1$ เป็นจำนวนเต็ม สรุปได้ว่า $a^2 + a$ เป็นจำนวนคู่ □

ตัวอย่าง 1.3.6

ถ้า n เป็นจำนวนเต็ม แล้ว $n^2 + 3n + 4$ เป็นจำนวนคู่

การพิสูจน์ ให้ n เป็นจำนวนเต็ม
กรณีที่ 1 n เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $n = 2k$ แล้ว

$$\begin{aligned} n^2 + 3n + 4 &= (2k)^2 + 3(2k) + 4 \\ &= 2\left(2k^2 + 3k + 2\right) \end{aligned}$$

จะเห็นว่า $2k^2 + 3k + 2$ เป็นจำนวนเต็ม ดังนั้น $n^2 + 3n + 4$ เป็นจำนวนคู่

กรณีที่ 2 n เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม c ซึ่ง $n = 2c + 1$ แล้ว

$$\begin{aligned} n^2 + 3n + 4 &= (2c+1)^2 + 3(2c+1) + 4 \\ &= 4c^2 + 4c + 1 + 6c + 3 + 4 \\ &= 4c^2 + 10c + 8 \\ &= 2\left(2c^2 + 5c + 4\right) \end{aligned}$$

จะเห็นว่า $2c^2 + 5c + 4$ เป็นจำนวนเต็ม สรุปได้ว่า $n^2 + 3n + 4$ เป็นจำนวนคู่ □

ตัวอย่าง 1.3.7

ถ้า a เป็นจำนวนเต็ม แล้ว $5a + a^2$ เป็นจำนวนคู่

การพิสูจน์ ให้ a เป็นจำนวนเต็ม

กรณีที่ 1 a เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k$ แล้ว

$$\begin{aligned} 5a + a^2 &= 5(2k) + (2k)^2 \\ &= 10k + 4k^2 \\ &= 2(5k + 2k^2) \end{aligned}$$

จะเห็นว่า $5k + 2k^2$ เป็นจำนวนเต็ม ดังนั้น $5a + a^2$ เป็นจำนวนคู่

กรณีที่ 2 a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม c ซึ่ง $a = 2c + 1$ แล้ว

$$\begin{aligned} 5a + a^2 &= 5(2c+1) + (2c+1)^2 \\ &= 10c + 5 + 4c^2 + 4c + 1 \\ &= 4c^2 + 14c + 6 \\ &= 2\left(2c^2 + 7c + 3\right) \end{aligned}$$

จะเห็นว่า $2c^2 + 7c + 3$ เป็นจำนวนเต็ม สรุปได้ว่า $5a + a^2$ เป็นจำนวนคู่ □

ตัวอย่าง 1.3.8

ให้ a, b เป็นจำนวนจริง ถ้า $a = 0$ หรือ $b = 0$ แล้ว $ab = 0$

การพิสูจน์ ให้ a, b เป็นจำนวนจริง

กรณีที่ 1 $a = 0$ จะได้ว่า

$$\begin{aligned} ab &= (0)b \\ &= 0 \cdot b \\ &= 0 \end{aligned}$$

ดังนั้น $ab = 0$

กรณีที่ 2 $b = 0$ จะได้ว่า

$$\begin{aligned} ab &= a(0) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

ดังนั้น $ab = 0$

สรุปได้ว่า ถ้า $a = 0$ หรือ $b = 0$ แล้ว $ab = 0$ □

1.3.3 การพิสูจน์ข้อความแบบผันกลับได้

ในตัวอย่าง 1.3.1 ได้พิสูจน์ว่า "ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่" ในตัวอย่าง 1.3.1 เมื่อ n เป็นจำนวนคู่ จะนำไปสู่ข้อสรุป n^2 เป็นจำนวนคู่ เมื่อตั้งคำถามต่อไปว่าในทางกลับกัน ข้อความนี้จะเป็นจริง หรือไม่ นั่นคือต้องพิสูจน์ว่า "ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่" ซึ่งได้พิสูจน์ไว้แล้วในตัวอย่าง 1.3.2 ทำให้ได้ว่าผลสามารถสรุปเหตุได้ด้วย อันหมายถึงการพิสูจน์ว่า

"n เป็นจำนวนคู่ **ก็ต่อเมื่อ** n^2 เป็นจำนวนคู่"

นั่นคือการพิสูจน์ในรูปแบบ $p \leftrightarrow q$ ซึ่งทำ 2 ขั้นตอนดังนี้

1. $p \to q$ เรียกว่าขั้น sufficient part (p เป็นเงื่อนไขที่เพียงพอสำหรับ q)
2. $q \to p$ เรียกว่าขั้น necessily part (p เป็นเงื่อนไขที่จำเป็นสำหรับ q)

เรียกว่า **การพิสูจน์แบบผันกลับได้ (poof of biconditional statements)**

ตัวอย่าง 1.3.9

ให้ n เป็นจำนวนเต็ม จงพิสูจน์ว่า n เป็นจำนวนคู่ ก็ต่อเมื่อ n^2 เป็นจำนวนคู่

การพิสูจน์ ให้ n เป็นจำนวนเต็ม
ขั้นตอนที่ 1 ต้องการพิสูจน์ว่า ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่ (แสดงการพิสูจน์ดังตัวอย่าง 1.3.1)
ขั้นตอนที่ 2 ต้องการพิสูจน์ว่า ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่ (แสดงการพิสูจน์ดังตัวอย่าง 1.3.2)
□

ตัวอย่าง 1.3.10

จงพิสูจน์ "จำนวนเต็ม a ใด ๆ a เป็นจำนวนคี่ ก็ต่อเมื่อ $a+3$ เป็นจำนวนคู่"

การพิสูจน์ ให้ a เป็นจำนวนเต็ม
ขั้นตอนที่ 1 สมมติ a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k+1$ แล้ว

$$a + 3 = (2k + 1) + 3 = 2(k + 2)$$

จะเห็นได้ว่า $k+2$ เป็นจำนวนเต็ม ดังนั้น $a+3$ เป็นจำนวนคู่
ขั้นตอนที่ 2 สมมติ $a+3$ เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม m ซึ่ง $a+3 = 2m$ แล้ว

$$a = 2m - 3 = 2(m - 2) + 1$$

เห็นได้ว่า $m-2$ เป็นจำนวนเต็ม ดังนั้น a เป็นจำนวนคี่ □

วัลลภ เหมวงษ์. (2562 : 61) ได้ให้ตัวอย่างการพิสูจน์ข้อความแบบผันกลับได้ ที่จะทำให้เข้าใจวิธีการพิสูจน์มากขึ้น ดังนี้

ตัวอย่าง 1.3.11

จงพิสูจน์ว่า "a^3 เป็นจำนวนคี่ ก็ต่อเมื่อ a เป็นจำนวนคี่"

การพิสูจน์ ให้ a เป็นจำนวนเต็ม

ขั้นตอนที่ 1 ($\Rightarrow$) จะพิสูจน์ว่า ถ้า a^3 เป็นจำนวนคี่ แล้ว a เป็นจำนวนคี่

ให้ a เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ที่ทำให้ $a = 2k$ จะได้ว่า

$$\begin{aligned} a^3 &= (2k)^3 \\ &= 8k^3 \\ &= 2(4k^3) \end{aligned}$$

ดังนั้น a^3 เป็นจำนวนเต็มคู่

ขั้นตอนที่ 2 ($\Leftarrow$) จะพิสูจน์ว่า ถ้า a เป็นจำนวนคี่ แล้ว a^3 เป็นจำนวนคี่

ให้ a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม m ที่ทำให้ $a = 2m + 1$ จะได้ว่า

$$\begin{aligned} a^3 &= (2m+1)^3 \\ &= 8m^3 + 12m^2 + 6m + 1 \\ &= 2(4m^3 + 6m^2 + 3m) + 1 \end{aligned}$$

ดังนั้น a^3 เป็นจำนวนเต็มคี่

สรุปได้ว่า a^3 เป็นจำนวนคี่ ก็ต่อเมื่อ a เป็นจำนวนคี่ □

ตัวอย่าง 1.3.12

จงพิสูจน์ว่า "a เป็นจำนวนคู่ ก็ต่อเมื่อ $a^2 - 1$ เป็นจำนวนคี่"

การพิสูจน์ ให้ a เป็นจำนวนเต็ม

ขั้นตอนที่ 1 ($\Rightarrow$) จะพิสูจน์ว่า ถ้า a เป็นจำนวนคู่ แล้ว $a^2 - 1$ เป็นจำนวนคี่

ให้ a เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ที่ทำให้ $a = 2k$ จะได้ว่า

$$\begin{aligned} a^2 - 1 &= (2k)^2 - 1 \\ &= 4k^2 - 1 \\ &= 4k^2 - 1 - 1 + 1 \\ &= 4k^2 - 2 + 1 \\ &= 2(2k^2 - 1) + 1 \end{aligned}$$

ดังนั้น $a^2 - 1$ เป็นจำนวนเต็มคี่

ขั้นตอนที่ 2 ($\Leftarrow$) จะพิสูจน์ว่า ถ้า $a^2 - 1$ เป็นจำนวนคี่ แล้ว a เป็นจำนวนคู่

ให้ a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม m ที่ทำให้ $a = 2m + 1$ จะได้ว่า

$$\begin{aligned} a^2 - 1 &= (2m+1)^2 - 1 \\ &= 4m^2 + 4m + 1 - 1 \\ &= 4m^2 + 4m \\ &= 2(2m^2 + 2m) \end{aligned}$$

ดังนั้น $a^2 - 1$ เป็นจำนวนเต็มคู่

สรุปได้ว่า a เป็นจำนวนคู่ ก็ต่อเมื่อ $a^2 - 1$ เป็นจำนวนคี่ □

1.3.4 การพิสูจน์โดยวิธีขัดแย้ง

เมื่อพิสูจน์โดยวิธีต่าง ๆ ที่ผ่านมาแล้วไม่สามารถทำได้ สามารถทำได้อีกทางหนึ่งคือ เมื่อต้องการพิสูจน์ข้อความ p เป็นจริงโดยการสมมติว่า $\sim p$ เป็นจริง แล้วนำไปสู่ข้อความขัดแย้ง c การพิสูจน์แบบนี้ได้จากสัจนิรันดร์ $(\sim p \to c) \to p$ เรียกวิธีนี้ว่า **การพิสูจน์โดยวิธีขัดแย้ง (poof by contradiction)** มีโครงการพิสูจน์ดังนี้

การพิสูจน์

สมมติ $\sim p$ เป็นจริง
$\vdots$
ดังนั้น เกิดข้อขัดแย้ง

□

ตัวอย่าง 1.3.13

จงพิสูจน์ว่า "ถ้า $a+3=b$ แล้ว $7(a+3)=7b$"

แนวคิด ให้ p แทนข้อความ "ถ้า $a+3=b$ แล้ว $7(a+3)=7b$" สมมติว่า $\sim p$ เป็นจริง นั่นคือ

$$a+3=b \text{ และ } 7(a+3) \neq 7b$$

การพิสูจน์ สมมติว่า $a+3=b$ และ $7(a+3)\neq 7b$ พิจารณา

$$\begin{aligned} 7(a+3) &\neq 7b \\ \frac{1}{7}\cdot 7(a+3) &\neq \frac{1}{7}\cdot 7b \\ a+3 &\neq b \end{aligned}$$

เกิดข้อขัดแย้ง ดังนั้นข้อความนี้เป็นจริง □

ตัวอย่าง 1.3.14

จงพิสูจน์ข้อความ "ไม่ว่า x จะเป็นจำนวนจริงใดก็ตามที่ไม่ใช่ศูนย์ จะได้ว่า $x^{-1}\neq 0$" โดยวิธีขัดแย้ง

แนวคิด ให้ p แทนข้อความ "$\forall x\in\mathbb{R}, x\neq 0 \to x^{-1}\neq 0$" สมมติว่า $\sim p$ เป็นจริง นั่นคือ

$$\exists x\in\mathbb{R}, x\neq 0 \wedge x^{-1}=0$$

การพิสูจน์ สมมติว่า มีจำนวนจริง x ซึ่ง $x\neq 0$ และ $x^{-1}=0$
เนื่องจาก $x\neq 0$ โดยสมบัติจำนวนจริงจะได้ว่า $x\,(x^{-1})=1$ แต่จากการสมมติ $x^{-1}=0$
จะได้ว่า $x\,(x^{-1})=x(0)=0$ เกิดข้อขัดแย้ง ดังนั้นข้อความนี้เป็นจริง □

ตัวอย่าง 1.3.15

จงพิสูจน์ข้อความ "ถ้า x,y เป็นจำนวนเต็ม แล้ว $x^2-4y\neq 2$" โดยวิธีขัดแย้ง

แนวคิด ให้ p แทนข้อความ "$\forall x,y\in\mathbb{Z}, x^2-4y\neq 2$" สมมติว่า $\sim p$ เป็นจริง นั่นคือ

$$\exists x,y\in\mathbb{Z}, x^2-4y=2$$

การพิสูจน์ สมมติว่า มีจำนวนจริง x และ y ซึ่ง $x^2 - 4y = 2$ แล้ว

$$x^2 = 2(2y + 1)$$

ดังนั้น x^2 เป็นจำนวนคู่ โดยตัวอย่าง 1.3.2 ทำให้ได้ว่า x เป็นจำนวนคู่
จะได้ว่ามีจำนวนเต็ม k ซึ่ง $x = 2k$ ทำให้ได้ว่า

$$\begin{aligned}(2k)^2 - 4y &= 2\\ 4k^2 - 4y &= 2\\ 2k^2 - 2y &= 1\\ 2\left(k^2 - y\right) &= 1\end{aligned}$$

จะได้ว่า 1 เป็นจำนวนคู่ เกิดข้อขัดแย้ง ดังนั้นข้อความนี้เป็นจริง □

ตัวอย่าง 1.3.16

กำหนดให้ A และ B เป็นเซตที่ไม่ใช่เซตว่าง จงพิสูจน์ว่า ถ้า $A \cap B = \varnothing$ แล้ว $A \not\subseteq B$

การพิสูจน์ สมมติว่า $A \cap B = \varnothing$ และ $A \subseteq B$
เนื่องจาก A และ B ไม่เป็นเซตว่าง แสดงว่ามีสมาชิกใน A
จะได้ว่าสมาชิกทุกตัวใน A เป็นสมาชิกใน B
ดังนั้น A และ B มีสมาชิกร่วมกัน นั่นคือมีสมาชิกใน $A \cap B$
จึงได้ว่า $A \cap B \neq \varnothing$ เกิดข้อขัดแย้งกับที่สมมติให้ $A \cap B = \varnothing$
สรุปได้ว่า ถ้า $A \cap B = \varnothing$ แล้ว $A \not\subseteq B$ □

ตัวอย่าง 1.3.17

จงใช้การพิสูจน์เพื่อหาข้อสรุปว่า $\sqrt{3} + \sqrt{6}$ น้อยกว่า หรือ มากกว่า $\sqrt{17}$

การพิสูจน์ **กรณีที่ 1** จะพิสูจน์ว่า $\sqrt{3} + \sqrt{6} < \sqrt{17}$
สมมติว่า $\sqrt{3} + \sqrt{6} \geq \sqrt{17}$ จะได้

$$\begin{aligned}(\sqrt{3} + \sqrt{6})^2 &\geq 17\\ 9 + 2\sqrt{18} &\geq 17\\ 2\sqrt{18} &\geq 8\\ 72 &\geq 64\end{aligned}$$

ไม่เกิดข้อขัดแย้ง ทำให้ได้ว่า $\sqrt{3} + \sqrt{6} < \sqrt{17}$ ไม่เป็นจริง
กรณีที่ 2 จะพิสูจน์ว่า $\sqrt{3} + \sqrt{6} > \sqrt{17}$
สมมติว่า $\sqrt{3} + \sqrt{6} \leq \sqrt{17}$ จะได้

$$\begin{aligned}(\sqrt{3} + \sqrt{6})^2 &\leq 17\\ 9 + 2\sqrt{18} &\leq 17\\ 2\sqrt{18} &\leq 8\\ 72 &\leq 64\end{aligned}$$

เกิดข้อขัดแย้ง ทำให้ได้ว่า $\sqrt{3} + \sqrt{6} > \sqrt{17}$ เป็นจริง
สรุปได้ว่า $\sqrt{3} + \sqrt{6}$ มากกว่า $\sqrt{17}$ □

1.3.5 การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว

การพิสูจ์ข้อความ $\exists! x \in \mathcal{U}, p(x)$ อ่านว่า มี x ใน $\mathcal{U}$ เพียงตัวเดียวเท่านั้นที่สอดคล้อง $p(x)$ ข้อความสมมูลกับ

$$(\exists x \in \mathcal{U}, p(x)) \wedge (\forall x, y \in \mathcal{U}, p(x) \wedge p(y) \to x = y)$$

ดังนั้นการพิสูจน์ $\exists! x \in \mathcal{U}, p(x)$ แบ่งการพิสูจน์ออกเป็น 2 ส่วนคือ

1. ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว (existence) $\exists x \in \mathcal{U}, p(x)$
2. ขั้นที่ 2 มีเพียงตัวเดียว (uniqueness) $\forall x, y \in \mathcal{U},\ p(x) \wedge p(y) \to x = y$

เรียกการพิสูจน์แบบนี้ว่า **การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว (uniqueness proofs)**

ตัวอย่าง 1.3.18

จงพิสูจน์ว่า "มีจำนวนจริง x เพียงตัวเดียวเท่านั้นซึ่ง $2^x = 1$"

แนวคิด เขียนสัญลักษณ์ได้เป็น $\exists! x \in \mathbb{R}, 2^x = 1$

การพิสูจน์ ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $x = 0$ จะได้ว่า

$$2^x = 2^0 = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $x, y \in \mathbb{R}$ สมมติ $2^x = 1$ และ $2^y = 1$ แล้ว

$$2^x = 1 = 2^y \quad \text{ดังนั้น} \quad 2^x = 2^y$$

จากสมบัติของเลขยกกำลังจะได้ว่า $x = y$ □

ตัวอย่าง 1.3.19

จงพิสูจน์ว่า "ทุก ๆ จำนวนจริง x จะมีจำนวนจริง y เพียงตัวเดียวซึ่ง $x + y = 1$"

แนวคิด เขียนสัญลักษณ์ได้เป็น $\forall x \in \mathbb{R}\ \exists! y \in \mathbb{R}, x + y = 1$

การพิสูจน์ ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $y = 1 - x$ ซึ่ง $y \in \mathbb{R}$ จะได้ว่า

$$x + y = x + (1 - x) = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $y, z \in \mathbb{R}$ สอดคล้อง $x + y = 1$ และ $x + z = 1$ แล้ว

$$x + y = 1 = x + z \quad \text{ดังนั้น} \quad x + y = x + z$$

จากสมบัติการตัดออกของการบวกบนจำนวนจริงจะได้ว่า $y = z$ □

ตัวอย่าง 1.3.20

จงพิสูจน์ว่า "มีจำนวนจริง x เพียงจำนวนจริงเดียวเท่านั้นที่ทำให้ $x^3 + 1 = 0$"

การพิสูจน์ ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $x = -1$ ซึ่ง $x \in \mathbb{R}$ จะได้ว่า

$$(-1)^3 + 1 = 0$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $x, y \in \mathbb{R}$ ซึ่ง $x^3 + 1 = 0$ และ $y^3 + 1 = 0$ จะได้

$$x^3 + 1 = y^3 + 1 \text{ ดังนั้น } x^3 = y^3$$

จากสมบัติของเลขยกกำลังจะได้ว่า $x = y$ □

ตัวอย่าง 1.3.21

กำหนดให้ $x \neq 0$ จงพิสูจน์ว่า "ตัวผกผันของทุก ๆ จำนวนจริง x จะมีเพียงตัวเดียวเท่านั้น"

การพิสูจน์ ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เนื่องจาก $x \neq 0$ เลือก $\frac{1}{x} \in \mathbb{R}$ จะได้ว่า

$$\frac{1}{x} \cdot x = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $x \neq 0, y \neq 0 \in \mathbb{R}$ ซึ่ง $\frac{1}{x} \cdot x = 1$ และ $\frac{1}{y} \cdot x = 1$ จะได้

$$\frac{1}{x} \cdot x = \frac{1}{y} \cdot x \text{ ดังนั้น } \frac{1}{x} = \frac{1}{y}$$

จากสมบัติของจำนวนจริงจะได้ว่า $x = y$ □

1.3.6 การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

หลักการอุปนัยเชิงคณิตศาสตร์ (principle of mathematical induction) แบ่งการพิสูจน์ออกเป็น 2 แบบ คือ หลักการอุปนัยเชิงคณิตศาสตร์แบบที่ 1 และหลักการอุปนัยเชิงคณิตศาสตร์แบบที่ 2 วิธีพิสูจน์หลักการอุปนัยเชิงคณิตศาสตร์แบบที่ 1 บางครั้งเรียกว่า **อุปนัยเชิงคณิตศาสตร์แบบอ่อน (weak mathematic induction)** และวิธีพิสูจน์หลักการอุปนัยเชิงคณิตศาสตร์แบบที่ 2 บางครั้งเรียกว่า **อุปนัยเชิงคณิตศาสตร์แบบเข้ม (strong mathematic induction)** (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 11, สมจิต โชติชัยสถิตย์. 2540 : 4-5, สมวงษ์ แปลงสพโชค. 2549 : 6)

ในการพิสูจน์หรือการให้เหตุผลทางทฤษฎีจำนวนนั้น หลักการพื้นฐานที่สำคัญมีอยู่ 2 ประการ คือ

1. ทุกสับเซตที่ไม่เท่ากับเซตว่างของ $\mathbb{N}$ จะมีสมาชิกตัวน้อยที่สุด ซึ่งหลักการนี้ได้กล่าวไว้แล้วในหลักการจัดอันดับดีข้างต้น

2. หลักอุปนัยเชิงคณิตศาสตร์ เป็นหลักการที่ใช้สำหรับพิสูจน์ประพจน์ต่าง ๆ ที่เป็นจริงสำหรับทุก ๆ ค่าของ n ที่เป็นจำนวนเต็มบวกซึ่งมีรายละเอียดดังนี้

ทฤษฎีบท 1.3.1 : หลักอุปนัยเชิงคณิตศาสตร์ที่ 1 (1^{st} Principle of Mathematical Induction)

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n ถ้า

(1) $P(1)$ เป็นจริง และ

(2) ถ้า $P(k)$ เป็นจริงแล้ว $P(k+1)$ เป็นจริง

สำหรับจำนวนเต็มบวก k ใด ๆ จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ ให้ $P(n)$ แทนข้อความที่สอดคล้องกับเงื่อนไข (1) และ (2)
ให้ $S = \{\, n \in \mathbb{N} \mid P(n) \text{ เป็นจริง} \,\}$
จาก (1) จะได้ $1 \in S$ และจาก (2) จะได้ว่า ถ้า $k \in S$ แล้ว $k+1 \in S$
ดังนั้น S เป็นเซตของจำนวนเต็มบวก
นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n □

ตัวอย่าง 1.3.22

จงพิสูจน์ว่า $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

การพิสูจน์ ให้ $P(n)$ แทน $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$
เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$
(1) $P(1)$ เป็นจริง เพราะว่า $1 = \dfrac{1(1+1)}{2}$
(2) สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1+2+3+\cdots+k = \dfrac{k(k+1)}{2}$
ดังนั้นจากสมบัติการเท่ากันของการบวก นำ $k+1$ บวกเข้าสองข้าง
จะได้ว่า
$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)\,[(k+1)+1]}{2} \end{aligned}$$
นั่นคือ $P(k+1)$ เป็นจริง
ดังนั้น $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$ □

ตัวอย่าง 1.3.23

พิจารณา
$$\begin{aligned} 1+3 &= 4 &&= 2^2 \\ 1+3+5 &= 9 &&= 3^2 \\ 1+3+5+7 &= 16 &&= 4^2 \\ 1+3+5+7+9 &= 25 &&= 5^2 \\ &\vdots \end{aligned}$$
จงพิสูจน์ว่า $1+3+5+\cdots+(2n-1) = n^2$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$

การพิสูจน์ ให้ $P(n)$ แทนข้อความ $1+3+5+7+\cdots+(2n-1) = n^2$
เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$
(1) $P(1)$ เป็นจริง เพราะว่า $1 = 1^2$
(2) สมมติว่า $P(k)$ เป็นจริง นั่นคือ $1+2+3+\cdots+(2k-1) = k^2$
ดังนั้นจากสมบัติการเท่ากันของการบวก นำ $2k+1$ บวกเข้าทั้งสองข้าง
จะได้ว่า $1+2+3+\cdots+(2k-1)+(2k+1) = k^2+(2k+1) = (k+1)^2$
นั่นคือ $P(k+1)$ เป็นจริง
ดังนั้น $1+3+5+7+\cdots+(2n-1) = n^2$ เป็นจริงสำหรับทุก $n \in \mathbb{N}$ □

ตัวอย่าง 1.3.24

จงพิสูจน์ว่า

$$1^2+2^2+3^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)$$

เป็นจริงสำหรับทุก $n\in\mathbb{N}$

การพิสูจน์ สำหรับจำนวนเต็มบวก n แต่ละตัว ให้ $P(n):1^2+2^2+3^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)$
เราจะต้องพิสูจน์ว่า $P(n)$ เป็นจริงสำหรับทุก $n\in\mathbb{N}$
(1) เนื่องจาก $1^2=1=\frac{1}{6}(1)(1+1)(2\cdot 1+1)$ ดังนั้น $P(1)$ เป็นจริง
(2) สมมติว่า $P(k)$ เป็นจริง
นั่นคือ $1^2+2^2+3^2+\cdots+k^2=\frac{1}{6}k(k+1)(2k+1)$
จะพิสูจน์ว่า $P(k+1)$ เป็นจริง
เนื่องจาก

$$\begin{aligned}1^2+2^2+3^2+\cdots+k^2&=\frac{1}{6}k(k+1)(2k+1)\\&=\frac{1}{6}k(k+1)(2k+1)+(k+1)^2\\&=\frac{1}{6}(k+1)\left(2k^2+7k+6\right)\\&=\frac{1}{6}(k+1)(k+2)(2k+3)\\&=\frac{1}{6}(k+1)[(k+1)+1][(2(k+1)+1)]\end{aligned}$$

ดังนั้น $P(k+1)$ เป็นจริง
เพราะฉะนั้น โดยการอุปนัยคณิตศาสตร์ สรุปได้ว่า $P(n)$ เป็นจริงสำหรับทุก $n\in\mathbb{N}$ □

ตัวอย่าง 1.3.25

สำหรับจำนวนเต็มบวก n ทุกตัว จงพิสูจน์ว่า

$$\frac{1}{(1)(2)}+\frac{1}{(2)(3)}+\frac{1}{(3)(4)}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$$

การพิสูจน์ สำหรับจำนวนเต็มบวก n แต่ละตัว ให้

$$P(n):\frac{1}{(1)(2)}+\frac{1}{(2)(3)}+\frac{1}{(3)(4)}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$$

(1) เนื่องจาก $\frac{1}{(1)(2)}=\frac{1}{2}=\frac{1}{1+1}$ ดังนั้น $P(1)$ เป็นจริง
(2) สมมติว่า $P(k)$ เป็นจริง นั่นคือ

$$\frac{1}{(1)(2)}+\frac{1}{(2)(3)}+\frac{1}{(3)(4)}+\cdots+\frac{1}{k(k+1)}=\frac{k}{k+1}$$

จะพิสูจน์ว่า $P(k+1)$ เป็นจริง

เนื่องจาก $\dfrac{1}{(1)(2)}+\dfrac{1}{(2)(3)}+\dfrac{1}{(3)(4)}+\cdots+\dfrac{1}{k(k+1)}+\dfrac{1}{(k+1)(k+2)}$

$$\begin{aligned}&=\frac{k}{(k+1)}+\frac{1}{(k+1)(k+2)}\\&=\frac{k^2+2k+1}{(k+1)(k+2)}\\&=\frac{(k+1)^2}{(k+1)(k+2)}\\&=\frac{k+1}{(k+1)+1}\end{aligned}$$

ดังนั้น $P(k+1)$ เป็นจริง

เพราะฉะนั้น โดยการอุปนัยเชิงคณิตศาสตร์ สรุปได้ว่า $P(n)$ เป็นจริงสำหรับจำนวนเต็มบวก n ทุกตัว □

การพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวกับจำนวนเต็มบวก n ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังต่อไปนี้

ทฤษฎีบท 1.3.2

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก n และ $a \in \mathbb{Z}$

(1) $P(a)$ เป็นจริง และ

(2) สำหรับจำนวนเต็มบวก k ซึ่ง $k \geq a$

ถ้า $P(k)$ เป็นจริงแล้ว $P(k+1)$ เป็นจริง จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq a$

การพิสูจน์ เนื่องจาก $n \geq a$ ดังนั้น $n = a, a+1, a+2, a+3, \ldots$

ถ้าให้ $m = n - a + 1$ จะได้ $m = 1, 2, 3, 4, \ldots$

และจะได้ $P(n)$ คือประโยคเดียวกับ $P(m+a-1)$

ในการพิสูจน์ว่าข้อความ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$

เป็นการเพียงพอที่เราจะพิสูจน์ว่าข้อความ $P(m+a-1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก m

ให้ $Q(m)$ แทนด้วย $P(m+a-1)$

จะได้ว่า $Q(1)$ แทนด้วย $P(1+a-1)$ ซึ่งก็คือ $P(a)$

$Q(k)$ แทนด้วย $P(k+a-1)$ และ $Q(k+1)$ แทนด้วย $P(k+1+a-1)$

(1) $Q(1)$ เป็นจริงเพราะ $P(a)$ เป็นจริงตามที่กำหนดให้ข้อ (1)

(2) ถ้า $Q(k)$ เป็นจริงจะได้ $P(k+a-1)$ เป็นจริงโดยที่ $k \geq 1$

จะได้ $k+a-1 \geq a$ เมื่อ $P(k+a-1)$ เป็นจริง

จากที่กำหนดให้ข้อ (2) จะได้ $P(k+1+a-1)$ เป็นจริง

นั่นคือ $Q(k+1)$ เป็นจริง

จาก (1) และ (2) สรุปว่า $Q(m)$ เป็นจริงสำหรับจำนวนเต็มบวก m

ดังนั้น $P(m+a-1)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก m ที่ $m \geq 1$

แต่ $n = m+a-1$ เมื่อ $m \geq 1$ จะได้ว่า $n \geq a$

จึงได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq a$ □

ตัวอย่าง 1.3.26

จงพิสูจน์ว่า $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 4$

การพิสูจน์ ให้ $P(n)$ แทนข้อความ $3^n > n^3$

(1) $P(4)$ เป็นจริง เพราะว่า $3^4 > 4^3$

(2) ถ้ายอมรับ $P(k)$ เป็นจริงเมื่อ $k \geq 4$

แล้วจะต้องแสดงว่า $P(k+1)$ เป็นจริง

สมมติว่า $P(k)$ เป็นจริง นั่นคือ $3^k > k^3$ เป็นจริง

จากสมบัติของจำนวนเต็ม นำ 3 คูณทั้งสองข้าง

จะได้ว่า $3^{k+1} > k^3 + k^3 + k^3 > k^3 + 3k^2 + 3k + 1$

ดังนั้น $3^{k+1} > (k+1)^3$ นั่นคือ $P(k+1)$ เป็นจริง

ดังนั้น $3^n > n^3$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 4$ □

ตัวอย่าง 1.3.27

จงพิสูจน์ว่า $n^n > n!$ สำหรับจำนวนเต็มบวก n ทุกตัวที่ $n \geq 2$

การพิสูจน์ สำหรับจำนวนเต็มบวก n แต่ละตัว ให้ $P(n) : n^n \geq n!$

(1) เนื่องจาก $2^2 = 4 > 2 = 2!$ ดังนั้น $P(2)$ เป็นจริง

(2) สมมติให้ $P(k)$ เป็นจริงสำหรับจำนวนเต็มบวก k ทุกตัวที่ $k \geq 2$ จะได้ว่า $k^k > k!$

ต่อไปจะแสดงว่า $P(k+1)$ เป็นจริง

เนื่องจาก $(k+1)^{k+1} = (k+1)^k(k+1) > k^k(k+1) > k!(k+1) = (k+1)!$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

ดังนั้น โดยการอุปนัยเชิงคณิตศาสตร์ เราสรุปได้ว่า $P(n)$ เป็นจริง

สำหรับจำนวนเต็ม n ทุกตัวที่ $n \geq 2$ □

ตัวอย่าง 1.3.28

จงพิสูจน์ว่า $2^n \geq 2(n+1)$ ทุกค่า $n \geq 5$

การพิสูจน์ ให้ $P(n)$ แทนข้อความ "$2^n \geq 2(n+1)$"

(1) จะแสดงว่า $P(5)$ เป็นจริง

เพราะว่า $2^5 = 32 \geq 2(5+1)$ จะได้ว่า $P(5)$ เป็นจริง

(2) จะแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 5$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 5$ เพราะฉะนั้น $2^k \geq 2(k+1)$

พิจารณา $2^{k+1} = 2(2^k)$

$$\geq 2\,(2(k+1))$$
$$= 2\,((k+1)+k+1)$$
$$\geq 2\,((k+1)+1)$$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยการอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \geq 5$

เพราะฉะนั้น $2^n \geq 2(n+1)$ ทุกค่า $n \geq 5$ □

ทฤษฎีบท 1.3.3 : หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 (2^{nd} Principle of Mathematical Induction)

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม n ถ้า

(1) $P(1)$ เป็นจริง และ

(2) ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก k ที่ $k < m$ แล้ว $P(m)$ เป็นจริง

จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ ให้ $S = \{n \in \mathbb{N} \mid P(n) \text{ เป็นเท็จ}\}$

สมมติว่า $S \neq \varnothing$ โดยหลักการจัดอันดับดี จะมี $m \in S$

ซึ่ง m เป็นจำนวนเต็มบวกที่น้อยที่สุดที่อยู่ใน S

ดังนั้น $P(m)$ เป็นเท็จ

เนื่องจาก $P(1)$ เป็นจริง ดังนั้น $m > 1$

แสดงว่า $P(k)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก k ที่ $k < m$

โดยสมมติฐานข้อ (2) จะได้ว่า $P(m)$ เป็นจริงซึ่งผลที่ได้ขัดแย้งกับ $m \in S$

ดังนั้นที่สมมติว่า $S \neq \varnothing$ เป็นเท็จ แสดงว่า $S \neq \varnothing$

นั่นคือ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n □

หมายเหตุ

1. โดยทั่วไปนิยมเรียกการพิสูจน์หลักอุปนัยเชิงคณิตศาสตร์ที่ 2 นี้ว่าหลักอุปนัยอย่างเข้ม (Strong Induction)
2. เราสามารถแสดงได้ว่าการพิสูจน์โดยใช้ทฤษฎีบท 1.3.3 อาจนำไปใช้พิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนเต็ม n ใด ๆ ที่ $n \geq a$ เมื่อ $a \in \mathbb{Z}$ ซึ่งมีรายละเอียดดังนี้

หลักอุปนัยอย่างเข้ม (Strong Induction)

ให้ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็มบวก $a \in \mathbb{Z}$ ซึ่ง

(1) $P(a)$ เป็นจริง

(2) ถ้า $P(a), P(a+1), P(a+2), \ldots, P(m-1)$ เป็นจริง

แล้ว $P(m)$ เป็นจริง จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็ม n ที่ $n \geq a$

ตัวอย่าง 1.3.29

พิจารณาลำดับ $1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$ ลำดับนี้เรียกว่า **ลำดับลูคัส** (Lucus sequence) โดยที่ $a_1 = 1, a_2 = 3$ และ $a_n = a_{n-1} + a_{n-2}$ สำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 3$ จงพิสูจน์ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ ให้ $P(n)$ แทน $a_n < \left(\frac{7}{4}\right)^n$

(1) $n = 1$ จะได้ $a_1 = 1 < \left(\frac{7}{4}\right)^1$ ดังนั้น $P(1)$ เป็นจริง

$n = 2$ จะได้ $a_2 = 3 < \left(\frac{7}{4}\right)^2$ ดังนั้น $P(2)$ เป็นจริง

(2) สมมติ $P(k)$ เป็นจริงสำหรับทุก k ที่ $k < m$ เมื่อ $m \geq 3$
ดังนั้น $a_{m-1} < \left(\frac{7}{4}\right)^{m-1}$ และ $a_{m-2} < \left(\frac{7}{4}\right)^{m-2}$
แต่ $a_m = a_{m-1} + a_{m-2} < \left(\frac{7}{4}\right)^{m-1} + \left(\frac{7}{4}\right)^{m-2} = \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}+1\right)$
ดังนั้น $a_m < \left(\frac{7}{4}\right)^{m-2}\left(\frac{11}{4}\right) < \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}\right)^2 < \left(\frac{7}{4}\right)^m$ เป็นจริง
นั่นคือ $P(m)$ เป็นจริง
โดยอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปได้ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n □

ตัวอย่าง 1.3.30

จงพิสูจน์ว่าทุก ๆ จำนวนเต็มบวก n จะมี t และ m เพียงคู่เดียวเท่านั้นที่ทำให้

$$n = 2^t \cdot m$$

โดยที่ $t \in \{0, 1, 2, \ldots\}$ และ m เป็นจำนวนเต็มคี่

การพิสูจน์ เพราะว่า $1 = 2^0 \cdot 1$ จะได้ว่า มี 0 และ 1 เพียงคู่เดียวเท่านั้นที่ทำให้ $1 = 2^0 \cdot 1$
สมมติว่า $n > 1$ จะได้ว่า n เป็นจำนวนเต็มคี่ หรือ n เป็นจำนวนเต็มคู่
ถ้า n เป็นจำนวนเต็มคี่ จะได้ว่า $n = 2^0 \cdot n$
และมี $t = 0$ และ $m = n$ เพียงคู่เดียวที่ทำให้ $n = 2^t \cdot m$
ถ้า n เป็นจำนวนเต็มคู่ แล้วจะมีจำนวนเต็มบวก $m < n$ ซึ่ง $n = 2m$
สมมติว่ามี r และ k เพียงคู่เดียวเท่านั้นที่ทำให้ $m = 2^r \cdot k$
โดยที่ $r \in \{0, 1, 2, \ldots\}$ และ k เป็นจำนวนเต็มคี่
ดังนั้น $n = 2m = 2 \cdot 2^r \cdot k = 2^{r+1} \cdot k$
เนื่องจาก n เป็นจำนวนเต็มคู่ และถ้า $n = 2^{t+1} \cdot h = 2^{r+1} \cdot k$
โดยที่ h และ k เป็นจำนวนเต็มคี่
จะได้ว่า $2^t \cdot h = 2^r \cdot k$ โดยสมมติฐานแสดงว่า $t = r$ และ $h = k$
แสดงว่า n สามารถเขียนในรูป $2^{r+1} \cdot k$ ได้เพียงแบบเดียว
เพราะฉะนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2
สรุปว่า ทุกจำนวนเต็มบวก n จะมี $t \in \{0, 1, 2, \ldots\}$ และ m เป็นจำนวนเต็มคี่
เพียงคู่เดียวเท่านั้นที่ทำให้ $n = 2^t \cdot m$ □

ตัวอย่าง 1.3.31

ให้ a_n เป็นลำดับ ซึ่งกำหนดโดย $a_1 = 1, a_2 = 8$ และ $a_n = a_{n-1} + 2a_{n-2}$ สำหรับ $n \geq 3$
จงพิสูจน์ว่า $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ สำหรับทุก $n \in \mathbb{N}$

การพิสูจน์ ให้ $P(n) : a_n = 3 \cdot 2^{n-1} + 2(-1)^n$
(1) $n = 1$ จะได้ $3 \cdot 2^0 + 2 \cdot (-1)^1 = 1$ ดังนั้น $P(1)$ เป็นจริง
$n = 2$ จะได้ $3 \cdot 2^1 + 2 \cdot (-1)^2 = 8$ ดังนั้น $P(2)$ เป็นจริง
(2) สมมติ $P(k)$ เป็นจริงสำหรับทุก k ที่ $k < m$ เมื่อ $m \geq 3$
ดังนั้น $a_{m-1} = 3 \cdot 2^{m-2} + 2(-1)^{m-1}$
และ $a_{m-2} = 3 \cdot 2^{m-3} + 2(-1)^{m-2}$

จะได้ว่า $a_m = a_{m-1} + 2a_{m-2}$

$$\begin{aligned}
&= 3 \cdot 2^{m-2} + 2(-1)^{m-1} + 2(3 \cdot 2^{m-3} + 2(-1)^{m-2}) \\
&= 3 \cdot 2^{m-2} + 2(-1)^{m-1} + 3 \cdot 2^{m-2} + 2 \cdot 2(-1)^{m-2} \\
&= 3 \cdot (2^{m-2} + 2^{m-2}) + 2 \cdot \left((-1)^{m-1} + 2(-1)^{m-2}\right) \\
&= 3 \cdot 2 \cdot 2^{m-2} + 2(-1)^{m} \cdot \left((-1)^{-1} + 2(-1)^{-2}\right) \\
&= 3 \cdot 2^{m-1} + 2(-1)^{m}
\end{aligned}$$

ดังนั้น $P(m)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปได้ว่า $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ สำหรับทุก $n \in \mathbb{N}$ □

ตัวอย่าง 1.3.32

ให้ a_n เป็นลำดับ ซึ่งกำหนดโดย $a_1 = 1, a_2 = 3$ และ $a_n = 2a_{n-1} - a_{n-2}$ สำหรับ $n \geq 3$ จงพิสูจน์ว่า $a_n = 2n - 1$ สำหรับทุก $n \in \mathbb{N}$

การพิสูจน์ ให้ $P(n) : a_n = 2n - 1$

(1) $n = 1$ จะได้ $2(1) - 1 = 1$ ดังนั้น $P(1)$ เป็นจริง

$n = 2$ จะได้ $2(2) - 1 = 3$ ดังนั้น $P(2)$ เป็นจริง

(2) สมมติ $P(k)$ เป็นจริงสำหรับทุก k ที่ $k < m$ เมื่อ $m \geq 3$

ดังนั้น $a_{m-1} = 2(m-1) - 1$ และ $a_{m-2} = 2(m-2) - 1$

จะได้ว่า $a_m = 2a_{m-1} - a_{m-2}$

$$\begin{aligned}
&= 2\left(2(m-1) - 1\right) - 2(m-2) + 1 \\
&= 2\left(2m - 3\right) - 2m + 5 \\
&= 4m - 6 - 2m + 5 \\
&= 2m - 1
\end{aligned}$$

ดังนั้น $P(m)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ที่ 2 สรุปได้ว่า $a_n = 2n - 1$ สำหรับทุก $n \in \mathbb{N}$ □

1.4 สมบัติจำนวนเต็ม

ในการศึกษาทฤษฎีจำนวนเบื้องต้นนั้น เรามุ่งเน้นการศึกษาสมบัติของจำนวนนับและจำนวนเต็มตลอดจนการพิสูจน์ข้อความที่เกี่ยวข้องกับจำนวนนับและจำนวนเต็ม และยังให้ผู้เรียนได้นำความรู้ที่ได้จากการศึกษาทฤษฎีจำนวนเพื่อเป็นพื้นฐานในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

ในหัวข้อนี้จะกล่าวถึง ระบบของจำนวนเต็ม ซึ่งเป็นระบบที่เราสามารถศึกษาสมบัติได้มากมาย และเอกภพสัมพัทธ์ที่เราจะอ้างถึงคือ เซตของจำนวนเต็ม $\mathbb{Z}$ โดยที่

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

ระบบจำนวนเต็มคือระบบที่ประกอบด้วยเซตของจำนวนเต็ม $\mathbb{Z}$ พร้อมด้วยการดำเนินการ "+" และ "." ที่สอดคล้องกับสัจพจน์ที่แบ่งได้ 3 กลุ่ม ดังนี้

กลุ่มที่ 1 สมบัติทางพีชคณิต (algebraic property)

กลุ่มที่ 2 สมบัติไตรวิภาค (trichotomy law)

กลุ่มที่ 3 หลักการจัดอันดับอย่างดี (well ordering principle)

สำหรับหัวข้อนี้เราจะกล่าวถึงระบบจำนวนเต็ม ซึ่งประกอบด้วยเซตของจำนวนเต็ม และการดำเนินการทวิภาค (binary operation) ได้แก่ การบวก (addition) แทนด้วย $+$ และการคูณ (multiplication) แทนด้วย $\cdot$ สมบัติเบื้องต้นของเซตของจำนวนเต็มภายใต้การดำเนินการบวกและการคูณ มีดังนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 7, พิมพ์เพ็ญ เวชชาชีวะ. 2558 : 33-42, Raji W. 2013 : 8-9, สุเทพ จันทร์สมศักดิ์. 2538 : 1-2, คณะกรรมการกลุ่มผลิตชุดวิชาตรรกศาสตร์ เซตและทฤษฎีจำนวน. 2529 : 279-282, สุภา สุจริตพงศ์. 2523 : 73-76)

สมบัติทางพีชคณิต (Algebraic properties)

P_1 : สมบัติปิด (closure laws)
สำหรับการบวก : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $a + b = c$
สำหรับการคูณ : ทุก ๆ $a, b \in \mathbb{Z}$ จะมี $c \in \mathbb{Z}$ เพียงตัวเดียวเท่านั้น ที่ทำให้ $a \cdot b = c$

P_2 : สมบัติการเปลี่ยนกลุ่ม (associative laws)
สำหรับการบวก : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a + b) + c = a + (b + c)$
สำหรับการคูณ : ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

P_3 : สมบัติการมีเอกลักษณ์ (existence of identities)
สำหรับการบวก : มี $0 \in \mathbb{Z}$ ซึ่ง $0 + a = a + 0 = a$ สำหรับทุก $a \in \mathbb{Z}$
สำหรับการคูณ : มี $1 \in \mathbb{Z}$ ซึ่ง $1 \cdot a = a \cdot 1 = a$ สำหรับทุก $a \in \mathbb{Z}$

P_4 : สมบัติการมีอินเวอร์สการบวก (existence of additive inverse)
สำหรับแต่ละ $a \in \mathbb{Z}$ จะมี $-a \in \mathbb{Z}$ ซึ่ง $(-a) + a = a + (-a) = 0$

P_5 : สมบัติการสลับที่ (commutative laws)
สำหรับการบวก : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a + b = b + a$
สำหรับการคูณ : ถ้า $a, b \in \mathbb{Z}$ แล้ว $a \cdot b = b \cdot a$

P_6 : สมบัติการแจกแจง (distributive law)
ถ้า $a, b, c \in \mathbb{Z}$ แล้ว $a \cdot (b + c) = a \cdot b + a \cdot c$ และ $(a + b) \cdot c = a \cdot c + b \cdot c$

ข้อตกลง เราจะใช้สัญลักษณ์ $(\mathbb{Z}, +, \cdot)$ แทนระบบจำนวนเต็ม และเราจะเขียน ab แทน $a \cdot b$ และ $a - b$ แทน $a + (-b)$

จากระบบจำนวนเต็มพร้อมด้วยสมบัติ 6 ข้อ เราอาจนำไปพิสูจน์หรือให้เหตุผลต่อความจริงดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.4.1

ข้อความต่อไปนี้เป็นจริง
1. ในระบบจำนวนเต็มจะมี 0 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการบวก
2. ในระบบจำนวนเต็มจะมี 1 เพียงตัวเดียวเท่านั้นที่เป็นสมาชิกเอกลักษณ์ของการคูณ
3. สำหรับจำนวนเต็ม a ใด ๆ $a0 = 0a = 0$
4. ถ้า $a, b, c \in \mathbb{Z}$ และ $a + b = a + c$ แล้ว $b = c$

การพิสูจน์ 1. สมมติว่า $x \in \mathbb{Z}$ ซึ่ง $a + x = a$ สำหรับจำนวนเต็ม a ใด ๆ
ดังนั้น $0 = 0 + x = x$ นั่นคือ $0 = x$

2. สมมติว่ามี $x \in \mathbb{Z}$ ซึ่ง $ax = a$ สำหรับจำนวนเต็ม a ใด ๆ
ดังนั้น $1 = 1x = x$ นั่นคือ $1 = x$

3. ให้ $a \in \mathbb{Z}$ จะได้ว่า $a0 = a(0 + 0) = a0 + a0$ ดังนั้น $a0 = 0$
และในทำนองเดียวกัน จะได้ว่า $0a = (0 + 0)a = 0a + 0a$ นั่นคือ $0a = 0$

4. สมมติว่า $a + b = a + c$ และให้ x แทนอินเวอร์สการบวกของ a
จะได้ว่า $b = 0 + b = (x + a) + b = x + (a + b) = x + (a + c)$
ดังนั้น $b = (x + a) + c = 0 + c = c$ □

ทฤษฎีบท 1.4.2

ข้อความต่อไปนี้เป็นจริง

1. สำหรับจำนวนเต็ม a ใด ๆ a จะมีสมาชิกอินเวอร์สของการบวกเพียงตัวเดียวเท่านั้น
2. สำหรับจำนวนเต็ม a ใด ๆ อินเวอร์สการบวกของ $-a$ คือ a
3. สำหรับจำนวนเต็ม a, b ใด ๆ จะได้ $(-a)b = a(-b) = -(ab)$ และ $(-a)(-b) = ab$

การพิสูจน์ 1. สมมติว่า $b \in \mathbb{Z}$ ซึ่ง $a + b = b + a = 0$ สำหรับจำนวนเต็ม a ใด ๆ
ดังนั้น $b = b + 0 = b + [a + (-a)] = (b + a) + (-a) = 0 + (-a) = -a$
นั่นคือ $b = -a$

2. ให้ $a \in \mathbb{Z}$ จะได้ว่า $(-a) + [-(-a)] = (-a) + a = 0$
ดังนั้น $-(-a) = a$
นั่นคือ อินเวอร์สการบวกของ $-a$ คือ a

3. ให้ $a, b \in \mathbb{Z}$ จะได้ว่า $ab+(-a)b = [a+(-a)]b = 0b = a0 = a[b+(-b)] = ab+a(-b)$
นั่นคือ $(-a)b = a(-b)$
พิสูจน์ในทำนองเดียวกันจะได้ว่า $(-a)b = -(ab)$
ต่อไปพิจารณา $(-a)(-b) + [-(-a)(-b)] = 0(-b) = ab + (-a)b$
เนื่องจาก $-(-a)(-b) = (-a)b$ ดังนั้น $(-a)(-b) = ab$ □

สมบัติไตรวิภาค (Trichotomy law)

P_7 : สมบัติไตรวิภาค
มีสับเซต $\mathbb{N}$ ของ $\mathbb{Z}$ ที่มีสมบัติว่า

1. $0 \notin \mathbb{N}$
2. ถ้า $a, b \in \mathbb{N}$ แล้ว $a + b \in \mathbb{N}$ และ $ab \in \mathbb{N}$
3. ถ้า $x \in \mathbb{Z}$ แล้ว $x \in \mathbb{N}$ หรือ $x = 0$ หรือ $-x \in \mathbb{N}$

สมบัติไตรวิภาคนี้มีประโยชน์ในการกำหนดนิยามเพื่อเปรียบเทียบสมาชิก 2 ตัวใด ๆ ในแง่ “มากกว่า” หรือ “น้อยกว่า”

บทนิยาม 1.4.1

ให้ $a, b \in \mathbb{Z}$ เรากล่าวว่า
a มากกว่า b เขียนแทนด้วย $a > b$ ก็ต่อเมื่อ $a - b \in \mathbb{N}$ และ
a น้อยกว่า b เขียนแทนด้วย $a < b$ ก็ต่อเมื่อ $b > a$

ทฤษฎีบท 1.4.3

ให้ $a, b, c, x, y \in \mathbb{Z}$ จะได้ว่า
1. ถ้า $a > b$ แล้ว $a + c > b + c$
2. ถ้า $a > b$ และ $b > c$ แล้ว $a > c$
3. ถ้า $a > b$ และ $x > y$ แล้ว $a + x > b + y$
4. ถ้า $a > b$ และ $x > 0$ แล้ว $ax > bx$
5. ถ้า $a > b$ และ $x < 0$ แล้ว $ax < bx$

การพิสูจน์ 1. เพราะว่า $(a + c) - (b + c) = a - b \in \mathbb{N}$ ดังนั้น $a + c > b + c$ □

สำหรับการพิสูจน์ในข้ออื่น ๆ สามารถกระทำได้โดยการใช้สมบัติไตรวิภาคของระบบจำนวนเต็ม จึงขอละไว้เพื่อเป็นแบบฝึกหัด

ทฤษฎีบท 1.4.4

ให้ $a, b, c, x, y \in \mathbb{Z}$ จะได้ว่า
1. ถ้า $a < b$ แล้ว $a + c < b + c$
2. ถ้า $a < b$ และ $b < c$ แล้ว $a < c$
3. ถ้า $a < b$ และ $x < y$ แล้ว $a + x < b + y$
4. ถ้า $a < b$ และ $x > 0$ แล้ว $ax < bx$
5. ถ้า $a < b$ และ $x < 0$ แล้ว $ax > bx$

การพิสูจน์ ขอให้ผู้เรียนพิสูจน์เป็นแบบฝึกหัด □

ทฤษฎีบทต่อไปจะแสดงว่าระบบจำนวนเต็มจะมีเซตที่สอดคล้องกับสัจพจน์ P_7 เพียงเซตเดียวเท่านั้น คือ $\mathbb{N} = \{1, 2, 3, \ldots\}$ นั่นคือ จากบทนิยามการเปรียบเทียบสมาชิกใน $\mathbb{Z}$ ในแง่ "มากกว่า" หรือ "น้อยกว่า" ซึ่งเราสามารถเปรียบเทียบได้เพียงแบบเดียวเท่านั้น (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 9-11, กัลยาณี ไชยวรินทรกุล. 2522 : 42)

ทฤษฎีบท 1.4.5

$\mathbb{Z}$ มีเพียงสับเซตเดียวเท่านั้นคือ $\mathbb{N}$ ที่สอดคล้องกับสมบัติไตรวิภาค

การพิสูจน์ สมมติว่า $S \subseteq \mathbb{Z}$ ที่สอดคล้องกับสมบัติไตรวิภาค จะได้ว่า $1 \in S$ หรือ $-1 \in S$
ถ้า $-1 \in S$ จะได้ว่า $(-1)(-1) = 1 \in S$ และ $1 + (-1) = 0 \in S$
ซึ่งเป็นไปไม่ได้ขัดแย้งกับ $0 \notin S$ ดังนั้น $1 \in S$
ให้ $n \in \mathbb{N}$ จะได้ว่า $n = 1 + 1 + 1 + \cdots + 1$ (n ตัว)
ดังนั้น $n \in S$ แสดงว่า $\mathbb{N} \subseteq S$ นั่นคือ $S = \mathbb{N}$ หรือ $S \setminus \mathbb{N} \neq \varnothing$
สมมติ $S \setminus \mathbb{N} \neq \varnothing$ จะได้ว่ามี $x \in S$ แต่ $x \notin \mathbb{N}$

ดังนั้น $x \neq 0$ นั่นคือ $-x \in \mathbb{N}$ จาก $x \in S$ และ $-x \in \mathbb{N} \subseteq S$
แสดงว่า $x + (-x) = 0 \in S$ ซึ่งเป็นไปไม่ได้จึงเกิดขัดแย้ง ดังนั้น $S = \mathbb{N}$ □

ทฤษฎีบท 1.4.6

ให้ $a, b \in \mathbb{Z}$ ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$

การพิสูจน์ ถ้า $a \neq 0$ และ $b \neq 0$ จากสมบัติไตรวิภาคจะได้ว่า $a \in \mathbb{N}$ หรือ $-a \in \mathbb{N}$
และ $b \in \mathbb{N}$ หรือ $-b \in \mathbb{N}$
ดังนั้น $ab \in \mathbb{N}$ หรือ $-(ab) \in \mathbb{N}$
นั่นคือ $ab \neq 0$ □

บทแทรก 1.4.1

ให้ $a, b, c \in \mathbb{Z}$ ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $b = c$

การพิสูจน์ สมมติว่า $ab = ac$ และ $a \neq 0$
จะได้ว่า $ab - ac = a(b - c) = 0$
ดังนั้น $b - c = 0$ นั่นคือ $b = c$ □

จากทฤษฎีบท 1.4.6 และบทแทรก 1.4.1 เราพบว่า สมบัติการตัดออกสำหรับการคูณ หรือสมบัติการไม่มีตัวหารของศูนย์แท้ (no proper zero divisor) ในระบบจำนวนเต็ม เป็นผลสืบเนื่องจากสัจพจน์ P_1 ถึง P_6

เพื่อให้การศึกษาสมบัติของจำนวนเต็มมีประสิทธิภาพมากขึ้นและเพื่อการพิสูจน์ข้อความ ต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มมีความสมเหตุสมผลมากขึ้น เราจึงกำหนดว่าเซตของจำนวนเต็มบวกมีสมบัติหลักการจัดอันดับดี

หลักการจัดอันดับดี (well ordering principle)

P_8 : ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า มี $x \in S$ ซึ่ง $x \leq a$ สำหรับทุก $a \in S$

สมบัติการจัดอันดับดีในระบบจำนวนเต็ม นำไปสู่ทฤษฎีบทที่น่าสนใจ ซึ่งสามารถนำไปประยุกต์ใช้ในการพิสูจน์ทฤษฎีบทต่าง ๆ ที่จะกล่าวถึงบทต่อ ๆ ไป

ทฤษฎีบท 1.4.7

ไม่มีจำนวนเต็มใดอยู่ระหว่าง 0 กับ 1

การพิสูจน์ ให้ $T = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ และสมมติว่า $T \neq \varnothing$
จากหลักการจัดอันดับอย่างดี จะได้ว่ามี $m \in T$ ซึ่ง $m \leq x$ สำหรับทุก $x \in T$
ดังนั้น $0 < m < 1$ นั่นคือ $0 < m^2 < m$ แสดงว่า $m^2 \in T$
จึงเกิดข้อขัดแย้งกับการเลือก m ที่เป็นจำนวนเต็มบวกที่น้อยที่สุดใน T
นั่นคือ $T = \varnothing$ □

ทฤษฎีบท 1.4.8

สมบัติของอาร์คีมิดีส (Archimedean property) สำหรับจำนวนเต็มบวก a และ b จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

การพิสูจน์ สมมติว่าข้อความในทฤษฎีบทไม่จริง
นั่นคือ มีจำนวนเต็มบวก a, b และทุกจำนวนเต็มบวก $n, na < b$
ให้ $S = \{b - na \mid n \in \mathbb{N}\}$ จากสมมติฐานจะเห็นว่า $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$
จากหลักการจัดอันดับดีจะมี $k \in \mathbb{N}$ ซึ่ง $m = b - ka$
ที่ m เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S
จาก $b - (k+1)a \in S$ และ $[b - (k+1)a] - [b - ka] = -a < 0$
ดังนั้น $b - (k+1)a < b - ka$
จึงเกิดข้อขัดแย้งในการเลือก $m = b - ka$ ที่เป็นสมาชิกที่น้อยที่สุดใน S □

หลักการจัดอันดับดียังนำไปสู่ทฤษฎีบทที่สำคัญที่ใช้เพื่อพิสูจน์ข้อความต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มบวก เรียกทฤษฎีบทนี้ว่า **"หลักอุปนัยเชิงคณิตศาสตร์"** (Principle of Mathematical Induction) ซึ่งได้กล่าวไว้แล้วในหัวข้อ 1.3

ทฤษฎีบท 1.4.9

ให้ $S \subseteq \mathbb{N}$ จะได้ว่า $\mathbb{N} = S$ ก็ต่อเมื่อ
1. $1 \in S$ และ
2. ถ้า $n \in S$ แล้ว $n + 1 \in S$

การพิสูจน์ ให้ $S = \mathbb{N}$ เห็นได้ชัดว่า (1) และ (2) เป็นจริง
สมมติว่า (1) และ (2) เป็นจริง และ $\mathbb{N} \setminus S \neq \varnothing$ โดยหลักการจัดอันดับดี
จะมี $m \in \mathbb{N} \setminus S$ ซึ่ง m เป็นจำนวนเต็มบวกที่น้อยที่สุดใน $\mathbb{N} \setminus S$
เพราะว่า $m - 1 < m$ ดังนั้น $m - 1 \notin \mathbb{N} \setminus S$
จาก $1 \in S$ แสดงว่า $m > 1$ ดังนั้น $m - 1 \in \mathbb{N}$
จากการเลือก m เราพบว่า $m - 1 \in S$
และจาก (2) จะได้ว่า $m = (m - 1) + 1 \in S$
ซึ่งเป็นไปไม่ได้เกิดข้อขัดแย้งที่ว่า $m \notin S$ ดังนั้น $\mathbb{N} = S$ □

หลักการจัดอันดับดีสามารถนำไปพิสูจน์หลักอุปนัยเชิงคณิตศาสตร์ได้ และในทางกลับกันหลักอุปนัยเชิงคณิตศาสตร์ก็สามารถพิสูจน์หลักการจัดอันดับดีได้เช่นกัน จึงกล่าวได้ว่าหลักการทั้งสองนี้สมมูลกันนั่นเอง

นพพร ธนะชัยขันธ์ (2543 : 13-14) ได้กล่าวถึงเซตเชิงอุปนัย พร้อมทั้งให้ข้อสังเกตที่ได้จากการนิยามเซตเชิงอุปนัยดังจะกล่าวต่อไปนี้

บทนิยาม 1.4.2

ให้ S เป็นเซตย่อยของ $\mathbb{R}$ จะกล่าวว่า S เป็นเซตเชิงอุปนัยก็ต่อเมื่อ S มีสมบัติ 2 ประการ คือ
(1) $1 \in S$ และ
(2) ถ้า $n \in S$ แล้ว $n + 1 \in S$

ตัวอย่าง 1.4.1

เซตของจำนวนจริง $\mathbb{R}$ เป็นเซตเชิงอุปนัยเพราะ $1 \in \mathbb{R}$ และถ้า $n \in \mathbb{R}$ เนื่องจาก $1 \in \mathbb{R}$ โดยสมบัติของการบวกใน $\mathbb{R}$ แล้วจะได้ว่า $n + 1 \in \mathbb{R}$ ดังนั้น $\mathbb{R}$ จึงเป็นเซตเชิงอุปนัย ในทำนองเดียวกันเซตของจำนวนจริงบวกทั้งหมด (แทนด้วย $\mathbb{R}^+$) ก็เป็นเซตเชิงอุปนัย

บทนิยาม 1.4.3

ให้ $\mathbb{Z}^+$ แทนอินเตอร์เซกชันของเซตเชิงอุปนัยทั้งหมด

ข้อสังเกต

1) จากบทนิยาม 1.4.3 จะได้ว่า $\mathbb{Z}^+$ เป็นเซตเชิงอุปนัย

2) $\mathbb{Z}^+$ เป็นเซตย่อยของเซตเชิงอุปนัยทุกเซต หรืออีกนัยหนึ่งคือ $\mathbb{Z}^+$ เป็นเซตเชิงอุปนัยที่เล็กที่สุด (smallest inductive set)

3) เนื่องจาก $\mathbb{R}^+$ เป็นเซตเชิงอุปนัย ดังนั้น $\mathbb{Z}^+ \subset \mathbb{R}^+$ นั่นแสดงว่าสมาชิกทุกตัวของ $\mathbb{Z}^+$ เป็นจำนวนจริงบวกเสมอ

4) เนื่องจาก Z^+ เป็นเซตเชิงอุปนัย จากบทนิยาม 1.4.2 จะได้ว่า $1 \in \mathbb{Z}^+$ และ $1+1=2 \in \mathbb{Z}^+$ และ $2+1=3 \in \mathbb{Z}^+$ ทำเช่นนี้ต่อไปเรื่อย ๆ จะได้ว่า $[1,2,3,\ldots] \subset \mathbb{Z}^+$ แต่ $[1,2,3,\ldots]$ เป็นเซตเชิงอุปนัย และ $\mathbb{Z}^+$ เป็นเซตเชิงอุปนัยที่เล็กที่สุด เพราะฉะนั้น $\mathbb{Z}^+ \subset [1,2,3,\ldots]$ นั่นคือ $\mathbb{Z}^+ = [1,2,3,\ldots]$

บทนิยาม 1.4.4

เรียกสมาชิกของ $\mathbb{Z}^+$ ว่าจำนวนเต็มบวก

ต่อไปเราจะศึกษาสมบัติต่าง ๆ ที่สำคัญของจำนวนเต็มบวก การพิสูจน์ในทฤษฎีบทต่อไปนี้จะอาศัยทฤษฎีบท 1.4.9 และสมบัติของเซตเชิงอุปนัย

ทฤษฎีบท 1.4.10

ถ้า $m \in \mathbb{Z}^+$ และ $n \in \mathbb{Z}^+$ แล้ว $m+n \in \mathbb{Z}^+$

การพิสูจน์ สำหรับจำนวนเต็มบวก m ซึ่งคงตัว ให้ $S = \{n \in \mathbb{Z}^+ \mid m+n \in \mathbb{Z}^+\}$ เราจะแสดงว่า $S = \mathbb{Z}^+$

1) เนื่องจาก $m \in \mathbb{Z}^+$ และ $\mathbb{Z}^+$ เป็นเซตเชิงอุปนัย ดังนั้น $m+1 \in \mathbb{Z}^+$
โดยบทนิยามของ S จะได้ว่า $1 \in S$

2) ถ้า $k \in S$ โดยบทนิยามของ S จะได้ว่า $m+k \in \mathbb{Z}^+$ แต่ $\mathbb{Z}^+$ เป็นเซตเชิงอุปนัย
ดังนั้น $(m+k)+1 \in \mathbb{Z}^+$
แต่ $(m+k)+1 = m+(k+1)$ ดังนั้น $m+(k+1) \in \mathbb{Z}^+$ ด้วย
โดยบทนิยามของ S จะได้ว่า $k+1 \in S$

จากข้อ 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์
จะได้ว่า $S = \mathbb{Z}^+$ นั่นแสดงว่า ถ้า $m \in \mathbb{Z}^+$ และ $n \in \mathbb{Z}^+$ แล้ว $m+n \in \mathbb{Z}^+$ □

ทฤษฎีบท 1.4.11

ถ้า $m \in \mathbb{Z}^+$ และ $n \in \mathbb{Z}^+$ แล้ว $mn \in \mathbb{Z}^+$

การพิสูจน์ สำหรับจำนวนเต็มบวก m ซึ่งคงตัว ให้ $S = \{n \in \mathbb{Z}^+ \mid mn \in \mathbb{Z}^+\}$ เราจะแสดงว่า $S = \mathbb{Z}^+$

1) เนื่องจาก $m \in \mathbb{Z}^+$ และ $m1 = m \in \mathbb{Z}^+$ โดยบทนิยามของ S ดังนั้น $1 \in S$

2) ถ้า $k \in S$ โดยบทนิยามของ S จะได้ว่า $mk \in \mathbb{Z}^+$ เนื่องจาก $m \in \mathbb{Z}^+$
โดยทฤษฎีบท 1.4.10 จะได้ว่า $mk+m \in \mathbb{Z}^+$ แต่ $mk+m = mk+m1 = m(k+1)$
เพราะฉะนั้น $m(k+1) \in \mathbb{Z}^+$ จากบทนิยามของ S จะได้ว่า $k+1 \in S$

จากข้อ 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์
จะได้ว่า $S = \mathbb{Z}^+$ นั่นแสดงว่า ถ้า $m \in \mathbb{Z}^+$ และ $n \in \mathbb{Z}^+$ แล้ว $mn \in \mathbb{Z}^+$ □

ทฤษฎีบท 1.4.12

สำหรับจำนวนเต็มบวก n ทุกตัว จะได้ว่า $1 \leq n$

การพิสูจน์ ให้ $S = \{n \in \mathbb{Z}^+ \mid 1 \leq n\}$ เราจะแสดงว่า $S = \mathbb{Z}^+$

1) เนื่องจาก $1 \leq 1$ ดังนั้น $1 \in S$

2) ถ้า $k \in S$ โดยนิยามของ S จะได้ว่า $1 \leq k$ แต่ $k \leq k+1$ ดังนั้น $1 \leq k+1$

โดยบทนิยามของ S จะได้ว่า $k+1 \in S$

จาก 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $S = \mathbb{Z}^+$

นั่นคือ สำหรับจำนวนเต็มบวก n ทุกตัว จะได้ว่า $1 \leq n$ □

ทฤษฎีบท 1.4.13

ถ้า $m \in \mathbb{Z}^+$ และ $m > 1$ แล้ว $m - 1 \in \mathbb{Z}^+$

การพิสูจน์ สมมติว่ามีจำนวนเต็มบวก t ซึ่ง $t > 1$ และ $t - 1 \notin \mathbb{Z}^+$ ให้ $S = \{m \in \mathbb{Z}^+ \mid m \neq 1\}$

จะแสดงว่า $S = \mathbb{Z}^+$

1) เนื่องจาก $t > 1$ แสดงว่า $1 \neq t$ ดังนั้น $1 \in S$

2) ถ้า $k \in S$ จะแสดงว่า $k+1 \in S$ โดยการนิยามพิสูจน์ทางอ้อม สมมติให้ $k+1 \in S$

โดยนิยามของ S จะได้ว่า $k+1 = t$ จะได้ว่า $k = t-1$

จากข้อสมมติฐาน $t - 1 \in \mathbb{Z}^+$ ดังนั้น $k \in \mathbb{Z}^+$

โดยบทนิยามของ S จะได้ว่า $k \notin S$ เกิดข้อขัดแย้งกับสมมติฐานที่ว่า $k \in S$

นั่นแสดงว่า $k+1 \in S$

จากข้อ 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์จะได้ว่า $S = \mathbb{Z}^+$

สรุปได้ว่า ถ้า $m \in \mathbb{Z}^+$ และ $m > 1$ แล้ว $m - 1 \in \mathbb{Z}^+$ □

ทฤษฎีบท 1.4.14

ไม่มีจำนวนเต็มบวกระหว่าง 1 และ 2

การพิสูจน์ ให้ $S = \{1\} \cup \{n \in \mathbb{R} \mid n \geq 2\}$

1) จากบทนิยามของ S จะได้ว่า $1 \in S$

2) ถ้า $k \in S$ จะได้ว่า $k = 1$ หรือ $k \geq 2$

กรณีที่ 1 ถ้า $k = 1$ จะได้ว่า $k + 1 = 1 + 1 = 2 \in S$

กรณีที่ 2 ถ้า $k \geq 2$ เพราะว่า $2 \geq 1$ ดังนั้น $k \geq 1$ เอา 1 บวกทั้งสองข้างของอสมการ

จะได้ว่า $k + 1 \geq 2$ จากบทนิยามของ S จะได้ว่า $k + 1 \in S$

จากข้อ 1) และข้อ 2) แสดงว่า S เป็นเซตเชิงอุปนัย แต่ $\mathbb{Z}^+$ เป็นเซตย่อยของเซตเชิงอุปนัยทุกเซต

ดังนั้น $\mathbb{Z}^+ \subset S$ จึงสรุปว่าไม่มีจำนวนเต็มบวกระหว่าง 1 และ 2

เพราะว่าถ้ามีจำนวนเต็มบวก t ที่อยู่ระหว่าง 1 และ 2 แล้วจะส่งผลให้ $t \in S$

ซึ่งเกิดข้อขัดแย้งกับบทนิยามของ S ที่กำหนด □

ต่อไปเราจะนำเสนอกรณีทั่วไปของทฤษฎีบทที่ 1.4.14 ดังทฤษฎีบทที่ 1.4.15

ทฤษฎีบท 1.4.15

ถ้า m เป็นจำนวนเต็มบวกแล้ว จะไม่มีจำนวนเต็มบวก n ซึ่ง $m < n < m + 1$

การพิสูจน์ ให้ $S = \{m \in \mathbb{Z}^+ \mid$ ไม่มี $n \in \mathbb{Z}^+$ ซึ่ง $m < n < m+1\}$

1) โดยทฤษฎีบท 1.4.14 จะได้ว่า $1 \in S$

2) ถ้า $k \in S$ อาศัยการพิสูจน์ว่า $k+1 \in S$

นั่นคือ ต้องการพิสูจน์ว่าไม่มี $n \in X$ ซึ่ง $k+1 < n < k+2$

แต่จะสมมติตรงกันข้ามว่ามี $n \in \mathbb{Z}^+$ ซึ่ง $k+1 < n < k+2$

เนื่องจาก $0 < k$ นำ 1 บวกทั้งสองข้างของสมการนี้

ดังนั้น $1 < k+1$ จากข้อสมมติ $k+1 < n$ แสดงว่า $1 < n$

โดยทฤษฎีบท 1.4.13 จะได้ว่า $n-1 \in \mathbb{Z}^+$

จากอสมการ $k+1 < n < k+2$ นำ -1 บวกตลอดสมการ จะได้ว่า

$$k < n-1 < k+1$$

ซึ่งทำให้ $k \notin S$ จึงเกิดข้อขัดแย้งกับสมการติฐานที่ว่า $k \in S$ ดังนั้น $k+1 \in S$

จากข้อ 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $S = \mathbb{Z}^+$

สรุปได้ว่า ถ้า $m \in \mathbb{Z}^+$ แล้วจะไม่มีจำนวนเต็มบวก n ซึ่ง $m < n < m+1$ □

ทฤษฎีบท 1.4.16

ถ้า $m \in \mathbb{Z}^+, n \in \mathbb{Z}^+$ และ $m > n$ จะได้ว่า $m-n \in \mathbb{Z}^+$

การพิสูจน์ ให้ $S = \{n \in \mathbb{Z}^+ \mid$ ถ้า $m \in \mathbb{Z}^+$ และ $m > n$ แล้ว $m-n \in \mathbb{Z}^+\}$

1) โดยทฤษฎีบท 1.4.13 จะได้ว่า $1 \in S$

2) ถ้า $k \in S$ นั่นคือเรากำหนดว่า ถ้า $m \in \mathbb{Z}^+, k \in \mathbb{Z}^+$ และ $m > k$ จะได้ว่า $m-k \in \mathbb{Z}^+$

เราต้องการพิสูจน์ว่า $k+1 \in S$ กล่าวคือ ต้องพิสูจน์ว่า ถ้า $m \in \mathbb{Z}^+, k+1 \in \mathbb{Z}^+$

และ $m > k+1$ จะได้ว่า $m-(k+1) \in \mathbb{Z}^+$

เนื่องจาก $m > k+1$ จะได้ว่า 1) $m > k$ และ 2) $m-k > 1$

จากข้อ 1) โดยสมมติฐาน $1 \in S$ จะได้ว่า $m-k \in \mathbb{Z}^+$

จาก $m-k \in \mathbb{Z}^+$ และข้อ 2) $m-k > 1$

โดยทฤษฎีบท 1.4.13 จะได้ว่า $(m-k)-1 \in \mathbb{Z}^+$ แต่ $(m-k)-1 = m-(k+1)$

ดังนั้น $m-(k+1) \in \mathbb{Z}^+$ นั้นคือ $k+1 \in S$

จากข้อ 1) และข้อ 2) โดยทฤษฎีบท 1.4.9 และหลักการอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $S = \mathbb{Z}^+$

นั่นคือ ถ้า $m \in \mathbb{Z}^+, n \in \mathbb{Z}^+$ และ $m > n$ จะได้ว่า $m-n \in \mathbb{Z}^+$ □

1.4.1 ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์ (2552 : 16-19) ให้ข้อแนะนำบางประการเกี่ยวกับจำนวนเต็ม ดังนี้

(1) ให้ a และ d เป็นจำนวนเต็มใด ๆ เราเรียกลำดับจำนวนเต็ม

$$a, a+d, a+2d, a+3d, \ldots, a+(n-1)d, \ldots$$

ว่า**ลำดับเลขคณิต** และเรียก a ว่า **พจน์แรก** เรียก d **ว่าพจน์ต่างร่วม** เช่น ลำดับ $3, 7, 9, 11, 13, \ldots$ เป็นลำดับเลขคณิต ที่ $a = 3$ และ $d = 2$

(2) ให้ a และ r เป็นจำนวนเต็มใด ๆ เราเรียกลำดับจำนวน

$$a, ar, ar^2, ar^3, \ldots ar^{n-1}, \ldots$$

ว่า**ลำดับเรขาคณิต** และเรียก a ว่า **พจน์แรก** เรียก r ว่า **อัตราส่วนร่วม** เช่น ลำดับ $5, -15, 45, -135, \ldots$ เป็นลำดับเรขาคณิตที่ $a = 5$ และ $r = -3$

(3) ผลบวก n พจน์แรกของลำดับเลขคณิต

$$a + (a + d) + (a + 2d) + \cdots + (a + (n - 1)d) = \frac{n}{2}\Big[2a + (n - 1)d\Big]$$

และผลบวก n พจน์แรกของเรขาคณิต

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \frac{a\,(r^n - 1)}{r - 1}$$

เช่น $2 + 4 + 6 + 8 + 10 + \cdots + 400 = \dfrac{200}{2}\Big[2(2) + (200 - 1)\Big]$ =40,200

$3 + 3 \cdot 2 + 3 \cdot 2^2 + 3 \cdot 2^3 + \cdots + 3 \cdot 2^{25} = \dfrac{3\,(2^{26} - 1)}{2 - 1} = 3\,(2^{26} - 1)$

(4) **สัญลักษณ์แทนการบวก** คือสัญลักษณ์ "$\sum$" อ่านว่า ซิกมา ซึ่งมีความหมายดังนี้

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + a_3 + a_4 + \cdots + a_m$$

เช่น $\displaystyle\sum_{k=1}^{6}(2k + 1) = (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + (2 \cdot 3 + 1) + \cdots + (2 \cdot 6 + 1)$

$\displaystyle\sum_{j=1}^{5} j = 1 + 2 + 3 + 4 + 5 = 15$

$\displaystyle\sum_{j=1}^{5} 2 = 2 + 2 + 2 + 2 + 2 = 10$

การใช้สัญลักษณ์ "$\sum$" อาจไม่ได้เริ่มจาก 1

เช่น $\displaystyle\sum_{k=3}^{5} k^2 = 3^2 + 4^2 + 5^2 = 50$

(5) **สัญลักษณ์แทนการคูณ** คือสัญลักษณ์ "$\prod$" อ่านว่า พาย มีความหมายดังนี้

$$\prod_{j=1}^{n} a_j = a_1 \times a_2 \times a_3 \times \cdots \times a_n$$

เช่น $\prod_{j=1}^{5} j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

$\prod_{j=1}^{5} 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$

ข้อเสนอแนะเพิ่มเติม

บทนิยาม 1.4.5 : ค่าสัมบูรณ์

ให้ $a \in \mathbb{Z}$ ค่าสัมบูรณ์ ของ a เขียนแทนด้วย $|\,a\,|$ นิยามดังนี้

$$|\,a\,| = \begin{cases} 0 & \text{ถ้า} \quad a = 0 \\ a & \text{ถ้า} \quad a \in \mathbb{N} \\ -a & \text{ถ้า} \quad -a \in \mathbb{N} \end{cases}$$

จากบทนิยามเราพบว่า

1. $|\,a\,| \geq 0$
2. $|\,a\,| = 0$ ก็ต่อเมื่อ $a = 0$
3. $-|\,a\,| \leq a \leq |\,a\,|$
4. $|\,a\,| \leq b$ ก็ต่อเมื่อ $-b \leq a \leq b$
   $|\,a\,| \geq b$ ก็ต่อเมื่อ $a \geq b$ หรือ $a \leq -b$
5. $|\,ab\,| = |\,a\,||\,b\,|$
6. $|\,a+b\,| \leq |\,a\,| + |\,b\,|$
7. $|\,a\,| - |\,b\,| \leq |\,a-b\,|$
8. $-(|\,a\,| + |\,b\,|) \leq a+b \leq |\,a\,| + |\,b\,|$
9. $||\,a\,| - |\,b\,|\,| \leq |\,a-b\,|$
10. $|\,a\,| = |\,b\,|$ ก็ต่อเมื่อ $a = b$ หรือ $a = -b$

สรุปท้ายบท

สิ่งที่สำคัญในบทนี้คือเน้นให้ผู้เรียนมีความรู้ความเข้าใจเกี่ยวกับสมบัติต่าง ๆ ของจำนวนเต็มตลอดจนวิธีการพิสูจน์สมบัติและทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็ม ตลอดจนให้นักศึกษามีความรู้ความเข้าใจวิธีการพิสูจน์โดยใช้หลักอุปนัยแบบต่าง ๆ โดยได้ยกตัวอย่างในการพิสูจน์โดยใช้หลักอุปนัยแบบต่าง ๆ ไว้อย่างละเอียดเข้าใจง่าย ซึ่งการพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์เป็นสิ่งสำคัญที่นักศึกษาสาขาวิชาคณิตศาสตร์ต้องรู้และพิสูจน์ได้เพราะต้องใช้เป็นพื้นฐานในการเรียนคณิตศาสตร์ในระดับที่สูงขึ้น

แบบฝึกหัดท้ายบทที่ 1

1. จงพิสูจน์ว่าข้อความต่อไปนี้เป็นจริง

   1.1 $a^{n+1} - 1 = (a-1)\left(a^n + a^{n-1} + \cdots + a + 1\right)$

   1.2 $1 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}\dfrac{n(n+1)}{2}$

   1.3 $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1) \cdot 2^{n+1} + 2$

   1.4 $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$

   1.5 $1 \cdot 3 + 2 \cdot 5 + 3 \cdot 7 + \cdots + (3n-2)(3n+1) = n\left(3n^2 + 3n - 2\right)$

2. จงพิสูจน์ว่า $\dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{n}} > \sqrt{n}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n \geq 2$

3. จงพิสูจน์ว่า $\displaystyle\sum_{i=1}^{n} \frac{1}{(3i-1)(3i+1)} = \frac{n}{3n+1}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

4. จงพิสูจน์ว่า $5^n + 5 < 5^{n+1}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

5. จงพิสูจน์ว่า $1 + \dfrac{1}{4} + \dfrac{1}{9} + \cdots + \dfrac{1}{n^2} \leq 2 - \dfrac{1}{n}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

6. ถ้า a เป็นจำนวนเต็มซึ่ง $a > -1$ และ $a \neq 0$ จงพิสูจน์ว่า $(1+a)^n > 1 + na$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ที่ $n > 2$

7. ให้ $a, b, c, d \in \mathbb{Z}$ จงพิสูจน์ว่า

   7.1 $-a = (-1)a$

   7.2 $(a-b) + (c-d) = (a+c) - (b+d)$

   7.3 $(a-b) - (c-d) = (a+d) - (b+c)$

   7.4 $(a-b)(c-d) = (ac+bd) - (ad+bc)$

   7.5 $a - b = c - d$ ก็ต่อเมื่อ $a + d = b + c$

   7.6 $(a-b)c = ac - bc$

8. ให้ $a, b, c, x, y \in \mathbb{Z}$ จงพิสูจน์ว่า

   8.1 $a < b$ ก็ต่อเมื่อ $x > y$

   8.2 $a - x < a - y$ ก็ต่อเมื่อ $x > y$ 8.3 ถ้า $a < 0$ แล้ว $ax > ay$ ก็ต่อเมื่อ $x < y$

   8.4 ถ้า $c > 0$ แล้ว $a < b$

   8.5 ถ้า $x + x + x + x = 0$ แล้ว $x = 0$

   8.6 ถ้า $a < b$ แล้ว $a^3 < b^3$

9. จงพิสูจน์ว่า ถ้า $a^7 = b^7$ แล้ว $a = b$

10. จงพิสูจน์ว่า $a^2 - ab + b^2 \geq 0$ เมื่อ $a, b \in \mathbb{Z}$

11. จงใช้หลักอุปนัยเชิงคณิตศาสตร์สรุปว่า $1(1!) + 2(2!) + 3(3!) + \cdots + n(n!) = (n+1)! - 1$

12. สำหรับจำนวนเต็มบวก n ใด ๆ จงพิสูจน์ว่า

12.1 $2 \times 6 \times 10 \times 14 \times \cdots \times (4n-2) = \dfrac{(2n)!}{n!}$

12.2 $2^n(n!)^2 \leq (2n)!$

12.3 $\dfrac{(2n)!}{2^n(n!)}$ เป็นจำนวนเต็มสำหรับทุก $n \in \mathbb{N} \cup \{0\}$

13. จงแสดงว่า ถ้า $2 \leq k \leq n-2$ แล้ว

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$$

สำหรับ $n \geq 4$

14. จงพิสูจน์ว่า สำหรับจำนวนเต็ม $n > 2$ จะได้

$$\binom{2}{2} = \binom{4}{2} + \binom{6}{2} + \binom{2n}{n} = n(n+1)(n+2)$$

(ข้อเสนอแนะ สำหรับ $m \geq 2$, $\binom{2m}{2} = 2\binom{m}{2} + m^2$)

เอกสารอ้างอิง

กัลยาณี ไชยวรินทรกุล. (2522). **ระบบจำนวน**. กรุงเทพฯ : โรงพิมพ์มหาวิทยาลัยรามคำแหง.

คณะกรรมการกลุ่มผลิตชุดวิชาตรรกศาสตร์ เซตและทฤษฎีจำนวน. (2529). **เอกสารการสอนชุดวิชาตรรกศาสตร์ เซตและทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์ชวนพิมพ์. (ฝ่ายการพิมพ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช)

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จารุวรรณ สิงห์ม่วง. (2011). **ทฤษฎีจำนวน : ราชินีแห่งคณิตศาสตร์**. Journal of Rajanagarindra. 8(19), 79-86

ช่อเอื้อง อุทิตะสาร. (2562). **เอกสารประกอบการสอน รายวิชาหลักการคณิตศาสตร์**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

พัฒนี อุดมกะวานิช. (2559). **หลักคณิตศาสตร์**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

พิมพ์เพ็ญ เวชชาชีวะ. (2558). **ระบบจำนวน**. กรุงเทพฯ : วีพริ้นท์ (1991).

มานัส บุญยัง. (2532). **หนังสือประกอบการเรียนพีชคณิต**. กรุงเทพฯ : โรงพิมพ์ สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

วัลลภ เหมวงษ์. (2562). **หลักการคณิตศาสตร์**. อุดรธานี : คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี.

สมจิต โชติชัยสถิตย์. (2540). **ทฤษฎีจำนวน 2**. ขอนแก่น : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

สุเทพ จันทร์สมศักดิ์. (2538). **ระบบจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

สุภา สุจริตพงศ์. (2523). **โครงสร้างของระบบจำนวน**. กรุงเทพฯ : สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย

Pual Glendinning. (2012). **Maths in minutes**. London, England : Quercus Editions Ltd.

Raji, W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

แผนบริหารการสอนประจำบทที่ 2

เนื้อหาประจำบท

1. ขั้นตอนวิธีการหาร
2. การหารลงตัว และสมบัติเบื้องต้นของการหารลงตัว
3. การพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์
4. ตัวหารร่วมมาก
5. ขั้นตอนวิธีแบบยุคลิด
6. ตัวคูณร่วมน้อย

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและคุณสมบัติของการหารลงตัวแก้โจทย์ปัญหาที่กำหนดให้ได้
2. พิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์ได้
3. ใช้นิยามของตัวหารร่วมมากและทฤษฎีที่เกี่ยวข้องพิสูจน์โจทย์ปัญหาที่กำหนดให้ได้
4. ใช้นิยามของตัวคูณร่วมน้อยและทฤษฎีที่เกี่ยวข้องพิสูจน์โจทย์ปัญหาที่กำหนดให้ได้
5. หา ห.ร.ม. โดยขั้นตอนวิธีแบบยุคลิดได้
6. ประยุกต์ใช้ความรู้ในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 ขั้นตอนวิธีการหาร
    1.2 การหารลงตัว และสมบัติเบื้องต้นของการหารลงตัว
    1.3 การพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์
    1.4 ตัวหารร่วมมาก
    1.5 ขั้นตอนวิธีแบบยุคลิด
    1.6 ตัวคูณร่วมน้อย
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม

3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 2
การหารลงตัว

ในบทที่ 1 ได้กล่าวถึงสมบัติเบื้องต้นของจำนวนเต็มพอสังเขป ในบทนี้จะกล่าวถึงสมบัติของจำนวนเต็มเกี่ยวกับการหารลงตัว ขั้นตอนวิธีการหาร ตัวหารร่วมมาก และตัวคูณร่วมน้อย ซึ่งเป็นเรื่องราวที่ได้มีการศึกษามาตั้งแต่สมัยยุคลิดประมาณ 300 ปีก่อนคริสต์ศักราช แนวคิดพื้นฐานได้พัฒนามาจนถึงปัจจุบัน โดยจะเริ่มต้นด้วยการศึกษาขั้นตอนวิธีการหาร

2.1 ขั้นตอนวิธีการหาร

ในหัวข้อนี้จะพิสูจน์ทฤษฎีบทที่มีความสำคัญในวิชาทฤษฎีจำนวน ซึ่งได้แก่ ทฤษฎีบทพื้นฐานของยุคลิด (fundamental theorem of Euclid) ธนัชยศ จำปาหวาย (2559 : 21-22) ได้กล่าวถึงการหารเราอาจจะรู้จักการหารในจำนวนจริงมาแล้วในเบื้องต้น แต่ในบทนี้จะกล่าวถึงการหารในระบบจำนวนเต็ม เช่น เมื่อหาร 20 ด้วย 7 จะได้ผลหารเท่ากับ 2 เศษเหลือเท่ากับ 6 เขียนได้เป็น

$$20 = 7(2) + 6$$

เรียกสมการนี้ว่า ขั้นตอนวิธีการหาร ในกรณีที่เศษเหลือเท่ากับ 0 จะเรียกว่าการหารลงตัว เช่น 5 หาร 10 ลงตัว เขียนเป็น

$$10 = 5(2)$$

ความรู้เกี่ยวกับ ตัวหาร พหุคูณ จำนวนเฉพาะ และจำนวนประกอบ ดังกล่าวเป็นหลักการที่มนุษย์ได้เรียนรู้มาอย่างน้อยตั้งแต่สมัยของยุคลิด หรือเมื่อประมาณ 350 ปีก่อนคริสตกาลมาแล้ว (Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery. 1991 : 4) และขั้นตอนวิธีการหารเป็นพื้นฐานประการหนึ่งที่สำคัญต่อการเรียนวิชาทฤษฎีจำนวน ซึ่งเป็นทฤษฎีบทเบื้องต้นของการนำไปใช้พิสูจน์สมบัติต่าง ๆ ของจำนวนเต็ม

ในการหาผลหารของจำนวนเต็มสองจำนวน เราอาจใช้วิธีการหารยาวดังอย่างต่อไปนี้ พิจารณา 112 หารด้วย 25

$$\begin{array}{r} 4 \\ 25\overline{)112} \\ \underline{100} \\ 12 \end{array}$$

แสดงว่า 112 หารด้วย 25 ไม่ลงตัว และได้ผลหารเท่ากับ 4 เศษเท่ากับ 12 เราสามารถเขียนความสัมพันธ์ระหว่างตัวเลข 4 ตัวนี้ได้เป็น $112 = 25(4) + 12$

จากความสัมพันธ์ข้างต้นเกี่ยวข้องกับทฤษฎีพื้นฐานของยุคลิกเรียกอีกอย่างหนึ่งว่า ทฤษฎีขั้นตอนวิธีการหาร ซึ่งจะกล่าวต่อไปนี้ (David M. Burton. 2007 : 17, โสภาพรรณ ทิพย์โยธา. 2545 : 18-20)

ทฤษฎีบท 2.1.1 : ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้น ที่ทำให้ $b = aq + r$ โดยที่ $0 \leq r < |a|$ จะเรียก q ว่า **ผลหาร** (quotient) และ r ว่า **เศษ** (remainder)

การพิสูจน์ จะพิสูจน์ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้ $b = aq + r, 0 \leq r < |\, a \,|$
โดยจะแบ่งการพิสูจน์ออกเป็นสองกรณี

กรณีที่ 1 ถ้า $a > 0$ แล้ว $|\, a \,| = a$
ให้ $S = \{b - ax \mid x \in \mathbb{Z} \text{ และ } b - ax \geq 0\}$
เนื่องจาก $a \geq 1$ จะได้ว่า $|\, b \,|a \geq |\, b \,|$ แสดงว่า $b - (-|\, b \,|)a \geq b + |\, b \,| \geq 0$ ดังนั้น $S \neq \varnothing$
แสดงว่า จะมี $s \in S$ ซึ่ง $s = 0$ หรือ $s > 0$
ถ้า $s = 0$ จะได้ว่ามี $q \in \mathbb{Z}$ ซึ่ง $s = b - aq$
นั่นคือ $b = aq + s$ เมื่อ $s = 0$
ถ้า $s > 0$ โดยหลักการจัดอันดับดี จะมี $r \in S$ ซึ่ง $r = s$ หรือ $r < s$
เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S
แสดงว่าจะมี $q \in \mathbb{Z}$ ซึ่ง $r = b - aq$
ดังนั้น $b = aq + r$ โดยที่ $r > 0$
ต่อไปจะแสดงว่า $r < a$ โดยสมมติว่า $r \geq a$
ดังนั้น $r - a = (b - aq) - a = b - a(q + 1) \geq 0$
แสดงว่า $r - a \in S$
แต่ $r - a < r$ ซึ่งขัดแย้งกับที่ว่า r เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S
ดังนั้น $r < a = |\, a \,|$
เพราะฉะนั้น มี $q, r \in \mathbb{Z}$ ที่ทำให้ $b = aq + r$ โดยที่ $0 \leq r < |\, a \,|$

กรณีที่ 2 ถ้า $a < 0$ แล้ว $|\, a \,| = -a$
จากกรณีที่ 1 จะได้ว่ามี $d, r \in \mathbb{Z}$
ที่ทำให้ $b = (-a)d + r = a(-d) + r,\ 0 \leq r < -a = |\, a \,|$
ให้ $q = -d$ แสดงว่ามี $q, r \in \mathbb{Z}$ ซึ่ง $b = aq + r$ โดยที่ $0 \leq r \leq |\, a \,|$
ต่อไปจะแสดงว่ามี $q, r \in \mathbb{Z}$ เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$
โดยที่ $0 \leq r < |\, a \,|$ นั่นคือสมมติว่ามี $q, r, q', r' \in \mathbb{Z}$
ที่ทำให้ $b = aq + r, 0 \leq r < |\, a \,|$ และ $b = aq' + r', 0 \leq r' < |\, a \,|$
จะพิสูจน์ว่า $q = q'$ และ $r = r'$
ให้ $b = aq + r, 0 \leq r < |\, a \,|$ และ $b = aq' + r', 0 \leq r' < |\, a \,|$
จะได้ว่า $|\, a \,||\, q - q' \,| = |\, r - r' \,|$ โดยที่ $0 \leq |\, r - r' \,| < |\, a \,|$
ดังนั้น $0 \leq |\, a \,||\, q - q' \,| < |\, a \,|$ แสดงว่า $0 \leq |\, q - q' \,| < 1$
และจาก $|\, q - q' \,|$ เป็นจำนวนเต็ม
จะได้ว่า $|\, q - q' \,| = 0$ และทำให้ $|\, r - r' \,| = 0$
นั่นคือ $q = q'$ และ $r = r'$ □

จากทฤษฎีบท 2.1.1 สามารถยกตัวอย่างเพื่อให้เกิดความเข้าใจมากขึ้นได้ดังนี้

ตัวอย่าง 2.1.1

1.) ให้ $b = 60$ และ $a = 7$ แล้วจะมี $q = 8$ และ $r = 4$ ที่ทำให้ $b = qa + r,\ 0 \leq r < |\, a \,|$

$$60 = (8)7 + 4, \quad 0 \leq 4 < |\, 7 \,|$$

2.) ให้ $b = -39$ และ $a = 6$ แล้วจะมี $q = -7$ และ $r = 3$ ที่ทำให้ $b = qa + r,\ 0 \leq r < |\, a \,|$

$$-39 = (-7)6 + 3, \quad 0 \leq 3 < |\, 6 \,|$$

ตัวอย่าง 2.1.2

จงหาค่า q และ r ตามทฤษฎีบท 2.1.1

(ก) $a = 52,\ b = 5$

เนื่องจาก $52 = 5 \cdot 10 + 2$ ดังนั้น $q = 10, r = 2$

(ข) $a = -52,\ b = 5$

เนื่องจาก $-52 = 5 \cdot (-11) + 3$ ดังนั้น $q = -11, r = 3$

(ค) $a = 52,\ b = -5$

เนื่องจาก $52 = (-5) \cdot (-10) + 2$ ดังนั้น $q = -10, r = 2$

(ง) $a = -52,\ b = -5$

เนื่องจาก $-52 = (-5) \cdot 11 + 3$ ดังนั้น $q = 11, r = 3$

ตัวอย่าง 2.1.3

ให้ $a = 5$ และ $b = 3$ จงหา q และ r ซึ่ง $5 = q(3) + r,\ 0 \leq r < 3$

วิธีทำ เนื่องจาก $5 = 1(3) + 2$

ดังนั้น $q = 1$ และ $r = 2$

ตัวอย่าง 2.1.4

ให้ $a = 59$ และ $b = -14$ จงหา q และ r ซึ่ง $59 = q(-14) + r,\ 0 \leq r < |-14| = 14$

วิธีทำ เนื่องจาก $59 = 4(14) + 3 = (-4)(-14) + 3$

ดังนั้น $q = -4$ และ $r = 3$

ตัวอย่าง 2.1.5

ให้ $a = -79$ และ $b = 11$ จงหา q และ r ซึ่ง $-79 = q(11) + r, 0 \leq r < 11$

วิธีทำ เนื่องจาก $79 = 7(11) + 2$

$$\begin{aligned} -79 &= -7(11) + (-2) \\ &= -7(11) - 11 + (2 + 11) \\ &= -8(11) + 9 \end{aligned}$$

ดังนั้น $q = -8$ และ $r = 9$

ตัวอย่าง 2.1.6

จงแสดงว่า ถ้า n เป็นจำนวนเต็มคี่ แล้วจะมีจำนวนเต็ม k ที่ทำให้ $n^2 = 8k + 1$

วิธีทำ ให้ n เป็นจำนวนเต็มคี่ พิจารณาจำนวนเต็มใด ๆ และ 4 จากขั้นตอนวิธีการหาร

จะมีจำนวนเต็ม q ที่ทำให้จำนวนเต็มใด ๆ

สามารถเขียนอยู่ในรูปของ $4q, 4q + 1, 4q + 2, 4q + 3$

เนื่องจาก n เป็นจำนวนเต็มคี่ จะได้ว่า $n = 4q + 1$ หรือ $n = 4q + 3$

ดังนั้น $n^2 = (4q + 1)^2$ หรือ $n^2 = (4q + 3)^2$

นั่นคือ $n^2 = 8\,(2q^2 + q) + 1$ หรือ $n^2 = 8\,(2q^2 + 3q + 1) + 1$

กรณีที่ 1 $n^2 = 8\,(2q^2 + q) + 1$

ให้ $k = 2q^2 + q$ จะได้ว่า $n^2 = 8k + 1$

กรณีที่ 2 $n^2 = 8\,(2q^2 + 3q + 1) + 1$

ให้ $k = 2q^2 + 3q + 1$ จะได้ว่า $n^2 = 8k + 1$

ดังนั้น กำลังสองของจำนวนเต็มคี่สามารถเขียนอยู่ในรูปของ $8k + 1$ เมื่อ $k \in \mathbb{Z}$

ตัวอย่าง 2.1.7

จงแสดงว่า สำหรับทุกๆจำนวนเต็ม $a, 3 \mid (a^3 - a)$

การพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ จะได้ว่า $a^3 - a = (a-1)a(a+1)$

โดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม q และ r ที่ $a = 3q + r$ โดยที่ $0 \leq r < 3$

นั่นคือ $r = 0$ หรือ $r = 1$ หรือ $r = 2$

กรณีที่ 1 $r = 0$ เราได้ว่า $3 \mid a$ ทำให้ $3 \mid (a^3 - a)$

กรณีที่ 2 $r = 1$ นั่นคือ $a = 3q + 1$ ทำให้ $a - 1 = 3q$ จะได้ว่า $3 \mid (a - 1)$

และทำให้ $3 \mid [(a-1)a(a+1)]$

กรณีที่ 3 $r = 2$ นั่นคือ $a = 3q + 2$ ทำให้ $a + 1 = 3q + 3 = 3(q + 1)$ จะได้ว่า $3 \mid (a + 1)$

และทำให้ $3 \mid [(a-1)a(a+1)]$

จากทุกกรณี เราจึงสรุปได้ว่า $3 \mid [(a-1)a(a+1)]$ นั่นคือ $3 \mid (a^3 - a)$ □

Gareth A. Jones and J. Mary Jones. (1998 : 3) ได้ยกตัวอย่างที่น่าสนใจเพิ่มเติมดังนี้

ตัวอย่าง 2.1.8

จงแสดงว่ากำลังสองของ n จะเหลือเศษ 0 หรือ 1 เมื่อหารด้วย 4

วิธีทำ ให้ $n = b^2$ และ $a = 4$ โดยทฤษฎีบท 2.1.1

จะได้ $b = 4q + r$ โดยที่ $r = 0, 1, 2$ และ 3

ดังนั้น $n = (4q + r)^2 = 16q^2 + 8qr + r^2$

ถ้า $r = 0$ แล้ว $n = 4(4q^2 + r) + 0$

ถ้า $r = 1$ แล้ว $n = 4(4q^2 + 2qr) + 1$

ถ้า $r = 2$ แล้ว $n = 4(4q^2 + 2qr + 1) + 0$

ถ้า $r = 3$ แล้ว $n = 4(4q^2 + 2qr + 2) + 1$

ดังนั้นกำลังสองของ n จะเหลือเศษ 0 หรือ 1 เมื่อหารด้วย 4

หมายเหตุ โดยขั้นตอนวิธีการหาร ทำให้สามารถจำแนกจำนวนเต็มออกเป็นกลุ่ม ๆ ตามเศษเหลือที่ได้จากการหารด้วยจำนวนเต็มที่ไม่ใช่ศูนย์ (ทบวงมหาวิทยาลัย. 2545 : 3) โดยถ้าเศษที่เหลือจากการหารจำนวนเต็ม n ด้วย 2 คือ 0 นั่นคือมีจำนวนเต็ม k ที่ทำให้ $n = 2k$ จะเรียก n ว่าจำนวนคู่ (even number) แต่ถ้าเศษเหลือที่เกิดจากการหารจำนวนเต็ม n ด้วย 2 คือ 1 นั่นคือ $n = 2k + 1$ บางจำนวนเต็ม k จะเรียก n ว่าจำนวนคี่ (odd number) (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 37)

2.2 การหารลงตัว และสมบัติเบื้องต้นของการหารลงตัว

ในการหารจำนวนเต็มด้วยจำนวนเต็ม เราพบว่า เศษที่เกิดจากการหารอาจเป็นศูนย์ได้ เช่น 132 หารด้วย 4 จะได้ว่า $132 = (33)(4) + 0$ ดังนั้น เศษของการหารคือ 0 เราจะเรียกการหารจำนวนเต็ม ด้วยจำนวนเต็มแล้วเหลือเศษศูนย์ว่า การหารลงตัว (divisibility) ซึ่งมีนิยามดังนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 15, จรินทร์ทิพย์ เฮงคราวิทย์, 2558 : 28, David M. Burton. 2007 : 20)

บทนิยาม 2.2.1

ถ้า a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ เราจะเรียก a ว่าเป็น **ตัวหาร** (divisor) หรือ **ตัวประกอบ** (factor) ตัวหนึ่งของ b ก็ต่อเมื่อ มีจำนวนเต็ม q ที่ทำให้ $b = aq$ ในกรณีที่ a เป็น ตัวหารของ b เราจะเรียกอีกแบบหนึ่งว่า a หาร b ลงตัว เขียนแทนด้วยสัญลักษณ์ $a \mid b$ และใช้ สัญลักษณ์ $a \nmid b$ แทน a หาร b ไม่ลงตัว

ตัวอย่าง 2.2.1

1.) $13 \mid 182$ เพราะมีจำนวนเต็ม 14 ที่ทำให้ $182 = (13)(14)$
2.) $-5 \mid 30$ เพราะมีจำนวนเต็ม -6 ที่ทำให้ $30 = (-5)(-6)$
3.) $17 \mid (-289)$ เพราะมีจำนวนเต็ม -17 ที่ทำให้ $-289 = (17)(-17)$
4.) $135 \mid 0$ เพราะมีจำนวนเต็ม 0 ที่ทำให้ $0 = (135)(0)$
5.) $4 \nmid 15$ เพราะไม่มีจำนวนเต็ม q ใด ๆ ที่ทำให้ $15 = 4q$

ตัวอย่าง 2.2.2

จงแสดงว่า ถ้า a เป็นจำนวนเต็ม แล้ว $3 \mid (a^3 - a)$

การพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ จากขั้นตอนวิธีการหาร a
สามารถเขียนอยู่ในรูปของ $3k$ หรือ $3k+1$
หรือ $3k+2$ สำหรับจำนวนเต็ม k บางจำนวน
ดังนั้น $a^3 - a = (3k)^3 - 3k = 3\left(9k^3 - k\right)$ จะได้ว่า $3 \mid (a^3 - a)$
หรือ $a^3 - a = (3k+1)^3 - (3k+1) = 3\left(9k^3 + 9k^2 + 2k\right)$ จะได้ว่า $3 \mid (a^3 - a)$
หรือ $a^3 - a = (3k+2)^3 - (3k+2) = 3\left(3k^3 + 18k^2 + 11k + 2\right)$
จะได้ว่า $3 \mid (a^3 - a)$
ดังนั้น ถ้า a เป็นจำนวนเต็มใด ๆ แล้ว $3 \mid (a^3 - a)$ □

ตัวอย่าง 2.2.3

$2 \mid 10$ เพราะมีจำนวนเต็ม 5 ซึ่ง $10 = (2)(5)$
$-3 \mid 21$ เพราะมีจำนวนเต็ม -7 ซึ่ง $21 = (-3)(-7)$
$2 \nmid 5$ เพราะไม่มีจำนวนเต็ม c ที่ทำให้ $5 = 2c$

ตัวหารของ 6 คือ $-6, -3, -2, -1, 1, 2, 3$ และ 6 ซึ่งเป็นจำนวนเต็มที่หาร 6 ลงตัว
ตัวหารบวกของ 6 คือ $1, 2, 3$ และ 6 ซึ่งเป็นจำนวนเต็มบวกที่หาร 6 ลงตัว
พหุคูณบวกของ 6 คือ $6, 12, 18, 24, \ldots$ ซึ่งเป็นจำนวนเต็มบวกที่ 6 หารลงตัวนั่นเอง

จาก a เป็นตัวหารของ b แล้วจะได้ว่า $-a$ ก็จะเป็นตัวหารของ b ด้วย (เพราะว่า $b = ac$ แล้ว $b = (-a)(-c)$ ด้วย) ตัวหารหรือตัวประกอบของจำนวนเต็มใด ๆ จะมีจำนวนเป็นคู่เสมอ ในการหาตัวหารทั้งหมดของจำนวนเต็มใด ๆ จึงเป็นการเพียงพอที่จะหาเฉพาะตัวหารที่เป็นบวก ส่วนตัวหารที่เป็นลบจะเป็นจำนวนที่สมนัย (correspond) กัน ด้วยเหตุผลดังกล่าวในการกล่าวถึงตัวหารโดยปกติจะพิจารณาเฉพาะตัวหารที่เป็นจำนวนบวกเท่านั้น ทฤษฎีบทที่จะกล่าวต่อไปนี้เป็นผลโดยตรงจากบทนิยามการหารลงตัว เป็นสมบัติเบื้องต้นที่ควรทราบ และเป็นข้อเท็จจริงที่ใช้การการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็มและจำนวนธรรมชาตินั้น พอสรุปได้ดังนี้ (สมจิต โชติชัยสถิตย์. 2540 : 7, ทิพวัลย์ พัฒนางกูร. 2552 : 28-30, สมวงษ์ แปลงประสพโชค. 2545 : 16, จิราภา ลิ้มบุพศิริพร. 2555 : 6, กิตติภูมิ บำรุงสงฆ์. 2519 : 184-185, David M. Burton. 2007 : 20, Koshy T. 2007 : 75, Coppel W.A. 2009 : 83)

ทฤษฎีบท 2.2.1

ให้ a, b, c เป็นจำนวนเต็ม จะได้ว่า

1.) $a \mid 0,\ 1 \mid a,\ a \mid a$

2.) $a \mid 1$ ก็ต่อเมื่อ $a = \pm 1$

3.) ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$

4.) ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$

5.) ถ้า $a \mid (b + c)$ และ $a \mid b$ แล้ว $a \mid c$

6.) $a \mid b$ และ $b \mid a$ ก็ต่อเมื่อ $a = \pm b$

7.) ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$

8.) ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx + cy)$ สำหรับทุกจำนวนเต็ม x, y

การพิสูจน์ เราจะพิสูจน์เฉพาะข้อ 4.) - 8.) สำหรับข้อ 1.) - 3.) ขอเว้นการพิสูจน์ไว้เป็นแบบฝึกหัด

4.) ให้ $a \mid b$ และ $c \mid d$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $d = cs$
ดังนั้น $bd = (ar)(cs) = (ac)(rs)$ โดยที่ $rs \in \mathbb{Z}$ นั่นคือ $ac \mid bd$

5.) ให้ $a \mid (b + c)$ และ $a \mid b$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b + c = ar$ และ $b = as$
ดังนั้น $c = ar - as = a(r - s)$ โดยที่ $r - s \in \mathbb{Z}$ นั่นคือ $a \mid c$

6.) ($\Rightarrow$) ให้ $a \mid b$ และ $b \mid a$ จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $a = bs$
ดังนั้น $b = (bs)r = b(sr)$ แสดงว่า $rs = 1$
เพราะฉะนั้น ($r = 1$ และ $s = 1$) หรือ ($r = -1$ และ $s = -1$)
นั่นคือ $a = \pm b$
($\Leftarrow$) ให้ $a = \pm b$ เห็นได้ชัดว่า $a \mid b$ และ $b \mid c$

7.) ให้ $a \mid b$ และ $b \neq 0$ จะได้ว่า มี $r \in \mathbb{Z}$ โดยที่ $r \neq 0$ ที่ทำให้ $b = ar$
เนื่องจาก $|b| = |a||r|$ และ $1 \leq |r|$ ดังนั้น $|a| \leq |a||r| = |b|$

8.) ให้ $a \mid b$ และ $a \mid c$ และให้ x, y เป็นจำนวนเต็มใด ๆ
จะได้ว่า มี $r, s \in \mathbb{Z}$ ซึ่ง $b = ar$ และ $c = as$
ดังนั้น $bx = arx$ และ $cy = asy$
แสดงว่า $bx + cy = arx + asy = a(rx + sy)$ โดยที่ $rx + sy \in \mathbb{Z}$
นั่นคือ $a \mid (bx + cy)$ □

ตัวอย่าง 2.2.4

1.) เพราะว่า $5 \mid 25$ และ $25 \mid 100$ จะได้ $5 \mid 100$
2.) เพราะว่า $-7 \mid 49$ และ $3 \mid 9$ จะได้ $-21 \mid 441$
3.) เพราะว่า $3 \mid 99$ และ $3 \mid 12$ จะได้ $3 \mid (99(-2) + 12(5))$
4.) เพราะว่า $x \mid 15$ และ $15 \mid x$ จะได้ $x = \pm 15$

จากทฤษฎีบท 2.2.1 ข้อ 8 เราสามารถขยายผลได้ดังนี้

บทแทรก 2.2.1

สำหรับจำนวนเต็ม $a, b_1, b_2, \ldots, b_n$ ใด ๆ ที่ $a \neq 0$ จะได้ว่า ถ้า $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$ แล้ว $a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$ เมื่อ $x_1, x_2, \ldots, x_n$ เป็นจำนวนเต็มใด ๆ

ตัวอย่าง 2.2.5

ให้ a, b, c เป็นจำนวนเต็ม จงแสดงว่า
1.) ถ้า $a \mid b$ แล้ว $a \mid bc$
2.) ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a^2 \mid bc$

การพิสูจน์ 1.) ให้ $a \mid b$ จะได้ว่า มี $k \in \mathbb{Z}$ ซึ่งทำให้ $b = ak$
คูณ c ตลอด จะได้ $bc = akc = a(kc) = am$ โดยที่ $m = kc \in \mathbb{Z}$
ดังนั้น $a \mid bc$

2.) ให้ $a \mid b$ และ $a \mid c$ จะได้ว่า มี $m, n \in \mathbb{Z}$ ซึ่ง $b = am$ และ $c = an$
จะได้ $bc = (am)(an) = a^2(mn) = a^2k$ โดยที่ $k = mn \in \mathbb{Z}$
ดังนั้น $a^2 \mid bc$ □

2.3 การพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์

ธนัชยศ จำปาหวาย (2559 : 42-44) ได้กล่าวว่า เมื่อต้องการพิสูจน์ข้อความ $3 \mid (5^n - 2^n)$ สำหรับ n เป็นจำนวนเต็มบวก จะเห็นได้ว่า $5^n - 2^n$ อยู่ในรูปเลขยกกำลัง ถ้าจะใช้ขั้นตอนวิธีการหารแบ่ง n ออกเป็นกรณีตามเศษเหลือจะไม่สามารถพิสูจน์ข้อความนี้ได้ อีกทางหนึ่งที่ทำได้คือใช้หลักอุปนัยเชิงคณิตศาสตร์พิสูจน์ข้อความดังกล่าว ซึ่งทำได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.3.1

จงแสดงว่า $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก

การพิสูจน์ ให้ $P(n)$ แทนข้อความ $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก
1. ขั้นฐาน : เนื่องจาก $3 \mid (5^1 - 2^1)$ ดังนั้น $P(1)$ เป็นจริง
2. ขั้นอุปนัย : สมมติว่า $P(k)$ เป็นจริง เมื่อ $k \in \mathbb{N}$ นั่นคือ $3 \mid \left(5^k - 2^k\right)$ มีจำนวนเต็ม q ซึ่ง

$$5^k - 2^k = 3q$$

โดยสมมติฐานจะได้ว่า

$$\begin{aligned} 5^{k+1} - 2^{k+1} &= 5 \cdot 5^k - 2 \cdot 2^k \\ &= (3+2) \cdot 5^k - 2 \cdot 2^k \\ &= 3 \cdot 5^k + 2 \cdot 5^k - 2 \cdot 2^k \\ &= 3 \cdot 5^k + 2\left(5^k - 2^k\right) \\ &= 3 \cdot 5^k + 2(3q) \\ &= 3\left(5^k + 2q\right) \end{aligned}$$

ดังนั้น $3 \mid \left(5^{k+1} - 2^{k+1}\right)$ นั่นคือ $P(k+1)$ เป็นจริง
สรุปได้ว่า $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก □

ตัวอย่าง 2.3.2

จงแสดงว่า $5 \mid (3^{3n+1} + 2^{n+1})$ เมื่อ n เป็นจำนวนเต็มบวก

การพิสูจน์ ให้ $P(n)$ แทนข้อความ $5 \mid (3^{3n+1} + 2^{n+1})$ เมื่อ n เป็นจำนวนเต็มบวก
1. ขั้นฐาน : เนื่องจาก $3^4 + 2^2 = 85$ ดังนั้น $5 \mid \left(3^{3(1)+1} + 2^{1+1}\right)$ ทำให้ได้ว่า $P(1)$ เป็นจริง
2. ขั้นอุปนัย : สมมติว่า $P(k)$ เป็นจริง เมื่อ $k \in \mathbb{N}$ นั่นคือ $5 \mid \left(3^{3k+1} + 2^{k+1}\right)$ มีจำนวนเต็ม q ซึ่ง

$$3^{3k+1} + 2^{k+1} = 5q$$

โดยสมมติฐานจะได้ว่า

$$\begin{aligned} 3^{3(k+1)+1} + 2^{(k+1)+1} &= 3^{(3k+1)+3} + 2^{k+1} \cdot 2 \\ &= 3^{(3k+1)} \cdot 3^3 + 2^{k+1} \cdot 2 \\ &= 3^{(3k+1)} \cdot 27 + 2^{k+1} \cdot 2 \\ &= 3^{(3k+1)} \cdot (25+2) + 2^{k+1} \cdot 2 \\ &= 3^{(3k+1)} \cdot 25 + 2\left(3^{(3k+1)} + 2^{k+1}\right) \\ &= 3^{(3k+1)} \cdot 25 + 2(5q) \\ &= 5\left(3^{(3k+1)} \cdot 5 + 2q\right) \end{aligned}$$

ดังนั้น $5 \mid \left(3^{3(k+1)+1} + 2^{(k+1)+1}\right)$ นั่นคือ $P(k+1)$ เป็นจริง
สรุปได้ว่า $5 \mid (3^{3n+1} + 2^{n+1})$ เมื่อ n เป็นจำนวนเต็มบวก □

ตัวอย่าง 2.3.3

จงแสดงว่า $8 \mid (5^{2n} + 7)$ เมื่อ n เป็นจำนวนเต็มบวก

การพิสูจน์ ให้ $P(n)$ แทนข้อความ $8 \mid (5^{2n} + 7)$ เมื่อ n เป็นจำนวนเต็มบวก
1. ขั้นฐาน : เนื่องจาก $5^2 + 7 = 32$ ดังนั้น $8 \mid (5^{2(1)} + 7)$ ทำให้ได้ว่า $P(1)$ เป็นจริง
2. ขั้นอุปนัย : สมมติว่า $P(k)$ เป็นจริง เมื่อ $k \in \mathbb{N}$ นั่นคือ $8 \mid (5^{2k} + 7)$ จะมีจำนวนเต็ม q ซึ่ง

$$5^{2k} + 7 = 8q$$

โดยสมมติฐานจะได้ว่า

$$\begin{aligned} 5^{2(k+1)} + 7 &= 5^{2k+2} + 7 \\ &= 5^{2k} \cdot 5^2 + 7 \\ &= (8q - 7) \cdot 25 + 7 \\ &= 8q \cdot 25 - 168 \\ &= 8(25q - 21) \end{aligned}$$

ดังนั้น $8 \mid (5^{2(k+1)} + 7)$
นั่นคือ $P(k+1)$ เป็นจริง
สรุปได้ว่า $8 \mid (5^{2n} + 7)$ เมื่อ n เป็นจำนวนเต็มบวก □

ตัวอย่าง 2.3.4

จงแสดงว่า $(3!)^n \mid (3n)!$ สำหรับทุกจำนวนนับ n

การพิสูจน์ ให้ $n \in \mathbb{N}$ และ $P(n)$ แทนข้อความ $(3!)^n \mid (3n)!$ สำหรับทุกจำนวนนับ n
1. ขั้นฐาน : เนื่องจาก $(3!)^1 = 3! = (3 \cdot 1)!$ นั่นคือ $(3!)^1 \mid (3 \cdot 1)!$ ดังนั้น $P(1)$ เป็นจริง
2. ขั้นอุปนัย : ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ $(3!)^k \mid (3k)!$
จะได้ว่ามีจำนวนเต็ม m ซึ่ง $(3k)! = m(3!)^k$ แล้ว

$$\begin{aligned} (3(k+1))! = (3k+3)! &= (3k+3)(3k+2)(3k+1)(3k)! \\ &= 3(k+1)(3k+2)(3k+1)m(3!)^k \end{aligned}$$

เมื่อให้ $a = 3k + 1$ จะได้ $(3k+2)(3k+1) = (a+1)a$

$$= a^2 + a$$

จะได้ว่า $2 \mid (a^2 + a)$ นั่นคือ

$$(3k+2)(3k+1) = 2p$$

สำหรับบางจำนวนเต็ม p ดังนั้น

$$\begin{aligned} (3(k+1))! = (3k+3)! &= 3(k+1)2pm(3!)^k = (k+1)pm \cdot 6(3!)^k \\ &= (k+1)pm \cdot 3!(3!)^k = (k+1)pm \cdot (3!)^{k+1} \end{aligned}$$

จะได้ว่า $(3!)^{k+1} \mid (3(k+1))!$ นั่นคือ $P(k+1)$ เป็นจริง
สรุปได้ว่า $(3!)^n \mid (3n)!$ สำหรับทุกจำนวนนับ n □

ตัวอย่าง 2.3.5

จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า

$6 \mid (7^n - 1)$ สำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ ให้ $P(n)$ แทน 6 หาร $7^n - 1$ ลงตัว

1) เพราะว่า $7^1 - 1 = 6$ ซึ่ง 6 หารลงตัว ดังนั้น $P(1)$ เป็นจริง

2) สมมติให้ $P(k)$ เป็นจริง นั่นคือ $6 \mid (7^k - 1)$
จะแสดงว่า $P(k+1)$ เป็นจริงด้วย นั่นคือจะแสดงว่า $6 \mid (7^{k+1} - 1)$

พิจารณา $7^{k+1}-1 = 7^k \cdot 7^1 - 1$

$= 7 \cdot 7^k - 1$

$= (6+1)7^k - 1$

$= 6 \cdot 7^k + (7^k - 1)$

แต่ $6 \mid 6 \cdot 7^k$ และ $6 \mid (7^k - 1)$

ดังนั้น $6 \mid [6 \cdot 7^k + (7^k - 1)]$

จะได้ว่า $P(k+1)$ เป็นจริง โดยหลักอุปนัยเชิงคณิตศาสตร์

จะได้ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

นั่นคือ $6 \mid (7^n - 1)$ สำหรับทุกจำนวนเต็มบวก n □

ตัวอย่าง 2.3.6

จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า

$$24 \mid (713 \cdot 9^{3n-2} + 15) \text{ สำหรับทุกจำนวนเต็มบวก } n$$

การพิสูจน์ ให้ $P(n)$ แทน $24 \mid (713 \cdot 9^{3n-2} + 15)$

1) เพราะว่า $24 \mid (713 \cdot 9^{3(1)-2} + 15)$ ดังนั้น $P(1)$ เป็นจริง

2) สมมติให้ $P(k)$ เป็นจริง นั่นคือ $24 \mid (713 \cdot 9^{3k-2} + 15)$

จะแสดงว่า $P(k+1)$ เป็นจริงด้วย นั่นคือจะแสดงว่า $24 \mid (713 \cdot 9^{3(k+1)-2} + 15)$

พิจารณา $713 \cdot 9^{3(k+1)-2} + 15 = 713 \cdot 9^3 \cdot 9^{3k-2} + 15$

$= 713 \cdot 9^3 \cdot 9^{3k-2} + 9^3(15) - 9^3(15) + 15$

$= 9^3(713 \cdot 9^{3k-2} + 15) - 9^3(15) + 15$

$= 9^3(713 \cdot 9^{3k-2} + 15) - 24(455)$

แต่ $24 \mid 9^3(713 \cdot 9^{3k-2} + 15)$ และ $24 \mid -24(455)$

ดังนั้น $24 \mid [9^3(713 \cdot 9^{3k-2} + 15) - 24(455)]$

จะได้ว่า $P(k+1)$ เป็นจริง โดยหลักอุปนัยเชิงคณิตศาสตร์

จะได้ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

นั่นคือ $24 \mid (713 \cdot 9^{3n-2} + 15)$ สำหรับทุกจำนวนเต็มบวก n □

ดำรงค์ ทิพย์โยธา (2556 : 10-12) ได้ให้ตัวอย่างเพิ่มเติมเกี่ยวกับการพิสูจน์การหารลงตัว โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.3.7

จงแสดงว่า $7 \mid (n^7 - n)$ ทุกค่า $n \in \mathbb{N}$

การพิสูจน์ ให้ $a_n = n^7 - n$

ให้ $P(n)$ แทนข้อความ "$7 \mid a_n$"

(1) จะแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $a_1 = 0$ เพราะฉะนั้น $7 \mid a_1$ จะได้ว่า $P(1)$ เป็นจริง

(2) จะแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

พิจารณา $a_{k+1} - a_k = \big((k+1)^7 - (k+1)\big) - (k^7 - k)$

$= (k+1)^7 - k^7 - 1$

$= (k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1) - k^7 - 1$

$= 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k$

$= 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k)$

เพราะฉะนั้น $a_{k+1} = 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k) + a_k$

จาก $P(k)$ เป็นจริง จะได้ว่า $7 \mid a_k$ และ $7 \mid 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k)$

เพราะฉะนั้น $7 \mid a_{k+1}$ ดังนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $7 \mid (n^7 - n)$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 2.3.8

ให้ a, b เป็นจำนวนเต็ม และ $a \neq b$ จงแสดงว่า $(a-b) \mid (a^n - b^n)$ ทุกค่า $n \in \mathbb{N}$

การพิสูจน์ ให้ $P(n)$ แทนข้อความ "$(a-b) \mid (a^n - b^n)$"

(1) จะแสดงว่า $P(n)$ เป็นจริง

เพราะว่า $(a-b) \mid (a-b)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) จะแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะฉะนั้น $(a-b) \mid (a^k - b^k)$

พิจารณา $a^{k+1} - b^{k+1} = aa^k - b^k b$

$= aa^k - ab^k + ab^k - b^k b$

$= a(a^k - b^k) + b^k(a-b)$

จาก $(a-b) \mid (a^k - b^k)$ และ $(a-b) \mid (a-b)$

จะได่ว่า $(a-b) \mid (a^{k+1} - b^{k+1})$ เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $(a-b) \mid (a^n - b^n)$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 2.3.9

จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า

$(a+b) \mid (a^{2n} - b^{2n})$ สำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ ให้ $P(n)$ แทน $(a+b) \mid (a^{2n} - b^{2n})$ สำหรับทุกจำนวนเต็มบวก n

1) เพราะว่า $a^{2(1)} - b^{2(1)} = (a+b)(a-b)$

จะได้ $(a+b) \mid (a+b)(a-b)$ ดังนั้น $P(1)$ เป็นจริง

2) สมมติให้ $P(k)$ เป็นจริง นั่นคือ $(a+b) \mid (a^{2k} - b^{2k})$

จะแสดงว่า $P(k+1)$ เป็นจริงด้วย นั่นคือจะแสดงว่า $(a+b) \mid (a^{2(k+1)} - b^{2(k+1)})$

พิจารณา $a^{2(k+1)} - b^{2(k+1)} = a^2 \cdot a^{2k} - b^2 \cdot b^{2k}$

$= a^2 \cdot a^{2k} - a^2 \cdot b^{2k} + a^2 \cdot b^{2k} - b^2 \cdot b^{2k}$

$= a^2(a^{2k} - b^{2k}) + b^{2k}(a^2 - b^2)$

แต่ $(a+b) \mid a^2(a^{2k} - b^{2k})$ และ $(a+b) \mid b^{2k}(a^2 - b^2)$

ดังนั้น $(a+b) \mid [a^2(a^{2k} - b^{2k}) + b^{2k}(a^2 - b^2)]$

นั่นคือ $(a+b) \mid (a^{2(k+1)} - b^{2(k+1)})$

จะได้ว่า $P(k+1)$ เป็นจริง โดยหลักอุปนัยเชิงคณิตศาสตร์

จะได้ $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n

นั่นคือ $(a+b) \mid (a^{2n} - b^{2n})$ สำหรับทุกจำนวนเต็มบวก n □

2.4 ตัวหารร่วมมาก

จรินทร์ทิพย์ เฮงคราวิทย์ (2558 : 45) ถ้า a, b เป็นจำนวนเต็มใด ๆ จำนวนเต็ม d จะเรียกว่า **ตัวหารร่วม** (common divisor) ของ a และ b ถ้า $d \mid a$ และ $d \mid b$ ดังนั้นเซตของตัวหารร่วมจะไม่ เป็นเซตว่าง เพราะว่ามี $1, -1$ เป็นตัวหารร่วมของ a และ b เสมอ เซตของตัวหารร่วมจะเป็นเซตจำกัด เมื่อ $a \neq 0$ หรือ $b \neq 0$ เป็นเซตอนันต์เมื่อ $a = b = 0$

ตัวอย่าง 2.4.1

จงหาเซตของตัวหารร่วมทั้งหมดของ 50 และ 76

วิธีทำ เซตของหารทั้งหมดของ 50 คือ $A = \{-1, -2, -5, -25, -50, 1, 2, 5, 25, 50\}$

เซตของตัวหารทั้งหมดของ 76 คือ $B = \{-1, -2, -4, -19, -38, -76, 1, 2, 4, 19, 38, 76\}$

จะได้ว่า $A \cap B = \{-1, -2, 1, 2\}$

ดังนั้นเซตของตัวหารร่วมทั้งหมดของ 50 และ 76 คือ $\{-1, -2, 1, 2\}$

ตัวอย่าง 2.4.2

จงหาตัวหารร่วมมากของ 24,60 และ 30

วิธีทำ เนื่องจากตัวหารที่เป็นบวกของ 24 คือ $1, 2, 3, 4, 6, 8, 12, 24$

ตัวหารที่เป็นบวกของ 60 คือ $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$

และตัวหารที่เป็นบวกของ 30 คือ $1, 2, 3, 5, 6, 10, 15, 30$

จะได้ว่าตัวหารร่วมที่เป็นบวกของ $24, 60$ และ 30 คือ $1, 2, 3$ และ 6

ดังนั้นตัวหารร่วมมากของ $24, 60$ และ 30 คือ 6

เขียนเป็นสัญลักษณ์ได้ว่า $(24, 60, 30) = 6$

จากตัวอย่างข้างต้นจะได้ว่าเซตของตัวหารร่วมจะมีสมาชิกที่มีค่ามากที่สุดหรือเป็นตัวหารร่วมที่มีค่ามากที่สุด ซึ่งนิยามดังนี้ (จิราภา ลิ้มบุพศิริพร. 2555 : 11, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 45, รัชนียา ถิรเดโชชัย. 2560 : 113, David M. Burton. 2007 : 21)

บทนิยาม 2.4.1

ให้ a, b เป็นจำนวนเต็ม ซึ่ง $a \neq 0$ หรือ $b \neq 0$ เราจะเรียกจำนวนเต็มบวก d ว่า **ตัวหารร่วมมาก** (greatest common divisor) หรือ ห.ร.ม. (G.C.D.) ของ a และ b เขียนแทนด้วย (a, b) ก็ต่อเมื่อ d มีสมบัติต่อไปนี้

(1) $d \mid a$ และ $d \mid b$

(2) ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$

จากบทนิยาม เราพบว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า

(1) เราสามารถหา (a, b) ได้เสมอ

(2) (a, b) มีเพียงจำนวนเดียวเท่านั้น

(3) $(a, b) = (a, -b) = (-a, b) = (-a, -b) = (b, a)$

(4) $(a, 0) = |a|$ เมื่อ $a \neq 0$

(5) ถ้า $a \mid b$ แล้ว $(a, b) = |a|$

ตัวอย่าง 2.4.3

1.) $(24, 84) = (84, 24) = 12$

2.) $(-6, -15) = (6, 15) = 3$

3.) $(-17, 289) = (17, -289) = 3$

4.) $(540, 450) = (-450, -540) = 90$

ตัวหารร่วมมากจะมีเพียงตัวเดียวเท่านั้น ดังทฤษฎีบทต่อไปนี้ (สมวงษ์ แปลงประสบโชค. 2545 : 24, ปวีณา ถ้ำแก้ว. 2558 : 89)

ทฤษฎีบท 2.4.1

ตัวหารร่วมมากของจำนวนเต็ม a และ b จะมีเพียงตัวเดียวเท่านั้น

การพิสูจน์ ให้ d เป็นตัวหารร่วมมาก ของ a และ b จะได้ $d \mid a$ และ $d \mid b$

ให้ c เป็นตัวหารร่วมมาก ของ a และ b จะได้ $c \mid a$ และ $c \mid b$

เนื่องจาก c และ d เป็นตัวหารร่วมของ a และ b ดังนั้น $c \mid d$ และ $d \mid c$

จาก $c \mid d$ และ $d \mid c$ และโดยที่ $c, d > 0$ จะได้ $c = d$ □

ตัวอย่าง 2.4.4

ตัวหารที่เป็นบวกทั้งหมดของ -12 คือ $1, 2, 3, 4$ และ 6

ตัวหารที่เป็นบวกทั้งหมดของ 30 คือ $1, 2, 3, 5, 6, 10, 15$ และ 30

ดังนั้น เซตของตัวหารร่วมคือ $1, 2, 3$ และ 6 จึงได้ว่า $(-12, 30) = 6$

ทฤษฎีบท 2.4.2

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า มี $x, y \in \mathbb{Z}$ ที่ทำให้ $(a, b) = ax + by$

การพิสูจน์ ให้ $X = \{am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0\}$

เนื่องจาก $a \neq 0$ หรือ $b \neq 0$ ดังนั้น $X \neq \varnothing$ และ $X \subseteq \mathbb{N}$

จากหลักการจัดอันดับดีจะได้ว่ามี $d \in X$ ซึ่ง d เป็นจำนวนเต็มบวกที่น้อยที่สุดใน X
ฉะนั้นมี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ ต่อไปนี้จะแสดงว่า $d = (a, b)$

(i) จาก $a, d \in \mathbb{Z}$ และ $d \in X$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$
ที่ทำให้ $a = dq + r, 0 \leq r < d$
$a = (ax + by)q + r, 0 \leq r < d$ (จาก $d = ax + by$)
$r = a - (ax + by)q, 0 \leq r < d$
ดังนั้น $r = a(1 - xq) + b(-yq), 0 \leq r < d$
จาก $0 \leq r < d$ จะได้ว่า $r = 0$ หรือ $0 < r < d$
ถ้า $0 < r < d$ จะได้ว่า $r \in X$ ซึ่งขัดแย้งกับการเลือก d เป็นจำนวนเต็มบวกที่น้อยที่สุดใน X
ดังนั้น $r = 0$ นั่นคือ $d \mid a$
จาก $b, d \in \mathbb{Z}$ และ $d \in X$ พิสูจน์ในทำนองเดียวกันจะได้ว่า $d \mid b$

(ii) ให้ $c \mid a$ และ $c \mid b$ จะได้ว่า $c \mid (ax + by)$ นั่นคือ $c \mid d$

จาก (i) และ (ii) จะได้ว่า มี $x, y \in \mathbb{Z}$ ซึ่งทำให้ $(a, b) = ax + by$ □

บทแทรก 2.4.1

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่าสำหรับจำนวนเต็ม c ใด ๆ ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid (a, b)$

การพิสูจน์ ให้ $d = (a, b)$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$
และจาก $c \mid a$ และ $c \mid b$ โดยทฤษฎีบท 2.2.1 ข้อ 8. จะได้ว่า $c \mid (ax + by)$
นั่นคือ $c \mid d$ □

ทฤษฎีบท 2.4.3

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า $(a, b) = 1$ ก็ต่อเมื่อมี $x, y \in \mathbb{Z}$ ที่ ทำให้ $1 = ax + by$

การพิสูจน์ ($\Rightarrow$) สมมติว่า $(a, b) = 1$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $1 = ax + by$
($\Leftarrow$) สมมติว่ามี $x, y \in \mathbb{Z}$ ซึ่งทำให้ $1 = ax + by$ และให้ $d = (a, b)$
จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (ax + by)$
นั่นคือ $d \mid 1$ แสดงว่า $(a, b) = 1$ □

จากทฤษฎีบท 2.4.3 สามารถขยายได้เป็นทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.4.4

สำหรับจำนนเต็ม $a_1, a_2, \ldots, a_n$ ใด ๆ $(a_1, a_2, \ldots, a_n) = 1$ ก็ต่อเมื่อ มีจำนวนเต็ม $x1, x_2, \ldots, x_n$ ที่ทำให้ $1 = a_1x_1 + a_2x_2 + \cdots + a_nx_n$

การพิสูจน์ พิสูจน์ในทำนองเดียวกันกับทฤษฎีบท 2.4.3 เว้นไว้เป็นแบบฝึกหัด □

ทฤษฎีบท 2.4.5

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ และ m เป็นจำนวนเต็มบวก จะได้ว่า $(ma, mb) = m(a, b)$

การพิสูจน์ ให้ $D = (ma, mb)$ และ $d = (a, b)$ โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x, y, u, v \in \mathbb{Z}$ ซึ่ง ทำให้ $D = (ma)x + (mb)y$ และ $d = au + bv$

(i) จาก $D = (ma, mb)$ จะได้ว่า $D \mid ma$ และ $D \mid mb$
ดังนั้น $D \mid (mau + mbv)$ นั่นคือ $D \mid md$

(ii) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (ax + by)$
จะได้ว่า $md \mid (ax + by)$ นั่นคือ $md \mid D$
จาก (i) และ (ii) จะได้ว่า $D = md$
แสดงว่า $(ma, mb) = m(a, b)$ □

ทฤษฎีบท 2.4.6

ถ้า $a, b \in \mathbb{Z}$ โดยที่ $d = (a, b)$ แล้ว $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

การพิสูจน์ ให้ $d = (a, b)$ จะได้ว่า $d = \left(\frac{da}{d}, \frac{db}{d}\right)$

โดยทฤษฎีบท 2.4.5 จะได้ $d = d\left(\frac{a}{d}, \frac{b}{d}\right)$ ดังนั้น $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ □

ดำรงค์ ทิพย์โยธา (2556 : 49) ได้ขยายทฤษฎีบท 2.4.6 ได้ผลดังทฤษฎีต่อไปนี้

ทฤษฎีบท 2.4.7

ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็ม ถ้า $d = (a_1, a_2, \ldots, a_n)$ แล้ว $\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$

การพิสูจน์ ให้ $d = (a_1, a_2, \ldots, a_n)$ $\cdots\cdots(1)$
สมมติ $\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) \neq 1$ $\cdots\cdots(2)$
เพราะฉะนั้น มีจำนวนเฉพาะ p เป็นตัวประกอบของ

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right)$$

เพราะฉะนั้น $p \mid \frac{a_i}{d}$ ทุกค่า $i = 1, 2, \ldots, n \Rightarrow pd \mid a_i$ ทุกค่า $i = 1, 2, \ldots, n$

$$\Rightarrow pd \mid (a_1, a_2, \ldots, a_n)$$
$$\Rightarrow pd \mid d$$
$$\Rightarrow pd \mid 1$$
$$\Rightarrow p \mid 1$$

เพราะฉะนั้น $p = 1$ เกิดข้อขัดแย้งกับที่ p เป็นจำนวนเฉพาะ
เพราะฉะนั้นที่สมมติ $\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) \neq 1$ ไม่จริง
เพราะฉะนั้น $\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$ □

ทฤษฎีบท 2.4.8

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ และ x เป็นจำนวนเต็ม จะได้ว่า

$$(a, b) = (a, b + ax) = (a + bx, b)$$

การพิสูจน์ ให้ $d=(a,b)$ และ $g=(a,b+ax)$ 2.4.2 จะได้ว่ามี $u,v,m,n\in\mathbb{Z}$ ที่
ทำให้ $d=au+bv$ และ $g=am+(b+ax)n$

(i) จาก $d=(a,b)$ จะได้ว่า $d\mid a$ และ $d\mid b$
ดังนั้นโดยทฤษฎีบท 2.2.1 ข้อ 8 จะได้ $d\mid(am+bn+axn)$ นั่นคือ $d\mid g$

(ii) จาก $g=(a,b+ax)$ จะได้ว่า $g\mid a$ และ $g\mid(b+ax)$
ดังนั้น $g\mid ax$ โดยทฤษฎีบท 2.2.1 ข้อ 5 จะได้ว่า $g\mid b$ ดังนั้น $g\mid(au+bv)$ นั่นคือ $g\mid d$
จาก (i) และ (ii) จะได้ว่า $d=g$ แสดงว่า $(a,b)=(a,b+ax)$
และในทำนองเดียวกันเราสามารถพิสูจน์ได้ว่า $(a,b)=(a+bx,b)$ □

ดำรงค์ ทิพย์โยธา (2556 : 40) ได้ยกตัวอย่างที่นำสมบัติที่ได้จากทฤษฎีบท 2.4.8 ไปใช้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.4.5

ให้ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่า $(n!+1,(n+1)!+1)=1$

การพิสูจน์ จากทฤษฎีบท 2.4.8 จะได้ว่า

$$\begin{aligned}(n!+1,(n+1)!+1)&=(n!+1,(n+1)!+1-(n!+1)(n+1))\\&=(n!+1,-n)\\&=(-n,n!+1)\\&=(-n,n!+1-n(n-1)!)\\&=(-n,1)\\&=1\end{aligned}$$

□

ตัวอย่าง 2.4.6

จงแสดงว่า $\dfrac{21n+4}{14n+3}$ เป็นเศษส่วนอย่างต่ำ ทุก ๆ จำนวนเต็มบวก n

การพิสูจน์ จากทฤษฎีบท 2.4.8 จะได้ว่า

$$\begin{aligned}(14n+3,21n+4)&=(14n+3,21n+4-(14n+3))\\&=(14n+3,7n+1)\\&=(7n+1,14n+3)\\&=(7n+1,14n+3-2(7n+1))\\&=(7n+1,1)\\&=1\end{aligned}$$

เพราะฉะนั้น $14n+3$ กับ $21n+4$ ไม่มีตัวประกอบร่วม
จะได้ว่า $\dfrac{21n+4}{14n+3}$ เป็นเศษส่วนอย่างต่ำ □

ทฤษฎีบท 2.4.9

ให้ $a, b, c, m \in \mathbb{Z}$ เป็นจำนวนเต็ม จะได้ว่า

1. ถ้า $(a, m) = (b, m) = 1$ แล้ว $(ab, m) = 1$
2. ถ้า $(a, m) = 1$ และ $b \mid a$ แล้ว $(b, m) = 1$
3. ถ้า $a \mid bc$ และ $(a, b) = 1$ แล้ว $a \mid c$
4. ถ้า $a \mid c$ และ $b \mid c$ โดยที่ $(a, b) = 1$ แล้ว $ab \mid c$

การพิสูจน์ 1. ให้ $(a, m) = (b, m) = 1$ จะได้ว่ามี $x, y, u, v \in \mathbb{Z}$ ซึ่ง
$ax + my = 1$ และ $bu + mv = 1$
ดังนั้น $1 = (ax + my)(bu + mv) = ab(xu) + m(axv + ybu + myv)$
โดยทฤษฎีบท 2.4.3 จะได้ว่า $(ab, m) = 1$

2. ให้ $(a, m) = 1$ และ $b \mid a$ จะได้ว่ามี $x, y, q \in \mathbb{Z}$ ซึ่ง $ax + my = 1$ และ bq
ดังนั้น $1 = (bq)x + my = b(qx) + my$
โดยทฤษฎีบท 2.4.4 จะได้ว่า $(b, m) = 1$

3. ให้ $a \mid bc$ และ $(a, b) = 1$ จะได้ว่ามี $q, x, y \in \mathbb{Z}$ ซึ่ง $bc = aq$ และ $ax + by = 1$
ดังนั้น $bcy = aqy$ และ $c = axc + byc$
ดังนั้น $c = axc + aqy = a(xc + qy)$ นั่นคือ $a \mid c$

4. ให้ $a \mid c$ และ $b \mid c$ โดยที่ $(a, b) = 1$ จะได้ว่ามี $k_1, k_2, x, y \in \mathbb{Z}$
ซึ่ง $c = ak_1, c = bk_2$ และ $ax + by = 1$
ดังนั้น $c = cax + cby = (bk_2)\, ax + (ak_1)\, by = ab\,(k_1x + k_1y)$
นั่นคือ $ab \mid c$ □

ทฤษฎีบท 2.4.10

ให้ $a, b, q, r \in \mathbb{Z}$ โดยที่ $a > 0$ และ $b = aq + r, 0 \leq r < a$ จะได้ว่า $(a, b) = (a, r)$

การพิสูจน์ ให้ $d = (a, b)$ และ $g = (a, r)$ จะต้องพิสูจน์ว่า $d = g$

(i) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$
และจาก $b = aq + r$ เราได้ $d \mid a$ และ $d \mid r$
ดังนั้น d เป็นตัวหารร่วมของ a และ r โดยบทแทรก 2.4.1 จะได้ว่า $d \mid g$

(ii) จาก $g = (a, r)$ จะได้ว่า $g \mid a$ และ $g \mid r$
และจาก $r = aq - b$ เราได้ $g \mid a$ และ $g \mid b$
ดังนั้น g เป็นตัวหารร่วมของ a และ b โดยบทแทรก 2.4.1 จะได้ว่า $g \mid d$
จาก (i) และ (ii) สรุปได้ว่า $(a, b) = (a, r)$ □

ตัวอย่าง 2.4.7

1. $(252, 298) = (198, 54) = (54, 36) = (36, 18) = (18, 0) = 18$
2. $(927, 315) = (315, 297) = (297, 18) = (18, 9) = (9, 0) = 9$
3. $(1000, 925) = (925, 75) = (75, 25) = (25, 0) = 25$
4. $(2004, 1106) = (1106, 898) = (898, 208) = (208, 66) = (66, 10) = (10, 6) = (6, 4) = 2$

ตัวอย่าง 2.4.8

จงหาค่าของ $(1769, 2378)$

วิธีทำ จาก $2378 = (1)(1769) + 609$ จะได้ $(1769, 2378) = (1769, 609)$
จาก $1769 = (2)(609) + 551$ จะได้ $(1769, 609) = (609, 551)$
จาก $609 = (1)(551) + 58$ จะได้ $(609, 551) = (551, 58)$
จาก $551 = (9)(58) + 29$ จะได้ $(551, 29) = (58, 29) = 29$
ดังนั้น $(1769, 2378) = 29$

ตัวอย่าง 2.4.9

จงหา $(216, 84)$ จงหาจำนวนเต็ม x, y ที่ทำให้ $(216, 84) = 216x + 84y$

วิธีทำ พิจารณา

$$\begin{aligned} 216 &= (84)(2) = 48 && \cdots(1) \\ 84 &= (48)(1) = 36 && \cdots(2) \\ 48 &= (36)(1) = 12 && \cdots(3) \\ 36 &= (12)(3) \end{aligned}$$

เพราะฉะนั้น $(216, 84) = 12$
โดยแทนค่าย้อนกลับจะได้

$$\begin{aligned} 12 &= 48 - (36)(1) && \cdots(3) \\ &= 48 - 36 \\ &= 48 - (84 - (48)(1)) && \cdots(2) \\ &= 2(48) - 84 \\ &= 2(216 - (84)(2)) - 84 && \cdots(1) \\ &= (216)(2) + (84)(-5) \end{aligned}$$

เพราะฉะนั้นมี $x = 2$ และ $y = -5$ ที่ทำให้ $12 = 216x + 84y$

หมายเหตุ 1. ขั้นตอนการคำนวณข้างต้นสามารถเขียนในรูปแบบตารางคำนวณดังนี้

		216	84		
ขั้นที่ 1	2	168			
		48	84		
			48	1	ขั้นที่ 2
		48	36		
ขั้นที่ 3	1	36			
		12	36		
			36	3	ขั้นที่ 4
			0		

เริ่มต้นให้ a เป็นจำนวนที่มากกว่า b

ขั้นที่ 1 หาจำนวนเต็มบวกค่ามากสุดคือ 2 ที่คูณกับ 84 แล้วมีค่าไม่เกิน 216 ได้ $216 - 84(2) = 48$

ขั้นที่ 2 หาจำนวนเต็มบวกค่ามากสุดคือ 1 ที่คูณกับ 48 แล้วมีค่าไม่เกิน 84 ได้ $84 - 48(1) = 36$

ขั้นที่ 3 หาจำนวนเต็มบวกค่ามากสุดคือ 1 ที่คูณกับ 36 แล้วมีค่าไม่เกิน 48 ได้ $48 - 36(1) = 12$

ขั้นที่ 4 หาจำนวนเต็มบวกค่ามากสุดคือ 3 ที่คูณกับ 12 แล้วมีค่าไม่เกิน 36 ได้ $36 - 12(3) = 0$

ในทำนองเดียวกันจะได้ $12 = (12, 36) = (36, 48) = (48, 84) = (84, 216)$

เพราะฉะนั้น $(216, 84) = 12$

รูปแบบตารางสามารถเขียนแบบย่อได้อีกแบบหนึ่งดังนี้

		216	84		
ขั้นที่ 1	2	168	48	1	ขั้นที่ 2
		48	36		
ขั้นที่ 3	1	36	36	3	ขั้นที่ 4
		12	0		

2. จำนวนเต็ม x, y ที่ทำให้ $(216, 84) = 216x + 84y$ มีได้หลายค่าเช่น
   $x = 2, y = -5$ จะได้ $216(2) + 84(-5) = 12$
   $x = 2 - 84, y = -5 + 216$ จะได้ $216(2 - 84) + 84(-5 + 216) = 12$
3. การหา $(216, 84)$ สามารถเลือกจากตัวประกอบที่เป็นจำนวนเฉพาะ $216 = 2^3 \cdot 3^3$ และ $84 = 2^3 \cdot 3 \cdot 7$
   $(216, 84) = 2^2 \cdot 3 = 12$ (ศึกษาข้อพิสูจน์และรายละเอียดมากขึ้นในหัวข้อต่อไป)

นพพร ธนะชัยขันธ์ (2543 : 52-53) ได้อธิบายผลที่ได้จากการศึกษาบทนิยาม 2.4.1 ของตัวหารร่วมมากไว้ว่า ให้ a และ b เป็นจำนวนเต็มที่อย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ จำนวนเต็มบวก d จะเป็น ห.ร.ม. ของ a และ b ก็ต่อเมื่อ $d \mid a$ และ $d \mid b$ แสดงว่า d เป็นตัวหารร่วมของ a และ b ก่อน และถ้ามีจำนวนเต็ม c ซึ่ง $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$ นั่นแสดงว่า d ต้องเป็นตัวหารร่วมมากที่มีค่ามากที่สุดนั่นเอง เราอาจกล่าวโดยสรุปได้ว่าจำนวนเต็มบวก d จะเป็น ห.ร.ม. ของจำนวนเต็ม a และ b ซึ่งอย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ ถ้า d เป็นตัวหารที่มีค่ามากที่สุดของ a และ b ต่อไปเราจะให้นิยามของ ห.ร.ม. ของจำนวนเต็มที่มีจำนวนมากกว่าสองตัว ซึ่งไม่เป็นศูนย์ทั้งหมดดังต่อไปนี้

บทนิยาม 2.4.2

ให้ $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเต็มซึ่งไม่เป็นศูนย์ทั้งหมด ตัวหารร่วมมากของ $a_1, a_2, a_3, \ldots, a_n$ คือจำนวนเต็มบวก d ที่มีค่ามากที่สุดซึ่ง $d \mid a_i$ สำหรับทุก $i = 1, 2, 3, \ldots, n$ และจะใช้สัญลักษณ์ $(a_1, a_2, a_3, \ldots, a_n)$ แทน ห.ร.ม. ของ $a_1, a_2, a_3, \ldots, a_n$

จากบทนิยาม เราพบว่า

1. เราสามารถหา $(a_1, a_2, a_3, \ldots, a_n)$ ได้เสมอและมีเพียงค่าเดียวเท่านั้น
2. $(a_1, a_2, a_3, \ldots, a_n) = ((a_1, a_2, a_3, \ldots, a_{n-1}), a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n))$
3. ถ้า $d = (a_1, a_2, a_3, \ldots, a_n)$ จะได้ว่ามี $x_1, x_2, x_3, \ldots, x_n \in \mathbb{Z}$ ที่ทำให้

$$d = a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n$$

4. ให้ $d = (a_1, a_2, a_3, \ldots, a_n)$ จะได้ว่าสำหรับทุก ๆ จำนวนเต็ม c ใด ๆ
   ถ้า $c \mid a_i$ สำหรับทุก $i = 1, 2, 3, \ldots, n$ แล้ว $c \mid d$
5. ให้ $d = (a_1, a_2, a_3, \ldots, a_n)$ จะได้ว่า $(a_1, a_2, a_3, \ldots, a_n) = 1$ ก็ต่อเมื่อ
   มีจำนวนเต็ม $x_1, x_2, x_3, \ldots, x_n$ ที่ทำให้ $a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = 1$

ตัวอย่าง 2.4.10

จงหาตัวหารร่วมมากของ $24, 60$ และ 30

วิธีทำ เนื่องจาก ตัวหารที่เป็นบวกของ 24 คือ $1, 2, 3, 4, 6, 8, 12, 24$
ตัวหารที่เป็นบวกของ 60 คือ $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$
ตัวหารที่เป็นบวกของ 30 คือ $1, 2, 3, 5, 6, 10, 15, 30$
จะได้ว่าตัวหารร่วมที่เป็นบวกของ $24, 60$ และ 30 คือ $1, 2, 3$ และ 6
ดังนั้น ตัวหารร่วมมากของ $24, 60$ และ 30 คือ 6
เขียนเป็นสัญลักษณ์ได้ว่า $(24, 60, 30) = 6$

ตัวอย่าง 2.4.11

1. $(12, 72, 18) = 6$
2. $(42, 49, 19) = 1$
3. $(198, 288, 512) = 2$
4. $(1819, 3587, -997) = 1$

2.5 ขั้นตอนวิธีแบบยุคลิด

ในการค้นหาตัวหารร่วมมากของจำนวนเต็มสองจำนวนที่มีค่ามาก ๆ นั้น มีวิธีการหนึ่งที่มีประสิทธิภาพและสะดวกอย่างยิ่งในทางปฏิบัติคือ การใช้ขั้นตอนแบบยุคลิด ยุคลิดค้นพบว่าในการหา ห.ร.ม. ของจำนวนเต็ม 2 จำนวนนั้นเกิดจากการใช้ขั้นตอนวิธีการหารหลาย ๆ ครั้ง ทฤษฎีบทต่อไปนี้จะเป็นเครื่องมือในการหา ห.ร.ม. ของจำนวนเต็ม a, b และหาจำนวนเต็ม x, y ที่ทำให้

$$(a, b) = ax + by$$

(David M. Burton. 2007 : 26, Underwood Dudley. 2012 : 7, Raji W. 2013 : 25)

ทฤษฎีบท 2.5.1 : ขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm)

ให้ $a, b \in \mathbb{Z}$ และ $a > 0$ จะได้ว่า มี $q_1, q_2, q_3, \ldots, q_n, q_{n+1}, r_1, r_2, r_3, \ldots, r_n \in \mathbb{Z}$ ที่ทำให้

$$\begin{aligned}
b &= aq_1 + r_1, & 0 < r_1 < a \\
a &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

และ $(a, b) = (a, r_n) = r_n$

การพิสูจน์ การพิสูจน์ของทฤษฎีบทนี้แบ่งออกเป็น 2 กรณี

กรณีที่ 1 ถ้า $a \mid b$ โดยขั้นตอนวิธีการหาร

จะได้ว่ามี $q, r \in \mathbb{Z}$ ซึ่ง $b = aq + r, r = 0$

และโดยทฤษฎี 2.4.9 จะได้ว่า $(a, b) = (a, r) = a$

กรณีที่ 2 ถ้า $a \mid b$ โดยขั้นตอนวิธีการหาร จะได้ว่ามี $q_1, r_1 \in \mathbb{Z}$

ซึ่ง $b = aq_1 + r_1$ เมื่อ $0 < r_1 < a$

จากความจริงที่ว่ามีจำนวนเต็มบวกที่น้อยกว่า a เป็นจำนวนจำกัดและการกระทำซ้ำ ๆ ของขั้นตอนวิธีการหาร จะได้ว่ามี $q_1, q_2, q_3, \ldots, q_n, q_{n+1}, r_2, r_3, \ldots, r_n \in \mathbb{Z}$ ที่ทำให้ โดยทฤษฎีบท 2.4.9 จะได้ว่า

$$\begin{aligned}
a &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

$$(a, b) = (a, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n \qquad \square$$

จากทฤษฎีบทขั้นตอนวิธีแบบยุคลิด เราพบว่าในหาค่า x และ y เมื่อ $(a, b) = ax + by$ นั้นสามารถหาแนวทางได้จากการกำจัดเศษ $r_{n-1}, \ldots, r_2, r_1$ จากสมการข้างต้น ซึ่งมีวิธีการดังนี้

เริ่มจากสมการกลุ่มรองสุดท้าย $r_n = r_{n-2} - q_n r_{n-1}$
แล้วแทนค่า r_{n-1} ด้วยค่าในสมการขั้นตอนวิธีแบบยุคลิด
จะได้ว่า $r_n = r_{n-2} - q_n \left(r_{n-3} - q_{n-1} r_{n-2}\right) = r_{n-2} \left(1 + q_1 q_{n-1}\right) + r_{n-3} \left(-q_n\right)$
สมการที่ได้นี้แสดงการเขียน r_n ในรูปผลบวกของ r_{n-2} และ r_{n-3}
ขั้นตอนต่อไป ทำซ้ำเช่นนี้ไปเรื่อย ๆ ซึ่งจะกำจัดเศษ $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ ตามลำดับ
จนในที่สุดจะได้สมการแสดงการเขียน r_n ในรูปผลบวกของ a และ b
แต่ r_n คือ ห.ร.ม. ของ a และ b
นั่นคือ วิธีการที่ทำให้เราทราบค่า x และ y
ที่ทำให้ $(a, b) = ax + by$

เพื่อให้เข้าใจทฤษฎีและขั้นตอนวิธีแบบยุคลิด ผู้เขียนขอยกตัวอย่างดังนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 43, ยศนันต์ มีมาก. 2555 : 11)

ตัวอย่าง 2.5.1

จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(12378, 3054)$ พร้อมทั้งแสดงวิธีการหาค่า x และ y ที่ทำให้ $(12378, 3054) = 12378x + 3054y$

วิธีทำ
$$\begin{aligned} 12378 &= (4)(3054) + 162 \\ 162 &= (1)(138) + 24 \\ 138 &= (5)(24) + 18 \\ 24 &= (10)(18) + 6 \\ 18 &= (3)(6) \end{aligned}$$

ดังนั้น $(12378, 3054) = 6$

ในการหาค่า x และ y ซึ่ง $12378x + 3054y = 6$ เราสามารถหาได้โดยการทำย้อนกลับซึ่งมีวิธีดังนี้

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138 \\ &= 6(162 - 138) - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\ &= 132 \cdot 12378 + (-535) \cdot 3054 \end{aligned}$$

ดังนั้น $6 = (12378)(132) + (3054)(-535)$

จะได้ว่า $x = 132$ และ $y = -535$

ตัวอย่าง 2.5.2

จงหา $(91, 259)$ โดยใช้ขั้นตอนวิธีของยุคลิด และหาจำนวนเต็ม x และ y ซึ่ง $(91, 259) = 91x + 259y$

วิธีทำ โดยขั้นตอนวิธีของยุคลิด เราได้ว่า

$$\begin{aligned} 259 &= 2 \cdot 91 + 77 \\ 91 &= 1 \cdot 77 + 14 \\ 77 &= 5 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 \end{aligned}$$

ดังนั้น $(91, 259) = 7$

โดยการแทนค่าย้อนกลับเราได้ว่า

$$\begin{aligned} 7 &= 77 - 5 \cdot (91 - 1 \cdot 77) \\ &= 6 \cdot (259 - 2 \cdot 91) - 5 \cdot 91 \\ &= 6 \cdot 259 + (-17) \cdot 91 \end{aligned}$$

เพราะฉะนั้น $x = -17$ และ $y = 6$ ซึ่ง $(91, 259) = 7 = 91x + 259y$

ตัวอย่าง 2.5.3

จงหา (352,486) และเขียนเป็นผลรวมเชิงส้นของของ 352 และ 486

วิธีทำ โดยขั้นตอนวิธีการหาร เราจะได้ระบบสมการ

$$\begin{aligned}
486 &= 1 \cdot 352 + 134 \\
352 &= 2 \cdot 134 + 84 \\
134 &= 1 \cdot 84 + 50 \\
84 &= 1 \cdot 50 + 34 \\
50 &= 1 \cdot 34 + 16 \\
34 &= 2 \cdot 16 + 2 \\
16 &= 8 \cdot 2 + 0
\end{aligned}$$

เศษตัวสุดท้ายในที่นี้คือ 2 ดังนั้น 2 เป็นตัวหารร่วมมากของ 352 และ 486 นั่นคือ $2 = (352, 486)$ ในการเขียน 2 เป็นผลรวมเชิงเส้นของ 352 และ 486 เราเริ่มจากบรรทัดรองสุดท้ายในระบบสมการข้างต้นและขจัดเศษ $16, 34, 50, 84, 134$ ทีละขั้น จะได้

$$\begin{aligned}
2 &= 34 - 2 \cdot 16 = 34 - 2(50 - 34) \\
&= 3 \cdot 34 - 2 \cdot 50 \\
&= 3(84 - 50) - 2 \cdot 50 \\
&= 3 \cdot 84 - 5 \cdot 50 \\
&= 3 \cdot 84 - 5(134 - 84) \\
&= 8 \cdot 84 - 5 \cdot 134 \\
&= 8(352 - 2 \cdot 134) - 5 \cdot 134 \\
&= 8 \cdot 352 - 21 \cdot 134 \\
&= 8 \cdot 352 - 21(486 - 352) \\
&= 29 \cdot 352 - 21 \cdot 486
\end{aligned}$$

ดังนั้น $2 = (352, 486) = 352x + 486y$ โดยที่ $x = 29$ และ $y = -21$

ในตัวอย่างข้างตันนี้ สังเกตอีกประการหนึ่งว่า การเขียน 2 เป็นผลเชิงเส้นของ 352 และ 486 ไม่ได้มีเพียงวิธีนี้วิธีเดียว ทางหนึ่งที่เป็นไปได้ที่เห็นได้ง่ายที่สุดคือนำ $352 \cdot 486$ บวกเข้าและลบออกจะได้

$$2 = (29 + 486)352 + (-21 - 352)486 = 515 \cdot 352 + (-373)486$$

ตัวอย่าง 2.5.4

จงหา ห.ร.ม. ของ 803 และ 154

วิธีทำ โดยทฤษฎีบท 2.5.1 ดังนั้น $a = 803$ และ $b = 154$ โดยขั้นตอนวิธีการหาร

จะได้ว่า $803 = 5 \cdot 154 + 33$

เนื่องจาก $r_1 = 33 > 0$ ใช้ขั้นตอนวิธีการหาร กับ $b = 154$ และ $r_1 = 33$

จะได้ว่า $154 = 4 \cdot 33 + 22$

เนื่องจาก $r_2 = 22 > 0$ ใช้ขั้นตอนวิธีการหาร กับ $r_1 = 33$ และ $r_2 = 22$
จะได้ว่า $33 = 1 \cdot 22 + 11$
เนื่องจาก $r_3 = 11 > 0$ ใช้ขั้นตอนวิธีการหาร กับ $r_2 = 22$ แลหะ $r_3 = 11$
จะได้ว่า $22 = 2 \cdot 11 + 0$ เนื่องจาก $r_4 = 0$ ดังนั้นขั้นตอนวิธีแบบยุคลิดจึงสิ้นสุด
จะได้ว่า $(803, 154) = r_3 = 11$

ตัวอย่าง 2.5.5

จงหา ห.ร.ม. ของ 864 และ 354 พร้อมทั้งเขียน $(864, 354)$ ในรูปการรวมเชิงเส้นของ 864 และ 354

วิธีทำ โดยขั้นตอนวิธีแบบยุคลิด จะได้ว่า

$$\begin{aligned} 864 &= 2 \cdot 354 + 156 \\ 354 &= 2 \cdot 156 + 42 \\ 156 &= 3 \cdot 42 + 30 \\ 42 &= 1 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

ดังนั้น $(864, 354) = 6$
เมื่อเขียนย้อนกลับ จะได้ว่า

$$\begin{aligned} 6 &= 30 - 2 \cdot 12 \\ &= 30 - 2(42 - 1 \cdot 30) \\ &= 3 \cdot 30 - 2 \cdot 42 \\ &= 3(156 - 3 \cdot 42) - 2 \cdot 42 \\ &= 3 \cdot 156 - 11 \cdot 42 \\ &= 3 \cdot 156 - 11(354 - 2 \cdot 156) \\ &= 25(864 - 2 \cdot 354) - 11 \cdot 354 \\ &= 25 \cdot 864 + (-61)354 \end{aligned}$$

ดังนั้น $(864, 354) = 6 = 25 \cdot 864 + (-61)354$

2.6 ตัวคูณร่วมน้อย

เรื่องที่มีความสัมพันธ์ควบคู่กับตัวหารร่วมมากของจำนวนเต็มสองจำนวน คือ **ตัวคูณร่วมน้อย** หรือ ค.ร.น. สำหรับจำนวนเต็ม c จะกล่าวว่า c เป็น**ตัวคูณร่วม** (common multiple) ของ a และ b ที่ ต่างก็ไม่เท่ากับศูนย์ ถ้า $a \mid b$ และ $b \mid c$ จากความนี้จะเห็นได้ว่า $0, ab, -ab$ ต่างก็เป็นตัวคูณของ a และ b เสมอแสดงว่าเซตของตัวคูณร่วมที่จะไม่ใช่เซตว่าง จากการจัดอันดับดี จะได้ว่า เซตนี้จะมีจำนวน เต็มบวกที่น้อยที่สุด เช่น เซตของตัวคูณร่วมที่เป็นบวกของ 8 และ 10 คือ $40, 80, 120, \ldots$ จะได้ว่า 40 เป็นสมาชิกที่มีค่าน้อยที่สุด จะเรียกจำนวน 40 นี้ว่าตัวคูณร่วมน้อยของ 8 และ 10 ซึ่งเราให้นิยามตัวคูณร่วมน้อยดังต่อไปนี้ (สมวงษ์ แปลงประสพ

โชค. 2545 : 32, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 65)

บทนิยาม 2.6.1

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ เราจะเรียกจำนวนเต็มบวก m ว่า **ตัวคูณร่วมน้อย** (least common multiple) หรือ **ค.ร.น.** (L.C.M.) ของ a และ b เขียนแทนด้วย $[a, b]$ ก็ต่อเมื่อ m มีสมบัติต่อไปนี้

(1) $a \mid m$ และ $b \mid m$

(2) สำหรับจำนวนเต็มบวก c ถ้า $a \mid b$ และ $b \mid c$ แล้ว $m \leq c$

จากบทนิยามเราพบว่า ถ้า $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า

(1) เซตของตัวคูณร่วมของ a และ b เป็นเซตอนันต์

(2) ถ้า m เป็นตัวคูณร่วมของ a และ b จะได้ว่า $-m$ เป็นตัวคูณร่วมของ a และ b

(3) $[a, b] = [b, a] = [a, -b] = [-a, b] = [-a, -b]$

(4) ถ้า $a \mid b$ แล้ว $[a, b] = |\, b \,|$

ตัวอย่าง 2.6.1

1. $[15, 21] = 105$
2. $[-24, -36] = 72$
3. $[3054, 12378] = 6,300,402$
4. $[-12, 30] = 60$
5. $[5, 11] = 55$

ข้อสังเกต (1) $[a, b] = [b, a]$

(2) $[a, b] = [|\, a \,|, |\, b \,|]$

(3) ถ้า $a \mid b$ แล้ว จะได้ว่า $[a, b] = |\, b \,|$

ทฤษฎีบท 2.6.1

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า สำหรับจำนวนเต็ม c ใด ๆ ถ้า $a \mid c$ และ $b \mid c$ แล้ว $[a, b] \mid c$

การพิสูจน์ ให้ $m = [a, b]$ และ c เป็นจำนวนเต็มใด ๆ ที่ $a \mid c$ และ $b \mid c$
โดยวิธีขั้นตอนการหารจะได้ว่า มี $g, r \in \mathbb{Z}$
ซึ่ง $c = mq + r, 0 \leq r < m$
แสดงว่า $r = c - mq, 0 \leq r < m$
จาก $a \mid c$ และ $b \mid c$ จะได้ว่า $a \mid r$ และ $b \mid r$
นั่นคือ เป็นตัวคูณร่วมของ a และ b
ถ้า $0 < r < m$ จะขัดแย้งกับ $m = [a, b]$
ดังนั้น $r = 0$ แสดงว่า $m \mid c$ □

ทฤษฎีบทต่อไปนี้ จะเป็นทฤษฎีบทที่แสดงถึงความสัมพันธ์ของ $a, b, (a, b)$ และ $[a, b]$ (David M. Burton. 2007 : 30)

ทฤษฎีบท 2.6.2

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ จะได้ว่า $(a,b)[a,b] = |\,ab\,|$

การพิสูจน์ จาก $(a,b) = (|\,a\,|, |\,b\,|)$ และ $[a,b] = [|\,a\,|, |\,b\,|]$
ดังนั้น จึงเป็นการเพียงพอที่จะพิสูจน์กรณีที่ $a, b \in \mathbb{N}$

(i) ให้ $d = (a,b)$ จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $a = dx$ และ $b = dy$
ให้ $m = \dfrac{ab}{d} = dxy$ จะได้ว่า $m = ay = bx$
แสดงว่า $a \mid m$ และ $b \mid m$ นั่นคือ m เป็นตัวคูณร่วมของ a และ b

(ii) ให้ c เป็นจำนวนเต็มบวกที่ $a \mid c$ และ $b \mid c$
จะได้ว่ามี $u, v \in \mathbb{Z}$ ซึ่ง $c = au$ และ $c = bv$
จาก $a = dx$ และ (i) จะได้ว่า $dxu = dyv$
ดังนั้น $x \mid yv$ แต่ $(x,y) = 1$ แสดงว่า $x \mid v$
ดังนั้น จะมี $r \in \mathbb{Z}$ ซึ่ง $v = xr$ และจาก $m = bx$ และ $c = bv$
จะได้ว่า $c = bxr = mr$ ดังนั้น $m \mid c$
จาก (i) และ (ii) สรุปว่า $m = [a,b]$ □

ตัวอย่าง 2.6.2

จงหา [803,154] จาก $(803, 154) = 11$

วิธีทำ โดยทฤษฎีบท 2.6.2 จะได้ว่า $(803,154)[803,154] = (803)(154)$

$$\begin{aligned} 11[803,154] &= 123662 \\ [803,154] &= \frac{123662}{11} \\ &= 11242 \end{aligned}$$

ตัวอย่าง 2.6.3

จำนวนนับสองจำนวนคูณกันได้ 80 และมี ห.ร.ม. เป็น 4 จงหา ค.ร.น. ของสองจำนวนนั้น

วิธีทำ สมมติจำนวนทั้งสองคือ a และ b จากทฤษฎีบท 2.6.2 จะได้ว่า

$$\begin{aligned} (a,b)[a,b] &= |\,ab\,| \\ 4[a,b] &= 80 \\ [a,b] &= \frac{80}{4} = 20 \end{aligned}$$

อีกวิธีหนึ่งที่สามารถหาตัวคูณร่วมน้อยของจำนวนเต็มสองจำนวนได้ดังทฤษฎีบทต่อไปนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 34)

ทฤษฎีบท 2.6.3

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ และ $m \in \mathbb{N}$ จะได้ว่า $[ma, mb] = m[a,b]$

การพิสูจน์ จากทฤษฎีบท 2.4.5 และทฤษฎีบท 2.6.2

จะได้ว่า $(ma, mb)[ma, mb] = m(a, b)[ma, mb] = |(ma)(mb)|$

ดังนั้น $[ma, mb] = \dfrac{|\, m^2ab\,|}{m(a, b)} = \dfrac{m^2|\, ab\,|}{m(a, b)} = m[a, b]$ □

ในทำนองเดียวกันกับตัวหารร่วมมาก เราสามารถขยายบทนิยามของตัวคูณร่วมและตัวคูณร่วมน้อยของจำนวนเต็มมากกว่าสองจำนวนได้ดังนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 34, จิราภา ลิ้มบุพศิริพร. 2555 : 31, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 167)

บทนิยาม 2.6.2

ให้ $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$ ซึ่ง $a \neq 0$ สำหรับ $i = 1, 2, 3, \ldots, n$ เราเรียก $m \in \mathbb{N}$ ว่า**ตัวคูณร่วม** (common multiple) ของ $a_1, a_2, a_3, \ldots, a_n$ ก็ต่อเมื่อ $a_i \mid m$ สำหรับ $i = 1, 2, 3, \ldots, n$ และเรียก m ว่า **ตัวคูณร่วมน้อย** (least common multiple) ของ $a_1, a_2, a_3, \ldots, a_n$ ก็ต่อเมื่อ $m \in \mathbb{N}$ และ m เป็นตัวคูณร่วมที่มีค่าน้อยที่สุด ซึ่งเขียนแทนด้วย $[a_1, a_2, a_3, \ldots, a_n]$

จากบทนิยาม 2.6.2 เราพบว่า

(1) เราสามารถหา $[a_1, a_2, a_3, \ldots, a_n]$ ได้เสมอและมีเพียงค่าเดียวเท่านั้น

(2) $[a_1, a_2, a_3, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n] = [a_1, a_2, \ldots, [a_{n-1}, a_n]]$

(3) ถ้า $a_i \mid c$ สำหรับ $i = 1, 2, 3, \ldots, n$ แล้ว $m \mid c$

ตัวอย่าง 2.6.4

1. $[7, 11, 13] = 1001$
2. $\begin{aligned}[3, 8, 10, 15] &= [[3, 8, 10], 15] \\ &= [[[3, 8], 10]15] \\ &= [[24, 10], 15] \\ &= [120, 15] \\ &= 120\end{aligned}$

ตัวอย่าง 2.6.5

จงหา $[10, 20, 32]$

วิธีทำ จาก $[20, 10] = 10[2, 1] = 20$

และ $[20, 32] = 4[5, 8] = 160$

ดังนั้น $[10, 20, 32] = 160$

สรุปท้ายบท

สิ่งที่สำคัญในบทที่ 2 คือการศึกษานิยามและสมบัติต่าง ๆ ของการหารลงตัว ตลอดจนนำสมบัติของการหารลงตัวมาช่วยในการแก้ปัญหาบางอย่างที่เกี่ยวข้องกับจำนวนเต็มดังที่เห็นในตัวอย่าง ซึ่งการศึกษาเกี่ยวกับสมบัติของการหารลงตัวเป็นสิ่งสำคัญมากในวิชาทฤษฎีจำนวน ถือได้ว่าเป็นหัวใจของวิชาทฤษฎีจำนวนก็ว่าได้เพราะเนื้อหาในบทต่อ ๆ ไปจะต้องใช้ความรู้เกี่ยวกับการหารลงตัวเข้ามาช่วย นอกจากนี้แล้วในบทนี้เราก็ได้พูดถึงการพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์ นิยามและทฤษฎีบทที่สำคัญที่เกี่ยวกับตัวหารร่วมมาก และตัวคูณร่วมน้อยตลอดจนแสดงให้เห็นถึงความสัมพันธ์ระหว่างตัวหารร่วมมากกับตัวคูณร่วมน้อย และได้แสดงวิธีการหาตัวหารร่วมมากโดยใช้ขั้นตอนวิธีแบบยุคลิดซึ่งวิธีนี้ช่วยในการหาตัวหารร่วมมากของจำนวนที่มีค่ามาก ๆ

แบบฝึกหัดท้ายบทที่ 2

1. จงใช้ขั้นตอนวิธีการหารเพื่อแสดงว่า

   (1.1) กำลังสองของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $3k$ หรือ $3k+1$ สำหรับจำนวนเต็ม k บางจำนวน

   (1.2) กำลังสามของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $9k$ หรือ $9k+1$ หรือ $9k+8$ สำหรับจำนวนเต็ม k บางจำนวน

   (1.3) กำลังสี่ของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $5k$ หรือ $5k+1$ สำหรับจำนวนเต็ม k บางจำนวน

2. จงแสดงว่า จำนวนเต็มที่เขียนอยู่ในรูปของ $6k+5$ โดยที่ k เป็นจำนวนเต็ม สามารถเขียนให้อยู่ในรูปของ $3j+2$ ได้ สำหรับจำนวนเต็ม j บางจำนวน

3. จงแสดงว่า $\dfrac{n(n+1)(2n+1)}{6}$ เป็นจำนวนเต็มเสมอ เมื่อ n เป็นจำนวนเต็มบวก
   (ข้อเสนอแนะ ใช้ขันตอนวิธีการหาร n สามารถเขียนให้อยู่ในรูปใดรูปหนึ่งของ

   $$6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$$

   สำหรับจำนวนเต็ม k บางจำนวน)

4. ถ้า n เป็นจำนวนเต็มคี่แล้ว จงแสดงว่า n^4+4n^2+11 สามารถเขียนอยู่ในรูปของ $16k$ สำหรับจำนวนเต็ม k บางจำนวน

5. มีจำนวนนับตั้งแต่ 1 ถึง 200 รวมทั้งสิ้นกี่จำนวน ซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2 และเม่อหาร ด้วย 14 แล้วเหลือเศษ 10

6. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มคี่แล้ว $16 \mid (a^4+b^4-2)$

7. จงแสดงว่า ผลคูณของจำนวนเต็ม 3 จำนวนที่เรียงต่อเนื่องกันจะหารด้วย 6 ลงตัว และผลคูณของจำนวนเต็ม 4 จำนวนที่เรียงต่อเนื่องกันจะหารด้วย 24 ลงตัว

8. จงหารจำนวนเต็มบวกที่มีค่ามากที่สุดที่นำไปหาร $n(n+1)(n+2)(n+3)(n+4)$ ได้ลงตัวเสมอ สำหรับทุกจำนวนเต็มบวก n

9. สำหรับจำนวนเต็มบวก n จงใช้หลักการอุปนัยเชิงคณิตศาสตร์พิสูจน์ข้อความต่อไปนี้

   (9.1) $8 \mid (5^{2n}+7)$ (ข้อเสนอแนะ $5^{2(k+1)}+7 = 5^2\left(5^{2k}+7\right)+\left(7-5^2\cdot 7\right)$)

   (9.2) $15 \mid (2^{4n}-1)$

   (9.3) $15 \mid (3^{3n+1}+2^{n+1})$

   (9.4) $24 \mid (2\cdot 7^n+3\cdot 5^n-5)$

   (9.5) $21 \mid (4^{n+1}+5^{2n-1})$

10. จงพิสูจน์ว่า ถ้า n เป็นจำนวนเต็มบวก แล้ว $(3!)^n \mid (3n)!$

11. ให้ a, b เป็นจำนวนเต็มบวกซึ่ง $a \,|b^2, b^2|\, a^3, a^3 \,|b^4, b^4|\, a^5, \ldots$ จงแสดงว่า $a = b$

12. ให้ a, b, c เป็นจำนวนเต็มและ $c \neq 0$ จงแสดงว่า $a \mid b$ ก็ต่อเมื่อ $ac \mid bc$

13. ให้ a, b เป็นจำนวนเต็มใด ๆ จงแสดงว่าถ้า $a \mid b$ แล้ว $a^n \mid b^n$ สำหรับทุกจำนวนเต็มบวก n

14. จงหาจำนวนเต็ม n ทั้งหมดที่ทำให้ $(n-3) \mid (n^3-3)$

15. จงแสดงว่า ถ้า a เป็นจำนวนเต็ม แล้ว $3 \mid a\,(2a^2+7)$

16. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคี่ แล้ว $32 \mid (a^2+3)\,(a^2+7)$

17. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มซึ่ง $(a, b) = 1$ แล้ว $(a+b, a-b) = 1$ หรือ 2

18. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มคู่ที่ไม่ใช่ศูนย์ทั้งคู่ แล้ว $(a, b) = 2\left(\dfrac{a}{2}, \dfrac{b}{2}\right)$

19. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่และ b เป็นจำนวนเต็มคี่ แล้ว $(a, b) = \left(\dfrac{a}{2}, b\right)$

20. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มซึ่ง $c \mid ab$ แล้ว $c \mid (a, c)(b, c)$

21. จงใช้หลักอุปนัยเชิงคณิตศาสตร์แสดงว่าถ้า $a_1, a_2, a_3, \ldots, a_n$ และ b เป็นจำนวนเต็มซึ่ง $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$ แล้ว $(a_1 a_2 a_3 \cdots a_n, b) = 1$

22. จงแสดงว่า ถ้า $(a, b) = 1$ แล้ว $(a^n, b^n) = 1$ สำหรับทุกจำนวนเต็มบวก n

23. จงแสดงว่า $(a^n, b^n) = (a, b)^n$ สำหรับทุกจำนวนเต็มบวก n

24. จงพิสูจน์ว่า ถ้ามีจำนวนเต็ม x และ y ที่ทำให้ $ax + by = (a, b)$ แล้ว $(x, y) = 1$

25. ให้ $a, b, c \in \mathbb{Z}$ และ $d = (a, b)$ จงพิสูจน์ว่า $a \mid bc$ ก็ต่อเมื่อ $\dfrac{a}{d} \mid c$

26. จงแสดงว่า ถ้า $(a, b) = 1$ และ $(a, c) = 1$ แล้ว $(a, bc) = 1$

27. จงแสดงว่า ถ้า $(a, b) = c$ แล้ว $(a^2, b^2) = c^2$

28. จงแสดงว่า ถ้า $a, m, n \in \mathbb{N}$ โดยที่ $m > n$ แล้ว $\left(a^{2^n}+1\right) \mid \left(a^{2^m}-1\right)$

29. จงแสดงว่าไม่มีจำนวนเต็ม x, y ที่สอดคล้องกับ $x + y = 100$ และ $(x, y) = 3$

30. จงแสดงว่า มี $x, y \in \mathbb{Z}$ จำนวนอนันต์ที่สอดคล้องกับ $x + y = 100$ และ $(x, y) = 5$

31. จงพิสูจน์ว่า $(n^3 + 2n, n^4 + 3n^2 + 1) = 1$ สำหรับทุกจำนวนเต็มบวก n

32. ให้ $a, m, n \in \mathbb{N}$ โดยที่ $m > n$ จงพิสูจน์ว่า $\left(a^{2^m}+1, a^{2^n}+1\right)$

    (32.1) ถ้า a เป็นจำนวนเต็มคู่

    (32.2) ถ้า a เป็นจำนวนเต็มคี่

33. ให้ a, b และ c เป็นจำนวนเต็ม จงแสดงว่า $[a, b] \mid c$ ก็ต่อเมื่อ $a \mid c$ และ $b \mid c$

34. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวก แล้ว $(a,b) = (a+b, [a,b])$

35. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มบวก แล้ว $([a,b],c) = [(a,c),(b,c)]$ และ $[(a,b),c] = ([a,c],[b,c])$

36. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็มบวกแล้ว $(a,b,c)[a,b,c] = \dfrac{abc}{(a,b)(a,c)(b,c)}$

37. จงแสดงว่า ถ้า $(a,b,c)[a,b,c] = abc$ แล้ว $(a,b) = (b,c) = (a,c) = 1$

38. จงแสดงว่า $(a,b,c)[a,b,c] = |\,abc\,|$

39. จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ ถ้าข้อความนั้นเป็นจริง จงพิสูจน์ถ้าข้อความนั้นเป็นเท็จจงยกตัวอย่างค้าน

    (39.1) ถ้า $(a,b) = (a,c)$ แล้ว $[a,b] = [a,c]$

    (39.2) ถ้า $(a,b) = (a,c)$ แล้ว $(a^2,b^2) = (a^2,c^2)$

    (39.3) ถ้า $(a,b) = (a,c)$ แล้ว $(a,b) = (a,b,c)$

    (39.4) ถ้า $(a,b) = 1$ แล้ว $(a^2,ab,b^2) = 1$

    (39.5) $[a^2,ab,b^2] = [a^2,b^2]$

เอกสารอ้างอิง

กิตติภูมิ บำรุงสงฆ์. (2519). **ทฤษฎีจำนวนเบื้องต้น**. นครราชสีมา : ภาควิชาคณิตศาสตร์ วิทยาลัยครูนครราชสีมา.

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จิราภา ลิ้มบุพศิริพร. (2555). **ทฤษฎีจำนวน**. นครปฐม : โรงพิมพ์มหาวิทยาลัยศิลปากร.

ดำรงค์ ทิพย์โยธา. (2556). **คณิตศาสตร์ปรนัยเล่มที่ 37 : โลกทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

ทบวงมหาวิทยาลัย. (2545). **ทฤษฎีจำนวนเบื้องต้น**. กรุงเทพฯ : โรงพิมพ์พิทักษ์การพิมพ์.

ทิพวัลย์ พัฒนางกูร. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : องค์การค้าของ สกสค.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

ปวีณา ถ้ำแก้ว. (2558). **ระบบจำนวน**. เชียงใหม่ : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเชียงใหม่.

ยศนันต์ มีมาก. (2555). **คู่มือประกอบสื่อการสอน วิชาคณิตศาสตร์ : ทฤษฎีจำนวนเบื้องต้น (เนื้อหาตอนที่ 1)**. คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

รัชนียา ถิรเดโชชัย. (2560). **ระบบจำนวน**. ร้อยเอ็ด : สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏร้อยเอ็ด.

สมจิต โชติชัยสถิตย์. (2540). **ทฤษฎีจำนวน 2**. ขอนแก่น : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

โสภาพรรณ ทิพย์โยธา. (2545). **ทฤษฎีจำนวน 1 (พิมพ์ครั้งที่ 6)**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

Coppel W.A. (2009). **Number Theory : An Introduction to Mathematics (2 ed.)**. New York : Springer Science & Business Media.

David M. Burton. (2007). **Elementary number theory (5 ed.)**. New York : The McGraw-HillCompanies, Inc.

Gareth A. Jones and J. Mary Jones. (1998). **Elementary number theory**. Springer Science & Business Media.

Ivan Niven, Herbert S. Zucker and Hugh L. Montgomery. (1991). **An introduction to Theory of Numbers**. New York : John Wiley & Sons, Inc.

Koshy T. (2007). **Elementary Number Theory with Applications (2 ed.)**. Elsevier Science.

Raji W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

Underwood Dudley. (2012). **Elementary Number Theory (2 ed.)**. Dover Publications.

แผนบริหารการสอนประจำบทที่ 3

เนื้อหาประจำบท

1. นิยามของจำนวนเฉพาะและข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ
2. ทฤษฎีบทหลักมูลของเลขคณิต
3. การค้นหาจำนวนเฉพาะ
4. ทฤษฎีบทที่สำคัญของจำนวนเฉพาะ
5. ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ
6. จำนวนเฉพาะแฟร์มาต์
7. จำนวนเฉพาะแมร์เซน

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามของจำนวนเฉพาะและทฤษฎีที่เกี่ยวข้องพิสูจน์โจทย์ปัญหาที่กำหนดให้ได้
2. ใช้ทฤษฎีที่เกี่ยวข้องกับจำนวนเฉพาะพิจารณาว่าจำนวนที่กำหนดให้เป็นจำนวนเฉพาะหรือเป็นจำนวนประกอบ
3. เข้าใจนิยาม ทฤษฎีบท การพิสูจน์แต่ละทฤษฎีบท และสามารถนำความรู้มาพิสูจน์แบบฝึกหัดที่กำหนดให้ได้
4. สามารถนำความรู้ที่ได้เป็นพื้นฐานในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 นิยามของจำนวนเฉพาะและข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ
    1.2 ทฤษฎีบทหลักมูลของเลขคณิต
    1.3 การค้นหาจำนวนเฉพาะ
    1.4 ทฤษฎีบทที่สำคัญของจำนวนเฉพาะ
    1.5 ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ
    1.6 จำนวนเฉพาะแฟร์มาต์
    1.7 จำนวนเฉพาะแมร์เซน
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 3
จำนวนเฉพาะ

จากคำกล่าวของเกาส์ที่ว่า “Mathematics is the queen of science, and number theory is the queen of mathematics” และในปี ค.ศ. 1993 โค (K.M. Koh) กล่าวอีกว่า “The theory of prime numbers is the queen of number theory” ดังนั้นในการศึกษาวิชาทฤษฎีจำนวน จำนวนเฉพาะ (prime number) เป็นเรื่องหนึ่งที่มีบทบาทและสำคัญยิ่งต่อการศึกษาเพราะว่าจำนวนเต็มบวกสามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ ซึ่งแสดงว่ามโนภาพเกี่ยวกับจำนวนเฉพาะจะสอดแทรกอยู่ในทุก ๆ หัวข้อที่เกี่ยวข้องกับจำนวนเต็ม รวมทั้งยังมีข้อคาดเดามากมายที่เกี่ยวข้องกับจำนวนเฉพาะ

ในการศึกษาเกี่ยวกับจำนวนเฉพาะนั้น เราจะมุ่งเน้นการศึกษาสมบัติของจำนวนเฉพาะตลอดจนการพิสูจน์ข้อความที่เกี่ยวกับจำนวนเฉพาะ นอกจากนั้นเรายังมุ่งเน้นให้ผู้เรียนได้เห็นวิวัฒนาการและความสวยงามของจำนวนเฉพาะที่นักคณิตศาสตร์ในอดีตได้ทุ่มเทความรู้ ความสามารถ เพื่อสร้างงานทางทฤษฎีจำนวน และยังให้ผู้เรียนได้นำความรู้ที่ได้รับจากการศึกษาดังกล่าวไปใช้ในการแก้ปัญหาต่าง ๆ รวมทั้งหาแนวทางในการตอบข้อคาดเดาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเฉพาะ

3.1 นิยามของจำนวนเฉพาะและข้อเท็จจริงบางประการเกี่ยวกับจำนวนเฉพาะ

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์ (2548 : 57-59) ได้กล่าวว่า อริสโตเติล (Aristotle 384-322 ปีก่อนคริสต์ศักราช) และยุคลิด ได้แยกจำนวนเต็มบวกออกจากกันเป็นสองกลุ่ม โดยกลุ่มแรกได้แก่ $2, 3, 5, 7, 11, 13, 17, \ldots$ ซึ่งเรียกว่า**จำนวนเฉพาะ** และอีกกลุ่มหนึ่งได้แก่ $4, 6, 8, 9, 10, 12, 14, \ldots$ ซึ่งเรียกว่า **จำนวนประกอบ** บทนิยามต่อไปนี้จะกล่าวถึงการพิจารณาว่าจำนวนเต็มใดเป็นจำนวนเฉพาะ

บทนิยาม 3.1.1

จำนวนเต็ม $p > 1$ เรียกว่า **จำนวนเฉพาะ (prime number)** ถ้าจำนวนเต็มบวกที่มาหารได้ลงตัวมีเพียง 1 และ p เท่านั้น จำนวนเต็มที่มากกว่า 1 และไม่ใช่จำนวนเฉพาะ จะเรียกว่า **จำนวนประกอบ (composite number)** หรือเราจะเรียกจำนวนเต็ม p ว่า จำนวนเฉพาะ ก็ต่อเมื่อ $p \neq \pm 1$ และถ้า $a, b \in \mathbb{Z}$ และ $p = ab$ แล้ว $a = \pm 1$ หรือ $b = \pm 1$

จากบทนิยามของจำนวนเฉพาะ เราพบว่า

(1) $2, -2$ เป็นจำนวนเฉพาะที่เป็นจำนวนเต็มคู่ จำนวนเฉพาะอื่น ๆ จะเป็นจำนวนเต็มคี่

(2) ถ้า p เป็นจำนวนเฉพาะ แล้ว $-p$ เป็นจำนวนเฉพาะ

(3) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ ถ้า $a \mid p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$

(4) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ จะได้ $p \nmid a$ ก็ต่อเมื่อ $(p, a) = 1$

(5) ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ จะได้ว่า $p \mid a$ ก็ต่อเมื่อ $(p, a) = |p|$

(6) ถ้า p และ q เป็นจำนวนเฉพาะและ $p \mid q$ แล้ว $p = q$

ข้อตกลง เราอาจกล่าวถึงจำนวนเฉพาะที่เป็นบวกเท่านั้น นั่นคือ ต่อไปนี้เมื่อกล่าวถึงจำนวนเฉพาะ p เราจะหมายถึง จำนวนเฉพาะ $p \in \mathbb{N}$ เท่านั้น และจำนวนเต็มที่มากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่า **จำนวนประกอบ** (composite number) กล่าวคือ n เป็นจำนวนประกอบ ก็ต่อเมื่อ มี $a, b \in \mathbb{N}$ ซึ่ง $1 < a \leq b < n$ ที่ทำให้ $n = ab$

ตัวอย่าง 3.1.1

$2, 3, 5$ เป็นจำนวนเฉพาะ แต่ $4, 6, 8$ เป็นจำนวนประกอบ

ตัวอย่าง 3.1.2

จำนวนเฉพาะ 20 ตัวแรกได้แก่ $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71$

ตัวอย่าง 3.1.3

จงหาจำนวนเฉพาะที่มีค่าระหว่าง 100 ถึง 300

วิธีทำ จำนวนเฉพาะทั้งหมดที่มีค่าอยู่ระหว่าง 100 ถึง 300 คือ

$101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193,$
$197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293$

ตัวอย่าง 3.1.4

จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $2^p - 1$ ไม่เป็นจำนวนเฉพาะ

การพิสูจน์ มีจำนวนเฉพาะ $p = 11$ ที่ทำให้ $2^{11} - 1 = 2047 = 23 \cdot 89$
ดังนั้น $2^{11} - 1$ ไม่เป็นจำนวนเฉพาะ □

ตัวอย่าง 3.1.5

แสดงว่า ถ้า n เป็นจำนวนประกอบ แล้ว $2^n - 1$ เป็นจำนวนประกอบ

การพิสูจน์ สมมติว่า n เป็นจำนวนประกอบ
จะต้องแสดงว่า $2^n - 1$ เป็นจำนวนประกอบ
เนื่องจาก n เป็นจำนวนประกอบ แสดงว่าจะมี $a, b \in \mathbb{N} \setminus \{1\}$ ซึ่ง $n = ab$
จาก $x^b - 1 = (x-1)\left(x^{b-1} + x^{b-2} + \cdots + x + 1\right)$ เมื่อ $x, b \in \mathbb{N}$
จะได้ว่า $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$

$$= (2^a - 1)\left[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1\right]$$

$$= MN$$

เมื่อ $M = 2^a - 1$ และ $N = (2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1$
นั่นคือ $M, N \in \mathbb{N} \setminus \{1\}$
ดังนั้น เราจึงได้ $2^n - 1$ เป็นจำนวนประกอบ □

ทฤษฎีบท 3.1.1

ทุกจำนวนเต็ม $n > 1$ จะมีจำนวนเฉพาะ p ซึ่ง $p \mid n$

การพิสูจน์ ให้ $S = \{n \in \mathbb{N} \mid n > 1$ และไม่มีจำนวนเฉพาะที่ $p \mid n\}$
สมมติว่า $S \neq \varnothing$ โดยหลักการจัดอันดับดี จะมี $n_0 \in S$
ซึ่ง n_0 เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุดใน S
ดังนั้น n_0 ไม่เป็นจำนวนเฉพาะ
แสดงว่าจะมี $d \in \mathbb{N}$ ซึ่ง $1 < d < n_0$ ที่ทำให้ $d \mid n_0$

นั่นคือ จะมีจำนวน p ซึ่ง $p \mid d$
ทำให้ได้ว่า $p \mid n_0$ ซึ่งขัดแย้งกับสมบัติของ $n_0 \in S$
ดังนั้น $S \neq \varnothing$
สรุปได้ว่า ทุก ๆ จำนวนเต็ม $n > 1$ จะมีจำนวนเฉพาะ p ซึ่ง $p \mid n$ □

ถ้าเรากำหนดให้ p เป็นจำนวนเฉพาะ และ $p \mid ab$ โดยที่ $a, b \in \mathbb{Z}$ จะได้ว่า $p \mid a$ หรือ $p \mid b$ ดังทฤษฎีบทต่อไปนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 35, นิตยา ตรีนันทวัน. 2544 : 52, David M. Burton. 2007 : 40)

ทฤษฎีบท 3.1.2

ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ จะได้ว่า ถ้า $p \mid ab$ แล้ว $p \mid a$ หรือ $p \mid b$

การพิสูจน์ ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ สมมติว่า $p \mid ab$ และ $p \nmid a$
จะได้ว่า $p \mid ab$ และ $(p, a) = 1$
โดยทฤษฎีบท 2.4.7 ข้อ 3. จะได้ว่า $p \mid b$ □

จากทฤษฎีบทที่ 3.1.2 นี้จะมีประโยชน์มากและสามารถนำไปประยุกต์ในวิชาคณิตศาสตร์โดยทั่วไป เช่น การพิสูจน์ว่า $\sqrt{p}$ เป็นจำนวนอตรรกยะ สำหรับ p ที่เป็นจำนวนเฉพาะ เป็นต้น นอกจากนี้ทฤษฎีบท 3.1.2 สามารถขยายออกไปในกรณีที่เป็นผลคูณของจำนวนมากกว่า 2 จำนวน จะกล่าวดังทฤษฎีบทต่อไปนี้ (David M. Burton. 2007 : 40, สมจิต โชติชัยสถิตย์. 2540 : 17)

ทฤษฎีบท 3.1.3

ให้ $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ จะได้ว่า ถ้า $p \mid a_1 a_2 \cdots a_n$ แล้วจะมี a_i ที่ $1 \leq i \leq n$ ซึ่ง $p \mid a_i$

การพิสูจน์ เราจะพิสูจน์ทฤษฎีบทนี้โดยใช้หลักการอุปนัยเชิงคณิตศาสตร์
(i) ถ้า $n = 1$ เห็นได้ชัดว่าทฤษฎีบทนี้เป็นจริง
ให้ $p \mid a_1 a_2$ จากทฤษฎีบท 3.1.1 จะได้ว่า $p \mid a_1$ หรือ $p \mid a_2$
ดังนั้น ทฤษฎีบทนี้เป็นจริงเมื่อ $n = 2$
(ii) สมมติว่าทฤษฎีบทนี้เป็นจริงเมื่อ $n = k$
จะต้องแสดงว่าทฤษฎีบทนี้เป็นจริงเมื่อ $n = k + 1$
ให้ $p \mid a_1 a_2 \cdots a_k a_{k+1}$ โดยทฤษฎีบท 3.1.2 จะได้ว่า $p \mid a_1 a_2 \cdots a_k$ หรือ $p \mid a_{k+1}$
กรณีที่ 1 ถ้า $p \mid a_{k+1}$ จะได้ว่ามี $i = k + 1$ ซึ่ง $p \mid a_i$
กรณีที่ 2 ถ้า $p \mid a_1 a_2 \cdots a_k$ จากสมมติฐานจะได้ว่ามี a_i ที่ $1 \leq i \leq k$
ซึ่ง $p \mid a_i$ ดังนั้นจะมี a_i ที่ $1 \leq i \leq k + 1$ ซึ่ง $p \mid a_i$
นั่นคือทฤษฎีบทนี้เป็นจริงเมื่อ $n = k + 1$
จาก (i) และ (ii) จะได้ว่า ถ้า $p \mid a_1 a_2 \cdots a_n$ แล้วจะมี a_i ที่ $1 \leq i \leq n$ ซึ่ง
$p \mid a_i$ เป็นจริง สำหรับทุกจำนวนเต็มบวก n □

จาก $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ และพิจารณาลำดับของจำนวนเต็มบวกที่เรียงต่อเนื่องกันต่อไปนี้
ลำดับ $14, 15, 16$ เป็นลำดับของจำนวนประกอบ 3 จำนวนเรียงกัน

ลำดับ $24, 25, 26, 27, 28$ เป็นลำดับของจำนวนประกอบ 5 จำนวนเรียงกัน

ลำดับ $120, 121, 122, 123, 124, 125, 126$ เป็นลำดับของจำนวนประกอบ 7 จำนวนเรียงกัน

ถ้าเราจะลองหาลำดับของจำนวนประกอบ 10 จำนวนเรียงกันหรือจำนวนประกอบ 20 จำนวนเรียงกันจะหาได้หรือไม่ คำตอบก็คือหาได้ ซึ่งเราสามารถค้นหาได้จากวิธีการที่จะกล่าวในตัวอย่างต่อไปนี้

ตัวอย่าง 3.1.6

ให้ $n \in \mathbb{N}$ จงแสดงว่ามีจำนวนประกอบเรียงต่อเนื่องกัน n จำนวน

วิธีทำ สำหรับ $i = 1, 2, 3, 4, \ldots, n+1$ จำนวน $(n+1)! + i$ เป็นจำนวนประกอบ

ดังนั้น ลำดับ $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$

เป็นลำดับของจำนวนประกอบ n จำนวนเรียงต่อเนื่องกัน

นพพร ธนชัยขันธ์ (2543 : 53) ได้ทำการพิสูจน์ว่า ถ้าให้ p และ q เป็นจำนวนเฉพาะทั้งคู่ ซึ่ง $p \mid q$ แล้ว $p = q$ การพิสูจน์ดังบทตั้งต่อไปนี้

บทตั้ง 3.1.1

ให้ p และ q เป็นจำนวนเฉพาะบวกทั้งคู่ ถ้า $p \mid q$ แล้ว $p = q$

การพิสูจน์ ให้ p และ q เป็นจำนวนเฉพาะที่ $p \mid q$

โดยบทนิยามของการหารลงตัวจะได้ว่ามีจำนวนเต็ม m ที่ $q = pm$

เนื่องจาก p และ q เป็นจำนวนเต็มบวก

ดังนั้น m เป็นจำนวนเต็มบวก นั่นคือ $m \geq 1$

แต่ถ้า $m > 1$ จะส่งผลให้ q เป็นจำนวนประกอบ

ซึ่งขัดแย้งกับข้อกำหนด ดังนั้น $m = 1$

ทำให้ได้ว่า $p = q$ □

ดำรงค์ ทิพย์โยธา (2556 : 68) ได้ใช้ข้อเท็จจริงจากบทตั้ง 3.1.1 มาใช้ในการพิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.1.4

ถ้า $q, p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะ และ $q \mid (p_1 p_2 \cdots p_n)$ แล้ว มี i ที่ทำให้ $q = p_i$

การพิสูจน์ ให้ $q, p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะ

และ $q \mid (p_1 p_2 \cdots p_n)$

โดยทฤษฎีบท 3.1.3 จะมี i ที่ทำให้ $q \mid p_i$

เพราะว่า q, p_i เป็นจำนวนเฉพาะ และ $q \mid p_i$

เพราะฉะนั้น $q = p_i$ □

บทนิยาม 3.1.2

จำนวนเต็ม $a_1, a_2, a_3, \ldots, a_n$ จะเรียกว่าเป็น **จำนวนเฉพาะสัมพัทธ์** (relatively prime numbers) ก็ต่อเมื่อ $(a_1, a_2, a_3, \ldots, a_n) = 1$ และถ้าทุก i, j ที่ $i \neq j, (a_i, a_j) = 1$ แล้วจะกล่าวว่า $a_1, a_2, a_3, \ldots, a_n$ เป็น **จำนวนเฉพาะสัมพัทธ์ทุกคู่** (pairwise relatively prime number)

ตัวอย่าง 3.1.7

1. $(53, 122, 471) = 1$
2. $(111, 1111, 11111) = 1$
3. $(101, 10101, 1010101) = 1$

ตัวอย่าง 3.1.8

1. 4 กับ 9 เป็นจำนวนเฉพาะสัมพัทธ์
2. $4, 6, 9$ เป็นจำนวนเฉพาะสัมพัทธ์ แต่ไม่เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่
3. $7, 9, 10$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ และเป็นจำนวนเฉพาะสัมพัทธ์

จากบทนิยาม 2.4.2 จะได้ว่า ถ้า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ เช่น $(24, 60, 49) = 1$ แสดงว่า $24, 60$ และ 49 เป็นจำนวนเฉพาะสัมพัทธ์ แต่จะเห็นว่า $(24, 60) = 12 \neq 1$ ดังนั้น $24, 60, 49$ ไม่เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แต่ถ้า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์เสมอ ซึ่งพิสูจน์ได้ตามทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.1.5

สำหรับจำนวนเต็ม $a_1, a_2, a_3, \ldots, a_n$ ใด ๆ ถ้า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์

การพิสูจน์ ให้ $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ และให้ $d = (a_1, a_2, a_3, \ldots, a_n)$
จะได้ว่า $d \mid a_1$ และ $d \mid a_2$ โดยบทแทรก 2.4.1
จะได้ว่า $d \mid (a_1, a_2)$ เพราะว่า $(a_1, a_2) = 1$ จะได้ $d = 1$
นั่นคือ $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ □

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์ (2548 : 69) ได้ยกตัวอย่างปัญหาที่เกี่ยวกับจำนวนเฉพาะสัมพัทธ์ทุกคู่ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.1.9

จากการคำนวณ เราพบว่า $2 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$ และ $3, 5, 17$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ จงตรวจสอบว่า จำนวนเต็มที่อยู่ในลำดับ

$$2 + 1,\ 2^2 + 1,\ 2^4 + 1,\ 2^8 + 1, \ldots, 2^{2^n} + 1, \ldots$$

เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่หรือไม่

วิธีทำ เขียนจำนวนเต็มแต่ละพจน์ของลำดับที่อยู่ในรูป $2^{2^n} + 1$ เป็น $(2^{2^n} - 1) + 2$
เนื่องจาก $2^{2^n} + 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1)$ ในทำนองเดียวกัน

$$\begin{aligned} 2^{2^{n-1}} - 1 &= (2^{2^{n-2}} + 1)(2^{2^{n-2}} - 1) \\ &= (2^{2^{n-2}} + 1)(2^{2^{n-3}} + 1) \cdots (2^{2^m} + 1) \cdots (2^2 + 1)(2 + 1)(2 - 1) \end{aligned}$$

ดังนั้น $2^{2^n} + 1 = \left[(2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1) \cdots (2^{2^m} + 1) \cdots (2^2 + 1)(2 + 1)(2 - 1)\right] + 2$
สมมติว่า $\left(2^{2^n} + 1, 2^{2^m} + 1\right) = d$ เมื่อ $m < n$

แสดงว่า $d \mid \left(2^{2^n}+1\right)$ และ $d \mid \left(2^{2^m}+1\right)$ ซึ่งทำให้ได้ว่า $d \mid 2$
จะได้ว่า $d = 1$ หรือ 2 เนื่องจาก $2^{2^n}+1$ และ $2^{2^m}+1$ เป็นจำนวนเต็มคี่เสมอ
ดังนั้น $\left(2^{2^n}+1, 2^{2^m}+1\right) = 1$
นั่นคือ จำนวนเต็มที่เขียนอยู่ในรูป $2^{2^n}+1, 2^{2^m}+1$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่
สำหรับจำนวนเต็มบวก m และ n ซึ่ง $m \neq n$

3.2 ทฤษฎีบทหลักมูลของเลขคณิต

ทฤษฎีบทต่อไปนี้เป็นทฤษฎีบทที่สำคัญอย่างยิ่งต่อการนำไปใช้ ในการศึกษาทฤษฎีบทต่าง ๆ ซึ่งยุคลิดเขียนไว้ในหนังสือ Euclid's Elements Book IX : Proposition 14

ทฤษฎีบท 3.2.1 : ทฤษฎีบทหลักมูลของเลขคณิต (The Fundamental Theorem of Arithmetic)

ให้ $n \in \mathbb{Z}$ และ $n > 1$ จะได้ว่า n สามารถเขียนได้ในรูป $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$ โดยที่ $p_1, p_2, p_3, \ldots, p_k$ เป็นจำนวนเฉพาะ ซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, \ldots, k$ และจะเขียน n ในรูปดังกล่าวได้เพียงแบบเดียวเท่านั้น

การพิสูจน์ (i) ให้ $n \in \mathbb{Z}$ ซึ่ง $n > 1$
จะพิสูจน์ว่า n สามารถเขียนได้ในรูปของผลคูณของจำนวนเฉพาะ
กรณีที่ 1 ถ้า n เป็นจำนวนเฉพาะ
จะได้ว่าการเขียน $n = n$ สามารถเขียนได้เพียงแบบเดียว
กรณีที่ 2 ถ้า n เป็นจำนวนประกอบ จะได้ว่ามี $a, b \in \mathbb{N}$
ซึ่ง $1 < a \leq b < n$ ที่ทำให้ $n = ab$
โดยหลักอุปนัยเชิงคณิตศาสตร์ที่ 2
ถ้าสมมติว่า a และ b สามารถเขียนได้ในรูปผลคูณของจำวนวนเฉพาะ
ดังนั้น $n = ab$ ก็สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ
ภายใต้การจัดลำดับการคูณที่เหมาะสม จะได้ว่า n สามารถเขียนได้ในรูป

$$n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$$

โดย p_i เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$
สำหรับทุก $i = 1, 2, 3, \ldots, k$
(ii) ต่อไปจะแสดงว่า การเขียน n ในรูปดังกล่าวจะเขียนได้เพียงแบบเดียว
สมมติให้ $n = p_1p_2\cdots p_r$ โดยที่ $p_1 \leq p_2 \leq \cdots \leq p_r$
และ $n = q_1q_2\cdots q_s$ โดยที่ $q_1 \leq q_2 \leq \cdots \leq q_s$
ดังนั้น $p_1 \mid q_1q_2\cdots q_s$
จากทฤษฎีบท 3.1.3 จะได้ว่า $p_1 \mid q_i$ สำหรับ i บางตัว
นั่นคือ $p_1 = q_i$ แสดงว่า $p_1 \geq q_1$
ในทำนองเดียวกันสามารถพิสูจน์ได้ว่า $q_1 \geq p_1$ แสดงว่า $p_1 = q_1$
จาก $p_1p_2\cdots p_r = q_1q_2\cdots q_s$ และ $p_1 = q_1$
โดยสมบัติการตัดออกสำหรับการคูณ จะได้ว่า $p_2p_3\cdots p_r = q_2q_3\cdots q_s$

พิสูจน์ในทำนองเดียวกันจะได้ว่า $p_2 = q_2,\ p_3 = q_3,\ p_4 = q_4, \ldots$ ตามลำดับ
ถ้า $r < s$ จะได้ว่า $1 = q_{r+1}q_{r+2}\cdots q_s$ ซึ่งเป็นไปไม่ได้
เพราะว่า $q_{r+1}, q_{r+2}, \ldots, q_s > 1$
ถ้า $r < s$ จะได้ว่า $1 = p_{s+1}p_{s+2}\cdots p_r$ ซึ่งเป็นไปไม่ได้
เพราะว่า $p_{s+1},\ p_{s+2}, \ldots, p_r > 1$
ดังนั้น $r = s$ นั่นคือ $p_1 = q_1,\ p_1 = q_2, \ldots, p_r = q_s = q_r$
จาก (i) และ (ii) สรุปได้ว่า n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้แบบเดียว □

ข้อตกลง เราจะเรียกการเขียน $n > 1$ ในรูป $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$ โดยที่ $p_1, p_2, p_3, \ldots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, \ldots, k$ ว่าเป็น **การเขียนในรูปแบบบัญญัติ** (canonical form) ของ n (สมจิต โชติชัยสถิตย์. 2540 : 19, ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2547 : 62, David M. Burton. 2007 : 42)

จากทฤษฎีบท 3.2.1 จะได้ว่า
(1) จำนวนเต็ม $n > 1$ สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะได้เพียงแบบเดียวเท่านั้น
(2) ให้ $m = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$ และ $n = p_1^{b_1}p_2^{b_2}p_3^{b_3}\cdots p_k^{b_k}$
โดยที่แต่ละจำนวนเต็ม a_i, b_i ซึ่ง $a_i \geq 0$ และ $b_i \geq 0$ โดยที่ไม่เป็นศูนย์พร้อมกัน
จะได้ว่า $(m, n) = p_1^{d_1}p_2^{d_2}p_3^{d_3}\cdots p_k^{d_k}$
และ $[m, n] = p_1^{c_1}p_2^{c_2}p_3^{c_3}\cdots p_k^{c_k}$
เมื่อ $d_i = \min\{a_i, b_i\}$ และ $c_i = \max\{a_i, b_i\}$ ทุก $i = 1, 2, 3, \ldots$
จากข้อสังเกตข้างต้น เราสามารถสรุปได้ว่า $(m, n)[m, n] = mn$

ทฤษฎีบทหลักมูลของเลขคณิตนี้เป็นเครื่องมือที่สำคัญมากในการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็ม เพราะเราสามารถทำได้โดยการพิจารณาว่าจำนวนเต็มนั้นเป็นจำนวนเฉพาะหรือผลคูณของจำนวนเฉพาะ ซึ่งทำให้ง่ายต่อการพิจารณา ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.2.1

จงเขียน $48, 15750$ และ 846846 ในรูปแบบบัญญัติ

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$$
$$15750 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$$
$$846846 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 47$$

ตัวอย่าง 3.2.2

จงหาจำนวนตัวหารทั้งหมดของ 4725

วิธีทำ เนื่องจาก $4725 = 3^3 \cdot 5^2 \cdot 7$ จะได้ว่าตัวหารของ 4725 คือ
$1,\ 3,\ 3^3,\ 5,\ 5^2,\ 7,\ 3{\cdot}5,\ 3{\cdot}5^2,\ 3{\cdot}5{\cdot}7,\ 3{\cdot}5^2{\cdot}7,\ 3^2{\cdot}5,\ 3^2{\cdot}5^2,\ 3^2{\cdot}5{\cdot}7,\ 3^2{\cdot}5^2{\cdot}7,\ 3^3{\cdot}5,\ 3^3{\cdot}5^2$
$3^3 \cdot 5 \cdot 7,\ 3^3 \cdot 5^2 \cdot 7,\ 5 \cdot 7,\ 5^2 \cdot 7,\ 3 \cdot 7,\ 3^2 \cdot 7,\ 3^3 \cdot 7$
ดังนั้น จำนวนตัวหารทั้งหมดของ 4725 คือ 24

รูปแบบบัญญัติของจำนวนเต็ม $a > 1$ ที่มีจำนวนเฉพาะจำนวนเดียว เราจะเรียก a ว่าเป็นกำลังเฉพาะ (prime power) เช่น $7 = 7^1$, $9 = 3^2$ และ $32 = 2^5$ เป็นต้น

นพพร ธนะชัยขันธ์ (2543 : 55-56) ได้กล่าวว่า นอกจากนี้แล้วทฤษฎีหลักมูลของเลขคณิตสามารถนำมาใช้ในการหา ห.ร.ม. และ ค.ร.น. ได้ โดยจะแสดงวิธีการดังกล่าวดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.2.3

จงหา $(756, 2205)$ และ $[756, 2205]$ โดยใช้การแยกตัวประกอบเฉพาะ

วิธีทำ เนื่องจากเมื่อเขียน 756 และ 2205 ในรูปแบบบัญญัติ
จะได้ว่า $756 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^1$
และ $2205 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^2$
เนื่องจาก $(756, 2205)$ ต้องหารทั้ง 756 และ 2205 ลงตัว
ดังนั้นเราจะเปรียบเทียบเลขชี้กำลังของจำนวนเฉพาะเป็นคู่ ๆ
ที่ปรากฏในรูปมาตรฐานของทั้งสองจำนวน แล้วเลือกเอาเลขชี้กำลังของจำนวนเฉพาะ
ที่มีค่าน้อยที่สุดในแต่ละคู่นั้น
จะได้ว่า $(756, 2205) = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 63$
ในทำนองเดียวกัน สำหรับ $[756, 2205]$ เนื่องจาก 756 และ 2205 จะต้องหาร $[756, 2205]$ ลงตัว
ดังนั้นเราจะเปรียบเทียบเลขชี้กำลังของจำนวนเฉพาะที่มีค่ามากที่สุดในแต่ละคู่นั้น
จะได้ว่า $[756, 2205] = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^2 = 26460$

จากตัวอย่าง 3.2.3 นำไปสู่ทฤษฎีบทที่น่าสนใจดังต่อไปนี้

ทฤษฎีบท 3.2.2

ให้ a และ b เป็นจำนวนเต็ม ซึ่ง $a > 1$ และ $b > 1$ เขียนในรูปมาตรฐาน $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ และ $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ เมื่อ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $a_1, aa_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ เป็นจำนวนเต็มที่ไม่เป็นลบ จะได้ว่า

$$(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}$$

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}$$

การพิสูจน์ สามารถพิสูจน์ได้โดยตรง โดยอาศัยทฤษฎีบท 3.2.1 และบทนิยามของ ห.ร.ม. และ ค.ร.น. □

จากทฤษฎีบท 3.2.2 เราสามารถหา ห.ร.ม. และ ค.ร.น. ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.2.4

ให้ $a = 264 = 2^3 \cdot 3 \cdot 11,\ b = 157950 = 2 \cdot 3^5 \cdot 5^2 \cdot 13$ จงหา (a, b) และ $[a, b]$

วิธีทำ ให้ $a = 264 = 2^3 \cdot 3 \cdot 11,\ b = 157950 = 2 \cdot 3^5 \cdot 5^2 \cdot 13$
เขียน a และ b ในรูปแบบที่มีตัวประกอบ $2, 3, 5, 11, 13$ เหมือนกัน
เพราะฉะนั้น $a = 2^3 \cdot 3^1 \cdot 11^1 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 11^1 \cdot 13^0$ และ
$b = 2^1 \cdot 3^5 \cdot 5^2 \cdot 13^1 = 2^1 \cdot 3^5 \cdot 5^2 \cdot 11^0 \cdot 13^1$
เพราะฉะนั้น $a_1 = 3,\ a_2 = 1,\ a_3 = 0,\ a_4 = 1,\ a_5 = 0$ และ
$b_1 = 1,\ b_2 = 5,\ b_3 = 2,\ b_4 = 0,\ b_5 = 1$

ให้ $d_1 = \min\{3,1\} = 1,\ d_2 = \min\{1,5\} = 1,\ d_3 = \min\{0,2\} = 0,$
$d_4 = \min\{1,0\} = 0,\ d_5 = \min\{0,1\} = 0$ และ
$e_1 = \max\{3,1\} = 3,\ e_2 = \max\{1,5\} = 5,\ e_3 = \max\{0,2\} = 2,$
$e_4 = \max\{1,0\} = 1,\ e_5 = \max\{0,1\} = 1$
เพราะฉะนั้น $(a,b) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 11^0 \cdot 13^0 = 2 \cdot 3 = 6$ และ
$$[a,b] = 2^3 \cdot 3^5 \cdot 5^2 \cdot 11^1 \cdot 13^1$$

ตัวอย่าง 3.2.5

ให้ $a = 2^3 \cdot 3 \cdot 7^2,\ b = 3^3 \cdot 5^2 \cdot 11$ จงหา (a,b) และ $[a,b]$

วิธีทำ ให้ $a = 2^3 \cdot 3 \cdot 7^2$ และ $b = 3^3 \cdot 5^2 \cdot 11$
เขียน a และ b ในรูปแบบที่มีตัวประกอบ $2, 3, 5, 11$ เหมือนกัน
เพราะฉะนั้น $a = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0$ และ
$$b = 2^0 \cdot 3^2 \cdot 5^2 \cdot 7^0 \cdot 11^1$$
จะได้ว่า $a_1 = 3,\ a_2 = 1,\ a_3 = 0,\ a_4 = 2,\ a_5 = 0$ และ
$b_1 = 0,\ b_2 = 2,\ b_3 = 2,\ b_4 = 0,\ b_5 = 1$
ให้ $d_1 = \min\{3,0\} = 0,\ d_2 = \min\{1,2\} = 1,\ d_3 = \min\{0,2\} = 0,$
$d_4 = \min\{2,0\} = 0,\ d_5 = \min\{0,1\} = 0$ และ
$e_1 = \max\{3,0\} = 3,\ e_2 = \max\{1,2\} = 2,\ e_3 = \max\{0,2\} = 2,$
$e_4 = \max\{2,0\} = 2,\ e_5 = \max\{0,1\} = 1$
เพราะฉะนั้น $(a,b) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3$ และ
$$[a,b] = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^1$$

3.3 การค้นหาจำนวนเฉพาะ

ถ้ากำหนดให้ n เป็นจำนวนเต็มบวก การที่จะตรวจสอบว่า n เป็นจำนวนเฉพาะหรือไม่ วิธีการหนึ่งก็คือการหาจำนวนเต็มบวกที่เป็นตัวหารที่น้อยกว่า n ถ้าไม่มีจำนวนใดหาร n ลงตัว ก็แสดงว่า n เป็นจำนวนเฉพาะ แต่วิธีการนี้จะใช้ประโยชน์ได้อย่างมีประสิทธิภาพก็ต่อเมื่อ n มีค่าไม่มากนัก เราสามารถลดขั้นตอนการตรวจสอบการเป็นจำนวนเฉพาะของ n ได้โดยทฤษฎีบทต่อไปนี้ (สมจิต โชติชัยสถิตย์. 2540 : 20, นงนุช สุขวารี และคณะ. 2547 : 187, นฤมล ศรชัยยืน. 2540 : 50)

ทฤษฎีบท 3.3.1

ถ้า n เป็นจำนวนประกอบ แล้วจะมีจำนวนเฉพาะ p ที่ $p \le \sqrt{n}$ และ $p \mid n$ (หรือ ถ้าไม่มีจำนวนเฉพาะ p ซึ่ง $p \le \sqrt{n}$ และ $p \mid n$ แล้ว n จะเป็นจำนวนเฉพาะ)

การพิสูจน์ ให้ n เป็นจำนวนประกอบ จะได้ว่ามี $a, b \in \mathbb{N}$
ซึ่ง $1 < a \le b < n$ ที่ทำให้ $n = ab$
ดังนั้น $a \mid n$ และ $b \mid n$ แสดงว่า $1 < a^2 \le ab = n$
ดังนั้น $a \le \sqrt{n}$
โดยทฤษฎีบท 3.1.1 จะมีจำนวนเฉพาะ p ซึ่ง $p \mid a$ ทำให้ได้ว่า $p \mid n$ และ $p \le \sqrt{n}$ □

ตัวอย่าง 3.3.1

จงตรวจสอบว่า 47 และ 89 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เพราะว่า $6 < \sqrt{47} < 7$ และ $2 \nmid 47,\ 3 \nmid 47,\ 5 \nmid 47$

เพราะฉะนั้น 47 เป็นจำนวนเฉพาะ

เพราะว่า $9 < \sqrt{89} < 10$ และ $2 \nmid 89,\ 3 \nmid 89,\ 5 \nmid 89,\ 7 \nmid 89$

เพราะฉะนั้น 89 เป็นจำนวนเฉพาะ

ตัวอย่าง 3.3.2

จงแสดงว่า 2017 เป็นจำนวนเฉพาะ

วิธีทำ เพราะว่า $45^2 = 2025$ และ $\sqrt{2017} < \sqrt{2025} = 45$

เพราะฉะนั้น $\sqrt{2017} < 45$

ให้ $A = \{p \mid p \text{ เป็นจำนวนเฉพาะ และ } p \leq \sqrt{2017}\}$

$= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 44\}$

เพราะว่า $\forall p \in A\ [p \nmid 2017]$ เพราะฉะนั้น 2017 เป็นจำนวนเฉพาะ

ตัวอย่าง 3.3.3

จงตรวจสอบว่า 401 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{401} < 21$ จากทฤษฎีบท 3.3.1

ถ้า 401 เป็นจำนวนประกอบแล้วจะมีจำนวนเฉพาะ p ที่ $p < 21$ และ p หาร 401 ลงตัว

แต่จากการตรวจสอบจำนวนเฉพาะทั้งหมดที่น้อยกว่า 21 คือ $2, 3, 5, 7, 11, 13, 17, 19$

ไม่มีจำนวนใดเลยที่หาร 401 ลงตัว

ดังนั้นสรุปได้ว่า 401 เป็นจำนวนเฉพาะ

ตัวอย่าง 3.3.4

จงตรวจสอบว่า 2093 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{2093} < 46$ ดังนั้นจำนวนเฉพาะที่น้อยกว่า 46

คือ $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$

แต่จากการตรวจสอบพบว่ามี 7 นำไปหาร 2093 ได้ลงตัว

ดังนั้น $2093 = 7 \cdot 299$ เป็นจำนวนประกอบ

ตัวอย่าง 3.3.5

จงหาจำนวนเฉพาะที่สามารถเขียนอยู่ในรูป $3n + 1$ ที่มีค่าน้อยกว่า 50

วิธีทำ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3n+1$	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49

ดังนั้น จำนวนเฉพาะทั้งหมดที่สามารถเขียนได้ในรูป $3n + 1$ ที่น้อยกว่า 50 คือ $7, 13, 19, 31, 37$ และ 43

อัจฉรา หาญชูวงศ์ (2542 : 23) ได้กล่าวถึงการหาจำนวนเฉพาะทุกตัวที่น้อยกว่าหรือเท่ากับ n เมื่อกำหนดจำนวนเต็ม n มาให้ โดยใช้ทฤษฎีบท 3.3.1 วิธีการนี้เรียกว่า ตะแกรงเอราโตสเทเนส (Sieve of Eratosthenes) ซึ่งทำได้ดังนี้

(1) ให้ $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots, p_k$ เป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$

(2) เขียนจำนวนเต็มตั้งแต่ 2 ถึง n

(3) วงกลม $p_1 = 2$ และกำจัดจำนวนเต็มทุกตัวในข้อ (2) ที่หารด้วย 2 ลงตัว

(4) วงกลม $p_2 = 3$ แล้วกำจัดจำนวนเต็มที่เหลือจากข้อ (3) ที่หารด้วย 3 ลงตัว

ทำเช่นนี้ต่อไปจนถึง p_k

จำนวนเต็มที่เหลือจะเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ n

ตัวอย่าง 3.3.6

จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 100

วิธีทำ จำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ $\sqrt{100} = 10$ คือ $2, 3, 5, 7$

กำจัดจำนวนเต็มที่หารด้วย $2, 3, 5$ และ 7 ลงตัวด้วย $/$, $//$, $\backslash$ และ $\backslash\backslash$ ตามลำดับ

	(2)	(3)	4	(5)	6	(7)	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

ดังนั้นจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 100 คือ $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ และ 97

3.4 ทฤษฎีบทที่สำคัญของจำนวนเฉพาะ

ทฤษฎีบทหนึ่งที่สำคัญของจำนวนเฉพาะที่จะกล่าวต่อไป คือ "มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์" นอกจากทฤษฎีบทนี้แล้วยังมีทฤษฎีบทอีกหลายทฤษฎีบทที่สำคัญซึ่งเกี่ยวข้องกับจำนวนเฉพาะ โดยเราจะนำมากล่าวไว้ในหัวข้อนี้

ยุคลิด ได้รับการยกย่องว่าเป็นนักคณิตศาสตร์คนแรกที่พิสูจน์ว่า "มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์" ซึ่งบทพิสูจน์ของเขาปรากฏในหนังสือ (Euclid's Element Book IX)

ทฤษฎีบท 3.4.1 : (Euclid)

มีจำนวนเฉพาะอยู่จำนวนอนันต์ (หรือไม่มีจำนวนเฉพาะที่มีค่ามากที่สุด)

การพิสูจน์ สมมติว่ามีจำนวนเฉพาะอยู่เป็นจำนวนจำกัด
นั่นคือ ให้ $p_1, p_2, p_3, \ldots, p_n$ เป็นลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปหามาก
และ p_n เป็นจำนวนเฉพาะที่มีค่ามากที่สุด
ให้ $N = p_1p_2p_3 \cdots p_n + 1$ จะได้ว่า $N > p_n$ แสดงว่า N เป็นจำนวนประกอบ
โดยทฤษฎีบท 3.1.1 จะมีจำนวนเฉพาะ p ซึ่ง $p \mid N$
และจากสมมติฐานจะได้ว่า $p \in \{p_1, p_2, \ldots, p_n\}$
ดังนั้น $p \mid p_1p_2 \cdots p_n$ แสดงว่า $p \mid 1$ ซึ่งเป็นไปไม่ได้
นั่นคือ มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ □

การพิสูจน์ว่าจำนวนเฉพาะมีจำนวนอนันต์ของยุคลิดนั้น ได้การยอมรับกว่า 2000 ปีมาแล้ว ต่อมานักคณิตศาสตร์รุ่นหลังได้พยายามที่จะหาแนวทางการพิสูจน์ของทฤษฎีบท 3.4.1 นี้ และอย่างน้อยที่เห็นปรากฏในหนังสือ Proofs from the Book (Aigner and Ziegler, 1998) ได้กล่าวถึงบทพิสูจน์ของทฤษฎีบทดังกล่าวนี้ที่แตกต่างกันไว้ถึง 6 แบบด้วยกัน ทฤษฎีบท 3.4.1 นี้ ถือว่ามีความสำคัญยิ่งของการนำไปสู่ข้อคาดเดาต่าง ๆ มากมายโดยจะกล่าวในหัวข้อต่อไป

ให้ p เป็นจำนวนเฉพาะและกำหนด p^* แทนผลคูณของจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ p จากการคำนวณค่าของ p^* เมื่อ $p = 2, 3, 5, 7, 11$ จะพบว่า

$$\begin{aligned} 2^* + 1 &= 2 + 1 = 3 \\ 3^* + 1 &= 2 \cdot 3 + 1 = 7 \\ 5^* + 1 &= 2 \cdot 3 \cdot 5 + 1 = 31 \\ 7^* + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \\ 11^* + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \end{aligned}$$

เป็นจำนวนเฉพาะทุกจำนวน
อย่างไรก็ตาม $13^* + 1 = 59 \cdot 509$

$17^* + 1 = 19 \cdot 97 \cdot 277$

$19^* + 1 = 347 \cdot 27953$

ไม่เป็นจำนวนเฉพาะ
จากตัวอย่างข้างต้นทำให้เราสามารถตั้งข้อคาดเดาขึ้นมาได้ดังนี้

ข้อคาดเดา มีจำนวนเฉพาะหรือจำนวนประกอบอยู่จำนวนอนันต์หรือไม่ที่เขียนอยู่ในรูป $p^* + 1$

ในปี ค.ศ. 1995 เราพบว่ามีจำนวนเฉพาะ 18 จำนวนที่เขียนอยู่ในรูป $p^* + 1$ ซึ่งได้แก่ $2^* + 1$, $3^* + 1$, $5^* + 1$, $7^* + 1$, $11^* + 1$, $31^* + 1$, $379^* + 1$, $1019^* + 1$, $1021^* + 1$, $2675^* + 1$ $3229^* + 1$, $4547^* + 1$, $4787^* + 1$, $11549^* + 1$, $13649^* + 1$, $18523^* + 1$, $23801^* + 1$ และ $24029^* + 1$ และจำนวนที่ใหญ่ที่สุดของจำนวนเฉพาะดังกล่าวนี้ประกอบด้วยเลขโดด 10359 หลัก นอกจากนี้พบว่า $p^* + 1$ เป็นจำนวนประกอบเมื่อ $p \leq 35000$ ยกเว้น $p = 2, 3, 57, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801$ และ 24029

เราจะเรียกจำนวนเต็มที่เขียนอยู่ในรูป $p^* + 1$ ว่า "**จำนวนเต็มแบบยุคลิด**" (Euclidean numbers) ทั้งนี้เพราะจำนวนเต็มดังกล่าวถูกพิจารณาโดยยุคลิด เมื่อเขาใช้พิสูจน์ข้อความ "มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์"

ทฤษฎีบท 3.4.2

ให้ $p_1, p_2, p_3, \ldots, p_n, p_{n+1}, \ldots$ เป็นลำดับของจำนวนเฉพาะที่เรียงจากน้อยไปมาก จะได้ว่า

$$p_{n+1} \leq p_1 p_2 p_3 \cdots p_n + 1$$

การพิสูจน์ **กรณีที่ 1** ถ้า $p^* = p_1 p_2 p_3 \cdots p_n + 1$ เป็นจำนวนเฉพาะ
เห็นได้ชัดว่า $p_n < p^*$ ดังนั้น $p_{n+1} \leq p^*$
กรณีที่ 2 ถ้า $P = p_1 p_2 p_3 \ldots p_n + 1$ เป็นจำนวนประกอบ
จะได้ว่ามีจำนวนเฉพาะ p' ที่เล็กที่สุดที่เป็นตัวหารของ p
แต่ $p_1 \nmid p,\ p_2 \nmid p,\ p_3 \nmid p, \ldots, p_n \nmid p$
เพราะว่า ถ้า $p_i \nmid p$ แล้ว $p_i \mid 1$ สำหรับทุก $i \in \{1, 2, 3, \ldots, n\}$
ดังนั้นจำนวนเฉพาะ p' ที่หาร p ลงตัวจะต้องมีค่ามากกว่า p_n
ซึ่งสรุปได้ว่า $p_{n+1} \leq p'$ และจาก p' เป็นตัวหารของ p จะได้ว่า $p_{n+1} \leq p'$
จากทั้งสองกรณีจะได้ว่า จำนวนเฉพาะตัวที่ $n+1$ คือ $p_{n+1} \leq p = p_1 p_2 p_3 \cdots p_n + 1$ □

ทฤษฎีบท 3.4.3

ให้ $p_1,\ p_2,\ p_3, \ldots, p_n, \ldots$ แทนลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปหามาก จะได้ว่า $p_n \leq 2^{2^{n-1}}$ สำหรับทุกจำนวนเต็มบวก n

การพิสูจน์ จะพิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ที่ 2
(i) $p_1 = 2 \leq 2^{2^0} = 2$ เป็นจริง
(ii) สมมติว่า $p_k \leq 2^{2^{k-1}}$ เป็นจริงสำหรับทุก $k \leq n$ จะต้องพิสูจน์ว่า $p_{n+1} \leq 2^{2^n}$
จาก $p_1 \leq 2^{2^{1-1}}, p_2 \leq 2^{2^{2-1}}, p_3 \leq 2^{2^{3-1}}, \ldots, p_n \leq 2^{2^{n-1}}$
จะได้ว่า $p_1 p_2 p_3 \cdots p_n \leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{n-1}}$

$$= 2^{2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}}$$

$$= 2^{2^n - 1}$$

ดังนั้น $p_1 p_2 p_3 \cdots p_n + 1 \leq 2^{2^n - 1} + 2^{2^n - 1}$
นั่นคือ $p_1 p_2 p_3 \cdots p_n + 1 \leq 2^{2^n}$
โดยทฤษฎีบท 3.4.2 จะได้ว่า $p_{n+1} \leq 2^{2^n}$
เพราะฉะนั้นจาก (i) และ (ii) สรุปได้ว่า $p_n \leq 2^{2^{n-1}}$ สำหรับทุก $n \in \mathbb{N}$ □

ตัวอย่าง 3.4.1

(1) $p_{30} = 113 \leq 2^{2^{30-1}}$
(2) $p_{100} = 541 \leq 2^{2^{100-1}}$

บทแทรก 3.4.1

สำหรับจำนวนเต็มบวก n จะมีจำนวนเฉพาะอย่างน้อยที่สุด $n+1$ จำนวนที่มีค่าน้อยกว่า 2^{2^n}

ในปี ค.ศ. 1845 โจเซฟ เบอร์ทราน (Joseph Bertrand ค.ศ. 1822-1900) ได้ตั้งข้อคาดเดาว่า "จะมีจำนวนเฉพาะหนึ่งจำนวนที่อยู่ระหว่าง n กับ $2n$ เมื่อ $n \geq 2$" ซึ่งเขามีความเชื่อมั่นว่าข้อคาดเดาที่ตั้งขึ้นเป็นจริง โดยการแสดงให้เห็นจริงได้เมื่อ $n \leq 3{,}000{,}000$ โดยพบจำนวนเฉพาะที่อยู่ระหว่าง n กับ $2n$ คือ

3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159389, ... ต่อมาในปี ค.ศ. 1850 พัฟนูติ ลีโววิช เชบีเชฟ (Pafnuti Lvovich Tschebychev ค.ศ. 1821-1894) นักคณิตศาสตร์ชาวรัสเซีย สามารถพิสูจน์ข้อคาดเดาของเบอร์ทรานได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.4.4 : (Tschebychev)

ให้ $n \in \mathbb{N}$ และ $n \geq 2$ จะได้ว่า มีจำนวนเฉพาะอย่างน้อยหนึ่งจำนวนในลำดับ $n, n+1, n+2, \ldots, 2n$

การพิสูจน์ของทฤษฎีบท 3.4.4 นี้ เชบีเชฟได้ใช้ความรู้ที่ลึกซึ้งและยาวมาก ต่อมาในปี ค.ศ. 1932 พอล เออร์ดอส (Paul Erdos ค.ศ. 1913-1996) นักคณิตศาสตร์ชาวฮังการีได้แสดงการพิสูจน์ทฤษฎีบทนี้ที่ง่ายกว่าของเชบีเชฟ ซึ่งในขณะนั้นเขามีอายุเพียง 19 ปี และผลงานชิ้นนี้ถือว่าเป็นผลงานชิ้นแรกของเขาที่ได้รับการตีพิมพ์ ผู้สนใจสามารถศึกษารายละเอียดได้จากหนังสือ Proofs from the Book ของ Martin Aigner and Gunter M. Ziegler หน้า 7-10 ในเวลา 65 ปีต่อมา เออร์ดอสสามารถสร้างผลงานทั้งหมดมากกว่า 1,500 ชิ้น

ทฤษฎีบทต่อไป ถือว่าเป็นทฤษฎีบทที่สำคัญอย่างยิ่งของจำนวนเฉพาะ ซึ่งมีชื่อว่า **ทฤษฎีบทของจำนวนเฉพาะ** (The Prime Number Theorem) โดยทฤษฎีบทนี้เกิดขึ้นจากการตั้งข้อคาดเดาของเกาส์ในปี ค.ศ. 1792 ซึ่งยังไม่มีการพิสูจน์ที่สมบูรณ์ ต่อมาในปี ค.ศ. 1896 ทฤษฎีบทนี้สามารถพิสูจน์ได้โดย อาดามาด์ (J.S. Hadamard ค.ศ. 1865-1963) และ ปูแซง (C.V. Poussin ค.ศ. 1866-1962) ซึ่งให้การพิสูจน์ที่แตกต่างกัน แต่ใช้ความรู้ด้านการวิเคราะห์เชิงซ้อนเหมือนกัน ต่อมาในปี ค.ศ. 1949 อาเทิล เซลเบอร์ก (Atle Selberg) ได้ทำให้เขาได้รับรางวัลสูงสุดคือ Fields Medal ซึ่งเทียบเท่ากับรางวัลโนเบล เมื่อปี ค.ศ. 1950 ในงาน International Congress of Mathematics ซึ่งจะจัดประจำทุก 4 ปี และสำหรับนักคณิตศาสตร์ที่อายุต่ำกว่า 40 ปี

ทฤษฎีบท 3.4.5 : ทฤษฎีบทของจำนวนเฉพาะ (The Prime Number Theorem)

ให้ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p ซึ่ง $p \leq n$ จะได้ว่า $\pi(n)$ มีค่าประมาณ $\dfrac{n}{\log n}$ เมื่อ n มีค่ามาก ๆ และ $\log n$ หมายถึงลอการิธึมฐานธรรมชาติของ n นั่นคือ $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n/\log n} = 1$

สำหรับการพิสูจน์ของทฤษฎีบท 3.4.5 นี้สามารถศึกษาได้จากหนังสือ Elementary Number Theory ของ David M. Burton (ปี ค.ศ. 2002) หน้า 352-359

ถ้า n มีค่ามาก ๆ แล้ว $\pi(n)$ จะมีค่าใกล้เคียงกับ $\dfrac{n}{\log n}$ ซึ่งพิจารณาได้จากตาราง ต่อไปนี้

n	$\pi(n)$	$\dfrac{n}{\log n}$	$\dfrac{\pi(n)}{n/\log n}$
10^3	168	145	1.159
10^4	1229	1086	1.132
10^5	9592	8686	1.104
10^6	78498	72382	1.084
10^7	664579	620420	1.071
10^8	5761455	542868	1.061

ถ้าเราแบ่งเซตของจำนวนเต็มบวกออกเป็น 4 กลุ่ม โดยพิจารณาจากเศษที่เกิดจากการหารจำนวนเต็มบวกนั้นด้วย 4 จะได้

$$\mathbb{N} = \{4k \mid k \in \mathbb{N}\} \cup \{4k+1 \mid k \in \mathbb{N}\} \cup \{4k+2 \mid k \in \mathbb{N}\} \cup \{4k+3 \mid k \in \mathbb{N}\}$$

และเราพบว่า ไม่มีจำนวนเฉพาะใน $\{4k \mid k \in \mathbb{N}\}$ และมี 2 ที่เป็นจำนวนเฉพาะเพียงจำนวนเดียวใน $\{4k+2 \mid k \in \mathbb{N}\}$ ส่วนจำนวนเฉพาะที่เหลือจะกระจายอยู่ในเซต $\{4k+1 \mid k \in \mathbb{N}\} \cup \{4k+3 \mid k \in \mathbb{N}\}$

ให้ $A = \{4k+1 \mid k \in \mathbb{N}\}$ และ $B = \{4k+3 \mid k \in \mathbb{N}\}$ เราพบว่า ผลคูณของสมาชิก 2 ตัวใน A ยังคงเป็นสมาชิกใน A ในขณะที่ผลคูณของสมาชิก 2 ตัวใน B จะเป็นสมาชิกใน A จากข้อสังเกตนี้นำไปสู่ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.4.6

ผลคูณของจำนวนเต็มที่เขียนอยู่ในรูป $4k+1$ ตั้งแต่สองจำนวนขึ้นไปจะเป็นจำนวนเต็มที่เขียนอยู่ในรูป $4k+1$

การพิสูจน์ ให้ $n_1 = 4k_1 + 1$ และ $n_2 = 4k_2 + 1$ เมื่อ k_1 และ k_2 เป็นจำนวนเต็ม

ดังนั้น $n_1 n_2 = (4k_1+1)(4k_2+1)$

$= 4(4k_1k_2 + k_1 + k_2) + 1$

$= 4k + 1$ เมื่อ $k = 4k_1k_2 + k_1 + k_2$ เป็นจำนวนเต็ม

โดยหลักอุปนัยเชิงคณิตศาสตร์ จะได้ว่า ทฤษฎีบทนี้เป็นจริง □

ทฤษฎีบท 3.4.7

มีจำนวนเฉพาะที่เขียนอยู่ในรูป $4k+3$ เป็นจำนวนอนันต์

การพิสูจน์ สมมติว่ามีจำนวนเฉพาะที่เขียนอยู่ในรูป $4k+3$ เป็นจำนวนจำกัด

นั่นคือ ให้ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะที่เขียนอยู่ในรูป $4k+3$

ทั้งหมดที่เรียงจากน้อยไปหามากและ p_n มีค่ามากที่สุด

ให้ $N = 4p_1p_2\cdots p_n - 1 = 4(p_1p_2\cdots p_n - 1) + 3$

จะได้ว่า $N > 1$ และ $N > p_n$

แสดงว่า N เป็นจำนวนประกอบ โดยทฤษฎีบท 3.2.1

จะได้ว่า N สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

นั่นคือ $N = q_1q_2\cdots q_t$ เมื่อ $q_1, q_2, \ldots, q_t$ เป็นจำนวนเฉพาะ

เนื่องจาก N เป็นจำนวนเต็มคี่ ดังนั้น q_i จะเขียนอยู่ในรูป $4k+1$ หรือ $4k+3$

ถ้าทุก q_i อยู่ในรูป $4k+1$ โดยทฤษฎีบท 3.4.6

จะได้ว่า N จะเขียนอยู่ในรูป $4k+1$ ซึ่งไม่จริง

ดังนั้น จะมี $q_r \in \{q_1, q_2, \ldots, q_t\}$ ซึ่งเขียนอยู่ในรูป $4k+3$

เพราะฉะนั้นมี $j \in \{1, 2, \ldots, n\}$ ซึ่ง $q_r = p_j$

นั่นคือ $p_j \mid N$ แต่ $p_j \mid p_1p_2\cdots p_n$

ดังนั้น $p_j \mid 1$ ซึ่งเป็นไปไม่ได้

สรุปได้ว่ามีจำนวนเฉพาะที่อยู่ในรูป $4k+3$ อยู่เป็นจำนวนอนันต์ □

จากทฤษฎีบท 3.4.7 ข้างต้นผู้เรียนอาจตั้งคำถามว่า จำนวนเฉพาะที่เขียนอยู่ในรูป $4k+1$ มีจำนวนอนันต์หรือไม่ หรือจำนวนเฉพาะที่เขียนในรูปแบบไหนจะมีจำนวนอนันต์ ปัญหานี้มีคำตอบแล้วโดยในปี ค.ศ. 1837 ดีริชเลต์เป็นผู้นำเสนอการพิสูจน์ โดยรายละเอียดของการพิสูจน์ปัญหานี้ยากเกินกว่าจะกล่าวไว้ ณ ที่นี้ ดังนั้นจะกล่าวเฉพาะตัวทฤษฎีบทเท่านั้นซึ่งมีรายละเอียดดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.4.8 : (Dirichlet)

ถ้า $a, b \in \mathbb{N}$ และ $(a, b) = 1$ แล้วจะมีจำนวนเฉพาะปรากฏอยู่ในลำดับเลขคณิตอนันต์เป็นจำนวนอนันต์

จากทฤษฎีบท 3.4.8 นี้ ถ้าเลือก $a = 999$ และ $b = 1000$ จะพบว่ามีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ที่ลงท้ายด้วย 999 เช่น $1999, 100999, 1000999, \ldots$ ปรากฏอยู่ในลำดับเลขคณิตอนันต์ ที่มีพจน์ที่ n คือ $1000n + 999$

ในทางกลับกันไม่มีลำดับเลขคณิตอนันต์ใด ที่จะทำให้สมาชิกในลำดับนั้นทุกตัวเป็นจำนวนเฉพาะ ให้ $a, a+b, a+2b, \ldots$ เป็นลำดับเลขคณิตอนันต์ โดยที่ $a, b \in \mathbb{N}$ จะได้ว่า พจน์ที่ $a+1$ คือ $a+ab = a(1+b)$ ดังนั้น ถ้า $a > 1$ แล้ว $a(1+b)$ ไม่เป็นจำนวนเฉพาะ

เรื่องเกี่ยวกับจำนวนเฉพาะยังมีอีกมากมายทั้งที่เป็นข้อคาดเดาและเป็นข้อเท็จจริงที่มีการพิสูจน์ได้แล้ว ในปี ค.ศ. 1737 ออยเลอร์ ได้พิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.4.9 : (Euler)

ให้ $p_1, p_2, p_3, \ldots$ แทนลำดับของจำนวนเฉพาะที่เรียงจากน้อยไปมาก จะได้ว่าอนุกรม $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots$ เป็นอนุกรมไดเวอร์เจนต์ (divergent series)

จากทฤษฎีบท 3.4.9 นี้ประกอบกับความจริงที่ว่า $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ เป็นอนุกรมคอนเวอร์เจนต์ (convergent series) เราอาจกล่าวได้ว่ามีจำนวนเฉพาะมากกว่าจำนวนที่เป็นกำลังสองสมบูรณ์

3.5 ข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ

ในหัวข้อนี้จะกล่าวถึงข้อคาดเดาที่เกี่ยวข้องกับจำนวนเฉพาะ เพื่อผู้เรียนจะได้เห็นวิวัฒนาการและความพยายามของนักคณิตศาสตร์ในอดีต

ข้อคาดเดาที่ 1 ข้อคาดเดาของโกลด์บัค (The Goldbach conjecture)

ในปี ค.ศ. 1742 โกลด์บัค (Christian Goldbach ค.ศ. 1690-1764) ได้ตั้งข้อคาดเดาไว้ 2 ข้อ คือ
(1) ทุก ๆ จำนวนเต็มคู่ $N \geq 6$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 2 จำนวนได้
(2) ทุก ๆ จำนวนเต็มคี่ $N \geq 9$ สามารถเขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้

ถ้าข้อคาดเดา (1) เป็นจริง แล้วข้อคาดเดา (2) สามารถพิสูจน์ให้เป็นจริงได้ไม่ยาก เพราะว่าถ้า n เป็นจำนวนเต็มคี่และ p เป็นจำนวนเฉพาะคี่ที่มีค่าน้อยกว่า n แล้ว $n-p$ จะเป็นจำนวนเต็มคู่ ถ้า $n-p$ เขียนอยู่ในรูปผลบวกของจำนวนเฉพาะคี่ 2 จำนวน คือ q และ r จะได้ว่า $n-p = q+r$ นั่นคือ $n = p+q+r$

การตรวจสอบข้อคาดเดา (1) อาจทำได้โดยใช้จำนวนที่มีค่าน้อย เช่น

$$\begin{aligned} 6 &= 3+3 & \qquad 14 &= 3+11 = 7+7 \\ 8 &= 3+5 & \qquad 16 &= 3+13 = 5+11 \\ 10 &= 3+7 & \qquad 18 &= 5+13 = 7+11 \\ 12 &= 5+7 & \qquad 20 &= 3+17 = 7+13 \end{aligned}$$

ต่อไปนี้เป็นจำนวนเต็มคู่ n ซึ่ง $6 \leq n \leq 100$ สามารถเขียนในรูปผลบวกของจำนวนเฉพาะสองจำนวนได้

$6 = 3 + 3$	$8 = 3 + 5$	$10 = 5 + 5$	$10 = 3 + 7$
$12 = 5 + 7$	$14 = 7 + 7$	$14 = 3 + 11$	$16 = 5 + 11$
$16 = 3 + 13$	$18 = 7 + 11$	$18 = 5 + 13$	$20 = 7 + 13$
$20 = 3 + 17$	$22 = 11 + 11$	$22 = 5 + 17$	$22 = 3 + 19$
$24 = 11 + 13$	$24 = 7 + 17$	$24 = 5 + 19$	$26 = 13 + 13$
$26 = 7 + 19$	$26 = 3 + 23$	$28 = 11 + 17$	$28 = 5 + 23$
$30 = 13 + 17$	$30 = 11 + 19$	$30 = 11 + 23$	$32 = 13 + 19$
$32 = 3 + 29$	$34 = 17 + 17$	$34 = 11 + 23$	$34 = 5 + 29$
$34 = 3 + 31$	$36 = 17 + 19$	$36 = 13 + 23$	$36 = 7 + 29$
$40 = 11 + 29$	$40 = 3 + 37$	$42 = 19 + 23$	$42 = 13 + 29$
$42 = 11 + 31$	$42 = 5 + 37$	$44 = 13 + 31$	$44 = 7 + 37$
$44 = 3 + 41$	$46 = 23 + 23$	$46 = 17 + 29$	$46 = 5 + 41$
$46 = 3 + 43$	$48 = 19 + 29$	$48 = 17 + 31$	$48 = 11 + 37$
$48 = 7 + 41$	$48 = 5 + 43$	$50 = 19 + 31$	$50 = 13 + 37$
$50 = 7 + 43$	$50 = 3 + 47$	$52 = 23 + 29$	$52 = 11 + 41$
$52 = 5 + 47$	$54 = 23 + 31$	$54 = 17 + 37$	$54 = 13 + 41$
$54 = 11 + 43$	$54 = 7 + 47$	$56 = 19 + 37$	$56 = 13 + 43$
$56 = 3 + 53$	$58 = 29 + 29$	$58 = 17 + 41$	$58 = 11 + 47$
$58 = 5 + 53$	$60 = 29 + 31$	$60 = 23 + 37$	$60 = 19 + 41$
$60 = 17 + 43$	$60 = 13 + 47$	$60 = 7 + 53$	$62 = 31 + 31$
$62 = 19 + 43$	$62 = 3 + 59$	$64 = 23 + 41$	$64 = 17 + 47$
$64 = 11 + 53$	$64 = 5 + 59$	$64 = 3 + 61$	$66 = 29 + 37$
$66 = 23 + 43$	$66 = 19 + 47$	$66 = 13 + 53$	$66 = 7 + 59$
$66 = 5 + 61$	$68 = 31 + 37$	$68 = 7 + 61$	$70 = 29 + 41$
$70 = 29 + 41$	$70 = 17 + 53$	$70 = 11 + 59$	$70 = 3 + 67$
$72 = 31 + 41$	$72 = 29 + 43$	$72 = 19 + 53$	$72 = 13 + 59$
$72 = 11 + 61$	$72 = 5 + 67$	$74 = 37 + 37$	$74 = 31 + 43$
$74 = 13 + 61$	$74 = 7 + 67$	$74 = 3 + 71$	$76 = 29 + 47$
$76 = 23 + 53$	$76 = 17 + 59$	$76 = 5 + 71$	$76 = 3 + 73$
$78 = 37 + 41$	$78 = 31 + 47$	$78 = 19 + 59$	$78 = 17 + 61$

$78 = 11 + 67$ $78 = 7 + 71$ $78 = 5 + 73$ $80 = 37 + 43$
$80 = 19 + 61$ $80 = 13 + 67$ $80 = 7 + 73$ $82 = 41 + 41$
$82 = 29 + 53$ $82 = 23 + 59$ $82 = 11 + 71$ $82 = 3 + 79$
$84 = 41 + 43$ $84 = 37 + 47$ $84 = 31 + 53$ $84 = 23 + 61$
$84 = 17 + 67$ $84 = 13 + 71$ $84 = 11 + 73$ $84 = 5 + 79$
$86 = 43 + 43$ $86 = 19 + 67$ $86 = 13 + 73$ $86 = 7 + 79$
$86 = 3 + 83$ $88 = 41 + 47$ $88 = 29 + 59$ $88 = 17 + 71$
$88 = 5 + 83$ $90 = 43 + 47$ $90 = 37 + 53$ $90 = 31 + 59$
$90 = 29 + 61$ $90 = 23 + 67$ $90 = 19 + 71$ $90 = 17 + 73$
$90 = 11 + 79$ $90 = 7 + 83$ $92 = 31 + 61$ $92 = 19 + 73$
$92 = 13 + 79$ $92 = 3 + 89$ $94 = 47 + 47$ $94 = 41 + 53$
$94 = 23 + 71$ $94 = 11 + 83$ $94 = 5 + 89$ $96 = 43 + 53$
$96 = 23 + 73$ $96 = 17 + 79$ $96 = 13 + 83$ $96 = 7 + 89$
$98 = 37 + 61$ $98 = 31 + 67$ $98 = 19 + 79$ $100 = 47 + 53$
$100 = 41 + 59$ $100 = 29 + 71$ $100 = 17 + 83$ $100 = 11 + 89$
$100 = 3 + 97$

ปิพปิง ได้ตรวจสอบข้อคาดเดานี้สำหรับจำนวนเต็มคู่จนถึง 100,000 และในปัจจุบันได้มีการตรวจสอบว่าข้อคาดเดานี้เป็นจริงสำหรับทุกจำนวนเต็มคู่ที่น้อยกว่า 10^{10} แต่การพิสูจน์ว่าข้อคาดเดานี้เป็นจริงสำหรับทุกจำนวนเต็มคู่ที่มากกว่า 4 ยังไม่มีใครทราบ

ในขณะที่ข้อคาดเดาของโกลด์บัคยังไม่ได้พิสูจน์นั้น ได้มีนักคณิตศาสตร์ชาวรัสเซีย ชื่อวิโนกราดอฟ (Vinogradov) ได้พยายามพิสูจน์ข้อคาดเดา (2) ในปี ค.ศ. 1937 และแสดงว่า "จำนวนคี่ทุกจำนวนที่มีค่ามากพอจะสามารถเขียนอยู่ในรูปของผลบวกของจำนวนเฉพาะคี่ 3 จำนวนได้" อย่างไรก็ตาม การพิสูจน์นี้เป็นแค่การพิสูจน์การมีอยู่ (existence proof) แต่ยังไม่มีใครบอกได้ว่าจำนวนที่มีค่ามากพอนั้นคือจำนวนใด จนกระทั่งในปี ค.ศ. 1988 มีผู้แสดงไว้ว่า จำนวนที่มีค่ามากพอคือ N ซึ่ง $N > k$ โดยที่ $k < 10^{400000}$

ข้อคาดเดาที่ 2

ให้ $n \in \mathbb{N}$ จะมีจำนวนเฉพาะ n จำนวนที่เรียงกันเป็นลำดับเลขคณิต

เออร์ดอส ได้ตั้งรางวัลสำหรับผู้ที่สามารถตอบข้อคาดเดาที่ 2 นี้ได้ไว้ถึง US $5000 อย่างไรก็ตามนักคณิตศาสตร์ชั้นนำของโลกมีความเชื่อว่าข้อคาดเดาที่ 2 นี้น่าจะเป็นจริงและมีผู้ที่สามารถหาจำนวนเฉพาะที่เรียงติดต่อเนื่องกันเป็นลำดับเลขคณิตได้ถึง 21 จำนวนแล้ว

$$142072321123 + 1419763024n \quad \cdots (0 \leq n \leq 20)$$

จากการสังเกตพบว่า $1^2 + 1 = 2,\ 2^2 + 1 = 5,\ 4^2 + 1 = 17,\ 6^2 + 1 = 37$ จากข้อสังเกตข้างต้นจึงเกิดข้อคาดเดาต่อไปนี้

ข้อคาดเดาที่ 3

มีจำนวนเฉพาะที่อยู่ในรูป $n^2 + 1$ อยู่ไม่จำกัดจำนวนหรือจำกัดจำนวน

ข้อคาดเดาที่ 4

จำนวนเฉพาะคู่แฝด (Twin primes) คือจำนวนเฉพาะ 2 จำนวนที่อยู่ในรูป $p, p+2$

เรามีข้อคาเดาว่าจะมีจำนวนเฉพาะคู่แฝดเป็นจำนวนจำกัดคู่หรือไม่จำกัดคู่ จำนวนเฉพาะคู่แฝดที่น้อยกว่า 51 จะมีทั้งหมด 6 คู่ คือ $(3,5),(5,7),(11,13),(17,19),(29,31)$ และ $(41,43)$

จากการใช้เครื่องคอมพิวเตอร์ พบว่ามีจำนวนเฉพาะคู่แฝดที่น้อยกว่า 30,000,000 อยู่ทั้งหมด 152,892 คู่ และจำนวนเฉพาะคู่แฝดที่อยู่ระหว่าง 999,999,990,000 และ 1,000,000,000,000 มี 15 คู่ และระหว่าง 1,000,000,000,000 และ 1,000,000,010,000 มี 20 คู่ คู่หนึ่งในจำนวนนี้ ได้แก่ 1,000,000,000,061 และ 1,000,000,000,063 ในปี ค.ศ. 1989 มีผู้ค้นพบจำนวนเฉพาะคู่แฝดคู่หนึ่งคือ $1706595 \cdot 2^{11235} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วย 3389 หลัก ต่อมาในปี ค.ศ. 2000 มีผู้ค้นพบจำนวนเฉพาะคู่แฝดคู่หนึ่งที่คิดว่าใหญ่ที่สุดคือ $665551035 \cdot 2^{50025} \pm 1$ โดยที่แต่ละจำนวนประกอบด้วย 24099 หลัก

3.6 จำนวนเฉพาะแฟร์มาต์

ในปี ค.ศ. 1640 แฟร์มาต์ได้ศึกษาจำนวนเต็มที่อยู่ในรูป $2^{2^n}+1$ ซึ่งมีรายละเอียดดังนี้

บทนิยาม 3.6.1 : จำนวนแฟร์มาต์

จำนวนแฟร์มาต์ (Fermat number) คือจำนวนเต็มที่อยู่ในรูป

$$F_n = 2^{2^n}+1, \quad n \geq 0$$

ถ้า F_n เป็นจำนวนเฉพาะ เราจะเรียกว่า F_n ว่า**จำนวนเฉพาะแฟร์มาต์** (Fermat prime)

แฟร์มาต์พบว่าจำนวนเต็ม $F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65537$ ต่างก็เป็นจำนวนเฉพาะ และเขายังตั้งข้อคาดเดาต่ออีกว่า $2^{2^1}+1,\ 2^{2^2}+1,\ 2^{2^3}+1,\ 2^{2^4}+1,\ldots$ เป็นจำนวนเฉพาะทุกจำนวน แต่ต่อมาในปี ค.ศ. 1732 ออยเลอร์ พบว่า $F_5 = 2^{2^5}+1 = 4{,}294{,}967{,}297 = 641 \cdot 6700417$ เป็นจำนวนประกอบ ซึ่งทำให้ข้อคาดเดาของแฟร์มาต์ไม่เป็นจริง

ในช่วงปี ค.ศ. 1878 ลูคัส (Edourd Lucas ค.ศ. 1842-1891) นักคณิตศาสตร์ชาวฝรั่งเศส ได้พิสูจน์ว่า F_6 เป็นจำนวนประกอบ เนื่องจาก $F_6 = 2^{2^6}+1 = 274177 \cdot 67280421310721$

จากการศึกษาค้นคว้าต่อมาพบว่า F_n เป็นจำนวนประกอบ สำหรับ $5 \leq n \leq 20$ และมีผู้พิสูจน์ได้ว่า F_{23472} เป็นจำนวนประกอบ อย่างไรก็ตาม ยังไม่มีผู้ใดพิสูจน์ได้ว่ามีจำนวนเฉพาะอยู่จำนวนอนันต์ ที่สามารถเขียนได้ในรูป $2^{2^n}+1$ หรือไม่ และยังไม่มีผู้ใดค้นพบจำนวนเฉพาะแฟร์มาต์ตัวอื่น ๆ อีกเลย

ดังนั้นอาจกล่าวได้ว่า จำนวนเฉพาะแฟร์มาต์ที่ค้นพบในปัจจุบัน ตัวที่ใหญ่ที่สุดคือ $F_4 = 65537$ และข้อคาดเดาที่ดีที่สุดคือ จำนวนแฟร์มาต์ $F_n > F_4$ เป็นจำนวนประกอบ ถ้าข้อคาดเดานี้เป็นจริง แสดงว่าจำนวนเฉพาะแฟร์มาต์มีได้จำกัดเพียง 5 จำนวนเท่านั้น และมีผู้พยายามที่จะค้นหาคุณลักษณะ ของ F_n ในกรณีที่ n มีค่าน้อย ๆ เช่น

$$F_7 = 2^{2^7}+1 = (59{,}649{,}589{,}127{,}497{,}217)(5{,}704{,}689{,}200{,}685{,}129{,}654{,}721)$$
$$F_8 = 2^{2^8}+1 = (1{,}238{,}926{,}361{,}552{,}897)M \text{ เมื่อ } M \text{ เป็นจำนวนเต็มบวกที่มี 62 หลัก}$$
$$F_{17} = 2^{2^{17}}+1 = (31{,}065{,}037{,}602{,}817)N \text{ เมื่อ } N \in \mathbb{N}$$

ตารางต่อไปนี้แสดงลักษณะการค้นพบจำนวนแฟร์มาต์ $F_n,\ \ 0 \leq n \leq 30$

n	ลักษณะของ F_n
$0, 1, 2, 3, 4$	เป็นจำนวนเฉพาะ
$5, 6, 7, 8, 9, 11$	แยกเป็นผลคูณของจำนวนเฉพาะได้
$10, 12, 13, 19, 30$	เราทราบตัวประกอบเพียง 2 หรือ 4 ตัวประกอบ
$15, 16, 17, 18, 21, 23, 25, 26, 27$	เราทราบเพียง 1 ตัวประกอบที่เป็นจำนวนเฉพาะ
$14, 20$	เป็นจำนวนประกอบแต่ไม่ทราบว่ามีตัวประกอบอะไรบ้าง
$22, 24, 28, 29$	ไม่ทราบลักษณะใด ๆ เลย

ตารางที่ 3.1 แสดงลักษณะของ F_n

ตัวอย่าง 3.6.1

ให้ F_n และ F_m เป็นจำนวนแฟร์มาต์ที่ $m > n$ จงแสดงว่า $(F_m, F_n) = 1$
(ข้อเสนอแนะ $x^k - 1 = (x+1)\left(x^{k-1} - x^{k-2} + \cdots + x - 1\right)$ เมื่อ k เป็นจำนวนเต็มคู่)

วิธีทำ ให้ $d = (F_m, F_n)$ และจะแสดงว่า $d = 1$

ให้ $x = 2^{2^n}$ และ $k = 2^{m-n}$

จะได้ว่า $\dfrac{F_m - 2}{F_n} = \dfrac{\left(2^{2^n}\right)^{2^{m-n}} - 1}{2^{2^n} - 1}$

ดังนั้น $\dfrac{F_m - 2}{F_n} = \dfrac{x^k - 1}{x+1} = x^{k-1} - x^{k-2} + \cdots + x - 1$

แสดงว่า $F_n \mid (F_m - 2)$ จาก $d \mid F_n$ จะได้ $d \mid (F_m - 2)$

และจาก $d \mid F_m$ และ $d \mid (F_m - 2)$ สรุปได้ว่า $d \mid 2$ แต่ d เป็นจำนวนเต็มคี่

ดังนั้น $d = 1$ เพราะฉะนั้น $(F_m, F_n) = 1$

3.7 จำนวนเฉพาะแมร์เซน

มาริน แมร์เซน (Marin Mersenne ค.ศ. 1588-1648) บาทหลวงชาวฝรั่งเศส เป็นนักคณิตศาสตร์คนหนึ่งที่มีความสนใจในการสร้างลำดับของจำนวนเต็มที่จะเป็นลำดับของจำนวนเฉพาะโดยเขาศึกษาลำดับของจำนวนเต็มที่อยู่ในรูป

$$M_n = 2^n - 1, \quad n \in \mathbb{N}$$

เราจึงตั้งชื่อเพื่อเป็นเกียรติแก่แมร์เซน โดยเรียกจำนวน $M_n = 2^n - 1$ ว่า**จำนวนแมร์เซน** (Mersenne number) และถ้า M_n เป็นจำนวนเฉพาะ เราจะเรียก M_n นี้ว่า**จำนวนเฉพาะแมร์เซน** (Mersenne prime)

จากการเขียน $n = ab$ เราพบวิธีการแยกตัวประกอบของ

$$M_n = 2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\right]$$

นี่คือการแสดงว่า ถ้า n เป็นจำนวนประกอบแล้ว $2^n - 1$ เป็นจำนวนประกอบ ซึ่งมีความหมายเหมือนกับทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.7.1

ถ้า M_n เป็นจำนวนเฉพาะแล้ว n เป็นจำนวนเฉพาะ

จากทฤษฎีบท 3.7.1 จะได้ว่าจำนวน M_p จะเป็นจำนวนเฉพาะแมร์เซนได้ ก็ต่อเมื่อ มีจำนวนเฉพาะ p ที่ทำให้ M_p เป็นจำนวนเฉพาะ เช่น $M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8191,$ $M_{17} = 131071$ และ $M_{19} = 524287$

แมร์เซนได้ตั้งข้อสังเกตว่า มีเพียง M_p ที่เป็นจำนวนเฉพาะเมื่อ $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ และ 257 เท่านั้น และเป็นจำนวนประกอบสำหรับจำนวนเฉพาะ p อื่น ๆ ที่น้อยกว่า 257 นักคณิตศาสตร์คนอื่น ๆ ในสมัยนั้นเชื่อว่าแมร์เซนไม่ได้ทดสอบความเป็นจำนวนเฉพาะของจำนวน เหล่านั้นทุกจำนวน ต่อมาในปี ค.ศ. 1772 ออยเลอร์ได้พิสูจน์ว่า M_{31} เป็นจำนวนเฉพาะ โดยทดสอบกับ ตัวหารที่เป็นจำนวนเฉพาะจนถึง 46339 แต่ M_{67}, M_{127} และ M_{257} เป็นจำนวนที่มีค่ามากเกินไปที่เขาจะตรวจสอบได้

จากการค้นคว้าต่อมาได้มีผู้พยายามตรวจสอบ M_p สำหรับจำนวนเฉพาะ p ซึ่งมีทั้งหมด 55 จำนวนที่น้อยกว่า 257 พบว่าข้อสังเกตของแมร์เซนผิดพลาดไป กล่าวคือ

$$M_{67} \text{ และ } M_{257} \text{ เป็นจำนวนประกอบ}$$
$$M_{61},\ M_{89} \text{ และ } M_{107} \text{ เป็นจำนวนเฉพาะ}$$

ในปี ค.ศ. 1876 ลูคัส ได้พิสูจน์ว่า M_{67} เป็นจำนวนประกอบแต่ก็ไม่สามารถหาตัวประกอบออกมาได้ ในเดือนตุลาคม ปี ค.ศ. 1903 ในการประชุม American Mathematical Society โคล (Frederick Nelson Cole ค.ศ. 1861-1927) นักคณิตศาสตร์ชาวเยอรมัน ได้เสนอผลงานในหัวข้อ "On the Factorization of Large Numbers" เมื่อเขาถูกเชิญให้ขึ้นไปนำเสนอ โคลเดินตรงไปที่กระดานดำโดยไม่กล่าวอะไร แล้วบรรจงเขียน $2^{67} - 1$ จากนั้นคำนวณออกมาทีละขั้นพร้อมทั้งผลคูณซึ่ง

$$2^{67} - 1 = (193707721)(761838257287)$$

โคลไม่ได้พูดและอธิบายอะไร ซึ่งทุกคนก็ไม่ได้สงสัยอะไรด้วย (ต่อมาโคลสารภาพกับเพื่อนของเขาว่า เขาใช้เวลาว่างตอนบ่ายวันอาทิตย์เป็นเวลา 20 ปี ในการหาตัวประกอบของ M_{67})

ในปี ค.ศ. 1932 เลห์เมอร์ (D.H. Lehmer) ได้แสดงว่า M_{257} ไม่เป็นจำนวนเฉพาะ ซึ่ง

$$M_{257} = (535006138814359)(1155685395246619182673033)N$$
$$N = 3745505985018109365817766300963131813 93$$

จากการศึกษาจำนวนแมร์เซนพบว่า เมื่อนำจำนวนเฉพาะแมร์เซน 4 ตัวแรก คือ $3, 7, 31$ และ 127 ไปแทน n ในสูตร $2^n - 1$ จะได้จำนวนแมร์เซนตัวใหม่ขึ้นมา จากการแทนค่านี้ นักคณิตศาสตร์ได้คาดหวังว่าวิธีนี้อาจทำให้ได้ว่ามีจำนวนเฉพาะแมร์เซนอยู่จำนวนอนันต์ จึงได้มีข้อคาดเดาว่า ถ้า M_p เป็นจำนวนเฉพาะแล้ว M_{M_p} เป็นจำนวนเฉพาะด้วยแต่ความคาดหวังก็ดับลง ในปี ค.ศ. 1953 เมื่อพบว่า

$$M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$$

เป็นจำนวนประกอบ (มีเลขโดด 2466 หลัก)

ในปี ค.ศ. 2001 พบว่า $M_{13466917}$ เป็นจำนวนเฉพาะแมร์เซนที่มีค่ามากที่สุด ปัญหาที่น่าสนใจในขณะนี้คือจำนวนเฉพาะ $M_p = 2^p - 1$ มีอยู่จำนวนอนันต์หรือไม่ ซึ่งปัญหานี้ยังเป็นปัญหาที่มีชื่อเสียงระดับโลกที่ยังไม่มีใครตอบได้

ตารางแสดงจำนวนเฉพาะแมร์เซนและจำนวนสมบูรณ์ที่เคยค้นพบ

ให้ p เป็นจำนวนเฉพาะที่ทำให้ $M_p = 2^p - 1$ เป็นจำนวนเฉพาะ เราจะเรียกจำนวน P_p ซึ่ง

$$P_p = 2^{p-1}\left(2^p - 1\right)$$

ว่าเป็น**จำนวนสมบูรณ์** (perfect number)

ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ		ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ
1	2	–	–		21	9689	1963	Gillies
2	3	–	–		22	9941	1963	Gillies
3	5	–	–		23	11213	1963	Gillies
4	7	–	–		24	19937	1971	Tuckerman
5	13	1456	Anonymous		25	21701	1978	Noll & Nickel
6	17	1588	Cataldi		26	23209	1979	Noll
7	19	1588	Cataldi		27	44497	1979	Nelson & Slowinski
8	31	1772	Euler		28	86243	1982	Slowinski
9	61	1883	Pervushin		29	110503	1988	Colquilt & Welsh
10	89	1911	Powers		30	132049	1983	Slowinski
11	107	1914	Powers		31	216091	1985	Slowinski
12	127	1876	Lucas		32	756839	1992	Slowinski & Gage
13	521	1952	Robinson		33	859433	1994	Slowinski & Gage
14	607	1952	Robinson		34	1257787	1996	Slowinski & Gage
15	1279	1952	Robinson		35	1398269	1996	Armenguad,et.al.
16	2203	1952	Robinson		36	2976221	1997	Spence,et.al.
17	2281	1952	Robinson		37	3021377	1998	Claekson,et.al.
18	3217	1957	Riesel		38	6972593	1999	Hajaratwala,et.al.
19	4253	1961	Herwitz		39	13466917	2001	Kurowski,et,al.
20	4423	1961	Herwitz		40	20996011	2003	Shafer,et.al.

ตารางที่ 3.2 ตารางแสดงจำนวนเฉพาะแมร์เซนที่เคยค้นพบ
ที่มา : ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552 : 86)

ทฤษฎีบท 3.7.2

ถ้า p และ $q = 2p + 1$ เป็นจำนวนเฉพาะ แล้ว $q \mid M_p$ หรือ $q \mid (M_p + 2)$ อย่างใดอย่างหนึ่งเพียงอย่างเดียวเท่านั้น

ทฤษฎีบท 3.7.3

ถ้า p เป็นจำนวนเฉพาะคี่ แล้วตัวหารของ M_p จะต้องเขียนอยู่ในรูป $2kp + 1$

ตัวอย่าง 3.7.1

(1) พิจารณา $M_{17} = 2^{17} - 1 = 131071$ พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{17} จะต้องเขียนอยู่ในรูป $2k(17) + 1 = 34k + 1$

(2) พิจารณา $M_{23} = 2^{23} - 1$ พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{23} จะต้องเขียนอยู่ในรูป $2k(23) + 1 = 46k + 1$

ตัวอย่าง 3.7.2

จงแสดงว่า จำนวนเฉพาะแมร์เซน M_{13} เป็นจำนวนเฉพาะ

วิธีทำ เนื่องจาก $M_{13} = 2^{13} - 1 = 8191$ และ $\sqrt{8191} \leq 91$

ดังนั้น ตัวหารของ M_{13} ที่เขียนอยู่ในรูป $2kp + 1 = 2k(13) + 1 = 26k + 1$

ซึ่งมีค่าน้อยกว่า 91 คือ 53 และ 79 ซึ่งเราพบว่า $53 \nmid 8191$ และ $79 \nmid 8191$

เพราะฉะนั้น M_{13} เป็นจำนวนเฉพาะ

สรุปท้ายบท

สิ่งสำคัญของบทที่ 3 คือมุ่งเน้นศึกษาสมบัติของจำนวนเฉพาะ โดยเน้นให้นักศึกษาเข้าใจนิยามและสมบัติของจำนวนเฉพาะ ตลอดจนสามารถวิเคราะห์จำนวนที่กำหนดให้ว่าเป็นจำนวนเฉพาะหรือจำนวนประกอบ และได้พูดถึงทฤษฎีหลักมูลของเลขคณิตซึ่งเป็นทฤษฎีที่สำคัญมากเป็นการพูดถึงความสัมพันธ์ระหว่างจำนวนเต็มและจำนวนเฉพาะ นอกจากนี้แล้วก็มีทฤษฎีที่ช่วยในการตรวจสอบว่าจำนวนที่เรากำลังพิจารณาอยู่นั้นเป็นจำนวนเฉพาะหรือไม่ ซึ่งทำให้เราตรวจสอบจำนวนที่มีค่ามาก ๆ ว่าเป็นจำนวนเฉพาะหรือไม่ได้ง่ายขึ้น ตอนสุดท้ายของบทนี้ได้พูดถึงทฤษฎีบทที่สำคัญของจำนวนเฉพาะซึ่งทำให้นักศึกษาสามารถนำความรู้นี้ไปใช้ในการเรียนบทต่อ ๆ ไปและในระดับที่สูงขึ้น

แบบฝึกหัดท้ายบทที่ 3

1. จงหาจำนวนเฉพาะทั้งหมดหารที่ 100! ลงตัว
2. จงตรวจสอบว่ามีจำนวนเฉพาะที่อยู่ระหว่าง 701 และ 1009 หรือไม่
3. ถ้า $p \geq q \geq 5$ และ p, q เป็นจำนวนเฉพาะทั้งคู่ จงแสดงว่า $24 \mid (p^2 - q^2)$
4. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะที่ $p \geq 5$ แล้ว $p^2 + 2$ เป็นจำนวนประกอบ
5. ให้ p เป็นจำนวนเฉพาะและ $p \mid a^n$ จงแสดงว่า $p^n \mid a^n$
6. จงตรวจจว่าจำนวนเต็มที่อยู่ในรูป $8^n + 1, n \geq 1$ เป็นจำนวนประกอบเมื่อใด
   (ข้อเสนอแนะ $(2^n + 1) \mid (2^{3n} + 1)$)
7. ให้ $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$ โดยที่ $n \geq 2$ จงพิสูจน์ว่า ถ้า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่แล้ว $[a_1, a_2, a_3, \ldots, a_n] = a_1 a_2 a_3 \cdots a_n$
8. จงหา $(308, 1176)$ และ $[308, 1176]$
9. จงตรวจสอบว่ามีจำนวนเฉพาะที่เขียนในรูป $6k + 3$ อยู่เป็นจำนวนอนันต์หรือไม่
10. จงหาจำนวนตัวหารทั้งหมดของ 846876
11. กำหนดให้ a, b และ c เป็นจำนวนเต็มบวก จงพิสูจน์ว่า

    (11.1) $([a, b], c) = [(a, b), (a, c)]$

    (11.2) $[(a, b), c] = ([a, b], [a, c])$

    (ข้อเสนอแนะ ใช้ $\min\{\max\{x, y\}, z\} = \max\{\min\{x, z\}, \min\{y, z\}\}$)
12. กำหนดให้ $a_1, a_2, \ldots, a_n$ และ b เป็นจำนวนเต็มบวก จงพิสูจน์ว่า

    (12.1) $([a_1, a_2, \ldots, a_n], b) = [(a_1, b), (a_2, b), \ldots, (a_n, b)]$

    (12.2) $[(a_1, a_2, \ldots, a_n), b] = ([a_1, b], [a_2, b], \ldots, [a_n, b])$
13. จงหา

    (13.1) จำนวนเฉพาะที่สามารถเขียนได้ในรูป $4k + 3, k \geq 0$ มา 20 จำนวน

    (13.2) จำนวนเฉพาะที่สามารถเขียนได้ในรูป $6k + 5, k \geq 0$ มา 20 จำนวน

    (13.3) จำนวนเฉพาะที่สามารถเขียนได้ในรูป $k^2 + k + 41, k \geq 0$ มา 20 จำนวน

    (13.4) จำนวนเฉพาะที่สามารถเขียนได้ในรูป $k^2 - 79k + 160, k \geq 0$ มา 20 จำนวน
14. เราสามารถหาจำนวนเฉพาะที่เขียนอยู่ในรูป $k^2 + k + 41$ ให้ติดต่อกัน 50 จำนวนได้หรือไม่
15. เราสามารถหาจำนวนเฉพาะที่เขียนอยู่ในรูป $k^2 + k + 17$ ให้ติดต่อกัน 100 จำนวนได้หรือไม่

16. จงตรวจสอบว่า $2^{19}-1$ เป็นจำนวนเฉพาะหรือจำนวนประกอบ

17. จงหาจำนวนเฉพาะ p ซึ่ง $p<100$ และ $p+2$ เป็นจำนวนเฉพาะ

18. จงเขียนจำนวนเต็มคู่ n ซึ่ง $10 \leq n \leq 100$ ในรูปผลบวกของจำนวนเฉพาะ 2 จำนวน

19. มีจำนวนเต็ม n ซึ่ง $6<n<20$ จำนวนใดบ้างที่ทำให้ n^2+1 เป็นจำนวนเฉพาะ

20. จงหาจำนวนเฉพาะ 2 จำนวนที่มากกว่า 11 ซึ่งสามารถเขียนได้ในรูป 2^n-1

21. จงหาจำนวนเต็มที่น้อยที่สุดที่มากกว่า 17 ซึ่งสามารถเขียนได้ในรูป 2^n+1

22. จงแสดงว่า จำนวนเฉพาะที่เขียนในรูป $8n+5$ มีจำนวนอนันต์

23. สำหรับจำนวนเต็มบวก $n>1$ จงแสดงว่า ทุกจำนวนเฉพาะที่หาร $n!+1$ ลงตัวจะเป็นจำนวนเต็มคี่ที่มีค่ามากกว่า n

24. จงแสดงว่า ถ้า $n \in \mathbb{N}$ ซึ่ง $n>2$ แล้วจะมีจำนวนเฉพาะ p ที่สอดคล้องกับ $n<p<n!$
(ข้อเสนอแนะ ถ้า $n!-1$ ไม่เป็นจำนวนเฉพาะ แล้วจะมีจำนวนเฉพาะ p ซึ่งถ้า $p \leq n$ แล้ว $p \mid n!$ ซึ่งจะได้ข้อขัดแย้ง)

25. ให้ p_n เป็นจำนวนเฉพาะตัวที่ n จงแสดงว่า $p_n>2n-1$ สำหรับ $n \geq 5$

26. ให้ $p_1, p_2, p_3, \ldots, p_n$ เป็นลำดับของจำนวนเฉพาะ จงตรวจสอบว่ามีจำนวนเต็มที่เขียนในรูป $p^* = p_1p_2p_3\cdots p_n+1$ เป็นกำลังสองสมบูรณ์หรือไม่
(ข้อเสนอแนะ p เขียนอยู่ในรูป $4k+3$ สำหรับ $n>1$)

27. จงแสดงว่าถ้า $n \in \mathbb{N}$ ซึ่ง $n \geq 2$ แล้วจะมีจำนวนเฉพาะ p ซึ่ง $p \leq n < 2p$

28. จงพิสูจน์ว่าจำนวนเต็มบวก n เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $n \mid [(n-1)!+1]$

29. จงแสดงว่าจำนวนเต็ม 1884,1960,1988 สามารถเขียนในรูปผลบวกของจำนวนเฉพาะ 2 จำนวนได้

30. จงแสดงว่าจำนวนเต็ม 1745,2215,2785 สามารถเขียนในรูปผลบวกของจำนวนเฉพาะ 3 จำนวนได้

31. จงยกตัวอย่างการเขียนจำนวนเฉพาะเรียงกัน 3 จำนวน และเป็นลำดับเลขคณิตด้วย มา 2 ชุด

32. สำหรับ $n>0$ จงพิสูจน์ว่า มีจำนวนประกอบที่เขียนอยู่ในรูป $2^{2n}+3$ อยู่จำนวนอนันต์

33. จงแสดงว่า จำนวนเต็มที่เขียนอยู่ในรูป $2^{2^n}+5$ เป็นจำนวนประกอบ

34. สำหรับ $n \geq 1$ จงแสดงว่า $(F_n, n)=1$

35. จงแสดงว่า M_{19} เป็นจำนวนเฉพาะ

36. จงแสดงว่า M_9, M_{14}, M_{15} และ M_{20} เป็นจำนวนประกอบ

37. จงตรวจสอบว่า M_{M_5} เป็นจำนวนเฉพาะหรือไม่

เอกสารอ้างอิง

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

ดำรงค์ ทิพย์โยธา. (2556). **คณิตศาสตร์ปรนัยเล่มที่ 37 : โลกทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

นงนุช สุขวารี และคณะ. (2547). **คณิตศาสตร์พื้นฐานสำหรับคอมพิวเตอร์**. กรุงเทพฯ : มูลนิธิ สอวน.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

นฤมล ศรชัยยืน. (2540). **ทฤษฎีจำนวน**. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่.

นิตยา ตรีนันทวัน. (2544). **ทฤษฎีจำนวน 1 (พิมพ์ครั้งที่ 6)**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยรามคำแหง

สมจิต โชติชัยสถิตย์. (2540). **ทฤษฎีจำนวน 2**. ขอนแก่น : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

David M. Burton. (2007). **Elementary number theory (5 ed.)**. New York : The McGraw-HillCompanies, Inc.

แผนบริหารการสอนประจำบทที่ 4

เนื้อหาประจำบท

1. นิยามและสมบัติของสมภาค
2. สมการสมภาค
3. สมภาคเชิงเส้น
4. ทฤษฎีบทเศษเหลือของจีน
5. ทฤษฎีบทของแฟร์มาต์และออยเลอร์

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและสมบัติพื้นฐานของสมภาคแก้โจทย์ปัญหาที่กำหนดให้ได้
2. นำความรู้ที่ได้ไปประยุกต์ใช้แก้ปัญหาในชีวิตประจำวันได้
3. สามารถวิเคราะห์สมภาคเชิงเส้นที่กำหนดให้ว่ามีผลเฉลยหรือไม่และถ้ามีผลเฉลยสามารถหาผลเฉลยทั้งหมดของสมภาคเชิงเส้นได้
4. สามารถใช้ทฤษฎีบทเศษเหลือของจีนแก้โจทย์ปัญหาที่กำหนดให้ได้
5. สามารถหาระบบส่วนตกค้างบริบูรณ์และระบบส่วนตกค้างลดทอนจากโจทย์ที่กำหนดให้ได้
6. เข้าใจทฤษฎีบทของออยเลอร์ ทฤษฎีบทของแฟร์มาต์ และสามารถนำความรู้มาพิสูจน์แบบฝึกหัดที่กำหนดให้ได้
7. สามารถนำความรู้ที่ได้เป็นพื้นฐานในการเรียนคณิตศาสตร์ชั้นสูงต่อไป

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    - 1.1 นิยามและสมบัติของสมภาค
    - 1.2 สมการสมภาค
    - 1.3 สมภาคเชิงเส้น
    - 1.4 ทฤษฎีบทเศษเหลือของจีน
    - 1.5 ทฤษฎีบทของแฟร์มาต์และออยเลอร์
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    - 2.1 ทำแบบฝึกหัดที่กำหนดให้
    - 2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    - 2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 4
สมภาค

ในการตรวจสอบจำนวนเต็มบวกที่ให้มาว่าจะหารด้วย 2 ลงตัวหรือไม่ เราอาจดูเฉพาะค่าประจำหลักหน่วยเท่านั้นก็สามารถสรุปได้ ในการตรวจสอบว่าจำนวนเต็มบวกที่ให้มาว่าจะหารด้วย 5 ลงตัวหรือไม่ เราอาจดูที่หลักหน่วยของจำนวนนั้นเท่านั้น เช่นกัน กล่าวคือ ถ้า $5 \mid n, n = a_k a_{k-1} \cdots a_2 a_1 a_0$ เป็นการเขียน แทน n ในระบบฐาน 10 จะได้ว่า $2 \mid n$ ก็ต่อเมื่อ $2 \mid a_0$ และ $5 \mid n$ ก็ต่อเมื่อ $5 \mid a_0$

จากแนวคิดที่กล่าวมาข้างต้นคือส่วนหนึ่งของ **สมภาค** (congruence) และแนวคิดที่เรียกว่าสมภาคนี้ได้ปรากฏขึ้นอย่างเป็นระบบ และได้แสดงให้เห็นว่าเป็นเครื่องมือที่สำคัญในการศึกษาทฤษฎีจำนวน ในปี ค.ศ. 1801 โดย คาร์ล ฟรีดริค เกาส์ (Carl Friedrich Gauss ค.ศ. 1777-1855) นักคณิตศาสตร์ชาวเยอรมัน ผู้ซึ่งได้รับการยกย่องว่าเป็นนักคณิตศาสตร์ที่ยอดเยี่ยมตลอดกาล เกาส์ได้กำหนดบทนิยามของสมภาค ซึ่งปรากฏในหนังสือของเขาเอง ชื่อ Disquisitiones Arthmeticae ในขณะที่เขามีอายุเพียง 24 ปี และผลงานชิ้นนี้ของเกาส์ได้นำไปสู่พัฒนาการทางด้านทฤษฎีจำนวนอย่างมาก

มีเรื่องเล่าว่าเกาส์ได้ส่งผลงานชิ้นนี้ไปยัง French Academy ในปี ค.ศ. 1800 เพื่อขอเผยแพร่ผลงาน แต่ถูกปฏิเสธจากผู้อ่านผลงานในขณะนั้น โดยผู้อ่านผลงานให้เหตุผลว่าผลงานชิ้นนี้ไม่ได้คุณภาพ อย่างไรก็ตามเมื่อมีผู้พยายามตรวจสอบเพื่อหาข้อยุติตามเรื่องที่เล่านี้ ผลปรากฏว่าในปี ค.ศ. 1935 ทาง French Academy รายงานว่าไม่มีประวัติการส่งผลงานของเกาส์ปรากฏอยู่ในฐานข้อมูล

เลโอพอลด์ โครเนคเคอร์ (Leopold Kronecker ค.ศ. 1823-1891) นักคณิตศาสตร์ชาวเยอรมัน ได้กล่าวสดุดีเกาส์ว่า "**น่าประหลาดใจจริง ๆ ที่คนเพียงคนเดียวและอายุก็ยังน้อยสามารถที่จะนำแสงสว่างและผลงานอันล้ำค่ามาตีแผ่และเหนือสิ่งอื่นใด การนำเสนอผลงานใหม่นี้ทำได้อย่างดีและรวบรวมได้อย่างเหมาะสม**" ผลงานของเกาส์ยังมีอีกมากมายทั้งในสาขาคณิตศาสตร์บริสุทธิ์และคณิตศาสตร์ประยุกต์เกาส์ได้รับปริญญาเอกเมื่อเขามีอายุ 22 ปี โดยการเขียนวิทยานิพนธ์ที่แสดงการพิสูจน์ ทฤษฎีบทพื้นฐานทางพีชคณิต (The Fundamental Theorem of Algebra)

เนื่องจากเกาส์ได้สร้างผลงานไว้มากมาย รวมทั้งผลงานทางด้านวิทยาศาสตร์ประกอบกับในช่วงคริสต์ศตวรรษที่ 19 มีนักคณิตศาสตร์และนักวิทยาศาสตร์ที่มีชื่อเสียงเกิดขึ้นมากมายในยุโรป เกาส์ได้รับการเสนอชื่อให้เป็นนักคณิตศาสตร์ที่ยอดเยี่ยมที่สุด และเขาได้ยกย่องว่าเป็น Princeps Mathematicorum (prince of Mathematicians) ซึ่งการยกย่องนี้ถือได้ว่าเป็นผู้ที่มีเกียรติเทียบได้กับ อาร์คิมีดีส (Archimedes ประมาณ 287-212 ปีก่อนคริสต์ศักราช) และ เซอร์ ไอแซก นิวตัน (Sir Isaac Newton ค.ศ. 1643-1727) คำกล่าวของเกาส์ที่แสดงให้เห็นถึงความสำคัญของคณิตศาสตร์และทฤษฎีจำนวน ซึ่งพวกเราชาวคณิตศาสตร์และวิทยาศาสตร์มักจะได้ยินอยู่เสมอก็คือ

"Mathematics is the Queen of Science,
and the theory of number is the Qucen of Mathematics."

4.1 นิยามและสมบัติของสมภาค

ในบทแรกของ Disquisitiones Arithmetiace เกาส์ได้ให้บทนิยามและสมบัติเบื้องต้นของสมภาค (conqruence) และเขาได้ใช้สัญลักษณ์ "$\equiv$" แทนสมภาคของจำนวนเต็ม 2 จำนวน เนื่องจากสมบัติของสมภาคและสมบัติของการเท่ากันของจำนวนเต็มมีข้อคล้ายคลึงกันอย่างน่าอัศจรรย์ (จิราภา ลิ้มบุพศิริพร. 2555 : 89, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 108, Rosen. K.H. 2005 : 142)

บทนิยาม 4.1.1

ให้ n เป็นจำนวนเต็มบวก สำหรับจำนวนเต็ม a และ b เราจะกล่าวว่า **a สมภาคกับ b มอดุโล n** เขียนแทนด้วย $a \equiv b \pmod{n}$ ก็ต่อเมื่อ n หาร $a-b$ ลงตัว และถ้า n หาร $a-b$ ไม่ลงตัว เราจะกล่าวว่า **a ไม่สมภาคกับ b มอดุโล n** ซึ่งเขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{n}$ ในที่นี้เรียกจำนวนเต็มบวก n ว่า **มอดุลัส** (modulus)

จากบทนิยามเราพบว่า สำหรับจำนวนเต็ม a, b และจำนวนเต็มบวก n จะได้ว่า

(1) $a \equiv b \pmod{n}$ ก็ต่อเมื่อ $n \mid (a-b)$

(2) $a \not\equiv b \pmod{n}$ ก็ต่อเมื่อ $n \nmid (a-b)$

(3) $a \equiv b \pmod{1}$ และ $a \equiv a \pmod{n}$

ตัวอย่าง 4.1.1

(1) $10 \equiv 2 \pmod{4}$ เพราะว่า $4 \mid (10-2)$

(2) $7 \not\equiv 3 \pmod{3}$ เพราะว่า $3 \nmid (7-3)$

(3) $-31 \equiv 11 \pmod{7}$ เพระว่า $7 \mid (-31-11)$

(4) $37 \equiv 112 \pmod{25}$ เพราะว่า $25 \mid (37-112)$

(5) $2^{10} \equiv 1 \pmod{3}$ เพราะว่า $3 \mid (2^{10}-1)$

(6) $-15 \not\equiv -63 \pmod{7}$ เพราะว่า $7 \nmid (-15+63)$

(7) $2 \equiv 16 \pmod{7}$ เพราะ $7 \mid (2-16) = -14$

(8) $7 \not\equiv 1 \pmod{7}$ เพราะ 7 หาร $(7-1) = 6$ ไม่ลงตัว

(9) $-10 \not\equiv 0 \pmod{4}$ เพราะ 4 หาร $(-10-0) = -10$ ไม่ลงตัว

(10) $11 \equiv -5 \pmod{4}$ เพราะ $4 \mid (11-(-5)) = 16$

(11) $-3 \equiv 19 \pmod{11}$ เพราะ $11 \mid (-3-19) = -22$

(12) $-89 \equiv -89 \pmod{31}$ เพราะ $31 \mid (-89+89) = 0$

จากบทนิยามของสมภาค ทำให้ได้ข้อสรุปอีกรูปแบบหนึ่งคือ (สมวงษ์ แปลงประสพโชค. 2545 : 46-47, ปิยวดี วงษ์ใหญ่. 2530 : 70-71)

ทฤษฎีบท 4.1.1

สำหรับจำนวนเต็ม a และ b ใด ๆ $a \equiv b \pmod{n}$ ก็ต่อเมื่อ a และ b มีเศษที่เหลือจากการหารด้วย n เท่ากัน

การพิสูจน์ ($\Rightarrow$) ให้ $a,\ \mathrm{b}, \in \mathbb{Z}$ และ $n \in \mathbb{N}$ โดยขั้นตอนวิธีการหาร จะมี $k_1, k_2, r_1, r_2 \in \mathbb{Z}$
ที่ทำให้ $a = nk_1 + r_1,\ 0 \le r_1 < n$ และ $b = nk_2 + r_2,\ 0 \le r_2 < n \quad \cdots (*)$
ดังนั้น $a - b = n(k_1 - k_2) + (r_1 - r_2)$ โดยที่ $0 \le |r_1 - r_2| < n$
จาก $n \mid (a-b)$ และ $n \mid n(k_1-k_2)$ จะได้ว่า $n \mid (r_1 - r_2)$
จาก $0 < |r_1 - r_2| < n$ จะได้ว่า $n \nmid (r_1 - r_2)$ ดังนั้น $|r_1 - r_2| = 0$
ดังนั้น $r_1 = r_2$
($\Leftarrow$) จาก $(*)$ สมมติว่า $r_1 = r_2$ จะได้ว่า $a - b = (nk_1 - r_1) - (nk_2 + r_2)$
ดังนั้น $a - b = n(k_1 - k_2)$ นั่นคือ $a \equiv b \pmod{n}$ □

ตัวอย่าง 4.1.2

จงหาเศษที่เกิดจากการหาร 3^{10} ด้วย 8

วิธีทำ เนื่องจาก $3^{10} \equiv 1 \pmod 8$ ดังนั้น 3^{10} หารด้วย 8 แล้วเหลือเศษ 1

ตัวอย่าง 4.1.3

ถ้า $2^{30} \equiv 13 \pmod{17}$ แล้ว จงหาเศษที่เกิดจากการหาร 2^{30} ด้วย 17

วิธีทำ เนื่องจาก $2^{30} \equiv 13 \pmod{17}$ ดังนั้น 2^{30} หารด้วย 17 แล้วเหลือเศษ 13

สมบัติของสมภาค

ทฤษฎีบทต่อไปนี้จะกล่าวเกี่ยวกับข้อคล้ายคลึงกันระหว่าง**การเท่ากัน**และ**การสมภาคกัน**ของจำนวนเต็ม (สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ. 2556 : 32-33, ดำรงค์ ทิพย์โยธา. 2556 : 199-200, Kenneth Ireland and Michael Rosen. 1990 : 29-30)

ทฤษฎีบท 4.1.2

ให้ $n \in \mathbb{N}$ และ $a, b, c, d, x, y \in \mathbb{Z}$ จะได้ว่า

1. ถ้า $a \equiv b \pmod n$ แล้ว $b \equiv a \pmod n$
2. ถ้า $a \equiv b \pmod n$ และ $b \equiv c \pmod n$ แล้ว $a \equiv c \pmod n$
3. ถ้า $a \equiv b \pmod n$ และ $c \equiv d \pmod n$ แล้ว $a + c \equiv b + d \pmod n$ และ $ac \equiv bd \pmod n$
4. ถ้า $a \equiv b \pmod n$ แล้ว $a + c \equiv b + c \pmod n$ และ $ac \equiv bc \pmod n$
5. ถ้า $a \equiv b \pmod n$ แล้ว $a^k \equiv b^k \pmod n$ สำหรับจำนวนเต็มบวก k
6. ถ้า $a \equiv b \pmod n$ และ $c \equiv d \pmod n$ แล้ว $ax + cy \equiv bx + dy \pmod n$
7. ถ้า $a \equiv b \pmod n$ และ $d \mid n$ โดยที่ $d > 0$ แล้ว $a \equiv b \pmod d$

การพิสูจน์ ให้ $n \in \mathbb{N}$ และ $a, b, c, d, x, y \in \mathbb{Z}$

1. ให้ $a \equiv b \pmod n$ จะได้ว่า $n \mid (a - b)$
   แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $a - b = nk$
   ดังนั้น $b - a = n(-k)$ ทำให้ได้ว่า $n \mid (b - a)$
   นั่นคือ $b \equiv a \pmod n$
2. ให้ $a \equiv b \pmod n$ และ $b \equiv c \pmod n$
   จะได้ว่า $n \mid (a - b)$ และ $n \mid (b - c)$
   แสดงว่า $n \mid [(a - b) + (b - c)]$ ทำให้ได้ว่า $n \mid (a - c)$
   ดังนั้น $a \equiv c \pmod n$
3. ให้ $a \equiv b \pmod n$ และ $c \equiv d \pmod n$
   จะได้ว่า $n \mid (a - b)$ และ $n \mid (c - d)$
   แสดงว่า $n \mid [(a - b) + (c - d)]$ ดังนั้น $n \mid [(a + c) - (b + d)]$
   จาก $n \mid (a - b)$ และ $n \mid (c - d)$
   จะมี $k_1, k_2 \in \mathbb{Z}$ ซึ่ง $a - b = nk_1$ และ $c - d = nk_2$
   และ $ac = (nk_1 + b)(nk_2 + d) = n(nk_1k_2 + k_1d + bk_2) + bd$

ทำให้ได้ว่า $n \mid ac - bd$
นั่นคือ $a + c \equiv b + d \pmod{n}$ และ $ac \equiv bd \pmod{n}$

4. ให้ $a \equiv b \pmod{n}$ เพราะว่า $c \equiv c \pmod{n}$ จากข้อ 3. ข้างต้น
จะได้ว่า $a + c \equiv b + c \pmod{n}$ และ $ac \equiv bc \pmod{n}$

5. ให้ $a \equiv b \pmod{n}$ และ $k \in \mathbb{N}$ โดยหลักอุปนัยเชิงคณิตศาสตร์
$k = 1$ เป็นจริงโดยการกำหนดให้
สมมติว่า $a^k \equiv b^k \pmod{n}$ เป็นจริง
โดยข้อ 3. จะได้ว่า $a \cdot a^k \equiv b \cdot b^k \pmod{n}$
ดังนั้น $a^{k+1} \equiv b^{k+1} \pmod{n}$
เพราะฉะนั้น $a^k \equiv b^k \pmod{n}$ เป็นจริงสำหรับทุกจำนวนเต็มบวก k

6. ให้ $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ โดยข้อ 4. ข้างต้น
จะได้ว่า $ax \equiv bx \pmod{n}$ และ $cy \equiv dy \pmod{n}$
โดยข้อ 3. จะได้ว่า $ax + cy \equiv bx + dy \pmod{n}$

7. ให้ $a \equiv b \pmod{n}$ และ $d \mid n$ โดยที่ $d > 0$
จะได้ว่า $n \mid (a - b)$ ดังนั้น $d \mid (a - b)$
นั่นคือ $a \equiv b \pmod{d}$ □

หมายเหตุ จากความจริงที่ว่า
(i) $a \equiv a \pmod{n}$
(ii) ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
(iii) ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$
สรุปได้ว่าความสัมพันธ์สมภาค มอดุโล n เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ (equivalence relation on $\mathbb{Z}$)

ตัวอย่าง 4.1.4

จงแสดงว่า 41 หาร $2^{20} - 1$ ลงตัว

การพิสูจน์ เนื่องจาก $2^5 \equiv -9 \pmod{41}$
จะได้ว่า $(2^5)^4 \equiv (-9)^4 \pmod{41}$
นั่นคือ $2^{20} \equiv (81)(81) \pmod{41}$
แต่ $81 \equiv -1 \pmod{41}$
โดยทฤษฎีบท 4.1.2 ข้อ 5. จะได้ว่า $(81)(81) \equiv (-1)(-1) \pmod{41}$
จาก $2^{20} \equiv (81)(81) \pmod{41}$ และ $(81)(81) \equiv 1 \pmod{41}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ว่า $2^{20} \equiv 1 \pmod{41}$
ดังนั้น $41 \mid (2^{20} - 1)$ □

ตัวอย่าง 4.1.5

จงหาเศษที่เกิดจากการหาร 7^{10} ด้วย 51

วิธีทำ เราต้องการหาเศษ x ซึ่ง $0 \leq x < 51$ ที่ทำให้ $7^{10} \equiv x \pmod{51}$
เนื่องจาก $49 \equiv -2 \pmod{51}$ จะได้ว่า $(49)^5 \equiv (-2)^5 \pmod{51}$
เพราะฉะนั้น $7^{10} \equiv (7^2)^5 \equiv (49)^5 \equiv (-2)^5 \equiv -32 \pmod{51}$

เนื่องจาก $-32 \equiv 19 \pmod{51}$
ฉะนั้นจาก $7^{10} \equiv -32 \pmod{51}$ และ $-32 \equiv 19 \pmod{51}$
จะได้ว่า $7^{10} \equiv 19 \pmod{51}$
ดังนั้น เศษที่เกิดจากการหาร 7^{10} ด้วย 51 คือ 19

ตัวอย่าง 4.1.6

จงหาเศษเหลือจากการหาร 17^{55} ด้วย 12

วิธีทำ เพราะว่า $17 \equiv 5 \pmod{12}$ เพราะฉะนั้น
$17^2 \equiv 5^2 \pmod{12} \equiv 25 \pmod{12} \equiv 1 \pmod{12}$
เพราะฉะนั้น $(17^2)^{27} \equiv 1^{27} \pmod{12} \equiv 1 \pmod{12}$
$17^{54} \equiv 1 \pmod{12}$
$17^{55} \equiv 17 \pmod{12} \equiv 5 \pmod{12}$
เพราะฉะนั้น $12 \mid (17^{55} - 5)$ ดังนั้น 12 หาร 17^{55} เหลือเศษ 5

ตัวอย่าง 4.1.7

จงหาเศษเหลือจากการหาร $29^3 \cdot 51$ ด้วย 15

วิธีทำ จาก $29 \equiv -1 \pmod{15} \quad \ldots (1)$
$51 \equiv 6 \pmod{15} \quad \cdots (2)$
จาก (1) และ (2) จะได้ $29^3 \cdot 51 \equiv (-1)^3(6) \pmod{15} \equiv -6 \pmod{15} \equiv 9 \pmod{15}$
เพราะฉะนั้นเศษเหลือจากการหาร $29^3 \cdot 51$ ด้วย 15 คือ 9

ตัวอย่าง 4.1.8

จงหาตัวเลข 2 หลักสุดท้ายของ 7^{77} เมื่อเขียนในระบบฐาน 10

วิธีทำ 2 หลักสุดท้ายของ 7^{77} เมื่อเขียนในระบบฐาน 10
คือเศษเหลือจากการหาร 7^{77} ด้วย 100
เพราะว่า $77 = 4(19) + 1$ เพราะฉะนั้นพิจารณาตามลำดับดังนี้
$7^4 \equiv 2401 \pmod{100} \equiv 1 \pmod{100}$
$(7^4)^{19} \equiv 1 \pmod{100}$
$(7^4)^{19}\, 7 \equiv 7 \pmod{100}$
$7^{[(4\cdot 19)+1]} \equiv 7 \pmod{100}$
$7^{77} \equiv 7 \pmod{100}$
ดังนั้น ตัวเลข 2 หลักสุดท้ายของ 7^{77} เมื่อเขียนในระบบฐาน 10 คือ 07

ตัวอย่าง 4.1.9

จงพิสูจน์ข้อความต่อไปนี้
(1) ถ้า a เป็นจำนวนเต็มคี่ แล้ว $a^2 \equiv 1 \pmod{8}$
(2) ถ้า a เป็นจำนวนเต็มคู่ แล้ว $a^2 \equiv 0 \pmod{4}$

การพิสูจน์ (1) ให้ a เป็นจำนวนเต็มคี่

จะได้ว่า $a = 2k+1$ สำหรับบางจำนวนเต็ม k บางตัว

ดังนั้น $a \equiv 1 \pmod 2$

จาก $a = 2k+1$ จะได้ว่า $a^2 = (2k+1)^2 = 4k^2+4k+1 = 8\left(\frac{1}{2}k^2+\frac{1}{2}k\right)+1$

โดยที่ $\frac{1}{2}k^2+\frac{1}{2}k$ เป็นจำนวนเต็ม

ดังนั้น $a^2 \equiv 1 \pmod 8$

(2) ให้ a เป็นจำนวนเต็มคู่

จะได้ว่า $a = 2k$ สำหรับบางจำนวนเต็ม k บางตัว

ดังนั้น $a \equiv 0 \pmod 2$ จะได้ว่า $a^2 \equiv 0 \pmod 4$ □

ตัวอย่าง 4.1.10

จงหาเศษที่เกิดจากการหาร $1^5+2^5+\cdots+10^5$ หารด้วย 4

วิธีทำ เนื่องจาก $1 \equiv 1 \pmod 4 \equiv 5 \pmod 4 \equiv 9 \pmod 4$

$2 \equiv 2 \pmod 4 \equiv 6 \pmod 4 \equiv 10 \pmod 4$

$3 \equiv 3 \pmod 4 \equiv 7 \pmod 4$

$4 \equiv 0 \pmod 4 \equiv 8 \pmod 4$

ดังนั้น $1^5 \equiv 1^5 \pmod 4 \equiv 5^5 \pmod 4 \equiv 9^5 \pmod 4$

$2^5 \equiv 2^5 \pmod 4 \equiv 6^5 \pmod 4 \equiv 10^5 \pmod 4$

$3^5 \equiv 3^5 \pmod 4 \equiv 7^5 \pmod 4$

$4^5 \equiv 0^5 \pmod 4 \equiv 8^5 \pmod 4$

เพราะฉะนั้น $1^5+2^5+\cdots+10^5 \equiv 3(1^5)+3(2^5)+2(3^5)+2(0^5) \pmod 4$

$\equiv 3+96+486+0 \pmod 4$

$\equiv 3+0+2 \pmod 4$

$\equiv 5 \pmod 4 \equiv 1 \pmod 4$

จะได้ว่า $1^5+2^5+\cdots+10^5$ หารด้วย 4 เหลือเศษ 1

ตัวอย่าง 4.1.11

กำหนด a, b เป็นจำนวนเต็ม และ p เป็นจำนวนเฉพาะบวก จงพิสูจน์ว่า
ถ้า $a^2 \equiv b^2 \pmod p$ แล้ว $a \equiv \pm b \pmod p$

การพิสูจน์ ให้ a, b เป็นจำนวนเต็ม และ p เป็นจำนวนเฉพาะบวก

สมมติว่า $a^2 \equiv b^2 \pmod p$ จะได้ว่า $p \mid (a^2+b^2)$

แต่ $(a^2+b^2) = (a+b)(a-b)$ ดังนั้น $p \mid (a+b)(a-b)$

เนื่องจาก p เป็นจำนวนเฉพาะ จะได้ว่า $p \mid (a+b)$ หรือ $p \mid (a-b)$

ดังนั้น $a \equiv -b \pmod p$ หรือ $a \equiv b \pmod p$

นั่นคือ $a \equiv \pm b \pmod p$ □

จากสมบัติของสมภาคเท่าที่ได้กล่าวมา เราพบว่า สมภาคมีสมบัติที่คล้ายกับสมบัติของการเท่ากัน แต่อาจมีสมบัติบางข้อที่ต้องพึงระวัง เช่น ในระบบจำนวนเต็ม "ถ้า $ax = ay$ และ $a \neq 0$ แล้ว $x = y$ จะพบว่า $ax \equiv ay \pmod{m}$ และ $a \neq 0$ แล้ว $x \equiv y \pmod{m}$" เป็นคำกล่าวที่ไม่จริง (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 131) แสดงได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1.3

ให้ $n \in \mathbb{N}$ และ $a, b, x, y \in \mathbb{Z}$

(1) ถ้า $a \equiv b \pmod{n}$ แล้ว $(a, n) = (b, n)$

(2) $ax \equiv ay \pmod{n}$ ก็ต่อเมื่อ $x \equiv y \left(\mod \frac{n}{(a,n)}\right)$

(3) ถ้า $ax \equiv ay \pmod{n}$ และ $(a, n) = 1$ แล้ว $x \equiv y \pmod{n}$

(4) ให้ $ax \equiv ay \pmod{n}$ และ n เป็นจำนวนเฉพาะซึ่ง $n \nmid a$ แล้ว $x \equiv y \pmod{n}$

การพิสูจน์ (1) ให้ $a \equiv b \pmod{n}$ จะได้ว่า $n \mid (a - b)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $(a - b) = nk$ ให้ $(b, n) = d$

โดยทฤษฎีบท 2.4.6 จะได้ว่า $(b + nk, n) = d$

นั่นคือ $(a, n) = (b, n)$

(2) ($\Rightarrow$) ให้ $ax \equiv ay \pmod{n}$ จะได้ว่า $n \mid (ax - ay)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $a(x - y) = nk$

ให้ $d = (a, n)$ จะได้ $d \mid a$ และ $d \mid n$

ดังนั้น $\frac{n}{d} \,\Big|\, \frac{a}{d}(x - y)$

โดยทฤษฎีบท 2.4.5 จะได้ $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

ดังนั้นโดยทฤษฎีบท 2.4.7 ข้อ 3. สรุปได้ว่า $\frac{n}{d} \,\Big|\, (x - y)$

นั่นคือ $x \equiv y \left(\mod \frac{n}{(a,n)}\right)$

($\Leftarrow$) ให้ $d = (a, n)$ และ $x \equiv y \left(\mod \frac{n}{d}\right)$ จะได้ $\frac{n}{d} \,\Big|\, (x - y)$

แสดงว่ามี $k \in \mathbb{Z}$ ซึ่ง $x - y = \frac{n}{d}k$

ดังนั้น $a(x - y) = a\left(\frac{n}{d}k\right)$

และจาก $d \mid a$ สรุปได้ว่า $n \mid a(x - y)$

นั่นคือ $ax \equiv ay \pmod{n}$

(3) ให้ $ax \equiv ay \pmod{n}$ และ $(a, n) = 1$ โดยข้อ (2) ข้างต้น

จะได้ว่า $x \equiv y \left(\mod \frac{n}{(a,n)}\right)$ นั่นคือ $x \equiv y \pmod{n}$

(4) ให้ $ax \equiv ay \pmod{n}$ และ n เป็นจำนวนเฉพาะซึ่ง $n \nmid a$

แสดงว่า $(a, n) = 1$ โดยข้อ (3) ข้างต้น จะได้ว่า $x \equiv y \pmod{n}$ □

ทฤษฎีบท 4.1.4

ให้ $a, b \in \mathbb{Z}$ และ $n_1, n_2, n_3, \ldots, n_r$ เป็นจำนวนเต็มบวกใด ๆ จะได้ว่า

(1) $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, 3, \ldots, r$ ก็ต่อเมื่อ $a \equiv b \pmod{[n_1, n_2, n_3, \ldots, n_r]}$

(2) ถ้า $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, 3, \ldots, r$ และ $n_1, n_2, n_3, \ldots, n_r$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a \equiv b \pmod{n_1 n_2 n_3 \cdots n_r}$

การพิสูจน์ (1) ($\Rightarrow$) ให้ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, 3, \ldots, r$
จะได้ว่า $n_i \mid (a - b)$ สำหรับ $i = 1, 2, 3, \ldots, r$
แสดงว่า $a - b$ เป็นตัวคูณร่วมของ $n_1, n_2, n_3, \ldots, n_r$
โดยทฤษฎีบท 2.6.1 จะได้ $[n_1, n_2, n_3, \ldots, n_r] \mid (a - b)$
นั่นคือ $a \equiv b \pmod{[n_1, n_2, n_3, \ldots, n_r]}$
($\Leftarrow$) ให้ $a \equiv b \pmod{[n_1, n_2, n_3, \ldots, n_r]}$
จะได้ $[n_1, n_2, n_3, \ldots, n_r] \mid (a - b)$
เนื่องจาก $n_i \mid [n_1, n_2, n_3, \ldots, n_r]$ สำหรับ $i = 1, 2, 3, \ldots, r$
ดังนั้น $n_i \mid (a - b)$ สำหรับ $i = 1, 2, 3, \ldots, r$
นั่นคือ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, 3, \ldots, r$
(2) ให้ $a \equiv b \pmod{n_i}$ สำหรับ $i = 1, 2, 3, \ldots, r$ และ $n_1, n_2, n_3, \ldots, n_r$
เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่
แสดงว่า $[n_1, n_2, n_3, \ldots, n_r] = n_1 n_2 n_3 \cdots n_r$
จากข้อ (1) ข้างต้น จะได้ว่า $a \equiv b \pmod{n_1 n_2 n_3 \cdots n_r}$ □

ทฤษฎีบท 4.1.5

ให้ $a \in \mathbb{Z}$ และ $n \in \mathbb{N}$ จะได้ว่ามี $r \in \mathbb{Z}$ ซึ่ง $0 \leq r < n$ เพียงค่าเดียวที่ทำให้ $a \equiv r \pmod{n}$

การพิสูจน์ ให้ $a \in \mathbb{Z}$ และ $n \in \mathbb{N}$ โดยขั้นตอนวิธีการหารจะได้ว่า
มี q, r เพียงคู่เดียวที่ทำให้ $a = nq + r$ โดยที่ $0 \leq r < n$ แสดงว่า $a - r = nq$
ดังนั้น $a \equiv r \pmod{n}$ โดยที่ $0 \leq r < n \quad \cdots (*)$
ต่อไปจะแสดงว่ามี r เพียงค่าเดียวที่สอดคล้องสมการ $(*)$
ให้ $r_1, r_2 \in \mathbb{Z}$ ซึ่ง $0 \leq r_1 \leq r_2 < n$ ที่สอดคล้อง $a \equiv r_1 \pmod{n}$ และ $a \equiv r_2 \pmod{n}$
จะได้ว่า $n \mid (a - r_1)$ และ $n \mid (a - r_2)$ โดยที่ $0 \leq r_2 - r_1 < n$
ดังนั้น $n \mid [(a - r_1) - (a - r_2)]$ นั่นคือ $n \mid (r_2 - r_1)$
ถ้า $0 < (r_2 - r_1) < n$ จะได้ว่า $n \nmid (r_2 - r_1)$
ดังนั้น $r_2 - r_1 = 0$ นั่นคือ $r_2 = r_1$
เพราะฉะนั้นสำหรับจำนวนเต็ม a ใด ๆ จะมีจำนวนเต็ม r ซึ่ง $0 \leq r < n$
เพียงค่าเดียวเท่านั้นที่ทำให้ $a \equiv r \pmod{n}$ □

จากทฤษฎีบท 4.1.5 เราพบว่า

1. ถ้า $r_1, r_2 \in \{0, 1, 2, \ldots, n - 1\}$ โดยที่ $r_1 \equiv r_2 \pmod{n}$ แล้ว $r_1 = r_2$
2. สมาชิกในเซต $\{0, 1, 2, \ldots, n - 1\}$ ที่ต่างกัน จะไม่สมภาคกันในมอดุโล n
3. ทุก ๆ จำนวนเต็ม a จะมี $r \in \{0, 1, 2, \ldots, n - 1\}$ เพียงค่าเดียวที่ทำให้ $a \equiv r \pmod{n}$ และค่า r นี้คือเศษเหลือจากการหาร a ด้วย n

4.2 สมการสมภาค

ในหัวข้อนี้เราจะศึกษาการหาคำตอบของสมการพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มและทำให้เราทราบวิธีการหาคำตอบทั้งหมดของสมการพหุนามในแง่ของสมภาคมอดุโล n ซึ่งมีรายละเอียดดังนี้ (ณรงค์ ปั้นนิ่ม และนิตติยา ปภาพจน์. 2552 : 136)

ทฤษฎีบท 4.2.1

ให้ $f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$ เป็นพหุนามที่มี $c_i \in \mathbb{Z}$ และ $c_m \neq 0$ จะได้ว่า
(1) ถ้า $a \equiv b \pmod n$ แล้ว $f(a) \equiv f(b) \pmod n$
(2) ถ้า a เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod n$ และ $a \equiv b \pmod n$ แล้ว b จะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod n$

การพิสูจน์ (1) จาก $a \equiv b \pmod n$ โดยทฤษฎีบท 4.1.2 ข้อ 5.
และโดยทฤษฎีบท 4.1.2 ข้อ 4. จะได้ว่า $c_i a^i \equiv c_i b^i \pmod n$ ทุก $i = 1, 2, \ldots, m$
ดังนั้น โดยทฤษฎีบท 4.1.2 ข้อ 3. จะได้
$c_m a^m + c_{m-1}a^{m-1} + \cdots + c_1 a + c_0 \equiv c_m b^m + c_{m-1}c^{m-1} + \cdots + c_1 b + c_0 \pmod n$
นั่นคือ $f(a) \equiv f(b) \pmod n$
(2) จาก a เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod n$ และ $a \equiv b \pmod n$
โดยข้อ (1) ข้างต้น จะได้ว่า $f(a) \equiv f(b) \pmod n$
ดังนั้น $f(b) \equiv 0 \pmod n$
นั่นคือ b เป็นคำตอบของสมการ $f(x) \equiv 0 \pmod n$ □

ให้ $i \in \{0, 1, 2, 3, 4, 5\}$ กำหนด $[i] = \{6k + i \mid k \in \mathbb{Z}\}$ เราพบว่า
(i) $[i] \neq \varnothing$
(ii) $[i] \cap [j] = \varnothing$ ทุก ๆ i, j ซึ่ง $0 \leq i < j \leq 5$
(iii) $\bigcup_{i=0}^{5} [i] = \mathbb{Z}$

จากความจริงข้างต้น แสดงถึงการแบ่งเซตของจำนวนเต็มออกเป็น 6 สับเซตที่แต่ละ 2 สับเซตที่แตกต่างกันไม่มีสมาชิกร่วมกัน ในกรณีทั่ว ๆ ไป $n \in \mathbb{N}$ เราสามารถกำหนด

$$[i] = \{nk + i \mid k \in \mathbb{Z}\}, \quad 0 \leq j \leq n - 1$$

จะได้ว่า $[i] \neq \varnothing,\ [i] \cap [j] = \varnothing,\ 0 \leq i < j \leq n - 1$
และ $\bigcup_{i=0}^{n-1} [i] = \mathbb{Z}$ จึงส่งผลให้เซตของจำนวนเต็มถูกแบ่งออกเป็น n สับเซต

ให้ $n \in \mathbb{N}$ กำหนด $n \,\Big|\, \left[a\left(x_0 + \frac{n}{d}t\right) - b\right]$, $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$

เราจะเรียก $\mathbb{Z}_n$ ว่า **เซตของจำนวนเต็มมอดุโล n**

$\mathbb{Z}_n$ มีบทบาทมากในการศึกษาทฤษฎีจำนวนโดยเฉพาะอย่างยิ่ง $\mathbb{Z}_n$ เป็นสิ่งสำคัญในการกำหนดแนวทางการศึกษา "สมการสมภาค" ซึ่งจะได้กล่าวต่อไปในแง่ของโครงสร้างของ $\langle \mathbb{Z}_n, +, \cdot \rangle$ เมื่อการดำเนินการ "+" และการศึกษาพีชคณิตเชิงนามธรรมเพื่อให้ผู้เรียนเกิดความเข้าใจเพราะระบบ $\langle \mathbb{Z}_n, +, \cdot \rangle$ มีโครงสร้างบางอย่างเหมือนกับ $\langle \mathbb{Z}, +, \cdot \rangle$ และมีโครงสร้างบางอย่างที่ต่างกัน

ผู้อ่านอาจคุ้นเคยกับการแก้สมการ เช่น การแก้สมการ $x^2 + x - 2 = 0$ หมายถึง การหาจำนวนจริง x_0 ซึ่ง $x_0^2 + x_0 - 2 = 0$ จากการใช้พีชคณิตเบื้องต้นเราทราบว่า

$$1^2 + 1 - 2 = 0 = (-2)^2 + (-2) - 2$$

ดังนั้น 1 และ -2 ต่างก็เป็นคำตอบของสมการ $x^2 + x - 2 = 0$

เราอาจพิจารณาการหาคำตอบของสมการ $2^x = 8$ ซึ่งเราพบว่า $x = 3$ คือคำตอบของสมการ $2^x = 8$ สำหรับการศึกษาสมการสมภาค เช่น $x^2 + x - 2 \equiv 0 \pmod 5$ เรามุ่งในการหาคำตอบ x_0 ที่เป็นจำนวนเต็ม ซึ่ง $x^2 + x - 2 \equiv 0 \pmod 5$

ถ้าจะกล่าวโดยทั่วไป ให้ f แทนฟังก์ชันที่มี x เป็นตัวแปรและกำหนดขอบเขตของตัวแปร x คือเซตของจำนวนเต็มและสำหรับทุก ๆ จำนวนเต็ม x ค่าของ $f(x)$ เป็นจำนวนเต็ม เราอาจสนใจการหาคำตอบของสมการ $f(x) \equiv 0 \pmod n$

กล่าวคือเราจะศึกษาสมการสมภาค $f(x) \equiv 0 \pmod n$ ก็ต่อเมื่อ f มีสมบัติว่า ถ้า $a \equiv b \pmod n$ แล้ว $f(a) \equiv f(b) \pmod n$

จากทฤษฎีบท 4.2.1 เราพบว่า ทุก ๆ พหุนาม $f(x)$ ที่มีสัมประสิทธิ์เป็นจำนวนเต็มสอดคล้องกับสมบัติดังกล่าว ในขณะที่สมการ $2^x - 8 \equiv 0 \pmod 5$ เป็นสมการที่ไม่สอดคล้องกับสมบัติพื้นฐานที่เราพึ่งจะศึกษา นอกจากนั้น ถ้าพิจารณาสมการ

$$|\,2x + 3\,| - 2 \equiv 0 \pmod 5$$

เราพบว่า $2 \equiv -3 \pmod 5$ แต่

$$|\,2(2) + 3\,| - 2 = 5 \not\equiv 1 = |\,2(-3) + 3\,| - 2 \pmod 5$$

ดังนั้นฟังก์ชัน f ที่กำหนดโดย $f(x) = |\,2x + 3\,| - 2$ จะเป็นฟังก์ชันที่ไม่สอดคล้องสมบัติพื้นฐานเช่นกัน

จากความจริงข้างต้นเราพบว่า ในการหาคำตอบของสมการสมภาค $f(x) \equiv 0 \pmod n$ ทั้งหมดนั้น เราอาจหาได้โดยการหาค่า $f(0), f(1), \ldots, f(n-1)$ และถ้า $f(i) \equiv 0 \pmod n,\ 0 \le i < n - 1$ จะได้ว่า $x = i + nk$ เป็นคำตอบของสมการดังกล่าว สำหรับทุกจำนวนเต็ม k

ตัวอย่าง 4.2.1

จงหาคำตอบของสมการ $x^2 + x - 2 \equiv 0 \pmod 5$

วิธีทำ จากทฤษฎีบท 4.2.1 พบว่า ถ้า $a \equiv b \pmod 5$ แล้ว $a^2 + a - 2 \equiv b^2 + b - 2 \pmod 5$

ซึ่งหมายความว่าการหาคำตอบ $x_0 \in \mathbb{Z}$ ทั้งหมดที่กำหนดให้ $x^2 + x - 2 \equiv 0 \pmod 5$

เป็นการเพียงพอที่จะเลือก x_0 จากสมาชิกแต่ละตัวในเซต $\{0, 1, 2, 3, 4\}$

เพราะว่า $0^2 + 0 - 2 \not\equiv 0 \pmod 5$

$1^2 + 1 - 2 \equiv 0 \pmod 5$

$2^2 + 2 - 2 \not\equiv 0 \pmod 5$

$3^2 + 3 - 2 \equiv 0 \pmod 5$

และ $4^2 + 4 - 2 \not\equiv 0 \pmod 5$

ดังนั้น คำตอบ x_0 ของสมการ $x^2 + x - 2 \equiv 0 \pmod 5$ ในเซต $\{0, 1, 2, 3, 4\}$ คือ $x_0 = 1, 3$

นั่นคือ คำตอบทั้งหมดของสมการ $x^2 + x - 2 \equiv 0 \pmod 5$ คือ

$\{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\} \cup \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 5\}$

จากตัวอย่าง 4.2.1 ข้างต้น ทำให้เราไม่มีความจำเป็นที่จะต้องจำแนกความแตกต่างระหว่าง 2 คำตอบที่สมภาคกัน เช่นทั้ง 1 และ 6 ต่างก็เป็นคำตอบของสมการ $x^2 + x - 2 \equiv 0 \pmod 5$ แต่ $1 \equiv 6 \pmod 5$ เมื่อเป็นเช่นนี้จะกล่าวว่า 1 และ 6 เป็นคำตอบที่สมภาคในมอดุโล 5 ดังนั้น สมการ $x^2 + x - 2 \equiv 0 \pmod 5$ มีเพียง 2 คำตอบเท่านั้นที่ไม่สมภาคกันในมอดุโล 5 คือ 1 และ 3

ตัวอย่าง 4.2.2

จงหาคำตอบ (ที่แตกต่างกัน) ทั้งหมดของ $x^2 + x - 2 \equiv 0 \pmod 9$ ที่ไม่สมภาคกันในมอดุโล 9

วิธีทำ ในการหาคำตอบของสมการสมภาคกันข้างต้น เป็นการเพียงพอที่จะหาคำตอบ x_0

เมื่อ $0^2 + 0 - 2 \not\equiv 0 \pmod 9$

$1^2 + 1 - 2 \equiv 0 \pmod 9$

$2^2 + 2 - 2 \not\equiv 0 \pmod 9$

$3^2 + 3 - 2 \not\equiv 0 \pmod 9$

$4^2 + 4 - 2 \equiv 0 \pmod 9$

$5^2 + 5 - 2 \not\equiv 0 \pmod 9$

$6^2 + 6 - 2 \not\equiv 0 \pmod 9$

$7^2 + 7 - 2 \equiv 0 \pmod 9$

และ $8^2 + 8 - 2 \not\equiv 0 \pmod 9$

ดังนั้น คำตอบ x_0 ของสมการ $x^2 + x - 2 \equiv 0 \pmod 9$ ในเซต $\{0, 1, 2, \ldots, 8\}$ คือ $x_0 = 1, 4, 7$

ตัวอย่าง 4.2.3

จงหาคำตอบ (ที่แตกต่างกัน) ทั้งหมดของสมการสมภาคต่อไปนี้

(1) $5x \equiv 3 \pmod 6$

(2) $6x \equiv 3 \pmod 9$

(3) $3x \equiv 5 \pmod 6$

วิธีทำ (1) จากการเลือก $x_0 \in \{0, 1, 2, 3, 4, 5\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 6

$5(0) \not\equiv 3 \pmod 6$, $5(1) \not\equiv 3 \pmod 6$, $5(2) \not\equiv 3 \pmod 6$, $5(3) \equiv 3 \pmod 6$,

$5(4) \not\equiv 3 \pmod 6$ และ $5(5) \not\equiv 3 \pmod 6$

ดังนั้นคำตอบ x_0 ของสมการ $5x \equiv 3 \pmod 6$ มีคำตอบที่แตกต่างกัน

เพียงคำตอบเดียวในมอดุโล 6 คือ $x_0 = 3$

(2) จากการเลือก $x_0 \in \{0, 1, 2, \ldots, 8\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 9

$6(0) \not\equiv 3 \pmod 9$, $6(1) \not\equiv 3 \pmod 9$, $6(2) \equiv 3 \pmod 9$, $6(3) \not\equiv 3 \pmod 9$,

$6(4) \not\equiv 3 \pmod 9$, $6(5) \equiv 3 \pmod 9$, $6(6) \not\equiv 3 \pmod 9$, $6(7) \not\equiv 3 \pmod 9$

และ $6(8) \equiv 3 \pmod 9$

นั่นคือ $x_0 = 2, 5, 8$

(3) จากการเลือก $x_0 \in \{0, 1, 2, 3, 4, 5\}$ เพื่อตรวจสอบ เราพบว่าในมอดุโล 6

$3(0) \not\equiv 5 \pmod 6$, $3(1) \not\equiv 5 \pmod 6$, $3(2) \not\equiv 5 \pmod 6$, $3(3) \not\equiv 5 \pmod 6$,

$3(4) \not\equiv 5 \pmod 6$ และ $3(5) \not\equiv 5 \pmod 6$

นั่นเป็นการแสดงว่าสมการ $3x \equiv 5 \pmod 6$ ไม่มีคำตอบ

ตัวอย่าง 4.2.4

จงพิจารณาว่า $5x \equiv 3 \pmod 6$ มีผลเฉลยหรือไม่ ถ้ามีจงหาผลเฉลยทั้งหมด

วิธีทำ โดยการแทนค่า $x = 0, 1, 2, 3, 4, 5$ ในสมการ $5x \equiv 3 \pmod 6$ จะได้

$5(0) = 0 \not\equiv 3 \pmod 6,\ 5(1) = 5 \not\equiv 3 \pmod 6,\ 5(2) = 10 \not\equiv 3 \pmod 6,$

$5(3) = 15 \equiv 3 \pmod 6,\ 5(4) = 20 \not\equiv 3 \pmod 6,\ 5(5) = 25 \not\equiv 3 \pmod 6$

เพราะฉะนั้นเซตผลเฉลยของสมการ $5x \equiv 3 \pmod 6$ คือ $[3]_6 = \{3, 3 \pm 6, 3 \pm 12, \ldots\}$

ตัวอย่าง 4.2.5

จงพิจารณาว่า $4x \equiv 12 \pmod 8$ มีผลเฉลยหรือไม่ ถ้ามีจงหาผลเฉลยทั้งหมด

วิธีทำ โดยการแทนค่า $x = 0, 1, 2, 3, 4, 5, 6, 7$ ในสมการ $4x \equiv 12 \pmod 8$ จะได้

$4(0) = 0 \not\equiv 12 \pmod 8,\ 4(1) = 4 \equiv 12 \pmod 8,\ 4(2) = 8 \not\equiv 12 \pmod 8,$

$4(3) = 12 \equiv 12 \pmod 8,\ 4(4) = 16 \not\equiv 12 \pmod 8,\ 4(5) = 20 \equiv 12 \pmod 8$

$4(6) = 24 \not\equiv 12 \pmod 8,\ 4(7) = 28 \equiv 12 \pmod 8$

เพราะฉะนั้นเซตผลเฉลยของสมการ $4x \equiv 12 \pmod 8$ คือ $[1]_8, [3]_8, [5]_8, [7]_8$

ตัวอย่าง 4.2.6

จงพิจารณา $2x \equiv 5 \pmod 4$ มีผลเฉลยหรือไม่ ถ้ามีจงหาผลเฉลยทั้งหมด

วิธีทำ โดยการแทนค่า $x = 0, 1, 2, 3$ ในสมการ $2x \equiv 5 \pmod 4$ จะได้

$2(0) = 0 \not\equiv 5 \pmod 4,\ 2(1) = 2 \not\equiv 5 \pmod 4,\ 2(2) = 4 \not\equiv 5 \pmod 4$

และ $2(3) = 6 \not\equiv 5 \pmod 4$

เพราะฉะนั้น $2x \equiv 5 \pmod 4$ ไม่มีผลเฉลย

จากตัวอย่างข้างต้น เราพบสมการที่อยู่ในรูป $ax \equiv b \pmod n$ อาจมีคำตอบหรือไม่มีคำตอบ และในกรณีสมการมีคำตอบ อาจมีคำตอบมากกว่า 1 คำตอบก็ได้ ซึ่งในหัวข้อถัดไปจะกล่าวถึงสมการสมภาคที่อยู่ในรูป $ax \equiv b \pmod n$ พร้อมนิยามและทฤษฎีบทที่เกี่ยวข้อง

4.3 สมภาคเชิงเส้น

ในหัวข้อนี้จะกล่าวถึงการหาผลเฉลยและทฤษฎีบทเกี่ยวกับการหาผลเฉลยของสมภาคเชิงเส้น โดยเราจะเริ่มต้นจากบทนิยามดังต่อไปนี้ (นพพร ธนะชัยขันธ์. 2543 : 81, สมวงษ์ แปลงประสพโชค. 2545 : 62, Raji W. 2013 : 60)

บทนิยาม 4.3.1

ให้ a, b และ n เป็นจำนวนเต็มโดยที่ $n > 0$ เรียกสมภาคที่อยู่ในรูป $ax \equiv b \pmod{n}$ ว่า **สมภาคเชิงเส้นที่มี x เป็นตัวแปร (a linear congruence in one variable x)** เรียก x_0 ที่ทำให้ $ax_0 \equiv b \pmod{n}$ เป็นจริงว่า **ผลเฉลย (solution)** ของ $ax \equiv b \pmod{n}$ และถ้ามีจำนวนเต็ม x_1 ที่ทำให้ $ax_1 \equiv b \pmod{n}$ เป็นจำนวนจริงอีกซึ่ง $x_0 \equiv x_1 \pmod{n}$ แล้วจะเรียก x_0 และ x_1 ว่าเป็น**ผลเฉลยที่ไม่ต่างกัน**หรือ**ผลเฉลยที่สมภาคกัน** (congruent solution) แต่ถ้า x_0 ไม่สมภาคกับ x_1 มอดุโล n จะเรียก x_0 และ x_1 ว่าเป็น**ผลเฉลยที่ต่างกัน**หรือ**ผลเฉลยที่ไม่สมภาคกัน** (incongruent solution)

ให้ a, b และ n เป็นจำนวนเต็มโดยที่ $n > 0$ เราจะพิจารณาหาผลเฉลยของสมภาคเชิงเส้น

$$ax \equiv b \pmod{n} \quad \cdots (\star)$$

ถ้า x_0 เป็นผลเฉลยของ $(\star)$ และ $x_1 \equiv x_0 \pmod{n}$ จะได้ว่า $ax_1 \equiv ax_0 \equiv b \pmod{n}$ นั่นคือ x_1 เป็นผลเฉลยของ $(\star)$ ด้วย ดังนั้นในการพิจารณาหาผลเฉลยของ $(\star)$ เราจะหาผลเฉลยที่ไม่สมภาคกันมอดุโล n ทั้งหมด ดังตัวอย่างต่อไปนี้ (วรรณธิดา ยลวิลาศ. 2560 : 78)

ตัวอย่าง 4.3.1

จงหาผลเฉลยของ $2x \equiv 3 \pmod{5}$

วิธีทำ แทนค่า $x = 0$ จะได้ $2 \cdot 0 \not\equiv 3 \pmod{5}$
แทนค่า $x = 1$ จะได้ $2 \cdot 1 \not\equiv 3 \pmod{5}$
แทนค่า $x = 2$ จะได้ $2 \cdot 2 \not\equiv 3 \pmod{5}$
แทนค่า $x = 3$ จะได้ $2 \cdot 3 \not\equiv 3 \pmod{5}$
แทนค่า $x = 4$ จะได้ $2 \cdot 4 \equiv 3 \pmod{5}$
ดังนั้น $x = 4$ เป็นหนึ่งในผลเฉลยของ $2x \equiv 3 \pmod{5}$
กล่าวคือ $x \equiv 4 \pmod{5}$ คือผลเฉลยของสมภาค

ทฤษฎีบทต่อไปนี้จะแสดงเงื่อนไขที่จำเป็นและเพียงพอที่จะทำให้สมการ $ax \equiv b \pmod{n}$ มีคำตอบพร้อมกับหาคำตอบทั้งหมดที่ไม่สมภาคกันมอดุโล n (วรางคณา ร่องมะรุด. 2523 : 30-31, ขนิษฐา ชมภูวิเศษ. 2559 : 97)

ทฤษฎีบท 4.3.1

ให้ $a, b, n \in \mathbb{Z}$ โดยที่ $n > 0$ และ $(a, n) = d$ จะได้ว่า
(1) **สมภาคเชิงเส้น** $ax \equiv b \pmod{n}$ มีคำตอบ $x \in \mathbb{Z}$ ก็ต่อเมื่อ $d \mid b$
(2) ถ้า $d \mid b$ แล้วสมการสมภาคเชิงเส้น $ax \equiv b \pmod{n}$ มีคำตอบอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล n และคำตอบเหล่านั้นคือ $x \equiv x_0 + t\frac{n}{d} \pmod{n}$ เมื่อ $t = 0, 1, 2, \ldots, d-1$ โดยที่ x_0 คือคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{n}$

การพิสูจน์ (1) $(\Rightarrow)$ สมมติว่าสมการ $ax \equiv b \pmod{n}$ มีคำตอบ
จะได้ว่ามี $x_0 \in \mathbb{Z}$ ซึ่ง $ax_0 \equiv b \pmod{n}$ แสดงว่า $n \mid (ax_0 - b)$

เนื่องจาก $d \mid n$ และ $d \mid a$ ดังนั้น $d \mid b$
($\Leftarrow$) สมมติว่า $d \mid b$ จะได้ว่ามี $k \in \mathbb{Z}$ ซึ่ง $b = dk$ และจาก $d = (a, n)$
โดยทฤษฎีบท 2.4.2 จะได้ว่ามี $x_0, y_0 \in \mathbb{Z}$ ซึ่ง $d = ax_0 + ny_0$
ทำให้ได้ว่า $b = dk = ax_0k + ny_0k$
ดังนั้น $n \mid (ax_0k - b)$ นั่นคือ $ax_0k \equiv b \pmod{n}$
แสดงว่าสมการ $ax \equiv b \pmod{n}$ มี $x = x_0k$

(2) **ตอนที่ 1** จาก $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ และ $1 \mid \frac{b}{d}$
แสดงว่าสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{n}{d}\right)$ มีคำตอบ
ให้ x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{n}{d}\right)$
จะได้ว่า $\frac{n}{d} \mid \left(\frac{a}{d}x_0 - \frac{b}{d}\right)$ แสดงว่าจะมี $k \in \mathbb{Z}$ ซึ่ง

$$\frac{a}{d}x_0 - \frac{b}{d} = \frac{n}{d}k \quad \cdots (*)$$

ให้ $t \in \mathbb{Z}$ จะแสดงว่า $x_0 + \frac{n}{d}t$ เป็นคำตอบของสมการ
เพราะว่า

$$\begin{aligned} a\left(x_0 + \frac{n}{d}t\right) - b &= ax_0 + \frac{an}{d}t - b \\ &= \frac{adx_0}{d} + \frac{ant}{d} - \frac{bd}{d} \\ &= d\left(\frac{a}{d}x_0 - \frac{b}{d}\right) + \frac{a}{d}nt \\ &= d\left(\frac{n}{d}k\right) + \frac{a}{d}nt \quad \left(\text{แทนค่าจาก}(*)\right) \\ &= n\left(k + \frac{a}{d}t\right) \end{aligned}$$

จาก $d \mid n$ และ $t \in \mathbb{Z}$ จะได้ $n \mid \left[a\left(x_0 + \frac{n}{d}t\right) - b\right]$
นั่นคือ $a\left(x_0 + \frac{n}{d}t\right) \equiv b \pmod{n}$ แสดงว่า $x_0 + \frac{n}{d}t$ เป็นคำตอบของ
สมการ $ax \equiv b \pmod{n}$ สำหรับทุกจำนวนเต็ม
ต่อไปจะแสดงว่าคำตอบของสมการ $ax \equiv b \pmod{n}$ จะเขียนอยู่ในรูป

$$x_0 + \frac{n}{d}q \quad \text{เมื่อ } q \in \mathbb{Z}$$

ให้ x_1 เป็นคำตอบใด ๆ ของสมการ $ax \equiv b \pmod{n}$
จะได้ $ax_1 \equiv b \pmod{n}$ เนื่องจาก $a\left(x_0 + \frac{n}{d}t\right) \equiv b \pmod{n}$
จะได้ว่า $ax_1 \equiv a\left(x_0 + \frac{n}{d}t\right) \pmod{n}$
ดังนั้น $\frac{a}{d}x_1 \equiv \frac{a}{d}\left(x_0 + \frac{n}{d}t\right) \left(\mod \frac{n}{d}\right)$
จาก $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$ โดยทฤษฎีบท 4.1.2 ข้อ 3.
จะได้ว่า $x_1 \equiv \left(x_0 + \frac{n}{d}t\right) \left(\mod \frac{n}{d}\right)$
แสดงว่าจะมี $t_1 \in \mathbb{Z}$ ซึ่ง $x_1 - \left(x_0 + \frac{n}{d}t\right) = \frac{n}{d}t_1$
ทำให้ได้ว่า $x_1 = x_0 + \frac{n}{d}(t + t_1)$

นั่นคือ มี $q = t + t_1 \in \mathbb{Z}$ ที่ทำให้ $x_1 = x_0 + \frac{n}{d}q$
สรุป คำตอบของสมการ $ax \equiv b \pmod{n}$ จะเขียนอยู่ในรูป

$$x \equiv x_0 + t\left(\frac{n}{d}\right) \pmod{n} \text{ เมื่อ } t \in \mathbb{Z}$$

โดยที่ x_0 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{n}{d}\right)$
ตอนที่ 2 ให้ $d = (a, n)$ และ $t \in \mathbb{Z}$ จะต้องแสดงว่า
สมการ $ax \equiv b \pmod{n}$ มีคำตอบอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล n
จาก $d, t \in \mathbb{Z}$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้
$t = dq + r$ โดยที่ $0 \leq r < d$
ดังนั้น $x_0 + t\frac{n}{d} = x_0 + (dq + r)\frac{n}{d} = x_0 + nq + r\frac{n}{d}$
แสดงว่า $x_0 + t\frac{n}{d} \equiv x_0 + r\frac{n}{d} \pmod{n}$ โดยที่ $0 \leq r \leq d - 1$
สรุป คำตอบของสมการ $ax \equiv b \pmod{n}$
จะมีอยู่ d คำตอบเท่านั้นที่ไม่สมภาคกันในมอดุโล n
คือ $x \equiv x_0 + \frac{n}{d}t \pmod{n}$ เมื่อ $t = 0, 1, 2, \ldots, d - 1$ □

จากทฤษฎีบท 4.3.1 เราพบว่า

1. ถ้า $d \nmid b$ แล้ว สมการสมภาคเชิงเส้น $ax \equiv b \pmod{n}$ ไม่มีคำตอบ
2. ถ้า x_0 เป็นคำตอบหนึ่งองสมการ $\frac{a}{d}x \equiv 1 \left(\mod \frac{n}{d}\right)$ แล้ว $x_1 = \frac{b}{d}x_0$ จะเป็นคำตอบของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{n}{d}\right)$

ดังนั้น ในการหาคำตอบของสมการสมภาคเชิงเส้น $ax \equiv b \pmod{n}$ เราอาจหาคำตอบหนึ่งคือ x_0 จากสมการ $\frac{a}{d}x \equiv 1 \left(\mod \frac{n}{d}\right)$ และให้ $x_1 = \frac{b}{d}x_0$ จะได้ว่า x_1 เป็นคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{n}{d}\right)$

ตัวอย่าง 4.3.2

(1) สมการสมภาคเชิงเส้น $14x \equiv 13 \pmod{21}$ ไม่มีคำตอบเพราะว่า $(14, 21) = 7$ และ $7 \nmid 13$
(2) สมการสมภาคเชิงเส้น $9x \equiv 15 \pmod{21}$ มีคำตอบเพราะว่า $(9, 21) = 3$ และ $3 \mid 15$
และสมการสมภาคเชิงเส้นนี้มีคำตอบอยู่ 3 คำตอบที่ไม่สมภาคกันในมอดุโล 21
เนื่องจาก $9x \equiv 15 \pmod{21}$ จะได้ $3x \equiv 5 \pmod{7}$
เพราะว่า $12 \equiv 5 \pmod{7}$ และ $(3, 7) = 1$
ดังนั้น $x \equiv 4 \pmod{7}$
นั่นคือ สมการสมภาคเชิงเส้น จะมีคำตอบคือ $x \equiv x \equiv 4, 11, 18 \pmod{21}$

ตัวอย่าง 4.3.3

จงหาคำตอบของสมการสมภาคเชิงเส้น $91x \equiv 98 \pmod{119}$

วิธีทำ เนื่องจาก $(91, 119) = 7$ และ $7 \mid 98$ ดังนั้นสมการสมภาคเชิงเส้นนี้มีคำตอบอยู่ 7 คำตอบ
ที่ไม่สมภาคกันในมอดุโล 119 จาก $91x \equiv 98 \pmod{119}$
จะได้ว่า $13x \equiv 14 \pmod{17}$ เพราะว่า $(13, 17) = 1$
จะได้ว่าสมการสมภาคเชิงเส้นสุดท้ายนี้มีคำตอบ คือ $x \equiv 5 \pmod{17}$

ดังนั้น สมการสมภาคเชิงเส้นที่กำหนดให้มีคำตอบ คือ $x \equiv 5, 22, 39, 56, 73, 90, 107 \pmod{119}$

ตัวอย่าง 4.3.4

สมภาคเชิงเส้น $7x \equiv 22 \pmod{39}$
มีราก เพราะ $(7, 39) = 1$ โดยขั้นตอนวิธียุคลิด เราได้ $1 = -11 \cdot 7 + 2 \cdot 39$
ดังนั้น $22 = -242 \cdot 7 + 44 \cdot 39$
รากหนึ่งของสมการที่กำหนดให้คือ $x_0 = -242$ และรากทั่วไป คือ $x = -242 + 39t$
โดยให้ $t = 7$ เราได้ $x = 31$ ซึ่งเป็นจำนวนเต็มบวกที่เล็กที่สุดที่น้อยกว่า 39
ดังนั้นรากของสมภาคที่กำหนดให้คือ $x \equiv 31 \pmod{39}$

ตัวอย่าง 4.3.5

จงหาคำตอบของสมการสมภาคเชิงเส้น $39x \equiv 65 \pmod{52}$

วิธีทำ เพราะว่า $(39, 52) = 13$ และ $13 \mid 65$
แสดงว่าสมการสมภาคเชิงเส้นนี้มีคำตอบของสมการ 13 คำตอบ
ที่ไม่สมภาคกันในมอดุโล 52 การหาคำตอบเริ่มจากการหา x_0 โดยพิจารณาจาก

$$\frac{39}{13}x_0 \equiv \frac{65}{13} \left(\mod \frac{52}{13} \right) \text{ และ } 3x_0 \equiv 5 \pmod{4}$$

ดังนั้น คำตอบของสมการคือ $x \equiv 3 + \frac{52}{13}t \pmod{52}$ เมื่อ $t = 0, 1, 2, \ldots, 12$
ซึ่งได้แก่ $x \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51 \pmod{52}$

ตัวอย่าง 4.3.6

จงหาผลเฉลยทั้งหมดของ $9x \equiv 12 \pmod{15}$

วิธีทำ เนื่องจาก $(9, 15) = 3$ และ $3 \mid 12$ ดังนั้น $9x \equiv 12 \pmod{15}$
มีผลเฉลยที่ไม่สมภาคกันมอดุโล 15 อยู่จำนวน 3 ค่า
พิจารณาสมการ $9x - 15y = 12$
โดยขั้นตอนวิธีแบบยุคลิดได้ว่า $3 = 9 \cdot 2 - 15 \cdot 1$ นั่นคือ $12 = 4(9 \cdot 2 - 15 \cdot 1) = 9 \cdot 8 - 15 \cdot 4$
ดังนั้น $x = 8$ และ $y = 4$ เป็นผลเฉลยของ $9x - 15y = 12$
ทำให้ได้ว่า $x = 8$ เป็นผลเฉลยของ $9x \equiv 12 \pmod{15}$
และผลเฉลยทั้งหมดคือ $8,\ 8 + \left(\frac{15}{3}\right) \cdot 1 = 13$ และ $8 + \left(\frac{15}{3}\right) \cdot 2 = 18 \equiv 3 \pmod{15}$

สมภาคเชิงเส้นที่มีผลเฉลยและมีเพียงผลเฉลยเดียว ดังทฤษฎีบทต่อไปนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2547 : 142, สมวงษ์ แปลงประสพโชค. 2545 : 63, David M. Burton. 2007 : 77, Underwood Dudley. 1969 : 35-36)

บทแทรก 4.3.1

สำหรับจำนวนเต็ม a, b และ n ใด ๆ โดยที่ n เป็นบวก ถ้า $(a, n) = 1$ แล้ว $ax \equiv b \pmod{n}$ จะมีผลเฉลยเพียงผลเฉลยเดียวมอดุโล n

บทนิยาม 4.3.2

ถ้า $(a,n)=1$ ผลเฉลยของ $ax \equiv 1 (\mathrm{mod} n)$ จะเรียกว่า **ตัวผกผัน** (inverse) ของ a มอดุโล n

ตัวอย่าง 4.3.7

ตัวผกผันของ 5 มอดุโล 7 คือ 3 เพราะ $5 \cdot 3 \equiv 1 \pmod 7$
ตัวผกผันของ 3 มอดุโล 20 คือ 7 เพราะ $3 \cdot 7 \equiv 1 \pmod{20}$

4.4 ทฤษฎีบทเศษเหลือของจีน

มีปัญหาหนึ่งที่ชาวจีนสมัยโบราณนิยมถามกัน คือ การหาจำนวนเต็มที่ เมื่อหารด้วย 3 จะมีเศษเหลือเป็น 2 เมื่อหารด้วย 5 จะมีเศษเหลือเป็น 4 และเมื่อหารด้วย 7 จะมีเศษเหลือเป็น 5 ปัญหานี้คือการหาค่าจำนวนเต็ม x ที่สอดคล้องกับระบบสมภาคต่อไปนี้

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

ในหัวข้อนี้เราจะกล่าวถึงการหาผลเฉลยของระบบสมภาคเช่นนี้ โดยในตอนแรก จะพิจารณาในกรณีพิเศษคือ เมื่อตัวมอดุลัสทั้งหมดเป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ (สมพร เรืองโชติวิทย์. 2521 : 137-138, วัลลภ เหมวงษ์. 2556 : 98)

ทฤษฎีบท 4.4.1 : ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)

ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวกที่เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ จะได้ว่า ไม่ว่า $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มใด ๆ ระบบสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

จะมีผลเฉลยเพียงตัวเดียว มอดุโล m เมื่อ $m = m_1 m_2 \cdots m_n$ นั่นคือ ถ้า x_0 เป็นผลเฉลยแล้ว ผลเฉลยทั้งหมดจะอยู่ในรูป $x_0 + km$ เมื่อ k เป็นจำนวนเต็มใด ๆ

การพิสูจน์ เนื่องจาก $m_1, m_2, \ldots, m_n$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่
ดังนั้น $[m_1, m_2, \ldots, m_n] = m_1 m_2 \cdots m_n$
ให้ $m = m_1 m_2 \cdots m_n$
เราแบ่งการพิสูจน์ออกเป็น 2 ตอน ตอนแรกจะพิสูจน์ว่าระบบสมภาคมีผลเฉลย สำหรับแต่ละ i
ให้ $m_i' = \dfrac{m}{m_i}$ ดังนั้น m_i' เป็นจำนวนเต็ม
เนื่องจาก ทุก ๆ $i \neq j$, $(m_j, m_i) = 1$ ดังนั้น $(m_i', m_i) = 1$

จะได้ว่ามีจำนวนเต็ม y_i ที่ $m_i' y_i \equiv 1 \pmod{m_i}$
ให้ $x_0 = a_1 m_1' y_1 + a_2 m_2' y_2 + \cdots + a_n m_n' y_n$ เนื่องจากสำหรับทุก $i \neq j, m_i \mid m_j'$
ดังนั้นสำหรับทุก $i, x_0 \equiv a_1 m_i' y_i \equiv a_i \pmod{m_i}$
นั่นคือ x_0 เป็นผลเฉลยของระบบสมภาค
ให้ x_1 เป็นผลเฉลยของระบบสมภาค ดังนั้นทุก $i, x_i \equiv a_i \equiv x_0 \pmod{m_i}$
ทำให้ $m_i \mid (x_1 - x_0)$ ทุก i ดังนั้น $m \mid (x_1 - x_0)$
นั่นคือ $x_1 \equiv x_0 \pmod{m}$ ดังนั้นจะมีจำนวนเต็ม k บางตัวที่ทำให้ $x_1 = x_0 + mk$ □

ตัวอย่าง 4.4.1

จงหาคำตอบทั้งหมดของระบบสมภาค

$$(*) \cdots \begin{cases} x \equiv 2 \pmod{4} & \cdots (1) \\ x \equiv 4 \pmod{7} & \cdots (2) \end{cases}$$

วิธีทำ ให้ $A = \{2 + 4k \mid k \in \mathbb{Z}\}$ และ $B = \{4 + 7k \mid k \in \mathbb{Z}\}$
จะเห็นได้ชัดว่า A คือเซตคำตอบของสมการ (1) ในขณะที่ B คือเซตคำตอบของสมการ (2)
จากการกำหนดค่า k ที่เหมาะสมของแต่ละเซต จะพบว่า $18 \in A \cap B$
นั่นคือ 18 เป็นคำตอบของระบบสมการ $(*)$
ให้ z เป็นคำตอบของระบบสมการ $(*)$ นั่นคือ $z \in A \cap B$
ดังนั้น $z \equiv 18 \pmod{4}$ และ $z \equiv 18 \pmod{7}$
แสดงว่า $z \equiv 18 \pmod{28}$ นั่นคือ ทุก ๆ z ซึ่ง ว่า $z \equiv 18 \pmod{28}$
จะเป็นคำตอบของระบบสมการ $(*)$ ทั้งสิ้น
ดังนั้น เซตคำตอบของระบบสมการ $(*)$ คือ $\{18 + 28\mathrm{k} \mid k \in \mathbb{Z}\}$
เนื่องจากระบบสมการ $(*)$ มีเพียง 2 สมการเท่านั้นซึ่งเราสามารถหาคำตอบร่วมได้โดยง่าย
เพื่อให้การแก้ปัญหาข้างต้นมีวิธีการที่สามารรถใช้ได้กับทุก ๆ ระบบสมการ
เราต้องมาวิเคราะห์ถึงสิ่งที่ต้องการหา เพื่อที่จะแก้ระบบสมการดังกล่าว

(i) จาก $a = 7$ และ $b = 4$ ให้ x_0 และ y_0 เป็นคำตอบของสมการ
$7x \equiv 1 \pmod{4}$ และ $4y \equiv 1 \pmod{7}$
ดังนั้น $x_0 \equiv -1 \pmod{4}$ และ $y_0 \equiv 2 \pmod{7}$

(ii) จาก $c = 2$ และ $d = 4$
จะได้ $z = ax_0c + by_0d = 7 \cdot (-1) \cdot 2 + 4 \cdot 2 \cdot 4 = 18$

ตัวอย่าง 4.4.2

จงหาผลเฉลยที่เป็นจำนวนเต็มบวกค่าน้อยสุดของระบบสมภาค

$$x \equiv 2 \pmod{3}$$
$$x \equiv 4 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$

วิธีทำ ให้ $m_1 = 3, m_2 = 5$ และ $m_3 = 7$ ดังนั้น $m = 3 \cdot 5 \cdot 7 = 105$
โดยที่ $m_1' = 5 \cdot 7 = 35, m_2' = 3 \cdot 7 = 21$ และ $m_3' = 3 \cdot 5 = 15$

$2y_1 \equiv 35y_1 \equiv 1 \pmod 3$ จะได้ $y_1 = 2$
$y_2 \equiv 21y_2 \equiv 1 \pmod 5$ จะได้ $y_2 = 1$
$y_3 \equiv 15y_3 \equiv 1 \pmod 7$ จะได้ $y_3 = 1$
ดังนั้น $x_0 = 2 \cdot 35 \cdot 2 + 4 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 = 299$ เป็นผลเฉลย
และผลเฉลยทั้งหมดคือ $299 + 105k$ เมื่อ k เป็นจำนวนเต็ม
ค่า k ที่ทำให้ได้ผลเฉลยที่เป็นบวกค่าน้อยสุดคือ $k = -2$
ผลเฉลยดังกล่าวคือ $299 + 105(-2) = 89$

ตัวอย่าง 4.4.3

อายุของชายผู้หนึ่งเมื่อหารด้วย 3 เหลือเศษ 2 เมื่อหารด้วย 4 เหลือเศษ 1 และเมื่อหารด้วย 5 เหลือเศษ 2 จงหาอายุของชายผู้นี้

วิธีทำ ให้ x เป็นอายุของชายผู้นี้ จากโจทย์จะได้ว่า

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 2 \pmod 5$$

เพราะว่า $(3,4) = 1,\ (3,5) = 1,\ (4,5) = 1$
จะได้ว่าระบบสมภาคนี้มีคำตอบเพียงชุดเดียวในมอดุโล 60 $(60 = 3 \cdot 4 \cdot 5)$
จากทฤษฎีบทเศษเหลือของจีนให้ $m = 3 \cdot 4 \cdot 5 = 60$
โดยที่ $m_1' = 4 \cdot 5 = 20,\ m_2' = 3 \cdot 5 = 15$
และ $m_3' = 3 \cdot 4 = 12$
ให้ x_1, x_2 และ x_3 เป็นคำตอบของสมภาค

$$20x_1 \equiv 1 \pmod 3 \text{ จะได้ } x_1 = 2$$
$$15x_2 \equiv 1 \pmod 4 \text{ จะได้ } x_2 = 3$$
$$12x_3 \equiv 1 \pmod 5 \text{ จะได้ } x_3 = 3$$

ดังนั้น $x_0 = 20 \cdot 2 \cdot 2 + 15 \cdot 1 \cdot 3 + 12 \cdot 2 \cdot 3 = 197$
ซึ่งทำให้ $x_0 = 197 \equiv 17 \pmod{60}$
แสดงว่าผลเฉลยของระบบสมภาคคือ $x \equiv 17 \pmod{60}$
ดังนั้นชายผู้นี้มีอายุ 17 ปี หรือ 77 ปี หรือ 137 ปี

ตัวอย่าง 4.4.4

จงหาผลเฉลยของระบบสมภาคต่อไปนี้

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 3 \pmod 5$$

วิธีทำ เราจะใช้สัญลักษณ์ตามการพิสูจน์ในทฤษฎีบท 4.4.1 ดังนี้

$$M = (3)(4)(5) = 60$$
$$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$$
$$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$$
$$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$$

ต่อไปจะเป็นการหาผลเฉลยของสมภาคเชิงเส้น $M_i x_i \equiv 1 \pmod{m_i}$ สำหรับ $i = 1, 2, 3$ โดยการตรวจพินิจ ดังนี้

จาก $M_1 x_1 \equiv 1 \pmod{m_1}$ คือ $20x_1 \equiv 1 \pmod 3$ ซึ่งสมมูลกับสมภาค $2x_1 \equiv 1 \pmod 3$ ดังนั้น $x_1 \equiv 2 \pmod 3$

จาก $M_2 x_2 \equiv 1 \pmod{m_2}$ คือ $15x_2 \equiv 1 \pmod 4$ ซึ่งสมมูลกับสมภาค $3x_2 \equiv 1 \pmod 4$ ดังนั้น $x_2 \equiv 3 \pmod 4$

จาก $M_3 x_3 \equiv 1 \pmod{m_3}$ คือ $13x_3 \equiv 1 \pmod 5$ ซึ่งสมมูลกับสมภาค $2x_3 \equiv 1 \pmod 5$ ดังนั้น $x_3 \equiv 3 \pmod 5$

เราจะหาผลเฉลย x โดยการแทนค่าของ $x_1 = 2,\ x_2 = 3$ และ $x_3 = 3$

$$\begin{aligned} x &= b_1 M_1 x_1 + b_2 M_2 x_2 + b_3 M_3 x_3 \\ &= (2)(20)(2) + (1)(15)(3) + (3)(12)(3) \\ &= 233 \\ &\equiv 53 \pmod{60} \end{aligned}$$

ที่จริงแล้วผลเฉลยของระบบสมภาคเชิงเส้นนี้คือจำนวนเต็มบวกทุกตัวที่สมภาคกับ 53 มอดุโล 60 แต่ 53 เป็นผลเฉลยบวกที่น้อยที่สุด ขอให้ผู้อ่านตรวจผลเฉลยด้วยตนเองว่าสอดคล้องกับทุกสมภาคเชิงเส้นที่กำหนดให้

ตัวอย่าง 4.4.5

จงหาผลเฉลยของสมภาคเชิงเส้น $17x \equiv 9 \pmod{276}$

วิธีทำ เนื่องจาก $276 = 3 \cdot 4 \cdot 23$ เป็นการเพียงพอที่จะหาผลเฉลยจากระบบสมภาค

$$17x \equiv 9 \pmod 3$$
$$17x \equiv 9 \pmod 4$$
$$17x \equiv 9 \pmod{23}$$

ซึ่งสมมูลกับระบบสมภาค

$$x \equiv 0 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 10 \pmod{23}$$

ให้ $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 23 = 276$ และ

$$\frac{m}{m_1} = \frac{276}{3} = 92,\ \frac{m}{m_2} = \frac{276}{4} = 69,\ \frac{m}{m_2} = \frac{276}{23} = 12$$

ให้ b_1, b_2, b_3 เป็นผลเฉลยของสมภาคเชิงเส้น

$$92x \equiv 1 \pmod 3$$
$$69x \equiv 1 \pmod 4$$
$$12x \equiv 1 \pmod{23}$$

ตามลำดับ
จะได้ว่า $b_1 = 2, b_2 = 1$ และ $b_3 = 2$ ดังนั้น

$$\begin{aligned} x_0 &= \sum_{i=1}^{3} \frac{m}{m_i} a_i b_i \\ &= \frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 + \frac{m}{m_3} a_3 b_3 \\ &= 92 \cdot 0 \cdot 2 \cdot + 69 \cdot 1 \cdot 1 + 12 \cdot 10 \cdot 2 \\ &= 309 \end{aligned}$$

นั่นคือ 309 เป็นผลเฉลยของระบบสมภาคที่กำหนดให้
และเป็นผลเฉลยใด ๆ ของระบบสมภาคจะอยู่ในรูป

$$x \equiv 309 \equiv 33 \pmod{276}$$

ซึ่งเป็นผลเฉลยของสมภาคเชิงเส้น $17x \equiv 9 \pmod{276}$ ตามที่ต้องการ

ตัวอย่าง 4.4.6

ในการหารากของระบบสมภาค

$$x \equiv 3 \pmod{17}$$
$$x \equiv 4 \pmod{11}$$
$$x \equiv 5 \pmod 6$$

เนื่องจาก $(17, 11) = (17, 6) = (11, 6) = 1$ โดยทฤษฎีบท 4.4.1
จะได้ว่าระบบสมภาคข้างต้นนี้มีราก จากสมภาคแรก เราได้
(1) $x = 3 + 17t_1$
แทน x นี้ในสมภาคที่สองจะได้
(2) $3 + 17t_1 \equiv 4 \pmod{11}$
หารากของสมภาค จะพบว่า $t_1 \equiv 2 \pmod{11}$ หรือคือ
(3) $t_1 = 2 + 11t_2$
แทน (3) ใน (1) จะได้
(4) $x = 3 + 17(2 + 11t_2) = 3 + 2 \cdot 17 + 17 \cdot 11t_2$
แทน (4) ใน (3) จะได้ $3 + 2(-1) + (-1)(-1)t_2 \equiv 5 \pmod 6$
ดังนั้น $t_2 \equiv 4 \pmod 6$
นั่นคือ $t_2 = 4 + 6t$ เพราะฉะนั้น $x = 3 \cdot 2 \cdot 17 + 4 \cdot 17 \cdot 11 + 17 \cdot 11 \cdot 6t$
นั่นคือ รากของระบบสมภาคที่กำหนดให้คือ $x \equiv 785 \pmod{1122}$

ตัวอย่าง 4.4.7

จงหาจำนวนเต็มบวกซึ่งเมื่อหารด้วย $5, 7, 11$ แล้วจะเหลือเศษ $2, 6, 5$ ตามลำดับ

วิธีทำ ให้ x เป็นจำนวนเต็มที่ต้องการ จากข้อกำหนดเราสามารถเขียนเป็นระบบสมภาคได้ดังนี้

$x \equiv 2 \pmod 5,\ x \equiv 6 \pmod 7,\ x \equiv 5 \pmod{11}$

ระบบสมภาคนี้มีรากเพราะว่า $(5, 7) = (5, 11),\ (7, 11) = 1$ จากสมภาคแรก เราได้

(1) $x = 2 + 5t_1$

แทน (1) ในสมภาคที่สอง จะได้

$2 + 5t_1 \equiv 6 \pmod 7$ หรือ $5t_1 \equiv 4 \pmod 7$

รากของสมภาคนี้คือ $t_1 \equiv 5 \pmod 7$

หรือคือ $t_1 = 5 + 7t_2$ แทนค่านี้ลงใน (1) จะได้

(2) $x = 27 + 35t_2$

แทน (2) ในสมภาคที่สาม จะได้

$27 + 35t_2 \equiv 5 \pmod{11}$

หรือ $35t_2 \equiv -22 \pmod{11}$

หา t_2 ได้ $t_2 \equiv 0 \pmod{11}$ หรือ $t_2 = 11t$

ดังนั้น $x = 27 + 35(11t)$

นั่นคือ $x \equiv 27 \pmod{385}$

จำนวนเต็มบวกที่ต้องการคือ 27 หรือ 412

ตัวอย่าง 4.4.8

จงหารากของระบบสมภาค $113x \equiv 4 \pmod 7, 5x \equiv 21 \pmod{13}, 6x \equiv 4 \pmod 8$

วิธีทำ เนื่องจาก $(113, 7) = 1, (5, 13) = 1$ และ $(6, 8) = 2$ ซึ่ง $2 \mid 4$

ดังนั้น ทุก ๆ สมภาคมีรากจากสมภาคแรก $113x \equiv 4 \pmod 7$

จะได้ $x \equiv 4 \pmod 7$ หรือ $x = 4 + 7t_1$ แทนค่านี้ลงในสมภาคที่สอง จะได้

$5(4 + 7t_1) \equiv 21 \pmod{13}$ หรือ $35t_1 \equiv 1 \pmod{13}$

เนื่องจาก $(35, 13) = 1$ สมภาคนี้มีราก หารากได้ $t_1 \equiv 3 \pmod{13}$

หรือ $t_1 = 3 + 13t_2$ แทน t_1 หาค่า x ได้ $x = 25 + 91t_2$

แทนค่า x ในสมภาคที่สาม จะได้

$$\begin{aligned} 6(25 + 91t_2) &\equiv 4 \pmod 8 \\ 546t_2 &\equiv -146 \pmod 8 \\ 2t_2 &\equiv 6 \pmod 8 \\ t_2 &\equiv 3 \pmod 4 \end{aligned}$$

หรือ $t_2 = 3 + 4t$ แทนค่า t_2 หา x ได้ $x = 25 + 91(3 + 4t) = 298 + 364t$

ดังนั้นรากร่วมของระบบสมภาคที่กำหนดมาให้คือ $x \equiv 298 \pmod{364}$

ตัวอย่าง 4.4.9

จงหาจำนวนเต็มบวกทั้งหมดที่หารด้วย $3, 4, 5$ แล้วเหลือเศษ 1 หรือ 2

วิธีทำ โจทย์ในตัวอย่างนี้สามารถแปลงให้อยู่ในรูปสมการสมภาคได้ กล่าวคือ

เราต้องการคำตอบของระบบสมภาค

$$\begin{aligned} x &\equiv 1 \text{ หรือ } 2 \pmod 3 \\ x &\equiv 1 \text{ หรือ } 2 \pmod 4 \\ x &\equiv 1 \text{ หรือ } 2 \pmod 5 \end{aligned}$$

ให้ $n_1 = 3, n_2 = 4, n_3 = 5$ ดังนั้น $n = 3 \cdot 4 \cdot 5 = 60$

และ $N_1 = \dfrac{60}{3} = 20,\ N_2 = \dfrac{60}{4} = 15,\ N_3 = \dfrac{60}{5} = 12$

และให้ $x_1,\ x_2,\ x_3$ เป็นคำตอบของสมภาค

$$\begin{aligned} 20x_1 &\equiv 1 \pmod 3 \\ 15x_2 &\equiv 1 \pmod 4 \\ 12x_3 &\equiv 1 \pmod 5 \end{aligned}$$

จะได้ว่า $x_1 = 2, x_2 = 3$ และ $x_3 = 3$

ดังนั้น คำตอบร่วมกันของสมการเชิงเส้น $x \equiv a_1 \pmod{n_i}$

คือ $x_0 = \displaystyle\sum_{j=1}^{3} N_j a_j x_j = (20)\,(a_1)\,(2) + (15)\,(a_2)\,(3) + (12)\,(a_3)\,(3)$

ซึ่งตารางต่อไปนี้จะแสดงคำตอบเมื่อกำหนดค่า $a_i = 3$ หรือ 2

a_1	a_2	a_3	$x \pmod{60}$
1	1	1	$40 + 345 + 36 \equiv 121 \equiv 1$
1	1	2	$40 + 45 + 72 \equiv 157 \equiv 37$
1	2	1	$40 + 90 + 36 \equiv 166 \equiv 46$
1	2	2	$40 + 90 + 72 \equiv 202 \equiv 22$
2	1	1	$80 + 45 + 36 \equiv 161 \equiv 41$
2	1	2	$80 + 45 + 72 \equiv 197 \equiv 17$
2	2	1	$80 + 90 + 36 \equiv 206 \equiv 26$
2	2	2	$80 + 90 + 72 \equiv 242 \equiv 2$

ตารางที่ 4.1 ตารางแสดงคำตอบเมื่อกำหนดค่า a_i

ดังนั้น จำนวนเต็มทั้งหมดที่หารด้วย $3, 4, 5$ แล้วเหลือเศษ 1 หรือ 2 คือ

$x \equiv 1,\ 2,\ 17,\ 22,\ 26,\ 37,\ 41$ หรือ $46 \pmod{60}$

ต่อไปเราจะพิจารณาการหาคำตอบของระบบสมการสมภาคเชิงเส้น ในกรณีทั่วไป ดังทฤษฎีบทต่อไปนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 149-150)

ทฤษฎีบท 4.4.2

ให้ m_1, m_2 เป็นจำนวนเต็มบวก และ b_1, b_2 เป็นจำนวนเต็มใด ๆ จะได้ว่าระบบสมภาค

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$

จะมีผลเฉลย ก็ต่อเมื่อ $(m_1, m_2) \mid (b_1 - b_2)$
และเมื่อมีผลเฉลยแล้ว จะมีผลเฉลยเพียงตัวเดียว มอดุโล $[m_1, m_2]$

การพิสูจน์ ให้ $d = (m_1, m_2)$ และ $m = [m_1, m_2]$
$(\Rightarrow)$ สมมติให้ระบบสมภาคมีผลเฉลยเป็น x_0
ดังนั้น $m_1 \mid (x_0 - b_1)$ และ $m_2 \mid (x_0 - b_2)$
ทำให้ได้ว่า $d \mid (x_0 - b_1)$ และ $d \mid (x_0 - b_2)$
ดังนั้น $d \mid [(x_0 - b_2) - (x_0 - b_1)]$ นั่นคือ $d \mid (b_1 - b_2)$
$(\Leftarrow)$ สมมติให้ $d \mid (b_1 - b_2)$ ผลเฉลยของ $x \equiv b_1 \pmod{m_1}$
คือ $x_1 = b_1 + km_1$ เมื่อ k เป็นจำนวนเต็ม
เราจะหา k ที่ทำให้ $b_1 + km_1$ เป็นผลเฉลยของ $x \equiv b_2 \pmod{m_2}$ ด้วย
ดังนั้น $b_1 + km_1 \equiv b_2 \pmod{m_2}$
นั่นคือหาค่า k จาก $km_1 \equiv (b_2 - b_1) \pmod{m_2}$ $\cdots (*)$
เนื่องจาก $d = (m_1, m_2) \mid (b_2 - b_1)$ จะได้ $(*)$ มีผลเฉลย ให้เป็น k_1
เราจึงได้ว่า $x_0 = b_1 + k_1 m_1$ เป็นผลเฉลยของระบบสมภาค
ต่อไปจะพิสูจน์ว่ามีผลเฉลยเพียงตัวเดียว มอดุโล $m = [m_1, m_2]$
ให้ x_1 เป็นผลเฉลยใด ๆ ของสมภาค
ดังนั้น $x_1 \equiv b_1 \pmod{m_1}$ และ $x_2 \equiv b_2 \pmod{m_2}$
ทำให้ได้ว่า $x_1 \equiv x_0 \pmod{m_1}$ และ $x_2 \equiv x_0 \pmod{m_2}$
จะได้ว่า $x_1 \equiv x_0 \pmod{m}$
นั่นคือ มีเพียงผลเฉลยเดียว มอดุโล m □

ตัวอย่าง 4.4.10

จงหาผลเฉลยของระบบสมภาค

$$x \equiv 9 \pmod{14}$$
$$x \equiv 6 \pmod{20}$$

วิธีทำ เพราะว่า $(14, 20) = 2$ และ $2 \nmid (9 - 6)$ ดังนั้นระบบสมการนี้ไม่มีผลเฉลย

ทฤษฎีบทต่อไปจะกล่าวถึงการมีผลเฉลยของระบบสมภาคที่มีมากกว่า 2 สมภาค (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 150)

ทฤษฎีบท 4.4.3

ให้ $m_1, m_2, \ldots, m_r$ เป็นจำนวนเต็มบวก และ $b_1, b_2, \ldots, b_r$ เป็นจำนวนเต็มใด ๆ

จะได้ว่าระบบสมภาค

$$\begin{aligned} x &\equiv b_1 \,(\mathrm{mod}\, m_1) \\ x &\equiv b_2 \,(\mathrm{mod}\, m_2) \\ x &\equiv b_3 \,(\mathrm{mod}\, m_3) \\ &\vdots \\ x &\equiv b_r \,(\mathrm{mod}\, m_r) \end{aligned}$$

จะมีผลเฉลย ก็ต่อเมื่อ $(m_i, m_j) \mid (b_i - b_j)$ สำหรับทุก $i, j \in \{1, 2, 3, \ldots, r\}$
และเมื่อมีผลเฉลยแล้ว จะมีผลเฉลยเพียงตัวเดียว มอดุโล $[m_1, m_2, \ldots, m_r]$

ตัวอย่าง 4.4.11

จงหาผลเฉลยของระบบสมภาค

$$(*) \cdots \begin{cases} x &\equiv 5 \,(\mathrm{mod}\, 6) \\ x &\equiv 17 \,(\mathrm{mod}\, 21) \\ x &\equiv 3 \,(\mathrm{mod}\, 28) \end{cases}$$

วิธีทำ เพราะว่า $(6, 21) = 3$ ซึ่ง $3 \mid (5 - 17), (21, 28) = 7$ ซึ่ง $7 \mid (17 - 3)$
และ $(6, 28) = 2$ ซึ่ง $2 \mid (5 - 3)$ ดังนั้นระบบสมภาคมีผลเฉลย
จาก $x \equiv 5 \,(\mathrm{mod}\, 6)$ มีผลเฉลยเดียวกับผลเฉลยของระบบสมภาค

$$\begin{aligned} x &\equiv 5 \equiv 1 \,(\mathrm{mod}\, 2) \\ x &\equiv 5 \equiv 2 \,(\mathrm{mod}\, 3) \end{aligned}$$

จาก $x \equiv 17 \,(\mathrm{mod}\, 21)$ มีผลเฉลยเดียวกับผลเฉลยของระบบสมภาค

$$\begin{aligned} x &\equiv 17 \equiv 2 \,(\mathrm{mod}\, 3) \\ x &\equiv 17 \equiv 3 \,(\mathrm{mod}\, 7) \end{aligned}$$

จาก $x \equiv 3 \,(\mathrm{mod}\, 28)$ มีผลเฉลยเดียวกับผลเฉลยของระบบสมภาค

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 3 \,(\mathrm{mod}\, 7) \end{aligned}$$

เนื่องจากผลเฉลยของสมภาค $x \equiv 3 \,(\mathrm{mod}\, 4)$
จะเป็นผลเฉลยเดียวกับผลเฉลยของสมภาค $x \equiv 1 \,(\mathrm{mod}\, 2)$
ดังนั้น ผลเฉลยของระบบสมภาค $(*)$ จะมีผลเฉลยเดียวกับผลเฉลยของระบบสมภาค

$$(**) \cdots \begin{cases} x &\equiv 2 \,(\mathrm{mod}\, 3) \\ x &\equiv 3 \,(\mathrm{mod}\, 4) \\ x &\equiv 3 \,(\mathrm{mod}\, 7) \end{cases}$$

โดยใช้ทฤษฎีบทเศษเหลือของจีน จะได้ผลเฉลยของระบบสมภาค $(**)$ คือ $x \equiv 59 \,(\mathrm{mod}\, 84)$

สมการสมภาคที่มีดีกรีมากกว่าหนึ่ง

ในการหาคำตอบของสมการสมภาคที่มีดีกรีมากกว่าหนึ่งนั้นมีความแตกต่างจากการหาคำตอบของสมการสมภาคเชิงเส้นมาก ทั้งนี้เพราะไม่มีวิธีการสำหรับที่จะสรุปได้เด่นชัดว่าสมการที่กำหนดให้จะมีคำตอบหรือไม่ และถ้ามีคำตอบจะมีจำนวนคำตอบเท่าไร

ให้ $x^2+x+7=0\,(\mathrm{mod}\,189) f(x)=c_mx^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0$ โดยที่ $c_i\in\mathbb{Z}$ และ $c_m\neq 0$ เราพบว่า ถ้า u เป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ และ $u\equiv v\,(\mathrm{mod}\,n)$ จะได้โดยทฤษฎีบท 4.2.1 ข้อ (2) ว่า v เป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$

จากข้อความข้างต้นเราพบว่า ถ้า n มีค่าน้อย เราสามารถแทนค่า x ในสมการด้วย $0,1,2,\ldots n-1$ เราก็จะได้คำตอบของสมการดังกล่าว

จากการประยุกต์ทฤษฎีบท 4.1.2 ข้อ 7. เราพบว่า ถ้า $d\mid n$ และ $d>0$ และ ถ้า u เป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ แล้ว u จะเป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ ดังนั้น ถ้า

$$n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\ldots p_r^{\alpha_r}$$

เป็นการเขียนแทน n ในรูปแบบบัญญัติ และ u เป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ แล้ว u จะเป็นคำตอบของสมการ $f(x)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ สำหรับทุก $i=1,2\ldots,r$ จากทฤษฎีบทเศษเหลือของจีน เราสามารถแสดงได้ว่าถ้าระบบสมการ $f(x)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ มีคำตอบ สำหรับทุก $i=1,2\ldots,r$ จะได้ว่าสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ จะมีคำตอบ ฉะนั้นเราจึงได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.4.4

ให้ $f(x)=c_mx^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0$ โดยที่ $c_i\in\mathbb{Z}$ และ $c_m\neq 0$ และ $n\in\mathbb{N}$ ซึ่ง $n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\ldots p_r^{\alpha_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ จะได้ว่าสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ มีคำตอบ ก็ต่อเมื่อสมการ $f(x)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ มีคำตอบ สำหรับทุก $i=1,2,\ldots,r$

การพิสูจน์ ให้ $n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\ldots p_r^{\alpha_r}$ เป็นการเขียนแทน n ในรูปแบบบัญญัติ
และ $f(x)=c_mx^m+c_{m-1}x^{m-1}+\ldots+c_1x+c_0$ โดยที่ $c_i\in\mathbb{Z}$ และ $c_m\neq 0$
$(\Rightarrow)$ สมมติว่าสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ มีคำตอบ จะได้ว่ามี $b_0\in\mathbb{Z}$
ซึ่ง $f\,(b_0)\equiv 0\ (\mathrm{mod}\,p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})$
แสดงว่า $f\,(b_0)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ สำหรับทุก $i=1,2,\ldots,r$
นั่นคือสมการ $f(x)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ สำหรับทุก $i=1,2,\ldots,r$
$(\Leftarrow)$ สมมติว่าสมการ $f(x)\equiv 0\ (\mathrm{mod}\,p_i^{\alpha_i})$ สำหรับทุก $i=1,2,\ldots,r$
จะได้ว่ามี $a_i\in\mathbb{Z}$ ซึ่ง $f\,(a_i)\equiv 0\ (\mathrm{mod}\,n_i)$ สำหรับทุก $i=1,2,\ldots,r$
และเมื่อ $n_i=p_i^{\alpha_i}$ โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า ระบบสมการ
$x\equiv a_i\,(\mathrm{mod}\,n_i)$ มีคำตอบ $\displaystyle\sum_{j=1}^{r}\frac{n}{n_j}b_ja_j$
เมื่อ b_j เป็นคำตอบของสมการ $\dfrac{n}{n_j}x\equiv 1\ (\mathrm{mod}\,n_j)$
จะเห็นได้ชัดว่า u เป็นคำตอบของสมการ $f(x)\equiv 0\,(\mathrm{mod}\,n)$ □

ตัวอย่าง 4.4.12

จงหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{15}$

วิธีทำ เพราะว่า $15 = 3 \cdot 5$ ดังนั้นการหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{15}$ ก็จะเหมือนกับการหาคำตอบของระบบสมการ

$$\begin{aligned} x^2 + x + 7 &\equiv 0 \pmod{3} \quad \cdots (1) \\ x^2 + x + 7 &\equiv 0 \pmod{5} \quad \cdots (2) \end{aligned}$$

จากการแทนค่า $x = 0, 1, 2$ ใน (1) พบว่า $x \equiv 1 \pmod{3}$ เป็นคำตอบของ (1)
จากการแทนค่า $x = 0, 1, 2, 3, 4$ ใน (2) พบว่า สมการ (2) ไม่มีคำตอบ
ดังนั้น สมการ $x^2 + x + 7 \equiv 0 \pmod{15}$ ไม่มีคำตอบ

ตัวอย่าง 4.4.13

จงหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$

วิธีทำ เพราะว่า $189 = 3^3 \cdot 7$ ดังนั้นการหาคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ ก็เหมือนกับการหาคำตอบของระบบสมการ

$$\begin{aligned} x^2 + x + 7 &\equiv 0 \pmod{3^3} \quad \cdots (1) \\ x^2 + x + 7 &\equiv 0 \pmod{7} \quad \cdots (2) \end{aligned}$$

เพราะว่าคำตอบของสมการ (1) คือ $x \equiv 4, 13, 22 \pmod{3^3}$
และคำตอบของสมการ (2) คือ $x \equiv 0, 6 \pmod{7}$
ฉะนั้นคือคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ จะมี 6 คำตอบ
โดยใช้ทฤษฎีบทเศษเหลือของจีน จะได้ $b_1 \equiv 4 \pmod{3^3}, b_2 \equiv 6 \pmod{7}$
และคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$ สามารถ เขียนได้ในรูป

$$u \equiv \frac{189}{27}(4)a_1 + \frac{189}{7}(6)a_2 \pmod{189}$$

โดยที่ $a_1 = 4, 13, 22$ และ $a_2 = 0, 6$
และจะได้ $u \equiv 28a_1 + 162a_2 \pmod{189}$
ดังนั้นจากการแทนค่า a_1 และ a_2 ในทุก ๆ กรณีจะได้

$$\begin{aligned} u &\equiv 28(4) + 162(0) \equiv 112 \pmod{189} \\ u &\equiv 28(4) + 162(6) \equiv 139 \pmod{189} \\ u &\equiv 28(13) + 162(0) \equiv 175 \pmod{189} \\ u &\equiv 28(13) + 162(6) \equiv 13 \pmod{189} \\ u &\equiv 28(22) + 162(0) \equiv 49 \pmod{189} \\ u &\equiv 28(22) + 162(6) \equiv 76 \pmod{189} \end{aligned}$$

เพราะฉะนั้นคำตอบของสมการ $x^2 + x + 7 \equiv 0 \pmod{189}$
คือ $x = 13, 49, 76, 112, 139, 175 \pmod{189}$

4.5 ทฤษฎีบทของแฟร์มาต์และออยเลอร์

ทฤษฎีบทของแฟร์มาต์ที่จะศึกษาในหัวข้อนี้มีใจความว่า ถ้า p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มใด ๆ ที่หารด้วย p ไม่ลงตัว แล้ว p จะหาร $a^{p-1}-1$ ลงตัว ทฤษฎีบทดังกล่าวนี้ แฟร์มาต์เขียนถึงเบสซี (Bessy ค.ศ. 1605-1670) ในปี ค.ศ. 1640 ซึ่งเขาไม่ได้พิสูจน์อะไรเป็นหลักฐานไว้ จนเวลาผ่านไปเกือบ 100 ปี ออยเลอร์ได้พบวิธีพิสูจน์และได้ตีพิมพ์เป็นครั้งแรก ในปี ค.ศ. 1736

ก่อนการศึกษาทฤษฎีบทของแฟร์มาต์ และออยเลอร์นั้น พื้นฐานที่จำเป็นอย่างหนึ่งคือ เราจะต้องรู้จักระบบส่วนตกค้างบริบูรณ์ และระบบส่วนตกค้าง ลดทอน และต่อไปจะกล่าวถึงระบบส่วนตกค้างบริบูรณ์มอดุโล n และชั้นส่วนตกค้าง ดังบทนิยามต่อไปนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2547 : 134, จิราภา ลิ้มบุพศิริพร. 2555 : 97, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 117)

บทนิยาม 4.5.1

ถ้า $a \equiv b \pmod{n}$ จะเรียก b ว่าเป็น**ส่วนตกค้าง** (residue) ของ a มอดุโล n และเรียกเซตของจำนวนเต็ม $\{a_1, a_2, \ldots, a_n\}$ ว่าเป็น**ระบบส่วนตกค้างบริบูรณ์** (complete residue system) มอดุโล n ก็ต่อเมื่อ ทุก ๆ จำนวนเต็ม a จะมี a_i เพียงตัวเดียวที่ทำให้ $a \equiv a_i \pmod{n}$ ชั้นสมมูลของ a_i คือ $\{a \mid a$ เป็นจำนวนเต็มและ $a \equiv a_i \pmod{n}\}$ เรียกว่า**ชั้นส่วนตกค้าง** (residue class) ของ a_i มอดุโล n

หมายเหตุ ให้ $x, q, r, n \in \mathbb{Z}$ โดยที่ $n \in \mathbb{N}$ และ $x = nq + r$ เราพบว่า $x \equiv r \pmod{n}$ และจะได้ว่า r เป็นส่วนที่ตกค้างของ x มอดุโล n แต่ถ้าเรากำหนด $x = nq + r$ โดยที่ $0 \leq r < n$ เราจะเรียก r ว่า**ส่วนตกค้างที่ไม่เป็นลบค่าน้อยสุดของ** x มอดุโล n ดังนั้น $\{0, 1, 2, \ldots, n-1\}$ เรียกว่า**ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นลบค่าน้อยสุด** (least non-negative residue system) มอดุโล n นั่นคือ จะมี $r \in \{0, 1, 2, \ldots, n-1\}$ เพียงจำนวนเดียวเท่านั้นที่เป็นส่วนตกค้างของ x มอดุโล n

จากบทนิยามเราพบว่า

1. $\{0, 1, 2, \ldots, n-1\}$ และ $\{1, 2, 3, \ldots, n\}$ ต่างก็เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
2. ถ้า $\{a_1, a_2, \ldots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $c \in \mathbb{Z}$ แล้ว $\{a_1 + c, a_2 + c, \ldots, a_n + c\}$ จะเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
3. $\{a_1, a_2, \ldots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n ก็ต่อเมื่อ ทุก ๆ a_i, a_j ถ้า $a_i \equiv a_j \pmod{n}$ แล้ว $a_i = a_j$
4. ถ้า $\{a_1, a_2, \ldots, a_n\}$ และ $\{b_1, b_2, \ldots, b_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แล้ว สำหรับทุก ๆ a_i จะมี b_j เพียงตัวเดียวที่ทำให้ $a_i \equiv b_j \pmod{n}$

ตัวอย่าง 4.5.1

(1) $\{-1, 5, 6, 7, 8\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5
เพราะว่า $-1 \equiv 4 \pmod{5}, 5 \equiv 0 \pmod{5}, 6 \equiv 1 \pmod{5}, 7 \equiv 2 \pmod{5}$ และ $8 \equiv 3 \pmod{5}$

(2) $\{8, -2, 6, 12, 1\}$ ไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5
เพราะว่า $8 \equiv -2 \pmod{5}$

(3) $\{-11, -3, 18, 16, 22\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5

เพราะว่า $-11 \equiv 4 \pmod 5, -3 \equiv 2 \pmod 5, 18 \equiv 3 \pmod 5, 16 \equiv 1 \pmod 5$
และ $22 \equiv 2 \pmod 5$

ตัวอย่าง 4.5.2

(1) $\{7, 4, -2, 8, -4, 9, 20\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 7
เพราะว่า $7 \equiv 0 \pmod 7, 8 \equiv 1 \pmod 7, 9 \equiv 2 \pmod 7, -4 \equiv 3 \pmod 7,$
$4 \equiv 4 \pmod 7, -2 \equiv 5 \pmod 7$ และ $20 \equiv 6 \pmod 7$
(2) $\{0, 1, 2, 3, 4, 5\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 6
จะได้ว่า $\{2, 3, 4, 5, 6, 7\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 6
แต่ $\{0, 2, 4, 6, 8, 10\}$ ไม่เป็นระบบส่วนตกค้างมอดุโล 6 เพราะว่า $2 \equiv 8 \pmod 6$

จากตัวอย่างข้างต้น ทำให้สรุปได้ว่า ถ้า $\{a_1, a_2, \ldots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $c \in \mathbb{Z}$ แล้ว $\{ca_1, ca_2, \ldots, ca_n\}$ อาจไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

ทฤษฎีบทต่อไปนี้ จะแสดงเงื่อนไขที่จำเป็นและเพียงพอที่จะทำให้ $\{ca_1, ca_2, \ldots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูณ์มอดุโล n

ทฤษฎีบท 4.5.1

ให้ $\{a_1, a_2, \ldots, a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ $(c, n) = 1$
จะได้ว่า $\{ca_1, ca_2, \ldots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

การพิสูจน์ สมมติว่า $\{ca_1, ca_2, \ldots, ca_n\}$ ไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
แสดงว่าจะมี $i \neq j$ ซึ่ง $ca_i \equiv ca_j (\mathrm{mod} n)$ เนื่องจาก $(c, n) = 1$
ดังนั้น $a_i \equiv a_j \pmod n$ เมื่อ $i \neq j$ ขัดแย้งกับสิ่งที่กำหนดให้
นั่นคือ $\{ca_1, ca_2, \ldots, ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n □

บทนิยาม 4.5.2

ระบบส่วนตกค้างลดทอน (reduced residue system) มอดุโล m คือเซตของจำนวนเต็มในระบบส่วนตกค้างบริบูรณ์ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, \ldots, m-1\}$ ซึ่งคือ $\{k \mid 0 \leq k \leq m$ ที่ $(k, m) = 1\}$ เรียกว่า **ระบบส่วนตกค้างลดทอนที่ไม่เป็นลบน้อยสุด** (least non-negative reduced residue system)

จากบทนิยามเราพบว่า
(1) เซตของจำนวนเต็ม r_i เป็นระบบส่วนตกค้างลดทอนมอดุโล n ก็ต่อเมื่อ
(1.1) $(r_i, n) = 1$ ทุก ๆ r_i
(1.2) ถ้า $i \neq j$ แล้ว $r_i \not\equiv r_j \pmod n$
(1.3) ถ้า x เป็นจำนวนเต็มที่ $(x, n) = 1$ แล้วมี r_i ที่ $x \equiv r_i \pmod n$
(2) ระบบส่วนตกค้างลดทอนมอดุโล n ทุกระบบจะมีจำนวนสมาชิกเท่ากัน

ตัวอย่าง 4.5.3

(1) ระบบส่วนตกค้างลดทอนมอดุโล 8
ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0,1,2,3,4,5,6,7\}$ คือ $\{1,3,5,7\}$
และที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{8,-7,2,11,4,5,14,15\}$ คือ $\{-7,11,5,15\}$

(2) ให้ p เป็นจำนวนเฉพาะ ระบบส่วนตกค้างลดทอนมอดุโล p
ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0,1,2,\ldots,p-1\}$ คือ $\{1,2,\ldots,p-1\}$

บทนิยาม 4.5.3

ให้ $\phi(m)$ เป็นจำนวนสมาชิกในระบบส่วนตกค้างลดทอนมอดุโล m นั่นคือ

$$\phi(m) = \text{จำนวนของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ } m$$

และเป็นจำนวนเฉพาะสัมพัทธ์กับ m
จะเห็นว่า $\phi(m)$ สามารถหาค่าได้ทุกค่าของจำนวนเต็มบวก m
และเรียกว่า ฟังก์ชันออยเลอร์-ฟี (Euler-Phi function)

ตัวอย่าง 4.5.4

(1) $\phi(12) = 4$ เพราะมีจำนวนเต็มบวก 4 จำนวนที่มีค่าน้อยกว่าหรือเท่ากับ 12
และเป็นจำนวนเฉพาะสัมพัทธ์กับ 12 คือ $1,5,7$ และ 13

(2) $\phi(14) = 6$ เพราะมีจำนวนเต็มบวก 6 จำนวนที่มีค่าน้อยกว่าหรือเท่ากับ 14
และเป็นจำนวนเฉพาะสัมพัทธ์กับ 14 คือ $1,3,5,9,11$ และ 13

(3) ถ้า p เป็นจำนวนเฉพาะแล้ว จำนวนเต็มบวกที่มีค่าน้อยกว่า p
และเป็นจำนวนเฉพาะสัมพัทธ์กับ p มี $p-1$ ตัว ดังนั้น $\phi(p) = p-1$

ทฤษฎีบท 4.5.2

ถ้า $\{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$ เป็นเซตของจำนวนเต็มซึ่งทุก ๆ $i, (a_i, n) = 1$ และทุก ๆ $i \neq j$, $a_i \equiv a_j \pmod{n}$ แล้ว $\{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n

การพิสูจน์ ให้ r_i เป็นเศษจากการหาร a_i ด้วย n
ดังนั้น $a_i \equiv r_i \pmod{n}$ และ $(r_i, n) = 1$
แสดงว่า $\{r_1, r_2, r_3, \ldots, r_{\phi(n)}\} \subseteq \{0,1,2,\ldots,n-1\}$ ซึ่งมีสมาชิก $\phi(n)$ ตัว
ดังนั้น $\{r_1, r_2, r_3, \ldots, r_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n
ที่ไม่เป็นลบค่าน้อยสุด ให้ a เป็นจำนวนเต็ม ใด $(a, n) = 1$
และให้ r เป็นเศษเหลือจากการหาร a ด้วย n
ทำให้ได้ว่า $a \equiv r \pmod{n}$ และ $(r, n) = 1$
ดังนั้นจะมี i ที่ $r = r_i$ นั่นคือ $a \equiv r = r_i \equiv a_i \pmod{n}$
สรุปได้ว่า $\{a_1, a_2, a_3, \ldots, a_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n □

ทฤษฎีบท 4.5.3

ให้ $(a,n)=1$ และให้ $\{r_1,r_2,r_3,\ldots,r_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n จะได้ว่า $\{ar_1,ar_2,ar_3,\ldots,ar_{\phi(n)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n

การพิสูจน์ เนื่องจาก $(a,n)=1$ และ $(r_i,n)=1$ ดังนั้น $(ar_i,n)=1$
เนื่องจาก $ar_1,ar_2,ar_3,\ldots,ar_{\phi(n)}$ มี $\phi(n)$ ตัว
ดังนั้น เราเพียงแค่แสดงว่า แต่ละคู่จะไม่สมภาคกัน สมมติว่า $ar_i\equiv ar_j\pmod n$
เนื่องจาก $(a,n)=1$ ดังนั้นโดยทฤษฎีบท 4.1.3 ข้อ 3.
จะได้ว่า $r_i\equiv r_j\pmod n$ ทำให้ได้ว่า $i=j$ □

ทฤษฎีบทต่อไปนี้ จะกล่าวถึงทฤษฎีบทของออยเลอร์ (จิราภา ลิ้มบุพศิริพร. 2555 : 135, สมใจ จิตพิทักษ์. 2547 : 144, Rosen K.M. 2005 : 235)

ทฤษฎีบท 4.5.4 : ทฤษฎีบทของออยเลอร์ (Euler's Theorem)

ถ้า $a\in\mathbb{Z}$ และ $n\in\mathbb{N}$ ซึ่ง $(a,n)=1$ แล้ว $a^{\phi(n)}\equiv 1\pmod n$

การพิสูจน์ การพิสูจน์ ให้ $r_1,r_2,r_3,\ldots,r_{\phi(n)}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n โดยทฤษฎีบท 4.5.2 ได้ว่า $ar_1,ar_2,ar_3,\ldots,ar_{\phi(n)}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล n ด้วย
นั่นคือ ทุก ๆ r_i จะมี ar_j ซึ่ง $ar_j\equiv r_i\pmod n$
ดังนั้น $ar_1\cdot ar_2\cdot ar_3\cdots ar_{\phi(n)}\equiv r_1\cdot r_2\cdot r_3\cdots r_{\phi(n)}\pmod n$
แสดงว่า $a^{\phi(n)}\left[r_1\cdot r_2\cdots r_{\phi(n)}\right]\equiv r_1\cdot r_2\cdots r_{\phi(n)}\pmod n$
เนื่องจากแต่ละ $(r_i,n)=1$ ดังนั้น $\left(r_1\cdot r_2\cdots r_{\phi(n)},n\right)=1$
โดยทฤษฎีบท 4.1.3 ข้อ 3. จะได้ว่า $a^{\phi(n)}\equiv 1\pmod n$ □

บทแทรก 4.5.1 : ทฤษฎีบทของแฟร์มาต์ (Fermats Little Theorem)

ให้ p เป็นจำนวนเฉพาะ และ a เป็น จำนวนเต็มที่ $p\nmid a$ จะได้ว่า $a^{p-1}\equiv 1\pmod p$

การพิสูจน์ จาก $p\nmid a$ และ p เป็นจำนวนเฉพาะ จะได้ $(a,p)=1$
และ $\phi(p)=p-1$
ดังนั้น $a^{p-1}\equiv 1\pmod p$ □

บทแทรก 4.5.2

ให้ p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มใด ๆ จะได้ว่า $a^p\equiv a\pmod p$

การพิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ และ p เป็นจำนวนเฉพาะ
กรณีที่ 1 $p\mid a$ จะได้ว่า $a\equiv 0\pmod p$ และ $a^p\equiv 0\pmod p$
ดังนั้น $a^p\equiv a\pmod p$
กรณีที่ 2 $p\nmid a$ จะได้ว่า $a^{p-1}\equiv 1\pmod p$
ดังนั้น $a^p\equiv a\pmod p$ □

ตัวอย่าง 4.5.5

จงหาเศษที่เกิดจากการหาร 3^{1000} ด้วย 17

วิธีทำ จากทฤษฎีบทของแฟร์มาต์จะได้ว่า $3^{16} \equiv 1 \pmod{17}$
ดังนั้น $3^{1000} = (3^{16})^{62} \cdot 3^8 \equiv 1^{62} \cdot 3^4 \cdot 3^4 \equiv (-4)(-4) = 16 \pmod{17}$
นั่นคือ เศษที่เกิดจากการหาร 3^{1000} ด้วย 17 คือ 16

ตัวอย่าง 4.5.6

จงพิจารณาว่า $2^{117} - 2$ หารด้วย 117 ลงตัวหรือไม่

วิธีทำ เนื่องจาก $2^7 = 128 \equiv 11 \pmod{117}$
จะได้ว่า $(2^7)^{16} \cdot 2^5 \equiv (11)^{16} \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$
แต่ $2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$
ดังนั้น $2^{117} \equiv 44 \pmod{117}$
แสดงว่า $2^{117} - 2$ หารด้วย 117 ไม่ลงตัว

ตัวอย่าง 4.5.7

จงแสดงว่า $3^{256} \equiv 21 \pmod{100}$

วิธีทำ เพราะว่า $3^{\phi(100)} \equiv 1 \pmod{100}$ แสดงว่า $3^{40} \equiv 1 \pmod{100}$
จะได้ว่า $(3^{40})^6 \cdot 3^{16} \equiv 1^{16} \cdot 3^{16} \pmod{100}$
และ $3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (61)^2 \equiv 21 \pmod{100}$
ดังนั้น $3^{256} \equiv 21 \pmod{100}$

ตัวอย่าง 4.5.8

จงหาเลขโดดสามหลักสุดท้าย ของ 7^{1000}

วิธีทำ เพราะว่า $7^{\phi(1000)} \equiv 1 \pmod{1000}$ แสดงว่า $7^{400} \equiv 1 \pmod{1000}$
และ $7^{1000} = (7^{400})^{25} \equiv 1^{25} = 1 \pmod{1000}$
ดังนั้นเลขโดดสามหลักสุดท้ายของ 7^{1000} คือ 001

ตัวอย่าง 4.5.9

จงหาค่า a เมื่อ $102^{1999} + 103^{1999} \equiv a \pmod{1999}$ โดยที่ $0 \leq a < 1999$

วิธีทำ เพราะว่า 1999 เป็นจำนวนเฉพาะ จะได้ว่า $102^{1998} \equiv 1 \pmod{1999}$
และ $103^{1998} \equiv 1 \pmod{1999}$
ดังนั้น $102^{1999} \equiv 102 \pmod{1999}$ และ $103^{1999} \equiv 103 \pmod{1999}$
แสดงว่า $102^{1999} + 103^{1999} \equiv 102 + 103 \pmod{1999}$ นั่นคือ $a = 205$

ทฤษฎีบท 4.5.5

ถ้า p และ q เป็นจำนวนเฉพาะที่ต่างกันซึ่ง $a^q \equiv a \pmod{p}$ และ $a^p \equiv a \pmod{q}$
แล้ว $a^{pq} \equiv a \pmod{pq}$

การพิสูจน์ ให้ p และ q เป็นจำนวนเฉพาะที่ต่างกัน และ $a \in \mathbb{Z}$
จะได้ว่า $a^q \equiv a \pmod{p}$ และ $a^p \equiv a \pmod{q}$

เนื่องจาก $a^q \equiv a \pmod{p}$ และ $a^p \equiv a \pmod{q}$
ดังนั้น $(a^q)^p \equiv a^p \pmod{p}$ และ $(a^p)^q \equiv a^q \pmod{q}$
แสดงว่า $a^{pq} \equiv a^p \equiv a \pmod{p}$ และ $a^{pq} \equiv a^q \equiv a \pmod{q}$
โดยทฤษฎีบท 4.1.4 จะได้ว่า $a^{pq} \equiv a \pmod{pq}$ □

ตัวอย่าง 4.5.10

จงแสดงว่า $2^{340} \equiv 1 \pmod{341}$

วิธีทำ เนื่องจาก $341 = 11 \cdot 13$ และ $2^{10} = 1024 = 31 \cdot 33 + 1$
จะได้ว่า $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$
และ $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$
ดังนั้น $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ นั่นคือ $2^{341} \equiv 2 \pmod{341}$
ทำให้ $2^{340} \equiv 1 \pmod{341}$

ทฤษฎีบท 4.5.6

ให้ p เป็นจำนวนเฉพาะ จะได้ว่า $x^2 \equiv 1 \pmod{p}$ ก็ต่อเมื่อ $x \equiv 1$ หรือ $-1 \pmod{p}$

การพิสูจน์ ($\Rightarrow$) สมมติว่า $x^2 \equiv 1 \pmod{p}$ ดังนั้น $p \mid (x^2 - 1)$
นั่นคือ $p \mid [(x-1)(x+1)]$
ทำให้ได้ว่า $p \mid (x-1)$ หรือ $p \mid (x+1)$
นั่นคือ $x \equiv 1$ หรือ $-1 \pmod{p}$
($\Leftarrow$) สมมติว่า $x \equiv 1$ หรือ $-1 \pmod{p}$
ดังนั้น $p \mid (x-1)$ หรือ $p \mid (x+1)$
จะได้ว่า $p \mid [(x-1)(x+1)]$ นั่นคือ $p \mid (x^2 - 1)$
นั่นคือ $x^2 \equiv 1 \pmod{p}$ □

หมายเหตุ ในทฤษฎีบท 4.5.6 ถ้า p ไม่เป็นจำนวนเฉพาะข้อความนี้จะไม่เป็นจริง เช่น พิจารณา $x \equiv 3 \pmod{8}$ จะได้ว่า $x^2 \equiv 1 \pmod{8}$ แต่ $x \not\equiv 1$ และ $x \not\equiv -1 \pmod{8}$ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2547 : 158)

ทฤษฎีบทต่อไปเป็นข้อคาดเดาของวิลสัน แต่สามารถพิสูจน์ได้โดยลากรองจ์ (Rosen K. H. 2005 : 215-216, David M. Burton. 2011 : 94)

ทฤษฎีบท 4.5.7 : ทฤษฎีบทของวิลสัน (Wilsons Theorem)

ให้ p เป็นจำนวนเฉพาะ จะได้ว่า $(p-1)! \equiv -1 \pmod{p}$

การพิสูจน์ ถ้า $p = 2$ หรือ 3 จะเห็นได้ชัดว่า $(p-1)! \equiv -1 \pmod{p}$
สำหรับ $p \geq 5$ ให้ $a \in \mathbb{Z}$ ซึ่ง $1 \leq a \leq p-1$ ดังนั้น $(a, p) = 1$
จะมีจำนวนเต็ม a' ซึ่ง $1 \leq a' \leq p-1$
ที่ทำให้ $aa' \equiv 1 \pmod{p}$ ถ้า $a = a'$ จะได้ว่า $a^2 \equiv 1 \pmod{p}$
ดังนั้นโดยทฤษฎีบท 4.5.6 จะได้ว่า $a \equiv 1$ หรือ $-1 \pmod{p}$
นั่นคือ $a = 1$ หรือ $p-1$ ทำให้ได้ว่า

ทุก a ที่ $2 \leq a \leq p-2$ มี a' เพียงตัวเดียวที่ $2 \leq a' \leq p-2$
และทำให้ $aa' \equiv 1 \pmod{p}$ นั่นคือ $(2)(3)(4)\cdots(p-2)$
จะจับคู่กันได้ $\frac{p-3}{2}$ คู่
ที่ผลเฉลยของแต่ละคู่จะสมภาคกับ 1 มอดุโล p
เพราะฉะนั้น $(2)(3)(4)\cdots(p-2) \equiv 1 \pmod{p}$ ซึ่งทำให้
$(p-1)! = (1)(2)(3)(4)\cdots(p-2)(p-1) \equiv -1 \pmod{p}$ □

ตัวอย่าง 4.5.11

จงหาเศษที่เกิดจากการหาร 15! ด้วย 17

วิธีทำ เนื่องจาก 17 เป็นจำนวนเฉพาะ จากทฤษฎีบทของวิลสัน
จะได้ว่า $16! = 16 \cdot 15! \equiv -1 \pmod{17}$
เนื่องจาก $16 \equiv -1 \pmod{17}$ ดังนั้น $16 \cdot 15! \equiv 16 \pmod{17}$
จาก $(16, 17) = 1$ โดยทฤษฎีบท 4.1.3 ข้อ 3.
จะได้ว่า $15! \equiv 1 \pmod{17}$
นั่นคือ เศษที่เกิดจากการหาร 15! ด้วย 17 คือ 1

ตัวอย่าง 4.5.12

จงแสดงว่า $18! \equiv -1 \pmod{437}$

วิธีทำ จาก $437 = 19 \cdot 23$ ซึ่ง 19 และ 23 เป็นจำนวนเฉพาะ
โดยทฤษฎีบทของวิลสัน จะได้ว่า $18! \equiv -1 \pmod{19}$ และ $22! \equiv -1 \pmod{23}$
เนื่องจาก $22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23}$
และ $-1 \equiv -22 \cdot 21 \cdot 20 \cdot 19 \pmod{23}$
ดังนั้น $22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -22 \cdot 21 \cdot 20 \cdot 19 \pmod{23}$
จาก $(22 \cdot 21 \cdot 20 \cdot 19, 23) = 1$ โดยทฤษฎีบท 4.1.3 ข้อ 3.
จะได้ว่า $18! \equiv -1 \pmod{23}$
ดังนั้นจาก $18! \equiv -1 \pmod{19}$ และ $18! \equiv -1 \pmod{23}$ โดยทฤษฎีบท 4.1.4
จะได้ว่า $18! \equiv -1 \pmod{437}$

ทฤษฎีบท 4.5.8

ให้ p เป็นจำนวนเฉพาะ จะได้ว่า $x^2 \equiv -1 \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $p = 2$ หรือ $p \equiv 1 \pmod{4}$

การพิสูจน์ ($\Rightarrow$) ให้ a เป็นผลเฉลยของ $x^2 \equiv -1 \pmod{p}$ และ p เป็นจำนวนเฉพาะคี่
นั่นคือ $a^2 \equiv -1 \pmod{p}$
ดังนั้น $p \nmid a$ และ $1 \equiv a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$
เนื่องจาก $\frac{p-1}{2}$ เป็นจำนวนเต็ม ดังนั้น $(-1)^{\frac{p-1}{2}} = 1$ หรือ -1
แต่ $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ และ $-1 \not\equiv 1 \pmod{p}$
ดังนั้น $(-1)^{\frac{p-1}{2}} = 1$ ทำให้ได้ว่า $\frac{p-1}{2}$ เป็นจำนวนเต็มคู่

นั่นคือ $4 \mid (p-1)$ แสดงว่า $p \equiv 1 \pmod 4$

($\Leftarrow$) ให้ $p \equiv 1 \pmod 4$ ดังนั้น $\dfrac{p-1}{2}$ เป็นจำนวนเต็มคู่

จากทฤษฎีบทของวิลสันจะได้ว่า

$$\begin{aligned}
-1 &\equiv (1)(2)\cdots\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) = (p-1)! \pmod p \\
&\equiv \prod_{j-1}^{n} j(p-j) \pmod p \text{ เมื่อ } n = \frac{p-1}{2} \\
&\equiv \prod_{j-1}^{n} \left(-j^2\right) = (-1)^{\frac{p-1}{2}} \prod_{j-1}^{n} j^2 = (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p \\
&\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p
\end{aligned}$$

แสดงว่า สมการ $x^2 \equiv -1 \pmod p$ มีผลเฉลยและผลเฉลยคือ $x = \left(\dfrac{p-1}{2}\right)!$

จากทฤษฎีบทของวิลสัน จะได้ว่ามีจำนวนประกอบไม่จำกัดในรูป $n! + 1$ □

สรุปท้ายบท

ในบทที่ 4 มุ่งเน้นให้นักศึกษาเข้าใจนิยามและสมบัติพื้นฐานของสมภาค และได้แสดงการพิสูจน์ทฤษฎีบทต่าง ๆ ที่เกี่ยวกับสมภาคโดยมีการยกตัวอย่างประกอบให้เข้าใจได้ง่ายขึ้น นอกจากนี้ยังได้พูดถึงสิ่งสำคัญอื่น ๆ อีกเช่น สมภาคเชิงเส้น ทฤษฎีบทเศษเหลือของจีน และทฤษฎีบทของแฟร์มาต์และออยเลอร์ซึ่งล้วนแต่เป็นเนื้อหาสำคัญของวิชาทฤษฎีจำนวนที่นักศึกษาต้องรู้เพื่อใช้ในการศึกษาทฤษฎีจำนวนที่สูงขึ้น

แบบฝึกหัดท้ายบทที่ 4

1. จงหาเศษที่เกิดจากการหาร 3^{10} ด้วย 51 และการหาร 21^{10} ด้วย 51

2. จงแสดงว่า ถ้า $(n, 7) = 1$ แล้ว $n^6 - 1$ หารด้วย 7 ลงตัว

3. จงแสดงว่า ถ้า $n^7 - n$ หารด้วย 42 ลงตัว สำหรับทุกจำนวนเต็มบวก n

4. จงหาเลขโดดหลักสุดท้ายของ 3^{400}

   (ข้อเสนอแนะ ใช้ $3^4 \equiv 1 \pmod 5$ และ $3^4 \equiv 1 \pmod 2$)

5. จงหาเลขโดดสองหลักสุดท้ายของ 3^{4000}

   (ข้อเสนอแนะ ใช้ $3^{20} \equiv 1 \pmod{25}$ และ $3^2 \equiv 1 \pmod 4$
   ดังนั้น $3^{20} \equiv 1 \pmod 4$ ซึ่งจะได้ $3^{20} \equiv 1 \pmod{100}$)

6. ให้ p เป็นจำนวนเฉพาะซึ่ง $n < p < 2n$ จงพิสูจน์ว่า $\binom{2n}{n} \equiv 0 \pmod p$

7. จงพิสูจน์ว่า สำหรับจำนวนเต็มบวกคี่ n ใดๆ $1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod n$ ข้อความนี้ยังเป็นจริงหรือไม่ ถ้า n เป็นจำนวนเต็มบวกคู่

8. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก $n, 4^n \equiv 1 + 3n \pmod 9$

9. ให้ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่าสำหรับทุกๆ จำนวนเต็ม $x, x^2 \equiv x \pmod p$ ก็ต่อเมื่อ
   $x \equiv 0$ หรือ $1 \pmod p$

10. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก $n, 11 \mid (2^{4n+3} + 5^{n+2})$ โดยไม่ใช้หลักอุปนัยเชิงคณิตศาสตร์

11. จงพิสูจน์ว่า ถ้า $a \equiv 2 \pmod 4$ แล้ว จะไม่มีจำนวนเต็ม b และ $m > 1$ ซึ่ง $a = b^m$

12. ให้ $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ โดยที่ a_i เป็นจำนวนเต็มที่ $0 \le a_i \le 9$
    จงพิสูจน์ว่า

    (12.1) $9 \mid a$ ก็ต่อเมื่อ $9 \mid (a_0 + a_1 + \cdots + a_n)$

    (12.2) $11 \mid a$ ก็ต่อเมื่อ $11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^n a_n)$

13. ให้ a เหมือนในข้อ 12 สำหรับทุกจำนวนเต็มบวก k ซึ่ง $k \le n$ ให้ $b_k = a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ นั่นคือ b_k เป็นจำนวนเต็มบวกที่ประกอบด้วยตัวเลข k หลักจากทางขวาของ a จงพิสูจน์ว่า $2^k \mid a$ ก็ต่อเมื่อ $2^k \mid b_k$

14. ให้ a และ n เป็นจำนวนเต็มบวกที่ $(a, n) = 1$ จงพิสูจน์ว่า สำหรับทุกๆ จำนวนเต็ม b
    $\{b, b + a, b = 2a, \ldots, b + (n-1)a\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

15. ให้ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่าเซตต่อไปนี้เป็นระบบตกค้างบริบูรณ์มอดุโล n

(15.1) $\left\{-\frac{n-1}{2}, \frac{n-3}{2}, \ldots, \frac{n-3}{2}, \frac{n-1}{2}\right\}$ เมื่อ n เป็นจำนวนเต็มคี่

(15.2) $\left\{-\frac{n}{2}, \frac{n-2}{2}, \ldots, \frac{n-2}{2}, \frac{n}{2}\right\}$ เมื่อ n เป็นจำนวนเต็มคู่

16. จงหาคำตอบทั้งหมดของสมการในแต่ละข้อต่อไปนี้

(16.1) $20x \equiv 4 \pmod{30}$

(16.2) $20x \equiv 3 \pmod{4}$

(16.3) $353x \equiv 254 \pmod{400}$

17. จงหาคำตอบของระบบสมการต่อไปนี้

(17.1) $x \equiv 1 \pmod{4}$

(17.2) $x \equiv 0 \pmod{3}$

(17.3) $x \equiv 5 \pmod{7}$

18. จงหาคำตอบของระบบสมการต่อไปนี้

(18.1) $x \equiv 1 \pmod{2}$

(18.2) $x \equiv 2 \pmod{3}$

(18.3) $x \equiv 3 \pmod{5}$

(18.4) $x \equiv 4 \pmod{7}$

19. จงหาจำนวนเต็มบวกทั้งหมดที่หารด้วย $2, 3, 6$ และ 12 แล้วเหลือเศษ $1, 2, 5$ และ 5 ตามลำดับ

20. ถ้า $f(x) \equiv 0 \pmod{p}$ มี j คำตอบ เมื่อ p เป็นจำนวนเฉพาะและ $g(x) \equiv 0 \pmod{p}$ ไม่มีคำตอบ จงพิสูจน์ว่า $f(x)g(x) \equiv 0 \pmod{p}$ มีเพียง j คำตอบเท่านั้น

21. ถ้าสมการ $f(x) \equiv 0 \pmod{n}$ มี n คำตอบ จงพิสูจน์ว่าจำนวนเต็มทุกจำนวนจะเป็นคำตอบของสมการ $f(x) \equiv 0 \pmod{4}$

22. จงพิสูจน์ว่า $n!$ จะหาผลคูณของจำนวนเต็ม n จำนวนเรียงต่อเนื่องกัน

23. จงหาคำตอบของสมการในแต่ล่ะข้อต่อไปนี้

(23.1) $x^3 + 4x + 8 \equiv 0 \pmod{15}$

(23.2) $x^2 + 2x - 3 \equiv 0 \pmod{45}$

(23.3) $x^3 + 2x - 3 \equiv 0 \pmod{9}$

(23.4) $x^2 + 2x - 3 \equiv 0 \pmod{5}$

(23.5) $x^3 + 9x^2 + 23x - 15 \equiv 0 \pmod{503}$

(23.6) $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$

24. จงพิสูจน์ว่า สำหรับจำนวนเต็มคี่ a ใด ๆ $1+2+3+\cdots+(a-1) \equiv \pmod{a}$
ข้อความนี้เป็นจริงหรือไม่ถ้า a เป็นจำนวนเต็มคู่

25. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็มบวก $n,\ 4^n \equiv 1+3n \pmod{9}$

26. จงหาเศษที่เหลือจากการหาร 3^{500} ด้วย 13

27. จงหาหลักหน่วยของ 2^{100}

28. ให้ p เป็นจำนวนเฉพะ จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็ม $x, x^2 \equiv x \pmod{p}$
ก็ต่อเมื่อ $x \equiv 0$ หรือ $1 \pmod{p}$

29. จงพิสูจน์ว่า สำหรับทุก ๆ จำนวนเต็ม $n, 11 \mid (2^{4n+3}+5^{n+2})$ โดยไม่ใช้หลักอุปนัยเชิงคณิตศาสตร์

30. จงพิสูจน์ว่า ถ้า $a \equiv 2(\mathrm{mod}4)$ แล้ว จะไม่มีจำนวนเต็ม b และ $m>1$ ซึ่ง $a=b^m$

31. จงหาตัวผกผันของ

(31.1) 5 มอดุโล 39

(31.2) 12 มอดุโล 27

32. จงหาจำนวนเต็มบวกทั้งหมดที่น้อยกว่า 15 และมีตัวผกผัน มอดุโล 15 พร้อมทั้งหาตัวผกผันของแต่ละตัวด้วย

33. จงพิจารณาว่า สมภาคเชิงเส้นต่อไปนี้ มีผลเฉลยหรือไม่ ถ้ามีจงหาผลเฉลยที่ไม่สมภาคกันทั้งหมด

(33.1) $34x \equiv 60 \pmod{98}$

(33.2) $140x \equiv 133 \pmod{301}$

(33.3) $128x \equiv 60 \pmod{98}$

(33.4) $36x \equiv 8 \pmod{102}$

34. จงหาจำนวนผลเฉลยที่ไม่สมภาคกันของสมภาคเชิงเส้นต่อไปนี้

(34.1) $25x \equiv 10 \pmod{45}$

(34.2) $25x \equiv 7 \pmod{45}$

(34.3) $25x \equiv 0 \pmod{98}$

(34.4) $15x \equiv 5 \pmod{45}$

35. จงหาเศษเหลือจากการหารจำนวนเต็มต่อไปนี้ด้วย 7

(35.1) $2222^{5555}+5555^{2222}$

(35.2) $10^{10}+10^{10^2}+10^{10^3}+\cdots+10^{10^{10}}$

36. ให้ p เป็นจำนวนเฉพาะที่ $p>5$ จงพิสูจน์ว่า มีจำนวนเทอมใน $9, 99, 999, 9999, \ldots$ อยู่เป็นจำนวนอนันต์ที่หารลงตัวด้วย p

37. จงพิสูจน์ว่า ถ้า a และ b เป็นจำนวนเฉพาะสัมพัทธ์กับ 91 แล้ว $91 \mid (b^{12} - a^{12})$

38. จงแสดงว่า ถ้า p และ q เป็นจำนวนเฉพาะที่ต่างกันแล้ว $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

39. จงพิสูจน์ว่า สำหรับทุกจำนวนเต็ม a ถ้า $(a, 72) = 1$ แล้ว $a^{12} \equiv 1 \pmod{72}$

40. จงพิสูจน์ว่า สำหรับทุกจำนวนเต็มบวก n ใด ๆ n เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $(n-1)! \equiv -1 \pmod{n}$

41. จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะที่ $p \equiv 3 \pmod{4}$ แล้ว $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$

42. จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะ แล้ว $(p-1)! \equiv (p-1) \pmod{1 + 2 + 3 + \cdots + (p-1)}$

43. ให้ p เป็นจำนวนเฉพาะคี่ จงพิสูจน์ว่า

(43.1) $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$

(43.2) $2^2 \cdot 4^2 \cdot 6^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$

44. จงพิสูจน์ว่า ถ้า $r_1, r_2, r_3, \ldots, r_{p-1}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล p แล้ว

$r_1, r_2, r_3, \ldots, r_{p-1} \equiv -1 \pmod{p}$

45. จงหาจำนวนทั้งหมดที่อยู่ระหว่าง 1000 ถึง 2000 ที่เมื่อหารด้วย $5, 7, 11$ แล้วได้เศษเหลือเป็น $1, 3, 5$ ตามลำดับ

เอกสารอ้างอิง

ขนิษฐา ชมภูวิเศษ. (2559). **ทฤษฎีจำนวน**. นครราชสีมา : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏนครราชสีมา.

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จิราภา ลิ้มบุพศิริพร. (2555). **ทฤษฎีจำนวน**. นครปฐม : โรงพิมพ์มหาวิทยาลัยศิลปากร.

ดำรงค์ ทิพย์โยธา. (2556). **คณิตศาสตร์ปรนัยเล่มที่ 37 : โลกทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

ปิยวดี วงษ์ใหญ่. (2530). **ทฤษฎีจำนวน**. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร.

วรรณธิดา ยลวิลาศ. (2560). **ทฤษฎีจำนวน**. กาฬสินธุ์ : คณะศิลปศาสตร์และวิทยาศาสตร์ มหาวิทยาลัยกาฬสินธุ์

วรางคณา ร่องมะรุด. (2523). **ทฤษีจำนวน 2**. กรุงเทพฯ : ยูไนเต็ดโปรดักชั่น.

วัลลภ เหมวงษ์. (2556). **ทฤษฎีจำนวน**. อุดรธานี : สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ. (2556). **ทฤษฎีจำนวน**. กรุงเทพฯ : ไฮเอ็ดพับลิชชิ่ง.

สมใจ จิตพิทักษ์. (2547). **ทฤษฎีจำนวน** (พิมพ์ครั้งที่ 3). สงขลา : ภารกิจเอกสารและตำรามหาวิทยาลัยทักษิณ.

สมพร เรืองโชติวิทย์. (2521). **ทฤษฎีจำนวน**. กรุงเทพฯ : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ บางเขน

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

David M. Burton. (2007). **Elementary number theory (6 ed.)**. New York : The McGraw-HillCompanies, Inc.

David M. Burton. (2011). **Elementary number theory (7 ed.)**. New York : The McGraw-HillCompanies, Inc.

Kenneth Ireland and Michael Rosen. (1990). **A Classical Introduction to Modern Number Theory (2 ed.)**. New York : Springer-Verlag, Inc.

Raji W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

Rosen K.H. (2005). **Elementary number theory and its applications (5 ed.)**. Boston : Pearson/Addison Wesley.

Underwood Dudley. (1969). **Elementary Number Theorem**. San Francisco : W.H. Freeman and Company.

แผนบริหารการสอนประจำบทที่ 5

เนื้อหาประจำบท

1. จำนวนและผลบวกของตัวหารที่เป็นบวก
2. ฟังก์ชันเมอบีอุส
3. ฟังก์ชันออยเลอร์-ฟี
4. จำนวนสมบูรณ์ จำนวนแมร์แซน จำนวนแฟร์มา

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและสมบัติพื้นฐานของจำนวนและผลบวกของตัวหารที่เป็นบวกแก้โจทย์ปัญหาที่กำหนดให้ได้
2. ใช้นิยามและสมบัติพื้นฐานของฟังก์ชันเมอบีอุสแก้โจทย์ปัญหาที่กำหนดให้ได้
3. ใช้นิยามและสมบัติพื้นฐานของฟังก์ชันออยเลอร์-ฟี แก้โจทย์ปัญหาที่กำหนดให้ได้
4. ใช้นิยามและสมบัติพื้นฐานของจำนวนสมบูรณ์ จำนวนแมร์แซน จำนวนแฟร์มาแก้โจทย์ปัญหาที่กำหนดให้ได้

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
   1.1 จำนวนและผลบวกของตัวหารที่เป็นบวก
   1.2 ฟังก์ชันเมอบีอุส
   1.3 ฟังก์ชันออยเลอร์-ฟี
   1.4 จำนวนสมบูรณ์ จำนวนแมร์แซน จำนวนแฟร์มา
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
   2.1 ทำแบบฝึกหัดที่กำหนดให้
   2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
   2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 5
ฟังก์ชันเลขคณิต

ในบทนี้เราจะศึกษาสมบัติของฟังก์ชันเลขคณิต (arithmetic function) หรือ ฟังก์ชันทฤษฎีจำนวน (number-theoretic function) คือฟังก์ชันที่มีโดเมนเป็นเซตของจำนวนเต็มบวก เนื่องจากค่าของฟังก์ชันทฤษฎีจำนวนไม่จำเป็นต้องเป็นจำนวนเต็มบวกหรือ เป็นจำนวนเต็ม ส่วนมากจะศึกษาเกี่ยวกับฟังก์ชันที่มีค่าของฟังก์ชันที่เป็นจำนวนเต็มบวก และฟังก์ชันอื่น ๆ ของทฤษฎีจำนวน ที่เราศึกษาในบทนี้ได้แก่ จำนวนและผลบวกของ ตัวหารที่เป็นบวก ฟังก์ชันเมอบีอุส ฟังก์ชันออยเลอร์-ฟี ฟังก์ชันจำนวนเต็มมากสุด จำนวนสมบูรณ์ จำนวนแมร์แซน และจำนวนแฟร์มา

5.1 จำนวนและผลบวกของตัวหารที่เป็นบวก

ฟังก์ชันที่มีค่าของฟังก์ชันที่เป็นจำนวนเต็มบวก ฟังก์ชันที่ทฤษฎีจำนวนแบบที่ง่าย ที่สุดคือ ฟังก์ชันจำนวนของตัวหาร (the number of divisor function) ดังจะกล่าวในบทนิยาม 5.1.1 และ ฟังก์ชันผลบวกของตัวหาร (the sum of divisor function) ดังจะกล่าวในบทนิยาม 5.1.2 ซึ่งเป็นฟังก์ชันเลขคณิตชนิดหนึ่ง (จิราภา ลิ้มบุพศิริพร. 2555 : 63, สมใจ จิตพิทักษ์. 2547 : 113, สมวงษ์ แปลงประสพโชค. 2545 : 97, David M. Burton. 2007 : 103)

บทนิยาม 5.1.1 : ฟังก์ชันจำนวนของตัวหาร

ฟังก์ชันจำนวนของตัวหาร (the number of divisor function) เขียนแทนด้วย τ เป็นฟังก์ชันเลขคณิต สำหรับ n เป็นจำนวนเต็มบวก ให้ $\tau(n)$ หมายถึง จำนวนตัวหารที่เป็นบวกของ n (number of positive divisor of n)

บทนิยาม 5.1.2 : ฟังก์ชันผลบวกของตัวหาร

ฟังก์ชันผลบวกของตัวหาร (the sum of divisor function) เขียนแทนด้วย σ เป็นฟังก์ชันเลขคณิต สำหรับ n เป็นจำนวนเต็มบวก ให้ $\sigma(n)$ หมายถึง ผลบวกของตัวหารที่เป็นบวกของ n (sum of positive divisor of n)

ตัวอย่าง 5.1.1

จงหา $\tau(n)$ และ $\sigma(n)$ เมื่อ $n = 1, 2, \ldots, 10$

วิธีทำ

n	ตัวหารที่เป็นบวกของ n	$\tau(n)$	$\sigma(n)$
1	1	$\tau(1) = 1$	$\sigma(1) = 1$
2	$1, 2$	$\tau(2) = 2$	$\sigma(2) = 1 + 2 = 3$
3	$1, 3$	$\tau(3) = 2$	$\sigma(3) = 1 + 3 = 4$
4	$1, 2, 4$	$\tau(4) = 3$	$\sigma(4) = 1 + 2 + 4 = 7$
5	$1, 5$	$\tau(5) = 2$	$\sigma(5) = 1 + 5 = 6$

n	ตัวหารที่เป็นบวกของ n	$\tau(n)$	$\sigma(n)$
6	$1, 2, 3, 6$	$\tau(6) = 4$	$\sigma(6) = 1 + 2 + 3 + 6 = 12$
7	$1, 7$	$\tau(7) = 2$	$\sigma(7) = 1 + 7 = 8$
8	$1, 2, 4, 8$	$\tau(8) = 4$	$\sigma(8) = 1 + 2 + 4 + 8 = 15$
9	$1, 3, 9$	$\tau(9) = 3$	$\sigma(9) = 1 + 3 + 9 = 13$
10	$1, 2, 5, 10$	$\tau(10) = 4$	$\sigma(10) = 1 + 2 + 5 + 10 = 18$

ตารางที่ 5.1 แสดงการหา $\tau(n)$ และ $\sigma(n)$

จากตัวอย่าง 5.1.1 จะเห็นว่า $\tau(n) = 2$ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ (มานะ เอกจริยวงศ์. 2542 : 168) และ $\sigma(n) = n + 1$ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

ก่อนที่เราจะศึกษารายละเอียดของฟังก์ชัน τ และฟังก์ชัน σ จะกล่าวถึงสัญลักษณ์

$$\sum_{d\,|\,n} f(d)$$

จะหมายถึง ผลบวกของค่า $f(d)$ เมื่อ d คือจำนวนเต็มบวกที่เป็นตัวหารของจำนวนเต็ม n ตัวอย่างเช่น

$$\sum_{d\,|\,18} f(d) = f(1) + f(2) + f(3) + f(6) + f(9) + f(18)$$

โดยใช้สัญลักษณ์ τ และ σ อาจเขียนได้ในรูป

$$\tau(n) = \sum_{d\,|\,n} 1 \text{ และ } \sigma(n) = \sum_{d\,|\,n} d$$

สัญลักษณ์ $\sum_{d\,|\,n} 1$ หมายถึงเราจะบวก 1 เท่ากับจำนวนตัวหารที่เป็นบวกของ n ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5.1.2

กำหนดให้ $n = 10$ จงหา $\tau(n)$ และ $\sigma(n)$

วิธีทำ จำนวนเต็ม 10 มีตัวหารที่เป็นบวกจำนวน 4 ตัว คือ $1, 2, 5$ และ 10

ดังนั้น $\tau(n) = \sum_{d\,|\,n} 1 = 1 + 1 + 1 + 1 = 4$

และ $\sigma(n) = \sum_{d\,|\,n} d = 1 + 2 + 5 + 10 = 18$

จากตัวอย่างข้างต้น เราจะพบว่าในการหาค่า $\tau(n)$ และ $\sigma(n)$ โดยใช้บทนิยาม 5.1.1 และบทนิยาม 5.1.2 จะต้องหาจำนวนของตัวหารที่เป็นบวกทั้งหมดของ n ในกรณีที่ n มีค่ามากต้องใช้เวลามากในการนับ จำนวนและหาผลบวกของตัวหารที่เป็นบวกของ n ทฤษฎีต่อไปนี้จะช่วยในการหาตัวหารที่เป็นบวกของจำนวนเต็มบวก n เมื่อ n เขียนใน **รูปแบบบัญญัติ** (canonical form) (สมใจ จิตพิทักษ์. 2547 : 114-115, สมวงษ์ แปลงประสพโชค. 2545 : 99, David M. Burton. 2007 : 104-105)

ทฤษฎีบท 5.1.1

สำหรับจำนวนเต็มบวก n ที่ $n > 1$ ถ้ารูปแบบบัญญัติของจำนวนเต็มบวก $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ เป็นการแยกตัวประกอบเฉพาะ (prime factorization) ของจำนวนเต็ม โดยที่ p_i เป็นจำนวนเฉพาะที่ไม่ซ้ำกัน และ k_i เป็นจำนวนเต็มบวก โดยที่ $i = 1, 2, \ldots, r$ จะได้ว่าตัวหารที่เป็นบวกของ n คือจำนวนเต็ม d ทั้งหลายที่เขียนในรูป $d = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ โดยที่ $0 \le a_i \le k_i$ $(i = 1, 2, \ldots, r)$

การพิสูจน์ สังเกตว่าตัวหาร $d = 1$ เมื่อ $a_1 = a_2 = \cdots = a_r = 0$
และ $d = n$ เมื่อ $a_1 = k_1, a_2 = k_2, \ldots, a_r = k_r$
สมมติให้ d เป็นตัวหารของ n นอกเหนือจาก 1 และ n ดังกล่าวแล้ว
ดังนั้น $n = dd'$ โดยที่ $d > 1, d^n > 1$
เขียน d และ d' ในรูปผลคูณของจำนวนเฉพาะ (ไม่จำเป็นต้องแตกต่างกัน) ดังนี้

$$d = q_1q_2\cdots q_s \text{ และ } d' = t_1t_2\cdots t_u$$

โดยที่ q_i, t_j เป็นจำนวนเฉพาะ

$$p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} = q_1q_2\ldots q_st_1t_2\cdots t_u$$

จำนวนเต็มบวก n เขียนในรูปผลคูณของจำนวนเฉพาะ 2 จำนวน
จากทฤษฎีบทหลักมูลของเลขคณิต จำนวนเฉพาะ q_i แต่ละจำนวนเท่ากับ p_j เพียงชุดเดียว
รวมจำนวนเฉพาะที่เท่ากันเข้าด้วยกันจะได้

$$d = q_1q_2\cdots q_sp_1^{a_1}p_2^{a_2}\cdots p_r^{a}$$

โดยที่ยอมให้ $a_i = 0$ ได้
ในทางกลับกัน จำนวนเต็ม $d = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ โดยที่ $0 \le a_i \le k_i$
เป็นตัวหารของ n สามารถเขียนได้ดังนี้

$$\begin{aligned} n &= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} \\ &= \left(p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}\right)\left(p_1^{k_1-a_1}p_2^{k_2-a_2}\cdots p_r^{k_r-a_r}\right) \\ &= dd' \end{aligned}$$

โดยที่ $d' = p_1^{k_1-a_1}p_2^{k_2-a_2}\cdots p_r^{k_r-a_r}$ และ $k_i - a_i \ge 0$ สำหรับแต่ละ i
ดังนั้น $d' > 0$ และ $d \mid n$ □

เราจะใช้ทฤษฎีบท 5.1.1 ช่วยในการพิสูจน์ทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 147, สมใจ จิตพิทักษ์. 2547 : 114-115, David M. Burton. 2007 : 104-105)

ทฤษฎีบท 5.1.2

สำหรับจำนวนเต็มบวก n ที่ $n > 1$ ถ้า $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ เขียนในรูปผลคูณของจำนวนเฉพาะ จะได้ว่า

1. $\tau(n) = (k_1 + 1)(k_2 + 2)\cdots(k_r + 1)$
2. $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$

การพิสูจน์ จากทฤษฎีบท 5.1.1 ตัวหารที่เป็นบวกของ n เป็นจำนวนเต็มบวก d ทั้งหมดอยู่ในรูป
$d = q_1 q_2 \cdots q_s p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ โดยที่ $0 \leq a_i \leq k_i$
แต่ a_1 สามารถเลือกค่าต่าง ๆ ได้ $k_1 + 1$ วิธี a_2 สามารถเลือกค่าต่าง ๆ ได้ $k_2 + 1$ วิธี
ดังนั้นตัวหารที่เป็นไปได้ของ n จะมีจำนวนทั้งหมดเท่ากับ

$$(k_1 + 1)\,(k_2 + 1) \cdots (k_r + 1)$$

นั่นคือ $\tau(n) = (k_1 + 1)\,(k_2 + 1) \cdots (k_r + 1)$
ในการคำนวณ $\sigma(n)$ พิจารณาผลคูณ

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}\right) \cdots \left(1 + p_r + p_r^2 + \cdots + p_r^{k}\right)$$

ตัวหารที่เป็นบวกของ n แต่ละตัว
จะปรากฏเป็นพจน์หนึ่งและพจน์เดียวในการกระจายผลคูณ ดังนี้

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right) \cdots \left(1 + p_r + p_r^2 + \cdots + p_r^{k}\right)$$

โดยใช้สูตรผลรวมของอนุกรมเรขาคณิตสำหรับแต่ละตัวประกอบ i ในพจน์ทางขวามือ จะได้

$$\sigma(n) = \left(1 + p_i + p_i^2 + \cdots + p_i^{k_1+1}\right) = \frac{p_i^{k_1+1} - 1}{p_i - 1}$$

ดังนั้น

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

□

โดยทั่วไป นิยมเขียนแทนผลคูณของจำนวนเต็มด้วยสัญลักษณ์ $\prod$ ตัวอย่างเช่น

$$\prod_{1 \leq d \leq 5} f(d) = f(1)f(2)f(3)f(4)f(5)$$

$$\prod_{d \,|\, 9} f(d) = f(1)f(3)f(9)$$

$$\prod_{p \,|\, 30} f(p) = f(2)f(3)f(5) \quad \text{โดยที่ } p \text{ เป็นจำนวนเฉพาะ}$$

ดังนั้น ผลที่ได้ในทฤษฎีบท 5.1.2 สามารถเขียนในแบบที่กะทัดรัดได้ดังนี้

และ

$$\tau(n) = \prod_{1 \leq i \leq r} (k_r + 1)$$

$$\sigma(n) = \prod_{1 \leq i \leq r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

วัลลภ เหมวงษ์. (2556 : 50-51) ได้ยกตัวอย่างเพื่อให้เข้าใจทฤษฎีมากขึ้น ดังนี้

ตัวอย่าง 5.1.3

เนื่องจาก $72 = (2^3)(3^2)$ ดังนั้น ตัวหารของ 72 คือ

$$(2^0)(3^0), (2^1)(3^0), (2^2)(3^0), (2^3)(3^0),$$
$$(2^0)(3^1), (2^1)(3^1), (2^2)(3^1), (2^3)(3^1),$$
$$(2^0)(3^2), (2^1)(3^2), (2^2)(3^2), (2^3)(3^2)$$

หรือ $1, 2, 4, 8, 3, 6, 12, 24, 9, 18, 36, 72$ มีทั้งหมด 12 จำนวน
หรือ โดยทฤษฎีบท 5.1.2 จะได้ว่า

$$\tau(72) = (3+1)(2+1) = (4)(3) = 12$$

ตัวอย่าง 5.1.4

กำหนดให้ $n = 180$ จงหา $\tau(n)$ และ $\sigma(n)$

วิธีทำ จำนวนเต็ม 180 เขียนในรูปผลคูณของจำนวนเฉพาะ คือ $180 = 2^2 \cdot 3^2 \cdot 5$

ดังนั้น $\tau(180) = (2+1)(2+1)(1+1) = 18$

และ $\sigma(180) = \dfrac{2^3-1}{2-1} \cdot \dfrac{3^3-1}{3-1} \cdot \dfrac{5^2-1}{5-1} = \dfrac{7 \cdot 26 \cdot 24}{1 \cdot 2 \cdot 4} = 7 \cdot 13 \cdot 6 = 546$

จากตัวอย่าง 5.1.4 สังเกตว่า

$\tau(2 \cdot 10) = \tau(20) = \tau(2^2 \cdot 5) = (2+1)(1+1) = 6$

และ $\tau(2)\tau(10) = \tau(20) = 2 \cdot 4 = 8$

ดังนั้น $\tau(2 \cdot 10) \neq \tau(2)\tau(10)$

ในขณะเดียวกัน $\sigma(2 \cdot 10) = \sigma(20) = \dfrac{2^3-1}{2-1} \cdot \dfrac{5^2-1}{5-1} = \dfrac{7 \cdot 24}{4} = 42$

และ $\sigma(2)\sigma(10) = \sigma(20) = \dfrac{2^3-1}{2-1} \cdot \dfrac{2^2-1}{2-1} \cdot \dfrac{5^2-1}{5-1} = \dfrac{3 \cdot 3 \cdot 24}{4} = 54$

ดังนั้น $\sigma(2 \cdot 10) \neq \sigma(2)\sigma(10)$

แต่ฟังก์ชันดังกล่าวจะเป็นจริงถ้าเราจำกัดเงื่อนไขว่า m และ n เป็นจำนวนเฉพาะสัมพัทธ์ ดังบทนิยามต่อไปนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 94-95, จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 149, จิราภา ลิ้มบุพศิริพร. 2555 : 66, นพพร ธนะชัยขันธ์. 2543 : 207, สมใจ จิตพิทักษ์. 2547 : 117, David M. Burton. 2007 : 107, Raji W. 2013 : 70)

บทนิยาม 5.1.3

ให้ f เป็นฟังก์ชันเลขคณิต จะเรียก f ว่าเป็นฟังก์ชันเชิงการคูณ (multiplicative function) ก็ต่อเมื่อ $f(mn) = f(m)f(n)$ สำหรับจำนวนเต็มบวก m และ n ซึ่ง $(m, n) = 1$ จะเรียก f ว่าเป็นฟังก์ชันเชิงการคูณบริบูรณ์ (completely multiplicative function) ก็ต่อเมื่อ $f(mn) = f(m)f(n)$ สำหรับจำนวนเต็มบวก m และ n

ตัวอย่าง 5.1.5

1. ฟังก์ชันต่อไปนี้เป็นฟังก์ชันเชิงการคูณ
   1) $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 0$
   2) $I : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $I(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } n \neq 1 \end{cases}$
2. ฟังก์ชันต่อไปนี้ไม่เป็นฟังก์ชันเชิงการคูณ
   1) $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 3$
   2) $f : \mathbb{N} \to \mathbb{C}$ กำหนดโดย $f(n) = n + i$
   3) $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n^2 + 2n$

ตัวอย่าง 5.1.6

สำหรับทุกจำนวนเต็มบวก n จงตรวจสอบว่าฟังก์ชันต่อไปนี้เป็นฟังก์ชันเชิงการคูณหรือไม่

1. $f(n) = 1$
2. $g(n) = n$
3. $h(n) = n^2$
4. $i(n) = 2n + 3$

วิธีทำ 1. ให้ $f(n) = 1$ สำหรับทุกจำนวนเต็มบวก n
ถ้า m และ n เป็นจำนวนเต็มบวกแล้ว $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$
ดังนั้น f เป็นฟังก์ชันเชิงการคูณ

2. ให้ $g(n) = n$ สำหรับทุกจำนวนเต็มบวก n
ถ้า m และ n เป็นจำนวนเต็มบวกแล้ว $g(mn) = mn = g(m)g(n)$
ดังนั้น g เป็นฟังก์ชันเชิงการคูณ

3. ให้ $h(n) = n^2$ สำหรับทุกจำนวนเต็มบวก n
ถ้า m และ n เป็นจำนวนเต็มบวกแล้ว $h(mn) = (mn)^2 = m^2n^2 = h(m)h(n)$
ดังนั้น h เป็นฟังก์ชันเชิงการคูณ

4. ให้ $i(n) = 2n + 3$ สำหรับทุกจำนวนเต็มบวก n
ถ้า m และ n เป็นจำนวนเต็มบวกแล้ว $i(mn) = 2mn + 3 \neq (2n + 3)(2m + 3) = i(m)i(n)$
ดังนั้น i ไม่เป็นฟังก์ชันเชิงการคูณ

เราพิจารณาฟังก์ชันเชิงการคูณอย่างง่าย กำหนดให้ $f(n) = 1$ และ $g(n) = n$ สำหรับทุกจำนวนเต็ม n โดยอุปนัยเชิงคณิตศาสตร์ ถ้า f เป็นฟังก์ชันเชิงการคูณ และ $n_1, n_2, \ldots, n_r$ เป็นจำนวนเฉพาะสัมพัทธ์เป็นคู่ ๆ จะได้ว่า $f(n_1, n_2, \ldots, n_r) = f(n_1)\, f(n_2) \cdots f(n_r)$

เราทราบว่าถ้า n เป็นจำนวนเต็มบวกที่มากกว่า 1 แล้ว เราสามารถแยกตัวประกอบของ n ในรูปจำนวนเฉพาะยกกำลัง (prime power) ได้เป็น $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ ถ้า f เป็นฟังก์ชันเชิงการคูณ จะได้ $f(n) = f\left(p_1^{k_1}\right) f\left(p_2^{k_2}\right) \cdots f\left(p_r^{k_r}\right)$

ถ้า f เป็นฟังก์ชันเชิงการคูณ ที่มีค่าไม่เป็นศูนย์ นั่นคือจะมีจำนวนเต็ม n บางค่าที่ $f(n) \neq 0$ จะได้ $f(n) = f(n \cdot 1) = f(n)f(1)$ ดังนั้น ในกรณีนี้จะได้ว่า $f(1) = 1$

เราจะพิสูจน์ว่า ฟังก์ชัน τ และฟังก์ชัน σ เป็นฟังก์ชันเชิงการคูณ ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 149, สมใจ จิตพิทักษ์. 2547 : 118, David M. Burton. 2007 : 107)

ทฤษฎีบท 5.1.3

ฟังก์ชัน τ และฟังก์ชัน σ เป็นฟังก์ชันเชิงการคูณ

การพิสูจน์ กำหนดให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $(m,n)=1$

ถ้า $m=n=1$ แล้ว $\tau(1)=\tau(1)\tau(1)=1$ และ $\sigma(1)=\sigma(1)\sigma(1)=1$ เป็นฟังก์ชันเชิงการคูณ

สมมติให้ $m>1, n>1$ และ m,n เขียนเป็นผลคูณของจำนวนเฉพาะในรูปแบบบัญญัติได้เป็น

$$m=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} \text{ และ } n=q_1^{j_1}p_2^{j_2}\cdots p_s^{j_s}$$

เป็นผลคูณของจำนวนเฉพาะของ m และ n เนื่องจาก $(m,n)=1$

ดังนั้น ไม่มี p_i ตัวใดเท่ากับ q_i จะได้ว่า mn เขียนในรูปผลคูณของจำนวนเฉพาะได้เป็น

$$mn=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}q_1^{j_1}p_2^{j_2}\cdots p_s^{j}$$

โดยทฤษฎีบท 5.1.6 จะได้

$$\tau(mn)=[(k_1+1)\cdots(k_r+1)]\,[(j_1+1)\cdots(j_s+1)]=\tau(m)\tau(n)$$

ในทำนองเดียวกัน โดยทฤษฎีบท 5.1.6 จะได้

$$\sigma(mn)=\left[\frac{p_1^{k_1+1}-1}{p_1-1}\cdots\frac{p_r^{k_r+1}-1}{p_r-1}\right]\left[\frac{p_1^{j_1+1}-1}{p_1-1}\cdots\frac{p_s^{j_0+1}-1}{p_s-1}\right]=\sigma(m)\sigma(n)$$

ดังนั้น ฟังก์ชัน τ และฟังก์ชัน σ เป็นฟังก์ชันเชิงการคูณ □

ทฤษฎีต่อไปจะกล่าวถึงฟังก์ชันรวมยอด (summation function) (จิราภา ลิ้มบุพศิริพร. 2555 : 65, สมใจ จิตพิทักษ์ 2547 : 119-120, Raji W. 2013 : 81)

ทฤษฎีบท 5.1.4

ถ้าฟังก์ชัน f เป็นฟังก์ชันเชิงการคูณ และ F นิยามโดย

$$F(n)=\sum_{d\,|\,n}f(d)$$

จะได้ว่า F เป็นฟังก์ชันเชิงการคูณ เรียกฟังก์ชัน F ว่า**ฟังก์ชันรวมยอด** (summation function) ของ f

การพิสูจน์ บทพิสูจน์ กำหนดให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $(m,n)=1$ ดังนั้น

$$F(mn)=\sum_{d\,|\,mn}f(d)=\sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}}f(d_1d_2)$$

ทั้งนี้เพราะตัวหาร d ของ mn สามารถเขียนในรูปผลคูณของตัวหาร d_1 ของ m และตัวหาร d_2 ของ n ซึ่ง $(d_1,d_2)=1$ โดยบทนิยามของฟังก์ชันเชิงการคูณจะได้

$$f(d_1d_2)=f(d_1)\,f(d_2)$$

ดังนั้น

$$\begin{aligned}F(mn)&=\sum_{\substack{d_1\,|\,m\\ d_2\,|\,n}}f(d_1d_2)=\sum_{d_1\,|\,m}f(d_1)\sum_{d_2\,|\,n}f(d_2)\\&=F(m)F(n)\end{aligned}$$

□

ตัวอย่างที่จะแสดงต่อไปนี้จะช่วยให้ผู้อ่านเข้าใจถึงการพิสูจน์ทฤษฎีบท 5.1.4 มากขึ้น (นพพร ธนะชัยขันธ์. 2543 : 209)

ตัวอย่าง 5.1.7

ให้ $m = 3$ และ $n = 4$

วิธีทำ จาก $F(3,4) = \sum_{d\,|\,12,\,d>0} f(d)$

$$\begin{aligned}
&= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\
&= f(1) + f(2) + f(4) + f(3) + f(6) + f(12) \\
&= f(1\cdot 1) + f(1\cdot 2) + f(1\cdot 4) + f(3\cdot 1) + f(3\cdot 2) + f(3\cdot 4) \\
&= f(1)f(1) + f(1)f(2) + f(1)f(4) + f(3)f(1) + f(3)f(2) + f(3)f(4) \\
&= [f(1) + f(3)]\,[f(1) + f(2) + f(4)] \\
&= \sum_{d\,|\,3,\,d>0} f(d) \sum_{d\,|\,4,\,d>0} f(d) \\
&= F(3)F(4)
\end{aligned}$$

5.2 ฟังก์ชันเมอบีอุส

ในหัวข้อนี้จะศึกษาฟังก์ชันเลขคณิตที่น่าสนใจอีกฟังก์ชันหนึ่งเป็นฟังก์ชันบนเซตของจำนวนเต็มบวกที่ประยุกต์ใช้ได้มาก นั่นคือ ฟังก์ชันเมอบีอุส (Möbius function) ดังบทนิยามต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 149, จิราภา ลิ้มบุพศิริพร. 2555 : 76, สมใจ จิตพิทักษ์. 2547 : 123, David M. Burton. 2007 : 112, Raji W. 2013 : 79, Rosen K. H. 2005 : 270)

บทนิยาม 5.2.1 : ฟังก์ชันเมอบีอุส (Möbius function)

ฟังก์ชันเมอบีอุส เขียนแทนด้วย μ เป็นฟังก์ชันเลขคณิต สำหรับ n เป็นจำนวนเต็มบวก ซึ่งนิยามโดย

$$\mu(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } n = p^2 \mid n \text{ สำหรับจำนวนเฉพาะ } p \text{ บางตัว} \\ (-1)^r & \text{ถ้า } n = p_1p_2\cdots p_r \text{ เมื่อ } p_i \text{ เป็นจำนวนเฉพาะที่แตกต่าง} \end{cases}$$

จากบทนิยาม 5.2.1 อาจกล่าวได้ว่า $\mu(n) = 0$ ถ้า n **ไม่ปลอดกำลังสอง** (not square-free) และ $\mu(n) = (-1)^r$ ถ้า n **ปลอดกำลังสอง** (square-free) และมีตัวประกอบจำนวนเฉพาะ r ตัว ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5.2.1

จงหา $\mu(n)$ เมื่อ n เป็นจำนวนต่อไปนี้

1. $2, 3, 5$
2. $4, 27, 625$
3. $10, 30$

วิธีทำ 1. $\mu(2) = -1,\ \mu(3) = -1$ และ $\mu(5) = -1$

2. $\mu(4) = \mu(2^2) = 0$ เพราะว่า $2^2 \mid 4$
   $\mu(27) = \mu(3^3) = 0$ เพราะว่า $3^3 \mid 27$
   $\mu(625) = \mu(5^4) = 0$ เพราะว่า $5^4 \mid 625$
3. $\mu(10) = \mu(2 \cdot 5) = (-1)(-1) = 1$
   $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)(-1)(-1) = -1$

จากตัวอย่าง 5.2.1 สรุปได้ว่า μ เป็นฟังก์ชันเชิงการคูณดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 152, สมใจ จิตพิทักษ์. 2547 : 124, David M. Burton. 2007 : 112, Raji W. 2013 : 80, Rosen K. H. 2005 : 270)

ทฤษฎีบท 5.2.1

ฟังก์ชัน μ เป็นฟังก์ชันเชิงการคูณ

การพิสูจน์ ต้องการแสดงว่า μ เป็นฟังก์ชันเชิงการคูณ นั่นคือต้องแสดงว่า

$$\mu(mn) = \mu(m)\mu(n)$$

กำหนดให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $(m, n) = 1$
ถ้า $m = n = 1$ แล้ว $\mu(1) = \mu(1)\mu(1) = 1$
ต่อไปสมมติว่า $m > 1$ และ $n > 1$
กรณีที่ 1 ถ้ามีจำนวนเฉพาะ p ที่ทำให้ $p^2 \mid m$ หรือ $p^2 \mid n$ แล้ว $p^2 \mid mn$
ดังนั้น

$$\mu(mn) = 0 = \mu(m)\mu(n)$$

กรณีที่ 2 ถ้าไม่มีจำนวนเฉพาะ p ที่ทำให้ $p^2 \mid m$ และไม่มีจำนวนเฉพาะ q ที่ทำให้ $q^2 \mid n$
ดังนั้น m และ n เป็นจำนวนเต็มที่ปลอดกำลังสอง กล่าวคือ

$$m = p_1 p_2 \cdots p_r \text{ และ } n = q_1 q_2 \cdots q_s$$

โดยที่ p_i และ q_j เป็นจำนวนเฉพาะที่แตกต่างกัน ทั้งนี้เนื่องจาก $(m, n) = 1$ จะได้ว่า

$$\mu(mn) = \mu\left(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s\right) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$$

ดังนั้น ฟังก์ชัน μ เป็นฟังก์ชันเชิงการคูณ □

ทฤษฎีบทต่อไปเราจะพิสูจน์ว่าฟังก์ชัน μ มีค่าเพียง 0 กับ 1 (สมใจ จิตพิทักษ์. 2547 : 124, David M. Burton. 2007 : 113, Rosen K. H. 2005 : 271)

ทฤษฎีบท 5.2.2

สำหรับ n เป็นจำนวนเต็มบวก ซึ่งนิยามโดย

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้า } n > 1 \end{cases}$$

โดยที่ d เป็นตัวหารที่เป็นบวกทั้งหมดของ n

การพิสูจน์ ในกรณีที่ $n = 1$ เราได้ $\sum_{d\,|\,n} \mu(d) = \mu(1) = 1$

สมมติให้ $n > 1$ เราได้ $F(n) = \sum_{d\,|\,n} f(d)$

เนื่องจาก μ เป็นฟังก์ชันเชิงการคูณ โดยทฤษฎีบท 5.1.4 จะได้ว่า F เป็นฟังก์ชันเชิงการคูณ ดังนั้น ถ้า n เขียนในรูปผลคูณของจำนวนเฉพาะในแบบมาตรฐานได้เป็น

$$F(n) = F\left(p_1^{k_1}\right) F\left(p_2^{k_2}\right) \cdots F\left(p_r^{k}\right)$$

สำหรับ p^k ใด ๆ ตัวหารที่เป็นบวกของ p^k คือ $1, p, p^2, \ldots, p^k$ ดังนั้น

$$\begin{aligned} F\left(p^k\right) &= \sum_{d\,|\,p^k} \mu(d) = \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu\left(p^k\right) \\ &= \mu(1) + \mu(p) = 0 \end{aligned}$$

□

สูตรที่สำคัญของฟังก์ชัน μ เป็นสูตรการผกผันเมอบีอุส ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 155, สมใจ จิตพิทักษ์. 2547 : 125, David M. Burton. 2007 : 113-114, Raji W. 2013 : 81, Rosen K. H. 2005 : 271-272)

ทฤษฎีบท 5.2.3 : สูตรการผกผันเมอบีอุส (Möbius inversion function)

กำหนดให้ f เป็นฟังก์ชันเลขคณิต และ F เป็นฟังก์ชันรวมยอดของ f ที่สัมพันธ์โดยสูตร

$$F(n) = \sum_{d\,|\,n} f(d)$$

จะได้ว่า $f(n) = \sum_{d\,|\,n} \mu(d) F\left(\frac{n}{d}\right)$ สำหรับจำนวนเต็มบวก n

การพิสูจน์ เราเริ่มจากการแทนค่า $\sum_{e\,|\,\frac{n}{d}} f(e)$ ในพจน์ฝั่งขวามือ คือ $F\left(\frac{n}{d}\right)$

จากบทนิยามฟังก์ชัน F เป็นฟังก์ชันรวมยอดของ f จะได้

$$\begin{aligned} \sum_{d\,|\,n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d\,|\,n} \mu(d) \sum_{e\,|\left(\frac{n}{d}\right)} f(e) \\ &= \sum_{d\,|\,n} \sum_{e\,|\left(\frac{n}{d}\right)} \mu(d) f(e) \end{aligned}$$

เนื่องจาก $d \mid n$ และ $e \,\Big|\, \left(\frac{n}{d}\right)$ ก็ต่อเมื่อ $e \mid n$ และ $d \,\Big|\, \left(\frac{n}{e}\right)$ จะได้ว่า

$$\begin{aligned} \sum_{d\,|\,n} \sum_{e\,|\left(\frac{n}{d}\right)} \mu(d) f(e) &= \sum_{e\,|\,n} \sum_{d\,|\left(\frac{n}{e}\right)} f(e)\mu(d) \\ &= \sum_{e\,|\,n} f(e) \sum_{d\,|\left(\frac{n}{e}\right)} \mu(d) \end{aligned}$$

โดยทฤษฎีบท 5.2.4 จะได้ว่า $\sum_{d\,|\left(\frac{n}{e}\right)} \mu(d) = 0$ ยกเว้นที่ $\frac{n}{e} = 1$

นั่นคือ เมื่อ $n = e$ ผลบวกเท่ากับ 1 ดังนั้น

$$\sum_{e\,|\,n} f(e) \sum_{d\,|\left(\frac{n}{e}\right)} \mu(d) = \sum_{e=n} f(e) \cdot 1 = f(n)$$

นั่นคือ $f(n) = \sum_{d\,|\,n} \mu(d) F\left(\frac{n}{d}\right)$ □

เพื่อให้เข้าใจการพิสูจน์ของทฤษฎีบท 5.2.3 มากยิ่งขึ้น พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง 5.2.2

พิจารณากรณี $n = 10$ ในผลบวก จะได้ว่า

$$\begin{aligned}
\sum_{d\,|\,10} \sum_{e\,|\left(\frac{10}{d}\right)} \mu(d) f(e) &= [\mu(1)f(1) + \mu(1)f(2) + \mu(1)f(5) + \mu(1)f(10)] \\
&\quad + [\mu(2)f(1) + \mu(2)f(5)] + [\mu(5)f(1) + \mu(5)f(2)] + \mu(10)f(1) \\
&= [f(1)\mu(1) + f(1)\mu(2) + f(1)\mu(5) + f(1)\mu(10)] \\
&\quad + [f(2)\mu(1) + f(2)\mu(5)] + [f(5)\mu(1) + f(5)\mu(2)] + f(10)\mu(1) \\
&= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] + f(2)[\mu(1) + \mu(5)] \\
&\quad + f(5)[\mu(1) + \mu(2)] + f(10)\mu(1) \\
&= \sum_{e\,|\,10} f(e) \sum_{d\,|\left(\frac{10}{e}\right)} \mu(d)
\end{aligned}$$

ตัวอย่าง 5.2.3

1. $\tau(n) = \sum_{d\,|\,n} 1$ จะได้ว่า $\sum_{d\,|\,n} \mu(d)\tau\left(\frac{n}{d}\right) = 1$
2. $\sigma(n) = \sum_{d\,|\,n} d$ จะได้ว่า $\sum_{d\,|\,n} \mu(d)\sigma\left(\frac{n}{d}\right) = n$

5.3 ฟังก์ชันออยเลอร์-ฟี

ฟังก์ชันเลขคณิตที่สำคัญมากอีกฟังก์ชันหนึ่งคือ ฟังก์ชันออยเลอร์-ฟี ซึ่งได้นิยามไว้ ในหัวข้อ 4.5 แล้วว่า $\phi(m)$ เป็นจำนวนสมาชิกในระบบส่วนตกค้างลดรูปมอดุโล m นั่นคือ จำนวนของจำนวนเต็มบวกทั้งหมดที่ไม่เกิน m และจะเป็นจำนวนเฉพาะสัมพัทธ์กับ m ในการหาค่าของฟังก์ชันออยเลอร์-ฟี โดยใช้บทนิยาม 4.5.3 เราต้องหาจำนวนเต็มบวกที่ไม่เกิน m และเป็นจำนวนเฉพาะสัมพัทธ์กับ m ก่อน จากนั้นจึงหาจำนวนของจำนวนเต็มบวกเหล่านี้ จะเห็นว่า ถ้าค่า m มาก จะไม่สะดวกในการหาค่า $\phi(m)$ ในหัวข้อนี้จะเป็นการหาสูตรที่ใช้คำนวณหาค่าของ $\phi(m)$ เมื่อ m เป็นจำนวนเต็มบวก พร้อมทั้งสมบัติที่สำคัญของฟังก์ชันนี้ ง่ายที่สุดคือเมื่อ m เป็นจำนวนเฉพาะ ดังจะกล่าวในทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 159, อัจฉรา หาญชูวงศ์. 2542 : 58, Raji W. 2013 : 73, Rosen K. H. 2005 : 240)

ทฤษฎีบท 5.3.1

ถ้า p เป็นจำนวนเฉพาะ แล้ว $\phi(p) = p - 1$

การพิสูจน์ สมมติ p เป็นจำนวนเฉพาะ
จะได้ว่า จำนวนเต็มบวกที่ไม่เกิน p จะเป็นจำนวนเฉพาะสัมพัทธ์กับ p ทุกจำนวน
ซึ่งจะมีอยู่ทั้งหมด $p - 1$ □

ต่อไปจะกล่าวถึง $\phi(m)$ เมื่อ $m = p^k$ ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 160, จิราภา ลิ้มบุพศิริพร. 2555 : 83, อัจฉรา หาญชูวงศ์. 2542 : 58, Raji W. 2013 : 73, Rosen K. H. 2005 : 241)

ทฤษฎีบท 5.3.2

ถ้า p เป็นจำนวนเฉพาะ และ k เป็นจำนวนเต็มบวก แล้ว

$$\phi\left(p^k\right) = p^k - p^{k-1}$$

การพิสูจน์ สมมติให้ p เป็นจำนวนเฉพาะ และ k เป็นจำนวนเต็มบวก
เห็นได้โดยง่ายว่า $\left(m, p^k\right) = 1$ ก็ต่อเมื่อ $p \nmid m$
และจะมีจำนวนเต็มบวก p^{k-1} จำนวนระหว่าง 1 ถึง p^k ที่หารด้วย p ลงตัว กล่าวคือ

$$p \mid p, 2p, 3p, \ldots, p^{k-1}p$$

ดังนั้น $\left\{1, 2, \ldots, p^k\right\}$ ประกอบด้วยจำนวนเต็ม $p^k - p^{k-1}$ จำนวน
ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ p
นั่นคือ $\phi\left(p^k\right) = p^k - p^{k-1}$ □

ตัวอย่าง 5.3.1

จงหา $\phi(32)$

วิธีทำ $\phi(32) = \phi\left(2^5\right) = 2^5 - 2^{5-1} = 16$

ตารางต่อไปนี้แสดงการหาค่าของ $\phi(n)$ เมื่อ $7 \leq n \leq 15$ (นภวรรณ นิลศรี. 2553 : 60)

n	จำนวนเต็มบวก $k \leq n$ ซึ่ง $(k, n) = 1$	$\phi(n)$
7	$1, 2, 3, 4, 5, 6$	6
8	$1, 3, 5, 7$	4
9	$1, 2, 4, 5, 7, 8$	6
10	$1, 3, 7, 9$	4
11	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	10
12	$1, 5, 7, 11$	4
13	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$	12
14	$1, 3, 5, 9, 11, 13$	6
15	$1, 2, 4, 7, 8, 11, 13, 14$	8

ตารางที่ 5.2 ตารางแสดงค่าของ $\phi(n)$

ในการหาสูตรคำนวณ $\phi(m)$ สำหรับ m ที่เป็นจำนวนเต็มบวก เราจะพิสูจน์ว่า ϕ เป็นฟังก์ชันเชิงการคูณ ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 161, สมใจ จิตพิทักษ์. 2547 : 138, อัจฉรา หาญชูวงศ์. 2542 : 58-59, Raji W. 2013 : 74, Rosen K. H. 2005 : 241-242)

ทฤษฎีบท 5.3.3

ϕ เป็นฟังก์ชันเชิงการคูณ นั่นคือ สำหรับจำนวนเต็มบวก m และ n ซึ่ง $(m,n)=1$

$$\phi(mn)=\phi(m)\phi(n)$$

การพิสูจน์ สมมติให้ m และ n ที่ $(m,n)=1$
ถ้า $m=1$ หรือ $n=1$ แล้ว $\phi(mn)=\phi(m)$ หรือ $\phi(mn)=\phi(n)$
เพราะว่า $\phi(1)=1$ ดังนั้น $\phi(mn)=\phi(m)\phi(n)$
ต่อไปสมมติว่า $m>1$ และ $n>1$
จัดเรียงลำดับจำนวนเต็ม ที่อยู่ระหว่าง 1 ถึง mn ดังนี้

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
r & m+r & 2m+r & \ldots & (n-1)m+r \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
m & 2m & 3m & \cdots & mn
\end{array}$$

เราจะนับจำนวนเต็ม k ที่ $(k,mn)=1$
นั่นคือ เราต้องนับจำนวนเต็ม k ที่ $(k,m)=1$ และ $(k,n)=1$
ให้ r เป็นจำนวนเต็มที่ $1\leq r\leq m$ ดังนั้น $(m,r)=(m,lm+r)$ เมื่อ l เป็นจำนวนเต็ม
เพราะฉะนั้น $(m,r)=1$ ก็ต่อเมื่อ $(m,lm+r)=1$
นั่นคือ ถ้า r เป็นจำนวนเฉพาะสัมพัทธ์กับ m แล้วจะได้ว่า
สมาชิกในแถวที่ r จะเป็นจำนวนเฉพาะสัมพัทธ์กับ m ด้วย
ต่อไปจะพิจารณาว่าในแถวที่ r มีสมาชิกอยู่เท่าไหร่เป็นจำนวนเฉพาะสัมพัทธ์กับ n
เนื่องจาก $(m,n)=1$ ดังนั้น สำหรับทุก ๆ $0\leq 1,j\leq(n-1)$
จะได้ว่า $lm+r\equiv(jm+r)\pmod n$ ก็ต่อเมื่อ $1\equiv j\pmod n$
เพราะว่า $0\leq 1,j\leq(n-1)$ ดังนั้น $1=j$ เพราะฉะนั้น
จึงได้ว่า จำนวนเต็ม n จำนวนในแถวที่ r จะเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n
นั่นคือ ในแถวที่ r จะมี $\phi(n)$ จำนวนที่เป็นจำนวนเฉพาะสัมพัทธ์กับ n
แต่เนื่องจาก จำนวนของจำนวนเต็ม r ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m
และ n มีทั้งหมด $\phi(m)\phi(n)$ จำนวน
นั่นคือ $\phi(mn)=\phi(m)\phi(n)$
จึงสรุปได้ว่า ϕ เป็นฟังก์ชันเชิงการคูณ □

รวมทฤษฎีบท 5.3.2 และ 5.3.3 จะได้สูตรใหม่ ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 162, สมใจ จิตพิทักษ์. 2547 : 139-140, อัจฉรา หาญชูวงศ์. 2542 : 59, Raji W. 2013 : 74-75, Rosen K. H. 2005 : 242-243)

ทฤษฎีบท 5.3.4

สำหรับจำนวนเต็มบวก n เขียนในรูปผลคูณของจำนวนเฉพาะในรูปแบบบัญญัติได้เป็น $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ แล้วจะได้

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

การพิสูจน์ โดยทฤษฎีบท 5.3.2 จะได้ว่า $1 \le i \le r$

$$\phi\left(p_i^{k_i}\right) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i}\left(1-\frac{1}{p_r}\right)$$

โดยทฤษฎีบท 5.3.3 จะได้ว่า

$$\begin{aligned}\phi(n) &= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right)\\ &= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\end{aligned}$$

□

จากทฤษฎีบท 5.3.4 เราอาจจะเขียน $\phi(n)$ โดยใช้สัญลักษณ์ $\prod$ ดังนี้

$$\phi(n) = \prod_{i=1}^{r} p_i^{k_i} - p_i^{k_i-1} = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

ตัวอย่าง 5.3.2

จงหา $\phi(1000)$

วิธีทำ $\phi(1000) = \phi\left(2^3\cdot 5^3\right) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400$

ตัวอย่าง 5.3.3

จงหา $\phi(n)$ เมื่อกำหนดจำนวนเต็ม n ให้ดังต่อไปนี้

1. 24
2. 160

วิธีทำ 1. เนื่องจาก $24 = 2^3\cdot 3^1$ จะได้ว่า

$$\phi(24) = 24\left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right) = 24\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 8$$

หรือ $\phi(24) = \left(2^3-2^2\right)\left(3^1-3^0\right) = 2^2(2-1)(3-1) = (4)(2) = 8$

2. เนื่องจาก $160 = 2^5\cdot 5^1$ จะได้ว่า

$$\phi(160) = 160\left(\frac{2-1}{2}\right)\left(\frac{5-1}{5}\right) = 160\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 64$$

หรือ $\phi(160) = \left(2^5-2^4\right)\left(5^1-5^0\right) = 2^4(2-1)(5-1) = (4)(16) = 64$

5.4 ฟังก์ชันจำนวนเต็มมากสุด

ฟังก์ชันจำนวนเต็มมากสุด (greatest integer) หรือ ฟังก์ชันวงเล็บ (bracket function) $\lfloor\ \rfloor$ มีส่วนสำคัญในการศึกษาปัญหาการหารลงตัว แม้ว่าฟังก์ชันนี้ไม่ได้เป็นฟังก์ชันเลขคณิต แต่จะเป็นฟังก์ชันที่ใช้กันมากในทฤษฎีจำนวนฟังก์ชันหนึ่ง ดังบทนิยามต่อไปนี้ (สมใจ จิตพิทักษ์. 2547 : 129, อัจฉรา หาญชูวงศ์. 2542 : 64, ภัททิรา เรืองสินทรัพย์. 2553 : 185, David M. Burton. 2007 : 117)

บทนิยาม 5.4.1

สำหรับจำนวนจริง x ใด ๆ กำหนดโดย $\lfloor x\rfloor$ คือ จำนวนเต็มมากสุดที่น้อยกว่าหรือเท่ากับ x นั่นคือ $x-1<\lfloor x\rfloor\leq x$

ตัวอย่าง 5.4.1

$$\left\lfloor -\frac{3}{2}\right\rfloor=-2,\ \left\lfloor\sqrt{2}\right\rfloor=1,\ \left\lfloor -\frac{5}{2}\right\rfloor=-3,\ \lfloor-\pi\rfloor=-4$$

ในกรณี x เป็นจำนวนเต็มจะได้ว่า $\lfloor x\rfloor=x$
จากบทนิยาม 5.4.1 จำนวนจริง x ใด ๆ จะสามารถเขียนได้เป็น

$$x=\lfloor x\rfloor+\theta$$

โดยที่ $0\leq\theta<1$

สมบัติเบื้องต้นของฟังก์ชัน $\lfloor x\rfloor$ มีดังทฤษฎีบทต่อไปนี้ (สมใจ จิตพิทักษ์. 2547 : 129, สมวงษ์ แปลงประสพโชค. 2545 : 109, อัจฉรา หาญชูวงศ์. 2542 : 65)

ทฤษฎีบท 5.4.1

ให้ x,y เป็นจำนวนจริงใด ๆ n เป็นจำนวนเต็ม จะได้

1. $\lfloor x+n\rfloor=\lfloor x\rfloor+n$
2. $\lfloor x+y\rfloor\geq\lfloor x\rfloor+\lfloor y\rfloor$
3. $\lfloor x\rfloor+\lfloor -x\rfloor=0$ ถ้า x เป็นจำนวนเต็ม หรือ -1 ถ้า x ไม่เป็นจำนวนเต็ม
4. $\left\lfloor\frac{x}{n}\right\rfloor=\left\lfloor\frac{\lfloor x\rfloor}{n}\right\rfloor$

การพิสูจน์ 1. ให้ $x=\lfloor x\rfloor+\theta,\ 0\leq\theta<1$
ดังนั้น $x+n=\lfloor x\rfloor+n+\theta,\ 0\leq\theta<1$
นั่นคือ $\lfloor x+n\rfloor=(x+n)-\theta=(x-\theta)-n=\lfloor x\rfloor+n$

2. ให้ $x=\lfloor x\rfloor+\theta_1, 0\leq\theta_1<1$
$y=\lfloor y\rfloor+\theta_2, 0\leq\theta_2<1$
ดังนั้น $x+y=\lfloor x\rfloor+\lfloor y\rfloor+\theta_1+\theta_2,\ 0\leq\theta_1+\theta_2<1$
ถ้า $0\leq\theta_1+\theta_2<1$ จะได้ $\lfloor x+y\rfloor=\lfloor x\rfloor+\lfloor y\rfloor$
ถ้า $1\leq\theta_1+\theta_2<2$ จะได้ $\lfloor x+y\rfloor=\lfloor x\rfloor+\lfloor y\rfloor+1$
นั่นคือ $\lfloor x+y\rfloor\geq\lfloor x\rfloor+\lfloor y\rfloor$

3. ถ้า x เป็นจำนวนเต็ม $\lfloor x \rfloor = x$ และ $\lfloor -x \rfloor = -x$
จะได้ $\lfloor x \rfloor + \lfloor -x \rfloor = x + (-x) = 0$
ถ้า x ไม่เป็นจำนวนเต็ม $x = \lfloor x \rfloor + \theta,\ 0 \leq \theta < 1$
คูณด้วย -1 จะได้ $-x = -x - \theta,\ 0 < \theta < 1$
$= -1 - \lfloor x \rfloor + (1 - \theta)$
ดังนั้น $\lfloor -x \rfloor = -1 - \lfloor x \rfloor$ เพราะว่า $0 < 1 - \theta < 1$
จะได้ $\lfloor x \rfloor + \lfloor -x \rfloor = 1$
นั่นคือ $\lfloor x \rfloor + \lfloor -x \rfloor = 0$ ถ้า x เป็นจำนวนเต็ม หรือ -1 ถ้า x ไม่เป็นจำนวนเต็ม

4. ให้ $\dfrac{x}{n} = \left\lfloor \dfrac{x}{n} \right\rfloor + \theta,\ 0 \leq \theta < 1$
ดังนั้น $x = n\left\lfloor \dfrac{x}{n} \right\rfloor + n\theta$ โดยข้อ 1.
จะได้ $\lfloor x \rfloor = n\left\lfloor \dfrac{x}{n} \right\rfloor + \lfloor n\theta \rfloor$
เพราะฉะนั้น $\dfrac{\lfloor x \rfloor}{n} = \left\lfloor \dfrac{x}{n} \right\rfloor + \dfrac{\lfloor n\theta \rfloor}{n}$
แต่ $0 \leq \dfrac{\lfloor n\theta \rfloor}{n} \leq \dfrac{n\theta}{n} = \theta < 1$
นั่นคือ $\left\lfloor \dfrac{x}{n} \right\rfloor = \left\lfloor \dfrac{\lfloor x \rfloor}{n} \right\rfloor$ □

ตัวอย่าง 5.4.2

1. $\lfloor 2.5 + 5 \rfloor = \lfloor 2.5 \rfloor + 5 = 7$
2. $\lfloor 2.5 + 3.5 \rfloor \geq \lfloor 2.5 \rfloor + \lfloor 3.5 \rfloor = 6 \geq 5$
3. $\lfloor 2 \rfloor + \lfloor -2 \rfloor = 0$
$\lfloor 2 \rfloor + \lfloor -2.5 \rfloor = 2 - 3 = -1$
4. $\left\lfloor \dfrac{5.2}{2} \right\rfloor = \left\lfloor \dfrac{\lfloor 5.2 \rfloor}{2} \right\rfloor$
$2 = 2$

ตัวอย่าง 5.4.3

จงหา $\displaystyle\sum_{k=1}^{\infty} \left\lfloor \frac{50}{2^k} \right\rfloor$

วิธีทำ $\displaystyle\sum_{k=1}^{\infty} \left\lfloor \frac{50}{2^k} \right\rfloor = \left\lfloor \frac{50}{2^1} \right\rfloor + \left\lfloor \frac{50}{2^2} \right\rfloor + \left\lfloor \frac{50}{2^3} \right\rfloor + \left\lfloor \frac{50}{2^4} \right\rfloor + \left\lfloor \frac{50}{2^5} \right\rfloor + \left\lfloor \frac{50}{2^6} \right\rfloor + \cdots$
$= 24 + 12 + 6 + 3 + 1 + 0 + \cdots$
$= 46$

ถ้า n เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะ เราจะหากำลังสูงสุดของ p ดังทฤษฎีบทต่อไปนี้ (สมใจ จิตพิทักษ์. 2547 : 130-131, สมวงษ์ แปลงประสพโชค. 2545 : 113, อัจฉรา หาญชูวงศ์. 2542 : 67, ภัททิรา เรืองสินทรัพย์. 2553 : 187)

ทฤษฎีบท 5.4.2 : สูตรของเดอโพลิกแนค (De Polignac's formular)

ถ้า n เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะ จะได้ว่า กำลังสูงสุดของ p ที่ $p^e \mid n!$ คือ

$$e_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

การพิสูจน์ ตั้งแต่ 1 ถึง n มีจำนวนที่หารด้วย p ลงตัว ได้แก่ $p, 2p, 3p, \ldots, tp$

โดยที่ t เป็นจำนวนเต็มมากที่สุด ซึ่ง $tp \leq n$ นั่นคือ $t = \left\lfloor \frac{n}{p} \right\rfloor$

ตั้งแต่ 1 ถึง n มีจำนวนที่หารด้วย p^2 ลงตัว ได้แก่ $p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2$

มีทั้งหมด $\left\lfloor \frac{n}{p^2} \right\rfloor$ จำนวน ตั้งแต่ 1 ถึง n มีจำนวนที่หารด้วย p^k ลงตัว เมื่อ $p^k \leq n$ ได้แก่

$p^k, 2p^k, 3p^k, \ldots, \left\lfloor \frac{n}{p^k} \right\rfloor p^k$ มีทั้งหมด $\left\lfloor \frac{n}{p^k} \right\rfloor$ จำนวน

จาก $n! = (1)(2)(3)\cdots(n)$

ถ้านำเอา p ไปหารตัวประกอบทางขวามือตัวละ 1 ครั้ง จะได้ลงตัว $\left\lfloor \frac{n}{p} \right\rfloor$ ครั้ง

ต่อมานำ p ไปหารตัวเลขซึ่งเป็นผลมาจากครั้งแรกจะได้ลงตัว $\left\lfloor \frac{n}{p^2} \right\rfloor$ ครั้ง

เมื่อนำ p ไปหารตัวเลขทางขวาตัวละครั้งไปเรื่อย ๆ จะไม่อาจหารได้อีก

จะได้จำนวนครั้งของการหารด้วย p รวมทั้งสิ้น ดังต่อไปนี้

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

นั่นคือ กำลังสูงสุดของ p คือ $e_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ ที่ทำให้ $p^e \mid n!$ □

ผลของทฤษฎีบท 5.4.2 ทำให้ได้สูตรการเขียน $n!$ เป็นผลคูณของจำนวนเฉพาะ ชื่อว่า**สูตรของเลอฌ็องดร์** (Legendre's fomular) ดังนี้

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor}$$

ตัวอย่าง 5.4.4

จงเขียน $20!$ เป็นผลคูณจำนวนเฉพาะ

วิธีทำ $20! = \prod_{p \leq 20} p^{\sum_{k=1}^{\infty} \left\lfloor \frac{20}{p^k} \right\rfloor}$

ถ้า $p = 2$ จะได้ $\sum_{k=1}^{\infty} \left\lfloor \frac{20}{2^k} \right\rfloor = \left\lfloor \frac{20}{2^1} \right\rfloor + \left\lfloor \frac{20}{2^2} \right\rfloor + \left\lfloor \frac{20}{2^3} \right\rfloor + \left\lfloor \frac{20}{2^4} \right\rfloor + \cdots$

$$= 10 + 5 + 2 + 1$$
$$= 18$$

ถ้า $p=3$ จะได้ $\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{20}{3^k}\right\rfloor=\left\lfloor\frac{20}{3^1}\right\rfloor+\left\lfloor\frac{20}{3^2}\right\rfloor+\left\lfloor\frac{20}{3^3}\right\rfloor+\cdots$

$$=6+2+0$$

$$=8$$

ถ้า $p=5$ จะได้ $\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{20}{5^k}\right\rfloor=\left\lfloor\frac{20}{5^1}\right\rfloor+\left\lfloor\frac{20}{5^2}\right\rfloor+\cdots$

$$=4+0$$

$$=4$$

ถ้า $p=7$ จะได้ $\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{20}{7^k}\right\rfloor=\left\lfloor\frac{20}{7^1}\right\rfloor+\left\lfloor\frac{20}{7^2}\right\rfloor+\cdots$

$$=2+0$$

$$=2$$

ถ้า $p=11,13,17,19$ จะได้ $\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor=1$

ดังนั้น $20!=2^{18}\cdot 3^5\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19$

ตัวอย่าง 5.4.5

จงหาค่า e_p ที่มากที่สุด ที่ $3^e \mid 60!$

วิธีทำ $e_p=\displaystyle\sum_{k=1}^{\infty}\left\lfloor\frac{60}{3^k}\right\rfloor=\left\lfloor\frac{60}{3^1}\right\rfloor+\left\lfloor\frac{60}{3^2}\right\rfloor+\left\lfloor\frac{60}{3^3}\right\rfloor+\cdots$

$$=20+6+2+0+\cdots$$

$$=28$$

กรณีที่ p ไม่ใช่จำนวนเฉพาะ เราสามารถหากำลังสูงสุดของ p ที่ $p^e \mid n!$ โดยวิธีการดังตัวอย่างต่อไปนี้ (ธนัชยศ จำปาหวาย. 2559 : 141)

ตัวอย่าง 5.4.6

จงหาจำนวนเต็ม k ที่มากสุดที่ทำให้ 18^k หาร $100!$ ลงตัว

วิธีทำ เนื่องจาก $18=2\cdot 3^2$ พิจารณากำลังสูงสุดของจำนวนเฉพาะ 2 และ 3 ได้ดังนี้

$$e_2(100)=\sum_{i=1}^{\infty}\left\lfloor\frac{100}{2^i}\right\rfloor=\left\lfloor\frac{100}{2}\right\rfloor+\left\lfloor\frac{100}{2^2}\right\rfloor+\left\lfloor\frac{100}{2^3}\right\rfloor+\left\lfloor\frac{100}{2^4}\right\rfloor+\left\lfloor\frac{100}{2^5}\right\rfloor+\left\lfloor\frac{100}{2^6}\right\rfloor$$

$$=50+25+12+6+3+1=97$$

$$e_3(100)=\sum_{i=1}^{\infty}\left\lfloor\frac{100}{3^i}\right\rfloor=\left\lfloor\frac{100}{3}\right\rfloor+\left\lfloor\frac{100}{3^2}\right\rfloor+\left\lfloor\frac{100}{3^3}\right\rfloor+\left\lfloor\frac{100}{3^4}\right\rfloor$$

$$=33+11+3+1=48$$

ดังนั้นรูปแบบบัญญัติของ 100! คือ $100! = 2^{97} \cdot 3^{48} \cdot 5^m \cdot 7^d \cdots 97$ เนื่องจาก

$$2^{97} \cdot 3^{48} = 2^{73} \cdot 2^{24} \cdot \left(3^2\right)^{24} = 2^{73} \left(2 \cdot 3^2\right)^{24} = 2^{73}(18)^{24}$$

ดังนั้น $k = 24$

5.5 จำนวนสมบูรณ์ จำนวนแมร์แซน จำนวนแฟร์มา

ในหัวข้อนี้จะกล่าวถึงจำนวนที่มีสมบัติพิเศษ ในบทนี้คือจำนวนสมบูรณ์ (perfect number) และเรื่องที่เกี่ยวข้องคือ จำนวนแมร์แซน (Mersenne number) และจำนวนแฟร์มา (Ferma number) เราจะเริ่มต้นด้วยจำนวนสมบูรณ์ ดังบทนิยามต่อไปนี้ (สมใจ จิตพิทักษ์. 2547 : 153, Raji W. 2013 : 82, Rosen K. H. 2005 : 257)

บทนิยาม 5.5.1 : จำนวนสมบูรณ์ (perfect number)

จำนวนเต็มบวก n จะเรียกว่า **จำนวนสมบูรณ์ (perfect number)** ถ้า $\sigma(n) = 2n$

ตัวหารที่เป็นบวกของ n ที่มีค่าน้อยกว่า n บางครั้งเรียกว่า **ตัวหารแท้ (proper divisors)** ของ n ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5.5.1

จำนวนสมบูรณ์ตัวแรกคือ 6 เพราะว่า 1, 2 และ 3 เป็นตัวหารแท้ของ 6
จะได้ $6 = 1 + 2 + 3$
ดังนั้น $\sigma(6) = 2(6) = 12$
จำนวนสมบูรณ์ตัวที่สอง คือ 28
เนื่องจาก $28 = 1 + 2 + 4 + 7 + 14$
ดังนั้น $\sigma(6) = 2(28) = 56$
นั่นคือ 6 และ 28 เป็นจำนวนสมบูรณ์

ในอีลีเมต์เล่ม 9 (Elements, Book IX) ยุคลิดพบว่าถ้าผลบวก

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = p$$

เป็นจำนวนเฉพาะแล้ว $2^{k-1} \cdot p$ เป็นจำนวนสมบูรณ์ (ซึ่งเป็นจำนวนคู่) จากสูตรผลบวกของอนุกรมเรขาคณิต

$$1 + 2 + 2^2 + 2^3 \cdots + 2^{k-1} = 2^k - 1$$

ทฤษฎีของยุคลิดอาจเขียนได้ ดังทฤษฎีบทต่อไปนี้ (สมใจ จิตพิทักษ์. 2547 : 155, David M. Burton. 2002 : 211, Raji W. 2013 : 83)

ทฤษฎีบท 5.5.1

จำนวนเต็มบวก n เป็นจำนวนสมบูรณ์คู่ ก็ต่อเมื่อ

$$n = \left(2^{k-1}\right)\left(2^k - 1\right)$$

สำหรับจำนวนเต็ม k ซึ่ง $k \geq 2$ และ $2^k - 1$ เป็นจำนวนเฉพาะ

การพิสูจน์ ($\Rightarrow$) จะแสดงว่า ถ้า $n = \left(2^{k-1}\right)\left(2^k - 1\right)$ ซึ่ง k เป็นจำนวนเต็ม
จะได้ว่า $k \geq 2$ และ $2^k - 1$ เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนสมบูรณ์
สังเกตว่า $2^k - 1$ เป็นจำนวนคี่ จะได้ว่า $\left(2^{k-1}, 2^k - 1\right) = 1$ และ σ เป็นฟังก์ชันเชิงการแยกคูณ
ดังนั้น $\sigma(n) = \sigma\left(2^{k-1}\right)\sigma\left(2^k - 1\right)$
จะได้ $\sigma\left(2^{k-1}\right) = \sigma\left(2^k - 1\right)$ และเนื่องจาก $\left(2^k - 1\right)$ เป็นจำนวนเฉพาะ
จะได้ว่า $\sigma\left(2^k - 1\right) = 2^k$ ดังนั้น $\sigma(n) = 2n$
($\Leftarrow$) ในทางกลับกัน สมมติว่า n เป็นจำนวนสมบูรณ์
ให้ $n = 2^r s$ ซึ่ง r และ s เป็นจำนวนเต็มบวก และ s เป็นจำนวนคี่
เนื่องจาก $(2^r, s) = 1$ จะได้ว่า

$$\sigma(n) = \sigma\left(2^r\right)\sigma(s) = \left(2^{r+1} - 1\right)\sigma(s)$$

จาก n เป็นจำนวนสมบูรณ์ จะได้ $\left(2^{r+1} - 1\right)\sigma(s) = 2^{r+1} \cdot s$
สังเกตว่า $(2^{r+1} - 1, 2^{r+1}) = 1$ และดังนั้น $2^{r+1} \mid \sigma(s)$
จะมีจำนวนเต็ม q ที่ทำให้ $\sigma(s) = 2^{r+1} \cdot q$ จะได้ว่า

$$\left(2^{r+1} - 1\right)\left(2^{r+1} \cdot q\right) = 2^{r+1} \cdot s$$

ดังนั้น

$$\left(2^{r+1} - 1\right) q = s \qquad \cdots (*)$$

จะได้ว่า $q \mid s$ ดังนั้น บวก q เข้าไปทั้งสองข้างของสมการ $(*)$ จะได้

$$s + q = \left(2^{r+1} - 1\right) q + q = 2^{r+1} q = \sigma(s)$$

ต้องแสดงว่า $q = 1$ จะได้ว่า ถ้า $q \neq 1$ แล้ว s จะมีตัวหารที่เป็นบวกของ s ที่แตกต่างกัน
อย่างน้อย 3 ตัว ดังนั้น $\sigma(s) \geq 1 + s + q$
ดังนั้น $q = 1$ และ $s = 2^{r+1} - 1$ จะได้ว่า $\sigma(s) = s + 1$
จะได้ว่า s เป็นจำนวนเฉพาะ เนื่องจากมีเพียง 1 และ s ที่หารลงตัว
นั่นคือ $n = (2^r)(2^{r+1} - 1)$ ซึ่ง $2^{r+1} - 1$ เป็นจำนวนเฉพาะ □

จากทฤษฎีบท 5.5.1 สามารถเขียนจำนวนสมบูรณ์คู่ในรูปแบบ $2^k - 1$ และ k ต้องเป็นจำนวนเฉพาะ ดังทฤษฎีบทต่อไปนี้ (Raji W. 2013 : 84, Rosen K. H. 2005 : 258)

ทฤษฎีบท 5.5.2

ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ ซึ่ง k เป็นจำนวนเต็มบวก แล้ว k เป็นจำนวนเฉพาะ

การพิสูจน์ สมมติว่า k ไม่เป็นจำนวนเฉพาะ จะได้ว่า $k = rs$
ซึ่ง $1 < r < k$ และ $1 < s < k$ สำหรับจำนวนเต็ม r และ s
จะได้ว่า $2^k - 1 = 2^{rs} - 1 = \left(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1\right)$
จาก $r > 1$ และ $(2^r - 1) > 1$ หาร $\left(2^k - 1\right)$ ลงตัว
จึงทำให้ได้ว่า $2^k - 1$ ไม่เป็นจำนวนเฉพาะ ซึ่งขัดแย้งกับที่สมมติ
ดังนั้น k เป็นจำนวนเฉพาะ □

จากทฤษฎีบท 5.5.2 เราพบว่าสำหรับจำนวนเฉพาะที่อยู่ในรูป 2^k-1 เราพิจารณาเพียงว่า จำนวนเต็ม k เป็นจำนวนเฉพาะ ผู้ที่ศึกษารูปแบบนี้เป็นนักคณิตศาสตร์ชาวฝรั่งเศสชื่อ มาแร็ง แมร์แซน (Marin Mersenne, ค.ศ. 1588-1648) ซึ่งเรียกจำนวนนี้ว่าจำนวนแมร์แซน ดังบทนิยามต่อไปนี้ (Raji W. 2013 : 84, Rosen K. H. 2005 : 258)

บทนิยาม 5.5.2 : จำนวนแมร์แซน (Mersenne numbers)

ถ้า k เป็นจำนวนเต็ม จำนวนเต็มที่อยู่ในรูป $M_k=2^k-1$ จะเรียกว่า **จำนวนแมร์แซน (Mersenne numbers)** ถ้า M_k เป็นจำนวนเฉพาะ จะเรียกว่า **จำนวนเฉพาะแมร์แซน (Mersenne prime numbers)**

ตัวอย่าง 5.5.2

$M_7=2^7-1=63$ เป็นจำนวนเฉพาะแมร์แซน
$M_{11}=2^{11}-1=2047=23\cdot 89$ เป็นจำนวนประกอบ

อีกทฤษฎีบทหนึ่งที่น่าสนใจ ที่ช่วยในการพิสูจน์ว่าจำนวนแมร์แซนเป็นจำนวนเฉพาะ ดังทฤษฎีบทต่อไปนี้ (Raji W. 2013 : 85, Rosen K. H. 2005 : 259)

ทฤษฎีบท 5.5.3

ถ้า p เป็นจำนวนเฉพาะ แล้วตัวหารของจำนวนแมร์แซน $M_p=2^p-1$ จะเขียนอยู่ในรูป $2kp+1$ ซึ่ง k เป็นจำนวนเต็มบวก

การพิสูจน์ กำหนดให้ p_1 เป็นการหารจำนวนเฉพาะ $M_p=2^p-1$
โดยทฤษฎีบทเล็กของแฟร์มา จะได้ว่า $p_1 \mid (2^{p_1-1}-1)$
จะได้ว่า $(2^p-1, 2^{p_1-1}-1)=2^{(p,p_1-1)}-1$
เนื่องจาก p_1 เป็นตัวหารร่วมของ 2^p-1 และ $2^{p_1-1}-1$
ดังนั้น ไม่เป็นจำนวนเฉพาะสัมพัทธ์
ดังนั้น $(p,p_1-1)=p$ จะได้ว่า $p \mid (p_1-1)$ จะมีจำนวนเต็มบวก k
ดังนั้น $p_1-1=mp$ จาก p_1 เป็นจำนวนคี่ แล้ว m เป็นจำนวนคู่ ดังนั้น $m=2k$
ดังนั้น $p_1=mp+1=2kp+1$
ทุกตัวหารของ M_p เป็นผลคูณของตัวหารจำนวนเฉพาะของ M_p
แต่ละตัวหารจำนวนเฉพาะของ M_p จะอยู่ในรูป $2kp+1$ □

ตัวอย่าง 5.5.3

$M_{13}=2^{13}-1=8191$ เป็นจำนวนเฉพาะ
โดยทฤษฎีบท 5.5.3 จำนวนเฉพาะทั้งหมดของ M_{13} จะเขียนอยู่ในรูป $2(13)k+1=26k+1$
หรือมีจำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{M_{13}}=\sqrt{8191}\approx 90.504$
จะได้ $2(13)2+1=26(2)+1=53$ เมื่อ $k=2$

$2(13)3+1=26(3)+1=79$ เมื่อ $k=3$

นั่นคือ 53 และ 79 เป็นจำนวนเฉพาะ

ต่อไปเราจะกล่าวถึงจำนวนแฟร์มา (Fermat numbers) ดังทฤษฎีบทต่อไปนี้ (วรรณธิดา ยลวิลาศ. 2560 : 169, Raji W. 2013 : 85)

บทนิยาม 5.5.3 : จำนวนแฟร์มา (Fermat numbers)

ถ้า k เป็นจำนวนเต็มที่ไม่เป็นลบ ที่เขียนอยู่ในรูป $F_k = 2^{2^k} + 1$ จะเรียกว่า **จำนวนแฟร์มา (Fermat numbers)** ถ้า F_k เป็นจำนวนเฉพาะ จะเรียกว่า **จำนวนเฉพาะแฟร์มา (Fermat prime numbers)**

ตัวอย่าง 5.5.4

$F_0 = 2^{2^0} + 1 = 2 + 1 = 3$ $\quad$ $F_1 = 2^{2^1} + 1 = 4 + 1 = 5$

$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$ $\quad$ $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$

$F_4 = 2^{2^+} + 1 = 2^{16} + 1 = 65537$

จากจำนวนในตัวอย่าง 5.5.4 เป็นจำนวนเฉพาะ ทำให้แฟร์มาคาดการณ์ว่าจำนวนแฟร์มาทุกจำนวนเป็นจำนวนเฉพาะ แต่สำหรับ $k = 5$ จะได้ F_5 =4,294,967,297 แต่แฟร์มาไม่ได้สอบข้อคาดการณ์นี้ จนกระทั่งในปี ค.ศ. 1732 ออยเลอร์ได้พิสูจน์ว่า F_5 หารด้วย 641 ลงตัว ดังนั้น F_5 ไม่ใช่จำนวนเฉพาะ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5.5.5

จงแสดงว่า 641 หาร F_5 ลงตัว

จาก $641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$

และจาก $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4 2^{28} + 1 = (641 - 5^4)\, 2^{28} + 1$

$= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1$

$= 641\,(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4)$

จึงได้ว่า $641 \mid F_5$

เราจะพิสูจน์สมบัติเกี่ยวกับจำนวนเหล่านี้ ดังทฤษฎีบทต่อไปนี้ (Raji W. 2013 : 86)

ทฤษฎีบท 5.5.4

สำหรับจำนวนเต็ม k จะได้ว่า $F_0 F_1 F_2 \cdots F_{k-1} = F_k - 2$

การพิสูจน์ เราจะพิสูจน์ทฤษฎีบท โดยเริ่มต้นที่ $k = 1$ จะได้ $F_{1-1} = F_0 = 3$

และ $F_1 - 2 = 5 - 2 = 3$ ดังนั้น $F_0 = F_1 - 2 = 3$ เป็นจริง

สมมติว่า $F_0 F_1 F_2 \cdots F_{k-1} = F_k - 2$

พิจารณา $F_0 F_1 F_2 \cdots F_k = F_{k+1} - 2$

จะได้ว่า $F_0 F_1 F_2 \cdots F_k = (F_k - 2)\, F_k$

$= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) = 2^{k+1} - 1 = F_{k+1} - 2$ $\square$

เราจะใช้ทฤษฎีบท 5.5.5 พิสูจน์จำนวนแฟร์มาเป็นจำนวนเฉพาะสัมพัทธ์กัน (วรรณธิดา ยลวิลาศ. 2560 : 170, Raji W. 2013 : 86)

ทฤษฎีบท 5.5.5

กำหนดให้ m และ n เป็นจำนวนเต็มที่ไม่เป็นลบ และ $m \neq n$ จะได้ว่า $(F_m, F_n) = 1$

การพิสูจน์ โดยไม่เสียนัยทั่วไป สมมติว่า $m < n$ โดยทฤษฎีบท 5.5.2 จะได้ว่า

$$F_0F_1F_2 \cdots F_m \cdots F_{n-1} = F_n - 2$$

สมมติว่ามีตัวหารร่วมของ F_m และ F_n กำหนดให้เป็น d
จะได้ว่า d หาร $F_n - F_0F_1F_2 \cdots F_m \cdots F_{n-1} = 2$ ลงตัว
ดังนั้น $d = 1$ หรือ $d = 2$
แต่เนื่องจาก F_n เป็นจำนวนคี่สำหรับ n ทุกตัว จึงได้ว่า $d = 1$
นั่นคือ F_m และ F_n เป็นจำนวนเฉพาะสัมพัทธ์กัน □

ตัวอย่าง 5.5.6

จากตัวอย่าง 5.5.4 จะเห็นว่า

$(F_0, F_1) = (3, 5) = 1$ $(F_0, F_2) = (3, 17) = 1$
$(F_0, F_3) = (3, 257) = 1$ $(F_1, F_3) = (5, 257) = 1$
$(F_3, F_4) = (257, 65537) = 1$

สรุปท้ายบท

ในบทที่ 5 เราได้กล่าวถึงฟังก์ชันเลขคณิตหรือฟังก์ชันทฤษฎีจำนวน ในบทนี้ได้แนะนำจำนวนและผลบวกของตัวหารที่เป็นบวก ฟังก์ชันเมอบีอุส ฟังก์ชันออยเลอร์-ฟี ฟังก์ชันจำนวนเต็มมากสุด จำนวนสมบูรณ์ จำนวนแมร์แซน และจำนวนแฟร์มา ฟังก์ชันเหล่านี้มีโดเมนเป็นเซตของจำนวนเต็มบวก โดยเฉพาะฟังก์ชันออยเลอร์-ฟีจะเกี่ยวข้องในการหารากปฐมและดรรชนี

แบบฝึกหัดท้ายบทที่ 5

1. จงหาจำนวนตัวหารและผลบวกของตัวหารของจำนวนต่อไปนี้

   (1.1) 122

   (1.2) 1424

   (1.3) 736

   (1.4) $2^3 \cdot 3^5 \cdot 7^2 \cdot 11$

2. จงแสดงว่า $\tau(242) = \tau(243) = \tau(244) = \tau(245)$

3. จงแสดงว่า $\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3) = \tau(n+4)$ ถ้า $n = 40311$

4. จงแสดงว่า ผลบวกของตัวหาร 326^2 และ 407^2 มีค่าเท่ากัน

5. จงแสดงว่าจำนวนต่อไปนี้ $17, 18, 26$ และ 27 มีสมบัติว่า แต่ละจำนวนเท่ากับผลบวกของตัวหารของกำลังสามของจำนวนนั้น

6. สำหรับ $k \geq 2$ จงแสดงว่า $n = 2^{k-1}$ สอดคล้องกับสมการ $\sigma(n) = 2n - 1$

7. จงหาค่าของฟังก์ชันเมอบีอุส ต่อไปนี้

   (7.1) $\mu(12)$

   (7.2) $\mu(50)$

   (7.3) $\mu(10!)$

   (7.4) $\mu(1001)$

8. สำหรับจำนวนเต็มบวก n จงแสดงว่า $\mu(n) = \mu(n+1) = \mu(n+2) = \mu(n+3) = 0$

9. จงหาค่าของ $\mu(n)$ สำหรับจำนวนเต็ม n โดยที่ $100 \leq n \leq 110$

10. สำหรับจำนวนเต็ม $n \geq 3$ จงแสดงว่า $\displaystyle\sum_{k=1}^{n} \mu(k!) = 1$

11. จงหา $\phi(n)$ เมื่อกำหนดจำนวนเต็ม n ให้ดังต่อไปนี้

   (11.1) 406

   (11.2) 1001

   (11.3) 1228

   (11.4) 36000

12. จงแสดงว่า สำหรับ $n = 1586$ จะได้ $\phi(n) = \phi(n+1) + \phi(n+2)$

13. จงแสดงว่า

    (13.1) ถ้า n เป็นจำนวนเต็มคี่ แล้ว $\phi(2n) = \phi(n)$

    (13.2) $\phi(3n) = 3\phi(n)$ ก็ต่อเมื่อ $3 \mid n$

14. จงพิสูจน์ว่า $\phi(n) = \phi(n+2)$ เป็นจริงเมื่อ $n = 2(2p-1)$ โดยที่ p และ $2p-1$ เป็นจำนวนเฉพาะคี่

15. จงพิสูจน์ว่า ถ้า x เป็นจำนวนเต็มแล้ว $\lfloor x \rfloor + \lfloor -x \rfloor = 0$ และ $\lfloor x \rfloor + \lfloor -x \rfloor = -1$

16. จงหากำลังของ 2,3 และ 5 ที่อยู่ในรูปแบบบัญญัติของ 533!

17. จงหาจำนวนเต็มบวก n ที่น้อยที่สุดที่ 5^7 หาร $n!$ ลงตัว

18. จงหาจำนวนเต็มของจำนวนที่ลงท้ายด้วยศูนย์ใน 1000!

19. จงหาจำนวนเต็มที่อยู่ระหว่าง 1000 และ 10000 ที่หารด้วย 7 ลงตัว

20. จงหาจำนวนของจำนวนเต็มที่น้อยกว่า 1000 ที่หารด้วย 3 ลงตัว แต่หารด้วย 4 ไม่ลงตัว

21. จงหาจำนวนสมบูรณ์มา 8 จำนวน

22. จำนวนแมร์แซน $M_p = 2^p - 1$ เมื่อ $p = 2, 3, 5, 7$ และ 11 มีจำนวนใดบ้างที่เป็นจำนวนเฉพาะ

23. จงพิสูจน์ว่า F_k อยู่ในรูป $12k + 5$ เมื่อ $k > 0$

เอกสารอ้างอิง

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จิราภา ลิ้มบุพศิริพร. (2555). **ทฤษฎีจำนวน**. นครปฐม : โรงพิมพ์มหาวิทยาลัยศิลปากร.

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

นภวรรณ นิลศรี. (2553). **ระบบจำนวนเต็มกับการประยุกต์**. นครปฐม : สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร.

ภัททิรา เรืองสินทรัพย์. (2553). **อสมการและสมการเชิงฟังก์ชัน (พิมพ์ครั้งที่ 3)**. กรุงเทพฯ : มูลนิธิ สอวน.

มานะ เอกจริยวงศ์. (2542). **ทฤษฎีจำนวนเบื้องต้น**. ลพบุรี : ศูนย์ตำราและเอกสารทางวิชาการ สถาบันราชภัฏเทพสตรี.

วรรณธิดา ยลวิลาศ. (2560). **ทฤษฎีจำนวน**. กาฬสินธุ์ : คณะศิลปศาสตร์และวิทยาศาสตร์ มหาวิทยาลัยกาฬสินธุ์

วัลลภ เหมวงษ์. (2556). **ทฤษฎีจำนวน**. อุดรธานี : สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี.

สมใจ จิตพิทักษ์. (2547). **ทฤษฎีจำนวน** (พิมพ์ครั้งที่ 3). สงขลา : ภารกิจเอกสารและตำรามหาวิทยาลัยทักษิณ.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน** (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม). กรุงเทพฯ : สถาบันราชภัฏพระนคร.

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

David M. Burton. (2002). **Elementary number theory (5 ed.)**. New York : The McGraw-HillCompanies, Inc.

David M. Burton. (2007). **Elementary number theory (6 ed.)**. New York : The McGraw-HillCompanies, Inc.

Raji W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

Rosen K.H. (2005). **Elementary number theory and its applications (5 ed.)**. Boston : Pearson/Addison Wesley.

แผนบริหารการสอนประจำบทที่ 6

เนื้อหาประจำบท

1. สมการไดโอแฟนไทน์เชิงเส้น
2. ระบบสมการไดโอแฟนไทน์เชิงเส้น
3. สามจำนวนพีทาโกรัส
4. ทฤษฎีบทสุดท้ายของแฟร์มา

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและสมบัติพื้นฐานของสมการไดโอแฟนไทน์เชิงเส้นแก้โจทย์ปัญหาที่กำหนดให้ได้
2. ใช้นิยามและสมบัติพื้นฐานของระบบสมการไดโอแฟนไทน์เชิงเส้นแก้โจทย์ปัญหาที่กำหนดให้ได้
3. ใช้นิยามและสมบัติพื้นฐานของสามจำนวนพีทาโกรัสแก้โจทย์ปัญหาที่กำหนดให้ได้
4. ใช้นิยามและสมบัติพื้นฐานของทฤษฎีบทสุดท้ายของแฟร์มาแก้โจทย์ปัญหาที่กำหนดให้ได้

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 สมการไดโอแฟนไทน์เชิงเส้น
    1.2 ระบบสมการไดโอแฟนไทน์เชิงเส้น
    1.3 สามจำนวนพีทาโกรัส
    1.4 ทฤษฎีบทสุดท้ายของแฟร์มา
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 6
สมการไดโอแฟนไทน์

ไดโอแฟนทัสแห่งอะเล็กซานเดรีย (Dioplants of Alexandria, ค.ศ. 200-284) เป็นนักคณิตศาสตร์ชาวกรีกได้รับการยกย่องว่าเป็น “บิดาของพีชคณิต” ผลงานเรียนที่มีชื่อเสียงมากคือหนังสือเลขคณิต (Arithmetica) ได้ตีพิมพ์หนังสือจำนวน 13 เล่ม แต่มีเหลือไว้ให้ศึกษาเพียง 6 เล่ม ประกอบด้วยการหาผลเฉลยประมาณ 150 ปัญหาปัญหาของไดโอแฟนทัส หลายปัญหากลายเป็นจุดเริ่มต้นของทฤษฎีจำนวนโดยเฉพาะอย่างยิ่ง ไดโอแฟนทัสสนใจผลเฉลยของสมการพีชคณิตที่มีตัวแปรไม่ทราบค่าสองตัวแปรหรือสามตัวแปรได้ โดยมีผลเลยเป็นจำนวนเต็ม

ประวัติช่วงชีวิตของไดโอแฟนทัสไม่ทราบแน่ชัด แต่ทราบช่วงชีวิตของท่านมาจากหนังสือรวมวรรณกรรมกรีก ประมาณ ค.ศ. 500 มีใจความว่า “ชีวิตในวัยเด็กของไดโอแฟนทัสเป็น 1 ใน 6 ของช่วงชีวิตเขา ช่วงในวัยหนุ่มของเขาเป็น 1 ใน 12 ของช่วงชีวิต ต่อมาอีก 1 ใน 7 ของช่วงชีวิตที่เขาได้แต่งงาน และอีก 5 ต่อมาภรรยาของเขาได้ให้กำเนิดบุตรชาย ซึ่งบุตรชายมีชีวิตอยู่เป็นกึ่งหนึ่งของช่วงชีวิตเขาและต่อมาอีก 4 ปีเขาก็ได้เสียชีวิตลง”

ปัญหาดังกล่าวสามารถเขียนเป็นสัญลักษณ์เพื่อหาอายุของไดโอแฟนทัส ได้ดังนี้

ให้ x แทนช่วงชีวิตของไดโอแฟนทัส
จะได้ $x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$
ซึ่งเมื่อหาผลเฉลยของสมการจะได้ว่า ไดโอแฟนทัสมีอายุ 84 ปี

ในปัจจุบันเมื่อกล่าวถึงสมการของไดโอแฟนทัสจะหมายถึงว่าสนใจผลเฉลยที่เป็นจำนวนเต็มเท่านั้นและเรียกสมการเหล่านี้ว่า สมการไดโอแฟนไทน์ (Diophantine equation) เพื่อให้เป็นเกียรติแก่ไดโอแฟนทัส เช่น สมการไดโอแฟนไทน์คือสมการสามจำนวนของพีทาโกรัส $x^2 + y^2 = z^2$ เป็นต้น

6.1 สมการไดโอแฟนไทน์เชิงเส้น

สมการไดโอแฟนไทน์นำมาใช้กับสมการใด ๆ ที่มีหนึ่งตัวแปรหรือมากกว่าหนึ่งตัวแปรและมีผลเฉลยเป็นจำนวนเต็ม ดังบทนิยามต่อไปนี้ (นพพร ธนะชัยขันธ์. 2543 : 130)

บทนิยาม 6.1.1

เรียกสมการใด ๆ ที่มีตัวแปรหนึ่งตัวหรือมากกว่าหนึ่งตัวและผลเฉลยเป็นจำนวนเต็มว่า **สมการไดโอแฟนไทน์ (Diophantine equation)**

ต่อไปจะให้บทนิยามของสมการไดโอแฟนไทน์เชิงเส้น ดังนี้ (นพพร ธนะชัยขันธ์. 2543 : 131, สมวงษ์ แปลงประสพโชค. 2545 : 72)

บทนิยาม 6.1.2

กำหนดให้ $a_1, a_2, \ldots, a_n, b$ ซึ่ง $a_1, a_2, \ldots, a_n$ ไม่เป็นศูนย์ และ $x_1, x_2, \ldots, x_n$ เป็นตัวแปรจำนวน n ตัวแปร เรียกว่า **สมการไดโอแฟนไทน์เชิงเส้น n ตัวแปร (Linear diophantine equation in n variables)** ที่สามารถเขียนในรูป $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$

คำว่า **เชิงเส้น (linear)** ในบทนิยาม 6.1.2 นั้นหมายถึงตัวแปรทุกตัว คือ $x_1, x_2, \ldots, x_n$ ที่ปรากฏในสมการ จะมีเลขยกกำลังเป็นหนึ่งเท่านั้น และไม่มีผลคูณของตัวแปรคู่ใดเลยปรากฏในสมการนั้น

ตัวอย่าง 6.1.1

จงพิจารณาว่าสมการต่อไปนี้เป็นสมการไดโอแฟนไทน์เชิงเส้นหรือไม่

1. $2x + 3y = 5$ เป็นสมการไดโอแฟนไทน์เชิงเส้น 2 ตัวแปร
2. $x^2 + 2y = 3$ ไม่เป็นสมการไดโอแฟนไทน์เชิงเส้น เพราะ x มีเลขชี้กำลังเป็น 2
3. $2xy = 4$ ไม่เป็นสมการไดโอแฟนไทน์เชิงเส้น เพราะมีผลคูณ xy ปรากฏในสมการ
4. $5x + 7y - 9z - w = 1$ เป็นสมการไดโอแฟนไทน์เชิงเส้น 4 ตัวแปร

จำนวนเต็มที่แทนค่าตัวแปรในสมการไดโอแฟนไทน์แล้วทำให้สมการเป็นจริงว่า ผลเฉลย (solution) ดังบทนิยามต่อไปนี้ (นพพร ธนะชัยขันธ์. 2543 : 131, สมวงษ์ แปลงประสพโชค. 2545 : 73)

บทนิยาม 6.1.3

เรียกจำนวนเต็มที่แทนค่าตัวแปรในสมการไดโอแฟนไทน์แล้วทำให้สมการเป็นจริงว่า **ผลเฉลย** (solution) เรียกผลเฉลยที่ประกอบด้วย**ค่าคงตัวไม่เจาะจงที่เป็นจำนวนเต็ม** (integral arbitrary constant) ว่า **ผลเฉลยทั่วไป** (general solution) และเรียกผลเฉยที่มีค่าเป็นจำนวนเต็มที่แน่นอนหรือผลเฉลยที่ได้จากการแทนค่าของค่าคงตัวในผลเฉลยทั่วไปว่า **ผลเฉลยเฉพาะ** (particular solution)

ตัวอย่าง 6.1.2

จงหาผลเฉลยทั่วไปของสมการไดโอแฟนไทน์ $3x + 4y = 26$

วิธีทำ เนื่องจาก $3x + 4y = 26$

เลือกค่าคงตัวไม่เจาะจงที่เป็นจำนวนเต็ม คือ $x = 6 - 4n$ และ $y = 3n + 2$

สำหรับจำนวนเต็ม n นี้เป็นค่าคงตัว

จะได้ $3(6 - 4n) + 4(3n + 2) = 26$ และ $y = 3n + 2$

เป็นผลเฉลยทั่วไปของสมการ $3x + 4y = 26$

เพราะเป็นจำนวนเต็มทำให้สมการเป็นจริง

ตัวอย่าง 6.1.3

จงหาผลเฉลยเฉพาะของสมการไดโอแฟนไทน์ $3x + 4y = 23$

วิธีทำ เนื่องจาก $3x + 4y = 23$

เลือกค่าคงตัวที่แน่นอนที่เป็นจำนวนเต็ม คือ $x = 5$ และ $y = 2$

จะได้ $3(5) + 4(2) = 23$

ดังนั้น $x = 5$ และ $y = 2$ เป็นผลเฉลยเฉพาะของสมการ $3x + 4y = 23$

เพราะเป็นจำนวนเต็มทำให้สมการเป็นจริง
แต่ถ้าเลือกค่าคงตัวที่ไม่เป็นจำนวนเต็ม คือ $x = \frac{7}{3}$ และ $y = 4$
จะได้ $3\left(\frac{7}{3}\right) + 4(4) = 23$ แต่เราไม่เรียก $x = \frac{7}{3}$ และ $y = 4$
ว่าเป็นผลเฉลยของสมการไดโอแฟนไทน์ $3x + 4y = 23$
เพราะว่า $\frac{7}{3}$ ไม่ใช่จำนวนเต็ม

จากตัวอย่าง 6.1.2 และ 6.1.3 เราอาจเรียกผลเฉลยทั่วไปและผลเฉลยเฉพาะสั้น ๆ ว่า ผลเฉลยก็ได้

ตัวอย่าง 6.1.4

จงหาผลเฉลยของสมการไดโอแฟนไทน์ $5x + 6y = 10$ มา 2 ผลเฉลย

วิธีทำ จาก $5x + 6y = 10$
จัดสมการใหม่จะได้ $y = \frac{10 - 5x}{6}$
สมมติค่าของจำนวนเต็ม x เพื่อหาค่าของจำนวนเต็ม y ที่ทำให้สมการเป็นจริง
จะได้ดังตารางที่ 6.1

x	-5	-4	-3	-2	-1	0	1	2	3
y	$\frac{35}{6}$	5	$\frac{25}{6}$	$\frac{20}{6}$	$\frac{15}{6}$	$\frac{10}{6}$	$\frac{5}{6}$	0	$-\frac{5}{6}$

ตารางที่ 6.1 ค่าของจำนวนเต็ม x และ y

จากตารางที่ 6.1 พบว่า $x = -4$ จะได้ $y = 5$ และ $x = 2$ จะได้ $y = 0$
เป็นผลเฉลยของสมการ $5x + 6y = 10$

จากตัวอย่างทั้งหมดที่ได้กล่าวมาจะเห็นว่าบางสมการมีผลเฉลยบางสมการไม่มีผลเฉลย ต่อไปจะเป็นการตรวจสอบว่าสมการไดโอแฟนไทน์เชิงเส้นสองตัวแปรที่กำหนดให้นั้น จะมีผลเฉลยหรือไม่ ดังทฤษฎีบทต่อไปนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 74, ไอริน ชุ่มเมืองเย็น. 2557 : 102)

ทฤษฎีบท 6.1.1

สมการไดโอแฟนไทน์ $ax + by = c$ ซึ่ง $d = (a, b)$ จะมีผลเฉลยเป็นจำนวนเต็มก็ต่อเมื่อ $d \mid c$

การพิสูจน์ ($\Rightarrow$) ให้ x_0, y_0 เป็นจำนวนเต็มซึ่ง $ax_0 + by_0 = c$
ให้ $d = (a, b)$ โดยบทนิยาม 2.4.1 จะได้ว่า $d \mid a$ และ $d \mid b$
ดังนั้น จะได้ว่า $d \mid ax_0$ และ $d \mid by_0$
โดยทฤษฎีบท 2.2.2 ข้อ 8 จะได้ว่า $d \mid (ax_0 + by_0)$
ดังนั้น $d \mid c$
($\Leftarrow$) ให้ $d \mid c$ โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม n ที่ทำให้ $dn = c$
เนื่องจาก $d = (a, b)$ โดยทฤษฎีบท 2.4.2 จะได้ว่า มีจำนวนเต็ม x_1, y_1
ซึ่ง $ax_1 + by_1 = d$ แทนค่า d จะได้ $(ax_1 + by_1)\, n = c$ หรือ $ax_1 n + by_1 n = c$
จะได้ $x_0 - x_1 n$ และ $y_0 - y_1 n$ เป็นผลเฉลยของสมการ $ax + by = c$
นั่นคือ $ax + by = c$ มีผลเฉลยเป็นจำนวนเต็ม $\square$

ตัวอย่าง 6.1.5

จงพิจารณาสมการไดโอแฟนไทน์ต่อไปนี้ มีผลเฉลยหรือไม่

1. $14x - 45y = 11$ โดยทฤษฎีบท 6.1.1 มีผลเฉลยเพราะว่า $(14, -45) = 1$ ซึ่ง $1 \mid 11$
2. $56x - 50y = 74$ โดยทฤษฎีบท 6.1.1 ไม่มีผลเฉลยเพราะว่า $(50, -50) = 2$ ซึ่ง $2 \nmid 74$
3. $6x - 30y = 32$ โดยทฤษฎีบท 6.1.1 ไม่มีผลเฉลยเพราะว่า $(6, 30) = 6$ ซึ่ง $6 \nmid 32$
4. $6x + 51y = 22$ โดยทฤษฎีบท 6.1.1 ไม่มีผลเฉลยเพราะว่า $(6, 51) = 3$ ซึ่ง $3 \nmid 22$
5. $33x + 14y = 115$ โดยทฤษฎีบท 6.1.1 มีผลเฉลยเพราะว่า $(33, 14) = 1$ ซึ่ง $1 \mid 115$
6. $14x + 35y = 93$ โดยทฤษฎีบท 6.1.1 ไม่มีผลเฉลยเพราะว่า $(14, 35) = 7$ ซึ่ง $7 \nmid 93$

จากทฤษฎีบท 6.1.1 ตรวจสอบว่าสมการไดโอแฟนไทน์เชิงเส้นที่กำหนดให้นั้น มีผลเฉลยหรือไม่ และถ้ามีผลเฉลย จะมีผลเฉลยทั้งหมดอยู่เป็นจำนวนเท่าใด ดังทฤษฎีบทต่อไปนี้ (นพพร ธนะชัยขันธ์. 2543 : 134, สมวงษ์ แปลงประสพโชค. 2545 : 74, Testini Benchaporn. 1976 : 34-35)

ทฤษฎีบท 6.1.2

ถ้า $x = x_0$ และ $y = y_0$ เป็นผลเฉลยคู่หนึ่งของสมการไดโอแฟนไทน์ $ax + by = c$ แล้วผลเฉลยทั้งหมดของสมการเขียนอยู่ในรูปทั่วไป คือ $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เมื่อ $d = (a, b)$ และ t เป็นจำนวนเต็ม

การพิสูจน์ การพิสูจน์สำหรับทฤษฎีบทนี้จะแยกเป็น 2 ตอน ดังนี้

ตอนที่ 1 เราจะพิสูจน์ว่า $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เมื่อ $d = (a, b)$ และ t เป็นจำนวนเต็มใด ๆ โดยแทนค่า x และ y ข้างซ้ายของสมการจะได้

$$\begin{aligned} a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{b}{d}t\right) &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

เพราะ x_0, y_0 เป็นผลเฉลยของสมการ
ดังนั้น $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เป็นผลเฉลยของสมการ เมื่อ t เป็นจำนวนเต็ม

ตอนที่ 2 เราจะพิสูจน์ว่า ทุกผลเฉลยของสมการจะสามารถเขียนในรูป $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ เป็นผลเฉลยของสมการ เมื่อ t เป็นจำนวนเต็ม
และ x_0 และ y_0 เป็นผลเฉลยคู่หนึ่งของสมการ $ax + by = c$
ให้ x, y เป็นผลเฉลยใด ๆ ของสมการ และ x_0, y_0 เป็นผลเฉลยหนึ่ง
จะได้ $ax + by = c$ และ $ax_0 + by_0 = c$
ดังนั้น $ax + by = ax_0 + by_0$
จะได้ $a(x - x_0) = b(y_0 - y)$
การที่ $d > 0$ ทั้งสองข้างของสมการ จะได้ว่า

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{6.1}$$

โดยบทนิยาม 2.2.1 จะได้ว่า $\frac{b}{d} \mid \left(\frac{a}{d}\right)(x - x_0)$

โดยทฤษฎีบท 2.4.7 ข้อ 3 จะได้ว่า $\frac{b}{d} \mid (x - x_0)$

โดยบทนิยาม 2.2.1 จะได้ว่า $x - x_0 = \left(\frac{b}{d}\right)t$

สำหรับ t เป็นจำนวนเต็ม

ดังนั้น $x = x_0 + \frac{b}{d}t$ แทนค่าของ $x = x_0 + \frac{b}{d}t$ ลงในสมการ 6.1 จะได้

$$\frac{a}{d}\left(x_0 + \left(\frac{b}{d}\right)t - x_0\right) = \frac{b}{d}(y_0 - y)$$

$$\frac{a}{d}\left(\frac{b}{d}\right)t = \frac{b}{d}(y_0 - y)$$

นำ $\frac{b}{d}$ หารตลอดทั้งสมการ

จะได้ $\frac{a}{d}t = (y_0 - y)$

ดังนั้น $y = y_0 - \left(\frac{a}{d}\right)t$

นั่นคือ ทุกผลเฉลยของสมการจะสามารถเขียนในรูป

$x = x_0 + \left(\frac{b}{d}\right)t$ และ $y = y_0 - \left(\frac{a}{d}\right)t$ เป็นผลเฉลยของสมการ เมื่อ t เป็นจำนวนเต็ม □

บทแทรก 6.1.1

ถ้า $(a, b) = 1$ และ x_0, y_0 เป็นผลเฉลยของสมการ $ax + by = c$ แล้ว ทุก ๆ ผลเฉลยของสมการสามารถเขียนได้อยู่ในรูป $x = x_0 + bt$ และ $y = y_0 - at$ เมื่อ t เป็นจำนวนเต็ม

สรุปการหาผลเฉลยของสมการ $ax + by = c$

(1) หา $d = (a, b)$

(2) ตรวจสอบว่า $d \mid c$ หรือ $d \nmid c$

(3) ถ้า $d \nmid c$ แล้วสมการ $ax + by = c$ ไม่ผลเฉลยในระบบจำนวนเต็ม

(4) ถ้า $d \mid c$ เราเขียน $d = ax_1 + by_1$ โดยการใช้ขั้นตอนวิธีแบบยุคลิด

(5) จากการเขียน $c = kd$ สำหรับบาง k ที่เป็นจำนวนเต็ม เราเลือก $x_0 = kx_1$ และ $y_0 = ky_1$

(6) สร้างผลเฉลยทั้งหมด $x = x_0 + \frac{b}{d}t$ และ $y = y_0 - \frac{a}{d}t$ โดยที่ t เป็นจำนวนเต็ม

ตัวอย่าง 6.1.6

จงหาผลเฉลยของสมการไดโอแฟนไทน์ $172x + 20y = 1000$

วิธีทำ ใช้ขั้นตอนของยุคลิดหา ห.ร.ม. ของ 172 และ 20 ดังนี้

$$172 = 8(20) + 12$$

$$20 = 1(12) + 8$$

$$12 = 1(8) + 4$$

$$8 = 2(4)$$

เพราะว่า $(172, 20) = 4$ และ $4 \mid 1000$ ดังนั้นสมการนี้มีผลเฉลย
ต่อไปจะเขียน 4 อยู่ในรูป $172m + 20n$ โดยการย้อนกลับจากขั้นตอนวิธีแบบยุคลิดดังนี้

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2(12) - 20 \\ &= 2(172 - 8(20)) - 20 \end{aligned}$$

ดังนั้น $4 = 2(172) + (-17)(20)$
คูณด้วย 250 จะได้ $1000 = (500)172 + (-4250)20$
จะได้ $x_0 = 500$ และ $y_0 = -4250$ เป็นผลเฉลยเฉพาะ
ดังนั้น คำตอบของสมการคือ $x = 500 + \dfrac{20}{4}t = 500 + 5t$
และ $y = -4250 - \dfrac{172}{4}t = -4250 - 43t$ เมื่อ t เป็นจำนวนเต็ม

จากตัวอย่าง 6.1.6 ความยากลำบากอยู่ที่การหาผลเฉลยชุดแรกแต่สมการ $ax + by = c$ สามารถเขียนในรูปสมภาคเชิงเส้นที่มีสองตัวแปรได้เป็น $ax \equiv c \pmod{b}$ และ $by \equiv c \pmod{a}$

ตัวอย่าง 6.1.7

จงหาผลเฉลยของสมการไดโอแฟนไทน์ $4x - 83y = -6$

วิธีทำ จากสมการไดโอแฟนไทน์

$$4x - 83y = -6 \tag{6.2}$$

โดยทฤษฎีบท 6.1.1 สมการมีผลเฉลยเพราะว่า $(4, -83) = 1$ ซึ่ง $1 \mid -6$
เขียนในรูปสมภาคเชิงเส้นที่มี y เป็นตัวแปร จะได้

$$83y \equiv 6 \pmod{4}$$

แต่ $83y \equiv -y \pmod{4}$ และ $6 \equiv -2 \pmod{4}$
จาก $-y \equiv 83y \pmod{4}$ และ $83y \equiv 6 \pmod{4}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $-y \equiv 6 \pmod{4}$
จาก $-y \equiv 6 \pmod{4}$ และ $6 \equiv -2 \pmod{4}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $-y \equiv -2 \pmod{4}$
ดังนั้น $y \equiv 2 \pmod{4}$ โดยบทนิยาม 4.1.1
จะได้ $4 \mid (y - 2)$ โดยบทนิยาม 2.2.1
จะได้ว่ามีจำนวนเต็ม t ที่ทำให้ $y - 2 = 4t$ หรือ $y = 2 + 4t$
เมื่อ t เป็นจำนวนเต็ม
แทนค่า $y = 2 + 4t$ ลงในสมการ 6.2 เพื่อหาค่า x
จะได้ว่า $4x - 83(2 + 4t) = -6$ ดังนั้น $x = 40 + 83t$
นั่นคือ ผลเฉลยทั้งหมดของสมการไดโอแฟนไทน์ $4x - 83y = -6$
จะเขียนในรูป $x = 40 + 83t$ และ $y = 2 + 14t$ เมื่อ t เป็นจำนวนเต็ม

ตัวอย่าง 6.1.8

จงหาผลเฉลยที่เป็นจำนวนเต็มบวก (ถ้ามี) ของสมการ $2475x + 420y = 15$

วิธีทำ จาก $(2475, 420) = 15$ และ $2475 \cdot 9 + 420 \cdot (-53) = 15$
ดังนั้นผลเฉลยทั้งหมดจะอยู่ในรูป

$$x = 9 + \frac{420}{15}t = 9 + 28t \quad \text{และ} \quad y = -53 - \frac{2475}{15}t = -53 - 165t$$

โดยที่ t เป็นจำนวนเต็ม
เราต้องการผลเฉลยเป็นจำนวนเต็มบวก จึงต้องหา t ที่ทำให้

$$9 + 28t > 0 \text{ และ } -53 - 165t > 0$$

นั่นคือ $t > \frac{-9}{28}$ และ $t < \frac{-53}{165}$
ฉะนั้น $\frac{-9}{28}t < t < \frac{-53}{165}$
เนื่องจาก t เป็นจำนวนเต็ม จึงได้ว่าสมการนี้ไม่มีผลเฉลยที่เป็นจำนวนเต็มบวก
ในชีวิตจริงมีอยู่บ่อยครั้งทีเดียวที่เราต้องการแก้สมการในรูป $ax + by = c$ ดังตัวอย่างที่จะแสดงต่อไปนี้

ตัวอย่าง 6.1.9

คุณแม่ให้เงินแพรว 1,500 บาท เพื่อซื้อเสื้อยืดมาไว้ขาย แพรวซื้อเสื้อเสร็จแล้วนำเงินมาคืนคุณแม่ 363 บาท พร้อมกับบอกคุณแม่ว่าเสื้อยืดแขนสั้นราคาตัวละ 39 บาท เสื้อยืดแขนยาวราคาตัวละ 39 บาท จงหาว่าแพรวซื้อเสื้ออย่างละกี่ตัว

วิธีทำ สมมติว่าแพรวซื้อเสื้อแขนสั้นมา x ตัว และซื้อเสื้อแขนยาวมา y ตัว จะได้ว่า

$$39x + 69y = 1137$$

เราทอนสมการในรูปง่ายขึ้น

$$13x + 23y = 379$$

ใช้ขั้นตอนยุคลิดในการหา ห.ร.ม. ของ 13 และ 23 จะได้ว่า

$$\begin{aligned} 23 &= 1(13) + 10 \\ 13 &= 1(10) + 3 \\ 10 &= 3(3) + 1 \\ 3 &= 3(1) \end{aligned}$$

ฉะนั้น $(13, 23) = 1$ และ $\begin{aligned} 1 &= 10 - 3(3) \\ &= 10 - 3(13 - 1(10)) \\ &= 4(10) - 3(13) \\ &= 4(23 - 1(13)) - 3(13) \\ &= (-7)13 + 4(23) \end{aligned}$

ดังนั้น $13 \cdot (-7 \cdot 379) + 23 \cdot (4 \cdot 379) = 379$
จะได้ว่า $x = -2653 + 23t$ และ $y = 1516 - 13t$

โดยที่ t เป็นจำนวนเต็ม เราต้องการให้ $x \geq 0$ และ $y \geq 0$ จึงได้ว่า

$$t \geq \frac{2653}{23} = 115\frac{8}{23} \quad \text{และ} \quad t \leq \frac{1516}{13} = 116\frac{8}{13}$$

ดังนั้น $t = 116$ ซึ่งทำให้ $x = 15$ และ $y = 8$
สรุปได้ว่า แพรวซื้อเสื้อยืดแขนสั้น 15 ตัว และซื้อเสื้อแขนยาวมา 8 ตัว

ตัวอย่าง 6.1.10

รถโดยสารประจำทางคันหนึ่งเก็บเงินค่าโดยสารผู้ใหญ่คนละ 11 บาท และเก็บเด็กคนละ 7 บาท ถ้าวันหนึ่งเก็บค่าโดยสารได้ 657 บาท อยากทราบว่ามีผู้ใหญ่และเด็กโดยสารในวันนั้นที่เป็นไปได้อย่างละกี่คน

วิธีทำ สมมติให้ ตัวแปร x แทนจำนวนผู้โดยสารที่เป็นผู้ใหญ่
และ ตัวแปร y แทนจำนวนผู้โดยสารที่เป็นเด็ก
เขียนเป็นสมการได้ดังนี้

$$11x + 7y = 657 \tag{6.3}$$

โดยทฤษฎีบท 6.1.1 สมการมีผลเฉลยเพราะว่า $(11, 7) = 1$ ซึ่ง $1 \mid 657$
เขียนในรูปสมภาคเชิงเส้นที่มี x เป็นตัวแปร จะได้

$$7y \equiv 657 \pmod{11}$$

แต่ $7y \equiv -4y \pmod{11}$ และ $657 \equiv -36 \pmod{11}$
จาก $-4y \equiv 7y \pmod{11}$ และ $7y \equiv 657 \pmod{11}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $-4y \equiv -36 \pmod{11}$
ดังนั้น $y \equiv 9 \pmod{11}$ โดยบทนิยาม 4.1.1
จะได้ $11 \mid (y - 9)$ โดยบทนิยาม 2.2.1
จะได้ว่ามีจำนวนเต็ม t ที่ทำให้ $y - 9 = 11t$ หรือ $y = 9 + 11t$
เมื่อ t เป็นจำนวนเต็ม แทนค่า $y = 9 + 11t$ ลงในสมการ 6.3
จะได้ว่า $x = 54 - 7t$ เนื่องจากผู้โดยสารเป็นจำนวนเต็มบวก
ดังนั้น ต้องการ $54 - 7t > 0$ และ $9 + 11t > 0$
จะได้ $t < \frac{54}{7}$ และ $t > -\frac{9}{11}$ หรือ $-\frac{9}{11} < t < \frac{54}{7}$
เมื่อ $t = 1, 2, 3, 4, 5, 6, 7$
แทนค่า t เพื่อหาค่า x และ y ลงในสมการ 6.3 จะได้จำนวนผู้โดยสารที่เป็นไปได้ดังตาราง 6.2

t	1	2	3	4	5	6	7
จำนวนผู้ใหญ่ (x)	47	40	33	26	19	12	5
จำนวนเด็ก (y)	20	31	42	53	64	75	86

ตารางที่ 6.2 จำนวนผู้โดยสารในแต่ละวัน

ต่อไปจะหาผลเฉลยของสมภาคเชิงเส้นที่มีสามตัวแปรหรือมากกว่าสามตัวแปร ดังทฤษฎีบทต่อไปนี้ (สมวงษ์ แปลงประสพโชค. 2545 : 78)

ทฤษฎีบท 6.1.3

สมการไดโอแฟนไทน์ $ax + by + cz = n$ มีผลเฉลยก็ต่อเมื่อ $d \mid n$ ซึ่ง $d = (a, b, c)$ และ t เป็นจำนวนเต็มใด ๆ

การพิสูจน์ จัดสมการ $ax + by + cz = n$ ใหม่จะได้

$$ax + by = n - cz$$

ซึ่งสมการจะมีจำนวนเต็ม x และ y ที่สอดคล้องก็ต่อเมื่อ $d_1 \mid (n - cz)$
โดยที่ $d_1 = (a, b)$ เขียนในรูปสมภาค $cz \equiv n \pmod{d_1}$
ซึ่งสมภาคดังกล่าวมีผลเฉลยเป็นจำนวนเต็มก็ต่อเมื่อ $d \mid n$ โดยที่ $d = (d_1, c)$
เนื่องจาก $d = (d_1, c) = ((a, b), c) = (a, b, c)$
ดังนั้น $ax + by + cz = n$ มีผลเฉลยก็ต่อเมื่อ $d \mid n$ โดยที่ $d = (a, b, c)$ □

ตัวอย่าง 6.1.11

จงหาผลเฉลยของสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$

วิธีทำ จากสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$
โดยทฤษฎีบท 6.1.3 สมการมีผลเฉลยเพราะว่า $(3, -6, 2) = 1$ ซึ่ง $1 \mid 11$
จัดสมการใหม่จะได้

$$3x - 6y = 11 - 2z \tag{6.4}$$

จะเห็นว่า $(3, -6) = 3$ ดังนั้น สมการ 6.4 มีผลเฉลยก็ต่อเมื่อ $3 \mid (11 - 2z)$
เราจะหา z ที่ทำให้ $3 \mid (11 - 2z)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$2z \equiv 11 \pmod{3}$$

แต่ $2z \equiv -z \pmod{3}$ และ $11 \equiv -1 \pmod{3}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $-z \equiv -1 \pmod{3}$ หรือ $z \equiv 1 \pmod{3}$
โดยบทนิยาม 4.1.1 จะได้ $3 \mid (z - 1)$ โดยบทนิยาม 2.2.1
จะได้ว่ามีจำนวนเต็ม t_1 ที่ทำให้ $z - 1 = 3t_1$ หรือ $z = 1 + 3t_1$ เมื่อ t_1 เป็นจำนวนเต็ม
แทนค่า $z = 1 + 3t_1$ ลงในสมการ 6.4
จะได้ว่า $3x - 6y = 11 - 2(1 + 3t_1) = 9 - 6t_1$
นำ 3 หารตลอดทั้งสองข้าง จะได้

$$x - 2y = 3 - 2t_1 \tag{6.5}$$

จะเห็นว่า $(1, -2) = 1$ ดังนั้น สมการ 6.5 มีผลเฉลยก็ต่อเมื่อ $1 \mid (3 - 2t_1)$
เราจะหา y ที่ทำให้ $1 \mid (3 - 2t_1)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$-2y \equiv 3 - 2t_1 \pmod{1}$$

แต่ $-2y \equiv -y \pmod{1}$ และ $3 - 2t_1 \equiv 0 \pmod{1}$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $-y \equiv 0 \pmod{1}$ หรือ $y \equiv 0 \pmod{1}$

โดยบทนิยาม 4.1.1 จะได้ $1 \mid y$
โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม t_2 ที่ทำให้ $y = t_2$ เมื่อ t_2 เป็นจำนวนเต็ม
แทนค่า $y = t_2$ ลงในสมการ 6.5 เพื่อหาค่า x
จะได้ว่า $x - 2(t_2) = 3 - 2t_1$
ดังนั้น $x = 3 - 2t_1 + 2t_2$
นั่นคือ ผลเฉลยทั้งหมดของสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$
จะเขียนในรูป $x = 3 - 2t_1 + 2t_2,\ y = t_2$ และ $z = 1 + 3t_1$ เมื่อ t_1, t_2 เป็นจำนวนเต็ม

ตัวอย่าง 6.1.12

จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 9z = 63$

วิธีทำ สมการ $3x - 6y + 9z = 63$ มีคำตอบ เพราะว่า $(3, -6, 9) = 3$ และ $3 \mid 63$
จัดสมการจะได้ $3x - 6y = 63 - 9z \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$
จะเห็นว่า $(3, -6) = 3$ และ $3 \mid (63 - 9z)$ เสมอ สำหรับทุกจำนวนเต็ม z
จึงให้ $z = t_1 \quad$ เมื่อ $t_1 \in \mathbb{Z}$
แทนค่า z ใน (1) จะได้ $3x - 6y = 63 - 9t_1$ นั่นคือ $x - 2y = 21 - 3t_1$
จะเห็นว่า $(1, -2) = 1$ และ $1 \mid (21 - 3t_1)$
ถ้าให้ $y = t_2$ เมื่อ $t_2 \in \mathbb{Z}$ จะได้ว่า $x = 2t_2 + 21 - 3t_1$
ดังนั้นคำตอบของสมการคือ

$$\left.\begin{aligned} x &= 2t_2 + 21 - 3t_1 \\ y &= t_2 \\ z &= t_1 \end{aligned}\right\} \quad \text{เมื่อ } t_1, t_2 \in \mathbb{Z}$$

ตัวอย่าง 6.1.13

จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 2z = 11$

วิธีทำ สมการ $3x - 6y + 2z = 11$ มีคำตอบเพราะว่า $(3, -6, 2) = 1$ และ $1 \mid 11$
จัดสมการจะได้ $3x - 6y = 11 - 2z \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$
จะเห็นว่า $(3, -6) = 3$ ดังนั้นสมการ (1) มีคำตอบก็ต่อเมื่อ $3 \mid (11 - 2z)$
เราจะหา z ที่ทำให้ $3 \mid (11 - 2z)$ โดยเขียนในรูปสมภาค ดังนี้

$$2z \equiv 11 \pmod 3$$

แต่ $2z \equiv -z \pmod 3$ และ $11 \equiv -1 \pmod 3$
ดังนั้น $-z \equiv -1 \pmod 3$ หรือ $z \equiv 1 \pmod 3$
จะได้ $z = 1 + 3t_1$ เมื่อ $t_1 \in \mathbb{Z}$
แทนค่า z ใน (1) จะได้ $3x - 6y = 11 - 2(1 + 3t_1)$

$$x - 2y = 3 - 2t_1 \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

เนื่องจาก $(1, -2) = 1$ และ $1 \mid (3 - 2t_1)$ เป็นจริงเสมอ
ดังนั้น สมการมีคำตอบจาก (2) ให้ $y = t_2$ เมื่อ $t_2 \in \mathbb{Z}$
จะได้ $x = 3 - 2t_1 + 2t_2$

ดังนั้น คำตอบของสมการคือ

$$\left.\begin{aligned} x &= 3 - 2t_1 + 2t_2 \\ y &= t_2 \\ z &= 1 + 3t_1 \end{aligned}\right\} \quad \text{เมื่อ } t_1, t_2 \in \mathbb{Z}$$

ตัวอย่าง 6.1.14

จงหาผลเฉลยของสมการไดโอแฟนไทน์ $27x + 33y + 45z + 77w = 707$

วิธีทำ จากสมการไดโอแฟนไทน์ $27x + 33y + 45z + 77w = 707$
การหาผลเฉลยของสมการไดโอแฟนไทน์นี้จะคล้ายกับตัวอย่าง 6.1.11 ดังนี้
สมการมีผลเฉลยเพราะว่า $(27, 33, 45, 77) = 1$ ซึ่ง $1 \mid 707$
จัดสมการใหม่จะได้

$$27x + 33y + 45z = 707 - 77w \tag{6.6}$$

จะเห็นว่า $(27, 33, 45) = 3$ ดังนั้นสมการ 6.6 มีผลเฉลยก็ต่อเมื่อ $3 \mid (707 - 77w)$
เราจะหา w ที่ทำให้ $3 \mid (707 - 77w)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$77w \equiv 707 \pmod 3$$

แต่ $77w \equiv 2w \pmod 3$ และ $707 \equiv 2 \pmod 3$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $2w \equiv 2 \pmod 3$ หรือ $w \equiv 1 \pmod 3$
โดยบทนิยาม 4.1.1 จะได้ $3 \mid (w - 1)$ โดยบทนิยาม 2.2.1
จะได้ว่ามีจำนวนเต็ม t_1 ที่ทำให้ $w - 1 = 3t_1$ หรือ $w = 1 + 3t_1$ เมื่อ t_1 เป็นจำนวนเต็ม
แทนค่า $w = 1 + 3t_1$ ลงในสมการ 6.6 จะได้ว่า

$$27x + 33y + 45z = 707 - 77(1 + 3t_1) = 630 - 231t_1$$

นำ 3 หารตลอดทั้งสองข้าง จะได้

$$9x + 11y + 15z = 210 - 77t_1 \tag{6.7}$$

จะเห็นว่า $(9, 11, 15) = 1$ ดังนั้น สมการ 6.7 มีผลเฉลยก็ต่อเมื่อ $1 \mid (210 - 77t_1)$
เราจะหา z ที่ทำให้ $1 \mid (210 - 77t_1)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$15z \equiv 210 - 77t_1 \pmod 1$$

แต่ $15z \equiv z \pmod 1$ และ $210 - 77t_1 \equiv 0 \pmod 1$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $z \equiv 0 \pmod 1$
โดยบทนิยาม 4.1.1 จะได้ $1 \mid z$
โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม t_2 ที่ทำให้ $z = t_2$ เมื่อ t_2 เป็นจำนวนเต็ม
แทนค่า $z = t_2$ ลงในสมการ 6.7 จะได้

$$9x + 11y = 210 - 77t_1 - 15t_2 \tag{6.8}$$

จะเห็นว่า $(9, 11) = 1$ ดังนั้น สมการ 6.8 มีผลเฉลยก็ต่อเมื่อ $1 \mid (210 - 77t_1 - 15t_2)$

เราจะหา y ที่ทำให้ $1 \mid (210 - 77t_1 - 15t_2)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$11y \equiv 210 - 77t_1 - 15t_2 \pmod 9$$

แต่ $11y \equiv 2y \pmod 9$
พิจารณา $210 \equiv 12 \pmod 9$

$77t_1 \equiv 14t_1 \pmod 9$

$15t_2 \equiv 6t_2 \pmod 9$

โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $2y \equiv 12 - 14t_1 - 6t_2 \pmod 9$
นำ 2 หารตลอดทั้งสมการจะได้

$$y \equiv 6 - 7t_1 - 3t_2 \pmod 9$$

โดยบทนิยาม 4.1.1 จะได้ $9 \mid y - (6 - 7t_1 - 3t_2)$ โดยบทนิยาม 2.2.1
จะได้ว่ามีจำนวนเต็ม t_3 ที่ทำให้ $y = 6 - 7t_1 - 3t_2 + 9t_3$ เมื่อ t_3 เป็นจำนวนเต็ม
แทนค่า $y = 6 - 7t_1 - 3t_2 + 9t_3$ ลงในสมการ 6.8
จะได้ $9x + 11\,(6 - 7t_1 - 3t_2 + 9t_3) = 210 - 77t_1 - 15t_2$
ดังนั้น $9x = 144 + 18t_2 - 99t_3$
นั่นคือ ผลเฉลยทั้งหมดของสมการไดโอแฟนไทน์ $27x + 33y + 45z + 77w = 707$
จะเขียนในรูป $x = 16 + 2t_2 - 11t_3,\ y = 6 - 7t_1 - 3t_2 + 9t_3,\ z = t_2$
และ $w = 1 + 3t_1$ เมื่อ t_1, t_2 และ t_3 เป็นจำนวนเต็ม

6.2 สมการไดโอแฟนไทน์กำลังสอง

ในหัวข้อนี้จะพิจารณาการหาคำตอบของสมการไดโอแฟนไทน์กำลังสอง ซึ่ง คำตอบของแต่ละสมการจะขึ้นอยู่กับการกำหนด n และเราต้องการจะหาจำนวนเต็ม n ทั้งหมดที่ทำให้สมการมีคำตอบ ดังทฤษฎีบทต่อไปนี้ (ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. 2552 : 186)

ทฤษฎีบท 6.2.1

สมการ $n = x^2 - y^2$ จะมีคำตอบ $x, y \in \mathbb{Z}$ ก็ต่อเมื่อ n เป็นจำนวนเต็มคี่ หรือ $4 \mid n$

การพิสูจน์ ($\Leftarrow$) สมมติว่า n เป็นจำนวนเต็มคี่ ดังนั้นจะมี $k \in \mathbb{Z}$ ที่ทำให้ $n = 2k - 1$
และจะได้ $x^2 - y^2 = (x - y)(x + y) = 2k - 1$
ให้ $x - y = 1$ และ $x + y = 2k - 1$ จะได้ $x = k$ และ $y = k - 1$
ถ้า $4 \mid n$ จะได้ว่ามี $k \in \mathbb{Z}$ ซึ่ง $n = 4k$
ฉะนั้น $x^2 - y^2 = (x - y)(x + y) = n = 4k$
ให้ $x - y = 2$ และ $x + y = 2k$ จะได้ $x = k + 1$ และ $y = k - 1$
($\Rightarrow$) สมมติว่า $n = x^2 - y^2$ มีคำตอบ จะได้ว่า ถ้า $x \equiv y \pmod 2$
จะได้ว่า $2 \mid (x - y)$ และ $2 \mid (x + y)$
ดังนั้น $4 \mid (x^2 - y^2)$ นั่นคือ $4 \mid n$
และถ้า $x \not\equiv y \pmod 2$ จะได้ว่า $x^2 - y^2 = n$ เป็นจำนวนเต็มคี่ □

ตัวอย่างต่อไปนี้จะเป็นการแสดงให้เห็นว่า ถ้า n เป็นจำนวนเต็มคี่ หรือ $4 \mid n$ จะทำให้สมการมีคำตอบเป็นจำนวนเต็ม (ธนัชยศ จำปาหวาย. 2559 : 169)

ตัวอย่าง 6.2.1

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 15$

วิธีทำ เนื่องจาก 15 เป็นจำนวนเต็มคี่ ดังนั้นสมการ $x^2 - y^2 = 15$ มีคำตอบเป็นจำนวนเต็ม

จาก $x^2 - y^2 = (x - y)(x + y)$ จะได้ว่า $(x - y)(x + y) = 15 = 1 \cdot 15 = 3 \cdot 5$

พิจารณาได้ ดังตารางต่อไปนี้

$x - y$	$x + y$	x	y
1	15	8	7
-1	-15	-8	-7
15	1	8	-7
-15	-1	-8	7
3	5	4	1
-3	-5	-4	-1
5	3	4	-1
-5	-3	-4	1

ดังนั้นคำตอบที่สอดคล้องสมการนี้คือ $(8, 7), (8, -7), (-8, 7), (-8, -7), (4, 1), (-4, 1), (4, -1)$ และ $(-4, -1)$

ตัวอย่าง 6.2.2

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 24$

วิธีทำ เนื่องจาก $4 \mid 24$ ดังนั้นสมการ $x^2 - y^2 = 24$ มีคำตอบเป็นจำนวนเต็ม

จาก $x^2 - y^2 = (x - y)(x + y)$ จะได้ว่า $(x - y)(x + y) = 24 = 1 \cdot 24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6$

x, y จะเป็นจำนวนเต็มก็ต่อเมื่อตัวประกอบทั้งคู่เป็นจำนวนคู่พร้อมกัน พิจารณาได้ดังตารางต่อไปนี้

$x - y$	$x + y$	x	y
2	12	7	5
-2	-12	-7	-5
12	2	7	-5
-12	-2	-7	5
4	6	5	1
-4	-6	-5	-1
6	4	5	-1
-6	-4	-5	1

ดังนั้นคำตอบที่สอดคล้องสมการนี้คือ $(7, 5), (7, -5), (-7, 5), (-7, -5), (5, 1), (-5, 1), (5, -1)$ และ $(-5, -1)$

ทฤษฎีบท 6.2.2

ให้ n เป็นจำนวนเต็ม จะได้ว่ามีจำนวนเต็ม x, y, z ที่ทำให้ $n = x^2 + y^2 - z^2$

การพิสูจน์ ให้ n เป็นจำนวนเต็ม จะได้มีจำนวนเต็ม x ที่ทำให้ $n - x^2$ เป็นจำนวนเต็มคี่
ดังนั้นจากทฤษฎีบท 6.2.1 เราพบว่า จะมีจำนวนเต็ม y, z ที่ทำให้ $n - x^2 = y^2 - z^2$
นั่นคือ จะมีจำนวนเต็ม x, y, z ที่ทำให้ $n = x^2 + y^2 - z^2$ □

ตัวอย่าง 6.2.3

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 + y^2 - z^2 = 8$ มาอย่างน้อย 5 ชุดคำตอบ

วิธีทำ พิจารณา $y^2 - z^2 = 8 - x^2$ จะได้ว่า $(y - z)(y + z) = 8 - x^2$
พิจารณา $8 - x^2$ เป็นจำนวนคี่ นั่นคือ x เป็นจำนวนคี่ จะได้ว่าสำหรับบางจำนวนเต็ม k, t
จะได้ $8 - x^2 = 2k + 1$ และ $x = 2t + 1$ แล้ว

$$\begin{aligned} 8 - (2t + 1)^2 &= 2k + 1 \\ 8 - 4t^2 - 4t - 1 &= 2k + 1 \\ 6 - 4t^2 - 4t &= 2k \\ 3 - 2t^2 - 2t &= k \end{aligned}$$

จาก $(y - z)(y + z) = 8 - x^2$ นั่นคือ $(y - z)(y + z) = 2k + 1 = 1 \cdot (2k + 1)$
เลือก $y - z = 1$ และ $y + z = 2k + 1$ จะได้ว่า $y = k + 1$ และ $z = k$
ดังนั้นคำตอบรูปแบบหนึ่งของ สมการ $x^2 + y^2 - z^2 = 8$ นี้คือ

$$\begin{aligned} x &= 2t + 1 \\ y &= k + 1 \\ z &= k \end{aligned}$$

เมื่อ $t, k \in \mathbb{Z}$ และ $k = 3 - 2t^2 - 2t$
ตารางต่อไปนี้แสดงคำตอบบางชุดของสมการ $x^2 + y^2 - z^2 = 8$

t	$k = 3 - 2t^2 - 2t$	$x = 2t + 1$	$y = k + 1$	$z = k$
-1	3	-1	4	3
0	3	1	4	3
1	-1	3	0	-1
2	-9	5	-8	-9
3	-21	7	-20	-21

ดังนั้นคำตอบ 5 ชุด ที่สอดคล้องสมการนี้คือ $(-1, 4, 3), (1, 4, 3), (3, 0, -1), (5, -8, -9)$
และ $(7, -20, -21)$

ตัวอย่าง 6.2.4

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 + y^2 - z^2 = 5$ มาอย่างน้อย 5 ชุดคำตอบ

วิธีทำ พิจารณา $y^2 - z^2 = 5 - x^2$ จะได้ว่า $(y - z)(y + z) = 5 - x^2$
พิจารณา $4 \mid (5 - x^2)$ นั่นคือ $5 - x^2 = 4k$ สำหรับบางจำนวนเต็ม k
จาก $(y - z)(y + z) = 5 - x^2$ นั่นคือ $(y - z)(y + z) = 4k = 2 \cdot 2k$
เลือก $y - z = 2$ และ $y + z = 2k$ จะได้ว่า $y = k + 1$ และ $z = k - 1$
จาก $5 - x^2 = 4k$ เลือก $k = -t^2 + t + 1$ จะได้ว่า

$$\begin{aligned} 5 - x^2 &= 4\left(-t^2 + t + 1\right) \\ 5 - x^2 &= -4t^2 + 4t + 4 \\ x^2 &= 4t^2 - 4t + 1 = (2t - 1)^2 \\ x &= 2t - 1 \end{aligned}$$

ดังนั้นคำตอบรูปแบบหนึ่งของสมการ $x^2 + y^2 - z^2 = 5$ นี้คือ

$$\begin{aligned} x &= 2t - 1 \\ y &= k + 1 \\ z &= k - 1 \end{aligned}$$

เมื่อ $t, k \in \mathbb{Z}$ และ $k = -t^2 + t + 1$
ตารางต่อไปนี้แสดงคำตอบบางชุดของสมการ $x^2 + y^2 - z^2 = 5$

t	$k = -t^2 + t + 1$	$x = 2t - 1$	$y = k + 1$	$z = k - 1$
-1	-1	-3	0	-2
0	1	-1	2	0
1	1	1	2	0
2	-1	3	0	-2
3	-5	5	-4	-6

ดังนันคำตอบ 5 ชุด ที่สอดคล้องสมการนี้คือ $(-3, 0, -2), (-1, 2, 0), (1, 2, 0), (3, 0, -2)$ และ $(5, -4, -6)$

6.3 ระบบสมการไดโอแฟนไทน์เชิงเส้น

บทนิยามต่อไปนี้จะกล่าวถึงการหาผลเฉลยของระบบสมการไดโอแฟนไทน์เชิงเส้น (สมวงษ์ แปลงประสพโชค. 2545 : 82)

บทนิยาม 6.3.1
กำหนดให้ m และ n เป็นจำนวนเต็ม ระบบสมการไดโอแฟนไทน์เชิงเส้นจะประกอบด้วย สมการไดโอแฟนไทน์เชิงเส้น m สมการ และ n ตัวแปร

สมการไดโอแฟนไทน์เชิงเส้นที่มากกว่าหนึ่งสมการ เราสามารถหาผลเฉลยร่วมกันของสมการ โดยนำผลเฉลยในรูปทั่วไปของสมการแรก แทนค่าหาตัวแปรในสมการที่สองเพื่อหาเงื่อนไขที่ทำให้ได้ผลเฉลยของระบบสมการ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.3.1

จงหาผลเฉลยทั่วไปของระบบสมการไดโอแฟนไทน์

$$2x + 3y + 5z = 23 \tag{6.9}$$
$$5x + 7y - z = 16 \tag{6.10}$$

วิธีทำ จากสมการ 6.9 โดยทฤษฎีบท 6.1.3 สมการมีผลเฉลยเพราะว่า $(2, 3, 5) = 1$ ซึ่ง $1 \mid 23$
จัดสมการใหม่จะได้

$$2x + 3y = 23 - 5z \tag{6.11}$$

จะเห็นว่า $(2, 3) = 1$ ดังนั้น สมการ 6.11 มีผลเฉลยก็ต่อเมื่อ $1 \mid (23 - 5z)$
เราจะหา z ที่ทำให้ $1 \mid (23 - 5z)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$5z \equiv 23 \,(\mathrm{mod}\ 1)$$

แต่ $5z \equiv z \,(\mathrm{mod}\ 1)$ และ $23 \equiv 0 \,(\mathrm{mod}\ 1)$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $z \equiv 0 \,(\mathrm{mod}\ 1)$
โดยบทนิยาม 4.1.1 จะได้ $1 \mid z$
โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม t_1 ที่ทำให้ $z = t_1$ เมื่อ t_1 เป็นจำนวนเต็ม
แทนค่า $z = t_1$ ลงในสมการ 6.11 จะได้ว่า

$$2x + 3y = 23 - 5t_1 \tag{6.12}$$

จะเห็นว่า $(2, 3) = 1$ ดังนั้น สมการ 6.12 มีผลเฉลยก็ต่อเมื่อ $1 \mid (23 - 5t_1)$
เราจะหา y ที่ทำให้ $1 \mid (23 - 5t_1)$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$3y \equiv 23 - 5t_1 \,(\mathrm{mod}\ 2)$$

แต่ $3y \equiv y \,(\mathrm{mod}\ 2)$
พิจารณา $23 \equiv 1 \,(\mathrm{mod}\ 2)$

$$5t_1 \equiv t_1 \,(\mathrm{mod}\ 2)$$

โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $y \equiv 1 - t_1 \,(\mathrm{mod}\ 2)$
โดยบทนิยาม 4.1.1 จะได้ $2 \mid [y - (1 - t_1)]$
โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม t_2 ที่ทำให้ $y = 1 - t_1 + 2t_2$ เมื่อ t_2 เป็นจำนวนเต็ม
แทนค่า $y = 1 - t_1 + 2t_2$ ลงในสมการ 6.12 เพื่อหาค่า x
จะได้ว่า $2x + 3(1 - t_1 + 2t_2) = 23 - 5t_1$
จะได้ $2x = 20 - 2t_1 - 6t_2$
นำ 2 หารตลอดทั้งสมการ
ดังนั้น $x = 10 - t_1 - 3t_2$
นั่นคือ ผลเฉลยทั้งหมดของระบบสมการไดโอแฟนไทน์

$$2x + 3y + 5z = 23$$
$$5x + 7y - z = 16$$

จะเขียนในรูป $x = 10 - t_1 - 3t_2, y = 1 - t_1 + 2t_2$ และ $z = t_1$

แทนค่า $x = 10 - t_1 - 3t_2, y = 1 - t_1 + 2t_2$ และ $z = t_1$ ลงในสมการ 6.10
จะได้ $5(10 - t_1 - 3t_2) + 7(1 - t_1 + 2t_2) - t_1 = 16$

$$-13t_1 - t_2 = -41$$

$$13t_1 + t_2 = 41$$

เมื่อ t_1, t_2 เป็นจำนวนเต็ม ที่ทำให้ เงื่อนไขนี้เป็นจริงเพราะว่า $(1, 2) = 1$ ซึ่ง $1 \mid 41$
ให้ $t_1 = T$ เมื่อ T เป็นจำนวนเต็ม จะได้ $t_2 = 41 - 13T$
ดังนั้น ผลเฉลยทั้งหมดของสมการคือ
$x = 10 - T - 3(41 - 13T) = 38T - 113, y = 1 - T + 2(40 - 13T) = 83 - 27T$
และ $z = T$ เมื่อ T เป็นจำนวนเต็ม
จากตัวอย่าง เราสรุปวิธีการหาผลเฉลยของระบบสมการไดโอแฟนไทน์ได้เป็นขั้นตอนดังนี้

ขั้นตอนการหาผลเฉลยของระบบสมการไดโอแฟนไทน์

ขั้นที่ 1 หาผลเฉลยที่เขียนในรูปทั่วไปของสมการใดสมการหนึ่งในระบบก่อน
ขั้นที่ 2 นำผลเฉลยที่เขียนในรูปทั่วไปที่ได้ไปแทนค่าตัวแปรในอีกสมการหนึ่งของระบบจะได้เงื่อนไขที่จะทำให้ผลเฉลยของสมการแรกเป็นผลเฉลยของสมการหลังด้วย
ขั้นที่ 3 นำเงื่อนไขไปแทนในผลเฉลยที่เขียนในรูปทั่วไปของสมการแรก จะได้ผลเฉลยที่สอดคล้องทั้งสองสมการ ซึ่งเป็นผลเฉลยของระบบสมการนั่นเอง

ในการหาผลเฉลยของระบบสมการไดโอแฟนไทน์ เราอาจใช้วิธีการเดียวกันกับการหาผลเฉลยของสมการเชิงเส้นหลายตัวแปร โดยการกำจัดตัวแปรให้เหลือน้อยลง นั่นคือทำสัมประสิทธิ์ของตัวแปรที่จะกำจัดให้เท่ากัน แล้วนำสมการสองสมการมาบวกหรือลบกัน ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.3.2

จงหาผลเฉลยทั่วไปของระบบสมการไดโอแฟนไทน์

$$x + y + z = 31 \tag{6.13}$$

$$x + 4y + 3z = 42 \tag{6.14}$$

วิธีทำ วิธีการกำจัดตัวแปร x โดยนำสมการ $6.14 - 6.13$ จะได้

$$3y + 2z = 11 \tag{6.15}$$

โดยทฤษฎีบท 6.1.1 สมการมีผลเฉลยเพราะว่า $(2, 3) = 1$ ซึ่ง $1 \mid 11$
เราจะหา y ที่ทำให้ $1 \mid 11$ โดยบทนิยาม 4.1.1 เขียนในรูปสมภาค ดังนี้

$$3y \equiv 11 \pmod 2$$

แต่ $3y \equiv y \pmod 2$ และ $11 \equiv 1 \pmod 2$
โดยทฤษฎีบท 4.1.2 ข้อ 2. จะได้ $y \equiv 1 \pmod 2$
โดยบทนิยาม 4.1.1 จะได้ $2 \mid (y - 1)$
โดยบทนิยาม 2.2.1 จะได้ว่ามีจำนวนเต็ม t_1 ที่ทำให้ $y = 1 + 2t_1$ เมื่อ t_1 เป็นจำนวนเต็ม
แทนค่า $y = 1 + 2t_1$ ลงในสมการ 6.15 เพื่อหาค่า z

จะได้ว่า $3(1+2t_1)+2z=11$ ดังนั้น $z=4-3t$
แทนค่า $y=1+2t_1$ และ $z=4-3t_1$ ลงในสมการ 6.13 เพื่อหาค่า x
จะได้ว่า $x+(1+2t_1)+(4-3t_1)=31$
ดังนั้น $x=26+t_1$
นั่นคือ ผลเฉลยทั้งหมดของระบบสมการไดโอแฟนไทน์

$$\begin{aligned} x+y+z&=31\\ x+4y+3z&=42 \end{aligned}$$

จะเขียนในรูป $x=26+t_1,\ y=1+2t_1$ และ $z=4-3t_1$ เมื่อ t_1 เป็นจำนวนเต็ม

6.4 สามจำนวนพีทาโกรัส

ทฤษฎีบทหนึ่งทางเรขาคณิตที่สำคัญมากในระดับมัธยมศึกษา คือ ทฤษฎีบทพีทาโกรัส (Pythagoras' theorem) กล่าวไว้ว่า ผลบวกของจัตุรัสของความยาวด้านประกอบมุมฉากของสามเหลี่ยมมุมฉากเท่ากับจัตุรัสของด้านตรงข้ามมุมฉาก และในทางกลับกันผลบวกของจัตุรัสของความยาวด้านที่สั้นสองด้านเท่ากับจัตุรัสของด้านที่สามแล้วสามเหลี่ยมนั้นเป็นสามเหลี่ยมมุมฉาก เราจะหาสามเหลี่ยมทั้งหมดที่มีความยาวของด้านเป็นจำนวนเต็ม เป็นการหาจำนวนเต็มบวกที่สอดคล้องกับสมการไดโอแฟนไทน์

$$x^2+y^2=z^2$$

เรียกจำนวนเต็มบวกสามจำนวนที่สอดคล้องกับสมการดังกล่าวว่า สามจำนวนพีทาโกรัส (Pythagorean triples) ดังบทนิยามต่อไปนี้ (วสันต์ จินดารัตนาภรณ์. 2549 : 217, Rosen K. H. 2005 : 510)

บทนิยาม 6.4.1
สามจำนวนพีทาโกรัส (Pythagorean triples) เรียกว่าปฐมฐาน ถ้า $(x,y,z)=1$

ตัวอย่าง 6.4.1
จำนวน $3,4,5$ และ $6,8,10$ และ $5,12,13$ เป็นสามจำนวนพีทาโกรัส
เพราะว่า $3^2+4^2=5^2$
$6^2+8^2=10^2$
และ $5^2+12^2=13^2$
ซึ่ง $3,4,5$ และ $5,12,13$ เป็นปฐมฐาน แต่ $6,8,10$ ไม่เป็นปฐมฐาน

สามารถแสดงได้ว่าว่าสามจำนวนพีทาโกรัส หาได้โดยการคูณจำนวนเต็มบวกกับสามจำนวนปฐมฐานของพีทาโกรัส ดังทฤษฎีบทต่อไปนี้ (จารุวรรณ สิงห์ม่วง. 2562 : 148-149)

ทฤษฎีบท 6.4.1
ถ้า $\{x,y,z\}$ เป็นสามจำนวนพีทาโกรัสและ $c\in\mathbb{N}$ จะได้ว่า $\{cx,cy,cz\}$ เป็นจำนวนสามพีทาโกรัส

การพิสูจน์ เนื่องจาก $(cx)^2+(cy)^2=c^2(x^2+y^2)=c^2z^2=(cz)^2$
ดังนั้น cx,cy,cz เป็นสามจำนวนพีทาโกรัส □

ทฤษฎีบท 6.4.2

ถ้า $\{x, y, z\}$ เป็นสามจำนวนพีทาโกรัสและ $d = (x, y, z)$ จะได้ว่า $\left\{\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right\}$ เป็นสามจำนวนพีทาโกรัส และ $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = 1$

การพิสูจน์ เนื่องจาก $\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2+y^2}{d^2} = \frac{z^2}{d^2} = \left(\frac{z}{d}\right)^2$

ดังนั้น $\left\{\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right\}$ เป็นสามจำนวนพีทาโกรัส □

ตัวอย่าง 6.4.2

(1) $\{3, 4, 5\}$ เป็นสามจำนวนพีทาโกรัส ทำให้
$\{2 \cdot 3, 2 \cdot 4, 2 \cdot 5\} = \{6, 8, 10\}$ เป็นสามจำนวนพีทาโกรัสด้วย

(2) $\{10, 24, 26\}$ เป็นสามจำนวนพีทาโกรัส โดยที่ $10^2 + 24^2 = 26^2$ และ $(10, 24, 26) = 2$ ทำให้
$\left\{\frac{10}{2}, \frac{24}{2}, \frac{26}{2}\right\} = \{5, 12, 13\}$ เป็นสามจำนวนพีทาโกรัสด้วย

นอกจากนี้ยังสามารถแสดงได้อีกว่า สามจำนวนพีทาโกรัสจะไม่มีสองจำนวนใด ๆ ซ้ำกัน ดังทฤษฎีบทต่อไปนี้ (วสันต์ จินดารัตนาภรณ์. 2549 : 218)

ทฤษฎีบท 6.4.3

ไม่มีสามจำนวนพีทาโกรัส $\{x, y, z\}$ ซึ่ง $x = y$

การพิสูจน์ จะพิสูจน์โดยข้อขัดแย้ง

ถ้ามีสามจำนวนพีทาโกรัส x, x, z ซึ่งเป็นสามเหลี่ยมหน้าจั่ว และจะได้ว่า $x^2 + x^2 = z^2$
นั่นคือ $z^2 = 2x^2$ จะได้ว่า z^2 เป็นจำนวนคู่ ทำให้ได้ว่า z เป็นจำนวนคู่ด้วย
ให้ $z = 2z_1$ เมื่อ z_1 เป็นจำนวนเต็ม จะได้ว่า $4z_1^2 = 2x^2$ จะได้ว่า x^2 เป็นจำนวนคู่
ทำให้ได้ว่า x เป็นจำนวนคู่ด้วย
ให้ $x = 2x_1$ เมื่อ x_1 เป็นจำนวนเต็ม
จะได้ว่า $z_1^2 = 2x_1^2 = x_1^2 + x_1^2$ เป็นสามเหลี่ยมหน้าจั่วอีกรูปหนึ่ง
และได้สามจำนวนพีทาโกรัสชุดที่ 2 x_1, x_1 และ z_1 ซึ่ง $x > x_1$ และ $z > z_1$
ทำเช่นนี้ไปจะได้สามจำนวนพี่ทาโกรัสชุดที่ 3 x_2, x_2 และ z_2 ซึ่ง $x_1 > x_2$ และ $z_1 > z_2$
ทำเช่นนี้ไปเรื่อย ๆ จะได้สามจำนวนพีทาโกรัสชุดต่อไป
ทำให้ได้ลำดับของจำนวน $x > x_1 > x_2 > \cdots$ เป็นลำดับอนันต์ของจำนวนเต็มบวก
ซึ่งเป็นไปไม่ได้
นั่นคือ ไม่มีสามจำนวนพีทาโกรัส $\{x, y, z\}$ ซึ่ง $x = y$ □

ตัวอย่าง 6.4.3

ถ้าด้านประกอบมุมฉากของรูปสามเหลี่ยมหน้าจั่วมุมฉากยาว a หน่วย
จะได้ว่า ด้านตรงข้ามมุมฉากของรูปสามเหลี่ยมหน้าจั่วมุมฉากนี้ยาว $a\sqrt{2}$ หน่วย
ทำให้ $\{a, a, a\sqrt{2}\}$ ไม่เป็นสามจำนวนพีทาโกรัส

จากทฤษฎีบท 6.4.3 จะได้บทตั้งดังต่อไปนี้ (วสันต์ จินดารัตนาภรณ์. 2549 : 219, Rosen K. H. 2005 : 511)

บทตั้ง 6.4.1

ถ้า x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส จะได้ว่า $(x, y) = (x, z) = (y, z) = 1$

การพิสูจน์ ถ้า x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส จึงได้ว่า $(x, y, z) = 1$
สมมติว่า $(x, y) > 1$ จึงได้ว่า จะมีจำนวนเฉพาะ p โดยที่ $p \mid x$ และ $p \mid y$
เนื่องจาก $p \mid x$ และ $p \mid y$ จะได้ว่า $p \mid (x^2 + y^2)$ ดังนั้น $p \mid z^2$
เพราะว่า $p \mid z^2$ จึงได้ว่า $p \mid z$ ซึ่งขัดแย้งกับที่ $(x, y, z) = 1$
ดังนั้น $(x, y) = 1$ ในทำนองเดียวกัน สามารถพิสูจน์ได้ว่า $(x, z) = (y, z) = 1$ □

บทตั้งต่อไป จะพิสูจน์เกี่ยวกับสมบัติของสามจำนวนปฐมฐานของพีทาโกรัส (วสันต์ จินดารัตนาภรณ์. 2549 : 219, Rosen K. H. 2005 : 511)

บทตั้ง 6.4.2

ถ้า x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส จะได้ว่า $x \not\equiv y \pmod 2$

การพิสูจน์ ถ้า x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส
ทั้ง x, y ไม่เป็นจำนวนคู่หรือเป็นจำนวนคี่พร้อมกัน
โดยบทตั้ง 6.4.1 เราทราบว่า $(x, y) = 1$
ดังนั้น x, y ไม่เป็นจำนวนคู่พร้อมกัน
ถ้าทั้ง x, y เป็นจำนวนคี่ จะได้ว่า

$$x^2 \equiv y^2 \equiv 1 \pmod 4$$

ดังนั้น

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4$$

ซึ่งเป็นไปไม่ได้ เพราะว่า z เป็นจำนวนเต็มคี่
ดังนั้นทั้ง x, y ไม่เป็นจำนวนคี่พร้อมกัน
นั่นคือ x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส แล้ว $x \not\equiv y \pmod 2$ □

บทตั้งสุดท้าย อาศัยทฤษฎีบทหลักมูลของเลขคณิต ดังต่อไปนี้ (วสันต์ จินดารัตนาภรณ์. 2549 : 219, Rosen K. H. 2005 : 512)

บทตั้ง 6.4.3

ถ้า r, s และ t เป็นจำนวนเต็มบวก โดยที่ $(r, s) = 1$ และ $rs = t^2$ จะได้ว่ามีจำนวนเต็ม m และ n ซึ่ง $r = m^2$ และ $s = n^2$

การพิสูจน์ ถ้า $r = 1$ หรือ $s = 1$ เห็นชัดว่าบทตั้งเป็นจริง
สมมติว่า $r > 1$ และ $s > 1$ โดยทฤษฎีบทหลักมูลของเรขาคณิต จะได้ว่า

$$r = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$$
$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v}$$
และ $$t = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$$

จาก $(r,s) = 1$ จึงได้ว่าจำนวนเฉพาะที่เป็นตัวประกอบของ r และ s ต่างกัน
และเนื่องจาก $rs = t^2$ จะได้ว่า

$$rs = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \cdots q_k^{2b_k}$$

โดยทฤษฎีบทหลักมูลของเลขคณิตจะได้ว่าจำนวนเฉพาะทั้งสองด้านของสมการข้างต้นเหมือนกัน
ดังนั้น p_i แต่ละตัวต้องเท่ากับ q_j สำหรับ i บางตัวและมีเลขชี้กำลังเท่ากัน
ดังนั้น $a_i = 2b_j$ ทำให้ได้ว่า a_i เป็นจำนวนคู่ และ $\dfrac{a_i}{2}$ เป็นจำนวนเต็ม
ให้

$$m = p_1^{\frac{a_1}{2}} p_2^{\frac{a_2}{2}} \cdots p_u^{\frac{a_u}{2}}$$

และ

$$n = p_{u+1}^{\frac{a_{u+1}}{2}} p_{u+2}^{\frac{a_{u+2}}{2}} \cdots p_v^{\frac{a_v}{2}}$$

ดังนั้น $r = m^2$ และ $s = n^2$ ซึ่ง m และ n เป็นจำนวนเต็ม □

เราจะพิสูจน์สามจำนวนปฐมฐานทั้งหมดของพีทาโกรัส ดังทฤษฎีบทต่อไปนี้ (วสันต์ จินดารัตนาภรณ์. 2549 : 220, อำพล ธรรมเจริญ. 2523 : 115-116, Rosen K. H. 2005 : 512-513)

ทฤษฎีบท 6.4.4

จำนวนเต็มบวก x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส โดยที่ y เป็นจำนวนเต็มคู่ ก็ต่อเมื่อ มีจำนวนเต็มบวก m และ n โดยที่ $m > n, (m,n) = 1$ และ $m \not\equiv n \pmod 2$ ที่ทำให้

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

การพิสูจน์ กำหนดให้ x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส
โดยบทตั้ง 6.4.2 จะได้ว่า $x \not\equiv y \pmod 2$
สมมติว่า y เป็นจำนวนเต็มคู่ x และ z เป็นจำนวนคี่
จะได้ว่าทั้ง $z + x$ และ $z - x$ เป็นจำนวนคู่ มีจำนวนเต็มบวก r และ s

ซึ่ง $r = \dfrac{(z+x)}{2}$ และ $s = \dfrac{(z-x)}{2}$
เพราะว่า $x^2 + y^2 = z^2$ เราจะได้ $y^2 = z^2 - x^2 = (z+x)(z-x)$
ดังนั้น $\left(\dfrac{y}{2}\right)^2 = \left(\dfrac{z+x}{2}\right)\left(\dfrac{z-x}{2}\right) = rs$
ให้ $(r,s) = d$ จาก $d \mid r$ และ $d \mid s$ จะได้ $d \mid (r+s) = z$ และ $d \mid (r-s) = x$
จึงได้ว่า $d \mid (r,s) = 1$ ดังนั้น $d = 1$

โดยบทตั้ง 6.4.3 จะมีจำนวนเต็มบวก m และ n โดยที่ $r = m^2$ และ $s = n^2$
เขียน x, y และ z ในพจน์ของ m และ n จะได้

$$\begin{aligned} x &= r - s = m^2 - n^2 \\ y &= \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn \\ z &= r + s = m^2 + n^2 \end{aligned}$$

ให้ $(m, n) = e$ จะได้ $e \mid m$ และ $e \mid n$ ทำให้ได้ว่า $e \mid x,\ e \mid y$ และ $e \mid z$
จะได้ว่า $e \mid (x, y, z) = 1$ ดังนั้น $e = 1$
จาก $(m, n) = 1$ และ m และ n ไม่เป็นจำนวนคี่พร้อมกัน จึงได้ว่า $m \not\equiv n \pmod 2$
สมมติว่า มีจำนวนเต็มบวก m และ n โดยที่ $m > n, (m, n) = 1$ และ $m \not\equiv n \pmod 2$
ที่ทำให้ $x = m^2 - n^2,\ y = 2mn$ และ $z = m^2 + n^2$ อยู่ในรูปสามจำนวนพีทาโกรัส
จะได้ $\quad x^2 + y^2 = \left(m^2 - n^2\right) + (2mn)^2$

$$\begin{aligned} &= \left(m^4 - 2m^2n^2 + n^4\right) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= \left(m^2 + n^2\right)^2 \end{aligned}$$

ถ้า $(x, y, z) = d > 1$ จะมีจำนวนเฉพาะ p โดยที่ $p \mid (x, y, z)$
เพราะว่า $x = m^2 - n^2$ และ $m \not\equiv n \pmod 2$ ทำให้ x เป็นจำนวนคี่ จึงได้ว่า $p \neq 2$
และเพราะว่า $p \mid x$ และ $p \mid z$ จะได้ว่า $p \mid (x + z) = 2m^2$ และ $p \mid (x - z) = 2n^2$
ดังนั้น $p \mid m$ และ $p \mid n$ ซึ่งขัดแย้งกับ $(m, n) = 1$
ดังนั้น $(x, y, z) = 1$ และ x, y และ z เป็นสามจำนวนปฐมฐานของพีทาโกรัส □

จารุวรรณ สิงห์ม่วง (2562 : 154-155) ได้เสนอวิธีในการหาสามจำนวนปฐมฐานของพีทาโกรัส โดยกำหนดให้ a เป็นหนึ่งในสามจำนวนปฐมฐานของพีทาโกรัส เราสามารถหาสามจำนวนพีทาโกรัสอีกสองจำนวนที่เหลือ ได้ดังนี้

กรณีที่ 1 ถ้า a เป็นจำนวนเต็มคี่

1. แยกตัวประกอบของ a เป็นผลคูณของสองจำนวนเฉพาะสัมพัทธ์นั่นคือ $a = xy$ โดยที่ $(x, y) = 1$ และถ้า a เป็นจำนวนเฉพาะจะได้ตัวประกอบของ a คือ a และ 1
2. เขียนตัวประกอบที่มีค่ามากในรูป $m + n$ และ เขียนตัวประกอบที่มีค่าน้อยในรูป $m - n$
3. แก้สมการจากข้อ 2 เพื่อหาค่า m และ n
4. หาค่า x, y, z จาก $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$

กรณีที่ 2 ถ้า a เป็นจำนวนเต็มคู่

1. ถ้า $4 \nmid a$ แล้วแสดงว่า a ไม่เป็นหนึ่งในสามจำนวนปฐมฐานของพีทาโกรัส
2. ถ้า $4 \mid a$ เราสามารถดำเนินการต่อไป ดังนี้

(2.1) เขียน a ในรูป $2mn$ โดยที่ $(m, n) = 1$ และมี m หรือ n เป็นจำนวนเต็มคู่และอีกจำนวนหนึ่งเป็นจำนวนเต็มคี่

(2.2) หาค่า x, y, z จาก $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$

ตัวอย่าง 6.4.4

(1) ให้ $m = 5$ และ $n = 2$ โดยที่ $m > n, (m, n) = 1$ และ $m \not\equiv n \pmod 2$
โดยทฤษฎีบท 6.4.4 จะได้ว่า

$$x = m^2 - n^2 = 5^2 - 2^2 = 21$$
$$y = 2mn = 2 \cdot 5 \cdot 2 = 20$$
$$z = m^2 + n^2 = 5^2 + 2^2 = 29$$

ดังนั้น 21, 20 และ 29 เป็นสามจำนวนปฐมฐานของพีทาโกรัส

(2) ให้ $m = 5$ และ $n = 4$ โดยที่ $m > n, (m, n) = 1$ และ $m \not\equiv n \pmod 2$
โดยทฤษฎีบท 6.4.4 จะได้ว่า

$$x = m^2 - n^2 = 5^2 - 4^2 = 9$$
$$y = 2mn = 2 \cdot 5 \cdot 4 = 40$$
$$z = m^2 + n^2 = 5^2 + 4^2 = 41$$

ดังนั้น 9, 40 และ 41 เป็นสามจำนวนปฐมฐานของพีทาโกรัส

ตัวอย่าง 6.4.5

ถ้ากำหนดให้ 45 เป็นจำนวนหนึ่งในสามจำนวนปฐมฐานของพีทาโกรัส จงหาจำนวนที่เหลืออีก 2 จำนวน

วิธีทำ 1) ให้ $45 = 9 \cdot 5$ ซึ่ง $(9, 5) = 1$

ดังนั้น $m + n = 9$ และ $m - n = 5$

โดยการแก้สมการ จะได้ $m = 7$ และ $n = 2$

ดังนั้น $x = m^2 - n^2 = 49 - 4 = 45,$

$y = 2mn = 2(7)(2) = 28,$

$z = m^2 + n^2 = 49 + 4 = 53$

จะได้ว่า $\{45, 28, 53\}$ เป็นสามจำนวนปฐมฐานของพีทาโกรัส

2) ให้ $45 = 45 \cdot 1$ ซึ่ง $(45, 1) = 1$

ดังนั้น $m + n = 45$ และ $m - n = 1$

โดยการแก้สมการ จะได้ $m = 23$ และ $n = 22$

ดังนั้น $x = m^2 - n^2 = 529 - 484 = 45,$

$y = 2mn = 2(23)(22) = 1012,$

$z = m^2 + n^2 = 529 + 484 = 1013$

จะได้ว่า $\{45, 1012, 1013\}$ เป็นสามจำนวนปฐมฐานของพีทาโกรัส

ตารางต่อไปนี้ แสดงสามจำนวนปฐมฐานของพีทาโกรัส เมื่อ $m \leq 6$ ซึ่งหาได้โดยใช้ทฤษฎีบท 6.4.4 (Rosen K. H. 2005 : 514)

m	n	$x = m^2 - n^2$	$y = 2mn$	$z = m^2 + n^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

ตารางที่ 6.3 สามจำนวนปฐมฐานของพีทาโกรัสบางจำนวน

จากตารางที่ 6.3 สามจำนวนปฐมฐานของพีทาโกรัส สังเกตเห็นว่า

1. จำนวนเต็ม x และ y ตัวใดตัวหนึ่งหารด้วย 3 หรือหารด้วย 4 ลงตัว
2. จำนวนเต็ม x, y หรือ z ตัวใดตัวหนึ่งหารด้วย 5 ลงตัว

6.5 ทฤษฎีบทสุดท้ายของแฟร์มา

วรรณธิดา ยลวิลาศ (2560 : 135-136) ได้กล่าวถึงทฤษฎีบทสุดท้ายของแฟร์มา ดังนี้ ในปี ค.ศ. 1637 แฟร์มาได้เขียนเป็นบทสรุปในบันทึกส่วนตัวว่าได้ค้นพบบทพิสูจน์ ของทฤษฎีบทที่ว่า “สมการ $x^n + y^n = z^n$ ไม่มีผลเฉลย x, y และ z ที่เป็นจำนวนเต็มบวก สำหรับทุก ๆ ค่าของจำนวนเต็มบวก n ที่ $n \geq 3$” แต่ไม่แสดงบทพิสูจน์ไว้โดยอ้างว่าเนื้อที่ที่เหลือในบันทึกนั้นไม่พอที่จะเขียนบทพิสูจน์ แต่แฟร์มาได้พิสูจน์เพียงว่าทฤษฎีบทนี้เป็นจริงกรณี $n = 4$ ในปี ค.ศ. 1770 ออยเลอร์พิสูจน์ว่าทฤษฎีบทนี้เป็นจริง สำหรับ $n = 3$ ซึ่งการพิสูจน์นั้นยังมีส่วนบกพร่องอยู่แต่นักคณิตศาสตร์รุ่นต่อมาได้แก้ไขให้ถูกต้องสมบูรณ์สำหรับกรณี $n = 5$ ดีรีเคลและเลอฌ็องดร์พิสูจน์ได้ใน ปี ค.ศ. 1825 ในกรณี $n = 6$ โดยใช้ผลจาก กรณี $n = 3$ สำหรับกรณี $n = 7$ กาเบรียล เลม (Gabriel Lame, ค.ศ. 1795-1870) พิสูจน์ได้ในปี ค.ศ. 1839 ต่อมาในปี ค.ศ. 1857 นักคณิตศาสตร์ชาวเยอรมันชื่อ คุมเมอร์ (Ernst Eduard Kummer, ค.ศ. 1810-1893) พิสูจน์ได้ว่าทฤษฎีบทนี้เป็นจริงสำหรับ n ที่มีค่าน้อยกว่า 100 นับเป็นเวลากว่า 300 ปีที่แฟร์มาได้เสนอทฤษฎีนี้ จนกระทั่งได้มีการตรวจสอบสำหรับ n ที่มีค่ามาก ๆ แต่การพิสูจน์ “ทฤษฎีบท” นี้ ว่าเป็นจริง สำหรับทุก ๆ $n \geq 3$ ยังไม่เป็นที่ทราบกัน จวบจนกระทั่งในปี ค.ศ. 1993 เมื่อ แอนดรูว์ ไวลส์ (Andrew Wiles, ค.ศ. 1953) นักคณิตศาสตร์ชาวอังกฤษ จากมหาวิทยาลัยพรินซ์ตัน ได้ประกาศต่อสาธารณชนว่า สามารถพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มาได้ โดยการจัดบรรยายอย่างต่อเนื่องในวันที่ 21-23 ของเดือนมิถุนายน ค.ศ. 1993 ที่สถาบันนิวตัน ในเมืองเคมบริดจ์ ประเทศอังกฤษ ไวลส์ได้ตรวจสอบบทพิสูจน์พร้อมกับคณะทำงาน จนกระทั่งเดือนธันวาคมในปีเดียวกัน ได้พบข้อบกพร่องของบทพิสูจน์บางประการ ไวลส์และเทย์เลอร์ (Richard Taylor, ค.ศ. 1962) จึงต้องเติมในส่วนที่บกพร่อง ให้ชัดเจนและถูกต้อง และในที่สุดก็สำเร็จลุล่วงในช่วงเดือนกันยายนปี ค.ศ. 1994 ไวลส์ได้พิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มา โดยใช้เครื่องมือในการพิสูจน์คือ เรขาคณิตเชิงพีชคณิต (ในเรื่องเส้นโค้งเชิงวงรีและรูปแบบมอดุลาร์) ทฤษฎีกาโลอิส และพีชคณิต Hecke บทพิสูจน์ของไวลส์และคณะได้รับการตีพิมพ์ลงในวารสาร Annuals of Mathematics เมื่อ ค.ศ. 1995 ไวลส์ใช้เวลา 7 ปีในการพิสูจน์ทฤษฎีบทสุดท้ายของแฟร์มา

สรุปท้ายบท

ในบทที่ 6 ได้กล่าวถึงการหาผลเฉลยของสมการเชิงเส้นที่เป็นจำนวนเต็ม เรียกสมการที่มีผลเฉลยเป็นจำนวนเต็มนี้ว่าสมการไดโอแฟนไทน์ เพื่อให้เป็นเกียรติแก่ไดโอแฟนทัสผู้ที่สนใจผลเฉลยของสมการพีชคณิตโดยมีผลเฉลยเป็นจำนวนเต็ม และยังสามารถหาผลเฉลยที่เป็นจำนวนเต็มของระบบสมการไดโอแฟนไทน์ได้อีกด้วย และในบทนี้ยังได้กล่าวถึงสามจำนวนพีทาโกรัสที่เป็นที่รู้จักกันดีในระดับมัธยมศึกษา ซึ่งสามจำนวนพีทาโกรัสนี้ก็เป็นสามจำนวนที่เป็นจำนวนเต็ม ในตอนท้ายของบทนี้ยังกล่าวถึงทฤษฎีบทสุดท้ายของแฟร์มาไว้อีกด้วย

แบบฝึกหัดท้ายบทที่ 6

1. จงหาผลเฉลยของสมการไดโอแฟนไทน์ต่อไปนี้ (ถ้ามี)

   (1.1) $6x + 8y = 3$

   (1.2) $4x + 33y = 28$

   (1.3) $3x + 4y = 12$

   (1.4) $6x - 15y = 1$

   (1.5) $4x + 9y = 7$

   (1.6) $117x - 6y = 1$

   (1.7) $x + y = 2$

   (1.8) $2x + y = 2$

   (1.9) $15x + 16y = 17$

   (1.10) $6x + 15y = 51$

   (1.11) $7x + 15y = 51$

   (1.12) $15x + 27y = 1$

   (1.13) $2x - 5y + 3z = 17$

   (1.14) $10x + 16y - 4z = 48$

   (1.15) $3x + 6y + 9z = 1$

   (1.16) $7x + 8y + 9z = 1$

2. ชายคนหนึ่งขายเสื้อตัวละ 180 บาท และขายกางเกงตัวละ 280 บาท เขาได้รับ เงิน 2,880 บาท ถามว่าขายไปอย่างละกี่ตัว

3. มีเงิน 50 บาท ต้องการซื้อแสตมป์ดวงละ 50 สตางค์ และดวงละ 1.25 บาทได้กี่วิธี

4. พ่อวัวกินหญ้าวันละ 2 ฟ่อน แม่วัวกินวันละฟ่อนครึ่ง ส่วนลูกวัวกินวันละครึ่งฟ่อน ปรากฏว่า วันหนึ่งหญ้าหมดไป 10 ฟ่อน ถามว่ามีพ่อวัว แม่วัวและลูกวัวอย่างละกี่ตัว

5. 5. ถ้า a, b เป็นจำนวนเต็มบวกและเป็นจำนวนเฉพาะสัมพัทธ์กัน จงพิสูจน์ว่า $ax - by = c$ มีผลเฉลยเป็นจำนวนเต็มบวก จำนวนผลเฉลยนี้นับไม่ถ้วน

6. จงหาผลเฉลยของระบบสมการไดโอแฟนไทน์เชิงเส้นต่อไปนี้

   (6.1) $2x + 2y + 7z = 22$

   (6.2) $2x + 6y + 4z = 3$

   (6.3) $7x - 4y - 5z = 29$

   (6.4) $3x + 2y - z = 4$

7. มีเงิน 100 บาท ต้องการแลกเหรียญ 5 บาท 1 บาท 50 สตางค์ โดยให้มีเหรียญทั้งสามชนิดรวมกัน 100 เหรียญ จะแลกได้กี่วิธี

8. ถุงใบหนึ่งมีเหรียญ 3 ชนิด คือ 5 บาท 1 บาท และ 50 สตางค์รวม 50 เหรียญ รวมเงินทั้งหมด 100 บาท มีเหรียญแต่ละชนิดอย่างละเท่าใด

9. จงหาสามจำนวนพีทาโกรัส a, b, c ซึ่ง $40 < c < 60$

10. สำหรับจำนวนเต็มบวก n จงแสดงว่า $(2n, n^2 - 1, n^2 + 1)$ เป็นสามจำนวนพีทาโกรัส

11. ถ้า (a, b, c) และ (x, y, z) เป็นสามจำนวนปฐมฐานของพีทาโกรัส แล้ว $(an - bx, ax + by, cz)$ เป็นสามจำนวนพีทาโกรัส

12. จงพิสูจน์ว่า $(3, 4, 5)$ เป็นสามจำนวนปฐมฐานของพีทาโกรัสเพียงชุดเดียวที่เป็นลำดับเลขคณิต อยู่ในรูป $(a, a + d, a + 2d)$

13. จงแสดงว่า ถ้า (x, y, z) เป็นสามจำนวนปฐมฐานของพีทาโกรัส แล้ว $12 \mid xyz$

เอกสารอ้างอิง

จารุวรรณ สิงห์ม่วง. (2562). **ทฤษฎีจำนวน**. กรุงเทพฯ : ทริปเปิ้ล เอ็ดดูเคชั่น.

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

วรรณธิดา ยลวิลาศ. (2560). **ทฤษฎีจำนวน**. กาฬสินธุ์ : คณะศิลปศาสตร์และวิทยาศาสตร์ มหาวิทยาลัยกาฬสินธุ์

วสันต์ จินดารัตนาภรณ์. (2549). **ทฤษฎีจำนวน**. เชียงใหม่ : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเชียงใหม่.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

อำพล ธรรมเจริญ. (2523). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 2)**. ชลบุรี : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ บางแสน

ไอริน ชุ่มเมืองเย็น. (2557). **ทฤษฎีจำนวน**. สาขาวิชาคณิตศาสตร์และสถิติ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏนครสวรรค์.

Rosen K.H. (2005). **Elementary number theory and its applications (5 ed.)**. Boston : Pearson/Addison Wesley.

Testini Benchaporn. (1976). **Number Theory**. Bangkok : Ramkhamheang University.

แผนบริหารการสอนประจำบทที่ 7

เนื้อหาประจำบท

1. พหุนาม
2. ทฤษฎีเศษเหลือ
3. เศษส่วนย่อย

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและสมบัติพื้นฐานของพหุนามแก้โจทย์ปัญหาที่กำหนดให้ได้
2. ใช้นิยามและสมบัติพื้นฐานของทฤษฎีเศษเหลือแก้โจทย์ปัญหาที่กำหนดให้ได้
3. ใช้นิยามและสมบัติพื้นฐานของเศษส่วนย่อยแก้โจทย์ปัญหาที่กำหนดให้ได้

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 พหุนาม
    1.2 ทฤษฎีเศษเหลือ
    1.3 เศษส่วนย่อย
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 7
ทฤษฎีบทเศษเหลือ

เมื่อพิจารณาการหารของจำนวนเต็ม เช่น 5 หาร 8 จะเศษเหลือเท่ากับ 3 โดยขั้นตอนวิธีการหารจะเขียนได้เป็น

$$8 = 5(1) + 3$$

อาศัยหลักการที่คล้ายคลึงกันสำหรับการหารของพหุนาม เช่น $x^2 + 2$ หาร $x^3 + 4x - 1$ มีขั้นตอนวิธีการหารคือ

$$x^3 + 4x - 1 = x(x^2 + 2) + (2x - 1)$$

ดังนั้น $x^2 + 2$ หาร $x^3 + 4x - 1$ เศษเหลือเท่ากับ $2x - 1$ และสังเกตได้ว่าเศษเหลือ $2x - 1$ มีดีกรีเท่ากับ 1 ซึ่งน้อยกว่าดีกรีของตัวหาร $x^2 + 2$ ที่มีดีกรีเท่ากับ 2 โดยขั้นตอนวิธีการหารของพหุนามจะมีบทบาทสำคัญต่อการพิสูจน์ทฤษฎีบทต่าง ๆ

7.1 พหุนาม

ในหัวข้อนี้จะกล่าวถึงนิยาม และทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องกับพหุนาม โดยเริ่มต้นด้วยนิยามของพหุนามดังนี้ (ธนัชยศ จำปาหวาย. 2559 : 175)

บทนิยาม 7.1.1

ให้ $n \in \mathbb{N} \cup \{0\}$ แล้ว

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

เรียกว่า **พหุนาม** (polynomial) และ $a_n, a_{n-1}, \ldots, a_1, a_0$ เรียกว่า **สัมประสิทธิ์** (coefficient) ของ $x^n, x^{n-1}, \ldots, x, 1$ ตามลำดับ ถ้า $a_n \neq 0$ เรียกว่า พหุนามดีกรี n และเขียน n แทนด้วย $\deg P(x)$
เรียก $a_n \neq 0$ ว่า **สัมประสิทธิ์ตัวนำ** (leading coefficient)
กรณี $a_n = 1$ เรียก $P(x)$ ว่า **พหุนามโมนิก** (monic polynomial)
กรณี $\deg P(x) = 0$ หรือ $P(x) = a_0 \neq 0$ เรียก $P(x)$ ว่า **พหุนามคงตัว** (constant polynomial)
กรณี $P(x) = 0$ เรียก **พหุนามศูนย์** (zero polynomail) และไม่นิยามดีกรีสำหรับพหุนามศูนย์

กำหนดเซตของพหุนามขึ้นกับชนิดของสัมประสิทธิ์ดังต่อไปนี้

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z} \text{ และ } n \in \mathbb{N} \cup \{0\}\}$$
$$\mathbb{R}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R} \text{ และ } n \in \mathbb{N} \cup \{0\}\}$$
$$\mathbb{C}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{C} \text{ และ } n \in \mathbb{N} \cup \{0\}\}$$

ตัวอย่าง 7.1.1

จงบอกองค์ประกอบของพหุนามต่อไปนี้
(1) $1 + 2x + x^3$
เป็นพหุนามโมนิกดีกรี 3 ที่มี $1, 2, 0, 1$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3$ ตามลำดับ

(2) $-2x^4 + 1.5x - 5$
เป็นพหุนามดีกรี 4 ที่มี $-5, 1.5, 0, 0, -2$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3, x^4$ ตามลำดับ
มีสัมประสิทธิ์ตัวนำคือ -2

จงบอกองค์ประกอบของพหุนามต่อไปนี้

(3) $3x^5 - \frac{3}{5}x^4 + \sqrt{2}$
เป็นพหุนามดีกรี 5 ที่มี $\sqrt{2}, 0, 0, 0, -\frac{3}{5}, 3$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3, x^4, x^5$ ตามลำดับ
มีสัมประสิทธิ์ตัวนำคือ 3

(4) $x^{1.5} + x + 1$
ไม่เป็นพหุนามเนื่องจากมีเลขยกกำลังของ x เป็น 1.5

บทนิยาม 7.1.2

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนาม แล้ว $P(x) = Q(x)$
ถ้า $\deg P(x) = \deg Q(x)$ และอยู่ในรูป

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

เมื่อ $n \in \mathbb{N} \cup \{0\}$ และ $a_n = b_n, a_{n-1} = b_{n-1}, \ldots, a_1 = b_1, a_0 = b_0$

เมื่อพิจารณาพหุนาม $P(x)$ และ $Q(x)$ ในแง่ของฟังก์ชันจะได้ว่า P และ Q เป็นฟังก์ชันบนจำนวนจริง ดังนั้น $P = Q$ ก็ต่อเมื่อ $P(x) = Q(x)$ ทุก ๆ $x \in \mathbb{R}$

บทนิยาม 7.1.3

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนามซึ่ง

$$P(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$
$$Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

เมื่อ $m, n \in \mathbb{N} \cup \{0\}$ และ $m \leq n$ แล้ว

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_{m+1}x^{m+1} + a_m x^m + \cdots + a_1 x + a_0$$

โดยที่ $a_{m+1} = a_{m+2} = \cdots = a_n = 0$ เมื่อ $m < n$

นิยามการบวกและการคูณ $P(x)$ และ $Q(x)$ คือ

$$P(x) + Q(x) = (a_n + b_n)\, x^n + (a_{n-1} + b_{n-1})\, x^{n-1} + \cdots + (a_1 + b_1)\, x + (a_0 + b_0)$$
$$P(x) \cdot Q(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_k x^k + \cdots + c_1 x + c_0$$

เมื่อ $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ โดยที่ $k = 0, 1, 2, \ldots, m+n$
ซึ่ง $a_k = b_k = 0$ ทุก ๆ $k > n$

สำหรับการคูณอาจทำได้โดยการใช้กฎการแจกแจงจากนั้นรวมพจน์ที่คล้ายกันเข้าด้วยกัน หรืออาจใช้ grid method ทำได้ดังนี้ (Josip Hercet, Lorraine Heienrichs, Palmira Mariz Seiler and Marlence Torres Skoumal. 2012 : 123)

	a_mx^m	$a_{m-1}x^{m-1}$	$a_{m-2}x^{m-2}$	$\cdots$	a_1x	a_0
b_nx^n	$a_mb_nx^{m+n}$	$a_{m-1}b_nx^{m+n-1}$	$a_{m-2}b_nx^{m+n-2}$	$\cdots$	$a_1b_nx^{n+1}$	$a_0b_nx^n$
$b_{n-1}x^{n-1}$	$a_mb_{n-1}x^{m+n-1}$	$a_{m-1}b_{n-1}x^{m+n-2}$	$a_{m-2}b_{n-1}x^{m+n-3}$	$\cdots$	$a_1b_{n-1}x^n$	$a_0b_{n-1}x^{n-1}$
$b_{n-2}x^{n-2}$	$a_mb_{n-2}x^{m+n-2}$	$a_{m-1}b_{n-2}x^{m+n-3}$	$a_{m-2}b_{n-2}x^{m+n-4}$	$\cdots$	$a_1b_{n-2}x^{n-1}$	$a_0b_{n-2}x^{n-2}$
$\vdots$				$\vdots$		
b_1x	$a_mb_1x^{m+1}$	$a_{m-1}b_1x^{m-2}$	$a_{m-2}b_1x^{m-3}$	$\cdots$	$a_1b_1x^2$	a_0b_1x
b_0x	$a_mb_0x^m$	$a_{m-1}b_0x^{m-1}$	$a_{m-2}b_0x^{m-2}$	$\cdots$	a_1b_0x	a_0b_0

ตารางที่ 7.1 แสดงผลคูณของสองพหุนามโดย grid method

โดยผลในตารางคือผลคูณของแต่ละพจน์ จะสังเกตเห็นว่าพจน์ที่คล้ายกันจะอยู่ในแนวทแยงขวาไปทางซ้ายทำให้วิธีนี้ง่ายต่อการคำนวณเมื่อคูณพหุนามดีกรีสูงและมีหลายพจน์ที่ไม่เป็นศูนย์

ตัวอย่าง 7.1.2

กำหนดให้ $P(x)=x^3+x^2-3x+1$ และ $Q(x)=x^2-3$ จงหา $P(x)+Q(x)$ และ $P(x)\cdot Q(x)$

วิธีทำ จะได้ว่า

$$\begin{aligned}P(x)+Q(x) &= \big(x^3+x^2-3x+1\big)+\big(x^2-3\big) = \big(x^3+x^2-3x+1\big)+\big(0x^3+x^2+0x-3\big)\\ &= (1+0)x^3+(1+1)x^2+(-3+0)x+(1-3)\\ &= x^3+2x^2-3x-2\end{aligned}$$

สำหรับการคูณ $P(x)\cdot Q(x)$ จะแสดงให้วิธีการคูณทั้ง 3 วิธี ดังนี้

1. โดยบทนิยาม ให้ $a_0=1, a_1=-3, a_2=1, a_3=1, a_4=a_5=0$ และ $b_0=-3, b_1=0, b_2=1, b_3=b_4=b_5=0$ จะได้ว่า

$$\begin{aligned}
c_0 &= a_0b_0 && = 1(-3) && = -3\\
c_1 &= a_0b_1+a_1b_0 && = 0-3(-3) && = 9\\
c_2 &= a_0b_2+a_1b_1+a_2b_0 && = 1(1)+0+1(-3) && = -2\\
c_3 &= a_0b_3+a_1b_2+a_2b_1+a_3b_0 && = 0-3(1)+0+1(-3) && = -6\\
c_4 &= a_0b_4+a_1b_3+a_2b_2+a_3b_1+a_4b_0 && = 0+0+1(1)+0+0 && = 1\\
c_5 &= a_0b_5+a_1b_4+a_2b_3+a_3b_2+a_4b_1+a_5b_0 && = 0+0+0+1(1)+0+0 && = 1
\end{aligned}$$

ดังนั้น

$$\begin{aligned}P(x)\cdot Q(x) &= \big(x^3+x^2-3x+1\big)\big(x^2-3\big)\\ &= c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0\\ &= x^5+x^4-6x^3-2x^2+9x-3\end{aligned}$$

2. โดยวิธีการแจกแจง

$$\begin{aligned} P(x)\cdot Q(x) &= \big(x^3+x^2-3x+1\big)\big(x^2-3\big) \\ &= x^5-3x^3+x^4-3x^2-3x^3+9x+x^2-3 \\ &= x^5+x^4-6x^3-2x^2+9x-3 \end{aligned}$$

3. โดย grid method

	x^3	x^2	$-3x$	1
x^2	x^5	x^4	$-3x^3$	x^2
$0x$	$0x^4$	$0x^3$	$0x^2$	$0x$
-3	$-3x^3$	$-3x^2$	$9x$	-3

ดังนั้น

$$\begin{aligned} P(x)\cdot Q(x) &= x^5+(1+0)x^4+(-3+0-3)x^3+(1+0-3)x^2+(0+9)x^3 \\ &= x^5+x^4-6x^3-2x^2+9x-3 \end{aligned}$$

ตัวอย่าง 7.1.3

กำหนด ให้ $Ax^3+Bx^2+Cx+D=(x-2)(x+3)(x+1)+7$ ทุก ๆ $x\in\mathbb{R}$
จงหาค่าของ A,B,C และ D

วิธีทำ พิจารณา

$$\begin{aligned} Ax^3+Bx^2+Cx+D &= (x-2)(x+3)(x+1)+7 \\ &= \big(x^2+x-6\big)\,(x+1)+7 \\ &= x^3+2x^2-5x+1 \end{aligned}$$

ดังนั้น $A=1,B=2,C=-5$ และ $D=1$

ตัวอย่าง 7.1.4

ถ้า a,b,c และ d เป็นจำนวนเต็มซึ่ง $(x-1)^2(ax+b)=cx^3+dx+4$ ทุก ๆ $x\in\mathbb{R}$ แล้ว $a+b+c+d$ เท่ากับเท่าใด

วิธีทำ พิจารณา

$$\begin{aligned} (x-1)^2(ax+b) &= cx^3+dx+4 \\ (x^2-2x+1)(ax+b) &= cx^3+dx+4 \\ ax^3+(b-2a)x^2+(a-2b)x+b &= cx^3+dx+4 \end{aligned}$$

จะได้ว่า $b=4, a-2b=d, b-2a=0$ และ $a=c$ ดังนั้น $a=2,c=2,d=-6$
แล้วจะได้ว่า $a+b+c+d=2+4+2-6=2$

ตัวอย่าง 7.1.5

จงหาค่าของ A, B และ C ที่ทำให้

พหุนาม $A(x-1)(x-2)+B(x-1)(x-3)+C(x-2)(x-3)$ เท่ากับพหุนามคงตัว 1

วิธีทำ สำหรับจำนวนจริง x ใด ๆ จะได้ว่า

$$A(x-1)(x-2)+B(x-1)(x-3)+C(x-2)(x-3)=1$$

เมื่อ $x=1$ จะได้ว่า $A(0)(-1)+B(0)(-2)+C(-1)(-2)=1$ นั่นคือ $2C=1$ ดังนั้น $C=\frac{1}{2}$
เมื่อ $x=2$ จะได้ว่า $A(1)(0)+B(1)(-1)+C(0)(-1)=1$ นั่นคือ $-B=1$ ดังนั้น $B=-1$
เมื่อ $x=3$ จะได้ว่า $A(2)(1)+B(2)(0)+C(1)(0)=1$ นั่นคือ $2A=1$ ดังนัน $A=\frac{1}{2}$

ตัวอย่าง 7.1.6

ให้ $P(x)\in\mathbb{Z}[x]$ ซึ่ง $P(x)=x^4+2x^3-3x^2+ax+b$ ถ้าพหุนาม $Q(x)$ ทำให้ $P(x)=[Q(x)]^2$ จงหา $a+b$

วิธีทำ เนื่องจาก $\deg P(x)=4$ และ $P(x)=[Q(x)]^2$ ดังนั้น $\deg Q(x)=2$ ให้ $Q(x)=cx^2+dx+e$
พิจารณา

$$\begin{aligned}x^4+2x^3-3x^2+ax+b&=\left(cx^2+dx+e\right)^2\\&=c^2x^4+d^2x^2+e^2+2cdx^3+2cex^2+2dex\\&=c^2x^4+2cdx^3+(d^2+2ce)x^2+2dex+e^2\end{aligned}$$

จะได้ว่า $c^2=1, 2cd=2, d^2+2ce=-3, 2de=a$ และ $b=e^2$
กรณี $c=1$ จะได้ว่า $d=1, e=-2, a=-4$ และ $b=4$ ดังนั้น $a+b=0$
กรณี $c=-1$ จะได้ว่า $d=-1, e=-2, a=4$ และ $b=4$ ดังนัน $a+b=8$

ทฤษฎีบท 7.1.1

ให้ $P(x), Q(x)\in\mathbb{Z}[x]$ ซึ่ง $P(x)$ และ $Q(x)$ ไม่ใช่พหุนามศูนย์ จะได้ว่า

$$\deg(P(x)+Q(x))\leq\max\{\deg P(x),\deg Q(x)\}$$
$$\deg(P(x)\cdot Q(x))=\deg P(x)+\deg Q(x)$$

เมื่อ $\max\{\deg P(x),\deg Q(x)\}$ คือค่ามากสุดของ $\deg P(x)$ แจะ $\deg Q(x)$

การพิสูจน์ ให้ $P(x), Q(x)\in\mathbb{Z}[x]$ ซึ่ง $\deg P(x)=m$ และ $\deg Q(x)=n$ ให้

$$\begin{aligned}P(x)&=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0 &&\text{เมื่อ } a_m\neq0\\Q(x)&=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0 &&\text{เมื่อ } b_n\neq0\end{aligned}$$

โดยไม่เสียนัยทั่วไป สมมติว่า $m\leq n$ จะได้ว่า

$$P(x)+Q(x)=(a_n+b_n)\,x^n+(a_{n-1}+b_{n-1})\,x^{n-1}+\cdots+(a_1+b_1)\,x+(a_0+b_0)$$

โดยที่ $a_{m+1} = a_{m+2} = \cdots = a_n = 0$ เมื่อ $m < n$
ดังนั้น $\deg\,(P(x)+Q(x)) \leq n = \max\{\deg P(x), \deg Q(x)\}$
พิจารณา

$$P(x)\cdot Q(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_k x^k + \cdots + c_1 x + c_0$$

เมื่อ $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$ โดยที่ $k = 0, 1, 2, \ldots, m+n$
ซึ่ง $a_k = b_k = 0$ ทุก ๆ $k > n$
เนื่องจาก $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_{m-1}b_{n+1} + a_mb_n + a_{m+1}b_{n-1} + \cdots + a_{m+n}b_0$
และ $a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_{m-1}b_{n+1} = 0$ และ $a_{m+1}b_{n-1} + \cdots + a_{m+n}b_0 = 0$
และ $a_mb_n \neq 0$
ดังนั้น $c_{m+n} = a_mb_n \neq 0$ ทำให้ได้ว่า $\deg(P(x)\cdot Q(x)) = m+n = \deg P(x) + \deg Q(x)$ □

ขั้นตอนวิธีการหารพหุนาม มีหลักการที่คล้ายคลึงกันกับวิธีการหารจำนวนเต็ม ดังจะกล่าวในทฤษฎีบทต่อไปนี้ (ธนัชยศ จำปาหวาย. 2559 : 179-181, ฉวีวรรณ รัตนประเสริฐ. 2552 : 113-114)

ทฤษฎีบท 7.1.2 : ขั้นตอนวิธีการหาร (The Division Algorithm)

ให้ $P(x)$ และ $S(x)$ เป็นพหุนาม โดยที่ $S(x)$ ไม่ใช่พหุนามศูนย์ แล้วจะมีพหุนาม $Q(x)$ และ $R(x)$ เพียงคู่เดียวที่สอดคล้องกับ

$$P(x) = Q(x)S(x) + R(x) \quad \text{เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x)$$

เรียก $Q(x)$ ว่า**ผลหาร** และ $R(x)$ ว่า**เศษเหลือ**

ข้อสังเกต ถ้า $R(x) = 0$ แล้วจะได้ว่า $S(x)$ หาร $P(x)$ ลงตัว หรือ $S(x)$ เป็นตัวประกอบของ $P(x)$

การพิสูจน์ ให้ $P(x)$ และ $S(x)$ เป็นพหุนาม โดยที่ $S(x)$ ไม่ใช่พหุนามศูนย์ จะแบ่งการพิสูจน์ออกเป็น 2 ส่วน
ส่วนแรกพิสูจน์ว่ามีพหุนาม $Q(x)$ และ $R(x)$ ที่สอดคล้อง

$$P(x) = Q(x)S(x) + R(x) \quad \text{เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x) \qquad (*)$$

ส่วนที่ 2 พิสูจน์ว่า มีพหุนาม $Q(x)$ และ $R(x)$ เพียงคู่เดียวเท่านั้นที่สอดคล้อง $(*)$
ถ้า $P(x) = 0$ แล้ว $P(x) = Q(x)\cdot 0 + 0$
พิจารณา $P(x) \neq 0$ ให้ $\deg P(x) = n$ และ $\deg S(x) = m$ เมื่อ

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad \text{เมื่อ } a_n \neq 0$$
$$S(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \quad \text{เมื่อ } b_m \neq 0$$

จะพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์บน n ถ้า $n = 0$ จะได้ว่า $P(x) = a_0 \neq 0$
กรณี $m = 0$ จะได้ว่า $S(x) = b_0 \neq 0$ แล้ว

$$P(x) = a_0 = a_0\cdot\frac{b_0}{a_0} + 0 = S(x)Q(x) + R(x)$$

เลือก $Q(x) = \dfrac{b_0}{a_0}$ และ $R(x) = 0$
กรณี $m > 0$ แล้ว

$$P(x) = S(x)\cdot 0 + P(x)$$

โดย $R(x) = P(x)$ ซึ่ง $\deg R(x) = \deg P(x) = 0 < m = \deg S(x)$
ดังนั้น $(*)$ เป็นจริงเมื่อ $n = 0$
ให้ $n > 0$ สมมติว่าสำหรับพหุนาม $F(x)$ ใด ๆ ซึ่ง $F(x) = 0$ หรือ $\deg F(x) < n$
จะมีพหุนาม $Q'(x)$ และ $R'(x)$ ที่ทำให้

$$F(x) = Q'(x)S(x) + R'(x) \quad \text{เมื่อ } R'(x) = 0 \text{ หรือ } \deg R'(x) < m$$

กรณี $n < m$ แล้ว $P(x) = S(x) \cdot 0 + P(x)$
กรณี $n \geq m$ แล้วให้

$$F(x) = P(x) - \frac{a_n}{b_m} S(x) x^{n-m}$$

จะได้ว่า $F(x) = 0$ หรือ $\deg F(x) < n$
โดยสมมติฐานการอุปนัยจะได้ว่ามีพหุนาม $Q(x)$ และ $R(x)$ ที่ทำให้

$$F(x) = Q(x)S(x) + R(x) \quad \text{เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < m$$

ทำให้ได้ว่า

$$\begin{aligned} P(x) &= \frac{a_n}{b_m} S(x) x^{n-m} + F(x) \\ &= \frac{a_n}{b_m} S(x) x^{n-m} + Q(x)S(x) + R(x) \\ &= S(x)\left(\frac{a_n}{b_m} x^{n-m} + Q(x) \right) + R(x) \end{aligned}$$

โดยที่ $R(x) = 0$ หรือ $\deg R(x) < m$
โดยหลักอุปนัยเชิงคณิตศาสตร์จะได้ว่า $(*)$ เป็นจริงทุกพหุนาม $P(x)$
ส่วนที่ 2 จะแสดงว่ามีพหุนาม $Q(x)$ และ $R(x)$ เพียงคู่เดียวเท่านั้นที่สอดคล้อง $(*)$
สมมติว่ามีพหุนาม $Q_1(x), Q_2(x)$ และ $R_1(x), R_2(x)$ ที่สอดคล้อง $(*)$ นั่นคือ

$$P(x) = Q_1(x)S(x) + R_1(x) \quad \text{เมื่อ } R_1(x) = 0 \text{ หรือ } \deg R_1(x) < m$$
$$P(x) = Q_2(x)S(x) + R_2(x) \quad \text{เมื่อ } R_2(x) = 0 \text{ หรือ } \deg R_2(x) < m$$

จะได้ว่า

$$\begin{aligned} [Q_2(x)S(x) + R_2(x)] - [Q_1(x)S(x) + R_1(x)] &= P(x) - P(x) \\ S(x)\left[Q_2(x) - Q_1(x)\right] + R_2(x) - R_1(x) &= 0 \\ S(x)\left[Q_2(x) - Q_1(x)\right] &= R_1(x) - R_2(x) \end{aligned}$$

สมมติว่า $R_1(x) - R_2(x) \neq 0$ แล้ว $Q_2(x) - Q_1(x) \neq 0$ ทำให้ได้ว่า

$$\begin{aligned} \deg\left(R_1(x) - R_2(x)\right) &< \deg S(x) \\ &\leq \deg S(x) + \deg\left(Q_2(x) - Q_1(x)\right) \\ &= \deg\left[S(x)\left(Q_2(x) - Q_1(x)\right)\right] \\ &= \deg\left(R_1(x) - R_2(x)\right) \end{aligned}$$

เกิดข้อขัดแย้ง ดังนั้น $R_1(x) - R_2(x) = 0$
สรุปได้ว่า $R_1(x) = R_2(x)$ แล้วทำให้ได้ด้วยว่า $Q_1(x) = Q_2(x)$ □

ตัวอย่าง 7.1.7

จงเขียนขั้นตอนวิธีการหารของ $S(x)$ หาร $P(x)$

1. $S(x) = x - 1$ และ $P(x) = x^3 + 2x^3 + 3x^2 + 4x + 5$
2. $S(x) = x^2 - 1$ และ $P(x) = x^4 + x^3 + x^2 + x + 1$

วิธีทำ 1. พิจารณา

$$\begin{aligned} P(x) &= x^3 + 2x^3 + 3x^2 + 4x + 5 \\ &= \left(x^3 - 3x^2 + 3x - 1\right) + 5x^2 + x + 6 \\ &= (x-1)^3 + 5(x^2 - 2x + 1) + 11x + 1 \\ &= (x-1)^3 + 5(x-1)^2 + 11(x-1) + 12 \\ &= (x-1)[(x-1)^2 + 5(x-1) + 11] + 12 \\ &= (x-1)(x^2 + 3x - 3) + 12 \end{aligned}$$

ดังนั้น $P(x) = S(x)\,(x^2 + 3x - 3) + 12$

2. พิจารณา

$$\begin{aligned} P(x) &= x^4 + x^3 + x^2 + x + 1 \\ &= \left(x^4 - 2x^2 + 1\right) + x^3 + 3x^2 + x \\ &= \left(x^2 - 1\right)^2 + x\left(x^2 - 1\right) + 3x^2 + 2x \\ &= \left(x^2 - 1\right)^2 + x\left(x^2 - 1\right) + 3\left(x^2 - 1\right) + 2x + 3 \\ &= \left(x^2 - 1\right)\left[\left(x^2 - 1\right) + x + 3\right] + 2x + 3 \\ &= \left(x^2 - 1\right)\left(x^2 + x + 2\right) + 2x + 3 \end{aligned}$$

ดังนั้น $P(x) = S(x)\,(x^2 + x + 2) + 2x + 3$

การเขียนขั้นตอนวิธีการหารอาจใช้ **การหารยาว** (long division) เพื่อหาผลหารและเศษเหลือดังตัวอย่างต่อไปนี้ (ธนัชยศ จำปาหวาย. 2559 : 182)

ตัวอย่าง 7.1.8

จงเขียนขั้นตอนวิธีการหารของ $x^2 + x + 1$ หาร $x^5 + 3x^3 + 2x^2 + x - 3$

วิธีทำ 1. จัดรูปพหุนาม $x^5 + 3x^3 + 2x^2 + x - 3$ ในรูป $x^2 + x + 1$

$$\begin{aligned} x^5 + 3x^3 + 2x^2 + x - 3 &= x^3\left(x^2 + x + 1\right) - x^4 + 2x^3 + 2x^2 + x - 3 \\ &= x^3\left(x^2 + x + 1\right) - x^2\left(x^2 + x + 1\right) + 3x^3 + 3x^2 + x - 3 \\ &= x^3\left(x^2 + x + 1\right) - x^2\left(x^2 + x + 1\right) + 3x\left(x^2 + x + 1\right) - 2x - 3 \\ &= \left(x^2 + x + 1\right)\left(x^3 - x^2 + 3x\right) - 2x - 3 \end{aligned}$$

วิธีทำ 2. การหารยาว

$$\begin{array}{r} x^3 - x^2 + 3x \\ x^2+x+1 \,\overline{)}\, x^5 + 0x^4 + 3x^3 + 2x^2 + x - 3 \\ \underline{x^5 + x^4 + x^3} \quad \downarrow \\ -x^4 + 2x^3 + 2x^2 \\ \underline{-x^4 - x^3 - x^2} \quad \downarrow \\ 3x^3 + 3x^2 + x \\ \underline{3x^3 + 3x^2 + 3x} \quad \downarrow \\ -2x - 3 \end{array}$$

ดังนั้น $x^5 + 3x^3 + 2x^2 + x - 3 = (x^2 + x + 1)(x^3 - x^2 + 3x) - 2x - 3$

ตัวอย่าง 7.1.9

ให้ $P(x) = x^3 + ax^2 + bx + 10$ เมื่อ a, b เป็นจำนวนเต็ม และ $Q(x) = x^2 + 9$ ถ้า $Q(x)$ หาร $P(x)$ เศษเหลือเท่ากับ 1 แล้ว $P(a + b)$ เท่ากับเท่าใด

วิธีทำ โดยขั้นตอนการหารจะได้มหุนาม $F(x)$ ซึ่ง

$$\begin{aligned} P(x) &= Q(x)F(x) + 1 \\ x^3 + ax^2 + bx + 10 &= (x^2 + 9)F(x) + 1 \end{aligned}$$

ดังนั้น $\deg F(x) = 1$ ให้ $F(x) = cx + d$ แล้ว

$$\begin{aligned} x^3 + ax^2 + bx + 10 &= (x^2 + 9)(cx + d) + 1 \\ &= cx^3 + dx^2 + 9cx + 9d + 1 \end{aligned}$$

จะได้ว่า $c = 1, d = a, b = 9c, 10 = 9d + 1$ ดังนั้น $a = 1$ และ $b = 9$ แล้ว

$$P(1 + 9) = P(10) = 10^3 + 10^2 + 9(10) + 10 = 1200$$

บทนิยาม 7.1.4

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนาม จะกล่าวว่า $\boldsymbol{Q(x)}$ **หาร** $\boldsymbol{P(x)}$ **ลงตัว** เขียนแทนด้วย $P(x) \mid Q(x)$ ถ้ามีพหุนาม $S(x)$ ซึ่ง $P(x) = Q(x)S(x)$ หรือกล่าวอีกนัยคือเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วย $Q(x)$ เท่ากับ 0 และเรียก $Q(x)$ ว่า**ตัวประกอบ** (factor) ของ $P(x)$

ตัวอย่าง 7.1.10

จงแสดงว่า $x^3 + 1$ หาร $x^5 - x^4 + 5x^3 + x^2 - x + 5$ ลงตัว

วิธีทำ พิจารณา

$$\begin{aligned} x^5 - x^4 + 5x^3 + x^2 - x + 5 &= x^2(x^3 + 1) - x^4 + 5x^3 - x + 5 \\ &= x^2(x^3 + 1) - x(x^3 + 1) + 5x^3 + 5 \\ &= x^2(x^3 + 1) - x(x^3 + 1) + 5(x^3 + 1) \\ &= (x^2 - x + 5)(x^3 + 1) \end{aligned}$$

ดังนั้น $x^3 + 1$ หาร $x^5 - x^4 + 5x^3 + x^2 - x + 5$ ลงตัว

ตัวอย่าง 7.1.11

จงตรวจสอบว่า x^2-2x+3 หาร x^4+x^3-2x+3 ลงตัวหรือไม่

วิธีทำ พิจารณา

$$\begin{aligned}x^4+x^3-2x+3 &= x^2\big(x^2-2x+3\big)+3x^3-3x^2-2x+3\\ &= x^2\big(x^2-2x+3\big)+3x\big(x^2-2x+3\big)+3x^2-11x+3\\ &= x^2\big(x^2-2x+3\big)+3x\big(x^2-2x+3\big)+3\big(x^2-2x+3\big)-5x-6\\ &= \big(x^2+3x+3\big)\big(x^2-2x+3\big)-5x-6\end{aligned}$$

ดังนั้น x^2-2x+3 หาร x^4+x^3-2x+3 ไม่ลงตัว

ตัวอย่าง 7.1.12

จงหาตัวประกอบทั้งหมดของ x^4-13x^2+36

วิธีทำ พิจารณา

$$\begin{aligned}x^4-13x^2+36 &= \big(x^2-4\big)\big(x^2-9\big)\\ &= (x-2)(x+2)(x-3)(x+3)\end{aligned}$$

ดังนั้น $x-2, x+2, x+3$ และ $x-3$ เป็นตัวประกอบของ x^4-13x^2+36

ตัวอย่าง 7.1.13

ถ้า a และ b เป็นจำนวนเต็ม และ ax^5+bx+4 หารด้วย $(x-1)^2$ ลงตัว แล้ว $a-b$ เท่ากับเท่าใด

วิธีทำ โดยขั้นตอนการหารจะได้ว่ามีพหุนาม $Q(x)$ ซึ่ง

$$ax^5+bx+4=\big(x^2-2x+1\big)Q(x)$$

ถ้า $x=1$ จะได้ว่า $a+b=-4$ และ $x=0$ จะได้ $Q(0)=4$
จากขั้นตอนการหารจะได้ว่า $\deg Q(x)=3$ ให้ $Q(x)=cx^3+dx^2+cx+4$ แล้ว

$$\begin{aligned}ax^5+bx+4 &= \big(x^2-2x+1\big)\big(cx^3+dx^2+ex+4\big)\\ &= cx^5+dx^4+ex^3+4x^2-2cx^4-2dx^3-2ex^2-8x+cx^3+dx^2+ex+4\\ &= cx^5+(d-2c)x^4+(e-2d+c)x^3+(4-2e+d)x^2+(-8+e)x+4\end{aligned}$$

จะได้ว่า $a=c, d-2c=0, e-2d+c=0, 4-2e+d=0, -8+e=b$ จะได้ว่า

$$\begin{aligned}e-2d+c&=0\\ (b+8)-2d+a&=0\\ (a+b)+8-2d&=0\\ -4+8-2d&=0\\ \therefore\quad d&=2\end{aligned}$$

ดังนั้น $a=c=1, e=3$ และ $b=-5$ แล้ว $a-b=1-(-5)=6$

7.2 ทฤษฎีเศษเหลือ

ในหัวข้อที่ผ่านมาได้กล่าวถึงขั้นตอนวิธีการการซึ่งจะทำให้มีเศษที่เหลือจากการหารเกิดขึ้น ในหัวข้อนี้จะกล่าวถึงนิยาม และทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องกับเศษเหลือ ดังนี้ (ธนัชยศ จำปาหวาย. 2559 : 184, ฉวีวรรณ รัตนประเสริฐ. 2552 : 114)

ทฤษฎีบท 7.2.1 : ทฤษฎีบทเศษเหลือ (The Remainder Theorem)

ให้ $P(x)$ เป็นพหุนาม และ $c \in \mathbb{R}$ แล้ว

$$x - c \text{ หาร } P(x) \text{ เศษเหลือเท่ากับ } P(c)$$

การพิสูจน์ จากขั้นตอนวิธีการหาร $x - c$ หาร $P(x)$ จะได้ว่ามี $Q(x)$ และ $R(x)$ ซึ่ง

$$P(x) = Q(x)(x - c) + R(x) \text{ เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < 1$$

กรณี $R(x) = 0$ จะได้ว่า $P(x) = Q(x)(x - c)$ แล้ว $P(c) = R(x)$

กรณี $\deg R(x) = 0$ แล้ว $R(x) = d$ เมื่อ d เป็นค่าคงที่ จะได้ว่า $P(x) = Q(x)(x - c) + d$ แล้ว

$$P(c) = d = R(x)$$

□

บทแทรก 7.2.1

ให้ $P(x)$ เป็นพหุนามซึ่ง $\deg P(x) > 0$ และ $c \in \mathbb{R}$ แล้ว $x - c$ เป็นตัวประกอบของ $P(x)$ ก็ต่อเมื่อ $P(c) = 0$

การพิสูจน์ ให้ $P(x)$ เป็นพหุนามซึ่ง $\deg P(x) > 0$ และ $c \in \mathbb{R}$

สมมติว่า $x - c$ เป็นตัวประกอบของ $P(x)$ นั่นคือ $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ 0

โดยทฤษฎีบท 7.2.1 จะได้ว่า $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ $P(c)$ ดังนั้น $P(c) = 0$

ในทางกลับกันสมมติว่า $P(c) = 0$ โดยทฤษฎีบท 7.2.1

เมื่อ $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ $P(c) = 0$ ดังนั้น $x - c$ เป็นตัวประกอบของ $P(x)$ □

ตัวอย่าง 7.2.1

จงหาเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วยตัวหารที่กำหนดในแต่ละข้อต่อไปนี้

1. $x - 1$ หาร $P(x) = x^4 - x^3 + 4x^2 + 5x + 2$
2. $x + 2$ หาร $P(x) = x^3 + 2x^2 + x - 3$

วิธีทำ 1. เศษเหลือเท่ากับ $P(1) = 1^4 - 1^3 + 4(1)^2 + 5(1) + 2 = 11$

2. เศษเหลือเท่ากับ $P(-2) = (-2)^3 + 2(-2)^2 + (-2) - 3 = -5$

ตัวอย่าง 7.2.2

จงหาค่า k ที่ทำให้ $x + 1$ หาร $3x^4 + 2x^2 + kx - 5$ เศษเหลือเท่ากับ -3

วิธีทำ จะได้ว่า

$$\begin{aligned} 3(-1)^4 + 2(-1)^2 + k(-1) - 5 &= -3 \\ 3 + 2 - k - 5 &= -3 \\ k &= 3 \end{aligned}$$

ตัวอย่าง 7.2.3

จงตรวจสอบว่าพหุนาม $x^3+2x^2+3x+10$ หารด้วยพหุนาม $x+2$ ลงตัวหรือไม่

วิธีทำ จากตัวหาร $x+2=x-(-2)$ จึงได้ $x-a=x-(-2)$

นั่นคือ $a=-2$

ให้ $P(x)=x^3+2x^2+3x+10$

จะได้ $\quad P(-2)=\left(-2^3\right)+2(-2)^2+3(-2)+10$

$$=-8+8-6+10$$

$$=4$$

นั่นคือ เศษจากการหารเท่ากับ 4

จึงสรุปได้ว่า $x^3+2x^2+3x+10$ หารด้วย $x+2$ ไม่ลงตัว

และยังได้ว่า $x+2$ ไม่ใช่ตัวประกอบของ $x^3+2x^2+3x+10$

ตัวอย่าง 7.2.4

ถ้าพหุนาม $6x^3+ax^2+bx-1$ หารด้วย $x+1$ ลงตัว แต่หารด้วย $x-1$ เศษเหลือเท่ากับ -24 แล้ว $2a-b$ เท่ากับเท่าใด

วิธีทำ จะได้ว่า

$$6(-1)^3+a(-1)^2+b(-1)-1=0$$
$$a-b=7$$

และ

$$6(1)^3+a(1)^2+b(1)-1=-24$$
$$a+b=-29$$

ดังนั้น $a=-11$ และ $b=-18$ แล้ว $2a-b=2(-11)-(-18)=-4$

ตัวอย่าง 7.2.5

ให้ $P(x)$ เป็นพหุนาม ถ้าหาร $P(x)$ ด้วย $x-1$ จะเศษเหลือเท่ากับ 3 และถ้าหาร $P(x)$ ด้วย $x-3$ จะเศษเหลือเท่ากับ 5 ถ้า $r(x)=ax+b$ คือเศษเหลือจากการหาร $P(x)$ ด้วย $(x-1)(x-3)$ แล้ว $3a+2b$ เท่ากับเท่าใด

วิธีทำ โดยทฤษฎีบทเศษเหลือจะได้ว่า $P(1)=3$ และ $P(3)=5$

และโดยขั้นตอนวิธีการหารพหุนาม $Q(x)$ ซึ่ง

$$P(x)=(x-1)(x-3)Q(x)+ax+b$$

แล้ว

$$3=P(1)=0+a+b$$
$$5=P(3)=0+3a+b$$

ดังนั้น $a=1$ และ $b=2$ แล้ว $3a+2b=3(1)+2(2)=7$

ตัวอย่าง 7.2.6

ให้ $P(x) = x^2+7x-3$ เมื่อหาร $P(x)$ ด้วย $x-p$ และ $x+q$ จะได้เศษเหลือเท่ากัน โดยที่ $p \neq -q$ แล้ว $p-q$ มีค่าเท่าใด

วิธีทำ โดยทฤษฎีบทเศษเหลือจะได้ว่า

$$\begin{aligned} P(p) &= P(-q) \\ p^2+7p-3 &= (-q)^2+7(-q)-3 \\ p^2-q^2+7p+7q &= 0 \\ (p-q)(p+q)+7(p+q) &= 0 \\ (p+q)[p-q+7] &= 0 \end{aligned}$$

เนื่องจาก $p+q \neq 0$ ดังนั้น $p-q+7=0$ นั่นคือ $P-q=-7$
จากทฤษฎีบท 7.2.1 เมื่อ $x-c$ หาร $P(x)$ จะได้เศษเหลือเท่ากับ $P(c)$ จะได้ว่า

$$P(x) = (x-c)Q(x)+P(c)$$

ให้ $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ เป็นพหุนามดีกรี n ซึ่ง $n \geq 1$
จะได้ว่า $\deg Q(x) = n-1$ นั่นคือให้

$$Q(x) = q_{n-1}x^{n-1} + \cdots + q_1x + q_0$$

ดังนั้น

$$\begin{aligned} a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 &= \left(q_{n-1}x^{n-1} + \cdots + q_1x + q_0\right)(x-c) + P(c) \\ &= q_{n-1}x^n + q_{n-2}x^{n-1} + \cdots + q_0x \\ &\quad - cq_{n-1}x^{n-1} - \cdots - cq_1x + cq_0 + P(c) \end{aligned}$$

จะได้ว่า

$$\begin{array}{lllll} q_{n-1} & & = a_n & & \\ q_{n-2} - cq_{n-1} & = a_{n-1} & \text{หรือ} & q_{n-2} = a_{n-1} + cq_{n-1} \\ q_{n-3} - cq_{n-2} & = a_{n-2} & \text{หรือ} & q_{n-3} = a_{n-2} + cq_{n-2} \\ & \vdots & & \vdots \\ q_1 - cq_2 & = a_2 & \text{หรือ} & q_1 = a_2 + cq_2 \\ q_2 - cq_1 & = a_1 & \text{หรือ} & q_0 = a_1 + cq_1 \\ P(c) - cq_0 & = a_0 & \text{หรือ} & P(c) = a_0 + cq_0 \end{array}$$

หรืออาจเขียนได้เป็น

$$\begin{array}{cccccccc} & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \\ + & & cq_{n-1} & cq_{n-2} & cq_{n-3} & \cdots & cq_1 & \\ \hline & q_{n-1} & q_{n-2} & q_{n-3} & q_{n-4} & \cdots & q_0 & P(c) \end{array}$$

เราเรียกวิธีการเขียนแบบนี้ว่า **การหารสังเคราะห์** (synthetic division) ทำให้ได้ผลหารและเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วย $x-c$

ตัวอย่าง 7.2.7

จงหาผลหารและเศษเหลือที่เกิดจากการหาร $3x^4 - 2x^3 + x^2 + 3x - 5$ ด้วย $x - 2$

วิธีทำ จะได้ว่า $c = 2$ และ $a_4 = q_3 = 3$ ดังนั้น

$$\begin{array}{rccccc} & 3 & -2 & 1 & 3 & -5 \\ + & & 2(3) & 2(4) & 2(9) & 2(21) \\ \hline & 3 & 4 & 9 & 21 & 37 \end{array}$$

ดังนั้นผลหารเท่ากับ $3x^3 + 4x^2 + 9x + 21$ และเศษเหลือคือ 37 เขียนขั้นตอนวิธีการหารได้เป็น

$$3x^4 - 2x^3 + x^2 + 3x - 5 = (3x^3 + 4x^2 + 9x + 21)(x - 2) + 37$$

บทนิยาม 7.2.1

ให้ $P(x)$ เป็นพหุนาม ถ้า $P(\alpha) = 0$ จะเรียก α ว่า**ราก** (root) ของพหุนาม หรือ $P(x)$ เป็น**คำตอบ** (solution) ของสมการ $P(x) = 0$

ข้อสังเกต โดยบทแทรก 7.2.1 จะได้ว่า

1. α เป็นรากก็ต่อเมื่อ $x - \alpha$ เป็นตัวประกอบของ $P(x)$
2. ถ้า $P(x) = Q(x)S(x)$ แล้วรากทุกตัวของ $Q(x)$ และรากทุกตัวของ $S(x)$ เป็นรากของ $P(x)$

ตัวอย่าง 7.2.8

จงหารากของพหุนาม $P(x)$ เมื่อกำหนดให้

1. $P(x) = x + 2$
2. $P(x) = x^2 - 1$
3. $P(x) = x^3 - x^2 - 2x$

วิธีทำ 1. เนื่องจาก $P(-2) = -2 + 2 = 0$ ดังนั้น -2 เป็นรากของ $P(x)$

2. เนื่องจาก $P(x) = x^2 - 1 = (x - 1)(x + 1)$ ดังนั้น $P(1) = 0$ และ $P(-1) = 0$ จะได้ว่า 1 และ -1 เป็นรากของ $P(x)$
3. เนื่องจาก $P(x) = x^3 - x^2 - 2x = x\,(x^2 - x - 2) = x(x + 1)(x - 2)$ ดังนั้น $P(0) = 0$, $P(-1) = 0$ และ $P(2) = 0$ จะได้ว่า $0, -1$ และ 2 เป็นรากของ $P(x)$

ทฤษฎีบท 7.2.2

ให้ $m, k \in \mathbb{Z}$ โดยที่ $m \neq 0$ ซึ่ง $(m, k) = 1$ และ

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

เมื่อ $P(x) \in \mathbb{Z}[x]$ เป็นพหุนามดีกรี n โดยที่ $a_0 \neq 0$

$$\text{ถ้า } x - \frac{k}{m} \text{ เป็นตัวประกอบของ } P(x) \text{ แล้ว } m \mid a_n \text{ และ } k \mid a_0$$

การพิสูจน์ สมมติว่า $x-\frac{k}{m}$ เป็นตัวประกอบของ $P(x)$ โดยบทแทรก 7.2.1 จะได้ว่า $P\left(\frac{k}{m}\right)=0$ นั่นคือ

$$\begin{aligned} a_n\left(\frac{k}{m}\right)^n+a_{n-1}\left(\frac{k}{m}\right)^{n-1}+\cdots+a_1\left(\frac{k}{m}\right)+a_0&=0\\ a_nk^n+a_{n-1}k^{n-1}m+\cdots+a_1km^{n-1}+a_0m^n&=0\\ \left(a_{n-1}k^{n-1}+\cdots+a_1km^{n-2}+a_0m^{n-1}\right)m&=-a_nk^n \end{aligned}$$

ดังนั้น $m \mid a_nk^n$ แต่เนื่องจาก $(m,k)=1$ จะได้ว่า $(m,k^n)=1$
สรุปได้ว่า $m \mid a_n$ ทำนองเดียวกันจะได้ว่า

$$\begin{aligned} a_nk^n+a_{n-1}k^{n-1}m+\cdots+a_1km^{n-1}+a_0m^n&=0\\ \left(a_nk^{n-1}+a_nk^{n-2}m+\cdots+a_1m^{n-2}\right)k&=-a_0m^n \end{aligned}$$

ดังนั้น $k \mid a_0m^n$ ทำให้สรุปได้ว่า $k \mid a_0$ □

บทแทรก 7.2.2

ให้ $P(x)\in\mathbb{Z}[x]$ และ $n\in\mathbb{N}$ โดยที่ $a_0\neq 0$ ซึ่ง

$$P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

แล้วรากที่เป็นจำนวนเต็มของ $P(x)$ ต้องเป็นตัวหารของ a_0

การพิสูจน์ เห็นได้ชัดจากทฤษฎีบท 7.2.2 □

จากทฤษฎีบท 7.2.2 บอกให้ทราบถึงเงื่อนไขสำหรับจำนวนตรรกยะที่เป็นรากของพหุนามที่มีสัมประสิทธิ์ที่เป็นจำนวนเต็ม ซึ่งจะเป็นเครื่องมือในการค้นหารากที่เป็นจำนวนตรรกยะของพหุนามดังกล่าว หรือกล่าวได้ว่ารากที่เป็นจำนวนตรรกยะทั้งหมดของ

$$P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

คืออัตราส่วนที่เป็นไปได้ของตัวหาร (รวมจำนวนลบด้วย) ของ k ต่อตัวหาร (รวมจำนวนลบด้วย) ของ m ดังตัวอย่างต่อไปนี้

ตัวอย่าง 7.2.9

จงหารากที่เป็นจำนวนตรรกยะทั้งหมดที่เป็นไปได้ของพหุนามต่อไปนี้

1. $P(x)=4x^2-1$
2. $P(x)=6x^3+11x^2-4x-4$
3. $P(x)=x^3-4x^2+x+6$

วิธีทำ 1. จะได้ว่า $a_0=-1$ และ $a_2=4$ ดังนั้น $m \mid 4$ คือ $m=\pm1,\pm2,\pm4$ และ $k \mid (-1)$ คือ $k=\pm1$
ดังนั้น $\frac{k}{m}=\pm1,\pm\frac{1}{2},\pm\frac{1}{4}$

2. จะได้ว่า $a_0 = -4$ และ $a_3 = 6$ ดังนั้น $m \mid 6$ คือ $m = \pm 1, \pm 2, \pm 3, \pm 6$ และ $k \mid (-4)$ คือ $k = \pm 1, \pm 2, \pm 4$ ดังนั้น $\frac{k}{m}$ ทั้งหมดที่เป็นไปได้คือ $\pm 1, \pm 2, \pm 4, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}, \pm\frac{1}{6}$
3. จะได้ $a_0 = 6$ แล้ว รากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ 6 คือ $\pm 1, \pm 2, \pm 3, \pm 6$

ตัวอย่าง 7.2.10

จงหาแสดงว่าพหุนาม $P(x) = x^3 + x + 1$ ไม่มีรากเป็นจำนวนเต็ม

วิธีทำ สมมติให้ $\alpha \in \mathbb{Z}$ เป็นรากของ $P(x)$ ดังนั้น $\alpha \mid 1$ นั่นคือ $\alpha = 1$ หรือ $\alpha = -1$ แต่

$$P(1) = 1^3 + 1 + 1 = 3 \neq 0$$
$$P(-1) = (-1)^3 + (-1) + 1 = -1 \neq 0$$

เกิดข้อขัดแย้งที่ α เป็นรากของ $P(x)$ ดังนั้น $P(x) = x^3 + x + 1$ ไม่มีรากที่เป็นจำนวนเต็ม

ตัวอย่าง 7.2.11

จงหารากที่เป็นจำนวนเต็มทั้งหมดของ $P(x) = x^3 - 6x^2 + 11x - 6$

วิธีทำ จะได้ว่า $a_0 = -6$ แล้วรากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ -6 คือ $\pm 1, \pm 2, \pm 3, \pm 6$ ตรวจสอบตัวหารที่ได้ดังนี้

$$\begin{aligned}
P(-1) &= (-1)^3 - 6(-1)^2 + 11(-1) - 6 = -24 \\
P(1) &= 1^3 - 6(1)^2 + 11(1) - 6 = 0 \\
P(-2) &= (-2)^3 - 6(-2)^2 + 11(-2) - 6 = -60 \\
P(2) &= (2)^3 - 6(2)^2 + 11(2) - 6 = 0 \\
P(-3) &= (-3)^3 - 6(-3)^2 + 11(-3) - 6 = -120 \\
P(3) &= (3)^3 - 6(3)^2 + 11(3) - 6 = 0 \\
P(-6) &= (-6)^3 - 6(-6)^2 + 11(-6) - 6 = -504 \\
P(-2) &= (6)^3 - 6(6)^2 + 11(6) - 6 = 60
\end{aligned}$$

ดังนั้น 1,2 และ 3 เป็นรากของ $P(x)$

จากตัวอย่าง 7.2.11 การตรวจสอบว่าตัวหารทั้งหมดของ a_0 ว่าเป็นหารหารากของพหุนาม $P(x)$ มีความยุ่งยากเมื่อ a_0 มีตัวหารจำนวนมาก ในทางปฏิบัติเราจะทำโดยหาตัวหารเพียงหนึ่งตัวที่เป็นรากของ $P(x)$ ต่อจากนั้นอาศัยการหารยาว หรือการเขียน $P(x)$ ในรูปของ $(x - c)$ เมื่อ c เป็นรากของพหุนาม $P(x)$ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 7.2.12

จงหารากที่เป็นจำนวนเต็มทั้งหมดของ $P(x) = x^4 + 2x^3 - 13x^2 - 14x + 24$

วิธีทำ จะได้ว่า $a_0 = 24$ แล้วรากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ 24 คือ $\pm 1, \pm 2, \pm 3, \pm 6, \pm 8, \pm 12, \pm 24$ เนื่องจาก $P(1) = (1)^4 + 2(1)^3 - 13(1)^2 - 14(1) + 24 = 0$

ดังนั้น $x-1$ เป็นตัวประกอบของ $P(x)$ พิจารณาการหารสังเคราะห์ จะได้ว่า $c=2$ และ $a_4=q_3=3$ ดังนั้น

$$\begin{array}{rrrrr} & 1 & 2 & -13 & -14 & 24 \\ + & & 1(1) & 1(3) & 1(-10) & 1(-24) \\ \hline & 1 & 3 & -10 & -24 & 0 \end{array}$$

ดังนั้นผลหารเท่ากับ $x^3+3x^2-10x-24$ เขียนได้เป็น

$$P(x)=\big(x^3+3x^2-10x-24\big)(x-1)$$

ให้ $Q(x)=x^3+3x^2-10x-24$ หารากของ $Q(x)$ โดยใช้ตัวหารเช่นเดียวกับ $P(x)$ จะได้ว่า $Q(3)=(3)^3+3(3)^2-10(3)-24=0$ ดังนั้น $x-3$ เป็นตัวประกอบของ $Q(x)$ หารสังเคราะห์ได้ดังนี้

$$\begin{array}{rrrrr} & 1 & 3 & -10 & -24 \\ + & & 3(1) & 3(6) & 3(8) \\ \hline & 1 & 6 & 8 & 0 \end{array}$$

ดังนั้น $Q(x)=\left(x^2+6x+8\right)(x-3)$ จะได้ว่า

$$\begin{aligned} P(x) &= \big(x^2+6x+8\big)\,(x-3)(x-1) \\ &= (x+2)(x+4)(x-3)(x-1) \end{aligned}$$

สรุปได้ว่า $1,3,-2$ และ -4 เป็นรากของ $P(x)=x^4+2x^3-13x^2-14x+24$

7.3 เศษส่วนย่อย

ธนัชยศ จำปาหวาย (2559 : 190) และ ฉวีวรรณ รัตนประเสริฐ (2552 : 144) ได้กล่าวถึงฟังก์ชันตรรกยะและเศษส่วนย่อยไว้ดังนี้

พิจารณาเศษส่วนที่ตัวเศษและตัวส่วนเป็นพหุนามซึ่งอยู่ในรูป

$$\frac{P(x)}{Q(x)} \text{ เมื่อ } P(x) \text{ เป็นพหุนาม และ } Q(x) \text{ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์}$$

ในแง่ฟังก์ชันจะเรียก $\dfrac{P(x)}{Q(x)}$ ว่า**ฟังก์ชันตรรกยะ** (rational function) และนิยามการบวกและการคูณฟังก์ชันตรรกยะดังนั้น

$$\begin{aligned} \frac{P_1(x)}{Q_1(x)}+\frac{P_1(x)}{Q_1(x)} &= \frac{P_1(x)Q_2(x)+P_2(x)Q_1(x)}{Q_1(x)Q_2(x)} \\ \frac{P_1(x)}{Q_1(x)}\cdot\frac{P_1(x)}{Q_1(x)} &= \frac{P_1(x)P_2(x)}{Q_1(x)Q_2(x)} \end{aligned}$$

ในหัวข้อนี้จะพิจารณาว่าสำหรับแต่ละฟังก์ชันตรรกยะ $\dfrac{P(x)}{Q(x)}$ จะสามารถเขียนในรูป

$$\frac{P(x)}{Q(x)}=\frac{P_1(x)}{Q_1(x)}+\frac{P_2(x)}{Q_2(x)}+\cdots+\frac{P_n(x)}{Q_n(x)}$$

ได้หรือไม่ โดยแต่ละ $P_i(x)$ และ $Q_i(x)$ มีดีกรีน้อยกว่า $P(x)$ และ $Q(x)$ ตามลำดับ โดยเรียกแต่ละ $\dfrac{P_i(x)}{Q_i(x)}$ ว่า**เศษส่วนย่อย** (partial fraction) ของ $\dfrac{P(x)}{Q(x)}$ สำหรับ $i = 1, 2, \ldots, n$

ทฤษฎีบท 7.3.1

ให้ $P(x)$ เป็นพหุนาม และ $Q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ จะได้ว่ามีพหุนาม $S(x)$ และ $R(x)$ โดยที่ $R(x) = 0$ หรือ $\deg R(x) < \deg Q(x)$ ซึ่งสอดคล้อง

$$\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$$

การพิสูจน์ ให้ $P(x)$ เป็นพหุนาม และ $Q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์

โดยขั้นตอนวิธีการหารจะได้ว่ามีพหุนาม $S(x)$ และ $R(x)$ เพียงคู่เดียวที่สอดคล้องกับ

$$P(x) = Q(x)S(x) + R(x) \text{ เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x)$$

ดังนั้น

$$\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$$

□

ตัวอย่าง 7.3.1

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปแบบตามทฤษฎีบท 7.3.1

1. $\dfrac{x^2 - 1}{x + 3}$
2. $\dfrac{x^2 + x + 5}{x^2 + 1}$
3. $\dfrac{x^2 + 2}{x^3 + 1}$

วิธีทำ 1. พิจารณาการหารสังเคราะห์

$$\begin{array}{rrrr} & 1 & 0 & -1 \\ + & & -3(1) & -3(-3) \\ \hline & 1 & -3 & 8 \\ \hline\hline \end{array}$$

ดังนั้น $x - 3$ และ 8 เป็นผลหารและเศษเหลือที่เกิดจากการหาร $x^2 - 1$ ด้วย $x + 3$ ทำให้ได้ว่า

$$\frac{x^2 - 1}{x + 3} = x - 3 + \frac{8}{x + 3}$$

2. จะได้ว่า

$$\frac{x^2 + x + 5}{x^2 + 1} = \frac{(x^2 + 1) + x + 4}{x^2 + 1} = 1 + \frac{x + 4}{x^2 + 1}$$

3. เนื่องจาก $x^2 + 2$ มีดีกรีน้อยกว่า $x^3 + 1$ ดังนั้น

$$\frac{x^2 + 2}{x^3 + 1} = 0 + \frac{x^2 + 2}{x^3 + 1}$$

ทฤษฎีบท 7.3.2

ให้ $Q(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$ เป็นพหุนามดีกรี $n \in \mathbb{N}$ เมื่อ $a_1, a_2, \ldots, a_n$ เป็นจำนวนจริงที่แตกต่างกัน และ $P(x)$ เป็นพหุนามที่ $\deg P(x) < n$ จะได้ว่า $\dfrac{P(x)}{Q(x)}$ สามารถเขียนเป็นผลบวกของเศษส่วนย่อยในรูปแบบ

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a_1} + \frac{c_2}{x-a_2} + \cdots + \frac{c_n}{x-a_n}$$

เมื่อ $c_i = \dfrac{P(a_i)}{Q_i(a_i)}$ โดยที่ $Q_i(x) = (x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$
สำหรับ $i = 1, 2, \ldots, n$

การพิสูจน์ พิสูจน์โดยวิธีอุปนัยเชิงคณิตศาสตร์บน n

ขั้นฐาน ถ้า $n = 1$ นั่นคือ $Q(x) = x - a_1$ แล้ว $P(x)$ เป็นพหุนามคงตัว ดังนั้นทฤษฎีบทนี้เป็นจริง

ขั้นอุปนัย สมมติว่าทฤษฎีบทนี้เป็นจริงทุก ๆ จำนวนนับ $k < n$

ให้ $Q(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$ โดยที่ $a_1, a_2, \ldots, a_n$ เป็นจำนวนจริงที่แตกต่างกัน

ให้ $Q_1(x) = (x-a_2)\cdots(x-a_n)$ แล้ว $Q_1(a_1) \neq 0$ เลือก $c_1 = \dfrac{P(a_1)}{Q_1(a_1)}$ ซึ่งจะทำให้ได้ว่า $P(a_1) = c_1 Q_1(a_1)$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $P_1(x)$ และจำนวนคงที่ R ซึ่ง

$$P(x) = (x-a_1)P_1(x) + R$$

แล้ว $R = P(a_1) = c_1 Q_1(a_1)$ ดังนั้น $P(x) = (x-a_1)P_1(x) + c_1 Q_1(x)$ ทำให้ได้ว่า

$$\begin{aligned}\frac{P(x)}{Q(x)} &= \frac{(x-a_1)P_1(x)}{Q(x)} + \frac{c_1 Q_1(x)}{Q(x)} \\ &= \frac{P_1(x)}{Q_1(x)} + \frac{c_1}{x-a_1}\end{aligned}$$

เนื่องจากดีกรีของ $P_1(x)$ น้อยกว่าดีกรีของ $Q_1(x)$ และ $Q_1(x) = (x-a_2)\cdots(x-a_n)$
โดยที่ $a_2, a_3, \ldots, a_n$ เป็นจำนวนจริงที่แตกต่างกัน
โดยสมมติฐานของการอุปนัยเชิงคณิตศาสตร์จะได้ว่าทฤษฎีบทนี้เป็นจริงสำหรับ $n \in \mathbb{N}$ □

ตัวอย่าง 7.3.2

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^4+4x+1}{x^3-x}$ ในรูปผลบวกของเศษส่วนย่อย

วิธีทำ ให้ $P(x) = x^4+4x+1$ และ $Q(x) = x^3 - x = x(x-1)(x+1)$ ดังนั้น

$$\frac{P(x)}{Q(x)} = \frac{x^4+4x+1}{x^3-x} = \frac{c_1}{x} + \frac{c_2}{x-1} + \frac{c_3}{x+1}$$

ให้ $Q_1 = (x-1)(x+1), Q_2 = x(x+1)$ และ $Q_3 = x(x-1)$ จะได้ว่า

$$c_1 = \frac{P(0)}{Q_1(0)} = \frac{(0)^4 + 4(0) + 1}{(0-1)(0+1)} = -1$$
$$c_2 = \frac{P(1)}{Q_2(1)} = \frac{(1)^4 + 4(1) + 1}{1(1+1)} = 3$$
$$c_3 = \frac{P(-1)}{Q_3(-1)} = \frac{(-1)^4 + 4(-1) + 1}{(-1)(-1-1)} = -1$$

ดังนั้น $\dfrac{x^4+4x+1}{x^3-x} = -\dfrac{1}{x} + \dfrac{3}{x-1} - \dfrac{1}{x+1}$

การหาค่า c_1, c_2, c_3 ในตัวอย่าง 7.3.2 จะทำได้ต้องอาศัยการจำสูตรในทฤษฎีบท 7.3.2 อาจหาค่าดังกล่าวโดยการเทียบสัมประสิทธิ์ของพหุนาม หรือแทนค่าฟังก์ชันในพหุนามดังตัวอย่างต่อไปนี้

ตัวอย่าง 7.3.3

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^2-6x+4}{x^3-4x}$ ในรูปผลบวกของเศษส่วนย่อย

วิธีทำ ให้ c_1, c_2, c_3 เป็นจำนวนจริงซึ่ง

$$\begin{aligned}\frac{x^2-6x+4}{x^3-4x} &= \frac{x^2-6x+4}{x(x-2)(x+2)} = \frac{c_1}{x} + \frac{c_2}{x-2} + \frac{c_3}{x+2} \\ &= \frac{c_1(x-2)(x+2) + c_2x(x+2) + c_3x(x-2)}{x(x-2)(x+2)}\end{aligned}$$

ดังนั้น $x^2-6x+4 = c_1(x-2)(x+2) + c_2x(x+2) + c_3x(x-2)$
เมื่อ $x=0$ จะได้ว่า $c_1(-2)(2) + 0 + 0 = 4$ นั่นคือ $-4c_1 = 4$ ดังนั้น $c_1 = -1$
เมื่อ $x=2$ จะได้ว่า $0 + c_2(2)(4) + 0 = -4$ นั่นคือ $8c_2 = -4$ ดังนั้น $c_2 = -\dfrac{1}{2}$
เมื่อ $x=-2$ จะได้ว่า $0 + 0 + c_3(-2)(-4) = 14$ นั่นคือ $-8c_3 = 14$ ดังนั้น $c_3 = -\dfrac{7}{4}$
ดังนั้น

$$\frac{x^2-6x+4}{x(x-2)(x+2)} = -\frac{1}{x} - \frac{1}{2(x-2)} - \frac{7}{4(x+2)}$$

ต่อไปจะเป็นตัวอย่างประโยชน์ที่ได้จากการเขียนฟังก์ชันตรรกยะในรูปผลบวกของเศษส่วนย่อย

ตัวอย่าง 7.3.4

จงหาผลบวกของอนุกรม $\displaystyle\sum_{k=2}^{n} \frac{1}{k^2-1}$ เมื่อ n เป็นจำนวนบวกคี่

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{1}{k^2-1} = \frac{1}{(k-1)(k+1)} = \frac{c_1}{k-1} + \frac{c_2}{k+1}$$

จะได้ว่า $1 = c_1(k+1) + c_2(k+1)$ แล้ว $c_1 = \frac{1}{2}$ และ $c_2 = -\frac{1}{2}$ ดังนั้น

$$\frac{1}{k^2-1} = \frac{1}{2}\left(\frac{1}{k-1} - \frac{1}{k+1}\right)$$

$$\begin{aligned}\sum_{k=2}^{n} \frac{1}{k^2-1} &= \frac{1}{2}\sum_{k=2}^{n}\left(\frac{1}{k-1} - \frac{1}{k+1}\right) \\ &= \frac{1}{2}\left[\left(\frac{1}{1} - \frac{1}{3}\right) + \left(\frac{1}{2} - \frac{1}{4}\right) + \left(\frac{1}{3} - \frac{1}{5}\right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n+1}\right)\right]\end{aligned}$$

เนื่องจาก n เป็นจำนวนคี่ จะได้ว่า $n+1$ เป็นจำนวนคู่ ดังนั้น

$$\begin{aligned}\sum_{k=2}^{n} \frac{1}{k^2-1} &= \frac{1}{2}\left[\left(1 - \frac{1}{n}\right) + \left(\frac{1}{2} - \frac{1}{n+1}\right)\right] \\ &= \frac{1}{2}\left[\frac{3}{2} - \frac{1}{n} - \frac{1}{n+1}\right]\end{aligned}$$

ตัวอย่าง 7.3.5

จงหา $\displaystyle\int \frac{1}{x^3-x}\,\mathrm{d}x$

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{1}{x^3-x} = \frac{1}{x(x-1)(x+1)} = \frac{c_1}{x} + \frac{c_2}{x-1} + \frac{c_3}{x+1}$$

จะได้ว่า $1 = c_1(x-1)(x+1) + c_2x(x+1) + c_3x(x-1)$

แล้ว $c_1 = -1, c_2 = \frac{1}{2}$ และ $c_3 = -\frac{1}{2}$ ดังนั้น

$$\frac{1}{x^3-x} = -\frac{1}{x} + \frac{1}{2(x-1)} - \frac{1}{2(x+1)}$$

$$\begin{aligned}\int \frac{1}{x^3-x}\,\mathrm{d}x &= -\int \frac{1}{x}\,\mathrm{d}x + \frac{1}{2}\int \frac{1}{x-1}\,\mathrm{d}x - \frac{1}{2}\int \frac{1}{x+1}\,\mathrm{d}x \\ &= -\ln|x| + \frac{1}{2}\ln|x-1| - \frac{1}{2}\ln|x+1| + C\end{aligned}$$

ทฤษฎีบท 7.3.3

ให้ $Q(x) = (x-a)^n$ เมื่อ $a \in \mathbb{R}$ และ $P(x)$ เป็นพหุนามที่ $\deg P(x) < n$ จะได้ว่ามีจำนวนจริง $c_1, c_2, \ldots, c_n$ ที่ทำให้

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a} + \frac{c_2}{(x-a)^2} + \cdots + \frac{c_n}{(x-a)^n}$$

การพิสูจน์ พิจารณาพหุนาม $x-a$ และ $P(x)$

โดยขั้นตอนวิธีการหารจะได้ว่ามีพหุนาม $q_1(x)$ และ $r_1 \in \mathbb{R}$ ซึ่ง

$$P(x) = (x-a)q_1(x) + r_1$$

พิจารณา $x-a$ และ $q_1(x)$ จะได้ว่ามีพหุนาม $q_2(x)$ และ $r_2 \in \mathbb{R}$ ซึ่ง

$$q_1(x) = (x-a)q_2(x) + r_2$$

ในทำนองเดียวกันจะได้ว่า

$$\begin{aligned} q_2(x) &= (x-a)q_3(x) + r_3 \\ q_3(x) &= (x-a)q_4(x) + r_4 \\ &\vdots \\ q_{n-2}(x) &= (x-a)q_{n-1}(x) + r_{n-1} \end{aligned}$$

ดังนั้น

$$\begin{aligned} P(x) &= (x-a)q_1(x) + r_1 \\ &= (x-a)^2 q_2(x) + (x-a)r_2 + r_1 \\ &= (x-a)^3 q_3(x) + (x-a)^2 r_3 + (x-a)r_2 + r_1 \\ &\vdots \\ &= (x-a)^{n-1} q_{n-1}(x) + (x-a)^{n-2} r_{n-1} + \cdots + (x-a)r_2 + r_1 \\ \frac{P(x)}{(x-a)^n} &= \frac{q_{n-1}(x)}{x-a} + \frac{r_{n-1}}{(x-a)^2} + \cdots + \frac{r_1}{(x-a)^n} \end{aligned}$$

เนื่องจาก $\deg P(x) < n$ และ $\deg q_{k+1}(x) = \deg q_k(x) - 1 < (n-k) - 1$
ทุก ๆ $k = 1, 2, \ldots, n-1$
ทำให้ได้ว่า $\deg q_{n-1}(x) = 0$ นั่นคือ $q_{n-1}(x)$ เป็นพหุนามคงตัว ให้ $c_1 = q_{n-1}(x), c_k = r_{n-k+1}$
สำหรับ $k = 2, 3, \ldots, n$ ดังนั้น

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a} + \frac{c_2}{(x-a)^2} + \cdots + \frac{c_n}{(x-a)^n}$$ □

บทแทรก 7.3.1

ให้ $Q(x) = (x-a)^n R(x)$ เป็นพหุนาม เมื่อ $a \in \mathbb{R}$ และ $R(x)$ เป็นพหุนามและ $P(x)$ เป็นพหุนาม ที่ $\deg P(x) < \deg Q(x)$ จะได้ว่ามีจำนวนจริง $c_1, c_2, \ldots, c_n$ และพหุนาม $S(x)$ ซึ่งดีกรีน้อยกว่า $R(x)$ ที่ทำให้

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a} + \frac{c_2}{(x-a)^2} + \cdots + \frac{c_n}{(x-a)^n} + \frac{S(x)}{R(x)}$$

การพิสูจน์ เป็นแบบฝึกหัด □

ตัวอย่าง 7.3.6

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปผลบวกเศษส่วนย่อย โดยไม่ต้องคำนวณค่าคงตัว

1. $\dfrac{1}{(x-1)^3}$

2. $\dfrac{x-3}{(x-2)^2(x+1)(x+2)}$
3. $\dfrac{x^2+1}{(x-2)^2\,(x^2-x-2)}$

วิธีทำ 1. มีจำนวนจริง c_1, c_2, c_3 ที่ทำให้

$$\frac{1}{(x-1)^3} = \frac{c_1}{x-1} + \frac{c_2}{(x-1)^2} + \frac{c_3}{(x-1)^3}$$

2. มีจำนวนจริง c_1, c_2, c_3, c_4 ที่ทำให้

$$\frac{x-3}{(x-2)^2(x+1)(x+2)} = \frac{c_1}{x-2} + \frac{c_2}{(x-2)^2} + \frac{c_3}{x+1} + \frac{c_4}{x+2}$$

3. เนื่องจาก $(x-2)^2\,(x^2-x-2) = (x-2)^2(x-2)(x+1) = (x-2)^3(x+1)$
ดังนั้นมีจำนวนจริง c_1, c_2, c_3, c_4 ที่ทำให้

$$\frac{x^2+1}{(x-2)^2\,(x^2-x-2)} = \frac{c_1}{x-2} + \frac{c_2}{(x-2)^2} + \frac{c_3}{(x-2)^3} + \frac{c_4}{x+1}$$

ตัวอย่าง 7.3.7

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^2+x+6}{(x+1)^2(x-1)}$ ในรูปผลบวกเศษส่วนย่อย

วิธีทำ มีจำนวนจริง c_1, c_2, c_3 ที่ทำให้

$$\begin{aligned}\frac{x^2+x+6}{(x+1)^2(x-1)} &= \frac{c_1}{x+1} + \frac{c_2}{(x+1)^2} + \frac{c_3}{x-1} \\ &= \frac{c_1(x+1)(x-1) + c_2(x-1) + c_3(x+1)^2}{(x+1)^2(x-1)}\end{aligned}$$

ดังนั้น $x^2+x+6 = c_1(x+1)(x-1) + c_2(x-1) + c_3(x+1)^2$
เมื่อ $x=1$ จะได้ว่า $c_1(2)(0) + c_2(0) + c_3(8) = 8$ นั่นคือ $8c_3 = 8$ ดังนั้น $c_3 = 1$
เมื่อ $x=-1$ จะได้ว่า $c_1(0)(-2) + c_2(-2) + c_3(0) = 6$ นั่นคือ $-2c_2 = 6$ ดังนั้น $c_2 = -3$
เมื่อ $x=0$ จะได้ว่า $c_1(1)(-1) + c_2(-1) + c_3(1) = 6$ นั่นคือ $-c_1 + 3 + 1 = 6$ ดังนั้น $c_1 = -2$
สรุปได้ว่า

$$\frac{x^2+x+6}{(x+1)^2(x-1)} = -\frac{2}{x+1} - \frac{3}{(x+1)^2} + \frac{1}{x-1}$$

ตัวอย่าง 7.3.8

จงหา $\displaystyle\int \frac{x^2+2x+3}{(x^2+x-2)\,(x^2-3x+2)}\,\mathrm{d}x$

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{x^2+2x+3}{(x^2+x-2)\,(x^2-3x+2)} = \frac{x^2+2x+3}{(x+2)(x-1)(x+2)(x+1)} = \frac{x^2+2x+3}{(x+2)^2(x-1)(x+1)}$$

จะได้ว่ามีจำนวนจริง c_1, c_2, c_3, c_4 ทำให้

$$\frac{x^2+2x+3}{(x^2+x-2)(x^2-3x+2)} = \frac{c_1}{x+2} + \frac{c_2}{(x+2)^2} + \frac{c_3}{(x-1)} + \frac{c_4}{(x+1)}$$

ดังนั้น

$$x^2+2x+3 = c_1(x+2)(x-1)(x+1)+c_2(x-1)(x+1)+c_3(x+2)^2(x+1)+c_4(x+2)^2(x-1)$$

เมื่อ $x=1$ จะได้ว่า $c_3(9)(2)=18$ นั่นคือ $18c_3=18$ ดังนั้น $c_3=1$
เมื่อ $x=-1$ จะได้ว่า $c_4(1)(-2)=14$ นั่นคือ $-2c_4=14$ ดังนั้น $c_4=-7$
เมื่อ $x=-2$ จะได้ว่า $c_2(-3)(-1)=15$ นั่นคือ $3c_2=15$ ดังนั้น $c_2=5$
เมื่อ $x=0$ จะได้ว่า $c_1(2)(-1)(1)+c_2(-1)(1)+c_3(4)(1)+c_4(4)(-1)=15$
นั่นคือ $-2c_1-5+4+28=15$ ดังนั้น $c_1=6$ จะได้ว่า

$$\frac{x^2+2x+3}{(x^2+x-2)(x^2-3x+2)} = \frac{6}{(x+2)} + \frac{5}{(x+2)^2} + \frac{1}{x-1} - \frac{7}{x+1}$$

$$\begin{aligned}\int \frac{x^2+2x+3}{(x^2+x-2)(x^2-3x+2)}\,\mathrm{d}x &= \int \frac{6}{(x+2)}\mathrm{d}x + \int \frac{5}{(x+2)^2}\,\mathrm{d}x + \int \frac{1}{x-1}\,\mathrm{d}x - \int \frac{7}{x+1}\,\mathrm{d}x \\ &= 6\ln|x-2| + \frac{5}{x+2} + \ln|x-1| - 7\ln|x+1| + C\end{aligned}$$

ต่อไปนี้จะเป็นผลบวกเศษส่วนย่อยในรูปแบบโดยทั่วไปซึ่งเป็นผลจาก ทฤษฎีบท 7.3.2 ทฤษฎีบท 7.3.3 และบทแทรก 7.3.1 กล่าวคือถ้า $Q(x) = [q_1(x)]^{n_1}[q_2(x)]^{n_2}\cdots[q_k(x)]^{n_k}$ โดยที่แต่ละ $q_i(x)$ เป็นพหุนามโมนิก ซึ่ง $\deg q_i(x) \geq 1$ และไม่ซ้ำกัน มีสมบัติว่าทุก ๆ พหุนาม $q(x)$ ซึ่ง $q(x) \mid q_i(x)$ แล้ว $q(x) = \pm 1$ หรือ $q(x) = \pm q_i(x)$ ให้ $P(x)$ เป็นพหุนามที่มีดีกรีน้อยกว่าดีกรีของ $Q(x)$ จะได้ว่า

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n_1}\frac{c_{1i}(x)}{[q_1(x)]^i} + \sum_{i=1}^{n_2}\frac{c_{2i}(x)}{[q_2(x)]^i} + \cdots + \sum_{i=1}^{n_k}\frac{c_{ki}(x)}{[q_k(x)]^i}$$

เมื่อ $c_{ij}(x)$ เป็นพหุนาม โดยที่ $c_{ij}(x)=0$ หรือ $\deg c_{ij}(x) < \deg q_i(x)$ ทุก ๆ i, j

ตัวอย่าง 7.3.9

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปผลบวกเศษส่วนย่อย โดยไม่ต้องคำนวณค่าคงตัว

1. $\dfrac{1}{(x^2+1)(x+1)}$
2. $\dfrac{x+3}{(x^2+x+1)^2(x-1)}$
3. $\dfrac{x^2+3}{(x^2+1)^2(x+1)^2(x-1)}$

วิธีทำ 1. มีจำนวนจริง A, B, C ที่ทำให้

$$\frac{1}{(x^2+1)(x+1)} = \frac{Ax+B}{x^2+1} + \frac{C}{x+1}$$

2. มีจำนวนจริง c_1, c_2, c_3, c_4, c_5 ที่ทำให้

$$\frac{x+3}{(x^2+x+1)^2(x-1)} = \frac{c_1+c_2x}{x^2+x+1} + \frac{c_3+c_4x}{(x^2+x+1)^2} + \frac{c_5}{(x-1)}$$

3. ดังนั้นมีจำนวนจริง $c_1, c_2, c_3, c_4, c_5, c_6, c_7$ ที่ทำให้

$$\frac{x^2+3}{(x^2+1)^2(x+1)^2(x-1)} = \frac{c_1+c_2x}{x^2+1} + \frac{c_3+c_4x}{(x^2+1)^2} + \frac{c_5}{x+1} + \frac{c_6}{(x+1)^2} + \frac{c_7}{x-1}$$

ตัวอย่าง 7.3.10

จงเขียนฟังก์ชันตรรกยะ $\dfrac{2x^4+3x^2-x}{(x^2+1)^2(x-1)}$ ในรูปผลบวกเศษส่วนย่อย

วิธีทำ มีจำนวนจริง c_1, c_2, c_3, c_4, c_5 ที่ทำให้

$$\frac{2x^4+3x^2-x}{(x^2+1)^2(x-1)} = \frac{c_1+c_2x}{x^2+1} + \frac{c_3+c_4x}{(x^2+1)^2} + \frac{c_5}{x-1}$$

ดังนั้น $2x^4+3x^2-x = (c_1+c_2x)(x^2+1)(x-1) + (c_3+c_4x)(x-1) + c_5(x^2+1)^2$
เมื่อ $x=1$ จะได้ว่า $4c_5 = 4$ นั่นคือ $c_5 = 1$ พิจารณาการแทนค่า $x = 0, -1, 2, -2$ จะได้ว่า

$$\begin{aligned}
-\quad c_1 \quad\quad\quad -\quad c_3 \quad\quad\quad &= -1 \\
-\quad 4c_1 + 4c_2 - 2c_3 + 2c_4 &= 2 \\
\quad\quad 5c_1 + 10c_2 + c_3 + 2c_4 &= 17 \\
-\quad 15c_1 + 30c_2 - 3c_3 + 6c_4 &= 21
\end{aligned}$$

จากการแก้ระบบสมการดังกล่าวจะได้ว่า $c_1 = 1, c_2 = 1, c_3 = 0, c_4 = 1$ ดังนั้น

$$\frac{2x^4+3x^2-x}{(x^2+1)^2(x-1)} = \frac{1+x}{x^2+1} + \frac{x}{(x^2+1)^2} + \frac{1}{x-1}$$

ตัวอย่าง 7.3.11

จงหา $\displaystyle\int \frac{x^2+x+1}{(x^2+1)^2}\,\mathrm{d}x$

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{x^2+x+1}{(x^2+1)^2} = \frac{(x^2+1)+x}{(x^2+1)^2} = \frac{1}{x^2+1} + \frac{x}{(x^2+1)^2}$$

จะได้ว่า

$$\begin{aligned}
\int \frac{x^2+x+1}{(x^2+1)^2}\mathrm{d}x &= \int \frac{1}{x^2+1}\mathrm{d}x + \int \frac{x}{(x^2+1)^2}\mathrm{d}x \\
&= \arctan(x) - \frac{1}{2(x^2+1)} + C
\end{aligned}$$

สรุปท้ายบท

ในบทนี้กล่าวถึงการให้ความหมายของพหุนาม $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ ดีกรี n เมื่อ $a_n \neq 0$ และไม่นิยามดีกรีในกรณีที่ $P(x) = 0$ จากนั้นนิยามการเท่ากันของพหุนามสองตัวก็ต่อเมื่อดีกรีเท่ากันและสัมประสิทธิ์ทุกตัวตรงกัน จากนั้นนิยามการบวกและการคูณของพหุนาม โดยเฉพาะการคูณอาจอาศัยวิธี grid method มาช่วยหาผลคูณในกรณีที่พหุนามมีดีกรีสูงและมีหลายพจน์ไม่ใช่ศูนย์ และอาศัยหลักการที่คล้ายคลึงกับขั้นตอนวิธีการหารในระบบจำนวนเต็ม จะได้ขั้นตอนวิธีการหารสำหรับพหุนามที่กล่าวไว้ว่า สำหรับ $P(x)$ และ $S(x)$ เป็นพหุนาม โดยที่ $S(x)$ ไม่ใช่พหุนามศูนย์ แล้วจะมีพหุนาม $Q(x)$ และ $R(x)$ เพียงคู่เดียวที่สอดคล้องกับ

$$P(x) = Q(x)S(x) + R(x) \text{ เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x)$$

ซึ่งการหาผลหารและเศษเหลือจากการหารยาว หรือการจัดรูปพหุนาม $P(x)$ ในรูป $Q(x)$ ในกรณีที่ $Q(x) = x - c$ โดยขั้นตอนวิธีการหารจะได้ทฤษฎีบทเศษเหลือที่ว่า

$$x - c \text{ หาร } P(x) \text{ เศษเหลือเท่ากับ } P(c)$$

ทฤษฎีบทนี้นำไปใช้ตรวจสอบรากของพหุนาม และยังนำไปสร้างวิธีการหารสังเคราะห์ซึ่งง่ายต่อการหาผลหารและเศษเหลือ จากนั้นศึกษาการตรวจสอบรากที่เป็นจำนวนตรรกยะของพหุนามใน $\mathbb{Z}[x]$ โดยเฉพาะกรณีพหุนามโมนิกที่ว่าถ้า $P(x) \in \mathbb{Z}[x]$ และ $n \in \mathbb{N}$ โดยที่ $a_0 \neq 0$ ซึ่ง

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

เป็นรากที่เป็นจำนวนเต็มของ $P(x)$ ต้องเป็นตัวหารของ a_0 สุดท้ายกล่าวถึงฟังก์ชันตรรกยะที่สามารถเขียน ในรูปเศษส่วนย่อยได้ ถ้า $\deg P(x) < n$ และ $a_1, a_2, \ldots, a_n$ แตกต่างกันทั้งหมดจะได้

$$\frac{P(x)}{(x-a_1)(x-a_2)\cdots(x-a_n)} = \frac{c_1}{x-a_1} + \frac{c_2}{x-a_2} + \cdots + \frac{c_n}{x-a_n}$$
$$\frac{P(x)}{(x-a_1)^n} = \frac{c_1}{x-a_1} + \frac{c_2}{(x-a_1)^2} + \cdots + \frac{c_n}{(x-a_n)^n}$$

และขยายแนวคิดไปยังกรณีทั่วไปคือถ้า $Q(x) = [q_1(x)]^{n_1}[q_2(x)]^{n_2}\cdots[q_k(x)]^{n_k}$ โดยที่แต่ละ $q_i(x)$ เป็นพหุนามโมนิก ซึ่ง $\deg q_i(x) \geq 1$ และไม่ซ้ำกัน มีสมบัติว่าทุก ๆ พหุนาม $q(x)$ ซึ่ง $q(x) \mid q_i(x)$ แล้ว $q(x) = \pm 1$ หรือ $q(x) = \pm q_i(x)$ ให้ $P(x)$ เป็นพหุนามที่มีดีกรีน้อยกว่าดีกรีของ $Q(x)$ จะได้ว่า

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n_1} \frac{c_{1i}(x)}{[q_1(x)]^i} + \sum_{i=1}^{n_2} \frac{c_{2i}(x)}{[q_2(x)]^i} + \cdots + \sum_{i=1}^{n_k} \frac{c_{ki}(x)}{[q_k(x)]^i}$$

เมื่อ $c_{ij}(x)$ เป็นพหุนาม โดยที่ $c_{ij}(x) = 0$ หรือ $\deg c_{ij}(x) < \deg q_i(x)$ ทุก ๆ i, j

แบบฝึกหัดท้ายบทที่ 7

1. จงหาเศษเหลือและผลหารจากการหาร $p(x)$ ด้วย $q(x)$

   (1.1) $q(x) = x - 1$ และ $p(x) = x^3 + x - 4$

   (1.2) $q(x) + 2$ และ $p(x) = x^3 - 2x^2 - x + 1$

   (1.3) $q(x) = 2x - 1$ และ $p(x) = x^4 + x - 4$

   (1.4) $q(x) = 1 - x^2$ และ $p(x) = 2x^4 + x^2 - x + 1$

2. จงหา k ที่สอดคล้องกับเงื่อนไขต่อไปนี้

   (2.1) $x - 1$ หาร $x^3 - 3x^2 + 4x + 2k$ เศษเหลือเท่ากับ -2

   (2.2) $x - 2$ หาร $x^3 + kx^2 + (k + 1)x + 5$ เศษเหลือเท่ากับ 5

   (2.3) $2x - 1$ หาร $2x^4 - 3kx + x - k$ ลงตัว

3. จงเขียนฟังก์ชันตรรกยะต่อไปนี้เป็นผลบวกของเศษส่วนย่อย

   (3.1) $\dfrac{4 - 2x}{(x + 1)(x + 3)}$

   (3.2) $\dfrac{4 - 2x}{(x^2 + 1)(x - 1)^2}$

   (3.3) $\dfrac{x}{(x^2 + 1)(x - 1)}$

   (3.4) $\dfrac{2x^2 + 5x - 1}{x^3 + x^2 - 2x}$

4. จงหาตัวประกอบของพหุนามต่อไปนี้

   (4.1) $x^3 + 6x^2 + 11x + 6$

   (4.2) $10x^3 + 3x^2 - 50x + 24$

   (4.3) $x^5 + 10x^3 - 10x^2 + 5x - 1$

   (4.4) $x^6 + 3x^5 + 2x^4 + x^2 + 3x + 2$

   (4.5) $2x^3 + 3x^2 - 5x - 6$

   (4.6) $12x^3 + 16x^2 - 5x - 3$

   (4.7) $3x^4 - 8x^3 + x^2 + 8x - 4$

   (4.8) $4x^4 - 4x^3 - 25x^2 + x + 6$

   (4.9) $2x^4 + 3x^3 - 16x^2 - 8x + 24$

   (4.10) $4x^5 + 16x^4 + 9x^3 - 31x^2 - 40x - 12$

   (4.11) $6x^5 + 11x^4 - 9x^3 - 13x^2 + 3x + 2$

   (4.12) $6x^5 + 13x^4 - 20x^3 - 10x^2 + 14x - 3$

5. จงหารากของสมหารต่อไปนี้

   (5.1) $x^3 - 2x^2 + x + 4 = 0$

   (5.2) $x^3 - 5x^2 - 2x + 10 = 0$

   (5.3) $2x^3 - 3x^2 - 7x - 6 = 0$

   (5.4) $x^3 - 2x^2 - 5x + 6 = 0$

   (5.5) $2x^3 - 7^2x + 7x - 2 = 0$

   (5.6) $x^5 + x^3 - 2x^2 - 12x = 0$

6. ถ้า $3x^2 - 13x + 4$ เป็นตัวประกอบของ $3x^3 + ax^2 + bx - 8$ แล้วค่าของ $a + b$ มีค่าเท่าใด

7. ให้ $a, b \in \mathbb{R}$ เมื่อ $x + 1$ หารพหุนาม $2x^4 - 7x^3 + ax^2 + 7x + b$ ลงตัว และได้ผลลัพธ์เท่ากับ $2x^3 - 9x^2 + 7x + b$ จงหา $a + b$

8. กำหนดให้ $P(x) = x^3 + ax^2 + bx + 2$ เมื่อ a, b เป็นจำนวนจริง ถ้า $x - 1$ และ $x + 3$ ต่างหาร $P(x)$ เศษเหลือเท่ากับ 5 แล้ว $a + 2b$ มีค่าเท่าใด

9. กำหนดให้ $P(x) = x^6 + ax^2 - x + b$ เมื่อ a, b เป็นจำนวนจริง ถ้า $x - 1$ หาร $P(x)$ เศษเหลือคือ -1 และ $x + 1$ หาร $P(x)$ เศษเหลือคือ 1 แล้ว x หาร $P(x)$ เศษเหลือเท่ากับเท่าใด

10. ถ้า $x^{2559} - ax - 1$ หารด้วย $x^2 - 1$ เศษเหลือเท่ากับ $r(x)$ และ $r(2) = 123$ จงหา a

11. ถ้า a, b และ c เป็นรากของพหุนาม $x^3 - 7x^2 - 6x + 5$ แล้ว $(a + b)(a + c)(b + c)$ มีค่าเท่าใด

เอกสารอ้างอิง

ฉวีวรรณ รัตนประเสริฐ. (2552). **พีชคณิต (พิมพ์ครั้งที่ 3)**. กรุงเทพฯ : มูลนิธิ สอวน.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

Josip Hercet, Lorraine Heienrichs, Palmira Mariz Seiler and Marlence Torres Skoumal. (2012). **Mathematics higher level**. New York: Oxford university press.

แผนบริหารการสอนประจำบทที่ 8

เนื้อหาประจำบท

1. อันดับของจำนวนเต็มมอดุโล
2. ทฤษฎีบทของดรรชนี
3. กฎภาวะส่วนกลับกำลังสอง
    3.1 สมภาคกำลังสอง
    3.2 สัญลักษณ์เลอจองด์
    3.3 กฎภาวะส่วนกลับกำลังสอง
    3.4 สัญลักษณ์ยาโคบี

วัตถุประสงค์เชิงพฤติกรรม

1. ใช้นิยามและสมบัติพื้นฐานของอันดับของจำนวนเต็มมอดุโลแก้โจทย์ปัญหาที่กำหนดให้ได้
2. ใช้นิยามและสมบัติพื้นฐานของทฤษฎีบทของดรรชนีแก้โจทย์ปัญหาที่กำหนดให้ได้
3. ใช้นิยามและสมบัติพื้นฐานของกฎภาวะส่วนกลับกำลังสองแก้โจทย์ปัญหาที่กำหนดให้ได้

วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. ผู้สอนบรรยายหัวข้อต่อไปนี้พร้อมเปิดโอกาสให้ซักถาม
    1.1 อันดับของจำนวนเต็มมอดุโล
    1.2 ทฤษฎีบทของดรรชนี
    1.3 กฎภาวะส่วนกลับกำลังสอง
2. ให้นักศึกษาทำกิจกรรมต่อไปนี้
    2.1 ทำแบบฝึกหัดที่กำหนดให้
    2.2 นำเสนอแบบฝึกหัดที่ได้รับมอบหมาย
    2.3 อภิปรายแลกเปลี่ยนเรียนรู้ซึ่งกันและกัน

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. ตำราต่าง ๆ ที่เกี่ยวข้อง
3. Slide Presentation

การวัดผลและการประเมินผล

1. สังเกตความสนใจของนักศึกษาขณะสอน
2. การตอบคำถาม
3. แบบทดสอบท้ายชั่วโมง
4. ใบงาน
5. การเสนองาน และอธิบายให้เพื่อนนชั้นเรียนเข้าใจ

บทที่ 8
รากปฐมฐาน ดรรชนีและกฎภาวะส่วนกลับกำลังสอง

ในบทที่ 4 เราพิจารณาหาผลเฉลยของสมภาคเชิงเส้น ในบทนี้เราจะพิจารณาหาผลเฉลยของสมภาคที่อยู่ในรูป $r^x \equiv a \pmod{m}$ เรียก r ว่ารากปฐมฐาน (primitive root) มอดุโล m และเรียก x ว่าดรรชนี (Index) โดยเราจะเริ่มต้นด้วยการศึกษาอันดับของจำนวนเต็มและศึกษาทฤษฎีบทเกี่ยวกับ อันดับของจำนวนเต็ม จากนั้นจะกล่าวถึงสมบัติของรากปฐมฐานมอดุโล m และศึกษาทฤษฎีบทของดรรชนีเพื่อที่จะนำไปใช้หาผลเฉลยของสมภาคได้สะดวกและรวดเร็วยิ่งขึ้น

8.1 อันดับของจำนวนเต็มมอดุโล m

ในบทที่ 4 ได้กล่าวถึงทฤษฎีบทของออยเลอร์แล้วว่า m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม ซึ่ง $(a,m)=1$ จะได้ว่า $a^{\phi(m)} \equiv 1 \pmod{m}$ ดังนั้นจะมีจำนวนเต็ม k ที่น้อยสุดที่ทำให้ $a^k \equiv 1 \pmod{m}$ ดังบทนิยามต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 170, จิราภา ลิ้มบุพศิริพร. 2555 : 140, Raji W. 2013 : 91, Rosen K. H. 2005 : 334)

บทนิยาม 8.1.1

ให้ a และ m เป็นจำนวนเต็มบวก โดยที่ $m>1$ และ $(a,m)=1$ เรียกจำนวนเต็ม k มีค่าน้อยสุด ที่ $a^k \equiv 1 \pmod{m}$ ว่า อันดับของ a มอดุโล m (the order of modulo) เขียนแทนด้วย $\operatorname{ord}_m a = k$

ตัวอย่าง 8.1.1

จงหาอันดับของ 2 มอดุโล 7

วิธีทำ เนื่องจาก
$$2^1 \equiv 2 \pmod{7}$$
$$2^2 \equiv 4 \pmod{7}$$
$$2^3 \equiv 1 \pmod{7}$$
$$2^4 \equiv 2 \pmod{7}$$
$$2^5 \equiv 4 \pmod{7}$$
$$2^6 \equiv 1 \pmod{7}$$

จะเห็นว่า 3 เป็นจำนวนเต็มบวกค่าน้อยสุด ที่ทำให้ $2^3 \equiv 1 \pmod{7}$

นั่นคือ อันดับของ 2 มอดุโล 7 คือ 3 หรือ $\operatorname{ord}_7 2 = 3$

ตัวอย่าง 8.1.1 เราได้ $2^k \equiv 1 \pmod{7}$ เมื่อ k เป็นพหุคูณของ 3 โดยที่ 3 เป็นอันดับของ 2 มอดุโล 7 เป็นกรณีตัวอย่าง กรณีทั่วไปจะกล่าวดังทฤษฎีบทต่อไปนี้ (จิราภา ลิ้มบุพศิริพร. 2555 : 140, สมใจ จิตพิทักษ์. 2547 : 176, Raji W. 2013 : 90)

ทฤษฎีบท 8.1.1

กำหนดให้ a เป็นจำนวนเต็ม ที่ $(a,m)=1$ และ k เป็นอันดับของ a มอดุโล m สำหรับทุกจำนวนเต็มบวก h จะได้ว่า $a^h \equiv 1 \pmod{m}$ ก็ต่อเมื่อ $k \mid h$

การพิสูจน์ ($\Rightarrow$) สมมติให้ h เป็นอันดับของ a มอดุโล m ที่ $a^h \equiv 1 \pmod{m}$
โดยขั้นตอนวิธีการหารจะมีจำนวนเต็ม q และ r โดยที่ $h = qk + r, 0 \leq r < k$
ดังนั้น $a^h = a^{qk+r} = \left(a^k\right)^q a^r$
จากสมมติ $a^h \equiv 1 \pmod{m}$ และ $a^k \equiv 1 \pmod{m}$
จะได้ว่า $a^r \equiv 1 \pmod{m}$
เนื่องจาก $0 \leq r < k$ จะได้ว่า $r = 0$
ดังนั้น $h = qk$ นั่นคือ $k \mid h$
($\Leftarrow$) สมมติ $k \mid h$ จะมีจำนวนเต็ม j ที่ทำให้ $h = kj$
เนื่องจาก $a^k \equiv 1 \pmod{m}$ ดังนั้น $\left(a^k\right)^j \equiv 1^j \pmod{m}$
นั่นคือ $a^h \equiv 1 \pmod{m}$ □

บทแทรกที่ได้จากทฤษฎีบท 8.1.1 ดังต่อไปนี้ (จิราภา ลิ้มบุพศิริพร. 2555 : 141, สมใจ จิตพิทักษ์. 2547 : 176, อัจฉรา หาญชูวงศ์. 2542 : 71, Rosen K. H. 2005 : 335)

บทแทรก 8.1.1

ถ้า $\text{ord}_m a = k$ แล้ว $k \mid \phi(m)$

การพิสูจน์ โดยทฤษฎีบทของออยเลอร์ $a^{\phi(m)} \equiv 1 \pmod{m}$
และจากทฤษฎีบท 8.1.1 จะได้ $k \mid \phi(m)$ □

ตัวอย่าง 8.1.2

จงหาอันดับของ 2 มอดุโล 13

วิธีทำ เนื่องจาก $\phi(13) = 12$
ดังนั้นเราจะพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k \mid 12$
นั่นคือ $k = 1, 2, 3, 4, 6$ และ 12 ขั้นตอนการคำนวณอาจเป็นได้ดังนี้

$$\begin{aligned}
2^1 &\equiv 2 \pmod{13} \\
2^2 &\equiv 4 \pmod{13} \\
2^3 &\equiv 8 \pmod{13} \\
2^4 &\equiv 3 \pmod{13} \\
2^6 &\equiv 4 \cdot 3 \equiv 12 \pmod{13} \\
2^{12} &\equiv 4 \cdot 8 \cdot 3 \equiv 96 \equiv 1 \pmod{13}
\end{aligned}$$

ดังนั้นจำนวนเต็มบวก k ค่าน้อยสุด ซึ่ง $k \mid \phi(13)$ และ $a^k \equiv 1 \pmod{13}$ คือ $k = 12$
นั่นคือ อันดับของ 2 มอดุโล 13 คือ 12 หรือ $\text{ord}_{13}\, 2 = 12$

ทฤษฎีบทต่อไปนี้เป็นทฤษฎีเบื้องต้นเกี่ยวกับอันดับของจำนวนเต็มอีกทฤษฎีหนึ่ง (จิราภา ลิ้มบุพศิริพร. 2555 : 142, สมใจ จิตพิทักษ์. 2547 : 177, Raji W. 2013 : 90-91)

ทฤษฎีบท 8.1.2

ถ้า $\text{ord}_m a = k$ จะได้ว่า $a^s \equiv a^t \pmod{m}$ ก็ต่อเมื่อ $s \equiv t \pmod{m}$

การพิสูจน์ ($\Rightarrow$) สมมติให้ $a^s \equiv a^t \pmod{m}$ ซึ่ง $(a, m) = 1$ และให้ $s \geq t$
โดยทฤษฎีบท 8.1.1 จะได้ $m \mid (s - t)$
นั่นคือ $s \equiv t \pmod{m}$
($\Leftarrow$) สมมติให้ $s \equiv t \pmod{m}$ โดยบทนิยาม 4.1.1
จะได้ $m \mid (s - t)$ จะได้ว่ามีจำนวนเต็ม q ที่ทำให้ $s = t + qk$
ดังนั้น $a^s = a^{t+qk} = a^t \cdot a^{qk}$ แต่ k เป็นอันดับของ a มอดุโล m
ดังนั้น
$$a^k \equiv 1 \pmod{m}$$
$$a^{qk} \equiv 1 \pmod{m}$$
$$a^t \cdot a^{qk} \equiv a^t \pmod{m}$$
นั่นคือ
$$a^s \equiv a^t \pmod{m}$$
□

บทแทรกที่ได้จากทฤษฎีบท 8.1.2 ดังต่อไปนี้ (จิราภา ลิ้มบุพศิริพร. 2555 : 142, สมใจ จิตพิทักษ์. 2547 : 177, David M. Burton. 2007 : 149)

บทแทรก 8.1.2

ถ้า $\text{ord}_m a = k$ จะได้ว่า $a, a^2, \ldots, a^k$ จะไม่สมภาคกันมอดุโล m

การพิสูจน์ ถ้ามี s และ t ซึ่ง $1 \leq s < t \leq k$ ซึ่ง $a^s \equiv a^t \pmod{m}$
โดยทฤษฎีบท 8.1.2 จะได้ว่า $s \equiv t \pmod{m}$
แต่ในกรณีนี้จะเกิดขึ้นไม่ได้นอกเสียจากว่า $s = t$ □

ทฤษฎีบทต่อไปนี้จะกล่าวเกี่ยวกับอันดับของ a กำลัง (power of a) ดังต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 174, จิราภา ลิ้มบุพศิริพร. 2555 : 142, สมวงษ์ แปลงประสพโชค. 2545 : 145, David M. Burton. 2007 : 149)

ทฤษฎีบท 8.1.3

ถ้า $\text{ord}_m a = k$ และ $h > 0$ จะได้ว่า $\text{ord}_m a^h = \left(\frac{k}{(h,k)}\right)$

การพิสูจน์ ให้ $d = (h, k)$ จะได้ว่า $h = (h_1, d)$ และ $k = (k_1, d)$ เมื่อ $(h_1, k_1) = 1$
จะได้ว่า $\left(a^h\right)^{k_1} = \left(a^{h_1 d}\right)^{\frac{k}{d}} = a^{kh_1} \equiv 1 \pmod{m}$
สมมติว่า $\text{ord}_m a^h = r$ จากทฤษฎีบท 8.1.1 จะได้ $r \mid k_1$ และ $\left(a^h\right)^r \equiv 1 \pmod{m}$
แต่ $\text{ord}_m a = k$ ดังนั้น $k \mid hr$ จะได้ $k_1 d \mid h_1 dr$
ดังนั้น $k_1 \mid h_1 r$ แต่ $(h_1, k_1) = 1$ ดังนั้น $k_1 \mid r$
เมื่อ $k_1 \mid r$ และ $r \mid k_1$ ดังนั้น $r = k_1 = \frac{k}{d} = \left(\frac{k}{(h,k)}\right)$ □

บทแทรกต่อไปนี้เป็นผลโดยตรงจากทฤษฎีบท 8.1.3 (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 174, สมใจ จิตพิทักษ์. 2547 : 177, David M. Burton. 2007 : 149)

บทแทรก 8.1.3

ถ้า $\operatorname{ord}_m a = k$ และถ้า $(h,k) = 1$ จะได้ว่า $\operatorname{ord}_m a^h = k$

การพิสูจน์ จากทฤษฎีบท 8.1.3 ถ้า $\operatorname{ord}_m a = k$ จะได้ว่า $\operatorname{ord}_m a^h = \left(\dfrac{k}{(h,k)}\right)$

ถ้า $(h,k) = 1$ จะได้ว่า $\operatorname{ord}_m a^h = k$ □

ตัวอย่าง 8.1.3

จงหาอันดับของ $5, 5^2, 5^3, 5^4, 5^5, 5^6$ มอดุโล 7

วิธีทำ ขั้นตอนการคำนวณอาจเป็นได้ดังนี้

$$\begin{aligned}
5^1 &\equiv 5 \pmod 7 \\
5^2 &\equiv 4 \pmod 7 \\
5^3 &\equiv 5 \times 4 = 20 \equiv 6 \pmod 7 \\
5^4 &\equiv 4 \times 4 = 16 \equiv 2 \pmod 7 \\
5^5 &\equiv 2 \times 5 = 10 \equiv 3 \pmod 7 \\
5^6 &\equiv 5 \times 3 = 15 \equiv 1 \pmod 7
\end{aligned}$$

เพราะฉะนั้น ทราบอันดับของทุกตัว ดังนี้

$$\begin{aligned}
\operatorname{ord}_7 5 &= \frac{6}{(1,6)} = 6, & \operatorname{ord}_7 5^2 &= \frac{6}{(2,6)} = 3 \\
\operatorname{ord}_7 5^3 &= \frac{6}{(3,6)} = 2, & \operatorname{ord}_7 5^4 &= \frac{6}{(4,6)} = 3 \\
\operatorname{ord}_7 5^5 &= \frac{6}{(5,6)} = 6, & \operatorname{ord}_7 5^6 &= \frac{6}{(6,6)} = 1
\end{aligned}$$

ตัวอย่าง 8.1.4

จงหาอันดับมอดุโล 13 ของจำนวนเต็มบวกที่น้อยกว่า 13

วิธีทำ ให้ $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ หาอันดับมอดุโล 13 ดังตารางที่ 8.1

n	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ord}_{13} n$	1	12	3	6	4	12	12	4	3	6	12	2

ตารางที่ 8.1 อันดับมอดุโล 13 ของจานวนเต็มบวกที่น้อยกว่า 13

จากตารางที่ 8.1 จะเห็นว่า $\operatorname{ord}_{13} 2 = 12$
ในขณะเดียวกัน $\operatorname{ord}_{13} 2^2 = 6$ และ $\operatorname{ord}_{13} 2^3 = 4$
โดยทฤษฎีบท 8.1.3 สามารถตรวจสอบจำนวนเต็มอื่น ๆ

ซึ่งมีอันดับ 12 มอดุโล 13 คือ 2^k ซึ่ง $(k, 12) = 1$ ได้แก่

$$2^5 \equiv 6 \pmod{13}$$
$$2^7 \equiv 11 \pmod{13}$$
$$2^{11} \equiv 7 \pmod{13}$$

ซึ่ง 5,7 และ 11 เป็นจำนวนเฉพาะสัมพัทธ์กับ 12

ถ้าจำนวนเต็ม a มีอันดับสูงสุดเท่าที่เป็นไปได้ เราจะเรียก a ว่า รากปฐมฐานของ m (primitive root of m) ดังบทนิยามต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 175, สมใจ จิตพิทักษ์. 2547 : 178, สมวงษ์ แปลงประสพโชค. 2545 : 146, David M. Burton. 2007 : 150)

บทนิยาม 8.1.2

ถ้า $\operatorname{ord}_m a = k$ และ $\operatorname{ord}_m a = \phi(m)$ จะเรียก a ว่ารากปฐมฐานของ m (primitive root of m) กล่าวอีกอย่างหนึ่งว่า m มีรากปฐมฐานเป็น a ก็ต่อเมื่อ $a^{\phi(m)} \equiv 1 \pmod{m}$ แต่ $a^k \not\equiv 1 \pmod{m}$ สำหรับจำนวนเต็ม k ซึ่ง $k < \phi(m)$

ตัวอย่าง 8.1.5

จงตรวจสอบว่า 2 และ 3 เป็นรากปฐมฐานของ 7 หรือไม่

วิธีทำ $\phi(7) = 6$ ให้ $a = 2$ และ 3 ขั้นตอนคำนวณดังนี้

$a = 2$	$a = 3$
$2^1 \equiv 2 \pmod{7}$	$3^1 \equiv 3 \pmod{7}$
$2^2 \equiv 4 \pmod{7}$	$3^2 \equiv 2 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$	$3^3 \equiv 6 \pmod{7}$
$2^4 \equiv 2 \pmod{7}$	$3^4 \equiv 4 \pmod{7}$
$2^5 \equiv 4 \pmod{7}$	$3^5 \equiv 5 \pmod{7}$
$2^6 \equiv 1 \pmod{7}$	$3^6 \equiv 1 \pmod{7}$

นั่นคือ 3 เป็นรากปฐมฐานของ 7 แต่ 2 ไม่เป็นรากปฐมฐานของ 7

วรางคณา ร่องมะรุด. (2523 : 118-119) ได้เฉลยแบบฝึกหัดเพื่อให้เกิดความเข้าใจบทนิยามมากขึ้นดังนี้

ตัวอย่าง 8.1.6

จงตรวจสอบว่า 3 และ 7 เป็นรากปฐมฐานของ 10 หรือไม่

วิธีทำ $\phi(10) = \phi(2)\phi(5) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$

ตรวจสอบ 3^k และ 7^k เมื่อ $k \leq 4$ ดังนี้

$3^1 \equiv 3 \pmod{10}$	$7^1 \equiv 7 \pmod{10}$
$3^2 \equiv 9 \pmod{10}$	$7^2 \equiv 9 \pmod{10}$
$3^3 \equiv 7 \pmod{10}$	$7^3 \equiv 3 \pmod{10}$
$3^4 \equiv 1 \pmod{10}$	$7^4 \equiv 1 \pmod{10}$

จะเห็นว่าเมื่อ $k < 4$ ได้ว่า $3^k \not\equiv 1 \pmod{10}$ และ $7^k \not\equiv 1 \pmod{10}$
แต่ $3^4 \equiv 1 \pmod{10}$ และ $7^4 \equiv 1 \pmod{10}$
นั่นคือ 3 และ 7 เป็นรากปฐมฐานของ 10

ตัวอย่าง 8.1.5 และ ตัวอย่าง 8.1.6 จะเห็นว่ารากปฐมฐานของ 7 และ 10 มีมากกว่า 1 ตัว แต่จำนวนเต็มทุกจำนวนไม่จำเป็นต้องมีรากปฐมฐาน ส่วนสำหรับจำนวนเฉพาะเราจะพิสูจน์ต่อไปว่ามีรากปฐมฐานเสมอ ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 175, สมใจ จิตพิทักษ์. 2547 : 176, สมวงษ์ แปลงประสพโชค, 2545 : 147, David M. Burton. 2007 : 150-151)

ทฤษฎีบท 8.1.4

ถ้า a เป็นรากปฐมฐานของ m จะได้ว่า $a^1, a^2, \ldots, a^{\phi(m)}$ จะเป็นระบบส่วนตกค้างลดทอนมอดุโล m

การพิสูจน์ เนื่องจาก a เป็นรากปฐมฐาน จะได้ว่า $(a, m) = 1$
ดังนั้น $a^1, a^2, \ldots, a^{\phi(m)}$ เป็นจำนวนเฉพาะสัมพัทธ์กับ m
และเนื่องจาก a เป็นรากปฐมฐาน ดังนั้น $\operatorname{ord}_m a = \phi(m)$
โดยบทนิยาม 8.1.2 จะได้ว่า $a^{\phi(m)} \equiv 1 \pmod{m}$ แต่ $a^k \not\equiv 1 \pmod{m}$
สำหรับจำนวนเต็มบวก k ซึ่ง $k < \phi(m)$ จากบทแทรก 8.1.2
จะได้ว่า $a^1, a^2, \ldots, a^{\phi(m)}$ ไม่สมภาคกันมอดุโล m
นั่นคือ $a^1, a^2, \ldots, a^{\phi(m)}$ จะเป็นระบบส่วนตกค้างลดทอนมอดุโล m □

จากทฤษฎีบท 8.1.4 $a^1, a^2, \ldots, a^{\phi(m)}$ จะเป็นระบบส่วนตกค้างลดทอนมอดุโล m ดังนั้นสมาชิก แต่ละตัวจึงไม่สมภาคกับ $a_1, a_2, \ldots, a_{\phi(m)}$ มอดุโล m เป็นคู่ ๆ แบบหนึ่งต่อหนึ่งโดยที่ $1 < a_i < m$ ในกรณีที่รากปฐมฐานหาได้ เราจะได้จากบทแทรกต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 177, สมใจ จิตพิทักษ์. 2547 : 179, David M. Burton. 2007 : 151)

บทแทรก 8.1.4

ถ้า m มีรากปฐมฐานแล้ว m จะมีรากปฐมฐานอยู่ $\phi(\phi(m))$ จำนวน

การพิสูจน์ สมมติให้ a เป็นรากปฐมฐานหนึ่งของ m ดังนั้น $\operatorname{ord}_m a = \phi(m)$
พิจารณา $a^1, a^2, \ldots, a^{\phi(m)}$ ซึ่งเป็นระบบส่วนตกค้างลดทอนมอดุโล m
โดยทฤษฎีบท 8.1.4 จะหารากปฐมฐานตัวอื่นได้จากสมาชิกของเซต $\{a^1, a^2, \ldots, a^{\phi(m)}\}$
โดยหา $\operatorname{ord}_m a$ แต่ละตัว จากทฤษฎีบท 8.1.3 ดังนี้

$$\operatorname{ord}_m a^2 = \frac{\phi(m)}{(2, \phi(m))}$$
$$\operatorname{ord}_m a^3 = \frac{\phi(m)}{(3, \phi(m))}$$
$$\vdots$$
$$\operatorname{ord}_m a^{\phi(m)} = \frac{\phi(m)}{(\phi(m), \phi(m))}$$

ดังนั้น $\operatorname{ord}_m a^k = \phi(m)$ ก็ต่อเมื่อ $(k, \phi(m)) = 1$ แต่จำนวน k ที่น้อยกว่า $\phi(m)$
ซึ่ง $(k, \phi(m)) = 1$ มี $\phi(\phi(m))$ จำนวน
นั่นคือ m มีรากปฐมฐานทั้งหมด $\phi(\phi(m))$ จำนวน □

ตัวอย่าง 8.1.7

จงหารากปฐมฐานของ 9

วิธีทำ เนื่องจาก $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$
ดังนั้น $\phi(\phi(9)) = \phi(6) = \phi(2)\phi(3) = 2$
นั่นคือรากปฐมฐานของ 9 มี 2 จำนวน

8.2 ทฤษฎีบทของดรรชนี

ในหัวข้อนี้จะศึกษาวิธีการใช้รากปฐมฐานกับสมภาค ถ้า r เป็นรากปฐมฐานมอดุโล m โดยทฤษฎีบท 8.1.4 จะได้ว่าจำนวนเต็ม $r, r^2, r^3, \ldots, r^{\phi(m)}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m ดังนั้น ถ้า a เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m จะได้ว่ามีจำนวนเต็ม x เพียงจำนวนเดียว ซึ่ง $1 \leq x \leq \phi(m)$ เขียนในรูปดังนี้

$$r^x \equiv a \pmod{m}$$

ดังจะกล่าวบทนิยามต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 196, มารศรี แนวจำปา. 2546 : 105, David M. Burton. 2007 : 163)

บทนิยาม 8.2.1

กำหนดให้ r เป็นรากปฐมฐานของ m ถ้า $(a, m) = 1$ จะได้ว่ามีจำนวนเต็ม x ที่มีค่าบวกน้อยสุด ที่ทำให้ $r^x \equiv a \pmod{m}$ แล้วจะเรียก x ว่า **ดรรชนี (Index)** ของ a เทียบกับฐาน r ซึ่ง $1 \leq x \leq \phi(m)$ เขียนแทนด้วย $x = \operatorname{ind}_r a$

ตัวอย่าง 8.2.1

กำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 5 และ

$$2^1 \equiv 2 \pmod{5}$$
$$2^2 \equiv 4 \pmod{5}$$
$$2^3 \equiv 3 \pmod{5}$$
$$2^4 \equiv 1 \pmod{5}$$

จึงได้ดรรชนีมอดุโล 5 เทียบกับฐาน 2
นั่นคือ $\operatorname{ind}_2 1 = 4,\ \operatorname{ind}_2 2 = 1,\ \operatorname{ind}_2 3 = 3,\ \operatorname{ind}_2 4 = 2$

ทฤษฎีบทต่อไปนี้จะกล่าวถึงสมบัติที่สำคัญของดรรชนีทำนองเดียวกับลอการิทึม ดังทฤษฎีบทต่อไปนี้ (จรินทร์ทิพย์ เฮงคราวิทย์. 2558 : 197, จิราภา ลิ้มบุพศิริพร. 2555 : 169, David M. Burton. 2007 : 164)

ทฤษฎีบท 8.2.1

ถ้า m เป็นจำนวนเต็มบวกซึ่งมี r เป็นรากปฐมฐาน ให้ a และ b เป็นจำนวนเต็ม โดยที่ $(a,m)=1$ และ $(b,m)=1$ จะได้ว่า

1. $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(m)}$ และ $\operatorname{ind}_r r \equiv 1 \pmod{\phi(m)}$
2. $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(m)}$
3. $\operatorname{ind}_r a^k \equiv k \cdot \operatorname{ind}_r a \pmod{\phi(m)}$ เมื่อ k เป็นจำนวนเต็มบวก

การพิสูจน์ 1. เนื่องจาก $r^{\operatorname{ind}_r 1} \equiv 1 \equiv r^0 \pmod{m}$ และ $r^{\operatorname{ind}_r 1} \equiv r \equiv r^1 \pmod{m}$
โดยทฤษฎีบท 8.1.2 จะได้ว่า $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(m)}$ และ $\operatorname{ind}_r r \equiv 1 \pmod{\phi(m)}$

2. จาก $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$ และ $r^{\operatorname{ind}_r b} \equiv b \pmod{m}$
โดยทฤษฎีบท 4.1.2 ข้อ 3. จะได้ว่า $r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \equiv r^{\operatorname{ind}_r a} r^{\operatorname{ind}_r b} \equiv ab \pmod{m}$
โดยทฤษฎีบท 8.1.2 จะได้ว่า $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(m)}$

3. กำหนดให้ k เป็นจำนวนเต็มบวก จาก $r^{\operatorname{ind}_r a} \equiv a \pmod{m}$
โดยทฤษฎีบท 4.1.2 ข้อ 5. จะได้ว่า
$r^{k\cdot\operatorname{ind}_r a} \equiv \left(r^{\operatorname{ind}_r a}\right)^k \equiv a^k \pmod{m}$
เนื่องจาก $r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{m}$
เพราะฉะนั้น $r^{\operatorname{ind}_r a^k} \equiv r^{k\cdot\operatorname{ind}_r a} \pmod{m}$
โดยทฤษฎีบท 8.1.2 จะได้ว่า
$\operatorname{ind}_r a^k \equiv k \cdot \operatorname{ind}_r a \pmod{\phi(m)}$ เมื่อ k เป็นจำนวนเต็มบวก □

ตัวอย่าง 8.2.2

กำหนดให้ $m=7$ และ $r=5$ เป็นรากปฐมฐานมอดุโล 7 ถ้า $\operatorname{ind}_5 2 = 4$ และ $\operatorname{ind}_5 3 = 5$ แล้ว จงหา $\operatorname{ind}_5 6$ และ $\operatorname{ind}_5 81$

วิธีทำ เนื่องจาก $\phi(7)=6$ ขั้นตอนการคำนวณจะได้

$$5^1 \equiv 5 \pmod{7} \quad 5^4 \equiv 2 \pmod{7}$$
$$5^2 \equiv 4 \pmod{7} \quad 5^5 \equiv 3 \pmod{7}$$
$$5^3 \equiv 6 \pmod{7} \quad 5^6 \equiv 1 \pmod{7}$$

แสดงดรรชนีของจำนวนเต็มเมื่อเทียบกับรากปฐมฐาน 5 มอดุโล 7 ดังตารางที่ 8.2

a	1	2	3	4	5	6
$\operatorname{ind}_5 a$	6	4	5	2	1	3

ตารางที่ 8.2 ดรรชนีของจำนวนเต็มเมื่อเทียบกับรากปฐมฐาน 5 มอดุโล 7

โดยทฤษฎีบท 8.2.1 ข้อ 2 และ 3 จะได้
$\operatorname{ind}_5 6 = \operatorname{ind}_5(2\cdot 3) \equiv \operatorname{ind}_5 2 + \operatorname{ind}_5 3 \equiv 4+5 = 9 \equiv 3 \pmod{6}$ และ
$\operatorname{ind}_5 81 = \operatorname{ind}_5 (3^4) \equiv 4 \cdot \operatorname{ind}_5 3 \equiv 4\cdot 5 = 20 \equiv 2 \pmod{6}$
นั่นคือ $\operatorname{ind}_5 6 = 3$ และ $\operatorname{ind}_5 81 = 2$

จากตาราง 8.2 สามารถหาส่วนตกค้างน้อยสุดได้ดังตาราง 8.3

a	1	2	3	4	5	6
$\operatorname{ind}_5 a$	6	4	5	2	1	3
$5^{\operatorname{ind}_5 a}$	5	4	6	2	3	1

ตารางที่ 8.3 ส่วนตกค้างน้อยสุดเมื่อเทียบกับรากปฐมฐาน 5 มอดุโล 7

โดยบรรทัดที่ 3 เป็นส่วนตกค้างน้อยสุดและจะเห็นว่า

$$2 \equiv 5^{\operatorname{ind}_5 2} = 5^4 \pmod 7 \text{ และ } 6 \equiv 5^{\operatorname{ind}_5 6} = 5^3 \pmod 7$$

ทฤษฎีบทของดรรชนีสามารถใช้หาผลเฉลยของสมภาคบางชนิดได้ เช่น สมภาคเชิงพหุนาม พิจารณา

$$x^k \equiv a \pmod m \tag{8.1}$$

โดยที่ m เป็นจำนวนเต็มบวกที่มีรากปฐมฐานและ $(a, m) = 1$ และ $k \geq 2$ โดยทฤษฎีบท 8.2.1 ข้อ 2. และข้อ 3. จึงได้ว่าสมภาค 8.1 สมมูลกับสมภาคเชิงเส้น

$$k \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\phi(m)} \tag{8.2}$$

เมื่อสมภาค 8.2 เป็นสมภาคเชิงเส้นที่มีตัวไม่ทราบค่าหรือตัวแปร

ถ้า $d = (k, \phi(m))$ และ $d \nmid \operatorname{ind} a$ จะได้ว่าสมภาค 8.2 ไม่มีผลเฉลย

ถ้า $d \mid \operatorname{ind} a$ จะได้ว่า 8.2 มีผลเฉลยของ $\operatorname{ind} x$ จำนวน d ผลเฉลยมอดุโล m ทำให้ตัวแปร x ในสมภาค 8.2 มีผลเฉลย d ผลเฉลยมอดุโล m ด้วย

ตัวอย่าง 8.2.3

จงหาผลเฉลยของ $2x^4 \equiv 5 \pmod{13}$ เมื่อกำหนดให้ $r = 2$ เป็นรากปฐมฐานมอดุโล 13

วิธีทำ เนื่องจาก $\phi(13) = 12$ กำหนดดังตารางที่ 8.4 ดังนี้

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6
$2^{\operatorname{ind}_2 a}$	2	4	8	3	6	12	11	9	5	10	7	1

ตารางที่ 8.4 ดรรชนีของจำนวนเต็มเมื่อเทียบกับฐาน 2 มอดุโล 12

โดยทฤษฎีบท 8.2.3 ข้อ 2. และข้อ 3. จะได้

$$\begin{aligned} \operatorname{ind}_2 2 + 4\operatorname{ind}_2 x &\equiv \operatorname{ind}_2 5 \pmod{12} \\ 1 + 4\operatorname{ind}_2 x &\equiv 9 \pmod{12} \\ 4\operatorname{ind}_2 x &\equiv 9 - 1 = 8 \pmod{12} \end{aligned}$$

ซึ่งสมมูลกับ $\operatorname{ind}_2 x \equiv 2 \left(\mod \frac{12}{(4,12)} = 3\right)$

จึงได้ว่า $\operatorname{ind}_2 x = 2, 5, 8, 11 \pmod{12}$

จากบทนิยาม 8.1.1 จะได้ว่า $x = 2^2, 2^5, 2^8, 2^{11} \pmod{13}$
จากตารางที่ 8.4 จะได้ $\operatorname{ind}_2 4 = 2, \operatorname{ind}_2 6 = 5, \operatorname{ind}_2 9 = 8$ และ $\operatorname{ind}_2 7 = 11$
ดรรชนีจึงได้ว่าสมภาค $2x^4 \equiv 5 \pmod{13}$ มีผลเฉลยดังนี้

$$x \equiv 4, 6, 9, 7 \pmod{13}$$

ดังนั้น ผลเฉลยของ $2x^4 \equiv 5 \pmod{13}$ คือ $x \equiv 4, 6, 9, 7 \pmod{13}$

เราสร้างตารางดรรชนีของรากปฐมฐานมอดุโล m ซึ่ง m ไม่จำเป็นต้องเป็นจำนวนเฉพาะ ในการหาผลเฉลยของสมภาคโดยอาศัยส่วนตกค้างน้อยสุด ดังตัวอย่างต่อไปนี้

ตัวอย่าง 8.2.4

จงหาผลเฉลยของ $4x^8 \equiv 25 \pmod{27}$ เมื่อกำหนดให้ $r = 2$ เป็นรากปฐมฐานมอดุโล 27

วิธีทำ เนื่องจาก $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$ กำหนดดังตารางที่ 8.5 ดังนี้

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^{\operatorname{ind}_2 a}$	2	4	8	16	5	10	20	13	26	25	23	19	11	22	17	7	14	1

ตารางที่ 8.5 ดรรชนีของจำนวนเต็มเมื่อเทียบกับฐาน 2 มอดุโล 18

โดยทฤษฎีบท 8.2.1 ข้อ 2. และข้อ 3. จะได้

$$\begin{aligned} \operatorname{ind}_2 4 + 8 \operatorname{ind}_2 x &\equiv \operatorname{ind}_2 25 \pmod{18} \\ 2 + 8 \operatorname{ind}_2 x &\equiv 10 \pmod{18} \\ \operatorname{sind}_2 x &\equiv 8 \pmod{18} \end{aligned}$$

ซึ่งสมมูลกับ $\operatorname{ind}_2 x \equiv 1 \left(\mod \frac{18}{(8,18)} = 9\right)$
จึงได้ว่า $\operatorname{ind}_2 x = 1, 10 \pmod{18}$
จากบทนิยาม 8.1.1 จะได้ว่า $x = 2^1, 2^{10} \pmod{27}$
จากตารางที่ 8.5 จะได้ $\operatorname{ind}_2 2 = 1$ และ $\operatorname{ind}_2 25 = 10$
ดรรชนีจึงได้ว่าสมภาค $4x^8 \equiv 25 \pmod{27}$ มีผลเฉลยดังนี้

$$x \equiv 2, 25 \pmod{27}$$

ดังนั้น ผลเฉลยของ $4x^8 \equiv 25 \pmod{27}$ คือ $x \equiv 2, 25 \pmod{27}$

ทฤษฎีบทต่อไปนี้จะช่วยในการตรวจสอบว่าสมภาคมีผลเฉลยหรือไม่ (David M. Burton. 2007 : 166)

ทฤษฎีบท 8.2.2

ให้ m เป็นจำนวนเต็มบวกที่มีรากปฐมฐาน ถ้า k เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม โดยที่ $(a, m) = 1$ จะได้ว่า $x^k \equiv a \pmod{m}$ มีผลเฉลย ก็ต่อเมื่อ $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ เมื่อ $d = (m, \phi(m))$ และถ้าสมภาค $x^k \equiv a \pmod{m}$ มีผลเฉลยแล้ว จะมีจำนวนผลเฉลยเท่ากับ d ผลเฉลย

การพิสูจน์ ($\Rightarrow$) ให้ r เป็นรากปฐมฐานมอดุโล m จากทฤษฎีบท 8.2.1 ข้อ 3.
จะได้ว่า สมภาค $k \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\phi(m)}$ ซึ่งมีตัวไม่ทราบค่า คือ $\operatorname{ind} x$
ดังนั้นโดยวิธีการหาผลเฉลยของสมภาคเชิงเส้น จะหาผลเฉลยได้ ก็ต่อเมื่อ $d \mid \operatorname{ind} a$
เมื่อ $d = (m, \phi(m))$ และจะมีผลเฉลยที่แตกต่างกัน d ผลเฉลย
ดังนั้นสรุปได้ว่า $x^k \equiv a \pmod{m}$ จะมีผลเฉลยก็ต่อเมื่อ $d \mid \operatorname{ind} a$
และถ้ามีผลเฉลยแล้วจะมี d ผลเฉลย
($\Leftarrow$) พิจารณา $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ เมื่อ $d = (m, \phi(m))$ จากทฤษฎีบท 8.2.1 ข้อ 1.
สมภาคนี้จะสมมูลกับ $\dfrac{\phi(m)}{d} \operatorname{ind} a \equiv 0 \pmod{m}$ สมภาคนี้จะเป็นจริง ก็ต่อเมื่อ $d \mid \operatorname{ind} a$
นั่นคือ $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ ก็ต่อเมื่อ $d \mid \operatorname{ind} a$ □

ตัวอย่าง 8.2.5

จากตัวอย่าง 8.2.4 จงหาผลเฉลยของ $4x^8 \equiv 25 \pmod{27}$ มีผลเฉลยหรือไม่ และถ้ามีจะมีกี่ผลเฉลย

วิธีทำ $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$ ดังนั้น $(\phi(m), n) = (18, 8) = 2$
นั่นคือ มีผลเฉลย 2 ผลเฉลย

8.3 กฎภาวะส่วนกลับกำลังสอง

ในหัวข้อนี้เราจะกล่าวถึงผลงานอีกชิ้นหนึ่งของเกาส์ ที่รู้จักกันในชื่อของ กฎภาวะส่วนกลับกำลังสอง (Quadratic Reciprocity Law) ซึ่งเป็นประโยชน์มากในการพิจารณาว่าสมภาคในรูป

$$x^2 \equiv a \pmod{p} \tag{8.3}$$

จะมีผลเฉลยหรือไม่ เมื่อ p เป็นจำนวนเฉพาะ

กฎภาวะส่วนกลับกำลังสองดังกล่าว คือ ถ้า p และ q เป็นจำนวนเฉพาะคี่ที่ต่างกันแล้ว จะได้ว่า $x^2 \equiv p \pmod{q}$ และ $x^2 \equiv q \pmod{p}$ จะมีผลเฉลยทั้งคู่ หรือ ไม่มีผลเฉลยทั้งคู่ ยกเว้นเมื่อทั้ง $p \equiv 3 \pmod{4}$ และ $q \equiv 3 \pmod{4}$ ซึ่งในกรณีนี้จะได้ว่า ถ้าสมภาคกำลังสองอันใดอันหนึ่งมีผลเฉลย แล้วอีกอันหนึ่งจะไม่มีผลเฉลย ประโยชน์ของทฤษฎีนี้เห็นได้จากการที่จะดูว่า

$$x^2 \equiv 5 \pmod{103} \tag{8.4}$$

จะมีผลเฉลยหรือไม่ โดยการดูว่า

$$x^2 \equiv 103 \pmod{5} \tag{8.5}$$

มีผลเฉลยหรือไม่แทน และเราสามารถพิจารณาได้โดยง่ายว่าสมการ 8.5 ไม่มีผลเฉลย เพราะกำลังสองในมอดุโล 5 มีแต่ 1 กับ 4 เท่านั้น ดังนั้นสรุปได้ว่าสมการ 8.4 ไม่มีผลเฉลยด้วย

8.3.1 สมภาคกำลังสอง

ในหัวข้อนี้ เราจะมาพิจารณาหาผลเฉลยของสมภาคกำลังสองในมอดุโล p เมื่อ p เป็นจำนวนเฉพาะ ซึ่งอยู่ในรูป

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{8.6}$$

โดยที่ $p \nmid a$

ถ้า $p = 2$ เราพิจารณาได้โดยง่ายว่าสมการ 8.6 มีผลเฉลยหรือไม่ โดยการพิจารณาว่า $x = 0$ หรือ $x = 1$ เป็นผลเฉลยหรือไม่ ดังนั้น เราจะพิจารณาสมการ 8.6 โดยที่ p เป็นจำนวนคี่ ซึ่งทำให้ได้ว่า $p \nmid 4a$ และ $4a\,(ax^2 + bx + c) = (2ax + b)^2 + 4ac - b^2$

ให้ $y = 2ax + b$ และ $d = b^2 - 4ac$ พิจารณา

$$y^2 \equiv d \pmod{p} \tag{8.7}$$

จะได้ว่า จำนวนเต็ม u เป็นผลเฉลยของสมการ 8.6 ก็ต่อเมื่อ $v \equiv 2au + b \pmod{p}$ เป็นผลเฉลยของสมการ 8.7 เนื่องจาก $(p, 2a) = 1$ ดังนั้น แต่ละ v ที่เป็นผลเฉลยของสมการ 8.7 จะมี u เพียงตัวเดียวมอดุโล p ที่ $v \equiv 2au + b \pmod{p}$ และผลเฉลย v ที่ไม่สมภาคกันมอดุโล p ของสมการ 8.7 จะได้ผลเฉลย u ที่ไม่สมภาคกันมอดุโล p ของสมการ 8.6

นั่นคือ เราลดทอนการหาผลเฉลยของสมภาคกำลังสองทั่ว ๆ ไป เป็นการหาผลเฉลยของสมภาคกำลังสองในรูป 8.7 ซึ่งถ้า p เป็นจำนวนเฉพาะที่มีค่าไม่มากนัก เราก็แทนค่า y ด้วย $0, 1, 2, \ldots, (p-1)/2$ ว่าค่าใดบ้างเป็นผลเฉลยของสมการ 8.7 และถ้า y เป็นผลเฉลยแล้ว $-y$ ก็เป็นผลเฉลยด้วย และถ้า $y \neq 0$ ทั้งสองค่านี้จะไม่สมภาคกันมอดุโล p ดังนั้นสรุปได้ว่าสมการ 8.7 ไม่มีผลเฉลยหรือมีผลเฉลยสองค่ามอดุโล p

ตัวอย่าง 8.3.1

จงลดทอนสมภาคต่อไปนี้ให้อยู่ในรูป $y^2 \equiv d \pmod{p}$ และพิจารณาว่ามีผลเฉลยหรือไม่
(ก) $3x^2 - x + 5 \equiv 0 \pmod{7}$
(ข) $x^2 - x + 1 \equiv 0 \pmod{5}$

วิธีทำ (ก) $12\,(3x^2 - x + 5) = 36x^2 - 12x + 60 = (6x - 1)^2 + 59$
ดังนั้น สมภาคที่กำหนดให้จะลดทอนเป็น $y^2 \equiv -59 \equiv 4 \pmod{7}$
ซึ่งได้ว่า $y \equiv 2 \pmod{7}$ และ $y \equiv -2 \pmod{7}$ เป็นผลเฉลย
ดังนั้น ผลเฉลยของสมภาคในข้อ (ก) คือผลเฉลยของ $6x - 1 \equiv 2 \pmod{7}$
หรือของ $6x - 1 \equiv -2 \pmod{7}$
ซึ่งก็คือ $x \equiv 4 \pmod{7}$ หรือ $x \equiv 1 \pmod{7}$ ตามลำดับ

(ข) $4\,(x^2 - x + 1) = (2x - 1)^2 + 3$
ดังนั้น สมภาคในข้อ (ข) ลดทอนเป็น $y^2 \equiv -3 \equiv 2 \pmod{5}$
ซึ่งไม่มีผลเฉลย ทำให้ $x^2 - x + 1 \equiv 0 \pmod{5}$ ไม่มีผลเฉลย

8.3.2 สัญลักษณ์เลอจองด์

ในหัวข้อนี้จะกล่าวถึงนิยาม และทฤษฎีบทที่เกี่ยวข้องกับสัญลักษณ์เลอจองด์ รวมไปถึงตัวอย่างที่จะทำให้เข้าใจมากขึ้น โดยเริ่มจากส่วนตกค้างกำลังสอง ดังนี้

บทนิยาม 8.3.1

ให้ m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม ที่ $(a, m) = 1$ เราจะกล่าวว่า a เป็น**ส่วนตกค้างกำลังสอง** (quadratic residue) มอดุโล m ก็ต่อเมื่อ $x^2 \equiv a \pmod{m}$ มีผลเฉลย แต่ถ้า $x^2 \equiv a \pmod{m}$ ไม่มีผลเฉลย เรากล่าวว่า a **ไม่เป็นส่วนตกค้างกำลังสอง** (quadratic nonresidue) มอดุโล m

ข้อสังเกต (1) ถ้า $a \equiv b \pmod{m}$ จะได้ว่า a เป็นส่วนตกค้างกำลังสองมอดุโล m ก็ต่อเมื่อ b เป็นส่วนตกค้างกำลังสองมอดุโล m ดังนั้น เราพิจารณาเฉพาะจำนวนเต็มบวกที่น้อยกว่า m

(2) ถ้า a เป็นรากปฐมฐานของ m จะได้ว่า ส่วนตกค้างกำลังสองมอดุโล m ทั้งหมด คือ จำนวนเต็ม ที่สมภาคกับ a^k เมื่อ k เป็นจำนวนเต็ม ที่ $1 \leq k \leq \phi(m)$ และ k เป็นจำนวนคู่

ตัวอย่าง 8.3.2

จงหาส่วนตกค้างกำลังสองมอดุโล 11 ทั้งหมด

วิธีทำ พิจารณากำลังสองทั้งหมดของจำนวนเต็ม $1, 2, 3, \ldots, 10$ มอดุโล 11

$$\begin{aligned} 1^2 &\equiv 10^2 \equiv 1 \pmod{11}, \\ 2^2 &\equiv 9^2 \equiv 4 \pmod{11}, \\ 3^2 &\equiv 8^2 \equiv 9 \pmod{11}, \\ 4^2 &\equiv 7^2 \equiv 5 \pmod{11}, \\ 5^2 &\equiv 6^2 \equiv 3 \pmod{11} \end{aligned}$$

ดังนั้น ส่วนตกค้างกำลังสองมอดุโล 11 ทั้งหมดคือ $1, 3, 4, 5$ และ 9

เราอาจจะพิจารณาได้อีกวิธีหนึ่งจากข้อสังเกต (2) เนื่องจาก 2 เป็นรากปฐมฐานของ 11

ดังนั้น ส่วนตกค้างกำลังสองมอดุโล 11 ทั้งหมดคือ

$$\begin{aligned} 2^2 &\equiv 4 \pmod{11}, \quad 2^4 \equiv 5 \pmod{11} \\ 2^6 &\equiv 9 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11} \end{aligned}$$

จากตัวอย่าง 8.3.2 จะเห็นได้ว่ามีส่วนตกค้างกำลังสองมอดุโล 11 อยู่จำนวน $\dfrac{11-1}{2} = 5$ ตัว ซึ่งเป็นจริงโดยทั่วไป

ทฤษฎีบท 8.3.1

ถ้า p เป็นจำนวนเฉพาะคี่แล้ว จะมีส่วนตกค้างกำลังสองมอดุโล p อยู่จำนวน $\dfrac{p-1}{2}$ ตัว

การพิสูจน์ เราจะหาส่วนตกค้างกำลังสองมอดุโล p ทั้งหมดจากจำนวนเต็มบวกที่น้อยกว่า p
ที่สมภาคกับ $1^2, 2^2, \ldots, (p-1)^2$ ซึ่งมีอยู่ทั้งหมด $p-1$ ตัว
แต่สำหรับแต่ละค่าของ a ที่ $1 \leq a \leq p-1$, $a^2 \equiv (p-a)^2 \pmod{p}$
และไม่มีตัวอื่นในบรรดา $1, 2, \ldots, p-1$ นอกจาก $p-a$ ที่มีกำลังสองสมภาคกับ a^2 มอดุโล p
ดังนั้น มีส่วนตกค้างกำลังสองอยู่ $\dfrac{p-1}{2}$ ตัว
และที่เหลือ $p-1-\dfrac{p-1}{2} = \dfrac{p-1}{2}$ ตัว ไม่เป็นส่วนตกค้างกำลังสอง □

บทนิยาม 8.3.2

ให้ p เป็นจำนวนเฉพาะคี่ และ a เป็นจำนวนเต็ม ที่ $p \nmid a$ **สัญลักษณ์เลอจองด์** (Legengre symbol) (a/p) จะกำหนดค่าได้ดังนี้

$$(a/p) = \begin{cases} 1 & \text{เมื่อ } a \text{ เป็นส่วนตกค้างกำลังสองมอดุโล } p \\ -1 & \text{เมื่อ } a \text{ ไม่เป็นส่วนตกค้างกำลังสองมอดุโล } p \end{cases}$$

หมายเหตุ สัญลักษณ์เลอจองด์ อาจเขียนได้อีกแบบหนึ่งคือ $\left(\frac{a}{p}\right)$

ตัวอย่าง 8.3.3

จากตัวอย่าง 8.3.2 เราได้ว่า

$$(1/11) = (3/11) = (4/11) = (5/11) = (9/11) = 1$$
$$\text{และ } (2/11) = (6/11) = (7/11) = (8/11) = (10/11) = -1$$

ทฤษฎีบท 8.3.2 : เกณฑ์ของออยเลอร์ (Euler's Criterion)

ถ้า p เป็นจำนวนเฉพาะที่เป็นคี่ และ a เป็นจำนวนเต็ม ที่ $p \nmid a$ แล้ว $(a/p) \equiv a^{(p-1)/2} \pmod{p}$

การพิสูจน์ เนื่องจาก p มีรากปฐมฐาน

ดังนั้นโดยทฤษฎีบท 4.3.1 $x^2 \equiv a \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $a^{(p-1)/2} \equiv 1 \pmod{p}$

นั่นคือ $(a/p) = 1$ ก็ต่อเมื่อ $a^{(p-1)/2} \equiv 1 \pmod{p}$

เนื่องจาก $p \nmid a$ ดังนั้น โดยทฤษฎีบทของแฟร์มาต์ (ทฤษฎีบท 2.4.4)

$a^{(p-1)/2}$ เป็นผลเฉลยของ $x^2 \equiv 1 \pmod{p}$ และโดยทฤษฎีบท 2.4.6

ได้ว่า $a^{(p-1)/2} \equiv 1$ หรือ $-1 \pmod{p}$ อย่างใดอย่างหนึ่งเพียงอย่างเดียว

ถ้า $a^{(p-1)/2} \equiv 1 \pmod{p}$ จะได้ $(a/p) = 1$ ทำให้ได้ว่า $(a/p) \equiv a^{(p-1)/2} \pmod{p}$

ถ้า $a^{(p-1)/2} \equiv -1 \pmod{p}$ จะได้ $(a/p) \neq 1$ นั่นคือ $(a/p) = -1 \equiv a^{(p-1)/2} \pmod{p}$

สรุปได้ว่า $(a/p) \equiv a^{(p-1)/2} \pmod{p}$ ตามต้องการ □

ตัวอย่าง 8.3.4

จงแสดงว่า 2 เป็นส่วนตกค้างกำลังสองมอดุโล 17

วิธีทำ เนื่องจาก $(2/17) \equiv 2^{16/2} = 2^8 \equiv 1 \pmod{17}$ และ $(2/17) = 1$ หรือ -1

ดังนั้นจึงสรุปได้ว่า $(2/17) = 1$ นั่นคือ 2 เป็นส่วนตกค้างกำลังสองมอดุโล 17

ทฤษฎีบท 8.3.3

ให้ p เป็นจำนวนเฉพาะคี่ และ a, b เป็นจำนวนเต็ม ที่ $p \nmid a$ และ $p \nmid b$ จะได้ว่า

(ก) $a \equiv b \pmod{p} \rightarrow (a/p) = (b/p)$

(ข) $(ab/p) = (a/p)(b/p)$

(ค) $(a^2/p) = 1$

การพิสูจน์ (ก) เห็นได้ชัดจากบทนิยามของ (a/b)

(ข) โดยทฤษฎีบท 8.3.2 $(ab/p) \equiv (ab)^{(p-1)/2} \pmod{p}$

ดังนั้น $(ab/p) \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \pmod{p}$

$\equiv (a/p)(b/p) \pmod{p}$

แต่เนื่องจากทั้งสองข้างมีค่าเป็น 1 หรือ -1 และ p เป็นจำนวนคี่

ดังนั้น $(ab/p) = (a/p)(b/p)$

(ค) $(a^2/p) = (a/p)^2 = 1^2$ หรือ $(-1)^2 = 1$ □

ทฤษฎีบท 8.3.4

ให้ p เป็นจำนวนเฉพาะคี่ จะได้ว่า $(-1/p) = (-1)^{(p-1)/2}$ นั่นคือ

$$(-1/p) = \begin{cases} 1 \text{ เมื่อ } p \equiv 1 \pmod{4} \\ -1 \text{ เมื่อ } p \equiv 3 \pmod{4} \end{cases}$$

การพิสูจน์ โดยทฤษฎีบท 8.3.2 จะได้ว่า $(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$

แต่เนื่องจากทั้งสองข้างมีค่าเป็น 1 หรือ -1 และ p เป็นจำนวนคี่

ดังนั้น $(-1/p) = (-1)^{(p-1)/2}$ □

ตัวอย่าง 8.3.5

$(-1/101) = 1$ เพราะว่า $101 \equiv 1 \pmod{4}$

$(-1/11) = 1$ เพราะว่า $11 \equiv 3 \pmod{4}$

ตัวอย่าง 8.3.6

จงพิจารณาว่า $x^2 \equiv 8 (\mathrm{mod} 17)$ มีผลเฉลยหรือไม่

วิธีทำ เนื่องจาก $8 \equiv -9 \pmod{17}$ ดังนั้น $(8/17) = (-9/17) = (-1/17)(9/17)$

แต่ $(9/17) = (3^2/17) = 1$ และ $(-1/17) = 1$ เพราะว่า $17 \equiv 1 \pmod{4}$

ดังนั้น $(8/17) = 1 \cdot 1 = 1$ นั่นคือ $x^2 \equiv 8 \pmod{17}$ มีผลเฉลย

ทฤษฎีบท 8.3.5 : บทแทรกของเกาส์ (Gauss's lemma)

ให้ p เป็นจำนวนเฉพาะคี่ และ a เป็นจำนวนเต็ม ที่ $p \nmid a$ สำหรับแต่ละค่า $i \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$

ให้ r_i เป็นจำนวนเต็มบวก ซึ่ง $r_i \leq p-1$ และ $r_i \equiv ia \pmod{p}$ ให้ $\mu_p(a) =$ จำนวนของ r_i ที่ $r_i > \frac{p}{2}$ จะได้ว่า $(a/p) = (-1)^{\mu_p(a)}$

การพิสูจน์ ให้ i และ j เป็นสมาชิกใด ๆ ที่ต่างกันในเซต $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$

จะได้ว่า $-p < i - j < p$ และ $0 < i + j < p$ ดังนั้น $p \nmid (i-j)a$ และ $p \nmid (i+j)a$

นั่นคือ $r_i \not\equiv r_j \pmod{p}$ และ $r_i \not\equiv -r_j \pmod{p}$

ให้ $I = \left\{ i \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \;\middle|\; r_i > \frac{p}{2} \right\}$ ดังนั้น จำนวนสมาชิกของ I คือ $\mu_p(a)$

และถ้า $i \in I$, $\quad 0 < p - r_i \leq \frac{p-1}{2}$

จะได้ว่า $\{r_i \mid i \notin I\} \cup \{p - r_i \mid i \in I\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$
และ $\{r_i \mid i \notin I\} \cap \{p - r_i \mid i \in I\} = \varnothing$ ทำให้ได้ว่า

$$\begin{aligned} a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a &\equiv r_1 r_2 \cdots r_{(p-1)/2} \pmod{p} \\ &\equiv (-1)^{\mu_p(a)} \cdot \prod_{i \in I} (p - r_i) \cdot \prod_{i \notin I} r_i \pmod{p} \\ &\equiv (-1)^{\mu_p(a)} \cdot 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right) \pmod{p} \end{aligned}$$

นั่นคือ $\left(\frac{p-1}{2}\right)! a^{(p-1)/2} \equiv (-1)^{\mu_p(a)} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$
แต่เนื่องจาก $p \nmid \left(\frac{p-1}{2}\right)!$ จึงได้ว่า $a^{(p-1)/2} \equiv (-1)^{\mu_p(a)} \pmod{p}$
และโดยทฤษฎีบท 8.3.2 (เกณฑ์ของออยเลอร์) จะได้ว่า $(a/p) \equiv (-1)^{\mu_p(a)} \pmod{p}$
เนื่องจากทั้งสองข้างมีค่าเป็น 1 หรือ -1 และ p เป็นจำนวนคี่
ดังนั้น $(a/p) = (-1)^{\mu_p(a)}$ ตามต้องการ □

ตัวอย่าง 8.3.7

จงหาค่า $(3/13)$

วิธีทำ $a = 3, p = 13$ และ $\frac{p-1}{2} = 6$
เนื่องจาก $a = 3, 2a = 6, 3a = 9, 4a = 12, 5a = 15$ และ $6a = 18$
ดังนั้น $r_1 = 3, r_2 = 6, r_3 = 9, r_4 = 12, r_5 = 3$ และ $r_6 = 5$
เพราะฉะนั้น $\mu_{13}(3) = 2$ และ $(3/13) = (-1)^{\mu_{13}(3)} = (-1)^2 = 1$

ทฤษฎีบท 8.3.6

สำหรับจำนวนเฉพาะคี่ p, $(2/p) = (-1)^{(p^2-1)/8}$ นั่นคือ

$$(2/p) = \begin{cases} 1 \text{ เมื่อ } p \equiv 1 \text{ หรือ } 7 \pmod{8} \\ -1 \text{ เมื่อ } p \equiv 3 \text{ หรือ } 5 \pmod{8} \end{cases}$$

การพิสูจน์ จะใช้ทฤษฎีบท 8.3.5
สำหรับ $1 \le i \le \frac{p-1}{4}$ เราได้ว่า $1 \le 2i \le \frac{p-1}{2}$
และ $\frac{p-1}{4} < i \le \frac{p-1}{2}$ เราได้ว่า $\frac{p-1}{2} < 2i \le p-1$
ในกรณีนี้ $r_i = 2i$ และ $\mu_p(2) = \frac{p-1}{2} - \frac{p-1}{4}$
เมื่อ $[x]$ หมายถึงจำนวนเต็ม ค่ามากสุดที่ไม่เกิน x

กรณี 1 $p \equiv 1 \pmod{8}$
ดังนั้น มีจำนวนเต็ม e ที่ $p = 8c + 1$ และ $\frac{p^2-1}{8} = 8e^2 + 2e$ เป็นจำนวนคู่
และ $\mu_p(2) = 8e/2 - [8e/4] = 4e - 2e = 2e$ ทำให้ $(2/p) = (-1)^{2e} = 1$

กรณี 2 $p \equiv 7 \pmod 8$

ดังนั้น มีจำนวนเต็ม e ที่ $p = 8e+7$ และ $\dfrac{p^2-1}{8} = 8e^2+14e+6$ เป็นจำนวนคู่

และ $\mu_p(2) = (8e+6)/2 - [(8e+6)/4] = (4e+3) - (2e+1) = 2e+2$

ทำให้ $(2/p) = (-1)^{2e+2} = 1$

กรณี 3 $p \equiv 3 \pmod 8$

ดังนั้น มีจำนวนเต็ม e ที่ $p = 8e+3$ และ $\dfrac{p^2-1}{8} = 8e^2+6e+1$ เป็นจำนวนคี่

และ $\mu_p(2) = (8e+2)/2 - [(8e+2)/4] = (4e+1) - (2e) = 2e+1$

ทำให้ $(2/p) = (-1)^{2e+1} = -1$

กรณี 4 $p \equiv 5 \pmod 8$

ดังนั้น มีจำนวนเต็ม e ที่ $p = 8e+5$ และ $\dfrac{p^2-1}{8} = 8e^2+10e+3$ เป็นจำนวนคี่

และ $\mu_p(2) = (8e+4)/2 - [(8e+4)/4] = (4e+2) - (2e+1) = 2e+1$

ทำให้ $(2/p) = (-1)^{2e+1} = -1$

เพราะฉะนั้น $(2/p) = \begin{cases} 1 \text{ เมื่อ } p \equiv 1 \text{ หรือ } 7 \pmod 8 \\ -1 \text{ เมื่อ } p \equiv 3 \text{ หรือ } 5 \pmod 8 \end{cases}$

$= (-1)^{(p^2-1)/8}$ □

ตัวอย่าง 8.3.8

จากทฤษฎีบท 8.3.6 ได้ว่า

$(2/17) = (2/31) = (2/103) = 1$ เพราะว่า $17 \equiv 1, 31 \equiv 7$ และ $103 \equiv 7 \pmod 8$

และ $(2/101) = (2/19) = (2/29) = -1$ เพราะว่า $101 \equiv 5, 19 \equiv 3$ และ $29 \equiv 5 \pmod 8$

ตัวอย่าง 8.3.9

จงหาค่า $(17/19)$

วิธีทำ เนื่องจาก $17 \equiv -2 \pmod{19}$

ดังนั้น โดยทฤษฎีบท 8.3.3 ได้ว่า $(17/19) = (-2/19) = (-1/19)(2/19)$

และเนื่องจาก $19 \equiv 3 \pmod 4$ และ $19 \equiv 3 \pmod 8$

ดังนั้น $(-1/19) = -1$ และ $(2/19) = -1$

ทำให้ $(17/19) = (-1)(-1) = 1$

8.3.3 กฎภาวะส่วนกลับกำลังสอง

ในหัวข้อนี้เราจะพิสูจน์กฎภาวะส่วนกลับกำลังสองที่กล่าวไว้ในตอนต้นของบทนี้

ทฤษฎีบท 8.3.7

ให้ p เป็นจำนวนเฉพาะคี่ และ a เป็นจำนวนเต็มคี่ที่ $p \nmid a$ จะได้ว่า

$$\mu_p(a) \equiv \sum_{i=1}^{(p-1)/2} [ia/p] \pmod 2$$

การพิสูจน์ ให้ I และ r_i เหมือนกับที่กำหนดให้ในบทพิสูจน์ของทฤษฎีบท 8.3.5

ดังนั้น สำหรับแต่ละ $i \in \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$, $ia = [ia/p]p + r_i$

จากบทพิสูจน์ของทฤษฎีบท 8.3.5 ได้ว่า

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} i &= \sum_{i\in I}(p - r_i) + \sum_{i\notin I} r_i \\ &= \sum_{i\in I} p - \sum_{i\in I} r_i + \sum_{i\notin I} r_i \\ &= p\mu_p(a) + 2\sum_{i\notin I} r_i - \sum_{i=1}^{(p-1)/2} r_i\end{aligned}$$

นั่นคือ $$\sum_{i=1}^{(p-1)/2} r_i = p\mu_p(a) + 2\sum_{i\notin I} r_i - \sum_{i=1}^{(p-1)/2} i$$

ดังนั้น $$\begin{aligned}a\sum_{i=1}^{(p-1)/2} i &= \sum_{i=1}^{(p-1)/2} ia = \sum_{i=1}^{(p-1)/2} [ia/p]p + \sum_{i=1}^{(p-1)/2} r_i \\ &= p\sum_{i=1}^{(p-1)/2} [ia/p] + p\mu_p(a) + 2\sum_{i\notin I} r_i - \sum_{i=1}^{(p-1)/2} i\end{aligned}$$

ทำให้ $$(a+1)\sum_{i=1}^{(p-1)/2} i = p\sum_{i=1}^{(p-1)/2} [ia/p] + p\mu_p(a) + 2\sum_{i\notin I} r_i$$

แต่เนื่องจาก a และ p เป็นจำนวนคี่ เราจึงได้ว่า

$$\mu_p(a) \equiv \sum_{i=1}^{(p-1)/2} [ia/p] \pmod 2$$

□

ทฤษฎีบท 8.3.8 : กฎภาวะส่วนกลับกำลังสอง (The Quadratic Reciprocal Law)

ให้ p และ q เป็นจำนวนเฉพาะคี่ที่ต่างกัน จะได้ว่า

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

การพิสูจน์ ให้ $S = \left\{(i,j) \in \mathbb{Z}\times\mathbb{Z} \mid 1 \le i \le \dfrac{p-1}{2} \text{ และ } 1 \le j \le \dfrac{q-1}{2}\right\}$

จะได้ว่า $|\,S\,| = \left(\dfrac{p-1}{2}\right)\left(\dfrac{q-1}{2}\right)$

ให้ $S_1 = \{(i,j) \in S \mid qi > pj\}$ และ $S_2 = \{(i,j) \in S \mid qi < pj\}$

เนื่องจาก p และ q เป็นจำนวนเฉพาะคี่ที่ต่างกัน

ดังนั้น ไม่มีจุด (i,j) ที่อยู่บนเส้นตรง $qx = py$

ทำให้ได้ว่า $S = S_1 \cup S_2$

เนื่องจาก $S_1 \cap S_2 = \varnothing$ ดังนั้น $|\,S\,| = |\,S_1\,| + |\,S_2\,|$

สำหรับแต่ละ i ที่ $1 \le i \le \dfrac{p-1}{2}$

จำนวนของจำนวนเต็ม j ที่ $1 \le j \le qi/p$ จะเป็น $[qi/p]$

ดังนั้น $$|S_1| = \sum_{i=1}^{(p-1)/2} [qi/p]$$

ในทำนองเดียวกัน $|S_2| = \sum_{j=1}^{(p-1)/2} [pj/q]$

เพราะฉะนั้น $$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = |S| = |S_1| + |S_2|$$
$$= \sum_{i=1}^{(p-1)/2} [qi/p] + \sum_{j=1}^{(p-1)/2} [pj/q]$$

โดยทฤษฎีบท 8.3.7 เราได้ว่า

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \equiv \mu_p(q) + \mu_q(p) \pmod 2$$

ซึ่งทำให้ได้ว่า $(p/q)(q/p) = (-1)^{\mu_p(q)}(-1)^{\mu_q(p)}$
$= (-1)^{\mu_p(q)+\mu_q(p)}$
$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ ตามต้องการ □

ข้อสังเกต จากทฤษฎีบท 8.3.8 จะเห็นว่า
(1) ถ้า $p \equiv 1 \pmod 4$ หรือ $q \equiv 1 \pmod 4$ แล้ว จะได้ว่า $(p/q) = (q/p)$
(2) ถ้า $p \equiv 3 \pmod 4$ หรือ $q \equiv 3 \pmod 4$ แล้ว จะได้ว่า $(p/q) = -(q/p)$

ตัวอย่าง 8.3.10

จงหาค่า $(78/101)$

วิธีทำ
$(78/101) = (2/101)(39/101)$ เพราะว่า $78 = 2 \cdot 39$
$= (-1)(101/39)$ เพราะว่า $101 \equiv 5 \pmod 8$ และ $101 \equiv 1 \pmod 4$
$= (-1)(23/39)$ เพราะว่า $101 \equiv 23 \pmod{39}$
$= (-1)(-1)(39/23)$ เพราะว่า $23 \equiv 3 \pmod 4$ และ $39 \equiv 3 \pmod 4$
$= (16/23)$ เพราะว่า $39 \equiv 16 \pmod{23}$
$= 1$ เพราะว่า $16 = 4^2$

ตัวอย่าง 8.3.11

จงหาจำนวนเฉพาะคี่ p ทั้งหมดที่ 3 เป็นส่วนตกค้างกำลังสองมอดุโล p

วิธีทำ เนื่องจาก

$$(3/p) = \begin{cases} (p/3) \text{ ถ้า } p \equiv 1 \pmod 4 \\ -(p/3) \text{ ถ้า } p \equiv 3 \equiv -1 \pmod 4 \end{cases}$$

และ $(p/3) = \begin{cases} 1 \text{ ถ้า } p \equiv 1 \pmod 3 \\ -1 \text{ ถ้า } p \equiv 2 \equiv -1 \pmod 3 \end{cases}$

ดังนั้น $(3/p) = 1$ ก็ต่อเมื่อ $(p \equiv 1 \pmod 4$ และ $p \equiv 1 \pmod 3)$
หรือ $(p \equiv -1 \pmod 4$ และ $p \equiv -1 \pmod 3)$

แต่ ($p \equiv 1 \pmod 4$ และ $p \equiv 1 \pmod 3$) ก็ต่อเมื่อ $p \equiv 1 \pmod{12}$
และ $p \equiv -1 \pmod 4$ และ $p \equiv -1 \pmod 3$ ก็ต่อเมื่อ $p \equiv -1 \pmod{12}$
เพราะฉะนั้น $(3/p) = 1$ ก็ต่อเมื่อ $p \equiv 1$ หรือ $-1 \pmod{12}$
นั่นคือ 3 เป็นส่วนตกค้างกำลังสองมอดุโล p ก็ต่อเมื่อ $p \equiv 1$ หรือ $-1 \pmod{12}$

หรือ $(3/p) = \begin{cases} 1 \text{ เมื่อ } p \equiv 1 \text{ หรือ } -1 \pmod{12} \\ -1 \text{ เมื่อ } p \equiv 5 \text{ หรือ } -5 \pmod{12} \end{cases}$

ตัวอย่าง 8.3.12

จงหาค่า $(6/p)$

วิธีทำ เนื่องจาก $(6/p) = (2/p)(3/p)$
ดังนั้น $(6/p) = 1$ ก็ต่อเมื่อ $(2/p) = (3/p) = 1$ หรือ $(2/p) = (3/p) = -1$
แต่โดยทฤษฎีบท 8.3.6 และตัวอย่าง 8.3.11

$$\begin{aligned}
(2/p) = 1 \text{ และ } (3/p) = 1 \quad &\text{ก็ต่อเมื่อ} \quad (p \equiv 1 \text{ หรือ } -1 \pmod 8) \text{ และ} \\
&\quad\ (p \equiv 1 \text{ หรือ } -1 \pmod{12}) \\
&\text{ก็ต่อเมื่อ} \quad (p \equiv 1 \pmod 8 \text{ และ } p \equiv 1 \pmod{12}) \text{ หรือ} \\
&\quad\ (p \equiv -1 \pmod 8 \text{ และ } p \equiv -1 \pmod{12}) \\
&\text{ก็ต่อเมื่อ} \quad p \equiv 1 \pmod{24} \text{ และ } p \equiv -1 \pmod{24} \\
\text{และ } (2/p) = -1 \text{ และ } (3/p) = -1 \quad &\text{ก็ต่อเมื่อ} \quad (p \equiv 3 \equiv -5 \text{ หรือ } -3 \equiv 5 \pmod 8) \text{ และ} \\
&\quad\ (p \equiv 5 \text{ หรือ } -5 \pmod{12}) \\
&\text{ก็ต่อเมื่อ} \quad (p \equiv 5 \pmod 8 \text{ และ } p \equiv 5 \pmod{12}) \text{ หรือ} \\
&\quad\ (p \equiv -5 \pmod 8 \text{ และ } p \equiv -5 \pmod{12}) \\
&\text{ก็ต่อเมื่อ} \quad p \equiv 5 \pmod{24} \text{ และ } p \equiv -5 \pmod{24}
\end{aligned}$$

เพราะฉะนั้น $(6/p) = 1$ ก็ต่อเมื่อ $p \equiv 1$ หรือ -1 หรือ 5 หรือ $-5 \pmod{24}$
หรือเขียนได้เป็น

$$(6/p) = \begin{cases} 1 \text{ เมื่อ } p \equiv 1 \text{ หรือ } -1 \text{ หรือ } 5 \text{ หรือ } -5 \pmod{24} \\ -1 \text{ เมื่อ } p \equiv 7 \text{ หรือ } -7 \text{ หรือ } 11 \text{ หรือ } -11 \pmod{24} \end{cases}$$

ในบทที่ 3 เราได้พิสูจน์แล้วว่า มีจำนวนเฉพาะ ที่อยู่ในรูป $4k+3$ อยู่เป็นจำนวนอนันต์ ต่อไปเราจะใช้สัญลักษณ์เลอจองด์พิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 8.3.9

มีจำนวนเฉพาะ ที่อยู่ในรูป $4k+1$ อยู่เป็นจำนวนอนันต์

การพิสูจน์ สมมติว่าไม่จริง
นั่นคือ สมมติว่ามีจำนวนเฉพาะ ที่อยู่ในรูป $4k+1$ อยู่ n ตัว ให้เป็น $p_1, p_2, \ldots, p_n$
ให้ $N = (2p_1p_2 \cdots p_n)^2 + 1$
ดังนั้น $N > 1$ และเป็นจำนวนคี่ ทำให้ได้ว่า มีจำนวนเฉพาะคี่ p ที่ $p \mid N$

นั่นคือ $(2p_1p_2\cdots p_n)^2 \equiv -1 \pmod{p}$
ซึ่งทำให้ $(-1/p) = 1$
โดยทฤษฎีบท 8.3.4 ได้ว่า $p \equiv 1 \pmod{4}$
นั่นคือ มีจำนวนเต็ม k ที่ทำให้ $p = 4k+1$ ดังนั้น $p = p_i$ สำหรับบางค่าของ i
เนื่องจาก $p \mid N$ ดังนั้น $p \mid \left(N - (2p_1p_2\cdots p_n)^2\right)$
นั่นคือ $p \mid 1$ ซึ่งเป็นไปไม่ได้
สรุปได้ว่า มีจำนวนเฉพาะ ที่อยู่ในรูป $4k+1$ อยู่เป็นจำนวนอนันต์ □

ทฤษฎีบท 8.3.10

มีจำนวนเฉพาะ ที่อยู่ในรูป $8k-1$ อยู่เป็นจำนวนอนันต์

การพิสูจน์ สมมติว่ามีจำนวนเฉพาะ ที่อยู่ในรูป $8k-1$ อยู่ n ตัว ให้เป็น $p_1, p_2, \ldots, p_n$
ให้ $N = (4p_1p_2\cdots p_n)^2 - 2$
ดังนั้น $N > 2$ และ ไม่เป็นกำลังของ 2 ทำให้มีจำนวนเฉพาะคี่ที่หาร N ลงตัว ให้เป็น p
และได้ว่า $(4p_1p_2\cdots p_n)^2 \equiv 2 \pmod{p}$
นั่นคือ $(2/p) = 1$
เพราะฉะนั้น $p \equiv 1$ หรือ $-1 \pmod{8}$
เนื่องจากผลคูณของจำนวนเต็ม ที่อยู่ในรูป $8k+1$ จะอยู่ในรูปเดียวกัน
และเนื่องจาก N เป็นจำนวนคู่
ดังนั้นถ้าจำนวนเฉพาะคี่ทุกตัวที่หาร N ลงตัว อยู่ในรูป $8k+1$ แล้ว
จะได้ว่า $N = 16e+2$ สำหรับจำนวนเต็ม e บางค่า
แต่ $N = 16m-2$ สำหรับบางค่าของจำนวนเต็ม m เราจึงได้ข้อขัดแย้งกัน
เพราะฉะนั้น จะมีจำนวนเฉพาะคี่ q ที่ $q \mid N$ และ q อยู่ในรูป $8k-1$
ดังนั้น $q = p_i$ สำหรับบางค่าของ i และ $q \mid (4p_1p_2\cdots p_n)^2$
ทำให้ได้ว่า $q \mid (4p_1p_2\cdots p_n)^2$
นั่นคือ $q \mid 2$ ซึ่งเป็นไปไม่ได้เพราะ q เป็นจำนวนคี่
สรุปได้ว่า มีจำนวนเฉพาะ ที่อยู่ในรูป $8k-1$ อยู่เป็นอนันต์ □

ทฤษฎีบท 8.3.11

ถ้า p และ $2p+1$ เป็นจำนวนเฉพาะคี่ทั้งคู่ จะได้ว่า $(-1)^{(p-1)/2}2$ เป็นรากปฐมฐานของ $2p+1$

การพิสูจน์ ให้ $q = 2p+1$
เนื่องจาก $\phi(q) = q-1 = 2p$ ดังนั้น อันดับของ 2 มอดุโล q จะเป็น 2, p หรือ $2p$

กรณี 1 $p \equiv 1 \pmod{4}$
ทำให้ได้ว่า $(-1)^{(p-1)/2}2 = 2$ และมีจำนวนเต็ม k ที่ $p = 4k+1$
ดังนั้น $q = 2(4k+1)+1 = 8k+3 \equiv 3 \pmod{8}$
โดยทฤษฎีบท 8.3.6 $(2/q) = -1$
แต่โดยทฤษฎีบท 8.3.2 $(2/q) \equiv 2^{(q-1)/2}2^p \pmod{q}$
เพราะฉะนั้น $2^p \equiv -1 \pmod{q}$ นั่นคือ อันดับของ 2 มอดุโล q ไม่เป็น p
นอกจากนี้ เนื่องจาก $q > 3$
ดังนั้น $2^2 \equiv 4 \not\equiv 1 \pmod{q}$

นั่นคือ อันดับของ 2 มอดุโล q ไม่เป็น 2
เราจึงได้ว่า อันดับของ 2 มอดุโล q เป็น $2p$
นั่นคือ 2 เป็นรากปฐมฐานมอดุโล q

กรณี 2 $2p \equiv 3 \pmod 4$
ทำให้ได้ว่า $(-1)^{(p-1)/2}2 = -2$ และมีจำนวนเต็ม k ที่ $p = 4k+3$
ดังนั้น $q = 2p+1 = 2(4k+3)+1 = 8k+7 \equiv -1 \pmod 8$
เพราะฉะนั้น $(-2/q) = (-1/q)(2/q) = (-1)(1) = -1$
แต่โดยทฤษฎีบท 8.3.2 $(-2/q) \equiv (-2)^{(q-1)/2} = (-2)^p \pmod q$
นั่นคือ $(-2)^p \equiv -1 \pmod q$
ต่อจากนี้ พิสูจน์ทำนองเดียวกันกับกรณี 1
เราจะสรุปได้ว่า -2 เป็นรากปฐมฐาน มอดุโล q □

ตัวอย่าง 8.3.13

(ก) $p = 29$ และ $q = 2p+1 = 59$ เป็นจำนวนเฉพาะ
เพราะฉะนั้น $(-1)^{(29-1)/2}2 = -2$ เป็นรากปฐมฐาน มอดุโล 59
(ข) $p = 83$ และ $q = 2p+1 = 167$ เป็นจำนวนเฉพาะ
เพราะฉะนั้น $(-1)^{(s3-1)/2}2 = -2$ เป็นรากปฐมฐานมอดุโล 167

ต่อไปเป็นการประยุกต์สัญลักษณ์เลอจองด์กับทฤษฎีบท 4.3.2 ในบทที่ 4 ในการพิจารณาว่าสมภาคกำลังสองที่มีมอดุลัสเป็นจำนวนเฉพาะคี่ยกกำลัง มีผลเฉลยหรือไม่

จากทฤษฎีบท 4.3.2 เมื่อ $k = 2, n$ เป็นจำนวนเต็มบวกใด ๆ และ a เป็นจำนวนเต็ม ที่ $p \nmid a$

$$x^2 \equiv a \pmod{p^n} \text{ มีผลเฉลยก็ต่อเมื่อ } x^2 \equiv a \pmod p \text{ มีผลเฉลย}$$

ทฤษฎีบท 8.3.12

ให้ p เป็นจำนวนเฉพาะคี่ a เป็นจำนวนเต็ม ที่ $p \nmid a$ จะได้ว่าสำหรับทุก ๆ จำนวนเต็มบวก n

$$x^2 \equiv a \pmod{p^n} \text{ มีผลเฉลยก็ต่อเมื่อ } (a/p) = 1$$

ตัวอย่าง 8.3.14

จงพิจารณาว่า สมภาคกำลังสองต่อไปนี้มีผลเฉลยหรือไม่
(ก) $x^2 \equiv -1 \pmod{25}$
(ข) $x^2 \equiv 7 \pmod{121}$

วิธีทำ (ก) เนื่องจาก $(-1/5) = 1$ ดังนั้น โดยทฤษฎีบท 8.3.12 $x^2 \equiv -1 \pmod{25}$ มีผลเฉลย
(ข) เนื่องจาก $(7/11) = -(11/7) = -(4/7) = -1$ ดังนั้น $x^2 \equiv 7 \pmod{121}$ ไม่มีผลเฉลย

นอกจากนี้เรายังสามารถพิจารณาสมภาคกำลังสองที่มีมอดุลัสอยู่ในรูป $p_1p_2 \dots p_n$ เมื่อ p_i เป็นจำนวนเฉพาะที่ต่างกัน

ตัวอย่าง 8.3.15

จงพิจารณาว่าสมการกำลังสอง $x^2 \equiv 248 \pmod{1357}$ มีผลเฉลยหรือไม่

วิธีทำ เนื่องจาก $1357 = 23 \cdot 59$

$$\begin{aligned}
\text{และ } (248/23) &= (18/23) && \text{เพราะว่า } 248 \equiv 18 \pmod{23} \\
&= (9/23)(2/23) \\
&= (2/23) && \text{เพราะว่า } (9/23) = (3/23)^2 = 1 \\
&= 1 && \text{เพราะว่า } 23 \equiv -1 \pmod{8} \\
\text{และ } (248/59) &= (12/59) && \text{เพราะว่า } 248 \equiv 12 \pmod{59} \\
&= (4/59)(3/59) \\
&= (3/59) && \text{เพราะว่า } (4/59) = (2/59)^2 = 1 \\
&= -(59/3) && \text{เพราะว่า } 59 \equiv 3 \pmod{4} \\
&= -(2/3) && \text{เพราะว่า } 59 \equiv 2 \pmod{3} \\
&= -(-1) && \text{เพราะว่า } 3 \equiv 3 \pmod{8} \\
&= 1
\end{aligned}$$

ดังนั้น $x^2 \equiv 248 \pmod{23}$ และ $x^2 \equiv 248 \pmod{59}$
มีผลเฉลยทั้งคู่ ให้เป็น x_1 และ x_2 ตามลำดับ
โดยทฤษฎีบทเศษเหลือของจีน (ทฤษฎีบท 2.3.1) จะมี x_0 เพียงตัวเดียวมอดุโล 1357 ที่

$$x_0 \equiv x_1 \pmod{23} \text{ และ } x_0 \equiv x_2 \pmod{59}$$

เพราะฉะนั้น $x_0^2 \equiv x_1^2 \equiv 248 \pmod{23}$ และ $x_0^2 \equiv x_2^2 \equiv 248 \pmod{59}$
เนื่องจาก $(23, 59) = 1$ ดังนั้น $x_0^2 \equiv 248 \pmod{1357}$
นั่นคือ สมภาคกำลังสองที่กำหนดให้มีผลเฉลย

หมายเหตุ ถ้ามี p_i ที่ $x^2 \equiv a \pmod{p_i}$ ไม่มีผลเฉลย จะสรุปได้ว่า $x^2 \equiv a \pmod{p_1 p_2 \cdots p_n}$ ไม่มีผลเฉลย

ในหัวข้อ 4.1 เรากล่าวถึงการทดสอบการเป็นจำนวนเฉพาะของจำนวนเมอร์เสนน์ ในตอนนี้ เราจะปิดท้ายหัวข้อนี้ด้วยการกล่าวถึง การทดสอบการเป็นจำนวนเฉพาะของจำนวนแฟร์มาต์ $F_n = 2^{2^n} + 1$

ทฤษฎีบท 8.3.13

ให้ $n \geq 2$ และ $F_n = 2^{2^n} + 1$ จะได้ว่า ถ้า q เป็นจำนวนเฉพาะ ที่ $q \mid F_n$ แล้วจะมีจำนวนเต็มบวก k ที่ $q = 2^{n+1}k + 1$

การพิสูจน์ ให้ q เป็นจำนวนเฉพาะ ที่ $q \mid F_n$ นั่นคือ $q \mid \left(2^{2^n} + 1\right)$ ดังนั้น $2^{2^n} \equiv -1 \pmod{q}$
เนื่องจาก $n \geq 2$ ดังนั้น $4 \mid 2^n$ ละทำให้ได้ว่า สมภาค $x^4 \equiv -1 \pmod{q}$ มีผลเฉลย
ดังนั้น โดยทฤษฎีบท 4.3.1 จะได้ว่า $(-1)^{\frac{q-1}{(4,q-1)}} \equiv 1 \pmod{q}$
ทำให้ได้ว่า $(q-1) \mid (4, q-1)$ เป็นจำนวนคู่ ให้ $d = (4, q-1)$ เนื่องจาก q เป็นจำนวนคี่
ดังนั้น $d = 2$ หรือ 4 ถ้า $d = 2$ จะทำให้ได้ว่า $q = 2r + 1$ โดยที่ r เป็นจำนวนคี่
ซึ่งทำให้ $(q-1)/(4, q-1) = 2r/2 = r$ เป็นจำนวนคี่ ซึ่งเป็นข้อขัดแย้ง ดังนั้น $d = 4$
จึงได้ว่า $4 \mid (q-1)$ และ $(q-1)/4$ เป็นจำนวนคู่ นั่นคือ $q \equiv 1 \pmod{8}$
โดยทฤษฎีบท 8.3.6 $(2/q) = 1$ ดังนั้น จะมีจำนวนเต็ม s ที่ $s^2 \equiv 2 \pmod{q}$

ทำให้ $s^{2^{n+1}} = (s^2)^{2^n} \equiv 2^{2^n} \equiv -1 \pmod{q}$
โดยทฤษฎีบท 4.3.1 $(-1)^{\frac{q-1}{(q-1,2^{n+1})}} \equiv 1 \pmod{q}$
เนื่องจาก q เป็นจำนวนเฉพาะคี่ ดังนั้น $(-1)^{\frac{q-1}{(q-1,2^{n+1})}} = 1$ นั่นคือ $\dfrac{q-1}{(q-1,2^{n+1})}$ เป็นจำนวนคู่
จาก $q \mid \left(2^{2^n}+1\right)$ จะได้ว่า $2^{2^n} \equiv -1 \pmod{q}$ ทำให้ได้ว่า $2^{2^{n+1}} \equiv 1 \pmod{q}$
ดังนั้น อันดับของ 2 มอดุโล q คือ 2^{n+1} แต่โดยทฤษฎีบทของแฟร์มาต์ (ทฤษฎีบท 2.4.4)
ได้ว่า $2^{q-1} \equiv 1 \pmod{q}$ ทำให้ได้โดยทฤษฎีบท 4.1.1 ว่า $2^{n+1} \mid (q-1)$
ดังนั้น $(q-1, 2^{n+1}) = 2^{n+1}$ ทำให้ $(q-1)/2^{n+1}$ เป็นจำนวนคู่ นั่นคือ $2^{n+1} \mid (q-1)$
ดังนั้น จะมีจำนวนเต็ม k ที่ $q = 2^{n+1}k+1$ ตามต้องการ □

เราสามารถใช้ทฤษฎีบท 8.3.13 ร่วมกับทฤษฎีบท 1.5.3 ทดสอบว่า F_n เป็นจำนวนเฉพาะ โดยการพิจารณาว่า จำนวนเฉพาะ q ที่ $q < \sqrt{F_n}$ และ q อยู่ในรูป $2^{n+1}k+1$ ทุกตัวว่า $q \nmid F_n$

ตัวอย่าง 8.3.16

จงพิจารณาว่า $F_4 = 2^{2^4}+1 = 65537$ เป็นจำนวนเฉพาะหรือไม่

วิธีทำ ให้ $a_k = 2^6k+1 = 64k+1$ ค่า a_k ที่ทำให้ $a_k < \sqrt{F_4} = \sqrt{65537} < 257$
คือ $a_1 = 65,\ a_2 = 129, a_3 = 193$
จะเห็นว่า มีเฉพาะ $a_3 = 193$ เท่านั้น ที่เป็นจำนวนเฉพาะ และ $193 \nmid 65537$
สรุปได้ว่า $F_4 = 65537$ เป็นจำนวนเฉพาะ

ทฤษฎีบท 8.3.14 : การทดสอบของเปอแปง (Pepin's Test)

สำหรับจำนวนเต็ม $n \geq 1$, F_n เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

การพิสูจน์ ($\Rightarrow$) สมมติ $F_n = 2^{2^n} = (2)^{2^{n-1}}$ เป็นจำนวนเฉพาะ
เนื่องจาก $n \geq 1$ ดังนั้น $F_n \equiv 1 \pmod{4}$ และเนื่องจาก $2^2 = 4 \equiv 1 \pmod{3}$
ดังนั้น $2^{2^n} = (2)^{2^{n-1}} \equiv 1 \pmod{3}$ ทำให้ $F_n = 2^{2^n}+1 \equiv 2 \pmod{3}$
ดังนั้น โดยทฤษฎีบท 5.3.2 $(3/F_n) = (F_n/3) = (2/3) = -1$
และโดยบทแทรกของเกาส์ จึงได้ว่า $-1 = (3/F_n) \equiv 3^{\frac{F_n-1}{2}} \pmod{F_n}$
($\Leftarrow$) สมมติว่า $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ ดังนั้น $3^{F_n-1} \equiv 1 \pmod{F_n}$ และ $(3, F_n) = 1$
ให้ p เป็นจำนวนเฉพาะที่ $p \mid F_n$
ดังนั้น $(3,p) = 1, 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{p}$ และ $3^{F_n-1} \equiv 1 \pmod{p}$
นั่นคือ อันดับของ 3 มอดุโล p คือ $F_n - 1$
โดยทฤษฎีบทของแฟร์มาต์และทฤษฎีบท 4.1.1 จะได้ว่า $(F_n-1) \mid (p-1)$
ทำให้ได้ว่า $F_n \leq p$ แต่เนื่องจาก $p \mid F_n$ เราจึงได้ด้วยว่า $p \leq F_n$
ดังนั้น $F_n = p$ เป็นจำนวนเฉพาะ □

ตัวอย่าง 8.3.17

จงใช้ทฤษฎีบท 8.3.14 แสดงว่า $F_3 = 2^{2^3}+1 = 2^8+1 = 257$ เป็นจำนวนเฉพาะ

วิธีทำ จาก $\dfrac{F_3-1}{2}=128$ และ $3^3=81\cdot 3=243\equiv -14\,(\mathrm{mod}\ 257)$

$$\begin{aligned}
3^{10}&\equiv(-14)^2=196\equiv -61\,(\mathrm{mod}\ 257)\\
3^{20}&\equiv(-61)(-61)=3721\equiv 123\,(\mathrm{mod}\ 257)\\
3^{40}&\equiv 123\cdot 123=15129\equiv 223\equiv -34\,(\mathrm{mod}\ 257)\\
3^{50}&\equiv(-34)(-34)=1156\equiv 128\,(\mathrm{mod}\ 257)\\
3^{120}&\equiv(-34)(128)=-4352\equiv -240\equiv 17\,(\mathrm{mod}\ 257)\\
3^{125}&=3^3\cdot 3^{120}\cdot 3^5\equiv 27\cdot 17\cdot(-14)=-6426\equiv -1\,(\mathrm{mod}\ 257)
\end{aligned}$$

เราจึงได้ว่า $3^{\frac{F_3-1}{2}}\equiv -1\ (\mathrm{mod}\ F_3)$ ดังนั้น โดยทฤษฎีบท 8.3.14 จึงได้ว่า F_3 เป็นจำนวนเฉพาะ

8.3.4 สัญลักษณ์ยาโคบี

ในหัวข้อนี้ เราจะขยายสัญลักษณ์เลอจองด์เป็นสัญลักษณ์ยาโคบี ดังนี้

บทนิยาม 8.3.3

ให้ n เป็นจำนวนบวกคี่ซึ่ง $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ เมื่อ p_i เป็นจำนวนเฉพาะคี่ที่ต่างกัน ให้ a เป็นจำนวนเต็ม ที่ $(a,n)=1$ **สัญลักษณ์ยาโคบี** (Jacobi symbol) กำหนดโดย

$$[a/n]=(a/p_1)^{k_1}\,(a/p_2)^{k_2}\cdots(a/p_r)^{k_r}$$

ตัวอย่าง 8.3.18

$[2/15]=(2/3)(2/5)=(-1)(-1)=1$
$[-1/12]=(-1/2)^2(-1/3)=(1)(-1)=-1$

ข้อสังเกต จากบทนิยาม 8.3.3 จะเห็นว่า ถ้า $n=p$ เป็นจำนวนเฉพาะ แล้ว $[a/p]=(a/p)$

จากบทนิยามของสัญลักษณ์เลอจองด์ เราได้ว่า สำหรับจำนวนเต็ม a ที่ $p\nmid a$

$$x^2\equiv a\,(\mathrm{mod}\ p)\text{ มีผลเฉลยก็ต่อเมื่อ }(a/p)=1$$

แต่สำหรับสัญลักษณ์ยาโคบี จะได้ว่า

ทฤษฎีบท 8.3.15

สำหรับจำนวนเต็ม a และ n ที่ n เป็นบวก และ $(a,n)=1$ ถ้า $x^2\equiv a\,(\mathrm{mod}\ n)$ มีผลเฉลยแล้ว $[a/n]=1$

การพิสูจน์ สมมติว่า $x^2\equiv a\,(\mathrm{mod}\ n)$ มีผลเฉลยจะได้ว่า สำหรับทุก ๆ จำนวนเฉพาะ p ที่ $p\mid n$
$x^2\equiv a\,(\mathrm{mod}\ p)$ มีผลเฉลยด้วย ทำให้ $(a,p)=1$ ดังนั้น $[a/n]=1$ ด้วย □

ส่วนกลับของทฤษฎีบท 8.3.15 ไม่เป็นจริงเสมอไป เช่น $[2/9]=(2/3)^2=1$ แต่ $x^2\equiv 2\,(\mathrm{mod}\ 9)$ ไม่มีผลเฉลย

ทฤษฎีบท 8.3.15 ใช้ประโยชน์ในการแสดงว่า สมภาค $x^2\equiv a\,(\mathrm{mod}\ n)$ ไม่มีผลเฉลย

ตัวอย่าง 8.3.19

จงพิจารณาว่า สมภาค $x^2 \equiv 2 \pmod{507}$ มีผลเฉลยหรือไม่

วิธีทำ เนื่องจาก $507 = 3 \cdot 13^2$ ดังนั้น $[2/507] = (2/3)(2/13)^2 = (-1)(-1)^2 = 1$
โดยทฤษฎีบท 8.3.15 จะได้ว่า $x^2 \equiv 2 \pmod{507}$ ไม่มีผลเฉลย

สัญลักษณ์ยาโคบีจะมีสมบัติเหมือนกับสมบัติต่อไปนี้ของสัญลักษณ์เลอจองด์

ทฤษฎีบท 8.3.16

ให้ n และ m เป็นจำนวนเต็มบวกคี่ a และ b เป็นจำนวนเต็ม ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ n และ m ทั้งคู่ จะได้ว่า
(ก) ถ้า $a \equiv b \pmod{n}$ แล้ว $[a/n] = [b/n]$
(ข) $[ab/n] = [a/n][b/n]$
(ค) $[a/nm] = [a/n][a/m]$

การพิสูจน์ (ก) สมมติว่า $a \equiv b \pmod{n}$ และให้ p เป็นจำนวนเฉพาะใด ๆ ที่ $p \mid n$
จะได้ว่า $a \equiv b \pmod{p}$ ดังนั้น $(a/p) = (b/p)$
เพราะฉะนั้น ทุก ๆ จำนวนเฉพาะ p ที่ $p \mid n, (a/p) = (b/p)$ ทำให้ได้ว่า $[a/n] = [b/n]$
(ข) และ (ค) ได้จากบทนิยามและทฤษฎีบท 8.3.3 □

ตัวอย่าง 8.3.20

จงพิจารณาว่า $x^2 \equiv 6 \pmod{35}$ มีผลเฉลยหรือไม่

วิธีทำ เนื่องจาก
$$\begin{aligned}[6/35] &= [2/35][3/35] \\ &= (2/5)(2/7)(3/5)(3/7) \\ &= (-1)(1)(5/3)(-1)(7/3) \\ &= (2/3)(1/3) \\ &= (-1)(1) \\ &= -1\end{aligned}$$
เพราะฉะนั้น $x^2 \equiv 6 \pmod{35}$ ไม่มีผลเฉลย

หมายเหตุ ในกรณีที่ $[a/n] = 1$ จะสรุปไม่ได้ว่า $x^2 \equiv a \pmod{n}$ มีผลเฉลยหรือไม่

ทฤษฎีบท 8.3.17

กำหนดให้ a และ b เป็นจำนวนเต็มคี่ จะได้ว่า
(ก) $\dfrac{ab-1}{2} = \dfrac{a-1}{2} + \dfrac{b-1}{2} \pmod{2}$
(ข) $\dfrac{a^2b^2-1}{8} = \dfrac{a^2-1}{8} + \dfrac{b^2-1}{8} \pmod{2}$

การพิสูจน์ (ก) เนื่องจาก a และ b เป็นจำนวนเต็มคี่ ดังนั้น $(a-1)(b-1) \equiv 0 \pmod{4}$
แต่ $(ab-1) - (a-1) - (b-1) = (a-1)(b-1)$

เพราะฉะนั้น $(ab-1) \equiv (a-1)+(b-1) \pmod 4$
แต่ $ab-1, a-1$ และ $b-1$ ทุกตัวเป็นจำนวนคู่
ดังนั้น จะได้ว่า $\dfrac{ab-1}{2} = \dfrac{a-1}{2} + \dfrac{b-1}{2} \pmod 2$ ตามต้องการ

(ข) เนื่องจาก ถ้า c เป็นจำนวนเต็มคี่แล้ว $8 \mid (c^2-1)$
ดังนั้น a^2b^2-1, a^2-1 และ b^2-1 ทุกตัวหารด้วย 8 ลงตัว
จึงได้ว่า $\dfrac{a^2b^2-1}{8} - \dfrac{a^2-1}{8} - \dfrac{b^2-1}{8} = \dfrac{(a^2-1)(b^2-1)}{8}$
แต่ $\dfrac{(a^2-1)(b^2-1)}{8}$ ยังหารด้วย 8 ลงตัว
ดังนั้น $\dfrac{a^2b^2-1}{8} = \dfrac{a^2-1}{8} + \dfrac{b^2-1}{8} \pmod 2$ □

ทฤษฎีบท 8.3.18

ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มคี่ จะได้ว่า

(ก) $\dfrac{a_1a_2\cdots a_n-1}{2} \equiv \dfrac{a_1-1}{2} + \dfrac{a_2-1}{2} + \cdots + \dfrac{a_n-1}{2} \pmod 2$

(ข) $\dfrac{a_1^2a_2^2\ldots a_n^2-1}{8} \equiv \dfrac{a_1^2-1}{8} + \dfrac{a_2^2-1}{8} + \cdots + \dfrac{a_n^2-1}{8} \pmod 2$

การพิสูจน์ โดยทฤษฎีบท 8.3.17 และหลักอุปนัยเชิงคณิตศาสตร์ □

ทฤษฎีบท 8.3.19

ให้ n เป็นจำนวนเต็มคี่ จะได้ว่า

(ก) $[-1/n] = (-1)^{\frac{n-1}{2}}$

(ข) $[2/n] = (-1)^{\frac{n^2-1}{8}}$

(ค) $[m/n][n/m] = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ เมื่อ m และ n เป็นจำนวนเต็มคี่ ที่ $(m,n)=1$

การพิสูจน์ ให้ $n = p_1p_2\ldots p_r$ เป็นผลคูณของจำนวนเฉพาะ p_i (ไม่จำเป็นต้องต่างกัน)
เนื่องจาก n เป็นจำนวนคี่ ดังนั้น ทุก ๆ p_i เป็นจำนวนเฉพาะคี่

(ก)
$$\begin{aligned}
[-1/n] &= (-1/p_1)(-1/p_2)\cdots(-1/p_r) && \text{โดยบทนิยาม}\\
&= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_r-1}{2}} && \text{โดยทฤษฎีบท 8.3.4}\\
&= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_r-1}{2}} &&\\
&= (-1)^{\frac{p_1p_2\cdots p_r-1}{2}} && \text{โดยทฤษฎีบท 8.3.18 (ก)}\\
&= (-1)^{\frac{n-1}{2}} &&
\end{aligned}$$

(ข)
$$\begin{aligned}
[2/n] &= (2/p_1)(2/p_2)\cdots(2/p_r) && \text{โดยบทนิยาม}\\
&= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_r^2-1}{8}} && \text{โดยทฤษฎีบท 8.3.6}\\
&= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_r^2-1}{8}} &&\\
&= (-1)^{\frac{p_1^2p_2^2\cdots p_r^2-1}{8}} && \text{โดยทฤษฎีบท 8.3.18 (ข)}\\
&= (-1)^{\frac{n^2-1}{8}} &&
\end{aligned}$$

(ค) ให้ $m = q_1 q_2 \cdots q_s$ เป็นผลคูณของจำนวนเฉพาะ q_j (ไม่จำเป็นต้องต่างกัน)
เนื่องจาก $(m,n) = 1$ ดังนั้น แต่ละ q_j ต่างกับ p_i ทุกตัว เพราะฉะนั้น

$$\begin{aligned}
[m/n] &= \prod_{i=1}^{r}\prod_{j=1}^{s}(q_j/p_i) && \text{โดยบทนิยามและทฤษฎีบท 8.3.16 (ค)}\\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\left(\frac{q_j-1}{2}\right)\left(\frac{p_i-1}{2}\right)}(p_i/q_j) && \text{โดยทฤษฎีบท 8.3.8}\\
&= \left(\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\left(\frac{q_j-1}{2}\right)\left(\frac{p_i-1}{2}\right)}\right)[n/m]\\
&= (-1)^e[n/m]
\end{aligned}$$

เมื่อ $e = \sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right)\left(\frac{p_i-1}{2}\right)$
ต่อไปจะพิสูจน์ว่า $e \equiv \left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right) \pmod 2$
เนื่องจาก $e = \sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right)\left(\frac{p_i-1}{2}\right)$

$$= \sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right)$$

และ $\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right) \equiv \left(\frac{p_1p_2\ldots p_r-1}{2}\right)\left(\frac{q_1q_2\ldots q_s-1}{2}\right) \pmod 2$
ดังนั้น $e \equiv \left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right) \pmod 2$
เพราะฉะนั้น $[m/n] = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}[n/m]$ ตามต้องการ □

ตัวอย่าง 8.3.21

จงหาค่า $[111/1001]$

วิธีทำ เนื่องจาก $1001 \equiv 1 \pmod 4$ ดังนั้น $[111/1001] = [1001/111]$
แต่ $1001 \equiv 2 \pmod{111}$ และ $111 \equiv -1 \pmod 8$
ดังนั้น โดยทฤษฎีบท 8.3.19 (ก) และทฤษฎีบท 8.3.19 (ข) จะได้ว่า $[1001/111] = [2/111] = 1$

ทฤษฎีบท 8.3.20

ให้ a เป็นจำนวนเต็มที่ $a > 1$ จะได้ว่า ถ้าไม่มีจำนวนเต็ม $k > 1$ ที่ $a = k^2$ แล้ว จะมีจำนวนเฉพาะ p อยู่เป็นจำนวนอนันต์ ที่ a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล p

การพิสูจน์ สมมติว่า ไม่มีจำนวนเต็ม $k > 1$ ที่ $a = k^2$ จะมีจำนวนเต็ม b และ c ที่ $a = b^2c$ โดยที่ $c > 1$ และไม่มีตัวประกอบที่เป็นกำลังสองนอกเหนือจาก 1
สำหรับทุก ๆ จำนวนเฉพาะ p ที่ $p \nmid a$, $\quad (a/p) = (b^2/p)\,(c/p) = (c/p)$
ซึ่งทำให้ได้ว่า a เป็นส่วนตกค้างกำลังสองมอดุโล p ก็ต่อเมื่อ c ส่วนตกค้างกำลังสองมอดุโล p
ดังนั้น ในกรณีนี้ เราพิจารณา c แทน a ได้

เราจึงสมมติให้ a เป็นจำนวนเต็มที่ไม่มีตัวประกอบที่เป็นกำลังสองนอกเหนือจาก 1
เราจะพิสูจน์ว่า สำหรับจำนวนเฉพาะ $q_1, q_2, \ldots, q_n$ ใด ๆ ที่ $q_i \nmid a$
และ a ไม่เป็นส่วนตกค้าง กำลังสองมอดุโล q_i จะมีจำนวนเฉพาะคี่ q ที่ต่างจาก $q_1, q_2, \ldots, q_n$
และ a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล q

กรณี 1 $a \neq \pm 2$

เพราะฉะนั้น $a \neq \pm 2^e p_1 p_2 \cdots p_r$ โดยที่ $c = 0$ หรือ $1, r \geq 1$
และ p_i เป็นจำนวนเฉพาะคี่ที่ต่างกัน
ให้ t เป็นจำนวนเต็ม ที่ไม่เป็นส่วนตกค้างกำลังสองมอดุโล p_r
โดยทฤษฎีบท 2.3.1 (ทฤษฎีเศษเหลือของจีน) จะมีจำนวนเต็ม b_1 ที่

$$\begin{aligned} b_1 &\equiv 1 \pmod{q_i} \quad i = 1, 2, \ldots, n \\ b_1 &\equiv 1 \pmod{8} \\ b_1 &\equiv 1 \pmod{p_j} \quad j = 1, 2, \ldots, r-1 \\ b_1 &\equiv t \pmod{p_r} \end{aligned}$$

เนื่องจาก $b_1 \equiv 1 \pmod{8}$ ดังนั้น สำหรับทุก ๆ $j \in \{1, 2, \ldots, r\}$

$$[p_j/b_1] = [b_1/p_j] = (b_1/p_j) \text{ และ } [-1/b_1] = 1 = [2/b_1]$$

เนื่องจาก $b_1 \equiv 1 \pmod{p_j}$ เมื่อ $j = 1, 2, \ldots r-1$ และ $b_1 \equiv t \pmod{p_r}$
ดังนั้น $(b_1/p_j) = (1/p_j) = 1$ เมื่อ $j = 1, 2, \ldots r-1$ และ $(b_1/p_r) = (t/p_r) = -1$
เพราะฉะนั้น เราได้ว่า

$$\begin{aligned} [a/b_1] &= [p_1/b_1]\,[p_2/b_1] \cdots [p_r/b_1] \\ &= [b_1/p_1]\,[b_1/p_2] \cdots [b_1/p_r] \\ &= (b_1/p_1)\,(b_1/p_2) \cdots (b_1/p_r) \\ &= -1 \end{aligned}$$

ทำให้ได้ว่า จะมีจำนวนเฉพาะคี่ q ที่ $q \mid b_1$ และ $(a/q) = -1$
เนื่องจาก $b_1 \equiv 1 \pmod{q_i}$ และ $q \mid b_1$
ดังนั้น $q \notin \{q_1, q_2, \ldots, q_n\}$ และ a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล q ตามต้องการ

กรณี 2 $a = 2$

โดยทฤษฎีบท 2.3.1 (ทฤษฎีเศษเหลือของจีน) จะมีจำนวนเต็ม b_2 ที่

$$\begin{aligned} b_2 &\equiv 1 \pmod{q_i}, \ i = 1, 2, \ldots, n \\ b_2 &\equiv 3 \pmod{8} \end{aligned}$$

ดังนั้น $[2/b_2] = -1$ ทำให้ได้ว่า จะมีจำนวนเฉพาะคี่ q ที่ $q \mid b_2$
และ $(2/q) = -1$ เนื่องจาก $b_2 \equiv 1 \pmod{q_i}$ ทุก i
ดังนั้น $q \notin \{q_1, q_2, \ldots, q_n\}$ และ $a = 2$ ไม่เป็นส่วนตกค้างกำลังสองมอดุโล

กรณี 3 $a = -2$

ไดยทฤษฎีบท 2.3.1 (ทฤษฎีเศษเหลือของจีน) จะมีจำนวนเต็ม b_3 ที่

$$\begin{aligned} b_3 &\equiv 1 \pmod{q_i}, \ i = 1, 2, \ldots, n \\ b_3 &\equiv -3 \pmod{8} \end{aligned}$$

เพราะฉะนั้น $b_3 \equiv -3 \equiv 1 \pmod 4$ และ $[2/b_3] = -1$
ซึ่งทำให้ $[-1/b_3] = 1$ และ $[-2/b_3] = [-1/b_3]\,[2/b_3] = -1$
ทำให้ได้ว่ามีจำนวนเฉพาะ q ที่ $q \mid b_3$ และ $[-2/q] = -1$
เนื่องจาก $b_3 \equiv 1 \pmod{q_i}$ ทุก i
ดังนั้น $q \notin \{q_1, q_2, \ldots, q_n\}$ และ $a = -2$ ไม่เป็นส่วนตกค้างกำลังสองมอดุโล d
จากทุกกรณี เราสรุปได้ว่า มีจำนวนเฉพาะ q ที่ a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล q
อยู่เป็นจำนวนอนันต์ □

สรุปท้ายบท

ในบทที่ 8 ได้กล่าวถึงการหาผลเฉลยของสมภาค ที่อยู่ในรูป $r^x \equiv a \pmod{m}$ เรียก r ว่ารากปฐมฐาน และเรียก x ว่า ดรรชนี โดยเริ่มต้นจากการหาอันดับของ r มอดุโล m และอาศัยรากปฐมฐาน r ในการหาดรรชนีที่มีสมบัติสำคัญเดียวกันกับลอการิทึม นอกจากนั้นยังได้กล่าวถึงกฎภาวะส่วนกลับกำลังสองและเรื่องอื่น ๆ ที่เกี่ยวข้อง ได้แก่ สมภาคกำลังสอง สัญลักษณ์เลอจองด์และสัญลักษณ์ยาโคบี

แบบฝึกหัดท้ายบทที่ 8

1. จงหาอันดับของจำนวนเต็ม 2, 3 และ 5

   (1.1) มอดุโล 17 (1.2) มอดุโล 19 (1.3) มอดุโล 23

2. จงพิสูจน์ข้อความต่อไปนี้

   (2.1) ถ้า $\operatorname{ord}_m a = hk$ แล้ว $\operatorname{ord}_m a^h = hk$

   (2.2) ถ้า p เป็นจำนวนเฉพาะคี่ และ $\operatorname{ord}_p a = 2k$ แล้ว $a^k \equiv -1 \pmod{p}$

   (2.3) ถ้า $\operatorname{ord}_m a = m - 1$ แล้ว n เป็นจำนวนเฉพาะ

3. ให้ $\operatorname{ord}_m a = h$ และ $\operatorname{ord}_m b = h$ จงแสดงว่า $\operatorname{ord}_m ab \mid hk$ และถ้า $(h, k) = 1$ แล้ว $\operatorname{ord}_m ab = hk$

4. จงแสดงว่า 2 เป็นรากปฐมฐานของ 19 แต่ไม่เป็นรากปฐมฐานของ 17

5. จงหารากปฐมฐานของ 11, 13 และ 19

6. จงแสดงว่า 15 ไม่มีรากปฐมฐาน

7. ถ้า a เป็นรากปฐมฐานของจำนวนเต็ม m จงพิสูจน์ว่าถ้า a^k เป็นรากปฐมฐานของ m ก็ต่อเมื่อ $(k, \phi(m)) = 1$

8. จงหาดรรชนีของ 5 เทียบกับแต่ละฐานที่เป็นรากปฐมฐานของ 13

9. ตารางต่อไปนี้แสดงดรรชนีของ a เทียบกับฐาน 3 ซึ่งเป็นรากปฐมฐานของ 17

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

   จงใช้ตารางดรรชนีดังกล่าวหาผลเฉลยของสมภาคต่อไปนี้

   (9.1) $x^2 \equiv 13 \pmod{17}$ (9.2) $8x^2 \equiv 10 \pmod{17}$ (9.3) $9x^2 \equiv 8 \pmod{17}$

10. จงหาดรรชนีของ a เทียบกับฐาน 2 ซึ่งเป็นรากปฐมฐานของ 11 แล้วเขียนลงในตาราง

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$										

11. จงตรวจสอบว่าสมภาคต่อไปนี้ มีผลเฉลยหรือไม่ ถ้ามีกี่ผลเฉลย

   (11.1) $7x^3 \equiv 3 \pmod{11}$ (11.2) $3x^4 \equiv 8 \pmod{11}$ (11.3) $x^8 \equiv 10 \pmod{11}$

12. ถ้า p เป็นจำนวนเฉพาะคี่แล้ว จงพิสูจน์ว่า

   (12.1) $x^2 \equiv -1 \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $p \equiv 1 \pmod{4}$

(12.2) $x^4 \equiv -1 \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $p \equiv 1 \pmod{8}$

13. ถ้า r เป็นรากปฐมฐานของจำนวนเฉพาะคี่ p จงแสดงว่า

$$\operatorname{ind}_r(-1) = \operatorname{ind}_r(p-1) = \frac{1}{2}(p-1)$$

14. จงพิจารณาว่า สมภาคกำลังสองต่อไปนี้ ข้อใดบ้างมีผลเฉลย และจงหาผลเฉลยที่ไม่สมภาคกันทั้งหมด

(14.1) $x^2 + 7x + 10 \equiv 0 \pmod{11}$

(14.2) $2x^2 + 10x - 11 \equiv 0 \pmod{13}$

(14.3) $5x^2 - 7x - 11 \equiv 0 \pmod{29}$

(14.4) $3x^2 + 7x - 21 \equiv 0 \pmod{23}$

15. จงพิสูจน์ว่า สมภาค $6x^2 + 5x + 1 \equiv 0 \pmod{p}$ มีผลเฉลยทุก ๆ จำนวนเฉพาะ p แต่สมการ $6x^2 + 5x + 1 = 0$ ไม่มีผลเฉลยที่เป็นจำนวนเต็ม

16. จงหาส่วนตกค้างกำลังสองมอดุโล 17 ทั้งหมด

17. กำหนดให้ 2 เป็นรากปฐมฐาน มอดุโล 29 จงหาจำนวนเต็ม a ที่ $0 \leq a < 29$ ทั้งหมด ที่ a เป็นส่วนตกค้างกำลังสองมอดุโล 29

18. ให้ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า

(18.1) $(1/p) + (2/p) + \cdots + ((p-1)/p) = 0$

(18.2) $(1 \cdot 2/p) + (2 \cdot 3/p) + \cdots + ((p-2)(p-1)/p) = -1$

19. จงใช้เกณฑ์ของออยเลอร์ (ทฤษฎีบท 8.3.2) พิสูจน์ว่า $1999 \mid (2^{099} - 1)$ เมื่อ 1999 เป็นจำนวนเฉพาะ

20. จงพิจารณาว่า $x^2 \equiv -2 \pmod{1999}$ มีผลเฉลยหรือไม่

21. จงใช้บทแทรกของเกาส์ (ทฤษฎีบท 5.2.2) หาค่า $(5/13)$

22. ให้ p เป็นจำนวนเฉพาะ ที่ $p \nmid a$ จงพิสูจน์ว่า

(22.1) จำนวนผลเฉลยที่ไม่สมภาคกันของ $x^2 \equiv b \pmod{p}$ คือ $1 + (b/p)$

(22.2) จำนวนผลเฉลยที่ไม่สมภาคกันของ $ax^2 + bx + c \equiv 0 \pmod{p}$ คือ $1 + ((b - 4ac)/p)$

23. ให้ p เป็นจำนวนเฉพาะ ที่ $p \equiv 1 \pmod{4}$ จงพิสูจน์ว่า

24. ให้ p เป็นจำนวนเฉพาะ ที่ $p \equiv 1 \pmod{4}$ จงพิสูจน์ว่า $(1/p) + (2/p) + \ldots + \left(\frac{p-1}{2}/p\right) = 0$

25. จงหาค่า $(-21/83), (69/73), (156/1009)$

26. จงพิจารณาว่า สมภาคกำลังสองต่อไปนี้ มีผลเฉลยหรือไม่

(26.1) $x^2 \equiv 73 \pmod{173}$

(26.2) $x^2 \equiv 31 \pmod{103}$

(26.3) $x^2 \equiv 5 \pmod{227}$

(26.4) $x^2 \equiv -7 \pmod{227}$

27. จงพิจารณาว่า สมภาคกำลังสองต่อไปนี้ มีผลเฉลยหรือไม่

(27.1) $x^2 \equiv 2 \pmod{49}$

(27.2) $x^2 \equiv 5 \pmod{49}$

(27.3) $x^2 \equiv 11 \pmod{169}$

(27.4) $x^2 \equiv 13 \pmod{625}$

28. จงหาจำนวนเฉพาะ p ที่ $p \neq 7$ และทำให้ $7x^2 + 2x + 1 \equiv 0 \pmod{p}$ มีผลเฉลย

29. ให้ p $q = 2^p - 1$ เป็นจำนวนเฉพาะคี่ จงหา $(3/p)$

30. จงหาจำนวนเฉพาะ p ทั้งหมดที่ 7 เป็นส่วนตกค้างกำลังสองมอดุโล p

31. จงหาจำนวนเฉพาะ p ทั้งหมดที่ $(-5/p) = 1$

32. จงหาจำนวนเฉพาะ p ทั้งหมดที่ 10 เป็นส่วนตกค้างกำลังสอง มอดุโล p

33. กำหนดให้ว่า p และ $q = 4p + 1$ เป็นจำนวนเฉพาะทั้งคู่ จงพิสูจน์ว่า

(33.1) ถ้า a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล q แล้ว a เป็นรากปฐมฐานมอดุโล q หรือ อันดับของ a มอดุโล q เป็น 4

(33.2) 2 เป็นรากปฐมฐานมอดุโล q

34. จงพิสูจน์ว่า มีจำนวนเฉพาะ ที่อยู่ในรูป $8k + 3$ อยู่เป็นจำนวนอนันต์
(ข้อเสนอแนะ : พิจารณา $N = (p_1 p_2 \cdots p_r)^2 + 2$ เมื่อ p_i อยู่ในรูป $\delta k + 3$)

35. จงหาจำนวนผลเฉลยที่ไม่สมภาคกัน ของ $x^2 \equiv -3 \pmod{37^2}$

36. จงพิจารณาว่า สมภาค $x^2 \equiv 29 \pmod{65}$ มีผลเฉลยหรือไม่

37. ให้ p และ q เป็นจำนวนเฉพาะคี่ที่ต่างกัน ถ้าจำนวนเต็ม a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล p และ มอดุโล q a เป็นส่วนตกค้างกำลังสองมอดุโล pq หรือไม่

38. กำหนดให้ว่า 1997 เป็นจำนวนเฉพาะ จงพิจารณาว่า $x^4 \equiv 49 \pmod{1997}$ มีผลเฉลยหรือไม่

39. จงหาค่าของ $[5/21], [2663/3299]$

40. จงพิจารณา โดยใช้สัญลักษณ์ยาโคบีว่า สมภาคกำลังสองต่อไปนี้ มีผลเฉลยหรือไม่

(40.1) $x^2 \equiv 39 \pmod{77}$

(40.2) $x^2 \equiv 2 \pmod{35}$

41. ให้ p, q เป็นจำนวนเฉพาะ a เป็นจำนวนเต็ม ที่ $(a, pq) = 1$ จงพิสูจน์หรือยกตัวอย่างค้านข้อความต่อไปนี้

(41.1) ถ้า $x^2 \equiv a \pmod{pq}$ มีผลเฉลย แล้ว $x^2 \equiv a \pmod{p}$ มีผลเฉลย และ $x^2 \equiv a \pmod{q}$ มีผลเฉลย

(41.2) ถ้า $x^2 \equiv a \pmod{p}$ มีผลเฉลย และ $x^2 \equiv a \pmod{q}$ มีผลเฉลย แล้ว $x^2 \equiv a \pmod{pq}$ มีผลเฉลย

42. ถ้า p เป็นจำนวนเฉพาะ ที่ $p \equiv 1 \pmod{4}$ และมีจำนวนเต็มบวก a และ b ที่ a เป็นจำนวนคี่ และ $p = a^2 + b^2$ แล้ว $(a/p) = 1$

(ข้อเสนอแนะ : ใช้ทฤษฎีบท 8.3.19 (ค))

เอกสารอ้างอิง

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จิราภา ลิ้มบุพศิริพร. (2555). **ทฤษฎีจำนวน**. นครปฐม : โรงพิมพ์มหาวิทยาลัยศิลปากร.

มารศรี แนวจำปา. (2546). **ทฤษฎีจำนวน**. อุบลราชธานี : คณะวิทยาศาสตร์และเทคโนโลยี สถาบันราชภัฏอุบลราชธานี.

วรางคณา ร่องมะรุด. (2523). **เฉลยแบบฝึกหัดทฤษฎีจำนวน 2**. กรุงเทพฯ : ยูไนเต็ดโปรดักชั่น.

สมใจ จิตพิทักษ์. (2547). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 3)**. สงขลา : ภารกิจเอกสารและตำรามหาวิทยาลัยทักษิณ.

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน** (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม). กรุงเทพฯ : สถาบันราชภัฏพระนคร.

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

David M. Burton. (2007). **Elementary number theory (6 ed.)**. New York : The McGraw-HillCompanies, Inc.

Raji W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

Rosen K.H. (2005). **Elementary number theory and its applications (5 ed.)**. Boston : Pearson/Addison Wesley.

บรรณานุกรม

กัลยาณี ไชยวรินทรกุล. (2522). **ระบบจำนวน**. กรุงเทพฯ : โรงพิมพ์มหาวิทยาลัยรามคำแหง.

กิตติภูมิ บำรุงสงฆ์. (2519). **ทฤษฎีจำนวนเบื้องต้น**. นครราชสีมา : ภาควิชาคณิตศาสตร์ วิทยาลัยครูนครราชสีมา.

ขนิษฐา ชมภูวิเศษ. (2559). **ทฤษฎีจำนวน**. นครราชสีมา : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏนครราชสีมา.

คณะกรรมการกลุ่มผลิตชุดวิชาตรรกศาสตร์ เซตและทฤษฎีจำนวน. (2529). **เอกสารการสอนชุดวิชาตรรกศาสตร์ เซตและทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์ชวนพิมพ์. (ฝ่ายการพิมพ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช)

จรินทร์ทิพย์ เฮงคราวิทย์. (2558). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จารุวรรณ สิงห์ม่วง. (2011). **ทฤษฎีจำนวน : ราชินีแห่งคณิตศาสตร์**. Journal of Rajanagarindra. 8(19), 79-86

จารุวรรณ สิงห์ม่วง. (2562). **ทฤษฎีจำนวน**. กรุงเทพฯ : ทริปเปิ้ล เอ็ดดูเคชั่น.

จิราภา ลิ้มบุพศิริพร. (2555). **ทฤษฎีจำนวน**. นครปฐม : โรงพิมพ์มหาวิทยาลัยศิลปากร.

ฉวีวรรณ รัตนประเสริฐ. (2552). **พีชคณิต (พิมพ์ครั้งที่ 3)**. กรุงเทพฯ : มูลนิธิ สอวน.

ช่อเอื้อง อุทิตะสาร. (2562). **เอกสารประกอบการสอน รายวิชาหลักการคณิตศาสตร์**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

ณรงค์ ปั้นนิ่ม และ นิตติยา ปภาพจน์. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : มูลนิธิ สอวน.

ดำรงค์ ทิพย์โยธา. (2556). **คณิตศาสตร์ปรนัยเล่มที่ 37 : โลกทฤษฎีจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

ทบวงมหาวิทยาลัย. (2545). **ทฤษฎีจำนวนเบื้องต้น**. กรุงเทพฯ : โรงพิมพ์พิทักษ์การพิมพ์.

ทิพวัลย์ พัฒนางกูร. (2552). **ทฤษฎีจำนวน**. กรุงเทพฯ : องค์การค้าของ สกสค.

ธนัชยศ จำปาหวาย. (2559). **ทฤษฎีจำนวน**. กรุงเทพฯ : คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา.

นงนุช สุขวารี และคณะ. (2547). **คณิตศาสตร์พื้นฐานสำหรับคอมพิวเตอร์**. กรุงเทพฯ : มูลนิธิ สอวน.

นพพร ธนะชัยขันธ์. (2543). **ทฤษฎีจำนวน**. กรุงเทพฯ : วิทยพัฒน์.

นภวรรณ นิลศรี. (2553). **ระบบจำนวนเต็มกับการประยุกต์**. นครปฐม : สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร.

นฤมล ศรชัยยืน. (2540). **ทฤษฎีจำนวน**. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่.

นิตยา ตรีนันทวัน. (2544). **ทฤษฎีจำนวน 1 (พิมพ์ครั้งที่ 6)**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยรามคำแหง

ปวีณา ถ้ำแก้ว. (2558). **ระบบจำนวน**. เชียงใหม่ : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเชียงใหม่.

ปิยวดี วงษ์ใหญ่. (2530). **ทฤษฎีจำนวน**. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร.

พัฒนี อุดมกะวานิช. (2559). **หลักคณิตศาสตร์**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

บรรณานุกรม (ต่อ)

พิมพ์เพ็ญ เวชชาชีวะ. (2558). **ระบบจำนวน**. กรุงเทพฯ : วีพริ้นท์ (1991).

ภัททิรา เรืองสินทรัพย์. (2553). **อสมการและสมการเชิงฟังก์ชัน (พิมพ์ครั้งที่ 3)**. กรุงเทพฯ : มูลนิธิสอวน.

มานะ เอกจริยวงศ์. (2542). **ทฤษฎีจำนวนเบื้องต้น**. ลพบุรี : ศูนย์ตำราและเอกสารทางวิชาการ สถาบันราชภัฏเทพสตรี.

มานัส บุญยัง. (2532). **หนังสือประกอบการเรียนพีชคณิต**. กรุงเทพฯ : โรงพิมพ์ สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

มารศรี แนวจำปา. (2546). **ทฤษฎีจำนวน**. อุบลราชธานี : คณะวิทยาศาสตร์และเทคโนโลยี สถาบันราชภัฏอุบลราชธานี.

ยศนันต์ มีมาก. (2555). **คู่มือประกอบสื่อการสอน วิชาคณิตศาสตร์ : ทฤษฎีจำนวนเบื้องต้น (เนื้อหาตอนที่ 1)**. คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

รัชนียา ถิรเดโชชัย. (2560). **ระบบจำนวน**. ร้อยเอ็ด : สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏร้อยเอ็ด.

วรรณธิดา ยลวิลาศ. (2560). **ทฤษฎีจำนวน**. กาฬสินธุ์ : คณะศิลปศาสตร์และวิทยาศาสตร์ มหาวิทยาลัยกาฬสินธุ์

วรางคณา ร่องมะรุด. (2523). **ทฤษีจำนวน 2**. กรุงเทพฯ : ยูไนเต็ดโปรดักชั่น.

วสันต์ จินดารัตนาภรณ์. (2549). **ทฤษฎีจำนวน**. เชียงใหม่ : คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเชียงใหม่.

วัลลภ เหมวงษ์. (2556). **ทฤษฎีจำนวน**. อุดรธานี : สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี.

วัลลภ เหมวงษ์. (2562). **หลักการคณิตศาสตร์**. อุดรธานี : คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ. (2556). **ทฤษฎีจำนวน**. กรุงเทพฯ : ไฮเอ็ดพับลิชชิ่ง.

สมใจ จิตพิทักษ์. (2547). **ทฤษฎีจำนวน** (พิมพ์ครั้งที่ 3). สงขลา : ภารกิจเอกสารและตำรามหาวิทยาลัยทักษิณ.

สมจิต โชติชัยสถิตย์. (2540). **ทฤษฎีจำนวน 2**. ขอนแก่น : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น.

สมพร เรืองโชติวิทย์. (2521). **ทฤษฎีจำนวน**. กรุงเทพฯ : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ บางเขน

สมวงษ์ แปลงประสพโชค. (2545). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม)**. กรุงเทพฯ : สถาบันราชภัฏพระนคร.

สุเทพ จันทร์สมศักดิ์. (2538). **ระบบจำนวน**. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

สุภา สุจริตพงศ์. (2523). **โครงสร้างของระบบจำนวน**. กรุงเทพฯ : สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย

โสภาพรรณ ทิพย์โยธา. (2545). **ทฤษฎีจำนวน 1 (พิมพ์ครั้งที่ 6)**. กรุงเทพฯ : สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

บรรณานุกรม (ต่อ)

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

อำพล ธรรมเจริญ. (2523). **ทฤษฎีจำนวน (พิมพ์ครั้งที่ 2)**. ชลบุรี : ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ บางแสน

ไอริน ชุ่มเมืองเย็น. (2557). **ทฤษฎีจำนวน**. สาขาวิชาคณิตศาสตร์และสถิติ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏนครสวรรค์.

Coppel W.A. (2009). **Number Theory : An Introduction to Mathematics (2 ed.)**. New York : Springer Science & Business Media.

David M. Burton. (2002). **Elementary number theory (5 ed.)**. New York : The McGraw-HillCompanies, Inc.

David M. Burton. (2007). **Elementary number theory (6 ed.)**. New York : The McGraw-HillCompanies, Inc.

David M. Burton. (2011). **Elementary number theory (7 ed.)**. New York : The McGraw-HillCompanies, Inc.

Gareth A. Jones and J. Mary Jones. (1998). **Elementary number theory**. Springer Science & Business Media.

Ivan Niven, Herbert S. Zucker and Hugh L. Montgomery. (1991). **An introduction to Theory of Numbers**. New York : John Wiley & Sons, Inc.

Josip Hercet, Lorraine Heienrichs, Palmira Mariz Seiler and Marlence Torres Skoumal. (2012). **Mathematics higher level**. New York: Oxford university press.

Kenneth Ireland and Michael Rosen. (1990). **A Classical Introduction to Modern Number Theory (2 ed.)**. New York : Springer-Verlag, Inc.

Koshy T. (2007). **Elementary Number Theory with Applications (2 ed.)**. Elsevier Science.

Pual Glendinning. (2012). **Maths in minutes**. London, England : Quercus Editions Ltd.

Raji, W. (2013). **An Introductory Course in Elementary Number Theory**. Washington, D.C. : The Saylor Foundation.

Rosen K.H. (2005). **Elementary number theory and its applications (5 ed.)**. Boston : Pearson/Addison Wesley.

Testini Benchaporn. (1976). **Number Theory**. Bangkok : Ramkhamheang University.

Underwood Dudley. (1969). **Elementary Number Theorem**. San Francisco : W.H. Freeman and Company.

Underwood Dudley. (2012). **Elementary Number Theory (2 ed.)**. Dover Publications.