บทที่ 2
ตัวหารร่วมมาก
(The Greatest Common Divisor)

2.1 ตัวหารร่วมมาก (The Greatest Common Divisor)

ถ้า a และ b เป็นจำนวนเต็มซึ่งไม่เป็นศูนย์พร้อมกันทั้งคู่ และ d เป็นจำนวนเต็มซึ่ง $d|a$ และ $d|b$ แล้ว เรากล่าวว่า d **เป็นตัวหารร่วม** (common divisor) ของ a และ b นอกจากนั้น จะเห็นได้ว่า เซตของตัวหารร่วมของ a และ b เป็นเซตจำกัด และมี 1 และ -1 เป็นสมาชิกเสมอ นั่นคือ เราสามารถกล่าวถึงตัวหารร่วมที่ใหญ่ที่สุดของ a และ b ได้

บทนิยาม 2.1 ให้ a และ b เป็นจำนวนเต็มซึ่งไม่เป็นศูนย์พร้อมกันทั้งคู่ จำนวนเต็ม d เรียกว่า เป็น **ตัวหารร่วมมาก** ของ a และ b ถ้า d เป็นตัวหารร่วมที่ใหญ่ที่สุดของ a และ b

และในกรณีที่ d เป็นตัวหารร่วมมากของ a และ b จะเขียนแทนด้วย

$$d = (a, b)$$

ตัวอย่าง 2.1 จงหา (24, 84)

วิธีทำ เพราะว่า

$$24 = 2\times 2\times 3\times 2$$

$$84 = 2\times 2\times 3\times 7$$

จะพบว่า ตัวหารร่วมของ 24 และ 84 คือ

$$1,\ 2,\ 3,\ 4,\ 6,\ 12,\ -1,\ -2,\ -3,\ -4,\ -6,\ -12$$

จะเห็นว่า ตัวหารร่วมที่ใหญ่ที่สุดของ 24 และ 84 คือ 12

ดังนั้น

$$(24, 84) = 12$$ #

จากบทนิยาม 2.1 จะพบว่า ตัวหารร่วมมากของ a และ b ต้องเป็นจำนวนเต็มบวกเสมอ ดังนั้น การพิจารณาหาค่า (a, b) จึงอาจพิจารณาเฉพาะตัวหารร่วมที่เป็นบวกเท่านั้น

ตัวอย่าง 2.2 จงหา $(-17, 289)$

วิธีทำ เพราะว่า

$$-17 = (-1)\times 17$$
$$289 = 17\times 17$$

จะพบว่า ตัวหารร่วมที่เป็นบวกของ -17 และ 289 คือ 17 และเป็นตัวหารร่วมที่ใหญ่ที่สุด

ดังนั้น $(-17, 289) = 17$ #

ตัวอย่าง 2.3 จงหา $(0, 44)$

วิธีทำ เพราะว่า $44|0$ และ $44|44$

ดังนั้น 44 จึงเป็นตัวหารร่วมของ 0 และ 44 และเป็นตัวหารร่วมที่ใหญ่ที่สุด

นั่นคือ $(0, 44) = 44$ #

ตัวอย่าง 2.4 จงหา $(17, 25)$

วิธีทำ เพราะว่า 17 เป็นจำนวนเฉพาะ ดังนั้น ตัวหารของ 17 ที่เป็นบวกคือ 1 และ 17 เท่านั้น แต่ $17 \nmid 25$

ดังนั้น $(17, 25) = 1$ #

จากตัวอย่าง 2.4 จะพบว่า 17 และ 25 ไม่มีตัวหารร่วมที่ใหญ่กว่า 1 ดังนั้น 17 และ 25 จะเรียกว่า เป็นจำนวนเฉพาะต่อกัน ดังจะให้บทนิยามในกรณีทั่วไปดังนี้

บทนิยาม 2.2 จำนวนเต็ม a และ b เรียกว่า **เป็นจำนวนเฉพาะต่อกัน** (relatively prime) ถ้า $(a, b) = 1$

ตัวอย่าง 2.5 เพราะว่า $(25, 42) = 1$

ดังนั้น 25 และ 42 จึงเป็นจำนวนเฉพาะต่อกัน #

ทฤษฎีบท 2.1 ให้ a และ b เป็นจำนวนเต็มซึ่งไม่เป็นศูนย์พร้อมกันทั้งคู่ และ $d = (a, b)$ แล้ว จะมีจำนวนเต็ม x และ y ที่ทำให้ $d = ax+by$

พิสูจน์ ให้

$$C = \{ax+by \mid x, y \text{ เป็นจำนวนเต็ม และ } ax+by > 0\}$$

เนื่องจาก a และ b ไม่เป็นศูนย์พร้อมกันทั้งคู่ สมมติ $a \neq 0$

ถ้า $a > 0$ จะได้ว่า $a \in C$

ถ้า $a < 0$ จะได้ว่า $-a \in C$

นั่นคือ $C \neq \phi$

ดังนั้น โดยคุณสมบัติการเป็นอันดับที่ดี C มีสมาชิกตัวที่เล็กที่สุด

ให้ d_0 เป็นสมาชิกที่เล็กที่สุดของ C และ x, y เป็นจำนวนเต็มที่ทำให้

$$d_0 = ax+by$$

จะแสดงว่า $d = d_0$

โดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q, r โดยที่ $0 \leqslant r < d_0$ และ

$$a = qd_0+r$$

ดังนั้น
$$\begin{aligned} r &= a-qd_0 \\ &= a-q(ax+by) \\ &= a(1-qx)+b(-qy) \end{aligned}$$

นั่นคือ ถ้า $r \neq 0$ จะได้ว่า $r \in C$ ซึ่งเป็นไปไม่ได้ ดังนั้น $r = 0$

เพราะฉะนั้น $d_0|a$

และโดยขั้นตอนวิธีการหารเช่นเดียวกัน จะมีจำนวนเต็ม q', r' โดยที่ $0 \leqslant r' < d_0$ และ

$$b = q'd_0+r'$$

ดังนั้น
$$\begin{aligned} r' &= b-q'd_0 \\ &= b-q'(ax+by) \\ &= a(-q'x)+b(1-q'y) \end{aligned}$$

นั่นคือ ถ้า $r' \neq 0$ จะได้ว่า $r' \in C$ ซึ่งเป็นไปไม่ได้ ดังนั้น $r' = 0$

เพราะฉะนั้น $d_0|b$

นั่นคือ d_0 เป็นตัวหารร่วมของ a และ b

เพราะว่า $d = (a, b)$

เพราะฉะนั้น $d_0 \leqslant d$

แต่เพราะว่า $d_0 = ax+by$ และ $d|a,\ d|b$

จึงได้ว่า $d|ax+by$ ซึ่งคือ $d|d_0$

ผลที่ตามมาก็คือ $d \leqslant d_0$ เพราะฉะนั้น $d = d_0$ #

บทแทรก 2.2 จำนวนเต็ม a และ b จะเป็นจำนวนเฉพาะต่อกันก็ต่อเมื่อมีจำนวนเต็ม x, y ที่ทำให้ $1 = ax+by$

พิสูจน์ ผลจากบทนิยาม 2.2 และทฤษฎีบท 2.1 #

จากบทนิยามของตัวหารร่วมมากของ a และ b เราอาจให้บทนิยามของ (a, b) ในลักษณะอื่นได้ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.3 $d = (a, b)$ ก็ต่อเมื่อ $d > 0,\ d|a,\ d|b$ และ $f|d$ ทุก ๆ จำนวนเต็ม f ที่เป็นตัวหารร่วมของ a และ b

พิสูจน์ สมมติ $d = (a, b)$

โดยบทนิยาม 2.1 $d > 0,\ d|a$ และ $d|b$

ให้ f เป็นตัวหารร่วมใด ๆ ของ a และ b

โดยทฤษฎีบทที่ 2.1 ให้ x และ y เป็นจำนวนเต็มที่ทำให้ $d = ax+by$

เพราะว่า $f|a$ และ $f|b$ จึงได้ว่า $f|ax+by$ นั่นคือ $f|d$

ในทางกลับกัน สมมติ $d > 0,\ d|a,\ d|b$ และ $f|d$ ทุก ๆ จำนวนเต็ม f ที่เป็นตัวหารร่วมของ a และ b

เพราะว่า $f|d$ ทุก ๆ จำนวนเต็ม f ที่เป็นตัวหารร่วมของ a และ b

จะได้ว่า $|f| \leqslant d$

ดังนั้น $d = (a, b)$ โดยบทนิยาม 2.1 #

ในกรณีที่ a และ b เป็นจำนวนเต็มที่มีตัวหารร่วมจำนวนมาก อาจจะสับสนในการหาตัวหารร่วมมากของ a และ b ดังนั้น จึงจะมีวิธีสำหรับการหาตัวหารร่วมมากของ a และ b ซึ่งเรียกว่า **ขั้นตอนวิธีของยุคลิด**

ทฤษฎีบท 2.4 *ขั้นตอนวิธีของยุคลิด* (The Euclidean Algorithm)

สำหรับจำนวนเต็ม $a, b > 0$

ถ้า $a = bq_1 + r_1 \qquad 0 \leqslant r_1 < b$

$b = r_1q_2 + r_2 \qquad 0 \leqslant r_2 < r_1$

$r_1 = r_2q_3 + r_3 \qquad 0 \leqslant r_3 < r_2$

$r_{k-2} = r_{k-1}q_k + r_k \qquad 0 \leqslant r_k < r_{k-1}$

$r_{k-1} = r_kq_{k+1}$

แล้ว $r_k = (a, b)$

พิสูจน์ เพราะว่า $r_{k-1} = r_kq_{k+1}$

จึงได้ว่า $r_k | r_{k-1}$

ผลที่ตามมาก็คือ $r_k | r_{k-2}$ เนื่องจาก $r_{k-2} = r_{k-1}q_k + r_k$

และเพราะว่า $r_{k-3} = r_{k-2}\, q_{k-1} + r_{k-1}$

จึงได้ว่า $r_k | r_{k-3}$

ทำกระบวนการดังกล่าวซ้ำต่อไป จะได้

$r_k | r_{k-4}, \ \ldots, \ r_k | b$ และ $r_k | a$

นั่นคือ r_k เป็นตัวหารร่วมของ a และ b

ให้ f เป็นตัวหารร่วมใด ๆ ของ a และ b จะได้ว่า $f | a$ และ $f | b$

ผลที่ตามมาก็คือ $f | r_1$

ดังนั้นจึงได้ $f | r_2, \ f | r_3, \ \ldots, \ f | r_k$

โดยทฤษฎีบท 2.3 $r_k = (a, b)$ #

ตัวอย่าง 2.6 จงหาค่า (252, 198) และถ้า $d = (252, 198)$ แล้ว จงหาจำนวนเต็ม x และ y ที่ทำให้ $d = 252x + 198y$

วิธีทำ โดยใช้ขั้นตอนวิธีของยุคลิด

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18$$

ดังนั้น $18 = (252, 198)$

และจาก

$$54 = 1 \cdot 36 + 18$$

จะได้ $18 = 54 - 1 \cdot 36$

$$= 54 - 1(198 - 3\cdot 54)$$
$$= 4\cdot 54 - 1\cdot 198$$
$$= 4(252 - 1\cdot 198) - 1\cdot 198$$
$$18 = 4\cdot 252 - 5\cdot 198$$

นั่นคือ $x = 4$ และ $y = -5$ #

ตัวอย่าง 2.7 จงหาตัวหารร่วมมากของ 288 และ 51 และถ้า $d = (288, 51)$ แล้ว จงหาจำนวนเต็ม x และ y ที่ทำให้ $d = 288x + 51y$

วิธีทำ โดยใช้ขั้นตอนวิธีการของยุคลิด

$$288 = 5\cdot 51 + 33$$
$$51 = 1\cdot 33 + 18$$
$$33 = 1\cdot 18 + 15$$
$$18 = 1\cdot 15 + 3$$
$$15 = 5.3$$

ดังนั้น $3 = (288, 51)$

จาก $18 = 1\cdot 15 + 3$

จะได้ $3 = 18 - 1\cdot 15$

$$= 18 - 1(33 - 1\cdot 18)$$
$$= 2\cdot 18 - 1\cdot 33$$
$$= 2(51 - 1\cdot 33) - 1\cdot 33$$
$$= 2\cdot 51 - 3\cdot 33$$
$$= 2\cdot 51 - 3(288 - 5\cdot 51)$$
$$3 = 17\cdot 51 - 3\cdot 288$$

นั่นคือ $x = -3$ และ $y = 17$ #

หมายเหตุ ถ้า $d = (a, b)$ แล้ว ค่า x และ y ที่ทำให้ $d = ax + by$ ไม่ได้มีชุดเดียว เช่น จะพบว่า

$$3 = -3\cdot 288 + 17\cdot 51$$

และ $3 = 48\cdot 288 + (-271)51$

เป็นต้น #

ทฤษฎีบท 2.5 ให้ a, b, c, d เป็นจำนวนเต็ม และ $d = (a, b)$ แล้ว

ก. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ข. $(a+cb, b) = (a, b)$

พิสูจน์ ก. จะแสดงว่า $\frac{a}{d}$ และ $\frac{b}{d}$ ไม่มีตัวหารร่วมที่เป็นจำนวนเต็มบวกมากกว่า 1

สมมติให้ e เป็นจำนวนเต็มบวกโดยที่ $e \mid \frac{a}{d}$ และ $e \mid \frac{b}{d}$

ดังนั้น จะมีจำนวนเต็ม k และ ℓ ที่ทำให้ $\frac{a}{d} = ke$

และ $\frac{b}{d} = \ell e$

ดังนั้น $a = ked$ และ $b = \ell ed$

ผลที่ตามมาก็คือ $ed \mid a$ และ $ed \mid b$

เพราะว่า $d = (a, b)$ ดังนั้น $ed \leqslant d$

แต่ $e \geqslant 1$ และ $d > 0$

ถ้า $e > 1$ จะได้ว่า $de > d$ ซึ่งเป็นไปไม่ได้

ดังนั้น $e = 1$

ผลที่ตามมาก็คือ $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ข. จะแสดงว่า $(a+cb, b) = (a, b)$ โดยแสดงว่า ตัวหารร่วมของ a และ b เป็นตัวหารร่วมของ a+cb และ b และตัวหารร่วมของ a+cb และ b เป็นตัวหารร่วมของ a และ b

ให้ e เป็นตัวหารร่วมของ a และ b

เพราะฉะนั้น จะได้ว่า $e \mid (a+cb)$

ผลที่ตามมาก็คือ e เป็นตัวหารร่วมของ a+cb และ b

ให้ f เป็นตัวหารร่วมของ a+cb และ b

ดังนั้น $f \mid (a+cb)-cb$ นั่นคือ $f \mid a$

เพราะฉะนั้น f เป็นตัวหารร่วมของ a และ b

จึงสรุปได้ว่า $(a+cb, b) = (a, b)$ #

ทฤษฎีบท 2.6 ให้ a, b, c เป็นจำนวนเต็ม โดยที่ $(a, b) = 1$ และ $a|bc$ แล้ว $a|c$

พิสูจน์ เพราะว่า $(a, b) = 1$ ดังนั้น จึงมีจำนวนเต็ม x และ y ที่ทำให้

$$1 = ax + by$$

เพราะฉะนั้น

$$c = acx + bcy$$

เพราะว่า $a|acx$ และ $a|bcy$ ผลที่ตามมาก็คือ $a|c$ #

บทแทรก 2.7 ให้ p เป็นจำนวนเฉพาะ และ b, c เป็นจำนวนเต็ม โดยที่ $p|bc$ แล้ว จะได้ว่า $p|b$ หรือ $p|c$

พิสูจน์ สมมติ $p \nmid b$ เนื่องจากตัวหารที่เป็นบวกของ p คือ 1 และ p เท่านั้น

จึงได้ว่า $(p, b) = 1$

ดังนั้น โดยทฤษฎีบท 2.6 $p|c$ #

บทแทรก 2.8 ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็ม และ p เป็นจำนวนเฉพาะ โดยที่ $p|a_1a_2\ldots a_n$ แล้ว $p|a_k$ สำหรับบางจำนวนเต็ม k ซึ่ง $1 \leqslant k \leqslant n$

พิสูจน์ พิสูจน์โดยทฤษฎีบท 2.6 บทแทรก 2.7 และทฤษฎีบทอุปนัยทางคณิตศาสตร์ #

บทแทรก 2.9 ถ้า $p, q_1, q_2, \ldots, q_n$ เป็นจำนวนเฉพาะ โดยที่ $p|q_1q_2\ldots q_n$ แล้ว $p = q_k$ สำหรับบาง k ซึ่ง $1 \leqslant k \leqslant n$

พิสูจน์ เพราะว่า $p|q_1q_2\ldots q_n$ และ p เป็นจำนวนเฉพาะ โดยบทแทรก 2.8 มีจำนวนเต็ม k ซึ่ง $1 \leqslant k \leqslant n$ และ $p|q_k$

เนื่องจาก q_k เป็นจำนวนเฉพาะ และ $p \neq 1$ จึงได้ว่า $p = q_k$ #

จากหัวข้อ 1.5 เราแสดงให้เห็นแล้วว่า จำนวนเต็มบวกทุกจำนวนสามารถเขียนได้เป็นผลคูณของจำนวนเฉพาะ และบทแทรก 2.9 นี้ จะช่วยแสดงให้เห็นว่า ถ้าไม่คำนึงถึงลำดับที่จำนวนเต็มบวกทุกจำนวนเขียนเป็นผลคูณของจำนวนเฉพาะได้แบบเดียวเท่านั้น

ทฤษฎีบท 2.10 *ทฤษฎีบทมูลฐานของเลขคณิต* (Fundamental Theorem of Arithmetic)

ถ้า n เป็นจำนวนเต็มบวก โดยที่ $n > 1$ แล้ว n สามารถเขียนเป็นผลคูณของจำนวนเฉพาะได้ และถ้าไม่คำนึงถึงลำดับที่ การเขียนผลคูณของจำนวนเฉพาะนี้เขียนได้แบบเดียวเท่านั้น

พิสูจน์ โดยทฤษฎีบท 1.16 n เขียนเป็นผลคูณของจำนวนเฉพาะได้

สมมติ n เขียนเป็นผลคูณของจำนวนเฉพาะได้สองแบบ คือ

$$n = p_1p_2\cdots p_r = q_1q_2\cdots q_s$$

โดยที่ $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ เป็นจำนวนเฉพาะ

และเพื่อความสะดวก สมมติ $r \leqslant s$ และ $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$

$$q_1 \leqslant q_2 \leqslant \ldots \leqslant q_s$$

เพราะว่า $p_1|p_1p_2\ldots p_r$ จึงได้ว่า $p_1|q_1q_2\ldots q_s$

โดยบทแทรก 2.9 มีจำนวนเต็ม k ซึ่ง $1 \leqslant k \leqslant s$ และ $p_1 = q_k$

เพราะว่า $q_k \geqslant q_1$ ดังนั้น $p_1 \geqslant q_1$

ในทำนองเดียวกัน เพราะว่า $q_1|p_1p_2\ldots p_r$

จึงได้ว่า $q_1 = p_\ell$ สำหรับบาง ℓ ซึ่ง $1 \leqslant \ell \leqslant r$

และเพราะว่า $p_\ell \geqslant p_1$ จึงได้ว่า $q_1 \geqslant p_1$ ผลที่ตามมาก็คือ $p_1 = q_1$

เพราะฉะนั้น จาก $p_1p_2\cdots p_r = q_1q_2\cdots q_s$

จึงได้ว่า

$$p_2p_3\cdots p_r = q_2q_3\cdots q_s$$

ทำกระบวนการแบบเดิมอีกครั้ง จะได้ว่า $p_2 = q_2$

นั่นคือ

$$p_3p_4\cdots p_r = q_3q_4\cdots q_s$$

และทำกระบวนการแบบนี้ต่อไปเรื่อย ๆ ถ้า $r < s$ จะได้

$$1 = q_{r+1}\cdots q_s$$

ซึ่งเป็นไปไม่ได้ เนื่องจาก $q_{r+1}, q_{r+2}, \ldots, q_s$ มากกว่า 1

ดังนั้น $r = s$ และ $p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_r = q_r$ #

บทแทรก 2.11 ทุกจำนวนเต็มบวก $n > 1$ สามารถเขียนได้ในรูปแบบของ

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$$

โดยที่ $p_1 < p_2 < \ldots < p_r$ เป็นจำนวนเฉพาะ และ $\alpha_1, \alpha_2, \ldots, \alpha_r$ เป็นจำนวนเต็มบวก และเขียนได้แบบเดียวเท่านั้น

พิสูจน์ ผลจากทฤษฎีบท 2.10 #

หมายเหตุ การเขียน $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$

โดยที่ $p_1, p_2, \ldots, p_r$ เป็นจำนวนเฉพาะ และ $p_1 < p_2 < \ldots < p_r$
เรียกว่า เขียนใน **รูปแบบบัญญัติ** (canonical form)

ตัวอย่าง 2.8 **จงเขียน** 360, 4725 **และ** 17460 **ให้เป็นรูปแบบบัญญัติ**

วิธีทำ

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$4725 = 3^3 \cdot 5^2 \cdot 7$$

$$17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

#

โดยทั่วไปแล้ว ถ้า $a|c$ และ $b|c$ แล้ว ข้อความ $ab|c$ อาจเป็นเท็จ เช่น $6|24$ และ $8|24$ แต่ $6 \cdot 8 \nmid 24$ แต่ถ้าเราเพิ่มเติมคุณสมบัติว่า a และ b เป็นจำนวนเฉพาะต่อกันแล้ว ข้อความ $ab|c$ เป็นจริง ดังพิสูจน์ให้เห็นได้ต่อไปนี้

ทฤษฎีบท 2.12 กำหนด a, b, c เป็นจำนวนเต็ม โดยที่ $a|c$, $b|c$ และ $(a, b) = 1$ แล้ว $ab|c$

พิสูจน์ เพราะว่า $a|c$ และ $b|c$ จึงมีจำนวนเต็ม r ที่ทำให้

$$c = ra$$

ผลที่ตามมาก็คือ $b|ra$ และเพราะว่า $(a, b) = 1$ โดยทฤษฎีบท 2.6 $b|r$
ดังนั้น จะมีจำนวนเต็ม t ที่ทำให้

$$r = bt$$

ดังนั้น

$$c = ra = bta = abt$$

นั่นคือ $ab|c$ #

บทแทรก 2.19 ถ้า m,, m_2, ... m,, 6ปีนจำนวนเต็ม โดยที่ (m_i, m_j) = I Qfl $i \neq j$ และ $m_i|a$ Qfl i = I, 2, ... n แล้ว $m|a$ 4เมอ $m = m_1 m_2 \ldots m_n$

พิสูจน์ ผลจากทฤษฎีบท 2.12 และทฤษฎีบทอุปนัยทางคณิตศาสตร์ #

ต่อไปจะได้ขยายแนวความคิดของตัวหารร่วมมากของจำนวนเต็มสองจำนวนไปเป็นตัวหารร่วมมากของจำนวนเต็มมากกว่าสองจำนวนดังนี้

บทนิยาม 2.3 ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกันหมด ตัวหารร่วมมากของ $a_1, a_2, \ldots, a_n$ คือ จำนวนเต็มที่ใหญ่ที่สุดที่หาร $a_1, a_2, \ldots, a_n$ ลงตัว

และถ้า d เป็นตัวหารร่วมมากของ $a_1, a_2, \ldots, a_n$ แล้ว จะเขียนแทนด้วย

$$d = (a_1, a_2, \ldots, a_n)$$

ตัวอย่าง 2.9 จงหา $(12, 18, 30)$

วิธีทำ เพราะว่า

$$12 = 2\cdot2\cdot3$$
$$18 = 2\cdot3\cdot3$$
$$30 = 2\cdot3\cdot5$$

จะได้ว่า ตัวหารร่วมที่เป็นบวกของ 12, 18, 30 คือ

$$1,\ 2,\ 3,\ 6$$

ซึ่งเห็นได้ว่า 6 เป็นตัวหารร่วมที่ใหญ่ที่สุด

ดังนั้น $6 = (12, 18, 30)$ #

ตัวอย่าง 2.10 จงหา $(10, 15, 25)$

วิธีทำ เพราะว่า

$$10 = 2.5$$
$$15 = 3.5$$
$$25 = 5\cdot5$$

จะเห็นว่า ตัวหารร่วมของ 10, 15, 25 ที่เป็นบวก คือ 1, 5

ดังนั้น $5 = (10, 15, 25)$ #

ทฤษฎีบทประกอบ 2.14 ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกันหมดแล้ว

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n))$$

พิสูจน์ ให้ f เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_{n-1}, a_n$

จะได้ว่า f เป็นตัวหารร่วมของ a_{n-1} และ a_n

นั่นคือ f เป็นตัวหารของ (a_{n-1}, a_n)

ผลที่ตามมาก็คือ ถ้า f เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_n$ แล้ว f เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)$

ให้ e เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)$

จะได้ว่า $e|(a_{n-1}, a_n)$ ผลที่ตามมาก็คือ $e|a_{n-1}, e|a_n$

นั่นคือ ถ้า e เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)$ แล้ว e เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n$

เพราะฉะนั้น

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n)) \qquad \#$$

ตัวอย่าง 2.11 จงหา (105, **140, 350)**

44

วิธีทำ

$$\begin{aligned}(105, 140, 350) &= (105, (140, 350)) \\ &= (105, 70) \\ &= 35\end{aligned} \qquad \#$$

บทนิยาม 2.4 เรากล่าวว่า จำนวนเต็ม $a_1, a_2, \ldots, a_n$ เป็น **จำนวนเฉพาะต่อกันทั้งกลุ่ม** (mutually relatively prime) ถ้า $(a_1, a_2, \ldots, a_n) = 1$

และเรากล่าวว่า จำนวนเต็ม $a_1, a_2, \ldots, a_n$ เป็น **จำนวนเฉพาะต่อกันทีละคู่** (pairwise relatively prime) ถ้า $(a_i, a_j) = 1$ ทุก $i \neq j$

ตัวอย่าง 2.12 พิจารณาจำนวนเต็ม 15, 21 และ 35

เพราะว่า

$$\begin{aligned}(15, 21, 35) &= (15, (21, 35)) \\ &= (15, 7) \\ &= 1\end{aligned}$$

ดังนั้น 15, 21, 35 เป็นจำนวนเฉพาะต่อกันทั้งกลุ่ม

แต่ 15, 21, 35 ไม่ใช่จำนวนเฉพาะต่อกันทีละคู่ เนื่องจาก $(21, 35) = 7 \neq 1$

#

ตัวอย่าง 2.13 พิจารณาจำนวนเต็ม 2, 7, 15

เพราะว่า

$$(2, 7) = 1$$

$$(7, 15) = 1$$

และ

$$(15, 2) = 1$$

ดังนั้น 2, 7, 15 เป็นจำนวนเฉพาะต่อกันทีละคู่ #

แบบฝึกหัด 2.1

1. จงหาตัวหารร่วมมากของจำนวนเต็มต่อไปนี้

1.1 15, 35	1.2 0, 111
1.3 -12, 18	1.4 99, 100
1.5 11, 121	1.6 100, 102

2. ให้ m เป็นจำนวนเต็มบวกใด ๆ จงแสดงว่า $(ma, mb) = m(a, b)$
3. จงหาค่า $(357, 629)$ และจำนวนเต็ม x, y ที่ทำให้

$$(357, 629) = 357x + 629y$$

4. จงหาค่า $(-357, 629)$ และจำนวนเต็ม x, y ที่ทำให้

$$(-357, 629) = -357x + 629y$$

5. จงหาค่า $(7700, 2233)$ และจำนวนเต็ม x, y ที่ทำให้

$$(7700, 2233) = 7700x + 2233y$$

6. จงหาค่า $(1819, 3587)$ และจำนวนเต็ม x, y ที่ทำให้

$$(1819, 3587) = 1819x + 3587y$$

7. จงแสดงว่า ถ้า a, b เป็นจำนวนเต็มคู่และไม่เป็นศูนย์พร้อมกันทั้งคู่ แล้ว

$$(a, b) = 2\left(\frac{a}{2}, \frac{b}{2}\right)$$

8. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่ และ b เป็นจำนวนเต็มคี่แล้ว

$$(a, b) = \left(\frac{a}{2}, b\right)$$

9. จงพิสูจน์ว่า $b|a$ ก็ต่อเมื่อ $(a, b) = |b|$
10. จงพิสูจน์ว่า ถ้า $(a, c) = 1$ และ $b|c$ แล้ว $(a, b) = 1$
11. จงพิสูจน์ว่า ถ้า $(a, b) = 1$ และ $c|(a+b)$ แล้ว $(c, a) = (c, b) = 1$
12. จงแสดงว่า ถ้า a, b, c เป็นจำนวนเต็ม โดยที่ $(a, b) = (a, c) = 1$ แล้ว $(a, bc) = 1$
13. ถ้า $a_1, a_2, \ldots, a_n$ และ b เป็นจำนวนเต็ม โดยที่ $(a_1, b) = (a_2, b) = \ldots = (a_n, b) = 1$ แล้ว $(a_1a_2\ldots a_n, b) = 1$
14. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็ม โดยที่ $c|ab$ แล้ว $c|(a, c)(b, c)$
15. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มบวก โดยที่ $(a, b) = 1$ แล้ว $(a^n, b^n) = 1$ ทุกจำนวนเต็มบวก n

16. **จงใช้ข้อ** 15 **พิสูจน์ว่า** ถ้า a และ b เป็นจำนวนเต็มบวก โดยที่ $a^n|b^n$ เมื่อ $n > 0$ แล้ว $a|b$

17. **ถ้า** a, b, c เป็นจำนวนเต็มที่ไม่เป็นศูนย์ และเป็นจำนวนเฉพาะต่อกันเป็นกลุ่มแล้ว จง **แสดงว่า** $(ab, c) = (a, b)(a, c)$

18. **จงหาค่าตัวหารร่วมมากของ**

18.1 8, 10, 12	18.2 5, 25, 75
18.3 99, 9999; 0	18.4 6, 15, 21
18.5 -7, 28, -35	18.6 0, 0, 1001

2.2 **ตัวคูณร่วมน้อย** (The Least Common Multiple)

ถ้า a, b และ m เป็นจำนวนเต็ม โดยที่ $a|m$ และ $b|m$ แล้ว เรากล่าวว่า m เป็น **ตัวคูณร่วมของ a และ b** (common multiple of a and b) และเห็นได้ชัดว่า สำหรับจำนวนเต็ม a และ b ใด ๆ ที่ไม่ใช่ศูนย์ ab และ $-ab$ เป็นตัวคูณร่วมของ a และ b เสมอ กล่าวคือ a และ b มีตัวคูณร่วมที่เป็นบวกเสมอ ดังนั้น โดยคุณสมบัติของการเป็นอันดับที่ดี สามารถกล่าวถึงตัวคูณร่วมบวกที่น้อยที่สุดได้

บทนิยาม 2.5 ถ้า m เป็นตัวคูณร่วมที่เป็นบวกที่น้อยที่สุดของ a และ b แล้ว เรียก m ว่าเป็น **ตัวคูณร่วมน้อยของ a และ b** (the least common multiple of a and b) และเขียนแทนด้วย

$$m = [a, b]$$

ตัวอย่าง 2.14 จงหา $[15, 25]$

วิธีทำ เพราะว่า

$$15 = 3\cdot 5$$

$$25 = 5\cdot 5$$

ตัวคูณร่วมของ 15 และ 25 ที่เป็นจำนวนเต็มบวกที่น้อยที่สุด คือ 75
ดังนั้น

$$75 = [15, 25]$$

#

ตัวอย่าง 2.15 จงหา $[7, 11]$

วิธีทำ เพราะว่า

$$7 = 1\cdot 7$$

$$11 = 1\cdot 11$$

ตัวคูณร่วมของ 7 และ 11 ที่เป็นจำนวนเต็มบวกที่น้อยที่สุด คือ 77
ดังนั้น

$$77 = [7, 11]$$

#

ทฤษฎีบทต่อไปนี้จะช่วยให้การคำนวณค่า $[a, b]$ ง่ายขึ้น

ทฤษฎีบท 2.15 ให้ m, a, b เป็นจำนวนเต็มใด ๆ โดยที่ a, b ไม่ใช่ศูนย์ แล้ว $m = [a, b]$ ก็ต่อเมื่อ $m > 0$ $a|m$, $b|m$ และ $m|n$ สำหรับทุกจำนวนเต็ม n ที่เป็นตัวคูณร่วมของ a และ b

พิสูจน์ สมมติ $m = [a, b]$

โดยบทนิยาม 2.5 $a|m$, $b|m$

ให้ n เป็นตัวคูณร่วมใด ๆ ของ a และ b และสมมติให้ $n > 0$

โดยคุณสมบัติของ m จะได้ว่า $m \leq n$

และโดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q และ r โดยที่ $0 \leq r < m$ และ

$$n = mq + r$$

ซึ่งได้ว่า

$$r = n - mq$$

เพราะว่า $a|n$ และ $a|m$ จึงได้ว่า $a|r$

เพราะว่า $b|n$ และ $b|m$ จึงได้ว่า $b|r$

ผลที่ตามมาก็คือ r เป็นตัวคูณร่วมของ a และ b แต่ $r < m$ ซึ่งเป็นตัวคูณร่วมมากที่น้อยที่สุด

ดังนั้น $r = 0$ นั่นคือ $m|n$

ในทางกลับกัน สมมติ $m > 0$ $a|m$, $b|m$ และ $m|n$ ทุกจำนวนเต็ม n ที่เป็นตัวคูณร่วมของ a และ b

เพราะว่า $m|n$ และ $m > 0$

จึงได้ว่า $m \leq |n|$ ทุก n ที่เป็นตัวคูณร่วมของ a และ b

นั่นคือ $m = [a, b]$ #

ทฤษฎีบท 2.16 ถ้า a, b เป็นจำนวนเต็ม โดยที่ $ab \neq 0$ แล้ว

$$[a, b] = \frac{|ab|}{(a, b)}$$

พิสูจน์ ให้ $d = (a, b)$

เพราะว่า $d|a$ และ $d|b$ ดังนั้น จะมีจำนวนเต็ม A, B โดยที่

$$a = Ad \quad \text{และ} \quad b = Bd$$

ให้ $$m = \frac{|ab|}{d}$$

ดังนั้น $m = |Ab| = |Ba|$ นั่นคือ $m > 0$

ผลที่ตามมาก็คือ $a|m$ และ $b|m$

ให้ n เป็นจำนวนเต็มบวกใด ๆ โดยที่ $a|n$ และ $b|n$

ดังนั้น จะมีจำนวนเต็ม r, s ที่ทำให้ $n = ar = bs$

ดังนั้น $n = Adr = Bds$

เพราะว่า $d \neq 0$ จึงได้ว่า $Ar = Bs$

ผลที่ตามมาก็คือ $A|Bs$ และโดยทฤษฎีบท 2.5 $(A, B) = 1$

ดังนั้น โดยทฤษฎีบท 2.6 จึงได้ว่า $A|s$

นั่นคือ มีจำนวนเต็ม t ที่ทำให้

$$s = At$$

ผลที่ตามมาก็คือ

$$n = bs = bAt = \begin{cases} mt & \text{ถ้า } bA > 0 \\ -mt & \text{ถ้า } bA < 0 \end{cases}$$

นั่นคือ $m|n$

ดังนั้น โดยทฤษฎีบท 2.16

$$m = [a, b]$$ #

ตัวอย่าง 2.16 จงหาค่า $[288, 51]$

วิธีทำ เพราะว่า $(288, 51) = 3$

ดังนั้น $[288, 51] = \dfrac{288 \cdot 51}{3} = 4896$ #

ทฤษฎีบท 2.17 ให้ a และ b เป็นจำนวนเต็ม และเขียน a และ b ได้เป็น

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

โดยที่ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะ a_i, b_i เป็นจำนวนเต็มที่ไม่เป็นลบทุก $i = 1, 2, \ldots, n$

แล้ว $[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}$

โดยที่ $\max\{a_i, b_i\}$ คือ ค่าที่มากที่สุดระหว่าง a_i และ b_i

พิสูจน์ ให้ $m = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \ldots p_n^{\max\{a_n, b_n\}}$

เห็นได้ชัดว่า $a|m$ และ $b|m$ และ $m > 0$

ให้ n เป็นตัวคูณร่วมใด ๆ ของ a และ b กล่าวคือ $a|n$ และ $b|n$

ดังนั้น จะมีจำนวนเต็ม r, s ที่ทำให้

$$n = ra = rp_1^{a_1}p_2^{a_2}\ldots p_n^{a_n} = sb = sp_1^{b_1}p_2^{b_2}\ldots p_n^{b_n}$$

จากบทแทรก 2.11 n เขียนเป็นรูปแบบบัญญัติได้เพียงแบบเดียวเท่านั้น

นั่นคือ จะต้องมีจำนวนเต็ม t ที่ทำให้

$$n = tp_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \ldots p_n^{\max\{a_n, b_n\}}$$

ผลที่ตามมาก็คือ $m|n$

ดังนั้น โดยทฤษฎีบท 2.15

$$m = [a, b]$$ #

ตัวอย่าง 2.17 ให้ $a = 2^2\cdot 3^3\cdot 5^5\cdot 7^7$ และ $b = 2^7\cdot 3^5\cdot 5^3\cdot 7^2$ จงหา $[a, b]$

วิธีทำ

$$[a, b] = 2^{\max\{2, 7\}}\, 3^{\max\{3, 5\}}\, 5^{\max\{5, 3\}}\, 7^{\max\{7, 2\}} = 2^7\cdot 3^5\cdot 5^5\cdot 7^7$$ #

ต่อไปจะได้ขยายแนวความคิดของตัวคูณร่วมน้อยของจำนวนเต็มสองจำนวนไปเป็นตัวคูณร่วมน้อยของจำนวนเต็มมากกว่าสองจำนวน ดังนี้

บทนิยาม 2.6 ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่เป็นศูนย์ และ m เป็นจำนวนเต็ม โดยที่ $a_i|m$ ทุก $i = 1, 2, \ldots, n$ แล้ว m เป็นตัวคูณร่วมน้อยของ $a_1, a_2, \ldots, a_n$ เขียนแทนด้วย

$$m = [a_1, a_2, \ldots, a_n]$$

ถ้า $m|k$ ทุกจำนวนเต็ม k ที่มีคุณสมบัติว่า $a_i|k$ ทุก $i = 1, 2, \ldots, n$

ตัวอย่าง 2.18 จงหา $[5, 10, 15]$

วิธีทำ เพราะว่า

$$5 = 1\cdot 5$$
$$10 = 2\cdot 5$$
$$15 = 3\cdot 5$$

จะเห็นว่า ตัวคูณร่วมน้อยของ 5, 10, 15 คือ 30 #

ทฤษฎีบท 2.18 ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่เป็นศูนย์ แล้ว

$$[a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_{n-2}, [a_{n-1}, a_n]]$$

พิสูจน์ ให้พิสูจน์เป็นแบบฝึกหัด

ตัวอย่าง 2.19 จงหาค่า $[108, 84, 78]$

วิธีทำ เพราะว่า

$$(84, 78) = 6$$

ดังนั้น

$$[84, 78] = \frac{84 \cdot 78}{6} = 1092$$

และ

$$(108, 1092) = 12$$

ดังนั้น $$[108, 1092] = \frac{108.1092}{12} = 9828$$

เพราะฉะนั้น

$$[108, 84, 78] = [108, 1092]$$
$$= 9828$$

#

แบบฝึกหัด 2.2

1. **จงหาค่าของ**

   1.1 $[357, 629]$ 1.2 $[-357, 629]$

   1.3 $[299, 377]$

2. **จงหาตัวคูณร่วมน้อยของ**

   2.1 $2\cdot3\cdot5\cdot7\cdot11\cdot13$ และ $17\cdot19\cdot23\cdot29$

   2.2 $2^3\cdot5^7\cdot41^{13}$ และ $2\cdot3\cdot5\cdot7\cdot11\cdot13$

   2.3 $47^{11}\,79^{111}\,101^{1001}$ และ $41^{11}\,83^{111}\,101^{1000}$

3. **ถ้า** c **เป็นจำนวนเต็ม โดยที่** $c > 0$ **จงแสดงว่า** $[ca, cb] = c[a, b]$

4. **จงพิสูจน์ว่า** $a|b$ **ก็ต่อเมื่อ** $[a, b] = |b|$

5. **จงหาจำนวนเต็ม** a, b **โดยที่** $(a, b) = 18$ **และ** $[a, b] = 540$

6. **จงหาค่า** $[6, 10, 15]$

7. **จงหาค่า** $[7, 11, 13]$

2.3 จำนวนสามจำนวนของปีทาโกรัส (Pythagorean Triples)

เราเคยทราบแล้วว่า ถ้าสามเหลี่ยมรูปหนึ่งมีความยาวด้านสามด้านเป็น 3 หน่วย 4 หน่วย และ 5 หน่วยแล้ว สามเหลี่ยมรูปนี้ต้องเป็นสามเหลี่ยมมุมฉาก และนอกจากนั้นจะได้ว่า

$$3^2 + 4^2 = 5^2$$

กล่าวคือ ถ้า x, y และ z เป็นจำนวนที่ทำให้

$$x^2 + y^2 = z^2$$

แล้วสามเหลี่ยมใด ๆ ที่มีความยาวด้านเป็น x หน่วย y หน่วย และ z หน่วย ต้องเป็นสามเหลี่ยมมุมฉากเสมอ

ดังนั้น จำนวนเต็มบวก x, y และ z ที่สอดคล้องเงื่อนไขว่า $x^2 + y^2 = z^2$ นี้ จะเรียกว่า **จำนวนสามจำนวนของปีทาโกรัส** (Pythagorean triples) นอกจากนั้น ถ้า x, y, z เป็นจำนวนสามจำนวนของปีทาโกรัสแล้ว kx, ky, kz เป็นจำนวนสามจำนวนของปีทาโกรัสเสมอทุกจำนวนเต็มบวก k

ดังนั้น การหาจำนวนสามจำนวนของปีทาโกรัสจึงเพียงพอที่จะหาจำนวนเต็มบวก x, y, z โดยที่ $(x, y, z) = 1$ และ $x^2 + y^2 = z^2$ ซึ่งเราเรียกว่า **จำนวนสามจำนวนปฐมฐานของปีทาโกรัส** (primitive Pythagorean triples) ซึ่งสามารถทำได้ดังนี้

ทฤษฎีบท 2.19 จำนวนเต็มบวก x, y, z โดยที่ x เป็นจำนวนเต็มคู่ จะเป็นจำนวนสามจำนวนปฐมฐานของปีทาโกรัสก็ต่อเมื่อมีจำนวนเต็ม s, t โดยที่ $s < t$, $(s, t) = 1$ s, t ไม่เป็นจำนวนคู่หรือจำนวนคี่พร้อมกัน และ $x = 2st$, $y = t^2 - s^2$, $z = t^2 + s^2$

พิสูจน์ กำหนดให้ x, y, z เป็นจำนวนสามจำนวนปฐมฐานของปีทาโกรัส

ดังนั้น $(x, y, z) = 1$

จะพิสูจน์ว่า $(x, y) = (y, z) = (x, t) = 1$

สมมติ $(x, z) = d > 1$

ดังนั้น จะมีจำนวนเฉพาะ p โดยที่ $p|d$ ผลที่ตามมาก็คือ $p|x$ และ $p|z$

และจึงได้ $p|x^2$ และ $p|z^2$

เพราะว่า $x^2 + y^2 = z^2$

จึงได้ว่า $p|y^2$ นั่นคือ $p|y$

ซึ่งขัดแย้งกับการที่ $(x, y, z) = 1$

ดังนั้น $(x, z) = 1$

ในทำนองเดียวกันก็สามารถพิสูจน์ได้ว่า $(x, y) = (y, z) = 1$ และเพราะว่า $(x, y) = 1$ ผลที่ตามมาก็คือ x และ y จะเป็นจำนวนเต็มคู่พร้อมกันทั้งสองจำนวนไม่ได้

ดังนั้น y จึงต้องเป็นจำนวนเต็มคี่ และเพราะว่า $x^2 + y^2 = z^2$ จึงทำให้ $z^2 = 4q + 1$ สำหรับจำนวนเต็ม q บางตัว จากตัวอย่าง 1.18 จะได้ว่า z เป็นจำนวนเต็มคี่

นั่นคือ $z - y$ และ $z + y$ เป็นจำนวนคู่ทั้งสองจำนวน

จาก $x^2 = z^2 - y^2 = (z - y)(z + y)$

ให้ $z - y = 2u$ และ $z + y = 2v$

นั่นคือ $z = v + u$ และ $y = v - u$

ถ้า u และ v เป็นจำนวนคู่ทั้งสองจำนวน จะได้ z และ y เป็นจำนวนคู่ ซึ่งเป็นไปไม่ได้

ถ้า u และ v เป็นจำนวนคี่ทั้งสองจำนวน จะได้ z และ y เป็นจำนวนคู่ ซึ่งเป็นไปไม่ได้

ดังนั้น u และ v ต้องเป็นจำนวนคู่หนึ่งจำนวน และจำนวนคี่หนึ่งจำนวน

และถ้า $d = (u, v)$ โดยที่ $d > 1$ จะพบว่ามีจำนวนเฉพาะ p ซึ่ง $p|x$, $p|y$ และ $p|z$ ซึ่งเป็นไปไม่ได้

นั่นคือ $(u, v) = 1$

เนื่องจาก x เป็นจำนวนคู่ จะได้ $\frac{x}{2}$ เป็นจำนวนเต็ม และ

$$\left(\frac{x}{2}\right)^2 = \frac{z-y}{2} \cdot \frac{z+y}{2} = u \cdot v$$

ให้ $\frac{x}{2} = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ เป็นรูปแบบบัญญัติของ $\frac{x}{2}$

จะได้ว่า

$$u \cdot v = p_1^{2a_1} p_2^{2a_2} \ldots p_r^{2a_r}$$

นั่นคือ $u | p_1^{2a_1} p_2^{2a_2} \ldots p_r^{2a_r}$ และ $v | p_1^{2a_1} p_2^{2a_2} \ldots p_r^{2a_r}$

ผลที่ตามมาก็คือ

$$u = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r} \quad \text{และ} \quad v = p_1^{c_1} p_2^{c_2} \ldots p_r^{c_r}$$

โดยที่ $b_i \geqslant 0$, $c_i \geqslant 0$ และ $b_i + c_i = 2a_i$ ทุก $i = 1, 2, \ldots, r$

ถ้ามี i บางตัวที่ $b_i \neq 0$ และ $c_i \neq 0$ แล้ว จะได้ว่า $p_i | u$ และ $p_i | v$ ซึ่งเป็นไปไม่ได้ เนื่องจาก $(u, v) = 1$

นั่นคือ สำหรับทุก i ; b_i, c_i ต้องมีจำนวนใดจำนวนหนึ่งเป็นศูนย์

และเพราะว่า $b_i + c_i = 2a_i$ ผลที่ตามมาก็คือ b_i และ c_i ต้องเป็นจำนวนคู่ทุก i

ให้ $b_i = 2u_i$ และ $c_i = 2v_i$ โดยที่ u_i, v_i เป็นจำนวนเต็ม

และ $s = p_1^{u_1}p_2^{u_2}\cdots p_r^{u_r}$ $t = p_1^{v_1}p_2^{v_2}\cdots p_r^{v_r}$

จะได้ $u = s^2$ และ $v = t^2$

นอกจากนั้น $(s, t) = 1$ และ s, t ไม่เป็นจำนวนคู่พร้อมกันและไม่เป็นจำนวนคี่พร้อมกัน เนื่องจาก u และ v จะไม่เป็นจำนวนเต็มคู่พร้อมกัน และไม่เป็นจำนวนเต็มคี่พร้อมกัน

เพราะฉะนั้น จะได้

$$x = 2\sqrt{u \cdot v} = 2st$$

$$y = v - u = t^2 - s^2$$

$$z = v + u = t^2 + s^2$$

นอกจากนั้น เพราะว่า $y > 0$ จึงได้ว่า $s < t$

ในทางกลับกัน สมมติ มีจำนวนเต็ม s, t ที่ $s < t$, $(s, t) = 1$, s, t ไม่เป็นจำนวนคู่พร้อมกันและไม่เป็นจำนวนคี่พร้อมกัน

และ $$x = 2st$$

$$y = t^2 - s^2$$

$$z = t^2 + s^2$$

จะได้ว่า

$$\begin{aligned} x^2 + y^2 &= (2st)^2 + (t^2 - s^2)^2 \\ &= 4s^2t^2 + t^4 - 2t^2s^2 + s^4 \\ &= t^4 + 2s^2t^2 + s^4 \\ &= (t^2 + s^2)^2 = z^2 \end{aligned}$$

ต่อไปจะแสดงว่า $(x, y, z) = 1$

เพราะว่า s และ t ไม่เป็นจำนวนคู่พร้อมกันและไม่เป็นจำนวนคี่พร้อมกัน จะได้ว่า x เป็นจำนวนคู่ y และ z เป็นจำนวนคี่

สมมติ $(y, z) = d > 1$ จะมีจำนวนเฉพาะ p โดยที่ $p|d$

ผลที่ตามมาก็คือ $p|y$ และ $p|z$ ซึ่งทำให้ p ต้องเป็นจำนวนเฉพาะคี่

ดังนั้น $p|z+y$ และ $p|z-y$

นั่นคือ $p|2t^2$ และ $p|2s^2$

ผลที่ตามมาก็คือ $p|t^2$ และ $p|s^2$

ซึ่งได้ว่า $p|t$ และ $p|s$ และทำให้ขัดแย้งกับ $(s, t) = 1$

ดังนั้น $(y, z) = 1$

ในทำนองเดียวกัน สามารถพิสูจน์ได้ว่า $(x, y) = (x, z) = 1$

นั่นคือ $(x, y, z) = 1$ #

ตัวอย่าง 2.20 จงหาค่าจำนวนสามจำนวนปฐมฐานของปีทาโกรัส เมื่อกำหนด $s = 1,\ t = 2$

วิธีทำ ให้

$$x = 2st = 2\cdot 1\cdot 2 = 4$$

$$y = t^2 - s^2 = 4 - 1 = 3$$

$$z = t^2 + s^2 = 4 + 1 = 5$$

ดังนั้น จำนวนสามจำนวนปฐมฐานของปีทาโกรัส คือ 3, 4, 5 #

แบบฝึกหัด 2.3

1. จงสร้างจำนวนสามจำนวนปฐมฐานของปีทาโกรัส เมื่อกำหนด s และ t ต่อไปนี้

1.1 $s = 1,\ t = 4$ | 1.2 $s = 2,\ t = 3$
1.3 $s = 1,\ t = 6$ | 1.4 $s = 2,\ t = 5$
1.5 $s = 3,\ t = 4$ | 1.6 $s = 1,\ t = 8$
1.7 $s = 2,\ t = 7$ | 1.8 $s = 4,\ t = 5$

2. จงแสดงว่า พื้นที่ของสามเหลี่ยมมุมฉากซึ่งมีด้านสามด้านเป็นจำนวนสามจำนวนของปีทาโกรัสต้องเป็นจำนวนเต็ม
3. จงแสดงว่า ถ้า x, y, z เป็นจำนวนสามจำนวนปฐมฐานของปีทาโกรัสแล้ว x หรือ y จะต้องหารด้วย 3 ลงตัว
4. จงแสดงว่า ถ้า x, y, z เป็นจำนวนสามจำนวนของปีทาโกรัสแล้ว ในระหว่าง x, y, z จะมีและมีแน่นอน หนึ่งจำนวนที่หารด้วย 5 ลงตัว
5. จงแสดงว่า ถ้า x, y, z เป็นจำนวนสามจำนวนของปีทาโกรัสแล้ว อย่างน้อยหนึ่งจำนวนในระหว่าง x, y, z ต้องหารด้วย 4 ลงตัว
6. จงแสดงว่า ทุกจำนวนเต็มบวกที่มากกว่า 3 เป็นหนึ่งในจำนวนสามจำนวนของปีทาโกรัส

2.4 **สมการดีโอฟานทีนเชิงเส้น** (Linear Diophantine Equations)

สมการ $ax+by = c$

เมื่อ a, b, c เป็นจำนวนจริง

เรียกว่า **สมการเชิงเส้น** (linear equation)

สมการเชิงเส้นบางสมการต้องการทราบผลเฉลยที่เป็นจำนวนเต็มเท่านั้น เช่น สมมติมีเงินอยู่ 510 บาท ต้องการแลกตั๋วแลกเงินไปรษณีย์ซึ่งมีเฉพาะราคาฉบับละ 20 บาท และ 50 บาทเท่านั้น ถ้าใช้แลกเงินทั้งหมด 510 บาท อยากทราบว่าจะได้ตั๋วแลกเงินไปรษณีย์อย่างละกี่ฉบับ

ปัญหาข้างต้นสามารถเขียนเป็นสมการเชิงเส้นได้ คือ

$$20x+50y = 510$$

สมการ $ax+by = c$

เมื่อ a, b, c เป็นจำนวนเต็ม

เรียกว่า **สมการดีโอฟานทีนเชิงเส้นใน 2 ตัวแปร** (Linear Diophantine Equations in two variables) ซึ่งจะพิจารณาผลเฉลยที่เป็นจำนวนเต็มของสมการได้ดังนี้

ทฤษฎีบท 2.20 ให้ a, b เป็นจำนวนเต็มบวก และ $d = (a, b)$

สมการ $ax+by = c$ ไม่มีผลเฉลย ถ้า $d\nmid c$

ถ้า $d|c$ สมการ $ax+by = c$ มีผลเฉลยมากมายเป็นจำนวนอนันต์

มากไปกว่านั้น ถ้า $x = x_0$ และ $y = y_0$ เป็นผลเฉลยของสมการแล้ว ทุกผลเฉลยของสมการจะอยู่ในรูปแบบของ

$$x = x_0+\frac{(b)}{d}n$$

$$y = y_0-\frac{(a)}{d}n \qquad \text{เมื่อ } n \text{ เป็นจำนวนเต็ม}$$

ซึ่งรูปแบบนี้เรียกว่า ผลเฉลยทั่วไป (general solution) ของสมการ

พิสูจน์ สมมติ x, y เป็นจำนวนเต็มที่ทำให้

$$ax+by = c$$

เพราะว่า $d = (a, b)$ ดังนั้น $d|a$ และ d/b

ผลที่ตามมาก็คือ $d|c$ นั่นคือ ถ้า $d\nmid c$ แล้ว สมการ $ax+by = c$ ไม่มีผลเฉลย

ต่อไปสมมติว่า $d|c$

เพราะว่า $d = (a, b)$

ดังนั้น จะมีจำนวนเต็ม s, t ที่ทำให้

$$d = as + bt$$

และเพราะว่า $d|c$ จะมีจำนวนเต็ม e ที่ทำให้ $c = de$

นั่นคือ $c = de = ase + bte$

เพราะฉะนั้น $x_0 = se$ และ $y_0 = te$ เป็นผลเฉลยของสมการที่เป็นจำนวนเต็ม

ต่อไปจะแสดงว่ามีผลเฉลยมากมายเป็นจำนวนอนันต์

ให้
$$x = x_0 + \frac{(b)}{d} n$$

$$y = y_0 - \frac{(a)}{d} n$$

เมื่อ n เป็นจำนวนเต็มใด ๆ

พิจารณา $ax + by$

จะได้
$$\begin{aligned} ax + by &= a\left[x_0 + \frac{(b)}{d} n\right] + b\left[y_0 - \frac{(a)}{d} n\right] \\ &= ax_0 + \frac{(ab)}{d} n + by_0 - \frac{(ab)}{d} n \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

นั่นคือ $x = x_0 + \frac{(b)}{d} n$ และ $y = y_0 - \frac{(a)}{d} n$

เป็นผลเฉลยของสมการทุกจำนวนเต็ม n

ต่อไปจะแสดงว่า ทุกผลเฉลยของสมการอยู่ในรูปแบบของ

$$x = x_0 + \frac{(b)}{d} n$$

$$y = y_0 - \frac{(a)}{d} n$$

เมื่อ x_0, y_0 เป็นผลเฉลยหนึ่ง และ n เป็นจำนวนเต็ม

สมมติ x, y เป็นจำนวนเต็ม โดยที่

$$ax + by = c$$

เพราะว่า $ax_0 + by_0 = c$

จะได้ว่า

$$(ax + by) - (ax_0 + by_0) = 0$$

$$a(x - x_0) + b(y - y_0) = 0$$

นั่นคือ

$$a(x - x_0) = b(y_0 - y)$$

และได้ว่า

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

เพราะว่า $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ผลที่ตามมาก็คือ $\frac{a}{d} \mid (y_0 - y)$

นั่นคือ จะมีจำนวนเต็ม n ที่ทำให้

$$y = y_0 - \left(\frac{a}{d}\right) n$$

เพราะว่า

$$a(x - x_0) = b(y_0 - y)$$

ดังนั้น

$$a(x - x_0) = b\left(\frac{a}{d}\right) n$$

นั่นคือ

$$x = x_0 + \left(\frac{b}{d}\right) n$$ #

ตัวอย่าง 2.21 จงหาผลเฉลยที่เป็นจำนวนเต็มของ $6x + 15y = 33$

วิธีทำ เพราะว่า $(6, 15) = 3$ และ $3 \nmid 83$

ดังนั้น $6x + 15y = 83$

ไม่มีผลเฉลยที่เป็นจำนวนเต็ม #

ตัวอย่าง 2.22 จงหาผลเฉลยที่เป็นจำนวนเต็มของ

$$172x + 20y = 1000$$

วิธีทำ หาตัวหารร่วมมากของ 172 และ 20 โดยขั้นตอนวิธีของยุคลิด

$$172 = 8\cdot 20+12$$

$$20 = 1\cdot 12+8$$

$$12 = 1\cdot 8+4$$

$$8 = 2\cdot 4$$

ดังนั้น $(172, 20) = 4$

เพราะว่า $4 \mid 1000$ ดังนั้น สมการนี้มีผลเฉลยที่เป็นจำนวนเต็ม

ต่อไปหา s และ t ที่ทำให้

$$4 = 172s+20t$$

จาก

$$12 = 1\cdot 8+4$$

จะได้

$$\begin{aligned} 4 &= 12-1\cdot 8 \\ &= 12-1\cdot(20-1\cdot 12) \\ &= 2\cdot 12-1\cdot 20 \\ &= 2(172-8\cdot 20)-1\cdot 20 \\ 4 &= 2\cdot 172-17\cdot 20 \\ 4 &= 2\cdot 172+(-17)20 \end{aligned}$$

คูณสมการทั้งสองข้างด้วย 250

$$1000 = 4\cdot 250 = 2\cdot 250\cdot 172+(-17)250\cdot 20$$

$$1000 = 500\cdot 172+(-4250)\cdot 20$$

นั่นคือ $x_0 = 500$, $y_0 = -4250$ เป็นผลเฉลยหนึ่งของสมการนี้

เพราะฉะนั้น ผลเฉลยทั่วไปคือ

$$x = x_0+\frac{(b)}{d}n = 500+\frac{(20)}{4}n$$

$$= 500+5n$$

$$y = y_0-\frac{(a)}{d}n = -4250-\frac{(172)}{4}n$$

$$= -4250-43n$$

เมื่อ n เป็นจำนวนเต็ม #

ในบางกรณีไม่เพียงแต่ต้องการผลเฉลยที่เป็นจำนวนเต็มเท่านั้น เราต้องการผลเฉลยที่เป็นจำนวนเต็มบวกด้วย ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.23 มีเงินอยู่ 510 บาท ต้องการแลกตั๋วแลกเงินไปรษณีย์ซึ่งมีเฉพาะราคาฉบับละ 20 บาท และ 50 บาทเท่านั้น ถ้าใช้เงินแลกทั้งหมด 510 บาท อยากทราบว่าจะได้ตั๋วแลกเงินไปรษณีย์อย่างละกี่ฉบับ

วิธีทำ จากปัญหาข้างต้นเขียนเป็นสมการดีโอฟานทีนเชิงเส้นได้ คือ

$$20x + 50y = 510$$

เพราะว่า $(20, 50) = 10$ และ $10 | 510$ ดังนั้น สมการนี้มีผลเฉลยที่เป็นจำนวนเต็ม

พิจารณาการหาผลเฉลยได้ดังนี้

หาตัวหารร่วมมากของ 20 และ 50 โดยขั้นตอนวิธีของยุคลิด

$$50 = 2 \cdot 20 + 10$$

$$20 = 2 \cdot 10$$

ซึ่งได้ว่า

$$10 = 50 - 2 \cdot 20$$

คูณสมการทั้งสองข้างด้วย 51

จะได้

$$510 = 51 \cdot 10 = 51 \cdot 50 - 51 \cdot 2 \cdot 20$$

$$510 = 51 \cdot 50 - 102 \cdot 20$$

นั่นคือ $x_0 = -102$, $y_0 = 51$ เป็นผลเฉลยหนึ่งของสมการ

เนื่องจากจำนวนตั๋วแลกเงินไปรษณีย์ต้องเป็นจำนวนเต็มบวกเสมอ ดังนั้น จึงพิจารณาผลเฉลยที่เป็นจำนวนเต็มบวก

เพราะว่าผลเฉลยทั่วไปคือ

$$x = x_0 + \frac{b}{d}n = -102 + 5n$$

$$y = y_0 - \frac{a}{d}n = 51 - 2n$$

หาค่า n ที่ทำให้ $-102 + 5n \geqslant 0$ และ $51 - 2n \geqslant 0$

พิจารณา

$$-102 + 5n \geqslant 0$$

$$5n \geqslant 102$$

$$n \geqslant \frac{102}{5} = 209$$

และ

$$51 - 2n \geqslant 0$$

$$51 \geqslant 2n$$

$$\frac{51}{2} \geqslant n$$

จึงได้ $20 \cdot 4 \leqslant n \leqslant 25 \cdot 5$

นั่นคือ $n = 21, 22, 23, 24, 25$

ดังนั้น ผลเฉลยที่เป็นจำนวนเต็มบวก มี 5 ผลเฉลย คือ

$(3, 9)$, $(8, 7)$, $(13, 5)$, $(18, 3)$ และ $(23, 1)$

แบบฝึกหัด 2.5

1. จงพิจารณาว่า สมการดีโอฟานทีนเชิงเส้นต่อไปนี้มีผลเฉลยที่เป็นจำนวนเต็มหรือไม่ และถ้ามีให้หาผลเฉลยเหล่านั้น

   1.1 $2x + 5y = 1$ 1.2 $17x + 13y = 100$ 1.5 $1402x + 1969y = 1$

   1.3 $21x + 14y = 147$ 1.4 $60x + 18y = 97$

2. จงหาผลเฉลยที่เป็นจำนวนเต็มของ

$$247x + 589y = 817$$

3. จงหาผลเฉลยที่เป็นจำนวนเต็มของ

$$999x - 49y = 5000$$

4. จงหาผลเฉลยที่เป็นจำนวนเต็มบวกของสมการต่อไปนี้

   4.1 $5x + 3y = 52$ 4.2 $15x + 7y = 111$

   4.3 $40x + 63y = 521$ 4.4 $123x + 57y = 531$

   4.5 $12x + 50y = 1$ 4.6 $12x + 501y = 274$

   4.7 $87x + 98y = 1000$

5. เจ้าของร้านผลไม้มีเงินทุนสำหรับสั่งผลไม้มาจำหน่าย 839 บาท เขาต้องการสั่งแอปเปิ้ลและส้มโอ โดยที่แอปเปิ้ลราคาใบละ 25 บาท ส้มโอราคาใบละ 18 บาท ถ้าเขาต้องการสั่งแอปเปิ้ลจำนวนมากกว่าส้มโอ เขาจะสั่งผลไม้ได้กี่แบบ

6. จงแสดงว่า สมการดีโอฟานทีนเชิงเส้น n ตัวแปร

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

   ไม่มีผลเฉลย ถ้า $d \nmid b$ เมื่อ $d = (a_1, a_2, \ldots, a_n)$
   และถ้า $d \mid b$ แล้ว มีผลเฉลยมากมายเป็นจำนวนอนันต์

7. จงหาผลเฉลยที่เป็นจำนวนเต็มของสมการต่อไปนี้

   7.1 $2x + 3y + 4z = 5$ 7.2 $7x + 21y + 35z = 8$

   7.3 $101x + 102y + 103z = 1$