

บทที่ 4

สมภาค

สมภาค(Congruence) เป็นสัญลักษณ์ที่เกิดขึ้นมาจากการหารลงตัว คาร์ล ฟรีดริช เกาส์ (Carl Friedrich Gauss) นักคณิตศาสตร์ชาวเยอรมัน ได้นำเสนอสัญลักษณ์ของสมภาคเป็นครั้งแรกโดยสมภาคนั้นได้เป็นเครื่องมือที่สำคัญอย่างหนึ่งของทฤษฎีจำนวน เพราะสามารถอธิบายสมบัติของการหารลงตัวได้อย่างสะดวก เข้าใจได้ง่าย และสามารถแก้ปัญหาในสิ่งที่ต้องคิดคำนวณซับซ้อนให้ง่ายขึ้น ความรู้เกี่ยวกับสมภาคนี้ได้ปรากฏในชีวิตประจำวันเสมอ เช่น การเดินของเข็มนาฬิกา เข็มชั่วโมง เข็มนาฬิกา และเข็มนาฬิกา ในเรื่องของปฏิทิน วันในหนึ่งสัปดาห์ เดือนในหนึ่งปี นอกจากนี้ยังเป็นแนวทางนำไปสู่ เรื่องราวที่น่าสนใจรูปแบบใหม่ ๆ และสิ่งที่ปรากฏอีกมากมาย ในบทนี้จะนำเสนอเนื้อหาที่สำคัญที่ใช้ในการศึกษาสมภาคดังนี้ สมบัติเบื้องต้นของสมภาค ส่วนตกค้างในมอดุโล(Modulo) ต่าง ๆ การหาผลเฉลยของสมภาคเชิงเส้น(Linear Congruence) และการหาผลเฉลยของระบบสมภาคเชิงเส้น(System of Linear Congruences) เพื่อเป็นพื้นฐานในการศึกษาทฤษฎีจำนวนขั้นสูงต่อไป

4.1 สมบัติเบื้องต้นของสมภาค

สมภาคเป็นเรื่องที่เกี่ยวข้องกับความสัมพันธ์ของจำนวนเต็มสองจำนวน ในอีกรูปแบบหนึ่งจำนวนเต็มบวกจำนวนหนึ่งจะหารผลต่างของสมาชิกสองตัวใด ๆ ในเซตได้ลงตัวดังบทนิยามต่อไปนี้

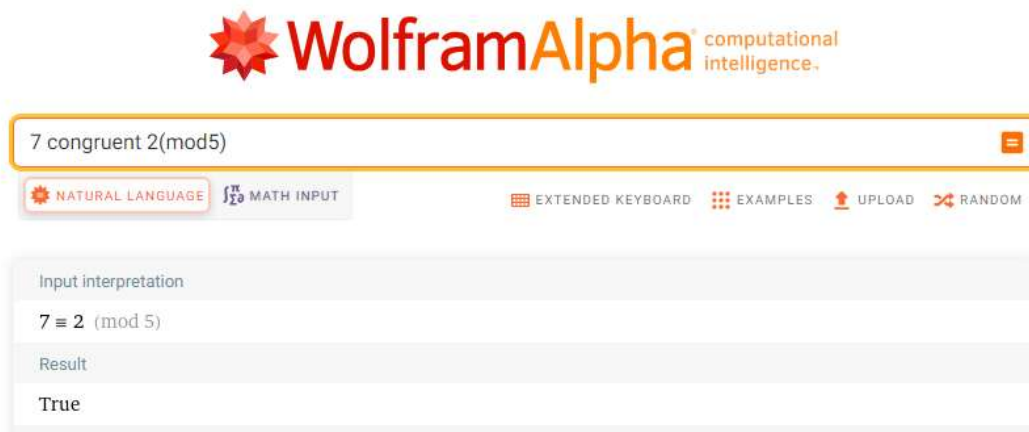
บทนิยาม 4.1

ให้ m เป็นจำนวนเต็มบวก a และ b เป็นจำนวนเต็ม ถ้า $m \mid (a - b)$ กล่าวได้ว่า a สมภาคกับ b มอดุโล m เขียนแทนด้วยสัญลักษณ์ $a \equiv b \pmod{m}$ เรียก m ว่าเป็น มอดุโล ถ้า $m \nmid (a - b)$ กล่าวได้ว่า a ไม่สมภาคกับ b มอดุโล m เขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{m}$

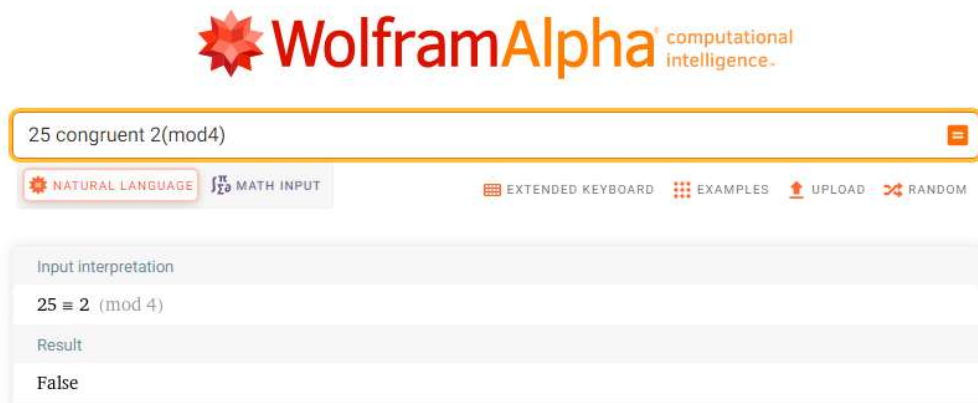
ตัวอย่าง 4.1

- $7 \equiv 2 \pmod{5}$ เนื่องจาก $5 \mid (7 - 2)$
- $25 \not\equiv 2 \pmod{4}$ เนื่องจาก $4 \nmid (25 - 2)$
- $-25 \not\equiv -2 \pmod{3}$ เนื่องจาก $3 \nmid (-25 + 2)$
- $a \equiv b \pmod{1}$ สำหรับ $a, b \in \mathbb{Z}$ เพราะว่า $1 \mid (a - b)$

จากตัวอย่าง 4.1 สามารถใช้ Wolfram Alpha เพื่อตรวจสอบสมภาคและไม่สมภาคกัน ในที่นี้จะยกตัวอย่างเพียง 2 ตัวอย่างส่วนข้ออื่น ๆ ก็ทำเหมือนกัน ดังภาพประกอบ 4.1 และ 4.2



ภาพประกอบ 4.1 ใช้ Wolfram Alpha เพื่อแสดงว่า $7 \equiv 2 \pmod{5}$



ภาพประกอบ 4.2 ใช้ Wolfram Alpha เพื่อแสดงว่า $25 \not\equiv 2 \pmod{4}$

จากตัวอย่าง 4.1 ข้อ 1 พบว่า ในกรณี $m = 1$ จะได้ $a \equiv b \pmod{m}$ สำหรับทุกจำนวนเต็ม a, b และในกรณี $m = 2$ จะได้ $a \equiv b \pmod{m}$ เมื่อ a, b เป็นจำนวนคู่เหมือนกัน หรือคี่เหมือนกัน ในการศึกษาสมภาคบางครั้งจำเป็นต้องเปลี่ยนสมภาคให้อยู่ในรูปของสมการโดยอาศัยทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1

ถ้า a และ b เป็นจำนวนเต็มใด ๆ จะได้ว่า $a \equiv b \pmod{m}$ ก็ต่อเมื่อ มีจำนวนเต็ม k ที่ทำให้ $a = b + km$

พิสูจน์

($\Rightarrow$) สมมติ $a \equiv b \pmod{m}$ แล้ว $m \mid (a - b)$

ดังนั้นจะมีจำนวนเต็ม k ที่ $km = a - b$

หรือ $a = b + km$

($\Leftarrow$) ถ้ามีจำนวนเต็ม k ที่ทำให้ $a = b + km$ แล้ว $km = a - b$

จะได้ว่า $m \mid (a - b)$

ดังนั้น $a \equiv b \pmod{m}$

ตัวอย่าง 4.2

กำหนดให้ $8 \equiv 3 \pmod{5}$ ได้ว่า $8 = 3 + (5 \times 1)$

กำหนดให้ $56 \equiv 2 \pmod{9}$ ได้ว่า $56 = 2 + (9 \times 6)$

กำหนดให้ $24 \equiv -3 \pmod{9}$ ได้ว่า $24 = -3 + (9 \times 3)$

ทฤษฎีบทต่อไปจะกล่าวถึงจำนวนเต็มสองจำนวนใด ๆ ถ้าสมภาคกับมอดุโล m แล้ว เมื่อถูกหารด้วยมอดุโลนั้น จะเหลือเศษเท่ากัน

ทฤษฎีบท 4.2

ถ้า a และ b เป็นจำนวนเต็มใด ๆ แล้ว $a \equiv b \pmod{m}$ ก็ต่อเมื่อ a และ b ถูกหารด้วย m แล้วเหลือเศษเท่ากัน

พิสูจน์

($\Rightarrow$) ให้ $a \equiv b \pmod{m}$ ดังนั้น $m \mid (a - b)$

จะมีจำนวนเต็ม k ที่ $a - b = km$ หรือ $a = b + km$

จากทฤษฎีบท 4.1 ในการนำ m ไปหาร b

จะมีจำนวนเต็ม q และ r ได้ ที่ทำให้

$$b = qm + r \text{ โดยที่ } 0 \leq r < m$$

จาก $a = km + b$ แทนค่า b จะได้

$$a = km + (qm + r) = (k + q)m + r \text{ โดยที่ } 0 \leq r < m$$

นั่นคือ เมื่อนำ m ไปหาร a และ b จะเหลือเศษเท่ากับ r เช่นกัน

($\Leftarrow$) ถ้านำ m ไปหาร a และ b แล้วเหลือเศษ r เท่ากัน

จะได้ว่า มีจำนวนเต็ม q_1, q_2 ที่ทำให้

$$a = q_1 m + r \quad \text{โดยที่ } 0 \leq r < m$$

$$a = q_2 m + r \quad \text{โดยที่ } 0 \leq r < m$$

ดังนั้น $a - b = (q_1 - q_2)m$ แต่ $q_1 - q_2$ เป็นจำนวนเต็ม

จะได้ว่า $m \mid (a - b)$ นั่นคือ $a \equiv b \pmod{m}$

ตัวอย่าง 4.3 จงตรวจสอบว่า $33 \equiv 21 \pmod{6}$ หรือไม่

วิธีทำ นำ 6 ไปหาร 33 พบว่า เหลือเศษ 3

นำ 6 ไปหาร 21 พบว่า เหลือเศษ 3

นั่นคือ เศษจากการหาร 33 และ 21 ด้วย 6 คือ 3 เท่ากัน

ดังนั้น $33 \equiv 21 \pmod{6}$

ตัวอย่าง 4.4 จงตรวจสอบว่า $43 \equiv 11 \pmod{7}$ หรือไม่

วิธีทำ นำ 7 ไปหาร 43 พบว่า เหลือเศษ 1

นำ 7 ไปหาร 11 พบว่า เหลือเศษ 4

พบว่าเศษจากการหาร 43 และ 11 ด้วย 7 ไม่เท่ากัน

ดังนั้น $43 \not\equiv 11 \pmod{7}$

นอกจากทฤษฎีที่กล่าวมาข้างต้นแล้ว สมภาคยังมีสมบัติอย่างหนึ่งของความสัมพันธ์ คือ ความสัมพันธ์สมมูล ซึ่งแสดงอยู่ในรูปทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.3

ความสัมพันธ์สมภาค มอดุโล m เป็นความสัมพันธ์สมมูล(Equivalence Relation) นั่นคือให้ m เป็นจำนวนเต็มบวก และ a, b, c เป็นจำนวนเต็มใด ๆ

1. สมบัติสะท้อน $a \equiv a \pmod{m}$
2. สมบัติสมมาตร ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$
3. สมบัติถ่ายทอด ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว
$$a \equiv c \pmod{m}$$

พิสูจน์

1. เนื่องจาก $m \mid (a - a)$

ดังนั้น $a \equiv a \pmod{m}$

2. จาก $a \equiv b \pmod{m}$
 จะได้ $m \mid (a - b)$ หรือ $m \mid (-1)(b - a)$
 ดังนั้น $m \mid (b - a)$
 นั่นคือ $b \equiv a \pmod{m}$
3. จาก $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$
 จะได้ $m \mid (a - b)$ และ $m \mid (b - c)$
 แสดงว่า $m \mid (a - b + b - c)$
 ดังนั้น $m \mid (a - c)$
 นั่นคือ $a \equiv c \pmod{m}$

สมภาคนั้นยังมีสมบัติบางอย่างที่คล้ายกับสมการ โดยเฉพาะในเรื่องของการบวก การลบและการคูณ เรียกว่า สมบัติเบื้องต้นของการเท่ากันของสมภาคดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.4

กำหนดให้ a, b, c, d เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก
 ถ้า $a \equiv b \pmod{m}$ แล้ว

1. $a + c \equiv b + c \pmod{m}$
2. $a - c \equiv b - c \pmod{m}$
3. $ac \equiv bc \pmod{m}$

พิสูจน์

1. จาก $a \equiv b \pmod{m}$ แล้ว $m \mid (a - b)$
 ดังนั้น ถ้าบวกเข้าและลบออก ด้วยจำนวนเต็ม c จะได้
 $m \mid (a - b + c - c)$
 ดังนั้น $m \mid (a + c) - (b + c)$
 นั่นคือ $a + c \equiv b + c \pmod{m}$
2. จาก $a \equiv b \pmod{m}$ แล้ว $m \mid (a - b)$
 ดังนั้น ถ้าลบออกและบวกเข้าด้วยจำนวนเต็ม c จะได้
 $m \mid (a - b - c + c)$
 ดังนั้น $m \mid (a - c) - (b - c)$
 นั่นคือ $a - c \equiv b - c \pmod{m}$

3. จาก $a \equiv b \pmod{m}$ แล้ว $m \mid (a - b)$

จะมีจำนวนเต็ม k ที่ทำให้

$$a - b = km \text{ และ } ac - bc = (kc)m$$

จะได้ $m \mid (a - b)c$

ดังนั้น $m \mid (ac - bc)$ นั่นคือ $ac \equiv bc \pmod{m}$

ตัวอย่าง 4.5 กำหนด $65 \equiv 20 \pmod{15}$

จะได้ $72 \equiv 27 \pmod{15}$ เนื่องจาก $65 + 7 \equiv 20 + 7 \pmod{15}$

จะได้ $55 \equiv 10 \pmod{15}$ เนื่องจาก $65 - 10 \equiv 20 - 10 \pmod{15}$

จะได้ $195 \equiv 60 \pmod{15}$ เนื่องจาก $65 \cdot 3 \equiv 20 \cdot 3 \pmod{15}$

ทฤษฎีบท 4.5

กำหนดให้ a, b, c เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก

สำหรับ $(c, m) = d$ ถ้า $ca \equiv cb \pmod{m}$ แล้ว $a \equiv b \pmod{\frac{m}{d}}$

พิสูจน์

เนื่องจาก $ca \equiv cb \pmod{m}$ จะได้ $m \mid (ca - cb)$

จะมีจำนวนเต็ม k ที่ทำให้ $ca - cb = km$

จะได้ว่า $\frac{c}{d}(a - b) = k \frac{m}{d}$

ดังนั้น $\frac{m}{d} \mid \frac{c}{d}(a - b)$ แต่ $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ เนื่องจาก $d = (c, m)$

จะได้ $\frac{c}{d}$ และ $\frac{m}{d}$ เป็นจำนวนเต็มและ $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$

จะได้ $\frac{m}{d} \mid (a - b)$ นั่นคือ $a \equiv b \pmod{\frac{m}{d}}$

ตัวอย่าง 4.6

กำหนดให้ $50 \equiv 20 \pmod{15}$

เนื่องจาก $(10, 15) = 5$ และ $10 \cdot 5 \equiv 10 \cdot 2 \pmod{15}$

จึงได้ว่า $5 \equiv 2 \pmod{\frac{15}{5}}$ นั่นคือ $5 \equiv 2 \pmod{3}$

บทแทรก 4.1

กำหนดให้ a, b, c เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก
สำหรับ $(c, m) = 1$ ถ้า $ac \equiv bc \pmod{m}$ แล้ว $a \equiv b \pmod{m}$

ตัวอย่าง 4.7

กำหนดให้ $42 \equiv 7 \pmod{5}$

เนื่องจาก $(7, 5) = 1$ และ $7 \cdot 6 \equiv 7 \cdot 1 \pmod{5}$

จึงได้ว่า $6 \equiv 1 \pmod{5}$

ทฤษฎีบท 4.6

กำหนดให้ a, b, c, d เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก โดยที่
 $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$

พิสูจน์

1. จาก $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ โดยทฤษฎีบท 4.4 ข้อที่ 1 จะได้

$$a + c \equiv b + c \pmod{m} \text{ และ}$$

$$c + b \equiv d + b \pmod{m} \text{ หรือ } b + c \equiv b + d \pmod{m}$$

จากทฤษฎีบท 4.3 ข้อที่ 3 จะได้

$$a + c \equiv b + d \pmod{m}$$

2. จาก $a \equiv b \pmod{m}$ โดยทฤษฎีบท 4.4 ข้อที่ 1 จะได้

$$a - c \equiv b - c \pmod{m} \text{ และ}$$

และจาก $c \equiv d \pmod{m}$ โดยทฤษฎีบท 4.4 ข้อที่ 3 จะได้

$$-c \equiv -d \pmod{m}$$

จากทฤษฎีบท 4.4 ข้อที่ 1 จะได้

$$b + (-c) \equiv b + (-d) \pmod{m} \text{ หรือ}$$

$$b - c \equiv b - d \pmod{m}$$

จากทฤษฎีบท 4.3 ข้อที่ 3 จะได้

$$a - c \equiv b - d \pmod{m}$$

3. จาก $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$

โดยทฤษฎีบท 4.4 ข้อที่ 3 จะได้

$$ac \equiv bc \pmod{m} \text{ และ}$$

$$cb \equiv db \pmod{m} \text{ หรือ } bc \equiv bd \pmod{m}$$

จากทฤษฎีบท 4.3 ข้อที่ 3 จะได้

$$ac \equiv bd \pmod{m}$$

ตัวอย่าง 4.8 กำหนดให้ $19 \equiv 3 \pmod{8}$ และ $17 \equiv 9 \pmod{8}$

$$\text{จะได้ } 19 + 17 \equiv 3 + 9 \pmod{8}$$

$$\text{จะได้ } 19 - 17 \equiv 3 - 9 \pmod{8}$$

$$\text{จะได้ } 19 \cdot 17 \equiv 3 \cdot 9 \pmod{8}$$

ทฤษฎีบท 4.7

กำหนดให้ a, b, c, d เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก

ถ้า $a \equiv b \pmod{m}$ แล้ว $a^n \equiv b^n \pmod{m}$ ทุกจำนวนเต็มบวก n

พิสูจน์ ใช้หลักอุปนัยเชิงคณิตศาสตร์ในการพิสูจน์ดังต่อไปนี้

ให้ $P(n)$ แทนข้อความ $a^n \equiv b^n \pmod{m}$

ขั้นฐาน

จาก $a \equiv b \pmod{m}$ ดังนั้น $P(1)$ เป็นจริง

ขั้นอุปนัย

สมมติ $P(k)$ เป็นจริงนั่นคือ $a^k \equiv b^k \pmod{m}$

จะแสดง $P(k+1)$ เป็นจริง นั่นคือจะแสดงว่า $a^{k+1} \equiv b^{k+1} \pmod{m}$

เนื่องจาก $a \cdot a^k \equiv b \cdot b^k \pmod{m}$ และ $a \equiv b \pmod{m}$

จะได้ $a^{k+1} \equiv b^{k+1} \pmod{m}$

ดังนั้น $P(k+1)$ เป็นจริง

จะได้ $P(n)$ เป็นจริง สำหรับทุกจำนวนเต็มบวก n

นั่นคือ $a^n \equiv b^n \pmod{m}$ เป็นจริง สำหรับทุกจำนวนเต็มบวก n

ตัวอย่าง 4.9

เนื่องจาก $7 \equiv 3 \pmod{4}$ จะได้ $7^3 \equiv 3^3 \pmod{4}$

เนื่องจาก $74 \equiv 2 \pmod{8}$ จะได้ $74^{51} \equiv 2^{51} \pmod{8}$

เนื่องจาก $89 \equiv 5 \pmod{21}$ จะได้ $89^{17} \equiv 5^{17} \pmod{21}$

จากทฤษฎีบทที่กล่าวมาข้างต้นทำให้สามารถนำการดำเนินการบางอย่างที่ใช้กับสมการ เช่น การบวก การคูณ และการยกกำลัง ด้วยจำนวนที่เท่ากันทั้งสองข้าง มาใช้กับสมภาคได้เพื่อนำไปประยุกต์ใช้กับปัญหาที่คิดคำนวณแบบซับซ้อนให้สามารถคิดคำนวณได้ง่ายขึ้น แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.10 จงหาเศษจากการหาร 3^{25} ด้วย 5

วิธีทำ เนื่องจาก $3^2 \equiv 4 \equiv -1 \pmod{5}$

$$\text{และ } (3^2)^{12} \equiv (-1)^{12} \equiv 1 \pmod{5}$$

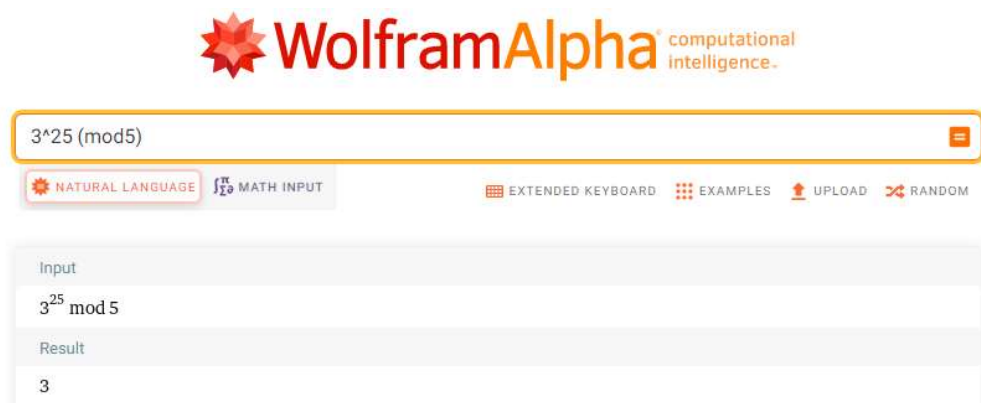
$$\text{จะได้ } 3^{25} \equiv (3^2)^{12} \cdot 3 \equiv 1 \cdot 3 \pmod{5} \equiv 3 \pmod{5}$$

นั่นคือ 3^{25} ถูกหารด้วย 5 เหลือเศษ 3

ดังนั้น เศษจากการหาร 3^{25} ด้วย 5 คือ 3

จากตัวอย่าง 4.10 ใช้ Wolfram Alpha เพื่อหาเศษจากการหาร 3^{25} ด้วย 5

ดังภาพประกอบ 4.3



ภาพประกอบ 4.3 ใช้ Wolfram Alpha เพื่อแสดงเศษจากการหาร 3^{25} ด้วย 5

ตัวอย่าง 4.11 จงตรวจสอบว่า $2^{20} - 1$ หารด้วย 41 ลงตัวหรือไม่

วิธีทำ เนื่องจาก $2^5 \equiv -9 \pmod{41}$

$$\text{จะได้ } (2^5)^4 \equiv (-9)^4 \pmod{41}$$

$$2^{20} \equiv (-9)^2(-9)^2 \pmod{41}$$

$$2^{20} \equiv (81)(81) \pmod{41}$$

$$\text{แต่ } 81 \equiv -1 \pmod{41} \text{ จะได้ } (81)(81) \equiv (-1)(-1) \pmod{41}$$

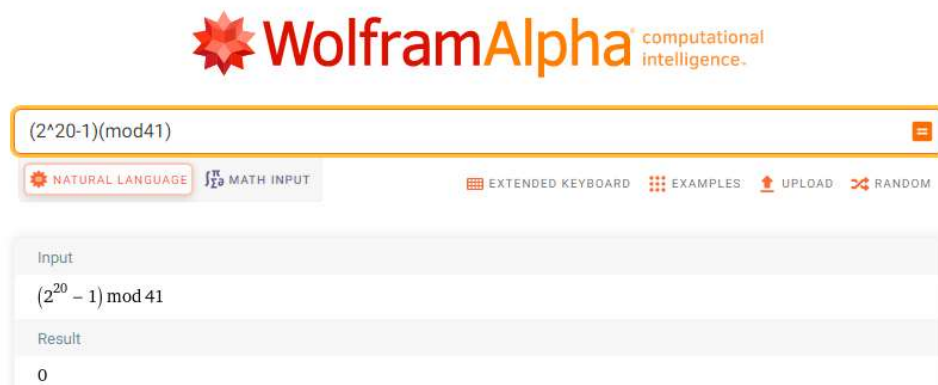
$$\text{ดังนั้น } 2^{20} \equiv (-1)(-1) \pmod{41}$$

$$\text{นั่นคือ } 2^{20} \equiv 1 \pmod{41}$$

$$\text{และ } 2^{20} - 1 \equiv 0 \pmod{41}$$

ดังนั้น $2^{20} - 1$ หารด้วย 41 ลงตัว

จากตัวอย่าง 4.11 ใช้ Wolfram Alpha เพื่อตรวจสอบว่า $2^{20} - 1$ หารด้วย 41 ลงตัวดังภาพประกอบ 4.4



ภาพประกอบ 4.4 ใช้ Wolfram Alpha เพื่อหาเศษจากการหาร $2^{20} - 1$ หารด้วย 41

ตัวอย่างที่ 4.12 จงหาเศษจากการหาร $(32517)(5328)$ ด้วย 14

วิธีทำ เนื่องจาก $32517 \equiv 9 \pmod{14}$

$$\text{และ } 5328 \equiv 8 \pmod{14}$$

$$\text{จะได้ว่า } (32517)(5328) \equiv (9)(8) \pmod{14}$$

$$\text{หรือ } (32517)(5328) \equiv 72 \pmod{14}$$

$$\text{เนื่องจาก } 72 \equiv 2 \pmod{14}$$

$$\text{นั่นคือ } (32517)(5328) \equiv 2 \pmod{14}$$

ดังนั้น $(32517)(5328)$ หารด้วย 14 เหลือเศษ 2

ตัวอย่าง 4.13 จงหาเศษจากการหาร $(375)2^{100} - 35^{87}$ ด้วย 6

วิธีทำ พิจารณา 375

$$\text{เนื่องจาก } 375 \equiv 3 \pmod{6}$$

พิจารณา 2^{100}

$$\text{เนื่องจาก } 2^{100} = (2^5)^{20} = 32^{20} \equiv 2^{20} \pmod{6}$$

$$\text{และ } 2^{20} = (2^5)^4 = 32^4 \equiv 2^4 \pmod{6}$$

$$\text{แสดงว่า } 2^{100} \equiv 16 \pmod{6}$$

พิจารณา 35

$$\text{เนื่องจาก } 35 \equiv -1 \pmod{6} \text{ จะได้ } 35^{87} \equiv (-1)^{87} \pmod{6}$$

$$\text{แสดงว่า } 35^{87} \equiv -1 \pmod{6}$$

$$\text{นั่นคือ } (375)2^{100} - 35^{87} \equiv (3)(4) - (-1) = 13 \equiv 1 \pmod{6}$$

ดังนั้น $(375)2^{100} - 35^{87}$ หารด้วย 6 เหลือเศษ 1

ตัวอย่างที่ 4.14 ให้ n หารด้วย 8 เหลือเศษ 5 จงหาเศษจากการหาร $n^3 + 5n$ ด้วย 8

วิธีทำ จาก n หารด้วย 8 เหลือเศษ 5

$$\text{แสดงว่า } n \equiv 5 \pmod{8}$$

$$\begin{aligned} \text{จะได้ } [n^3 + 5n] \pmod{8} &\equiv (5^3 + 5(5)) \pmod{8} \\ &\equiv 150 \pmod{8} \end{aligned}$$

$$\text{เนื่องจาก } 150 \equiv 6 \pmod{8} \text{ แสดงว่า } [n^3 + 5n] \pmod{8} \equiv 6 \pmod{8}$$

ดังนั้น $n^3 + 5n$ หารด้วย 8 เหลือเศษ 6

4.2 ชั้นส่วนตกค้าง(Residue Class)

ในหัวข้อที่ผ่านมาพบว่าสมภาคเป็นความสัมพันธ์สมมูลบนเซตของจำนวนเต็ม แต่ถ้าเซตของจำนวนเต็มถูกแบ่งออกเป็นเซตย่อยที่ไม่มีส่วนร่วมกันทุกคู่ จะเรียกเซตนี้ว่า ชั้นส่วนตกค้าง ซึ่งแสดงไว้ในบทนิยามต่อไปนี้

บทนิยาม 4.2

ถ้า $a \equiv b \pmod{m}$ เรียก b เป็นส่วนตกค้าง(Residue Class)ของ a

มอดุโล m โดยที่

$b \in \{0, 1, 2, \dots, m-1\}$ ให้ C_n เป็นเซตของส่วนตกค้างทั้งหมดของ a นั่นคือ

$$C_n = \{x \mid x \in I, x \equiv a \pmod{m}\}$$

เซต C_n เรียกว่า ชั้นส่วนตกค้างมอดุโล m

ชั้นส่วนตกค้างมอดุโล m นั้นเกิดจากที่ m สามารถแบ่งจำนวนเต็มซึ่งสมภาคกันออกเป็น m ชั้น และจำนวนเต็มในแต่ละชั้นเมื่อหารด้วย m แล้วเหลือเศษเท่ากัน เช่น ในมอดุโล 5 จะแบ่งจำนวนเต็มเป็น 5 ชั้น ดังนี้

$$C_0 = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$C_1 = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$C_2 = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$C_3 = \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$C_4 = \{\dots, -6, -1, 4, 9, 14, \dots\}$$

บทนิยาม 4.3

ถ้า S เป็นสับเซตของจำนวนเต็ม จะเรียกเซต S ว่าเป็นระบบส่วนตกค้างบริบูรณ์ (Complete Residue System) ถ้าจำนวนเต็มใด ๆ แต่ละตัวสมภาคกับสมาชิกของ S ตัวใดตัวหนึ่งเพียงตัวเดียวเท่านั้น

ตัวอย่าง 4.15

1. $\{5, 8, 11\}$ ไม่เป็นระบบบริบูรณ์ของส่วนตกค้างมอดุโล 3 เนื่องจาก

$$5 \equiv 2 \pmod{3}$$

$$8 \equiv 2 \pmod{3}$$

$$12 \equiv 0 \pmod{3}$$

2. $\{0, 1, 2, 3, 4, 5\}$ เป็นระบบบริบูรณ์ของส่วนตกค้างมอดุโล 6 เนื่องจาก

$$0 \equiv 0 \pmod{6}$$

$$3 \equiv 3 \pmod{6}$$

$$1 \equiv 1 \pmod{6}$$

$$4 \equiv 4 \pmod{6}$$

$$2 \equiv 2 \pmod{6}$$

$$5 \equiv 5 \pmod{6}$$

3. $\{12, 13, 8, -3, 22, 11\}$ เป็นระบบบริบูรณ์ของส่วนตกค้างมอดุโล 6 เนื่องจาก

$$12 \equiv 0 \pmod{6}$$

$$-3 \equiv 3 \pmod{6}$$

$$13 \equiv 1 \pmod{6}$$

$$22 \equiv 4 \pmod{6}$$

$$8 \equiv 2 \pmod{6}$$

$$11 \equiv 5 \pmod{6}$$

สมาชิกใน $\{12, 13, 8, -3, 22, 11\}$ สมภาคกับสมาชิกในระบบส่วนตกค้างบริบูรณ์มอดุโล 6 ในลักษณะหนึ่งต่อหนึ่ง ถ้านำระบบส่วนตกค้างบริบูรณ์มอดุโล 6 มาหาเซตย่อยที่มีสมาชิกของเซตย่อยเป็นจำนวนเฉพาะสัมพัทธ์กับ 6 เรียกเซตนี้ว่า เป็นระบบส่วนตกค้างลดรูปมอดุโล 6 นั้นเองสำหรับบทนิยามต่อไปจะแสดงดังบทนิยามของระบบส่วนตกค้างลดรูปมอดุโล m

บทนิยาม 4.4

เซตย่อยของระบบบริบูรณ์ของส่วนตกค้างมอดุโล m ที่อยู่ในรูป $\{a_1, a_2, \dots, a_k\}$ เรียกว่า ระบบส่วนตกค้างลดรูป(Reduced Residue System) มอดุโล m ก็ต่อเมื่อ

1. $(a_i, m) = 1$ สำหรับทุก ๆ $i = 1, 2, \dots, k$
2. $a_i \equiv a_j \pmod{m}$ ถ้า $i \equiv j$
3. สำหรับจำนวนเต็ม n ที่ $(n, m) = 1$ จะได้ว่ามี a_k ที่ทำให้ $n \equiv a_k \pmod{m}$

สำหรับเซตย่อยของระบบส่วนตกค้างบริบูรณ์มอดุโล m อยู่ในรูป

$$\{a \mid 0 \leq a < m, (a, m) = 1\}$$

จะเรียกว่า ระบบส่วนตกค้างลดรูปที่ไม่เป็นลบค่าน้อยสุดมอดุโล m

ตัวอย่าง 4.16

1. $\{0, 1, 2, 3, 4, 5, 6, 7\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 8 แต่ $\{1, 3, 5, 7\}$ เป็นระบบส่วนตกค้างลดรูปที่ไม่เป็นลบค่าน้อยสุดมอดุโล 8
2. $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 10 แต่ $\{1, 3, 7, 9\}$ เป็นระบบส่วนตกค้างลดรูปที่ไม่เป็นลบค่าน้อยสุดมอดุโล 10

วิธีเลือกระบบส่วนตกค้างบริบูรณ์มีได้หลายแบบ แต่ละเซตจะมีสมบัติที่เกี่ยวกับสมภาคเป็นเหมือนกัน ดังนั้นเมื่อกล่าวถึงสมบัติของส่วนตกค้างบริบูรณ์ จะพิจารณาในระบบที่ประกอบด้วยจำนวนเต็มบวกที่น้อยกว่า m ที่รวมศูนย์ด้วย ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.8

ถ้า S เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m และ $(m, n) = 1$ โดยที่ $n \in I$ แล้วสำหรับจำนวนเต็ม r ใด ๆ เซต C ซึ่ง $C = \{qn + r \mid q \in s\}$ จะเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m ด้วย

พิสูจน์

เนื่องจาก S มีสมาชิก m ตัว ดังนั้น C มีสมาชิก m

สมมติว่า $q_1, q_2 \in S$ ซึ่งทำให้ $q_1 n + r \equiv q_2 n + r \pmod{m}$

จะได้ว่า $q_1 n \equiv q_2 n \pmod{m}$ และ $(m, n) = 1$

จะได้ว่า $q_1 \equiv q_2 \pmod{m}$ แต่ $q_1, q_2 \in S$ เป็นระบบส่วนตกค้างบริบูรณ์

ดังนั้น $q_1 = q_2$ ซึ่งทำให้ $q_1 n + r = q_2 n + r$
 นั่นคือ C เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

4.3 สมภาคเชิงเส้น

ในหัวข้อนี้จะกล่าวถึงสมภาคของตัวแปรที่มีเลขชี้กำลังเป็นหนึ่งที่อยู่ในรูป $ax \equiv b \pmod{m}$ รวมทั้งการหาคำตอบทั้งหมดของสมภาคเชิงเส้นที่อยู่ในรูปดังกล่าว ที่ไม่สมภาคกัน และก่อนที่จะศึกษาเรื่องสมภาคเชิงเส้นและการหาผลเฉลยนั้นต้องเข้าใจความหมายของสมภาคเชิงเส้น และผลเฉลยของสมภาคเชิงเส้นดังบทนิยามต่อไปนี้

บทนิยาม 4.5.

ให้ a, b เป็นจำนวนเต็มและ m เป็นจำนวนเต็มบวก สมภาคที่อยู่ในรูป $ax \equiv b \pmod{m}$ เมื่อ x เป็นจำนวนเต็มที่ไม่ทราบค่า เรียกสมภาคเชิงเส้นตัวแปรเดียว

บทนิยาม 4.6

จำนวนเต็ม x_0 ใด ๆ ที่สอดคล้องกับสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ เรียกว่าผลเฉลยของสมภาคเชิงเส้น นั่นคือ $ax_0 \equiv b \pmod{m}$

จากบทนิยาม $ax_0 \equiv b \pmod{m}$ ก็ต่อเมื่อ $n \mid ax_0 - b$ หรือ $y_0 n = ax_0 - b$ สำหรับจำนวนเต็ม y_0 บางจำนวน

ตัวอย่าง 4.17 กำหนด $3x \equiv 9 \pmod{12}$

ให้ $x = 3$ จะได้ว่า $3(3) \equiv 9 \pmod{12}$

แสดงว่า $x = 3$ เป็นผลเฉลยของ $3x \equiv 9 \pmod{12}$

ให้ $x = 5$ จะได้ว่า $3(5) \not\equiv 9 \pmod{12}$

แสดงว่า $x = 5$ ไม่เป็นผลเฉลยของ $3x \equiv 9 \pmod{12}$

ทฤษฎีบท 4.9

ถ้า x_0 เป็นผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ และ $x_0 \equiv y_0 \pmod{m}$ แล้ว y_0 เป็นผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$

พิสูจน์

กำหนดให้ x_0 เป็นผลเฉลยของสมภาคเชิงเส้น

$$ax \equiv b \pmod{m} \text{ และ } x_0 \equiv y_0 \pmod{m}$$

ดังนั้นจะได้ว่า $ax_0 \equiv ay_0 \pmod{m}$

เนื่องจาก $ax_0 \equiv b \pmod{m}$

จะได้ $ay_0 \equiv b \pmod{m}$

นั่นคือ y_0 เป็นผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$

สำหรับทฤษฎีบท 4.9 นั้นพบว่าสมภาค $ax \equiv b \pmod{m}$ มีผลเฉลยแล้วสามารถหาผลเฉลยที่สมภาคกันได้เป็นจำนวนอนันต์ผลเฉลย แต่สิ่งที่ต้องการค้นหาคือมีผลเฉลยอื่น ๆ อีกหรือไม่ที่ไม่สมภาคกับผลเฉลยเริ่มต้นที่หามาได้ ซึ่งอาศัยบทนิยามผลเฉลยที่ไม่สมภาคกันว่าเป็นผลเฉลยที่แตกต่างกัน ดังบทนิยามต่อไปนี้

บทนิยาม 4.7

กำหนดให้ x_0, y_0 เป็นผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ กล่าวว่า

x_0 กับ y_0 เป็นผลเฉลยที่แตกต่างกันถ้า $x_0 \not\equiv y_0 \pmod{m}$

x_0 กับ y_0 เป็นผลเฉลยที่ไม่แตกต่างกันถ้า $x_0 \equiv y_0 \pmod{m}$

ตัวอย่าง 4.18 กำหนด $3x \equiv 6 \pmod{15}$

เนื่องจาก $3(2) \equiv 6 \pmod{15}$

และ $3(-13) \equiv 6 \pmod{15}$

แสดงว่า $x = 2$ และ $x = -13$ สอดคล้องกับสมภาค $3x \equiv 6 \pmod{15}$

และ $2 \equiv -13 \pmod{15}$

ดังนั้น $x = 2$ และ $x = -13$ เป็นผลเฉลยที่ไม่แตกต่างกัน

ในการหาผลเฉลยที่แตกต่างกันทั้งหมดของสมภาค $ax \equiv b \pmod{m}$ สามารถทำได้โดยการแทนค่า x เป็น $0, 1, 2, \dots, m-1$ ในสมภาค จะทำให้ทราบว่าผลเฉลยที่แตกต่างกันทั้งหมดกี่ผลเฉลย แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.19 จงหาผลเฉลยของสมภาค $2x \equiv 3 \pmod{5}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2, 3, 4$ ดังต่อไปนี้

$$x = 0 \text{ จะได้ } 2 \cdot 0 \not\equiv 3 \pmod{5}$$

$$x = 1 \text{ จะได้ } 2 \cdot 1 \not\equiv 3 \pmod{5}$$

$$x = 2 \text{ จะได้ } 2 \cdot 2 \not\equiv 3 \pmod{5}$$

$$x = 3 \text{ จะได้ } 2 \cdot 3 \not\equiv 3 \pmod{5}$$

$$x = 4 \text{ จะได้ } 2 \cdot 4 \equiv 3 \pmod{5}$$

ดังนั้น ผลเฉลยของสมภาคนี้คือ $x \equiv 4 \pmod{5}$ หรือ $x \in \{\dots, -6, -1, 4, 9, 14, \dots\}$

จากตัวอย่าง 4.19 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของสมภาค $2x \equiv 3 \pmod{5}$ ดังภาพประกอบ 4.5



ภาพประกอบ 4.5 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของ $2x \equiv 3 \pmod{5}$

ตัวอย่าง 4.20 จงหาผลเฉลยของสมภาค $2x \equiv 6 \pmod{4}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2, 3$ ดังต่อไปนี้

$$x = 0 \text{ จะได้ } 2 \cdot 0 \not\equiv 6 \pmod{4}$$

$$x = 1 \text{ จะได้ } 2 \cdot 1 \equiv 6 \pmod{4}$$

$$x = 2 \text{ จะได้ } 2 \cdot 2 \not\equiv 6 \pmod{4}$$

$$x = 3 \text{ จะได้ } 2 \cdot 3 \equiv 6 \pmod{4}$$

เนื่องจาก $3 \not\equiv 1 \pmod{4}$ แสดงว่ามีผลเฉลยที่แตกต่างกันสองผลเฉลย

ดังนั้น ผลเฉลยของสมภาคนี้มีสองผลเฉลยที่แตกต่างกันสองผลเฉลย คือ $x \equiv 1 \pmod{4}$

$$\text{และ } x \equiv 3 \pmod{4}$$

ตัวอย่าง 4.21 จงหาผลเฉลยของสมภาค $2x \equiv 3 \pmod{4}$

วิธีทำ แทนค่า x ด้วย $0, 1, 2, 3$ ดังต่อไปนี้

$$x = 0 \text{ จะได้ } 2 \cdot 0 \not\equiv 3 \pmod{4}$$

$$x = 1 \text{ จะได้ } 2 \cdot 1 \not\equiv 3 \pmod{4}$$

$$x = 2 \text{ จะได้ } 2 \cdot 2 \not\equiv 3 \pmod{4}$$

$$x = 3 \text{ จะได้ } 2 \cdot 3 \not\equiv 3 \pmod{4}$$

ดังนั้น สมภาคนี้ไม่มีผลเฉลย

จากตัวอย่างที่ผ่านมาในการหาผลเฉลยทั้งหมดของสมภาค $ax \equiv b \pmod{m}$ ที่ไม่สมภาค นั้นเหมาะสำหรับกรณีที่ m ที่มีค่าน้อยเพราะง่ายในการแทนค่า สำหรับในกรณีที่ m มีค่ามาก ๆ นั้น จึงไม่เหมาะสมในการใช้วิธีการดังกล่าว สำหรับทฤษฎีบทต่อไปเป็นทฤษฎีที่มีความสำคัญในการ แก้ปัญหาสมภาคเชิงเส้น เพราะนอกจากจะช่วยหาผลเฉลยแล้วยังสามารถตรวจสอบได้ด้วยว่าสมภาค เชิงเส้นนั้นมีผลเฉลยหรือไม่

ทฤษฎีบท 4.10

ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก และ $d = (a, m)$ จะได้ว่า

1. สมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีผลเฉลยในจำนวนเต็มก็ต่อเมื่อ $d|b$

2. ถ้า $d|b$ แล้วสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีผลเฉลยอยู่ d ตัว

ที่ผลเฉลยไม่สมภาคกันในมอดุโล m และผลเฉลยเหล่านั้น คือ

$$x = x_0 + t \frac{m}{d} \pmod{m} \quad \text{เมื่อ } t = 0, 1, 2, \dots, d-1$$

โดยที่ x_0 เป็นผลเฉลยหนึ่งของ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

พิสูจน์

1. จะแสดงว่า สมภาคเชิงเส้น $ax \equiv b \pmod{m}$ จะมีคำตอบก็ต่อเมื่อ $d|b$

($\Rightarrow$) สมมติว่า $ax \equiv b \pmod{m}$ มีผลเฉลย

จะได้ว่า x_0 เป็นจำนวนเต็ม ที่ทำให้ $ax_0 \equiv b \pmod{m}$

แสดงว่า $m|(ax_0 - b)$

เนื่องจาก $d|m$ และ $d|a$ ดังนั้น $d|b$

($\Leftarrow$) สมมติว่า $d|b$ จะมีจำนวนเต็ม k ที่ทำให้ $b = dk$ และจาก

$d = (a, m)$ จะได้ว่ามี x_0, y_0 ที่ทำให้ $d = ax_0 + my_0$

จะได้ว่า

$$\begin{aligned} b &= dk \\ &= (ax_0 + my_0)k \\ &= ax_0k + my_0k \end{aligned}$$

ดังนั้น $m \mid ax_0k - b$ นั่นคือ $ax_0k \equiv b \pmod{m}$

แสดงว่า $ax \equiv b \pmod{m}$ มีผลเฉลยคือ x_0k

2. จะแสดงว่า ถ้าสมภาคดังกล่าวมีคำตอบแล้ว จำนวนคำตอบจะเท่ากับ (a, m) คำตอบกำหนดให้ $d = (a, m)$ การพิสูจน์แบ่งออกเป็น 2 ตอนดังนี้

ตอนที่ 1 จาก $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ และ $1 \mid \frac{b}{d}$ แสดงว่า $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

มีผลเฉลยให้ x_0 เป็นผลเฉลยหนึ่งของ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

จะได้ว่า $\frac{m}{d} \left(\frac{a}{d}x_0 - \frac{b}{d} \right)$ แสดงว่ามีจำนวนเต็ม k ที่ทำให้

$$\frac{a}{d}x_0 - \frac{b}{d} = \frac{m}{d}k$$

ให้ t เป็นจำนวนเต็ม จะแสดงว่า $x_0 + \frac{m}{d}t$ เป็นผลเฉลยของสมการ

$$\text{เพราะว่า } a \left(x_0 + \frac{m}{d}t \right) - b = ax_0 + \frac{am}{d}t - b$$

$$\begin{aligned} &= \frac{adx_0}{d} + \frac{amt}{d} - \frac{bd}{d} \\ &= d \left(\frac{a}{d}x_0 - \frac{b}{d} \right) + \frac{a}{d}mt \\ &= d \left(\frac{m}{d}k \right) + \frac{a}{d}mt \\ &= m \left(k + \frac{a}{d}t \right) \end{aligned}$$

จาก $d \mid a$ และ t เป็นจำนวนเต็ม จะได้ $m \mid \left[a \left(x_0 + \frac{m}{d}t \right) - b \right]$

นั่นคือ $a \left(x_0 + \frac{m}{d}t \right) \equiv b \pmod{m}$ แสดงว่า $x_0 + \frac{m}{d}t$ เป็นผลเฉลย

ของ $ax \equiv b \pmod{m}$ สำหรับทุกจำนวนเต็ม t

ต่อไปจะแสดงว่าผลเฉลยของ $ax \equiv b \pmod{m}$ จะเขียนอยู่ในรูป

$$x_0 + \frac{m}{d}q \text{ เมื่อ } q \text{ เป็นจำนวนเต็ม}$$

ให้ x_1 เป็นผลเฉลยของ $ax \equiv b \pmod{m}$

จะได้ $ax_1 \equiv b \pmod{m}$ เนื่องจาก $a\left(x_0 + \frac{m}{d}t\right) \equiv b \pmod{m}$

จะได้ว่า $ax_1 \equiv a\left(x_0 + \frac{m}{d}t\right) \pmod{m}$

ดังนั้น $\frac{a}{d}x_1 \equiv \frac{a}{d}\left(x_0 + \frac{m}{d}t\right) \pmod{\frac{m}{d}}$

จาก $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ จะได้ว่า

$$x_1 \equiv \left(x_0 + \frac{m}{d}t\right) \pmod{\frac{m}{d}}$$

แสดงว่าจะมี จำนวนเต็ม t_1 ที่ทำให้ $x_1 - \left(x_0 + \frac{m}{d}t\right) = \frac{m}{d}t_1$ จะได้ว่า

$$x_1 = x_0 + \frac{m}{d}(t + t_1)$$

นั่นคือ มี $q = t + t_1$ เป็นจำนวนเต็มที่ทำให้ $x_1 = x_0 + \frac{m}{d}q$

ดังนั้น ผลเฉลยของ $ax \equiv b \pmod{m}$ จะเขียนอยู่ในรูป $x \equiv x_0 + t\left(\frac{m}{d}\right) \pmod{m}$

เมื่อ t เป็นจำนวนเต็มโดยที่ x_0 เป็นผลเฉลยหนึ่งของ $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

ตอนที่ 2 ให้ $d = (a, m)$ และ t เป็นจำนวนเต็ม จะต้องแสดงว่า

$ax \equiv b \pmod{m}$ มีผลเฉลย d ตัว ที่ผลเฉลยไม่สมภาคกันในมอดุโล m

จาก d, t เป็นจำนวนเต็ม โดยขั้นตอนวิธีการหารจะได้ว่า มี q, r เป็นจำนวนเต็มที่ทำให้ $t = dq + r$ โดยที่ $0 \leq r < d$

$$\text{ดังนั้น } x_0 + t\left(\frac{m}{d}\right) = x_0 + (dq + r)\frac{m}{d} = x_0 + mq + r\frac{m}{d}$$

$$\text{แสดงว่า } x_0 + t\left(\frac{m}{d}\right) \equiv x_0 + r\frac{m}{d} \pmod{m} \text{ โดยที่ } 0 \leq r < d - 1$$

ดังนั้น ผลเฉลยของ $ax \equiv b \pmod{m}$ จะมีอยู่ d ตัวเท่านั้นที่ผลเฉลยไม่สมภาคกัน

ในมอดุโล m คือ $x \equiv x_0 + \frac{m}{d}t \pmod{m}$ เมื่อ $t = 0, 1, 2, \dots, d - 1$

จากทฤษฎีบทพบว่า ถ้า $d \nmid b$ แล้วสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ ไม่มีผลเฉลย ในการ

ผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ อาจหาผลเฉลยหนึ่งคือ x_0 จากสมภาค

$$\frac{a}{d}x \equiv 1 \left(\text{mod } \frac{m}{d} \right)$$

และให้ $x_1 \equiv \frac{b}{d}x_0$ จะได้ว่า x_1 เป็นผลเฉลยหนึ่งของสมภาค

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d} \right)$$

นอกจากนี้ยังพบว่าถ้า a และ m เป็นจำนวนเฉพาะสัมพัทธ์กันแล้วทำให้สมภาคนั้นมีผลเฉลยเพียงผลเฉลยเดียวโดยนำเสนอเป็นทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 4.11

ถ้า $(a, m) = 1$ แล้วสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีเพียงผลเฉลยเดียว

พิสูจน์

เพราะว่า $(a, m) = 1$ จะได้ว่า มีจำนวนเต็ม r และ q ที่ทำให้ $ar + ms = 1$

เป็นการรวมเชิงเส้น คุณด้วย b จะได้

$$a(rb) + m(sb) = b$$

$$a(rb) - b = m(sb)$$

$$\text{ดังนั้น } a(rb) \equiv b \pmod{m}$$

นั่นคือ (rb) เป็นผลเฉลยของ $ax \equiv b \pmod{m}$

ถ้ามี q เป็นผลเฉลยอีกค่าหนึ่ง จะได้

$$aq \equiv b \pmod{m}$$

$$\text{ดังนั้น } ax \equiv arb \pmod{m}$$

แต่ $(a, m) = 1$ จะได้ว่า $q \equiv rb \pmod{m}$

จะได้ว่า $ax \equiv b \pmod{m}$ มีเพียงผลเฉลยเดียว

ตัวอย่าง 4.22 สมภาคต่อไปนี้ไม่มีผลเฉลย

$$9x \equiv 11 \pmod{15} \text{ ไม่มีผลเฉลย เพราะ } (9, 15) = 3 \text{ และ } 3 \nmid 11$$

$$5x \equiv 12 \pmod{20} \text{ ไม่มีผลเฉลย เพราะ } (5, 20) = 5 \text{ และ } 5 \nmid 12$$

$$3x \equiv 2 \pmod{21} \text{ ไม่มีผลเฉลย เพราะ } (3, 21) = 3 \text{ และ } 3 \nmid 2$$

$$10x \equiv 7 \pmod{40} \text{ ไม่มีผลเฉลย เพราะ } (10, 40) = 10 \text{ และ } 10 \nmid 7$$

จากตัวอย่าง 4.22 ใช้ Wolfram Alpha เพื่อแสดงว่าสมภาคไม่มีผลเฉลยและในที่นี้จะยกตัวอย่างเฉพาะสมภาค $9x \equiv 11 \pmod{15}$ เท่านั้น ดังภาพประกอบ 4.6



ภาพประกอบ 4.6 ใช้ Wolfram Alpha เพื่อแสดงว่า $9x \equiv 11 \pmod{15}$ ไม่มีผลเฉลย

ตัวอย่าง 2.23 จงตรวจสอบว่าสมภาค $9x \equiv 15 \pmod{21}$ มีผลเฉลยหรือไม่ถ้ามีจงหาผลเฉลยของทั้งหมดที่ไม่สมภาคกัน

วิธีทำ เนื่องจาก $(9, 21) = 3$ ซึ่ง $3 \nmid 15$

แสดงว่าสมภาคนี้มีผลเฉลยและมีทั้งหมด 3 ผลเฉลยที่ไม่สมภาคกันในมอดุโล 21 จาก $9x \equiv 15 \pmod{21}$ จะได้

$$3 \cdot 3x \equiv 3 \cdot 5 \pmod{21} \text{ เนื่องจาก } (3, 21) = 3 \text{ จะได้}$$

$$3x \equiv 5 \pmod{\frac{21}{3}} \text{ หรือ}$$

$$3x \equiv 5 \pmod{7}$$

$$\text{เนื่องจาก } 3(4) \equiv 5 \pmod{7}$$

แสดงว่า 4 เป็นผลเฉลยหนึ่งของสมภาค

ผลเฉลยทั้งหมด 3 ผลเฉลย มีดังนี้

$$x \equiv 4 + \left(\frac{21}{3}\right)t \pmod{21} \text{ เมื่อ } t = 0, 1, 2$$

$$\text{หรือ } x \equiv 4 + 7t \pmod{21} \text{ เมื่อ } t = 0, 1, 2$$

$$\text{จะได้ } x \equiv 4, 11, 18 \pmod{21}$$

ดังนั้น ผลเฉลยของสมภาค $9x \equiv 15 \pmod{21}$ ที่ไม่สมภาคกันมี 3 ผลเฉลย ได้แก่

$$x \equiv 4 \pmod{21}, x \equiv 11 \pmod{21} \text{ และ } x \equiv 18 \pmod{21}$$

ตัวอย่าง 2.24 จงหาผลเฉลยของสมภาค $4x \equiv -100 \pmod{56}$

วิธีทำ เนื่องจาก $(4, 56) = 4$ ซึ่ง $4 \nmid -100$

แสดงว่าสมภาคนี้มีผลเฉลยและมีทั้งหมด 4 ผลเฉลยที่ไม่สมภาคกันในมอดุโล 56

จาก $4x \equiv -100 \pmod{56}$ จะได้

$$4 \cdot 1x \equiv 4 \cdot (-25) \pmod{56} \text{ เนื่องจาก } (4, 56) = 4 \text{ จะได้}$$

$$x \equiv -25 \pmod{\frac{56}{4}} \text{ หรือ}$$

$$x \equiv -25 \pmod{14}$$

เนื่องจาก $3 \equiv -25 \pmod{14}$

แสดงว่า 3 เป็นผลเฉลยหนึ่งของสมภาค

ผลเฉลยทั้งหมด 4 ผลเฉลย มีดังนี้

$$x \equiv 3 + \left(\frac{56}{4}\right)t \pmod{56} \text{ เมื่อ } t = 0, 1, 2, 3$$

$$\text{หรือ } x \equiv 3 + 14t \pmod{56} \text{ เมื่อ } t = 0, 1, 2, 3$$

$$\text{จะได้ } x \equiv 3, 17, 31, 45 \pmod{56}$$

ดังนั้น ผลเฉลยของสมภาค $4x \equiv -100 \pmod{56}$ ที่ไม่สมภาคกันมี 4 ผลเฉลย ได้แก่

$$x \equiv 3 \pmod{56}, x \equiv 17 \pmod{56}, x \equiv 31 \pmod{56} \text{ และ } x \equiv 45 \pmod{56}$$

จากตัวอย่างที่ผ่านมาพบว่าสมภาคเชิงเส้นอาจมีผลเฉลยหรือไม่มีผลเฉลยก็ได้ และยังสามารถหาผลเฉลยทั้งหมดที่ไม่สมภาคกันได้อีกด้วยแต่ปัญหาการหาผลเฉลยในตัวอย่างที่ผ่านมาคือการหาผลเฉลยแรกของสมภาค ต่อไปจะเป็นการนำเสนอวิธีการในการหาผลเฉลยของสมภาคโดยใช้ตัวผกผันตัวบทนิยามและทฤษฎีบทต่อไปนี้

บทนิยาม 4.8

ให้ a เป็นจำนวนเต็มโดยที่ $(a, m) = 1$ ถ้ามีจำนวนเต็ม x ซึ่ง $ax \equiv 1 \pmod{m}$ จะเรียกว่า a มีตัวผกผัน มอดุโล m และเรียก x ว่า **ตัวผกผันมอดุโล m**

ตัวอย่าง 4.25 จงหาตัวผกผันของ 2 มอดุโล 4

วิธีทำ ต้องการหา x ซึ่งทำให้ $2x \equiv 1 \pmod{4}$

แทนค่า x ด้วย 0, 1, 2 และ 3 ดังต่อไปนี้

$$x = 0 \text{ จะได้ } 2 \cdot 0 \not\equiv 1 \pmod{4}$$

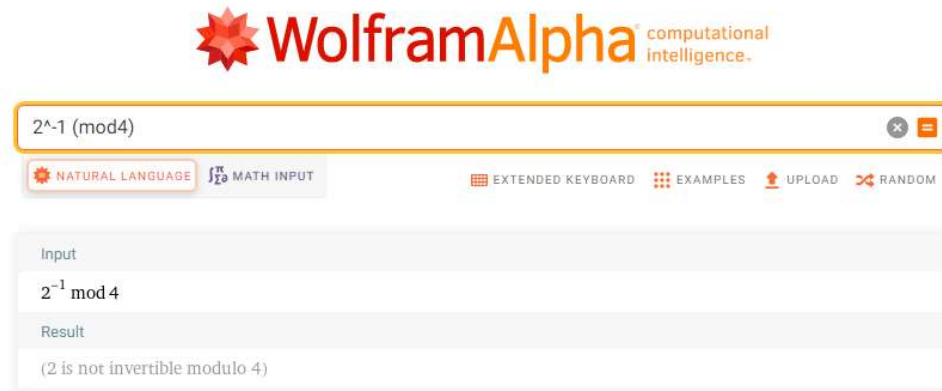
$$x = 1 \text{ จะได้ } 2 \cdot 1 \not\equiv 1 \pmod{4}$$

$$x = 2 \text{ จะได้ } 2 \cdot 2 \not\equiv 1(\text{mod } 4)$$

$$x = 3 \text{ จะได้ } 2 \cdot 3 \not\equiv 1(\text{mod } 4)$$

ดังนั้น ไม่มีผกผันของ 2 โมดูล 4

จากตัวอย่าง 4.25 ใช้ Wolfram Alpha เพื่อหาตัวผกผันของ 2 โมดูล 4 แสดงได้ ดังภาพประกอบ 4.7



ภาพประกอบ 4.7 ใช้ Wolfram Alpha เพื่อแสดงว่าไม่มีผกผันของ 2 โมดูล 4

ตัวอย่าง 4.26 จงหาตัวผกผันของ 7 โมดูล 4

วิธีทำ ต้องการหา x ซึ่งทำให้ $7x \equiv 1(\text{mod } 4)$

แทนค่า x ด้วย 0, 1, 2 และ 3 ดังต่อไปนี้

$$x = 0 \text{ จะได้ } 7 \cdot 0 \not\equiv 1(\text{mod } 4)$$

$$x = 1 \text{ จะได้ } 7 \cdot 1 \not\equiv 1(\text{mod } 4)$$

$$x = 2 \text{ จะได้ } 7 \cdot 2 \not\equiv 1(\text{mod } 4)$$

$$x = 3 \text{ จะได้ } 7 \cdot 3 \equiv 1(\text{mod } 4)$$

ดังนั้น 3 เป็นผกผันของ 7 โมดูล 4

จากตัวอย่าง 4.26 ใช้ Wolfram Alpha เพื่อหาตัวผกผันของ 7 โมดูล 4 แสดงได้ ดังภาพประกอบ 4.8



ภาพประกอบ 4.8 ใช้ Wolfram Alpha เพื่อแสดงว่า 3 เป็นผกผันของ 7 มอดุโล 4

จากตัวอย่างจะพบว่าตัวผกผันนั้นอาจจะมีหรือไม่มีก็ได้ และปัญหาอีกอย่างหนึ่งที่พบในตัวอย่างที่ผ่านมาคือสำหรับในกรณีที่หาตัวผกผันมอดุโลมีค่ามาก ๆ นั้น ทำให้เสียเวลาและไม่สะดวกในการหา ดังนั้นจึงมีวิธีการในอีกรูปแบบหนึ่งที่น่ามาตรวจสอบว่ามีตัวผกผันหรือไม่ โดยจะนำเสนอในรูปแบบทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.12

ให้ a เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวกที่มากกว่า 1 ซึ่ง $(a, m) = 1$ แล้วตัวผกผัน a มอดุโล m จะหาค่าได้ และมีเพียงค่าเดียวเท่านั้นที่ไม่สมภาคกันในมอดุโล m

พิสูจน์

เนื่องจาก $\{0, 1, 2, \dots, m-1\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

และ $(a, m) = 1$ จะได้ว่า

$\{0, a, 2a, \dots, (m-1)a\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

ดังนั้นจะมีจำนวนเต็ม $x \in \{0, 1, 2, \dots, m-1\}$ เพียงจำนวนเดียวเท่านั้นที่

$$ax \equiv 1 \pmod{m}$$

นั่นคือ a มีตัวผกผันมอดุโล m เพียงค่าเดียวเท่านั้นในเซต $\{0, 1, 2, \dots, m-1\}$

สำหรับตัวอย่างต่อไปจะเป็นการนำทฤษฎีบท 4.12 ไปตรวจสอบว่ามีตัวผกผันหรือไม่และหาตัวผกผันจากการประยุกต์ขั้นตอนแบบยุคลิด

ตัวอย่าง 4.27 จงหาตัวผกผันของ 15 มอดุโล 61

วิธีทำ เนื่องจาก $(15, 61) = 1$ แสดงว่า ผกผันของ 15 มอดุโล 61 หาค่าได้จากขั้นตอนวิธีของยุคลิดจะได้ว่า

$$61 = 15(4) + 1$$

$$\text{หรือ } 1 = 61 + (-4)(15)$$

$$\text{จะได้ } 61 + (-4)15 \equiv 1 \pmod{61}$$

$$\text{เนื่องจาก } 61 \equiv 0 \pmod{61} \text{ ทำให้ได้ว่า } (-4)15 \equiv 1 \pmod{61}$$

ดังนั้น -4 เป็นตัวผกผันของ 15 มอดุโล 61

ตัวอย่าง 4.28 จงหาตัวผกผันของ 15 มอดุโล 62

วิธีทำ เนื่องจาก $(15, 62) = 1$ แสดงว่า ผกผันของ 15 มอดุโล 62 หาค่าได้จากขั้นตอนวิธีของยุคลิดจะได้ว่า

$$62 = 15(4) + 2 \quad \text{หรือ} \quad 2 = 62 - 15(4)$$

$$15 = 2(7) + 1 \quad \text{หรือ} \quad 1 = 15 - 2(7)$$

ทำย้อนกลับจะได้ว่า

$$\begin{aligned} 1 &= 15 - 2(7) \\ &= 15 - [62 - 15(4)](7) \\ &= 15 - 62(7) + 15(28) \\ &= 15(29) - 62(7) \end{aligned}$$

$$\text{จากสมการ } 15(29) + 62(-7) = 1$$

$$\text{จะได้ } 15(29) + 62(-7) \equiv 1 \pmod{62}$$

$$\text{เนื่องจาก } 62(-7) \equiv 0 \pmod{62} \text{ ทำให้ได้ว่า } 15(29) \equiv 1 \pmod{62}$$

ดังนั้น 29 เป็นตัวผกผันของ 15 มอดุโล 62

ทฤษฎีบท 4.13

ให้ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็มบวก จะได้ว่า a เป็นตัวผกผันมอดุโล p ก็ต่อเมื่อ $a \equiv 1 \pmod{p}$ หรือ $a \equiv -1 \pmod{p}$

พิสูจน์

$$(\Rightarrow) \text{ ถ้า } a \equiv 1 \pmod{p} \text{ หรือ } a \equiv -1 \pmod{p} \text{ แล้ว } a^2 \equiv 1 \pmod{p}$$

ดังนั้น a เป็นตัวผกผันมอดุโล p ของตัวมันเอง

$$(\Leftarrow) \text{ ถ้า } a \text{ เป็นตัวผกผันมอดุโล } p \text{ ของตัวมันเอง แล้ว } a^2 = a \cdot a \equiv 1 \pmod{p}$$

แสดงว่า $p \mid (a^2 - 1)$

เนื่องจาก $a^2 - 1 = (a - 1)(a + 1)$ จะได้ $p \mid (a - 1)(a + 1)$

ดังนั้น $a \equiv 1 \pmod{p}$ หรือ $a \equiv -1 \pmod{p}$

เนื่องจากตัวผกผันของ a มอดุโล m ถ้าหาค่าได้จะมีเพียงค่าเดียวเท่านั้น ดังนั้นสามารถนำตัวผกผันมาช่วยในการหาผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ ได้ เมื่อกำหนดให้ $\bar{a}$ เป็นตัวผกผันของ a มอดุโล m ถ้า $ax \equiv b \pmod{m}$ แล้วสามารถคูณทั้งสองข้างของสมภาคนี้ด้วย $\bar{a}$ ได้

$$\begin{aligned}\bar{a}(ax) &\equiv \bar{a}b \pmod{m} \\ x &\equiv \bar{a}b \pmod{m}\end{aligned}$$

ตัวอย่าง 4.29 จงหาผลเฉลยของสมภาคเชิงเส้น $15x \equiv 17 \pmod{62}$

วิธีทำ จากตัวอย่าง 4.28 ได้ว่า 29 เป็นตัวผกผันของ 15 มอดุโล 62
คูณทั้งสองข้างของสมภาคด้วย 29 จะได้

$$\begin{aligned}(29)15x &\equiv (29)17 \pmod{62} \\ x &\equiv 493 \pmod{62}\end{aligned}$$

เนื่องจาก $493 \equiv 59 \pmod{62}$

จะได้ $x \equiv 59 \pmod{62}$

เนื่องจาก $(15, 62) = 1$ แสดงว่าสมภาค $15x \equiv 17 \pmod{62}$ มี 1 ผลเฉลย

ดังนั้น ผลเฉลยของสมภาคเชิงเส้น $15x \equiv 17 \pmod{62}$ คือ $x \equiv 59 \pmod{62}$

ตัวอย่าง 4.30 จงหาผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{23}$

วิธีทำ ดำเนินการหาผกผันของ 6 มอดุโล 23 ดังนี้

เนื่องจาก $(6, 23) = 1$ แสดงว่า ผกผันของ 6 มอดุโล 23 หาค่าได้

จากขั้นตอนวิธีของยุคลิดจะได้ว่า

$$23 = 6(3) + 5 \quad \text{หรือ} \quad 5 = 23 - 6(3)$$

$$6 = 5(1) + 1 \quad \text{หรือ} \quad 1 = 6 - 5(1)$$

ทำย้อนกลับจะได้ว่า

$$\begin{aligned}
 1 &= 6 - 5(1) \\
 &= 6 - [23 - 6(3)](1) \\
 &= 6 - 23(1) + 6(3) \\
 &= 6(4) - 23(1)
 \end{aligned}$$

ทำให้ได้ว่า $6(4) - 23(1) \equiv 1 \pmod{23}$ เนื่องจาก $23(1) \equiv 0 \pmod{23}$

แสดงว่า $6(4) \equiv 1 \pmod{23}$

นั่นคือ 4 เป็นผกผันของ 6 มอดุโล 23

คูณทั้งสองข้างของสมภาคด้วย 4 จะได้

$$\begin{aligned}
 (4)6x &\equiv (4)5 \pmod{23} \\
 x &\equiv 20 \pmod{23}
 \end{aligned}$$

ดังนั้น ผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{23}$ คือ $x \equiv 20 \pmod{23}$

4.4 ระบบสมภาคเชิงเส้น

ในหัวข้อที่ผ่านมาจะเป็นการหาผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ โดยมีผลเฉลยอยู่ในรูปแบบ $x \equiv c \pmod{m}$ แต่ถ้ามีสมภาคเชิงเส้นมากกว่าหนึ่ง สมภาคแล้วจะเรียกว่าระบบสมภาคเชิงเส้น ดังบทนิยามต่อไปนี้

บทนิยาม 4.9

สมภาคเชิงเส้น

$$\begin{aligned}
 a_1x &\equiv b_1 \pmod{m_1} \\
 a_2x &\equiv b_2 \pmod{m_2} \\
 &\vdots \\
 a_nx &\equiv b_n \pmod{m_n}
 \end{aligned}$$

เรียกสมภาคเหล่านี้ว่าระบบสมภาคเชิงเส้น เมื่อ a_i, b_i เป็นจำนวนเต็มบวก

สำหรับทุก $i = 1, 2, 3, \dots, n$

Rosen K. H. (2014 : 162) ได้กล่าวว่าระบบสมภาคเชิงเส้นนี้สร้างมาจากปัญหาของชาวจีนโบราณในประมาณคริสต์ศตวรรษที่ 1 ซันซู (Sun-Tsue) ได้ตั้งปัญหาไว้ว่า “มีจำนวนเต็มใดบ้างที่หารด้วย 3, 5, 7 แล้วมีเศษเหลือเป็น 2, 3, 2 ตามลำดับ” จากปัญหาดังกล่าวสามารถเขียนให้อยู่ในระบบสมภาคเชิงเส้นได้ดังนี้

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5} \quad \text{และ} \quad x \equiv 2 \pmod{7}$$

เพื่อให้เป็นเกียรติแก่ชาวจีนจึงเรียกทฤษฎีบทเกี่ยวกับการหาผลเฉลยร่วมกันของ ระบบสมภาคเชิงเส้นว่า “ทฤษฎีเศษเหลือของชาวจีน” แสดงในรูปแบบทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 4.14 (ทฤษฎีบทเศษเหลือของชาวจีน)

ให้ $m_1, m_2, \dots, m_r$ เป็นจำนวนเฉพาะสัมพัทธ์บวกทุกคู่ แล้วระบบสมภาคเชิงเส้น ต่อไปนี้

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

จะมีผลเฉลยร่วมกันเพียงผลเฉลยเดียวมอดุโล $M = m_1 m_2 \cdots m_r$

พิสูจน์

กำหนดให้ $M = m_1 m_2 \cdots m_r$ และ $M_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$

เนื่องจาก $m_1, m_2, \dots, m_r$ เป็นจำนวนเฉพาะสัมพัทธ์บวกทุกคู่

ดังนั้น $(M_k, m_k) = 1$ เพราะฉะนั้นสมภาคเชิงเส้น $M_k x \equiv 1 \pmod{m_k}$

มีเพียงผลเฉลยเดียว ผลเฉลยให้เป็น x_k

จะได้ $M_k m_k \equiv 1 \pmod{m_k}$ และจะได้ $a_k M_k x_k \equiv a_k \pmod{m_k}$

พิจารณา M_k เนื่องจาก $m_i \mid M_k$ ถ้า $i \neq k$

กำหนดให้ $y = a_1 M_1 x_1 + \cdots + a_r M_r x_r$ จะได้ว่า

$$y \equiv a_1 M_1 x_1 + \cdots + a_r M_r x_r \equiv a_k M_k x_k \pmod{m_k} \equiv a_k \pmod{m_k}$$

ดังนั้น y เป็นผลเฉลยร่วมกันของระบบสมภาคเชิงเส้น

ต่อไปจะแสดงว่า ระบบสมภาคเชิงเส้นมีผลเฉลยเพียงผลเฉลยเดียวที่แตกต่างกัน มอดุโล M

กำหนดให้ x เป็นผลเฉลยร่วมกันของระบบสมภาคเชิงเส้น

จะได้ว่า $x \equiv a_k \pmod{m_k}$ สำหรับ $k = 1, 2, \dots, r$

ดังนั้น $y \equiv a_k \pmod{m_k}$ ดังนั้นจะได้ $m_k \mid (y - x)$

เนื่องจาก $m_1, m_2, \dots, m_r$ เป็นจำนวนเฉพาะสัมพัทธ์บวกทุกคู่

จะได้ $m_1, m_2, \dots, m_r \mid (y - x)$

นั่นคือ $x \equiv y \pmod{m_1, m_2, \dots, m_r}$ หรือ $x \equiv y \pmod{M}$

ตัวอย่าง 3.31 จงหาผลเฉลยของระบบสมภาคเชิงเส้นต่อไปนี้

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

วิธีทำ จาก $M = m_1 m_2 \cdots m_r$ และ $M_k = \frac{M}{m_k}$

$$\text{จะได้ } M = 3 \cdot 5 \cdot 7 = 105$$

$$\text{และ } M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15$$

$$\text{จาก } a_1 = 2, a_2 = 3, a_3 = 2$$

ต่อไปหา x_k จาก $M_k x \equiv 1 \pmod{m_k}$ ดังนี้

$$35x_1 \equiv 1 \pmod{3} \text{ จะได้ } x_1 \equiv 2 \pmod{3}$$

$$21x_2 \equiv 1 \pmod{5} \text{ จะได้ } x_2 \equiv 1 \pmod{5}$$

$$15x_3 \equiv 1 \pmod{7} \text{ จะได้ } x_3 \equiv 1 \pmod{7}$$

จาก $x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{M}$ จะได้ผลเฉลยของระบบสมภาคคือ

$$x = (2)(35)(2) + (3)(21)(1) + (2)(15)(1) \equiv 233 \pmod{105}$$

แต่เนื่องจาก $233 \equiv 23 \pmod{105}$ จะได้ว่า $x \equiv 23 \pmod{105}$

ดังนั้น ผลเฉลยของระบบสมภาคคือ $x \equiv 23 \pmod{105}$

จากตัวอย่าง 4.31 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้น

ดังภาพประกอบ 4.9



ภาพประกอบ 4.9 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาค $x \equiv 2 \pmod{3}$,

$$x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}$$

ตัวอย่าง 4.32 จงหาผลเฉลยของระบบสมภาคเชิงเส้นต่อไปนี้

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{7}$$

วิธีทำ จาก $M = m_1 m_2 \cdots m_r$ และ $M_k = \frac{M}{m_k}$ จะได้ $M = 2 \cdot 3 \cdot 7 = 42$

$$\text{และ } M_1 = \frac{42}{2} = 21, M_2 = \frac{42}{3} = 14, M_3 = \frac{42}{7} = 6$$

$$\text{จาก } a_1 = 1, a_2 = 2, a_3 = 1$$

ต่อไปหา x_k จาก $M_k x_k \equiv 1 \pmod{m_k}$ ดังนี้

$$21x_1 \equiv 1 \pmod{2} \text{ จะได้ } x_1 \equiv 1 \pmod{2}$$

$$14x_2 \equiv 1 \pmod{3} \text{ จะได้ } x_2 \equiv 2 \pmod{3}$$

$$6x_3 \equiv 1 \pmod{7} \text{ จะได้ } x_3 \equiv 6 \pmod{7}$$

จาก $x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{M}$ จะได้ผลเฉลยของระบบสมภาคคือ

$$x \equiv (1)(21)(1) + (2)(14)(2) + (1)(6)(6) \equiv 113 \pmod{42}$$

แต่เนื่องจาก $113 \equiv 29 \pmod{42}$ จะได้ว่า $x \equiv 29 \pmod{42}$

ดังนั้น ผลเฉลยของระบบสมภาคคือ $x \equiv 29 \pmod{42}$

ทฤษฎีบทพิเศษเหลือของจีน ทำให้ทราบวิธีการหาผลเฉลยของระบบสมภาคเชิงเส้นที่มีมอดุโลเป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แต่ถ้าสำหรับในกรณีที่มีมอดุโลไม่เป็นจำนวนเฉพาะสัมพัทธ์กัน สามารถหาผลเฉลยที่เป็นจำนวนเต็มที่เป็นคำตอบรวมของทุก ๆ สมภาคได้ โดยเริ่มจากระบบสมภาคเชิงเส้นสองสมภาคจากทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.15

กำหนดระบบสมภาคเชิงเส้น

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

1. ระบบสมภาคจะมีผลเฉลยก็ต่อเมื่อ $(m_1, m_2) \mid (a_2 - a_1)$
2. ถ้าระบบสมภาคเชิงเส้นมีผลเฉลยแล้วผลเฉลยจะอยู่ในรูป

$$x \equiv x_0 \pmod{[m_1, m_2]}$$

และผลเฉลยมีเพียงผลเฉลยเดียวในมอดุโล $[m_1, m_2]$

พิสูจน์

1. จากสมภาค $x \equiv a_1 \pmod{m_1}$

ดังนั้น $x = a_1 + m_1 y$ โดยที่ y เป็นจำนวนเต็ม

แทนค่า x ใน $x \equiv a_2 \pmod{m_2}$ จะได้

$$a_1 + m_1 y \equiv a_2 \pmod{m_2}$$

นั่นคือ $m_1 y \equiv a_2 - a_1 \pmod{m_2}$ จะมีผลเฉลยก็ต่อเมื่อ $(m_1, m_2) \mid (a_2 - a_1)$

2. กำหนดให้ระบบสมภาคเชิงเส้นมีผลเฉลย

จากข้อที่ 1 จะได้ $(m_1 m_2) \mid (a_2 - a_1)$ แสดงว่า $m_1 y \equiv a_2 - a_1 \pmod{m_2}$ มีผลเฉลย

สมมติให้ y_0 เป็นผลเฉลยของ $m_1 y \equiv a_2 - a_1 \pmod{m_2}$

ดังนั้นผลเฉลยจะอยู่ในรูป $y_0 + \frac{m_2}{(m_1, m_2)} t$ เมื่อ t เป็นจำนวนเต็ม

จาก $x = a_1 + m_1 y$ โดยที่ y เป็นจำนวนเต็ม

จะได้

$$\begin{aligned} x &= a_1 + m_1 \left(y_0 + \frac{m_2}{(m_1, m_2)} t \right) \text{ โดยที่ } y_0, t \text{ เป็นจำนวนเต็ม} \\ &= a_1 + m_1 y_0 + \frac{m_1 m_2}{(m_1, m_2)} t \end{aligned}$$

นั่นคือ $x = a_1 + m_1 y_0 + [m_1, m_2] t$

ดังนั้น $x = x_0 + [m_1, m_2] t$ โดยที่ t และ $x_0 = a_1 + m_1 y_0$ เป็นจำนวนเต็ม

นั่นคือ $x \equiv x_0 \pmod{[m_1, m_2]}$ เป็นผลเฉลยของสมภาคเชิงเส้น

ให้ x_1 และ x_2 เป็นจำนวนเต็ม ซึ่ง $x_1 \equiv a_1 \pmod{m_1}$ และ $x_2 \equiv a_2 \pmod{m_2}$

เนื่องจาก $x_0 \equiv a_1 \pmod{m_1}$ และ $x_0 \equiv a_2 \pmod{m_2}$

จะได้ $x_1 \equiv x_0 \pmod{m_1}$ และ $x_2 \equiv x_0 \pmod{m_2}$

ดังนั้น $m_1 \mid (x_1 - x_0)$ และ $m_2 \mid (x_1 - x_0)$ แสดงว่า $(m_1, m_2) \mid (a_2 - a_1)$

นั่นคือ $x_1 \equiv x_0 \pmod{[m_1, m_2]}$

แสดงว่าระบบสมภาคเชิงเส้นมีเพียงผลเฉลยเดียวในมอดุโล $[m_1, m_2]$

ตัวอย่าง 4.32 จงแสดงว่าระบบสมภาคต่อไปนี้ไม่มีผลเฉลย

$$x \equiv 4 \pmod{5}$$

$$x \equiv 6 \pmod{15}$$

เนื่องจาก $(5, 15) = 5$ และ $6 - 4 = 2$ ซึ่ง $5 \nmid 2$

ดังนั้นระบบสมภาคเชิงเส้นที่กำหนดให้ไม่มีผลเฉลยที่เป็นจำนวนเต็ม

จากตัวอย่าง 4.32 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้นแสดงได้
ดังภาพประกอบ 4.10



ภาพประกอบ 4.10 ใช้ Wolfram Alpha เพื่อแสดงว่าระบบสมภาคเชิงเส้น $x \equiv 4 \pmod{5}$

$$x \equiv 6 \pmod{15} \text{ ไม่มีผลเฉลย}$$

ตัวอย่าง 4.33 จงหาผลเฉลยของระบบสมภาคเชิงเส้นต่อไปนี้

$$x \equiv 2 \pmod{6}$$

$$x \equiv 5 \pmod{15}$$

วิธีทำ เนื่องจาก $(6, 15) = 3$ และ $5 - 2 = 3$ ซึ่ง $3 \mid 3$ จะได้ว่าระบบสมภาคเชิงเส้นนี้มีผลเฉลย

จากสมภาค $x \equiv 2 \pmod{6}$ จะมี k ที่เป็นจำนวนเต็มที่ทำให้ $x = 6k + 2$

แทนค่า $x = 6k + 2$ ใน $x \equiv 5 \pmod{15}$

จะได้

$$6k + 2 \equiv 5 \pmod{15}$$

$$6k \equiv 3 \pmod{15}$$

$$6k \equiv 3 \pmod{15}$$

และสมภาค $6k \equiv 3 \pmod{15}$ มีผลเฉลยคือ $k \equiv 3 \pmod{5}$

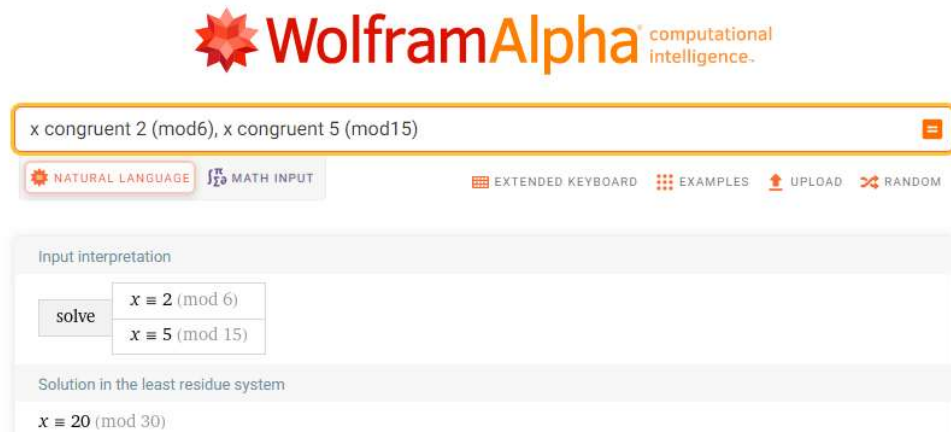
แสดงว่า $k = 5k_1 + 3$ เมื่อ k_1 เป็นจำนวนเต็ม

$$\text{จะได้ } x = 6(5k_1 + 3) + 2 = 30k_1 + 20$$

นั่นคือ $x \equiv 20 \pmod{30}$ เป็นผลเฉลยของระบบสมภาคเชิงเส้น

ดังนั้น ผลเฉลยของระบบสมภาคเชิงเส้นคือ $x \equiv 20 \pmod{30}$

จากตัวอย่าง 4.33 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้น
ดังภาพประกอบ 4.11



ภาพประกอบ 4.11 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้น

การใช้ทฤษฎีบทที่ผ่านมาในการหาผลเฉลยระบบสมภาคเชิงเส้นนั้นพบว่าสามารถหาผลเฉลยของระบบสมภาคสองสมภาคเท่านั้น สำหรับในกรณีที่ระบบสมภาคเชิงเส้นที่มีสมภาคมากกว่าสองสมภาคนั้นสามารถหาผลเฉลยโดยใช้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.16

กำหนดระบบสมภาคเชิงเส้น

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

1. ระบบสมภาคจะมีผลเฉลยก็ต่อเมื่อ $(m_i, m_j) \mid (a_j - a_i)$ สำหรับทุก i, j ซึ่ง $i \neq j$
2. ถ้าคำตอบหนึ่งเป็น x_0 แล้วคำตอบทั่วไปคือ $x \equiv x_0 \pmod{[m_1, m_2, \dots, m_n]}$

พิสูจน์

1. จากสมภาค $x \equiv a_i \pmod{m_i}$

ดังนั้น $x = a_i + m_i y$ โดยที่ y เป็นจำนวนเต็ม

แทนค่า x ใน $x \equiv a_j \pmod{m_j}$ จะได้

$$a_i + m_i y \equiv a_j \pmod{m_j}$$

นั่นคือ $m_i y \equiv a_j - a_i \pmod{m_j}$ จะมีผลเฉลยก็ต่อเมื่อ

$$(m_i, m_j) \mid (a_j - a_i) \text{ สำหรับทุก } i, j \text{ ซึ่ง } i \neq j$$

2. ให้ x_0 เป็นคำตอบของระบบสมภาค และถ้า x_i เป็นคำตอบใด ๆ ของระบบสมภาค แล้ว

$$x_1 \equiv a_1 \equiv x_0 \pmod{m_1}$$

$$x_1 \equiv a_2 \equiv x_0 \pmod{m_2}$$

$$\vdots \quad \vdots$$

$$x_1 \equiv a_n \equiv x_0 \pmod{m_n}$$

$$\text{จะได้ว่า } m_1 \mid (x_1 - x_0), m_2 \mid (x_1 - x_0), \dots, m_n \mid (x_1 - x_0)$$

$$\text{ดังนั้น } [m_1, m_2, \dots, m_n] \mid (x_1 - x_0) \text{ แสดงว่า } x \equiv x_0 \pmod{[m_1, m_2, \dots, m_n]}$$

$$\text{เพราะฉะนั้นคำตอบทั่วไปของระบบสมภาคเชิงเส้น คือ } x \equiv x_0 \pmod{[m_1, m_2, \dots, m_n]}$$

ตัวอย่าง 4.34 จงหาผลเฉลยของระบบสมภาคเชิงเส้นต่อไปนี้

$$x \equiv 2 \pmod{3}$$

$$x \equiv 5 \pmod{15}$$

$$x \equiv 8 \pmod{12}$$

วิธีทำ เนื่องจาก $(3, 15) \mid 5 - 2$, $(15, 12) \mid 8 - 5$ และ $(12, 3) \mid 8 - 2$

แสดงว่าระบบสมภาคเชิงเส้นนี้มีผลเฉลย

จากสมภาค $x \equiv 2 \pmod{3}$ จะมี k_1 ที่เป็นจำนวนเต็มที่ทำให้ $x = 3k_1 + 2$

แทนค่า $x = 3k_1 + 2$ ใน $x \equiv 5 \pmod{15}$

จะได้

$$3k_1 + 2 \equiv 5 \pmod{15}$$

$$3k_1 \equiv 3 \pmod{15}$$

$$k_1 \equiv 1 \pmod{5}$$

แสดงว่า $k_1 = 5k_2 + 1$ โดยที่ k_2 เป็นจำนวนเต็ม

จะได้ $x = 3(5k_2 + 1) + 2 = 15k_2 + 5$

แทนค่า $x = 15k_2 + 5$ ใน $x \equiv 8 \pmod{12}$ จะได้

$$15k_2 + 5 \equiv 8 \pmod{12}$$

$$15k_2 \equiv 3 \pmod{12}$$

$$k_2 \equiv 1 \pmod{4}$$

แสดงว่า $k_2 = 4k_3 + 1$ เมื่อ k_3 เป็นจำนวนเต็ม

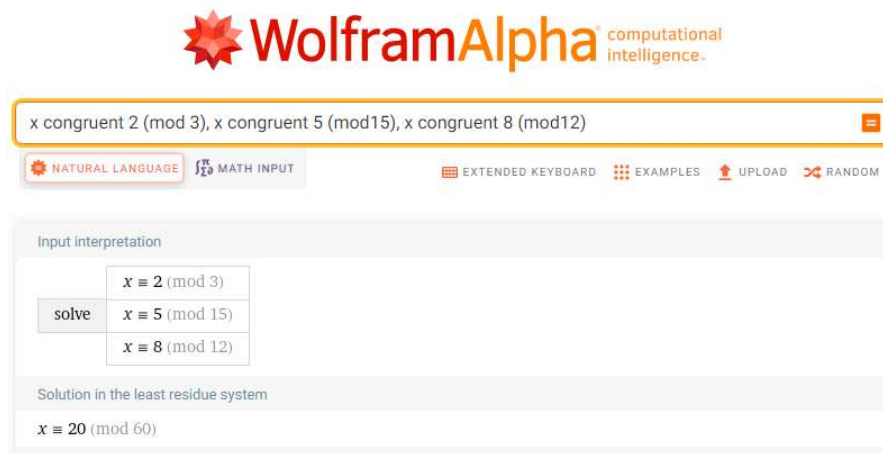
แทนค่า k_2 ใน $x = 15k_2 + 5$

จะได้ $x = 15(4k_3 + 1) + 5 = 60k_3 + 20$

นั่นคือ $x \equiv 20 \pmod{60}$ เป็นผลเฉลยของระบบสมภาคเชิงเส้น

ดังนั้น ผลเฉลยของระบบสมภาคเชิงเส้นคือ $x \equiv 20 \pmod{60}$

จากตัวอย่าง 4.34 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้น
 ดังภาพประกอบ 4.12



ภาพประกอบ 4.12 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของระบบสมภาคเชิงเส้น

4.5 สรุปท้ายบทที่ 4

a สมภาคกับ b มอดุโล m เขียนแทนด้วยสัญลักษณ์ $a \equiv b \pmod{m}$ หมายความว่า $m \mid a - b$ แสดงว่า $a = mk + b$ สำหรับบางจำนวนเต็ม k และในทางตรงข้าม a ไม่สมภาคกับ b มอดุโล m เขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{m}$ หมายความว่า $m \nmid (a - b)$ โดยเรียกจำนวนเต็ม m ว่าเป็นมอดุโลของสมภาค นอกจากนี้ยังพบว่า $a \equiv b \pmod{m}$ ก็ต่อเมื่อ a และ b มีเศษเหลือที่ไม่เป็นลบจากการหารด้วย n เท่ากัน จากคุณสมบัตินี้สามารถนำไปแก้ปัญหการหารลงตัวได้หลากหลายรูปแบบ เนื่องจากสมภาคมีคุณสมบัติที่คล้ายกับสมการ เช่น การบวก การคูณ ด้วยจำนวนที่เท่ากันทั้งสองข้าง และยังมีสมบัติต่าง ๆ เพิ่มเข้ามาเพื่อช่วยในการหาผลเฉลยสมภาคเชิงเส้นที่มีหนึ่งตัวแปร และจากทฤษฎีบทเศษเหลือของจีนทำให้สามารถหาผลเฉลยของระบบสมภาคเชิงเส้นได้แต่ยังอยู่ภายใต้ข้อจำกัดที่ว่าระบบสมภาคต้องมีมอดุโลเป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ และสัมประสิทธิ์ของตัวแปรในแต่ละสมภาคต้องเป็นหนึ่งเท่านั้น สำหรับการหารระบบสมภาคเชิงเส้นนอกเหนือจากข้อจำกัดดังกล่าว และมีเพียงแค่สองสมภาคที่อยู่ในรูปแบบ $x \equiv a_1 \pmod{m_1}$ และ $x \equiv a_2 \pmod{m_2}$ พบว่าระบบสมภาคจะมีผลเฉลยก็ต่อเมื่อ $(m_1, m_2) \mid (a_2 - a_1)$ ถ้าระบบสมภาคเชิงเส้นมีผลเฉลยแล้วผลเฉลยจะอยู่ในรูป $x \equiv x_0 \pmod{[m_1, m_2]}$ และผลเฉลยมีเพียงผลเฉลยเดียวสำหรับการหาผลเฉลยของสมภาคเชิงเส้นที่มากกว่าสองสมภาคที่อยู่ในรูปแบบ $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_n \pmod{m_n}$ ระบบสมภาคจะมีผลเฉลยก็ต่อเมื่อ $(m_i, m_j) \mid (a_j - a_i)$ สำหรับทุก i, j และถ้าคำตอบหนึ่งเป็น x_0 แล้วคำตอบทั่วไปคือ $x \equiv x_0 \pmod{[m_1, m_2, \dots, m_n]}$

แบบฝึกหัดท้ายบทที่ 4

1. พิจารณาข้อความต่อไปนี้ว่า จริงหรือเท็จ พร้อมบอกเหตุผล
 - 1.1 $385 \equiv 322(\text{mod } 3)$
 - 1.2 $-385 \equiv -322(\text{mod } 3)$
 - 1.3 ถ้า $12x \equiv 15(\text{mod } 35)$ แล้ว $4x \equiv 5(\text{mod } 7)$
 - 1.4 ถ้า $2x \equiv 8(\text{mod } 7)$ แล้ว $x \equiv 4(\text{mod } 7)$
 - 1.5 ถ้า $3x \equiv 12y(\text{mod } 21)$ แล้ว $x \equiv 3y(\text{mod } 7)$
2. จงหาเศษเหลือที่ได้จากการหาร จำนวนในแต่ละข้อต่อไปนี้
 - 2.1 20^{50} หารด้วย 7
 - 2.2 41^{65} หารด้วย 7
 - 2.3 7^{10} หารด้วย 51
 - 2.4 5^{21} หารด้วย 127
 - 2.5 $1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5$ หารด้วย 4
3. ให้ n หารด้วย 9 เหลือเศษ 5 จงหาเศษจากการหาร $n(n^2 + 7n - 2)$ ด้วย 9
4. จงพิสูจน์ว่า $n^5 - n$ หารด้วย 5 ลงตัว สำหรับแต่ละจำนวนเต็ม n
5. จงพิสูจน์ว่า $n(n^2 + 5)$ หารด้วย 6 ลงตัว สำหรับแต่ละจำนวนเต็ม n
6. จงหาผลเฉลยของสมภาคเชิงเส้นต่อไปนี้
 - 6.1 $2x \equiv 5(\text{mod } 7)$
 - 6.2 $7x \equiv 3(\text{mod } 11)$
 - 6.3 $2x \equiv 7(\text{mod } 9)$
 - 6.4 $35x \equiv 5(\text{mod } 7)$
 - 6.5 $6x \equiv 15(\text{mod } 21)$
 - 6.6 $9x \equiv 15(\text{mod } 100)$
 - 6.7 $15x \equiv 14(\text{mod } 21)$
 - 6.8 $2x \equiv 6(\text{mod } 12)$
7. จงหาตัวผกผันต่อไปนี้
 - 7.1 ตัวผกผัน 3 โมดูล 5
 - 7.2 ตัวผกผัน 5 โมดูล 21
 - 7.3 ตัวผกผัน 11 โมดูล 12
 - 7.4 ตัวผกผัน 13 โมดูล 100
 - 7.5 ตัวผกผัน 3 โมดูล 101
 - 7.6 ตัวผกผัน -3 โมดูล 10
 - 7.7 ตัวผกผัน -11 โมดูล
 - 7.8 ตัวผกผัน -7 โมดูล 80

8. จงหาผลเฉลยของระบบสมภาคเชิงเส้น ต่อไปนี้

$$\begin{aligned} 8.1 \quad x &\equiv 5(\text{mod } 7) \\ x &\equiv 7(\text{mod } 11) \end{aligned}$$

$$\begin{aligned} 8.2 \quad x &\equiv 2(\text{mod } 6) \\ x &\equiv 5(\text{mod } 9) \end{aligned}$$

$$\begin{aligned} 8.3 \quad 2x &\equiv 1(\text{mod } 3), \\ 3x &\equiv 2(\text{mod } 5) \\ 5x &\equiv 4(\text{mod } 7) \end{aligned}$$

$$\begin{aligned} 8.4 \quad x &\equiv 3(\text{mod } 2) \\ x &\equiv 2(\text{mod } 3) \\ x &\equiv 4(\text{mod } 5) \end{aligned}$$

$$\begin{aligned} 8.5 \quad x &\equiv 3(\text{mod } 5) \\ x &\equiv 4(\text{mod } 7) \\ x &\equiv 7(\text{mod } 9) \end{aligned}$$

$$\begin{aligned} 8.6 \quad x &\equiv 3(\text{mod } 4) \\ x &\equiv 2(\text{mod } 7) \\ x &\equiv 7(\text{mod } 11) \end{aligned}$$

$$\begin{aligned} 8.7 \quad x &\equiv 3(\text{mod } 4) \\ x &\equiv 2(\text{mod } 5) \\ x &\equiv 5(\text{mod } 6) \end{aligned}$$

$$\begin{aligned} 8.8 \quad x &\equiv 2(\text{mod } 3) \\ x &\equiv 3(\text{mod } 7) \\ x &\equiv 7(\text{mod } 10) \end{aligned}$$