

บทที่ 9

ส่วนตกค้างกำลังสอง

ส่วนตกค้างกำลังสองส่วนตกค้างกำลังสอง(Quadratic Residue) เป็นตัวช่วยสำคัญสำหรับการหาผลเฉลยของสมภาคในรูป $ax^2 + bx + c \equiv 0 \pmod{p}$ และทำให้เกิดกฎส่วนกลับกำลังสอง (Quadratic Reciprocity) เพราะกฎนี้เป็นกฎที่มีความสำคัญอย่างมากในการหาผลเฉลยของสมภาคกำลังสอง โดยเลอจองดร์ได้กำหนดสัญลักษณ์ขึ้นมาซึ่งสัญลักษณ์เกี่ยวข้องกับส่วนตกค้างกำลังสองโดยตรง และเป็นสัญลักษณ์ที่ใช้ในการตรวจสอบอีกทางหนึ่งว่าสมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลยหรือไม่ แต่ข้อจำกัดของสัญลักษณ์เลอจองดร์(Legendre Symbol) นั้นสามารถตรวจสอบได้เฉพาะกรณีที่มี p เป็นจำนวนเฉพาะเท่านั้น แต่สำหรับสัญลักษณ์ของโคบี(Jacobi Symbol) เป็นสัญลักษณ์ที่ขยายของสัญลักษณ์เลอจองดร์โดยใช้ในกรณีทั่วไปโดยไม่ต้องเป็นจำนวนเฉพาะ ในบทนี้จะนำเสนอเนื้อหาที่สำคัญที่ใช้ในการศึกษาส่วนตกค้างกำลังสองประกอบด้วยส่วนตกค้างกำลังสอง สัญลักษณ์เลอจองดร์ กฎส่วนกลับกำลังสอง และสัญลักษณ์ยาโคบี

9.1 ส่วนตกค้างกำลังสอง

ในบทที่ผ่านมาได้ศึกษาการหาผลเฉลยของสมภาคเชิงเส้นที่มีหนึ่งตัวแปรที่อยู่ในรูป $ax \equiv b \pmod{m}$ ด้วยวิธีใช้คุณสมบัติทั่วไปของสมภาค และนำดัชนีมาแก้ปัญหาสมภาคดังกล่าว นอกจากนี้ยังรวมไปถึงสมภาคที่อยู่ในรูป $ax^n \equiv b \pmod{m}$ สำหรับการศึกษาส่วนตกค้างกำลังสองนั้นจะเป็นการศึกษาหาผลเฉลยของสมภาคกำลังสองที่มีหนึ่งตัวแปรที่มีรูปทั่วไปดังสมภาค (1)

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \dots(1)$$

เมื่อ a, b และ c เป็นเต็ม และ p เป็นจำนวนเฉพาะ โดยจะเน้นการศึกษาสมภาคกำลังสองที่อยู่ในรูปแบบเฉพาะสำหรับกรณี $(a, p) = 1$ การศึกษาสมภาคกำลังสองในกรณีที่ $p = 2$ เป็นการพิจารณาว่าผลเฉลยคือ $x = 0$ หรือ $x \neq 0$ เพียงเท่านั้นซึ่งการตรวจสอบนั้นไม่มีความซับซ้อน ดังนั้นจึงพิจารณาเฉพาะกรณีที่ p เป็นจำนวนเฉพาะคี่ โดยเริ่มจากบทนิยามของสมภาคกำลังสองดังต่อไปนี้

บทนิยาม 9.1

เมื่อ a, b และ c เป็นจำนวนเต็ม และ p เป็นจำนวนเฉพาะคี่ สมภาค $ax^2 + bx + c \equiv 0 \pmod{p}$ เป็นสมภาคกำลังสอง เมื่อ $a \not\equiv 0 \pmod{p}$

เนื่องจาก p เป็นจำนวนเฉพาะคี่ ซึ่งทำให้ได้ว่า $(4a, p) = 1$ ดังนั้นสมภาค (1) สมมูลกับ

$$\begin{aligned}
4a(ax^2 + bx + c) &\equiv 0 \pmod{p} \\
4a^2x^2 + 4abx + 4ac &\equiv 0 \pmod{p} \\
(2ax)^2 + 2(2ax)b + b^2 &\equiv b^2 - 4ac \pmod{p} \\
(2ax + b)^2 &\equiv (b^2 - 4ac) \pmod{p}
\end{aligned}$$

ให้ $y = 2ax + b$ และ $d = b^2 - 4ac$ สามารถเปลี่ยนให้อยู่ในรูป

$$y^2 \equiv d \pmod{p} \quad \dots(2)$$

จะเห็นว่าสมภาค (1) ในกรณีที่ p เป็นจำนวนเฉพาะคี่แล้วเราสามารถจัดให้อยู่ในรูปสมภาค $y^2 \equiv d \pmod{p}$ ซึ่งเป็นรูปแบบสมภาคที่ได้ศึกษามาแล้วในบทที่ผ่านมา เมื่อได้ผลเฉลยของสมภาคดังกล่าวแล้วแทนค่า $y = 2ax + b$ ดำเนินการหาผลเฉลยในรูปแบบสมภาคเชิงเส้นหนึ่งตัวแปร การหาผลเฉลยของสมภาค $ax^2 + bx + c \equiv 0 \pmod{p}$ ด้วยวิธีที่การที่กล่าวมาแสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 9.1 จงหาผลเฉลยของสมภาคกำลังสอง $x^2 + 5x + 6 \equiv 0 \pmod{5}$

วิธีทำ จากสมภาค $x^2 + 5x + 6 \equiv 0 \pmod{5}$

นำ 4 คูณตลอดสมภาค จะได้

$$\begin{aligned}
4x^2 + 20x + 24 &\equiv 0 \pmod{5} \\
(2x)^2 + 2(2x)5 + 5^2 &\equiv 5^2 - 24 \pmod{5} \\
(2x + 5)^2 &\equiv 1 \pmod{5}
\end{aligned}$$

ให้ $y = 2x + 5$ จะได้ $y^2 \equiv 1 \pmod{5}$

หาผลเฉลยของสมภาค $y^2 \equiv 1 \pmod{5}$ ดังต่อไปนี้

เนื่องจาก 2 เป็นรากปฐมฐานมอดุโล 5 พิจารณา

$$\begin{aligned}
2^1 &\equiv 2 \pmod{5} & 2^3 &\equiv 3 \pmod{5} \\
2^2 &\equiv 4 \pmod{5} & 2^4 &\equiv 1 \pmod{5}
\end{aligned}$$

จากสมภาค $y^2 \equiv 1 \pmod{5}$ จะได้

$$\begin{aligned}
ind_2 y^2 &\equiv ind_2 1 \pmod{\phi(5)} \\
2ind_2 y &\equiv 4 \pmod{4} \\
ind_2 y &\equiv 2 \pmod{2}
\end{aligned}$$

แสดงว่า $ind_2 y \equiv 2, 4 \pmod{4}$

จากบทนิยามของดัชนีจะได้ $y \equiv 2^2, 2^4 \pmod{5}$

เนื่องจาก $2^2 \equiv 4 \pmod{5}$ และ $2^4 \equiv 1 \pmod{5}$

นั่นคือ $y \equiv 1, 4 \pmod{5}$ เป็นผลเฉลยของสมภาค $y^2 \equiv 1 \pmod{5}$

ต่อไปหาผลเฉลยของสมภาคเชิงเส้น $y \equiv 1 \pmod{5}$ และ $y \equiv 4 \pmod{5}$

แทนค่า $y = 2x + 5$ ในสมภาคเชิงเส้น $y \equiv 1 \pmod{5}$ จะได้

$$\begin{aligned} 2x + 5 &\equiv 1 \pmod{5} \\ 2x &\equiv 1 - 5 \pmod{5} \\ 2x &\equiv 1 \pmod{5} \\ 2x &\equiv 6 \pmod{5} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

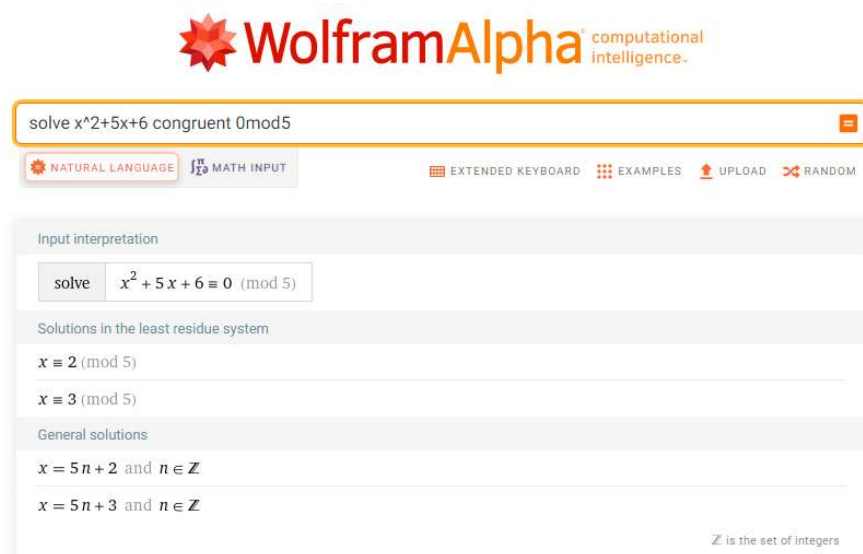
แทนค่า $y = 2x + 5$ ในสมภาคเชิงเส้น $y \equiv 4 \pmod{5}$ จะได้

$$\begin{aligned} 2x + 5 &\equiv 4 \pmod{5} \\ 2x &\equiv 4 \pmod{5} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

ดังนั้น $x \equiv 2, 3 \pmod{5}$ เป็นผลเฉลยของสมภาค $x^2 + 5x + 6 \equiv 0 \pmod{5}$

จากตัวอย่าง 9.1 ใช้ Wolfram Alpha เพื่อหาผลเฉลย $x^2 + 5x + 6 \equiv 0 \pmod{5}$ ดัง

ภาพประกอบ 9.1



ภาพประกอบ 9.1 ใช้ Wolfram Alpha เพื่อแสดงว่า $x \equiv 2, 3 \pmod{5}$ เป็นผลเฉลย

ของสมภาค $x^2 + 5x + 6 \equiv 0 \pmod{5}$

การหาเงื่อนไขที่ใช้พิจารณาว่าสมภาค $x^2 \equiv a \pmod{p}$ เมื่อ $(a, p) = 1$ มีผลเฉลยหรือไม่ นั้นเป็นปัญหาสำคัญอีกประการหนึ่งดังนั้นเพื่อให้เข้าใจความหมายสำหรับมีหรือไม่มีผลเฉลยนั้น ก่อนอื่นเริ่มจากการศึกษาบทนิยามต่อไปนี้

บทนิยาม 9.2

กำหนดให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็ม ซึ่ง $(a, p) = 1$

ถ้า $x^2 \equiv a \pmod{p}$ มีผลเฉลยแล้ว จะเรียก a ว่าเป็นส่วนตกค้างกำลังสองของ p

ถ้า $x^2 \equiv a \pmod{p}$ ไม่มีผลเฉลย จะเรียก a ว่าไม่เป็นส่วนตกค้างกำลังสองของ p

จากตัวอย่าง 9.1 พบว่า $y^2 \equiv 1 \pmod{5}$ มีผลเฉลยคือ 1 และ 4 นั่นคือ 1 และ 4 เป็นส่วนตกค้างกำลังสองของ 5 นั่นเอง

ตัวอย่าง 9.2 จงหาจำนวนเต็มซึ่งเป็นส่วนตกค้างกำลังสองและไม่เป็นส่วนตกค้างกำลังสองของ 13

วิธีทำ ในการหาส่วนตกค้างกำลังสองของ 13 เราจะหาจำนวนเต็ม a ซึ่ง $1 \leq a \leq 12$

และทำให้สมภาค $x^2 \equiv a \pmod{13}$ มีผลเฉลยเนื่องจาก

$$\begin{array}{ll} 1^2 \equiv 1 \pmod{13} & 7^2 \equiv 10 \pmod{13} \\ 2^2 \equiv 4 \pmod{13} & 8^2 \equiv 12 \pmod{13} \\ 3^2 \equiv 9 \pmod{13} & 9^2 \equiv 3 \pmod{13} \\ 4^2 \equiv 3 \pmod{13} & 10^2 \equiv 9 \pmod{13} \\ 5^2 \equiv 12 \pmod{13} & 11^2 \equiv 4 \pmod{13} \\ 6^2 \equiv 10 \pmod{13} & 12^2 \equiv 1 \pmod{13} \end{array}$$

จำนวนเต็ม a ที่มีสมบัติดังกล่าวคือ 1, 3, 4, 9, 10, 12

ดังนั้น จำนวนเต็มที่เป็นส่วนตกค้างกำลังสองของ 13 คือ 1, 3, 4, 9, 10, 12

จำนวนเต็มที่ไม่เป็นส่วนตกค้างกำลังสองของ 13 คือ 2, 5, 6, 7, 8, 11

จากตัวอย่าง 9.2 ใช้ Wolfram Alpha เพื่อหาส่วนตกค้างกำลังสองของ 13 ดังภาพประกอบ 9.2



ภาพประกอบ 9.2 ใช้ Wolfram Alpha แสดงว่า 1, 3, 4, 9, 10, 12 เป็นส่วนตกค้างกำลังสองของ 13

ตัวอย่าง 9.3 จงหาพิจารณาว่า 6 เป็นส่วนตกค้างกำลังสองมอดุโล 11 หรือไม่

วิธีทำ ในการตรวจสอบว่า 6 เป็นส่วนตกค้างกำลังสองมอดุโล 11 หรือไม่นั้น

ต้องตรวจสอบว่ามี $x^2 \equiv 6 \pmod{13}$ ดังต่อไปนี้

$$\begin{array}{ll} 1^2 \equiv 1 \pmod{11} \not\equiv 6 \pmod{11} & 6^2 \equiv 3 \pmod{11} \not\equiv 6 \pmod{11} \\ 2^2 \equiv 4 \pmod{11} \not\equiv 6 \pmod{11} & 7^2 \equiv 5 \pmod{11} \not\equiv 6 \pmod{11} \\ 3^2 \equiv 9 \pmod{11} \not\equiv 6 \pmod{11} & 8^2 \equiv 9 \pmod{11} \not\equiv 6 \pmod{11} \\ 4^2 \equiv 5 \pmod{11} \not\equiv 6 \pmod{11} & 9^2 \equiv 4 \pmod{11} \not\equiv 6 \pmod{11} \\ 5^2 \equiv 3 \pmod{11} \not\equiv 6 \pmod{11} & 10^2 \equiv 1 \pmod{11} \not\equiv 6 \pmod{11} \end{array}$$

พบว่าไม่มีจำนวนเต็มใดเลยที่เป็นผลเฉลยของ $x^2 \equiv 6 \pmod{13}$

ดังนั้น 6 ไม่เป็นส่วนตกค้างกำลังสองมอดุโล 11

จากตัวอย่างที่ผ่านมาพบว่าการตรวจสอบว่าจำนวนใดเป็นส่วนตกค้างกำลังสองมอดุโล p พบว่าต้องตรวจสอบ $x^2 \equiv a \pmod{p}$ โดยการแทนค่า x ตั้งแต่ $x = 1$ ไปจนถึง $p - 1$ ทำให้การตรวจสอบด้วยวิธีดังกล่าวไม่เหมาะสมสำหรับในกรณีที่ p มีค่ามาก ๆ ซึ่งออยเลอร์ได้ค้นพบวิธีการที่ใช้ในการตรวจสอบว่าจำนวนเต็มที่กำหนดให้เป็นส่วนตกค้างกำลังสองของจำนวนเฉพาะหรือไม่โดยนำเสนอเป็นทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 9.1 หลักเกณฑ์ของออยเลอร์ (Euler's rule)

กำหนดให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็มที่ $(a, p) = 1$ จะได้ว่า a เป็นส่วนตกค้างกำลังสองของ p ก็ต่อเมื่อ $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

พิสูจน์

($\Rightarrow$) สมมติให้ a เป็นส่วนตกค้างกำลังสองของ p

ดังนั้น สมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลย ให้เป็น x_0

เนื่องจาก $(a, p) = 1$ ดังนั้น $x_0^2 \equiv a \pmod{p}$

จะได้ $(x_0^2, p) = 1$ หรือ $(x_0, p) = 1$ โดยทฤษฎีบทเล็กของแฟร์มา จะได้

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod{p}$$

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

($\Leftarrow$) สมมติให้ $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ จะแสดงว่า a เป็นส่วนตกค้างกำลังสองของ p

กำหนดให้ r เป็นรากปฐมฐานของ p

ดังนั้น $a \equiv r^k \pmod{p}$ สำหรับจำนวนเต็ม k บางตัวที่ $1 \leq k \leq p-1$

ดังนั้น $r^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ จะได้

อันดับของ r คือ $p-1$ จะได้ $p-1 \mid \frac{k(p-1)}{2}$

จะได้ว่า k ต้องเป็นจำนวนคู่ให้ $k = 2j$ เพราะฉะนั้น

$$(r^j)^2 \equiv r^{2j} \equiv r^k \equiv a \pmod{p}$$

ได้ว่า r^j เป็นผลเฉลยของสมการ $x^2 \equiv a \pmod{p}$

นั่นคือ a เป็นส่วนตกค้างกำลังสองของ จำนวนเฉพาะ p

ถ้า p เป็นจำนวนเฉพาะคี่และ $(a, p) = 1$ แล้ว

$$\left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) = a^{p-1} - 1 \equiv 0 \pmod{p}$$

ดังนั้น $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ เป็นส่วนตกค้างกำลังสอง หรือ $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

ไม่เป็นส่วนตกค้างกำลังสอง ใดๆอย่างหนึ่ง

จากตัวอย่าง 9.3 เราสามารถตรวจสอบโดยใช้ ทฤษฎีบท 9.1 และพบว่า 6 ไม่เป็นส่วนตกค้าง

กำลังสองมอดุโล 11 เนื่องจาก $6^{\frac{11-1}{2}} = 6^5 \equiv -1 \pmod{11} \not\equiv 1 \pmod{11}$

ตัวอย่าง 9.4 จงพิจารณาว่า 2 และ 3 เป็นส่วนตกค้างกำลังสองของ 13 หรือไม่

วิธีทำ เนื่องจาก

$$2^{\frac{13-1}{2}} \equiv 2^6 \equiv 64 \equiv -1 \pmod{13} \not\equiv 1 \pmod{13}$$

และ

$$3^{\frac{13-1}{2}} \equiv 3^6 \equiv 729 \equiv 1 \pmod{13}$$

ดังนั้น 2 ไม่เป็นส่วนตกค้างกำลังสองของ 13

3 เป็นส่วนตกค้างกำลังสองของ 13

9.2 สัญลักษณเลอฌ็องดร์

Andreescu and Andrica (2009 : 170) กล่าวว่าสัญลักษณเลอฌ็องดร์ เป็นสัญลักษณที่มีความเกี่ยวข้องกับส่วนตกค้างกำลังสองโดยนักคณิตศาสตร์ชาวฝรั่งเศสชื่อ อาเดรียง มารี เลอฌ็องดร์ ได้กำหนดสัญลักษณขึ้นมาเพื่อใช้สำหรับศึกษาส่วนกลับกำลังสอง โดยมีบทนิยามดังต่อไปนี้

บทนิยาม 9.3

กำหนดให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็มที่ $(a, p) = 1$

สัญลักษณ์เลอช็องตร์ นิยามดังนี้

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ถ้า } a \text{ เป็นส่วนตกค้างกำลังสองของ } p \\ -1 & \text{ถ้า } a \text{ ไม่เป็นส่วนตกค้างกำลังสองของ } p \end{cases}$$

ในบางครั้งสัญลักษณ์เลอช็องตร์เขียนได้อีกแบบหนึ่งคือ (a / p)

จากตัวอย่าง 9.2 พบว่า 1, 3, 4, 9, 10, 12 เป็นส่วนตกค้างกำลังสองของ 13 และ 2, 5, 6, 7, 8, 11 ไม่เป็นส่วนตกค้างกำลังสองของ 13 เขียนให้อยู่ในรูปแบบสัญลักษณ์ของเลอช็องตร์ ได้ดังต่อไปนี้

$$\begin{aligned} \left(\frac{1}{13}\right) &= \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1 \\ \left(\frac{2}{13}\right) &= \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{11}{13}\right) = -1 \end{aligned}$$

จะเห็นว่าสัญลักษณ์ของเลอช็องตร์ นั้นเกี่ยวข้องกับส่วนตกค้างกำลังสองโดยตรงนั้น หมายความว่าสมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $\left(\frac{a}{p}\right) = 1$ และสมภาค $x^2 \equiv a \pmod{p}$

ไม่มีผลเฉลยก็ต่อเมื่อ $\left(\frac{a}{p}\right) = -1$

ตัวอย่าง 9.5 จงหา $\left(\frac{2}{11}\right), \left(\frac{5}{11}\right)$ และ $\left(\frac{8}{11}\right)$

วิธีทำ การหา $\left(\frac{2}{11}\right), \left(\frac{5}{11}\right)$ และ $\left(\frac{8}{11}\right)$

จะต้องตรวจสอบว่า 2, 5 และ 8 เป็นส่วนตกค้างมอดุโล 11 หรือไม่

นั่นคือต้องตรวจสอบว่า $x^2 \equiv a \pmod{11}$ เมื่อ $a = 2, 5, 8$ มีผลเฉลยหรือไม่

พิจารณา

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11} & 6^2 &\equiv 3 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} & 7^2 &\equiv 5 \pmod{11} \\ 3^2 &\equiv 9 \pmod{11} & 8^2 &\equiv 9 \pmod{11} \end{aligned}$$

$$4^2 \equiv 5 \pmod{11}$$

$$9^2 \equiv 4 \pmod{11}$$

$$5^2 \equiv 3 \pmod{11}$$

$$10^2 \equiv 1 \pmod{11}$$

พบว่า $x^2 \not\equiv 2 \pmod{11}$, $x^2 \equiv 5 \pmod{11}$ และ $x^2 \not\equiv 8 \pmod{11}$

ดังนั้น $\left(\frac{2}{11}\right) = -1$, $\left(\frac{5}{11}\right) = 1$ และ $\left(\frac{8}{11}\right) = -1$

จากตัวอย่าง 9.5 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{a}{p}\right)$ เมื่อ p เป็นจำนวนเฉพาะคี่

และ a เป็นจำนวนเต็มและในที่นี้จะยกตัวอย่างเฉพาะ $\left(\frac{2}{11}\right)$ ดังภาพประกอบ 9.3



ภาพประกอบ 9.3 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{2}{11}\right) = -1$

จากตัวอย่าง 9.5 สามารถหา $\left(\frac{2}{11}\right)$, $\left(\frac{5}{11}\right)$ และ $\left(\frac{8}{11}\right)$ ด้วยเกณฑ์ของออยเลอร์ดังต่อไปนี้

$$2^{\frac{11-1}{2}} = 2^5 = 32 \equiv -1 \pmod{11}$$

$$5^{\frac{11-1}{2}} = 5^5 = 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \pmod{11} \equiv 1 \pmod{11}$$

$$8^{\frac{11-1}{2}} = 8^5 = 8^2 \cdot 8^2 \cdot 8 \equiv (-2)(-2)8 \pmod{11} \equiv -1 \pmod{11}$$

แสดงว่า 2 และ 8 ไม่เป็นส่วนตกค้างมอดุโล 11 นั่นคือ $\left(\frac{2}{11}\right) = \left(\frac{8}{11}\right) = -1$ และ

5 เป็นส่วนตกค้างมอดุโล 11 นั่นคือ $\left(\frac{5}{11}\right) = 1$

นอกจากการหาค่า $\left(\frac{a}{p}\right)$ เมื่อ p เป็นจำนวนเฉพาะคี่ด้วยวิธีในตัวอย่างที่ผ่านมาและการ
เกณฑ์ของออยเลอร์ยังมีอีกวิธีที่สามารถหาส่วนตกค้างกำลังสองได้ง่ายสะดวก และรวดเร็วจากทฤษฎี
บทต่อไป

ทฤษฎีบท 9.2

กำหนดให้ p เป็นจำนวนเฉพาะคี่ a และ b เป็นจำนวนเต็มที่ $(a, p) = 1$ และ
 $(b, p) = 1$ จะได้ว่า

1. ถ้า $a \equiv b \pmod{p}$ แล้ว $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{a^2}{p}\right) = 1$

พิสูจน์

1. ถ้า $a \equiv b \pmod{p}$

พิจารณากรณีที่ $\left(\frac{a}{p}\right) = 1$ นั่นคือ $x^2 \equiv a \pmod{p}$ มีผลเฉลย

ให้เป็น x_0 ดังนั้น $x_0^2 \equiv a \pmod{p}$

จาก $a \equiv b \pmod{p}$ จะได้ $x_0^2 \equiv b \pmod{p}$

นั่นคือ x_0 เป็นผลเฉลยของ $x^2 \equiv b \pmod{p}$

จะได้ว่า $x^2 \equiv b \pmod{p}$ มีผลเฉลยเพราะฉะนั้น

$$\left(\frac{b}{p}\right) = 1$$

พิจารณากรณีที่ $\left(\frac{a}{p}\right) = -1$ นั่นคือ $x^2 \equiv a \pmod{p}$ ไม่มีผลเฉลย

จาก $a \equiv b \pmod{p}$ จะได้ $x^2 \equiv b \pmod{p}$ ไม่มีผลเฉลย

ดังนั้น $\left(\frac{b}{p}\right) = -1$

นั่นคือ $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2. เนื่องจาก $\left(\frac{1}{p}\right) = 1$ จะได้

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} \equiv (b)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

เนื่องจากสัญลักษณ์เลอซีงตร์ มีค่าเป็นไปได้ 2 ค่าคือ 1 หรือ -1

พิจารณาถ้า $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

จะได้ $1 \equiv -1 \pmod{p}$ ซึ่งขัดแย้งกับ p เป็นจำนวนเฉพาะคี่

ซึ่งเป็นไปไม่ได้เพราะ $p > 2$.

ดังนั้น $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3. เนื่องจาก a เป็นผลเฉลยของ $x^2 \equiv a^2 \pmod{p}$

ดังนั้น $\left(\frac{a^2}{p}\right) = 1$

ตัวอย่าง 9.6 จงหา $\left(\frac{-25}{11}\right)$

วิธีทำ เนื่องจาก $\left(\frac{-25}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{25}{11}\right)$

และ $25 \equiv 3 \pmod{11}$ จะได้ $\left(\frac{25}{11}\right) = \left(\frac{3}{11}\right)$ นั่นคือ

$$\begin{aligned} \left(\frac{-25}{11}\right) &= \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) \\ &= \left(\frac{-3}{11}\right) \\ &= \left(\frac{8}{11}\right) \end{aligned}$$

จากตัวอย่าง 9.5 จะได้ $\left(\frac{8}{11}\right) = -1$

ดังนั้น $\left(\frac{-25}{11}\right) = -1$

จากตัวอย่าง 9.6 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{-25}{11}\right)$ ดังภาพประกอบ 9.4



legendre symbol (-25,11)

NATURAL LANGUAGE MATH INPUT EXTENDED KEYBOARD EXAMPLES UPLOAD RANDOM

Input

$\left(\frac{-25}{11}\right)$

$\left(\frac{n}{m}\right)$ is the Jacobi symbol

Result

-1

ภาพประกอบ 9.4 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{-25}{11}\right) = -1$

ทฤษฎีบท 9.2 นี้ยังสามารถนำไปช่วยตรวจสอบได้ว่าสมภาคกำลังสอง $x^2 \equiv a \pmod{p}$ มีผลเฉลยหรือไม่โดยพิจารณา $\left(\frac{a}{p}\right) = 1$ หรือไม่แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 9.7 จงตรวจสอบว่าสมภาค $x^2 \equiv 334 \pmod{31}$ มีผลเฉลยหรือไม่

วิธีทำ สมภาค $x^2 \equiv 334 \pmod{31}$ มีผลเฉลยก็ต่อเมื่อ $\left(\frac{334}{31}\right) = 1$

เนื่องจาก $334 \equiv 24 \pmod{31}$ จะได้

$$\left(\frac{334}{31}\right) = \left(\frac{24}{31}\right) = \left(\frac{3 \times 2 \times 2^2}{31}\right) = \left(\frac{3}{31}\right) \left(\frac{2}{31}\right) \left(\frac{2^2}{31}\right)$$

เนื่องจาก $\left(\frac{2^2}{31}\right) = 1$ จะได้

$$\left(\frac{334}{31}\right) = \left(\frac{3}{31}\right) \left(\frac{2}{31}\right)$$

พิจารณา $3^{\frac{31-1}{2}} \equiv 3^{15} \equiv -1 \pmod{31}$ นั่นคือ $\left(\frac{3}{31}\right) = -1$

พิจารณา $2^{\frac{31-1}{2}} \equiv 2^{15} \equiv 1 \pmod{31}$ นั่นคือ $\left(\frac{2}{31}\right) = 1$

แสดงว่า $\left(\frac{334}{31}\right) = (1)(-1) = -1$

ดังนั้น $x^2 \equiv 334 \pmod{31}$ ไม่มีผลเฉลย

ทฤษฎีบทต่อไปเป็นทฤษฎีที่ใช้ในการหาค่า $\left(\frac{-1}{p}\right)$ ภายใต้เงื่อนไขเฉพาะบางอย่างของ p

ทฤษฎีบท 9.3

กำหนดให้ p เป็นจำนวนเฉพาะคี่ แล้ว

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{4} \\ -1 & \text{ถ้า } p \equiv 3 \pmod{4} \end{cases}$$

พิสูจน์

ให้ p เป็นจำนวนเฉพาะคี่ จะได้

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

จาก $\left(\frac{-1}{p}\right)$ และ $(-1)^{\frac{p-1}{2}}$ มีค่าเป็น 1 หรือ -1

ให้ p เป็นจำนวนเฉพาะคี่ จะได้

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

กรณี $p \equiv 1 \pmod{4}$

จะได้ $p = 4k + 1$ เมื่อ k เป็นจำนวนเต็ม

$$\text{ดังนั้น } \left(\frac{-1}{p}\right) = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$$

กรณี $p \equiv 3 \pmod{4}$

จะได้ $p = 4l + 3$ เมื่อ l เป็นจำนวนเต็ม

$$\text{ดังนั้น } \left(\frac{-1}{p}\right) = (-1)^{\frac{4l+2}{2}} = (-1)^{2l+1} = -1$$

ตัวอย่าง 9.8 จงหา $\left(\frac{-1}{11}\right)$

วิธีทำ เนื่องจาก 11 เป็นจำนวนเฉพาะคี่ และ

$$11 \equiv 3 \pmod{4}$$

$$\text{ดังนั้น } \left(\frac{-1}{11}\right) = -1$$

ทฤษฎีบท 9.3 นอกจากจะใช้หาค่า $\left(\frac{-1}{p}\right)$ แล้ว สิ่งที่ได้ต่อจากทฤษฎีบทนี้คือสามารถตรวจสอบได้ว่าสมภาคกำลังสอง $x^2 \equiv a \pmod{p}$ แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 9.9 จงตรวจสอบว่าสมภาค $x^2 \equiv -9 \pmod{31}$ มีผลเฉลยหรือไม่

วิธีทำ สมภาค $x^2 \equiv -9 \pmod{31}$ มีผลเฉลยก็ต่อเมื่อ $\left(\frac{-9}{31}\right) = 1$

$$\left(\frac{-9}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{9}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{3^2}{31}\right)$$

เนื่องจาก $\left(\frac{-1}{31}\right) = -1$ เพราะว่า $31 \equiv 3 \pmod{4}$ และเนื่องจาก $\left(\frac{3^2}{31}\right) = 1$

$$\left(\frac{-9}{31}\right) = (-1)(1) = -1$$

ดังนั้น สมภาค $x^2 \equiv -9 \pmod{31}$ ไม่มีผลเฉลย

การหาส่วนตกค้างนอกจากการใช้ทฤษฎีบทที่ได้ศึกษามาแล้วยังมีอีกวิธีในการพิจารณาส่วนตกค้างกำลังสองซึ่งเรียกว่าบทตั้งของเกาส์ และนำเสนอเป็นทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 9.4 บทตั้งของเกาส์(Gauss's Lemma)

กำหนดให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็มที่ $(a, p) = 1$

ให้ n แทนจำนวนสมาชิกในเซต $S = \left\{a, 2a, \dots, \left(\frac{p-1}{2}\right)a\right\}$ ซึ่งเมื่อหารด้วย p

แล้วเหลือเศษมีค่ามากกว่า $\frac{p}{2}$ จะได้ว่า $\left(\frac{a}{p}\right) = (-1)^n$

พิสูจน์

เนื่องจาก $(a, p) = 1$ เราพบว่าจำนวนเต็ม 2 จำนวนใด ๆ ที่แตกต่างกันในเซต

S จะไม่สมภาคมอดุโล p และไม่มีจำนวนเต็มใด ๆ ในเซต S สมภาคกับศูนย์

ให้ $r_1, r_2, \dots, r_m$ เศษเหลือที่ได้จากการหารด้วย p ที่ $1 \leq r_j < \frac{p}{2}$ และ

$s_1, s_2, \dots, s_n$ เป็นเศษเหลือที่ $p > s_i > \frac{p}{2}$ แล้ว $m + n = \frac{p-1}{2}$

และจำนวนเต็ม

$$r_1, r_2, \dots, r_m, p - s_1, p - s_2, \dots, p - s_n$$

เป็นจำนวนเต็มบวกและน้อยกว่า $\frac{p}{2}$

ในการพิสูจน์ว่าจำนวนเต็มเหล่านี้แตกต่างกันทั้งหมดเป็นการเพียงพอที่จะพิสูจน์ว่าไม่มี $p - s_i$ ตัวใดเท่ากับ r_j ใด ๆ สมมติในทางตรงข้ามว่า

$$p - s_i = r_j \text{ สำหรับจำนวนเต็ม } i \text{ และ } j \text{ บางตัว}$$

จะมีจำนวนเต็ม u และ v ที่

$$1 \leq u, v \leq \frac{p-1}{2}$$

โดยที่

$$s_i \equiv ua \pmod{p} \text{ และ } r_j \equiv va \pmod{p}$$

เพราะฉะนั้น

$$(u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$$

แต่ $(a, p) = 1$ จะได้ $u+v \equiv 0 \pmod{p}$ แต่สมภาคนี้จะเป็นจริงไม่ได้

เพราะว่า $1 < u+v \leq p-1$ เนื่องจาก $m+n = \frac{p-1}{2}$ ดังนั้น

$$r_1, r_2, \dots, r_m, p - s_1, p - s_2, \dots, p - s_n$$

คือจำนวนเต็ม $1, 2, \dots, \frac{p-1}{2}$ โดยที่ลำดับไม่จำเป็นต้องตรงกัน

ผลคูณของจำนวนเต็มเหล่านี้คือ $\frac{p-1}{2}!$

$$\begin{aligned} \frac{p-1}{2}! &\equiv r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \\ &\equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \pmod{p} \\ &\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p} \end{aligned}$$

แต่จากที่เราทราบว่า $r_1, r_2, \dots, r_m, s_1, s_2, \dots, s_n$ สมภาคมอดุโล p กับ

$a, 2a, \dots, \left(\frac{p-1}{2}\right)a$ ในลำดับใดลำดับหนึ่ง ดังนั้น

$$\begin{aligned} \frac{p-1}{2}! &\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right)a \pmod{p} \\ &\equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned}$$

เนื่องจาก $\frac{p-1}{2}!$ เป็นจำนวนเฉพาะสัมพัทธ์กับ p จะได้

$$1 \equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \pmod{p}$$

โดยการคูณ $(-1)^n$ จะได้

$$a^{\left(\frac{p-1}{2}\right)} \equiv (-1)^n \pmod{p}$$

แสดงว่า

$$\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \equiv (-1)^n \pmod{p}$$

เพราะว่า $\left(\frac{a}{p}\right)$ มีค่าเป็น 1 หรือ -1 เท่านั้น

$$\text{นั่นคือ } \left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$$

ตัวอย่าง 9.10 จงหา $\left(\frac{6}{17}\right)$ โดยใช้บทตั้งของเกาส์

วิธีทำ เนื่องจาก $\frac{p-1}{2} = \frac{17-1}{2} = 8$ เพราะฉะนั้นจะได้

$$S = \{a, 2a, 3a, 4a, 5a, 6a, 7a, 8a\} = \{6, 12, 18, 24, 30, 36, 42, 48\}$$

พิจารณาเศษเหลือที่เหลือจากการหารจำนวนเต็มใน S ด้วย 17 ดังนี้

6 หารด้วย 17 เหลือเศษ 6

12 หารด้วย 17 เหลือเศษ 12

18 หารด้วย 17 เหลือเศษ 1

24 หารด้วย 17 เหลือเศษ 7

30 หารด้วย 17 เหลือเศษ 13

36 หารด้วย 17 เหลือเศษ 2

42 หารด้วย 17 เหลือเศษ 8

48 หารด้วย 17 เหลือเศษ 14

จะเห็นว่าจำนวนเต็มในเซต S ที่หารด้วย 17 แล้วมีเศษเหลือมากกว่า $\frac{17}{2}$

มีทั้งหมด 3 จำนวน จากบทตั้งของเกาส์จะได้ว่า

$$\left(\frac{a}{p}\right) = \left(\frac{6}{17}\right) = (-1)^3 = -1$$

$$\text{ดังนั้น } \left(\frac{6}{17}\right) = -1$$

จากตัวอย่าง 9.10 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{6}{17}\right)$ ดังภาพประกอบ 9.5



ภาพประกอบ 9.5 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{6}{17}\right) = -1$

ตัวอย่าง 9.11 จงหา $\left(\frac{3}{13}\right)$ โดยใช้บทตั้งของเกาส์

วิธีทำ เนื่องจาก $\frac{p-1}{2} = \frac{13-1}{2} = 6$ เพราะฉะนั้นจะได้

$$S = \{a, 2a, 3a, 4a, 5a, 6a\} = \{3, 6, 9, 12, 15, 18\}$$

พิจารณาเศษเหลือที่เหลือจากการหารจำนวนเต็มใน S ด้วย 11 ดังนี้

3 หารด้วย 13 เหลือเศษ 3

6 หารด้วย 13 เหลือเศษ 6

9 หารด้วย 13 เหลือเศษ 9

12 หารด้วย 13 เหลือเศษ 12

15 หารด้วย 13 เหลือเศษ 2

18 หารด้วย 13 เหลือเศษ 5

จะเห็นว่าจำนวนเต็มในเซต S ที่หารด้วย 13 แล้วมีเศษเหลือมากกว่า $\frac{13}{2}$

มีทั้งหมด 2 จำนวนจากบทตั้งของเกาส์จะได้ว่า

$$\left(\frac{a}{p}\right) = \left(\frac{3}{13}\right) = (-1)^2 = 1$$

ดังนั้น $\left(\frac{3}{13}\right) = 1$

จาก $\left(\frac{6}{17}\right) = -1$ และ $\left(\frac{3}{13}\right) = 1$ ในตัวอย่าง 9.10 และ 9.11 ทำให้ทราบว่าสมภาค $x^2 \equiv 6 \pmod{17}$ ไม่มีผลเฉลย และ $x^2 \equiv 3 \pmod{13}$ มีผลเฉลย นอกจากนี้ผลที่ตามมาจากบทตั้งของเกาส์ทำให้สามารถหาค่า $\left(\frac{2}{p}\right)$ ภายใต้เงื่อนไขเฉพาะบางอย่างของ p แสดงอยู่ในรูปทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 9.5

กำหนดให้ p เป็นจำนวนเฉพาะคี่ แล้ว

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{8} \text{ หรือ } p \equiv 7 \pmod{8} \\ -1 & \text{ถ้า } p \equiv 3 \pmod{8} \text{ หรือ } p \equiv 5 \pmod{8} \end{cases}$$

พิสูจน์

จากบทตั้งของเกาส์จะได้ว่า $\left(\frac{2}{p}\right) = (-1)^n$ โดยที่ n เป็นจำนวนของจำนวนเต็มในเซต

$$S = \left\{1 \cdot 2, 2 \cdot 2, \dots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

ซึ่งเมื่อหารด้วย p แล้วเหลือเศษเหลือเกิน $\frac{2}{p}$ สมาชิกทุกจำนวนในเซต S

จะน้อยกว่า p ดังนั้นจึงเป็นการเพียงพอที่จะนับว่ามีกี่จำนวนที่เกิน $\frac{2}{p}$

สำหรับ $1 \leq k \leq \frac{p-1}{2}$ เรามี $2k < \frac{p}{2}$ ก็ต่อเมื่อ $k < \frac{p}{4}$

ถ้า $\lfloor \cdot \rfloor$ แทนฟังก์ชันจำนวนเต็มมากที่สุดแล้ว จะมีจำนวนเต็มใน S

ที่น้อยกว่า $\frac{2}{p}$ อยู่ $\left\lfloor \frac{p}{4} \right\rfloor$ เพราะฉะนั้น

$$n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$$

เป็นจำนวนของจำนวนเต็มที่เกิน $\frac{2}{p}$

เนื่องจาก p เป็นจำนวนเฉพาะคี่ p อาจจะอยู่ในรูปใดรูปหนึ่ง คือ

$$8k+1, 8k+3, 8k+5 \text{ หรือ } 8k+7$$

พิจารณา ดังนี้

ถ้า $p = 8k + 1$ แล้ว

$$n = \frac{8k + 1 - 1}{2} - \left\lfloor \frac{8k + 1}{4} \right\rfloor = 4k - \left\lfloor 2k + \frac{1}{4} \right\rfloor = 4k - 2k = 2k$$

ถ้า $p = 8k + 3$ แล้ว

$$n = \frac{8k + 3 - 1}{2} - \left\lfloor \frac{8k + 3}{4} \right\rfloor = 4k + 1 - \left\lfloor 2k + \frac{3}{4} \right\rfloor = 2k + 1$$

ถ้า $p = 8k + 5$ แล้ว

$$\begin{aligned} n &= \frac{8k + 5 - 1}{2} - \left\lfloor \frac{8k + 5}{4} \right\rfloor = 4k + 2 - \left\lfloor 2k + 1 + \frac{1}{4} \right\rfloor \\ &= 4k + 2 - (2k + 1) = 2k + 1 \end{aligned}$$

ถ้า $p = 8k + 7$ แล้ว

$$\begin{aligned} n &= \frac{8k + 7 - 1}{2} - \left\lfloor \frac{8k + 7}{4} \right\rfloor = 4k + 3 - \left\lfloor 2k + 1 + \frac{3}{4} \right\rfloor \\ &= 4k + 3 - (2k + 1) = 2k + 2 \end{aligned}$$

ดังนั้นเมื่อ p อยู่ในรูป $8k + 1$ หรือ $8k + 7$ แล้ว n เป็น คู่ และ $\left(\frac{2}{p}\right) = 1$

เมื่อ p อยู่ในรูป $8k + 3$ หรือ $8k + 5$ แล้ว n เป็น คี่ และ $\left(\frac{2}{p}\right) = -1$

สังเกตว่าถ้าจำนวนเฉพาะ p อยู่ในรูป $8k \pm 1$

นั่นคือ $p \equiv 1 \pmod{8}$ หรือ $p \equiv 7 \pmod{8}$ แล้ว

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$$

เป็นจำนวนเต็มคู่ ในกรณีนี้เราได้

$$(-1)^{\frac{p^2-1}{8}} = 1 = \left(\frac{2}{p}\right)$$

และถ้าจำนวนเฉพาะ p อยู่ในรูป $8k \pm 3$

นั่นคือ $p \equiv 3 \pmod{8}$ หรือ $p \equiv 5 \pmod{8}$ แล้ว

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 84k + 8}{8} = 8k^2 \pm 6k + 1$$

เป็นจำนวนเต็มคี่ ในกรณีนี้เราได้

$$(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$$

ตัวอย่าง 9.12

$$\left(\frac{2}{17}\right) = 1 \text{ เนื่องจาก } 17 \equiv 1 \pmod{8}$$

$$\left(\frac{2}{31}\right) = 1 \text{ เนื่องจาก } 31 \equiv 7 \pmod{8}$$

$$\left(\frac{2}{103}\right) = 1 \text{ เนื่องจาก } 103 \equiv 7 \pmod{8}$$

$$\left(\frac{2}{101}\right) = -1 \text{ เนื่องจาก } 101 \equiv 5 \pmod{8}$$

$$\left(\frac{2}{19}\right) = -1 \text{ เนื่องจาก } 19 \equiv 3 \pmod{8}$$

9.3 กฎส่วนกลับกำลังสอง

ในการตรวจสอบว่าสมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลยหรือไม่ในหัวข้อที่ผ่านมา ใช้วิธีการตรวจสอบโดยการใช้สัญลักษณ์เลอจองดร์ สำหรับกฎส่วนกลับกำลังสองนี้ก็เป็นอีกวิธีที่เป็นประโยชน์ในการตรวจสอบสมภาค $x^2 \equiv a \pmod{p}$ ว่ามีผลเฉลยหรือไม่ โดยเริ่มจาก ปัญหาความสัมพันธ์ $\left(\frac{p}{q}\right)$ และ $\left(\frac{q}{p}\right)$ เมื่อ p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน ในปี ค.ศ. 1785 เลอจองดร์ ได้แสดงความสัมพันธ์ดังกล่าว และเรียกว่ากฎส่วนกลับกำลังสอง ในปี ค.ศ. 1783 เกาส์ เป็นบุคคลแรกที่สามารถพิสูจน์กฎส่วนกลับกำลังสองได้อย่างสมบูรณ์ แสดงในรูปทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 9.6 (กฎส่วนกลับกำลังสอง)

กำหนดให้ p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน จะได้ว่า

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

พิสูจน์

พิจารณาสี่เหลี่ยมด้านขนานในระนาบ xy โดยมีจุดยอดอยู่ที่จุด

$$(0,0), \left(\frac{p}{2}, 0\right), \left(0, \frac{q}{2}\right) \text{ และ } \left(\frac{p}{2}, \frac{q}{2}\right)$$

ให้ R เป็นบริเวณภายในสี่เหลี่ยมรูปนี้โดยไม่รวมเส้นขอบ

จะเรียกจุดที่มีพิกัดเป็นจำนวนเต็มว่าจุดแลตทิซ

เราต้องการนับจำนวนแลตทิซในบริเวณ R

เนื่องจาก p และ q ต่างก็เป็นจำนวนเฉพาะ จุดแลตทิซใน R

ประกอบด้วยจุด (m, n) ซึ่ง $1 \leq n \leq \frac{(p-1)}{2}$ และ $1 \leq m \leq \frac{(q-1)}{2}$

ดังนั้นจำนวนจุดทั้งหมดจะเท่ากับ $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

เส้นทแยงมุม D จาก $(0,0)$ ไปยัง $\left(\frac{p}{2}, \frac{q}{2}\right)$ มีสมการเป็น $y = \left(\frac{q}{p}\right)x$ หรือ

$py = qx$ เพราะว่า $(p, q) = 1$ ดังนั้นไม่มีจุดแลตทิซภายใน R อยู่บน D

เพราะถ้ามีจุดแลตทิซ (m, n) บน D ดังนั้น $pn = qm$ นั่นคือ $p|m$ และ $q|n$

ซึ่งเป็นไปไม่ได้ เพราะว่า $1 \leq m < p$ และ $1 \leq n < q$

สมมติให้ T_1 แทนส่วนของ R ที่อยู่ใต้เส้นทแยงมุม D

และ T_2 แทนส่วนของ R ที่อยู่เหนือเส้นทแยงมุม D

การนับจุดแลตทิซใน R จึงเท่ากับการนับจุดในแลตทิซภายในสามเหลี่ยมสองรูปนี้

จำนวนของจำนวนเต็มในช่วง $0 < y < \frac{kq}{p}$ คือ $\left\lfloor \frac{kq}{p} \right\rfloor$ ดังนั้น สำหรับ

$1 \leq k \leq \frac{(p-1)}{2}$ จะมีจุดแลตทิซที่อยู่เหนือจุด $(k, 0)$ ไปยัง $\left(k, \frac{kq}{p}\right)$

จะมีทั้งหมดเท่ากับ $\left\lfloor \frac{kq}{p} \right\rfloor$ เพราะฉะนั้น จำนวนแลตทิซที่อยู่ใน T_1 เท่ากับ

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$$

การคำนวณในทำนองเดียวกัน โดยการสลับเปลี่ยนบทบาทของ q และ p

จะได้ว่า จำนวนจุดแลตทิซทั้งหมดใน T_2 เท่ากับ

$$\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$$

ดังนั้นจำนวนจุดแลตทิซทั้งหมดใน R เท่ากับ

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$$

จะได้

$$\begin{aligned}
\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= \left((-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor}\right) \left((-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor}\right) \\
&= (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor} + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \\
&= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}
\end{aligned}$$

นั่นคือ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

ความสัมพันธ์ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ เมื่อ p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน ที่เป็นกฎส่วนกลับ

กำลังสองในทฤษฎีบทที่ผ่านมาแล้วยังมีความสัมพันธ์ในรูปแบบอื่น ๆ โดยแสดงอยู่ในรูปบทแทรกต่อไป

บทแทรก 9.1

กำหนดให้ p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน จะได้ว่า

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{4} \text{ หรือ } q \equiv 1 \pmod{4} \\ -1 & \text{ถ้า } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

พิสูจน์

เพราะว่า $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ เป็นจำนวนคู่ ก็ต่อเมื่อ

$$p = 4k + 1 \text{ หรือ } q = 4k + 1$$

โดยทฤษฎีบทกฎส่วนกลับกำลังสองจะได้ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$

เพราะว่า $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ เป็นจำนวนคี่ ก็ต่อเมื่อ

$$p = 4k + 3 \text{ หรือ } q = 4k + 3$$

โดยทฤษฎีบทกฎส่วนกลับกำลังสองจะได้ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$

ถ้า $\left(\frac{q}{p}\right)$ คูณเข้าทั้งสองข้างของสมภาคในบทแทรก 9.1 และจากข้อเท็จจริง $\left(\frac{q}{p}\right)^2 = 1$

จะได้บทแทรกดังต่อไปนี้

บทแทรก 9.2

กำหนดให้ p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน จะได้ว่า

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{ถ้า } p \equiv 1 \pmod{4} \text{ หรือ } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{ถ้า } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

พิสูจน์

ให้ $p \equiv 1 \pmod{4}$ หรือ $q \equiv 1 \pmod{4}$ โดยบทแทรก 9.1 จะได้

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$$

ดังนั้น $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = \left(\frac{q}{p}\right)$ เนื่องจาก $\left(\frac{q}{p}\right)^2 = 1$

$$\text{เพราะฉะนั้น } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

ให้ $p \equiv q \equiv 3 \pmod{4}$ โดยบทแทรก 9.1 จะได้

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$$

ดังนั้น $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = -\left(\frac{q}{p}\right)$ เนื่องจาก $\left(\frac{q}{p}\right)^2 = 1$

$$\text{เพราะฉะนั้น } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

ตัวอย่าง 9.13 จงหา $\left(\frac{5}{17}\right)$

วิธีทำ เนื่องจาก $5 \equiv 1 \pmod{4}$ และ $17 \equiv 1 \pmod{4}$

$$\text{แสดงว่า } \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right)$$

$$\text{เนื่องจาก } \left(\frac{17}{5}\right) = \left(\frac{3}{5}\right)$$

$$\text{พิจารณาหา } \left(\frac{3}{5}\right) \text{ จาก } 3^{\frac{5-1}{2}} = 3^2 \equiv -1 \pmod{5}$$

$$\text{ดังนั้น } \left(\frac{5}{17}\right) = -1$$

$$\text{ตัวอย่าง 9.14 จงหา } \left(\frac{13}{17}\right)$$

$$\text{วิธีทำ เนื่องจาก } 13 \equiv 1 \pmod{4} \text{ และ } 17 \equiv 1 \pmod{4}$$

$$\text{แสดงว่า } \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$$

$$\text{เนื่องจาก } \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right)$$

$$\text{และ } \left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$$

$$\text{ดังนั้น } \left(\frac{13}{17}\right) = 1$$

$$\text{ตัวอย่าง 9.15 จงหา } \left(\frac{7}{23}\right)$$

$$\text{วิธีทำ เนื่องจาก } 7 \equiv 3 \pmod{4} \text{ และ } 23 \equiv 3 \pmod{4}$$

$$\text{แสดงว่า } \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right)$$

$$\text{เนื่องจาก } \left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right)$$

$$\text{พิจารณาหา } \left(\frac{2}{7}\right) \text{ จาก } 2^{\frac{7-1}{2}} \equiv 2^3 \equiv 1 \pmod{7}$$

$$\text{นั่นคือ } -\left(\frac{2}{7}\right) = -1$$

$$\text{ดังนั้น } \left(\frac{7}{23}\right) = -1$$

ตัวอย่าง 9.16 จงหา $\left(\frac{559}{53}\right)$

วิธีทำ เนื่องจาก $53 \equiv 1 \pmod{4}$ และ $29 \equiv 1 \pmod{4}$ จะได้

$$\left(\frac{559}{53}\right) = \left(\frac{29}{53}\right) = \left(\frac{53}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{2^2}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$$

พิจารณา $\left(\frac{2}{29}\right)$ ดังต่อไปนี้

$$\left(\frac{2}{29}\right) = \left(\frac{29}{2}\right) = \left(\frac{1}{2}\right) = 1$$

พิจารณา $\left(\frac{3}{29}\right)$ ดังต่อไปนี้

$$\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\text{จะได้ } \left(\frac{559}{53}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = (1)(1) = 1$$

ดังนั้น $\left(\frac{559}{53}\right) = 1$

จากตัวอย่าง 9.16 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{559}{53}\right)$ ดังภาพประกอบ 9.6



ภาพประกอบ 9.6 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{559}{53}\right) = 1$

กรณีเฉพาะอีกกรณีหนึ่งของสัญลักษณ์เลอจองดร์ที่อยู่ในรูป $\left(\frac{3}{p}\right)$ โดยที่ p เป็นจำนวนเฉพาะคี่โดยที่ $p \neq 3$ นำเสนอในรูปแบบทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 9.7

กำหนดให้ p เป็นจำนวนเฉพาะคี่ โดยที่ $p \neq 3$ แล้ว

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv \pm 1 \pmod{12} \\ -1 & \text{ถ้า } p \equiv \pm 5 \pmod{12} \end{cases}$$

พิสูจน์

เนื่องจาก $3 \equiv 3 \pmod{4}$ โดยบทแทรก 9.2 จะได้

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{ถ้า } p \equiv 1 \pmod{4} \\ -\left(\frac{p}{3}\right) & \text{ถ้า } p \equiv 3 \pmod{4} \end{cases}$$

จาก p เป็นจำนวนเฉพาะคี่

แสดงว่า $p \equiv 1 \pmod{3}$ หรือ $p \equiv 2 \pmod{3}$ อย่างใดอย่างหนึ่ง

จากทฤษฎีบท 9.2 ข้อ 1 จะได้

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{1}{3}\right) & \text{ถ้า } p \equiv 1 \pmod{3} \\ \left(\frac{2}{3}\right) & \text{ถ้า } p \equiv 2 \pmod{3} \end{cases}$$

จากทฤษฎีบท 9.2 ข้อ 2 จะได้

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{3} \\ -1 & \text{ถ้า } p \equiv 2 \pmod{3} \end{cases}$$

จากสมภาคข้างต้นจะได้ว่า

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{4} \text{ และ } p \equiv 1 \pmod{3} \text{ หรือ} \\ & \text{ถ้า } p \equiv 3 \pmod{4} \text{ และ } p \equiv 2 \pmod{3} \\ -1 & \text{ถ้า } p \equiv 1 \pmod{4} \text{ และ } p \equiv 2 \pmod{3} \text{ หรือ} \\ & \text{ถ้า } p \equiv 3 \pmod{4} \text{ และ } p \equiv 1 \pmod{3} \end{cases}$$

หรือ

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv 1 \pmod{4} \text{ และ } p \equiv 1 \pmod{3} \text{ หรือ} \\ & \text{ถ้า } p \equiv -1 \pmod{4} \text{ และ } p \equiv -1 \pmod{3} \\ -1 & \text{ถ้า } p \equiv 5 \pmod{4} \text{ และ } p \equiv 5 \pmod{3} \text{ หรือ} \\ & \text{ถ้า } p \equiv -5 \pmod{4} \text{ และ } p \equiv -5 \pmod{3} \end{cases}$$

จะได้

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ถ้า } p \equiv \pm 1 \pmod{12} \\ -1 & \text{ถ้า } p \equiv \pm 5 \pmod{12} \end{cases}$$

ตัวอย่าง 9.17

$$\left(\frac{3}{17}\right) = -1 \text{ เนื่องจาก } 17 \equiv 5 \pmod{12}$$

$$\left(\frac{3}{733}\right) = 1 \text{ เนื่องจาก } 733 \equiv 1 \pmod{12}$$

$$\left(\frac{3}{941}\right) = -1 \text{ เนื่องจาก } 941 \equiv 5 \pmod{12}$$

9.4 สัญลักษณ์ยาโคบี

สัญลักษณ์ยาโคบี เป็นสัญลักษณ์ที่มีความเกี่ยวข้องกับส่วนตกค้างกำลังสอง ซึ่งสัญลักษณ์นี้เป็นสัญลักษณ์ที่เป็นกรณีทั่วไปของสัญลักษณ์เลอจองด์ โดยนักคณิตศาสตร์ชาวเยอรมัน ชื่อ คาร์ล กุสทาวฟ ยาคอบ ยาโคบี มีบทนิยามดังต่อไปนี้

บทนิยาม 9.4

กำหนดให้ n เป็นจำนวนเต็มบวกคี่ซึ่งสามารถเขียนอยู่ในรูปผลคูณของจำนวนเฉพาะ $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ และ a เป็นจำนวนเต็มที่ $(a, n) = 1$ สัญลักษณ์ยาโคบี

$\left(\frac{a}{n}\right)$ กำหนดโดย

$$\left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{k_i} = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_r}\right)^{k_r}$$

ตัวอย่าง 9.18 จงหาค่า $\left(\frac{2}{9}\right)$

วิธีทำ เนื่องจาก $9 = 3 \cdot 3$

$$\text{จะได้ } \left(\frac{2}{9}\right) = \left(\frac{2}{3 \cdot 3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = \left(\frac{2}{3}\right)^2 = 1$$

ดังนั้น $\left(\frac{2}{9}\right) = 1$

จากตัวอย่าง 9.18 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{2}{9}\right)$ ดังภาพประกอบ 9.7



ภาพประกอบ 9.7 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{2}{9}\right) = 1$

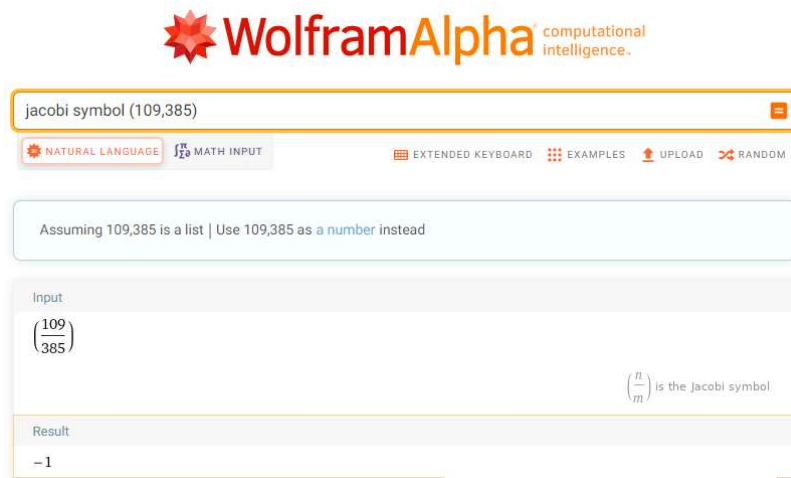
ตัวอย่าง 9.19 จงหาค่า $\left(\frac{109}{385}\right)$

วิธีทำ เนื่องจาก $385 = 5 \cdot 7 \cdot 11$

$$\begin{aligned} \text{จะได้ } \left(\frac{109}{385}\right) &= \left(\frac{109}{5 \cdot 7 \cdot 11}\right) \\ &= \left(\frac{109}{5}\right)\left(\frac{109}{7}\right)\left(\frac{109}{11}\right) \\ &= \left(\frac{4}{5}\right)\left(\frac{4}{7}\right)\left(\frac{10}{11}\right) \\ &= \left(\frac{2^2}{5}\right)\left(\frac{2^2}{7}\right)\left(\frac{10}{11}\right) \\ &= 1 \cdot 1 \cdot (-1) \\ &= -1 \end{aligned}$$

ดังนั้น $\left(\frac{109}{385}\right) = -1$

จากตัวอย่าง 9.19 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{109}{385}\right)$ ดังภาพประกอบ 9.8



ภาพประกอบ 9.8 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{109}{385}\right) = -1$

สัญลักษณ์ยาโคบี $\left(\frac{a}{n}\right)$ ในกรณีที่ n เป็นจำนวนเฉพาะเราพบว่าสัญลักษณ์ยาโคบีกับ

สัญลักษณ์เลอจองดร์ คือสัญลักษณ์เดียวกัน ทำให้สมบัติของสัญลักษณ์ยาโคบีบางสมบัตินั้นคล้ายกันกับสัญลักษณ์เลอจองดร์ ซึ่งจะนำเสนอเป็นทฤษฎีบทต่อไปนี้

ทฤษฎีบท 9.8

กำหนดให้ n และ m เป็นจำนวนเต็มบวกคือ a และ b เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์กับ n และ m จะได้ว่า

1. ถ้า $a \equiv b \pmod{n}$ แล้ว $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$
3. $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \left(\frac{a}{m}\right)$

พิสูจน์

ให้ n เขียนในรูปผลคูณของจำนวนเฉพาะได้เป็น

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \text{ และ } m = q_1^{e_1} q_2^{e_2} \dots q_s^{e_s}$$

1. จาก $(a, n) = 1$ จึงได้ว่า $(a, p_i) = 1$ สำหรับ $1 \leq i \leq r$
 เนื่องจาก $a \equiv b \pmod{n}$ จึงได้ว่า $a \equiv b \pmod{p_i}$

โดยทฤษฎีบท 9.2 จึงได้ว่า

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \text{ สำหรับ } 1 \leq i \leq r$$

$$\text{ดังนั้น } \left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{k_i} = \prod_{i=1}^r \left(\frac{b}{p_i}\right)^{k_i} = \left(\frac{b}{n}\right)$$

2. จาก $(a, n) = 1$ จึงได้ว่า $(a, p_i) = 1$ สำหรับ $1 \leq i \leq r$

โดยบทนิยาม และทฤษฎีบท 9.2 จึงได้ว่า

$$\begin{aligned} \left(\frac{ab}{n}\right) &= \prod_{i=1}^r \left(\frac{ab}{p_i}\right)^{k_i} \\ &= \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{k_i} \left(\frac{b}{p_i}\right)^{k_i} \\ &= \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{k_i} \prod_{i=1}^r \left(\frac{b}{p_i}\right)^{k_i} \\ &= \left(\frac{a}{n}\right) \left(\frac{b}{n}\right) \end{aligned}$$

3. จาก $(a, n) = 1$ จึงได้ว่า $(a, p_i) = (a, q_j) = 1$ สำหรับ $1 \leq i \leq r$

และ $1 \leq i \leq s$ โดยบทนิยาม และทฤษฎีบท 9.2 จึงได้ว่า

$$\begin{aligned} \left(\frac{a}{nm}\right) &= \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{k_i} \prod_{i=1}^s \left(\frac{a}{q_i}\right)^{e_i} \\ &= \left(\frac{a}{n}\right) \left(\frac{a}{m}\right) \end{aligned}$$

ตัวอย่าง 9.20 จงหา $\left(\frac{21}{55}\right)$

วิธีทำ เนื่องจาก 55 เป็นจำนวนเต็มบวกคี่ โดยที่ $55 = 5 \cdot 11$

5 และ 11 เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์กับ 21
 จะได้

$$\left(\frac{21}{55}\right) = \left(\frac{7}{55}\right) \left(\frac{3}{55}\right)$$

พิจารณา

$$\left(\frac{7}{55}\right) = \left(\frac{7}{5}\right)\left(\frac{7}{11}\right) = (-1)(-1) = 1$$

$$\left(\frac{3}{55}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{11}\right) = (-1)(1) = -1$$

ดังนั้น $\left(\frac{21}{55}\right) = -1$

จากตัวอย่าง 9.20 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{21}{55}\right)$ ดังภาพประกอบ 9.9



ภาพประกอบ 9.9 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{21}{55}\right) = -1$

สำหรับทฤษฎีบทต่อไปเป็นทฤษฎีบทที่ใช้ในการหาค่า $\left(\frac{a}{n}\right)$ โดยที่ n เป็นจำนวนเต็มบวก

ที่มากกว่า 2 แบ่งเป็นสองกรณีคือกรณีที่ $a = -1$ และ $a = 2$

ทฤษฎีบท 9.9

กำหนดให้ n เป็นจำนวนเต็มบวกที่ โดยที่ $n > 2$ จะได้ว่า

$$1. \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

$$2. \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

พิสูจน์

ให้ n เขียนในรูปผลคูณของจำนวนเฉพาะได้เป็น

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

1. จาก $(a, n) = 1$ จึงได้ว่า $(a, p_i) = 1$ สำหรับ $1 \leq i, j \leq r$

โดยทฤษฎีบท 9.2 จะได้

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right)^{k_i} = \left[(-1)^{\sum_{i=1}^r \frac{p_i-1}{2}}\right]^{k_i} = (-1)^{\sum_{i=1}^r \frac{k_i(p_i-1)}{2}}$$

สามารถเขียน n ได้ใหม่ในรูป

$$n = \prod_{i=1}^r (1 + (p_i - 1))^{k_i}$$

เพราะว่า $p_i - 1$ เป็นจำนวนคู่ จึงได้ว่า

$$(1 + (p_i - 1))^{k_i} = 1 + k_i(p_i - 1) \pmod{4}$$

และ

$$(1 + k_i(p_i - 1))(1 + k_j(p_j - 1)) \equiv (1 + k_i(p_i - 1)) + k_j(p_j - 1) \pmod{4}$$

ดังนั้น

$$n = \sum_{i=1}^r (1 + k_i(p_i - 1)) \pmod{4}$$

จะได้ว่า

$$\frac{n-1}{2} = \sum_{i=1}^r \frac{k_i(p_i - 1)}{2} \pmod{2}$$

$$\text{และจาก } \left(\frac{-1}{n}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right)^{k_i} = \left[(-1)^{\sum_{i=1}^r \frac{p_i-1}{2}}\right]^{k_i} = (-1)^{\sum_{i=1}^r \frac{k_i(p_i-1)}{2}}$$

$$\text{นั่นคือ } \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

2. จาก $(a, n) = 1$ จึงได้ว่า $(a, p_i) = 1$ สำหรับ $1 \leq i, j \leq r$

โดยทฤษฎีบท 9.2 จะได้ว่า

$$\left(\frac{2}{n}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right)^{k_i} = \prod_{i=1}^r \left[(-1)^{\frac{p_i^2-1}{8}}\right]^{k_i} = \left[(-1)^{\sum_{i=1}^r \left(\frac{p_i^2-1}{8}\right)}\right]^{k_i} = (-1)^{\sum_{i=1}^r \left(\frac{k_i(p_i^2-1)}{8}\right)}$$

และ

$$n^2 = \prod_{i=1}^r (1 + (p_i^2 - 1))^{k_i}$$

เพราะว่า $p_i^2 - 1 \equiv 0 \pmod{8}$ เราจะได้ว่า

$$(1 + (p_i^2 - 1))^{k_i} = 1 + k_i(p_i^2 - 1) \pmod{64}$$

และ

$$(1 + k_i(p_i^2 - 1))(1 + k_j(p_j^2 - 1)) \equiv (1 + k_i(p_i^2 - 1)) + k_j(p_j^2 - 1) \pmod{64}$$

ดังนั้น

$$n^2 = \sum_{i=1}^r (1 + k_i(p_i^2 - 1)) \pmod{64}$$

จะได้ว่า

$$\frac{n^2 - 1}{8} = \sum_{i=1}^r \frac{k_i(p_i^2 - 1)}{8} \pmod{8}$$

และจาก

$$\left(\frac{2}{n}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right)^{k_i} = \prod_{i=1}^r \left[(-1)^{\frac{p_i^2-1}{8}}\right]^{k_i} = \left[(-1)^{\sum_{i=1}^r \left(\frac{p_i^2-1}{8}\right)}\right]^{k_i} = (-1)^{\sum_{i=1}^r \left(\frac{k_i(p_i^2-1)}{8}\right)}$$

นั่นคือ

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

ตัวอย่าง 9.21 จงหาค่า $\left(\frac{2}{101}\right)$

วิธีทำ เนื่องจาก 101 เป็นจำนวนเต็มบวกคือ

จะได้

$$\left(\frac{2}{101}\right) = (-1)^{\frac{101^2-1}{8}} = (-1)^{1275} = -1$$

ดังนั้น $\left(\frac{2}{101}\right) = -1$

ตัวอย่าง 9.22 จงหาค่า $\left(\frac{-1}{9}\right)$

วิธีทำ เนื่องจาก 9 เป็นจำนวนเต็มบวกคือ

จะได้

$$\left(\frac{-1}{9}\right) = (-1)^{\frac{9-1}{2}} = (-1)^4 = 1$$

ดังนั้น $\left(\frac{-1}{9}\right) = 1$

ตัวอย่าง 9.23 จงหาค่า $\left(\frac{10}{21}\right)$

วิธีทำ เนื่องจาก 21 เป็นจำนวนเต็มบวกคี่ โดยที่ $21 = 3 \cdot 7$

3 และ 7 เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์กับ 10
จะได้

$$\left(\frac{10}{21}\right) = \left(\frac{2}{21}\right) \left(\frac{5}{21}\right)$$

พิจารณา

$$\left(\frac{2}{21}\right) = (-1)^{\frac{21^2-1}{8}} = (-1)^{55} = -1$$

$$\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right) \left(\frac{5}{7}\right) = (-1)(-1) = 1$$

ดังนั้น $\left(\frac{10}{21}\right) = -1$

จากตัวอย่าง 9.23 สามารถใช้ Wolfram Alpha เพื่อหา $\left(\frac{10}{21}\right)$ ดังภาพประกอบ 9.10



ภาพประกอบ 9.10 ใช้ Wolfram Alpha เพื่อแสดงว่า $\left(\frac{10}{21}\right) = -1$

การตรวจสอบสมภาค $x^2 \equiv a \pmod{p}$ ว่ามีผลเฉลยหรือไม่ขึ้นโดยสัญลักษณ์ของเลอจองดร์

สำหรับจำนวนเต็ม a ที่ $(a, p) = 1$ สมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $\left(\frac{a}{p}\right) = 1$ แต่

สำหรับสัญลักษณ์ของยาโคบีนั้น บทกลับของทฤษฎีจะไม่เป็นจริง ซึ่งได้นำเสนอในรูปแบบทฤษฎีบท
ดังต่อไปนี้

ทฤษฎีบท 9.10

สำหรับจำนวนเต็ม a และ n โดยที่ n เป็นจำนวนเต็มบวก และ $(a, n) = 1$

ถ้าสมภาค $x^2 \equiv a \pmod{n}$ มีผลเฉลยแล้ว $\left(\frac{a}{n}\right) = 1$

พิสูจน์

สมภาค $x^2 \equiv a \pmod{n}$ มีผลเฉลย จะได้ว่า

สำหรับทุก ๆ จำนวนเฉพาะ p ที่ $p|n$

ทำให้ $x^2 \equiv a \pmod{p}$ มีผลเฉลยด้วย ทำให้ $(a, p) = 1$

$$\text{ดังนั้น } \left(\frac{a}{p}\right) = 1$$

บทกลับของทฤษฎีบท 9.10 นั้นไม่จริงเสมอไป เช่น $\left(\frac{a}{n}\right) = 1$ แต่ $x^2 \equiv a \pmod{n}$ อาจจะมีหรือไม่มีผลเฉลยก็ได้ แต่ทฤษฎีบทดังกล่าวนี้เพียงใช้ตรวจสอบว่า $x^2 \equiv a \pmod{n}$ ไม่มีผลเฉลย เช่น จากตัวอย่าง $\left(\frac{2}{101}\right) = -1$ และ $\left(\frac{10}{21}\right) = -1$ แสดงว่าสมภาค $x^2 \equiv 2 \pmod{101}$ และ $x^2 \equiv 10 \pmod{21}$ ไม่มีผลเฉลย

ทฤษฎีบทต่อไปจะแสดงว่าส่วนกลับกำลังสองสำหรับสัญลักษณ์ยาโคบินั้นเป็นจริงเหมือนกันกับส่วนกลับของสัญลักษณ์เลอจองด์

ทฤษฎีบท 9.11

กำหนดให้ n และ m เป็นจำนวนเต็มบวกคู่ ซึ่ง $(m, n) = 1$ จะได้ว่า

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\left(\frac{n-1}{2}\right)\left(\frac{m-1}{2}\right)}$$

พิสูจน์

ให้ $m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ เมื่อ $p_1, p_2, \dots, p_s$ เป็นจำนวนเฉพาะคู่

และ $n = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$ เมื่อ $q_1, q_2, \dots, q_r$ เป็นจำนวนเฉพาะคู่

ดังนั้น

$$\left(\frac{m}{n}\right) = \prod_{i=1}^r \left(\frac{m}{q_j}\right)^{b_i} = \prod_{i=1}^r \prod_{j=1}^s \left(\frac{p_j}{q_i}\right)^{b_i a_j}$$

และ

$$\left(\frac{n}{m}\right) = \prod_{j=1}^s \left(\frac{n}{p_j}\right)^{a_j} = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{q_i}{p_j}\right)^{a_j b_i}$$

ดังนั้น

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \prod_{i=1}^r \prod_{j=1}^s \left[\left(\frac{p_j}{q_j}\right) \left(\frac{q_i}{p_j}\right) \right]^{a_j b_i}$$

โดยทฤษฎีบท 9.6 สำหรับทุก $1 \leq i \leq r$ และ $1 \leq j \leq s$ จะได้

$$\left(\frac{p_j}{q_i}\right) \left(\frac{q_i}{p_j}\right) = (-1)^{\left(\frac{p_j-1}{2}\right) \left(\frac{q_i-1}{2}\right)}$$

ดังนั้น

$$\begin{aligned} \left(\frac{m}{n}\right) \left(\frac{n}{m}\right) &= \prod_{i=1}^r \prod_{j=1}^s \left[(-1)^{\left(\frac{p_j-1}{2}\right) \left(\frac{q_i-1}{2}\right)} \right]^{a_j b_i} \\ &= \prod_{i=1}^r \prod_{j=1}^s (-1)^{a_j \left(\frac{p_j-1}{2}\right) b_i \left(\frac{q_i-1}{2}\right)} \\ &= (-1)^{\sum_{i=1}^r \sum_{j=1}^s a_j \left(\frac{p_j-1}{2}\right) b_i \left(\frac{q_i-1}{2}\right)} \end{aligned}$$

จะได้

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\sum_{i=1}^r a_j \left(\frac{p_j-1}{2}\right) \sum_{j=1}^s b_i \left(\frac{q_i-1}{2}\right)}$$

และ

$$\sum_{i=1}^r \sum_{j=1}^s a_j \left(\frac{p_j-1}{2}\right) b_i \left(\frac{q_i-1}{2}\right) = \sum_{j=1}^s a_j \left(\frac{p_j-1}{2}\right) \sum_{i=1}^r b_i \left(\frac{q_i-1}{2}\right)$$

โดยทฤษฎีบท 9.9 จะได้

$$\sum_{j=1}^s a_j \left(\frac{p_j-1}{2}\right) \equiv \frac{m-1}{2} \pmod{2}$$

และ

$$\sum_{i=1}^r b_i \left(\frac{q_i-1}{2}\right) \equiv \frac{n-1}{2} \pmod{2}$$

ดังนั้น

$$\sum_{i=1}^r \sum_{j=1}^s a_j \left(\frac{p_j - 1}{2} \right) b_i \left(\frac{q_i - 1}{2} \right) \equiv \left(\frac{m-1}{2} \right) \left(\frac{n-1}{2} \right) \pmod{2}$$

ทำให้ได้ว่า

$$\left(\frac{n}{m} \right) \left(\frac{m}{n} \right) = (-1)^{\left(\frac{n-1}{2} \right) \left(\frac{m-1}{2} \right)}$$

9.5 สรุปท้ายบทที่ 9

ให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็ม ซึ่ง $(a, p) = 1$ ถ้า $x^2 \equiv a \pmod{p}$ มีผลเฉลย แล้วเรียก a ว่าเป็นส่วนตกค้างกำลังสองของ p ส่วนตกค้างกำลังสองเป็นเครื่องมือที่สำคัญอีกอย่างหนึ่งในการหารผลเฉลยของสมภาคในรูป $ax^2 + bx + c \equiv 0 \pmod{p}$ สำหรับการตรวจสอบว่าจำนวนใดเป็นส่วนตกค้างกำลังสองนั้นมีหลากหลายวิธีซึ่งได้นำเสนอในรูปแบบทฤษฎีบทต่อมา เลอช็องตร์ ได้กำหนดสัญลักษณ์ขึ้นมาซึ่งเกี่ยวข้องกับส่วนตกค้างกำลังสองโดยตรงนั้นเพื่อแสดงว่าสมภาค $x^2 \equiv a \pmod{p}$ มีผลเฉลยก็ต่อเมื่อ $\left(\frac{a}{p} \right) = 1$ และสมภาค $x^2 \equiv a \pmod{p}$ ไม่มีผล

เฉลยก็ต่อเมื่อ $\left(\frac{a}{p} \right) = -1$ การหาค่า $\left(\frac{a}{p} \right)$ นั้นมีหลายรูปแบบได้มีการนำเสนอในรูปแบบทฤษฎีบท

ต่าง ๆ สำหรับกรณี p และ q เป็นจำนวนเฉพาะคี่ที่แตกต่างกัน $\left(\frac{p}{q} \right) = \left(\frac{q}{p} \right)$ ถ้า $p \equiv 1 \pmod{4}$

หรือ $q \equiv 1 \pmod{4}$ และ $\left(\frac{p}{q} \right) = -\left(\frac{q}{p} \right)$ ถ้า $p \equiv 3 \pmod{4}$ และ $q \equiv 3 \pmod{4}$ และ

สัญลักษณ์ของยาโคบินั้นเป็นสัญลักษณ์ในกรณีทั่วไปของสัญลักษณ์เลอช็องตร์นั่นเอง นั่นคือ

$\left(\frac{a}{n} \right) = \prod_{i=1}^r \left(\frac{a}{p_i} \right)^{k_i} = \left(\frac{a}{p_1} \right)^{k_1} \left(\frac{a}{p_2} \right)^{k_2} \cdots \left(\frac{a}{p_r} \right)^{k_r}$ เมื่อ n เป็นจำนวนเต็มบวกคี่ซึ่งเขียนอยู่ในรูปผลคูณ

ของจำนวนเฉพาะ $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ และ a เป็นจำนวนเต็มที่ $(a, n) = 1$

แบบฝึกหัดท้ายบทที่ 9

1. จงหาจำนวนเต็มซึ่งเป็นส่วนตกค้างกำลังสองและไม่ใช่ส่วนตกค้างกำลังสองของจำนวนต่อไปนี้

1.1 7

1.2 15

1.3 17

2. จงใช้เกณฑ์ของออยเลอร์เพื่อตรวจสอบว่า 2, 5, 6 และ 8 เป็นส่วนตกค้างกำลังสองของจำนวนต่อไปนี้หรือไม่

2.1 5

2.2 11

2.3 19

3. จงหาค่าต่อไปนี้

3.1 $\left(\frac{2}{5}\right)$

3.2 $\left(\frac{5}{7}\right)$

3.3 $\left(\frac{4}{11}\right)$

3.4 $\left(\frac{2}{13}\right)$

3.5 $\left(\frac{7}{17}\right)$

3.6 $\left(\frac{53}{11}\right)$

3.7 $\left(\frac{-18}{13}\right)$

3.8 $\left(\frac{-36}{17}\right)$

3.9 $\left(\frac{3}{877}\right)$

3.10 $\left(\frac{3}{1061}\right)$

3.11 $\left(\frac{12}{509}\right)$

3.12 $\left(\frac{75}{109}\right)$

4. จงตรวจสอบว่าสมภาคต่อไปนี้^๑มีผลเฉลยหรือไม่

4.1 $x^2 \equiv 34 \pmod{7}$

4.2 $x^2 \equiv 512 \pmod{27}$

4.3 $x^2 \equiv 134 \pmod{19}$

4.4 $x^2 \equiv 60 \pmod{29}$

4.5 $x^2 \equiv -4 \pmod{19}$

4.6 $x^2 \equiv -49 \pmod{71}$

4.7 $x^2 \equiv -25 \pmod{29}$

4.8 $x^2 \equiv -25 \pmod{107}$

4.9 $x^2 \equiv 12 \pmod{139}$

4.10 $x^2 \equiv 51 \pmod{197}$

5. จงใช้สัญลักษณ์ยาโคบีเพื่อหาค่า

$$5.1 \quad \left(\frac{7}{15} \right)$$

$$5.2 \quad \left(\frac{5}{21} \right)$$

$$5.3 \quad \left(\frac{4}{55} \right)$$

$$5.4 \quad \left(\frac{2}{99} \right)$$

$$5.5 \quad \left(\frac{2}{107} \right)$$

$$5.6 \quad \left(\frac{-7}{120} \right)$$

$$5.7 \quad \left(\frac{-4}{135} \right)$$

$$5.8 \quad \left(\frac{51}{304} \right)$$

6. จงใช้ทฤษฎีบท 9.9 เพื่อหาค่า

$$6.1 \quad \left(\frac{-1}{15} \right)$$

$$6.2 \quad \left(\frac{2}{21} \right)$$

$$6.3 \quad \left(\frac{-1}{55} \right)$$

$$6.4 \quad \left(\frac{2}{99} \right)$$

$$6.5 \quad \left(\frac{-1}{107} \right)$$

$$6.6 \quad \left(\frac{2}{121} \right)$$

$$6.7 \quad \left(\frac{-1}{135} \right)$$

$$6.8 \quad \left(\frac{2}{311} \right)$$

7. จงพิจารณาโดยใช้สัญลักษณ์ยาโคบีว่าสมภาคกำลังสองต่อไปนี้ มีผลเฉลยหรือไม่

$$7.1 \quad x^2 \equiv 2 \pmod{15}$$

$$7.2 \quad x^2 \equiv -1 \pmod{27}$$

$$7.3 \quad x^2 \equiv 6 \pmod{35}$$

$$7.4 \quad x^2 \equiv 8 \pmod{35}$$

$$7.5 \quad x^2 \equiv 5 \pmod{38}$$

$$7.6 \quad x^2 \equiv -4 \pmod{33}$$