ทฤษฎีจำนวน NUMBER THEORY

อาจารย์ ดร.ธนัชยศ จำปาหวาย

สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

ทฤษฎีจำนวน Number Theory (ปลายภาค)

- บทที่ 5 สมภาค
- บทที่ 6 ฟังก์ชันเลขคณิต
- บทที่ 7 สมการไดโอแฟนไทน์
- บทที่ 8 ทฤษฎีบทเศษเหลือ

บทที่ 5 สมภาค

นิยามและสมบัติ

บทนิยาม

ให้ $a, b \in \mathbb{Z}$ และ $m \in \mathbb{Z}^+$ จะกล่าวว่า

a และ b **สมภาคกัน (congruent) มอดุโล (modulo)** m หรือ

a **สมภาคกับ** b **มอดุโล** m เขียนแทนด้วย $a \equiv b \pmod{m}$ นิยามโดย

$$a \equiv b \pmod{m} \qquad \text{ก็ต่อเมื่อ} \qquad m \mid (b-a)$$

a ไม่สมภาคกับ b มอดุโล m เขียนแทนด้วย $a \not\equiv b \pmod{m}$

ข้อสังเกต

1. $a \not\equiv b \pmod{m}$ ก็ต่อเมื่อ $m \nmid (b-a)$
2. $a \equiv b \pmod{1}$ และ $a \equiv a \pmod{m}$

ตัวอย่าง

จงให้เหตุผลเกี่ยวกับการสมภาคต่อไปนี้

1. $2 \equiv 5 \pmod 3$ เพราะว่า $3 \mid (5-3)$
2. $-3 \equiv 7 \pmod 5$ เพราะว่า $5 \mid (7-(-3))$
3. $-15 \equiv -3 \pmod 6$ เพราะว่า $6 \mid (-3-(-15))$
4. $5 \not\equiv 7 \pmod 3$ เพราะว่า $3 \nmid (7-5)$

ทฤษฎีบท

ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้ว

$$a \equiv b \pmod{m} \qquad \text{ก็ต่อเมื่อ} \qquad a \text{ และ } b \text{ มีเศษเหลือจากการหารด้วย } m \text{ เท่ากัน}$$

บทพิสูจน์.

ให้ $a, b \in \mathbb{Z}$ และ $m \in \mathbb{Z}^+$ โดยขั้นตอนวิธีการหารจะได้ว่ามีจำนวนเต็ม q_1, q_2, r_1, r_2 ซึ่ง

$$a = mq_1 + r_1 \qquad \text{เมื่อ } 0 \leq r_1 < m$$

$$b = mq_2 + r_2 \qquad \text{เมื่อ } 0 \leq r_2 < m$$

จะได้ว่า $b - a = m(q_2 - q_1) + (r_2 - r_1)$ โดยที่ $0 \leq |r_2 - r_1| < m$
สมมติว่า $a \equiv b \pmod{m}$ จะได้ว่า $m \mid (b - a)$ จะได้ว่า $m \mid (r_2 - r_1)$ เนื่องจาก $m \nmid (r_2 - r_1)$ เมื่อ $0 < |r_2 - r_1| < m$ ทำให้ได้ว่า $|r_2 - r_1| = 0$ นั่นคือ $r_1 = r_2$ ในทางกลับกันสมมติว่า $r_1 = r_2$ เห็นได้ชัดว่า $m \mid (b - a)$ สรุปได้ว่า $a \equiv b \pmod{m}$ □

ตัวอย่าง

จงให้เหตุผลสมภาคต่อไปนี้

1. $123 \equiv 192 \pmod 3$ เพราะว่า 3 หาร 123 และ 192 เหลือเศษ 0 เท่ากัน
2. $-124 \not\equiv 77 \pmod 5$ เพราะว่า 5 หาร -124 เหลือเศษ 1 แต่หาร 77 เหลือเศษ 2
3. $687 \equiv 176 \pmod 7$ เพราะว่า 7 หาร 687 และ 176 เหลือเศษ 1 เท่ากัน

ทฤษฎีบท

ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้ว

1. ***สมบัติสะท้อน (Reflexive law)***

   $a \equiv a \pmod{m}$

2. ***สมบัติสมมาตร (Symmetric law)***

   ถ้า $a \equiv b \pmod{m}$ *แล้ว* $b \equiv a \pmod{m}$

3. ***สมบัติถ่ายทอด (Transitive law)***

   ถ้า $a \equiv b \pmod{m}$ *และ* $b \equiv c \pmod{m}$ *แล้ว* $a \equiv c \pmod{m}$

บทพิสูจน์.

ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก

1. เนื่องจาก $m \mid (a-a)$ ดังนั้น $a \equiv a \pmod{m}$
2. สมมติว่า $a \equiv b \pmod{m}$ ดังนั้น $m \mid (b-a)$ เนื่องจาก $a-b=-(b-a)$ นั่นคือ $m \mid (a-b)$ สรุปได้ว่า $b \equiv a \pmod{m}$
3. สมมติว่า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ จะได้ว่า $m \mid (b-a)$ และ $m \mid (c-b)$ เนื่องจาก $c-a=(b-a)+(c-b)$ ดังนั้น $m \mid (c-a)$ สรุปได้ว่า $a \equiv c \pmod{m}$

□

ทฤษฎีบท

ให้ $a, b, c, d \in \mathbb{Z}$ *และ* $m \in \mathbb{Z}^+$ *ถ้า* $a \equiv b \pmod{m}$ *และ* $c \equiv d \pmod{m}$ *แล้ว*

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

บทพิสูจน์.

ให้ a, b, c, d เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก สมมติว่า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ จะได้ว่า $m \mid (b-a)$ และ $m \mid (d-c)$

1. เนื่องจาก $(b+d)-(a+c) = (b-a)+(d-c)$ ดังนั้น $m \mid [(b+d)-(a+c)]$ สรุปได้ว่า $a + c \equiv b + d \pmod{m}$

2. จะได้ว่า $m \mid (bc-ac)$ และ $m \mid (bd-bc)$ เนื่องจาก $ac - bd = (bc-ac)+(bd-bc)$ ดังนั้น $m \mid (bd-ac)$ สรุปได้ว่า $ac \equiv bd \pmod{m}$

□

ทฤษฎีบท

ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ แล้ว

1. *ถ้า $a \equiv b \pmod{m}$ แล้ว $a + c \equiv b + c \pmod{m}$*
2. *ถ้า $a \equiv b \pmod{m}$ แล้ว $ac \equiv bc \pmod{m}$*

บทพิสูจน์.

ให้ a, b, c เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก สมมติ $a \equiv b \pmod{m}$ จะได้ว่า $m \mid (b - a)$

1. เนื่องจาก $(b + c) - (a + c) = b - a$ ดังนั้น $m \mid [(b + c) - (a + c)]$ สรุปได้ว่า $a + c \equiv b + c \pmod{m}$
2. จะได้ว่า $m \mid (bc - ac)$ ดังนั้น $ac \equiv bc \pmod{m}$ □

ตัวอย่าง

ให้ a, b, c, d, x, y เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จงแสดงว่า

$$\text{ถ้า} \quad a \equiv b \pmod{m} \quad \text{และ} \quad c \equiv d \pmod{m} \quad \text{แล้ว} \quad ax + cy \equiv bx + dy \pmod{m}$$

ทฤษฎีบท

ให้ a, b เป็นจำนวนเต็ม และ m, k เป็นจำนวนเต็มบวก แล้ว

$$\text{ถ้า} \quad a \equiv b \pmod{m} \quad \text{แล้ว} \quad a^k \equiv b^k \pmod{m}$$

ตัวอย่าง

จงแสดงว่า 41 หาร $2^{20}-1$ ลงตัว

วิธีทำ เนื่องจาก $2^5 \equiv -9 \pmod{41}$ และ $81 \equiv -1 \pmod{41}$ จะได้ว่า

$$\begin{aligned}
(2^5)^4 &\equiv (-9)^4 && \pmod{41} \\
2^{20} &\equiv (81)(81) && \pmod{41} \\
&\equiv (-1)(-1) && \pmod{41} \\
&\equiv 1 && \pmod{41}
\end{aligned}$$

ดังนั้น $41 \mid (2^{20}-1)$

ตัวอย่าง

จงหาเศษที่เกิดจากการหาร

1. 8 หาร 3^{10}

   วิธีทำ เนื่องจาก $3^2 \equiv 1 \pmod 8$ จะได้ว่า

$$\begin{aligned} (3^2)^5 &\equiv 1^4 \pmod 8 \\ 3^{10} &\equiv 1 \pmod 8 \end{aligned}$$

   ดังนั้น 8 หาร 3^{10} เศษเหลือเท่ากับ 1

2. 51 หาร 3^{10}

   วิธีทำ เนื่องจาก $3^5 \equiv -12 \pmod{51}$ จะได้ว่า

$$\begin{aligned} (3^5)^2 &\equiv (-12)^2 \pmod{51} \\ 3^{10} &\equiv 144 \pmod{51} \\ &\equiv 42 \pmod{51} \end{aligned}$$

   ดังนั้น 51 หาร 3^{10} เศษเหลือเท่ากับ 42

ตัวอย่าง

จงหาเลขโดดหลักสุดท้ายของ 3^{4000}

วิธีทำ เนื่องจาก $3^4 \equiv 1 \pmod{10}$ จะได้ว่า

$$\begin{aligned} (3^4)^{1000} &\equiv 1^{1000} \pmod{10} \\ 3^{4000} &\equiv 1 \pmod{10} \end{aligned}$$

ดังนั้นเลขโดดหลักสุดท้ายของ 3^{4000} คือ 1

ตัวอย่าง

จงแสดงว่า $4^n \equiv 1 + 3n \pmod 9$ ทุกจำนวนเต็มบวก n

บทพิสูจน์.

ให้ $P(n)$ แทนข้อความ $4^n \equiv 1 + 3n \pmod 9$ เห็นได้ชัดว่า $4^1 \equiv 1 + 3(1) \pmod 9$
ดังนั้น $P(1)$ เป็นจริง ให้ $k \in \mathbb{N}$ สมมติว่า $P(k)$ เป็นจริง นั่นคือ $4^k \equiv 1 + 3k \pmod 9$ จะได้ว่า

$$\begin{aligned} 4^k \cdot 4 &\equiv 4(1 + 3k) \pmod 9 \\ 4^{k+1} &\equiv 4 + 12k \pmod 9 \end{aligned}$$

เนื่องจาก $12 \equiv 3 \pmod 9$ แล้ว $12k \equiv 3k \pmod 9$ ดังนั้น

$$\begin{aligned} 4^{k+1} &\equiv 4 + 3k \pmod 9 \\ &\equiv 1 + 3(k+1) \pmod 9 \end{aligned}$$

ดังนั้น $P(k+1)$ เป็นจริง โดยหลักอุปนัยเชิงคณิตศาสตร์สรุปได้ว่า

$$4^n \equiv 1 + 3n \pmod 9 \quad \text{ทุกจำนวนเต็มบวก } n$$

Theorem

ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

$$\text{ถ้า } a \equiv b \pmod{m} \text{ แล้ว } gcd(a, m) = gcd(b, m)$$

บทพิสูจน์.

ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก สมมติว่า $a \equiv b \pmod{m}$ จะได้ว่า $m \mid (b - a)$ นั่นคือมีจำนวนเต็ม x ซึ่ง $b - a = mx$ หรือ $b = a + mx$ โดยทฤษฎีบท **??** จะได้ว่า

$$\gcd(b, m) = \gcd(a + mx, m) = \gcd(a, m)$$

□

Theorem

ให้ $a, b, n \in \mathbb{Z}$ และ m เป็นจำนวนเต็มบวก ซึ่ง $d = gcd(m, n)$ จะได้ว่า

$$an \equiv bn \pmod{m} \quad \text{ก็ต่อเมื่อ} \quad a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$$

บทแทรก

ให้ a, b, p เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก จะได้ว่า

1. ถ้า $an \equiv bn \pmod{m}$ และ $\gcd(m, n) = 1$ แล้ว $a \equiv b \pmod{m}$
2. ถ้า $an \equiv bn \pmod{p}$ และ p เป็นจำนวนเฉพาะที่ $p \nmid n$ แล้ว $a \equiv b \pmod{p}$

Theorem

ให้ a, b เป็นจำนวนเต็ม และ m_1, m_2 เป็นจำนวนเต็มบวก จะได้ว่า

1. *ถ้า $a \equiv b \pmod{m_1}$ และ $a \equiv b \pmod{m_2}$ แล้ว $a \equiv b \pmod{\ell cm(m_1, m_2)}$*
2. *ถ้า $a \equiv b \pmod{m_1}$ และ $a \equiv b \pmod{m_2}$ และ $gcd(m_1, m_2) = 1$ แล้ว $a \equiv b \pmod{m_1 m_2}$*

ตัวอย่าง

จงหาเลขโดดสองหลักสุดท้ายของ 3^{4000}

วิธีทำ เนื่องจาก $3^2 \equiv 1 \pmod 4$ และ $3^{20} = (3^5 \cdot 3^5)^2 \equiv [(-7)(-7)]^2 \equiv 1 \pmod{25}$ จะได้ว่า

$$\begin{aligned} 3^{4000} = (3^2)^{2000} &\equiv 1^{2000} \equiv 1 \pmod 4 \\ 3^{4000} = (3^{20})^{200} &\equiv 1^{200} \equiv 1 \pmod{25} \\ \therefore \quad 3^{4000} &\equiv 1 \pmod{100} \end{aligned}$$

ดังนั้นเลขโดดสองหลักสุดท้ายของ 3^{4000} คือ 01

Theorem

ให้ a, b เป็นจำนวนเต็ม และ $m_1, m_2, ..., m_k$ เป็นจำนวนเต็มบวก จะได้ว่า

1. *ถ้า $a \equiv b \pmod{m_i}$ $i = 1, 2, ..., k$ แล้ว $a \equiv b \pmod{\ell cm(m_1, m_2, ..., m_k)}$*
2. *ถ้า $a \equiv b \pmod{m_1}$ และ $m_1, m_2, ..., m_k$ เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ แล้ว $a \equiv b \pmod{m_1 m_2 \cdots m_k}$*

Theorem

ทุก ๆ จำนวนเต็ม a จะมีจำนวนเต็ม r เพียงตัวเดียวที่ $0 \leq r < m$ เมื่อ m เป็นจำนวนเต็มบวก และ

$$a \equiv r \pmod{m}$$

บทนิยาม

ถ้า $a \equiv b \pmod{m}$ จะเรียก b ว่าเป็น**ส่วนตกค้าง (residue)** ของ a มอดุโล m เซตของ

$$\{a_1, a_2, \ldots, a_m\}$$

จะเป็น**ระบบส่วนตกค้างบริบูรณ์ (complete residue system)** มอดุโล m ก็ต่อเมื่อ ทุก ๆ จำนวนเต็ม a จะมี a_i เพียงตัวเดียวที่ทำให้ $a \equiv a_i \pmod{m}$ ชั้นสมมูลของ a_i คือ

$$\{a : a \in \mathbb{Z},\ a \equiv a_i \pmod{m}\}$$

จะเรียกว่า **ชั้นส่วนตกค้าง (residue class)** ของ a_i มอดุโล m

ตัวอย่าง

จงหาส่วนตกค้างของ 5 มอดุโล 7 ทั้งหมดที่เป็นไปได้

วิธีทำ ให้ b เป็นส่วนตกค้างของ 5 มอดุโล 7 ดังนั้น $5 \equiv b \pmod{7}$ สำหรับจำนวนเต็ม k ใด ๆ $b = 5 + 7k$ ดังนั้นส่วนตกค้างของ 5 มอดุโล 7 ทั้งหมดคือ $5 + 7k$ เมื่อ $k \in \mathbb{Z}$ ตัวอย่างเช่น $b = -9, -2, 5, 12, 19, 26$ เป็นส่วนตกค้างของ 5 มอดุโล 7

ตัวอย่าง

จงตรวจสอบว่าจงหาเซตต่อไปนี้ระบบส่วนตกค้างบริบูรณ์มอดุโล 5 หรือไม่

1. $\{-1, 5, 6, 7, 8\}$
   วิธีทำ เนื่องจาก $-1 \equiv 4 \pmod 5$, $5 \equiv 0 \pmod 5$, $6 \equiv 1 \pmod 5$, $7 \equiv 2 \pmod 5$ และ $8 \equiv 3 \pmod 5$ ดังนั้น $\{-1, 5, 6, 7, 8\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5

2. $\{-11, -3, 18, 16, 22\}$
   วิธีทำ เนื่องจาก $-11 \equiv 4 \pmod 5$, $-3 \equiv 2 \pmod 5$, $18 \equiv 3 \pmod 5$, $16 \equiv 1 \pmod 5$ และ $22 \equiv 2 \pmod 5$ ดังนั้น $\{-11, -3, 18, 16, 22\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5

3. $\{8, -2, 6, 12, 1\}$
   วิธีทำ เนื่องจาก $8 \equiv -2 \pmod 5$ ดังนั้น $\{8, -2, 6, 12, 1\}$ ไม่เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 5

บทนิยาม

เราจะเรียกเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

$$\{0, 1, 2, ..., m-1\}$$

ว่า**ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นค่าลบน้อยสุด** (least non-negative complete residue system) มอดุโล m

ตัวอย่างเช่น $\{0, 1, 2, 3, 4, 5, 6\}$ เป็นระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นค่าลบน้อยสุด มอดุโล 7

Theorem

$\{a_1, a_2, ..., a_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m และ $gcd(c, m) = 1$
จะได้ว่า $\{ca_1, ca_2, ..., ca_m\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล m

สมการสมภาค

พิจารณาจำนวนเต็ม x ที่สอดคล้องสมการสมภาค

$$6x \equiv 4 \pmod 8$$

จะได้ว่า $6x = 4 + 8k$ เมื่อ $k \in \mathbb{Z}$ นั่นคือ

$$x = \frac{4+8k}{6} = \frac{2+4k}{3}$$

มีเขียนคำตอบบางส่วน ดังตารางต่อไปนี้

k	x
-11	-14
-5	-6
1	2
7	10
13	18

k	x
-8	-10
-2	-2
4	6
10	14
16	22

สำหรับคำตอบในระบบส่วนตกค้างบริบูรณ์มอดุโล 8 จะได้คำตอบคือ $x = 2, 6$ ซึ่งเรียกว่า**คำตอบที่ไม่สมภาค**

Theorem

ให้ a, b เป็นจำนวนเต็ม และ m จำนวนเต็มบวก และ $gcd(a, m) = d$ จะได้ว่า

$$\text{สมการสมภาคเชิงเส้น} \quad ax \equiv b \pmod{m} \quad \text{มีคำตอบ } x \in \mathbb{Z} \qquad \text{ก็ต่อเมื่อ} \qquad d \mid b$$

ถ้า $d \mid b$ จะมีคำตอบอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล m และคำตอบนั่นคือ

$$x \equiv x_0 + t\frac{m}{d} \pmod{m} \qquad \text{เมื่อ} \quad t = 0, 1, 2, ..., d-1$$

โดยที่ x_0 คือคำตอบหนึ่งของสมการ $\frac{a}{d}x \equiv \frac{b}{d} \left(mod\ \frac{m}{d}\right)$

จากทฤษฎีบท พบว่า

1. ถ้า $d \nmid b$ สมการสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ ไม่มีคำตอบ
2. ถ้า $d \mid b$ สมการสมภาคเชิงเส้น $ax \equiv b \pmod{m}$ มีอยู่ d คำตอบที่ไม่สมภาคกันในมอดุโล m
3. ถ้า $d = 1$ แล้วสมการ $ax \equiv b \pmod{m}$ มีเพียงคำตอบเดียวที่ไม่สมภาคกัน ในมอดุโล m หรือกล่าวได้อีกนัยว่า ถ้า x_1 และ x_2 เป็นคำตอบของสมการ $ax \equiv b \pmod{m}$ แล้ว $x_1 \equiv x_2 \pmod{m}$

ตัวอย่าง

จงหาคำตอบของสมการสมภาคเชิงเส้นต่อไปนี้

1. $9x \equiv 21 \pmod{30}$

   วิธีทำ เนื่องจาก $\gcd(9, 30) = 3$ และ $3 \mid 21$ ดังนั้น $9x \equiv 21 \pmod{30}$ มีคำตอบ หา x_0 จากสมการ $3x \equiv 7 \pmod{10}$ จะได้ $x_0 = 9$ เนื่องจาก $3(9) \equiv 7 \pmod{10}$
   ดังนั้นคำตอบคือ

   $$x \equiv 9 + 10t \pmod{30}$$

   โดยที่ $t = 0, 1, 2$ นั่นคือสมการสมภาคเชิงเส้นจะมีคำตอบคือ

   $$x \equiv 9, 19, 29 \pmod{30}$$

2. $14x \equiv 15 \pmod{28}$

   วิธีทำ เนื่องจาก $\gcd(14, 28) = 7$ และ $7 \nmid 15$ ดังนั้น $14x \equiv 15 \pmod{28}$ ไม่มีคำตอบ

ตัวอย่าง

จงหาคำตอบของสมการสมภาคเชิงเส้น $6x \equiv 21 \pmod{39}$

เนื่องจาก $\gcd(6, 39) = 3$ และ $3 \mid 21$ ดังนั้น $6x \equiv 21 \pmod{39}$ มีคำตอบ หา x_0 จากสมการ $2x \equiv 7 \pmod{13}$ จะได้ $x_0 = 10$ เนื่องจาก $2(10) \equiv 7 \pmod{13}$ ดังนั้นคำตอบคือ

$$x \equiv 10 + 13t \pmod{39}$$

โดยที่ $t = 0, 1, 2$ นั่นคือสมการสมภาคเชิงเส้นจะมีคำตอบคือ

$$x \equiv 10, 23, 36 \pmod{39}$$

ตัวอย่าง

จงหาคำตอบของสมการสมภาคเชิงเส้น $39x \equiv 65 \pmod{52}$

วิธีทำ เนื่องจาก $\gcd(39, 52) = 13$ และ $13 \mid 65$ ดังนั้น $39x \equiv 65 \pmod{52}$ มีคำตอบ หา x_0 จากสมการ $3x \equiv 5 \pmod{4}$ จะได้ $x_0 = 3$ เนื่องจาก $3(3) \equiv 5 \pmod{4}$ ดังนั้นคำตอบคือ

$$x \equiv 3 + 4t \pmod{52}$$

โดยที่ $t = 0, 1, 2, 3, ..., 12$ นั่นคือสมการสมภาคเชิงเส้นจะมีคำตอบคือ

$$x \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51 \pmod{52}$$

ตัวอย่าง

จงหาคำตอบที่ไม่สมภาคกัน ของสมการสมภาคเชิงเส้น $91x \equiv 98 \pmod{119}$

วิธีทำ เนื่องจาก $\gcd(91, 119) = 7$ และ $7 \mid 98$ ดังนั้น $91x \equiv 98 \pmod{119}$ มีคำตอบ หา x_0 จากสมการ $13x \equiv 14 \pmod{17}$ พิจารณา

$$\begin{aligned} 13x &\equiv 14 \pmod{17} \\ -4x &\equiv -3 \pmod{17} \\ 4x &\equiv 3 \pmod{17} \\ 16x &\equiv 12 \pmod{17} \\ -x &\equiv -5 \pmod{17} \\ x &\equiv 5 \pmod{17} \end{aligned}$$

จะได้ $x_0 = 5$ ดังนั้นคำตอบคือ

$$x \equiv 5 + 17t \pmod{119}$$

โดยที่ $t = 0, 1, 2, 3, 4, 5, 6$ นั่นคือสมการสมภาคเชิงเส้นจะมีคำตอบคือ

$$x \equiv 5, 22, 39, 56, 73, 90, 107 \pmod{119}$$

ตัวอย่าง

โรงงานผลิตเสื้อยืดแห่งหนึ่งพบว่าเมื่อแบ่งจำนวนเสื้อยืดคอกลมออกเป็น 102 กอง จะเหลือเสื้อยืดคอกลมจำนวน 12 ตัว ถ้าจำนวนเสื้อยืดคอกลมมีจำนวนเป็น 36 เท่าของเสื้อยืดคอวี พบว่าจำนวนเสื้อยืดคอวีมีมากกว่า 80 ตัว แต่ไม่เกิน 100 ตัว จงหาจำนวนเสื้อยืดคอวีและคอกลม

วิธีทำ ให้ x แทนจำนวนของเสื้อยืดคอวี ดังนั้นจำนวนเสื้อยืดคอกลมคือ $36x$ ตัว และสอดคล้องสมการ

$$36x \equiv 12 \pmod{102}$$

เนื่องจาก $\gcd(36, 102) = 6$ และ $6 \mid 12$ ดังนั้น $36x \equiv 12 \pmod{102}$ มีคำตอบ หา x_0 จากสมการ $6x \equiv 2 \pmod{17}$ พิจารณา

$$\begin{aligned} 6x &\equiv 2 \pmod{17} \\ 18x &\equiv 6 \pmod{17} \\ x &\equiv 6 \pmod{17} \end{aligned}$$

จะได้ $x_0 = 6$ ดังนั้นคำตอบคือ

$$x \equiv 6 + 17t \pmod{102}$$

โดยที่ $t = 0, 1, 2, 3, 4, 5$ นั่นคือสมการสมภาคเชิงเส้นจะมีคำตอบคือ

$$x \equiv 6, 23, 40, 57, 74, 91 \pmod{102}$$

ดังนั้น เสื้อยืดคอวีมีจำนวน 91 ตัว และเสื้อยืดคอกลมมีจำนวน 3276 ตัว

ทฤษฎีบทเศษเหลือของจีน

คำถามหนึ่งที่มักได้ยินบ่อยครั้งในเรื่องการหารคือ มีจำนวนเต็มอะไรเมื่อหารด้วย 4 เศษเหลือเป็น 3 และหารด้วย 5 เศษเหลือเป็น 4 คำถามนี้คือจำนวนเต็ม x ที่สอดคล้องระบบสมการสมภาค

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

นั่นคือต้องหา x ที่สอดคล้อง $x = 3 + 4t$ และ $x = 4 + 5s$ เมื่อ $t, s \in \mathbb{Z}$ เมื่อพิจารณาแล้วจะได้ $x = 79$ เมื่อ $t = 19$ และ $s = 15$ ให้ z เป็นคำตอบของระบบสมการจะได้ว่า

$$z \equiv 79 \pmod 4 \qquad \text{และ} \qquad z \equiv 79 \pmod 5$$

เนื่องจาก $\gcd(4, 5) = 1$ ดังนั้น $z \equiv 79 \pmod{20}$ คำตอบของระบบสมการนี้คือ

$$79 + 20k, \qquad k \in \mathbb{Z}$$

พิจารณาระบบสมการสมภาค

$$\begin{aligned} nx &\equiv 1 \pmod{m} \\ mx &\equiv 1 \pmod{n} \end{aligned}$$

ให้ $m, n \in \mathbb{N}$ และ $\gcd(m, n) = 1$ ขั้นแรกให้ x_1 และ x_2 เป็นคำของระบบสมการ $nx \equiv 1 \pmod{m}$ และ $mx \equiv 1 \pmod{n}$ ตามลำดับ สำหรับทุก ๆ จำนวนเต็ม a, b จะได้ว่า

$$\begin{aligned} nx_1 a &\equiv a \pmod{m} \\ mx_2 b &\equiv b \pmod{n} \end{aligned}$$

นั่นคือ $x_1 a$ และ $x_2 b$ เป็นคำตอบของระบบสมการ

$$\begin{aligned} nx &\equiv a \pmod{m} \\ mx &\equiv b \pmod{n} \end{aligned}$$

ให้ $x_0 = nx_1 a + mx_2 b$ จะได้ว่า

$$x_0 = nx_1 a + mx_2 b \equiv nx_1 a + 0 \equiv a \pmod{m}$$

$$x_0 = nx_1 a + mx_2 b \equiv 0 + mx_2 b \equiv b \pmod{n}$$

นี้คือการแสดงว่า $x_0 = nx_1a + mx_2b$ เป็นคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Theorem

ให้ $m, n \in \mathbb{N}$ และ $gcd(m, n) = 1$ จะได้ว่าระบบสมการ

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล mn กล่าวคือ จะมี $x_0 \in \mathbb{Z}$ ซึ่ง $x_0 \equiv a \pmod{m}$ และ $x_0 \equiv b \pmod{n}$ และถ้า x_1 และ x_2 เป็นคำตอบของระบบแล้ว $x_1 \equiv x_2 \pmod{mn}$

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 5 \pmod 9 \end{aligned}$$

วิธีทำ เห็นได้ว่า $\gcd(7,9) = 1$ ให้ $a = 2, b = 5, m = 7, n = 9$ พิจารณาระบบสมการ

$$\begin{aligned} 9x &\equiv 1 \pmod 7 \\ 7x &\equiv 1 \pmod 9 \end{aligned}$$

จะได้ว่า $x_1 = 4$ และ $x_2 = 4$ เป็นคำของระบบสมการ $9x \equiv 1 \pmod 7$ และ $7x \equiv 1 \pmod 9$ ตามลำดับ แล้ว

$$x_0 = nx_1a + mx_2b = 9(4)(2) + 7(4)(5) = 212$$

ดังนั้นคำตอบของระบบสมการนี้คือ $x \equiv 212 \equiv 23 \pmod{63}$ นั่นคือ

$$23 + 63t, \qquad t \in \mathbb{Z}$$

ตัวอย่าง

จงหาจำนวนเต็มเมื่อหารด้วย 6 เศษเหลือเท่ากับ 3 หารด้วย 11 เศษเหลือเท่ากับ 5

วิธีทำ ให้ x เป็นจำนวนเต็มที่สอดคล้องระบบสมการ

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

เห็นได้ว่า $\gcd(6,11)=1$ ให้ $a=3, b=5, m=6, n=11$ พิจารณาระบบสมการ

$$\begin{aligned} 11x &\equiv 1 \pmod 6 \\ 6x &\equiv 1 \pmod{11} \end{aligned}$$

จะได้ว่า $x_1=5$ และ $x_2=2$ เป็นคำของระบบสมการ $11x\equiv 1 \pmod 6$ และ $6x\equiv 1 \pmod{11}$ ตามลำดับแล้ว

$$x_0 = nx_1a + mx_2b = 11(5)(3) + 6(2)(5) = 225$$

ดังนั้นคำตอบของระบบสมการนี้คือ $x\equiv 225 \equiv 27 \pmod{66}$ นั่นคือ

$$27+66t, \qquad t\in\mathbb{Z}$$

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} 2x &\equiv 1 \pmod{5} \\ 3x &\equiv 5 \pmod{11} \end{aligned}$$

วิธีทำ พิจารณา

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

และ

$$\begin{aligned} 3x &\equiv 5 \pmod{11} \\ 12x &\equiv 20 \pmod{11} \\ x &\equiv 9 \pmod{11} \end{aligned}$$

ดังนั้นคำตอบ x จะสอดคล้องระบบสมการ

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 9 \pmod{11} \end{aligned}$$

เห็นได้ว่า $\gcd(5,11)=1$ ให้ $a=3, b=9, m=5, n=11$ พิจารณาระบบสมการ

$$\begin{aligned} 11x &\equiv 1 \pmod 5 \\ 5x &\equiv 1 \pmod{11} \end{aligned}$$

จะได้ว่า $x_1=1$ และ $x_2=9$ เป็นคำของระบบสมการ $11x\equiv 1 \pmod 5$ และ $5x\equiv 1 \pmod{11}$ ตามลำดับแล้ว

$$x_0 = nx_1a + mx_2b = 11(1)(3) + 5(9)(9) = 438$$

ดังนั้นคำตอบของระบบสมการนี้คือ $x\equiv 438\equiv 53 \pmod{55}$ นั่นคือ

$$53+55t, \qquad t\in\mathbb{Z}$$

ต่อไปจะพิจารณาในระบบสมการที่มากกว่า 2 สมการ เช่นจงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \end{aligned}$$

เมื่อ $\gcd(m_1, m_2) = \gcd(m_1, m_3) = \gcd(m_2, m_3) = 1$

ให้ $x_0 = m_2 m_3 x_1 a_1 + m_1 m_3 x_2 a_2 + m_1 m_2 x_3 a_3$ สำหรับจำนวนเต็ม x_1, x_2, x_3 ใด ๆ จะได้ว่า

$$\begin{aligned} x_0 &\equiv m_2 m_3 x_1 a_1 + 0 + 0 \pmod{m_1} \\ x_0 &\equiv 0 + m_1 m_3 x_2 a_2 + 0 \pmod{m_2} \\ x_0 &\equiv 0 + 0 + m_1 m_2 x_3 a_3 \pmod{m_3} \end{aligned}$$

ในการหาคำตอบของระบบสมการข้างต้นเลือก x_1, x_2, x_3 ที่สอดคล้องสมการ

$$\begin{aligned} m_2 m_3 x &\equiv a_1 \pmod{m_1} \\ m_1 m_3 x &\equiv a_2 \pmod{m_2} \\ m_1 m_2 x &\equiv a_3 \pmod{m_3} \end{aligned}$$

ถ้า x_1, x_2 เป็นคำตอบของระบบสมการ จะได้ว่า $x_1 \equiv x_2 \pmod{m_1 m_2 m_3}$

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 5 \pmod 4 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

วิธีทำ เห็นได้ว่า $\gcd(3,4) = \gcd(3,7) = \gcd(4,7) = 1$

ให้ $a_1 = 2, a_2 = 5, a_3 = 4, m_1 = 3, m_2 = 4, m_3 = 7$ พิจารณาระบบสมการ

$$\begin{aligned} 4(7)x &= 28x = x \equiv 1 \pmod 3 \quad \ldots \quad (1) \\ 3(7)x &= 21x = x \equiv 1 \pmod 4 \quad \ldots \quad (2) \\ 3(4)x &= 12x = 5x \equiv 1 \pmod 7 \quad \ldots \quad (3) \end{aligned}$$

จะได้ว่า $x_1 = 1, x_2 = 1$ และ $x_3 = 3$ เป็นคำของระบบสมการ (1), (2) และ (3) ตามลำดับ แล้ว

$$\begin{aligned} x_0 &= m_2 m_3 x_1 a_1 + m_1 m_3 x_2 a_2 + m_1 m_2 x_3 a_3 \\ &= 4(7)(1)(2) + 3(7)(1)(5) + 3(4)(3)(4) \\ &= 56 + 105 + 144 \\ &= 305 \end{aligned}$$

ดังนั้นคำตอบของระบบสมการนี้คือ $x \equiv 305 \equiv 53 \pmod{84}$ นั่นคือ

$$53 + 84t, \qquad t \in \mathbb{Z}$$

Theorem

ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)

ให้ $m_1, m_2, ..., m_k$ *เป็นจำนวนเต็มบวกซึ่ง* $gcd(m_i, m_j) = 1$ *สำหรับ* $i \neq j$

จะได้ว่าระบบสมการสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

มีคำตอบของระบบสมการเพียงคำตอบเดียวในมอดุโล $m = m_1 m_2 m_3 ... m_k$ *กล่าวคือจะมี* $x_0 \in \mathbb{Z}$ *ซึ่ง* $x_0 \equiv a_i \pmod{m_i}$ *ทุก* $i = 1, 2, ..., k$ *ถ้า* x_1 *และ* x_2 *เป็นคำตอบของสมการ* $x_1 \equiv x_2 \pmod{m}$

ตัวอย่าง

จงหาคำตอบของสมการสมภาค $17x \equiv 9 \pmod{276}$

วิธีทำ เนื่องจาก $276 = 3 \cdot 4 \cdot 23$ ดังนั้น x เป็นจำนวนเต็มที่สอดคล้องระบบสมการ

$$\begin{aligned} 17x &\equiv 9 \pmod{3} \longrightarrow 2x \equiv 0 \pmod{3} \\ 17x &\equiv 9 \pmod{4} \longrightarrow x \equiv 1 \pmod{4} \\ 17x &\equiv 9 \pmod{23} \longrightarrow 17x \equiv 9 \pmod{23} \end{aligned}$$

จะสอดคล้องสมการ $17x \equiv 9 \pmod{276}$ พิจารณา

$$\begin{aligned} 2x &\equiv 0 \pmod{3} \\ 10x &\equiv 0 \pmod{3} \\ x &\equiv 0 \pmod{0} \end{aligned}$$

และ

$$\begin{aligned} 17x &\equiv 9 \pmod{23} \\ -6x &\equiv 9 \pmod{23} \\ 24x &\equiv -36 \pmod{23} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

ดังนั้นหาคำตอบจากระบบสมการสมภาค

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 10 \pmod{23} \end{aligned}$$

เห็นได้ว่า $\gcd(3,4) = \gcd(3,23) = \gcd(3,23) = 1$

ให้ $a_1 = 0, a_2 = 1, a_3 = 10, m_1 = 3, m_2 = 4, m_3 = 23$ พิจารณาระบบสมการ

$$\begin{aligned} 4(23)x &= 92x = 2x \equiv 1 \pmod 3 \quad \ldots \quad (1) \\ 3(23)x &= 69x = x \equiv 1 \pmod 4 \quad \ldots \quad (2) \\ 3(4)x &= 12x = 12x \equiv 1 \pmod{23} \quad \ldots \quad (3) \end{aligned}$$

จะได้ว่า $x_1 = 2, x_2 = 1$ และ $x_3 = 2$ เป็นคำของระบบสมการ (1), (2) และ (3) ตามลำดับ แล้ว

$$\begin{aligned} x_0 &= m_2 m_3 x_1 a_1 + m_1 m_3 x_2 a_2 + m_1 m_2 x_3 a_3 \\ &= 4(23)(2)(0) + 3(23)(1)(1) + 3(4)(2)(10) \\ &= 0 + 69 + 240 \\ &= 309 \end{aligned}$$

จะได้ว่าคำตอบของระบบสมการนี้คือ $x \equiv 309 \equiv 33 \pmod{276}$ นั่นคือ

$$33 + 276t, \quad t \in \mathbb{Z}$$

สรุปได้ว่าเป็นคำตอบของสมการ $17x \equiv 9 \pmod{276}$

Theorem

ให้ m_1, m_2 *เป็นจำนวนเต็มบวกและ* $a_1, a_2 \in \mathbb{Z}$ *จะได้ระบบสมการสมภาค*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

มีคำตอบ ก็ต่อเมื่อ $gcd(m_1, m_2) \mid (a_1 - a_2)$

และถ้ามีคำตอบแล้ว จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $m = \ell cm(m_1, m_2)$

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 11 \pmod{16} \\ x &\equiv 5 \pmod{20} \end{aligned}$$

วิธีทำ เนื่องจาก $\gcd(16, 20) = 4$ และ $4 \nmid (11 - 5)$ ดังนั้นระบบสมการนี้ไม่มีคำตอบ

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 13 \pmod{15} \\ x &\equiv 7 \pmod{21} \end{aligned}$$

วิธีทำ จะเห็นว่า $\gcd(15, 21) = 3$ และ $3 \mid (13 - 7)$ ดังนั้นระบบสมการนี้มีคำตอบ

จาก $x \equiv 13 \pmod{15}$ มีคำตอบเดียวกับระบบคำตอบของสมการ

$$\begin{aligned} x &\equiv 13 \pmod{3} \longrightarrow x \equiv 1 \pmod{3} \\ x &\equiv 13 \pmod{5} \longrightarrow x \equiv 3 \pmod{5} \end{aligned}$$

จาก $x \equiv 7 \pmod{21}$ มีคำตอบเดียวกับระบบคำตอบของสมการ

$$\begin{aligned} x &\equiv 7 \pmod{3} \longrightarrow x \equiv 1 \pmod{3} \\ x &\equiv 7 \pmod{7} \longrightarrow x \equiv 0 \pmod{7} \end{aligned}$$

ดังนั้นคำตอบของระบบสมการนี้จะสอดคล้องระบบสมการ

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 0 \pmod 7 \end{aligned}$$

ให้ $a_1 = 1, a_2 = 3, a_3 = 0, m_1 = 3, m_2 = 5, m_3 = 7$ พิจารณาระบบสมการ

$$\begin{aligned} 5(7)x &= 35x = 2x \equiv 1 \pmod 3 \quad \ldots \quad (1) \\ 3(7)x &= 21x = x \equiv 1 \pmod 5 \quad \ldots \quad (2) \\ 3(5)x &= 15x = x \equiv 1 \pmod 7 \quad \ldots \quad (3) \end{aligned}$$

จะได้ว่า $x_1 = 2, x_2 = 1$ และ $x_3 = 1$ เป็นคำของระบบสมการ (1), (2) และ (3) ตามลำดับ แล้ว

$$\begin{aligned} x_0 &= m_2 m_3 x_1 a_1 + m_1 m_3 x_2 a_2 + m_1 m_2 x_3 a_3 \\ &= 5(7)(2)(1) + 3(7)(1)(3) + 3(5)(1)(0) \\ &= 70 + 63 + 0 \\ &= 133 \end{aligned}$$

จะได้ว่าคำตอบของระบบสมการนี้คือ $x \equiv 133 \equiv 28 \pmod{105}$ นั่นคือ

$$28 + 105t, \quad t \in \mathbb{Z}$$

Theorem

ให้ $m_1, m_2, \ldots, m_k$ *เป็นจำนวนเต็มบวกและ* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$

จะได้ว่าระบบสมการสมภาค

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

มีคำตอบ ก็ต่อเมื่อ $\gcd(m_i, m_j) \mid (a_i - a_j)$ *สำหรับทุก* $i, j \in \{1, 2, \ldots, k\}$

และถ้ามีคำตอบแล้ว จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $\ell cm(m_1, m_2, \ldots, m_k)$

ตัวอย่าง

จงหาคำตอบของระบบสมการ

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 17 \pmod{21} \\ x &\equiv 3 \pmod{28} \end{aligned}$$

วิธีทำ เนื่องจาก $\gcd(6, 21) = 3$ ซึ่ง $3 \mid (17 - 5)$, $\gcd(6, 28) = 2$ ซึ่ง $2 \mid (5 - 3)$
และ $\gcd(21, 28) = 7$ ซึ่ง $7 \mid (17 - 3)$ ดังนั้นระบบสมการนี้มีคำตอบ
จาก $x \equiv 5 \pmod 6$ มีคำตอบเดียวกับระบบคำตอบของสมการ

$$\begin{aligned} x &\equiv 5 \pmod 2 \longrightarrow x \equiv 1 \pmod 2 \\ x &\equiv 5 \pmod 3 \longrightarrow x \equiv 2 \pmod 3 \end{aligned}$$

จาก $x \equiv 17 \pmod{21}$ มีคำตอบเดียวกับระบบคำตอบของสมการ

$$\begin{aligned} x &\equiv 17 \pmod 3 \longrightarrow x \equiv 2 \pmod 3 \\ x &\equiv 17 \pmod 7 \longrightarrow x \equiv 3 \pmod 7 \end{aligned}$$

จาก $x \equiv 3 \pmod{28}$ มีคำตอบเดียวกับระบบคำตอบของสมการ

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

เนื่องจากคำของสมการ $x \equiv 3 \pmod 4$ จะเป็นคำตอบของสมการ $x \equiv 1 \pmod 2$ ดังนั้นคำตอบของระบบสมการนี้จะสอดคล้องระบบสมการ

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

ให้ $a_1 = 2, a_2 = 3, a_3 = 3, m_1 = 3, m_2 = 4, m_3 = 7$ พิจารณาระบบสมการ

$$\begin{aligned} 4(7)x &= 28x = x \equiv 1 \pmod 3 \quad \ldots \quad (1) \\ 3(7)x &= 21x = x \equiv 1 \pmod 4 \quad \ldots \quad (2) \\ 3(4)x &= 12x = 5x \equiv 1 \pmod 7 \quad \ldots \quad (3) \end{aligned}$$

จะได้ว่า $x_1 = 1, x_2 = 1$ และ $x_3 = 3$ เป็นคำของระบบสมการ (1), (2) และ (3) ตามลำดับ แล้ว

$$\begin{aligned} x_0 &= m_2 m_3 x_1 a_1 + m_1 m_3 x_2 a_2 + m_1 m_2 x_3 a_3 \\ &= 4(7)(1)(2) + 3(7)(1)(3) + 3(4)(3)(3) \\ &= 56 + 63 + 108 \\ &= 227 \end{aligned}$$

จะได้ว่าคำตอบของระบบสมการนี้คือ $x \equiv 227 \equiv 59 \pmod{84}$ นั่นคือ

$$59 + 84t, \quad t \in \mathbb{Z}$$

ระบบส่วนตกค้างลดทอน

บทนิยาม

ระบบส่วนตกค้างลดทอน (reduced residue system) มอดุโล m คือเซตของจำนวนเต็มในระบบส่วนตกค้างบริบูรณ์ที่เป็นจำนวนเฉพาะสัมพัทธ์กับ m

(ก) ระบบส่วนตกค้างลดทอนมอดุโล m ที่ได้จากระบบส่วนตกค้างบริบูรณ์ $\{0, 1, 2, ..., m-1\}$ คือ

$$\{k : 0 \leq k < m \text{ และ } \gcd(k, m) = 1\}$$

เรียกว่า **ระบบส่วนตกค้างลดทอนที่ไม่เป็นลบค่าน้อยสุด** (least non-negative reduced residue system) มอดุโล m

(ข) $\phi(m)$ แทนจำนวนสมาชิกของระบบส่วนตกค้างลดทอนมอดุโล m

ข้อสังเกต

จากนิยามข้างต้นจะได้ว่า

1. เซตของจำนวนเต็ม r_i เป็นระบบส่วนตกค้างลดทอนมอดุโล m ก็ต่อเมื่อ
   (1) $\gcd(r_i, m) = 1$ ทุก ๆ r_i
   (2) ถ้า $i \neq j$ แล้ว $r_i \not\equiv r_j \pmod{m}$
   (3) ถ้า $x \in \mathbb{Z}$ ที่ $\gcd(x, m) = 1$ แล้วมี r_i ที่ $x \equiv r_i \pmod{m}$
2. ระบบส่วนตกค้างลดทอนมอดุโล m ทุกระบบมีจำนวนสมาชิกเท่ากัน
3. $\phi(p) = p - 1$ เมื่อ p เป็นจำนวนเฉพาะ

ตัวอย่าง

จงยกตัวอย่างระบบส่วนตกค้างลดทอนมอดุโล 5 และ 8 มาอย่างน้อย 2 ระบบ

วิธีทำ แสดงได้ดังตารางต่อไปนี้

มอดุโล m	ระบบส่วนตกค้างบริบูรณ์	ระบบส่วนตกค้างลดทอนมอดุโล m
5	$\{0,1,2,3,4\}$	$\{1,2,3,4\}$
	$\{8,-1,11,-15,7\}$	$\{8,-1,11,7\}$
8	$\{0,1,2,3,4,5,6,7\}$	$\{1,3,5,7\}$
	$\{8,-1,14,5,12,-5,10,1\}$	$\{-1,5,-5,1\}$

Theorem

ถ้า $\{a_1, a_2, ..., a_{\phi(m)}\}$ *เป็นเซตของจำนวนเต็มซึ่งทุก ๆ* i, $gcd(a_i, m) = 1$ *และ ทุก ๆ* $i \neq j$, $a_i \not\equiv a_j \pmod{m}$ *แล้ว* $\{a_1, a_2, ..., a_{\phi(m)}\}$ *เป็นระบบส่วนตกค้างลดทอนมอดุโล* m

บทพิสูจน์.

สมมติว่า $\{a_1, a_2, ..., a_{\phi(m)}\}$ เป็นเซตของจำนวนเต็มซึ่งทุก ๆ i, $\gcd(a_i, m) = 1$ และทุก ๆ $i \neq j$, $a_i \not\equiv a_j \pmod{m}$ ให้ r_i เป็นเศษเหลือจากการหาร a_i ด้วย m ดังนั้น $a_i \equiv r_i \pmod{m}$ และ $\gcd(r_i, m) = 1$ แสดงว่า

$$\{r_1, r_2, ..., r_{\phi(m)}\} \subseteq \{0, 1, 2, ..., m-1\}$$

และมีสมาชิก $\phi(m)$ ตัว ดังนั้น $\{r_1, r_2, ..., r_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m ที่ไม่เป็นลบค่าน้อยสุด ให้ a เป็นจำนวนเต็มใด ๆ $\gcd(a, m) = 1$ และให้ r เป็นเศษเหลือจากการหาร a ด้วย m ทำให้ได้ว่า $a \equiv r \pmod{m}$ และ $\gcd(r, m) = 1$ ดังนั้นจะมี i ซึ่ง $r = i_i$ นั่นคือ

$$a \equiv r = r \equiv a_i \pmod{m}$$

สรุปได้ว่า $\{a_1, a_2, ..., a_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m □

Theorem

ให้ $gcd(a, m) = 1$ *และ* $\{r_1, r_2, ..., r_{\phi(m)}\}$ *เป็นระบบส่วนตกค้างลดทอนมอดุโล* m *จะได้ว่า*

$$\{ar_1, ar_2, ..., ar_{\phi(m)}\}$$

เป็นระบบส่วนตกค้างลดทอนมอดุโล m

บทพิสูจน์.

ให้ $\gcd(a, m) = 1$ สมมติ $\{r_1, r_2, ..., r_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m เนื่องจาก $\gcd(a, m) = 1$ และ $\gcd(r_i, m) = 1$ จะได้ $\gcd(ar_i, m) = 1$ โดยทฤษฎีบท 12 เพียงพอที่จะแสดงว่าแต่ละคู่ไม่สมภาคกัน สมมติว่า $ar_i \equiv ar_j \pmod{m}$ เนื่องจาก $\gcd(a, m) = 1$ จะได้ $r_i \equiv r_j \pmod{m}$ ฉะนั้น $r_i = r_j$ □

Theorem

ทฤษฎีบทของออยเลอร์ (Euler's Theorem)

ถ้า $a \in \mathbb{Z}$ *และ* $m \in \mathbb{N}$ *ซึ่ง* $gcd(a, m) = 1$ *แล้ว*

$$a^{\phi(m)} \equiv 1 \ (mod\ m)$$

บทพิสูจน์.

ให้ $a \in \mathbb{Z}$ และ $m \in \mathbb{N}$ ซึ่ง $\gcd(a, m) = 1$ ให้ $\{r_1, r_2, ..., r_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m จะได้ว่า $\{ar_1, ar_2, ..., ar_{\phi(m)}\}$ เป็นระบบส่วนตกค้างลดทอนมอดุโล m ดังนั้น

$$\begin{aligned} ar_1 \cdot ar_2 \cdot ... \cdot ar_{\phi(m)} &\equiv r_1 r_2 ... r_{\phi(m)} \pmod{m} \\ a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} &\equiv r_1 r_2 ... r_{\phi(m)} \pmod{m} \end{aligned}$$

เนื่องจาก $\gcd(m, r_i) = 1$ ทุก ๆ i จะได้ว่า $\gcd(r_1 r_2 ... r_{\phi(m)}, m) = 1$ สรุปได้ว่า $a^{\phi(n)} \equiv 1 \pmod{n}$ □

ตัวอย่าง

100 หาร 3^{256} มีเศษเหลือเท่าใด

วิธีทำ เนื่องจาก $\gcd(100, 3) = 1$ และ $\phi(100) = 40$ โดยทฤษฎีบทของออยเลอร์จะได้

$$\begin{aligned} 3^{40} &\equiv 1 \pmod{100} \\ 3^{240} = (3^{40})^6 &\equiv 1^6 \pmod{100} \\ 3^{240} &\equiv 1 \pmod{100} \end{aligned}$$

เนื่องจาก $3^4 = 81 \equiv -19 \pmod{100}$ ดังนั้น

$$\begin{aligned} (3^4)^4 &\equiv (-19)^4 \pmod{100} \\ 3^{16} &\equiv (-19)^2(-19)^2 \pmod{100} \\ &\equiv (361)(361) \pmod{100} \\ &\equiv (61)(61) \pmod{100} \\ &\equiv 3721 \pmod{100} \\ &\equiv 21 \pmod{100} \end{aligned}$$

ทำให้ได้ว่า

$$\begin{aligned} 3^{240} \cdot 3^{16} &\equiv 1 \cdot 21 \pmod{100} \\ 3^{256} \cdot 3^{16} &\equiv 21 \pmod{100} \end{aligned}$$

สรุปได้ว่า 100 หาร 3^{256} เศษเหลือเท่ากับ 21

ตัวอย่าง

จงหาเลขโดดสามหลักสุดท้ายของ 7^{10000}

วิธีทำ เนื่องจาก $\gcd(1000, 7) = 1$ และ $\phi(1000) = 400$ โดยทฤษฎีบทของออยเลอร์จะได้

$$\begin{aligned} 7^{400} &\equiv 1 \pmod{1000} \\ (7^{400})^{25} &\equiv 1^{25} \pmod{1000} \\ 7^{10000} &\equiv 1 \pmod{1000} \end{aligned}$$

สรุปได้ว่า เลขโดดสามหลักสุดท้ายของ 7^{10000} คือ 001

บทแทรก

ทฤษฎีบทของแฟร์มาต์ (Fermat's Little Theorem)
ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ โดยที่ $p \nmid a$ แล้ว

$$a^{p-1} \equiv 1 \pmod{p}$$

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหาร 3^{1000} ด้วย 17

วิธีทำ เนื่องจาก 17 เป็นจำนวนเฉพาะซึ่ง $17 \nmid 3$ โดยทฤษฎีบทของแฟร์มาต์จะได้

$$\begin{aligned}
3^{17-1} = 3^{16} &\equiv 1 && \pmod{17} \\
3^{992} = (3^{16})^{62} &\equiv 1^{62} = 1 && \pmod{17} \\
3^{1000} = 3^{992} \cdot 3^{8} &\equiv 1 \cdot 3^{8} && \pmod{17} \\
&\equiv 3^{4} \cdot 3^{4} && \pmod{17} \\
&\equiv (81)(81) && \pmod{17} \\
&\equiv (-4)(-4) && \pmod{17} \\
&\equiv 16 && \pmod{17}
\end{aligned}$$

Theorem

ทฤษฎีบทของวิลสัน (Wilson's Theorem)

ให้ p เป็นจำนวนเฉพาะ จะได้

$$(p-1)! \equiv -1 \ (mod\ p)$$

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหาร $15!$ ด้วย 17

วิธีทำ เนื่องจาก 17 เป็นจำนวนเฉพาะ โดยทฤษฎีบทของวิลสันจะได้ว่า $16! \equiv -1 \pmod{17}$ ดังนั้น

$$\begin{aligned} 16 \cdot 15! &\equiv -1 \pmod{17} \\ (-1) \cdot 15! &\equiv -1 \pmod{17} \\ 15! &\equiv 1 \pmod{17} \end{aligned}$$

สรุปได้ว่า เศษเหลือที่เกิดจากการหาร $15!$ ด้วย 17 คือ 1

ตัวอย่าง

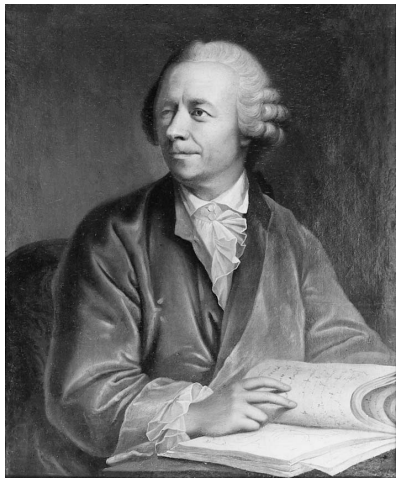
จงหาเศษเหลือที่เกิดจากการหาร $2(26)!$ ด้วย 29

วิธีทำ เนื่องจาก 29 เป็นจำนวนเฉพาะ โดยทฤษฎีบทของวิลสันจะได้ว่า $28! \equiv -1 \pmod{29}$ ดังนั้น

$$\begin{aligned} 28 \cdot 27 \cdot 26! &\equiv -1 \pmod{29} \\ (-1)(-2) \cdot 26! &\equiv -1 \pmod{29} \\ 2(26!) &\equiv 1 \pmod{29} \end{aligned}$$

สรุปได้ว่า เศษเหลือที่เกิดจากการหาร $2(26!)$ ด้วย 29 คือ -1

บทที่ 6 ฟังก์ชันเลขคณิต



ฟังก์ชันเลขคณิต

บทนิยาม

ฟังก์ชันที่มีโดเมนเป็นเซตของจำนวนเต็มบวก และเรจน์เป็นสับเซตของจำนวนเชิงซ้อน เรียกว่า **ฟังก์ชันเลขคณิต**

ตัวอย่างฟังก์ชันเลขคณิต

1. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 2n$
2. $f : \mathbb{N} \to \mathbb{C}$ กำหนดโดย $f(n) = n + i$
3. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) =$ จำนวนตัวประกอบที่เป็นจำนวนเฉพาะของ n

ตัวอย่างฟังก์ชันที่ไม่เป็นฟังก์ชันเลขคณิต

1. $f : \mathbb{C} \to \mathbb{R}$ กำหนดโดย $f(x) = |x|$
2. $f : \mathbb{Z} \to \mathbb{R}$ กำหนดโดย $f(n) = n^2$

ตัวอย่าง

ให้ $\lambda : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย

$$\lambda(n) = \begin{cases} 1 & \text{เมื่อ } n = 1 \\ (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k} & \text{เมื่อ } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \text{ (รูปแบบบัญญัติ)} \end{cases}$$

เรียกว่า ฟังก์ชันลีอูวิลล์ (Liouville's λ–function) จงหา $\lambda(2), \lambda(6)$ และ $\lambda(12)$

1. $\lambda(2) = (-1)^1 = -1$
2. $\lambda(6) = \lambda(2 \cdot 3) = (-1)^{1+1} = 1$
3. $\lambda(12) = \lambda(2^2 \cdot 3) = (-1)^{2+1} = -1$

ตัวอย่าง

ให้ $\Lambda : \mathbb{N} \to \mathbb{R}$ กำหนดโดย

$$\Lambda(n) = \begin{cases} \log p & \text{ถ้า } n = p^a \text{ เมื่อ } p \text{ เป็นจำนวนเฉพาะ และ } a \in \mathbb{N} \\ 0 & \text{ถ้า } n \text{ เป็นอย่างอื่น} \end{cases}$$

เรียกว่า ฟังก์ชันมานเกอลท์ (Mangoldt's function) จงหา $\Lambda(2), \Lambda(6)$ และ $\Lambda(9)$

1. $\Lambda(2) = \log 2$
2. $\Lambda(6) = \Lambda(2 \cdot 3) = 0$
3. $\Lambda(9) = \Lambda(3^2) = \log 3$

ตัวอย่าง

ให้ $\mu : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย

$$\mu(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ 0 & \text{ถ้ามีจำนวนเฉพาะ } p \text{ ซึ่ง } p^2 \mid n \\ (-1)^k & \text{ถ้า } n = p_1 p_2 \cdots p_k \text{ เมื่อ } p_i \text{ เป็นจำนวนเฉพาะที่แตกต่างกัน} \end{cases}$$

เรียกว่า ฟังก์ชันเมอบิอุส (Mobius function) จงหา $\mu(2), \mu(6), \mu(9)$ และ $\mu(105)$

1. $\mu(2) = (-1)^1 = -1$
2. $\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$
3. $\mu(9) = \mu(3^2) = 0$
4. $\mu(105) = \mu(3 \cdot 5 \cdot 7) = (-1)^3 = -1$

ฟังก์ชันเชิงการคูณ

บทนิยาม

ฟังก์ชันเลขคณิต f จะเรียกว่า **ฟังก์ชันเชิงการคูณ** (multiplicative function) ก็ต่อเมื่อ

$$f(mn) = f(n)f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m \text{ และ } \gcd(m, n) = 1$$

และเรียกว่า **ฟังก์ชันเชิงการคูณแบบบริบูรณ์** (completely multiplicative function) ก็ต่อเมื่อ

$$f(mn) = f(n)f(m) \qquad \text{สำหรับทุกจำนวนเต็ม } n, m$$

ตัวอย่าง

จงตรวจสอบฟังก์ชันเลขคณิตต่อไปนี้ว่าเป็นฟังก์ชันเชิงการคูณ และ/หรือ ฟังก์ชันเชิงการคูณแบบบริบูรณ์

1. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = 0$
   วิธีทำ ให้ $n, m \in \mathbb{N}$ จะได้ว่า
   $$f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$$
   ดังนั้น f ฟังก์ชันเชิงการคูณแบบบริบูรณ์

2. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n$
   วิธีทำ ให้ $n, m \in \mathbb{N}$ จะได้ว่า
   $$f(mn) = mn = f(m)f(n)$$
   ดังนั้น f ฟังก์ชันเชิงการคูณแบบบริบูรณ์

3. $f : \mathbb{N} \to \mathbb{Z}$ กำหนดโดย $f(n) = n^2$
   วิธีทำ ให้ $n, m \in \mathbb{N}$ จะได้ว่า
   $$f(mn) = (mn)^2 = m^2 n^2 = f(m)f(n)$$
   ดังนั้น f ฟังก์ชันเชิงการคูณแบบบริบูรณ์

4. $f : \mathbb{N} \to \mathbb{C}$ กำหนดโดย $f(n) = n + i$
   วิธีทำ เลือก $m = 2$ และ $n = 3$ ซึ่ง $\gcd(m, n) = 1$ และ
   $$f(2 \cdot 3) = f(6) = 6 + i \neq 5 + 5i = (2 + i)(3 + i) = f(2)f(3)$$

Theorem

ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ แล้ว

$$f \text{ เป็นฟังก์ชันเชิงการคูณ} \quad \text{ก็ต่อเมื่อ} \quad f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f(p_k^{\alpha_k})$$

Theorem

ให้ f เป็นฟังก์ชันเลขคณิต โดยที่ $f(1) = 1$ และ $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ จะได้ว่า f เป็นฟังก์ชันเชิงการคูณแบบบริบูรณ์ ก็ต่อเมื่อ

$$f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \ldots f(p_k)^{\alpha_k}$$

บทแทรก

ให้ f เป็นฟังก์ชันเชิงการคูณ โดยที่ $f(1) = 1$ และ $n \in \mathbb{N}$ จะได้ว่า f เป็นฟังก์ชันเชิงการคูณแบบบริบูรณ์ ก็ต่อเมื่อ

$$f(p^m) = (f(p))^m \text{ เมื่อ } p \text{ เป็นจำนวนเฉพาะที่ } p \mid n \text{ และ } m \in \mathbb{N}$$

ต่อไปจะกล่าวถึงสัญลักษณ์แทนการบวกของฟังก์ชันเลขคณิต f คือ

$$\sum_{d|n} f(d) \quad \text{หมายถึง ผลบวกของ } f(d) \text{ เมื่อ } d \text{ เป็นตัวหารที่เป็นบวกของ } n$$

ตัวอย่างเช่น $\sum_{d|3} f(d) = f(1) + f(3)$ และ $\sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6)$ เป็นต้น

ตัวอย่าง

ให้ฟังก์ชันเลขคณิต $f(n) = n^2$ จงหาของ $\sum_{d|4} f(d)$, $\sum_{d|6} f(d)$ และ $\sum_{d|12} f(d)$

วิธีทำ

$$\sum_{d|4} f(d) = f(1) + f(2) + f(4) = 1^2 + 2^2 + 4^2 = 21$$

$$\sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$$

$$\begin{aligned}\sum_{d|12} f(d) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\ &= 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210\end{aligned}$$

สัญลักษณ์แทนการคูณของฟังก์ชันเลขคณิต f คือ

$$\prod_{i=1}^{k} f(i) = f(1)f(2)f(3)\cdots f(k)$$

ตัวอย่างเช่น $\prod_{i=1}^{3} f(i) = f(1)f(2)f(3)$ และ $\prod_{n=1}^{5} n = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$ เป็นต้น

ฟังก์ชันเทา

บทนิยาม

ให้ $n \in \mathbb{N}$ กำหนดให้

$$\tau(n) = \text{จำนวนตัวหารที่เป็นบวกของ } n$$

เรียกฟังก์ชันนี้ว่า **ฟังก์ชันเทา** (tau function)

ข้อสังเกต

ให้ $n \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. τ เป็นฟังก์ชันเลขคณิต
2. $\tau(1) = 1$
3. $\tau(n) = \sum_{d|n} 1$

ตัวอย่าง

จงหาค่าของ

1. $\tau(12)$

   วิธีทำ เนื่องจาก $1, 2, 3, 4, 6, 12$ เป็นตัวหารของ 12 ดังนั้น $\tau(12) = 6$

2. $\tau(23)$

   วิธีทำ เนื่องจาก $1, 23$ เป็นตัวหารของ 23 ดังนั้น $\tau(23) = 2$

3. $\tau(308)$

   วิธีทำ เนื่องจาก $308 = 2^2 \cdot 7 \cdot 11$ นั่นคือ $1, 2, 4, 7, 11, 14, 22, 28, 44, 77, 154, 308$ เป็นตัวหารของ 308 ดังนั้น $\tau(308) = 12$

4. $\tau(625)$

   เนื่องจาก $625 = 5^2 = 4$ นั่นคือ $1, 5, 25, 125, 625$ เป็นตัวหารของ 625 ดังนั้น $\tau(625) = 5$

Theorem

ถ้า p เป็นจำนวนเฉพาะ $a \in \mathbb{N}$ แล้ว

1. $\tau(p) = 2$
2. $\tau(p^a) = a + 1$

Theorem

ให้ $n \in \mathbb{N}$ และ $n > 1$ ถ้า $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ ในรูปแบบบัญญัติ แล้ว

$$\tau(n) = \prod_{i=1}^{k}(\alpha_i + 1) = (a_1 + 1)(a_2 + 2)\cdots(a_k + 1)$$

ตัวอย่าง

จงหาค่าของ

1. $\tau(500)$

   วิธีทำ $\tau(500) = \tau(2^2 \cdot 5^3) = (2+1)(3+1) = 12$

2. $\tau(720)$

   วิธีทำ $\tau(720) = \tau(2^4 \cdot 3^2 \cdot 5) = (4+1)(2+1)(1+1) = 30$

3. $\tau(1000)$

   วิธีทำ $\tau(1000) = \tau(2^3 \cdot 5^3) = (3+1)(3+1) = 16$

4. $\tau(8820)$

   วิธีทำ $\tau(8820) = \tau(2^2 \cdot 3^2 \cdot 5 \cdot 7^2) = (2+1)(2+1)(1+1)(2+1) = 54$

Theorem

ฟังก์ชันเทาเป็นฟังก์ชันเชิงการคูณ

ตัวอย่าง

ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ และ $n = 2^{k-1}(2^k - 1)$ จงหาค่าของ $\tau(n)$

วิธีทำ เห็นได้ชัดว่า $\gcd(2^k - 1, 2^{k-1}) = 1$ เนื่องจาก τ เป็นฟังก์ชันเชิงการคูณ และ $2^k - 1$ เป็นจำนวนเฉพาะ จะได้ว่า

$$\begin{aligned}\tau(n) &= \tau(2^{k-1} \cdot (2^k - 1)) \\ &= \tau(2^{k-1})\tau(2^k - 1) \\ &= (k - 1 + 1)(2) = 2k\end{aligned}$$

ดังนั้น $\tau(n) = 2k$

ฟังก์ชันซิกมา

บทนิยาม

ให้ $n, k \in \mathbb{N}$ กำหนดให้

$$\sigma(n) = \text{ผลบวกของตัวหารที่เป็นบวกทั้งหมดของ } n$$

เรียกฟังก์ชันนี้ว่า **ฟังก์ชันซิกมา (sigma function)** และนิยาม

$$\sigma_k(n) = \text{ผลบวกของกำลัง } k \text{ ของตัวหารที่เป็นบวกทั้งหมดของ } n$$

ข้อสังเกต

ให้ $n, k \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. σ และ σ_k เป็นฟังก์ชันเลขคณิต ทุก ๆ $k \in \mathbb{N}$
2. $\sigma = \sigma_1$
3. $\sigma(1) = 1$ และ $\sigma_k(1) = 1$
4. $\sigma(n) = \sum_{d|n} d$ และ $\sigma_k(n) = \sum_{d|n} d^k$

ตัวอย่าง

จงหาค่าของ

1. $\sigma(6)$ และ $\sigma_2(6)$

   วิธีทำ $\sigma(6) = 1 + 2 + 3 + 6 = 12$ และ $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$

2. $\sigma(7)$ และ $\sigma_3(7)$

   วิธีทำ $\sigma(7) = 1 + 7 = 8$ และ $\sigma_3(7) = 1^3 + 7^3 = 344$

3. $\sigma(81)$ และ $\sigma_2(81)$

   วิธีทำ $\sigma(81) = \sigma(3^4) = 1 + 3 + 9 + 27 + 81 = 121$ และ
   $\sigma_2(81) = \sigma_2(3^4) = 1^2 + 3^2 + 9^2 + 27^2 + 81^2 = 7381$

Theorem

ถ้า p เป็นจำนวนเฉพาะ แล้ว

$$\sigma(p) = 1 + p \qquad \text{และ} \qquad \sigma_k(p) = 1 + p^k$$

Theorem

ถ้า p เป็นจำนวนเฉพาะ และ $a \in \mathbb{N}$ แล้ว

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} \qquad \text{และ} \qquad \sigma_k(p^a) = \frac{(p^k)^{a+1} - 1}{p^k - 1}$$

ตัวอย่าง

จงหาค่าของ

1. $\sigma(16)$

   วิธีทำ $\sigma(16) = \sigma(2^4) = \dfrac{2^5 - 1}{2 - 1} = 31$

2. $\sigma_2(343)$

   วิธีทำ $\sigma_2(343) = \sigma_2(7^3) = \dfrac{(7^2)^4 - 1}{7^2 - 1} = 120100$

3. $\sigma(729)$

   วิธีทำ $\sigma(729) = \sigma(3^6) = \dfrac{3^7 - 1}{3 - 1} = 1093$

Lemma

ให้ n_1, n_2 เป็นจำนวนเต็มซึ่ง $gcd(n_1, n_2) = 1$ จะได้ว่าทุก ๆ จำนวนเต็มบวก d ซึ่ง $d \mid n_1 n_2$ ก็ต่อเมื่อ มีจำนวนเต็มบวก d_1 และ d_2 ที่ $d = d_1 d_2$ และ $d_1 \mid n_1$, $d_2 \mid n_2$ นอกจากนี้ ถ้า $d_1 \mid n_1$, $d_2 \mid n_2$ และ $d_1' \mid n_1$, $d_2' \mid n_2$ โดยที่ $d_1 d_2 = d_1' d_2'$ แล้ว $d_1 = d_1'$ และ $d_2 = d_2'$

Theorem

ฟังก์ชันซิกมาเป็นฟังก์ชันเชิงการคูณ

ตัวอย่าง

จงหาค่าของ

1. $\sigma(600)$

   วิธีทำ $\sigma(600) = \sigma(2^3 \cdot 3 \cdot 5^2) = \sigma(2^3)\sigma(3)\sigma(5^2) = \dfrac{2^4-1}{2-1}(1+3)\dfrac{5^3-1}{5-1} = 1860$

2. $\sigma_2(200)$

   วิธีทำ $\sigma_2(200) = \sigma_2(2^3 \cdot 5^2) = \sigma_2(2^3)\sigma_2(5^2) = \dfrac{(2^2)^4-1}{2^2-1} \cdot \dfrac{(5^2)^3-1}{5^2-1} = 55355$

3. $\sigma(3250)$

   วิธีทำ $\sigma(3250) = \sigma(2 \cdot 5^3 \cdot 13) = \sigma(2)\sigma(5^3)\sigma(13) = (1+2)\dfrac{5^4-1}{5-1}(1+13) = 6552$

Theorem

ถ้า $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *รูปแบบบัญญัติ แล้ว*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \qquad \text{และ} \qquad \sigma_k(n) = \prod_{i=1}^{k} \frac{(p_i^k)^{\alpha_i+1} - 1}{p_i^k - 1}$$

ตัวอย่าง

ถ้า $2^k - 1$ เป็นจำนวนเฉพาะ และ $n = 2^{k-1}(2^k - 1)$ จงหาค่าของ $\sigma(n)$

วิธีทำ เนื่องจาก $2^k - 1$ เป็นจำนวนเฉพาะ และ $\gcd(2^{k-1}, 2^k - 1) = 1$ ดังนั้น

$$\begin{aligned}
\sigma(n) &= \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) \\
&= \frac{2^k - 1}{2 - 1} \cdot (1 + 2^k + 1) \\
&= (2^k - 1)(2^k) \\
&= 2 \cdot 2^{k-1}(2^k - 1) = 2n
\end{aligned}$$

บทนิยาม

เรียกจำนวนนับ n ว่า **จำนวนสมบูรณ์ (perfect number)** ถ้า $\sigma(n) = 2n$

จากตัวอย่างที่ผ่านมาทำให้ได้ตัวอย่างจำนวนสมบูรณ์ดังตาราง

k	$2^k - 1$	จำนวนสมบูรณ์ $n = 2^{k-1}(2^k - 1)$
2	3	6
3	7	28
5	31	496
7	127	8,128
13	8191	335,500,336
17	131071	8,589,869,056

ฟังก์ชันออยเลอร์-ฟี

บทนิยาม

ให้ $n \in \mathbb{N}$ นิยาม

$$\phi(n) = \text{จำนวนของจำนวนเต็มบวก } k \leq n \text{ และ } \gcd(k, n) = 1$$

เรียกว่า **ฟังก์ชันฟีออยเลอร์** (Euler phi function) หรือ **ฟังก์ชันฟี** (phi function)

ข้อสังเกต

ให้ $n \in \mathbb{N}$ จากบทนิยามจะได้ว่า

1. ϕ เป็นฟังก์ชันเลขคณิต
2. $\phi(1) = 1$

ต่อไปแสดงตัวอย่าง $\phi(n)$ เมื่อ $2 \leq n \leq 10$

n	จำนวนเต็มบวก $k \leq n$ ซึ่ง $\gcd(k, n) = 1$	$\phi(n)$
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4

ตัวอย่าง

จงหาค่าของ

1. $\phi(15)$

   วิธีทำ จำนวนเต็มบวก $k \leq 15$ ซึ่ง $\gcd(k, 15) = 1$ คือ 1, 2, 4, 7, 8, 11, 13, 14 ดังนั้น $\phi(15) = 8$

2. $\phi(17)$

   วิธีทำ จำนวนเต็มบวก $k \leq 17$ ซึ่ง $\gcd(k, 17) = 1$ คือ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ดังนั้น $\phi(17) = 16$

3. $\phi(25)$

   วิธีทำ จำนวนเต็มบวก $k \leq 25$ ซึ่ง $\gcd(k, 25) = 1$ คือ 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24 ดังนั้น $\phi(25) = 20$

4. $\phi(36)$

   วิธีทำ จำนวนเต็มบวก $k \leq 36$ ซึ่ง $\gcd(k, 36) = 1$ คือ 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 ดังนั้น $\phi(36) = 12$

Theorem

ถ้า p เป็นจำนวนเฉพาะ แล้ว $\phi(p) = p - 1$

ตัวอย่าง

จงหาค่าของ

1. $\phi(37)$
   วิธีทำ เนื่องจาก 37 เป็นจำนวนเฉพาะ ดังนั้น $\phi(37) = 37 - 1 = 36$
2. $\phi(101)$
   วิธีทำ เนื่องจาก 101 เป็นจำนวนเฉพาะ ดังนั้น $\phi(101) = 101 - 1 = 100$
3. $\phi(1277)$
   วิธีทำ เนื่องจาก 1277 เป็นจำนวนเฉพาะ ดังนั้น $\phi(1277) = 1277 - 1 = 1276$

ตัวอย่าง

จงหาค่าของ $\phi(625)$

วิธีทำ เนื่องจาก $625 = 5^4$ พิจารณา

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 2(5) \\ 11 & 12 & 13 & 14 & 3(5) \\ & & & \vdots & \\ 621 & 622 & 623 & 624 & 125(5) = 5^3(5) = 625 \end{array}$$

นั่นคือจำนวนแต็มที่ 5 หารลงตัวอยู่แนวตั้งสุดท้าย มีจำนวนทั้งหมดเท่ากับ $125 = 5^3$ ตัว ดังนั้นจำนวนเต็ม k ซึ่ง $\gcd(k, 625) = 1$ เท่ากับ $5^4 - 5^3$ สรุปได้ว่า $\phi(625) = \phi(5^4) = 5^4 - 5^3 = 500$

Theorem

ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{N}$ แล้ว $\phi(p^a) = p^a - p^{a-1}$

1. $\phi(97)$

   วิธีทำ $\phi(97) = 97^1 - 97^0 = 96$

2. $\phi(64)$

   วิธีทำ $\phi(64) = \phi(2^6) = 2^6 - 2^5 = 32$

3. $\phi(343)$

   วิธีทำ $\phi(343) = \phi(7^3) = 7^3 - 7^2 = 294$

4. $\phi(625)$

   วิธีทำ $\phi(625) = \phi(5^4) = 5^4 - 5^3 = 500$

5. $\phi(729)$

   วิธีทำ $\phi(729) = \phi(3^6) = 3^6 - 3^5 = 486$

Theorem

ฟังก์ชันฟีออยเลอร์เป็นฟังก์ชันเชิงการคูณ

บทแทรก

ให้ $m_1, m_2, ..., m_k \in \mathbb{N}$ และ $\gcd(m_i, m_j) = 1$ ทุก ๆ $i \neq j$ แล้ว

$$\phi(m_1, m_2 ... m_k) = \phi(m_1)\phi(m_2)...\phi(m_k)$$

ตัวอย่าง

จงหาค่าของ

1. $\phi(72)$

   วิธีทำ $\phi(72) = \phi(2^3 \cdot 3^2) = \phi(2^3)\phi(3^2) = (2^3 - 2^2)(3^2 - 3^1) = 4(6) = 24$

2. $\phi(500)$

   วิธีทำ $\phi(500) = \phi(2^2 \cdot 5^3) = \phi(2^2)\phi(5^3) = (2^2 - 2^1)(5^3 - 5^2) = 2(100) = 200$

3. $\phi(1000)$

   วิธีทำ $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4(100) = 400$

ถ้า $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ เป็นการเขียน n ในรูปแบบบัญญัติ แล้ว

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

1. $\phi(225)$

   วิธีทำ เนื่องจาก $225 = 3^2 \cdot 5^2$ ดังนั้น

   $$\phi(225) = 225 \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 120$$

2. $\phi(360)$

   วิธีทำ เนื่องจาก $360 = 2^3 \cdot 3^2 \cdot 5$ ดังนั้น

   $$\phi(360) = 360 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 96$$

3. $\phi(900)$

   วิธีทำ เนื่องจาก $900 = 2^2 \cdot 3^2 \cdot 5^2$ ดังนั้น

   $$\phi(900) = 900 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 240$$

ตัวอย่าง

จงหาค่าของ $\sum_{d|n} \phi(d)$ เมื่อ

1. $n = 12$

ตัวประกอบ (d) ของ 12	1	2	3	4	6	12
$\phi(d)$	1	1	2	2	2	4

ดังนั้น $\sum_{d|12} \phi(d) = 1 + 1 + 2 + 2 + 2 + 4 = 12$

2. $n = 20$

ตัวประกอบ (d) ของ 20	1	2	4	5	10	20
$\phi(d)$	1	1	2	4	4	8

ดังนั้น $\sum_{d|20} \phi(d) = 1 + 1 + 2 + 4 + 4 + 8 = 20$

Theorem

ให้ $n \in \mathbb{N}$ *แล้ว*

$$\sum_{d|n} \phi(d) = n$$

ฟังก์ชันจำนวนเต็มค่ามากสุด

บทนิยาม

สำหรับจำนวนจริง x ใด ๆ

$$[x] \text{ คือจำนวนเต็มค่ามากสุดที่มีค่าน้อยกว่าหรือเท่ากับ } x$$

เรียก $[x]$ ว่า **ฟังก์ชันจำนวนเต็มค่ามากสุด** (the greatest integer function)

ตัวอย่างเช่น $[1.5] = 1$, $[-2.14] = -3$, $[\sqrt{3}] = 1$, $[\frac{15}{7}] = 2$ และ $[3] = 3$

ข้อสังเกต

สำหรับจำนวนจริง x จะได้ว่า

1. $[x] \leq x \leq [x] + 1$
2. $0 \leq x - [x] \leq 1$

โดยสมบัติจำนวนจริงที่ว่า ทุกจำนวนจริง x ใด ๆ จะมีจำนวนเต็ม n ที่ $n \leq x < n+1$ ทำให้ได้

$$x = n + (x - n) \qquad \text{โดยที่} \qquad 0 \leq x - n < 1$$

นั่นคือ $x = n + k$ เมื่อ k เป็นจำนวนจริงที่ $0 \leq k < 1$ ซึ่งในกรณีนี้ $[x] = k$ นั่นเอง

Theorem

สำหรับจำนวนจริง x ใด ๆ จะได้ว่า

1. *ถ้า $x \geq 0$ แล้ว* $[x] = \sum_{1 \leq i \leq x} 1$
2. $[x] + [-x] = \begin{cases} 0 & \text{ถ้า } x \in \mathbb{Z} \\ -1 & \text{ถ้า } x \notin \mathbb{Z} \end{cases}$
3. $[x + m] = [x] + m$ *เมื่อ m เป็นจำนวนเต็ม*
4. $\left[\frac{x}{m}\right] = \left[\frac{[x]}{m}\right]$ *เมื่อ m เป็นจำนวนเต็มบวก*
5. $-[-x]$ *คือจำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ x*
6. *ถ้า n และ m เป็นจำนวนเต็มบวก จำนวนของจำนวนเต็มจากเซตของ $\{1, 2, \ldots, n\}$ ที่หาร n ลงตัวด้วย m คือ* $\left[\frac{n}{m}\right]$

สำหรับจำนวนเต็ม a และ b โดยขั้นตอนการหารจะได้ว่ามีจำนวนเต็ม q และ r ซึ่ง $b = aq + r$ เมื่อ $0 \leq r < a$ ทำให้ได้ว่า

$$\frac{b}{a} = q + \frac{r}{a} \qquad \text{โดยที่} \qquad 0 \leq \frac{r}{a} < 1$$

นั่นคือ

$$q = \left[\frac{b}{a}\right] \qquad \text{และ} \qquad r = b - aq = b - a\left[\frac{b}{a}\right]$$

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหาร -934 ด้วย 248

วิธีทำ ให้ $b = -934$ และ $a = 248$ แล้ว $q = \left[\frac{-934}{248}\right] = [-3.67] = -4$ ดังนั้น

$$r = b - aq = -934 - 248(-4) = 58$$

ดังนั้นเศษที่เกิดจากการหาร -934 ด้วย 248 เท่ากับ 58

ต่อไปจะใช้ฟังก์ชันจำนวนเต็มค่ามากสุดช่วยในการเขียนรูปแบบบัญญัติของจำนวนที่อยู่ในรูปแฟคทอเรียล กำหนดให้ $A = \{1, 2, 3, ..., n\}$ และ $a \in \mathbb{N}$ ให้

$$X_a = \{x \in A : a \text{ หาร } x \text{ ลงตัว }\}$$

แล้วจะได้ว่า $|X_a| = \left[\frac{n}{a}\right]$ จงหาจำนวนเต็ม k มากสุดที่ทำให้ 2^k หาร $100!$ ลงตัว นั่นคือ $100!$ เขียนรูปแบบบัญญัติคือ

$$100! = 2^k \cdot 3^{a_1} \cdot 5^{a_2} \cdot 7^{a_3} \cdots 97$$

พิจารณา $100! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots 97 \cdot 98 \cdot 99 \cdot 100$ พบว่าถ้า $A = \{1, 2, 3, ..., 100\}$ จะได้ว่า

$$X_{2^1} = \{x \in A : 2^1 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^1}| = \left[\frac{100}{2^1}\right] = 50$$

$$X_{2^2} = \{x \in A : 2^2 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^2}| = \left[\frac{100}{2^2}\right] = 25$$

$$X_{2^3} = \{x \in A : 2^3 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^3}| = \left[\frac{100}{2^3}\right] = 12$$

$$X_{2^4} = \{x \in A : 2^4 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^4}| = \left[\frac{100}{2^4}\right] = 6$$

$$X_{2^5} = \{x \in A : 2^5 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^5}| = \left[\frac{100}{2^5}\right] = 3$$

$$X_{2^6} = \{x \in A : 2^6 \text{ หาร } x \text{ ลงตัว }\} \quad \text{จะได้ว่า} \quad |X_{2^6}| = \left[\frac{100}{2^6}\right] = 1$$

ดังนั้น $k = 50 + 25 + 12 + 6 + 3 + 1 = 97$ นั่นคือ

$$k = \sum_{i=1}^{6} |X_{2^i}| = \sum_{i=1}^{6} \left[\frac{100}{2^i}\right]$$

จะใช้สัญลักษณ์ $e_p(n)$ แทน $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ ในตัวอย่างนี้คือ $k = e_2(100)$ จากการสังเกตนี้ทำให้ได้ทฤษฎีบทต่อไปนี้

Theorem

ให้ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนเต็มบวก จะได้ว่ากำลังสูงสุดของ p ที่หาร $n!$ ลงตัวคือ

$$e_p(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

ตัวอย่าง

จงหาจำนวนเต็ม k มากสุดที่ทำให้ 3^k หาร $500!$ ลงตัว

วิธีทำ โดยทฤษฎีบท 31 จะได้ว่า $k = e_3(500)$ ดังนั้น

$$\begin{aligned} k = e_3(500) &= \sum_{i=1}^{\infty} \left[\frac{500}{3^i}\right] \\ &= \left[\frac{500}{3}\right] + \left[\frac{500}{3^2}\right] + \left[\frac{500}{3^3}\right] + \left[\frac{500}{3^4}\right] + \left[\frac{500}{3^5}\right] + \left[\frac{500}{3^6}\right] \\ &= 166 + 55 + 18 + 6 + 2 \\ &= 247 \end{aligned}$$

ตัวอย่าง

จงหาจำนวนเต็ม k มากสุดที่ทำให้ 18^k หาร $100!$ ลงตัว

วิธีทำ เนื่องจาก $18 = 2 \cdot 3^2$ พิจารณากำลังสูงสุดของจำนวนเฉพาะ 2 และ 3 ได้ดังนี้

$$e_2(100) = \sum_{i=1}^{\infty} \left[\frac{100}{2^i}\right] = \left[\frac{100}{2}\right] + \left[\frac{100}{2^2}\right] + \left[\frac{100}{2^3}\right] + \left[\frac{100}{2^4}\right] + \left[\frac{100}{2^5}\right] + \left[\frac{100}{2^6}\right]$$

$$= 50 + 25 + 12 + 6 + 3 + 1 = 97$$

$$e_3(100) = \sum_{i=1}^{\infty} \left[\frac{100}{3^i}\right] = \left[\frac{100}{3}\right] + \left[\frac{100}{3^2}\right] + \left[\frac{100}{3^3}\right] + \left[\frac{100}{3^4}\right]$$

$$= 33 + 11 + 3 + 1 = 48$$

ดังนั้นรูปแบบบัญญัติของ $100!$ คือ $100! = 2^{97} \cdot 3^{48} \cdot 5^m \cdot 7^d \cdots 97$ เนื่องจาก

$$2^{97} \cdot 3^{48} = 2^{73} \cdot 2^{24} \cdot (3^2)^{24} = 2^{73}(2 \cdot 3^2)^{24} = 2^{73}(18)^{24}$$

ดังนั้น $k = 24$

ตัวอย่าง

จงหาจำนวนที่ลงท้ายด้วยศูนย์ทั้งหมดของ 1000!

วิธีทำ จำนวนที่ลงท้ายด้วยศูนย์ทั้งหมดของ 1000! คือกำลังสูงสุดของ 10 ที่หาร 1000! ลงตัว เนื่องจาก $10 = 2 \cdot 5$ นั่นคือค่าต่ำสุดของ $e_2(1000)$ และ $e_5(1000)$ เนื่องจาก $e_5(1000) < e_2(1000)$ ดังนั้นกำลังสูงสุดของ 10 ที่หาร 1000! ลงตัวเท่ากับ $e_5(1000)$ หาได้จาก

$$\begin{aligned} e_5(1000) &= \sum_{i=1}^{\infty} \left[\frac{1000}{5^i}\right] = \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] \\ &= 200 + 40 + 8 + 1 \\ &= 249 \end{aligned}$$

ดังนั้น จำนวนที่ลงท้ายด้วยศูนย์ทั้งหมดของ 1000! เท่ากับ 249 จำนวน

บทที่ 7 สมการไดโอแฟนไทน์

สมการเชิงเส้นดีกรีหนึ่ง

ในหัวข้อนี้เราสนใจหาเงื่อนไขที่เพียงพอที่จะแสดงว่าสมการ

$$ax + by = c \qquad \text{เมื่อ } a, b, c \in \mathbb{Z}$$

ถ้า $a = 0$ หรือ $b = 0$ สามารถหาคำตอบได้โดยง่าย เช่น $ax = c$ สมการนี้มีคำตอบก็ต่อเมื่อ $a \mid c$ และคำตอบคือ $x = \frac{c}{a}$ ทำให้สนใจกรณีที่ $a \neq 0$ และ $b \neq 0$

Theorem

ให้ $a, b, c \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ แล้ว

$$\text{สมการ} \quad ax + by = c \quad \text{มีคำตอบ } x, y \in \mathbb{Z} \qquad \text{ก็ต่อเมื่อ} \qquad \gcd(a, b) \mid c$$

บทพิสูจน์.

ให้ $a, b \in \mathbb{Z}$ ซึ่ง $a \neq 0$ และ $b \neq 0$ กำหนดให้ $\gcd(a, b) = d$ สมมติว่า $x_0, y_0 \in \mathbb{Z}$ เป็นคำตอบของสมการ $ax + by = c$ ดังนั้น $ax_0 + by_0 = c$ เนื่องจาก $d \mid a$ และ $d \mid b$ ดังนั้น $d \mid (ax_0 + by_0)$ นั่นคือ $d \mid c$ ในทางกลับกัน สมมติว่า $d \mid c$ ดังนั้น $c = dk$ สำหรับบางจำนวนเต็ม k เนื่องจาก $\gcd(a, b) = d$ จะได้ว่ามีจำนวนเต็ม x_1, y_1 ซึ่ง $d = ax_1 + by_1$ นั่นคือ

$$c = dk = a(kx_1) + b(ky_1)$$

ดังนั้น kx_1, ky_1 เป็นคำตอบของสมการ $ax + by = c$ □

จงตรวจสอบสมการไดโอแฟนไทน์ต่อไปนี้ว่ามีคำตอบหรือไม่

1. $2x + 3y = 5$
   วิธีทำ เนื่องจาก $\gcd(2, 3) = 1$ และ $1 \mid 5$ ดังนั้น $2x + 3y = 5$ มีคำตอบ
2. $42x + 21y = 15$
   วิธีทำ เนื่องจาก $\gcd(42, 21) = 7$ และ $7 \nmid 15$ ดังนั้น $42x + 21y = 15$ ไม่มีคำตอบ
3. $50x + 15y = 20$
   วิธีทำ เนื่องจาก $\gcd(50, 15) = 5$ และ $5 \mid 20$ ดังนั้น $50x + 15y = 20$ มีคำตอบ

Theorem

ให้ $a, b, c \in \mathbb{Z}$ *ซึ่ง* $a \neq 0$ *และ* $b \neq 0$ *ถ้าสมการ* $ax + by = c$ *มีคำตอบเป็น* $x = x_0$ *และ* $y = y_0$ *เรียกคำตอบนี้ว่า* ***คำตอบเฉพาะราย (particular solution)*** *และ* $d = gcd(a, b)$ *แล้วทุก ๆ คำตอบของสมการ* $ax + by = c$ *เขียนในรูป*

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t \qquad \text{เมื่อ } t \in \mathbb{Z}$$

ตัวอย่าง

จงหาคำตอบของสมการไดโอแฟนไทน์ $4x + 5y = 13$

วิธีทำ เนื่องจาก $\gcd(4, 5) = 1$ ดังนั้นสมการ $4x + 5y = 13$ มีคำตอบ ต่อไปจะหาคำตอบเฉพาะรายโดยใช้ขั้นตอนวิธีแบบยุคลิด

$$\begin{array}{rcrcr|rrrl} 5 & = & 5(1) & + & 4(0) & 5 & 1 & 0 & R_1 \\ 4 & = & 5(0) & + & 4(1) & 4 & 0 & 1 & R_2 \\ 1 & = & 5(1) & + & 4(-1) & 1 & 1 & -1 & R_3 = R_1 - R_2 \end{array}$$

ดังนั้น $5(1) + 4(-1) = 1$ นั่นคือ $4(-13) + 5(13) = 13$ จะได้ว่า $x_0 = -13$ และ $y_0 = 13$ สรุปได้ว่าคำตอบของสมการ $4x + 5y = 13$ คือ

$$x = -13 + 5t, \qquad y = 13 - 4t \qquad \text{เมื่อ } t \in \mathbb{Z}$$

จากตัวอย่างข้างต้นการหาคำตอบเฉพาะรายอาจทำได้อีกวิธี เมื่อพิจารณา $4x + 5y = 13$

พบว่า	$4x - 13 = -5y$	หรือ	$5y - 13 = -4x$
จะได้ว่า	$5 \mid (4x - 13)$	หรือ	$4 \mid (5y - 13)$
ดังนั้น	$4x \equiv 13 \pmod 5$	หรือ	$5y \equiv 13 \pmod 4$

จะได้ว่า

$$\begin{aligned} 4x &\equiv 3 \pmod 5 \\ 4 \cdot 4x &\equiv 4 \cdot 3 \pmod 5 \\ 16x &\equiv 12 \pmod 5 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

เลือก $x_0 = 2$ จะได้ $4(2) + 5y_0 = 13$ นั่นคือ $y_0 = 1$ ดังนั้น $x_0 = 2, y_0 = 1$ เป็นคำตอบเฉพาะรายของสมการ $4x + 5y = 13$

วิธีการคำตอบเฉพาะรายของ $ax + by = c$

พบว่า	$ax - c = -by$	หรือ	$by - c = -ax$
จะได้ว่า	$b \mid (ax - c)$	หรือ	$a \mid (by - c)$
ดังนั้น	$ax \equiv c \pmod b$	หรือ	$by \equiv c \pmod a$

สรุปวิธีหาคำตอบเฉพาะรายของ $ax + by = c$ ด้วยคำตอบของสมการสมภาค

$$ax \equiv c \pmod b \qquad \text{หรือ} \qquad by \equiv c \pmod a$$

สรุปขั้นตอนการหาคำตอบของสมการไดโอแฟนไทน์ $ax + by = c$

1. หา $d = \gcd(a, b)$
2. ตรวจสอบว่า $d \mid c$ หรือ $d \nmid c$
3. ถ้า $d \nmid c$ แล้วสมการ $ax + by = c$ ไม่มีคำตอบในระบบจำนวนเต็ม
4. ถ้า $d \mid c$ แล้วสมการ $ax + by = c$ มีคำตอบในระบบจำนวนเต็ม

   หาคำตอบเฉพาะราย โดยเลือกได้ 2 วิธี ดังนี้

   (ก) ขั้นตอนวิธีแบบยุคลิด จาก $d = ax_1 + by_1$ และ $c = dk$ เลือก $x_0 = kx_1$ และ $y_0 = ky_1$

   (ข) สมการสมภาค $ax \equiv c \pmod{b}$ หรือ $by \equiv c \pmod{a}$

   หา x_0 เป็นคำตอบของ $ax \equiv c \pmod{b}$ แล้วหา y_0 จากสมการ $ax_0 + by_0 = c$

   หา y_0 เป็นคำตอบของ $by \equiv c \pmod{a}$ แล้วหา x_0 จากสมการ $ax_0 + by_0 = c$
5. สร้างคำตอบทั้งหมด

ตัวอย่าง

จงหาคำตอบเฉพาะรายของสมการไดโอแฟนไทน์ $80x - 62y = 90$ โดยใช้ขั้นตอนวิธีแบบยุคลิด

วิธีทำ เนื่องจาก $\gcd(80, -62) = 2$ จะได้ว่า $2 \mid 90$ ดังนั้นสมการ $80x - 62y = 90$ มีคำตอบ ต่อไปจะหาคำตอบเฉพาะราย โดยใช้ขั้นตอนวิธีแบบยุคลิด

$$\begin{array}{rcrcr|rrrl}
80 &=& 80(1) &+& 62(0) & 80 & 1 & 0 & R_1 \\
62 &=& 80(0) &+& 62(1) & 62 & 0 & 1 & R_2 \\
18 &=& 80(1) &+& 62(-1) & 18 & 1 & -1 & R_3 = R_1 - R_2 \\
8 &=& 80(-3) &+& 62(4) & 8 & -3 & 4 & R_4 = R_2 - 3R_3 \\
2 &=& 80(7) &+& 62(-9) & 2 & 7 & -9 & R_5 = R_3 - 2R_4
\end{array}$$

ดังนั้น $80(7) - 62(9) = 2$ นั่นคือ $80(315) - 62(405) = 90$ จะได้ว่า $x_0 = 315$ และ $y_0 = 405$ เป็นคำตอบเฉพาะรายของ $80x - 62y = 90$

ตัวอย่าง

เด็กชายเอ ได้เงินค่าขนมจากพ่อจำนวน 200 บาท ถ้าเราทราบเพียงว่าพ่อของเด็กชายเอให้เป็นธนบัตร 2 ชนิด คือธนบัตรชนิด 20 บาท และธนบัตรชนิด 50 บาทเท่านั้น จงหาจำนวนธนบัตรที่เด็กชายเอได้รับทั้งหมด

วิธีทำ ให้ x แทนจำนวนธนบัตรชนิด 20 บาท และ y แทนจำนวนธนบัตรชนิด 50 บาท จะได้ว่า

$$20x + 50y = 200$$

เนื่องจาก $\gcd(20, 50) = 10$ แล้ว $10 \mid 200$ ดังนั้น สมการนี้มีคำตอบในระบบจำนวนเต็ม เห็นได้ชัดว่า $x_0 = 0$ และ $y_0 = 4$ เป็นคำตอบเฉพาะรายของสมการนี้ ดังนั้น

$$x = 5t, \qquad y = 4 - 2t \qquad \text{เมื่อ } t \in \mathbb{Z}$$

เนื่องจาก $5t = x > 0$ ดังนั้น $t > 0$ และ $4 - 2t = y > 0$ ดังนั้น $t < 2$ ทำให้ได้ $t = 1$ สรุปได้ว่า $x = 5, y = 2$ นั่นคือ เด็กชายเอมีธนบัตรชนิด 20 บาทจำนวน 5 ใบ และธนบัตรชนิด 50 บาทจำนวน 2 ใบ

พิจารณาการหาคำตอบของสมการไดโอแฟนไทน์

$$ax + by + cz = m$$

ให้ $d = \gcd(a, b, c)$ และ $d_0 = \gcd(a, b)$ ถ้า $d \mid m$ สมการนี้มีคำตอบในระบบจำนวนเต็ม พิจารณาสมการ

$$ax + by = m - cz$$

ดังนั้น $d_0 \mid (m - cz)$ นั่นคือ

$$cz \equiv m \pmod{d_0}$$

ให้ z_0 เป็นคำตอบของสมการ $cz \equiv m \pmod{d_0}$ เนื่องจาก $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = d$ และ $d \mid m$ ดังนั้น

$$z = z_0 + \frac{d_0}{d}t \qquad \text{เมื่อ} \qquad t \in \mathbb{Z}$$

เมื่อแทน z ลงในสมการไดโอแฟนไทน์ $ax + by + cz = m$ ทำให้ได้สมการไดโอแฟนไทน์ 2 ตัวแปร แล้วดำเนินการหาคำตอบของสมการด้วยวิธีเดิมที่กล่าวมาแล้ว

ตัวอย่าง

จงหาคำตอบของสมการไดโอแฟนไทน์ $3x - 6y + 9z = 63$

วิธีทำ ให้ $\gcd(3, -6, 9) = 3$ เนื่องจาก $3 \mid 63$ ดังนั้นสมการ $3x - 6y + 9z = 63$ มีคำตอบในระบบจำนวนเต็ม จะได้ว่า

$$3x - 6y = 63 - 9z$$

เนื่องจาก $\gcd(3, -6) = 3$ ดังนั้น $3 \mid (63 - 9z)$ นั่นคือ $9z \equiv 63 \pmod 3$ เห็นได้ชัดว่าคำตอบของสมการสมภาคนี้คือจำนวนเต็มใดก็ได้ ให้ $z = t$ เมื่อ $t \in \mathbb{Z}$ นั่นคือ

$$3x - 6y = 63 - 9t$$

$$x - 2y = 21 - 3t$$

$$x = 21 - 3t + 2y$$

$$x = 21 - 3t + 2s$$

ให้ $y = s$ เมื่อ $s \in \mathbb{Z}$ ดังนั้นคำตอบของสมการ $3x - 6y + 9z = 63$ คือ

$$\begin{aligned} x &= 21 - 3t + 2s \\ y &= s \qquad \text{เมื่อ } t, s \in \mathbb{Z} \\ z &= t \end{aligned}$$

ตัวอย่าง

มานะมีธนบัตร 1 ใบมูลค่า 50 บาท ต้องการแลกเหรียญ 3 ชนิดคือ เหรียญ 2 บาท เหรียญ 5 บาท และเหรียญ 10 บาท ถามว่ามานะจะได้เหรียญทั้งหมดกี่แบบโดยต้องมีเหรียญแต่ละชนิดอย่างน้อย 1 เหรียญ

วิธีทำ ให้ x แทนจำนวนเหรียญชนิด 2 บาท

y แทนจำนวนเหรียญชนิด 5 บาท

z แทนจำนวนเหรียญชนิด 10 บาท

จะได้ว่าสมการไดโอแฟนไทน์คือ

$$2x + 5y + 10z = 50$$

ให้ $\gcd(2, 5, 10) = 1$ เนื่องจาก $1 \mid 50$ ดังนั้นสมการ $2x + 5y + 10z = 50$ มีคำตอบในระบบจำนวนเต็ม จะได้ว่า

$$2x + 5y = 50 - 10z$$

เนื่องจาก $\gcd(2, 5) = 1$ ดังนั้น $1 \mid (50 - 10z)$ นั่นคือ $10z \equiv 50 \pmod 1$ เห็นได้ชัดว่าคำตอบของสมการสมภาคนี้คือจำนวนเต็มใดก็ได้ ให้ $z = t$ เมื่อ $t \in \mathbb{Z}$ นั่นคือ

$$2x + 5y = 50 - 10t$$

$$2x + 10t = 50 - 5y$$

$$2(x + 5t) = 5(10 - y)$$

ดังนั้น $2 \mid 5(10 - y)$ เนื่องจาก $\gcd(2, 5) = 1$ ดังนั้น $2 \mid (10 - y)$ ให้ $10 - y = 2s$ หรือ $y = 10 - 2s$ เมื่อ $s \in \mathbb{Z}$ จะได้ว่า

$$2x + 5(10 - 2s) = 50 - 10t$$

$$2x + 50 - 10s = 50 - 10t$$

เนื่องจาก x, y, z ไม่เป็นจำนวนเต็มลบ ดังนั้น $z = t > 0$ และ $y = 10 - 2s > 0$ นั่นคือ $s < 5$ และ $x = 5s - 5t > 0$ จะได้ $t < s$ ดังนั้นสรุปเงื่อนไขได้ดังต่อไปนี้

$$t > 0, \quad t < s \quad \text{และ} \quad s < 5$$

เขียนแจกแจงดังตารางต่อไปนี้

t	s	$x = 5s - 5t$	$y = 10 - 2s$	$z = t$
1	2	5	6	1
1	3	10	4	1
1	4	15	2	1
2	3	5	4	2
2	4	10	2	2
3	4	5	2	3

ดังนั้นมานะสามารถแลกเหรียญได้ทั้งหมด 6 แบบ ดังนี้

แบบที่	จำนวนเหรียญชนิด 2 บาท	จำนวนเหรียญชนิด 5 บาท	จำนวนเหรียญชนิด 10 บาท
1	5	6	1
2	10	4	1
3	15	2	1
4	5	4	2
5	10	2	2
6	5	2	3

ตัวอย่าง

จงหาสมการไดโอแฟนไทน์มาอย่างน้อยหนึ่งสมการที่มีคำตอบเป็น

$$\begin{aligned} x &= 12 + 4s - 7t \\ y &= 5 - 2s \qquad \text{เมื่อ } t, s \in \mathbb{Z} \\ z &= t \end{aligned}$$

วิธีทำ จากสมการ $x = 12 + s - 7t$ และ $2s = 5 - y$ และ $z = t$ จะได้ว่า

$$\begin{aligned} 2x &= 24 + 8s - 14t \\ 2x &= 24 + 4(5 - y) - 14z \\ 2x &= 24 + 20 - 4y - 14z \\ 2x + 4y + 14z &= 44 \end{aligned}$$

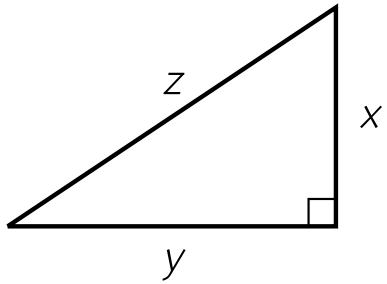
ดังนั้นสมการไดโอแฟนไทน์ที่มีคำตอบดังกล่าวคือ $2x + 4y + 14z = 44$

สมการพีทาโกรัส

ในหัวข้อนี้จะพิจารณาสมการพีทาโกรัส

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

เพื่อศึกษาวิธีการหาคำตอบที่เป็นจำนวนเต็มบวกทั้งหมด ซึ่งเรียกว่าสมการไดโอแฟนไทน์ดีกรีสอง 3 ตัวแปร หรือกล่าวอีกนัยคือการหาความยาวด้านทั้งสามของสามเหลี่ยมมุมฉาก



รูปที่ 3 สามเหลี่ยมมุมฉากแสดงความยาวแต่ละด้าน

ให้ x_0, y_0, z_0 เป็นคำตอบของสมการ $x^2 + y^2 = z^2$ เราเขียนแทนด้วย $\{x_0, y_0, z_0\}$ ตัวอย่างเช่น $\{3, 4, 5\}$ และ $\{5, 12, 13\}$ เป็นต้น

บทนิยาม

ให้ x, y, z เป็นจำนวนเต็มบวกซึ่ง $x < z$ และ $y < z$

สามสิ่งอันดับพีทาโกรัส (Pythagorean Triple) คือ $\{x, y, z\}$ ที่สอดคล้องสมการ

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

ตัวอย่างสามสิ่งอันดับพีทาโกรัส เช่น $\{3, 4, 5\}$, $\{4, 3, 5\}$, $\{7, 24, 25\}$ เป็นต้น

จงตรวจสอบจำนวนต่อไปนี้ว่าเป็นสามสิ่งอันดับพีทาโกรัสหรือไม่

1. $\{15, 8, 17\}$

   วิธีทำ เนื่องจาก $15^2 + 8^2 = 225 + 64 = 289 = 17^2$

   ดังนั้น $\{15, 8, 17\}$ เป็นสามสิ่งอันดับพีทาโกรัส

2. $\{21, 20, 29\}$

   วิธีทำ เนื่องจาก $21^2 + 20^2 = 441 + 400 = 841 = 29^2$

   ดังนั้น $\{21, 20, 29\}$ เป็นสามสิ่งอันดับพีทาโกรัส

3. $\{12, 84, 87\}$

   วิธีทำ เนื่องจาก $12^2 + 84^2 = 144 + 7056 = 7200 \neq 7569 = 87^2$

   ดังนั้น $\{12, 84, 87\}$ ไม่เป็นสามสิ่งอันดับพีทาโกรัส

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

$$x = k, \quad y = \frac{k^2 - 1}{2} \quad \text{และ} \quad z = \frac{k^2 + 1}{2} \quad \text{เมื่อ } k \text{ เป็นจำนวนคี่ที่มากกว่า 1}$$

ซึ่งจะเห็นว่า

$$\begin{aligned} x^2 + y^2 &= k^2 + \left(\frac{k^2 - 1}{2}\right)^2 = k^2 + \frac{k^4 - 2k^2 + 1}{4} \\ &= \frac{k^4 + 2k^2 + 1}{2} = \left(\frac{k^2 + 1}{2}\right)^2 = z^2 \end{aligned}$$

ดังนั้น $\left\{k, \frac{k^2 - 1}{2}, \frac{k^2 + 1}{2}\right\}$ เป็นสามสิ่งอันดับพีทาโกรัส เมื่อ k เป็นจำนวนคี่ที่มากกว่า 1

ตัวอย่างสามสิ่งอันดับพีทาโกรัสจากคำตอบของพีทาโกรัสแสดงดังตารางต่อไปนี้

$x = k$	$y = \frac{k^2 - 1}{2}$	$z = \frac{k^2 + 1}{2}$
3	4	5
5	12	13
7	24	25
9	40	41
11	60	61
13	84	85
15	112	113
17	144	145
19	180	181
21	220	221

$x = k$	$y = \frac{k^2 - 1}{2}$	$z = \frac{k^2 + 1}{2}$
23	264	265
25	312	313
27	364	365
29	420	421
31	480	481
33	544	545
35	612	613
37	684	685
39	760	761
41	840	841

Theorem

ถ้า $\{a, b, c\}$ *เป็นสามสิ่งอันดับพีทาโกรัส และ* $k \in \mathbb{N}$ *แล้ว*

$$\{ka, kb, kc\} \qquad \text{เป็นสามสิ่งอันดับพีทาโกรัส}$$

บทพิสูจน์.

สมมติว่า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $k \in \mathbb{N}$ จะได้ว่า

$$a^2 + b^2 = c^2$$
$$k^2a^2 + k^2b^2 = k^2c^2$$
$$(ka)^2 + (kb)^2 = (kc)^2$$

เนื่องจาก $a < c$, $b < c$ และ $k \in \mathbb{N}$ จะได้ว่า $ka < kc$ และ $kb < kc$
ดังนั้น $\{ka, kb, kc\}$ เป็นสามสิ่งอันดับพีทาโกรัส

Theorem

ถ้า $\{a, b, c\}$ *เป็นสามสิ่งอันดับพีทาโกรัส และ* $d = gcd(a, b, c)$ *แล้ว*

$$\left\{\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right\} \quad \text{เป็นสามสิ่งอันดับพีทาโกรัส}$$

มากกว่านั้นจะได้ด้วยว่า $gcd\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = 1$

บทพิสูจน์.

สมมติว่า $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $d = \gcd(a, b, c)$ จะได้ว่า

$$a^2 + b^2 = c^2$$

$$\frac{a^2 + b^2}{d^2} = \frac{c^2}{d^2}$$

$$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2$$

เนื่องจาก $a < c$, $b < c$ และ $d > 0$ จะได้ว่า $\frac{a}{d} < \frac{c}{d}$ และ $\frac{b}{d} < \frac{c}{d}$

ดังนั้น $\left\{\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right\}$ เป็นสามสิ่งอันดับพีทาโกรัส □

Theorem

ถ้า $\{a, b, c\}$ *เป็นสามสิ่งอันดับพีทาโกรัส และ* $gcd(a, b, c) = 1$ *แล้ว*

$$gcd(a, b) = gcd(a, c) = gcd(b, c) = 1$$

บทพิสูจน์.

ให้ $\{a, b, c\}$ เป็นสามสิ่งอันดับพีทาโกรัส และ $\gcd(a, b, c) = 1$ ให้ $d = \gcd(a, b)$
สมติว่ามีจำนวนเฉพาะ p ซึ่ง $p \mid d$ จะได้ว่า $p \mid a$ และ $p \mid b$ นั่นคือ $p \mid a^2$ และ $p \mid b^2$ ฉะนั้น $p \mid (a^2 + b^2)$ จะได้ว่า $p \mid c^2$ นั่นคือ $p \mid c$ ดังนั้น p เป็นตัวหารของ a, b, c เนื่องจาก $\gcd(a, b, c) = 1$ ดังนั้น $p = 1$ เกิดข้อขัดแย้งที่ p เป็นจำนวนเฉพาะ ดังนั้นไม่มีจำนวนเฉพาะใด ๆ ที่หาร d ลงตัวนั่นคือ $d = 1$ พิสูจน์ในทำนองเดียวกัน $\gcd(a, c) = 1$ และ $\gcd(b, c) = 1$ □

บทนิยาม

เรียกสามสิ่งอันดับพีทาโกรัส $\{a, b, c\}$ ว่า **สามสิ่งอันดับพีทาโกรัสปฐมฐาน (Primitive Pythagorean Triple)** ถ้า $\gcd(a, b, c) = 1$

จงตรวจสอบสามสิ่งอันดับพีทาโกรัสต่อไปนี้ว่าเป็นสามสิ่งอันดับพีทาโกรัสปฐมฐานหรือไม่

1. $\{3, 4, 5\}$
   วิธีทำ เนื่องจาก $\gcd(3, 4, 5) = 1$ ดังนั้น $\{3, 4, 5\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน
2. $\{8, 15, 17\}$
   วิธีทำ เนื่องจาก $\gcd(8, 15, 17) = 1$ ดังนั้น $\{8, 15, 17\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน
3. $\{10, 24, 26\}$
   วิธีทำ เนื่องจาก $\gcd(10, 24, 26) = 2 \neq 1$
   ดังนั้น $\{10, 24, 26\}$ ไม่เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน
4. $\{45, 200, 205\}$
   วิธีทำ เนื่องจาก $\gcd(45, 200, 205) = 5 \neq 1$
   ดังนั้น $\{45, 200, 205\}$ ไม่เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน

Theorem

ถ้า $\{a, b, c\}$ *สามสิ่งอันดับพีทาโกรัสปฐมฐาน จะได้ว่า* $a \not\equiv b \pmod 2$

หมายเหตุ $a \not\equiv b \pmod 2$ หมายความว่า a, b เป็นจำนวนคู่พร้อมกันไม่ได้ และเป็นจำนวนคี่พร้อมกันไม่ได้ นั่นคือถ้าตัวหนึ่งเป็นจำนวนคู่อีกตัวหนึ่งจะเป็นจำนวนคี่

Theorem

$\{a, b, c\}$ *เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน ก็ต่อเมื่อ มีจำนวนเต็ม* u, v *ซึ่ง* $u > v > 0$, $gcd(u, v) = 1$ *และ* $u \not\equiv v \pmod 2$ *ที่ทำให้*

$$a = u^2 - v^2, \qquad b = 2uv \qquad \text{และ} \qquad c = u^2 + v^2$$

จากทฤษฎีบทดังกล่าว ทำให้ทราบว่าสามารถหาสามสิ่งอันดับพีทาโกรัสปฐมฐานได้ไม่จำกัดจำนวน ดังแสดงตัวอย่างตามตาราง

u	v	a	b	c
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65

u	v	a	b	c
7	6	13	84	85
8	1	63	16	65
8	3	55	48	73
8	5	39	80	89
8	7	15	112	113
9	1	80	36	85
9	4	65	72	97
9	5	56	90	106
9	7	32	126	130
9	8	17	144	145

u	v	a	b	c
10	1	99	20	101
10	3	91	60	109
10	7	51	140	149
10	9	19	180	181
11	2	117	44	125
11	4	105	88	137
11	6	85	132	157
11	8	57	176	185
11	10	21	220	221
12	1	143	24	145

ตัวอย่าง

จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐาน โดยใช้ทฤษฎีบท 38
เมื่อ $u = 15$ และ $u = 23$

วิธีทำ กรณี $u = 15$ เนื่องจาก $15 > v$ และ $\gcd(15, v) = 1$ ซึ่ง $15 \not\equiv v \pmod 2$
จะได้ $v = 2, 4, 8, 14$ หาสามสิ่งอันดับพีทาโกรัสปฐมฐาน $\{a, b, c\}$ โดย

$$a = 15^2 - v^2, \qquad b = 2(15)v \qquad \text{และ} \qquad c = 15^2 + v^2$$

สรุปได้ดังตารางต่อไปนี้

u	v	$a = u^2 - v^2$	$b = 2uv$	$c = u^2 + v^2$
15	2	221	60	229
15	4	209	120	241
15	8	161	240	289
15	14	29	420	421

กรณี $u = 23$ เนื่องจาก $23 > v$ และ $\gcd(23, v) = 1$ ซึ่ง $23 \not\equiv v \pmod 2$

จะได้ $v = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22$ หาสามสิ่งอันดับพีทาโกรัสปฐมฐาน $\{a, b, c\}$ โดย

$$a = 23^2 - v^2, \qquad b = 2(23)v \qquad \text{และ} \qquad c = 23^2 + v^2$$

สรุปได้ดังตารางต่อไปนี้

u	v	$a = u^2 - v^2$	$b = 2uv$	$c = u^2 + v^2$
23	2	525	92	533
23	4	513	184	545
23	6	493	276	565
23	8	465	368	593
23	10	429	460	629
23	12	385	552	673
23	14	333	644	725
23	16	273	736	785
23	18	205	828	853
23	20	129	920	929
23	22	45	1012	1013

ในกรณี $u = p$ เมื่อ $p > 2$ เป็นจำนวนเฉพาะ หา v ที่สอดคล้องเงื่อนไข $\gcd(u, v) = 1$ คือ $v = 1, 2, 3, 4, ..., p - 1$ แต่ v ต้องไม่เป็นจำนวนคี่เพราะว่า u เป็นจำนวนคี่ ดังนั้น

$$v = 2, 4, 6, ..., p - 1$$

และจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐานเท่ากับ $\frac{p-1}{2}$ ชุด

ต่อไปจะกล่าวถึงวิธีการหาสามสิ่งอันดับพีทาโกรัสปฐมฐาน $\{a, b, c\}$ เมื่อกำหนด a หรือ b โดยอาศัยทฤษฎีบท 38 จะเห็นว่า $b = 2uv$ เป็นจำนวนคู่ ดังนั้น $a = u^2 - v^2 = (u - v)(u + v)$ เป็นจำนวนคี่ จึงพิจารณาเป็น 2 กรณีคือจำนวนนั้นเป็นจำนวนคี่และเป็นจำนวคู่

กรณี x เป็นจำนวนเต็มคี่

1. แยกตัวประกอบของ x ออกเป็นผลคูณของสองจำนวน
2. เขียนตัวประกอบมากสุดในรูป $u + v$
   เขียนตัวประกอบน้อยสุดในรูป $u - v$
3. แก้สมการใน ข้อ 2. เพื่อหา u และ v
4. หา $\{a, b, c\}$ จาก $a = u^2 - v^2$, $b = 2uv$ และ $c = u^2 + v^2$

ตัวอย่าง

กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัสปฐมฐาน
จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐานที่เป็นไปได้ทั้งหมด

1. 35

   วิธีทำ เนื่องจาก $35 = 1 \cdot 35 = 5 \cdot 7$ จะได้ว่า

$u-v$	$u+v$	u	v	$a=u^2-v^2$	$b=2uv$	$c=u^2+v^2$
1	35	18	17	35	612	613
5	7	6	1	35	12	37

   ดังนั้น $\{35, 12, 37\}$ และ $\{35, 612, 613\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน

2. 51

   วิธีทำ เนื่องจาก $51 = 1 \cdot 51 = 3 \cdot 17$ จะได้ว่า

$u-v$	$u+v$	u	v	$a=u^2-v^2$	$b=2uv$	$c=u^2+v^2$
1	51	26	25	51	1300	1301
3	17	10	7	51	140	149

ในกรณี x เป็นจำนวนคู่ จะได้ $x = 2uv$ และ u, v ไม่เป็นจำนวนคี่พร้อมกัน ดังนั้นมีจำนวนหนึ่งเป็นจำนวนคู่ทำให้ได้ $4 \mid x$ ถ้า $4 \nmid x$ สรุปได้ว่า x ไม่เป็นหนึ่งในจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐาน

กรณี x เป็นจำนวนเต็มคู่

1. ถ้า $4 \nmid x$ แสดงว่า x ไม่เป็นหนึ่งในจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐาน
2. ถ้า $4 \mid x$ แล้ว $x = 2uv$ โดยที่ $\gcd(u, v) = 1$ และ $u > v > 0$ ดังนั้นมี u หรือ v เป็นจำนวนคู่ และอีกจำนวนหนึ่งเป็นจำนวนคี่
3. หา u และ v ที่สอดคล้อง ข้อ 2.
4. หา $\{a, b, c\}$ จาก $a = u^2 - v^2, \quad b = 2uv \quad$ และ $\quad c = u^2 + v^2$

ตัวอย่าง

กำหนดให้จำนวนต่อไปนี้เป็นจำนวนหนึ่งในสามสิ่งอันดับพีทาโกรัสปฐมฐาน
จงหาสามสิ่งอันดับพีทาโกรัสปฐมฐานที่เป็นไปได้ทั้งหมด

1 24

วิธีทำ เนื่องจาก $4 \mid 24$ ดังนั้นพิจารณา $24 = 2(12) = 2(12 \cdot 1) = 2(2 \cdot 6) = 2(3 \cdot 4)$ จะได้ว่า

u	v	$a = u^2 - v^2$	$b = 2uv$	$c = u^2 + v^2$
12	1	143	24	145
4	3	7	24	25

ดังนั้น $\{143, 24, 145\}$ และ $\{7, 24, 25\}$ เป็นสามสิ่งอันดับพีทาโกรัสปฐมฐาน

1 42

วิธีทำ เนื่องจาก $4 \nmid 42$ ดังนั้น 42 ไม่เป็นหนึ่งในจำนวนของสามสิ่งอันดับพีทาโกรัสปฐมฐาน

Lemma

ให้ x เป็นจำนวนเต็ม จะได้ว่า

1. *เศษเหลือที่เกิดจากการหาร x ด้วย 3 เท่ากับ 0 หรือ 1 เท่านั้น*
2. *เศษเหลือที่เกิดจากการหาร x ด้วย 5 เท่ากับ 0 หรือ 1 หรือ 4 เท่านั้น*

บทพิสูจน์.

ให้ x เป็นจำนวนเต็ม

1. โดยขั้นตอนการหารจะได้ว่า $x \equiv 0$ หรือ 1 หรือ $2 \pmod 3$ นั่นคือ $x^2 \equiv 0$ หรือ 1 หรือ $4 \pmod 3$
   สรุปได้ว่า $x^2 \equiv 0$ หรือ $1 \pmod 3$
2. โดยขั้นตอนการหารจะได้ว่า $x \equiv 0$ หรือ 1 หรือ 2 หรือ 3 หรือ $4 \pmod 5$
   นั่นคือ $x^2 \equiv 0$ หรือ 1 หรือ 4 หรือ 9 หรือ $16 \pmod 5$ สรุปได้ว่า $x^2 \equiv 0$ หรือ 1 หรือ $4 \pmod 5$

Theorem

ถ้า $\{a, b, c\}$ *เป็นสามสิ่งอันดับพีทาโกรัส จะได้ว่า*

1. $3 \mid a$ *หรือ* $3 \mid b$
2. $5 \mid a$ *หรือ* $5 \mid b$ *หรือ* $5 \mid c$

Theorem

ให้ $\{a, b, c\}$ *และ* $\{x, y, z\}$ *เป็นสามสิ่งอันดับพีทาโกรัส จะได้ว่า*

$$\{|by - ax|, bx + ay, cz\} \text{ เป็นสามสิ่งอันดับพีทาโกรัส}$$

Theorem

ให้ $\{a, b, c\}$ *และ* $\{x, y, z\}$ *เป็นสามสิ่งอันดับพีทาโกรัส จะได้ว่า*

$$\{|by - ax|, bx + ay, cz\} \text{ เป็นสามสิ่งอันดับพีทาโกรัส}$$

บทพิสูจน์.

สมมติว่า $\{a, b, c\}$ และ $\{x, y, z\}$ จะได้ว่า $a^2 + b^2 = c^2$ และ $x^2 + y^2 = z^2$ แล้ว

$$\begin{aligned} |by - ax|^2 + (bx + ay)^2 &= b^2y^2 - 2abxy + a^2x^2 + b^2x^2 + 2abxy + a^2y^2 \\ &= b^2(y^2 + x^2) + a^2(x^2 + y^2) \\ &= (a^2 + b^2)(x^2 + y^2) \\ &= c^2z^2 \end{aligned}$$

ดังนั้น $\{|by - ax|, bx + ay, cz\}$ เป็นสามสิ่งอันดับพีทาโกรัส □

บทแทรก

ให้ $\{a, b, c\}$ จะได้ว่า $\{|b^2 - a^2|, 2ab, c^2\}$ เป็นสามสิ่งอันดับพีทาโกรัส

ตัวอย่าง

จงหาสามจำนวนของปีทาโกรัส ที่เกิดจากสามจำนวนของปีทาโกรัสที่กำหนดให้

1. $\{3,4,5\}$ และ $\{3,4,5\}$
   วิธีทำ จะได้ว่า $4^2-3^2=7$, $2(3)(4)=24$ และ $5^2=25$
   ดังนั้น $\{7,24,25\}$ เป็นสามสิ่งอันดับพีทาโกรัส

2. $\{3,4,5\}$ และ $\{5,12,13\}$
   วิธีทำ จะได้ว่า $4(12)-3(5)=33$, $3(12)+4(5)=56$ และ $5(13)=65$
   ดังนั้น $\{33,56,65\}$ เป็นสามสิ่งอันดับพีทาโกรัส

3. $\{3,4,5\}$ และ $\{8,15,17\}$
   วิธีทำ จะได้ว่า $4(15)-3(8)=36$, $3(15)+4(8)=77$ และ $5(17)=85$
   ดังนั้น $\{36,77,85\}$ เป็นสามสิ่งอันดับพีทาโกรัส

4. $\{8,15,17\}$ และ $\{7,24,25\}$
   วิธีทำ จะได้ว่า $15(24)-8(7)=304$, $8(24)+15(7)=297$ และ $17(25)=425$
   ดังนั้น $\{297,304,425\}$ เป็นสามสิ่งอันดับพีทาโกรัส

สมการไดโอแฟนไทน์กำลังสอง

Theorem

ให้ c เป็นจำนวนเต็ม สมการ $x^2 - y^2 = c$ มีคำตอบเป็นจำนวนเต็ม ก็ต่อเมื่อ

$$c \text{ เป็นจำนวนเต็มคี่ หรือ } 4 \mid c$$

บทพิสูจน์.

c เป็นจำนวนเต็ม ให้ x_0, y_0 เป็นคำตอบของสมการ $x^2 - y^2 = c$ ดังนั้น $x_0^2 - y_0^2 = c$

กรณี $x_0 \equiv y_0 \pmod 2$ จะได้ว่า $x_0 \equiv -y_0 \pmod 2$ ดังนั้น $2 \mid (x_0 + y_0)$ และ $2 \mid (x_0 + y_0)$

นั่นคือ $4 \mid (x_0^2 - y_0^2)$ ดังนั้น $4 \mid c$

กรณี $x_0 \not\equiv y_0 \pmod 2$ จะได้ว่า x, y ไม่เป็นจำนวนคู่พร้อมกัน หรือไม่เป็นจำนวนคี่พร้อมกัน ดังนั้น $x^2 - y^2 = c$ เป็นจำนวนคี่

ในทางกลับกัน สมมติว่า c เป็นจำนวนคี่ นั่นคือ $c = 2k + 1$ สำหรับบางจำนวนเต็ม k เลือก $x_0 = k + 1$ และ $y_0 = k$ จะได้ว่า

$$\begin{aligned} x^2 - y^2 &= (x - y)(x + y) \\ &= (k + 1 - k)(k + 1 + k) \\ &= 2k + 1 \\ &= c \end{aligned}$$

ดังนั้น x_0, y_0 เป็นคำตอบของสมการ $x^2 - y^2 = c$ ถ้า $4 \mid c$ ให้ $c = 4q$ สำหรับบางจำนวนเต็ม q เลือก $x_0 = q + 1$ และ $y_0 = q - 1$ จะได้ว่า

$$\begin{aligned} x^2 - y^2 &= (x - y)(x + y) \\ &= (q + 1 - q + 1)(q + 1 + q - 1) \\ &= 4q \\ &= c \end{aligned}$$

ดังนั้น x_0, y_0 เป็นคำตอบของสมการ $x^2 - y^2 = c$

□

ตัวอย่าง

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 15$

วิธีทำ จาก $x^2 - y^2 = (x-y)(x+y)$ จะได้ว่า $(x-y)(x+y) = 15 = 1 \cdot 15 = 3 \cdot 5$ พิจารณาได้ดังตารางต่อไปนี้

$x-y$	$x+y$	x	y
1	15	8	7
-1	-15	-8	-7
15	1	8	-7
-15	-1	-8	7
3	5	4	1
-3	-5	-4	-1
5	3	4	-1
-5	-3	-4	1

ดังนั้นคำตอบที่สอดคล้องสมการนี้คือ $(8,7), (8,-7), (-8,7), (-8,-7), (4,1), (-4,1), (4,-1)$ และ $(-4,-1)$

ตัวอย่าง

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 - y^2 = 24$

วิธีทำ จาก $x^2 - y^2 = (x-y)(x+y)$ จะได้ว่า $(x-y)(x+y) = 24 = 1 \cdot 24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6$ x, y จะเป็นจำนวนเต็มก็ต่อเมื่อตัวประกอบทั้งคู่เป็นจำนวนคู่พร้อมกัน พิจารณาได้ดังตารางต่อไปนี้

$x-y$	$x+y$	x	y
2	12	7	5
-2	-12	-7	-5
12	2	7	-5
-12	-2	-7	5
4	6	5	1
-4	-6	-5	-1
6	4	5	-1
-6	-4	-5	1

ดังนั้นคำตอบที่สอดคล้องสมการนี้คือ $(7,5), (7,-5), (-7,5), (-7,-5), (5,1), (-5,1), (5,-1)$ และ $(-5,-1)$

Theorem

ให้ $c \in \mathbb{Z}$ แล้วมีจำนวนเต็ม x, y, z ซึ่ง $x^2 + y^2 - z^2 = c$

บทพิสูจน์.

c เป็นจำนวนเต็ม จะมีจำนวนเต็ม x ซึ่ง $c - x^2$ เป็นจำนวนคี่ ดังนั้นโดยทฤษฎีบท 43 นั่นคือมีจำนวนเต็ม y, z ที่ทำให้ $y^2 - z^2 = c - x^2$ นั่นคือมีจำนวนเต็ม x, y, z ซึ่ง $x^2 + y^2 - z^2 = c$ □

ตัวอย่าง

จงหาคำตอบของสมการไดโอแฟนไทน์ $x^2 + y^2 - z^2 = 8$ มาอย่างน้อย 5 ชุดคำตอบ

วิธีทำ พิจารณา $y^2 - z^2 = 8 - x^2$ จะได้ว่า $(y - z)(y + z) = 8 - x^2$
พิจารณา $8 - x^2$ เป็นจำนวนคี่ นั่นคือ x เป็นจำนวนคี่ จะได้ว่าสำหรับบางจำนวนเต็ม k, t จะได้ $8 - x^2 = 2k + 1$ และ $x = 2t + 1$ แล้ว

$$8 - (2t + 1)^2 = 2k + 1$$

$$8 - 4t^2 - 4t - 1 = 2k + 1$$

$$6 - 4t^2 - 4t = 2k$$

$$3 - 2t^2 - 2t = k$$

จาก $(y - z)(y + z) = 8 - x^2$ นั่นคือ $(y - z)(y + z) = 2k + 1 = 1 \cdot (2k + 1)$
เลือก $y - z = 1$ และ $y + z = 2k + 1$ จะได้ว่า $y = k + 1$ และ $z = k$ ดังนั้นคำตอบรูปแบบหนึ่งของสมการ $x^2 + y^2 - z^2 = 8$ นี้คือ

$$\begin{aligned} x &= 2t + 1 \\ y &= k + 1 \quad \text{เมื่อ } t, k \in \mathbb{Z} \text{ และ } k = 3 - 2t^2 - 2t \\ z &= k \end{aligned}$$

ตารางต่อไปนี้แสดงคำตอบบางชุดของสมการ $x^2 + y^2 - z^2 = 8$

t	$k = 3 - 2t^2 - 2t$	$x = 2t + 1$	$y = k + 1$	$z = k$
-1	3	-1	4	3
0	3	1	4	3
1	-1	3	0	-1
2	-9	5	-8	-9

ตัวอย่าง

จงหาจำนวนเต็มบวก a, b, c ที่เป็นคำตอบของสมการ

$$a^3 - b^3 - c^3 = 3abc$$

$$a^2 = 2(b + c)$$

วิธีทำ เนื่องจาก $3abc$ เป็นจำนวนเต็มบวก จะได้ว่า $b^3 < a^3$ และ $c^3 < a^3$ นั่นคือ $b < a$ และ $c < a$ ดังนั้น $b + c < 2a$ แล้ว

$$a^2 = 2(b + c) < 4a$$

ฉะนั้น $a < 4$ นั่นคือ $a = 1, 2, 3$ เนื่องจาก $a^2 = 2(b + c)$ แสดงว่า a เป็นจำนวนคู่ ดังนั้น $a = 2$ ทำให้ได้ว่า และ $2^2 = 2(b + c)$ นั่นคือ $b + c = 2$ จะได้ $b = c = 1$

บทที่ 8 ทฤษฎีบทเศษเหลือ

พหุนาม

บทนิยาม

ให้ $n \in \mathbb{N} \cup \{0\}$ แล้ว

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

เรียกว่า **พหุนาม** (polynomial) และ $a_n, a_{n-1}, \ldots, a_1, a_0$ เรียกว่า **สัมประสิทธิ์** (coefficient) ของ $x^n, x^{n-1}, \ldots, x, 1$ ตามลำดับ ถ้า $a_n \neq 0$ เรียกว่า พหุนามดีกรี n และเขียน n แทนด้วย $\deg P(x)$

เรียก $a_n \neq 0$ ว่า **สัมประสิทธิ์ตัวนำ** (leading coefficient)

กรณี $a_n = 1$ เรียก $P(x)$ ว่า **พหุนามโมนิก** (monic polynomial)

กรณี $\deg P(x) = 0$ หรือ $P(x) = a_0 \neq 0$ เรียก $P(x)$ ว่า **พหุนามคงตัว** (constant polynomial)

กรณี $P(x) = 0$ เรียก **พหุนามศูนย์** (zero polynomaial) และไม่นิยามดีกรีสำหรับพหุนามศูนย์

กำหนดเซตของพหุนามขึ้นกับชนิดของสัมประสิทธิ์ดังต่อไปนี้

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z} \text{ และ } n \in \mathbb{N} \cup \{0\}\}$$

$$\mathbb{R}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R} \text{ และ } n \in \mathbb{N} \cup \{0\}\}$$

ตัวอย่าง

จงบอกองค์ประกอบของพหุนามต่อไปนี้

1. $1 + 2x + x^3$
   เป็นพหุนามโมนิกดีกรี 3 ที่มี $1, 2, 0, 1$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3$ ตามลำดับ
2. $-2x^4 + 1.5x - 5$
   เป็นพหุนามดีกรี 4 ที่มี $-5, 1.5, 0, 0, -2$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3, x^4$ ตามลำดับ
   มีสัมประสิทธิ์ตัวนำคือ -2
3. $3x^5 - \frac{3}{5}x^4 + \sqrt{2}$
   เป็นพหุนามดีกรี 5 ที่มี $\sqrt{2}, 0, 0, 0, -\frac{3}{5}, 3$ เป็นสัมประสิทธิ์ของ $1, x, x^2, x^3, x^4, x^5$ ตามลำดับ
   มีสัมประสิทธิ์ตัวนำคือ 3
4. $x^{1.5} + x + 1$
   ไม่เป็นพหุนามเนื่องจากมีเลขยกกำลังของ x เป็น 1.5

บทนิยาม

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนาม แล้ว $P(x) = Q(x)$
ถ้า $\deg P(x) = \deg Q(x)$ และอยู่ในรูป

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

เมื่อ $n \in \mathbb{N} \cup \{0\}$ และ $a_n = b_n,\ a_{n-1} = b_{n-1}, \ldots, a_1 = b_1, a_0 = b_0$

เมื่อพิจารณาพหุนาม $P(x)$ และ $Q(x)$ ในแง่ของฟังก์ชันจะได้ว่า P และ Q เป็นฟังก์ชันบนจำนวนจริง ดังนั้น
$P = Q$ ก็ต่อเมื่อ $P(x) = Q(x)$ ทุก ๆ $x \in \mathbb{R}$

บทนิยาม

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนามซึ่ง

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

เมื่อ $m, n \in \mathbb{N} \cup \{0\}$ และ $m \leq n$ แล้ว

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_{m+1} x^{m+1} + a_m x^m + \cdots + a_1 x + a_0$$

โดยที่ $a_{m+1} = a_{m+2} = \ldots = a_n = 0$ เมื่อ $m < n$ นิยามการบวกและการคูณ $P(x)$ และ $Q(x)$ คือ

$$P(x) + Q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

$$P(x) \cdot Q(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \cdots + c_k x^k + \cdots + c_1 x + c_0$$

เมื่อ $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ โดยที่ $k = 0, 1, 2, \ldots, m+n$ ซึ่ง $a_k = b_k = 0$ ทุก ๆ $k > n$

สำหรับการคูณอาจทำได้โดยการใช้กฎการแจกแจงจากนั้นรวมพจน์ที่คล้ายกันเข้าด้วยกัน หรืออาจใช้ grid method ทำได้ดังนี้

	$a_m x^m$	$a_{m-1} x^{m-1}$	$a_{m-2} x^{m-2}$	$\cdots$	$a_1 x$	a_0
$b_n x^n$	$a_m b_n x^{m+n}$	$a_{m-1} b_n x^{m+n-1}$	$a_{m-2} b_n x^{m+n-2}$	$\cdots$	$a_1 b_n x^{n+1}$	$a_0 b_n x^n$
$b_{n-1} x^{n-1}$	$a_m b_{n-1} x^{m+n-1}$	$a_{m-1} b_{n-1} x^{m+n-2}$	$a_{m-2} b_{n-1} x^{m+n-3}$	$\cdots$	$a_1 b_{n-1} x^n$	$a_0 b_{n-1} x^{n-1}$
$b_{n-2} x^{n-2}$	$a_m b_{n-2} x^{m+n-2}$	$a_{m-1} b_{n-2} x^{m+n-3}$	$a_{m-2} b_{n-2} x^{m+n-4}$	$\cdots$	$a_1 b_{n-2} x^{n-1}$	$a_0 b_{n-2} x^{n-2}$
$\vdots$				$\vdots$		
$b_1 x$	$a_m b_1 x^{m+1}$	$a_{m-1} b_1 x^{m-2}$	$a_{m-2} b_1 x^{m-3}$	$\cdots$	$a_1 b_1 x^2$	$a_0 b_1 x$
$b_0 x$	$a_m b_0 x^m$	$a_{m-1} b_0 x^{m-1}$	$a_{m-2} b_0 x^{m-2}$	$\cdots$	$a_1 b_0 x$	$a_0 b_0$

ตัวอย่าง

กำหนดให้ $P(x) = x^3 + x^2 - 3x + 1$ และ $Q(x) = x^2 - 3$

จงหา $P(x) + Q(x)$ และ $P(x) \cdot Q(x)$

วิธีทำ จะได้ว่า

$$\begin{aligned} P(x) + Q(x) &= (x^3 + x^2 - 3x + 1) + (x^2 - 3) = (x^3 + x^2 - 3x + 1) + (0x^3 + x^2 + 0x - 3) \\ &= (1 + 0)x^3 + (1 + 1)x^2 + (-3 + 0)x + (1 - 3) \\ &= x^3 + 2x^2 - 3x - 2 \end{aligned}$$

สำหรับการคูณ $P(x) \cdot Q(x)$ จะแสดงให้วิธีการคูณทั้ง 3 วิธี ดังนี้

1. โดยบทนิยาม ให้ $a_0 = 1, a_1 = -3, a_2 = 1, a_3 = 1, a_4 = a_5 = 0$ และ $b_0 = -3, b_1 = 0, b_2 = 1, b_3 = b_4 = b_5 = 0$ จะได้ว่า

$$\begin{array}{lllll} c_0 & = a_0 b_0 & = 1(-3) & = & -3 \\ c_1 & = a_0 b_1 + a_1 b_0 & = 0 - 3(-3) & = & 9 \\ c_2 & = a_0 b_2 + a_1 b_1 + a_2 b_0 & = 1(1) + 0 + 1(-3) & = & -2 \\ c_3 & = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 & = 0 - 3(1) + 0 + 1(-3) & = & -6 \\ c_4 & = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 & = 0 + 0 + 1(1) + 0 + 0 & = & 1 \\ c_5 & = a_0 b_5 + a_1 b_4 + a_2 b_3 + a_3 b_2 + a_4 b_1 + a_5 b_0 & = 0 + 0 + 0 + 1(1) + 0 + 0 & = & 1 \end{array}$$

ดังนั้น

$$\begin{aligned} P(x)\cdot Q(x) &= (x^3+x^2-3x+1)(x^2-3) \\ &= c_5x^5+c_4x^4+c_3x^3+c)2x^2+c_1x+c_0 \\ &= x^5+x^4-6x^3-2x^2+9x-3 \end{aligned}$$

2. โดยวิธีการแจกแจง

$$\begin{aligned} P(x)\cdot Q(x) &= (x^3+x^2-3x+1)(x^2-3) \\ &= x^5-3x^3+x^4-3x^2-3x^3+9x+x^2-3 \\ &= x^5+x^4-6x^3-2x^2+9x-3 \end{aligned}$$

3. โดย grid method

	x^3	x^2	$-3x$	1
x^2	x^5	x^4	$-3x^3$	x^2
$0x$	$0x^4$	$0x^3$	$0x^2$	$0x$
-3	$-3x^3$	$-3x^2$	$9x$	-3

ดังนั้น

$$\begin{aligned} P(x)\cdot Q(x) &= x^5+(1+0)x^4+(-3+0-3)x^3+(1+0-3)x^2+(0+9)x^3 \\ &= x^5+x^4-6x^3-2x^2+9x-3 \end{aligned}$$

ตัวอย่าง

กำหนดให้ $Ax^3 + Bx^2 + Cx + D = (x-2)(x+3)(x+1) + 7$ ทุก ๆ $x \in \mathbb{R}$ จงหาค่าของ A, B และ C

วิธีทำ พิจารณา

$$\begin{aligned} Ax^3 + Bx^2 + Cx + D &= (x-2)(x+3)(x+1) + 7 \\ &= (x^2 + x - 6)(x+1) + 7 \\ &= x^3 + 2x^2 - 5x + 1 \end{aligned}$$

ดังนั้น $A = 1, B = 2, C = -5$ และ $D = 1$

ตัวอย่าง

ถ้า a, b, c และ d เป็นจำนวนเต็มซึ่ง $(x-1)^2(ax+b) = cx^3 + dx + 4$ ทุก ๆ $x \in \mathbb{R}$ แล้ว $a+b+c+d$ เท่ากับเท่าใด

วิธีทำ พิจารณา

$$\begin{aligned} (x-1)^2(ax+b) &= cx^3 + dx + 4 \\ (x^2 - 2x + 1)(ax+b) &= cx^3 + dx + 4 \\ ax^3 + (b-2a)x^2 + (a-2b)x + b &= cx^3 + dx + 4 \end{aligned}$$

จะได้ว่า $b = 4$, $a - 2b = d$, $b - 2a = 0$ และ $a = c$ ดังนั้น $a = 2, c = 2, d = -6$ แล้วจะได้ว่า $a+b+c+d = 2+4+2-6 = 2$

ตัวอย่าง

จงหาค่าของ A, B และ C ที่ทำให้

พหุนาม $A(x-1)(x-2)+B(x-1)(x-3)+C(x-2)(x-3)$ เท่ากับพหุนามคงตัว 1

วิธีทำ สำหรับจำนวนจริง x ใด ๆ จะได้ว่า

$$A(x-1)(x-2)+B(x-1)(x-3)+C(x-2)(x-3)=1$$

เมื่อ $x=1$ จะได้ว่า $A(0)(-1)+B(0)(-2)+C(-1)(-2)=1$ นั่นคือ $2C=1$ ดังนั้น $C=\frac{1}{2}$
เมื่อ $x=2$ จะได้ว่า $A(1)(0)+B(1)(-1)+C(0)(-1)=1$ นั่นคือ $-B=1$ ดังนั้น $B=-1$
เมื่อ $x=3$ จะได้ว่า $A(2)(1)+B(2)(0)+C(1)(0)=1$ นั่นคือ $2A=1$ ดังนั้น $A=\frac{1}{2}$

Theorem

ให้ $P(x), Q(x) \in \mathbb{Z}[x]$ *ซึ่ง* $P(x)$ *และ* $Q(x)$ *ไม่ใช่พหุนามศูนย์ จะได้ว่า*

$$deg\ (P(x) + Q(x)) \leq \max\{deg\ P(x), deg\ Q(x)\}$$

$$deg\ (P(x) \cdot Q(x)) = deg\ P(x) + deg\ Q(x)$$

เมื่อ $\max\{deg\ P(x), deg\ Q(x)\}$ *คือค่ามากสุดของ* $deg\ P(x)$ *และ* $deg\ Q(x)$

Theorem

ขั้นตอนวิธีการหาร (The Division Algorithm)

ให้ $P(x)$ และ $S(x)$ เป็นพหุนาม โดยที่ $S(x)$ ไม่ใช่พหุนามศูนย์ แล้วจะมีพหุนาม $Q(x)$ และ $R(x)$ เพียงคู่เดียวที่สอดคล้องกับ

$$P(x) = Q(x)S(x) + R(x) \qquad \text{เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x)$$

*เรียก $Q(x)$ ว่า**ผลหาร** และ $R(x)$ ว่า**เศษเหลือ***

ข้อสังเกต ถ้า $R(x) = 0$ แล้วจะได้ว่า $S(x)$ หาร $P(x)$ ลงตัว หรือ $S(x)$ เป็นตัวประกอบของ $P(x)$

ตัวอย่าง

จงเขียนขั้นตอนวิธีการหารของ $S(x)$ หาร $P(x)$

1. $S(x) = x - 1$ และ $P(x) = x^3 + 2x^3 + 3x^2 + 4x + 5$
   วิธีทำ พิจารณา

$$\begin{aligned} P(x) &= x^3 + 2x^3 + 3x^2 + 4x + 5 \\ &= (x^3 - 3x^2 + 3x - 1) + 5x^2 + x + 6 \\ &= (x-1)^3 + 5(x^2 - 2x + 1) + 11x + 1 \\ &= (x-1)^3 + 5(x-1)^2 + 11(x-1) + 12 \\ &= (x-1)[(x-1)^2 + 5(x-1) + 11] + 12 \\ &= (x-1)(x^2 + 3x - 3) + 12 \end{aligned}$$

   ดังนั้น $P(x) = S(x)(x^2 + 3x - 3) + 12$

2. $S(x) = x^2 - 1$ และ $P(x) = x^4 + x^3 + x^2 + x + 1$
   วิธีทำ พิจารณา

$$\begin{aligned} P(x) &= x^4 + x^3 + x^2 + x + 1 \\ &= (x^4 - 2x^2 + 1) + x^3 + 3x^2 + x \\ &= (x^2 - 1)^2 + x(x^2 - 1) + 3x^2 + 2x \\ &= (x^2 - 1)^2 + x(x^2 - 1) + 3(x^2 - 1) + 2x + 3 \end{aligned}$$

การเขียนขั้นตอนวิธีการหารอาจใช้ **การหารยาว (long division)** เพื่อหาผลหารและเศษเหลือ ดังตัวอย่างต่อไปนี้

ตัวอย่าง

จงเขียนขั้นตอนวิธีการหารของ x^2+x+1 หาร $x^5+3x^3+2x^2+x-3$

วิธีทำ พิจารณาการเขียนขั้นตอนวิธีการหาร 2 วิธีคือ

วิธีที่ 1. จัดรูปพหุนาม $x^5+3x^3+2x^2+x-3$ ในรูป x^2+x+1

$$\begin{aligned}
x^5+3x^3+2x^2+x-3 &= x^3(x^2+x+1)-x^4+2x^3+2x^2+x-3\\
&= x^3(x^2+x+1)-x^2(x^2+x+1)+3x^3+3x^2+x-3\\
&= x^3(x^2+x+1)-x^2(x^2+x+1)+3x(x^2+x+1)-2x-3\\
&= (x^2+x+1)(x^3-x^2+3x)-2x-3
\end{aligned}$$

วิธีที่ 2. การหารยาว

$$\begin{array}{r|lllllllllll}
 & & & & & x^3 & - & x^2 & + & 3x & & \\
\hline
x^2+x+1 & & x^5 & + & 0x^4 & + & 3x^3 & + & 2x^2 & + & x & - & 3 \\
 & - & (x^5 & + & x^4 & + & x^3) & & & & & & \\
 & & & - & x^4 & + & 2x^3 & + & 2x^2 & + & x & - & 3 \\
 & & -(& - & x^4 & - & x^3 & - & x^2) & & & & \\
 & & & & & & 3x^3 & + & 3x^2 & + & x & - & 3 \\
 & & & & & -(& 3x^3 & + & 3x^2 & + & 3x) & & \\
 & & & & & & & & & - & 2x & - & 3
\end{array}$$

ดังนั้น $x^5+3x^3+2x^2+x-3=(x^2+x+1)(x^3-x^2+3x)-2x-3$

ตัวอย่าง

ให้ $P(x) = x^3 + ax^2 + bx + 10$ เมื่อ a, b เป็นจำนวนเต็ม และ $Q(x) = x^2 + 9$ ถ้า $Q(x)$ หาร $P(x)$ เศษเหลือเท่ากับ 1 แล้ว $P(a+b)$ เท่ากับเท่าใด

วิธีทำ โดยขั้นตอนการหารจะได้มีพหุนาม $F(x)$ ซึ่ง

$$P(x) = Q(x)F(x) + 1$$

$$x^3 + ax^2 + bx + 10 = (x^2 + 9)F(x) + 1$$

ดังนั้น $\deg F(x) = 1$ ให้ $F(x) = cx + d$ แล้ว

$$\begin{aligned} x^3 + ax^2 + bx + 10 &= (x^2 + 9)(cx + d) + 1 \\ &= cx^3 + dx^2 + 9cx + 9d + 1 \end{aligned}$$

จะได้ว่า $c = 1$, $d = a$, $b = 9c$, $10 = 9d + 1$ ดังนั้น $a = 1$ และ $b = 9$ แล้ว

$$P(1 + 9) = P(10) = 10^3 + 10^2 + 9(10) + 10 = 1200$$

บทนิยาม

ให้ $P(x)$ และ $Q(x)$ เป็นพหุนาม จะกล่าวว่า $Q(x)$ **หาร** $P(x)$ **ลงตัว** เขียนแทนด้วย $Q(x) \mid P(x)$ ถ้ามีพหุนาม $S(x)$ ซึ่ง $P(x) = Q(x)S(x)$ หรือกล่าวอีกนัยคือเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วย $Q(x)$ เท่ากับ 0 และเรียก $Q(x)$ ว่า **ตัวประกอบ (factor)** ของ $P(x)$

ตัวอย่าง

จงแสดงว่า x^3+1 หาร $x^5-x^4+5x^3+x^2-x+5$ ลงตัว

วิธีทำ พิจารณา

$$\begin{aligned} x^5-x^4+5x^3+x^2-x+5 &= x^2(x^3+1)-x^4+5x^3-x+5 \\ &= x^2(x^3+1)-x(x^3+1)+5x^3+5 \\ &= x^2(x^3+1)-x(x^3+1)+5(x^3+1) \\ &= (x^2-x+5)(x^3+1) \end{aligned}$$

ดังนั้น x^3+1 หาร $x^5-x^4+5x^3+x^2-x+5$ ลงตัว

ตัวอย่าง

จงหาตัวประกอบทั้งหมดของ $x^4 - 13x^2 + 36$

วิธีทำ พิจารณา

$$\begin{aligned} x^4 - 13x^2 + 36 &= (x^2 - 4)(x^2 - 9) \\ &= (x-2)(x+2)(x-3)(x+3) \end{aligned}$$

ดังนั้น $x-2, x+2, x-3$ และ $x+3$ เป็นตัวประกอบของ $x^4 - 13x^2 + 36$

ทฤษฎีเศษเหลือ

Theorem

ทฤษฎีบทเศษเหลือ (The Remainder Theorem)

ให้ $P(x)$ เป็นพหุนาม และ $c \in \mathbb{R}$ แล้ว

$$x-c \quad \text{หาร} \quad P(x) \quad \text{เศษเหลือเท่ากับ} \quad P(c)$$

บทพิสูจน์.

จากขั้นตอนวิธีการหาร $x-c$ หาร $P(x)$ จะได้ว่ามี $Q(x)$ และ $R(x)$ ซึ่ง

$$P(x) = Q(x)(x-c) + R(x) \text{ เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < 1$$

กรณี $R(x) = 0$ จะได้ว่า $P(x) = Q(x)(x-c)$ แล้ว $P(c) = R(x)$

กรณี $\deg R(x) = 0$ แล้ว $R(x) = d$ เมื่อ d เป็นค่าคงที่ จะได้ว่า $P(x) = Q(x)(x-c) + d$

แล้ว $P(c) = d = R(x)$ □

บทแทรก

ให้ $P(x)$ เป็นพหุนามซึ่ง $\deg P(x) > 0$ และ $c \in \mathbb{R}$ แล้ว

$$x - c \text{ เป็นตัวประกอบของ } P(x) \quad \text{ก็ต่อเมื่อ} \quad P(c) = 0$$

บทพิสูจน์.

ให้ $P(x)$ เป็นพหุนามซึ่ง $\deg P(x) > 0$ และ $c \in \mathbb{R}$ สมมติว่า $x - c$ เป็นตัวประกอบของ $P(x)$ นั่นคือ $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ 0 โดยทฤษฎีบท 47 จะได้ว่า $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ $P(c)$ ดังนั้น $P(c) = 0$ ในทางกลับกันสมมติว่า $P(c) = 0$ โดยทฤษฎีบท 47 เมื่อ $x - c$ หาร $P(x)$ เศษเหลือเท่ากับ $P(c) = 0$ ดังนั้น $x - c$ เป็นตัวประกอบของ $P(x)$ □

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วยตัวหารที่กำหนดในแต่ละข้อต่อไปนี้

1. $x-1$ หาร $P(x)=x^4-x^3+4x^2+5x+2$

   วิธีทำ เศษเหลือเท่ากับ $P(1)=1^4-1^3+4(1)^2+5(1)+2=11$

2. $x+2$ หาร $P(x)=x^3+2x^2+x-3$

   วิธีทำ เศษเหลือเท่ากับ $P(-2)=(-2)^3+2(-2)^2+(-2)-3=-5$

ตัวอย่าง

จงหาค่า k ที่ทำให้ $x+1$ หาร $3x^4+2x^2+kx-5$ เศษเหลือเท่ากับ -3

วิธีทำ จะได้ว่า

$$\begin{aligned} 3(-1)^4+2(-1)^2+k(-1)-5&=-3\\ 3+2-k-5&=-3\\ k&=3 \end{aligned}$$

ตัวอย่าง

ถ้าพหุนาม $6x^3 + ax^2 + bx - 1$ หารด้วย $x - 1$ ลงตัว แต่หารด้วย $x + 1$ เศษเหลือเท่ากับ -24 แล้ว $2a - b$ เท่ากับเท่าใด

วิธีทำ จะได้ว่า

$$6(-1)^3 + a(-1)^2 + b(-1) - 1 = 0$$
$$a - b = 7$$

และ

$$6(1)^3 + a(1)^2 + b(1) - 1 = -24$$
$$a + b = -29$$

ดังนั้น $a = -11$ และ $b = -18$ แล้ว $2a - b = 2(-11) - (-18) = -4$

ตัวอย่าง

ให้ $P(x)$ เป็นพหุนาม ถ้าหาร $P(x)$ ด้วย $x-1$ จะเศษเหลือเท่ากับ 3 และถ้าหาร $P(x)$ ด้วย $x-3$ จะเศษเหลือเท่ากับ 5 ถ้า $r(x)=ax+b$ คือเศษเหลือจากการหาร $P(x)$ ด้วย $(x-1)(x-3)$ แล้ว $3a+2b$ เท่ากับเท่าใด

วิธีทำ โดยทฤษฎีบทเศษเหลือจะได้ว่า $P(1)=3$ และ $P(3)=5$
และโดยขั้นตอนวิธีการหารพหุนาม $Q(x)$ ซึ่ง

$$P(x)=(x-1)(x-3)Q(x)+ax+b$$

แล้ว

$$3=P(1)=0+a+b$$

$$5=P(3)=0+3a+b$$

ดังนั้น $a=1$ และ $b=2$ แล้ว $3a+2b=3(1)+2(2)=7$

จากทฤษฎีบทเศษเหลือ เมื่อ $x-c$ หาร $P(x)$ จะได้เศษเหลือเท่ากับ $P(c)$ จะได้ว่า

$$P(x) = (x-c)Q(x) + P(c)$$

ให้ $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ เป็นพหุนามดีกรี n ซึ่ง $n \geq 1$ จะได้ว่า $\deg Q(x) = n-1$ นั่นคือให้

$$Q(x) = q_{n-1}x^{n-1} + \cdots + q_1 x + q_0$$

ดังนั้น

$$\begin{aligned} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 &= (q_{n-1}x^{n-1} + \cdots + q_1 x + q_0)(x-c) + P(c) \\ &= q_{n-1}x^n + q_{n-2}x^{n-1} + \cdots + q_0 x \\ &\quad - cq_{n-1}x^{n-1} - \cdots - cq_1 x + cq_0 + P(c) \end{aligned}$$

จะได้ว่า

$$
\begin{array}{lllll}
q_{n-1} & & = & a_n & \\
q_{n-2} - cq_{n-1} & = & a_{n-1} & \text{หรือ} & q_{n-2} = a_{n-1} + cq_{n-1} \\
q_{n-3} - cq_{n-2} & = & a_{n-2} & \text{หรือ} & q_{n-3} = a_{n-2} + cq_{n-2} \\
 & \vdots & & & \vdots \\
q_1 - cq_2 & = & a_2 & \text{หรือ} & q_1 = a_2 + cq_2 \\
q_0 - cq_1 & = & a_1 & \text{หรือ} & q_0 = a_1 + cq_1 \\
P(c) - cq_0 & = & a_0 & \text{หรือ} & P(c) = a_0 + cq_0
\end{array}
$$

หรืออาจเขียนได้เป็น

$$
\begin{array}{cccccccc}
 & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \\
+ & & cq_{n-1} & cq_{n-2} & cq_{n-3} & \cdots & cq_1 & \\
\hline
 & q_{n-1} & q_{n-2} & q_{n-3} & q_{n-4} & \cdots & q_0 & P(c)
\end{array}
$$

เราเรียกการวิธีการเขียนแบบนี้ว่า **การหารสังเคราะห์** (sythetic division) ทำให้ได้ผลหารและเศษเหลือที่เกิดจากการหาร $P(x)$ ด้วย $x - c$

ตัวอย่าง

จงหาผลหารและเศษเหลือที่เกิดจากการหาร $3x^4 - 2x^3 + x^2 + 3x - 5$ ด้วย $x - 2$

วิธีทำ จะได้ว่า $c = 2$ และ $a_4 = q_3 = 3$ ดังนั้น

$$\begin{array}{rrrrrr} & 3 & -2 & 1 & 3 & -5 \\ + & & 2(3) & 2(4) & 2(9) & 2(21) \\ \hline & 3 & 4 & 9 & 21 & 37 \end{array}$$

ดังนั้นผลหารเท่ากับ $3x^3 + 4x^2 + 9x + 21$ และเศษเหลือคือ 37 เขียนขั้นตอนวิธีการหารได้เป็น

$$3x^4 - 2x^3 + x^2 + 3x - 5 = (3x^3 + 4x^2 + 9x + 21)(x - 2) + 37$$

บทนิยาม

ให้ $P(x)$ เป็นพหุนาม ถ้า $P(\alpha) = 0$ จะเรียก α ว่า**ราก (root)** ของพหุนาม $P(x)$ หรือ α เป็น**คำตอบ (solution)** ของสมการ $P(x) = 0$

ข้อสังเกต

โดยบทแทรก 4.15 จะได้ว่า

1. α เป็นรากของก็ต่อเมื่อ $x - \alpha$ เป็นตัวประกอบของ $P(x)$
2. ถ้า $P(x) = Q(x)S(x)$ แล้วรากทุกตัวของ $Q(x)$ และรากทุกตัวของ $S(x)$ เป็นรากของ $P(x)$

ตัวอย่าง

จงหารากของพหุนาม $P(x)$ เมื่อกำหนดให้

1. $P(x) = x + 2$
   วิธีทำ เนื่องจาก $P(-2) = -2 + 2 = 0$ ดังนั้น -2 เป็นรากของ $P(x)$

2. $P(x) = x^2 - 1$
   วิธีทำ เนื่องจาก $P(x) = x^2 - 1 = (x-1)(x+1)$ ดังนั้น $P(1) = 0$ และ $P(-1) = 0$
   จะได้ว่า 1 และ -1 เป็นรากของ $P(x)$

3. $P(x) = x^3 - x^2 - 2x$
   วิธีทำ เนื่องจาก $P(x) = x^3 - x^2 - 2x = x(x^2 - x - 2) = x(x+1)(x-2)$ ดังนั้น $P(0) = 0$,
   $P(-1) = 0$ และ $P(2) = 0$ จะได้ว่า $0, -1$ และ 2 เป็นรากของ $P(x)$

Theorem

ให้ $m, k \in \mathbb{Z}$ *โดยที่* $m \neq 0$ *ซึ่ง* $gcd(m, k) = 1$ *และ*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

เมื่อ $P(x) \in \mathbb{Z}[x]$ *เป็นพหุนามดีกรี* n *โดยที่* $a_0 \neq 0$

$$\text{ถ้า } x - \frac{k}{m} \text{ เป็นตัวประกอบของ } P(x) \text{ แล้ว } m \mid a_n \text{ และ } k \mid a_0$$

บทแทรก

ให้ $P(x) \in \mathbb{Z}[x]$ และ $n \in \mathbb{N}$ โดยที่ $a_0 \neq 0$ ซึ่ง

$$P(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

แล้วรากที่เป็นจำนวนเต็มของ $P(x)$ ต้องเป็นตัวหารของ a_0

ตัวอย่าง

จงหารากที่เป็นจำนวนตรรกยะทั้งหมดที่เป็นไปได้ของพหุนามต่อไปนี้

1. $P(x) = 4x^2 - 1$

   วิธีทำ จะได้ว่า $a_0 = -1$ และ $a_2 = 4$ ดังนั้น $m \mid 4$ คือ $m = \pm 1, \pm 2 \pm 4$ และ $k \mid (-1)$ คือ $k = \pm 1$ ดังนั้น $\frac{k}{m} = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}$

2. $P(x) = 6x^3 + 11x^2 - 4x - 4$

   วิธีทำ จะได้ว่า $a_0 = -4$ และ $a_3 = 6$ ดังนั้น $m \mid 6$ คือ $m = \pm 1, \pm 2, \pm 3, \pm 6$ และ $k \mid (-4)$ คือ $k = \pm 1, \pm 2, \pm 4$ ดังนั้น $\frac{k}{m}$ ทั้งหมดที่เป็นไปได้คือ $\pm 1, \pm 2, \pm 4, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}, \pm\frac{1}{6}$

3. $P(x) = x^3 - 4x^2 + x + 6$

   วิธีทำ จะได้ว่า $a_0 = 6$ แล้ว รากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ 6 คือ $\pm 1, \pm 2, \pm 3, \pm 6$

ตัวอย่าง

จงหาแสดงว่าพหุนาม $P(x) = x^3 + x + 1$ ไม่มีรากเป็นจำนวนเต็ม

วิธีทำ สมมติว่า $\alpha \in \mathbb{Z}$ เป็นรากของ $P(x)$ ดังนั้น $\alpha \mid 1$ นั่นคือ $\alpha = 1$ หรือ -1 แต่

$$P(1) = 1^3 + 1 + 1 = 3 \neq 0$$

$$P(-1) = (-1)^3 + (-1) + 1 = -1 \neq 0$$

เกิดข้อขัดแย้งที่ α เป็นรากของ $P(x)$ ดังนั้น $P(x) = x^3 + x + 1$ ไม่มีรากที่เป็นจำนวนเต็ม

ตัวอย่าง

จงหารากที่เป็นจำนวนเต็มทั้งหมดของ $P(x) = x^3 - 6x^2 + 11x - 6$

วิธีทำ จะได้ว่า $a_0 = -6$ แล้วรากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ -6 คือ $\pm 1, \pm 2, \pm 3, \pm 6$ ตรวจสอบตัวหารที่ได้ดังนี้

$$P(-1) = (-1)^3 - 6(-1)^2 + 11(-1) - 6 = -24$$

$$P(1) = 1^3 - 6(1)^2 + 11(1) - 6 = 0$$

$$P(-2) = (-2)^3 - 6(-2)^2 + 11(-2) - 6 = -60$$

$$P(2) = (2)^3 - 6(2)^2 + 11(2) - 6 = 0$$

$$P(-3) = (-3)^3 - 6(-3)^2 + 11(-3) - 6 = -120$$

$$P(3) = (3)^3 - 6(3)^2 + 11(3) - 6 = 0$$

$$P(-6) = (-6)^3 - 6(-6)^2 + 11(-6) - 6 = -504$$

$$P(-2) = (6)^3 - 6(6)^2 + 11(6) - 6 = 60$$

ดังนั้น $1, 2$ และ 3 เป็นรากของ $P(x)$

จงหารากที่เป็นจำนวนเต็มทั้งหมดของ $P(x) = x^4 + 2x^3 - 13x^2 - 14x + 24$

วิธีทำ จะได้ว่า $a_0 = 24$ แล้วรากที่เป็นจำนวนเต็มที่เป็นไปได้คือตัวหารของ 24 คือ $\pm 1, \pm 2, \pm 3, \pm 6, \pm 8, \pm 12, \pm 24$ เนื่องจาก $P(1) = 1^4 + 2(1)^3 - 13(1)^2 - 14(1) + 24 = 0$ ดังนั้น $x - 1$ เป็นตัวประกอบของ $P(x)$ พิจารณาการหารสังเคราะห์ จะได้ว่า $c = 2$ และ $a_4 = q_3 = 3$ ดังนั้น

	1	2	-13	-14	24
$+$		$1(1)$	$1(3)$	$1(-10)$	$1(-24)$
	1	3	-10	-24	0

ดังนั้นผลหารเท่ากับ $x^3 + 3x^2 - 10x - 24$ เขียนได้เป็น

$$P(x) = (x^3 + 3x^2 - 10x - 24)(x - 1)$$

ให้ $Q(x) = x^3 + 3x^2 - 10x - 24$ หารากของ $Q(x)$ โดยใช้ตัวหารเช่นเดียวกับ $P(x)$ จะได้ว่า $Q(3) = 3^3 + 3(3)^2 - 10(3) - 24 = 0$ ดังนั้น $x - 3$ เป็นตัวประกอบของ $Q(x)$ หารสังเคราะห์ได้ดังนี้

	1	3	-10	-24
$+$		$3(1)$	$3(6)$	$3(8)$
	1	6	8	0

ดังนั้น $Q(x) = (x^2 + 6x + 8)(x - 3)$ จะได้ว่า

$$\begin{aligned} P(x) &= (x^2 + 6x + 8)(x - 3)(x - 1) \\ &= (x + 2)(x + 4)(x - 3)(x - 1) \end{aligned}$$

สรุปได้ว่า $1, 3, -2$ และ -4 เป็นรากของ $P(x)$

เศษส่วนย่อย

พิจารณาเศษส่วนที่ตัวเศษและตัวส่วนเป็นพหุนามซึ่งอยู่ในรูป

$$\frac{P(x)}{Q(x)} \quad \text{เมื่อ } P(x) \text{ เป็นพหุนาม และ } Q(x) \text{ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์}$$

ในแง่ฟังก์ชันจะเรียก $\frac{P(x)}{Q(x)}$ ว่า**ฟังก์ชันตรรกยะ (rational function)** และนิยามการบวกและการคูณฟังก์ชันตรรกยะดังนั้น

$$\frac{P_1(x)}{Q_1(x)} + \frac{P_1(x)}{Q_1(x)} = \frac{P_1(x)Q_2(x) + P_2(x)Q_1(x)}{Q_1(x)Q_2(x)}$$
$$\frac{P_1(x)}{Q_1(x)} \cdot \frac{P_1(x)}{Q_1(x)} = \frac{P_1(x)P_2(x)}{Q_1(x)Q_2(x)}$$

ในหัวข้อนี้จะพิจารณาว่าสำหรับแต่ละฟังก์ชันตรรกยะ $\frac{P(x)}{Q(x)}$ จะสามารถเขียนในรูป

$$\frac{P(x)}{Q(x)} = \frac{P_1(x)}{Q_1(x)} + \frac{P_2(x)}{Q_2(x)} + \cdots + \frac{P_n(x)}{Q_n(x)}$$

ได้หรือไม่ โดยแต่ละ $P_i(x)$ และ $Q_i(x)$ มีดีกรีน้อยกว่า $P(x)$ และ $Q(x)$ ตามลำดับ โดยเรียกแต่ละ $\frac{P_i(x)}{Q_i(x)}$ ว่า**เศษส่วนย่อย (partial fraction)** ของ $\frac{P(x)}{Q(x)}$ สำหรับ $i = 1, 2, \ldots, n$

Theorem

ให้ $P(x)$ เป็นพหุนาม และ $Q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์
จะได้ว่ามีพหุนาม $S(x)$ และ $R(x)$ โดยที่ $R(x) = 0$ หรือ $\deg R(x) < \deg Q(x)$ ซึ่งสอดคล้อง

$$\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$$

บทพิสูจน์.

ให้ $P(x)$ เป็นพหุนาม และ $Q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์
โดยขั้นตอนวิธีการหารจะได้ว่ามีพหุนาม $S(x)$ และ $R(x)$ เพียงคู่เดียวที่สอดคล้องกับ

$$P(x) = Q(x)S(x) + R(x) \qquad \text{เมื่อ } R(x) = 0 \text{ หรือ } \deg R(x) < \deg S(x)$$

ดังนั้น

$$\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปแบบตามทฤษฎีบท

1. $\dfrac{x^2-1}{x+3}$

วิธีทำ พิจารณาการสังเคราะห์

$$\begin{array}{rrr} & 1 & 0 & -1 \\ + & & -3(1) & -3(-3) \\ \hline & 1 & -3 & 8 \\ \hline\hline \end{array}$$

ดังนั้น $x-3$ และ 8 เป็นผลหารและเศษเหลือที่เกิดจากการหาร x^2-1 ด้วย $x+3$ ทำให้ได้ว่า

$$\frac{x^2-1}{x+3} = x-3+\frac{8}{x+3}$$

2. $\dfrac{x^2+x+5}{x^2+1}$

วิธีทำ จะได้ว่า

$$\frac{x^2+x+5}{x^2+1} = \frac{(x^2+1)+x+4}{x^2+1} = 1+\frac{x+4}{x^2+1}$$

Theorem

ให้ $Q(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$ *เป็นพหุนามดีกรี* $n \in \mathbb{N}$ *เมื่อ* $a_1, a_2, ..., a_n$ *เป็นจำนวนจริงที่แตกต่างกัน และ* $P(x)$ *เป็นพหุนามที่* $\deg P(x) < n$ *จะได้ว่า* $\dfrac{P(x)}{Q(x)}$ *สามารถเขียนเป็นผลบวกของเศษส่วนย่อยในรูปแบบ*

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a_1} + \frac{c_2}{x-a_2} + \cdots + \frac{c_n}{x-a_n}$$

เมื่อ $c_i = \dfrac{P(a_i)}{Q_i(a_i)}$ *โดยที่* $Q_i(x) = (x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$ *สำหรับ* $i = 1, 2, ..., n$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^2+4x+1}{x^3-x}$ ในรูปผลบวกของเศษส่วนย่อย

วิธีทำ ให้ $P(x)=x^2+4x+1$ และ $Q(x)=x^3-x=x(x-1)(x+1)$ ดังนั้น

$$\frac{P(x)}{Q(x)}=\frac{x^2+4x+1}{x^3-x}=\frac{c_1}{x}+\frac{c_2}{x-1}+\frac{c_3}{x+1}$$

ให้ $Q_1=(x-1)(x+1)$, $Q_2=x(x+1)$ และ $Q_3=x(x-1)$ จะได้ว่า

$$c_1=\frac{P(0)}{Q_1(0)}=\frac{0^2+4(0)+1}{(0-1)(0+1)}=-1$$
$$c_2=\frac{P(1)}{Q_2(1)}=\frac{1^2+4(1)+1}{1(1+1)}=3$$
$$c_3=\frac{P(-1)}{Q_3(-1)}=\frac{(-1)^2+4(-1)+1}{(-1)(-1-1)}=-1$$

ดังนั้น

$$\frac{x^2+4x+1}{x^3-x}=-\frac{1}{x}+\frac{3}{x-1}-\frac{1}{x+1}$$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^2-6x+4}{x^3-4x}$ ในรูปผลบวกของเศษส่วนย่อย

วิธีทำ ให้ c_1, c_2, c_3 เป็นจำนวนจริงซึ่ง

$$\begin{aligned}\frac{x^2-6x+4}{x^3-4x} &= \frac{x^2-6x+2}{x(x-2)(x+2)} = \frac{c_1}{x}+\frac{c_2}{x-2}+\frac{c_3}{x+2}\\ &= \frac{c_1(x-2)(x+2)+c_2x(x+2)+c_3x(x-2)}{x(x-2)(x+2)}\end{aligned}$$

ดังนั้น $x^2-6x+4 = c_1(x-2)(x+2)+c_2x(x+2)+c_3x(x-2)$

เมื่อ $x=0$ จะได้ว่า $c_1(-2)(2)+0+0=4$ นั่นคือ $-4c_1=4$ ดังนั้น $c_1=-1$

เมื่อ $x=2$ จะได้ว่า $0+c_2(2)(4)+0=-4$ นั่นคือ $8c_2=-4$ ดังนั้น $c_2=-\dfrac{1}{2}$

เมื่อ $x=-2$ จะได้ว่า $0+0+c_3(-2)(-4)=14$ นั่นคือ $-8c_3=14$ ดังนั้น $c_3=-\dfrac{7}{4}$

ดังนั้น

$$\frac{x^2-6x+4}{x^3-4x} = -\frac{1}{x}-\frac{1}{2(x-2)}-\frac{7}{4(x+2)}$$

ตัวอย่าง

จงหาผลบวกของอนุกรม $\sum_{k=2}^{n} \frac{1}{n^2-1}$ เมื่อ n เป็นจำนวนบวกคี่

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{1}{n^2-1} = \frac{1}{(n-1)(n+1)} = \frac{c_1}{n-1} + \frac{c_2}{n+1}$$

จะได้ว่า $1 = c_1(n+1) + c_2(n+1)$ แล้ว $c_1 = \frac{1}{2}$ และ $c_2 = -\frac{1}{2}$ ดังนั้น

$$\begin{aligned}
\frac{1}{n^2-1} &= \frac{1}{2}\left(\frac{1}{n-1} - \frac{1}{n+1}\right) \\
\sum_{k=2}^{n} \frac{1}{n^2-1} &= \frac{1}{2}\sum_{k=2}^{n}\left(\frac{1}{n-1} - \frac{1}{n+1}\right) \\
&= \frac{1}{2}\left[\left(\frac{1}{1} - \frac{1}{3}\right) + \left(\frac{1}{2} - \frac{1}{4}\right) + \left(\frac{1}{3} - \frac{1}{5}\right) + \left(\frac{1}{4} - \frac{1}{6}\right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n+1}\right)\right]
\end{aligned}$$

เนื่องจาก n เป็นจำนวนคี่ จะได้ว่า $n+1$ เป็นจำนวนคู่ ดังนั้น

$$\begin{aligned}
\sum_{k=2}^{n} \frac{1}{n^2-1} &= \frac{1}{2}\left[\left(1 - \frac{1}{n-2}\right) + \left(\frac{1}{2} - \frac{1}{n+1}\right)\right] \\
&= \frac{1}{2}\left[\frac{3}{2} - \frac{1}{n-2} - \frac{1}{n+1}\right]
\end{aligned}$$

ตัวอย่าง

จงหา $\int \frac{1}{x^3 - x}\, dx$

วิธีทำ พิจารณาฟังก์ชันตรรกยะ

$$\frac{1}{x^3 - x} = \frac{1}{x(x-1)(x+1)} = \frac{c_1}{x} + \frac{c_2}{x-1} + \frac{c_3}{x+1}$$

จะได้ว่า $1 = c_1(x-1)(x+1) + c_2 x(x+1) + c_3 x(x-1)$
แล้ว $c_1 = -1$, $c_2 = \frac{1}{2}$ และ $c_3 = -\frac{1}{2}$ ดังนั้น

$$\frac{1}{x^3 - x} = -\frac{1}{x} + \frac{1}{2(x-1)} - \frac{1}{2(x+1)}$$

$$\begin{aligned}\int \frac{1}{x^3 - x}\, dx &= -\int \frac{1}{x}\, dx + \frac{1}{2}\int \frac{1}{x-1}\, dx - \frac{1}{2}\int \frac{1}{x+1}\, dx \\ &= -\ell n|x| + \frac{1}{2}\ell n|x-1| - \frac{1}{2}\ell n|x+1| + C\end{aligned}$$

Theorem

ให้ $Q(x) = (x-a)^n$ *เมื่อ* $a \in \mathbb{R}$ *และ* $P(x)$ *เป็นพหุนามที่* $\deg P(x) < n$ *จะได้ว่ามีจำนวนจริง* $c_1, c_2, ..., c_n$ *ที่ทำให้*

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a} + \frac{c_2}{(x-a)^2} + \cdots + \frac{c_n}{(x-a)^n}$$

บทแทรก

ให้ $Q(x) = (x-a)^n R(x)$ เป็นพหุนาม เมื่อ $a \in \mathbb{R}$ และ $R(x)$ เป็นพหุนาม และ $P(x)$ เป็นพหุนามที่ $\deg P(x) < \deg Q(x)$ จะได้ว่ามีจำนวนจริง $c_1, c_2, ..., c_n$ และพหุนาม $S(x)$ ซึ่งดีกรีน้อยกว่า $R(x)$ ที่ทำให้

$$\frac{P(x)}{Q(x)} = \frac{c_1}{x-a} + \frac{c_2}{(x-a)^2} + \cdots + \frac{c_n}{(x-a)^n} + \frac{S(x)}{R(x)}$$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปผลบวกเศษส่วนย่อย โดยไม่ต้องคำนวนค่าคงตัว

1. $\dfrac{1}{(x-1)^3}$

   วิธีทำ มีจำนวนจริง c_1, c_2, c_3 ที่ทำให้

   $$\frac{1}{(x-1)^3} = \frac{c_1}{x-1} + \frac{c_2}{(x-1)^2} + \frac{c_3}{(x-1)^3}$$

2. $\dfrac{x^2+1}{(x-2)^2(x^2-x-2)}$

   วิธีทำ เนื่องจาก $(x-2)^2(x^2-x-2) = (x-2)^2(x-2)(x+1) = (x-2)^3(x+1)$
   ดังนั้นมีจำนวนจริง c_1, c_2, c_3, c_4 ที่ทำให้

   $$\frac{x^2+1}{(x-2)^3(x+1)} = \frac{c_1}{x-2} + \frac{c_2}{(x-2)^2} + \frac{c_3}{(x-2)^3} + \frac{c_4}{x+1}$$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะ $\dfrac{x^2+x+6}{(x+1)^2(x-1)}$ ในรูปผลบวกเศษส่วนย่อย

วิธีทำ มีจำนวนจริง c_1, c_2, c_3 ที่ทำให้

$$\begin{aligned}\frac{x^2+x+6}{(x+1)^2(x-1)} &= \frac{c_1}{x+1}+\frac{c_2}{(x+1)^2}+\frac{c_3}{x-1}\\ &= \frac{c_1(x+1)(x-1)+c_2(x-1)+c_3(x+1)^2}{(x-1)^2(x+1)}\end{aligned}$$

ดังนั้น $x^2+x+6 = c_1(x+1)(x-1)+c_2(x-1)+c_3(x+1)^2$

เมื่อ $x=1$ จะได้ว่า $c_1(2)(0)+c_2(0)+c_3(8)=8$ นั่นคือ $8c_3=8$ ดังนั้น $c_3=1$

เมื่อ $x=-1$ จะได้ว่า $c_1(0)(-2)+c_2(-2)+c_3(0)=6$ นั่นคือ $-2c_2=6$ ดังนั้น $c_2=-3$

เมื่อ $x=0$ จะได้ว่า $c_1(1)(-1)+c_2(-1)+c_3(1)=6$ นั่นคือ $-c_1+3+1=6$ ดังนั้น $c_1=-2$

สรุปได้ว่า

$$\frac{x^2+x+6}{(x+1)^2(x-1)} = -\frac{2}{x+1}-\frac{3}{(x+1)^2}+\frac{1}{x-1}$$

ต่อไปนี้จะเป็นผลบวกเศษส่วนย่อยในรูปแบบโดยทั่วไปซึ่งเป็นผลจาก ทฤษฎีบทต่างๆก่อนหน้านี้ กล่าวคือถ้า $Q(x) = [q_1(x)]^{n_1}[q_2(x)]^{n_2}\cdots[q_k(x)]^{n_k}$ โดยที่แต่ละ $q_i(x)$ เป็นพหุนามโมนิก ซึ่ง $\deg q_i(x) \geq 1$ และไม่ซ้ากัน มีสมบัติว่าทุก ๆ พหุนาม $q(x)$ ซึ่ง $q(x) \mid q_i(x)$ แล้ว $q(x) = \pm 1$ หรือ $q(x) = \pm q_i(x)$ ให้ $P(x)$ เป็นพุนามที่มีดีกรีน้อยกว่าดีกรีของ $Q(x)$ จะได้ว่า

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n_1} \frac{c_{1i}(x)}{[q_1(x)]^i} + \sum_{i=1}^{n_2} \frac{c_{2i}(x)}{[q_2(x)]^i} + \cdots + \sum_{i=1}^{n_k} \frac{c_{ki}(x)}{[q_k(x)]^i}$$

เมื่อ $c_{ij}(x)$ เป็นพหุนาม โดยที่ $c_{ij}(x) = 0$ หรือ $\deg c_{ij(x)} < \deg q_i(x)$ ทุก ๆ i, j

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะต่อไปนี้ในรูปผลบวกเศษส่วนย่อย โดยไม่ต้องคำนวนค่าคงตัว

1. $\dfrac{1}{(x^2+1)(x+1)}$

   วิธีทำ มีจำนวนจริง A, B, C ที่ทำให้

   $$\frac{1}{(x^2+1)(x+1)} = \frac{Ax+B}{x^2+1} + \frac{C}{x+1}$$

2. $\dfrac{x^2+3}{(x^2+1)^2(x+1)^2(x-1)}$

   วิธีทำ ดังนั้นมีจำนวนจริง $c_1, c_2, c_3, c_4, c_5, c_6$ ที่ทำให้

   $$\frac{x^2+3}{(x^2+1)^2(x+1)^2(x-1)} = \frac{c_1+c_2x}{x^2+1} + \frac{c_3+c_4x}{(x^2+1)^2} + \frac{c_4}{x+1} + \frac{c_5}{(x+1)^2} + \frac{c_6}{x-1}$$

ตัวอย่าง

จงเขียนฟังก์ชันตรรกยะ $\dfrac{2x^4+3x^2-x}{(x^2+1)^2(x-1)}$ ในรูปผลบวกเศษส่วนย่อย

วิธีทำ มีจำนวนจริง c_1, c_2, c_3, c_4, c_5 ที่ทำให้

$$\frac{2x^4+3x^2-x}{(x^2+1)^2(x-1)} = \frac{c_1+c_2x}{x^2+1} + \frac{c_3+c_4x}{(x^2+1)^2} + \frac{c_5}{x-1}$$

ดังนั้น $2x^4+3x^2-x = (c_1+c_2x)(x^2+1)(x-1) + (c_3+c_4x)(x-1) + c_5(x^2+1)^2$
เมื่อ $x=1$ จะได้ว่า $4c_5 = 4$ นั่นคือ $c_5 = 1$ พิจารณาการแทนค่า $x = 0, -1, 2, -2$ จะได้ว่า

$$\begin{aligned}
-c_1 &- c_3 &&= -1\\
-4c_1 + 4c_2 &- 2c_3 + 2c_4 &&= 2\\
5c_1 + 10c_2 &+ c_3 + 2c_4 &&= 17\\
-15c_1 + 30c_2 &- 3c_3 + 6c_4 &&= 21
\end{aligned}$$

จากการแก้ระบบสมการดังกล่าวจะได้ว่า $c_1 = 1, c_2 = 1, c_3 = 0, c_4 = 1$ ดังนั้น

$$\frac{2x^4+3x^2-x}{(x^2+1)^2(x-1)} = \frac{1+x}{x^2+1} + \frac{x}{(x^2+1)^2} + \frac{1}{x-1}$$