

บทที่ 6

ทฤษฎีบทสมภาค

สมภาคเป็นเรื่องเกี่ยวกับการหารลงตัวที่ได้ศึกษาในบทที่ผ่านมาแล้วนั้นเป็นที่ยอมรับกันว่าสมภาคนั้นเป็นพื้นฐานที่สำคัญในการศึกษาทฤษฎีจำนวน เพราะสามารถนำอธิบายสมบัติของการหารลงตัวได้อย่างสะดวก เข้าใจได้ง่าย ความสัมพันธ์นี้ช่วยให้สามารถตอบปัญหาในสิ่งที่ต้องคิดคำนวณซับซ้อนทำให้สามารถคำนวณได้ง่ายขึ้น และยังเป็นแนวทางนำไปสู่เรื่องราวที่น่าสนใจใหม่ ๆ อีกมากมาย แต่การนำสมภาคมาแก้ปัญหาบางอย่าง หรือการนำสมภาคไปพัฒนาในเรื่องทฤษฎีจำนวนนั้น จำเป็นต้องศึกษาทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องสมภาคให้มากขึ้น เพื่อให้เกิดความสะดวกและรวดเร็วในการแก้ปัญหาในรูปแบบต่าง ๆ เช่นการหาผกผันในมอดุโลต่าง ๆ ที่ได้ศึกษาในบทที่ผ่านมาพบว่ามีขั้นตอนที่ยุ่งยากและซับซ้อน ซึ่งการหาผกผันมอดุโลก็เป็นเครื่องมือที่สำคัญอีกอย่างในการหาผลเฉลยของสมภาคเชิงเส้นสำหรับในบทนี้จะเป็นการศึกษาทฤษฎีบทที่เกี่ยวข้องกับสมภาคสำหรับนำไปแก้ปัญหาสมภาคในรูปแบบต่าง ๆ ดังนี้ ทฤษฎีบทน้อยของแฟร์มา(Fermat's Little Theorem) ทฤษฎีบทวิลสัน(Wilson's Theorem) จำนวนเฉพาะเทียม(Pseudoprime) และทฤษฎีบทออยเลอร์(Euler's Theorem)

6.1 ทฤษฎีบทเล็กแฟร์มา

ในปี ค.ศ. 1640 นักคณิตศาสตร์ชาวฝรั่งเศสชื่อ ปีแยร์ เดอ แฟร์มา(Pierre de Fermat) ได้ส่งจดหมายถึงเพื่อนซึ่งเป็นนักคณิตศาสตร์ชาวฝรั่งเศสชื่อ เบอ์นาร์ต แฟร์นิเคิล เดอ เบสซี(Bernard Frénicle de Bessy) โดยมีข้อความในจดหมายว่า “จำนวนเฉพาะ p หาร $a^{p-1} - 1$ ลงตัวเมื่อ a เป็นจำนวนเต็มใด ๆ ซึ่งหาร ด้วย p ไม่ลงตัว” แต่แฟร์มาไม่ได้เขียนวิธีพิสูจน์ไว้ในจดหมาย จนกระทั่งในปี ค.ศ. 1736 เลออนฮาร์ด ออยเลอร์(Leonhard Euler) ได้เป็นผู้พิสูจน์ทฤษฎีบทนี้เป็นคนแรก และเป็นที่รู้จักกันในนามทฤษฎีบทเล็กแฟร์มา

ทฤษฎีบท 6.1 (ทฤษฎีบทเล็กแฟร์มา)

กำหนดให้ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็ม ถ้า $p \nmid a$
แล้ว $a^{p-1} \equiv 1 \pmod{p}$

พิสูจน์

กำหนดให้ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็ม ซึ่ง $p \nmid a$

พิจารณาจำนวนเต็ม

$a, 2a, 3a, \dots, (p-1)a$ ซึ่งมี $(p-1)$ จำนวน

จะได้ว่า $p \nmid ia$ ทุก $i = 1, 2, \dots, p-1$

เนื่องจาก ถ้า $p \mid ia$ จะได้ว่า $p \mid i$ หรือ $p \mid a$ ซึ่งเป็นไปไม่ได้

ต่อไปพบว่าทุกคู่ของ $a, 2a, 3a, \dots, (p-1)a$ ไม่สมภาคกันในมอดุโล p แสดง

เนื่องจาก $p \nmid a$ จะได้ $(p, a) = 1$ ดังนั้นจะมี i, j โดยที่ $ia \equiv ja \pmod{p}$

จะได้ $i \equiv j \pmod{p}$ ส่งผลให้ $i = j$ เนื่องจาก $i, j \in \{1, 2, 3, \dots, p-1\}$

และเพราะว่า $a, 2a, 3a, \dots, (p-1)a$ ไม่มีจำนวนใดที่อยู่ในชั้นเดียวกับ 0 ในมอดุโล p

จึงได้ว่าส่วนตกค้างที่เล็กที่สุดของ $a, 2a, 3a, \dots, (p-1)a$ แต่ละจำนวนจะต้องเป็น

จำนวนหนึ่งและจำนวนเดียวเท่านั้นใน $1, 2, 3, \dots, (p-1)$

จึงได้ว่า

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

หรือ

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$$

เนื่องจาก $((p-1)!, p) = 1$ จะได้ว่า $a^{p-1} \equiv 1 \pmod{p}$

ตัวอย่าง 6.1 จงแสดงว่า $4^4 \equiv 1 \pmod{5}$

วิธีทำ เนื่องจาก

$$\begin{array}{ll} 1 \cdot 4 \equiv 4 \pmod{5} & 3 \cdot 4 \equiv 2 \pmod{5} \\ 2 \cdot 4 \equiv 3 \pmod{5} & 4 \cdot 4 \equiv 1 \pmod{5} \end{array}$$

คูณสมภาคเหล่านี้เข้าด้วยกัน จะได้

$$(1 \cdot 4)(2 \cdot 4)(3 \cdot 4)(4 \cdot 4) \equiv (4 \cdot 3 \cdot 2 \cdot 1) \pmod{5}$$

หรือ

$$4^4 (1 \cdot 2 \cdot 3 \cdot 4) \equiv (1 \cdot 2 \cdot 3 \cdot 4) \pmod{5}$$

จะได้ $4^4 \cdot 4! \equiv 4! \pmod{5}$

หรือ $4^4 \equiv 1 \pmod{5}$

ดังนั้น $4^4 \equiv 1 \pmod{5}$

ในตัวอย่าง 6.1 การตรวจสอบว่า $4^4 \equiv 1 \pmod{5}$ สามารถใช้ทฤษฎีบทเล็กแฟร์มา ได้โดยตรง เนื่องจาก 5 จำนวนเฉพาะและ 4 เป็นจำนวนเต็ม ที่โดยที่ $5 \nmid 4$ นอกจากนี้ทฤษฎีบทเล็กแฟร์มายังสามารถนำไปแก้ปัญหาก็เกี่ยวข้องกันสมภาคในรูปแบบต่าง ๆ ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.2 จงหาเศษเหลือที่เกิดจากการหาร 12^{7113} ด้วย 29

วิธีทำ เนื่องจาก $7113 = 28(254) + 1$ จะได้

$$12^{7113} = 12^{28(254)+1} = 12^{28(254)} \cdot 12$$

เนื่องจาก 29 จำนวนเฉพาะและ 12 เป็นจำนวนเต็ม ที่โดยที่ $29 \nmid 12$

โดยทฤษฎีบทเล็กแฟร์มาจะได้

$$12^{28} \equiv 1 \pmod{29}$$

นั่นคือ $12^{28(254)} \equiv 1 \pmod{29}$

และเนื่องจาก $12 \equiv 12 \pmod{29}$

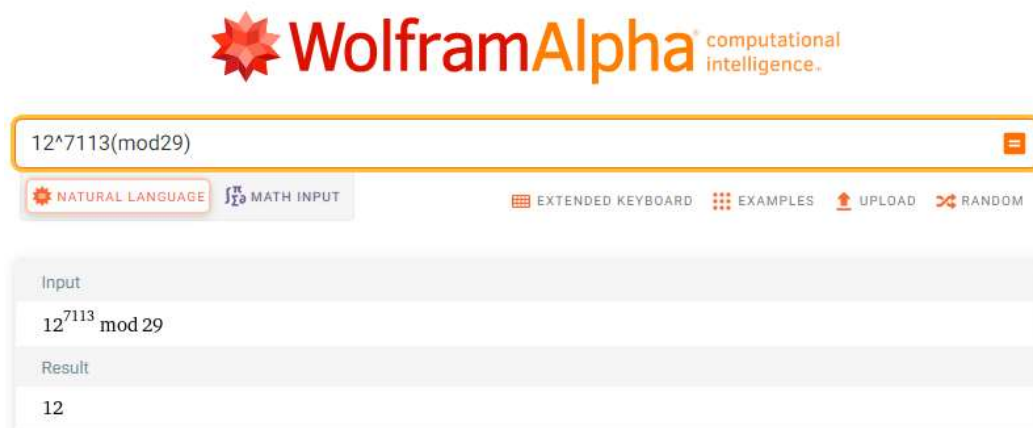
จะได้

$$\begin{aligned} 12^{7113} &= 12^{28(254)+1} \\ &= 12^{28(254)} \cdot 12 \\ &\equiv 1 \cdot 12 \pmod{29} \\ &\equiv 12 \pmod{29} \end{aligned}$$

ดังนั้น เศษที่เกิดจากการหาร 12^{7113} ด้วย 29 คือ 12

จากตัวอย่าง 6.2 ใช้ Wolfram Alpha หาเศษที่เกิดจากการหาร 12^{7113} ด้วย 29

ดังภาพประกอบ 6.1



ภาพประกอบ 6.1 ใช้ Wolfram Alpha เพื่อแสดงเศษที่เกิดจากการหาร 12^{7113} ด้วย 29 คือ 12

จากทฤษฎีบทเล็กแฟร์มาถ้าตัดเงื่อนไข $p \nmid a$ สำหรับการขยายไปสู่กรณีที่จำนวนเต็ม a ที่เป็นจำนวนเฉพาะสัมพันธ์กับจำนวนเฉพาะ p ดังแสดงในรูปแบบบทแทรกต่อไปนี้

บทแทรก 6.1

กำหนดให้ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็มใด ๆ
 จะได้ว่า $a^p \equiv a \pmod{p}$

พิสูจน์

กำหนดให้ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็มใด ๆ

ถ้า $p \mid a$ แล้วจะได้ $p \mid a^p$ ดังนั้น $a^p \equiv a \equiv 0 \pmod{p}$

ถ้า $p \nmid a$ จากทฤษฎีบทเล็กแฟร์มาทราบว่า $a^{p-1} \equiv 1 \pmod{p}$

คูณด้วย a ทั้งสองข้างของสมภาคจะได้ $a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p}$

นั่นคือ $a^p \equiv a \pmod{p}$

บทแทรก 6.1 สามารถนำไปแก้ปัญหาก็เกี่ยวข้องกัสมภาคในรูปแบบต่าง ๆ ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.3 จงแสดงว่า $8^{68} + 9^{18} \equiv 12 \pmod{17}$

วิธีทำ เนื่องจาก $68 = (17)(4)$ และ $18 = (17)(1) + 1$ แสดงว่า

$$8^{68} = 8^{(17)(4)} \text{ และ } 9^{18} = 9^{(17)(1)+1}$$

จากบทแทรก 6.1 จะได้

$$8^{17} \equiv 8 \pmod{17} \text{ และ } 9^{17} \equiv 9 \pmod{17}$$

แสดงว่า

$$\begin{aligned} 8^{68} + 9^{18} &= 8^{(17)(4)} + 9^{(17)(1)+1} \\ &= 8^{(17)(4)} + 9^{(17)(1)} \cdot 9 \\ &\equiv 8^4 + 9 \cdot 9 \pmod{17} \\ &\equiv 8^2 \cdot 8^2 + 9^2 \pmod{17} \\ &\equiv (-4)(-4) + 13 \pmod{17} \\ &\equiv 16 + 13 \pmod{17} \\ &\equiv 12 \pmod{17} \end{aligned}$$

ดังนั้น $8^{68} + 9^{18} \equiv 12 \pmod{17}$

ตัวอย่าง 6.4 จงหาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ 3^{29} มอดุโล 13

วิธีทำ เนื่องจาก $29 = 13(2) + 3$ แสดงว่า

$$3^{29} = 3^{13(2)+3} = 3^{13(2)} \cdot 3^3$$

จากบทแทรก 6.1 จะได้

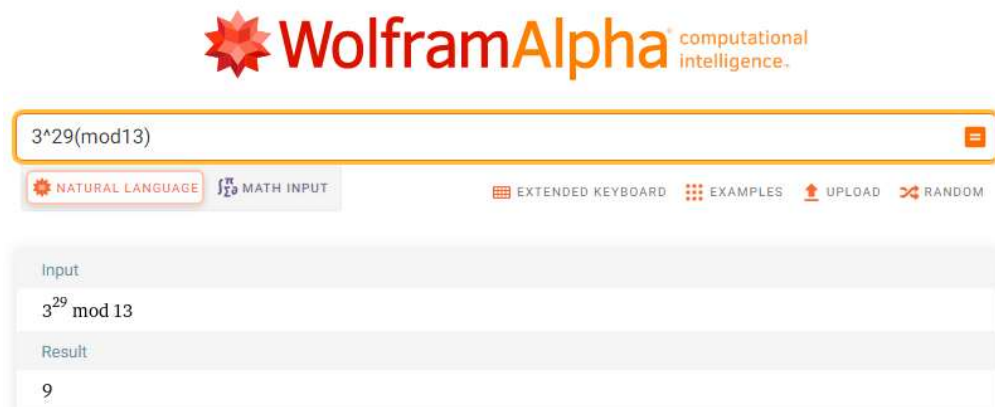
$$3^{13} \equiv 3 \pmod{13}$$

แสดงว่า

$$\begin{aligned} 3^{29} &= 3^{13(2)} \cdot 3^3 \\ &\equiv 3^2 \cdot 3^3 \pmod{13} \\ &\equiv 3^2 \cdot 1 \pmod{13} \\ &\equiv 9 \pmod{13} \end{aligned}$$

ดังนั้น 9 เป็นส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ 3^{29} มอดุโล 13

จากตัวอย่าง 6.4 ใช้ Wolfram Alpha หาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ 3^{29} มอดุโล 13 ดังภาพประกอบ 6.2



ภาพประกอบ 6.2 ใช้ Wolfram Alpha เพื่อแสดงว่า 9 เป็นส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ 3^{29} มอดุโล 13

ทฤษฎีบทเล็กแฟร์มาสามารถนำมาประยุกต์ใช้ในการหาตัวผกผันของจำนวนเต็มมอดุโลที่เป็นจำนวนเฉพาะได้ ดังทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 6.2

ถ้า p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็ม โดยที่ $p \nmid a$ แล้ว a^{p-2} เป็นผกผันของ a มอดุโล p

พิสูจน์

เนื่องจาก $p \nmid a$ โดยทฤษฎีบทเล็กแฟร์มา จะได้ว่า

$$a^{p-1} \equiv 1 \pmod{p}$$

แสดงว่า

$$a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$$

ดังนั้น a^{p-2} เป็นตัวผกผันของ a โมดูล p

ตัวอย่าง 6.5 จงหาผกผันของ 2 โมดูล 11

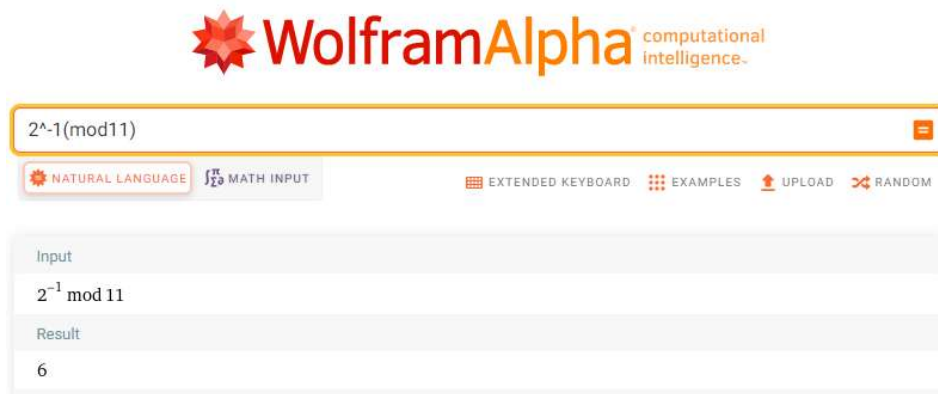
วิธีทำ เนื่องจาก $11 \nmid 2$ จะได้

$$2^{11-2} = 2^9 = 512 \equiv 6 \pmod{11}$$

นั่นคือ $2^{11-2} \equiv 6 \pmod{11}$

ดังนั้น ผกผันของ 2 โมดูล 11 คือ 6

จากตัวอย่าง 6.5 ใช้ Wolfram Alpha เพื่อหาตัวผกผันของ 2 โมดูล 11 แสดงได้ดังภาพประกอบ 6.3



ภาพประกอบ 6.3 ใช้ Wolfram Alpha เพื่อแสดงว่า 6 เป็นผกผันของ 2 โมดูล 11

ในบทที่ผ่านมาว่าผกผันนั้นเป็นเครื่องมือที่สำคัญอีกอย่างหนึ่งในการหาผลเฉลยของสมภาคเชิงเส้น (Linear Congruence) และทฤษฎีบท 6.4 ก็เป็นวิธีการหาผกผันที่ง่ายสะดวก และรวดเร็วทำให้สามารถหาผลเฉลยของสมภาคเชิงเส้นได้สะดวกมากยิ่งขึ้นดังที่แสดงในตัวอย่างต่อไปนี้

ตัวอย่าง 6.6 จงหาผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{17}$

วิธีทำ ดำเนินการหาผกผันของ 6 โมดูล 17 ดังนี้

เนื่องจาก $17 \nmid 6$ จะได้

$$6^{17-2} = 6^{15} = 6^{2(7)+1} = 6^{2(7)} \cdot 6 \equiv 2^7 \cdot 6 \pmod{17} \equiv 3 \pmod{17}$$

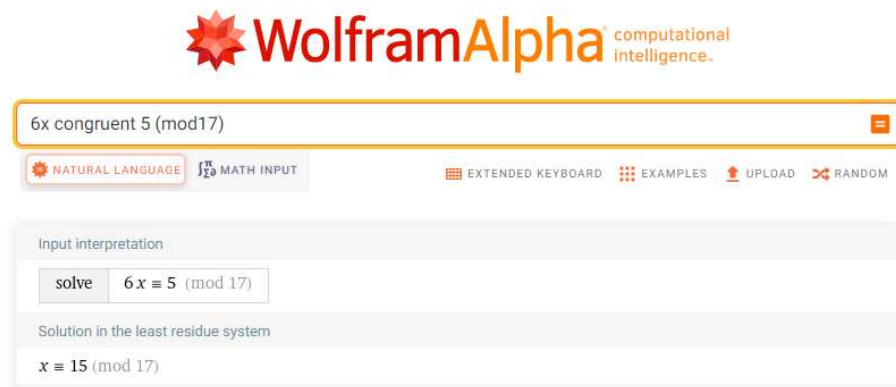
แสดงว่าผกผันของ 6 โมดูล 17 คือ 3

คูณทั้งสองข้างของสมภาคด้วย 3 จะได้

$$\begin{aligned}(3)6x &\equiv (3)5 \pmod{17} \\ x &\equiv 15 \pmod{23}\end{aligned}$$

ดังนั้น ผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{17}$ คือ $x \equiv 15 \pmod{17}$

จากตัวอย่าง 6.6 ใช้ Wolfram Alpha เพื่อหาผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{17}$ ดังภาพประกอบ 6.4



ภาพประกอบ 6.4 ใช้ Wolfram Alpha เพื่อแสดงว่า $x \equiv 15 \pmod{17}$ เป็นผลเฉลยของสมภาคเชิงเส้น $6x \equiv 5 \pmod{17}$

การหาผลเฉลยของสมภาคเชิงเส้นนั้นจากทฤษฎีบทเล็กแฟร์มา ในตัวอย่างที่ผ่านมานั้นเป็นอีกหนึ่งวิธี ต่อไปจะเป็นการหาผลเฉลยของสมภาคเชิงเส้นมอดุโลจำนวนเฉพาะ โดยนำเสนอเป็นบทแทรกดังต่อไปนี้

บทแทรก 6.2

ถ้า a และ b เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะโดยที่ $p \nmid a$ แล้ว ผลเฉลยของสมภาคเชิงเส้น $ax \equiv b \pmod{p}$ คือจำนวนเต็ม x โดยที่ $x \equiv a^{p-2}b \pmod{p}$

พิสูจน์

ให้ $ax \equiv b \pmod{p}$ เนื่องจาก $p \nmid a$

จากทฤษฎีบท 6.4 จะได้ว่า a^{p-2} เป็นผกผัน ของ a มอดุโล p

คูณทั้งสองข้างของสมภาค $ax \equiv b \pmod{p}$ ด้วย a^{p-2} จะได้

$$a^{p-2}ax \equiv a^{p-2}b \pmod{p}$$

ดังนั้น

$$x \equiv a^{p-2}b \pmod{p}$$

ตัวอย่าง 6.7 จงหาผลเฉลยของสมภาคเชิงเส้น $7x \equiv 12 \pmod{17}$

วิธีทำ จากสมภาคเชิงเส้นจะได้ว่า

$$a = 7, b = 12 \text{ และ } p = 17$$

เนื่องจาก $7 \nmid 17$

แสดงว่าผลเฉลยของสมภาคดังกล่าวคือ $x \equiv a^{p-2}b \pmod{p}$

$$x \equiv 7^{15} \cdot 12 \pmod{17} \equiv (7^3)^5 \cdot 12 \pmod{17}$$

เนื่องจาก $7^3 \equiv 3 \pmod{17}$

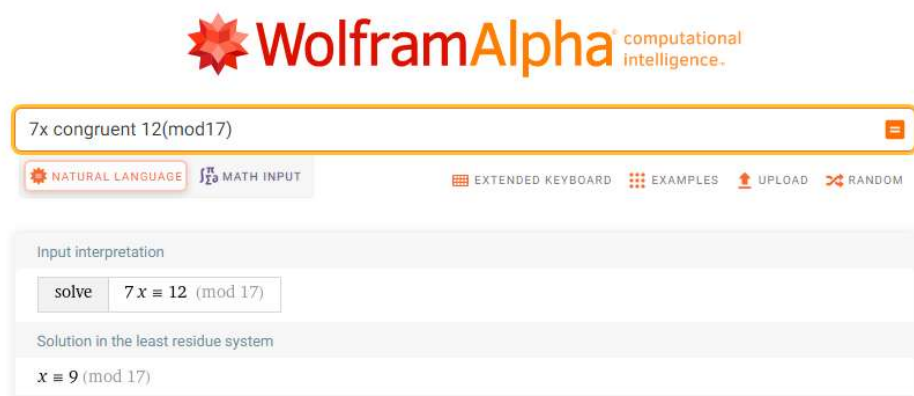
จะได้

$$\begin{aligned} x &\equiv (3)^5 \cdot 12 \pmod{17} \\ &\equiv 243 \cdot 12 \pmod{17} \\ &\equiv 5 \cdot 12 \pmod{17} \\ &\equiv 60 \pmod{17} \\ &\equiv 9 \pmod{17} \end{aligned}$$

ดังนั้น ผลเฉลยของสมภาคเชิงเส้น $7x \equiv 12 \pmod{17}$ คือ $x \equiv 9 \pmod{17}$

จากตัวอย่าง 6.7 ใช้ Wolfram Alpha ผลเฉลยของสมภาคเชิงเส้น $7x \equiv 12 \pmod{17}$

ดังภาพประกอบ 6.5



ภาพประกอบ 6.5 ใช้ Wolfram Alpha เพื่อแสดงว่า $x \equiv 9 \pmod{17}$ เป็นผลเฉลยของสมภาคเชิงเส้น $7x \equiv 12 \pmod{17}$

6.2 ทฤษฎีบทวิลสัน

เอ็ดเวิร์ด วอร์นนิ่ง(Edward Waring) นักคณิตศาสตร์ชาวอังกฤษ ได้กล่าวไว้ในหนังสือและได้ตีพิมพ์ในปี ค.ศ. 1770 ว่าศิษย์ของเขาชื่อ จอห์น วิลสัน(John Wilson) ได้ตั้งข้อคาดการณ์ไว้ว่า ถ้า p เป็นจำนวนเฉพาะ แล้ว p หาร $(p-1)!+1$ ลงตัว แนวคิดพื้นฐานมาจากการคำนวณ ซึ่งวิลสันสังเกตว่า

$$2 \text{ หาร } (1-1)!+1 = 2$$

$$3 \text{ หาร } (3-1)!+1 = 3$$

$$5 \text{ หาร } (5-1)!+1 = 25$$

$$7 \text{ หาร } (7-1)!+1 = 721$$

อย่างไรก็ตามทั้งวอร์นนิ่งและวิลสันไม่สามารถพิสูจน์ข้อความคาดการณ์นี้ได้ จนกระทั่งปี ค.ศ. 1771 นักคณิตศาสตร์ชาวอิตาลี ชื่อ โฌแซ็ฟ หลุยส์ ลากร็องฌ์(Joseph-Louis Lagrange) ได้พิสูจน์ข้อความดังกล่าวนี้ได้สำเร็จ และเรียก ทฤษฎีบทดังกล่าวว่า ทฤษฎีบทวิลสัน (Rosen, 2014 : 215-216)

ทฤษฎีบท 6.3 (ทฤษฎีบทวิลสัน)

ถ้า p เป็นจำนวนเฉพาะ จะได้ว่า $(p-1)! \equiv -1 \pmod{p}$

พิสูจน์

กรณีที่ 1 เมื่อ $p = 2$ พิจารณาค่าของ $(p-1)!$ จะได้ $(2-1)! = 1! = 1$

และเนื่องจาก $1 \equiv -1 \pmod{2}$ ดังนั้นทฤษฎีบทนี้เป็นจริงสำหรับ $p = 2$

กรณีที่ 2 เมื่อ p เป็นจำนวนเฉพาะ และ $p > 2$

พิจารณาเซตของจำนวนเต็ม $S = \{1, 2, 3, \dots, p-1\}$

เนื่องจาก p เป็นจำนวนเฉพาะ ดังนั้นสำหรับทุกจำนวนเต็ม $a \in S$

จะมีตัวผกผันการคูณ $\bar{a} \in S$ เพียงตัวเดียวเสมอ ที่ทำให้

$$a\bar{a} \equiv 1 \pmod{p}$$

พิจารณาสมาชิก a ที่เป็นตัวผกผันของตนเอง $a = \bar{a}$ โดยการหา

ผลเฉลยของสมการสมภาค

$$a^2 \equiv 1 \pmod{p}$$

$$a^2 - 1 \equiv 0 \pmod{p}$$

$$(a-1)(a+1) \equiv 0 \pmod{p}$$

เนื่องจาก p เป็นจำนวนเฉพาะ ดังนั้น $p \nmid (a-1)$ หรือ $p \nmid (a+1)$ แสดงว่า

$$a-1 \equiv 0 \pmod{p} \text{ นั่นคือ } a \equiv 1 \pmod{p}$$

$$a+1 \equiv 0 \pmod{p} \text{ นั่นคือ } a \equiv -1 \pmod{p} \equiv p-1 \pmod{p}$$

ดังนั้นในเซต S มีเพียง 1 และ $p-1$ เท่านั้นที่เป็นตัวผกผันของตัวเอง

ส่วนสมาชิกที่เหลืออีก $p - 3$ ตัว ในเซต $\{2, 3, \dots, p - 2\}$ สามารถจับคู่กันเป็นคู่ ๆ โดยที่แต่ละคู่คูณกันได้ 1 เสมอดังนั้น เมื่อพิจารณาค่า $(p - 1)!$ จะได้

$$(p - 1)! \equiv 1 \cdot (2 \cdot 3 \cdots (p - 2)) (p - 1)$$

เนื่องจากพจน์ตรงกลางจับคู่คูณกันได้ 1 ทั้งหมด จะได้ว่า

$$\begin{aligned} (p - 1)! &\equiv 1 \cdot (1) (p - 1) \pmod{p} \\ &\equiv p - 1 \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

ตัวอย่าง 6.8 จงแสดงว่า $10! \equiv -1 \pmod{11}$

วิธีทำ เนื่องจาก $p = 11$ เป็นจำนวนเฉพาะ จะได้ว่า

$$\begin{aligned} (11 - 1)! &= 1 \cdot [2 \cdot 3 \cdot 4 \cdots 8 \cdot 9] \cdot 10 \equiv 1 \cdot 1 \cdot 10 \pmod{11} \\ &\equiv 10 \pmod{11} \\ &\equiv -1 \pmod{11} \end{aligned}$$

สามารถใช้ทฤษฎีบทวิลสันหาได้โดยตรงนั่นคือ $10! = (11 - 1)! \equiv -1 \pmod{11}$

ดังนั้น $10! \equiv -1 \pmod{11}$

ตัวอย่าง 6.9 จงใช้ทฤษฎีบทวิลสันเพื่อหาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ $22!$ มอดุโล 23

วิธีทำ เนื่องจาก $p = 23$ เป็นจำนวนเฉพาะ

จากทฤษฎีบทวิลสันจะได้

$$(23 - 1)! \equiv -1 \pmod{23} \equiv 22 \pmod{23}$$

ดังนั้น ส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ $22!$ มอดุโล 23 คือ 22

จากตัวอย่าง 6.9 ใช้ Wolfram Alpha หาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ $22!$ มอดุโล 23 ดังภาพประกอบ 6.6



ภาพประกอบ 6.6 ใช้ Wolfram Alpha เพื่อแสดงส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ $22!$ มอดุโล 23 คือ 22

สำหรับตัวอย่างที่ผ่านมาเป็นการใช้ทฤษฎีบทวิลสันแก้ปัญหาโดยตรง แต่สำหรับตัวอย่างต่อไป จะเป็นการประยุกต์ทฤษฎีบทดังกล่าวสำหรับนำมาแก้ปัญหา

ตัวอย่าง 6.10 จงหาเศษจากการหาร $109 + 18!$ ด้วย 19

วิธีทำ เนื่องจาก 19 เป็นจำนวนเฉพาะ

จากทฤษฎีบทวิลสันจะได้ว่า

$$18! \equiv -1 \pmod{19}$$

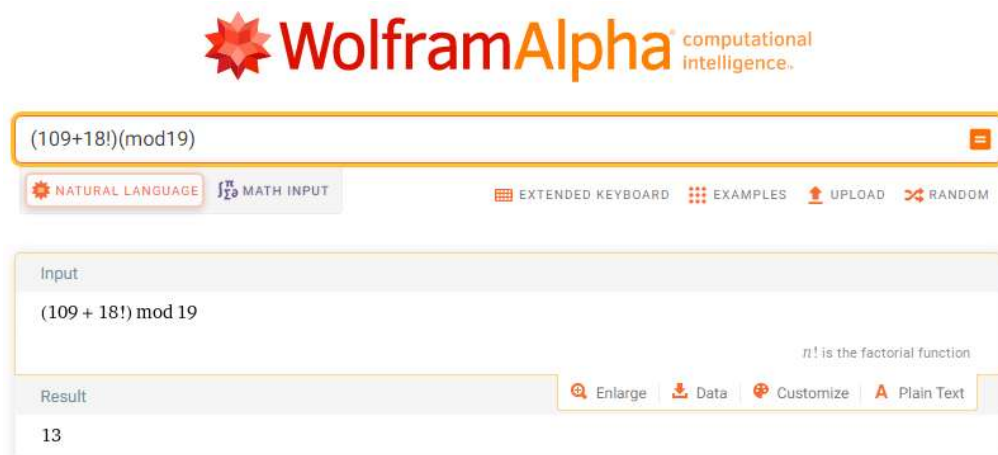
และ $109 \equiv 14 \pmod{19}$

แสดงว่า

$$\begin{aligned} 109 + 18! &\equiv 14 - 1 \pmod{19} \\ &\equiv 13 \pmod{19} \end{aligned}$$

ดังนั้น เศษจากการหาร $109 + 18!$ ด้วย 19 คือ 13

จากตัวอย่าง 6.10 ใช้ Wolfram Alpha หาเศษจากการหาร $109 + 18!$ ด้วย 19
ดังภาพประกอบ 6.7



ภาพประกอบ 6.7 ใช้ Wolfram Alpha เพื่อแสดงว่าเศษจากการหาร $109 + 18!$ ด้วย 19 คือ 13

ตัวอย่าง 6.11 จงหาเศษจากการหาร $14!$ ด้วย 13

วิธีทำ เนื่องจาก $14! = 14 \cdot 13 \cdot 12!$

13 เป็นจำนวนเฉพาะ จากทฤษฎีบทวิลสันจะได้

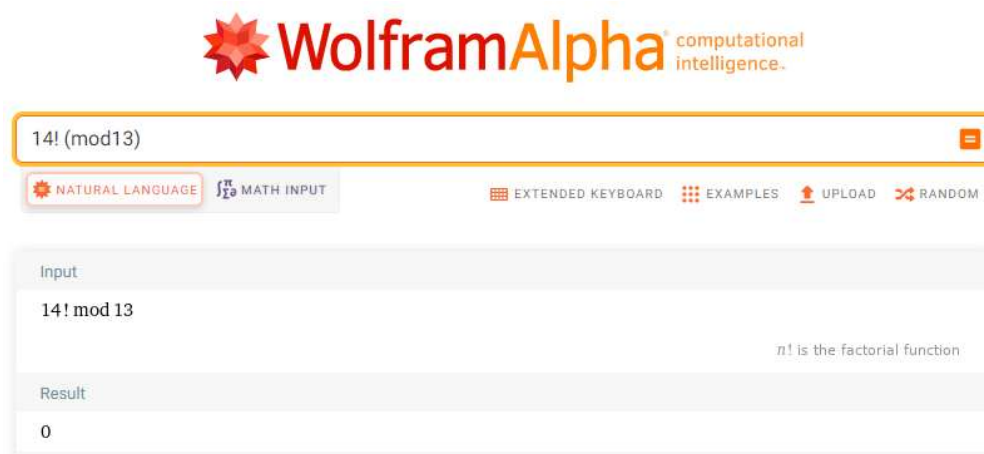
$$(13 - 1)! = 12! \equiv -1 \pmod{13} \equiv 12 \pmod{13}$$

เนื่องจาก $14 \equiv 1 \pmod{13}$ และ $13 \equiv 0 \pmod{13}$ แสดงว่า

$$\begin{aligned}
 14 \cdot 13 \cdot 12! &\equiv 1 \cdot 0 \cdot 12! \pmod{13} \\
 &\equiv 0 \pmod{13}
 \end{aligned}$$

ดังนั้น เศษจากการหาร $14!$ ด้วย 13 คือ 0

จากตัวอย่าง 6.11 ใช้ Wolfram Alpha หาเศษจากการหาร $14!$ ด้วย 13 ดังภาพประกอบ 6.8



ภาพประกอบ 6.8 ใช้ Wolfram Alpha เพื่อแสดงเศษจากการหาร $14!$ ด้วย 13 คือ 0

ตัวอย่าง 6.12 จงหาเศษจากการหาร $57!$ ด้วย 61

วิธีทำ พิจารณา $60! = 60 \cdot 59 \cdot 58 \cdot 57!$ และ เนื่องจาก

$$\begin{aligned}
 60 &\equiv -1 \pmod{61} \\
 59 &\equiv -2 \pmod{61} \\
 58 &\equiv -3 \pmod{61}
 \end{aligned}$$

จะได้

$$\begin{aligned}
 60! &\equiv (-1)(-2)(-3)(57!) \pmod{61} \\
 &\equiv -6(57!) \pmod{61}
 \end{aligned}$$

61 เป็นจำนวนเฉพาะ จากทฤษฎีบทวิลสันจะได้ว่า $60! \equiv -1 \pmod{61}$

แสดงว่า

$$-6(57!) \equiv -1 \pmod{61}$$

หรือ

$$6(57!) \equiv 1 \pmod{61}$$

แสดงว่า $57!$ เป็นตัวผกผัน 6 มอดุโล 61

เนื่องจาก $(6, 61) = 1$ ทำให้ได้ว่าตัวผกผัน 6 มอดุโล 61 จะหาค่าได้ และมีเพียงค่าเดียว

หาตัวผกผันของตัวผกผัน 6 มอดุโล 61

$$6x \equiv 1 \pmod{61}$$

จากขั้นตอนวิธีของยุคลิดจะได้ว่า

$$61 = 6(10) + 1$$

ทำย้อนกลับจะได้ว่า

$$1 = 61 + 6(-10)$$

เนื่องจาก $61 \equiv 0 \pmod{61}$ ทำให้ได้ว่า

$$6(-10) \equiv 1 \pmod{61}$$

หรือ

$$6(51) \equiv 1 \pmod{61}$$

แสดงว่า 51 เป็นผกผันของ 6 มอดุโล 61

$$\text{จึงได้ว่า } 57! \equiv 51 \pmod{61}$$

ดังนั้น เศษจากการหาร $57!$ ด้วย 61 คือ 51

จากตัวอย่าง 6.12 ใช้ Wolfram Alpha หาเศษจากการหาร $57!$ ด้วย 61 ดังภาพประกอบ 6.9



ภาพประกอบ 6.9 ใช้ Wolfram Alpha เพื่อแสดงเศษจากการหาร $57!$ ด้วย 61 คือ 51

สำหรับบทกลับของทฤษฎีบทของวิลสันนั้นก็เป็นจริงด้วยและมีความสำคัญอย่างมากในที่ใช้ในการตรวจสอบจำนวนเฉพาะรวมทั้งยังสามารถนำมาแก้ปัญหาบางปัญหาของทฤษฎีจำนวนได้

ทฤษฎีบท 6.4 (บทกลับของทฤษฎีบทวิลสัน)

ถ้า m เป็นจำนวนเต็มบวก ซึ่ง $m \geq 2$ ถ้า $(m-1)! \equiv -1 \pmod{m}$

แล้ว m เป็น จำนวนเฉพาะ

พิสูจน์

สมมติ m เป็นจำนวนประกอบ จะได้ว่า $m = ab$ ซึ่ง $a, b \in \mathbb{N}$ และ $1 < a, b < m$

เนื่องจาก $a \mid m$ และ $m \mid [(m-1)! + 1]$ ดังนั้น $a \mid [(m-1)! + 1]$

และเนื่องจาก $1 < a < m$ ดังนั้น $a \mid (m-1)!$

ทำให้ได้ว่า

$$a \mid [(m-1)! + 1 - (m-1)!]$$

หรือ

$$a \mid 1$$

แสดงว่า $a = 1$ จึงเกิดข้อขัดแย้งกับสมมุติฐาน ($1 < a, b < m$)

จึงสรุปได้ว่า m เป็น จำนวนเฉพาะ

จะเห็นได้ว่าจากทฤษฎีบทของวิลสัน และบทกลับของทฤษฎีบทวิลสัน เป็นเงื่อนไขจำเป็นและเพียงพอสำหรับจำนวนเต็มบวกที่จะเป็นจำนวนเฉพาะคือ ถ้า m เป็นจำนวนเต็มบวก ซึ่ง $m \geq 2$ แล้ว m เป็น จำนวนเฉพาะ ก็ต่อเมื่อ $(m-1)! \equiv -1 \pmod{m}$

ตัวอย่าง 6.13 จงใช้บทกลับของทฤษฎีบทวิลสันตรวจสอบว่า 5 และ 9 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ พิจารณา

$$\begin{aligned} (5-1)! &= 4! \\ &\equiv 24 \pmod{5} \\ &\equiv -1 \pmod{5} \end{aligned}$$

เนื่องจาก $(5-1)! \equiv -1 \pmod{5}$

จากบทกลับของทฤษฎีบทวิลสันจะได้ว่า 5 เป็นจำนวนเฉพาะ

พิจารณา

$$\begin{aligned} (9-1)! &= 8! \\ &\equiv 5760 \pmod{9} \\ &\equiv 0 \pmod{9} \end{aligned}$$

เนื่องจาก $(9-1)! \not\equiv -1 \pmod{9}$

จากข้อความแย้งสลับที่ของทฤษฎีบทวิลสันจะได้ว่า 9 ไม่เป็นจำนวนเฉพาะ

6.3 จำนวนเฉพาะเทียม

ผลจากทฤษฎีบทเล็กแฟร์มาทำให้ได้บทแทรกดังนี้ ถ้า p เป็นจำนวนเฉพาะและ a เป็นจำนวนเต็มใด ๆ แล้ว $a^p \equiv a \pmod{p}$ บทกลับของบทแทรกนี้สามารถตรวจสอบจำนวนว่าเป็นจำนวนประกอบได้ โดยถ้าสามารถหาจำนวนเต็ม a โดยที่ $a^m \not\equiv a \pmod{m}$ แล้วจะได้ว่า m เป็นจำนวนประกอบ และในหัวข้อนี้จะเป็นการศึกษาจำนวนประกอบ m ที่มีคุณสมบัติดังกล่าว

ตัวอย่าง 6.14 จงแสดงว่า 63 เป็นจำนวนประกอบ

วิธีทำ การแสดงว่า 63 เป็นจำนวนประกอบ เป็นการหาจำนวนเต็ม a โดยที่ $a^{63} \not\equiv a \pmod{63}$

เนื่องจาก $2^6 \equiv 1 \pmod{63}$ จะได้

$$2^{63} = (2^6)^{10} \cdot 2^3 \equiv 1^{10} \cdot 2^3 \pmod{63} \equiv 8 \pmod{63}$$

เนื่องจาก $2^{63} \equiv 8 \pmod{63}$

แสดงว่า $2^{63} \not\equiv 2 \pmod{63}$

ดังนั้น 63 เป็นจำนวนประกอบ

การใช้ทฤษฎีบทเล็กแฟร์มานั้นสามารถแสดงได้ว่าจำนวนเต็มบางจำนวนเป็นจำนวนประกอบ ชาวจีนเชื่อว่า $2^m \equiv 2 \pmod{m}$ แล้ว m จะต้องเป็นจำนวนเฉพาะ ซึ่งข้อความนี้เป็นจริงสำหรับ $1 \leq m \leq 340$ แต่ต่อมาในปี ค.ศ. 1919 นักคณิตศาสตร์ชาวฝรั่งเศสชื่อปีแยร์ เฟรเดอริก ซารุส (Pierre Frédéric Sarrus) พบว่าบทกลับของทฤษฎีบทนั้นไม่จริง ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.15

$$2^{341} \equiv 2 \pmod{341} \text{ แต่ } 341 \text{ ไม่ใช่จำนวนเฉพาะเนื่องจาก } 341 = 11 \cdot 31$$

$$2^{561} \equiv 2 \pmod{561} \text{ แต่ } 561 \text{ ไม่ใช่จำนวนเฉพาะเนื่องจาก } 561 = 3 \cdot 11 \cdot 17$$

$$2^{645} \equiv 2 \pmod{645} \text{ แต่ } 645 \text{ ไม่ใช่จำนวนเฉพาะเนื่องจาก } 645 = 3 \cdot 5 \cdot 43$$

$$2^{1104} \equiv 1 \pmod{1105} \text{ แต่ } 1105 \text{ ไม่ใช่จำนวนเฉพาะเนื่องจาก } 1105 = 5 \cdot 13 \cdot 17$$

จากตัวอย่างข้างต้นพบว่า $a^m \equiv a \pmod{m}$ แต่ m นั้นเป็นจำนวนประกอบได้ จำนวนนี้ยังเป็นประโยชน์สำหรับการศึกษาทฤษฎีจำนวนอีกด้วย เพื่อให้เกิดความเข้าใจตรงกันจึงได้มีบทนิยามของจำนวน m ที่มีสมบัติดังกล่าวดังนี้

บทนิยาม 6.1

ให้ a เป็นจำนวนเต็มบวก ถ้า m เป็นจำนวนประกอบที่เป็นบวก และ $a^m \equiv a \pmod{m}$ แล้วจะเรียก m ว่า **จำนวนเฉพาะเทียมฐาน a** (Pseudoprime to base a)

จากบทนิยามพบว่า ถ้า $(a, m) = 1$ แล้วสมภาค $a^m \equiv a \pmod{m}$ สมมูลกับสมภาค $a^{m-1} \equiv 1 \pmod{m}$ เนื่องจาก

$$\begin{aligned} \frac{a^m}{a} &\equiv \frac{a}{a} \left(\pmod{\frac{m}{(a, m)}} \right) \\ a^{m-1} &\equiv 1 \pmod{m} \end{aligned}$$

และ

$$\begin{aligned} a^{m-1} &\equiv 1 \pmod{m} \\ aa^{m-1} &\equiv a \pmod{m} \\ aa^m &\equiv a \pmod{m} \end{aligned}$$

เนื่องจากสมภาค $a^m \equiv a \pmod{m}$ สมมูลกับสมภาค $a^{m-1} \equiv 1 \pmod{m}$ ทำให้สามารถตรวจสอบจำนวนเฉพาะเทียมได้อีกรูปแบบดังแสดงในตัวอย่างต่อไปนี้

ตัวอย่าง 6.16

1. จำนวนประกอบ 341 เป็นจำนวนเฉพาะเทียมฐาน 2 เนื่องจาก $2^{340} \equiv 1 \pmod{341}$
2. จำนวนประกอบ 561 เป็นจำนวนเฉพาะเทียมฐาน 2 เนื่องจาก $2^{560} \equiv 1 \pmod{561}$
3. จำนวนประกอบ 645 เป็นจำนวนเฉพาะเทียมฐาน 2 เนื่องจาก $2^{644} \equiv 1 \pmod{645}$
4. จำนวนประกอบ 1105 เป็นจำนวนเฉพาะเทียมฐาน 2 เนื่องจาก $2^{1104} \equiv 1 \pmod{1105}$

จำนวนเฉพาะเทียมทั้ง 4 ตัวที่แสดงในตัวอย่าง 6.15 และ 6.16 เป็นจำนวนเฉพาะเทียมฐาน 2 ที่เป็นจำนวนคี่ 4 ตัวแรก และ 161038 จำนวนเฉพาะเทียมฐานสองที่เล็กที่สุดที่เป็นจำนวนคี่ นอกจากจำนวนเฉพาะที่ได้กล่าวมาข้างต้นแล้วยังสามารถสร้างจำนวนเฉพาะเทียมได้เป็นจำนวนอนันต์ ซึ่งแสดงไว้ในบทตั้ง และทฤษฎีบทต่อไปนี้

บทตั้ง 6.1

ให้ m, n เป็นจำนวนเต็มบวก และ $m \mid n$ จะได้ว่า $(2^m - 1) \mid (2^n - 1)$

พิสูจน์

เนื่องจาก $m \mid n$ ดังนั้น $n = km$ สำหรับบางจำนวนเต็มบวก k จะได้ว่า

$$\begin{aligned} 2^n - 1 &= 2^{km} - 1 \\ &= (2^m - 1) \left[2^{(k-1)m} + 2^{(k-2)m} + \dots + 2^m + 1 \right] \end{aligned}$$

ดังนั้น $(2^m - 1) \mid (2^n - 1)$

บทตั้ง 6.2

ให้ m เป็นจำนวนเฉพาะเทียมและเป็นจำนวนคี่ จะได้ว่า $2^m - 1$ เป็นจำนวนเฉพาะเทียมและเป็นจำนวนคี่

พิสูจน์ ให้ m เป็นจำนวนเฉพาะเทียม

จะได้ว่า m เป็นจำนวนประกอบและ $2^m \equiv 2 \pmod{m}$

เนื่องจาก m เป็นจำนวนคี่ ดังนั้น $2^{m-1} \equiv 1 \pmod{m}$

ให้ $m = rs$ เมื่อ $1 < r, s < m$ และ $M = 2^m - 1$

เนื่องจาก $r \mid m$ จากบทตั้ง 6.1 จะได้ว่า

$$(2^r - 1) \mid (2^m - 1)$$

นั่นคือ $(2^m - 1) \mid M$ ดังนั้น M เป็นจำนวนคี่

ต่อไปจะแสดงว่า $2^M \equiv 2 \pmod{M}$ ดังนี้

เนื่องจาก $2^m \equiv 2 \pmod{m}$ ดังนั้น

$$m \mid (2^m - 2)$$

จะได้ว่า $(2^m - 2) = km$ สำหรับบางค่า $k \in \mathbb{Z}$

นั่นคือ $(M - 1) = km$ ทำให้ได้ว่า

$$2^{(M-1)} - 1 = 2^{km} - 1$$

จากบทตั้ง 6.1 จะได้ว่า $M = 2^{M-1} \mid (2^{km} - 1)$

ดังนั้น $2^{(M-1)} - 1 \equiv 0 \pmod{M}$

นั่นคือ $2^{(M-1)} \equiv 1 \pmod{M}$ ทำให้ได้ว่า $2^M \equiv 2 \pmod{M}$

ตัวอย่าง 6.17 ถ้า 341 เป็นจำนวนเฉพาะเทียมแล้ว จงสร้างเฉพาะเทียมอีก 3 จำนวน

วิธีทำ เนื่องจาก 341 เป็นจำนวนเฉพาะเทียม จะได้

$$2^{341} - 1 \text{ เป็นจำนวนเฉพาะเทียม}$$

$$2^{(2^{341}-1)} - 1 \text{ เป็นจำนวนเฉพาะเทียม}$$

$$2^{\left(2^{(2^{341}-1)}-1\right)} - 1 \text{ เป็นจำนวนเฉพาะเทียม}$$

ทฤษฎีบท 6.5

มีจำนวนเฉพาะเทียมเป็นจำนวนอนันต์

พิสูจน์

ให้ n_i เป็นจำนวนเฉพาะเทียมที่เป็นจำนวนคี่ จากบทตั้ง 6.2

จะได้จำนวนเฉพาะเทียมที่เป็นจำนวนคี่ n_{i+1} คือ $2^{n_i} - 1$ สำหรับ $i = 0, 1, 2, \dots$

ให้ $n_0 = 341$ จะได้จำนวนเฉพาะเทียมเป็นจำนวนอนันต์

จากตัวอย่างที่ผ่านมาพบว่า 341 เป็นจำนวนเฉพาะเทียมฐาน 2 ในตัวอย่างต่อไปจะตรวจสอบว่านอกจากเป็นจำนวนเฉพาะเทียมฐาน 2 แล้วเป็นจำนวนเฉพาะในฐานอื่น ๆ อีกหรือไม่ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.18 จงตรวจสอบว่า 341 เป็นจำนวนเฉพาะฐาน a หรือไม่ เมื่อ $2 \leq a \leq 11$

วิธีทำ เนื่องจาก

$$\begin{aligned} 2^{340} &\equiv 1 \pmod{341} \\ 3^{340} &\equiv 56 \pmod{341} \\ 4^{340} &\equiv 1 \pmod{341} \\ 5^{340} &\equiv 67 \pmod{341} \\ 6^{340} &\equiv 56 \pmod{341} \\ 7^{340} &\equiv 56 \pmod{341} \\ 8^{340} &\equiv 1 \pmod{341} \\ 9^{340} &\equiv 67 \pmod{341} \\ 10^{340} &\equiv 67 \pmod{341} \\ 11^{340} &\equiv 253 \pmod{341} \end{aligned}$$

ดังนั้น 341 เป็นจำนวนเฉพาะเทียมฐาน 2, 4 และ ฐาน 8

บทนิยาม 6.2

สำหรับจำนวนเต็มบวก a ทุกจำนวน โดยที่ $(a, m) = 1$ จำนวนประกอบ m ที่สอดคล้องกับสมภาค $a^{m-1} \equiv 1 \pmod{m}$ เรียกว่า **จำนวนเฉพาะเทียมสมบูรณ์** หรือ **จำนวนคาร์ไมเคิล**

Burton (2011 : 149) ได้กล่าวว่า การตั้งชื่อจำนวนคาร์ไมเคิลเพื่อเป็นเกียรติแก่นักคณิตศาสตร์ชาวอเมริกัน ชื่อ คาร์ไมเคิล (Robert Daniel Carmichael) ซึ่งเป็นผู้ที่สังเกตเห็นว่ามีจำนวนที่มีสมบัตินี้เป็นคนแรก จากบทความชิ้นแรกของเขาที่กล่าวเกี่ยวกับเรื่องนี้ได้ตีพิมพ์ในปี ค.ศ. 1910 คาร์ไมเคิล ได้กล่าวถึงจำนวนเฉพาะเทียมสมบูรณ์ 4 จำนวน ดังนี้

$$561 = 3 \cdot 11 \cdot 17$$

$$1105 = 5 \cdot 13 \cdot 17$$

$$2821 = 7 \cdot 13 \cdot 31$$

$$15841 = 7 \cdot 31 \cdot 73$$

อีกสองปีต่อมา คาร์ไมเคิลได้นำเสนอจำนวนเฉพาะเทียมสมบูรณ์อีก 11 จำนวนซึ่งมีตัวประกอบเฉพาะ 3 ตัว และพบจำนวนเฉพาะเทียมสมบูรณ์อีก 1 ตัวที่มีตัวประกอบเฉพาะ 4 ตัว คือ

$$16046641 = 13 \cdot 37 \cdot 73 \cdot 457$$

Rosen (2014 : 228) ได้กล่าวว่าในปี ค.ศ. 1912 คาร์ไมเคิลได้คาดการณ์ว่า จำนวนเฉพาะเทียมสมบูรณ์มีไม่จำกัดจำนวน โดยในปี ค.ศ. 1992 อัลฟอร์ด, แกรนด์วิลล์ และ โปเมแรนซ์ ได้พิสูจน์ว่าข้อความคาดการณ์ของ คาร์ไมเคิลเป็นจริง

ตัวอย่าง 6.19 จงแสดงว่า 1105 เป็นจำนวนคาร์ไมเคิล

วิธีทำ เนื่องจาก $1105 = 5 \cdot 13 \cdot 17$

ถ้า $(a, 1105) = 1$ แล้วจะได้ว่า $(a, 5) = (a, 13) = (a, 17) = 1$

โดยทฤษฎีบทเล็กแฟร์มา จะได้

$$a^4 \equiv 1 \pmod{5}, a^{12} \equiv 1 \pmod{13} \text{ และ } a^{16} \equiv 1 \pmod{17}$$

แสดงว่า

$$a^{1104} = (a^4)^{552} \equiv 1 \pmod{5}$$

$$a^{1104} = (a^{12})^{92} \equiv 1 \pmod{13}$$

$$a^{1104} = (a^{16})^{69} \equiv 1 \pmod{17}$$

นั่นคือ $a^{1104} \equiv 1 \pmod{1105}$ สำหรับจำนวนเต็ม a ทุกจำนวนโดยที่ $(a, 1105) = 1$

ดังนั้น จำนวน 1,105 เป็นจำนวนคาร์ไมเคิล

6.4 ทฤษฎีบทออยเลอร์

ออยเลอร์ ได้ขยายทฤษฎีบทเล็กแฟร์มา จาก $a^{p-1} \equiv 1 \pmod{p}$ ในกรณีที่ p เป็นจำนวนเฉพาะไปสู่กรณีทั่วไป โดยขยายทฤษฎีบทเล็กแฟร์มาในกรณีที่สมภาคที่มีมอดุโลเป็นจำนวนเฉพาะไปสู่สมภาคที่มีมอดุโลเป็นจำนวนเต็มบวกใด ๆ ในการศึกษาทฤษฎีบทดังกล่าวนี้ ออยเลอร์ได้นำฟังก์ชันฟีออยเลอร์ และบทตั้งที่เกี่ยวข้องดังต่อไปนี้

ทฤษฎีบท 6.6

ให้ m เป็นจำนวนเต็ม a เป็นจำนวนเต็มบวก และ $(a, m) = 1$ ให้ $r_1, r_2, \dots, r_{\phi(m)}$ เป็นจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ m ซึ่ง $(r_i, m) = 1$ เมื่อ $i = 1, 2, 3, \dots, \phi(m)$ จะได้ว่า ส่วนตกค้างค่าน้อยสุดของ $ar_1, ar_2, \dots, ar_{\phi(m)}$ มอดุโล m คือ $r_1, r_2, \dots, r_{\phi(m)}$

พิสูจน์

จะแสดงว่า $(ar_i, m) = 1$ สำหรับแต่ละ $i = 1, 2, 3, \dots, \phi(m)$

สมมติให้ $(ar_i, m) > 1$ และ $(ar_i, m) = p$ โดยที่ p เป็นจำนวนเฉพาะ

จะได้ว่า $p \mid ar_i$ และ $p \mid m$

จะได้ว่า $p \mid a$ หรือ $p \mid r_i$ และ $p \mid m$

แสดงว่า $(r_i, m) \neq 1$ ซึ่งเกิดข้อขัดแย้ง แสดงว่า $p \nmid a$

จาก $p \nmid a$ และ $p \mid m$ ดังนั้น $p \nmid (a, m)$ ซึ่งเกิดข้อขัดแย้ง แสดงว่า $(ar_i, m) = 1$

ต่อไปจะแสดงว่า $ar_i \not\equiv ar_j \pmod{m}$ ซึ่ง $1 \leq i < j \leq \phi(m)$

สมมติว่า $ar_i \equiv ar_j \pmod{m}$ (จะแสดงว่า $r_i = r_j$)

เนื่องจาก $(a, m) = 1$ จะได้ว่า $r_i \equiv r_j \pmod{m}$

และเนื่องจาก r_i, r_j เป็นส่วนตกค้างค่าน้อยสุดมอดุโล m ดังนั้น $r_i = r_j$

นั่นคือ ถ้า $r_i \neq r_j$ แล้ว $ar_i \not\equiv ar_j \pmod{m}$

แสดงว่า ส่วนตกค้างค่าน้อยสุดของ $ar_1, ar_2, \dots, ar_{\phi(m)}$ มอดุโล m คือ $r_1, r_2, \dots, r_{\phi(m)}$

ตัวอย่าง 6.20 จงหาส่วนตกค้างค่าน้อยสุดของ 25, 125, 175, 275, 325 และ 425 มอดุโล 18

วิธีทำ ให้ $m = 18$ และ $a = 25$ จะเห็นว่า $\phi(18) = 6$ และเนื่องจาก

$$25 \cdot 1 = 25 \equiv 7 \pmod{18}$$

$$25 \cdot 5 = 125 \equiv 17 \pmod{18}$$

$$25 \cdot 7 = 175 \equiv 13 \pmod{18}$$

$$25 \cdot 11 = 275 \equiv 5 \pmod{18}$$

$$25 \cdot 13 = 325 \equiv 1 \pmod{18}$$

$$25 \cdot 17 = 425 \equiv 11 \pmod{18}$$

และ $(r_i, m) = 1$, $r_i = 1, 5, 7, 11, 13, 17$

ดังนั้น ส่วนตกค้างค่าน้อยสุดของ 25, 125, 175, 275, 325 และ 425 มอดุโล 18 คือ 1, 5, 7, 11, 13 และ 17

ทฤษฎีบท 6.7 (ทฤษฎีบททอยเลอร์)

กำหนดให้ m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม ซึ่ง $(a, m) = 1$
 จะได้ว่า $a^{\phi(m)} \equiv 1 \pmod{m}$

พิสูจน์

ให้ $r_1, r_2, \dots, r_{\phi(m)}$ ส่วนตกค้างค่าน้อยสุดมอดุโล m

ซึ่ง $(r_i, m) = 1, i = 1, 2, 3, \dots, \phi(m)$

จะได้ว่าจำนวนเต็ม $ar_1, ar_2, \dots, ar_{\phi(m)}$ สัมภาคกับ $r_1, r_2, \dots, r_{\phi(m)}$ โดยไม่คำนึงถึงลำดับ
 ดังนั้น

$$ar_1 \equiv r_1 \pmod{m}$$

$$ar_2 \equiv r_2 \pmod{m}$$

$\vdots$

$$ar_{\phi(m)} \equiv r_{\phi(m)} \pmod{m}$$

คูณสมภาคเหล่านี้เข้าด้วยกันจะได้

$$(ar_1)(ar_2) \cdots (ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m} \text{ หรือ}$$

$$a^{\phi(m)} (r_1 r_2 \cdots r_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

เนื่องจาก $(r_i, m) = 1$ นั่นคือ $(r_1, r_2, \dots, r_{\phi(m)}) = 1$

แสดงว่า $a^{\phi(m)} \equiv 1 \pmod{m}$

จากทฤษฎีบททอยเลอร์ ถ้า $m = p$ เป็นจำนวนเฉพาะแล้ว $\phi(m) = \phi(p) = p - 1$

ดังนั้น ถ้า $(a, p) = 1$ แล้ว $a^{p-1} \equiv a^{\phi(m)} \equiv 1 \pmod{m}$

ตัวอย่าง 6.21 จงแสดงว่า $25^{\phi(18)} \equiv 1 \pmod{12}$

วิธีทำ จากตัวอย่าง 6.20 พบว่า

$$(25 \cdot 1)(25 \cdot 5)(25 \cdot 7)(25 \cdot 11)(25 \cdot 13)(25 \cdot 17) \equiv 7 \cdot 17 \cdot 13 \cdot 5 \cdot 1 \cdot 11 \pmod{18}$$

แสดงว่า

$$25^6 (5 \cdot 7 \cdot 11 \cdot 13 \cdot 17) \equiv 7 \cdot 17 \cdot 13 \cdot 5 \cdot 1 \cdot 11 \pmod{18}$$

และเนื่องจาก $(7 \cdot 17 \cdot 13 \cdot 5 \cdot 1 \cdot 11) = 1$ แสดงว่า $25^6 \equiv 1 \pmod{18}$

ดังนั้น $25^{\phi(18)} \equiv 1 \pmod{12}$

ทฤษฎีบททอยเลอร์นั้นเป็นทฤษฎีที่มีความสำคัญมากอีกทฤษฎีหนึ่ง เพราะสามารถนำมาประยุกต์เพื่อแก้ปัญหาสมภาคมอดุโลต่าง ๆ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 6.22 จงหาเศษเหลือที่ได้จากการหาร 2^{855} ด้วย 13

วิธีทำ เนื่องจาก $(2, 13) = 1$ และ $\phi(13) = 12$

จากทฤษฎีบททอยเลอร์จะได้ว่า

$$2^{\phi(13)} \equiv 1 \pmod{13} \text{ หรือ}$$

$$2^{12} \equiv 1 \pmod{13}$$

พิจารณา

$$\begin{aligned} 2^{855} &= (2^{12})^{71} \cdot 2^3 \\ &\equiv 1^{71} \cdot 8 \pmod{13} \\ &\equiv 8 \pmod{13} \end{aligned}$$

ดังนั้น เศษเหลือที่ได้จากการหาร 2^{855} ด้วย 13 คือ 8

ตัวอย่าง 6.23 จงหาเศษเหลือที่ได้จากการหาร 11^{146} ด้วย 180

วิธีทำ เนื่องจาก $(11, 180) = 1$ และ

$$\phi(180) = \phi(2^2 \cdot 3^2 \cdot 5) = 180 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 48$$

จากทฤษฎีบททอยเลอร์จะได้ว่า

$$11^{\phi(180)} \equiv 1 \pmod{180} \text{ หรือ}$$

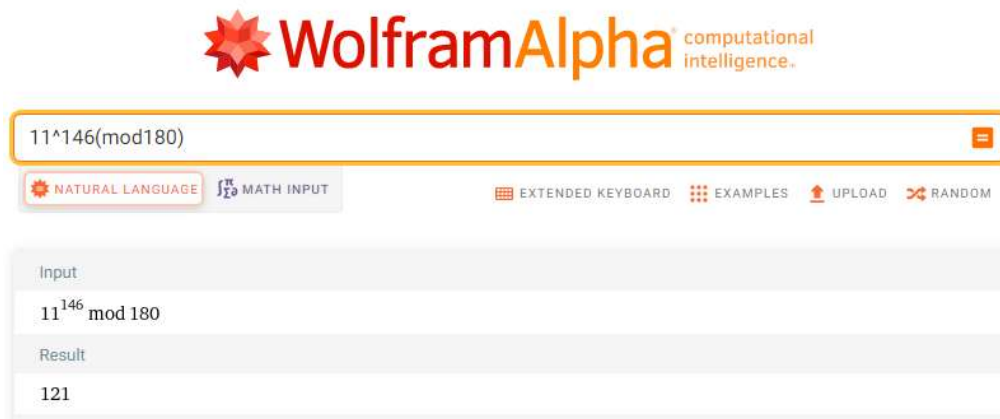
$$11^{48} \equiv 1 \pmod{180}$$

พิจารณา

$$\begin{aligned} 11^{146} &= (11^{48})^3 \cdot 11^2 \\ &\equiv 1^3 \cdot 11^2 \pmod{180} \\ &\equiv 11^2 \pmod{180} \\ &\equiv 121 \pmod{180} \end{aligned}$$

ดังนั้น เศษเหลือที่เกิดจากการหาร 11^{146} ด้วย 180 คือ 121

จากตัวอย่าง 6.23 ใช้ Wolfram Alpha เพื่อหาเศษเหลือที่เกิดจากการหาร 11^{146} ด้วย 180
ดังภาพประกอบ 6.10



ภาพประกอบ 6.10 ใช้ Wolfram Alpha เพื่อแสดงว่าเศษเหลือที่เกิดจากการหาร 11^{146} ด้วย 180 คือ 121

ตัวอย่าง 6.24 จงหาเลขโดดสองหลักสุดท้ายของ 3^{2004}

วิธีทำ ในการหาเลขโดดสองหลักสุดท้ายของ 3^{2004} เป็นการหาเศษเหลือที่เกิดจากการหาร 3^{2004} ด้วย 100

เนื่องจาก $(3, 100) = 1$ และ

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$$

จากทฤษฎีบทออยเลอร์จะได้ว่า

$$3^{\phi(100)} \equiv 1 \pmod{100} \text{ หรือ}$$

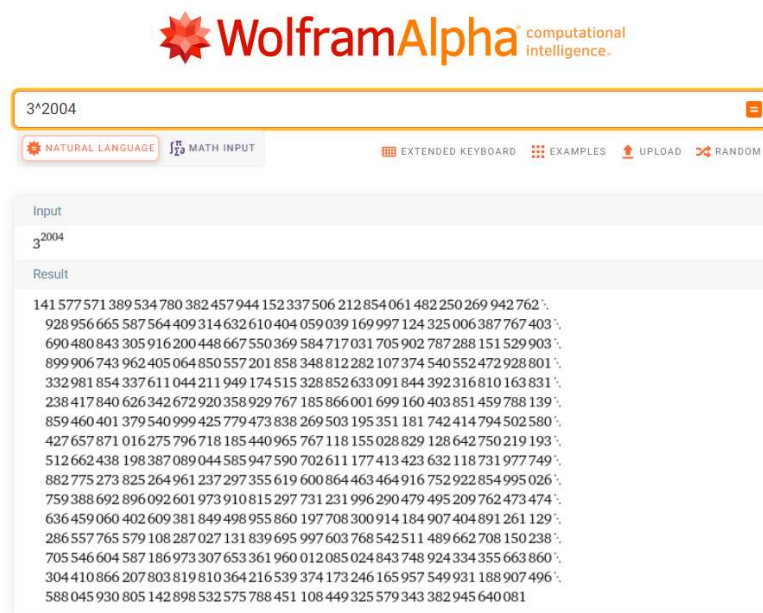
$$3^{40} \equiv 1 \pmod{100}$$

พิจารณา

$$\begin{aligned} 3^{2004} &= (3^{40})^{50} \cdot 3^4 \\ &\equiv 1^{50} \cdot 3^4 \pmod{100} \\ &\equiv 3^4 \pmod{100} \\ &\equiv 81 \pmod{100} \end{aligned}$$

ดังนั้น เลขโดดสองหลักสุดท้ายของ 3^{2004} คือ 81

จากตัวอย่าง 6.24 ใช้ Wolfram Alpha เพื่อหาเลขโดดสองหลักสุดท้ายของ 3^{2004} ดังภาพประกอบ 6.11



ภาพประกอบ 6.11 ใช้ Wolfram Alpha เพื่อแสดงว่า 81 เป็นเลขโดดสองหลักสุดท้ายของ 3^{2004}

ทฤษฎีบททอยเลอร์นอกจากจะนำมาประยุกต์ใช้ในการแก้ปัญหาสมภาคแล้วยังสามารถนำไปประยุกต์ใช้ในการหาตัวผกผันมอดุโล m ได้ ด้วยวิธีการดังนี้

ถ้า a และ m เป็นจำนวนเฉพาะสัมพัทธ์กัน นั่นคือ $(a, m) = 1$ ทำให้ได้ว่า

$$a \cdot a^{\phi(m)-1} = a^{\phi(m)} \equiv 1 \pmod{m}$$

แสดงว่า $a^{\phi(m)-1}$ เป็นตัวผกผันของ a มอดุโล m

ตัวอย่าง 6.25 จงหาตัวผกผันของ 2 มอดุโล 9

วิธีทำ เนื่องจาก $(2, 9) = 1$

แสดงว่า $2^{\phi(9)-1}$ เป็นตัวผกผันของ 2 มอดุโล 9

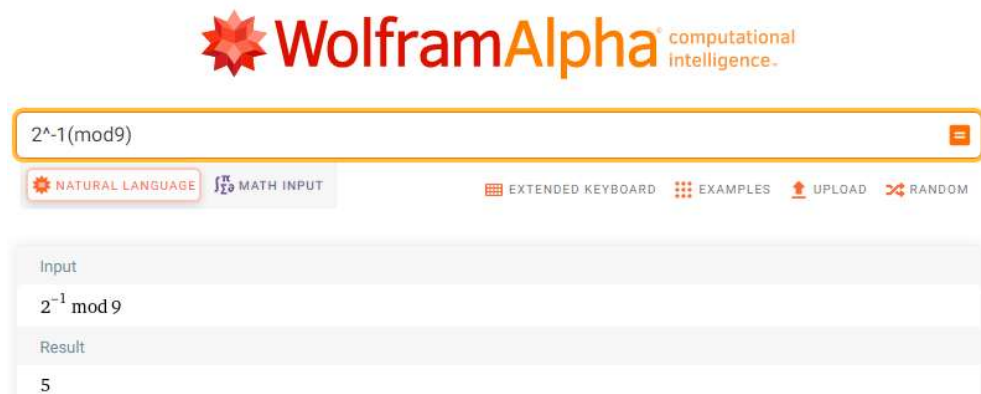
$$\phi(9) = \phi(3^2) = 9 \left(1 - \frac{1}{3}\right) = 6$$

พิจารณา

$$\begin{aligned} 2^{\phi(9)-1} &= 2^{6-1} \\ &= 32 \\ &\equiv 5 \pmod{9} \end{aligned}$$

ดังนั้น 5 เป็นผกผันของ 2 มอดุโล 9

จากตัวอย่าง 6.25 ใช้ Wolfram Alpha เพื่อหาตัวผกผันของ 2 โมดูล 9 ดังภาพประกอบ 6.11



ภาพประกอบ 6.12 ใช้ Wolfram Alpha เพื่อแสดงว่า 5 เป็นผกผันของ 2 โมดูล 9

การหาผกผันนั้นเป็นเครื่องมือที่สำคัญอีกอย่างหนึ่งในการหาผลเฉลยของสมภาคเชิงเส้น และจากตัวอย่างที่ผ่านมาการนำทฤษฎีบทของเลอว์มาประยุกต์ใช้ในการหาผกผันซึ่งเป็นวิธีที่ง่ายสะดวกและรวดเร็ว และสำหรับตัวอย่างต่อไปจะเป็นการประยุกต์ใช้ทฤษฎีบทของเลอว์เพื่อหาผลเฉลยของสมภาคเชิงเส้น

ตัวอย่าง 6.26 จงหาผลเฉลยของสมภาคเชิงเส้น $2x \equiv 5 \pmod{13}$

วิธีทำ เนื่องจาก $(2, 13) = 1$ และ $\phi(13) = 12$

แสดงว่า $2^{\phi(13)-1} = 2^{11}$ เป็นตัวผกผันของ 2 โมดูล 13

ผลเฉลยของสมภาค $2x \equiv 5 \pmod{13}$ คือ

$$\begin{aligned} 2^{11} \cdot 2x &\equiv 2^{11} \cdot 5 \pmod{13} \\ x &\equiv (2^4)^2 \cdot 2^3 \cdot 5 \pmod{13} \\ &\equiv 3^2 \cdot 8 \cdot 5 \pmod{13} \\ &\equiv 9 \cdot 40 \pmod{13} \\ &\equiv 9 \cdot 1 \pmod{13} \\ &\equiv 9 \pmod{13} \end{aligned}$$

ดังนั้น ผลเฉลยของสมภาคเชิงเส้น $2x \equiv 5 \pmod{13}$ คือ $x \equiv 9 \pmod{13}$

จากตัวอย่าง 6.26 ใช้ Wolfram Alpha ผลเฉลยของสมภาคเชิงเส้น $2x \equiv 5 \pmod{13}$ ดัง

ภาพประกอบ 6.13



ภาพประกอบ 6.13 ใช้ Wolfram Alpha เพื่อแสดงว่า $x \equiv 9 \pmod{13}$ เป็นผลเฉลยของสมภาคเชิงเส้น $2x \equiv 5 \pmod{13}$

6.5 สรุปท้ายบทที่ 6

วิลสันได้ตั้งข้อคาดการณ์ไว้ว่า ถ้า p เป็นจำนวนเฉพาะ แล้ว p หาร $(p-1)! + 1$ ลงตัว แต่เขาไม่ได้เป็นผู้พิสูจน์ข้อคาดการณ์ดังกล่าว ต่อมา โฌแซ็ฟ หลุยส์ ลากร็องฌ์ ได้เป็นผู้พิสูจน์ และตเรียกชื่อทฤษฎีบทดังกล่าวว่าทฤษฎีบทวิลสัน โดยทฤษฎีบทนี้มีส่วนสำคัญในการแก้ปัญหสมภาคที่อยู่ในรูปแบบแฟกทอเรียล และยังสามารถนำไปประยุกต์ใช้ในการตรวจสอบจำนวนประกอบได้อีกด้วยได้อีกด้วย สำหรับทฤษฎีบทเล็กแฟร์มานั้นเขาเป็นผู้คิดค้นว่าสำหรับ p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็ม ถ้า $p \nmid a$ แล้ว $a^{p-1} \equiv 1 \pmod{p}$ เลออน ฮาร์ด และ ออยเลอร์ ได้เป็นผู้พิสูจน์ทฤษฎีบทดังกล่าว โดยทฤษฎีบทนี้ช่วยลดทอนขั้นตอนในการแก้ปัญหสมภาคในรูปแบบ $a^n \equiv b \pmod{m}$ กรณีที่ n มีค่ามาก ๆ และ m เป็นจำนวนเฉพาะ รวมทั้งยังสามารถประยุกต์ใช้ทฤษฎีบทนี้เพื่อหาตัวผกผันของจำนวนเต็มมอดุโลที่เป็นจำนวนเฉพาะ ได้สะดวกและรวดเร็วมากยิ่งขึ้น ต่อมา ชารุส ก็พบว่าบทกลับของทฤษฎีบทเล็กแฟร์มานั้นไม่จริง ทำให้เกิดจำนวนเฉพาะขึ้นมาในอีกรูปแบบที่เรียกกันว่าจำนวนเฉพาะเทียม ซึ่งจำนวนเฉพาะเทียมตัวอื่น ๆ นั้นสามารถสร้างได้จากจำนวนเฉพาะเทียมตัวแรก ทำให้พบว่าจำนวนเฉพาะเทียมนั้นมีอยู่เป็นจำนวนอนันต์นั่นเอง สำหรับทฤษฎีบทออยเลอร์ นั้นเขาได้ขยายทฤษฎีบทเล็กแฟร์มา จาก $a^{p-1} \equiv 1 \pmod{p}$ ในกรณีที่ p เป็นจำนวนเฉพาะไปสู่กรณีทั่วไป นั่นคือขยายทฤษฎีบทเล็กแฟร์มาในกรณีที่สมภาคที่มีมอดุโลเป็นจำนวนเฉพาะไปสู่สมภาคที่มีมอดุโลเป็นจำนวนเต็มบวกใด ๆ ในการศึกษาสมภาคนี้เขาได้ใช้ฟังก์ชันฟิออยเลอร์ หรือ $\phi(m)$ และทฤษฎีบทนี้เป็นประโยชน์อย่างมากในการแก้ปัญห สมภาคในรูปแบบ $a^n \equiv b \pmod{m}$ กรณีที่ n มีค่ามาก ๆ และ m เป็นจำนวนประกอบรวมทั้งยังสามารถประยุกต์ใช้ทฤษฎีบทนี้เพื่อหาตัวผกผันของจำนวนเต็มมอดุโลที่เป็นจำนวนเฉพาะได้สะดวกและรวดเร็วมากยิ่งขึ้น

แบบฝึกหัดท้ายบทที่ 6

1. จงแสดงว่า

1.1 $6! \equiv -1 \pmod{7}$

1.2 $16! \equiv -1 \pmod{17}$

1.3 $22! \equiv -1 \pmod{23}$

1.4 $198! \equiv -1 \pmod{199}$

2. จงใช้ทฤษฎีบทวิลสันหาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ $12!$ มอดุโล 13

3. จงใช้ทฤษฎีบทวิลสันหาเศษจากการหารต่อไปนี้

3.1 หาร $82 + 6!$ ด้วย 7

3.2 หาร $102 + 16!$ ด้วย 17

3.3 หาร $210 + 22!$ ด้วย 23

3.4 หาร $202 + 198!$ ด้วย 199

4. จงแสดงว่า 15 เป็นจำนวนประกอบโดยใช้ทฤษฎีบทวิลสัน

5. จงใช้ทฤษฎีบทเล็กแฟร์มาตรวจสอบว่าสมภาคที่กำหนดให้ต่อไปนี้เป็นจริงหรือไม่

5.1 $6^{10} \equiv 1 \pmod{11}$

5.2 $14^{198} \equiv 1 \pmod{199}$

5.3 $5^{112} \equiv 3 \pmod{11}$

5.4 $3^{289} \equiv 2 \pmod{17}$

6. จงใช้ทฤษฎีบทเล็กแฟร์มาหาผกผันของ จำนวนต่อไปนี้

6.1 2 มอดุโล 7

6.2 5 มอดุโล 13

6.3 2 มอดุโล 19

6.4 6 มอดุโล 41

7. จงหาส่วนตกค้างที่ไม่เป็นลบน้อยสุดของ 3^{144} มอดุโล 13

8. จงใช้ทฤษฎีบททอยเลอร์ในการตรวจสอบว่าสมภาคที่กำหนดให้ต่อไปนี้เป็นจริงหรือไม่

8.2 $2^{340} \not\equiv 2 \pmod{340}$

8.3 $3^{90} \equiv 1 \pmod{91}$

8.3 $4^{14} \equiv 1 \pmod{15}$

8.4 $5^{123} \equiv 1 \pmod{124}$

9. จงตรวจสอบว่าจำนวนต่อไปนี้เป็นจำนวนคาร์ไมเคิลหรือไม่

9.1 $105 = 3 \cdot 5 \cdot 7$

9.2 $231 = 3 \cdot 7 \cdot 11$

9.3 $273 = 3 \cdot 7 \cdot 13$

9.4 $561 = 3 \cdot 11 \cdot 17$

9.5 $1311 = 3 \cdot 19 \cdot 23$

9.6 $1729 = 7 \cdot 13 \cdot 19$

10. จงใช้ทฤษฎีบทออยเลอร์เพื่อหาค่าต่อไปนี้

10.1 เศษเหลือที่ได้จากการหาร 3^{201} ด้วย 11

10.2 เศษเหลือที่ได้จากการหาร 17^{111} ด้วย 180

10.3 เศษเหลือที่ได้จากการหาร 13^{50} ด้วย 120

11. จงใช้ทฤษฎีบทออยเลอร์เพื่อหาเลขโดดสองหลักสุดท้ายของ 5^{104}

12. จงใช้ทฤษฎีบทออยเลอร์เพื่อหาผกผันของ จำนวนต่อไปนี้

12.1 2 มอดุโล 15

12.2 3 มอดุโล 14

12.3 2 มอดุโล 21

12.4 17 มอดุโล 40

13. จงใช้ทฤษฎีบทเล็กแฟร์มา หรือ ทฤษฎีบทออยเลอร์เพื่อหาผลเฉลยของสมภาคต่อไปนี้

13.1 $2x \equiv 5 \pmod{7}$

13.2 $21x \equiv 5 \pmod{8}$

13.3 $2x \equiv 7 \pmod{9}$

13.4 $35x \equiv 5 \pmod{16}$

13.5 $19x \equiv 30 \pmod{40}$

13.6 $91x \equiv 15 \pmod{18}$

13.7 $17x \equiv 14 \pmod{21}$

13.8 $128x \equiv 83 \pmod{101}$