ทฤษฎีจำนวน NUMBER THEORY

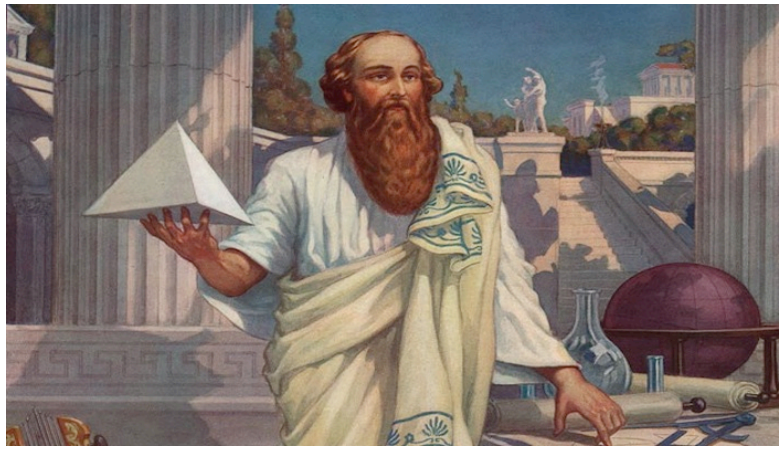
อาจารย์ ดร.ธนัชยศ จำปาหวาย

สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

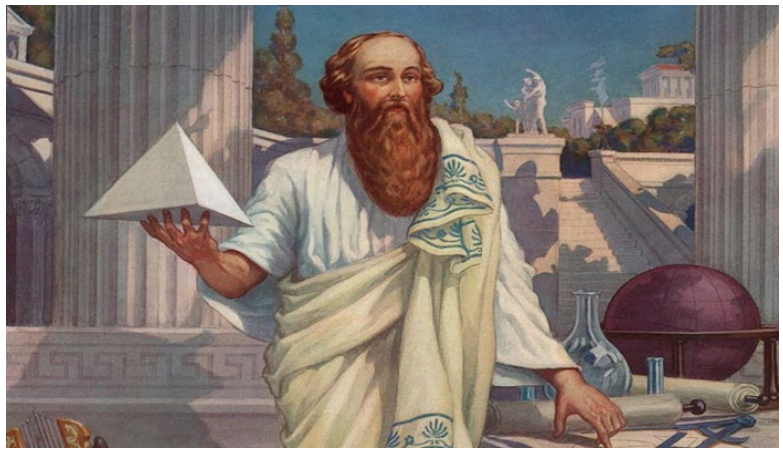
ทฤษฎีจำนวน Number Theory (กลางภาค)

- บทที่ 1 ความรู้พื้นฐาน
- บทที่ 2 การหารลงตัว
- บทที่ 3 ตัวหารร่วมมาก
- บทที่ 4 จำนวนเฉพาะ

บทที่ 1 ความรู้พื้นฐาน



วิวัฒนาการของวิชาทฤษฎีจำนวน



พีทาโกรัส (Pythagoras 569–500 ปีก่อนคริสต์ศักราช)

จำนวนมิตรภาพ (amicable numbers) คู่แรกคือ 284 และ 220

ตัวหารแท้ของ 284 คือ 1, 2, 4, 71 และ 142 แล้วผลบวกคือ

$$1 + 2 + 4 + 71 + 142 = 220$$

ตัวหารแท้ของ 220 คือ 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 และ 110 แล้วผลบวกคือ

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

ปีที่ค้นพบ	ผู้คนพบ	จำนวนมิตรภาพ
ค.ศ. 1636	Pierre De Fermat (1601–1665)	17,296 และ 18,416
ค.ศ. 1686	Rene Descartes (1596–1650)	9,363,584 และ 9,437,056
ค.ศ. 1830	Adrien Marie Legendre (1752–1833)	2,172,649,216 และ 8,520,191
ค.ศ. 1866	Nicolo Painini ชาวอิตาลีอายุ 16 ปี	1,184 และ 1,210

จำนวนสมบูรณ์ (perfect number) คือจำนวนที่เท่ากับผลบวกของตัวหารแท้ของจำนวนนั้น 6 มีตัวหารแท้ คือ 1 2 และ 3 และ

$$1 + 2 + 3 = 6$$

จำนวนสมบูรณ์อีกสองจำนวนต่อมา คือ 28 และ 496 กระทั่งในปี ค.ศ. 2016 ได้พบทั้งหมด 49 จำนวน

ยุคลิดแห่งอเล็กซานเดรีย (Euclic of Alexandria 450–380 ปีก่อนคริสต์ศักราช)

ดีโอฟานโตสแห่งอะเล็กซานเดรีย (Diophantos of Alexandria 300– 250 ปีก่อนคริสตกาล)

ปิแยร์ เดอ แฟร์มาต์ (Pierre de Fermat 1601–1665)

คาร์ล ฟรีดริช เกาส์ (Carl Fridrich Gauss 1777–1855)

เซตเบื้องต้น

เซต (Set) เป็นคำอนิยาม การเขียนเซตประกอบด้วย 2 วิธีคือ

1. **วิธีแจกแจงสมาชิก (Tubular form)** การเขียนเซตแบบแจกแจงสมาชิก คือการเขียนเซตโดยเขียนสมาชิกลงในเครื่องหมายวงเล็บปีกกา $\{\}$ และใช้เครื่องหมายจุลภาค $(,)$ คั่นระหว่างสมาชิกแต่ละตัว ตัวอย่างเช่น $\{1,2,3\}, \{4,5,6\}$ และ $\{a,b,c\}$ เป็นต้น

2. **วิธีบอกเงื่อนไขของสมาชิก (Set builder form)** การเขียนเซตแบบบอกเงื่อนไขประกอบด้วย 2 ส่วน ส่วนแรกหมายถึงสมาชิก และส่วนที่สองคือเงื่อนไขของสมาชิก โดยมีเครื่องหมายทวิภาค $(:)$ คั่นระหว่างสองส่วนนั้น อ่านว่า "โดยที่"

$$A = \{ \text{ สมาชิก } : \text{ เงื่อนไขของสมาชิก } \}$$

ตัวอย่างเช่น $A = \{x : x \text{ เป็นจำนวนเต็มบวกที่น้อยกว่า } 5\}$ หมายถึง เซต A คือเซตของ x โดยที่ x เป็นจำนวนเต็มบวกที่น้อยกว่า 5 และเขียนแจกแจงสมาชิกได้เป็น $A = \{1,2,3,4,5\}$

สับเซต (subset) $A \subseteq B$ หมายถึง A ที่มีสมาชิกทุกตัวอยู่ในเซต B
ในเบื้องต้นเพื่อให้ง่ายต่อการนำไปใช้ กำหนดสัญลักษณ์ดังนี้

$\mathbb{C}$	แทนเซตของจำนวนเชิงซ้อน	$\mathbb{Z}$	แทนเซตของจำนวนเต็ม
$\mathbb{R}$	แทนเซตของจำนวนจริง	$\mathbb{N}$	แทนเซตของจำนวนนับ

เซตที่ไม่มีสมาชิกคือ**เซตว่าง** (empty set) เขียนแทนด้วย $\varnothing$ และ **เอกภพสัมพัทธ์** (universe) คือเซตที่ถูกกำหนดขึ้นโดยจะกล่าวถึงสิ่งที่เป็นสมาชิกของเซตนี้เท่านั้น และนิยมใช้ $\mathcal{U}$ และนิยามการดำเนินการบนเซตดังนี้

ยูเนียน (union)	$A \cup B = \{x \in \mathcal{U} : x \in A \text{ หรือ } x \in B\}$
อินเตอร์เซกชัน (intersection)	$A \cap B = \{x \in \mathcal{U} : x \in A \text{ และ } x \in B\}$
ผลต่าง (difference)	$A - B = \{x \in \mathcal{U} : x \in A \text{ และ } x \notin B\}$
ส่วนเติมเต็ม (complement)	$A^c = \{x \in \mathcal{U} : x \notin A\}$

ในกรณีที่ทราบจำนวนสมาชิกของเซต A เขียน $|A|$ แทนจำนวนสมาชิกของ A และได้ว่า

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A| = |\mathcal{U}| - |A^c|$$

การพิสูจน์เบื้องต้น

ตัวเชื่อมประพจน์ 4 ชนิดคือ

1. และ เขียนแทนด้วย $\wedge$
2. หรือ เขียนแทนด้วย $\vee$
3. ถ้า...แล้ว เขียนแทนด้วย $\rightarrow$
4. ก็ต่อเมื่อ เขียนแทนด้วย $\leftrightarrow$

สรุปค่าความจริงในแต่ละกรณีตามตารางดังต่อไปนี้

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	F	T	F	F
F	F	F	F	T	T

p	$\sim p$
T	F
F	T

วิธีการพิสูจน์

1. การพิสูจน์ข้อความแบบมีเงื่อนไข
2. การพิสูจน์โดยการแจกแจงกรณี
3. การพิสูจน์ข้อความแบบผันกลับได้
4. การพิสูจน์โดยวิธีขัดแย้ง
5. การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว
6. การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

การพิสูจน์ข้อความแบบมีเงื่อนไข

การพิสูจน์ในรูปแบบ $p \to q$:

	สมมติ	p	เป็นจริง
		$\vdots$	
	ดังนั้น	q	เป็นจริง (ข้อสรุป) $\square$

ตัวอย่าง

จงพิสูจน์ว่า " ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่ "

บทพิสูจน์.

ให้ n เป็นจำนวนเต็มใด ๆ สมมติว่า n เป็นจำนวนคู่ จะได้ว่ามี $k \in \mathbb{Z}$ ซึ่ง $n = 2k$ แล้ว

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

เนื่องจาก $2k^2$ เป็นจำนวนเต็ม ดังนั้น n^2 เป็นจำนวนคู่ $\square$

ตัวอย่าง

จงพิสูจน์ว่า " ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่ "
แนวคิด เขียนเป็นสัญลักษณ์จะได้เป็น

$$\forall n \in \mathbb{Z},\ n^2 \text{ เป็นจำนวนคู่ } \rightarrow n \text{ เป็นจำนวนคู่}$$

เราจะ**พิสูจน์โดยวิธีแย้งสลับที่** ดังนั้นเราจะทำการพิสูจน์ข้อความต่อไปนี้

$$\forall n \in \mathbb{Z},\ n \text{ เป็นจำนวนคี่ } \rightarrow n^2 \text{ เป็นจำนวนคี่}$$

บทพิสูจน์.

ให้ n เป็นจำนวนเต็มใด ๆ สมมติว่า n เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $n = 2k+1$ แล้วจะได้ว่า

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

เนื่องจาก $2k^2 + 2k$ เป็นจำนวนเต็ม ดังนั้น n^2 เป็นจำนวนคี่ □

การพิสูจน์โดยการแจกแจงกรณี

การพิสูจน์ข้อความในรูปแบบ $(p \vee q) \rightarrow r$ ต้องพิสูจน์ว่าทั้ง 2 กรณีเป็นจริงคือ

กรณีที่ 1 $p \rightarrow r$

สมมติ	p	เป็นจริง
	$\vdots$	
ดังนั้น	r	เป็นจริง

กรณีที่ 2 $q \rightarrow r$

สมมติ	q	เป็นจริง	
	$\vdots$		
ดังนั้น	r	เป็นจริง	$\square$

ตัวอย่าง

จงพิสูจน์ว่า "ถ้า a เป็นจำนวนคู่ หรือ a เป็นจำนวนคี่ แล้ว $a^2 + a$ เป็นจำนวนคู่"

แนวคิด เขียนข้อความในรูปสัญลักษณ์คือ

$$\forall a \in \mathbb{Z},\ (a \text{ เป็นจำนวนคู่ } \vee\ a \text{ เป็นจำนวนคี่ }) \rightarrow a^2 + a \text{ เป็นจำนวนคู่}$$

บทพิสูจน์.

ให้ a เป็นจำนวนเต็มใด ๆ

กรณีที่ 1 สมมติว่า a เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k$ แล้ว

$$a^2 + a = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k)$$

เนื่องจาก $2k^2 + k$ เป็นจำนวนเต็ม สรุปได้ว่า $a^2 + a$ เป็นจำนวนคู่

กรณีที่ 2 สมมติว่า a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม c ซึ่ง $a = 2c + 1$ แล้ว

$$a^2 + a = (2c+1)^2 + (2c+1) = 4c^2 + 4c + 1 + 2c + 1 = 2(2c^2 + 3c + 1)$$

เนื่องจาก $2c^2 + 3c + 1$ เป็นจำนวนเต็ม สรุปได้ว่า $a^2 + a$ เป็นจำนวนคู่ □

การพิสูจน์ข้อความแบบผันกลับได้

การพิสูจน์ในรูปแบบ $p \leftrightarrow q$ ซึ่งทำ 2 ขั้นตอนดังนี้

1. $p \rightarrow q$ เรียกว่าขั้น sufficient part (p เป็นเงื่อนไขที่เพียงพอสำหรับ q)
2. $q \rightarrow p$ เรียกว่าขั้น necessily part (p เป็นเงื่อนไขที่จำเป็นสำหรับ q)

ตัวอย่าง

จงพิสูจน์ "จำนวนเต็ม a ใด ๆ a เป็นจำนวนคี่ ก็ต่อเมื่อ $a+3$ เป็นจำนวนคู่"

บทพิสูจน์.

ให้ a เป็นจำนวนเต็ม

ขั้นตอนที่ 1 สมมติ a เป็นจำนวนคี่ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $a = 2k+1$ แล้ว

$$a+3 = (2k+1)+3 = 2(k+2)$$

จะเห็นได้ว่า $k+2$ เป็นจำนวนเต็ม ดังนั้น $a+3$ เป็นจำนวนเต็มคู่

ขั้นตอนที่ 2 สมมติ $a+3$ เป็นจำนวนเต็มคู่ จะได้ว่ามีจำนวนเต็ม m ซึ่ง $a+3 = 2m$ แล้ว

$$a = 2m-3 = 2(m-2)+1$$

เห็นได้ว่า $m-2$ เป็นจำนวนเต็ม ดังนั้น a เป็นจำนวนคี่ □

การพิสูจน์โดยวิธีขัดแย้ง

ต้องการพิสูจน์ข้อความ p เป็นจริงโดยการสมมติว่า $\sim p$ เป็นจริง
แล้วนำไปสู่ข้อความขัดแย้ง c การพิสูจน์แบบนี้ได้จากสัจนิรันดร์ $(\sim p \to c) \to p$

สมมติ $\sim p$ เป็นจริง

$\vdots$

ดังนั้น เกิดข้อขัดแย้ง $\square$

ตัวอย่าง

จงพิสูจน์ข้อความ "ไม่ว่า x จะเป็นจำนวนจริงใดก็ตามที่ไม่ใช่ศูนย์ จะได้ว่า $x^{-1} \neq 0$" โดยวิธีขัดแย้ง

แนวคิด ให้ p แทนข้อความ $\forall x \in \mathbb{R},\ x \neq 0 \to x^{-1} \neq 0$ สมมติว่า $\sim p$ เป็นจริง นั่นคือ

$$\exists x \in \mathbb{R},\ x \neq 0 \wedge x^{-1} = 0$$

บทพิสูจน์.

สมมติว่า มีจำนวนจริง x ซึ่ง $x \neq 0$ และ $x^{-1} = 0$ เนื่องจาก $x \neq 0$ โดยสมบัติจำนวนจริงจะได้ว่า $x(x^{-1}) = 1$ แต่จากการสมมติ $x^{-1} = 0$ จะได้ว่า

$$1 = x(x^{-1}) = x(0) = 0$$

เกิดข้อขัดแย้ง ดังนั้นข้อความนี้เป็นจริง □

การพิสูจน์ข้อความซึ่งเป็นไปได้อย่างเดียว

การพิสูจน์ข้อความ $\exists! x \in \mathcal{U},\ p(x)$ อ่านว่า มี x ใน $\mathcal{U}$ เพียงตัวเดียวเท่านั้นที่สอดคล้อง $p(x)$

$$(\exists x \in \mathcal{U},\ p(x)) \wedge (\forall x, y \in \mathcal{U},\ p(x) \wedge p(y) \rightarrow x = y)$$

ดังนั้นการพิสูจน์ $\exists! x \in \mathcal{U},\ p(x)$ แบ่งการพิสูจน์ออกเป็น 2 ส่วนคือ

1. **ขั้นที่ 1** มีอย่างน้อยหนึ่งตัว (existence)

   $\exists x \in \mathcal{U},\ p(x)$

2. **ขั้นที่ 2** มีเพียงตัวเดียว (uniqueness)

   $\forall x, y \in \mathcal{U},\ p(x) \wedge p(y) \rightarrow x = y$

ตัวอย่าง

จงพิสูจน์ว่า "มีจำนวนจริง x เพียงตัวเดียวเท่านั้นซึ่ง $2^x = 1$"

แนวคิด เขียนสัญลักษณ์ได้เป็น $\exists! x \in \mathbb{R},\ 2^x = 1$

บทพิสูจน์.

ขั้นที่ 1 มีอย่างน้อยหนึ่งตัว เลือก $x = 0$ จะได้ว่า

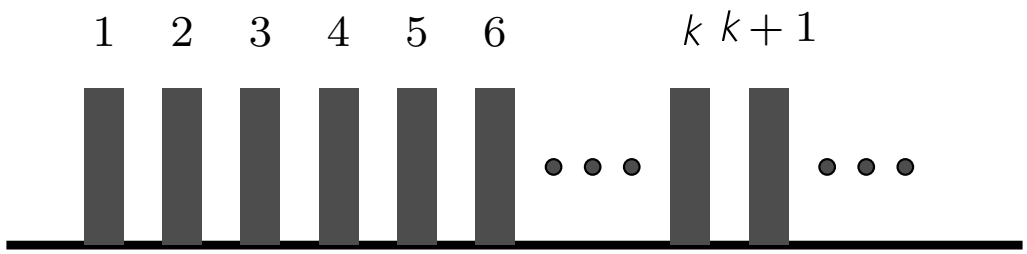
$$2^x = 2^0 = 1$$

ขั้นที่ 2 มีเพียงตัวเดียว ให้ $x, y \in \mathbb{R}$ สมมติ $2^x = 1$ และ $2^y = 1$ แล้ว

$$2^x = 1 = 2^y \quad \text{ดังนั้น} \quad 2^x = 2^y$$

จากสมบัติของเลขยกกำลังจะได้ว่า $x = y$ □

การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์



การพิสูจน์ข้อความรูปแบบ

$$\forall n \in \mathbb{N},\ P(n)$$

เมื่อ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

1. **ขั้นฐาน** (Basic step) : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** (Inductive step) : สำหรับจำนวนนับ k ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

ตัวอย่าง

จงแสดงว่า $1+2+3+4+\ldots+n=\dfrac{n(n+1)}{2}$ สำหรับทุกจำนวนนับ n

บทพิสูจน์.

ให้ $n\in\mathbb{N}$ และ $P(n)$ แทนข้อความ $1+2+3+4+\ldots+n=\dfrac{n(n+1)}{2}$

1. **ขั้นฐาน** : เนื่องจาก $1=\dfrac{1(1+1)}{2}$ ดังนั้น $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : ให้ $k\in\mathbb{N}$ สมมติ $P(k)$ เป็นจริง นั่นคือ $1+2+3+4+\ldots+k=\frac{k(k+1)}{2}$
   โดยสมมติฐาน จะได้ว่า

$$\begin{aligned}1+2+3+4+\ldots+k+(k+1)&=\frac{k(k+1)}{2}+(k+1)\\&=(k+1)\left[\frac{k}{2}+1\right]=\frac{(k+1)(k+2)}{2}\end{aligned}$$

   ทำให้สรุปได้ว่า $P(k+1)$ เป็นจริง

ดังนั้น $1+2+3+4+\ldots+n=\dfrac{n(n+1)}{2}$ ทุกจำนวนนับ n □

การพิสูจน์อุปนัยเชิงคณิตศาสตร์ที่ขั้นฐานเริ่มต้นที่ $n_0 \in \mathbb{Z}$ ข้อความในรูปแบบ

$$\forall n \in \mathbb{Z}, n \geq n_0,\ P(n)$$

เมื่อ $P(n)$ แทนข้อความที่เกี่ยวข้องกับจำนวนเต็ม ถ้า

1. **ขั้นฐาน** : $P(n_0)$ เป็นจริง
2. **ขั้นอุปนัย** : สำหรับจำนวนเต็ม k ซึ่ง $k \geq n_0$ ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

สรุปได้ว่า $\forall n \in \mathbb{Z}, n \geq n_0, P(n)$ เป็นจริง หรือ $P(n)$ เป็นจริงสำหรับจำนวนนับ ซึ่ง $n \geq n_0$

ตัวอย่าง

จงหาจำนวนนับเริ่มต้นที่ทำให้ข้อความนี้เป็นจริงพร้อมทั้งพิสูจน์ $2^n \geq n^2$

พิจารณา $2 = 2^1 \geq 1^2 = 1$, $4 = 2^2 \geq 2^2 = 4$, $8 = 2^3 \geq 3^2 = 9$, $16 = 2^4 \geq 4^2 = 16$, $32 = 2^5 \leq 5^2 = 25$, $64 = 2^4 \leq 6^2 = 36$ ดังนั้นข้อความเป็นจริงเมื่อเริ่ม $n_0 = 4$

บทพิสูจน์.

ให้ $P(n)$ แทนข้อความ $2^n \geq n^2$

1. **ขั้นฐาน** : เนื่องจาก $16 = 2^4 \geq 4^2 = 16$ ดังนั้น $P(4)$ เป็นจริง
2. **ขั้นอุปนัย** : สมมติว่า $P(k)$ เป็นจริง สำหรับจำนวนนับ $k \geq 4$ นั่นคือ $2^k \geq k^2$

เนื่องจาก $k \geq 4$ ดังนั้น $k^2 \geq 4k = 2k + 2k$ และ $2k > 1$ ฉะนั้น $k^2 \geq 2k + 1$ จากสมมติฐานจะได้

$$2^{k+1} = 2^k \cdot 2 \geq 2(k^2) = k^2 + k^2 \geq k^2 + 2k + 1 = (k+1)^2$$

ดังนั้น $2^n \geq n^2$ เป็นจริงทุกจำนวนนับ $n \geq 4$ □

ในกรณีข้อความเกี่ยวกับจำนวนนับไม่สามารถพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ที่กล่าวมาข้างต้น อาจจะใช้รูปแบบการพิสูจน์ได้ดังต่อไปนี้ ให้ $P(n)$ แทนข้อความเกี่ยวกับจำนวนนับ ถ้า

1. **ขั้นฐาน** : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนนับ k ที่ $k < m$ แล้ว $P(m)$ เป็นจริง

สรุปได้ว่า $\forall n \in \mathbb{N}$, $P(n)$ เป็นจริง หรือ $P(n)$ เป็นจริงสำหรับทุกจำนวนนับ n

ตัวอย่าง

ลำดับลูคัส (Lucus sequence) นิยามโดย $a_1 = 1,\ a_2 = 3$ และ

$$a_n = a_{n-1} + a_{n-2} \qquad \text{สำหรับ } n = 3, 4, 5, \ldots$$

จงพิสูจน์ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนนับ n

บทพิสูจน์. ให้ $P(n)$ แทนข้อความ $a_n < \left(\frac{7}{4}\right)^n$

1. **ขั้นฐาน** : เนื่องจาก $a_1 = 1 < \left(\frac{7}{4}\right)^1$ ดังนั้น $P(1)$ เป็นจริง

   เนื่องจาก $a_2 = 3 < \left(\frac{7}{4}\right)^2$ ดังนั้น $P(2)$ เป็นจริง

2. **ขั้นอุปนัย** : สมมติว่า $P(k)$ เป็นจริง สำหรับจำนวนนับ $k < m$ เมื่อ $m \geq 3$ ดังนั้น

$$a_{m-1} < \left(\frac{7}{4}\right)^{m-1} \qquad \text{และ} \qquad a_{m-2} < \left(\frac{7}{4}\right)^{m-2}$$

จะได้ว่า

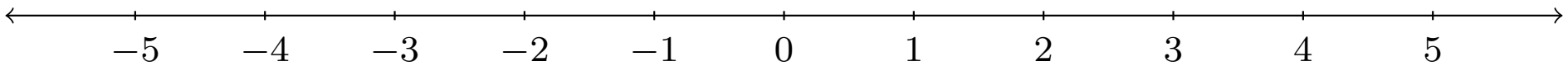
$$\begin{aligned}
a_m &= a_{m-1} + a_{m-2} \\
&< \left(\frac{7}{4}\right)^{m-1} + \left(\frac{7}{4}\right)^{m-2} = \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}\right) + \left(\frac{7}{4}\right)^{m-2} \\
&= \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}+1\right) = \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}\right) = \left(\frac{7}{4}\right)^{m-2}\left(\frac{14}{16}\right) \\
&< \left(\frac{7}{4}\right)^{m-2}\left(\frac{49}{16}\right) = \left(\frac{7}{4}\right)^{m-2}\left(\frac{7}{4}\right)^{2} = \left(\frac{7}{4}\right)^{m}
\end{aligned}$$

ดังนั้น $P(m)$ เป็นจริง

โดยหลักอุปนัยเชิงคณิตศาสตร์สรุปได้ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนนับ n

สมบัติจำนวนเต็ม

$\mathbb{Z}$ แทนเซตจำนวนเต็ม ดังนั้น $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ และแสดงได้ดังแผนภาพ



สัจพจน์จำนวนเต็ม

(A1) **สมบัติปิด** (closer laws)

สำหรับการบวก : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x + y \in \mathbb{Z}$

สำหรับการคูณ : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x \cdot y \in \mathbb{Z}$

(A2) **สมบัติสลับที่** (commutative laws)

สำหรับการบวก : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x + y = y + x$

สำหรับการคูณ : ทุก ๆ $x, y \in \mathbb{Z}$ จะได้ว่า $x \cdot y = y \cdot x$

(A3) **สมบัติการเปลี่ยนหมู่** (associative laws)

สำหรับการบวก : ทุก ๆ $x, y, z \in \mathbb{Z}$ จะได้ว่า $(x + y) + z = x + (y + z)$

สำหรับการคูณ : ทุก ๆ $x, y, z \in \mathbb{Z}$ จะได้ว่า $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(A4) **สมบัติการมีเอกลักษณ์ (existence of identities)**

สำหรับการบวก : มี $0 \in \mathbb{Z}$ ซึ่ง $x+0=x=0+x$ ทุก ๆ $x \in \mathbb{Z}$

เรียก 0 ว่าเอกลักษณ์การบวก (additive identity)

สำหรับการคูณ : มี $1 \in \mathbb{Z}$ ซึ่ง $x \cdot 1 = x = 1 \cdot x$ ทุก ๆ $x \in \mathbb{Z}$

เรียก 1 ว่าเอกลักษณ์การคูณ (multiplicative identity)

(A5) **สมบัติการมีตัวผกผัน (existence of inverse)**

สำหรับการบวก : สำหรับ $x \in \mathbb{Z}$ จะมี $-x \in \mathbb{Z}$ ซึ่ง $x+(-x)=0=(-x)+x$

เรียก $-x$ ว่าตัวผกผันการบวกของ x

(A6) **สมบัติการแจกแจง (distributive laws)**

สำหรับ $x, y, z \in \mathbb{Z}$ จะได้ว่า

$$x \cdot (y+z) = x \cdot y + x \cdot z \quad \text{และ} \quad (y+z) \cdot x = y \cdot x + z \cdot x$$

นิยมเขียน xy แทน $x \cdot y$ และ $x - y$ แทน $x + (-y)$

ข้อสังเกต

จาก A5 จะเห็นว่า x เป็นตัวผกผันการบวกของ $-x$ ดังนั้น $x = -(-x)$

Theorem

ให้ a, b, c เป็นจำนวนเต็ม แล้ว

1. $a0 = 0 = 0a$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$
4. *ถ้า* $a + b = a + c$ *แล้ว* $b = c$

Theorem

ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. $(-1)a = a(-1) = -a$
2. $-(a + b) = -a - b$
3. $a(b - c) = ab - ac$

(A7) **กฎไตรวิภาค** (Trichotomy law)

มีสับเซต $\mathbb{N}$ ของ $\mathbb{Z}$ คือ $\mathbb{N} = \{1, 2, 3, ...\}$ ที่มีสมบัติ

1. $0 \notin \mathbb{N}$
2. ถ้า $a, b \in \mathbb{N}$ แล้ว $a + b \in \mathbb{N}$ และ $ab \in \mathbb{N}$
3. ถ้า $x \in \mathbb{Z}$ แล้ว $x \in \mathbb{N}$ หรือ $x = 0$ หรือ $-x \in \mathbb{N}$

บทนิยาม

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

a **มากกว่า** (greater than) b เขียนแทนด้วย $a > b$ ก็ต่อเมื่อ $a - b \in \mathbb{N}$

a **น้อยกว่า** (less than) b เขียนแทนด้วย $a < b$ ก็ต่อเมื่อ $b > a$

Theorem

ให้ $a, b, c, x, y \in \mathbb{Z}$ แล้ว

1. ถ้า $a > b$ แล้ว $a + c > b + c$
2. ถ้า $a > b$ และ $b > c$ แล้ว $a > c$
3. ถ้า $a > b$ และ $x > y$ แล้ว $a + x > b + y$
4. ถ้า $a > b$ และ $x > 0$ แล้ว $ax > bx$
5. ถ้า $a > b$ และ $x < 0$ แล้ว $ax < bx$

(A8) **หลักการจัดอันดับดี (Well Ordering Principle)**

ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า S มีสมาชิกตัวเล็กสุด หรือ มี $m \in S$ ซึ่ง $m \leq s$ ทุก ๆ $s \in S$

Theorem

หลักการของอาร์คีมีดีส (Archimedean Principle)

สำหรับจำนวนเต็มบวก a และ b ใด ๆ จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

บทพิสูจน์.

พิสูจน์โดยวิธีขัดแย้ง สมมติว่า มีจำนวนเต็มบวก a, b สำหรับทุก ๆ จำนวนเต็มบวก n ซึ่งสอดคล้อง $na < b$ จะได้ว่า $b - an \in \mathbb{N}$ ให้

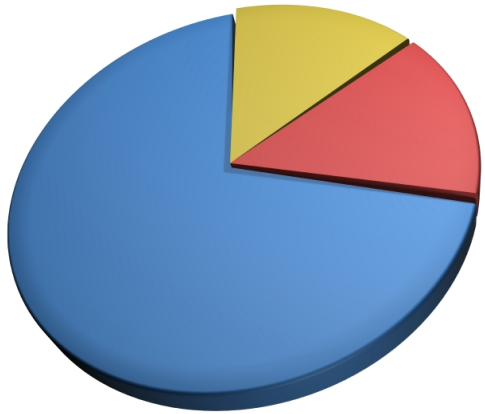
$$S = \{b - na : n \in \mathbb{N}\}$$

เห็นได้ชัดว่า $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ โดยหลักการจัดอันดับดี จะได้ว่า S มีสมาชิกตัวเล็กสุดเรียกว่า m นั่นคือ $m = b - ka$ สำหรับบางจำนวนเต็มบวก k พิจารณา

$$[b - (k+1)a] - [b - ka] = -a < 0$$

ทำให้ได้ว่า $b - (k+1)a < b - ka$ เนื่องจาก $b - (k+1)a \in S$ ทำให้เกิดข้อขัดแย้งที่ว่า m เป็นสมาชิกตัวเล็กสุดใน S □

บทที่ 2 การหารลงตัว



ขั้นตอนวิธีการหาร

เมื่อหาร 20 ด้วย 7 จะได้ผลหารเท่ากับ 2 เศษเหลือเท่ากับ 6 เขียนได้เป็น

$$20 = 7(2) + 6$$

เรียกสมการนี้ว่า ขั้นตอนวิธีการหาร

Theorem

ขั้นตอนวิธีการหาร (The Division Algorithm)

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ แล้วมีจำนวนเต็ม q และ r เพียงคู่เดียวที่ทำให้

$$b = aq + r \qquad \text{โดยที่} \qquad 0 \leq r < |a| \tag{$*$}$$

*เรียก q ว่า**ผลหาร (quotient)** และ r ว่า**เศษเหลือ (remainder)***

พิสูจน์ขั้นตอนวิธีการหาร

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$

กรณีที่ 1. $a > 0$ นั่นคือ $a = |a|$ พิจารณา $b - ax$ เมื่อ x เป็นจำนวนเต็ม

ถ้า $b - ax = 0$ จะได้ว่า $b = ax + 0$ นั่นคือ $q = x$ และ $r = 0$ ซึ่งสอดคล้อง $(*)$

ต่อไปพิจารณา $b - ax \neq 0$ ทุก ๆ จำนวนเต็ม x กำหนดให้

$$S = \{b - ax : x \text{ เป็นจำนวนเต็ม และ } b - ax > 0\}$$

เนื่องจาก $a \neq 0$ ดังนั้น $\frac{b}{a}$ เป็นจำนวนตรรกยะ จะได้ว่ามีจำนวนเต็ม k ซึ่ง $k < \frac{b}{a}$ แล้ว

$$b - ak > 0$$

ดังนั้น $S \neq \varnothing$ และ $S \subseteq \mathbb{N}$ โดยหลักการจัดอันดับดี S มีสมาชิกตัวน้อยสุด สมมติให้เป็น r

ดังนั้นมีจำนวนเต็ม q ซึ่ง

$$r = b - aq \qquad \text{และ} \qquad r > 0$$

ต่อไปเราจะพิสูจน์ว่า $r < a$ โดยใช้วิธีขัดแย้ง สมมติว่า $r \geq a$ ดังนั้น

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

โดยการเกณฑ์การพิจารณาจะได้ว่า $b - a(q+1) > 0$ ดังนั้น $r - a = b - a(q+1) \in S$
แต่ $r - a < r$ ทำให้เกิดข้อขัดแย้งกับ r ที่เป็นสมาชิกตัวน้อยสุดของ S ดังนั้น $r < a = |a|$
นั่นคือ q และ r สอดคล้องเงื่อนไข $(*)$

กรณีที่ 2. $a < 0$ นั่นคือ $-a = |a| > 0$ โดยกรณีที่ 1 จะได้ว่ามีจำนวนเต็ม q_1 และ r_1 ที่ทำให้

$$b = (-a)q_1 + r_1 \qquad \text{โดยที่} \qquad 0 \leq r_1 < -a = |a|$$

เลือก $q = -q_1$ และ $r = r_1$ ดังนั้นมีจำนวนเต็ม q และ r สอดคล้องเงื่อนไข $(*)$

สุดท้ายจะพิสูจน์ว่า จำนวนเต็ม q และ r ที่สอดคล้องเงื่อนไข $(*)$ มีเพียงชุดเดียวเท่านั้น
ให้ q_1, r_1 และ q_2, r_2 เป็นจำนวนเต็มที่สอดคล้อง

$$b = aq_1 + r_1 \qquad \text{โดยที่} \qquad 0 \leq r_1 < |a|$$
$$b = aq_2 + r_2 \qquad \text{โดยที่} \qquad 0 \leq r_2 < |a|$$

เราจะแสดงว่า $r_1 = r_2$ และ $q_1 = q_2$ สมมติว่า $r_1 < r_2$ จะได้ว่า

$$a(q_1 - q_2) = r_2 - r_1 > 0$$

แล้วจะได้ว่า

$$|a| \leq |a||q_1 - q_2| = |r_2 - r_1| = r_2 - r_1 \tag{1}$$

แต่ $r_1 \geq 0$ และ $r_1 < r_2$ ทำให้ได้ว่า $r_2 - r_1 \leq r_2 < |a|$ ทำให้เกิดขัดขัดแย้งกับ $(*)$ ในกรณีที่ $r_1 > r_2$ จะเกิดข้อขัดแย้งในทำนองเดียวกัน สรุปได้ว่า $r_1 = r_2$ เป็นผลให้ได้ว่า $aq_1 = aq_2$ เนื่องจาก $a \neq 0$ ดังนั้น $q_1 = q_2$

ตัวอย่าง

จงเขียนการหารต่อไปนี้โดยใช้ขั้นตอนการหาร

1. 11 หาร 111
   คำตอบคือ $111 = 11(10) + 1$
2. 9 หาร -108
   คำตอบคือ $-108 = 9(-12) + 0$
3. -12 หาร 1205
   คำตอบคือ $1205 = -12(-100) + 5$
4. -5 หาร -183
   คำตอบคือ $-183 = -5(38) + 7$

ข้อสังเกต

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จากขั้นตอนวิธีการหารอาจนิยามเศษ r เป็นจำนวนเต็มลบได้ โดยที่ q และ r จะขาดสมบัติความเป็นหนึ่งเดียว กล่าวคือ

$$b = aq + r \qquad \text{โดยที่} \qquad 0 \leq |r| < |a|$$

เช่น 3 หาร 2 ได้เศษเท่ากับ 2 หรือ -1 โดยการพิจารณารูปได้ 2 กรณีดังนั้น

$$2 = 3(0) + 2 \qquad \text{และ} \qquad 2 = 3(1) - 1$$

ตัวอย่าง

จงเขียนรูปแบบทั้งหมดของจำนวนเต็ม a เมื่อกำหนดให้

1. 2 หาร a

   วิธีทำ โดยขั้นตอนการหาร มีจำนวนเต็ม q และ r ซึ่ง $a = 2q + r$ โดยที่ $0 \leq r < 2$ นั่นคือ

   $$a = 2q \quad \text{และ} \quad a = 2q + 1$$

2. 3 หาร a

   วิธีทำ โดยขั้นตอนการหาร มีจำนวนเต็ม q และ r ซึ่ง $a = 3q + r$ โดยที่ $0 \leq r < 3$ นั่นคือ

   $$a = 3q,\ a = 3q + 1 \text{ และ } a = 3q + 2$$

3. 5 หาร a

   วิธีทำ โดยขั้นตอนการหาร มีจำนวนเต็ม q และ r ซึ่ง $a = 5q + r$ โดยที่ $0 \leq r < 5$ นั่นคือ

   $$a = 5q,\ a = 5q + 1,\ a = 5q + 2,\ a = 5q + 3 \text{ และ } a = 5q + 4$$

ตัวอย่าง

จงแสดงว่า**กำลังสอง**ของจำนวนเต็มใด ๆ จะอยู่ในรูป $3k$ หรือ $3k+1$ สำหรับบางจำนวนเต็ม k

บทพิสูจน์.

ให้ a เป็นจำนวนเต็มใด ๆ โดยขั้นตอนการหาร มีจำนวนเต็ม q และ r ซึ่ง $a = 3q + r$ โดยที่ $0 \leq r < 3$ นั่นคือ $a = 3q$, $a = 3q+1$ และ $a = 3q+2$

กรณี $a = 3q$ จะได้ว่า $a^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3k$
เมื่อให้ $k = 3q^2$

กรณี $a = 3q+1$ จะได้ว่า $a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$
เมื่อให้ $k = 3q^2 + 2q$

กรณี $a = 3q+2$ จะได้ว่า $a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) = 3k + 1$
เมื่อให้ $k = 3q^2 + 4q + 1$

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

Theorem

ให้ a, b และ c เป็นจำนวนเต็มโดยที่ $a \neq 0$ ถ้า

$$a \text{ หาร } b \text{ เศษเหลือเท่ากับ } r$$
$$a \text{ หาร } c \text{ เศษเหลือเท่ากับ } s$$

แล้ว

(ก) *เศษเหลือจากการหาร $b + c$ ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร $r + s$ ด้วย a*

(ข) *เศษเหลือจากการหาร bc ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร rs ด้วย a*

ตัวอย่าง

ให้ m และ n เป็นจำนวนเต็มบวก ถ้า 5 หาร m เศษเหลือเท่ากับ 4 และ 5 หาร n เศษเหลือเท่ากับ 2 แล้ว 5 หารจำนวนต่อไปนี้ เศษเหลือเท่าใด

1. $m+n$

   วิธีทำ เศษเหลือจากการหาร $m+n$ ด้วย 5 เท่ากับเศษเหลือที่ได้จากการ $4+2=6$ ด้วย 5
   ดังนั้น 5 หาร $m+n$ เศษเหลือเท่ากับ 1

2. mn

   วิธีทำ เศษเหลือจากการหาร mn ด้วย 5 เท่ากับเศษเหลือที่ได้จากการ $4(2)=8$ ด้วย 5
   ดังนั้น 5 หาร mn เศษเหลือเท่ากับ 3

3. $n-m$

   วิธีทำ เศษเหลือจากการหาร $m-n$ ด้วย 5 เท่ากับเศษเหลือที่ได้จากการ $2-4=-2$ ด้วย 5 มีจำนวนเต็ม q ซึ่ง $m-n=5q+(-2)=5q-5+3=5(q-1)+3$ ดังนั้น 5 หาร $n-m$ เศษเหลือเท่ากับ 3

Theorem

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ และ n เป็นจำนวนนับ ถ้า a หาร b เศษเหลือเท่ากับ r แล้ว

เศษเหลือจากการหาร b^n ด้วย a เท่ากับเศษเหลือที่ได้จากการหาร r^n ด้วย a

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหารต่อไปนี้

1. 2 หาร 5^{100}

   วิธีทำ เนื่องจาก 2 หาร 5 เศษเหลือเท่ากับ 1 ดังนั้น 2 หาร 5^{100} เศษเหลือเท่ากับ $1^{100} = 1$

2. 3 หาร $2^{999} \cdot 5^{898}$

   เนื่องจาก 3 หาร 2 เศษเหลือเท่ากับ -1 จะได้ว่า 3 หาร 2^{999} เศษเหลือเท่ากับ $(-1)^{999} = -1$

   เนื่องจาก 3 หาร 5 เศษเหลือเท่ากับ -1 จะได้ว่า 3 หาร 5^{898} เศษเหลือเท่ากับ $(-1)^{898} = 1$

   สรุปได้ว่า 3 หาร $2^{999} + 5^{898}$ เศษเหลือเท่ากับ $-1 + 1 = 0$

ตัวอย่าง

จงหาเศษเหลือที่เกิดจากการหารต่อไปนี้

1. 7 หาร 100^{2558}

   เนื่องจาก 7 หาร 100 เศษเหลือเท่ากับ 2 จะได้ว่า

   เศษเหลือจากการหาร 100^{2558} ด้วย 7 เท่ากับเศษเหลือที่ได้จากการหาร 2^{2558} ด้วย 7

   เนื่องจาก 7 หาร $2^6 = 64$ เศษเหลือเท่ากับ 1 จะได้ว่า เศษเหลือจากการหาร $(2^6)^{426} \cdot 2^2 = 2^{2558}$

   ด้วย 7 เท่ากับเศษเหลือที่ได้จากการหาร $1^{426} \cdot 4 = 4$ ด้วย 7

   สรุปได้ว่า 7 หาร 100^{2558} เศษเหลือเท่ากับ 4

2. 31 หาร 2^{2018}

   เนื่องจาก 31 หาร $2^5 = 32$ เศษเหลือเท่ากับ 1 ดังนั้น เศษเหลือจากการหาร $(2^5)^{403} \cdot 2^3 = 2^{2018}$

   ด้วย 31 เท่ากับเศษเหลือที่ได้จากการหาร $1^{403} \cdot 8 = 8$ ด้วย 31

   สรุปได้ว่า 31 หาร 2^{2018} เศษเหลือเท่ากับ 8

การหาเลขท้ายหนึ่งตัวและสองตัว

1. หลักหน่วย (เลขท้าย) ของจำนวนเต็มบวก a คือเศษเหลือจากการหาร a ด้วย 10
2. สองหลักสุดท้าย ของจำนวนเต็มบวก a คือเศษเหลือจากการหาร a ด้วย 100

ตัวอย่าง

จงหาหลักหน่วยของ 2^{1000}

เนื่องจาก 10 หาร $2^5 = 32$ เศษเหลือเท่ากับ 2 ดังนั้น

10 หาร $2^{1000} = (2^5)^{200}$	เศษเหลือเท่ากับ	การหาร 2^{200} ด้วย 10
10 หาร $2^{200} = (2^5)^{40}$	เศษเหลือเท่ากับ	การหาร 2^{40} ด้วย 10
10 หาร $2^{40} = (2^5)^8$	เศษเหลือเท่ากับ	การหาร $2^8 = 256$ ด้วย 10
10 หาร 256	เศษเหลือเท่ากับ 6	

ดังนั้นหลักหน่วยของ 2^{1000} คือ 6

ตัวอย่าง

จงหาหลักหน่วยของ 3^{1999}

เนื่องจาก 10 หาร $3^4 = 81$ เศษเหลือเท่ากับ 1 ดังนั้น

10 หาร $3^{1999} = (3^4)^{499} \cdot 3^3$ เศษเหลือเท่ากับ การหาร $1^{499} \cdot 27 = 27$ ด้วย 10

ดังนั้น 10 หาร 3^{1996} เศษเหลือเท่ากับ 7 สรุปได้ว่าหลักหน่วยของ 3^{1999} คือ 7

ตัวอย่าง

จงหาหลักหน่วยของ 3^{1999} $(3^{100} + 5^{100})^{100}$

ตัวอย่าง

จงหาสองหลักสุดท้ายของจำนวนต่อไปนี้

1. 7^{2558}

   เนื่องจาก 100 หาร $7^4 = 2401$ เศษเหลือเท่ากับ 1

   ดังนั้น 100 หาร $(7^4)^{639} \cdot 7^2 = 7^{2558}$ เศษเหลือเท่ากับ $1^{639} \cdot 49 = 49$

   ดังนั้นสองหลักสุดท้ายของ 7^{2558} คือ 49

2. 2^{100}

   เนื่องจาก 100 หาร $2^{10} = 1024$ เศษเหลือเท่ากับ 24

   ดังนั้น 100 หาร $2^{100} = (2^{10})^{10}$ เศษเหลือเท่ากับ 100 หาร $24^{10} = 3^{10} \cdot 2^{30}$

   เศษเหลือเท่ากับ 100 หาร $(3^5)^2 \cdot (2^{10})^3$

   เศษเหลือเท่ากับ 100 หาร $(43)^2 \cdot (24)^3$

   เศษเหลือเท่ากับ 100 หาร $49 \cdot 24 = 1176$

   ดังนั้นสองหลักสุดท้ายของ 2^{100} คือ 76

การหารลงตัว

บทนิยาม

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า a **หาร** b **ลงตัว** แทนด้วยสัญลักษณ์ $a \mid b$ นิยามโดย

$$a \mid b \quad \text{ก็ต่อเมื่อ} \quad \text{มีจำนวนเต็ม} \quad c \quad \text{ที่ทำให้} \quad b = ac$$

เรียก a ว่า**ตัวหาร** (divisor) หรือ **ตัวประกอบ** (factor) ของ b หรือเรียก b ว่าเป็น**พหุคูณ** (multiple) ของ a
ถ้า a **หาร** b **ไม่ลงตัว** เขียนแทนด้วย $a \nmid b$

ข้อสังเกต

สำหรับจำนวนเต็ม a ใด ๆ

1. $1 \mid a$
2. $a \mid 0$ เมื่อ $a \neq 0$
3. $a \mid a$ เมื่อ $a \neq 0$

เนื่องจาก $a = 1(a)$, $0 = 0(a)$ และ $a = 1(a)$

ตัวอย่าง

จงให้เหตุผลเกี่ยวกับการหารต่อไปนี้ตามนิยามการหารลงตัว

1. $13 \mid 182$ เพราะว่า $182 = 14(13)$
2. $-5 \mid 30$ เพราะว่า $30 = 6(-5)$
3. $15 \mid (-225)$ เพราะว่า $-225 = -15(15)$
4. $-12 \mid (-108)$ เพราะว่า $-108 = 9(-12)$
5. $133 \mid 0$ เพราะว่า $0 = 0(133)$
6. $7 \nmid 17$ เพราะว่า $17 = 2(7) + 3$

ตัวอย่าง

จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไข

1. $a \mid 10$

   วิธีทำ a คือตัวหารของ 10 ดังนั้น $a = 1, 2, 5, 10$

2. $(a-1) \mid 48$

   วิธีทำ $a-1$ คือตัวหารของ 48 จะได้ว่า

$$a - 1 = 1, 2, 3, 4, 6, 8, 12, 24, 48$$

$$a = 2, 3, 4, 5, 7, 9, 13, 25, 49$$

ตัวอย่าง

จงแสดงว่าไม่มีจำนวนเต็ม a ใด ๆ ซึ่ง $2 \mid a$ และ $2 \mid (a+1)$

บทพิสูจน์.

สมมติว่ามีจำนวนเต็ม a ซึ่ง $2 \mid a$ และ $2 \mid (a+1)$ จะได้ว่ามีจำนวนเต็ม x และ y ซึ่ง

$$a = 2x \qquad \text{และ} \qquad a+1 = 2y$$

จะได้ว่า $2x+1 = 2y$ หรือ $1 = 2(y-x)$ ดังนั้น 1 เป็นจำนวนคู่จึงเกิดข้อขัดแย้ง
ดังนั้นไม่มีจำนวนเต็ม a ใด ๆ ซึ่ง $2 \mid a$ และ $2 \mid (a+1)$ □

ตัวอย่าง

สำหรับจำนวนเต็ม k ใด ๆ ซึ่ง

$$d \mid (24k+29) \quad \text{และ} \quad d \mid (3k+2)$$

จงหาจำนวนเต็มบวก d ซึ่งมากกว่า 1

วิธีทำ จะได้ว่ามีจำนวนเต็ม x และ y ซึ่ง

$$\begin{aligned} 24k+29 &= dx \\ 3k+2 &= dy \\ \therefore \quad (24k+29)-8(3k+2) &= dx-8(dy) \\ \therefore \quad 13 &= d(x-8y) \end{aligned}$$

ดังนั้น $d \mid 13$ นั่นคือ $d = 13$

ตัวอย่าง

ถ้า d เป็นจำนวนเต็มบวกที่มากกว่า 1 และจำนวน $3456, 2561$ และ 1308 หารด้วย d มีเศษเหลือเท่ากันคือ r แล้ว $d+r$ เท่ากับเท่าใด

วิธีทำ จะได้ว่ามีจำนวนเต็ม x, y, z และ r ซึ่ง

$$3456 = dx + r \qquad \ldots(1)$$

$$2561 = dy + r \qquad \ldots(2)$$

$$1308 = dz + r \qquad \ldots(3)$$

$$(1) - (2): \quad 895 = d(x-y)$$

$$(1) - (3): \quad 2148 = d(x-z)$$

$$(2) - (3): \quad 1253 = d(y-z)$$

ดังนั้น $d \mid 895$, $d \mid 2148$ และ $d \mid 1253$ เนื่องจาก $895 = 179 \cdot 5$, $2148 = 179 \cdot 12$ และ $1253 = 179 \cdot 7$ ดังนั้น $d = 179$

การพิสูจน์การหารลงตัวโดยใช้ขั้นตอนการหาร

ตัวอย่าง

จงแสดงว่า $2 \mid (a^2 + a)$ เมื่อ a เป็นจำนวนเต็ม

บทพิสูจน์.

ให้ a เป็นจำนวนเต็ม โดยขั้นตอนการหารมีจำนวนเต็ม q ซึ่ง $a = 2q$ หรือ $a = 2q + 1$

กรณี $a = 2q$ จะได้ว่า $a^2 + a = (2q)^2 + 2q = 2(2q^2 + q)$ ดังนั้น $2 \mid (a^2 + a)$

กรณี $a = 2q + 1$ จะได้ว่า

$$\begin{aligned} a^2 + a &= (2q+1)^2 + (2q+1) \\ &= 4q^2 + 6q + 2 \\ &= 2(2q^2 + 3q + 1) \end{aligned}$$

ดังนั้น $2 \mid (a^2 + a)$

ตัวอย่าง

จงแสดงว่า $8 \mid (a^2-1)$ เมื่อ a เป็นจำนวนเต็มคี่

บทพิสูจน์.

ให้ a เป็นจำนวนเต็ม โดยขั้นตอนการหารมีจำนวนเต็ม q ซึ่ง $a=4q$ หรือ $a=4q+1$ หรือ $a=4q+2$ หรือ $a=4q+3$ สมมติ a เป็นจำนวนคี่จะได้ว่า $a=4q+1$ หรือ $a=4q+3$

กรณี $a=4q+1$ จะได้ว่า

$$a^2-1=(4q+1)^2-1=16q^2+8q+1-1=16q^2+8q=8(2q^2+q)$$

ดังนั้น $8 \mid (a^2-1)$

กรณี $a=4q+3$ จะได้ว่า

$$a^2-1=(4q+3)^2-1=16q^2+24q+9-1=16q^2+24q+8=8(2q^2+3q+1)$$

ดังนั้น $8 \mid (a^2-1)$

สมบัติการหารลงตัว

Theorem

ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. *ถ้า* $a \mid b$ *และ* $b \neq 0$ *แล้ว* $|a| \leq |b|$
2. *ถ้า* $a \mid b$ *และ* $b \mid a$ *แล้ว* $a = \pm b$
3. *ถ้า* $a \mid b$ *และ* $b \mid c$ *แล้ว* $a \mid c$

Theorem

ให้ a, b, c และ d เป็นจำนวนเต็ม แล้ว

1. *ถ้า* $a \mid b$ *และ* $c \mid d$ *แล้ว* $ac \mid bd$
2. *ถ้า* $a \mid b$ *แล้ว* $a^n \mid b^n$ *ทุก ๆ จำนวนนับ* n

บทพิสูจน์.

ให้ a, b, c และ d เป็นจำนวนเต็ม

1. สมมติ $a \mid b$ และ $c \mid d$ จะได้ว่ามีจำนวนเต็ม k และ p ซึ่ง $b = ak$ และ $d = cq$ ดังนั้น

$$bd = (ak)(cq) = ac(kp)$$

สรุปได้ว่า $ac \mid bd$

2. พิสูจน์โดยวิธีอุปนัยเชิงคณิตศาสตร์ กรณี $n = 1$ เห็นได้ชัดว่าข้อความนี้เป็นจริง สมมติว่า ถ้า $a \mid b$ แล้ว $a^k \mid b^k$ สำหรับจำนวนนับ k ใด ๆ สมมติว่า $a \mid b$ โดยสมมติฐานจะได้ว่า $a^k \mid b^k$ จากข้อ 1 จะได้ว่า $a \cdot a^k \mid b \cdot b^k$ หรือ

$$a^{k+1} \mid b^{k+1}$$

สรุปได้ว่า ถ้า $a \mid b$ แล้ว $a^n \mid b^n$ ทุก ๆ จำนวนนับ n

Theorem

ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. *ถ้า* $a \mid b$ *แล้ว* $a \mid bx$ *ทุก ๆ จำนวนเต็ม* x
2. *ถ้า* $a \mid b$ *แล้ว* $a \mid b^n$ *ทุก ๆ จำนวนนับ* n

Theorem

ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. *ถ้า* $a \mid b$ *และ* $a \mid c$ *แล้ว* $a \mid (b + c)$
2. *ถ้า* $a \mid b$ *และ* $a \mid c$ *แล้ว* $a \mid bc$
3. *ถ้า* $a \mid b$ *และ* $a \mid c$ *แล้ว* $a \mid (bx + cy)$ *ทุก ๆ จำนวนเต็ม* x *และ* y

Theorem

ให้ a, b และ c เป็นจำนวนเต็ม

$$\text{ถ้า} \quad a \mid (b+c) \quad \text{และ} \quad a \mid b \quad \text{แล้ว} \quad a \mid c$$

บทพิสูจน์.

ให้ a, b และ c เป็นจำนวนเต็ม สมมติ $a \mid (b+c)$ และ $a \mid b$ จะได้ว่ามีจำนวนเต็ม k และ p ซึ่ง $b+c = ak$ และ $b = ap$ แล้ว

$$c = ak - b = ak - ap = a(k-p)$$

ดังนั้น $a \mid c$ □

บทแทรก

ให้ a, c และ k เป็นจำนวนเต็ม ถ้า $a \mid (ak+c)$ แล้ว $a \mid c$

ตัวอย่าง

จงหาจำนวนเต็มบวก a ทั้งหมดที่สอดคล้องเงื่อนไข

1. $a \mid (a+2)^2$
   วิธีทำ เนื่องจาก $(a+2)^2 = a^2+4a+4 = a(a+4)+4$ จะได้ว่า $a \mid 4$ ดังนั้น $a = 1, 2, 4$

2. $(a+1) \mid (a^2+1)$
   วิธีทำ เนื่องจาก $a^2+1 = (a^2+2a+1)-2a-2+2 = (a+1)^2-2(a+1)+2$
   จะได้ว่า $(a+1) \mid 2$ นั่นคือ $a+1 = 1, 2$ สรุปได้ว่า $a = 0, 1$ ดังนั้น $a = 1$

3. $(a-1) \mid (a+1)^3$
   วิธีทำ เนื่องจาก

$$\begin{aligned}(a+1)^3 &= [(a-1)+2]^3 \\ &= (a-1)^3+6(a-1)^2+12(a-1)+8\end{aligned}$$

   นั่นคือ $(a-1) \mid 8$ สรุปได้ว่า $a-1 = 1, 2, 4, 8$ ดังนั้น $a = 2, 3, 5, 9$

ตัวอย่าง

ให้ $abcd$ เป็นเลขฐานสิบสี่หลัก จงแสดงว่า $9 \mid abcd$ ก็ต่อเมื่อ $9 \mid (a+b+c+d)$

วิธีทำ พิจารณา $abcd = a \times 10^3 + b \times 10^2 + c \times 10 + d$ จะได้ว่า

$$\begin{aligned} abc &= a(1+999) + b(1+99) + c(1+9) + d \\ &= 999a + 99b + 9c + (a+b+c+d) \\ &= 9(111a + 11b + c) + (a+b+c+d) \end{aligned}$$

ทำให้สรุปได้ว่า $9 \mid abcd$ ก็ต่อเมื่อ $9 \mid (a+b+c+d)$

ยิ่งไปกว่านั้นสรุปได้ด้วยว่า $3 \mid abcd$ ก็ต่อเมื่อ $3 \mid (a+b+c+d)$

ให้ $a_1, a_2, ..., a_n \in \{0, 1, 2, ..., 9\}$ (เลขโดด) และ $a_1 a_2 ... a_n$ เป็นเลขฐานสิบ n หลัก โดยที่ $a_1 \neq 0$

1. $2 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $2 \mid a_n$
2. $3 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $3 \mid (a_1 + a_2 + ... + a_n)$
3. $4 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $4 \mid a_{n-1} a_n$
4. $5 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $5 \mid a_n$
5. $6 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $3 \mid (a_1 + a_2 + ... + a_n)$ และ $2 \mid a_n$
6. $7 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $7 \mid (a_1 a_2 ... a_{n-1} - 2a_n)$
7. $8 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $8 \mid a_{n-2} a_{n-1} a_n$
8. $9 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $9 \mid (a_1 + a_2 + ... + a_n)$
9. $10 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $10 \mid a_n$
10. $11 \mid a_1 a_2 ... a_n$ ก็ต่อเมื่อ $11 \mid (a_n - a_{n-1} + a_{n-2} - a_{n-3} + ... \pm a_1)$

ตัวอย่าง

จงตรวจสอบการหารลงตัวของจำนวนต่อไปนี้

1. 1236 และ 22481 หารด้วย 3 ลงตัว หรือไม่
   วิธีทำ เนื่องจาก $3 \mid (1+2+3+6)$ ดังนั้น $3 \mid 1236$
   เนื่องจาก $3 \nmid (2+2+4+8+1)$ ดังนั้น $3 \nmid 22481$

2. $1,236$ และ $57,230$ หารด้วย 4 ลงตัว หรือไม่
   วิธีทำ เนื่องจาก $4 \mid 36$ ดังนั้น $4 \mid 1236$ เนื่องจาก $4 \nmid 30$ ดังนั้น $4 \nmid 57230$

3. $9,248$ และ $21,482$ หารด้วย 8 ลงตัว หรือไม่
   วิธีทำ เนื่องจาก $8 \nmid 248$ ดังนั้น $8 \nmid 9248$ เนื่องจาก $8 \nmid 482$ ดังนั้น $8 \nmid 21482$

4. $1,233$ และ $210,135$ หารด้วย 9 ลงตัว หรือไม่
   วิธีทำ เนื่องจาก $9 \mid (1+2+3+3)$ ดังนั้น $9 \mid 1233$
   เนื่องจาก $9 \nmid (2+1+0+1+3+5)$ ดังนั้น $9 \nmid 210,135$

5. $1,034$ และ $100,236$ หารด้วย 11 ลงตัว หรือไม่
   วิธีทำ เนื่องจาก $11 \mid (4-3+0-1)$ ดังนั้น $11 \mid 1034$
   เนื่องจาก $11 \nmid (6-3+2-0+0-1)$ ดังนั้น $11 \nmid 100236$

การพิสูจน์การหารลงตัวโดยใช้หลักอุปนัยเชิงคณิตศาสตร์

ตัวอย่าง

จงแสดงว่า $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก

บทพิสูจน์.

ให้ $P(n)$ แทนข้อความ $3 \mid (5^n - 2^n)$ เมื่อ n เป็นจำนวนเต็มบวก

1. **ขั้นฐาน** : เนื่องจาก $3 \mid (5^1 - 2^1)$ ดังนั้น $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : สมมติว่า $P(k)$ เป็นจริง เมื่อ $k \in \mathbb{N}$ นั่นคือ $3 \mid (5^k - 2^k)$ จะมีจำนวนเต็ม q ซึ่ง $5^k - 2^k = 3q$ โดยสมมติฐานจะได้ว่า

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

ดังนั้น $3 \mid (5^{k+1} - 2^{k+1})$ นั่นคือ $P(k+1)$ เป็นจริง

ตัวอย่าง

จงแสดงว่า $8 \mid (5^{2n}+7)$ เมื่อ n เป็นจำนวนเต็มบวก

บทพิสูจน์.

ให้ $P(n)$ แทนข้อความ $8 \mid (5^{2n}+7)$ เมื่อ n เป็นจำนวนเต็มบวก

1. **ขั้นฐาน** : เนื่องจาก $5^2+7=32$ ดังนั้น $8 \mid (5^{2(1)}+7)$ ทำให้ได้ว่า $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : สมมติว่า $P(k)$ เป็นจริง เมื่อ $k \in \mathbb{N}$ นั่นคือ $8 \mid (5^{2k}+7)$ จะมีจำนวนเต็ม q ซึ่ง $5^{2k}+7=8q$ โดยสมมติฐานจะได้ว่า

$$\begin{aligned} 5^{2(k+1)}+7 &= 5^{2k+2}+7 = 5^{2k}\cdot 5^2+7 = 5^{2k}\cdot 25+7 \\ &= (8q-7)25+7 = 8q\cdot 25-168 = 8(25q-21) \end{aligned}$$

ดังนั้น $8 \mid 5^{2(k+1)}+7$ นั่นคือ $P(k+1)$ เป็นจริง

สรุปได้ว่า $8 \mid (5^{2n}+7)$ เมื่อ n เป็นจำนวนเต็มบวก $\square$

บทที่ 3 ตัวหารร่วมมาก

ตัวหารร่วมมาก

บทนิยาม

ให้ a, b และ d เป็นจำนวนเต็ม

$$d \text{ เป็น } \textbf{ตัวหารร่วม (common divisor)} \text{ ของ } a \text{ และ } b \text{ ถ้า } d \mid a \text{ และ } d \mid b$$

ข้อสังเกต

A แทนเซตของตัวหารของ a และ B แทนเซตของตัวหารของ b แล้ว $A \cap B$ คือเซตของตัวหารร่วมของ a และ b

1. เนื่องจาก $1 \mid a$ และ $1 \mid b$ ดังนั้น $A \cap B \neq \varnothing$
2. ถ้า $a = 0$ แล้ว A เป็นเซตอนันต์ เพราะจำนวนเต็มที่ไม่ใช่ศูนย์ทุกจำนวนเป็นตัวหารของ 0
3. ถ้า $a = b = 0$ แล้ว $A \cap B$ เป็นเซตอนันต์ เหตุผลเดียวกับข้อ 2
4. ถ้า $a \neq 0$ และ $b \neq 0$ แล้ว $A \cap B$ เป็นเซตจำกัด
5. A เป็นเซตของตัวหารของ $-a$ ทำนองเดียวกัน B เป็นเซตของตัวหารของ $-b$

ตัวอย่าง

จงหาเซตของตัวร่วมของสองจำนวนต่อไปนี้

1. 125 และ -215

   เซตของตัวหารของ 125 คือ $\{\pm1, \pm5, \pm25, \pm125\}$

   เซตของตัวหารของ -215 คือ $\{\pm1, \pm5, \pm43, \pm215\}$

   ดังนั้นเซตของตัวหารร่วมของ 125 และ -215 คือ $\{\pm1, \pm5\}$

2. 252 และ 225

   เซตของตัวหารของ 252 คือ

   $$\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm9, \pm12, \pm14, \pm18, \pm21, \pm28, \pm36, \pm42, \pm63, \pm84, \pm126, \pm252\}$$

   เซตของตัวหารของ 225 คือ $\{\pm1, \pm3, \pm5, \pm9, \pm15, \pm25, \pm45, \pm75, \pm225\}$

   ดังนั้นเซตของตัวหารร่วมของ 252 และ 225 คือ $\{\pm1, \pm3, \pm9\}$

บทนิยาม

ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน จำนวนเต็ม d เป็น**ตัวหารร่วมมาก** (greatest common divisior) หรือ **ห.ร.ม.** (g.c.d.) ของ a และ b เขียนแทนด้วย $\gcd(a,b)$ ก็ต่อเมื่อ

(ก) $d \mid a$ และ $d \mid b$

(ข) ทุกจำนวนเต็ม c ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$

ข้อสังเกต

a และ b เป็นจำนวนเต็มที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่า

1. $\gcd(a,b) > 0$
2. $\gcd(a,b) = \gcd(b,a) = \gcd(|a|,|b|) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$
3. ถ้า $a \neq 0$ แล้ว $\gcd(a,0) = |a|$
4. ถ้า $a \mid b$ แล้ว $\gcd(a,b) = |a|$

ตัวอย่าง

จงหาตัวหารร่วมมากของจำนวนแต่ละคู่ต่อไปนี้

1. 125 และ -215

   วิธีทำ เซตของตัวหารร่วมของ 125 และ -215 คือ $\{\pm 1, \pm 5\}$

   ดังนั้น $\gcd(125, -215) = 5$

2. 252 และ 225

   วิธีทำ เซตของตัวหารร่วมของ 252 และ 225 คือ $\{\pm 1, \pm 3, \pm 9\}$

   ดังนั้น $\gcd(252, 225) = 9$

ตัวอย่าง

กำหนดให้ a เป็น ห.ร.ม. ของ 403 และ 465 และ b เป็น ห.ร.ม. ของ 431 และ 465 แล้ว $a-b$ มีค่าเท่าใด

วิธีทำ พิจารณาการแยกตัวประกอบของแต่ละจำนวนดังนี้

$$465 = 2 \times 5 \times 31$$

$$403 = 13 \times 31$$

$$431 = 1 \times 431$$

จะได้ว่า $a = \gcd(403, 465) = 31$ และ $b = \gcd(431, 465) = 1$ ดังนั้น $a - b = 31 - 1 = 30$

ตัวอย่าง

ถ้า n เป็นจำนวนเต็มบวกที่มากที่สุด ซึ่งหาร 90 เศษเหลือคือ 6 และหาร 150 เศษเหลือคือ 3 แล้ว n หาร 41 เศษเหลือเท่าใด

วิธีทำ เนื่องจาก n หาร 90 เศษเหลือคือ 6 และหาร 150 เศษเหลือคือ 3 จะได้ว่ามีจำนวนเต็ม p, q ซึ่ง

$$\begin{aligned} 90 &= nq + 6 \\ \therefore \quad 84 &= nq \\ 150 &= np + 3 \\ \therefore \quad 147 &= np \end{aligned}$$

ดังนั้น $n \mid 84$ และ $n \mid 147$ เนื่องจาก n เป็นจำนวนเต็มมากสุดที่สอดคล้องเงื่อนไขดังกล่าว นั่นคือ $n = \gcd(84, 147)$ พิจารณา

3	84	147
7	28	49
	4	7

ดังนั้น $n = \gcd(84, 147) = 3 \times 7 = 21$

สมบัติ ห.ร.ม.

Theorem

ให้ $a, b \in \mathbb{Z}$ *โดยที่* $a \neq 0$ *และ* $b \neq 0$ *และ* $d = gcd(a, b)$ *แล้ว*

$$\text{จะมี } x, y \in \mathbb{Z} \text{ ที่ทำให้} \qquad d = ax + by$$

บทพิสูจน์. ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ ให้

$$S = \{am + bn : m, n \in \mathbb{Z} \text{ และ } am + bn > 0\}$$

เนื่องจาก $a \neq 0$ และ $b \neq 0$ ดังนั้น $S \neq \varnothing$ และ $S \subseteq \mathbb{N}$ โดยหลักการจัดอันดับไว้ดีแล้วจะได้ว่ามี $d' \in S$ ซึ่งเป็นจำนวนเต็มบวกที่น้อยที่สุดใน S นั่นคือมีจำนวนเต็ม $x, y \in \mathbb{Z}$ ซึ่ง $d' = ax + by$ ต่อไปจะแสดงว่า d' เป็น ห.ร.ม. ของ a และ b

(ก) เนื่องจาก $a, d' \in \mathbb{Z}$ โดยขั้นตอนการหาร จะได้ว่ามีจำนวนเต็ม q, r ซึ่ง

$$a = qd' + r \qquad \text{เมื่อ} \qquad 0 \leq r < d'$$

จะได้ว่า

$$a = q(ax + by) = r$$

$$r = a - q(ax + by)$$

$$\therefore \qquad r = a(1 - qx) + b(-qy)$$

จะแสดงว่า $r = 0$ สมมติว่า $r \neq 0$ ดังนั้น $0 < r < d'$ เนื่องจาก $1 - qx$ และ $-qy$ เป็นจำนวนเต็ม และ $r > 0$ นั่นคือ $r \in S$ แต่ $r < d'$ เกิดข้อขัดแย้งที่ว่า d' เป็นจำนวนเต็มบวกน้อยสุดใน S ดังนั้น $r = 0$ สรุปได้ว่า $d' \mid a$ ในทำนองเดียวกัน สำหรับ b, d' เป็นจำนวนเต็ม พิสูจน์ได้ว่า $b \mid d'$

(ข) ให้ c เป็นจำนวนเต็มบวกซึ่ง $c \mid a$ และ $c \mid b$ จะได้ว่า $c \mid (ax + by)$ นั่นคือ $c \mid d'$ สรุปได้ว่า $c \leq d'$

จาก (ก) และ (ข) สรุปได้ว่า d' เป็น ห.ร.ม.ของ a และ b นั่นคือ $d' = d = \gcd(a, b)$ และ $d = ax + by$

บทแทรก

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ $d = \gcd(a, b)$ จะได้ว่าสำหรับจำนวนเต็ม c ใด ๆ ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$

Theorem

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

$$gcd(a, b) = 1 \quad \text{ก็ต่อเมื่อ} \quad \text{มี} \quad x, y \in \mathbb{Z} \quad \text{ที่ทำให้} \quad 1 = ax + by$$

บทพิสูจน์.

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ สมมติ $\gcd(a, b) = 1$ จะได้ว่ามีจำนวนเต็ม x, y ซึ่ง $1 = ax + by$ ในทางกลับกัน สมมติ มี $x, y \in \mathbb{Z}$ ที่ทำให้ $1 = ax + by$ ให้ $d = \gcd(a, b)$ จะได้ว่า $d \mid a$ และ $d \mid b$ จะได้ว่า $c \mid (ax + by)$ ดังนั้น $d \mid 1$ สรุปได้ว่า $d = 1$ □

Theorem

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ ซึ่ง $gcd(a, b) = 1$ จะได้ว่า

$$gcd(a, b^n) = 1 \text{ สำหรับจำนวนนับ } n \text{ ใด ๆ}$$

Theorem

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ m เป็นจำนวนเต็มบวก แล้ว

$$gcd(ma, mb) = m \cdot gcd(a, b)$$

Theorem

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

Theorem

ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ x เป็นจำนวนเต็ม แล้ว

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

ตัวอย่าง

จงหาตัวหารร่วมมากของ 75 และ 100 โดยใช้ทฤษฎีบท

$$\begin{aligned}
\gcd(75, 100) &= \gcd(75, 25 + 75(1)) \\
&= \gcd(75, 25) = \gcd(25, 75) \\
&= \gcd(25, 0 + 25(3)) \\
&= \gcd(25, 0) = 25
\end{aligned}$$

Theorem

ให้ a, b, c, m เป็นจำนวนเต็ม จะได้ว่า

1. *ถ้า* $gcd(a, m) = gcd(b, m) = 1$ *แล้ว* $gcd(ab, m) = 1$
2. *ถ้า* $gcd(a, m) = 1$ *และ* $b \mid a$ *แล้ว* $gcd(b, m) = 1$
3. *ถ้า* $a \mid bc$ *และ* $gcd(a, b) = 1$ *แล้ว* $a \mid c$
4. *ถ้า* $a \mid c$ *และ* $b \mid c$ *โดยที่* $gcd(a, b) = 1$ *แล้ว* $ab \mid c$

ตัวอย่าง

มีจำนวนเต็มตั้งแต่ 1 ถึง 1000 ที่หารด้วย 3 และ 5 ลงตัว ทั้งหมดกี่จำนวน

วิธีทำ ให้ $x \in \{1, 2, 3, ..., 1000\}$ ซึ่ง $3 \mid x$ และ $5 \mid x$
เนื่องจาก $\gcd(3, 5) = 1$ จะได้ว่า $15 \mid x$ ดังนั้น x ที่เป็นไปได้คือ

$$15, 30, 45, ..., 990$$

มีทั้งหมด 66 จำนวน

ตัวอย่าง

จงแสดงว่า สำหรับจำนวนเต็ม a, b, c ใด ๆ

$$\text{ถ้า } ab \mid c \text{ และ } \gcd(a,b) = 1 \quad \text{แล้ว} \quad a \mid c \text{ และ } b \mid c$$

บทพิสูจน์.

ให้ a, b, c เป็นจำนวนเต็ม สมมติว่า $ab \mid c$ และ $\gcd(a,b) = 1$ จะได้ว่ามีจำนวนเต็ม x, y ซึ่ง $1 = ax + by$ และมีจำนวนเต็ม k ซึ่ง $c = abk$ ดังนั้น

$$\begin{aligned} 1 \cdot c &= (ax + by)(abk) \\ c &= a(abkx + b^2ky) = b(a^2xk + abky) \end{aligned}$$

ดังนั้น $a \mid c$ และ $b \mid c$ □

Theorem

ให้ a, b, q, r เป็นจำนวนเต็ม โดยที่ $a > 0$ และ $b = aq + r$ เมื่อ $0 \leq r < a$ แล้ว

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

ตัวอย่าง

จงหาตัวหารร่วมมากของ 252 และ 198 โดยใช้ทฤษฎีบท

$$\begin{aligned}
\gcd(198, 252) &= \gcd(198, 54) && \text{เนื่องจาก} \quad 252 = 198(1) + 54 \\
&= \gcd(54, 36) && \text{เนื่องจาก} \quad 198 = 54(3) + 36 \\
&= \gcd(36, 20) && \text{เนื่องจาก} \quad 54 = 36(1) + 20 \\
&= \gcd(20, 16) && \text{เนื่องจาก} \quad 36 = 20(1) + 16 \\
&= \gcd(16, 4) && \text{เนื่องจาก} \quad 20 = 16(1) + 4 \\
&= \gcd(4, 0) && \text{เนื่องจาก} \quad 16 = 4(4) + 0 \\
&= 4
\end{aligned}$$

ดังนั้น $\gcd(198, 252) = 4$

ตัวอย่าง

จงแสดงว่า สำหรับจำนวนเต็มบวก n ใด ๆ

$$\gcd(n^3+2n, n^4+3n^2+1) = 1$$

วิธีทำ พิจารณา

$$\begin{aligned}
\gcd(n^3+2n, n^4+3n^2+1) &= \gcd(n^3+2n, (n^3+2n)(n)+(n^2+1)) \\
&= \gcd(n^3+2n, n^2+1) \\
&= \gcd(n(n^2+1)+n, n^2+1) \\
&= \gcd(n, n^2+1) \\
&= \gcd(n, 1) = 1
\end{aligned}$$

สรุปได้ว่า $\gcd(n^3+2n, n^4+3n^2+1) = 1$

บทนิยาม

ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

จำนวนเต็มบวก d จะเป็น**ตัวหารร่วม**ของ $a_1, a_2, \ldots, a_n$ ก็ต่อเมื่อ $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$

และ d จะเป็น**ตัวหารร่วมมาก**ของ $a_1, a_2, \ldots, a_n$ เขียนแทนด้วย $\gcd(a_1, a_2, \ldots, a_n)$ ก็ต่อเมื่อ

(1) d เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_n$ และ

(2) สำหรับจำนวนเต็มบวก c ถ้า c เป็นตัวหารร่วมของ $a_1, a_2, \ldots, a_n$ แล้ว $d \leq c$

Theorem

สำหรับจำนวนเต็ม $a_1, a_2, \ldots, a_n$ ที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

1. $gcd(gcd(a_1, a_2), a_3, \ldots, a_n) = gcd(a_1, a_2, \ldots, a_n)$
2. $gcd(gcd(a_1, a_2, \ldots, a_{n-1}), a_n) = gcd(a_1, a_2, \ldots, a_n)$

ตัวอย่าง

จงหาตัวหารร่วมมากต่อไปนี้

1. $\gcd(4, 6, 18)$

   วิธีทำ

$$\gcd(4, 6, 18) = \gcd(\gcd(4, 6), 18) = \gcd(2, 18) = 2$$

2. $\gcd(350, 49, 140, 105)$

   วิธีทำ

$$\begin{aligned}\gcd(350, 49, 140, 105) &= \gcd(\gcd(350, 49), 140, 105) \\ &= \gcd(7, 140, 150) \\ &= \gcd(\gcd(7, 140), 105) \\ &= \gcd(7, 105) = 7\end{aligned}$$

ขั้นตอนวิธีแบบยูคลิด

เมื่อ $d = \gcd(a, b)$ แล้วจะหาจำนวนเต็ม x, y ที่ทำให้

$$d = ax + by$$

ตัวอย่างเช่น $\gcd(2, 3) = 1$ จะได้ว่า $1 = 2(2) + 3(-1)$ นั่นคือ $x = 2$ และ $y = -1$ ซึ่งหาได้ไม่ยาก สำหรับตัวอย่าง $\gcd(305, 168) = d$ ตัวหารร่วมมากของ 305 และ 168 สามารถคำนวณได้ไม่ยาก แต่เมื่อต้องการทราบค่าจำนวนเต็ม x, y ที่สอดคล้อง

$$d = 305x + 168y$$

คงเกิดความยุ่งยากในกรหา ถ้าไม่มีเครื่องมืออื่น ๆ มาช่วยในการคำนวณคงต้องใช้เวลานานจึงจะหาค่าดังกล่าวได้สำเร็จ ในหัวข้อนี้จะมีทฤษฎีบทที่มาช่วยในการคำนวณจำนวนเต็ม x, y อันเป็นวิธีการของยุคลิดที่ได้พิสูจน์ไว้เมื่อครั้งยังมีชีวิตอยู่เรียกว่า ขั้นตอนวิธีแบบยุคลิด ดังทฤษฎีบทต่อไปนี้

Theorem

ขั้นตอนวิธีแบบยุคลิด (Euclidean Algorithm)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a > 0$ จะได้ว่ามีจำนวนเต็ม

$$q_i \quad \text{เมื่อ} \quad i = 1, 2, 3, .., n+1 \qquad \text{และ} \qquad r_j \quad \text{เมื่อ} \quad j = 1, 2, 3, .., n \quad \text{ที่ทำให้}$$

$$\begin{aligned}
b &= aq_1 + r_1 && \text{เมื่อ} \quad 0 < r_1 < a \\
a &= r_1 q_2 + r_2 && \text{เมื่อ} \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && \text{เมื่อ} \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && \text{เมื่อ} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

และ $gcd(a, b) = r_n$

ตัวอย่าง

จงหา $d = \gcd(305, 168)$ และหาจำนวนเต็ม x, y ซึ่งทำให้ $d = 305x + 168y$

$$
\begin{array}{rcrcrcrcrcl}
305 & = & 168(1) & + & 37 & \longrightarrow & 137 & = & 308 & - & 168(1) \\
305 & = & 168(1) & + & 37 & \longrightarrow & 137 & = & 308 & - & 168(1) \\
168 & = & 137(1) & + & 31 & \longrightarrow & 31 & = & 168 & - & 137(1) \\
137 & = & 31(4) & + & 13 & \longrightarrow & 13 & = & 137 & - & 31(4) \\
31 & = & 13(2) & + & 5 & \longrightarrow & 5 & = & 31 & - & 13(2) \\
13 & = & 5(2) & + & 3 & \longrightarrow & 3 & = & 13 & - & 5(2) \\
5 & = & 3(1) & + & 2 & \longrightarrow & 2 & = & 5 & - & 3(1) \\
3 & = & 2(1) & + & 1 & \longrightarrow & 1 & = & 3 & - & 2(1) \\
2 & = & 1(2) & & & & & & & &
\end{array}
$$

ดังนั้น $\gcd(305, 168) = 1$ แล้วจะได้ว่า

$$\begin{aligned}
1 &= 3 - 2(1) = 3 - [5 - 3(1)](1) = 3 - 5(1) + 3(1) = 3(2) - 5(1) \\
&= [13 - 5(2)](2) - 5(1) = 13(2) - 5(4) - 5(1) = 13(2) - 5(5) \\
&= 13(2) - [31 - 13(2)](5) = 13(2) - 31(5) + 13(10) = 13(12) - 31(5) \\
&= [137 - 31(4)](12) - 31(5) = 137(12) - 31(48) - 31(5) = 137(12) - 31(53) \\
&= 137(12) - [168 - 137(1)](53) = 137(12) - 168(53) + 137(53) = 137(65) - 168(53) \\
&= [305 - 168(1)](65) - 168(53) = 305(65) - 168(65) - 168(53) = 305(65) - 168(118) \\
&= 305(65) + 168(-118)
\end{aligned}$$

ทำให้ได้ว่า $x = 65$ และ $y = -118$

หาจำนวน x, y ที่สอดคล้องสมการ $\gcd(a,b) = ax + by$ โดยใช้การดำเนินการบนแถวตามขั้นตอนดังนี้

1. เลือกตัวมากสุดระหว่าง a และ b เป็นแถวที่ 1 เรียกว่า R_1 โดยเขียนไว้ท้ายสุดของแถว และอีกจำนวนเป็นแถวที่ 2 เรียกว่า R_2 โดยเขียนไว้ท้ายสุดของแถวเช่นกัน โดยเขียนกั้นด้วย | ระหว่างสมการกับเมตริกซ์ สมมติว่า $b > a$ เขียนได้ดังนี้

$$\begin{array}{rcrcr|rrrr} b & = & b(1) & + & a(0) & b & 1 & 0 & R_1 \\ a & = & b(0) & + & a(1) & a & 0 & 1 & R_2 \end{array}$$

2. แถวที่ 3 เรียกว่า R_3 จะเกิดจาก $R_3 = R_1 - q_1 R_2$ เมื่อ $b = aq_1 + r_1$ โดยที่ $0 \leq r_1 < a$ จะได้

$$\begin{array}{rcrcr|rrrr} b & = & b(1) & + & a(0) & b & 1 & 0 & R_1 \\ a & = & b(0) & + & a(1) & a & 0 & 1 & R_2 \\ r_1 & = & b(1) & + & a(-q_1) & r_1 & 1 & -q_1 & R_3 = R_1 - q_1 R_2 \end{array}$$

3. แถวที่ 4 เรียกว่า R_4 จะเกิดจาก $R_4 = R_2 - q_2 R_3$ เมื่อ $b = r_1 q_2 + r_2$ โดยที่ $0 \leq r_2 < r_1$ ทำเช่นนี้ไปเรื่อย ๆ จนแถวสุดท้ายเป็น $\gcd(a,b)$ อยู่ซ้ายมือ ตามขั้นตอนวิธีการหารแบบยุคลิด แล้วจะได้ $\gcd(a,b) = ax + by$ นั่นเอง

ตัวอย่าง

จงหา $d = \gcd(27, 22)$ และหาจำนวนเต็ม x, y ซึ่งทำให้ $d = 27xx + 22y$

วิธีทำ พิจารณาการดำเนินการบนแถวดังต่อไปนี้

$$\begin{array}{rcrcr|rrrl}
27 &=& 27(1) &+& 22(0) & 27 & 1 & 0 & R_1 \\
22 &=& 27(0) &+& 22(1) & 22 & 0 & 1 & R_2 \\
5 &=& 27(1) &+& 22(-1) & 5 & 1 & -1 & R_3 = R_1 - R_2 \\
2 &=& 27(-4) &+& 22(5) & 2 & -4 & 5 & R_4 = R_2 - 4R_3 \\
1 &=& 27(9) &+& 22(-11) & 1 & 9 & -11 & R_5 = R_3 - 2R_4
\end{array}$$

ดังนั้น $x = 9$ และ $y = -11$

ตัวอย่าง

จงหาจำนวนเต็ม x และ y ที่สอดคล้องสมการ $71x - 50y = 1$

วิธีทำ พิจารณาการดำเนินการบนแถวดังต่อไปนี้

$$\begin{array}{rcrcr|rrrl}
71 &=& 71(1) &+& 50(0) & 71 & 1 & 0 & R_1 \\
50 &=& 71(0) &+& 50(1) & 50 & 0 & 1 & R_2 \\
21 &=& 71(1) &+& 50(-1) & 21 & 1 & -1 & R_3 = R_1 - R_2 \\
8 &=& 71(-2) &+& 50(3) & 8 & -2 & 3 & R_4 = R_2 - 2R_3 \\
5 &=& 71(5) &+& 50(-7) & 5 & 5 & -7 & R_5 = R_3 - 3R_4 \\
3 &=& 71(-7) &+& 50(10) & 3 & -7 & 10 & R_6 = R_4 - R_5 \\
2 &=& 71(12) &+& 50(-17) & 2 & 12 & -17 & R_7 = R_5 - R_6 \\
1 &=& 71(-19) &+& 50(27) & 1 & -19 & 27 & R_8 = R_6 - R_7
\end{array}$$

ดังนั้น $1 = 71(-19) + 50(27)$ หรือ $1 = 71(-19) - 50(-27)$ สรุปได้ว่า $x = -19$ และ $y = -27$

ตัวคูณร่วมน้อย

บทนิยาม

ให้ a, b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ และ m เป็นจำนวนเต็มบวก

$$m \text{ เป็น } \textbf{ตัวคูณร่วม (common multiple)} \text{ ของ } a \text{ และ } b \quad \text{ถ้า} \quad a \mid m \quad \text{และ} \quad b \mid m$$

ข้อสังเกต

ให้ A แทนเซตของจำนวนเต็มที่หารด้วย a ลงตัว และ B แทนเซตของจำนวนเต็มที่หารด้วย b ลงตัว แล้ว

$$A \cap B \text{ คือเซตของตัวคูณร่วมของ } a \text{ และ } b$$

1. เนื่องจาก $a \mid a$ และ $b \mid b$ ดังนั้น $A \cap B \neq \varnothing$
2. ถ้า $a = 1$ แล้ว A เป็นเซตของจำนวนเต็มบวก
3. A และ B เป็นเซตอนันต์

ตัวอย่าง

จงหาตัวคูณร่วมน้อยของ

1. 2 และ 3

   เซตของจำนวนเต็มบวกที่ 2 หารลงตัว คือ $\{2, 4, 6, 8, 10, 12...\}$

   เซตของจำนวนเต็มบวกที่ 3 หารลงตัว คือ $\{3, 6, 9, 12, ...\}$

   ดังนั้นเซตของตัวคูณร่วมของ 2 และ 3 คือ $\{6, 12, 18, ...\}$

2. 6 และ 9

   เซตของจำนวนเต็มบวกที่ 6 หารลงตัว คือ $\{6, 12, 18, 24, 30, 36...\}$

   เซตของจำนวนเต็มบวกที่ 9 หารลงตัว คือ $\{9, 18, 27, 36, ...\}$

   ดังนั้นเซตของตัวคูณร่วมของ 6 และ 9 คือ $\{18, 36, 54, ...\}$

บทนิยาม

ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ จำนวนเต็มบวก m จะเป็น**ตัวคูณร่วมน้อย** (least common multiple) หรือ **ค.ร.น.** (l.c.m.) ของ a และ b เขียนแทนด้วย $\ell\text{cm}(a,b)$ ก็ต่อเมื่อ

(ก) $a \mid m$ และ $b \mid m$

(ข) ทุกจำนวนเต็มบวก c ถ้า $a \mid c$ และ $b \mid c$ แล้ว $m \leq c$

ตัวอย่าง

จงหาตัวคูณร่วมน้อยของจำนวนแต่ละคู่ต่อไปนี้

1. 15 และ 21
   วิธีทำ เนื่องจาก $15 = 3 \cdot 5$ และ $21 = 3 \cdot 7$ ดังนั้น $\ell\text{cm}(15,21) = 3 \cdot 5 \cdot 7 = 105$

2. 125 และ -55
   วิธีทำ เนื่องจาก $125 = 5^3$ และ $55 = 5 \cdot 11$ ดังนั้น $\ell\text{cm}(125,-55) = 5^3 \cdot 11 = 1375$

3. 588 และ 1050
   วิธีทำ เนื่องจาก $588 = 2^2 \cdot 3 \cdot 7^2$ และ $1050 = 2 \cdot 3 \cdot 5^2 \cdot 7$ ดังนั้น

ตัวอย่าง

ให้ a และ b เป็นจำนวนเต็มบวก ซึ่ง $a < b$ สอดคล้องเงื่อนไข

(1) 5 หาร a ลงตัว และ 3 หาร b ลงตัว

(2) a และ b เป็นจำนวนเฉพาะสัมพัทธ์กัน

(3) ค.ร.น. ของ a และ b เท่ากับ 165

จงหาจำนวน a และ b

วิธีทำ โดยเงื่อนไขจะได้ $\ell\text{cm}(a,b) = 165 = 3 \cdot 5 \cdot 11$ และ $\gcd(a,b) = 1$ ซึ่ง $5 \mid a$ และ $3 \mid b$ สรุปได้ดังตารางต่อไปนี้

a	b	$\ell\text{cm}(a,b)$	$\gcd(a,b)$
$5 \cdot 11$	3	$3 \cdot 5 \cdot 11$	1
5	$3 \cdot 11$	$3 \cdot 5 \cdot 11$	1

เนื่องจาก $a < b$ ดังนั้น $a = 5$ และ $b = 33$

Theorem

ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ จะได้ว่า $gcd(a, b) \cdot \ell cm(a, b) = |ab|$

บทพิสูจน์. ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ ให้ $d = \gcd(a, b)$ จะได้ว่ามีจำนวนเต็ม p, q ซึ่ง $a = dp$ และ $b = dq$ ให้

$$m = \frac{|ab|}{d} = \frac{|(dp)(dq)|}{d} = |dpq|$$

ดังนั้น m เป็นจำนวนเต็มบวก และ $m = |dpq| = |aq| = |bp|$ ทำให้ได้ว่า $a \mid m$ และ $b \mid m$ นั่นคือ m เป็นตัวคูณร่วมของ a และ b ให้ c เป็นจำนวนเต็มบวกซึ่ง $a \mid c$ และ $b \mid c$ จะได้ว่ามีจำนวนเต็ม u, v ซึ่ง $c = au$ และ $c = bv$ เนื่องจาก $d = \gcd(a, b)$ จะได้ว่ามีจำนวนเต็ม x, y ซึ่ง $d = ax + by$ จะได้ว่า

$$\begin{aligned}
mdc &= |cab| \\
mc(ax + by) &= c|ab| \\
m(cax + cby) &= c|ab| \\
m(bvax + auby) &= c|ab| \\
mab(vx + uy) &= c|ab| \\
\pm m(vx + uy) &= c
\end{aligned}$$

Theorem

ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ และ $m = \ell cm(a, b)$ จะได้ว่า

$$\text{สำหรับจำนวนเต็ม } c \text{ ใด ๆ} \quad \text{ถ้า} \quad a \mid c \quad \text{และ} \quad b \mid c \quad \text{แล้ว} \quad m \mid c$$

Theorem

ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ และ $k \in \mathbb{N}$ จะได้ว่า

$$\ell cm(ka, kb) = k \cdot \ell cm(a, b)$$

บทพิสูจน์. ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ ให้ $k \in \mathbb{N}$ จะได้ว่า

$$\begin{aligned}
\ell\text{cm}(ka, kb) \cdot \gcd(ka, kb) &= |(ka)(kb)| = k^2|ab| \\
\ell\text{cm}(ka, kb) \cdot k\gcd(a, b) &= k^2|ab| \\
\therefore \quad \ell\text{cm}(ka, kb) &= \frac{k|ab|}{\gcd(a, b)} \\
&= \frac{k\ell\text{cm}(a, b) \cdot \gcd(a, b)}{\gcd(a, b)} \\
&= k\ell\text{cm}(a, b)
\end{aligned}$$

บทนิยาม

ให้ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

จำนวนเต็มบวก m จะเป็น**ตัวคูณร่วม**ของ $a_1, a_2, \ldots, a_n$ ก็ต่อเมื่อ $a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m$

และ m จะเป็น**ตัวคูณร่วมน้อย**ของ $a_1, a_2, \ldots, a_n$ เขียนแทนด้วย $\ell\mathrm{cm}(a_1, a_2, ., , , a_n)$ ก็ต่อเมื่อ

(1) m เป็นตัวคูณร่วมของ $a_1, a_2, \ldots, a_n$ และ

(2) สำหรับจำนวนเต็มบวก c ถ้า c เป็นตัวคูณร่วมของ $a_1, a_2, \ldots, a_n$ แล้ว $m \leq c$

ตัวอย่าง

ถ้า x เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่ง $9, 12$ และ 15 หาร x ลงตัว แต่ 11 หาร x เศษเหลือเท่ากับ 7 แล้ว x มีค่าเท่าใด

วิธีทำ จะได้ว่า x เป็นตัวคูณร่วมของ $9, 12$ และ 15 เนื่องจาก $\ell\text{cm}(9, 12, 15) = 180$ ดังนั้น $180 \mid x$ จะได้ว่ามีจำนวนเต็ม q ซึ่ง

$$x = 180q = (11 \cdot 16 + 4)q = 11(16q) + 4q$$

เนื่องจาก11 หาร x เศษเหลือเท่ากับ 7 จะได้ว่ามีจำนวนเต็ม d ซึ่ง $x = 11d + 7$
ดังนั้นหา q ที่เล็กที่สุดที่ทำให้ 11 หาร $4q$ เศษเหลือเท่ากับ 7 แสดงได้ดังตารางต่อไปนี้

q	1	2	3	4	5	6	7	8	9	10
เศษเหลือจากการหาร $4q$ ด้วย 11	4	8	1	5	9	2	6	10	3	7

ดังนั้น $q = 10$ สรุปได้ว่า $x = 180$

Theorem

สำหรับจำนวนเต็ม $a_1, a_2, ..., a_n$ *ที่ไม่ใช่ศูนย์พร้อมกัน แล้ว*

1. $\ell cm(\ell cm(a_1, a_2), a_3, ..., a_n) = \ell cm(a_1, a_2, ..., a_n)$
2. $\ell cm(\ell cm(a_1, a_2, ..., a_{n-1}), a_n) = \ell cm(a_1, a_2, ..., a_n)$

ตัวอย่าง

จงหาตัวคูณร่วมน้อยของจำนวนต่อไปนี้

1. $\ell\text{cm}(4, 6, 18)$

   วิธีทำ $\ell\text{cm}(4, 6, 18) = \ell\text{cm}(\ell\text{cm}(4, 6), 18) = \ell\text{cm}(12, 18) = 36$

2. $\ell\text{cm}(35, 49, 42, 63)$

   วิธีทำ

$$\begin{aligned}\ell\text{cm}(35, 49, 42, 63) &= \ell\text{cm}(\ell\text{cm}(35, 49), 42, 63) = \ell\text{cm}(245, 42, 63)\\ &= \ell\text{cm}(\ell\text{cm}(245, 42), 63) = \ell\text{cm}(1470, 63) = 4410\end{aligned}$$

บทที่ 4 จำนวนเฉพาะ

นิยามและสมบัติบางประการ

บทนิยาม

จำนวนเต็ม p ที่มากกว่า 1 เรียกว่า **จำนวนเฉพาะ (prime)** ก็ต่อเมื่อ

$$p \quad \text{มีตัวหารคือ} \quad \pm 1 \quad \text{และ} \quad \pm p \quad \text{เท่านั้น}$$

จำนวนเต็มที่มากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่า **จำนวนประกอบ (composite number)**

ตัวอย่างจำนวนเฉพาะที่ไม่เกิน 30

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

และจำนวนประกอบที่ไม่เกิน 30

$$4,\ 6,\ 8,\ 9,\ 10,\ 12,\ 14,\ 15,\ 16,\ 18,\ 20,\ 21,\ 22,\ 24,\ 25,\ 26,\ 27,\ 28,\ 30$$

ข้อสังเกต

จากนิยามจะได้ว่า

1. 2 เป็นจำนวนเฉพาะที่เป็นจำนวนคู่เพียงตัวเดียวเท่านั้น
2. p เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $d \nmid p$ ทุก ๆ จำนวนเต็ม d ซึ่ง $1 < d < p$
3. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ ถ้า $a \mid p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$
4. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \mid a$ ก็ต่อเมื่อ $\gcd(a, p) = p$
5. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \nmid a$ ก็ต่อเมื่อ $\gcd(a, p) = 1$
6. ให้ p และ q เป็นจำนวนเฉพาะ ถ้า $p \mid q$ แล้ว $p = q$
7. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม d ซึ่ง $1 < d < a$ ที่ทำให้ $d \mid a$
8. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม b, c ซึ่ง $1 < b \leq c < a$ ที่ทำให้ $a = bc$

ตัวอย่าง

จงแสดงว่า ถ้า n จำนวนประกอบ แล้ว $2^n - 1$ เป็นจำนวนประกอบ

บทพิสูจน์.

ให้ n จำนวนประกอบ จะได้ว่ามีจำนวนเต็มบวก b, c ที่มากกว่า 1 ซึ่ง $n = bc$ โดย

$$x^c - 1 = (x-1)(x^{c-1} + x^{c-2} + \cdots + x + 1) \qquad \text{เมื่อ } x \in \mathbb{N}$$

จะได้ว่า

$$\begin{aligned} 2^n - 1 &= (2^b)^c - 1 \\ &= (2^b - 1)((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1) \end{aligned}$$

จะเห็นได้ว่า $2^b - 1$ และ $(2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1$ เป็นจำนวนนับที่มากกว่า 1 สรุปได้ว่า $2^n - 1$ เป็นจำนวนประกอบ □

โดยกฎแย้งสลับ สรุปได้ว่า

ถ้า $2^n - 1$ เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ

Theorem

ทุกจำนวนเต็ม a ที่มากกว่า 1 จะมีจำนวนเฉพาะ p ที่ $p \mid a$

บทพิสูจน์.

ให้ a จำนวนจำนวนเต็มที่มากกว่า 1 สมมติว่าไม่มีจำนวนเฉพาะ p ซึ่ง $p \mid a$ กำหนดให้

$$S = \{b \in \mathbb{N} : b > 1 \text{ และไม่มีจำนวนเฉพาะ } p \text{ ซึ่ง } p \mid b\}$$

โดยสมมติฐานจะได้ว่า $a \in S$ ดังนั้น $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ โดยหลักการจัดอันดับดีจะได้ว่า S มีสมาชิกตัวเล็กสุดเรียกว่า m ดังนั้น m ไม่เป็นจำนวนเฉพาะ (เนื่องจาก $m \mid m$) จะได้ว่ามี $d \in \mathbb{N}$ ซึ่ง $1 < d < m$ และ $d \mid m$ จะได้ว่า $d \notin S$ ดังนั้นมีจำนวนเฉพาะ $p \mid d$ ทำให้ได้ว่า $p \mid m$ เกิดข้อขัดแย้งกับเงื่อนไขที่ $m \in S$ □

Theorem (ยุคลิด)

มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์

บทพิสูจน์.

สมมติว่าจำนวนเฉพาะมีจำกัดตัว ให้ P เป็นจำนวนเฉพาะสูงสุด กำหนดให้

$$Q = 2 \times 3 \times 4 \times \cdots \times P + 1$$

จะเห็นได้ชัดว่า $Q > P$ ดังนั้น Q ไม่ใช่จำนวนเฉพาะ จะได้ว่ามีจำนวนเฉพาะ q ซึ่ง $q \mid Q$ จากรูปแบบของ Q ที่กำหนดจะเห็นได้ว่าไม่มีจำนวนเต็มใด ๆ จาก 2 ถึง P ที่จะหาร Q ได้ลงตัวเพราะได้เศษเหลือเท่ากับ 1 เสมอ ดังนั้น $q > P$ เกิดข้อขัดแย้งกับสมมติฐาน □

ตัวอย่าง

ให้ $n \in \mathbb{N}$ จงแสดงว่ามีจำนวนประกอบเรียงต่อกัน n จำนวน

วิธีทำ ให้ $k = 2, 3, 4, ..., n+1$ พิจารณาจำนวน $(n+1)! + k$ ดังลำดับต่อไปนี้

$$(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, ..., (n+1)! + (n+1)$$

เห็นได้ชัดว่าเป็นจำนวนประกอบ n จำนวนเรียงติดกัน เนื่องจาก $k \mid [(n+1)! + k]$ ทุก ๆ k ตัวอย่างเช่น

1. $n = 3$ จะได้จำนวน $4! + k$ เมื่อ $k = 2, 3, 4$ ดังลำดับต่อไปนี้ $26, 27, 28$
2. $n = 4$ จะได้จำนวน $5! + k$ เมื่อ $k = 2, 3, 4, 5$ ดังลำดับต่อไปนี้ $122, 123, 124, 125$

Theorem (ทฤษฎีบทนำของยุคลิด)

ให้ p เป็นจำนวนเฉพาะ และ $a, b \in \mathbb{Z}$ จะได้ว่า

$$\text{ถ้า} \quad p \mid ab \quad \text{แล้ว} \quad p \mid a \quad \text{หรือ} \quad p \mid b$$

บทพิสูจน์.

ให้ p เป็นจำนวนเฉพาะ สมมติว่า $p \mid ab$ และ $p \nmid a$ จะได้ว่า $\gcd(p, a) = 1$ จะได้ว่า $p \mid b$ □

ตัวอย่าง

จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องเงื่อนไข $p \mid (p+1)250$

วิธีทำ เนื่องจาก $p \nmid p+1$ ดังนั้น $p \mid 250$ และ $250 = 5^3 \cdot 2$ สรุปได้ว่า $p = 2, 5$

บทแทรก

ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ แล้ว

สำหรับจำนวนนับ n ถ้า $p \mid a^n$ แล้ว $p \mid a$

ตัวอย่าง

จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไขต่อไปนี้

1. $p \mid 590^{15}$
   จะได้ว่า $p \mid 590$ เนื่องจาก $590 = 59 \cdot 2 \cdot 5$ ดังนั้น $p = 2, 5, 59$
2. $p \mid 10920^{99}$
   จะได้ว่า $p \mid 10920$ เนื่องจาก $10920 = 2^3 \cdot 3 \cdot 5 \cdot 13$ ดังนั้น $p = 2, 3, 5, 7, 13$
3. $p \mid (630 + p)^4$
   จะได้ว่า $p \mid (630 + p)$ แล้ว $p \mid 630$ เนื่องจาก $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ ดังนั้น $p = 2, 3, 5, 7$
4. $p \mid (150 - 3p)^{251}$
   จะได้ว่า $p \mid (150 - 3p)$ แล้ว $p \mid 150$ เนื่องจาก $150 = 2 \cdot 3 \cdot 5^2$ ดังนั้น $p = 2, 3, 5$

ทฤษฎีบทหลักมูลเลขคณิต

Theorem

ทฤษฎีบทหลักมูลเลขคณิต *(The Fundamental Theorem of Arithmematic)*
จำนวนเต็มที่มากกว่า 1 ใด ๆ สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ และถ้าไม่คิดลำดับเป็นสำคัญแล้ว การเขียนนี้ทำได้เพียงวิธีเดียวเท่านั้น
หรือกล่าวได้ว่า จำนวนเต็ม $n > 1$ *สามารถเขียนในรูป*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

โดยที่ $p_1, p_2, p_3, ..., p_k$ *เป็นจำนวนเฉพาะซึ่ง* $p_1 < p_2 < p_3 < ... < p_k$ *และ* $a_i \in \mathbb{N}$ *สำหรับทุก* $i = 1, 2, 3, ..., k$ *และเขียน* n *ในรูปดังกล่าวได้เพียงแบบเดียวเท่านั้น เรียกการเขียน* n *รูปแบบนี้ว่า* ***รูปแบบบัญญัติ*** *(canonical form) ของ* n

ตัวอย่างจำนวนที่เขียนในรูปแบบบัญญัติ

1. $48 = 2^4 \cdot 3$
2. $150^2 = 2^2 \cdot 3^2 \cdot 5^4$
3. $1225 = 5^2 \cdot 7^2$
4. $4725 = 3^3 \cdot 5^2 \cdot 7$
5. $1000^3 = 2^9 \cdot 5^9$
6. $3528^5 = 2^{15} \cdot 3^{10} \cdot 7^{10}$
7. $15750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$
8. $846876 = 2^2 \cdot 3 \cdot 70573$

ถ้า $n > 1$ และ $m > 1$ และเขียนรูปแบบบัญญัติได้ดังนี้

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k} \qquad \text{และ} \qquad m = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots p_k^{b_k}$$

เมื่อแต่ละจำนวนเต็ม $a_i \geq 0$ และ $b_i \geq 0$ โดยที่ไม่เป็นศูนย์พร้อมกัน จะได้ว่า

$$\gcd(n, m) = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdots p_k^{c_k}$$
$$\ell\text{cm}(n, m) = p_1^{d_1} \cdot p_2^{d_2} \cdot p_3^{d_3} \cdots p_k^{d_k}$$

โดยที่ d_i และ c_i คือ ค่าต่ำสุดและสูงสุด ของ a_i และ b_i ตามลำดับ สำหรับทุก ๆ $i \in \{1, 2, 3, ..., k\}$

ตัวอย่าง

จงหาตัวหารร่วมมากและตัวคูณร่วมน้อยของจำนวนต่อไปนี้

1. 308 และ 1,176

   วิธีทำ เนื่องจาก $308 = 2^2 \cdot 7 \cdot 11$ และ $1176 = 2^3 \cdot 3 \cdot 7^2$ ดังนั้น

$$\gcd(308, 1176) = 2^2 \cdot 7 = 28$$

$$\ell\text{cm}(308, 1176) = 2^3 \cdot 3 \cdot 7^2 \cdot 11 = 12936$$

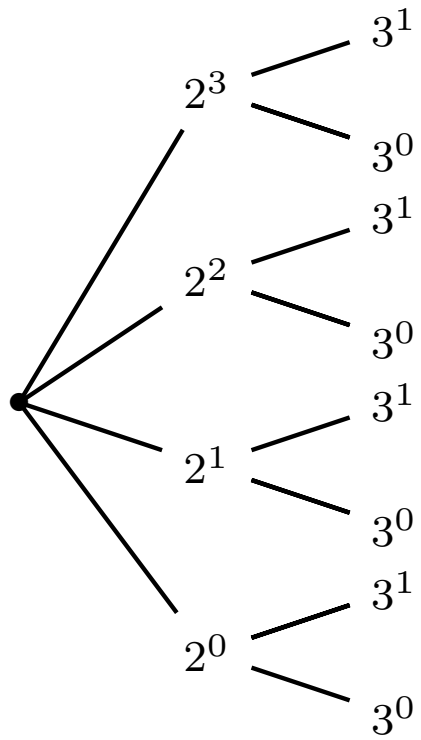
2. 31,752 และ 4,725

   วิธีทำ เนื่องจาก $31752 = 2^3 \cdot 3^4 \cdot 7^2$ และ $4725 = 3^3 \cdot 5^2 \cdot 7$ ดังนั้น

$$\gcd(31752, 4725) = 3^3 \cdot 7 = 189$$

$$\ell\text{cm}(31752, 4725) = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7^2 = 793800$$

พิจารณาการหาตัวหารทั้งหมดของ $24 = 2^3 \cdot 3$ เขียนแผนภาพต้นไม้ได้ดังนี้



จากแผนภาพจะได้ว่าตัวหารของ 24 คือ

$2^0 \cdot 3^0$	$2^0 \cdot 3^1$	$2^1 \cdot 3^0$	$2^1 \cdot 3^1$
$2^2 \cdot 3^0$	$2^2 \cdot 3^1$	$2^3 \cdot 3^0$	$2^3 \cdot 3^1$

หรือ $1, 2, 3, 4, 6, 8, 12, 24$

Theorem

ให้ $n \in \mathbb{Z}$ *ซึ่ง* $n > 1$ *มีรูปแบบบัญญัติคือ*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

เมื่อ $a_i \in \mathbb{N}$ *ทุก ๆ* i *แล้วจำนวนตัวประกอบทั้งหมดของ* n *มีทั้งหมด*

$$(a_1 + 1)(a_2 + 1)(a_3 + 1) \cdots (a_k + 1)$$

ตัวอย่าง

จงหาจำนวนตัวหารทั้งหมดของ

1. 1,225

   วิธีทำ เนื่องจาก $1225 = 5^2 \cdot 7^2$

   ดังนั้นจำนวนตัวหารทั้งหมดของ 1125 คือ $(2 + 1)(2 + 1) = 9$ ตัว

2. 100^3

   วิธีทำ เนื่องจาก $100^3 = 2^6 \cdot 5^6$

   ดังนั้นจำนวนตัวหารทั้งหมดของ 100^3 คือ $(6 + 1)(6 + 1) = 49$ ตัว

การค้นหาจำนวนเฉพาะ

Theorem

ถ้า a เป็นจำนวนประกอบ แล้วจะมีจำนวนเฉพาะ p ซึ่ง

$$p \leq \sqrt{a} \qquad \text{และ} \qquad p \mid a$$

บทพิสูจน์.

ให้ a เป็นจำนวนประกอบ จะได้ว่ามี $1 < n \leq m < a$ ซึ่ง ที่ทำให้ $a = nm$ ดังนั้น $m \mid a$ และ $n \mid a$ แสดงว่า

$$1 < n^2 \leq mn = a$$

ดังนั้น $n \leq \sqrt{a}$ จะได้ว่ามีจำนวนเฉพาะ p ซึ่ง $p \mid n$ ทำให้ได้ว่า $p \mid a$ และ $p \leq \sqrt{a}$ □

ตัวอย่าง

จงตรวจสอบจำนวนต่อไปนี้ว่าเป็นจำนวนเฉพาะหรือไม่

1. 101

   วิธีทำ เนื่องจากจำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{101} \approx 10.05$ คือ $2, 3, 5, 7$ และทุกตัวหาร 101 ไม่ลงตัวดังนั้น 101 เป็นจำนวนเฉพาะ

2. 113

   วิธีทำ เนื่องจากจำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{113} \approx 10.63$ คือ $2, 3, 5, 7$ และทุกตัวหาร 113 ไม่ลงตัวดังนั้น 113 เป็นจำนวนเฉพาะ

3. 313

   วิธีทำ เนื่องจากจำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{313} \approx 17.69$ คือ $2, 3, 5, 7, 11, 13, 17$ และทุกตัวหาร 313 ไม่ลงตัวดังนั้น 313 เป็นจำนวนเฉพาะ

4. 719

   วิธีทำ เนื่องจากจำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{719} \approx 26.81$ คือ $2, 3, 5, 7, 11, 13, 17, 19, 23$ และทุกตัวหาร 719 ไม่ลงตัวดังนั้น 101 เป็นจำนวนเฉพาะ

ต่อไปจะกล่าวถึงการหาจำนวนเฉพาะทุกตัวที่น้อยกว่าหรือเท่ากับ n เมื่อกำหนดจำนวนเต็ม n โดยใช้กฎแย้งสลับที่ของทฤษฎีบท

$$\text{ถ้าทุกจำนวนเฉพาะ } p \text{ ซึ่ง } p \leq \sqrt{a} \text{ และ } p \nmid a \text{ แล้ว } a \text{ เป็นจำนวนเฉพาะ}$$

วิธีการนี้เรียกว่า **ตะแกรงเอราโตสเทเนส (The sieve of Eratosthesnes)** ซึ่งทำได้ดังนี้

(1) $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_k$ เป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$

(2) เขียนจำนวนเต็มตั้งแต่ 2 ถึง n

(3) วงกลม p_1 แล้วกำจัดจำนวนทุกตัวในข้อ (2) ที่หารด้วย p_1 ลงตัว

(4) ทำข้อ (3) ซ้ำไปเรื่อยจาก $p_2, p_3, \ldots, p_k$

จำนวนเต็มที่เหลือจะเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่า n

ตัวอย่าง

จงตรวจสอบจำนวนเฉพาะที่ไม่เกิน 50

วิธีทำ จำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ $\sqrt{50}$ คือ $2, 3, 5, 7$ ทำได้โดย
ขั้นแรกกำจัดจำนวนเต็มที่หารด้วย 2 ลงตัว ด้วยเครื่องหมาย /

	②	3	4̸	5	6̸	7	8̸	9	10̸
11	12̸	13	14̸	15	16̸	17	18̸	19	20̸
21	22̸	23	24̸	25	26̸	27	28̸	29	30̸
31	32̸	33	34̸	35	36̸	37	38̸	39	40̸
41	42̸	43	44̸	45	46̸	47	48̸	49	50̸

ขั้นถัดไปกำจัดจำนวนเต็มที่หารด้วย 3 ลงตัว ด้วยเครื่องหมาย $\times$

	②	③	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

แล้วกำจัดจำนวนเต็มที่หารด้วย 5 ลงตัว ด้วยเครื่องหมาย //

	②	③	4	⑤	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

สุดท้ายกำจัดจำนวนเต็มที่หารด้วย 7 ลงตัว ด้วยเครื่องหมาย \

	②	③	4	⑤	6	⑦	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

สรุปได้ว่าจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 50 คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 35, 37, 41, 43, 47

ตัวอย่าง

จงตรวจสอบว่า 2,093 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจากจำนวนเฉพาะทั้งหมดที่น้อยกว่า $\sqrt{2093} \approx 45.74$ คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 35, 37, 41, 43 แต่ $7 \mid 2093$ ดังนั้น 2093 ไม่เป็นจำนวนเฉพาะ

ตัวอย่าง

จงหาจำนวนเฉพาะที่ไม่เกิน 50 ที่สามารถเขียนในรูป $3k+1$ ได้

วิธีทำ พิจารณาดังตารางต่อไปนี้

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3k+1$	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49

ดังนั้นจำนวนเฉพาะที่ไม่เกิน 50 ที่สามารถเขียนในรูป $3k+1$ ได้คือ 7, 13, 19, 31, 37, 43

จำนวนเฉพาะทั้งหมดที่น้อยกว่า 1,000

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509
521	523	541	547	557	563	569	571	577	587	593	599
601	607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743	751
757	761	769	773	787	797	809	811	821	823	827	829
839	853	859	863	877	881	883	887	907	911	919	929
937	941	947	953	967	971	977	983	911	997		

บทนิยาม

จำนวนแฟร์มาต์ (Fermat Numbers) คือจำนวนที่อยู่ในรูป

$$F_n = 2^{2^n} + 1 \qquad \text{เมื่อ } n \geq 0$$

ตัวอย่างเช่น

$$F_0 = 3 \qquad F_1 = 5 \qquad F_2 = 17 \qquad F_3 = 257 \qquad F_4 = 65537$$

ทั้ง 5 จำนวนล้วนเป็นจำนวนเฉพาะแฟร์มาต์คาดเดาว่าจำนวนต่อ ๆ น่าจะเป็นจำนวนเฉพาะ ต่อมาในปี ค.ศ. 1732 ออยเลอร์พบว่า $F_5 = 4294967297 = 641 \cdot 6700417$ ทำให้คำกล่าาของแฟร์มาต์เป็นเท็จ ดังนั้นถ้า F_n เป็นจำนวนเฉพาะ จะเรียก F_n ว่า **จำนวนเฉพาะแฟร์มาต์ (Fermat prime)** และในปี ค.ศ. 1878 ลูคัส นักคณิตศาสตร์ชาวฝรั่งเศสได้พิสูจน์ว่า

$$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 274177 \cdot 67280421310721$$

ดังนั้น F_6 เป็นจำนวนประกอบ จากการศึกษาพบว่าจำนวนแฟร์มาต์ F_n เป็นจำนวนประกอบสำหรับ $5 \leq n \leq 50$ อย่างไรก็ตามยังไม่มีผู้ใดพิสูจน์ได้ว่าจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ที่สามารถเขียนในรูป $2^{2^n} + 1$ หรือไม่ และยังไม่มีผู้ใดพบจำนวนเฉพาะของแฟร์มาต์ตัวอื่น ๆ อีกเลย

Theorem

สำหรับ $m > n$ แล้ว $gcd(F_m, F_n) = 1$

บทพิสูจน์.

ให้ $m, n \in \mathbb{Z}$ และ $m > n \geq 0$ กำหนดให้ $\gcd(F_m, F_n) = d$ จะแสดงว่า $d = 1$ ให้ $x = 2^{2^n}$ และ $k = 2^{m-n}$ พิจารณา

$$\begin{aligned} F_m - 2 &= (2^{2^n})^{2^{m-n}} - 1 \\ &= x^k - 1 \\ &= (x+1)(x^{k-1} - x^{k-2} + \cdots + x - 1) \\ &= (2^{2^n} + 1)(x^{k-1} - x^{k-2} + \cdots + x - 1) \\ &= F_n(x^{k-1} - x^{k-2} + \cdots + x - 1) \end{aligned}$$

ดังนั้น $F_n \mid (F_m - 2)$ เนื่องจาก $d \mid F_n$ ฉะนั้น $d \mid (F_m - 2)$ และ $d \mid F_m$ ทำให้ได้ว่า $d \mid 2$ แต่ d เป็นจำนวนคี่ ดังนั้น $d = 1$ □

บทนิยาม

จำนวนมาร์เซน (Mersenne Numbers) คือจำนวนที่อยู่ในรูป

$$M_n = 2^n - 1 \qquad \text{เมื่อ } n \in \mathbb{N}$$

ตัวอย่างเช่น

$$M_1 = 1 \qquad M_2 = 3 \qquad M_3 = 7 \qquad M_4 = 15 \qquad M_5 = 31$$

ถ้า M_n เป็นจำนวนเฉพาะ เราจะเรียก M_n ว่า **จำนวนเฉพาะแมร์เซน (Mersenne prime)**

Theorem

ถ้า M_n เป็นจำนวนเฉพาะ แล้ว n เป็นจำนวนเฉพาะ

บทพิสูจน์.

พิสูจน์โดยวิธีแย้งสลับที่ ให้ n จำนวนประกอบ นั่นคือมีจำนวนเต็มบวก b, c ที่มากกว่า 1 ซึ่ง $n = bc$ โดย

$$x^c - 1 = (x-1)(x^{c-1} + x^{c-2} + \cdots + x + 1) \qquad \text{เมื่อ } x \in \mathbb{N}$$

จะได้ว่า

$$\begin{aligned} M_n = 2^n - 1 &= (2^b)^c - 1 \\ &= (2^b - 1)((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1) \end{aligned}$$

จะเห็นได้ว่า $2^b - 1$ และ $(2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1$ เป็นจำนวนนับที่มากกว่า 1 สรุปได้ว่า M_n เป็นจำนวนประกอบ □

จากทฤษฎีบทดังกล่าวจะได้ว่าจำนวน M_p เป็นจำนวนเฉพาะของแมร์เซนได้ ก็ต่อเมื่อ มีจำนวนเฉพาะ p ที่ทำให้ M_p เป็นจำนวนเฉพาะเช่น

$$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8191$$