

บทที่ 2

การหารลงตัว

การหารของจำนวนเต็มสองจำนวนนั้นมีจำนวนที่เกี่ยวข้องประกอบด้วย ตัวตั้งหาร (Dividend) ตัวหารตัวหาร (Divisor) ผลหารผลหาร (Quotient) และเศษเหลือ (Remainder) โดยมีความสัมพันธ์ที่เกี่ยวข้องกันดังนี้ ตัวตั้ง หารด้วยตัวหารคูณกับผลหารบวกด้วยเศษของการหาร ในการหาผลหารของจำนวนเต็มสองจำนวนสามารถใช้วิธีการหารยาวหรือการหารสั้นเพื่อให้ได้ผลลัพธ์ตามที่ต้องการ ในส่วนของผลการหารนั้นถ้าพิจารณาจากเศษที่เกิดจากการหาร ถ้าเศษจากการหารเป็นศูนย์จะเรียกการหารนั้นว่าการหารลงตัว แต่ถ้าเศษที่เกิดจากการหารไม่เป็นศูนย์ แสดงว่าการหารนั้นไม่ลงตัวนั่นเอง นอกจากการหารสั้นและหารยาวแล้วผู้อ่านต้องมีความรู้เกี่ยวกับ ตัวหาร พหุคูณพหุคูณ (Multiple) และจำนวนประกอบ (Composite Number) ซึ่งจำนวนดังกล่าวเป็นหลักการที่มนุษย์ได้เรียนรู้ เมื่อประมาณ 350 ปีก่อนคริสตกาล ซึ่งในบทนี้จะนำเสนอเนื้อหาสำคัญที่ใช้ในการศึกษาการหารลงตัว ดังต่อไปนี้ ขั้นตอนวิธีการหาร (Division Algorithm) การหารลงตัว (Exact Division) ตัวหารร่วมมาก ขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm) และตัวคูณร่วมน้อยเพื่อเป็นพื้นฐานในการศึกษาทฤษฎีจำนวนขั้นสูงต่อไป

2.1 ขั้นตอนวิธีการหาร

ในการหารผลหารของจำนวนเต็มสองจำนวนสามารถใช้วิธีการหารสั้นหรือหารยาวได้เช่น ต้องการหาร 113 ด้วย 12 สามารถแสดงการหารด้วยวิธีการหารดังต่อไปนี้

$$\begin{array}{r} 9 \\ 12 \overline{) 113} \\ \underline{108} \\ 5 \end{array}$$

จากการตั้งหารพบว่า 113 หารด้วย 12 ไม่ลงตัว โดยได้ผลหารเท่ากับ 9 และมีเศษจากการหารเท่ากับ 5 จากความสัมพันธ์ของตัวเลขทั้งหมดนี้เขียนได้อยู่ในรูป $113 = 12(9) + 5$ และจากวิธีการเดียวกัน 1,065 หารด้วย 71 จะพบว่าเศษจากการหาร 1,065 ด้วย 71 มีค่าเท่ากับศูนย์ซึ่งหมายความว่า 1,065 หารด้วย 71 ลงตัว แสดงความสัมพันธ์ได้เป็น $1065 = 71(15) + 0$ จากความสัมพันธ์ข้างต้นเกี่ยวข้องกับทฤษฎีบทพื้นฐานเกี่ยวกับขั้นตอนวิธีการหารลงตัวโดยแสดงไว้ในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1 (ขั้นตอนวิธีการหาร)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$ โดยที่ $0 \leq r < |a|$ จะเรียก q ว่าผลหาร และ r ว่า เศษเหลือ

พิสูจน์ แบ่งการพิสูจน์ออกเป็น 2 ตอน ดังต่อไปนี้

ตอนที่ 1 จะพิสูจน์ว่า $q, r \in \mathbb{Z}$ ที่ทำให้ $b = aq + r, 0 \leq r < |a|$

โดยจะแบ่งการพิสูจน์ออกเป็นสองกรณี

กรณี 1 ถ้า $a > 0$ แล้ว $|a| = a$ ให้ $S = \{b - ax \mid x \in \mathbb{Z} \text{ และ } b - ax \geq 0\}$

เนื่องจาก $a \geq 1$ จะได้ว่า $|b|a \geq |b|$

แสดงว่า $b - (-|b|a) \geq b + |b| \geq 0$ ดังนั้น $S \neq \emptyset$

แสดงว่าจะมี $s \in S$ ซึ่ง $s = 0$ หรือ $s > 0$

ถ้า $s = 0$ จะได้ว่ามี $q \in \mathbb{Z}$ ซึ่ง $s = b - aq$

นั่นคือ $b = aq + s$ เมื่อ $s = 0$

ถ้า $s > 0$ โดยหลักการจัดอันดับดี จะมี $r \in S$ ซึ่ง

$r = s$ หรือ $r < s$ เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

แสดงว่าจะมี $q \in \mathbb{Z}$ ซึ่ง $r = b - aq$

ดังนั้น $b = aq + r$ โดยที่ $r > 0$

ต่อไปจะแสดงว่า $r < a$ โดยสมมติว่า $r \geq a$

ดังนั้น $r - a = (b - aq) - a = b - a(q + 1) \geq 0$

แสดงว่า $r - a \in S$

แต่ $r - a < r$ ซึ่งขัดแย้งกับที่ว่า r เป็นจำนวนเต็มบวกที่น้อยที่สุดใน S

ดังนั้น $r < a = |a|$

เพราะฉะนั้นมี $q, r \in \mathbb{Z}$ ที่ทำให้

$b = aq + r$ โดยที่ $0 \leq r < |a|$

กรณี 2 ถ้า $a < 0$ แล้ว $|a| = -a$

จากกรณี 1 จะได้ว่า $d, r \in \mathbb{Z}$ ที่ทำให้

$b = (-a)d + r = a(-d) + r, 0 \leq r < -a = |a|$

ให้ $q = -d$ แสดงว่ามี $q, r \in \mathbb{Z}$ ซึ่ง

$b = aq + r$ โดยที่ $0 \leq r < |a|$

ตอนที่ 2 ต่อไปจะแสดงว่ามี $q, r \in \mathbb{Z}$ เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$

โดยที่ $0 \leq r < |a|$ นั่นคือสมมติว่ามี $q, r, q', r' \in \mathbb{Z}$ ที่ทำให้

$$b = aq + r, 0 \leq r < |a|$$

$$\text{และ } b = aq' + r', 0 \leq r' < |a|$$

จะพิสูจน์ว่า $q = q'$ และ $r = r'$

$$\text{ให้ } b = aq + r, 0 \leq r < |a| \text{ และ } b = aq' + r', 0 \leq r' < |a|$$

$$\text{จะได้ว่า } |a||q - q'| = |r - r'| \text{ โดยที่ } 0 \leq |r - r'| < |a|$$

$$\text{ดังนั้น } 0 \leq |a||q - q'| < |a| \text{ แสดงว่า } 0 \leq |q - q'| < 1$$

$$\text{และจาก } |q - q'| \text{ เป็นจำนวนเต็ม จะได้ว่า } |q - q'| = 0 \text{ และทำให้ } |r - r'| = 0$$

$$\text{นั่นคือ } q = q' \text{ และ } r = r'$$

ดังนั้น มีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$ โดยที่ $0 \leq r < |a|$

ตัวอย่าง 2.1 จงหาจำนวนเต็ม q และ r ที่ $b = aq + r$ โดยที่ $0 \leq r < |a|$ เมื่อกำหนดให้

$$a = 18 \text{ และ } b = 47$$

วิธีทำ เนื่องจาก 47 หารด้วย 18 ได้ผลหารเท่ากับ 2 และมีเศษจากการหารเท่ากับ 11 นั่นคือ

$$47 = 18(2) + 11$$

$$\text{จากรูปทั่วไป } b = aq + r \text{ โดยที่ } a = 18 \text{ และ } b = 47$$

$$\text{ดังนั้น } q = 2 \text{ และ } r = 11$$

ตัวอย่าง 2.2 จงแสดงว่ากำลังสองของ n เมื่อหารด้วย 5 จะเหลือเศษเป็น 0, 1 หรือ 4

วิธีทำ ให้ $b = n^2$ และ $a = 5$ โดยทฤษฎีบท 2.1

$$\text{จะได้ } n = 5q + r \text{ โดยที่ } r = 0, 1, 2, 3, 4$$

$$\text{ดังนั้น } b = (5q + r)^2 = 25q^2 + 10qr + r^2$$

$$\text{ถ้า } r = 0 \text{ แล้ว } b = 25q^2 + 10q(0) + (0)^2 = 5(5q^2) + 0$$

$$\text{ถ้า } r = 1 \text{ แล้ว } b = 25q^2 + 10q(1) + (1)^2 = 5(5q^2 + 2q) + 1$$

$$\text{ถ้า } r = 2 \text{ แล้ว } b = 25q^2 + 10q(2) + (2)^2 = 5(5q^2 + 4q) + 4$$

$$\text{ถ้า } r = 3 \text{ แล้ว } b = 25q^2 + 10q(3) + (3)^2 = 5(5q^2 + 6q + 1) + 4$$

$$\text{ถ้า } r = 4 \text{ แล้ว } b = 25q^2 + 10q(4) + (4)^2 = 5(5q^2 + 8q + 3) + 1$$

ดังนั้น จากทุกกรณีข้างต้นแสดงให้เห็นว่า b เมื่อหารด้วย 5 จะเหลือเศษเป็น 0, 1 หรือ 4

ตัวอย่าง 2.3 จงแสดงว่า $\frac{n(n^2 + 2)}{3}$ เป็นจำนวนเต็มเสมอ เมื่อ n เป็นจำนวนเต็มบวก

วิธีทำ จะแสดงว่า $n(n^2 + 2)$ หารด้วย 3 จะเหลือเศษเป็น 0 เท่านั้น

ให้ $m = n(n^2 + 2)$ และ $a = 3$ โดยทฤษฎีบท 2.1

จะได้ $n = 3q + r$ โดยที่ $r = 0, 1, 2$

$$\text{ดังนั้น } m = (3q + r)[(3q + r)^2 + 2] = 27q^3 + 27q^2r + 9qr^2 + 6q + r^3 + 2r$$

$$\begin{aligned} \text{ถ้า } r = 0 \text{ แล้ว } m &= 27q^3 + 27q^2(0) + 9q(0)^2 + 6q + (0)^3 + 2(0) \\ &= 27q^3 + 6q \\ &= 3(9q^3 + 2q) + 0 \end{aligned}$$

$$\begin{aligned} \text{ถ้า } r = 1 \text{ แล้ว } m &= 27q^3 + 27q^2(1) + 9q(1)^2 + 6q + (1)^3 + 2(1) \\ &= 27q^3 + 27q^2 + 9q + 6q + 3 \\ &= 3(9q^3 + 9q^2 + 3q + 2q + 1) + 0 \end{aligned}$$

$$\begin{aligned} \text{ถ้า } r = 2 \text{ แล้ว } m &= 27q^3 + 27q^2(2) + 9q(2)^2 + 6q + (2)^3 + 2(2) \\ &= 27q^3 + 54q^2 + 36q + 6q + 12 \\ &= 3(9q^3 + 18q^2 + 12q + 2q + 4) + 0 \end{aligned}$$

ดังนั้น $\frac{n(n^2 + 2)}{3}$ เป็นจำนวนเต็มเสมอ เมื่อ n เป็นจำนวนเต็มบวก

ตัวอย่าง 2.4 จงแสดงว่ากำลังสองของจำนวนเต็มใด ๆ จะอยู่ในรูป $3k$ หรือ $3k + 1$ สำหรับบางจำนวนเต็ม k

วิธีทำ ให้ b เป็นจำนวนเต็มใด ๆ โดยทฤษฎีบท 2.1

จะมีจำนวนเต็ม q และ r ซึ่ง $b = 3q + r$ โดยที่ $r = 0, 1, 2$

นั่นคือ $b = 3q, b = 3q + 1$ และ $b = 3q + 2$

กรณีที่ $b = 3q$ จะได้

$$b^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3k$$

เมื่อ $k = 3q^2$

กรณีที่ $b = 3q + 1$ จะได้

$$b^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$$

เมื่อ $k = 3q^2 + 2q$

กรณีที่ $b = 3q + 2$ จะได้

$$b^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) = 3k$$

เมื่อ $k = 3q^2 + 4q + 1$

ดังนั้น กำลังสองของจำนวนเต็มใด ๆ จะอยู่ในรูป $3k$ หรือ $3k + 1$ สำหรับบางจำนวนเต็ม k

ตัวอย่าง 2.5 จงหาจำนวนนับตั้งแต่ 1 ถึง 500 ทั้งหมดที่หารด้วย 7 เศษเหลือคือ 2 และเมื่อหารด้วย 16 เศษเหลือคือ 7

วิธีทำ ให้ $b \in \{1, 2, 3, 4, \dots, 500\}$ ซึ่งสอดคล้อง

$$b = 7q + 2 \quad \text{เมื่อ } q \in \mathbb{Z}$$

$$\text{และ } b = 16p + 7 \quad \text{เมื่อ } p \in \mathbb{Z}$$

ดังนั้น $7q + 2 = 16p + 7$ แล้ว

$$7q = 16p + 5$$

$$q = \frac{16p + 5}{7}$$

สรุปเป็นตารางดังนี้

p	1	8	15	22	29
q	3	19	35	51	67
b	23	135	247	359	471

ตารางสิ้นสุดที่ $p = 29$ เนื่องจากเป็นค่าสุดท้ายที่ทำให้ $b \leq 500$ หากพิจารณาค่าถัดไป ($p = 36$) จะได้ $b = 583$ ซึ่งเกินขอบเขตที่โจทย์กำหนด

ดังนั้น จำนวนนับตั้งแต่ 1 ถึง 500 ทั้งหมดที่หารด้วย 7 เหลือเศษ 2 และเมื่อหารด้วย 16 เหลือเศษ 7 คือ 23, 135, 247 และ 471

ตัวอย่าง 2.6 ให้ n หารด้วย 8 เหลือเศษ 3 จงหาว่า $n^2 + 4n$ หารด้วย 8 จะเหลือเศษเท่าไร

วิธีทำ เนื่องจาก n หารด้วย 8 เหลือเศษ 3 แสดงว่า

$$n = 8k + 3 \quad \text{เมื่อ } k \in \mathbb{Z}$$

$$\text{พิจารณา } n^2 + 4n = (8k + 3)^2 + 4(8k + 3)$$

$$= 64k^2 + 48k + 9 + 32k + 12$$

$$= 64k^2 + 80k + 21$$

$$= 64k^2 + 80k + 16 + 5$$

$$= 8(8k^2 + 10k + 2) + 5$$

ดังนั้น $n^2 + 4n$ หารด้วย 8 เหลือเศษเท่ากับ 5

2.2 การหารลงตัว

ในการหารจำนวนเต็มด้วยจำนวนเต็ม พบว่าเศษที่เกิดจากการหารอาจเป็นศูนย์ได้หรือไม่เป็นศูนย์ก็ได้ เช่น 148 หารด้วย 4 จะได้ว่า $148 = (37)(4) + 0$ ถ้าพบว่าเศษของการหารคือ 0 เรียกการหารจำนวนเต็มด้วยจำนวนเต็มแล้วเหลือเศษศูนย์ว่าการหารลงตัว โดยมีบทนิยามดังต่อไปนี้

บทนิยาม 2.1

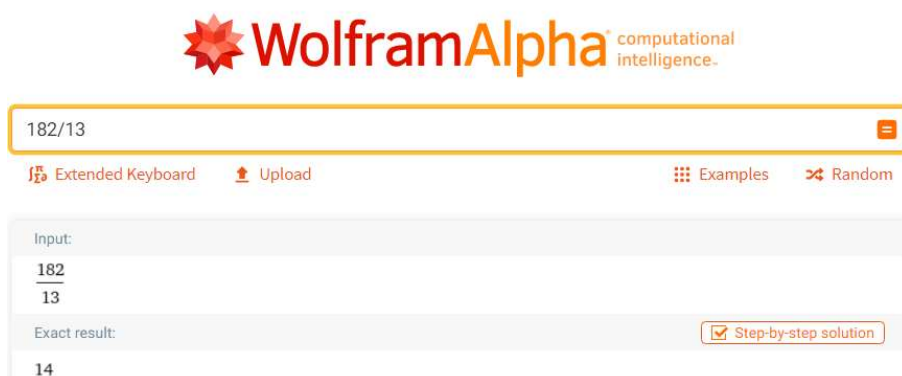
ถ้า a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ เรียกว่า a ว่าเป็น **ตัวหาร** หรือ **ตัวประกอบ** ตัวหนึ่งของ b ก็ต่อเมื่อ มีจำนวนเต็ม q ที่ทำให้ $b = aq$ ในกรณี a เป็นตัวหารของ b จะเรียกอีกแบบหนึ่งว่า a หาร b ลงตัว เขียนแทนด้วยสัญลักษณ์ $a|b$ และใช้สัญลักษณ์ $a \nmid b$ แทน a หาร b ไม่ลงตัว

ตัวอย่าง 2.7

$$13 \mid 182 \text{ เพราะมีจำนวนเต็ม } 14 \text{ ที่ทำให้ } 182 = (13)(14)$$

$$15 \nmid 145 \text{ เพราะไม่มีจำนวนเต็ม } q \text{ ใด ๆ เลยที่ทำให้ } 145 = 15q$$

ในตัวอย่างต่อไปได้มีการแสดงวิธีใช้วูลแฟรมแอลฟา(Wolfram Alpha) ซึ่งเป็นซอฟต์แวร์ที่สามารถเรียกใช้งานได้โดยไม่เสียค่าใช้จ่าย ด้วยการสื่อสารผ่านทางอินเทอร์เน็ต จากเว็บไซต์ www.wolframalpha.com ในการแก้ปัญหาบางปัญหาของทฤษฎีจำนวน โดยผู้ที่สนใจสามารถเข้าไปในเว็บไซต์แล้วพิมพ์คำสั่งเหมือนที่ได้แสดงไว้ในภาพประกอบ เช่น ตัวอย่าง 2.7 สามารถใช้ Wolfram Alpha เพื่อตรวจสอบว่ามีจำนวนเต็ม 14 ที่ทำให้ $182 = (13)(14)$ ดังภาพประกอบ 2.1



ภาพประกอบ 2.1 ใช้ Wolfram Alpha เพื่อแสดงว่า $13 \mid 182$

เช่นเดียวกันสามารถใช้ Wolfram Alpha เพื่อตรวจสอบว่าไม่มีจำนวนเต็ม q ไต ๆ เลยที่ทำให้ $145 = 15q$ ดังภาพประกอบ 2.2



ภาพประกอบ 2.2 ใช้ Wolfram Alpha เพื่อแสดงว่า $15 \nmid 145$

ตัวอย่าง 2.8 จงหาตัวประกอบทั้งหมดของ 225

เนื่องจาก $225 = 5 \times 45$

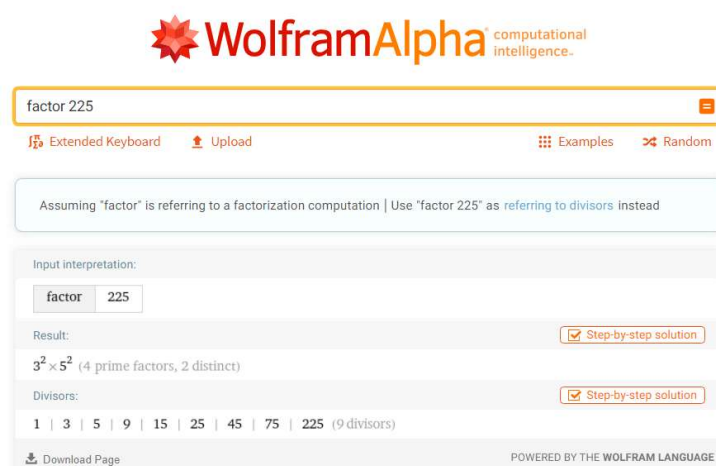
$$= 5 \times 5 \times 9$$

$$= 5 \times 5 \times 3 \times 3$$

ดังนั้นตัวประกอบทั้งหมดของ 225 คือ $\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 25, \pm 45, \pm 75$

ແລະ ± 225

จากตัวอย่าง 2.8 สามารถใช้ Wolfram Alpha เพื่อหาตัวประกอบทั้งหมดของ 225
ดังภาพประกอบ 2.3



ภาพประกอบ 2.3 ใช้ Wolfram Alpha เพื่อหาตัวประกอบทั้งหมดของ 225

ตัวหารหรือตัวประกอบของจำนวนเต็มใด ๆ จะมีจำนวนเป็นคู่เสมอเนื่องจากถ้า b หารด้วย a ลงตัว แล้วก็จะหารด้วย $-a$ ลงตัวด้วยเช่นกัน ในการกล่าวถึงตัวหารโดยปกติจะพิจารณาเฉพาะตัวหารที่เป็นจำนวนบวกเท่านั้น สำหรับการศึกษาเกี่ยวกับการหารลงตัว สมบัติเบื้องต้นของการหารลงตัว และข้อเท็จจริงที่จะนำไปใช้ในการแก้ปัญหาล่าง ๆ ที่เกี่ยวข้องกันกับจำนวนเต็ม ได้แสดงไว้ในทฤษฎีบทและบทแทรกต่อไปนี้ดังต่อไปนี้

ทฤษฎีบท 2.2 ให้ a, b, c เป็นจำนวนเต็มที่ไม่เป็นศูนย์ จะได้ว่า

1. $a|0, 1|a, a|a$
2. ถ้า $a|b$ และ $b|c$ แล้ว $a|c$
3. ถ้า $a|b$ และ $c|d$ แล้ว $ac|bd$
4. ถ้า $a|b$ แล้ว $a|bc$
5. $a|b$ ก็ต่อเมื่อ $ac|bc$
6. ถ้า $a|b$ และ $b|a$ แล้ว $a = b$ หรือ $a = -b$
7. ถ้า $a|b$ แล้ว $|a| \leq |b|$
8. $a|1$ ก็ต่อเมื่อ $a = \pm 1$
9. ถ้า $a|b$ และ $a|c$ แล้ว $a|(bx + cy)$ สำหรับทุกจำนวนเต็ม x, y
10. ถ้า $a|(b + c)$ และ $a|b$ แล้ว $a|c$

พิสูจน์

1. เพราะว่า $0 = a \cdot 0$ เพราะฉะนั้น $a|0$
 เพราะว่า $a = a \cdot 1$ เพราะฉะนั้น $a|a$
 เพราะว่า $a = 1 \cdot a$ เพราะฉะนั้น $1|a$
2. สมมติให้ $a|b$ และ $b|c$ เพราะฉะนั้นจะมีจำนวนเต็ม x, y ที่ทำให้
 $b = ax$ และ $c = by$
 เพราะฉะนั้น $c = (ax)y = a(xy)$
 ให้ $z = xy$ สำหรับบางจำนวนเต็ม z
 จะได้ $c = az$
 ดังนั้น $a|c$
3. สมมติให้ $a|b$ และ $c|d$ เพราะฉะนั้นจะมีจำนวนเต็ม x, y ที่ทำให้
 $b = ax$ และ $d = cy$

เพราะฉะนั้น $bd = (ax)(cy) = (ac)(xy)$

ให้ $z = xy$

ดังนั้น $bd = (ac)z$ นั่นคือ $ac \mid bd$

4. สมมติให้ $a \mid b$ เพราะฉะนั้นจะมีจำนวนเต็ม x ที่ทำให้

$$b = ax \text{ และ } bc = (ax)c = a(xc)$$

ให้ $z = xc$

ดังนั้น $bc = az$ นั่นคือ $a \mid bc$

5. ($\Rightarrow$) สมมติให้ $a \mid b$ เพราะฉะนั้นจะมีจำนวนเต็ม x ที่ทำให้

$$b = ax \text{ และ } bc = (ax)c = ac(x)$$

ดังนั้น $ac \mid bc$

- ($\Leftarrow$) สมมติให้ $ac \mid bc$ สำหรับ c ที่ไม่เป็นศูนย์ เพราะฉะนั้นจะมีจำนวนเต็ม x ที่ทำให้

$$bc = ac(x) \text{ หรือ } b = a(x)$$

ดังนั้น $a \mid b$

6. สมมติให้ $a \mid b$ และ $b \mid a$ เพราะฉะนั้นจะมีจำนวนเต็ม x, y ที่ทำให้

$$b = ax \text{ และ } a = by$$

จะได้ $b = (by)x = b(xy)$

นั่นคือ $xy = 1$ แสดงว่า $x = 1$ และ $y = 1$ หรือ $x = -1$ และ $y = -1$

ดังนั้น $a = b$ หรือ $a = -b$

7. สมมติให้ $a \mid b$ และ $b \neq 0$ เพราะฉะนั้นจะมีจำนวนเต็ม x ที่ทำให้

$$b = ax \text{ เนื่องจาก } b \neq 0 \text{ จะได้ } x \neq 0$$

เพราะฉะนั้น $|x| \geq 1$

นั่นคือ $|a| \leq |a||x| = |ax| = |b|$

ดังนั้น $|a| \leq |b|$

8. ($\Rightarrow$) ให้ $a \mid 1$ เพราะฉะนั้น $|a| \leq |1|$ นั่นคือ $|a| \leq 1$

เนื่องจาก a เป็นจำนวนเต็มที่ไม่เป็นศูนย์

แสดงว่า $|a|$ เป็นไปได้มีเพียงค่าเดียวเท่านั้นคือ $|a| = 1$

ดังนั้น $a = \pm 1$

- ($\Leftarrow$) เห็นได้ชัดว่า ถ้า $a = \pm 1$ แล้ว $a \mid 1$

9. สมมติ $a \mid b$ และ $a \mid c$ เพราะฉะนั้น จะมีจำนวนเต็ม m และ n ที่ทำให้

$$b = am \text{ และ } c = an$$

ให้ x และ y เป็นจำนวนเต็มใด ๆ จะได้

$$bx = (am)x \text{ และ } cy = (an)y$$

และ

$$\begin{aligned} bx + cy &= (am)x + (an)y \\ &= (amx) + (any) \\ &= a(mx) + a(ny) \\ &= a[(mx) + (ny)] \end{aligned}$$

แสดงว่า $a \mid (bx + cy)$

10 สมมติให้ $a \mid (b + c)$ และ $a \mid b$ เพราะฉะนั้น จะมีจำนวนเต็ม x และ y ที่ทำให้

$$b + c = ax \text{ และ } b = ay$$

จะได้ $ay + c = ax$ หรือ

$$\begin{aligned} c &= ax - ay \\ &= a(x - y) \end{aligned}$$

แสดงว่า $a \mid c$

ตัวอย่าง 2.9

$$7 \mid 49 \text{ และ } 2 \mid 26 \text{ จะได้ } 14 \mid 1274$$

$$3 \mid 21 \text{ และ } 3 \mid 105 \text{ จะได้ } 3 \mid (21(2) + 105(14))$$

$$\text{ถ้า } x \mid 12 \text{ และ } 12 \mid x \text{ แล้ว } x = \pm 12$$

บทแทรก 2.1

สำหรับจำนวนเต็ม $a, b_1, b_2, \dots, b_n$ ใด ๆ $a \neq 0$ จะได้ว่า

ถ้า $a \mid b_1, a \mid b_2, \dots, a \mid b_n$ แล้ว $a \mid (b_1x_1 + b_2x_2 + \dots + b_nx_n)$

เมื่อ $x_1, x_2, \dots, x_n$ เป็นจำนวนเต็มใด ๆ

พิสูจน์ การพิสูจน์คล้ายกันกับทฤษฎีบท 2.2 ข้อ 9

ตัวอย่าง 2.10 จงแสดงว่า ถ้า a เป็นจำนวนคู่แล้ว $a^2 + 2a$ หารด้วย 4 ลงตัว

วิธีทำ เนื่องจาก a เป็นจำนวนคู่

$$\text{ทำให้ } 2 \mid a$$

$$\text{ดังนั้น } 4 \mid a^2 \text{ และ } 4 \mid 2a$$

นั่นคือ $4 \mid (a^2 + 2a)$

ดังนั้น a เป็นจำนวนคู่แล้ว $a^2 + 2a$ หารด้วย 4 ลงตัว

ตัวอย่าง 2.11 จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า 6 หาร $7^n - 1$ ลงตัว สำหรับจำนวนเต็มบวก n

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

1. ขั้นฐาน

$$7^1 - 1 = 6 \text{ ซึ่งหารลงตัว ดังนั้น } P(1) \text{ เป็นจริง}$$

2. ขั้นอุปนัย

ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ 6 หาร $7^k - 1$ ลงตัว

จะแสดงว่า $P(k+1)$ เป็นจริง

$$\begin{aligned} \text{พิจารณา } 7^{k+1} - 1 &= 7 \cdot 7^k - 1 \\ &= (6 + 1)(7^k - 1) \\ &= 6(7^k - 1) + (7^k - 1) \end{aligned}$$

เนื่องจาก 6 หาร $7^k - 1$ และ $6(7^k - 1)$ ลงตัว

แสดงว่า $6(7^k - 1) + (7^k - 1)$ ลงตัว

แสดงว่า $P(k+1)$ เป็นจริง

ดังนั้น โดยหลักอุปนัยเชิงคณิตศาสตร์จะได้ว่า 6 หาร $7^n - 1$ ลงตัว

ตัวอย่าง 2.12 จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า $(a+b) \mid (a^{2^n} - b^{2^n})$ สำหรับจำนวนเต็มบวก n

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

1. ขั้นฐาน

$$\text{เนื่องจาก } a^{2^{(1)}} - b^{2^{(1)}} = (a-b)(a+b)$$

$$\text{จะได้ } (a+b) \mid (a-b)(a+b)$$

ดังนั้น $P(1)$ เป็นจริง

2. ขั้นอุปนัย

ให้ $k \in \mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ $(a+b) \mid (a^{2^k} - b^{2^k})$

จะแสดงว่า $P(k+1)$ เป็นจริง

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

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

เนื่องจาก $(a+b)|(a^{2k} - b^{2k})$ และ $(a+b)|(a^2 - b^2)$

แสดงว่า $(a+b)|a^2(a^{2k} - b^{2k}) + b^{2k}(a^2 - b^2)$ นั่นคือ $P(k+1)$ เป็นจริง

ดังนั้น โดยหลักอุปนัยเชิงคณิตศาสตร์จะได้ว่า $(a+b)|(a^{2n} - b^{2n})$

2.3 ตัวหารร่วมมาก

การศึกษาเพื่อค้นหาจำนวนเต็มบวกที่มีค่ามากที่สุดที่นำไปหารจำนวนสองจำนวน หรือมากกว่าได้ลงตัวนั้น คือการหาตัวหารร่วมมากนั่นเอง โดยในหัวข้อนี้จะเป็นการศึกษาการหาตัวหารร่วมมากด้วยวิธีการต่าง ๆ บทนิยามและทฤษฎีบทที่สำคัญที่เกี่ยวข้องกับตัวหารร่วมมาก เพื่อนำไปประยุกต์ใช้ในการแก้ปัญหบางในปัญหาของจำนวนเต็ม ก่อนที่จะกล่าวถึงวิธีการหาตัวหารร่วมมากและทฤษฎีบทที่เกี่ยวข้องนั้น ต้องทำความรู้จักกับความหมายรวมทั้งสัญลักษณ์ต่าง ๆ ที่เกี่ยวข้องในบทนิยามต่อไปนี้

บทนิยาม 2.2

กำหนดให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกันและ d เป็นจำนวนเต็มบวก จะเรียก d ว่า **ตัวหารร่วมมาก** หรือ **ห.ร.ม.** ของ a และ b ก็ต่อเมื่อ d มีคุณสมบัติต่อไปนี้

1. $d|a$ และ $d|b$
2. ถ้า $c|a$ และ $c|b$ แล้ว $c \leq d$

ใช้สัญลักษณ์ (a, b) หรือ $\gcd(a, b)$ แทน **ห.ร.ม.** ของ a และ b นั่นคือ $d = (a, b)$

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

1. สามารถหา (a, b) ได้เสมอ
2. (a, b) มีเพียงจำนวนเดียวเท่านั้น
3. $(a, b) = (a, -b) = (-a, -b) = (b, a)$
4. $(a, 0) = |a|$ เมื่อ $a \neq 0$
5. ถ้า $a|b$ แล้ว $(a, b) = |a|$

เพื่อให้เข้าใจตัวหารร่วมมากนั้นก่อนอื่นขอยกตัวอย่างวิธีการหาตัวหารร่วม และตัวหารร่วมมากดังต่อไปนี้

ตัวอย่าง 2.13 จงหาเซตของตัวหารร่วมทั้งหมดของ 50 และ 76

วิธีทำ กำหนดให้ A แทนเซตของตัวหารร่วมทั้งหมดของ 50 จะได้

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

และ B แทนเซตของตัวหารทั้งหมดของ 76 จะได้

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

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

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

จากตัวอย่างพบว่าเซตของตัวหารร่วมจะมีสมาชิกที่มีค่ามากที่สุดหรือเป็นตัวหารร่วมที่มีค่ามากที่สุด คือ 2 จึงสรุปได้ว่า $2 = (50, 76)$

ตัวอย่าง 2.14 จงหา $(28, 64)$

วิธีทำ จำนวนเต็มบวกที่หาร 28 ลงตัวได้แก่ 1, 2, 4, 7, 14 และ 28

จำนวนเต็มบวกที่หาร 64 ลงตัวได้แก่ 1, 2, 4, 8, 16, 32 และ 64

ตัวหารร่วมของ 28 และ 64 ได้แก่ 1, 2, 4

ดังนั้น $(28, 64) = 4$

จากตัวอย่าง 2.14 สามารถใช้ Wolfram Alpha เพื่อหา $(28, 64)$ ดังภาพประกอบ 2.4



ภาพประกอบ 2.4 ใช้ Wolfram Alpha เพื่อหา $(28, 64)$

การหาตัวหารร่วมมากนั้นเกิดจากการหาตัวหารที่มีร่วมกันและเลือกตัวที่มากที่สุดเพียงตัวเดียวเท่านั้น ดังนั้นตัวหารร่วมมากจึงมีได้เพียงแค่ตัวเดียวเท่านั้น ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.3

ตัวหารร่วมมากของจำนวนเต็ม a และ b จะมีจำนวนเดียวเท่านั้น

พิสูจน์

ให้ d เป็น ตัวหารร่วมมากของ a และ b จะได้ $d|a$ และ $d|b$

ให้ c เป็น ตัวหารร่วมมากของ a และ b จะได้ $c|a$ และ $c|b$

เนื่องจาก c และ d เป็นตัวหารร่วมของ a และ b ดังนั้น $c|d$

เนื่องจาก d และ c เป็นตัวหารของ a และ b ดังนั้น $d|c$

จาก $c|d$ และ $d|c$ โดยที่ $c, d > 0$ จะได้ $c = d$

จากตัวอย่างที่ผ่านมาพบว่าการหาตัวหารร่วมมากของจำนวนเต็มสองจำนวนด้วยการพิจารณาตัวหารร่วมทั้งหมดของแต่ละจำนวนนั้นไม่เหมาะสมในกรณีที่ต้องการหาตัวหารร่วมของสองจำนวนที่มีค่ามาก ๆ โดยในทฤษฎีบทและบทแทรกต่อไปสามารถนำไปแก้ปัญหาดังกล่าวได้ รวมทั้งเป็นพื้นฐานที่นำไปประยุกต์ใช้ในการแก้ปัญหาในทฤษฎีจำนวนขั้นสูงต่อไป

ทฤษฎีบท 2.4

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ หรือ $b \neq 0$ จะได้ว่ามี $x, y \in \mathbb{Z}$

ที่ทำให้ $(a, b) = ax + by$

พิสูจน์

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

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

จากหลักการจัดอันดับดีจะได้ว่ามี $d \in X$ ซึ่ง d เป็นจำนวนเต็มบวกที่น้อยที่สุดใน X

ฉะนั้น $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$ ต่อไปจะแสดงว่า $d = (a, b)$

(i) จาก $a, d \in \mathbb{Z}$ และ $d \in X$ โดยขั้นตอนวิธีการหารจะได้ว่ามี $q, r \in \mathbb{Z}$ ที่ทำให้

$$a = dq + r; \quad 0 \leq r < d$$

$$a = (ax + by)q + r; \quad 0 \leq r < d$$

$$r = a - (ax + by)q; \quad 0 \leq r < d$$

ดังนั้น $r = a(1 - xq) + b(-yq); 0 \leq r < d$

จาก $0 \leq r < d$ จะได้ว่า $r = 0$ หรือ $0 < r < d$

ถ้า $0 < r < d$ จะได้ $r \in X$

ซึ่งขัดแย้งกับการเลือก d เป็นจำนวนเต็มบวก

น้อยที่สุดใน X

ดังนั้น $r = 0$ นั่นคือ $d \mid a$

จาก $b, d \in \mathbb{Z}$ และ $d \in X$ พิสูจน์ในทำนองเดียวกันจะได้ว่า $d \mid b$

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

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

ตัวอย่าง 2.15

$$(12, 20) = 4 = 12(2) + 20(-1)$$

$$(-8, 36) = 4 = -8(4) + 36(1)$$

$$(18, 30) = 6 = 18(-3) + 30(2)$$

บทแทรก 2.2

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่าสำหรับจำนวนเต็ม c ใด ๆ

ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid (a, b)$

พิสูจน์

เนื่องจาก $d = (a, b)$ โดยทฤษฎี 2.4 จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $d = ax + by$

จะได้ว่า $c \mid (ax + by)$

และเนื่องจาก $c \mid a$ และ $c \mid b$ โดยทฤษฎี 2.2 ข้อ 9 นั่นคือ $c \mid d$

ทฤษฎีบท 2.5

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า $(a, b) = 1$ ก็ต่อเมื่อ $x, y \in \mathbb{Z}$

ที่ทำให้ $1 = ax + by$

พิสูจน์

($\Rightarrow$) สมมติ $(a, b) = 1$ โดยทฤษฎีบท 2.4 จะได้ว่า

$$x, y \in \mathbb{Z} \text{ ซึ่ง } 1 = ax + by$$

($\Leftarrow$) สมมติว่ามี $x, y \in \mathbb{Z}$ ซึ่งทำให้ $1 = ax + by$ และให้ $d = (a, b)$

จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (ax + by)$

นั่นคือ $d \mid 1$

แสดงว่า $(a, b) = 1$

ทฤษฎีบท 2.6

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

พิสูจน์

ให้ $D = (ma, mb)$ และ $d = (a, b)$ โดยทฤษฎีบท 2.4 จะได้ว่า $x, y, u, v \in \mathbb{Z}$ ซึ่งทำให้

$$D = (ma)x + (mb)y \text{ และ } d = au + bv$$

(i) จาก $D = (ma, mb)$ จะได้ว่า $D \mid ma$ และ $D \mid mb$

ดังนั้น $D \mid (mau + mbv)$ นั่นคือ $D \mid md$

(ii) จาก $d = (a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (max + mby)$

นั่นคือ $md \mid D$

จาก (i) และ (ii) จะได้ว่า $D = md$ แสดงว่า $(ma, mb) = m(a, b)$

ทฤษฎีบท 2.7

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

พิสูจน์

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

$$\text{โดยทฤษฎีบท 2.6 จะได้ } d = d\left(\frac{a}{d}, \frac{b}{d}\right) \text{ ดังนั้น } \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

ตัวอย่าง 2.16

$$(12, 20) = 4 \text{ และ } \left(\frac{12}{4}, \frac{20}{4}\right) = (3, 5) = 1$$

$$(12, -30) = 6 \text{ และ } \left(\frac{12}{6}, \frac{-30}{6}\right) = (2, -5) = 1$$

ทฤษฎีบท 2.8

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ หรือ $b \neq 0$ และ x เป็นจำนวนเต็ม
จะได้ว่า $(a, b) = (a, b + ax) = (a + bx, b)$

พิสูจน์

ให้ $d = (a, b)$ และ $g = (a, b + ax)$ โดยทฤษฎีบท 2.4 จะได้ว่ามี $u, v, m, n \in \mathbb{Z}$

ที่ทำให้ $d = au + bv$ และ $g = am + (b + ax)n$

(i) จาก $d = (a, b)$ จะได้ว่า $d|a$ และ $d|b$

ดังนั้นโดยทฤษฎี 2.2 ข้อ 9 จะได้ $d|(am + bn + axn)$ นั่นคือ $d|g$

(ii) จาก $g = (a, b + ax)$ จะได้ว่า $g|a$ และ $g|(b + ax)$

ดังนั้น $g|ax$

โดยทฤษฎีบท 2.2 ข้อ 10 จะได้ว่า $g|b$ ดังนั้น $g|(au + bv)$

นั่นคือ $g|d$

จาก (i) และ (ii) จะได้ว่า $d = g$

แสดงว่า $(a, b) = (a, b + ax)$

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

ทฤษฎีบท 2.9

ให้ $a, b \in \mathbb{Z}$ เป็นจำนวนเต็มจะได้ว่า

1. ถ้า $(a, m) = (b, m) = 1$ แล้ว $(ab, m) = 1$

2. ถ้า $(a, m) = 1$ และ $b|a$ แล้ว $(b, m) = 1$

3. ถ้า $a|bc$ และ $(a, b) = 1$ แล้ว $a|c$

4. ถ้า $a|c$ และ $b|c$ โดยที่ $(a, b) = 1$ แล้ว $ab|c$

พิสูจน์

1. ให้ $(a, m) = (b, m) = 1$ จะได้ว่ามี $x, y, u, v \in \mathbb{Z}$ ซึ่ง

$$ax + my = 1 \text{ และ } bu + mv = 1$$

ดังนั้น $1 = (ax + my)(bu + mv) = ab(xu) + m(axv + ybu + myv)$

โดยทฤษฎีบท 2.5 จะได้ว่า $(ab, m) = 1$

2. ให้ $(a, m) = 1$ และ $b|a$ จะได้ว่ามี $x, y, q \in \mathbb{Z}$ ซึ่ง
 $ax + my = 1$ และ $a = bq$
 ดังนั้น $1 = (bq)x + my = b(qx) + my$
 โดยทฤษฎีบท 2.5 จะได้ว่า $(b, m) = 1$
3. ให้ $a|bc$ และ $(a, b) = 1$ จะได้ว่ามี $q, x, y \in \mathbb{Z}$ ซึ่ง
 $bc = aq$ และ $ax + by = 1$
 ดังนั้น $bcy = aqy$ และ $c = axc + byc$
 และ $c = axc + aqy = a(xc + qy)$ นั่นคือ $a|c$
4. ให้ $a|c$ และ $b|c$ โดยที่ $(a, b) = 1$ จะได้ว่ามี $k_1, k_2, x, y \in \mathbb{Z}$ ซึ่ง
 $c = ak_1, c = bk_2$ และ $ax + by = 1$
 ดังนั้น $c = cax + cby = (bk_2)ax + (ak_1)by = ab(k_2x + k_1y)$
 นั่นคือ $ab|c$

ทฤษฎีบท 2.10

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

พิสูจน์

พิจารณาความสัมพันธ์ที่กำหนดให้ $b = aq + r$ หรือ

$$r = b - aq$$

จาก ทฤษฎีบท 2.8 จะได้ว่า

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

เนื่องจาก q เป็นจำนวนเต็ม ดังนั้น $-q$ จึงเป็นจำนวนเต็มด้วย

ให้ $x = -q$ จะได้

$$\begin{aligned}(a, b) &= (a, b + a(-q)) \\ &= (a, b - aq)\end{aligned}$$

เนื่องจาก $r = b - aq$ จะได้

$$(a, b) = (a, r)$$

บทแทรกและทฤษฎีบทที่ได้แสดงไว้ในข้างต้นนั้นทำให้สามารถหาตัวหารร่วมมากได้สะดวกและรวดเร็วมากยิ่งขึ้น แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.17 จงหาค่าของ $(927, 315)$

วิธีทำ $927 = 315(2) + 297$ แสดงว่า $(927, 315) = (315, 297)$

$315 = 297(1) + 18$ แสดงว่า $(315, 297) = (297, 18)$

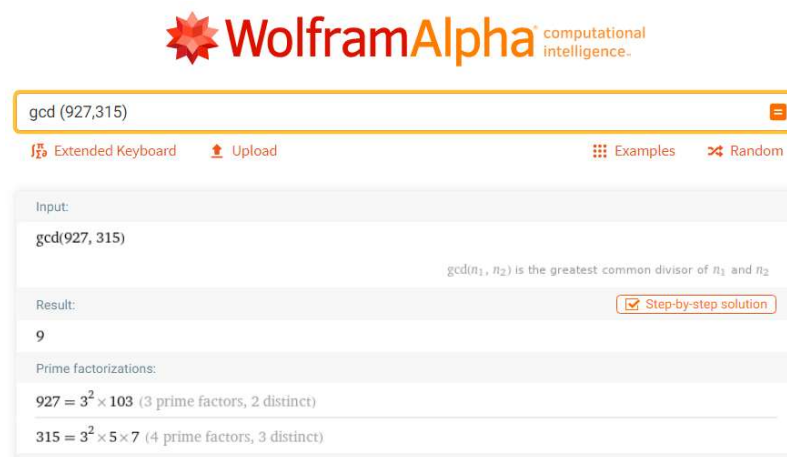
$297 = 18(16) + 9$ แสดงว่า $(297, 18) = (18, 9)$

$18 = 9(2) + 0$ แสดงว่า $(18, 9) = (9, 0) = 9$

นั่นคือ $(927, 315) = (9, 0) = 9$

ดังนั้น $(927, 315) = 9$

จากตัวอย่าง 2.17 สามารถใช้ Wolfram Alpha เพื่อหา $(927, 315)$ ดังภาพประกอบ 2.5



ภาพประกอบ 2.5 ใช้ Wolfram Alpha เพื่อหา $(927, 315)$

จากการศึกษาบทนิยามและทฤษฎีบทพร้อมทั้งตัวอย่างที่ผ่านมาจะเป็นการศึกษาตัวหารร่วมมากของจำนวนเต็มเพียงสองจำนวนเท่านั้น ต่อไปจะเป็นการแสดงบทนิยามของตัวหารร่วมมากของจำนวนเต็มที่มีมากกว่าสองจำนวน ดังบทนิยามต่อไปนี้

บทนิยาม 2.3

ให้ $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ ซึ่งมี $a_i \neq 0$ สำหรับ i บางตัว เรียก $d \in \mathbb{Z}$ ว่า **ตัวหารร่วม** ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ $d \mid a_i$ สำหรับ $i = 1, 2, 3, \dots, n$ และเรียก d ว่า **ตัวหารร่วมมาก** ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ d เป็นตัวหารร่วมที่มีค่ามากที่สุด ซึ่งเขียนแทนด้วย $d = (a_1, a_2, a_3, \dots, a_n)$

จากบทนิยาม พบว่า

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

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

ตัวอย่าง 2.16 จงหา $(42, 64, 78)$

วิธีทำ จำนวนเต็มบวกที่หาร 42 ลงตัวได้แก่ 1, 2, 6, 7, 14, 21 และ 42

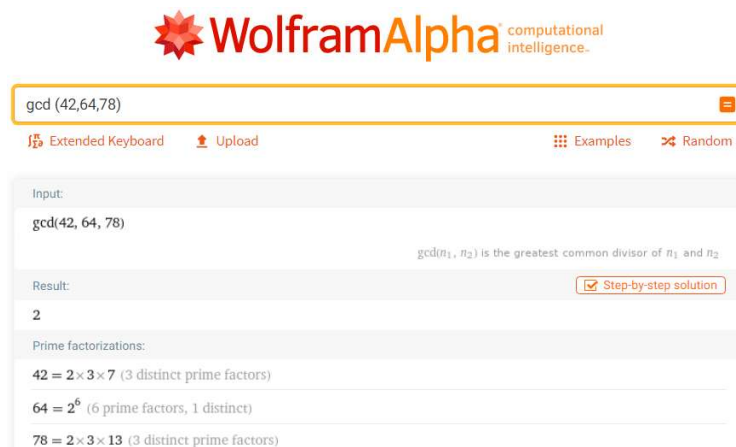
จำนวนเต็มบวกที่หาร 64 ลงตัวได้แก่ 1, 2, 4, 8, 16, 32 และ 64

จำนวนเต็มบวกที่หาร 78 ลงตัวได้แก่ 1, 2, 3, 6, 13, 26, 39 และ 78

ตัวหารร่วมของ 42, 64 และ 78 ได้แก่ 1, 2

ดังนั้น $2 = (42, 64, 78)$

จากตัวอย่าง 2.16 สามารถใช้ Wolfram Alpha เพื่อหา $(42, 64, 78)$ ดังภาพประกอบ 2.6



ภาพประกอบ 2.6 ใช้ Wolfram Alpha เพื่อหา $(42, 64, 78)$

2.4 ขั้นตอนวิธีแบบยุคลิด

ในการค้นหาตัวร่วมมากของจำนวนเต็มสองจำนวนหรือมากกว่าสามารถทำได้หลายวิธีไม่ว่าจะเป็นการหาด้วยการพิจารณาตัวหารร่วมของแต่ละจำนวน หรือการนำทฤษฎีบทมาประยุกต์ใช้ สำหรับขั้นตอนวิธีแบบยุคลิดนั้นเป็นการใช้ขั้นตอนวิธีการหารซ้ำกันหลายครั้ง โดยแสดงไว้ในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.11 (ขั้นตอนวิธีแบบยุคลิด)

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

$$b = aq_1 + r_1, \quad 0 \leq r_1 < a$$

$$a = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$\vdots$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}$$

$$\text{และ } (a, b) = (a, r_n) = r_n$$

พิสูจน์ การพิสูจน์ของทฤษฎีบทนี้แบ่งออกเป็นสองกรณีดังนี้

กรณี 1 ถ้า $a \mid b$ โดยขั้นตอนวิธีการหาร

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

และโดยทฤษฎีบท 2.10 จะได้ว่า $(a, b) = (a, r) = a$

กรณี 2 ถ้า $a \nmid b$ โดยขั้นตอนวิธีการหารจะได้ว่า $q_1, r_1 \in \mathbb{Z}$

$$b = aq_1 + r_1 \text{ เมื่อ } 0 < r_1 < a$$

จากความจริงที่ว่าจำนวนเต็มบวกที่น้อยกว่า a เป็นจำนวนจำกัด

และใช้การกระทำซ้ำ ๆ ของขั้นตอนวิธีการหาร

จะได้ว่ามี $q_2, q_3, \dots, q_n, q_{n+1}, r_1, r_2, \dots, r_n \in \mathbb{Z}$ ที่ทำให้

$$a = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$\vdots$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}$$

โดยทฤษฎีบท 2.10 จะได้ว่า

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

ตัวอย่าง 2.17 จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(142, 1226)$

วิธีทำ $1226 = 142(8) + 90$

$$142 = 90(1) + 52$$

$$90 = 52(1) + 38$$

$$52 = 38(1) + 14$$

$$38 = 14(2) + 10$$

$$14 = 10(1) + 4$$

$$10 = 4(2) + 2$$

$$4 = 2(2)$$

ดังนั้น $(142, 1226) = 2$

ตัวอย่าง 2.18 จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(12378, 3054)$

วิธีทำ $12378 = (3054)(4) + 162$

$$3054 = (162)(18) + 138$$

$$162 = (138)(1) + 24$$

$$138 = (24)(5) + 18$$

$$24 = (18)(1) + 6$$

$$18 = (6)(3)$$

ดังนั้น $(12378, 3054) = 6$

จากทฤษฎีบทขั้นตอนวิธีแบบยุคลิดพบว่าในการหาค่า x และ y เมื่อ $(a, b) = ax + by$ สามารถหาแนวทางได้จากการกำจัดเศษ $r_{n-1}, \dots, r_2, r_1$ จากสมการข้างต้น มีวิธีการดังนี้

เริ่มจากสมการกลุ่มรองสุดท้าย

$$r_n = r_{n-2} - q_n r_{n-1}$$

แล้วแทนค่า r_{n-1} ด้วยค่าในสมการขั้นตอนวิธีแบบยุคลิด จะได้ว่า

$$\begin{aligned} r_n &= r_{n-2} q_n (r_{n-3} - q_{n-1} r_{n-2}) \\ &= r_{n-2} (1 + q_n q_{n-1}) + r_{n-3} (-q_n) \end{aligned}$$

จะเห็นว่าสมการที่ได้นี้แสดงการเขียน r_n ในรูปผลบวกของ r_{n-2} และ r_{n-3} ขั้นตอนต่อไปนี้ทำซ้ำเช่นนี้ไปเรื่อย ๆ ซึ่งจะกำจัดเศษ $r_{n-1}, r_{n-2}, \dots, r_2, r_1$ ตามลำดับ จนในที่สุดจะได้สมการแสดงการเขียน r_n ในรูปผลบวกของ a และ b แต่ r_n คือ ห.ร.ม ของ a และ b นั่นคือ วิธีการที่ทำให้ทราบค่า x และ y ที่ทำให้ $(a, b) = ax + by$ แสดงได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.19 จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(78, 32)$ พร้อมทั้งแสดงวิธีการหาค่า x และ y ที่ทำให้ $(78, 32) = 78x + 32y$

วิธีทำ $78 = 32(2) + 14$

$$32 = 14(2) + 4$$

$$14 = 4(3) + 2$$

$$4 = 2(2)$$

จะได้ $(78, 32) = 2$

หาค่า x และ y ที่ทำให้ $(78, 32) = 78x + 32y$ ดังนี้

$$\begin{aligned} 2 &= 14 - 4(3) \\ &= 14 - [32 - 14(2)]3 \\ &= 14 - [32(3) - 14(6)] \\ &= 14(7) - 32(3) \\ &= [78 - 32(2)](7) - 32(3) \\ &= 78(7) - 32(14) - 32(3) \\ &= 78(7) - 32(17) \\ &= 78(7) + 32(-17) \end{aligned}$$

ดังนั้น $x = 7$ และ $y = -17$ ที่ทำให้ $(78, 32) = 78x + 32y$

ตัวอย่าง 2.20 จงใช้ขั้นตอนวิธีแบบยุคลิดในการหา $(243, 198)$ พร้อมทั้งแสดงวิธีการหาค่า x และ y ที่ทำให้ $(243, 198) = 243x + 198y$

วิธีทำ $243 = 198(1) + 45$

$$198 = 45(4) + 18$$

$$45 = 18(2) + 9$$

$$18 = 9(2)$$

จะได้ $(243, 198) = 9$

หาค่า x และ y ที่ทำให้ $(243, 198) = 243x + 198y$ ดังนี้

$$\begin{aligned} 9 &= 45 - 18(2) \\ &= 45 - [198 - 45(4)](2) \\ &= 45 - [198(2) - 45(8)] \\ &= 45(9) - 198(2) \end{aligned}$$

$$\begin{aligned}
&= [243 - 198](9) - 198(2) \\
&= 243(9) - 198(9) - 198(2) \\
&= 243(9) - 198(11) \\
&= 243(9) + 198(-11)
\end{aligned}$$

ดังนั้น $x = 9$ และ $y = -11$ ที่ทำให้ $(243, 198) = 243x + 198y$

2.5 ตัวคูณร่วมน้อย

การศึกษาเพื่อค้นหาจำนวนเต็มบวกที่มีค่ามากที่สุดที่นำไปหารจำนวนสองจำนวนหรือมากกว่าได้ลงตัวนั้นศึกษาผ่านมาแล้วนั้นคือการหาตัวหารร่วมมาก แต่สำหรับในหัวข้อนี้จะเป็นศึกษาเรื่องที่มีความสัมพันธ์ควบคู่กับตัวหารร่วมมากของจำนวนเต็มสองจำนวน ซึ่งมีบทบาทสำคัญในการศึกษาทฤษฎีจำนวน สำหรับตัวคูณร่วมน้อยนั้นมีบทนิยามที่เกี่ยวข้องดังต่อไปนี้

บทนิยาม 2.4

a เป็นจำนวนเต็มที่ไม่เป็นศูนย์ ถ้า $a|n$ เรียก n ว่า **พหุคูณ** ของ a

บทนิยาม 2.5

กำหนดให้ a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน และ m เป็นจำนวนเต็มบวก จะเรียก m ว่า **ตัวคูณร่วมน้อย** หรือ ค.ร.น. ของ a และ b ก็ต่อเมื่อ m มีคุณสมบัติต่อไปนี้

1. $a|m$ และ $b|m$

2. สำหรับจำนวนเต็มบวก c ถ้า $a|c$ และ $b|c$ แล้ว $m \leq c$

ใช้สัญลักษณ์ $[a, b]$ หรือ $\text{lcm}[a, b]$ แทน ค.ร.น. ของ a และ b นั่นคือ $m = [a, b]$

ตัวอย่าง 2.21 จงหา $[30, 45]$

วิธีทำ พหุคูณของ 30 ได้แก่ $0, \pm 30, \pm 60, \pm 90, \pm 120, \pm 150, \pm 180, \dots$

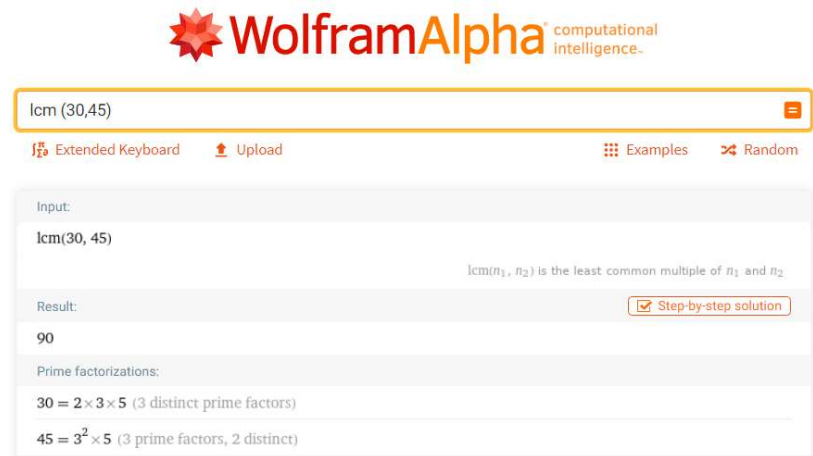
พหุคูณของ 21 ได้แก่ $0, \pm 45, \pm 90, \pm 135, \pm 180, \pm 225, \pm 315, \dots$

ตัวคูณร่วมของ 30 และ 45 คือ $\pm 90, \pm 180, \dots$

ตัวคูณร่วมที่เป็นบวกที่มีค่าน้อยที่สุดคือ 90

ดังนั้น $[30, 45] = 90$

จากตัวอย่าง 2.21 สามารถใช้ Wolfram Alpha เพื่อหา $[30, 45]$ ดังภาพประกอบ 2.7



ภาพประกอบ 2.7 ใช้ Wolfram Alpha เพื่อหา $[30, 45]$

การหาตัวคูณร่วมน้อยในตัวอย่างที่ผ่านมาเหมาะสำหรับการหาตัวคูณร่วมน้อยของสองจำนวนที่หาพหุคูณได้ไม่ยาก แต่ถ้าในกรณีที่สองจำนวนดังกล่าวนี้มีค่ามาก ๆ ทำให้ไม่สะดวกในการหาพหุคูณ ต่อไปเป็นการนำเสนอทฤษฎีบทที่เกี่ยวข้องกับการแก้ปัญหาค้นหาตัวคูณร่วมน้อยดังกล่าว รวมทั้ง ทฤษฎีบทที่เกี่ยวข้องเพื่อนำไปศึกษาทฤษฎีจำนวนขั้นสูงต่อไป

ทฤษฎีบท 2.11

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

พิสูจน์ ให้ $m = [a, b]$ และ c เป็นจำนวนเต็มใด ๆ ที่ $a|c$ และ $b|c$

โดยขั้นตอนวิธีการหารจะได้ว่า มี $q, r \in \mathbb{Z}$ ซึ่ง $c = mq + r$, $0 \leq r < m$

แสดงว่า $r = c - mq$, $0 \leq r < m$ จาก $a|c$ และ $b|c$ จะได้ว่า $a|r$ และ $b|r$

นั่นคือ r เป็นตัวคูณร่วมของ a และ b ถ้า $0 < r < m$ จะขัดแย้งกับ $m = [a, b]$

ดังนั้น $r = 0$ แสดงว่า $m|c$

ทฤษฎีบท 2.12

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

พิสูจน์

$$\text{จาก } (a, b) = (|a|, |b|) \text{ และ } [a, b] = [|a|, |b|]$$

ดังนั้น จึงเป็นการเพียงพอที่จะพิสูจน์กรณีที่ $a, b \in \mathbb{N}$

(i) ให้ $d = (a, b)$ จะได้ว่ามี $x, y \in \mathbb{Z}$ ซึ่ง $a = dx$ และ $b = dy$

$$\text{ให้ } m = \frac{ab}{d} = dxy \text{ จะได้ว่า } m = ay = bx$$

แสดงว่า $a|m$ และ $b|m$ นั่นคือ m เป็นตัวคูณร่วมของ a และ b

(ii) ให้ c เป็นจำนวนเต็มบวกที่ $a|c$ และ $b|c$

จะได้ว่ามี $u, v \in \mathbb{Z}$ ซึ่ง $c = au$ และ $c = bv$

จาก $a = dx$ และ $b = dy$ จะได้ว่า $dxu = dyv$

ดังนั้น $x|yu$ แต่ $(x, y) = 1$ แสดงว่า $x|v$

ดังนั้น จะมี $r \in \mathbb{Z}$ ซึ่ง $v = xr$ และจาก $m = bx$ และ $c = bv$

จะได้ว่า $c = bxr = mr$ ดังนั้น $m|c$

จาก (i) และ (ii) สรุปว่า $m = [a, b]$ นั่นคือ $(a, b)[a, b] = ab$

ตัวอย่าง 2.22 จำนวนนับสองจำนวนคูณกันได้ 80 และมี ห.ร.ม. เป็น 4 จงหา ค.ร.น. ของสองจำนวนดังกล่าว

วิธีทำ สมมติจำนวนทั้งสอง คือ a และ b จาก ทฤษฎีบท 2.11 จะได้

$$\begin{aligned} (a, b)[a, b] &= |ab| \\ 4[a, b] &= 80 \\ [a, b] &= 20 \end{aligned}$$

ดังนั้น ค.ร.น. ของสองจำนวนดังกล่าวคือ 20

ทฤษฎีบท 2.12

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ และ $m \in \mathbb{N}$ จะได้ว่า

$$[ma, mb] = m[a, b]$$

พิสูจน์ จากทฤษฎีบท 2.6 และทฤษฎีบท 2.11 จะได้ว่า

$$\begin{aligned} (ma, mb)[ma, mb] &= m(a, b)[ma, mb] \\ &= |(ma)(mb)| \end{aligned}$$

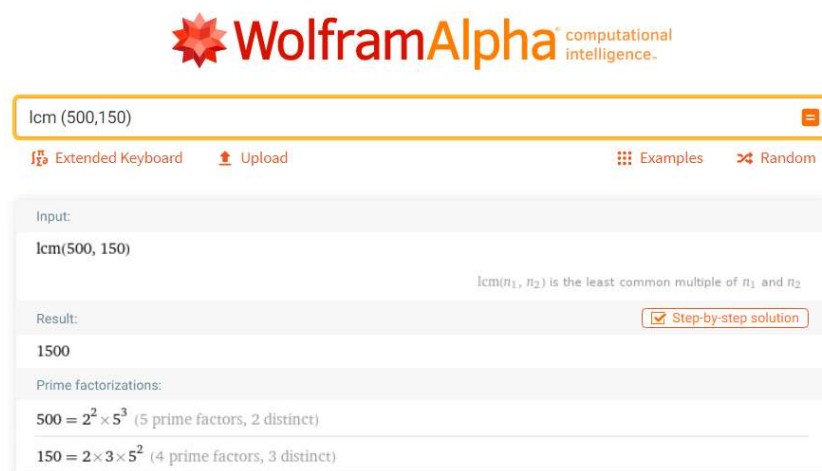
$$\begin{aligned}
 \text{ดังนั้น} \quad [ma, mb] &= \frac{|m^2 ab|}{m(a, b)} \\
 &= \frac{m|ab|}{m(a, b)} \\
 &= m[a, b]
 \end{aligned}$$

ตัวอย่าง 2.23 จงหา $[500, 150]$

$$\begin{aligned}
 \text{วิธีทำ} \quad [500, 150] &= 10[50, 15] \\
 &= 10 \times 5[10, 3] \\
 &= 10 \times 5 \times 10 \times 3 \\
 &= 1500
 \end{aligned}$$

$$\text{ดังนั้น} \quad [500, 150] = 1500$$

จากตัวอย่าง 2.23 สามารถใช้ Wolfram Alpha เพื่อหา $[500, 150]$ ดังภาพประกอบ 2.8



ภาพประกอบ 2.8 ใช้ Wolfram Alpha เพื่อหา $[500, 150]$

ตัวอย่าง 2.24 จงหา $[8100, 630]$

$$\begin{aligned}
 \text{วิธีทำ} \quad [8100, 630] &= 90[90, 7] \\
 &= 90 \times 90 \times 8 \\
 &= 56700
 \end{aligned}$$

$$\text{ดังนั้น} \quad [8100, 630] = 56700$$

ตัวคูณร่วมน้อยสามารถขยายบทนิยามของตัวคูณร่วม และตัวคูณร่วมน้อยของจำนวนเต็มที่มีมากกว่าสองจำนวน คล้ายกันกับตัวหารร่วมมาก โดยแสดงไว้ในบทนิยามต่อไปนี้

บทนิยาม 2.6

ให้ $a_1, a_2, a_3, \dots, a_n \in \mathbb{Z}$ ซึ่ง $a_i \neq 0$ สำหรับ $i = 1, 2, 3, \dots, n$

เรียก $m \in \mathbb{Z}$ ว่า **ตัวคูณร่วม** ของ $a_1, a_2, a_3, \dots, a_n$ ก็ต่อเมื่อ $a_i \mid m$

สำหรับ $i = 1, 2, 3, \dots, n$ และเรียก m ว่า **ตัวคูณร่วมน้อย** ของ $a_1, a_2, a_3, \dots, a_n$

ก็ต่อเมื่อ $m \in \mathbb{N}$ และ m เป็นตัวคูณร่วมที่มีค่าน้อยที่สุด

ซึ่งเขียนแทนด้วย $[a_1, a_2, a_3, \dots, a_n]$

ตัวอย่าง 2.25 จงหา $[3, 8, 10, 15, 32, 60]$

$$\begin{aligned}
 \text{วิธีทำ} \quad [3, 8, 10, 15, 32] &= [[3, 8], 10, 15, 32, 60] \\
 &= [[24, 10], 15, 32, 60] \\
 &= [2[12, 5], 15, 32, 60] \\
 &= [2 \times 12 \times 5, 15, 32, 60] \\
 &= [120, 15, 32, 60] \\
 &= [[120, 15], 32, 60] \\
 &= [15[8, 1], 32, 60] \\
 &= [15 \times 8 \times 1, 32, 60] \\
 &= [120, 32, 60] \\
 &= [[120, 32], 60] \\
 &= [8[15, 4], 60] \\
 &= [8 \times 15 \times 4, 60] \\
 &= [480, 60] \\
 &= 60[8, 1] \\
 &= 60 \times 8 \times 1 \\
 &= 480
 \end{aligned}$$

$$\text{ดังนั้น} \quad [3, 8, 10, 15, 32, 60] = 480$$

จากตัวอย่าง 2.25 สามารถใช้ Wolfram Alpha เพื่อหา $[3, 8, 10, 15, 32, 60]$

ดังภาพประกอบ 2.9

WolframAlpha computational intelligence.

lcm(3,8,10,15,32,60)

NATURAL LANGUAGE MATH INPUT EXTENDED KEYBOARD EXAMPLES UPLOAD RANDOM

Input

lcm(3, 8, 10, 15, 32, 60)

lcm(n_1, n_2) is the least common multiple of n_1 and n_2

Result ☒ Step-by-step solution

480

Prime factorizations

3 is prime

$8 = 2^3$ (3 prime factors, 1 distinct)

$10 = 2 \times 5$ (2 distinct prime factors)

$15 = 3 \times 5$ (2 distinct prime factors)

$32 = 2^5$ (5 prime factors, 1 distinct)

$60 = 2^2 \times 3 \times 5$ (4 prime factors, 3 distinct)

ภาพประกอบ 2.9 ใช้ Wolfram Alpha เพื่อหา $[3, 8, 10, 15, 32, 60]$

2.6 สรุปท้ายบทที่ 2

ในการหาผลหารของจำนวนเต็มสองจำนวนสามารถหาได้โดยขั้นตอนวิธีการหาร กำหนดให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นที่ทำให้ $b = aq + r$ โดยที่ $0 \leq r < |a|$ จะเรียก q ว่าผลหาร เรียก r ว่าเศษเหลือ กรณีที่ $r = 0$ แสดงว่า b หารด้วย a ลงตัวเขียนแทนด้วยสัญลักษณ์ $a | b$ แต่ถ้า $r \neq 0$ แสดงว่า b หารด้วย a ไม่ลงตัวเขียนแทนด้วยสัญลักษณ์ $a \nmid b$ และการหารลงตัวนั้นเป็นพื้นฐานสำคัญในการหาตัวหารร่วมมากและตัวคูณร่วมน้อย กล่าวคือ ถ้า $d = (a, b)$ เรียก d ว่า ตัวหารร่วมมาก หรือ ห.ร.ม. ของ a และ b ก็ต่อเมื่อ d มีคุณสมบัติต่อไปนี้ $d | a$ และ $d | b$ ถ้า $c | a$ และ $c | b$ แล้ว $c \leq d$ สำหรับการหาตัวหารร่วมมากนั้นสามารถใช้ขั้นตอนวิธีแบบยุคลิด เนื่องจากยุคลิดค้นพบว่าการหาตัวหารร่วมมากของจำนวนเต็มสองจำนวนนั้นเกิดจากการใช้ขั้นตอนวิธีการหารหลาย ๆ ครั้ง สำหรับตัวคูณร่วมน้อยแทนด้วย $m = [a, b]$ เรียก m ว่าตัวคูณร่วมน้อยของ a และ b หรือ ค.ร.น. ของ a และ b ก็ต่อเมื่อ m มีคุณสมบัติต่อไปนี้ $a | m$ และ $b | m$ และ สำหรับจำนวนเต็มบวก c ถ้า $a | c$ และ $b | c$ แล้ว $m \leq c$ นอกจากนี้ยังขยายนิยามการหารร่วมมากและคูณร่วมน้อยของจำนวนเต็มมากกว่าสองจำนวนรวมทั้งบทแทรก และทฤษฎีบทที่จะนำไปประยุกต์ใช้ในการแก้ปัญหาเกี่ยวกับจำนวนเต็มจากการหาตัวหารร่วมมาก และการคูณร่วมน้อย สำหรับเป็นพื้นฐานในการศึกษาทฤษฎีจำนวนขั้นสูงต่อไป

แบบฝึกหัดท้ายบทที่ 2

1. จงพิสูจน์ว่า สำหรับจำนวนเต็ม a, b, c, d ที่ $a \neq 0$ ถ้า $a|b, a|c$ และ $a|d$ แล้ว $a|(bx + cy + dz)$ เมื่อ x, y, z เป็นจำนวนเต็มใด ๆ
2. จงหาจำนวนเต็ม q และ r ที่ $b = aq + r$ โดยที่ $0 \leq r < |a|$ เมื่อกำหนดให้ $a = 23$ และ $b = 107$
3. จงแสดงว่ากำลังสองของ n เมื่อหารด้วย 4 จะเหลือเศษเป็น 0 หรือ 1
4. จงแสดงว่า $\frac{n(n+1)(n+2)}{3}$ เป็นจำนวนเต็มเสมอเมื่อ n เป็นจำนวนเต็มบวก
5. กำลังสามของจำนวนเต็มใด ๆ สามารถเขียนอยู่ในรูปของ $9k$ หรือ $9k+1$ หรือ $9k+8$ สำหรับจำนวนเต็ม k บางจำนวน
6. ถ้า n เป็นจำนวนคี่แล้ว $n^2 + 4n + 11$ สามารถเขียนให้อยู่ในรูปของ $8k$ สำหรับจำนวนเต็ม k บางจำนวน
7. มีจำนวนนับตั้งแต่ 1 ถึง 200 รวมทั้งสิ้นกี่จำนวนซึ่งเมื่อหารด้วย 6 แล้วเหลือเศษ 2 และเมื่อหารด้วย 14 แล้วเหลือเศษ 10
8. จงแสดงว่าถ้า a และ b เป็นจำนวนคี่แล้ว $4|(a^4 + b^4 + 2)$
9. จงใช้อุปนัยเชิงคณิตศาสตร์แสดงว่า $(a-1)|(a^2-1)^n$ สำหรับจำนวนเต็มบวก n
10. จงแสดงวิธีทำเพื่อหาค่าต่อไปนี้
 - 10.1 $(18, 81)$
 - 10.2 $(84, 24)$
 - 10.3 $(17, 289)$
 - 10.4 $(540, 450)$
 - 10.5 $(1000, 925)$
 - 10.6 $(2004, 1106)$
11. จงหาค่า x และ y ที่สอดคล้อง
 - 11.1 $98x + 46y = 2$
 - 11.2 $246x - 198y = 6$
 - 11.3 $1246x + 168y = 14$
 - 11.4 $1246x + 1068y = 178$
12. จงแสดงวิธีทำเพื่อหาค่าต่อไปนี้
 - 12.1 $[18, 63]$
 - 12.2 $[84, 24]$
 - 12.3 $[17, 289]$
 - 12.4 $[540, 450]$
 - 12.5 $[3, 11, 24]$
 - 12.6 $[3, 14, 21, 33]$

