ทฤษฎีจำนวน (Number Theory)

การหารลงตัว • จำนวนเฉพาะ • ห.ร.ม./ค.ร.น. • สมภาค (Modular Arithmetic)

None W. (Yuan)

สารบัญ (Outline)

1. การหารลงตัว (Divisibility)
2. จำนวนเฉพาะและจำนวนประกอบ
3. ห.ร.ม. และ ค.ร.น. (GCD & LCM)
4. สมภาค (Modular Arithmetic)
5. เลขฐาน (Number Bases)
6. สรุป

ก่อนเรียน (Prerequisites)

สิ่งที่ควรรู้ก่อนเรียน

- **จำนวนเต็ม** — การบวก ลบ คูณ หาร, การหารเอาเศษ
- **เลขยกกำลัง** — a^n, การคูณเลขยกกำลัง
- **จำนวนจริง** — ความรู้พื้นฐานเกี่ยวกับจำนวน

ทฤษฎีจำนวนคืออะไร?

การศึกษาเกี่ยวกับ **จำนวนเต็ม** และสมบัติของมัน — โดยเฉพาะการหารลงตัว จำนวนเฉพาะ และการหาเศษจากการหาร

การหารลงตัว

Divisibility

การหารลงตัว

นิยาม

a **หาร** b **ลงตัว** เขียนแทนด้วย $a \mid b$ ก็ต่อเมื่อ มีจำนวนเต็ม k ที่ทำให้ $b = ak$

อ่านว่า: "a divides b" หรือ "a เป็นตัวหารของ b"

ตัวอย่าง

$3 \mid 12$ เพราะ $12 = 3 \times 4$ $\quad 7 \mid 0$ เพราะ $0 = 7 \times 0$ $\quad 5 \nmid 13$

ขั้นตอนการหาร (Division Algorithm)

สำหรับ $a \in \mathbb{Z}$, $b > 0$: มี q, r เพียงคู่เดียวที่ $a = bq + r$, $0 \leq r < b$

q = ผลหาร, r = เศษ

ตัวอย่าง: $17 = 5 \times 3 + 2$ $\quad -13 = 5 \times (-3) + 2$ (เศษ ≥ 0 เสมอ!)

กฎการหารลงตัว (Divisibility Rules)

หลักหน่วย/หลักสุดท้าย

2: หลักหน่วย $0, 2, 4, 6, 8$

5: หลักหน่วย 0 หรือ 5

10: หลักหน่วย 0

4: 2 หลักสุดท้าย $\div 4$ ลงตัว

8: 3 หลักสุดท้าย $\div 8$ ลงตัว

ผลรวมเลขโดด

3: ผลรวมเลขโดด $\div 3$ ลงตัว

9: ผลรวมเลขโดด $\div 9$ ลงตัว

ตัวอย่าง

12345: หารด้วย 5 ลงตัว (หลักหน่วย 5), หารด้วย 3 ลงตัว $(1 + 2 + 3 + 4 + 5 = 15)$

2024: หารด้วย 4 ลงตัว $(04 \div 4 = 1)$

จำนวนเฉพาะและจำนวนประกอบ

จำนวนเฉพาะ (Prime Numbers)

นิยาม

จำนวนเฉพาะ คือจำนวนเต็มบวกที่มากกว่า 1 และมีตัวหารบวกเพียงสองตัวคือ 1 และตัวมันเอง

จำนวนประกอบ (Composite) คือจำนวนเต็มบวกที่มากกว่า 1 และไม่ใช่จำนวนเฉพาะ

จำนวนเฉพาะ < 50

$2, 3, 5, 7, 11, 13,$
$17, 19, 23, 29,$
$31, 37, 41, 43, 47$

2 เป็นจำนวนเฉพาะคู่เพียงตัวเดียว!

หมายเหตุ

- 1 **ไม่ใช่** จำนวนเฉพาะ และ **ไม่ใช่** จำนวนประกอบ
- จำนวนเฉพาะมี **ไม่จำกัด**

ตัวอย่าง: จำนวนประกอบ

$4 = 2 \times 2 \qquad 30 = 2 \times 3 \times 5$

$91 = 7 \times 13$ (91 ไม่ใช่จำนวนเฉพาะ!)

การแยกตัวประกอบเฉพาะ (Prime Factorization)

ทฤษฎีบทหลักมูลของเลขคณิต

จำนวนเต็มบวกทุกตัวที่มากกว่า 1 สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ **เพียงแบบเดียว** (ไม่นับลำดับ)

ตัวอย่าง

$60 = 2^2 \times 3 \times 5 \qquad 84 = 2^2 \times 3 \times 7$

$126 = 2 \times 3^2 \times 7 \qquad 1000 = 2^3 \times 5^3$

การตรวจสอบว่าเป็นจำนวนเฉพาะ

ในการตรวจสอบว่า n เป็นจำนวนเฉพาะหรือไม่ ทดลองหารด้วยจำนวนเฉพาะทุกตัวที่ $\leq \sqrt{n}$ ก็พอ

ตัวอย่าง: 101 — ทดลอง $2, 3, 5, 7$ ($\sqrt{101} \approx 10$)

ไม่มีตัวใดหารลงตัว $\rightarrow$ 101 เป็นจำนวนเฉพาะ ✓

ห.ร.ม. และ ค.ร.น.

GCD & LCM

ห.ร.ม. (GCD) และ ค.ร.น. (LCM)

นิยาม

ห.ร.ม. ของ a, b คือจำนวนเต็มบวกที่มากที่สุดที่หารทั้ง a และ b ลงตัว

ค.ร.น. ของ a, b คือจำนวนเต็มบวกที่น้อยที่สุดที่ a และ b หารลงตัว

วิธีแยกตัวประกอบ

$12 = 2^2 \times 3 \quad 18 = 2 \times 3^2$

$\text{GCD} = 2^{\min(2,1)} \times 3^{\min(1,2)} = 2 \times 3 = 6$

$\text{LCM} = 2^{\max(2,1)} \times 3^{\max(1,2)} = 2^2 \times 3^2 = 36$

สูตรสำคัญ

$\text{ab} = \textbf{GCD}(\text{a}, \text{b}) \times \textbf{LCM}(\text{a}, \text{b})$

$12 \times 18 = 6 \times 36 = 216 \quad \checkmark$

ขั้นตอนวิธีของยุคลิด (Euclidean Algorithm)

วิธีหา GCD โดยไม่ต้องแยกตัวประกอบ

หลักการ: $\text{GCD}(a, b) = \text{GCD}(b, a \bmod b)$ (ทำซ้ำจนเหลือ 0)

ตัวอย่าง: Euclidean Algorithm (252 กับ 105)

$252 = 2 \times 105 + 42 \quad \rightarrow \quad$ GCD(105, 42)

$105 = 2 \times 42 + 21 \quad \rightarrow \quad$ GCD(42, 21)

$42 = 2 \times 21 + 0 \quad \rightarrow \quad$ **GCD = 21**

ตัวอย่าง: Euclidean Algorithm (126 กับ 35)

$126 = 3 \times 35 + 21 \quad \rightarrow \quad$ GCD(35, 21)

$35 = 1 \times 21 + 14 \quad \rightarrow \quad$ GCD(21, 14)

$21 = 1 \times 14 + 7 \quad \rightarrow \quad$ GCD(14, 7) $\qquad 14 = 2 \times 7 + 0 \quad \rightarrow \quad$ **GCD = 7**

สมภาค

Modular Arithmetic

สมภาคคืออะไร?

นิยาม

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

อ่านว่า: "a สมภาคกับ b มอดุโล m" (หรือ "a congruent to b modulo m")

ความหมาย: a และ b **เหลือเศษเท่ากัน** เมื่อหารด้วย m

ตัวอย่าง

$17 \equiv 5 \pmod{12}$ เพราะ $17 - 5 = 12$ หารด้วย 12 ลงตัว

$23 \equiv 3 \pmod{5}$ เพราะ $23 = 4 \times 5 + 3$ และ 3 หารด้วย 5 เหลือเศษ 3

$-7 \equiv 3 \pmod{5}$ เพราะ $-7 - 3 = -10$ หารด้วย 5 ลงตัว

คิดง่าย ๆ

"mod m" คือการวนรอบแบบนาฬิกา: นาฬิกามี 12 ชั่วโมง — 14 นาฬิกา $\equiv 2$ นาฬิกา (mod 12)

สมบัติของสมภาค

สมบัติพื้นฐาน

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

1. $a + c \equiv b + d \pmod{m}$ (บวกกันได้)
2. $a - c \equiv b - d \pmod{m}$ (ลบกันได้)
3. $ac \equiv bd \pmod{m}$ (คูณกันได้)
4. $a^n \equiv b^n \pmod{m}$ (ยกกำลังได้)

ตัวอย่าง: ลดทอนก่อนคำนวณ

จงหา $23 \times 18 \pmod{5}$

วิธีตรง: $23 \times 18 = 414$, $414 \div 5 = 82$ เศษ 4

วิธีสมภาค: $23 \equiv 3 \pmod{5}$, $18 \equiv 3 \pmod{5}$ $\quad 3 \times 3 = 9 \equiv 4 \pmod{5}$ เท่ากัน!

การหาเศษจากเลขยกกำลัง: ดูแพทเทิร์น

แนวคิด

หา **วัฏจักร (cycle)** ของเศษจากการยกกำลัง: คำนวณ $a^1, a^2, a^3, \ldots \pmod{m}$ จนกว่าเศษจะซ้ำ

ตัวอย่าง: เศษของ 7^{2025} หารด้วย 10

หลักหน่วยของ $7^n \pmod{10}$:

$7^1 = 7 \equiv 7 \quad 7^2 = 49 \equiv 9 \quad 7^3 = 343 \equiv 3 \quad 7^4 = 2401 \equiv 1$

$7^5 \equiv 7 \quad \rightarrow$ **วัฏจักรยาว 4:** $\{7, 9, 3, 1\}$

$2025 \div 4 = 506$ เศษ $1 \quad \rightarrow \quad 7^{2025} \equiv 7^1 \equiv 7 \pmod{10}$

เศษ $= 7$ (หลักหน่วยของ 7^{2025} คือ 7)

ตัวอย่าง: เศษของเลขยกกำลังขนาดใหญ่ (ต่อ)

โจทย์ 1: $3^{100} \pmod 7$

$3^1 \equiv 3,\ 3^2 \equiv 9 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 18 \equiv 4,\ 3^5 \equiv 12 \equiv 5,\ 3^6 \equiv 15 \equiv 1$

วัฏจักรยาว 6: $\{3, 2, 6, 4, 5, 1\}$ $\quad 100 \div 6 = 16$ เศษ 4

$3^{100} \equiv 3^4 \equiv 4 \pmod 7$

โจทย์ 2: $2^{50} \pmod{13}$

$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 16 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12 \equiv -1$

$2^{12} \equiv (-1)^2 \equiv 1$ (วัฏจักรยาว 12)

$50 \div 12 = 4$ เศษ 2 $\quad \rightarrow \quad 2^{50} \equiv 2^2 \equiv 4 \pmod{13}$

ตัวอย่าง: ผลรวมเลขยกกำลังขนาดใหญ่

โจทย์: เศษของ $2018^{2019} + 2019^{2020} + 2020^{2021}$ หารด้วย 13

ลดทอนฐานก่อน:

$2018 \div 13 = 155$ เศษ $3 \quad \rightarrow \quad 2018 \equiv 3 \pmod{13}$

$2019 \equiv 4 \pmod{13} \quad 2020 \equiv 5 \pmod{13}$

หาเศษทีละพจน์: ใช้ Fermat: $a^{12} \equiv 1 \pmod{13}$ ถ้า $13 \nmid a$

$3^{2019} = 3^{12\times168+3} \equiv 3^3 \equiv 27 \equiv 1 \pmod{13}$

$4^{2020} = 4^{12\times168+4} \equiv 4^4 = 256 \equiv 9 \pmod{13}$

$5^{2021} = 5^{12\times168+5} \equiv 5^5 = 3125 \equiv 5 \pmod{13}$

เศษรวม $= 1 + 9 + 5 = 15 \equiv 2 \pmod{13}$

ทฤษฎีบทของแฟร์มาต์ (Fermat's Little Theorem)

Fermat's Little Theorem

ถ้า p เป็นจำนวนเฉพาะ และ $p \nmid a$ แล้ว:

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

หรือรูปทั่วไป: $a^p \equiv a \pmod{p}$

ตัวอย่าง

1. $2^{10} \equiv 1 \pmod{11}$ (ตรวจสอบ: $1024 \div 11 = 93$ เศษ 1)
2. $5^6 \equiv 1 \pmod{7}$ (ตรวจสอบ: $15625 \div 7 = 2232$ เศษ 1)
3. หา $7^{100} \pmod{5}$:

$7^4 \equiv 1 \pmod{5}$ (Fermat: $p = 5$)

$100 = 4 \times 25 \quad \rightarrow \quad 7^{100} = (7^4)^{25} \equiv 1^{25} \equiv 1 \pmod{5}$

ตัวอย่าง: โจทย์วันในสัปดาห์

โจทย์

วันนี้เป็นวันเสาร์ที่ 19 กรกฎาคม 2025 อยากทราบว่าอีก 1000 วันข้างหน้าจะเป็นวันอะไร?

วิธีทำ

วันในสัปดาห์มี 7 วัน — ใช้ mod 7

กำหนด: เสาร์ $= 0$, อาทิตย์ $= 1$, จันทร์ $= 2$, อังคาร $= 3$, พุธ $= 4$, พฤหัส $= 5$, ศุกร์ $= 6$

$1000 \div 7 = 142$ เศษ 6

6 วันหลังจากวันเสาร์: เสาร์ $(0) \to$ อาทิตย์ $(1) \to$ จันทร์ $(2) \to$ อังคาร $(3) \to$ พุธ $(4) \to$ พฤหัส $(5) \to$ **ศุกร์** (6)

ตอบ: วันศุกร์

ตัวอย่างเพิ่มเติม: สมภาค

โจทย์ 1: จำนวนที่หารด้วย 5 เหลือเศษ 3 และหารด้วย 7 เหลือเศษ 2

$x \equiv 3 \pmod 5$ และ $x \equiv 2 \pmod 7$

จาก $x \equiv 3 \pmod 5$: $x = 5k + 3$

แทนในสมการที่สอง: $5k + 3 \equiv 2 \pmod 7$

$5k \equiv -1 \equiv 6 \pmod 7$

คูณด้วยผกผันของ 5 mod 7: $5 \times 3 = 15 \equiv 1 \pmod 7 \quad \rightarrow \quad k \equiv 6 \times 3 \equiv 18 \equiv 4 \pmod 7$

$k = 7t + 4 \quad \rightarrow \quad x = 5(7t + 4) + 3 = 35t + 23$

$x \equiv 23 \pmod{35}$ **(คำตอบทั่วไป)**

ตัวอย่าง: หลักหน่วยของเลขยกกำลังซ้อน

โจทย์: จงหาหลักหน่วยของ 7^{7^7}

หลักหน่วยของ 7^n มีวัฏจักร $\{7, 9, 3, 1\}$ ขึ้นกับ n mod 4

หา 7^7 mod 4: $7 \equiv 3 \pmod 4$, $3^2 = 9 \equiv 1 \pmod 4$

$7^7 \equiv 3^7 = 3^{2\times 3+1} \equiv 1^3 \times 3 \equiv 3 \pmod 4$

ดังนั้น $7^{7^7} \equiv 7^3 \equiv 343 \equiv 3 \pmod{10}$

หลักหน่วยคือ 3

โจทย์ 2: จงหาหลักหน่วยของ $2^{2024} + 3^{2024}$

2^n mod 10: วัฏจักร $\{2, 4, 8, 6\}$ $\quad 2024 \div 4$ เศษ $0 \to 2^{2024} \equiv 6$

3^n mod 10: วัฏจักร $\{3, 9, 7, 1\}$ $\quad 2024 \div 4$ เศษ $0 \to 3^{2024} \equiv 1$

$6 + 1 = 7$ **หลักหน่วยคือ 7**

เลขฐาน

Number Bases

เลขฐาน

แนวคิด

ตัวเลขที่เราใช้ในชีวิตประจำวันเป็น **เลขฐานสิบ** (decimal) แต่เราสามารถเขียนจำนวนในฐานอื่น ๆ ได้

การเปลี่ยนฐาน n เป็นฐานสิบ

$(a_k a_{k-1} \ldots a_1 a_0)_n$

$= a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$

ตัวอย่าง:

$(1011)_2 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 = 11$

$(2A)_{16} = 2 \times 16 + 10 = 42$

การเปลี่ยนฐานสิบเป็นฐาน n

หารด้วย n ซ้ำ ๆ เอาเศษมาเรียงจากล่างขึ้นบน

ตัวอย่าง: 12 เป็นฐาน 2

$12 \div 2 = 6$ เศษ 0

$6 \div 2 = 3$ เศษ 0

$3 \div 2 = 1$ เศษ 1

$1 \div 2 = 0$ เศษ 1

$(12)_{10} = (1100)_2$

สรุป

สรุปเนื้อหา

สิ่งที่ได้เรียนรู้

- **การหารลงตัว**: $a \mid b$, กฎการหาร
- **จำนวนเฉพาะ**: มีแค่ 1 กับตัวมันเองที่หารลงตัว
- **จำนวนประกอบ**: เขียนเป็นผลคูณของจำนวนเฉพาะได้
- **GCD/LCM**: แยกตัวประกอบ, Euclidean algorithm
- **GCD $\times$ LCM =** ab
- **สมภาค**: $a \equiv b \pmod{m} \iff m \mid (a - b)$
- **สมบัติ**: บวก ลบ คูณ ยกกำลัง ใน mod ได้
- **Fermat**: $a^{p-1} \equiv 1 \pmod{p}$ (p เฉพาะ)
- **เลขยกกำลัง**: หาวัฏจักรของเศษ
- **เลขฐาน**: เปลี่ยนไป-กลับระหว่างฐานต่าง ๆ

เอกสารนี้เป็นส่วนหนึ่งของเนื้อหาเตรียมสอบ **สอวน. คอมพิวเตอร์**

Special thanks to **Pana W.** for the original English-version slide.