

บทที่ 8

รากปฐมฐานและดัชนี

การหาคำตอบของสมภาคเชิงเส้นที่อยู่ในรูป $ax \equiv b \pmod{m}$ ในบทที่ผ่านมาจะเป็นการหาโดยใช้สมบัติเบื้องต้นของสมภาค รวมทั้งการนำทฤษฎีบทเศษเหลือของชาวจีนมาประยุกต์ใช้ในการหาคำตอบของระบบสมภาค และสมภาคกำลังสอง สำหรับการศึกษารากปฐมฐาน(Primitive Root) และดัชนี(Index) นั้นเป็นการศึกษาเกี่ยวกับสมภาคในอีกรูปแบบหนึ่งสำหรับนำมาแก้ปัญหาการหาผลเฉลยของสมภาคเชิงเส้น และสมภาคไม่เชิงเส้นได้สะดวกและรวดเร็วมากยิ่งขึ้น โดยเริ่มจากการหาจำนวนเต็มบวก k ที่น้อยที่สุดที่สอดคล้องกับสมภาค $a^k \equiv 1 \pmod{m}$ และศึกษาการหาอันดับ (Order) ของจำนวนเต็มใด ๆ ในมอดุโล m ที่ $\text{ord}_m a = \phi(m)$ การศึกษารากปฐมฐานและดัชนีนั้นเป็นการศึกษาทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องในการค้นหารากปฐมฐานว่าทุกจำนวนเต็มใด ๆ จะมีรากปฐมฐานหรือไม่และถ้ามีรากปฐมฐานแล้วจะมีรากปฐมฐานทั้งหมดเท่าใด สำหรับในหัวข้อสุดท้ายเป็นการศึกษาสมบัติรวมทั้งทฤษฎีบทต่าง ๆ ของดัชนี

8.1 อันดับของจำนวนเต็มมอดุโล m

อันดับของจำนวนเต็มมอดุโล m เป็นการศึกษาจำนวนเต็ม k ที่สอดคล้องกับสมภาค $a^k \equiv 1 \pmod{m}$ โดยที่ k นั้นเป็นจำนวนเต็มบวกที่มีค่าน้อยสุด แสดงได้ดังบทนิยามต่อไปนี้

บทนิยาม 8.1

ให้ a และ m เป็นจำนวนเต็มบวก โดยที่ $m > 1$ และ $(a, m) = 1$ เรียกจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $a^k \equiv 1 \pmod{m}$ ว่า อันดับของ a มอดุโล m เขียนแทนด้วย $\text{ord}_m a = k$

สัญลักษณ์ $\text{ord}_m a$ เกาส์เป็นผู้นำเสนอ ไว้ในหนังสือชื่อ Disquisitiones Arithmeticae ปรากฏในปี ค.ศ. 1810 และสัญลักษณ์นี้ก็ใช้กันมาจนถึงปัจจุบัน

ตัวอย่าง 8.1 จงหาอันดับของ 3 มอดุโล 5

วิธีทำ หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $3^k \equiv 1 \pmod{5}$ โดยพิจารณาดังต่อไปนี้

$$3^1 \equiv 3 \pmod{5}$$

$$3^2 \equiv 4 \pmod{5}$$

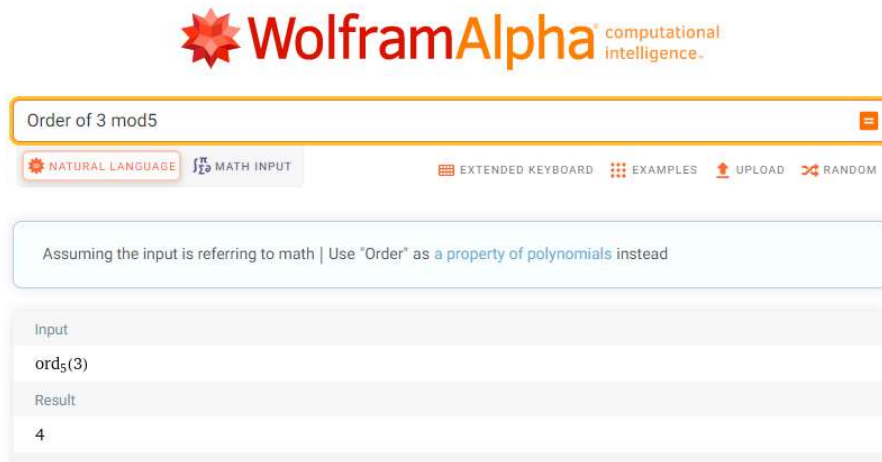
$$3^3 \equiv 2 \pmod{5}$$

$$3^4 \equiv 1 \pmod{5}$$

พบว่า 4 เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ $3^4 \equiv 1 \pmod{5}$

ดังนั้น $\text{ord}_5 3 = 4$

จากตัวอย่าง 8.1 ใช้ Wolfram Alpha เพื่อหาอันดับของ 3 โมดูล 5 ดังภาพประกอบ 8.1



ภาพประกอบ 8.1 ใช้ Wolfram Alpha เพื่อแสดงว่า $\text{ord}_5 3 = 4$

จากสมบัติของสมภาคในทที่ผ่านมานั้นพบว่า ถ้า $a \equiv b \pmod{m}$ และ $a^k \equiv 1 \pmod{m}$ เนื่องจาก $a^k \equiv b^k \pmod{m}$ แสดงว่า $b^k \equiv 1 \pmod{m}$ หมายความว่าถ้าจำนวนเต็มสองจำนวนสมภาคกันในมอดุโล m แล้ว จำนวนทั้งสองจำนวนจะมีอันดับในมอดุโล m เท่ากัน จากคุณสมบัติดังกล่าวทำให้สามารถหาอันดับของจำนวนเต็มมอดุโล m ได้สะดวกและรวดเร็วมากยิ่งขึ้นดังแสดงในตัวอย่างต่อไปนี้

ตัวอย่าง 8.2 จงหา $\text{ord}_4 19$

วิธีทำ เนื่องจาก $19 \equiv 3 \pmod{4}$

แสดงว่า $\text{ord}_4 19 = \text{ord}_4 3$

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $3^k \equiv 1 \pmod{4}$ โดยพิจารณาดังต่อไปนี้

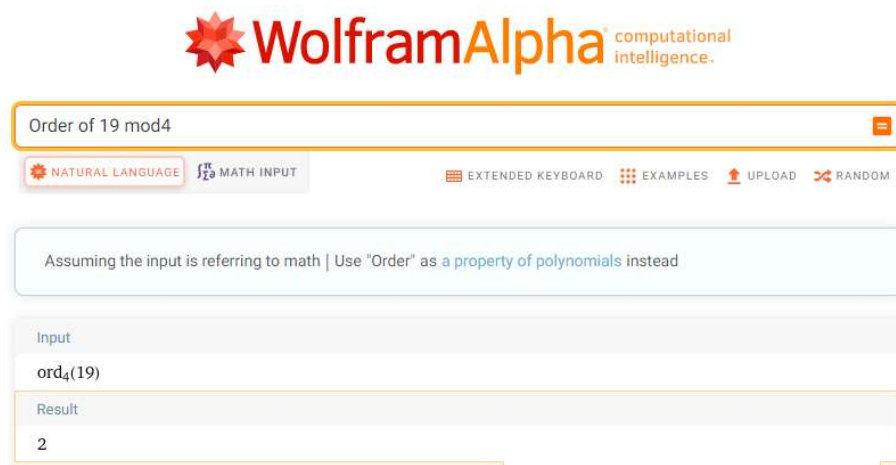
$$3^1 \equiv 3 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

นั่นคือ $\text{ord}_4 3 = 2 = \text{ord}_4 19$

ดังนั้น $\text{ord}_4 19 = 2$

จากตัวอย่าง 8.2 ใช้ Wolfram Alpha เพื่อหา $\text{ord}_4 19$ ดังภาพประกอบ 8.2



ภาพประกอบ 8.2 ใช้ Wolfram Alpha เพื่อแสดงว่า $\text{ord}_4 19 = 2$

การหาอันดับของ a มอดุโล m ในตัวอย่างที่ผ่านมานั้นทำโดยพิจารณาจากการหาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $a^k \equiv 1 \pmod{m}$ โดยใช้วิธีแทนค่า k เริ่มตั้งแต่ $k = 1$ ไปจนถึง $k = m - 1$ ซึ่งในการกรณีที่ a หรือ m เป็นจำนวนเต็มที่มีค่ามาก ๆ นั้นจะทำให้เสียเวลาในการตรวจสอบและทำให้เกิดข้อผิดพลาดได้ง่าย สำหรับทฤษฎีบทและบทแทรกต่อไปนี้สามารถช่วยแก้ปัญหาดังกล่าวโดยไม่ต้องแทนทุก ๆ ค่า k ตั้งแต่ $k = 1$ ไปจนถึง $k = m - 1$

ทฤษฎีบท 8.1

กำหนดให้ a เป็นจำนวนเต็ม ที่ $(a, m) = 1$ และ k เป็นอันดับของ a มอดุโล m สำหรับทุกจำนวนเต็มบวก h จะได้ว่า $a^h \equiv 1 \pmod{m}$ ก็ต่อเมื่อ $k \mid h$

พิสูจน์

($\Rightarrow$) สมมติให้ h เป็นอันดับของ a มอดุโล m ที่ $a^h \equiv 1 \pmod{m}$

โดยขั้นตอนวิธีการหารจะมีจำนวนเต็ม q และ r

โดยที่ $h = qk + r, 0 \leq r < k$

ดังนั้น $a^h = a^{qk+r} = (a^k)^q a^r$

จากสมมติ $a^h \equiv 1 \pmod{m}$ และ $a^k \equiv 1 \pmod{m}$

จะได้ว่า $a^r \equiv 1 \pmod{m}$ เนื่องจาก $0 \leq r < k$

จะได้ว่า $r = 0$ ดังนั้น $h = qk$

นั่นคือ $k \mid h$

($\Leftarrow$) สมมติ $k|h$ จะมีจำนวนเต็ม j ที่ทำให้ $h = kj$

เนื่องจาก $a^k \equiv 1 \pmod{m}$

ดังนั้น $(a^k)^j \equiv 1^j \pmod{m}$

นั่นคือ $a^h \equiv 1 \pmod{m}$

บทแทรก 8.1

ถ้า $\text{ord}_m a = k$ แล้ว $k|\phi(m)$

พิสูจน์

โดยทฤษฎีบทของออยเลอร์ $a^{\phi(m)} \equiv 1 \pmod{m}$ และจากทฤษฎีบท 8.1

จะได้ $k|\phi(m)$

ตัวอย่าง 8.3 จงหาอันดับของ 4 มอดุโล 13

วิธีทำ เนื่องจาก $\phi(13) = 12$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|12$

นั่นคือ $k = 1, 2, 3, 4, 6$ และ 12

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $4^k \equiv 1 \pmod{13}$ โดยพิจารณาดังต่อไปนี้

$$4^1 \equiv 4 \pmod{13}$$

$$4^2 \equiv 3 \pmod{13}$$

$$4^3 \equiv 12 \pmod{13}$$

$$4^4 \equiv 9 \pmod{13}$$

$$4^6 \equiv 1 \pmod{13}$$

$$4^{12} \equiv 1 \pmod{13}$$

จำนวนเต็มบวก k ค่าน้อยสุด ซึ่ง $k|\phi(13)$ และ $a^k \equiv 1 \pmod{13}$ คือ $k = 6$

ดังนั้น อันดับของ 4 มอดุโล 13 คือ 6 หรือ $\text{ord}_{13} 4 = 6$

ตัวอย่าง 8.4 จงหาอันดับของ 7 มอดุโล 12

วิธีทำ เนื่องจาก $\phi(12) = 4$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|4$

นั่นคือ $k = 1, 2$ และ 4

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $7^k \equiv 1 \pmod{12}$ โดยพิจารณาดังต่อไปนี้

$$5^1 \equiv 5 \pmod{12}$$

$$5^2 \equiv 1 \pmod{12}$$

จำนวนเต็มบวก k ค่าน้อยสุด ซึ่ง $k \mid \phi(12)$ และ $a^k \equiv 1 \pmod{12}$ คือ $k = 2$

ดังนั้น อันดับของ 5 มอดุโล 12 คือ 2 หรือ $\text{ord}_{12} 5 = 2$

ตัวอย่าง 8.5 จงหาอันดับของ 3 มอดุโล 20

วิธีทำ เนื่องจาก $\phi(20) = \phi(2^2 \cdot 5) = 20 \left(\frac{2-1}{2} \right) \left(\frac{5-1}{5} \right) = 8$

ดังนั้นพิจารณานับจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k \mid 8$

นั่นคือ $k = 1, 2, 4$ และ 8

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $3^k \equiv 1 \pmod{20}$ โดยพิจารณาดังต่อไปนี้

$$3^1 \equiv 3 \pmod{20}$$

$$3^2 \equiv 9 \pmod{20}$$

$$3^4 \equiv 1 \pmod{20}$$

จำนวนเต็มบวก k ค่าน้อยสุด ซึ่ง $k \mid \phi(20)$ และ $a^k \equiv 1 \pmod{20}$ คือ $k = 4$

ดังนั้น อันดับของ 3 มอดุโล 20 คือ 4 หรือ $\text{ord}_{20} 3 = 4$

สำหรับทฤษฎีบทและบทแทรกที่ได้แสดงต่อนั้น เกี่ยวข้องกับอันดับของจำนวนเต็ม ซึ่งเป็นพื้นฐานในการศึกษาอันดับของจำนวนเต็มในรูปแบบที่แตกต่างออกไปจากที่ได้กล่าวมาแล้วข้างต้น

ทฤษฎีบท 8.2

ถ้า $\text{ord}_m a = k$ จะได้ว่า $a^s \equiv a^t \pmod{m}$ ก็ต่อเมื่อ $r \equiv s \pmod{k}$

พิสูจน์

($\Rightarrow$) สมมติให้ $a^s \equiv a^t \pmod{m}$ ซึ่ง $(a, m) = 1$ และให้ $s \geq t$

จะได้ $k \mid (s - t)$

นั่นคือ $s \equiv t \pmod{k}$

($\Leftarrow$) สมมติให้ $s \equiv t \pmod{k}$ จะได้ $k \mid (s - t)$

แสดงว่ามีจำนวนเต็ม q ที่ทำให้ $s = t + qk$

นั่นคือ $a^s \equiv a^t \pmod{m}$

$$a^{q^k} \equiv 1 \pmod{m}$$

$$a^t \cdot a^{q^k} \equiv a^t \pmod{m}$$

ดังนั้น $a^s \equiv a^t \pmod{m}$

จากทฤษฎีบท 8.2 จะได้บทแทรกดังต่อไปนี้

บทแทรก 8.2

ถ้า $\text{ord}_m a = k$ จะได้ว่า $a, a^2, \dots, a^k$ จะไม่สมภาคมอดุโล m กัน

พิสูจน์

ถ้ามี s และ t ซึ่ง $1 \leq s < t \leq k$ ซึ่ง $a^s \equiv a^t \pmod{m}$
 จะได้ว่า $s \equiv t \pmod{k}$ ซึ่งเป็นไปไม่ได้ ยกเว้นเมื่อ $s = t$

ทฤษฎีบท 8.3

ถ้า $\text{ord}_m a = k$ และ $h > 0$ จะได้ว่า $\text{ord}_m a^h = \frac{k}{(h, k)}$

พิสูจน์

ให้ $d = (h, k)$ จะได้ว่า $h = (h_1, d)$ และ $k = (k_1, d)$ เมื่อ $(h_1, k_1) = 1$

จะได้ว่า $(a^h)^{k_1} = (a^{h_1 d})^{\frac{k}{d}} = a^{k h_1} \equiv 1 \pmod{m}$

สมมติว่า $\text{ord}_m a^h = r$ จะได้ $r | k_1$

และ $(a^h)^r \equiv 1 \pmod{m}$ แต่ $\text{ord}_m a = k$ ดังนั้น $k | hr$

จะได้ $k_1 d | h_1 dr$ ดังนั้น $k_1 | h_1 r$ แต่ $(h_1, k_1) = 1$ ดังนั้น $k_1 | r$

เมื่อ $k_1 | r$ และ $r | k_1$ ดังนั้น $r = k_1 = \frac{k}{d} = \left(\frac{k}{(h, k)} \right)$

จากทฤษฎีบทข้างต้นทำให้ได้บทแทรกดังต่อไปนี้

บทแทรก 8.3

ถ้า $\text{ord}_m a = k$ และถ้า $(h, k) = 1$ จะได้ว่า $\text{ord}_m a^h = k$

พิสูจน์

จากทฤษฎีบท 8.3 ถ้า $\text{ord}_m a = k$ จะได้ว่า $\text{ord}_m a^h = \left(\frac{k}{h, k} \right)$

ถ้า $(h, k) = 1$ จะได้ว่า $\text{ord}_m a^h = k$

ตัวอย่าง 8.6 กำหนดให้ $\text{ord}_{13} 2 = 12$ จงหาค่า $\text{ord}_{13} 4, \text{ord}_{13} 8, \text{ord}_{13} 16, \text{ord}_{13} 128$

และ $\text{ord}_{13} 512$

วิธีทำ เนื่องจาก $\text{ord}_{13} 2 = 12$

จากทฤษฎีบท 8.3 จะได้

$$\text{ord}_{13} 4 = \text{ord}_{13} 2^2 = \frac{12}{(2, 12)} = \frac{12}{2} = 6$$

$$\text{ord}_{13} 8 = \text{ord}_{13} 2^3 = \frac{12}{(3, 12)} = \frac{12}{3} = 4$$

$$\text{ord}_{13} 16 = \text{ord}_{13} 2^4 = \frac{12}{(4, 12)} = \frac{12}{4} = 3$$

$$\text{ord}_{13} 128 = \text{ord}_{13} 2^7 = \frac{12}{(7, 12)} = \frac{12}{1} = 12$$

$$\text{ord}_{13} 512 = \text{ord}_{13} 2^9 = \frac{12}{(9, 12)} = \frac{12}{3} = 4$$

และจากบทแทรก 8.3 พบว่า $\text{ord}_{13} 128 = \text{ord}_{13} 2^7 = \text{ord}_{13} 2 = 12$

เนื่องจาก $(7, 12) = 1$

ดังนั้น $\text{ord}_{13} 4 = 6, \text{ord}_{13} 8 = 4, \text{ord}_{13} 16 = 3, \text{ord}_{13} 128 = 12$ และ $\text{ord}_{13} 512 = 4$

ตัวอย่าง 8.7 จงหาอันดับของจำนวนเต็ม 64 มอดุล 5

วิธีทำ เนื่องจาก $64 = 4^3$ พิจารณา $\text{ord}_5 4$ ดังนี้

เนื่องจาก $\phi(5) = 4$

พิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k \mid 4$

นั่นคือ $k = 1, 2$ และ 4

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $4^k \equiv 1 \pmod{5}$ โดยพิจารณาดังต่อไปนี้

$$4^1 \equiv 4 \pmod{5}$$

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

นั่นคือ $\text{ord}_5 4 = 2$

เนื่องจาก $64 = 4^3$ และ $(3, 2) = 1$

ทำให้ $\text{ord}_5 64 = \text{ord}_5 (4^3) = 2$

ดังนั้น อันดับของจำนวนเต็ม 64 มอดุโล 5 คือ 2

ตัวอย่าง 8.9 จงหาอันดับของจำนวนเต็ม 729 มอดุโล 5

วิธีทำ เนื่องจาก $729 = 3^6$ พิจารณา $\text{ord}_5 3$ ดังนี้

เนื่องจาก $\phi(5) = 4$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k \mid 4$

นั่นคือ $k = 1, 2$ และ 4

หาจำนวนเต็มบวก k ที่มีค่าน้อยสุด ที่ $3^k \equiv 1 \pmod{5}$ โดยพิจารณาดังต่อไปนี้

$$3^1 \equiv 3 \pmod{5}$$

$$3^2 \equiv 4 \pmod{5}$$

$$3^4 \equiv 1 \pmod{5}$$

นั่นคือ $\text{ord}_5 3 = 4$

เนื่องจาก $729 = 3^6$ และ $(6, 4) = 2$

$$\text{ทำให้ } \text{ord}_5 729 = \text{ord}_5 (3^6) = \frac{4}{(6, 4)} = \frac{4}{2} = 2$$

ดังนั้น อันดับของจำนวนเต็ม 729 มอดุโล 5 คือ 2

8.2 รากปฐมฐาน

ในหัวข้อที่ผ่านมาพบว่าอันดับของ a มอดุโล m นั้นมีค่าน้อยกว่าหรือเท่ากับ $\phi(m)$ สำหรับในหัวข้อนี้จะศึกษากรณีที่อันดับของ a มอดุโล m มีค่าเท่ากับ $\phi(m)$ เริ่มจากการศึกษาบทนิยามดังต่อไปนี้

บทนิยาม 8.2

ให้ m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม ซึ่ง $(a, m) = 1$

จะเรียก a ว่ารากปฐมฐานของ m ก็ต่อเมื่อ $\text{ord}_m a = \phi(m)$

จากบทนิยามพบว่า a เป็นรากปฐมฐานของ m ก็ต่อเมื่อ ไม่มีจำนวนเต็มบวก $k < \phi(m)$ ที่ทำให้ $a^k \equiv 1 \pmod{m}$

ตัวอย่าง 8.10 จงพิจารณาว่า 2 เป็นรากปฐมฐานของ 7 หรือไม่

วิธีทำ เนื่องจาก $\phi(7) = 6$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|6$

นั่นคือ $k = 1, 2, 3$ และ 6

พิจารณา

$$2^1 \equiv 2 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

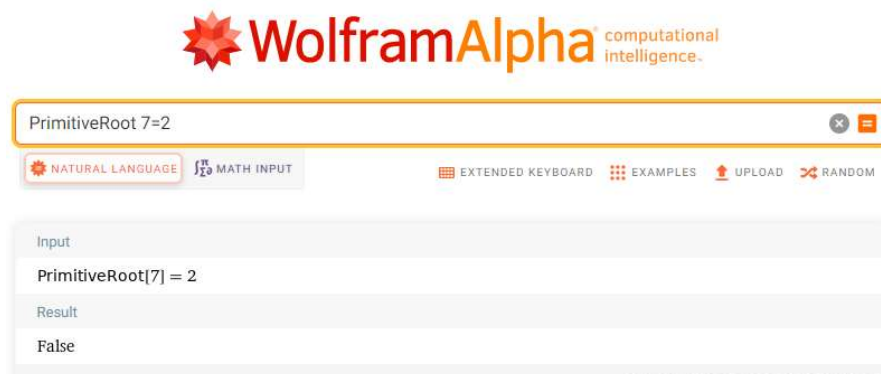
$$2^3 \equiv 1 \pmod{7}$$

$$2^6 \equiv 1 \pmod{7}$$

เนื่องจาก $\text{ord}_7 2 = 3 \neq \phi(7)$

ดังนั้น 2 ไม่เป็นรากปฐมฐานของ 7

จากตัวอย่าง 8.10 ใช้ Wolfram Alpha เพื่อตรวจสอบว่า 2 เป็นรากปฐมฐานของ 7 หรือไม่



ภาพประกอบ 8.3 ใช้ Wolfram Alpha เพื่อแสดงว่า 2 ไม่เป็นรากปฐมฐานของ 7

ตัวอย่าง 8.11 จงพิจารณาว่า 6 เป็นรากปฐมฐานของ 13 หรือไม่

วิธีทำ เนื่องจาก $\phi(13) = 12$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|12$

นั่นคือ $k = 1, 2, 3, 4, 6$ และ 12

พิจารณา

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

$$6^2 \equiv 10 \pmod{13}$$

$$6^3 \equiv 8 \pmod{13}$$

$$\begin{aligned}6^4 &\equiv 9 \pmod{13} \\6^6 &\equiv 12 \pmod{13} \\6^{12} &\equiv 1 \pmod{13}\end{aligned}$$

เนื่องจาก $\text{ord}_{13} 6 = 12 = \phi(13)$

ดังนั้น 6 เป็นรากปฐมฐานของ 13

ตัวอย่าง 8.12 จงตรวจสอบว่า 3 และ 7 เป็นรากปฐมฐานของ 10 หรือไม่

วิธีทำ เนื่องจาก $\phi(10) = \phi(2 \cdot 5) = 10 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 4$

ดังนั้นพิจารณาจำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|4$

นั่นคือ $k = 1, 2$ และ 4

พิจารณา

$$\begin{aligned}3^1 &\equiv 3 \pmod{10} & 7^1 &\equiv 7 \pmod{10} \\3^2 &\equiv 9 \pmod{10} & \text{และ} & 7^2 \equiv 9 \pmod{10} \\3^4 &\equiv 1 \pmod{10} & 7^4 &\equiv 1 \pmod{10}\end{aligned}$$

เนื่องจาก $\text{ord}_{10} 3 = 4 = \phi(10)$ และ $\text{ord}_{10} 7 = 4 = \phi(10)$

ดังนั้น 3 และ 7 เป็นรากปฐมฐานของ 10

จากตัวอย่างพบว่าจำนวนเต็ม n นั้นอาจจะมีหรือไม่มีรากปฐมฐาน และถ้ามีรากปฐมฐานแล้ว อาจจะมีเพียงหนึ่งหรือมากกว่าหนึ่ง สำหรับทฤษฎีบทต่อไปจะเป็นการสร้างเซตที่เป็นระบบลดทอนของ ส่วนตกค้างมอดุโล m โดยใช้รากปฐมฐานของ m ดังต่อไปนี้

ทฤษฎีบท 8.4

ถ้า a เป็นรากปฐมฐานของ m แล้วจะได้ว่า $a^1, a^2, \dots, a^{\phi(m)}$ เป็นระบบ ส่วนตกค้างลดรูปมอดุโล m

พิสูจน์

เนื่องจาก a เป็นรากปฐมฐาน จะได้ว่า $(a, m) = 1$

ดังนั้น $a^1, a^2, \dots, a^{\phi(m)}$ เป็นจำนวนเฉพาะสัมพัทธ์กับ m

และเนื่องจาก a เป็นรากปฐมฐาน ดังนั้น $\text{ord}_m a = \phi(m)$

จะได้ว่า $a^{\phi(m)} \equiv 1 \pmod{m}$ แต่ $a^k \not\equiv 1 \pmod{m}$

สำหรับจำนวนเต็มบวก k ซึ่ง $k < \phi(m)$

จะได้ว่า $a^1, a^2, \dots, a^{\phi(m)}$ ไม่สมภาคมอดุโล m กัน
 นั่นคือ $a^1, a^2, \dots, a^{\phi(m)}$ จะเป็นระบบส่วนตกค้างลดรูปมอดุโล m

ตัวอย่าง 8.13

จากตัวอย่าง 8.12 พบว่า 3 และ 7 เป็นรากปฐมฐานของ 10

$$\text{และ } \phi(10) = 4$$

ดังนั้น $3, 3^2, 3^3, 3^4$ และ $7, 7^2, 7^3, 7^4$ เป็นระบบส่วนตกค้างลดรูปมอดุโล 10

ตัวอย่าง 8.14 จงหาระบบส่วนตกค้างลดรูปมอดุโล 9

วิธีทำ เนื่องจาก $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$

จำนวนเต็มบวก k ที่เป็นไปได้ทั้งหมดซึ่ง $k|6$ นั่นคือ $k = 1, 2, 3$ และ 6

พิจารณา

$$2^1 \equiv 2 \pmod{9}$$

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

$$2^3 \equiv 8 \pmod{9}$$

$$2^6 \equiv 1 \pmod{9}$$

แสดงว่า $\text{ord}_9 2 = 6 = \phi(9)$ แสดงว่า 2 เป็นรากปฐมฐานของ 9

ดังนั้น $2, 2^2, 2^3, 2^4, 2^5, 2^6$ เป็นระบบส่วนตกค้างลดรูปมอดุโล 9

จากทฤษฎีบท 8.4 พบว่า $a^1, a^2, \dots, a^{\phi(m)}$ เป็นระบบส่วนตกค้างลดรูปมอดุโล m ทำให้เราสามารถทราบจำนวนของรากปฐมฐานทั้งหมดได้และแสดงไว้ในบทแทรกต่อไปนี้

บทแทรก 8.4

ถ้า m มีรากปฐมฐานแล้ว m จะมีรากปฐมฐานอยู่ $\phi(\phi(m))$ จำนวน

พิสูจน์

สมมติให้ a เป็นรากปฐมฐานหนึ่งของ m ดังนั้น $\text{ord}_m a = \phi(m)$

พิจารณา $a^1, a^2, \dots, a^{\phi(m)}$ ซึ่งเป็นระบบส่วนตกค้างลดรูปมอดุโล m

จะหารากปฐมฐานตัวอื่นได้จากสมาชิกของ $\{a^1, a^2, \dots, a^{\phi(m)}\}$

โดยหา $\text{ord}_m a$ ดังนี้

$$\begin{aligned}
ord_m a^2 &= \frac{\phi(m)}{(2, \phi(m))} \\
ord_m a^3 &= \frac{\phi(m)}{(3, \phi(m))} \\
ord_m a^4 &= \frac{\phi(m)}{(4, \phi(m))} \\
&\vdots \\
ord_m a^{\phi(m)} &= \frac{\phi(m)}{(3, \phi(m))}
\end{aligned}$$

ดังนั้น $ord_m a^k = \phi(m)$ ก็ต่อเมื่อ $(k, \phi(m)) = 1$

แต่จำนวน k ที่น้อยกว่า $\phi(m)$ ซึ่ง $(k, \phi(m)) = 1$ มี $\phi(\phi(m))$ จำนวน

นั่นคือ m มีรากปฐมฐานทั้งหมด $\phi(\phi(m))$ จำนวน

ตัวอย่าง 8.15 จงหาจำนวนรากปฐมฐานทั้งหมดของ 11

วิธีทำ เนื่องจาก $\phi(11) = 10$

$$\text{และ } \phi(\phi(11)) = \phi(10) = \phi(2 \cdot 5) = 10 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 4$$

ดังนั้น รากปฐมฐานทั้งหมดของ 11 มี 4 จำนวน

8.3 รากปฐมฐานสำหรับจำนวนเฉพาะและการมีรากปฐมฐาน

ในหัวข้อที่ผ่านมาพบว่า a เป็นรากปฐมฐานของ m ก็ต่อเมื่อ $ord_m a = \phi(m)$ โดยที่ $(a, m) = 1$ โดยเราสามารถตรวจสอบการจำนวนเต็มว่าเป็นรากปฐมฐานของแต่ละจำนวนหรือไม่นั้นสามารถตรวจสอบได้โดยใช้บทนิยาม นอกจากนี้ยังมีทฤษฎีบทที่สามารถตรวจสอบจำนวนรากปฐมฐานมีอยู่ทั้งหมดได้ สำหรับในหัวข้อนี้จะศึกษาว่าจำนวนเต็มในรูปแบบใดบ้างที่มีรากปฐมฐาน ซึ่งส่วนแรกจะแสดงว่าจำนวนเฉพาะทุกจำนวนมีรากปฐมฐาน

ทฤษฎีบท 8.5

ให้ p เป็นจำนวนเฉพาะ และ d เป็นจำนวนเต็มบวก โดยที่ $d \mid (p-1)$
แล้วจะมีจำนวนเต็มที่มีอันดับมอดุโล p เป็น d อยู่ $\phi(d)$ จำนวนที่ไม่ลงรอยกัน

พิสูจน์

กำหนดให้ $d > 0$ สำหรับแต่ละตัวหาร d ของ $p-1$

ให้ $F(d)$ คือจำนวนเต็ม k โดยที่ $1 \leq k \leq p-1$ และ $\text{ord}_p k = d$

เนื่องจากสำหรับแต่ละ k โดยที่ $1 \leq k \leq p-1$ และ $\text{ord}_p k \mid (p-1)$

$$\text{จะได้ } p-1 = \sum_{d \mid (p-1)} F(d)$$

โดยทฤษฎีบทของเกาส์ จะได้

$$p-1 = \sum_{d \mid (p-1)} \phi(d)$$

แสดงว่า

$$\sum_{d \mid (p-1)} F(d) = \sum_{d \mid (p-1)} \phi(d)$$

ต่อไปจะแสดงว่า $F(d) \leq \phi(d)$ ทุกตัวหาร d ของ $p-1$

ให้ d เป็นตัวหารของ $p-1$ นั่นคือ $d \mid (p-1)$

ถ้า $F(d) = 0$ จะได้ว่า $F(d) \leq \phi(d)$ เป็นจริง

สมมติให้ $F(d) \neq 0$ จะได้ว่ามีจำนวนจริง a โดยที่ $1 \leq a \leq p-1$ และ $\text{ord}_p a = d$

แสดงว่า จำนวนเต็มทุกคู่ใน $a, a^2, a^3, \dots, a^d$ จะไม่สมภาคกันในมอดุโล p

และทุกจำนวนเต็มในชุดนี้เป็นรากของ $x^d - 1$ มอดุโล p เนื่องจาก

$$(a^k)^d = (a^d)^k \equiv 1 \pmod{p} \text{ ทุกจำนวนเต็มบวก } k$$

เนื่องจาก $x^d - 1$ มีและมีย่างแน่นอน d ราก มอดุโล p

นั่นคือทุกรากของ $x^d - 1$ จะสมภาคกันกับ a^k ใน มอดุโล p สำหรับบางจำนวนเต็ม k

แสดงว่า จำนวนเต็มที่มีอันดับมอดุโล p เป็น d นั้น จะต้องสมภาคกันมอดุโล p

กับจำนวนหนึ่งจำนวนใดใน $a, a^2, a^3, \dots, a^d$ แต่เนื่องจาก

$$\text{ord}_p a^k = \frac{\text{ord}_m a}{(k, \text{ord}_m a)} = \frac{d}{(k, d)}$$

นั่นคือ $\text{ord}_p a^k = d$ ก็ต่อเมื่อ $(k, d) = 1$

แสดงว่าจำนวนของจำนวนเต็ม k ที่ทำให้ $\text{ord}_p a^k = d$ มี $\phi(d)$ จำนวน

นั่นคือ ถ้ามีจำนวนเต็มหนึ่งตัวที่มีอันดับเป็น d มอดุโล p แล้วจะมีแน่นอน $\phi(d)$ จำนวน

จะได้ $F(d) \leq \phi(d)$ ทุกตัวหารบวก d ของ $p-1$

$$\text{และเนื่องจาก } \sum_{d \mid (p-1)} F(d) = \sum_{d \mid (p-1)} \phi(d)$$

ดังนั้น $F(d) = \phi(d)$ ทุกตัวหารบวก d ของ $p-1$

บทแทรก 8.5

ถ้า p เป็นจำนวนเฉพาะแล้ว จะมีรากปฐมฐานมอดุโล p และมี $\phi(p-1)$ จำนวนที่ไม่สมภาคกัน

พิสูจน์

ให้ p เป็นจำนวนเฉพาะ และเนื่องจาก $(p-1)|(p-1)$

โดยทฤษฎีบท 8.5 จะได้ว่ามีจำนวนเต็ม $\phi(p-1)$ จำนวนที่ไม่สมภาคกันในมอดุโล p

และมีอันดับเป็น $p-1$ มอดุโล p

แสดงว่า p มีรากปฐมฐาน $\phi(p-1)$ จำนวนที่ไม่สมภาคกัน

ทฤษฎีบท 8.6

ไม่มีรากปฐมฐานมอดุโล 2^k สำหรับจำนวนเต็ม $k \geq 3$

พิสูจน์

จำนวนเต็ม a จะเป็นรากปฐมฐานของ 2^k ได้นั้น a ต้องเป็นจำนวนเฉพาะที่อยู่

ถัดจาก 2^k นั่นคือ a ต้องเป็นจำนวนเต็มคี่

พิจารณาโดยให้ a เป็นจำนวนเต็มคี่ ใด ๆ โดยที่ $1 \leq a \leq 2^k$

จะพิสูจน์ว่า $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ สำหรับจำนวนเต็ม $k \geq 3$

ข้อความนี้เป็นจริงสำหรับ $k = 3$

เนื่องจากจำนวนเต็มบวกที่น้อยกว่า 2^3 คือ 1, 3, 5, 7 และ

$$1^2 \equiv 1 \pmod{2^3}$$

$$3^2 \equiv 1 \pmod{2^3}$$

$$5^2 \equiv 1 \pmod{2^3}$$

$$7^2 \equiv 1 \pmod{2^3}$$

สมมติให้ข้อความ $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ เป็นจริง เมื่อ $k = n$ นั่นคือ

$$a^{2^{n-2}} \equiv 1 \pmod{2^n} \text{ เป็นจริง}$$

จะแสดงว่าข้อความนี้เป็นจริงเมื่อ $k = n + 1$

เนื่องจาก $a^{2^{n-2}} \equiv 1 \pmod{2^n}$

จึงมีจำนวนเต็ม b ที่ทำให้

$$a^{2^{n-2}} = 1 + b2^n$$

ยกกำลังสองทั้งสองข้างจะได้

$$\begin{aligned}\left(a^{2^{n-2}}\right)^2 &= \left(1 + b2^n\right)^2 \\ a^{2^{n-1}} &= 1 + b2^{n+1} + \left(b2^n\right)^2 \\ &= 1 + 2^{n+1}\left(b + b^2 2^{n-1}\right)\end{aligned}$$

นั่นคือ $a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$

แสดงว่า $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ เป็นจริงสำหรับจำนวนเต็ม $k \geq 3$

และเนื่องจาก $\phi(2^k) = 2^{k-1}$ จึงได้ว่า

$$a^{\frac{\phi(2^k)}{2}} \equiv 1 \pmod{2^k} \text{ สำหรับจำนวนเต็มคี่ } a \text{ และ } k \geq 3$$

แสดงว่าไม่มีรากปฐมฐานมอดุโล 2^k สำหรับจำนวนเต็ม $k \geq 3$

ทฤษฎีบท 8.7

ให้ m, n เป็นจำนวนเต็ม โดยที่ $m, n > 2$ และ $(m, n) = 1$ แล้ว

mn ไม่มีรากปฐมฐาน

พิสูจน์

ให้ a เป็นจำนวนเต็ม โดยที่ $(a, mn) = 1$ เนื่องจาก $(m, n) = 1$

จะได้ $(a, m) = 1$ และ $(a, n) = 1$

ให้ $h = [\phi(m), \phi(n)]$ และ $d = (\phi(m), \phi(n))$

เนื่องจาก $\phi(m)$ และ $\phi(n)$ เป็นเลขคู่ จะได้ว่า $d \geq 2$ นั่นคือ

$$h = [\phi(m), \phi(n)] = \frac{\phi(m) \cdot \phi(n)}{d} \leq \frac{\phi(mn)}{2}$$

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

$$a^h = \left(a^{\phi(m)}\right)^{\frac{\phi(n)}{d}} \equiv 1^{\frac{\phi(n)}{d}} \pmod{m} \equiv 1 \pmod{m}$$

และในทำนองเดียวกัน เนื่องจาก $a^{\phi(n)} \equiv 1 \pmod{n}$ จะได้

$$a^h \equiv 1 \pmod{n}$$

เนื่องจาก $(m, n) = 1$ แสดงว่า $a^h \equiv 1 \pmod{mn}$ นั่นคือ

$$\text{ord}_{mn} a \leq \frac{\phi(mn)}{2}$$

แสดงว่า mn ไม่มีรากปฐมฐาน

บทแทรก 8.6

จำนวนเต็ม m ไม่มีรากปฐมฐาน ถ้า

1. m มีตัวหารเป็นจำนวนเฉพาะที่สองจำนวน หรือ
2. m อยู่ในรูปแบบของ $m = 2^n p^k$ เมื่อ p เป็นจำนวนเฉพาะ และ $n \geq 2$

พิสูจน์ ผลจากทฤษฎีบท 8.7

ต่อไปจะเป็นการพิจารณาจำนวนเต็มในรูปแบบ $2^2, p^k$ และ $2p^k$ เมื่อ p เป็นจำนวนเฉพาะ คือว่าจะมีรากปฐมฐานหรือไม่ และการพิสูจน์ทฤษฎีบทและบทแทรกนั้น มีทฤษฎีบทที่เกี่ยวข้องได้ นำเสนอในรูปแบบบทตั้งดังต่อไปนี้

บทตั้ง 8.1

ให้ p เป็นจำนวนเฉพาะคี่แล้ว จะมีจำนวนเต็ม r โดยที่ r เป็นรากปฐมฐานของ p และ $r^{p-1} \not\equiv 1 \pmod{p^2}$

พิสูจน์

เนื่องจาก p เป็นจำนวนเฉพาะคี่ โดยบทแทรก 8.5 จะได้ว่า p มีรากปฐมฐาน

ให้ r เป็นรากปฐมฐานของ p ถ้า $r^{p-1} \not\equiv 1 \pmod{p^2}$ ทฤษฎีบทเป็นจริง

สมมติให้ $r^{p-1} \equiv 1 \pmod{p^2}$

กำหนดให้ $r' = r + p$

เนื่องจาก $r' \equiv r \pmod{p}$ แสดงว่า r' เป็นรากปฐมฐานของ p ด้วย

โดยทฤษฎีบทวินามจะได้

$$(r')^{p-1} \equiv (r + p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$$

เนื่องจาก $r^{p-1} \equiv 1 \pmod{p^2}$ จะได้

$$\begin{aligned} (r')^{p-1} &\equiv 1 + (p-1)pr^{p-2} \pmod{p^2} \\ &\equiv 1 + p^2r^{p-2} - pr^{p-2} \pmod{p^2} \\ &\equiv 1 - pr^{p-2} \pmod{p^2} \end{aligned}$$

เนื่องจาก r เป็นรากปฐมฐานของ p จะได้ $(r, p) = 1$ และ $p \nmid r^{p-2}$

แสดงว่า $r^{p-1} \not\equiv 1 \pmod{p^2}$

บทแทรก 8.7

ถ้า p เป็นจำนวนเฉพาะคี่แล้ว p^2 มีรากปฐมฐาน กล่าวคือ
 ถ้า r เป็นรากปฐมฐานของ p แล้ว r หรือ $r + p$ จะเป็นรากปฐมฐานของ p^2

พิสูจน์

ให้ r เป็นรากปฐมฐานของ p

จะได้ว่า $\text{ord}_p r = \phi(p) = p - 1$

ให้ $n = \text{ord}_{p^2} r$ แสดงว่า $r^n \equiv 1 \pmod{p^2}$ และ $r^n \equiv 1 \pmod{p}$

ดังนั้น $\text{ord}_p r \mid n$ แสดงว่า $(p - 1) \mid n$

และเนื่องจาก $\phi(p^2) = p(p - 1)$ จะได้ $n \mid p(p - 1)$

เนื่องจาก $(p - 1) \mid n$ และ $n \mid p(p - 1)$ จะได้ว่า $n = p$ หรือ $n = p - 1$

กรณีที่ $n = p$ จะได้ว่า r เป็นรากปฐมฐานของ p^2

กรณีที่ $n = p - 1$ จะได้ว่า $r' = r + p$ เป็นรากปฐมฐานของ p

โดยที่ $(r')^{p-1} \not\equiv 1 \pmod{p^2}$

และในทำนองเดียวกันสามารถแสดงได้ว่า $\text{ord}_{p^2} r' = \phi(p^2)$

นั่นคือ r' เป็นรากปฐมฐานของ p^2

ตัวอย่าง 8.16 กำหนดให้ 3 เป็นรากปฐมฐานของ 17 จงตรวจสอบว่า 3 เป็นรากปฐมฐานของ 289 ด้วยหรือไม่

วิธีทำ เนื่องจาก $17^2 = 289$

และ $3^{p-1} = 3^{16} \not\equiv 1 \pmod{289}$

ดังนั้น 3 เป็นรากปฐมฐานของ 289

ทฤษฎีบทต่อไปจะเป็นการศึกษาในกรณีที่ p เป็นจำนวนเฉพาะคี่แล้ว p^k มีรากปฐมฐาน
 ภายใต้เงื่อนไข $k \geq 2$

บทตั้ง 8.2

ถ้า p เป็นจำนวนเฉพาะคี่ และ r เป็นรากปฐมฐานของ p โดยที่
 $r^{p-1} \not\equiv 1 \pmod{p^2}$ แล้ว $r^{p^{k-2}}(p - 1) \not\equiv 1 \pmod{p^k}$ สำหรับจำนวนเต็ม $k \geq 2$

พิสูจน์

พิสูจน์โดยวิธีอุปนัยทางคณิตศาสตร์บน k

จากบทตั้ง 8.1 พบว่ากรณี $k = 2$ จะได้ว่า ทฤษฎีบทเป็นจริง

สมมติว่าทฤษฎีบทเป็นจริงสำหรับจำนวนเต็ม $n \geq 2$

จะแสดงว่าทฤษฎีบทเป็นจริง เมื่อ $k = n + 1$

เนื่องจาก $(r, p^{n-1}) = (r, p^n) = 1$ จากทฤษฎีบทของออยเลอร์ จะได้ว่า

$$r^{p^{n-2}(p-1)} = r^{\phi(p^{n-1})} \equiv 1 \pmod{p^{n-1}}$$

แสดงว่าจะมีจำนวนเต็ม a ที่ทำให้

$$r^{p^{n-2}(p-1)} = 1 + ap^{n-1}$$

เนื่องจากทฤษฎีบทเป็นจริงเมื่อ $k = n$ แสดงว่า $r^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$

นั่นคือ $p \nmid a$ แสดงว่า

$$r^{p^{n-1}(p-1)} = (1 + ap^{n-1})^p \equiv 1 + ap^n \pmod{p^{n+1}}$$

และเนื่องจาก $p \nmid a$ จะได้ว่า $r^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$

นั่นคือ ทฤษฎีบทเป็นจริงเมื่อ $k = n + 1$

ดังนั้น ทฤษฎีบทเป็นจริงทุกจำนวนเต็ม $k \geq 2$

ทฤษฎีบท 8.8

ให้ p เป็นจำนวนเฉพาะคี่ และ k เป็นจำนวนเต็ม โดยที่ $k \geq 1$ แล้ว p^k มีรากปฐมฐาน

พิสูจน์

กำหนดให้ r เป็นรากปฐมฐานของ p โดยที่

$$r^{p-1} \not\equiv 1 \pmod{p^2} \text{ และ } r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

จะแสดงว่า r เป็นรากปฐมฐานของ p^k ทุก $k \geq 1$

ให้ $n = \text{ord}_{p^k} r$

เนื่องจาก $\phi(p^k) = p^{k-1}(p-1)$ จะได้ $n \mid p^{k-1}(p-1)$

เนื่องจาก $r^n \equiv 1 \pmod{p^k}$ จะได้ $r^n \equiv 1 \pmod{p}$

นั่นคือ $(p-1) \mid n$

เนื่องจาก $n \mid p^{k-1}(p-1)$ และ $(p-1) \mid n$

แสดงว่า n อยู่ในรูปแบบของ $p^m(p-1)$ สำหรับบางจำนวนเต็ม $1 \leq m \leq k-1$

ถ้า $n \neq p^{k-1}(p-1)$ แล้วจะได้ว่า $n \mid p^{k-2}(p-1)$

ซึ่งทำให้

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k} \text{ เป็นไปไม่ได้}$$

นั่นคือ $n = p^{k-1}(p-1)$

ดังนั้น r เป็นรากปฐมฐานของ p^k ทุกจำนวนเต็ม $k \geq 1$

ตัวอย่าง 8.17 กำหนดให้ 3 เป็นรากปฐมฐานของ 7 จงตรวจสอบว่า 3 เป็นรากปฐมฐานของ 7^k เมื่อ $k > 1$ หรือไม่

วิธีทำ เนื่องจาก $7^2 = 49$

และ $3^{p-1} = 3^6 \not\equiv 1 \pmod{49}$ แสดงว่า 3 เป็นรากปฐมฐานของ 7^2

โดยทฤษฎีบท 8.8 จะได้ว่า 3 เป็นรากปฐมฐานของ 7^k เมื่อ $k \geq 1$

ดังนั้น 3 เป็นรากปฐมฐานของ 7^k เมื่อ $k > 1$

บทแทรก 8.8

ให้ p เป็นจำนวนเต็มคี่ และ k เป็นจำนวนเต็ม โดยที่ $k \geq 1$

แล้ว $2p^k$ มีรากปฐมฐาน

พิสูจน์

ให้ r เป็นรากปฐมฐานของ p^k โดยที่ r เป็นจำนวนคี่

ดังนั้น $(r, 2p^k) = 1$

และเนื่องจาก $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$

ให้ $n = \text{ord}_{2p^k} r$ จะได้ว่า $n \mid \phi(p^k)$

และเนื่องจาก $r^n \equiv 1 \pmod{2p^k}$ จะได้ว่า $r^n \equiv 1 \pmod{p^k}$

ดังนั้น $\phi(p^k) \mid n$ นั่นคือ $n = \phi(p^k) = \phi(2p^k)$

ดังนั้น r เป็นรากปฐมฐานของ $2p^k$

ตัวอย่าง 8.18 จงตรวจสอบว่า 3 เป็นรากปฐมฐานของ 4 หรือไม่

วิธีทำ เนื่องจากตัวหารบวกของ 4 คือ 1, 2, 4 และ $\phi(4) = 2$

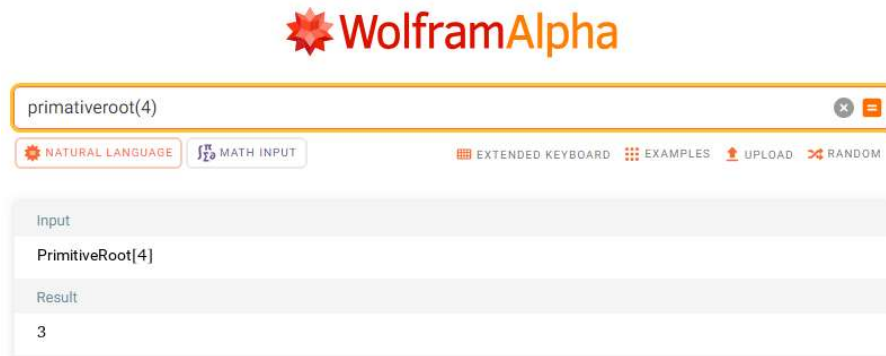
$$3^1 \equiv 3 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

แสดงว่า $\text{ord}_4 3 = 2 = \phi(4)$

ดังนั้น 3 เป็นรากปฐมฐานของ 4

จากตัวอย่าง 8.18 ใช้ Wolfram Alpha เพื่อแสดงว่า 3 เป็นรากปฐมฐานของ 4 ดังภาพประกอบ 8.4



ภาพประกอบ 8.4 ใช้ Wolfram Alpha เพื่อแสดงว่า 3 เป็นรากปฐมฐานของ 4

8.4 ทฤษฎีบทของดซ์นี

ในหัวข้อที่ผ่านมาพบว่าถ้า a เป็นรากปฐมฐานของ m จะได้ว่า $a^1, a^2, \dots, a^{\phi(m)}$ จะเป็นระบบส่วนตกค้างลดรูปมอดุโล m สำหรับในหัวข้อนี้จะเป็นการศึกษาในกรณีที่ a เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m แล้วสามารถเขียน a ให้อยู่ในรูป $r^x \equiv a \pmod{m}$ ดังบทนิยามต่อไปนี้

บทนิยาม 8.3

กำหนดให้ r เป็นรากปฐมฐานของ m ถ้า $(a, m) = 1$ จะได้ว่ามีจำนวนเต็ม x ที่มีค่าบวกน้อยสุด ที่ทำให้ $r^x \equiv a \pmod{m}$ แล้วจะเรียก x ว่า **ดซ์นี** ของ a เทียบกับฐาน r ซึ่ง $1 \leq x \leq \phi(m)$ เขียนแทนด้วย $x = \text{ind}_r a$

ตัวอย่าง 8.19 กำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 5 จงหาดซ์นี

วิธีทำ หาดซ์นีของ a เทียบกับฐาน 2 มอดุโล 5 โดยที่ $a = 1, 2, 3, 4$

พิจารณา

$$2^1 \equiv 2 \pmod{5}$$

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

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

ดังนั้น $\text{ind}_2 1 = 4$, $\text{ind}_2 2 = 1$, $\text{ind}_2 3 = 3$ และ $\text{ind}_2 4 = 2$

ตัวอย่าง 8.20 กำหนดให้ 3 และ 5 เป็นรากปฐมฐานมอดุโล 7 จงหาดัชนี

วิธีทำ หาดัชนีของ a เทียบกับฐาน 3 และ 5 มอดุโล 7 โดยที่ $a = 1, 2, 3, 4, 5, 6$

พิจารณา

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

ดังนั้น $\text{ind}_3 1 = 6$, $\text{ind}_3 2 = 2$, $\text{ind}_3 3 = 1$, $\text{ind}_3 4 = 4$, $\text{ind}_3 5 = 5$, $\text{ind}_3 6 = 3$

$\text{ind}_5 1 = 6$, $\text{ind}_5 2 = 4$, $\text{ind}_5 3 = 5$, $\text{ind}_5 4 = 2$, $\text{ind}_5 5 = 1$, $\text{ind}_5 6 = 3$

จากตัวอย่าง 8.19 พบว่าดัชนีของจำนวนเต็มใด ๆ เมื่อเทียบกับรากปฐมฐานที่แตกต่างกันไม่จำเป็นต้องเท่ากัน ต่อไปจะเป็นการแสดงสมบัติที่สำคัญของดัชนีในรูปแบบทฤษฎีบท ดังต่อไปนี้

ทฤษฎีบท 8.9

ถ้า m เป็นจำนวนเต็มบวกซึ่งมี r เป็นรากปฐมฐานให้ a และ b เป็นจำนวนเต็ม โดยที่ $(a, m) = 1$ และ $(b, m) = 1$ จะได้ว่า

1. $\text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$ และ $\text{ind}_r r \equiv 1 \pmod{\phi(m)}$
2. $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$
3. $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$ เมื่อ k เป็นจำนวนเต็มบวก

พิสูจน์

(1) เนื่องจาก $r^{\text{ind}_r 1} \equiv 1 \equiv r^0 \pmod{m}$ และ $r^{\text{ind}_r r} \equiv r \equiv r^1 \pmod{m}$ จะได้

$$\text{ind}_r 1 \equiv 0 \pmod{\phi(m)} \text{ และ } \text{ind}_r r \equiv 1 \pmod{\phi(m)}$$

- (2) จาก $r^{\text{ind}_r a} \equiv a \pmod{m}$ และ $r^{\text{ind}_r b} \equiv b \pmod{m}$ จะได้ว่า
 $r^{\text{ind}_r a + \text{ind}_r b} \equiv r^{\text{ind}_r a} r^{\text{ind}_r b} \equiv ab \pmod{m}$ และ
 $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$
- (3) กำหนดให้ k เป็นจำนวนเต็มบวก จาก $r^{\text{ind}_r a} \equiv a \pmod{m}$ จะได้ว่า
 $r^{k \cdot \text{ind}_r a} \equiv \left(r^{\text{ind}_r a}\right)^k \equiv a^k \pmod{m}$
 เนื่องจาก $r^{\text{ind}_r a^k} \equiv a^k \pmod{m}$
 เพราะฉะนั้น $r^{\text{ind}_r a^k} \equiv r^{k \cdot \text{ind}_r a} \pmod{m}$ และ
 $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$ เมื่อ k เป็นจำนวนเต็มบวก

ตัวอย่าง 8.21 กำหนดให้ $m = 7$ และ $r = 5$ เป็นรากปฐมฐานมอดุโล 7 จงหา $\text{ind}_5 6$, $\text{ind}_5 16$ และ $\text{ind}_5 18$

วิธีทำ เนื่องจาก $\phi(7) = 6$

พิจารณา

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

จะได้

$$\begin{aligned} \text{ind}_5 6 &= \text{ind}_5(2 \cdot 3) \equiv \text{ind}_5 2 + \text{ind}_5 3 \pmod{\phi(7)} \equiv 4 + 5 \pmod{6} \equiv 3 \pmod{6} \\ \text{ind}_5 16 &= \text{ind}_5(2^4) \equiv 4 \text{ind}_5 2 \pmod{\phi(7)} \equiv 4 \cdot 4 \pmod{6} \equiv 4 \pmod{6} \\ \text{ind}_5 18 &= \text{ind}_5(2 \cdot 3^2) \equiv \text{ind}_5 2 + \text{ind}_5 3^2 \pmod{\phi(7)} \equiv \text{ind}_5 2 + 2 \text{ind}_5 3 \pmod{6} \\ &\equiv 4 + (2 \cdot 5) \pmod{6} \equiv 2 \pmod{6} \end{aligned}$$

ดังนั้น $\text{ind}_5 6 \equiv 3 \pmod{6}$, $\text{ind}_5 16 \equiv 4 \pmod{6}$ และ $\text{ind}_5 18 \equiv 2 \pmod{6}$

ดัชนีสามารถนำมาประยุกต์ใช้ในการหาผลเฉลยของสมภาคบางรูปแบบจากวิธีการและทฤษฎีบทดังต่อไปนี้

กำหนดให้

$$x^k \equiv a \pmod{m} \quad \dots(1)$$

โดยที่ m เป็นจำนวนเต็มบวกที่มีรากปฐมฐานและ $(a, m) = 1$ และ $k \geq 2$ จึงได้ว่าสมภาค (1) สมมูลกับสมภาคเชิงเส้น

$$k \cdot \text{ind} \equiv \text{ind } a \pmod{\phi(m)} \quad \dots(2)$$

เมื่อสมภาค (2) เป็นสมภาคเชิงเส้นที่มีตัวไม่ทราบค่าหรือตัวแปร

ถ้า $d = (k, \phi(m))$ และ $d \nmid \text{ind } a$ จะได้ว่าสมภาค (2) ไม่มีผลเฉลย

ถ้า $d \mid \text{ind } a$ จะได้ว่า (2) มีผลเฉลย และมีจำนวน d ผลเฉลยมอดุโล m

ทำให้ตัวแปร x ในสมภาค (1) มีผลเฉลย d ผลเฉลยมอดุโล m ด้วย

ทฤษฎีบท 8.10

กำหนดให้ m เป็นจำนวนเต็มบวกที่มี r เป็นรากปฐมฐาน a, b เป็นจำนวนเต็ม ซึ่ง $(a, b) = 1, (b, m) = 1$ แล้ว $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$

พิสูจน์

($\Rightarrow$) กำหนดให้ m เป็นจำนวนเต็มบวกที่มี r เป็นรากปฐมฐาน a, b เป็นจำนวนเต็ม ซึ่ง

$$(a, b) = 1, (b, m) = 1 \text{ และ } a \equiv b \pmod{m}$$

จะพิสูจน์ว่า $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$

จากที่กำหนดให้ $a \equiv b \pmod{m}$

เนื่องจาก $r^{\text{ind}_r a} \equiv a \pmod{m}$ และ $r^{\text{ind}_r b} \equiv b \pmod{m}$

ดังนั้น $r^{\text{ind}_r a} \equiv r^{\text{ind}_r b} \pmod{m}$

จะได้ $\text{ind}_r a \equiv \text{ind}_r b \pmod{(\text{ord}_m r)}$ แต่ $\text{ord}_m r = \phi(m)$

ดังนั้น $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$

($\Leftarrow$) กำหนดให้ m เป็นจำนวนเต็มบวกที่มี r เป็นรากปฐมฐาน a, b เป็นจำนวนเต็ม ซึ่ง

$$(a, b) = 1, (b, m) = 1 \text{ และ } \text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$$

จะพิสูจน์ว่า $a \equiv b \pmod{m}$

จากที่กำหนดให้ $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$

ดังนั้นจะมีจำนวนเต็ม k ซึ่ง $\text{ind}_r a = \text{ind}_r b + k\phi(m)$

เนื่องจาก $r^{\text{ind}_r a} \equiv a \pmod{m}$ และ $r^{\text{ind}_r b} \equiv b \pmod{m}$

ดังนั้น $a \equiv r^{\text{ind}_r a} \pmod{m}$ และ $b \equiv r^{\text{ind}_r b} \pmod{m}$

จะได้ $a \equiv r^{\text{ind}_r b + k\phi(m)} \pmod{m}$

$$\text{นั่นคือ } a \equiv b \left(r^{k\phi(m)} \right) (\text{mod } m) \quad \dots(1)$$

$$\text{เนื่องจาก } r^{\phi(m)} \equiv 1 (\text{mod } m) \text{ และ } r^{k\phi(m)} \equiv 1 (\text{mod } m)$$

$$\text{ดังนั้น } \left(r^{\phi(m)} \right)^k \equiv 1 (\text{mod } m)$$

$$\text{นั่นคือ } b \left(r^{k\phi(m)} \right) \equiv b \left(r^{\phi(m)} \right)^k \equiv b (\text{mod } m) \quad \dots(2)$$

$$\text{จาก (1) และ (2) จะได้ } a \equiv b (\text{mod } m)$$

การนำดัชนีไปช่วยในการหาผลเฉลยของสมภาคเชิงเส้น และสมภาคในรูปแบบอื่น ๆ แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 8.22 จงหาผลเฉลยของสมภาคเชิงเส้น $2x \equiv 7 (\text{mod } 13)$ เมื่อกำหนดให้ 2 เป็นรากปฐม

ฐานมอดุโล 13

วิธีทำ เนื่องจาก $\phi(13) = 12$

พิจารณา

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

$$\text{จากสมภาค } 2x \equiv 7 (\text{mod } 13) \text{ จะได้ } \text{ind}_2 2x \equiv \text{ind}_2 7 (\text{mod } \phi(13))$$

พิจารณา

$$\begin{aligned} \text{ind}_2 2 + \text{ind}_2 x &\equiv \text{ind}_2 7 (\text{mod } 12) \\ 1 + \text{ind}_2 x &\equiv 11 (\text{mod } 12) \\ \text{ind}_2 x &\equiv 10 (\text{mod } 12) \end{aligned}$$

$$\text{จากบทนิยามของดัชนีจะได้ } x \equiv 2^{10} (\text{mod } 13) \text{ หรือ } x \equiv 10 (\text{mod } 13)$$

$$\text{ดังนั้น } x \equiv 10 (\text{mod } 13) \text{ เป็นผลเฉลยของสมภาคเชิงเส้น } 2x \equiv 7 (\text{mod } 13)$$

ตัวอย่าง 8.23 จงหาผลเฉลยของสมภาคเชิงเส้น $9x \equiv 1 (\text{mod } 5)$ เมื่อกำหนดให้ 2 เป็นรากปฐม

ฐานมอดุโล 5

วิธีทำ เนื่องจาก 2 เป็นรากปฐมฐานมอดุโล 5

พิจารณา

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

จากสมภาค $9x \equiv 1 \pmod{5}$ จะได้ $\text{ind}_2 9x \equiv \text{ind}_2 1 \pmod{\phi(5)}$

พิจารณา

$$\begin{aligned}\text{ind}_2 9 + \text{ind}_2 x &\equiv \text{ind}_2 1 \pmod{4} \\ \text{ind}_2 3^2 + \text{ind}_2 x &\equiv 4 \pmod{4} \\ 2\text{ind}_2 3 + \text{ind}_2 x &\equiv 4 \pmod{4} \\ 2 \cdot 3 + \text{ind}_2 x &\equiv 4 \pmod{4} \\ 6 + \text{ind}_2 x &\equiv 4 \pmod{4} \\ \text{ind}_2 x &\equiv 2 \pmod{4}\end{aligned}$$

จากบทนิยามของดัชนีจะได้ $x \equiv 2^2 \pmod{5}$ นั่นคือ $x \equiv 4 \pmod{5}$

ดังนั้น $x \equiv 4 \pmod{5}$ เป็นผลเฉลยของสมภาคเชิงเส้น $9x \equiv 1 \pmod{5}$

ตัวอย่าง 8.24 จงหาผลเฉลยของสมภาค $6x^{12} \equiv 11 \pmod{17}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐาน

มอดุโล 17

วิธีทำ เนื่องจาก 3 เป็นรากปฐมฐานของ 17 และ $\phi(17) = 16$

พิจารณา

$$\begin{array}{ll}3^1 \equiv 3 \pmod{17} & 3^9 \equiv 14 \pmod{17} \\3^2 \equiv 9 \pmod{17} & 3^{10} \equiv 8 \pmod{17} \\3^3 \equiv 10 \pmod{17} & 3^{11} \equiv 7 \pmod{17} \\3^4 \equiv 13 \pmod{17} & 3^{12} \equiv 4 \pmod{17} \\3^5 \equiv 5 \pmod{17} & 3^{13} \equiv 12 \pmod{17} \\3^6 \equiv 15 \pmod{17} & 3^{14} \equiv 2 \pmod{17} \\3^7 \equiv 11 \pmod{17} & 3^{15} \equiv 6 \pmod{17} \\3^8 \equiv 16 \pmod{17} & 3^{16} \equiv 1 \pmod{17}\end{array}$$

จากสมภาค $6x^{12} \equiv 11 \pmod{17}$ จะได้ $\text{ind}_3 6x^{12} \equiv \text{ind}_3 11 \pmod{\phi(17)}$

พิจารณา

$$\begin{aligned}\text{ind}_3 6 + \text{ind}_3 x^{12} &\equiv \text{ind}_3 11 \pmod{16} \\ 15 + 12\text{ind}_3 x &\equiv 7 \pmod{16}\end{aligned}$$

$$12ind_3 x \equiv 8 \pmod{16}$$

$$3ind_3 x \equiv 2 \pmod{4}$$

$$\text{แสดงว่า } 3ind_3 x \equiv 2, 6, 10, 14 \pmod{16}$$

$$\text{จากบทนิยามของดัชนีจะได้ } x \equiv 3^2, 3^6, 3^{10}, 3^{14} \pmod{17}$$

เนื่องจาก

$$3^2 \equiv 9 \pmod{17}$$

$$3^6 \equiv 15 \pmod{17}$$

$$3^{10} \equiv 8 \pmod{17}$$

$$3^{14} \equiv 2 \pmod{17}$$

$$\text{ดังนั้น } x \equiv 2, 8, 9, 15 \pmod{17} \text{ เป็นผลเฉลยของสมภาค } 6x^{12} \equiv 11 \pmod{17}$$

ในหัวข้อที่ผ่านมาพบว่าถ้าจำนวนใด ๆ มีรากปฐมฐานแล้วอาจจะมีรากปฐมฐานมากกว่า 1 ได้ ดังนั้นในการหาผลเฉลยของสมภาคโดยใช้ดัชนีนั้นสามารถใช้รากปฐมฐานตัวใดก็ได้ก็ได้อีกแต่ก็สามารถได้ผลเฉลยเป็นชุดเดียวกัน ดังตัวอย่างต่อไปนี้

ตัวอย่าง 8.25 จงหาผลเฉลยของสมภาค $4x^9 \equiv 7 \pmod{13}$ เมื่อกำหนดให้ 2 และ 6 เป็นราก

ปฐมฐานมอดุโล 13

วิธีทำ ให้ 2 เป็นรากปฐมฐานของ 13 และ $\phi(13) = 12$

พิจารณา

$$2^1 \equiv 2 \pmod{13} \quad 2^7 \equiv 11 \pmod{13}$$

$$2^2 \equiv 4 \pmod{13} \quad 2^8 \equiv 9 \pmod{13}$$

$$2^3 \equiv 8 \pmod{13} \quad 2^9 \equiv 5 \pmod{13}$$

$$2^4 \equiv 3 \pmod{13} \quad 2^{10} \equiv 10 \pmod{13}$$

$$2^5 \equiv 6 \pmod{13} \quad 2^{11} \equiv 7 \pmod{13}$$

$$2^6 \equiv 12 \pmod{13} \quad 2^{12} \equiv 1 \pmod{13}$$

$$\text{จากสมภาค } 4x^9 \equiv 7 \pmod{13} \text{ จะได้ } 4x^9 \equiv 7 \equiv 20 \pmod{13}$$

$$\text{นั่นคือ } x^9 \equiv 5 \pmod{13}$$

พิจารณา

$$ind_2 x^9 \equiv ind_2 5 \pmod{\phi(13)}$$

$$9ind_2 x \equiv 9 \pmod{12}$$

$$ind_2 x \equiv 1 \pmod{4}$$

$$\text{แสดงว่า } ind_2 x \equiv 1, 5, 9 \pmod{12}$$

จากบทนิยามของดัชนีจะได้ $x \equiv 2^1, 2^5, 2^9 \pmod{13}$

เนื่องจาก

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

$$2^5 \equiv 6 \pmod{13}$$

$$2^9 \equiv 5 \pmod{13}$$

นั่นคือ $x \equiv 2, 8, 9, 15 \pmod{17}$ เป็นผลเฉลยของสมภาค $6x^{12} \equiv 11 \pmod{17}$

ให้ 6 เป็นรากปฐมฐานของ 13 และ $\phi(13) = 12$

พิจารณา

$$6^1 \equiv 6 \pmod{13} \quad 6^7 \equiv 7 \pmod{13}$$

$$6^2 \equiv 10 \pmod{13} \quad 6^8 \equiv 3 \pmod{13}$$

$$6^3 \equiv 8 \pmod{13} \quad 6^9 \equiv 5 \pmod{13}$$

$$6^4 \equiv 9 \pmod{13} \quad 6^{10} \equiv 4 \pmod{13}$$

$$6^5 \equiv 2 \pmod{13} \quad 6^{11} \equiv 11 \pmod{13}$$

$$6^6 \equiv 12 \pmod{13} \quad 6^{12} \equiv 1 \pmod{13}$$

จากสมภาค $4x^9 \equiv 7 \pmod{13}$ จะได้ $4x^9 \equiv 7 \equiv 20 \pmod{13}$

นั่นคือ $x^9 \equiv 5 \pmod{13}$

พิจารณา

$$\text{ind}_6 x^9 \equiv \text{ind}_6 5 \pmod{\phi(13)}$$

$$9\text{ind}_6 x \equiv 9 \pmod{12}$$

$$\text{ind}_2 x \equiv 1 \pmod{4}$$

แสดงว่า $\text{ind}_2 x \equiv 1, 5, 9 \pmod{12}$

จากบทนิยามของดัชนีจะได้ $x \equiv 2^1, 2^5, 2^9 \pmod{13}$

เนื่องจาก

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

$$2^5 \equiv 6 \pmod{13}$$

$$2^9 \equiv 5 \pmod{13}$$

นั่นคือ $x \equiv 2, 8, 9, 15 \pmod{17}$ เป็นผลเฉลยของสมภาค $6x^{12} \equiv 11 \pmod{17}$

ดังนั้น ผลเฉลยของสมภาค $6x^{12} \equiv 11 \pmod{17}$ คือ $x \equiv 2, 8, 9, 15 \pmod{17}$

จากการศึกษาในบทที่ผ่านมาพบว่สมภาคบางสมภาคอาจจะมีหรือไม่มีผลเฉลยก็ได้ ดังนั้นก่อนที่จะหาผลเฉลยต้องตรวจสอบก่อนว่าสมภาคที่กำหนดให้นั้นมีผลเฉลยหรือไม่ และถ้ามีผลเฉลยแล้วจะมีผลเฉลยทั้งหมดกี่ผลเฉลย สำหรับทฤษฎีบทไปนั้นจะเป็นอีกทฤษฎีบทหนึ่งที่มีความสำคัญ

อย่างมากที่ใช้สำหรับตรวจสอบว่าสมภาคมีผลเฉลยหรือไม่และยังสามารถตรวจสอบจำนวนผลเฉลยทั้งหมดได้

ทฤษฎีบท 8.11

ให้ m เป็นจำนวนเต็มบวกที่มีรากปฐมฐาน และ a เป็นจำนวนเต็ม
ซึ่ง $(a, m) = 1$ แล้ว $x^k \equiv a \pmod{m}$ จะมีผลเฉลยก็ต่อเมื่อ $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$
เมื่อ $d = (m, \phi(m))$ และถ้าสมภาค $x^k \equiv a \pmod{m}$ มีผลเฉลยแล้ว จะมีจำนวนผล
เฉลยเท่ากับ d ผลเฉลย

พิสูจน์

($\Rightarrow$) ให้ r เป็นรากปฐมฐานมอดุโล m

จะได้ว่า สมภาค $k \text{ ind } x \equiv \text{ind } a \pmod{\phi(m)}$ ซึ่งมีตัวไม่ทราบค่าคือ $\text{ind } x$

ดังนั้นโดยวิธีการหาผลเฉลยของสมภาคเชิงเส้น จะหาผลเฉลยได้

ก็ต่อเมื่อ $d \mid \text{ind } a$ เมื่อ $d = (m, \phi(m))$ และจะมีผลเฉลยที่แตกต่างกัน

d ผลเฉลย ดังนั้นสรุปได้ว่า $x^k \equiv a \pmod{m}$ จะมีผลเฉลยก็ต่อเมื่อ

$d \mid \text{ind } a$ และถ้ามีผลเฉลยแล้วจะมี d ผลเฉลย

($\Leftarrow$) พิจารณา $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ เมื่อ $d = (m, \phi(m))$ สมภาคนี้จะสมมูลกับ

$\frac{\phi(m)}{d} \text{ ind } a \equiv 0 \pmod{\phi(m)}$ และสมภาคนี้จะจริงก็ต่อเมื่อ $d \mid \text{ind } a$

นั่นคือ $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$ ก็ต่อเมื่อ $d \mid \text{ind } a$

ตัวอย่าง 8.26 จงพิจารณาว่าสมภาค $3x^5 \equiv 10 \pmod{17}$ มีผลเฉลยหรือไม่ ถ้ามีจงบอกจำนวนผลเฉลย เมื่อกำหนดให้ 5 เป็นรากปฐมฐานมอดุโล 17

วิธีทำ จากสมภาค $3x^5 \equiv 10 \pmod{17}$ จะได้ $3x^5 \equiv 10 \pmod{17} \equiv 27 \pmod{17}$

นั่นคือ $x^5 \equiv 9 \pmod{17}$ เนื่องจาก $\phi(17) = 16$ และ $(16, 5) = 1$

นั่นคือ $9^{\frac{16}{1}} \equiv 9^{16} \pmod{17}$ และเนื่องจาก $9^{16} \equiv 1 \pmod{17}$

ดังนั้น สมภาค $3x^5 \equiv 10 \pmod{17}$ มีผลเฉลย และมี 1 ผลเฉลย

ตัวอย่าง 8.27 จงพิจารณาว่าสมภาค $x^3 \equiv 4 \pmod{13}$ มีผลเฉลยหรือไม่ ถ้ามีจงบอกจำนวนผลเฉลย เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 13

วิธีทำ เนื่องจาก $\phi(13) = 12$ และ $(12, 3) = 3$

$$\text{นั่นคือ } 4^{\frac{12}{3}} \equiv 4^4 \pmod{13} \text{ แต่ } 4^4 \equiv 9 \pmod{13} \not\equiv 1 \pmod{13}$$

ดังนั้น สมภาค $x^3 \equiv 4 \pmod{13}$ ไม่มีผลเฉลย

8.5 สรุปท้ายบทที่ 8

การหาจำนวนเต็ม k ที่สอดคล้องกับสมภาค $a^k \equiv 1 \pmod{m}$ โดยที่ k นั้นเป็นจำนวนเต็มบวกที่มีค่าน้อยสุดแทนด้วยสัญลักษณ์ $\text{ord}_m a = k$ หมายความว่าอันดับของ a มอดุโล m มีค่าเท่ากับ k สำหรับวิธีการหาอันดับของ a มอดุโล m นั้นจะเป็นการหาโดยตรงจากการแทนค่า k ไปเรื่อย ๆ ตั้งแต่ $k = 1$ ไปจนถึง $k = m - 1$ ซึ่งวิธีการดังกล่าวนี้ไม่เหมาะกับกรณีที่ m ที่มีค่ามาก ซึ่งในที่นี้ได้แนะนำทฤษฎีต่างที่ช่วยแก้ปัญหาการหา $\text{ord}_m a$ สำหรับในกรณีที่ $\text{ord}_m a = \phi(m)$ โดยที่ $(a, m) = 1$ เรียก a ว่าเป็น รากปฐมฐานของ m นอกจากนี้ยังพบว่าจำนวนใด ๆ นั้นจะมีหรือไม่มีรากปฐมฐานก็ได้และถ้ามีรากปฐมฐานแล้วอาจจะมีมากกว่า 1 ได้ มีการนำเสนอทฤษฎีบทรวมทั้งบทแทรกไว้สำหรับตรวจสอบรากปฐมฐาน สำหรับจำนวนเฉพาะและการมีรากปฐมฐานพบว่าจำนวนเต็ม $n \geq 1$ มีรากปฐมฐานก็ต่อเมื่อ $n = 2, 4, p^k$ หรือ $2p^k$ เมื่อ p เป็นจำนวนเฉพาะคี่ สำหรับกรณีที่ $(a, m) = 1$ จะได้ว่ามีจำนวนเต็ม x ที่มีค่าน้อยสุด ที่ทำให้ $r^x \equiv a \pmod{m}$ โดยที่ $1 \leq x \leq \phi(m)$ เรียก x ว่าดัชนีของ a เทียบกับฐาน r เขียนแทนด้วย $x = \text{ind}_r a$ ดัชนีของจำนวนเต็มเดียวกันเมื่อเทียบกับรากปฐมฐานที่แตกต่างกันไม่จำเป็นต้องเท่ากัน โดยได้แสดงสมบัติที่สำคัญของดัชนี ในรูปแบบทฤษฎีบท นอกจากนี้ยังสามารถนำทฤษฎีบทของดัชนีมาประยุกต์ใช้ในการหาผลเฉลยของ สมภาคเชิงเส้น สมภาคไม่เชิงเส้นบางรูปแบบได้

แบบฝึกหัดท้ายบทที่ 8

1. จงหาอันดับของจำนวนเต็ม 3, 5 และ 11
 - 1.1 มอดุโล 13
 - 1.2 มอดุโล 17
 - 1.3 มอดุโล 23
2. กำหนดให้ a, m และ x เป็นจำนวนเต็มบวกโดยที่ $(a, m) = 1$ จงพิสูจน์ว่า ถ้า $\text{ord}_m a \mid x$ แล้ว $a^x \equiv 1 \pmod{m}$
3. จงหาอันดับของจำนวนเต็ม 928
 - 3.1 มอดุโล 5
 - 3.2 มอดุโล 7
 - 3.3 มอดุโล 13
4. จงแสดงว่า 2 เป็นรากปฐมฐานของ 19 แต่ไม่เป็นรากปฐมฐานของ 17
5. จงหารากปฐมฐานของ 11, 13 และ 19
6. จงตรวจสอบว่า 15 มีรากปฐมฐานหรือไม่
7. กำหนดให้ 2 เป็นรากปฐมฐานของ 19 จงหาระบบส่วนตกค้างลดรูปมอดุโล 19
8. จงหาจำนวนรากปฐมฐานทั้งหมดของจำนวนต่อไปนี้
 - 8.1 7
 - 8.2 13
 - 8.3 15
 - 8.4 18
 - 8.5 23
 - 8.6 25
9. จงหาจำนวนรากปฐมฐานทั้งหมดของจำนวนต่อไปนี้
 - 9.1 $(3)^2$
 - 9.2 $(7)^2$
 - 9.3 $(13)^2$
 - 9.4 $(17)^2$
10. จงหาจำนวนรากปฐมฐานของจำนวนที่กำหนดให้ต่อไปนี้เมื่อ k เป็นจำนวนเต็มบวก
 - 10.1 3^k
 - 10.2 7^k
 - 10.3 13^k
 - 10.4 17^k

11. กำหนดให้ 2 และ 6 เป็นรากปฐมฐานมอดุโล 13 จงหาตัวชี้
12. จงหาผลเฉลยของสมภาคต่อไปนี้
 - 12.1 $7x \equiv 1 \pmod{13}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 13
 - 12.2 $6x \equiv 11 \pmod{17}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 17
 - 12.3 $2x \equiv 3 \pmod{7}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 7
 - 12.4 $2x \equiv 3 \pmod{5}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 5
 - 12.5 $4x^9 \equiv 7 \pmod{13}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 13
 - 12.6 $3x^5 \equiv 10 \pmod{17}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 17
13. ตรวจสอบว่าสมภาคต่อไปนี้ มีผลเฉลยหรือไม่ ถ้ามีจงบอกจำนวนผลเฉลย
 - 13.1 $5x \equiv 1 \pmod{13}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 13
 - 13.2 $6x \equiv 12 \pmod{17}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 17
 - 13.3 $2x^2 \equiv 3 \pmod{7}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 7
 - 13.4 $2x^5 \equiv 3 \pmod{5}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 5
 - 13.5 $x^9 \equiv 7 \pmod{13}$ เมื่อกำหนดให้ 2 เป็นรากปฐมฐานมอดุโล 13
 - 13.6 $5x^5 \equiv 10 \pmod{17}$ เมื่อกำหนดให้ 3 เป็นรากปฐมฐานมอดุโล 17