บทที่ 4
ทฤษฎีจำนวนเบื้องต้น

ทฤษฎีจำนวนเป็นวิชาที่ศึกษาเกี่ยวกับจำนวนเต็มและสมบัติต่าง ๆ ของจำนวนเต็ม ซึ่งสมบัติดังกล่าวมีจำนวนมากมายและลึกซึ้ง แต่ในที่นี้ จะศึกษาเพียงเรื่อง การหารลงตัว ขั้นตอนวิธีการหาร ตัวหารร่วมมาก ตัวคูณร่วมน้อย จำนวนเฉพาะ และคอนกรูเอินซ์

4.1 ขั้นตอนวิธีของยุคลิด

ทฤษฎีบท 4.1.1 ถ้า a และ b เป็นจำนวนเต็มโดยที่ $b \neq 0$ จะมีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้นซึ่ง $a = qb + r$ และ $0 \leq r < |b|$

พิสูจน์ ตอนแรกจะพิสูจน์ว่า มีจำนวนเต็ม q และ r ซึ่ง $a = qb + r$ และ $0 \leq r < |b|$

พิจารณาเซต S โดยที่ $S = \{a - xb \mid x \in Z$ และ $a - xb \geq 0\}$

ถ้า $b > 0$

จะได้ว่า $b \geq 1$ เพราะ b เป็นจำนวนเต็ม

ดังนั้น $-|a|b \leq -|a| \leq a$

เพราะฉะนั้น $a - (-|a|b) \geq 0$

ถ้า $b < 0$

จะได้ว่า $b \leq -1$

ดังนั้น $|a|b \leq -|a| \leq a$

เพราะฉะนั้น $a - (|a|b) \geq 0$

ดังนั้น $S \neq \emptyset$

ถ้า $0 \in S$ จะได้ว่า 0 เป็นสมาชิกแรกของ S ให้ $r = 0$

ถ้า $0 \notin S$ โดยหลักการเป็นอันดับดีแล้ว S จะมีสมาชิกแรกให้เป็น r ดังนั้นไม่ว่ากรณีใด ก็จะมี r ซึ่งเป็นสมาชิกแรกของ S

ให้ q เป็นจำนวนเต็มซึ่ง $r = a - qb \geq 0$

สมมุติว่า $r \geq |b|$

จะได้ว่า $r - |b| \geq 0$

ดังนั้น
$$\begin{aligned} r - |b| &= (a - qb) - |b| \\ &= a - (qb + |b|) \\ &= a - (q \pm 1)b \end{aligned}$$

เพราะฉะนั้น $r - |b| \in S$

ดังนั้น $r \leq r - |b|$ เพราะ r เป็นสมาชิกแรกของ S

ซึ่งขัดกับ $r - |b| < r$

ดังนั้นสมมุติฐานว่า $r \geq |b|$ ไม่จริง เพราะฉะนั้น $r < |b|$

เพราะฉะนั้นจึงสรุปได้ว่า มีจำนวนเต็ม q และ r ซึ่ง $a = qb + r$ และ $0 \leq r < |b|$

ตอนนี้เราจะพิสูจน์ว่า จำนวนเต็ม q และ r ที่มีสมบัติดังกล่าวข้างต้นมีเพียงคู่เดียวเท่านั้น

สมมุติว่า $a = bq + r \quad , \quad 0 \leq r < |b|$

และ $a = bq' + r' \quad , \quad 0 \leq r' < |b|$

ดังนั้น $r - r' = b(q' - q)$

$|r - r'| = |b||q - q'|$

แต่ $|r - r'| < |b|$

ดังนั้น $|b||q - q'| < |b|$

เพราะฉะนั้น $|q - q'| < 1$

แต่ค่าสมบูรณ์ต้องมากกว่าหรือเท่ากับศูนย์ และ $|q - q'|$ เป็นจำนวนเต็ม

ดังนั้น $|q - q'| = 0$

เพราะฉะนั้น $q = q'$

และ $r = r'$

นิยมเรียกทฤษฎีบท 4.1.1 นี้ว่า **ขั้นตอนวิธีหาร** (Division Algorithm) หรือ **ทฤษฎีบทพื้นฐานของยุคลิด** (Fundamental Theorem of Euclid)

ถ้า $r \neq 0$ แสดงว่า a หารด้วย b แล้วได้ผลลัพธ์ b และเหลือเศษ r นั่นคือ a หาร b ไม่ลงตัว

ตัวอย่าง 4.1.1 ถ้า $a = 57$ และ $b = -25$ จงหา q และ r ซึ่ง

$$57 = q(-25) + r \quad , \quad 0 \leq r < 25$$

....

....

....

....

....

....

ตัวอย่าง 4.1.2 ถ้า $a = -68$ และ $b = 12$ จงหา q และ r ซึ่ง

$$-68 = q(12) + r \, , \quad 0 \leq r < 12$$

....

....

....

....

....

....

เราจะใช้ขั้นตอนวิธีการหารช่วยในการพิสูจน์ จำนวนเต็ม 2 จำนวนใด ๆ ซึ่งอย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ จะมีตัวหารร่วมมากเสมอ

ทฤษฎีบท 4.1.2 ให้ a และ b เป็นจำนวนเต็ม ซึ่งอย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ จะได้ว่า a และ b จะมีตัวหารร่วมมากเพียงตัวเดียวเท่านั้น และจะมีจำนวนเต็ม m และ n ซึ่งตัวหารร่วมมากนั้นจะเท่ากับ $ma + nb$

ข้อสังเกต ในการพิสูจน์ เราทราบว่าตัวหารร่วมมากเป็นจำนวนเต็มบวกซึ่งมีค่าน้อยที่สุดซึ่งอยู่ในรูป $xa + yb$

ต่อไปนี้ จะแสดงวิธีหาตัวหารร่วมมาก ซึ่งมีชื่อว่า **ขั้นตอนวิธีของยุคลิด** (Euclidean Algorithm)

ถ้า a และ b เป็นจำนวนเต็มบวก จะได้ว่า

$$
\begin{aligned}
a &= q_1 b + r_1 && ,0 \le r_1 < b,\ q_1,\ r_1 \in Z^+ \\
b &= q_2 r_1 + r_2 && ,0 \le r_2 < r_1,\ q_2,\ r_2 \in Z^+ \\
r_1 &= q_3 r_2 + r_3 && ,0 \le r_3 < r_2,\ q_3,\ r_3 \in Z^+ \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && ,0 \le r_n < r_{n-1},\ q_n,\ r_n \in Z^+ \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
$$

เนื่องจากเศษ $r_1,\ r_2, \ldots$ มีค่าน้อยลงเรื่อยๆ ในที่สุดจะต้องเท่ากับศูนย์

ให้ r_n เป็นเศษตัวสุดท้ายที่ไม่เท่ากับศูนย์ จะได้ว่า $r_{n+1} = 0$

ถ้า $c = (a,\ b)$ จะได้ว่า $c \mid a$ และ $c \mid b$ และเนื่องจาก $r_1 = a - q_1 b$ ดังนั้น $c \mid r_1$ โดยเหตุผลเดียวกัน จะได้ว่า $c \mid r_2$, $c \mid r_3, \ldots, c \mid r_n$

จากสมการสุดท้ายของขั้นตอนวิธีของยุคลิด $r_n \mid r_{n-1}$

เนื่องจาก $r_n \mid (q_n r_{n-1} + r_n)$ ดังนั้น $r_n \mid r_{n-2}$

โดยเหตุผลเดียวกัน $r_n \mid r_{n-3}, \ldots, r_n \mid r_2, r_n \mid r_1, r_n \mid b$ และ $r_n \mid a$ ดังนั้น $r_n \mid c$

เพราะฉะนั้น $r_n = c$ ดังนั้น $r_n = (a,\ b)$

ตัวอย่าง 4.1.3 จงหา ห.ร.ม ของ 26 และ 118

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

ตัวอย่าง 4.1.4 จงหา ห.ร.ม ของ 9035 และ 364

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

วิธีการนี้สามารถใช้หาตัวหารร่วมมากของจำนวนเต็มซึ่งไม่เท่ากับศูนย์ เช่นจากตัวอย่าง 4.1.4 สรุปได้ว่า

$$\begin{aligned}(9035, -364) &= 13\\(-9035,\ 364) &= 13\\(-9035,\ -364) &= 13\end{aligned}$$

บทนิยาม 4.1.1 ถ้า a และ b เป็นจำนวนเต็มซึ่งอย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ a และ b จะเป็นจำนวนเฉพาะสัมพัทธ์ (relatively prime) ก็ต่อเมื่อ $(a, b) = 1$

บทแทรก 4.1.3 ให้ a และ b เป็นจำนวนเต็มซึ่งอย่างน้อยหนึ่งตัวต้องไม่เท่ากับศูนย์ ถ้า a และ b เป็นจำนวนเฉพาะสัมพัทธ์ จะมีจำนวนเต็ม m และ n ซึ่ง $ma + nb = 1$

พิสูจน์ เป็นผลโดยตรงจากทฤษฎีบท 4.1.2 ในกรณีที่ตัวหารร่วมมากเท่ากับ 1

ทฤษฎีบท 4.1.4 ทฤษฎีบทพื้นฐานของเลขคณิต

จำนวนเต็มบวก $n > 1$ ทุกตัวสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกและยกเว้นการเรียงลำดับตัวประกอบสามารถเขียนได้วิธีเดียว

พิสูจน์ ตอนแรกจะพิสูจน์ว่า $n > 1$ ทุกตัวสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวก

ให้ $P(n)$ แทนประพจน์ จำนวนเต็มบวก $n > 1$ สามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวก

ถ้า n เป็นจำนวนเฉพาะ จะถือว่า n เป็นผลคูณที่มีแฟกเตอร์ตัวเดียว ดังนั้นในกรณีนี้ $P(n)$ เป็นจริง โดยเฉพาะ $P(2)$ เป็นจริง

สมมุติว่า n ไม่ใช่จำนวนเฉพาะและ $P(m)$ เป็นจริงสำหรับจำนวนเต็มบวก $m < n$

เนื่องจาก n ไม่ใช่จำนวนเฉพาะ ดังนั้นจะมีจำนวนเต็มบวก h ซึ่งไม่ใช่ 1 และไม่ใช่ n ซึ่ง $n = hk,\ k \in Z^+$

เนื่องจาก $1 < h < n$ และ $1 < k < n$ ดังนั้นโดยสมมุติฐานจำนวนเต็มบวก h และ k สามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวก ดังนั้น n ซึ่งเท่ากับ hk จึงสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวก

โดยหลักการอุปนัยเชิงคณิตศาสตร์ สรุปได้ว่า จำนวนเต็มบวก $n > 1$ ทุกตัวสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวก

ต่อไปนี้จะพิสูจน์ว่า ยกเว้นการเรียงลำดับตัวประกอบ ผลคูณของจำนวนเฉพาะที่เป็นบวกนี้สามารถเขียนเพียงวิธีเดียว

ตอนแรกจะพิสูจน์ว่า ถ้าจำนวนเต็มบวก m สามารถเขียนในรูป ผลคูณของจำนวนเฉพาะที่เป็นบวกเพียงวิธีเดียวแล้ว จำนวนเฉพาะที่เป็นบวกซึ่งหาร m ต้องอยู่ในผลคูณนั้น (*)

ถ้า p เป็นจำนวนเฉพาะที่เป็นบวกซึ่งหาร m จะได้ว่า $m = pq,\ q \in Z^+$ เมื่อแทน q ด้วยผลคูณของจำนวนเฉพาะที่เป็นบวก m จะเขียนอยู่ในรูป ผลคูณของจำนวนเฉพาะที่เป็นบวก ซึ่งตัวหนึ่งคือ p เนื่องจากผลคูณนี้มีวิธีเดียว ดังนั้น p เป็นตัวประกอบตัวหนึ่ง

ต่อไปนี้จะพิสูจน์ สำหรับจำนวนเต็มบวก $n > 1$ สามารถเขียน n ในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกเพียงวิธีเดียวเท่านั้น

(1) $N = 2$ เป็นจริง

(2) สมมุติว่าสำหรับจำนวนเต็มบวก k ทุกตัวซึ่ง $k < n$ สามารถเขียน k ในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกเพียงวิธีเดียวเท่านั้น

ถ้า n เป็นจำนวนเฉพาะ ไม่มีอะไรที่ต้องพิสูจน์

ถ้า n ไม่ใช่จำนวนเฉพาะและสมมุติว่า n สามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกได้ 2 วิธี

a) $n = p_1 p_2 \dots p_h$

b) $n = q_1 q_2 \dots q_k$

โดยที่ $p_1, p_2, \dots, p_h$ และ $q_1, q_2, \dots, q_k$ เป็นจำนวนเฉพาะสำหรับ $i \in \{1, 2, \dots, h\}$ และ $j \in \{1, 2, \dots, k\}$ และ $p_j \neq q_j$ เพราะถ้ามีจำนวนเฉพาะที่เป็นบวกตัวเดียวกันในทั้งสองผลคูณ สามารถตัดจำนวนเฉพาะร่วมออกทำให้ได้จำนวนเต็มบวกซึ่งน้อยกว่า n และสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกได้ 2 วิธี ขัดกับสมมุติฐาน โดยสมบัติการสลับที่สามารถสลับที่จำนวนเฉพาะในผลคูณ จึงสามารถให้ p_1 เป็นจำนวนเฉพาะที่เป็นบวกที่มีค่าน้อยที่สุดในผลคูณ a)

เนื่องจาก n ไม่ใช่จำนวนเฉพาะจะมีตัวประกอบตัวอื่นนอกเหนือจาก p_1 ในผลคูณ a) ดังนั้น $n \geq p_1^2$ ในทำนองเดียวกันให้ q_1 เป็นจำนวนเฉพาะที่เป็นบวกที่มีค่าน้อยที่สุดในผลคูณ b) ดังนั้น $n \geq q_1^2$

เนื่องจาก $p_1 \neq q_1$ ดังนั้น $p_1 < q_1$ หรือ $p_1 > q_1$

ในกรณี $p_1 < q_1$ จะได้ว่า $p_1^2 < p_1q_1$ และ $p_1q_1 < q_1^2$

ดังนั้น $p_1^2 < p_1q_1 < q_1^2$

ในกรณี $p_1 > q_1$ จะได้ว่า $p_1^2 > p_1q_1$ และ $p_1q_1 > q_1^2$

ดังนั้น $p_1^2 > p_1q_1 > q_1^2$

ดังนั้นในทั้งสองกรณี $n > p_1q_1$ และ $n - p_1q_1$ เป็นจำนวนเต็มบวกที่น้อยกว่า n เพราะฉะนั้น $n - p_1q_1$ สามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกได้เพียงวิธีเดียว

เนื่องจาก
$$\begin{aligned} n - p_1q_1 &= p_1(p_2 \dots p_h) - p_1q_1 \\ &= p_1[(p_2 \dots p_h) - q_1] \end{aligned}$$

ดังนั้น p_1 หาร $n - p_1q_1$ เพราะฉะนั้นโดย (*) p_1 เป็นตัวปะกอบของ $n - p_1q_1$

ในทำนองเดียวกัน q_1 เป็นตัวประกอบของ $n - p_1q_1$

ดังนั้น $n - p_1q_1 = p_1q_1P$ โดยที่ P คือ 1 หรือ ผลคูณของจำนวนเฉพาะที่เป็นบวก

เนื่องจาก $n = p_1q_1 + p_1q_1P$ ดังนั้น $p_1q_1 \mid n$

เนื่องจาก $n = p_1q_1 \dots p_h$ ดังนั้น $p_1p_2 \dots p_h = p_1q_1(1 + P)$

ตัด p_1 ออกจะได้ว่า $p_2 \dots p_h = p_1q_1(1+P)$ ดังนั้น $q_1 \mid p_2 \dots p_h$

แต่เนื่องจาก $p_2 \dots p_h$ เป็นการเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกของจำนวนเต็มบวก $m < n$ ดังนั้นโดย (*) q_1 ต้องอยู่ในผลคูณ $p_2 \dots p_h$ ซึ่งขัดกับ $p_i \neq q_j$

ดังนั้นสำหรับจำนวนเต็มบวก $n > 1$ ทุกตัวสามารถเขียนในรูปผลคูณของจำนวนเฉพาะที่เป็นบวกได้เพียงวิธีเดียว (ยกเว้นการเรียงลำดับตัวประกอบ)

ทฤษฎีบทพื้นฐานของเลขคณิตนั้น พิสูจน์สำหรับจำนวนเต็มบวกซึ่งมากกว่า 1 แต่สามารถขยายไปสำหรับจำนวนเต็มซึ่งไม่เท่ากับศูนย์

ถ้า n เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ $|n| = n$ หรือ $|n| = -n$

ดังนั้น $n = \dfrac{n}{|n|}\,|n|$ โดยที่ $\dfrac{n}{|n|}$ เท่ากับ 1 หรือ -1 ดังนั้นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ สามารถเขียนในรูปผลคูณจองจำนวนเต็มบวกกับ 1 หรือ -1 เพราะฉะนั้นจึงอาจเขียนทฤษฎีบทพื้นฐานของเลขคณิตได้ดังนี้ จำนวนเต็มทุกตัวที่ไม่เท่ากับศูนย์ ยกเว้น 1 หรือ -1 สามารถเขียนในรูปผลคูณของ $\dfrac{n}{|n|}$ และผลคูณของจำนวนเฉพาะที่เป็นบวก

ทฤษฎีบท 4.1.5 ให้ a, b และ c เป็นจำนวนเต็มใด ๆ ถ้า $a \mid bc$ และ $(a, b) = 1$ แล้ว $a \mid c$

ทฤษฎีบท 4.1.6 ให้ p เป็นจำนวนเฉพาะ และ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็ม ถ้า $p \mid (a_1 a_2, \ldots a_n)$ จะได้ว่า $p \mid a_i$ สำหรับ i บางตัวใน $\{1, 2, \ldots, n\}$

ทฤษฎีบท 4.1.7 ถ้า a และ b เป็นจำนวนเต็มบวก ตัวคูณร่วมน้อยจะมีเพียงตัวเดียวเท่านั้น และ $(a,\ b)[a,\ b] = ab$

แบบฝึกหัด 4.1

1. สำหรับจำนวน m และ n แต่ละคู่ที่กำหนดให้ จงหา q และ r โดยที่

$$n = mq + r \qquad ,0 \le r < |m|$$

(1) $n = 66 \quad , m = 38$

(2) $n = 45 \quad , m = 29$

(3) $n = -15 \quad , m = 7$

(4) $n = 163 \quad , m = -35$

(5) $n = -33 \quad , m = -9$

(6) $n = -1203 \quad , m = 125$

(7) $n = 303 \quad , m = -92$

2. เขียน 4367 ในรูปผลคูณของจำนวนเฉพาะ

3. จงหาจำนวนเต็ม m และ n ซึ่ง

(1) $(18,\ 256) = 18m + 256n$

(2) $(-125,\ 165) = (-125)m + 165n$

(3) $(64,\ 216) = 64m + 216n$

(4) $(110,\ -273) = 110m + (-273)n$

(5) $(-604, -168) = (-604)m + (-168)n$

(6) $(167,\ -23) = 167m + (-23)n$

4. ถ้า a, b และ c เป็นจำนวนเต็มซึ่ง $a \mid bc$ จงหาตัวอย่างซึ่ง a หาร b ไม่ลงตัวและ a หาร c ไม่ลงตัว

5. ถ้า n เป็นจำนวนเต็มบวก a และ b เป็นจำนวนเต็มซึ่งมีอย่างน้อยหนึ่งตัว ต้องไม่เท่ากับศูนย์ จงพิสูจน์ว่า $(na,\ nb) = n(a,\ b)$

6. ถ้า n เป็นจำนวนเต็มบวก และ $(a,\ b) = 1$ จงพิสูจน์ว่า $(a^n,\ b) = 1$

7. จงให้บทนิยามของตัวหารร่วมมากของจำนวนเต็ม 3 จำนวน

8. ถ้า $(a,\ b) = 1$, $a \mid c$ และ $b \mid c$ จงพิสูจน์ว่า $ab \mid c$

9. ถ้า $(a,\ b) = (a,\ c) = 1$ จงพิสูจน์ว่า $(a,\ bc) = 1$

4.2 คอนกรูเอินซ์

เกาส์ (Gauss , ค.ศ.1777-1855) เป็นนักคณิตศาสตร์ท่านแรกที่ใช้ความสัมพันธ์คอนกรูเอินซ์ (congruence) โดยให้บทนิยามดังนี้

บทนิยาม 4.2.1 ถ้า a และ b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก a จะเป็นคอนกรูเอินท์กับ b มอดุโล m (a is congruent to b modulo m) ก็ต่อเมื่อ มีจำนวนเต็ม k ซึ่ง $a - b = km$

เขียน $a \equiv b \pmod{m}$ แทน a คอนกรูเอินท์กับ b มอดุโล m

และเขียน $a \not\equiv b \pmod{m}$ แทน a ไม่คอนกรูเอินท์กับ b มอดุโล m

ข้อสังเกต บทนิยาม 4.2.1 บอกว่า a จะเป็นคอนกรูเอินท์กับ b มอดุโล m ก็ต่อเมื่อ $a - b$ หารด้วย m ลงตัว ดังนั้นอาจนิยามว่า $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $m \mid a - b$

ตัวอย่าง 4.2.1

$51 \equiv 6 \pmod{5}$ เพราะ ....

$92 \equiv -3 \pmod{5}$ เพราะ ....

$-8 \equiv 72 \pmod{5}$ เพราะ ....

$12 \not\equiv 4 \pmod{5}$ เพราะ ....

การที่เกาส์ใช้สัญลักษณ์ “ $\equiv$ ” ก็เพราะความสัมพันธ์คอนกรูเอินท์มีสมบัติคล้ายกับ “ $=$ ” ในระบบจำนวน ความสัมพันธ์ทั้งสองอย่างนี้ เป็นตัวอย่างของความสัมพันธ์สมมูล (equivalence relation) ซึ่งอาจจะให้บทนิยามดังนี้

บทนิยาม 4.2.1 ถ้า r เป็นความสัมพันธ์ในเซต A

(1) r จะเป็นความสัมพันธ์ที่มีสมบัติการสะท้อน (reflexive relation) ก็ต่อเมื่อสำหรับสมาชิก x ทุกตัวของ A จะได้ $x\ r\ x$

(2) r จะเป็นความสัมพันธ์ที่มีสมบัติการสมมาตร (symmetric relation) ก็ต่อเมื่อสำหรับสมาชิก x และ y ทุกตัวของ A ถ้า $x\ r\ y$ จะได้ $y\ r\ x$

(3) r จะเป็นความสัมพันธ์ที่มีการถ่ายทอด (transitive relation) ก็ต่อเมื่อสำหรับสมาชิก x, y และ z ทุกตัวของ A ถ้า $x\ r\ y$ และ $y\ r\ z$ จะได้ $x\ r\ z$

ความสัมพันธ์ใดซึ่งมีสมบัติทั้ง 3 ประการดังกล่าวข้างต้น เรียกความสัมพันธ์ นั้นว่า “ความสัมพันธ์สมมูล”

ทฤษฎีบท 4.2.1 ความสัมพันธ์คอนกรูเอินท์โมดุโล m เป็นความสัมพันธ์สมมูล

....

....

....

....

....

....

....

....

ทฤษฎีบท 4.2.2 a จะคอนกรูเอินท์กับ b มอดุโล m ก็ต่อเมื่อ a และ b เมื่อหารด้วย m จะเหลือเศษเท่ากัน

....

....

....

....

....

....

....

....

....

....

ตัวอย่าง 4.2.2 41 หารด้วย 3 เหลือเศษ 2

23 หารด้วย 3 เหลือเศษ 2

ดังนั้น $41 \equiv 23 \pmod{3}$

ตัวอย่าง 4.2.3 13 หารด้วย 5 เหลือเศษ 3

34 หารด้วย 5 เหลือเศษ 4

ดังนั้น $13 \not\equiv 34 \pmod{5}$

ทฤษฎีบท 4.2.3 ถ้า $a \equiv b \pmod{m}$ และ t เป็นจำนวนเต็มใด ๆ จะได้ว่า

(1) $a + t \equiv b + t \pmod{m}$

(2) $at \equiv bt \pmod{m}$

....

....

....

....

....

....

....

....

....

....

ทฤษฎีบท 4.2.4 ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ จะได้ว่า

(1) $a + c \equiv b + d \pmod{m}$

(2) $a - c \equiv b - d \pmod{m}$

(3) $ac \equiv bd \pmod{m}$

ทฤษฎีบท 4.2.5 ถ้า $a \equiv b \pmod{m}$ และ n เป็นจำนวนเต็มบวกใด ๆ
จะได้ว่า $a^n \equiv b^n \pmod{m}$

ตัวอย่าง 4.2.4 17 หาร 2^{30} เหลือเศษเท่าใด$89 \equiv 1 \pmod{8}$

ตัวอย่าง 4.2.5 7^{10} หารด้วย 50 เหลือเศษเท่าไร

ตัวอย่าง 4.2.6 จงพิสูจน์ว่า จำนวนเต็มใด ๆ เมื่อยกกำลังสองแล้วหารด้วย 4 จะลงตัวหรือ

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

ทฤษฎีบท 4.2.6 ถ้า $ca \equiv cb \pmod{m}$, $c \not\equiv 0 \pmod{m}$, $d = (c, m)$ และ $m = dw$ จะได้ว่า $a \equiv b \pmod{w}$

....

....

....

....

....

....

....

....

....

....

ทฤษฎีบท 4.2.7 ถ้า $ca \equiv cb \pmod{m}$, c และ m เป็นจำนวนเฉพาะสัมพัทธ์ จะได้ว่า $a \equiv b \pmod{m}$

....

....

....

....

....

....

....

....

....

ให้ $A = \{1, 2, 3, 4\}$ และ $C = \{\{1, 2\}, \{3, 4\}\}$
เราจะได้ว่า C เป็นเซตของเซตซึ่งมีคุณสมบัติดังนี้

(1) ทั้ง $\{1, 2\}$ และ $\{3, 4\}$ ต่างก็ไม่ใช่เซตว่าง
(2) $\{1, 2\} \cap \{3, 4\} = \emptyset$
(3) $\{1, 2\} \cup \{3, 4\} = \{1, 2, 3, 4\} = A$

เรียก C ว่าพาร์ทิชัน (partition) ของ A

บทนิยาม 4.2.3 พาร์ทิชันของเซต A คือเซตของเซต C ซึ่งมีคุณสมบัติดังนี้

(1) สำหรับสมาชิก x ทุกตัวของ C , $x \neq \emptyset$
(2) สำหรับสมาชิก x และ y ทุกตัวของ C ถ้า $x \neq y$ จะได้ว่า $x \cap y = \emptyset$
(3) ยูเนียนของสมาชิกทุกตัวของ C จะเท่ากับ A

ตัวอย่าง 2.2.7 กำหนดให้ $A = \{1, 2, 3, 4, 5\}$

$C_1 = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}$

$C_2 = \{\{1, 2\}, \{3, 4, 5\}, \emptyset\}$

$C_3 = \{\{1\}, \{2\}, \{3\}, \{4\}\}$

$C_4 = \{1, 2, 3, 4, 5\}$

$C_5 = \{\{1\}, \{2\}, \{3\}, \{4\}, 5\}$

$C_6 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$

$C_7 = \{\{1, 2, 3, 4\}, \{5\}\}$

ตัวอย่าง 2.2.8 กำหนดให้

$$0 \equiv \ldots, -6, -3, 0, 3, 6, \ldots \pmod{3}$$
$$1 \equiv \ldots, -5, -2, 1, 4, 7, \ldots \pmod{3}$$
$$2 \equiv \ldots, -4, -1, 2, 5, 8, \ldots \pmod{3}$$

ถ้าเราให้ $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
$= \{x \mid x = 3k,\ k \in Z\}$
$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
$= \{x \mid x = 3k + 1,\ k \in Z\}$
$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
$= \{x \mid x = 3k + 2,\ k \in Z\}$

จะได้ว่า $Z_3 = \{[0], [1], [2]\}$ เป็นพาร์ทิชันของ Z

เรียกสมาชิกของ Z_3 ว่า เรสิดิวคลาสมอดูโล 3 (residue class modulo 3)

ในกรณีทั่วไป ถ้า m เป็นจำนวนเต็มบวก

ให้ $[0] = \{x \mid x = km,\ k \in Z\}$
$[1] = \{x \mid x = km + 1,\ k \in Z\}$
$\vdots$
$[m-1] = \{x \mid x = km + (m-1),\ k \in Z\}$

จะได้ว่า $\{[0], [1], [2], \ldots, [m-1]\}$ เป็นพาร์ทิชั่นของ Z

เราให้บทนิยามการบวกและการคูณของเรสิดิวคลาสมอดุโล m ดังนี้

บทนิยาม 4.2.4 $[i] + [j]$ คือเรสิดิวคลาสซึ่งประกอบด้วยผลบวกของสมาชิกของ $[i]$ และ $[j]$
$[i][j]$ คือเรสิดิวคลาส ซึ่งประกอบด้วยผลคูณของสมาชิกของ $[i]$ และ $[j]$

เราจะต้องตรวจดูว่าบทนิยามของเรานี้แจ่มชัด (well defined) นั้นคือต้องตรวจดูว่า การบวกและการคูณที่เรานิยามนี้ จะได้ผลลัพท์เป็นเรสิดิวคลาสเดียวเท่านั้น

ถ้า $a_i, a_i' \in [i]$ และ $a_j, a_j' \in [j]$

เนื่องจาก $a_i \equiv a_i' \pmod{m}$ และ $a_j \equiv a_j' \pmod{m}$

ดังนั้น $a_i + a_j \equiv a_i' + a_j' \pmod{m}$ และ $a_i a_j \equiv a_i' a_j' \pmod{m}$

นั่นคือ $a_i + a_j,\ a_i' + a_j' \in [r],\ r \equiv i + j \pmod{m},\ 0 \le r < m$
$a_i a_j,\ a_i' a_j' \in [s],\ s \equiv ij \pmod{m},\ 0 \le s < m$

เพราะฉะนั้น บทนิยามของเราแจ่มชัด

ตัวอย่าง 2.2.17 $Z_3 = \{[0], [1], [2]\}$

....

....

....

....

....

....

....

แบบฝึกหัด 4.2

1. จงตรวจดูแต่ละข้อว่าเป็นจริงหรือเท็จ เพราะเหตุใด
   (1) $76 \equiv 56 \pmod 2$
   (2) $5 \equiv 32 \pmod 3$
   (3) $11 \equiv -7 \pmod 4$
   (4) $-6 \equiv -54 \pmod 5$
   (5) $14 \equiv -36 \pmod 6$
   (6) $-13 \equiv 75 \pmod 7$
   (7) $57 \equiv 99 \pmod 8$
   (8) $42 \equiv -93 \pmod 9$
   (9) $3 \not\equiv -192 \pmod{15}$
   (10) $604 \not\equiv 301 \pmod{33}$
2. ถ้า $a \equiv b \pmod m$ และ $d \mid m$ จงพิสูจน์ว่า $a \equiv b \pmod d$
3. $(3)(7)(13)(515)(25)$ หารด้วย 23 แล้วเศษเหลือเท่าไร
4. จงพิสูจน์ว่าจำนวนเต็มใดจะหารด้วย 8 ลงตัว ก็ต่อเมื่อเลขท้าย 3 ตัวหารด้วย 8 ลงตัว
5. จงคำนวณหา $n = 625^4 + 663$ และตรวจความถูกต้อง (บางส่วน) โดยวิธี casting out nines
6. จงพิสูจน์ว่าจำนวนเต็มใดจะหารด้วย 3 ลงตัว ก็ต่อเมื่อผลบวกของเลขทุกหลักรวมกัน แล้วหารด้วย 3 ลงตัว
7. 3^{10} หารด้วย 51 เหลือเศษเท่าไร
   4^{10} หารด้วย 51 เหลือเศษเท่าไร
   10^{503} หารด้วย 7 เหลือเศษเท่าไร
   5^{27} หารด้วย 127 เหลือเศษเท่าไร
   5^{65} หารด้วย 127 เหลือเศษเท่าไร
8. จงพิสูจน์ว่า $2^{23} - 1$ มี 47 เป็นตัวประกอบ
9. จงพิสูจน์ว่า $2^{23} - 1$ หารด้วย 23 ลงตัว
10. จงพิสูจน์ว่า จำนวนเต็มใดจะหารด้วย 25 ลงตัวก็ต่อเมื่อเลขท้าย 2 ตัวเท่ากับ 25 , 50 , 75 หรือ 00
11. จงพิสูจน์ว่า กำลังสองของจำนวนเต็มใด ๆ ไม่สามารถมีเลขท้ายเท่ากับ 79
12. ให้ $Z_4 = \{[0], [1], [2], [3]\}$ จงเขียนเรสิดิวคลาสของ Z_4 แต่ละตัวในรูปเซต
13. จงเขียนตารางการบวกและการคูณของ Z_4
14. จงเขียนตารางการบวกและการคูณของ Z_5