

เสริมความรู้สู่คณิตศาสตร์โอลิมปิกระหว่างประเทศ

โลกทฤษฎีจำนวน Number Theory

Congruence modulo n

Gauss's theorem

Wilson's theorem

Euler's theorem

Fermat's theorem

Fermat's Little theorem

Fermat number

Mersenne number

Perfect number

Fibonacci number

Triangular number

Floor function

Ceiling function

Primitive root

คณิตศาสตร์ปรัญญ เล่มที่ 37

รองศาสตราจารย์ ดำรงค์ กิทยโศภิต
ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

โลกทฤษฎีจำนวน

รองศาสตราจารย์ ดำรงค์ ทิพย์โยธา

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ชื่อหนังสือ : คณิตศาสตร์ปรัญ เล่มที่ 37 โลกทฤษฎีจำนวน

ชื่อผู้แต่ง : รองศาสตราจารย์ ดำรงค์ ทิพย์โยธา

จัดทำโดย : รองศาสตราจารย์ ดำรงค์ ทิพย์โยธา

พิมพ์ครั้งที่ : 1

เดือนและปีที่ พ.ศ. ที่จัดพิมพ์ : ตุลาคม พ.ศ. 2561

เลขมาตรฐานสากลประจำหนังสืออิเล็กทรอนิกส์

ISBN (e-book) : 978-616-478-098-9

พิมพ์ที่ : ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

คำนำ

วิชา **ทฤษฎีจำนวน** มีความสำคัญในการศึกษาคณิตศาสตร์ทั้งคณิตศาสตร์บริสุทธิ์และคณิตศาสตร์ประยุกต์หลายสาขา มหาวิทยาลัยหลายแห่งจัดให้เป็นวิชาบังคับในการเรียนระดับปริญญาตรี สำหรับนักเรียนที่ต้องการเป็นตัวแทนประเทศไทยเพื่อสอบคณิตศาสตร์โอลิมปิกระหว่างประเทศ (IMO) ต้องถือว่าวิชาทฤษฎีจำนวนเป็นวิชาบังคับที่ต้องรู้เป็นอย่างยิ่ง เนื่องจากข้อสอบคัดเลือก IMO ตั้งแต่รอบแรกของประเทศไทยผู้ออกข้อสอบต้องออกข้อสอบทฤษฎีจำนวนแน่นอน จนกระทั่งนักเรียนได้เป็นตัวแทนของประเทศไทยในการสอบคณิตศาสตร์โอลิมปิกระหว่างประเทศ (IMO) ข้อสอบที่แข่งขันกันยังต้องออกเนื้อหาทฤษฎีจำนวน เพราะฉะนั้นมีความจำเป็นอย่างยิ่งสำหรับนักเรียนที่ต้องการเป็นตัวแทนประเทศไทยเพื่อเข้าสอบคณิตศาสตร์โอลิมปิกระหว่างประเทศทุกคนต้องมีความรู้ทฤษฎีจำนวน

หนังสือ **โลกทฤษฎีจำนวน** เล่มนี้รวบรวมเนื้อหาของทฤษฎีจำนวนที่สำคัญสามารถใช้เป็นตำราประกอบการเรียนการสอนวิชาทฤษฎีจำนวนในระดับปริญญาตรีได้ สำหรับนักเรียนที่ต้องการเป็นตัวแทนประเทศไทยเพื่อสอบคณิตศาสตร์โอลิมปิกระหว่างประเทศ สามารถใช้เป็นหนังสือเล่มนี้เป็นตำราเพื่อศึกษาเนื้อหาของทฤษฎีจำนวนเพื่อเตรียมสอบได้

เนื้อหาภายในเล่มมี บทนิยาม ทฤษฎีบท ตัวอย่าง และ แบบฝึกหัดที่มีเฉลยทุกข้อเพื่อประโยชน์ในการเตรียมสอบโดยมีเนื้อหาที่สำคัญเช่น

- หลักอุปนัยเชิงคณิตศาสตร์ การหารลงตัว ขั้นตอนวิธีการหาร
- ตัวหารร่วมมาก ตัวคูณร่วมน้อย จำนวนเฉพาะ ทฤษฎีบทหลักมูลของเลขคณิต
- ลงรอย สมการลงรอย
- ฟังก์ชันเลขคณิต ฟังก์ชันแยกคูณ ฟังก์ชันพหุคูณ ฟังก์ชันพหุคูณ ฟังก์ชันเลขคณิต
- สมการไดโอแฟนไทน์เชิงเส้น
- ทฤษฎีบทเศษเหลือของจีน
- Gauss's theorem, Wilson's theorem, Euler's theorem
- Fermat's theorem, Fermat's little theorem
- รากปฐมฐาน
- จำนวนแฟร์มาต์ จำนวนเมอร์เซน จำนวนสมบูรณ์ จำนวนฟีโบนัชชี จำนวนสามเหลี่ยม

สุดท้ายนี้ขอขอบคุณผู้อ่านทุกท่านที่ติดตามผลงานคณิตศาสตร์ปรนัยมาโดยตลอด

รองศาสตราจารย์ ดำรงค์ ทิพย์โยธา

สารบัญ

บทที่ 1 ระบบจำนวนเต็ม	1 – 28
1.1 ระบบจำนวนเต็ม	1
1.2 หลักการจัดอันดับดี	1
1.3 อุปนัยเชิงคณิตศาสตร์	2
1.4 การหารลงตัว	4
บทที่ 2 ตัวหารร่วมมากและตัวคูณร่วมน้อย	29 – 62
2.1 ตัวหารร่วมมาก	29
2.2 ตัวคูณร่วมน้อย	50
บทที่ 3 ทฤษฎีบทหลักมูลของเลขคณิต	63 – 90
3.1 ตะแกรงเอราโตสเทเนส	63
3.2 ทฤษฎีบทหลักมูลของเลขคณิต	69
บทที่ 4 ฟังก์ชันพหุนาม ฟังก์ชันพหุนาม ฟังก์ชันลอจองต์	91 – 134
4.1 ฟังก์ชันพหุนามและฟังก์ชันพหุนาม	91
4.2 ฟังก์ชันลอจองต์	102
บทที่ 5 ฟังก์ชันเลขคณิต	135 – 198
5.1 ฟังก์ชันเลขคณิต	135
5.2 ฟังก์ชันเทา	141
5.3 ฟังก์ชันซิกมา	143
5.4 ฟังก์ชันออยเลอร์-ฟี	155
บทที่ 6 ลงรอย	199 – 328
6.1 ลงรอย	199
6.2 ระบบสมบูรณ์ของส่วนตกค้าง	220
6.3 ทฤษฎีบทของแฟร์มาต์และทฤษฎีบทของออยเลอร์	229
บทที่ 7 สมการลงรอย	329 – 396
7.1 สมการลงรอย	329
7.2 ระบบสมการลงรอย	335

7.3 สมการไดโอแฟนไทน์เชิงเส้น	346
7.4 Quadratic Residues	352
7.5 การหาผลเฉลยของ $f(x) \equiv 0 \pmod{n}$	358
7.6 การหาผลเฉลยของ $f(x) \equiv 0 \pmod{p^k}$	361
บทที่ 8 รากปฐมฐาน	397 – 452
8.1 รากปฐมฐาน	397
8.2 เศษตกค้างยกกำลัง	417
8.3 อันดับสากล	436
บทที่ 9 จำนวนแฟร์มาต์ จำนวนเมอร์เซน จำนวนสมบูรณ์ จำนวนฟีโบนัชชี จำนวนสามเหลี่ยม	453 – 476
9.1 จำนวนแฟร์มาต์	453
9.2 จำนวนเมอร์เซน	455
9.3 จำนวนสมบูรณ์	457
9.4 จำนวนฟีโบนัชชี	462
9.5 จำนวนสามเหลี่ยม	463

ข้อตกลงเกี่ยวกับสัญลักษณ์

$\mathbb{Z}$	เซตของจำนวนเต็ม	$\mathbb{Z}^+$	เซตของจำนวนเต็มบวก, เซตของจำนวนนับ
$\mathbb{Z}^-$	เซตของจำนวนเต็มลบ	$\mathbb{N}$	เซตของจำนวนเต็มบวก, เซตของจำนวนนับ
$\mathbb{N}^0$	เซตของจำนวนเต็มบวกหรือศูนย์	$\mathbb{Q}$	เซตของจำนวนตรรก
$\mathbb{Q}^+$	เซตของจำนวนตรรกบวก	$\mathbb{Q}^-$	เซตของจำนวนตรรกลบ
$\mathbb{Q}^0$	เซตของจำนวนตรรกบวกหรือศูนย์	$\mathbb{R}$	เซตของจำนวนจริง
$\mathbb{R}^+$	เซตของจำนวนจริงบวก	$\mathbb{R}^-$	เซตของจำนวนจริงลบ
$\mathbb{R}^0$	เซตของจำนวนจริงบวกหรือศูนย์	$\mathbb{C}$	เซตของจำนวนเชิงซ้อน

ให้ a เป็นจำนวนจริง

Floor function $\lfloor a \rfloor$ คือจำนวนเต็มค่ามากที่สุดที่น้อยกว่าหรือเท่ากับ a เช่น $\lfloor 2.4 \rfloor = 2$

Ceiling function $\lceil a \rceil$ คือจำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ a เช่น $\lceil 2.4 \rceil = 3$

Fractional part function $\{ a \} = a - \lfloor a \rfloor$

บทที่ 1

ระบบจำนวนเต็ม



Euclid of Alexandria
about 325 BC - about 265 BC

1.1 ระบบจำนวนเต็ม

ระบบจำนวนเต็ม $(\mathbb{Z}, +, \cdot)$ คือระบบที่ประกอบด้วยเซตของจำนวนเต็ม $(\mathbb{Z})$ และการดำเนินการบวก $(+)$ และการดำเนินการคูณ $(\cdot)$ ที่มีคุณสมบัติ

1. ทุกค่า $a, b \in \mathbb{Z}$ จะได้ $a + b \in \mathbb{Z}$ (สมบัติปิดภายใต้การบวก)
2. ทุกค่า $a, b \in \mathbb{Z}$ จะได้ $a + b = b + a$ (สมบัติสลับที่ภายใต้การบวก)
3. ทุกค่า $a, b, c \in \mathbb{Z}$ จะได้ $(a + b) + c = a + (b + c)$ (สมบัติเปลี่ยนกลุ่มภายใต้การบวก)
4. มี $0 \in \mathbb{Z}$ ที่ทำให้ $a + 0 = a = 0 + a$ ทุกค่า $a \in \mathbb{Z}$ (สมบัติมีเอกลักษณ์ภายใต้การบวก)
5. ทุกค่า $a \in \mathbb{Z}$ จะมี $-a \in \mathbb{Z}$ ที่ทำให้ $a + (-a) = 0 = (-a) + a$ (สมบัติมีอินเวอร์สภายใต้การบวก)

หมายเหตุ $a \cdot b$ แทนด้วย ab

6. ทุกค่า $a, b \in \mathbb{Z}$ จะได้ $ab \in \mathbb{Z}$ (สมบัติปิดภายใต้การคูณ)
7. ทุกค่า $a, b \in \mathbb{Z}$ จะได้ $ab = ba$ (สมบัติสลับที่ภายใต้การคูณ)
8. ทุกค่า $a, b, c \in \mathbb{Z}$ จะได้ $(ab)c = a(bc)$ (สมบัติเปลี่ยนกลุ่มภายใต้การคูณ)
9. มี $1 \in \mathbb{Z}$ ที่ทำให้ $a \cdot 1 = a = 1 \cdot a$ ทุกค่า $a \in \mathbb{Z}$ (สมบัติมีเอกลักษณ์ภายใต้การคูณ)
10. ทุกค่า $a, b, c \in \mathbb{Z}$ จะได้ $a(b + c) = ab + ac$ และ $(a + b)c = ac + bc$ (สมบัติการกระจาย)

1.2 หลักการจัดอันดับดี (Well ordering principle)

ทฤษฎีบท 1.2.1 ให้ $S \subset \mathbb{N}$ และ $S \neq \emptyset$ จะมี $x \in S$ ที่ทำให้ $x \leq a$ ทุกค่า $a \in S$

เพราะฉะนั้นทุกสับเซตของ $\mathbb{N}$ ที่ไม่เป็นเซตว่างต้องมีสมาชิกค่าน้อยสุด เช่น $\mathbb{N}$ มีสมาชิกค่าน้อยสุดคือ 1
เพราะฉะนั้น ถ้า $S \subset \mathbb{N}$ และ $S \neq \emptyset$ แล้ว มี $x \in S$ ที่ทำให้ $x = \min(S)$

ทฤษฎีบท 1.2.2 ไม่มีจำนวนเต็มระหว่าง 0 และ 1

ข้อพิสูจน์ ให้ $T = \{a \in \mathbb{Z} \mid 0 < a < 1\}$

สมมติ $T \neq \emptyset$... (1)

โดยหลักการจัดอันดับดีจะได้ว่า T มีสมาชิกค่าน้อยสุด ให้ m เป็นสมาชิกค่าน้อยสุดของ T ... (2)

เพราะฉะนั้น $m \leq a$ ทุกค่า $a \in T$ เพราะว่า $m \in T$ เพราะฉะนั้น $0 < m < 1$

เพราะว่า $0 < m < 1$ เพราะฉะนั้น m คูณตลอดจะได้ $0 < m^2 < m$... (3)

เพราะว่า $0 < m^2 < m$ และ $0 < m < 1$ เพราะฉะนั้น $0 < m^2 < 1$ เพราะฉะนั้น $m^2 \in T$

เพราะว่า $m^2 \in T$ และจาก (3) $0 < m^2 < m$ เกิดข้อขัดแย้งกับ (2) เพราะฉะนั้นที่สมมติ (1) ไม่จริง

เพราะฉะนั้น $T = \emptyset$ เพราะฉะนั้นไม่มีจำนวนเต็มระหว่าง 0 และ 1 □

ทฤษฎีบท 1.2.3 สมบัติของอาร์คิมิดีส (Archimedean property)

ทุกจำนวนเต็มบวก a, b จะมีจำนวนเต็มบวก n ที่ทำให้ $an \geq b$

ข้อพิสูจน์ สมมติ “ทุกจำนวนเต็มบวก a, b จะมีจำนวนเต็มบวก n ที่ทำให้ $an \geq b$ ” ไม่จริง ... (1)

เพราะฉะนั้นมีจำนวนเต็มบวก a, b และมีจำนวนเต็มบวก n ที่ทำให้ $an < b$

เพราะฉะนั้น $b - an > 0$... (2)

ให้ $S = \{b - ax \mid x \in \mathbb{N} \text{ และ } b - ax > 0\}$ เพราะฉะนั้น $S \subset \mathbb{N}$

จาก (2) จะได้ $b - an \in S$ เพราะฉะนั้น $S \neq \emptyset$

เพราะว่า $S \subset \mathbb{N}$ และ $S \neq \emptyset$

โดยหลักการจัดอันดับดีจะได้ว่า S มีสมาชิกค่าน้อยสุด ให้ m เป็นสมาชิกค่าน้อยสุดของ S ... (3)

เพราะฉะนั้นมีจำนวนเต็มบวก k ที่ทำให้ $m = b - ak$... (4)

เพราะว่า $S = \{b - ax \mid x \in \mathbb{N} \text{ และ } b - ax > 0\}$ และ $k + 1 \in \mathbb{N}$

เพราะฉะนั้น $b - (k + 1)a \in \mathbb{N}$... (5)

เพราะว่า $(b - (k + 1)a) - (b - ak) = -a$ และ a เป็นจำนวนเต็มบวก

เพราะฉะนั้น $(b - (k + 1)a) - (b - ak) < 0$ เพราะฉะนั้น $b - (k + 1)a < b - ak$

เพราะว่า $m = b - ak$ เพราะฉะนั้น $b - (k + 1)a < m$... (6)

จาก (3), (5) และ (6) จะเกิดข้อขัดแย้งกับคำว่า m เป็นสมาชิกค่าน้อยสุดของ S

เพราะฉะนั้นที่สมมติ (1) ไม่จริง

เพราะฉะนั้นทุกจำนวนเต็มบวก a, b จะมีจำนวนเต็มบวก n ที่ทำให้ $an \geq b$ □

1.3 อุปนัยเชิงคณิตศาสตร์ (Principle of mathematical induction)

ให้ $P(n)$ เป็นข้อความเกี่ยวกับ n

การพิสูจน์ว่า $P(n)$ เป็นจริงโดยใช้อุปนัยเชิงคณิตศาสตร์มีหลายรูปแบบให้เลือกใช้ตามความเหมาะสม

แบบที่ 1 ถ้า (1) $P(1)$ เป็นจริง

(2) ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

แล้ว $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

แบบที่ 2 ให้ m เป็นจำนวนเต็มบวกและ $m \geq 1$

ถ้า (1) $P(m)$ เป็นจริง

(2) ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq m$ แล้ว $P(k + 1)$ เป็นจริง

แล้ว $P(n)$ เป็นจริง ทุกค่า $n = m, m + 1, m + 2, \dots$

แบบที่ 3 ถ้า (1) $P(1)$ เป็นจริง

(2) ถ้า $P(k)$ เป็นจริง เมื่อ $k < n$ แล้ว $P(n)$ เป็นจริง

แล้ว $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

แบบที่ 4 อุปนัยเชิงคณิตศาสตร์อย่างเข้ม (Principle of strong mathematical induction)

ให้ m เป็นจำนวนเต็มบวกและ $m \geq 1$

ถ้า (1) $P(m)$ เป็นจริง

(2) ถ้า $P(m), P(m + 1), \dots, P(k)$ เป็นจริง ทุกค่า $k \geq m$ แล้ว $P(k + 1)$ เป็นจริง

แล้ว $P(n)$ เป็นจริง ทุกค่า $n \geq m$

ตัวอย่าง 1.3.1 จงแสดงว่า $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ ทุกค่า $n \in \mathbb{N}$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $\frac{1}{1+1} = \frac{1}{2} = \frac{1}{1 \cdot 2}$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะฉะนั้น $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{k(k+1)} = \frac{k}{k+1}$ บวกด้วย $\frac{1}{(k+1)(k+2)}$ ทั้งสองข้างจะได้

$$\begin{aligned} \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} \left(k + \frac{k}{k+2} \right) = \frac{k}{k+1} \left(\frac{k^2 + 2k + 1}{k+2} \right) = \frac{(k+1)^2}{(k+1)(k+2)} = \frac{(k+1)}{(k+1)+1} \end{aligned}$$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 1.3.2 จงแสดงว่า $2^n < n!$ ทุกค่า $n \geq 4$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $2^n < n!$ ”

(1) การแสดงว่า $P(4)$ เป็นจริง

เพราะว่า $2^4 = 16 < 24 = 4!$ เพราะฉะนั้น $P(4)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 4$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 4$ เพราะฉะนั้น $2^k < k!$ เมื่อ $k \geq 4$

... (1)

$$2^{k+1} = 2(2^k)$$

$$< (k + 1)(2^k)$$

$$(k \geq 4)$$

$$< (k + 1)(k!) \quad (\text{จาก (1)})$$

$$= (k + 1)!$$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \geq 4$

เพราะฉะนั้น $2^n < n!$ ทุกค่า $n \geq 4$ □

ตัวอย่าง 1.3.3 ทุกจำนวนเต็มบวก n จะมีจำนวนเต็ม t และ m คู่เดียวที่ทำให้ $n = 2^t m$

เมื่อ m เป็นเลขคี่และ t เป็นจำนวนเต็มบวกหรือศูนย์

แนวคิด ให้ $P(n)$ แทนข้อความ “จำนวนเต็มบวก n จะมีจำนวนเต็ม t และ m คู่เดียวที่ทำให้ $n = 2^t m$ เมื่อ m เป็นเลขคี่และ t เป็นจำนวนเต็มบวกหรือศูนย์”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $1 = 2^0 \cdot 1$ เพราะฉะนั้นมีจำนวนเต็ม $t = 0$ และ $m = 1$ คู่เดียวที่ทำให้ $1 = 2^0 \cdot 1$

เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(1), P(2), \dots, P(n - 1)$ เป็นจริง เมื่อ $n \geq 1$ แล้ว $P(n)$ เป็นจริง

สมมติ $P(1), P(2), \dots, P(n - 1)$ เป็นจริง เมื่อ $n \geq 1$... (1)

กรณีที่ 1 n เป็นเลขคี่

เพราะฉะนั้น $n = 2^0 n$ เพราะฉะนั้นมีจำนวนเต็ม $t = 0$ และ $m = n$ คู่เดียวที่ทำให้ $n = 2^0 n$

กรณีที่ 2 n เป็นเลขคู่

เพราะฉะนั้นมีจำนวนเต็มบวก m และ $m < n$ ที่ทำให้ $n = 2m$ จาก (1) จะได้ $P(m)$ เป็นจริง

เพราะฉะนั้นมีจำนวนเต็ม r และ k คู่เดียวที่ทำให้ $m = 2^r k$... (2)

เมื่อ k เป็นเลขคี่และ r เป็นจำนวนเต็มบวกหรือศูนย์

เพราะฉะนั้น $n = 2m = 2(2^r k) = 2^{r+1} k$

สมมติ $n = 2^{s+1} g$ เมื่อ g เป็นเลขคี่และ $s + 1$ เป็นจำนวนเต็มบวกหรือศูนย์

เพราะฉะนั้น $2^{r+1} k = n = 2^{s+1} g \Rightarrow 2^{r+1} k = 2m = 2^{s+1} g$ เพราะฉะนั้น $2^r k = m = 2^s g$... (3)

จาก (2) และ (3) จะได้ $r = s$ และ $k = g$ เพราะฉะนั้น n เขียนได้แบบเดียว

เพราะฉะนั้น $P(n)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \geq 1$ □

1.4 การหารลงตัว

บทนิยาม 1.4.1 ให้ a, b เป็นจำนวนเต็มและ $b \neq 0$

b หาร a ลงตัว (b divides a) ก็ต่อเมื่อ มีจำนวนเต็ม n ที่ทำให้ $a = bn$

ตัวอย่างเช่น $4 \mid 16, 2 \mid 16, 3 \nmid 15$

ข้อตกลง 1. b หาร a ลงตัว แทนด้วย $b \mid a$ และ b หาร a ไม่ลงตัว แทนด้วย $b \nmid a$

2. ถ้า $b \mid a$ แล้ว b เรียกว่า **ตัวหาร** ของ a และ a เรียกว่า **พหุคูณ** ของ b

3. เพราะว่าทุกจำนวนเต็ม $x \neq 0$ จะได้ $x \mid 0$ เพราะฉะนั้น 0 จะมีตัวหารอยู่เป็นจำนวนอนันต์

ทฤษฎีบท 1.4.1 ให้ a, b, c เป็นจำนวนเต็ม จะได้

1. $a \mid a$ และ $1 \mid a$
2. $a \mid b$ ก็ต่อเมื่อ $\frac{b}{a}$ เป็นจำนวนเต็ม
3. $a \mid 1$ ก็ต่อเมื่อ $a = \pm 1$
4. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
5. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$
6. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
7. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = \pm b$
8. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx + cy)$ ทุกจำนวนเต็ม x และ y
 เพราะฉะนั้น ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (b + c)$
9. ถ้า $x \mid y$ และ $x \mid (y + z)$ แล้ว $x \mid z$ (เพราะฉะนั้น ถ้า $x \mid y$ และ $x \mid (y - z)$ แล้ว $x \mid z$)
10. ถ้า $x \mid y$ และ $y \neq 0$ แล้ว $\frac{y}{x} \mid y$
11. ให้ $z \neq 0$ จะได้ $(x \mid y)$ ก็ต่อเมื่อ $xz \mid yz$

ข้อพิสูจน์ 1. เพราะว่า $a = 1 \cdot a$ เพราะฉะนั้น $a \mid a$

เพราะว่า $a = 1 \cdot a$ เพราะฉะนั้น $1 \mid a$

2. $a \mid b \Leftrightarrow$ มีจำนวนเต็ม x ที่ทำให้ $b = ax$
 $\Leftrightarrow$ มีจำนวนเต็ม x ที่ทำให้ $x = \frac{b}{a}$
 $\Leftrightarrow \frac{b}{a}$ เป็นจำนวนเต็ม

เพราะฉะนั้น $a \mid b$ ก็ต่อเมื่อ $\frac{b}{a}$ เป็นจำนวนเต็ม

3. $(\Rightarrow)$ ให้ $a \mid 1$ เพราะฉะนั้นมีจำนวนเต็ม x ที่ทำให้ $1 = ax$ เพราะฉะนั้น $1 = |ax| = |a| |x|$

เพราะฉะนั้น $|a| = 1$ และ $|x| = 1$ เพราะฉะนั้น $a = 1$ หรือ $a = -1$

$(\Leftarrow)$ ให้ $a = \pm 1$ เพราะฉะนั้น $a = 1$ หรือ $a = -1$ เพราะฉะนั้น $a \mid 1$

4. สมมติ $a \mid b$ และ $b \mid c$

เพราะฉะนั้นมีจำนวนเต็ม x, y ที่ทำให้ $b = ax$ และ $c = by$ เพราะฉะนั้น $c = (ax)y = a(xy)$

เพราะว่า xy เป็นจำนวนเต็ม เพราะฉะนั้น $a \mid c$

5. สมมติ $a \mid b$ และ $c \mid d$

เพราะฉะนั้นมีจำนวนเต็ม x, y ที่ทำให้ $b = ax$ และ $c = dy$ เพราะฉะนั้น $bd = (ac)(xy)$

เพราะว่า xy เป็นจำนวนเต็ม เพราะฉะนั้น $ac \mid bd$

6. สมมติ $a \mid b$ และ $b \neq 0$

เพราะฉะนั้นมีจำนวนเต็ม c ที่ทำให้ $b = ac$

เพราะว่า $b \neq 0$ เพราะฉะนั้น $c \neq 0$ เพราะฉะนั้น $|c| \geq 1$... (1)

$$\begin{aligned} |b| &= |ac| \\ &= |a| |c| \\ &\geq |a| (1) \quad (\text{จาก (1)}) \\ &= |a| \end{aligned}$$

7. สมมติ $a|b$ และ $b|a$ เพราะฉะนั้น $a \neq 0$ และ $b \neq 0$

จากข้อ 6 จะได้ $|a| \leq |b|$ และ $|b| \leq |a|$ เพราะฉะนั้น $|a| = |b|$ เพราะฉะนั้น $a = \pm b$

8. สมมติ $a|b$ และ $a|c$ เพราะฉะนั้นมีจำนวนเต็ม m, n ที่ทำให้ $b = am$ และ $c = an$

ให้ x, y เป็นจำนวนเต็ม

เพราะฉะนั้น $bx = a(mx)$ และ $cy = a(ny)$ เพราะฉะนั้น $bx + cy = a(mx + ny)$ เพราะฉะนั้น $a|(bx + cy)$

9. สมมติ $x|y$ และ $x|(y + z)$ จากข้อ 8 จะได้ $x|((y + z) + (-1)y)$ เพราะฉะนั้น $x|z$

10. สมมติ $x|y$ และ $y \neq 0$

เพราะฉะนั้นมีจำนวนเต็ม z ที่ทำให้ $y = xz$ เพราะฉะนั้น $z|y$ และ $z = \frac{y}{x}$

เพราะว่า $z = \frac{y}{x}$ และ $z|y$ เพราะฉะนั้น $\frac{y}{x}|y$

11. ให้ $z \neq 0$

($\Rightarrow$) สมมติ $x|y$

เพราะฉะนั้นมีจำนวนเต็ม m ที่ทำให้ $y = mx$ เพราะฉะนั้น $yz = m(xz)$ เพราะฉะนั้น $xz|yz$

($\Leftarrow$) สมมติ $xz|yz$

เพราะฉะนั้นมีจำนวนเต็ม m ที่ทำให้ $yz = m(xz)$

เพราะว่า $z \neq 0$ เพราะฉะนั้น $y = mx$ เพราะฉะนั้น $x|y$ □

ทฤษฎีบท 1.4.2 ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a, b เป็นจำนวนเต็มและ $b > 0$

จะมีจำนวนเต็ม q และ r ชัดเดียวที่ทำให้ $a = qb + r$ โดยที่ $0 \leq r < b$

ข้อตกลง q เรียกว่า ผลหาร (quotient) และ r เรียกว่า เศษเหลือ (remainder)

ข้อพิสูจน์ แบบที่ 1 ให้ q เป็นส่วนจำนวนเต็มของ $\frac{a}{b}$ และ $u = \frac{a}{b} - q$

เพราะฉะนั้น $\frac{a}{b} = q + u$, q เป็นจำนวนเต็มและ u เป็นจำนวนจริงและ $0 \leq u < 1$

เพราะว่า $\frac{a}{b}$, q เป็นจำนวนตรรกยะและ $u = \frac{a}{b} - q$ เพราะฉะนั้น u เป็นจำนวนตรรกยะ

เพราะว่า $\frac{a}{b} = q + u \Rightarrow a = bq + bu$

$$\Rightarrow bu = a - bq$$

$\Rightarrow bu$ เป็นจำนวนเต็ม

ให้ $r = bu$

เพราะฉะนั้น r เป็นจำนวนเต็ม เพราะว่า $b > 0$ และ $0 \leq u < 1$ เพราะฉะนั้น $0 \leq bu < b$

เพราะว่า $r = bu$ และ $0 \leq bu < b$ เพราะฉะนั้น $0 \leq r < b$

เพราะฉะนั้นมีจำนวนเต็ม q และ r ที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$... (1)

การพิสูจน์ว่า มีจำนวนเต็ม q, r ชัดเดียวที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

ให้ q', r' เป็นจำนวนเต็มที่ทำให้ $a = bq' + r'$ โดยที่ $0 \leq r' < b$... (2)

เพราะว่า $0 \leq r' < b$ เพราะฉะนั้น $-b < -r' \leq 0$... (3)

เพราะฉะนั้น $bq + r = a = bq' + r'$ และ $-b < -r' \leq 0$... (4)

เพราะว่า $-b < -r' \leq 0$ และ $0 \leq r < b$ เพราะฉะนั้น $-b < r - r' < b$

เพราะว่า $b > 0$ และ $-b < r - r' < b$ เพราะฉะนั้น $-1 < \frac{r-r'}{b} < 1$... (5)

จาก (4) $bq + r = a = bq' + r' \Rightarrow bq' - bq = r - r'$

$$\Rightarrow q' - q = \frac{r-r'}{b} \quad (b > 0)$$

$$\Rightarrow -1 < q' - q < 1 \quad (\text{จาก (5)})$$

$$\Rightarrow q' - q = 0 \quad (q' - q \text{ เป็นจำนวนเต็ม})$$

$$\Rightarrow q' = q \quad \dots (6)$$

จาก (4) $bq + r = a = bq' + r'$ และจาก (6) $q' = q$ เพราะฉะนั้น $r = r'$

เพราะฉะนั้นมีจำนวนเต็ม q, r ชัดเดียวที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

แบบที่ 2 ให้ $S = \{a - bx \mid x \text{ เป็นจำนวนเต็มและ } a - bx \geq 0\}$ เพราะฉะนั้น $S \subset \mathbb{N} \cup \{0\}$

กรณีที่ 1 $a = 0$ เพราะฉะนั้น $0 = 0 - b \cdot 0 \geq 0$ เพราะฉะนั้น $0 \in S$

กรณีที่ 2 $a > 0$ เพราะฉะนั้น $a = a - b \cdot 0 \geq 0$ เพราะฉะนั้น $a \in S$

กรณีที่ 3 $a < 0$ เพราะฉะนั้น $|a| \geq 1$

$$a - (-|a|)b = a + |a|b$$

$$\geq a + |a| \quad (b \geq 1 \Rightarrow |a|b \geq |a|)$$

$$= a + (-a) \quad (a < 0 \Rightarrow |a| = -a)$$

$$= 0$$

ให้ $x = -|a|$ เพราะฉะนั้น $a - bx \geq 0$ เพราะฉะนั้น $a - bx \in S$

จากทั้ง 3 กรณีจะได้ $S \neq \emptyset$

เพราะว่า $S \subset \mathbb{N} \cup \{0\}$ และ $S \neq \emptyset$ เพราะฉะนั้นโดยหลักการจัดอันดับดีจะได้ S มีสมาชิกค่าน้อยสุด

ให้ r เป็นสมาชิกค่าน้อยสุดของ S ... (1)

เพราะว่า $r \in S$ เพราะฉะนั้นมีจำนวนเต็มบวก q ที่ทำให้ $r = a - bq$... (2)

เพราะว่า $r \in S$ เพราะฉะนั้น $0 \leq r$... (3)

สมมติ $r \geq b$... (4)

เพราะฉะนั้น $r - b \geq 0$

เพราะว่า $r - b = a - bq - b = a - b(q + 1)$ และ $r - b \geq 0$ เพราะฉะนั้น $r - b \in S$

เพราะว่า $r - b \in S$ และ $r - b < r$ เพราะฉะนั้นเกิดข้อขัดแย้งกับ (1)

เพราะฉะนั้นที่สมมติ (4) ไม่จริง

เพราะฉะนั้น $r < b$... (5)

จาก (3) และ (5) จะได้ $0 \leq r < b$... (6)

จาก (2) และ (6) จะได้ $a = bq + r$ โดยที่ $0 \leq r < b$... (7)

การพิสูจน์ว่า มีจำนวนเต็ม q, r ชัดเดียวที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

ให้ q', r' เป็นจำนวนเต็มที่ทำให้ $a = bq' + r'$ โดยที่ $0 \leq r' < b$... (8)

เพราะว่า $0 \leq r' < b$ เพราะฉะนั้น $-b < -r' \leq 0$... (9)

เพราะฉะนั้น $bq + r = a = bq' + r'$ และ $-b < -r' \leq 0$ และ $0 \leq r < b$... (10)

เพราะฉะนั้น $r' - r = b(q - q')$... (11)

$$\begin{aligned} |r' - r| &= |b(q - q')| \\ &= |b| |q - q'| \\ &= b |q - q'| \quad (b > 0) \end{aligned} \quad \dots (12)$$

เพราะว่า $0 \leq r' < b$ เพราะฉะนั้น $-b < -r' \leq 0$

จาก (7) $0 \leq r < b$ และจาก (9) $-b < -r' \leq 0$ จะได้ $-b < r - r' < b$ เพราะฉะนั้น $0 \leq |r' - r| < b$... (13)

จาก (12) และ (13) จะได้ $0 \leq b |q - q'| < b$

เพราะว่า $b > 0$ เพราะฉะนั้น $0 \leq |q - q'| < 1$

เพราะว่า $|q - q'|$ เป็นจำนวนเต็มและ $0 \leq |q - q'| < 1$

เพราะฉะนั้น $q - q' = 0$ เพราะฉะนั้น $q' = q$

เพราะว่า $bq + r = a = bq' + r'$ และ $q' = q$ เพราะฉะนั้น $r = r'$

เพราะฉะนั้นมีจำนวนเต็ม q, r ชัดเดียวที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$ □

ทฤษฎีบท 1.4.3 ให้ a, b เป็นจำนวนเต็มและ $b \neq 0$

จะมีจำนวนเต็ม q และ r ชัดเดียวที่ทำให้ $a = qb + r$ และ $0 \leq r < |b|$

ข้อพิสูจน์ กรณีที่ 1 $b > 0$ เพราะฉะนั้น $|b| = b$

โดยทฤษฎีบท 1.4.2 จะมีจำนวนเต็ม q และ r ชัดเดียวที่ทำให้ $a = qb + r$ และ $0 \leq r < b$

เพราะฉะนั้นมีจำนวนเต็ม q และ r ชัดเดียวที่ทำให้ $a = qb + r$ และ $0 \leq r < |b|$

กรณีที่ 2 $b < 0$ เพราะฉะนั้น $|b| = -b$ และ $|b| > 0$ เพราะฉะนั้น $b = -|b|$ และ $|b| > 0$... (1)

โดยทฤษฎีบท 1.4.2 จะมีจำนวนเต็ม q', r' ชัดเดียวที่ทำให้ $a = q'|b| + r'$ และ $0 \leq r' < |b|$... (2)

$$\text{ให้ } q = -q' \quad \dots (3)$$

$$a = q' | b | + r' \quad (\text{จาก (2)})$$

$$= (-q) | b | + r' \quad (\text{จาก (3)})$$

$$= q(-| b |) + r \quad (\text{ให้ } r = r')$$

$$= qb + r \quad (\text{จาก (1)})$$

เพราะฉะนั้นมีจำนวนเต็ม $q = -q'$ และ $r = r'$ ชัดเจนที่ทำให้ $a = qb + r$ และ $0 \leq r < | b |$ □

บทนิยาม 1.4.2 จำนวนเต็ม a เป็นจำนวนคู่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c$

จำนวนเต็ม a เป็นจำนวนคี่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c + 1$

เพราะฉะนั้น a เป็นจำนวนเต็มคู่ ก็ต่อเมื่อ $2 | a$

บทนิยาม 1.4.3 1. จำนวนเต็มบวก k ตัว $a_1, a_2, \dots, a_k$ เรียงค่ากัน

ก็ต่อเมื่อ มีจำนวนเต็ม m ที่ทำให้ $a_i = m + i, i = 1, 2, \dots, k$

2. จำนวนเต็มบวกคู่ k ตัว $a_1, a_2, \dots, a_k$ เรียงค่ากัน

ก็ต่อเมื่อ มีจำนวนเต็มบวกคู่ m ที่ทำให้ $a_i = m + 2i, i = 1, 2, \dots, k$

3. จำนวนเต็มบวกคี่ k ตัว $a_1, a_2, \dots, a_k$ เรียงค่ากัน

ก็ต่อเมื่อ มีจำนวนเต็มบวกคี่ m ที่ทำให้ $a_i = m + 2i, i = 1, 2, \dots, k$

ตัวอย่าง 1.4.1 จงแสดงว่า $2 | n(n + 1)$ ทุกจำนวนเต็ม n

แนวคิด กรณีที่ 1 n เป็นจำนวนคู่ เพราะฉะนั้น $2 | n$ เพราะฉะนั้น $2 | n(n + 1)$

กรณีที่ 2 n เป็นจำนวนคี่ เพราะฉะนั้นจะมีจำนวนเต็ม c ที่ $n = 2c + 1$ ทำให้ $n + 1 = 2c + 2 = 2(c + 1)$

เพราะฉะนั้น $2 | (n + 1)$ เพราะฉะนั้น $2 | n(n + 1)$ □

ตัวอย่าง 1.4.2 ให้ n เป็นจำนวนเต็ม m เป็นจำนวนเต็มบวก จะได้ $m | n(n + 1)(n + 2) \dots (n + m - 1)$

เพราะฉะนั้นผลคูณของจำนวนเต็มที่เรียงกัน m ตัว จะหารด้วย m ลงตัว

แนวคิด แบบที่ 1 ให้ n เป็นจำนวนเต็มและ m เป็นจำนวนเต็มบวก

โดยขั้นตอนวิธีการหารจะมีจำนวนเต็ม q และ r ที่ทำให้ $n = mq + r$ โดยที่ $0 \leq r < m$... (1)

กรณีที่ 1 $r = 0$ เพราะฉะนั้น $m | n$ เพราะฉะนั้น $m | n(n + 1)(n + 2) \dots (n + m - 1)$

กรณีที่ 2 $1 \leq r < m$ เพราะว่า $1 \leq r < m \Rightarrow 1 \leq m - r \leq m - 1$

$$\Rightarrow n + 1 \leq n + m - r \leq n + m - 1$$

$$\Rightarrow n + 1 \leq mq + r + m - r \leq n + m - 1 \quad (\text{จาก (1) } n = mq + r)$$

$$\Rightarrow n + 1 \leq mq + m \leq n + m - 1$$

$$\Rightarrow n + 1 \leq m(q + 1) \leq n + m - 1$$

เพราะฉะนั้น $m(q + 1) \in \{n + 1, n + 2, \dots, n + m - 1\}$

เพราะว่า $m | m(q + 1)$ เพราะฉะนั้นมีสมาชิก $k \in \{n + 1, n + 2, \dots, n + m - 1\}$ ที่ทำให้ $m | k$

เพราะฉะนั้น $m \mid n(n+1)(n+2) \dots (n+m-1)$

แบบที่ 2 ให้ m เป็นจำนวนเต็มบวกและ $a_n = n(n+1)(n+2) \dots (n+m-1)$

ให้ $P(n)$ แทนข้อความ “ $m \mid a_n$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $a_1 = (1)(1+1)(1+2) \dots (1+m-1) = 1 \cdot 2 \cdot 3 \dots m$ เพราะฉะนั้น $m \mid a_1$

เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} a_{k+1} - a_k &= (k+1)((k+1)+1)((k+1)+2) \dots ((k+1)+m-1) - k(k+1)(k+2) \dots (k+m-1) \\ &= (k+1)(k+2)(k+3) \dots (k+m) - k(k+1)(k+2) \dots (k+m-1) \\ &= (k+1)(k+2) \dots (k+m-1)((k+m) - k) \\ &= m(k+1)(k+2) \dots (k+m-1) \end{aligned}$$

เพราะฉะนั้น $a_{k+1} = a_k + m(k+1)(k+2) \dots (k+m-1)$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow m \mid a_k)$ และ $m \mid m(k+1)(k+2) \dots (k+m-1)$ เพราะฉะนั้น $m \mid a_{k+1}$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $m \mid n(n+1)(n+2) \dots (n+m-1)$ ทุกค่า $n \in \mathbb{N}$

แบบที่ 3 เพราะว่ $n, n+1, n+2, \dots, n+m-1$ เป็นจำนวนเต็มที่เรียงค่ากัน n ตัว

เพราะฉะนั้นมีอย่างน้อยหนึ่งตัวจาก $n, n+1, n+2, \dots, n+m-1$ ที่หารด้วย n ลงตัว

เพราะฉะนั้น $m \mid n(n+1)(n+2) \dots (n+m-1)$

□

ตัวอย่าง 1.4.3 จงแสดงว่า $7 \mid (n^7 - n)$ ทุกค่า $n \in \mathbb{N}$

แนวคิด ให้ $a_n = n^7 - n$

ให้ $P(n)$ แทนข้อความ “ $7 \mid a_n$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $a_1 = 0$ เพราะฉะนั้น $7 \mid a_1$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} a_{k+1} - a_k &= ((k+1)^7 - (k+1)) - (k^7 - k) \\ &= (k+1)^7 - k^7 - 1 \\ &= (k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1) - k^7 - 1 \\ &= 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k \\ &= 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k) \end{aligned}$$

เพราะฉะนั้น $a_{k+1} = 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k) + a_k$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow 7 \mid a_k)$ และ $7 \mid 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k)$

เพราะฉะนั้น $7 \mid a_{k+1}$ เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $7 \mid (n^7 - n)$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 1.4.4 ให้ a, b เป็นจำนวนเต็ม จงแสดงว่า $(a+b) \mid (a^{2n} - b^{2n})$ ทุกค่า $n \in \mathbb{N}$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $(a+b) \mid (a^{2n} - b^{2n})$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $a^2 - b^2 = (a+b)(a-b)$ เพราะฉะนั้น $(a+b) \mid (a^2 - b^2)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะฉะนั้น $(a+b) \mid (a^{2k} - b^{2k})$... (1)

$$\begin{aligned} a^{2(k+1)} - b^{2(k+1)} &= a^2 a^{2k} - b^2 b^{2k} \\ &= a^2 a^{2k} - a^2 b^{2k} + a^2 b^{2k} - b^2 b^{2k} && \text{(บวกเข้าและลบออก)} \\ &= a^2 (a^{2k} - b^{2k}) + b^{2k} (a^2 - b^2) \end{aligned}$$

เพราะว่า $(a+b) \mid (a^{2k} - b^{2k})$ (จาก (1)) และ $(a+b) \mid (a^2 - b^2)$

เพราะฉะนั้น $(a+b) \mid (a^{2(k+1)} - b^{2(k+1)})$ เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $(a+b) \mid (a^{2n} - b^{2n})$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 1.4.5 ให้ a, b เป็นจำนวนเต็มและ $a \neq b$ จงแสดงว่า $(a-b) \mid (a^n - b^n)$ ทุกค่า $n \in \mathbb{N}$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $(a-b) \mid (a^n - b^n)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $(a-b) \mid (a-b)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะฉะนั้น $(a-b) \mid (a^k - b^k)$... (1)

$$\begin{aligned} a^{k+1} - b^{k+1} &= a a^k - b^k b \\ &= a a^k - a b^k + a b^k - b^k b && \text{(บวกเข้าและลบออก)} \\ &= a(a^k - b^k) + b^k (a - b) \end{aligned}$$

เพราะว่า $(a-b) \mid (a^k - b^k)$ (จาก (1)) และ $(a-b) \mid (a-b)$ เพราะฉะนั้น $(a-b) \mid (a^{k+1} - b^{k+1})$

เพราะฉะนั้น $P(k+1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $(a-b) \mid (a^n - b^n)$ ทุกค่า $n \in \mathbb{N}$ □

ตัวอย่าง 1.4.6 ให้ a, b เป็นจำนวนเต็ม จงแสดงว่า $(a + b) \mid (a^{2n-1} + b^{2n-1})$ ทุกค่า $n \in \mathbb{N}$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $(a + b) \mid (a^{2n-1} + b^{2n-1})$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $a^{2(1)-1} + b^{2(1)-1} = a + b$ เพราะฉะนั้น $(a + b) \mid (a^{2(1)-1} + b^{2(1)-1})$

เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะฉะนั้น $(a + b) \mid (a^{2k-1} + b^{2k-1})$... (1)

$$a^{2(k+1)-1} + b^{2(k+1)-1} = a^{2k+1} + b^{2k+1}$$

$$= a^2 a^{2k-1} + b^2 b^{2k-1}$$

$$= a^2 a^{2k-1} + a^2 b^{2k-1} - a^2 b^{2k-1} + b^2 b^{2k-1} \quad (\text{บวกเข้าและลบออก})$$

$$= a^2 (a^{2k-1} + b^{2k-1}) - b^{2k-1} (a^2 - b^2)$$

เพราะว่า $(a + b) \mid (a^2 - b^2)$ และ $(a + b) \mid (a^{2k-1} + b^{2k-1})$ (จาก (1))

เพราะฉะนั้น $(a + b) \mid (a^{2(k+1)-1} + b^{2(k+1)-1})$ เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $(a + b) \mid (a^{2n-1} + b^{2n-1})$ ทุกค่า $n \in \mathbb{N}$ □

หมายเหตุ 1. $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1})$

$$2. a^{2n+1} + b^{2n+1} = (a + b)(a^{2n} - a^{2n-1}b + \dots - ab^{2n-1} + b^{2n})$$

$$3. a^{2n} - b^{2n} = (a + b)(a^{2n-1} - a^{2n-2}b + a^{2n-3}b^2 - \dots - b^{2n-1})$$

ตัวอย่าง 1.4.7 จงแสดงว่า $2^n \geq 2(n + 1)$ ทุกค่า $n \geq 5$

แนวคิด ให้ $P(n)$ แทนข้อความ “ $2^n \geq 2(n + 1)$ ”

(1) การแสดงว่า $P(5)$ เป็นจริง

เพราะว่า $2^5 = 32 \geq 2(5 + 1)$ เพราะฉะนั้น $P(5)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 5$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 5$ เพราะฉะนั้น $2^k \geq 2(k + 1)$... (1)

$$2^{k+1} = 2(2^k)$$

$$\geq 2(2(k + 1)) \quad (\text{จาก (1)})$$

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

$$\geq 2((k + 1) + 1)$$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \geq 5$

เพราะฉะนั้น $2^n \geq 2(n + 1)$ ทุกค่า $n \geq 5$ □

แบบฝึกหัดบทที่ 1

1. จงแสดงว่า $n^4 \leq 2^n$ ทุกค่า $n \geq 16$
2. จงแสดงว่า $3 \mid (7^n + 2)$ ทุกค่า $n \in \mathbb{N}$
3. จงแสดงว่า $4 \mid (5^n + 3)$ ทุกค่า $n \in \mathbb{N}$
4. จงแสดงว่า $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ ทุกค่า $n \in \mathbb{N}$
5. จงแสดงว่า $4 \mid n(n+1)(n+2)$ ก็ต่อเมื่อ $4 \mid n$ หรือ $4 \mid (n+1)$ หรือ $4 \mid (n+2)$
6. จงแสดงว่า $6400 \mid (9^{2n} - 80n - 1)$ ทุกค่า $n \in \mathbb{N}$
7. จงแสดงว่า $3 \mid (4^n + 2)$ ทุกค่า $n \in \mathbb{N}$
8. จงแสดงว่า $13 \mid (4^{2n+1} + 3^{n+2})$ ทุกค่า $n \in \mathbb{N}$
9. จงแสดงว่า $24 \mid (713(9^{3n-2}) + 15)$ ทุกค่า $n \in \mathbb{N}$
10. จงแสดงว่า $24 \mid (16^n + 9^{3n-2} - 1)$ ทุกค่า $n \in \mathbb{N}$
11. จงแสดงว่า $9 \mid ((2)10^n + (3)10^{n-1} + 4)$ ทุกค่า $n \in \mathbb{N}$
12. จงแสดงว่า $11 \mid ((8)10^{2n} + (6)10^{2n-1} + 9)$ ทุกค่า $n \in \mathbb{N}$
13. ให้ n เป็นจำนวนเต็มบวก จงแสดงว่า
 - 13.1 2^n เป็นผลบวกของจำนวนคู่สองจำนวนที่เรียงค่ากัน
 - 13.2 3^n เป็นผลบวกของจำนวนเต็มสามจำนวนที่เรียงค่ากัน
14. ให้ k เป็นเลขคู่
 จงแสดงว่า $\{(n_1, n_2, \dots, n_k) \mid n_1, n_2, \dots, n_k \text{ เป็นเลขคี่ และ } \frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} = 1\} = \emptyset$
15. ในกล่องมีตัวเลข 1, 2, 3, 4, 5, 6, 7 บรรจุอยู่
 เลือกจำนวน 5 จำนวน a_1, a_2, a_3, a_4, a_5 ออกมาจากกล่องพร้อมกันและให้ $a = a_1 a_2 a_3 a_4 a_5$
 จงหาค่าของ a ที่ทำให้ไม่สามารถบอกได้ว่าผลบวกของจำนวนที่เหลือในกล่องเป็นเลขคู่หรือเลขคี่
16. ให้ n เป็นจำนวนเต็มบวก จงแสดงว่า $2 \mid (3^{(2^n)} + 1)$ และ $4 \nmid (3^{(2^n)} + 1)$
17. จงหาตัวหารที่ใหญ่ที่สุดของ 1001001001 และตัวหารนั้นมีค่าน้อยกว่า 10000
18. ให้ a, b, c, d, e, f เป็นจำนวนเต็มบวกที่เขียนบนหน้าของลูกบาศก์
 ทุกๆ สามหน้าของลูกบาศก์ที่มีจุดมุมร่วมกันจะกำหนดค่าตัวเลขเป็นผลคูณของจำนวนที่ปรากฏบนสามหน้าของลูกบาศก์ที่มีจุดมุมร่วมกันนั้น
 ให้ผลบวกของจำนวนทั้งหกที่จุดมุมมีค่าเท่ากับ 2013
 จงหาค่าของ $a + b + c + d + e + f$
19. ให้ $a_1 < a_2 < a_3 < a_4 < a_5 < a_6$ เป็นลำดับเพิ่มของจำนวนเต็มบวก
 และ $a_i \mid a_{i+1}$ ทุกค่า $i = 1, 2, 3, 4, 5$ และผลบวกของจำนวนทั้ง 6 ตัวมีค่าเท่ากับ 79
 จงหาค่าของ a_6
20. จงหาจำนวนเต็มบวก n ค่ามากที่สุดที่ทำให้ $(n+10) \mid (n^3 + 100)$

21. จงหาจุดมุมของลูกบาศก์ ABCDEFGH ใน R^3 และระนาบ $M : ax + by + cz = d$ ที่ทำให้ระยะทาง A, B, C, D, E, F, G, H กับระนาบ M เป็น 0, 1, 2, 3, 4, 5, 6, 7 ตามลำดับ
22. จงแสดงว่าจำนวนเต็มบวกเขียนได้เป็น $a^2 + b^2 - c^2$ เมื่อ a, b, c เป็นจำนวนเต็มบวกและ $a < b < c$
23. จงแสดงว่า ด้วยการเปลี่ยนเครื่องหมาย + หรือ - จะทำให้ผลบวก $\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4n + 1)$ เกิดค่าของเลขคือบวกทุกค่าที่มีค่าน้อยกว่าหรือเท่ากับ $(2n + 1)(4n + 1)$
24. ให้ m เป็นจำนวนเต็มบวกและ $p(m) =$ จำนวนเต็มบวกที่ค่ามากที่สุดที่เป็นตัวหารของ m
 จงแสดงว่า $\frac{2n}{3} < \frac{p(1)}{1} + \frac{p(2)}{2} + \dots + \frac{p(n)}{n} < \frac{2(n+1)}{3}$ ทุกจำนวนเต็มบวก n
25. จงหาจำนวนเต็มบวก r ค่าน้อยสุดที่ทำให้ทุกจำนวนเต็มบวก a, b, c, d จะได้ $((abcd)!)^r$ หารด้วยผลคูณของจำนวน 14 ตัวต่อไปนี้ลงตัว
 $(a!)^{bcd+1}, (b!)^{acd+1}, (c!)^{abd+1}, (d!)^{abc+1},$
 $((ab)!)^{cd+1}, ((ac)!)^{bd+1}, ((ad)!)^{bc+1}, ((bc)!)^{ad+1}, ((bd)!)^{ac+1}, ((cd)!)^{ab+1},$
 $((abc)!)^{d+1}, ((abd)!)^{c+1}, ((acd)!)^{b+1}, ((bcd)!)^{a+1}$

เฉลยแบบฝึกหัดบทที่ 1

1. แนวคิด ให้ $P(n)$ แทนข้อความ “ $n^4 \leq 2^n$ ”

(1) การแสดงว่า $P(16)$ เป็นจริง

เพราะว่า $16^4 = 2^{16}$ เพราะฉะนั้น $P(16)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 16$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 16$

$$\begin{aligned}
 (k+1)^4 &= k^4 + 4k^3 + 6k^2 + 4k + 1 \\
 &\leq 2^k + 4k^3 + 6k^2 + 4k + 1 && (P(k) \text{ เป็นจริง} \Rightarrow k^4 \leq 2^k) \\
 &\leq 2^k + 4k^3 + 6k^3 + 4k^3 + k^3 && (k \geq 16 \Rightarrow k \leq k^3, k^2 \leq k^3) \\
 &\leq 2^k + 15k^3 \\
 &\leq 2^k + k^4 && (\text{เพราะว่า } k \geq 16) \\
 &\leq 2^k + 2^k && (P(k) \text{ เป็นจริง} \Rightarrow k^4 \leq 2^k) \\
 &\leq 2^{k+1}
 \end{aligned}$$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \geq 16$

เพราะฉะนั้น $n^4 \leq 2^n$ ทุกค่า $n \geq 16$

□

2. แนวคิด ให้ $P(n)$ แทนข้อความ “ $3 \mid (7^n + 2)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $3 \mid (7 + 2)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$7^{k+1} + 2 = 7(7^k) + 2 = 7(7^k + 2) - 7(2) + 2 = 7(7^k + 2) - 12$$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow 3 \mid (7^k + 2))$ และ $3 \mid 12$ เพราะฉะนั้น $3 \mid (7^{k+1} + 2)$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $3 \mid (7^n + 2)$ ทุกค่า $n \in \mathbb{N}$

□

3. แนวคิด ให้ $P(n)$ แทนข้อความ “ $4 \mid (5^n + 3)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $4 \mid (5 + 3)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$5^{k+1} + 3 = 5(5^k) + 3 = 5(5^k + 3) - 15 + 3 = 5(5^k + 3) - 12$$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow 4 \mid (5^k + 3))$ และ $4 \mid 12$ เพราะฉะนั้น $4 \mid (5^{k+1} + 3)$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $4 \mid (5^n + 3)$ ทุกค่า $n \in \mathbb{N}$ □

4. แนวคิด ให้ $P(n)$ แทนข้อความ “ $9 \mid (n^3 + (n + 1)^3 + (n + 2)^3)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $(1^3 + 2^3 + 3^3) = 36$ เพราะฉะนั้น $9 \mid (1^3 + 2^3 + 3^3)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\text{เพราะฉะนั้น } 9 \mid (k^3 + (k + 1)^3 + (k + 2)^3) \quad \dots (1)$$

$$(k + 1)^3 + (k + 2)^3 + (k + 3)^3 = k^3 + (k + 1)^3 + (k + 2)^3 + (k + 3)^3 - k^3 \quad \dots (2)$$

$$(k + 3)^3 - k^3 = (k + 3 - k)((k + 3)^2 + (k + 3)k + k^2)$$

$$= (3)(k^2 + 6k + 9 + k^2 + 3k + k^2)$$

$$= (3)(3k^2 + 9k + 9)$$

$$= (9)(k^2 + 3k + 3)$$

... (3)

จาก (2) และ (3) จะได้

$$(k + 1)^3 + (k + 2)^3 + (k + 3)^3 = k^3 + (k + 1)^3 + (k + 2)^3 + (9)(k^2 + 3k + 3) \quad \dots (4)$$

จาก (1) และ (4) จะได้ $9 \mid ((k + 1)^3 + (k + 2)^3 + (k + 3)^3)$ เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $9 \mid (n^3 + (n + 1)^3 + (n + 2)^3)$ ทุกค่า $n \in \mathbb{N}$ □

5. แนวคิด ($\Leftarrow$) ให้ $4 \mid n$ หรือ $4 \mid (n + 1)$ หรือ $4 \mid (n + 2)$

เพราะฉะนั้น $4 \mid n(n + 1)(n + 2)$

$$(\Rightarrow) \text{ ให้ } 4 \mid n(n + 1)(n + 2) \quad \dots (1)$$

รูปแบบของ n คือ $4k$ หรือ $4k + 1$ หรือ $4k + 2$ หรือ $4k + 3$ เมื่อ k เป็นจำนวนเต็ม

กรณีที่ 1 $n = 4k$ เพราะฉะนั้น $4 \mid n$

กรณีที่ 2 $n = 4k + 1$

$$\text{เพราะฉะนั้น } n(n + 1)(n + 2) = (4k + 1)(4k + 2)(4k + 3) = 64k^3 + 96k^2 + 44k + 6$$

เพราะฉะนั้น $4 \nmid n(n + 1)(n + 2)$ ขัดแย้งกับ (1) เพราะฉะนั้น $n = 4k + 1$ ไม่ได้

กรณีที่ 3 $n = 4k + 2$ เพราะฉะนั้น $4 \mid (n + 2)$

กรณีที่ 4 $n = 4k + 3$ เพราะฉะนั้น $4 \mid (n + 1)$

เพราะฉะนั้น $4 \mid n$ หรือ $4 \mid (n + 1)$ หรือ $4 \mid (n + 2)$ □

6. แนวคิด ให้ $P(n)$ แทนข้อความ “ $6400 \mid (9^{2n} - 80n - 1)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $9^2 - 80 - 1 = 0$ และ $6400 \mid 0$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} 9^{2(k+1)} - 80(k+1) - 1 &= (81)9^{2k} - 80k - 81 \\ &= (80)(9^{2k} - 1) + (9^{2k} - 80k - 1) \\ &= (80)(81^k - 1) + (9^{2k} - 80k - 1) \end{aligned} \quad \dots (1)$$

$$P(k) \text{ เป็นจริง} \Rightarrow 6400 \mid (9^{2k} - 80k - 1) \quad \dots (2)$$

$$\text{จากตัวอย่าง 1.4.5 จะได้ } (81 - 1) \mid (81^k - 1) \Rightarrow 80 \mid (81^k - 1) \text{ เพราะฉะนั้น } 6400 \mid (80)(81^k - 1) \dots (3)$$

จาก (1), (2) และ (3) จะได้ $6400 \mid (9^{2(k+1)} - 80(k+1) - 1)$ เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $6400 \mid (9^{2n} - 80n - 1)$ ทุกค่า $n \in \mathbb{N}$ □

7. แนวคิด ให้ $P(n)$ แทนข้อความ “ $3 \mid (4^n + 2)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $4 + 2 = 6$ และ $3 \mid 6$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$4^{k+1} + 2 = 4 \cdot 4^k + 2 = 4(4^k + 2) - 6$$

$$\text{เพราะว่า } (P(k) \text{ เป็นจริง} \Rightarrow 3 \mid (4^k + 2)) \text{ และ } 3 \mid 6$$

เพราะฉะนั้น $3 \mid (4^{k+1} + 2)$ ลงตัว เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $3 \mid (4^n + 2)$ ทุกค่า $n \in \mathbb{N}$ □

8. แนวคิด ให้ $P(n)$ แทนข้อความ “ $13 \mid (4^{2n+1} + 3^{n+2})$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

$$\text{เพราะว่า } 4^{2(1)+1} + 3^{1+2} = 64 + 27 = 91 = 13(7) \text{ เพราะฉะนั้น } P(1) \text{ เป็นจริง}$$

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} 4^{2(k+1)+1} + 3^{(k+1)+2} &= 16(4^{2k+1}) + 3(3^{k+2}) \\ &= 16(4^{2k+1} + 3^{k+2}) - 13(3^{k+2}) \end{aligned}$$

$$\text{เพราะว่า } (P(k) \text{ เป็นจริง} \Rightarrow 13 \mid (4^{2k+1} + 3^{k+2})) \text{ และ } 13 \mid 13(3^{k+2})$$

เพราะฉะนั้น $13 \mid (4^{2(k+1)+1} + 3^{(k+1)+2})$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า n

เพราะฉะนั้น $13 \mid (4^{2n+1} + 3^{n+2})$ ทุกค่า $n \in \mathbb{N}$ □

9. แนวคิด ให้ $P(n)$ แทนข้อความ “ $24 \mid (713(9^{3n-2}) + 15)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $713(9^{3(1)-2}) + 15 = 713(9) + 15 = 6432 = 268(24)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} 713(9^{3(k+1)-2}) + 15 &= 713(9^3(9^{3k-2})) + 15 \\ &= 9^3(713(9^{3k-2}) + 15) - 15(9^3 - 1) \\ &= 729(713(9^{3k-2}) + 15) - 24(455) \end{aligned}$$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow 24 \mid (713(9^{3k-2}) + 15))$ และ $24 \mid 24(455)$

เพราะฉะนั้น $24 \mid (713(9^{3(k+1)-2}) + 15)$ เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $24 \mid (713(9^{3n-2}) + 15)$ ทุกค่า $n \in \mathbb{N}$ □

10. แนวคิด ให้ $P(n)$ แทนข้อความ “ $24 \mid (16^n + 9^{3n-2} - 1)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $16 + 9 - 1 = 24$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned} 16^{k+1} + 9^{3(k+1)-2} - 1 &= 16(16^k) + 9^3(9^{3k-2}) - 1 \\ &= 16(16^k) + 729(9^{3k-2}) - 1 \\ &= 16(16^k + 9^{3k-2} - 1) - 16(9^{3k-2}) + 729(9^{3k-2}) + 16 - 1 \\ &= 16(16^k + 9^{3k-2} - 1) + 713(9^{3k-2}) + 15 \end{aligned}$$

เพราะว่า $(P(k) \text{ เป็นจริง} \Rightarrow 24 \mid (16^k + 9^{3k-2} - 1))$ และ $24 \mid (713(9^{3k-2}) + 15)$ (จากข้อ 9)

เพราะฉะนั้น $24 \mid (16^{k+1} + 9^{3(k+1)-2} - 1)$ เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $24 \mid (16^n + 9^{3n-2} - 1)$ ทุกค่า $n \in \mathbb{N}$ □

11. แนวคิด ให้ $P(n)$ แทนข้อความ “ $9 \mid ((2)10^n + (3)10^{n-1} + 4)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $(2)10^1 + (3)10^{1-1} + 4 = 20 + 3 + 4 = 27$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned}(2)10^{k+1} + (3)10^{(k+1)-1} + 4 &= 10(2)10^k + 10(3)10^{k-1} + 4 \\ &= 10((2)10^k + 10(3)10^{k-1} + 4) - 36\end{aligned}$$

เพราะว่า $(P(k) \text{ เป็นจริง } \Rightarrow 9 \mid ((2)10^k + (3)10^{k-1} + 4))$ และ $9 \mid 36$

เพราะฉะนั้น $9 \mid ((2)10^{k+1} + (3)10^{(k+1)-1} + 4)$ เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $9 \mid ((2)10^n + (3)10^{n-1} + 4)$ ทุกค่า $n \in \mathbb{N}$ □

12. แนวคิด ให้ $P(n)$ แทนข้อความ “ $11 \mid ((8)10^{2n} + (6)10^{2n-1} + 9)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

เพราะว่า $(8)10^2 + (6)10^{2-1} + 9 = 800 + 60 + 9 = 869 = 79(11)$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

$$\begin{aligned}(8)10^{2(k+1)} + (6)10^{2(k+1)-1} + 9 &= 100(8)10^{2k} + 100(6)10^{2k-1} + 9 \\ &= 100(8)10^{2k} + 100(6)10^{2k-1} + 9 \\ &= 100((8)10^{2k} + (6)10^{2k-1} + 9) - 900 + 9 \\ &= 100((8)10^{2k} + (6)10^{2k-1} + 9) - 891\end{aligned}$$

เพราะว่า $(P(k) \text{ เป็นจริง } \Rightarrow 11 \mid ((8)10^{2k} + (6)10^{2k-1} + 9))$ และ $11 \mid 891$

เพราะฉะนั้น $11 \mid ((8)10^{2(k+1)} + (6)10^{2(k+1)-1} + 9)$ เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n \in \mathbb{N}$

เพราะฉะนั้น $11 \mid ((8)10^{2n} + (6)10^{2n-1} + 9)$ ทุกค่า $n \in \mathbb{N}$ □

13. แนวคิด 13.1 เพราะว่ $2^n = 2(2^{n-1}) = 2^{n-1} + 2^{n-1} = (2^{n-1} - 1) + (2^{n-1} + 1)$

และ $2^{n-1} - 1, 2^{n-1} + 1$ เป็นจำนวนคี่

เพราะฉะนั้น 2^n เป็นผลบวกของจำนวนคี่สองจำนวนที่เรียงค่ากัน

13.2 เพราะว่ $3^n = 3 \cdot 3^{n-1} = 3^{n-1} + 3^{n-1} + 3^{n-1} = (3^{n-1} - 1) + 3^{n-1} + (3^{n-1} + 1)$

เพราะฉะนั้น 3^n เป็นผลบวกของจำนวนเต็มสามจำนวนที่เรียงค่ากัน □

14. แนวคิด กำหนดให้ k เป็นเลขคู่

... (1)

สมมติ $\{(n_1, n_2, \dots, n_k) \mid n_1, n_2, \dots, n_k \text{ เป็นเลขคี่และ } \frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} = 1\} \neq \emptyset$... (2)

เพราะฉะนั้นมี $n_1, n_2, \dots, n_k$ เป็นเลขคี่ และ $\frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} = 1$... (3)

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} = \frac{1}{n_1 n_2 \dots n_k} \left(\frac{n_1 n_2 \dots n_k}{n_1} + \frac{n_1 n_2 \dots n_k}{n_2} + \dots + \frac{n_1 n_2 \dots n_k}{n_k} \right)$$

ให้ $s_i = \frac{n_1 n_2 \dots n_k}{n_i}, i = 1, 2, \dots, k$

เพราะว่า $n_1, n_2, \dots, n_k$ เป็นเลขคู่ เพราะฉะนั้น s_i เป็นเลขคี่, $i = 1, 2, \dots, k$... (4)

$$\text{และ } 1 = \frac{1}{n_1 n_2 \dots n_k} (s_1 + s_2 + \dots + s_k)$$

เพราะฉะนั้น $n_1 n_2 \dots n_k = s_1 + s_2 + \dots + s_k$... (5)

เพราะว่าจาก (4) s_i เป็นเลขคี่ทุกค่า i และจาก (1) k เป็นเลขคู่

เพราะฉะนั้น $s_1 + s_2 + \dots + s_k$ เป็นเลขคู่ ... (6)

เพราะว่า $n_1, n_2, \dots, n_k$ เป็นเลขคี่ เพราะฉะนั้น $n_1 n_2 \dots n_k$ เป็นเลขคี่ ... (7)

จาก (5), (6) และ (7) เกิดข้อขัดแย้งกัน เพราะฉะนั้นที่สมมติ (2) ไม่จริง

เพราะฉะนั้น $\{(n_1, n_2, \dots, n_k) \mid n_1, n_2, \dots, n_k \text{ เป็นเลขคี่และ } \frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} = 1\} = \emptyset \quad \square$

15. แนวคิด ให้ $s = 1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$ เพราะฉะนั้น s เป็นเลขคู่ ... (1)

ให้ $\{x, y\} = \{1, 2, 3, 4, 5, 6, 7\} - \{a_1, a_2, a_3, a_4, a_5\}$ และ $a = a_1 a_2 a_3 a_4 a_5$... (2)

เพราะฉะนั้น $xy = \frac{7!}{a} = \frac{5040}{a}$... (3)

เพราะฉะนั้นการรู้ค่า a จึงมีผลเทียบเท่ากับการรู้ค่า xy ... (4)

เพราะว่าสองจำนวนใดๆ ใน $\{1, 2, 3, 4, 5, 6, 7\}$ คูณกันมีค่าระหว่าง 2 ถึง 42 ... (5)

เพราะว่า $\forall z \in \{2, 3, \dots, 42\} - \{6, 12\}$ จะมี $x, y \in \{1, 2, 3, 4, 5, 6, 7\}$ และ $x \neq y$

คู่เดียวที่ทำให้ $xy = z$ เพราะฉะนั้นพิจารณาเฉพาะ $xy = 12$ หรือ $xy = 6$... (6)

เพราะว่าจำนวนวิธีที่เลขสองตัวต่างกันใน $\{1, 2, 3, 4, 5, 6, 7\}$ จะมีผลคูณเท่ากับ 12

มี 2 วิธีคือ $\{2, 6\}$ และ $\{3, 4\}$... (7)

และจำนวนวิธีที่เลขสองตัวต่างกันใน $\{1, 2, 3, 4, 5, 6, 7\}$ จะมีผลคูณเท่ากับ 6

มี 2 วิธีคือ $\{1, 6\}$ และ $\{2, 3\}$... (8)

$$\text{และ } a = 840 \Rightarrow xy = \frac{5040}{840} = 6$$

$$\Rightarrow \{x, y\} = \{2, 3\} \text{ หรือ } \{x, y\} = \{1, 6\} \quad (\text{จาก (8)})$$

$$\Rightarrow x + y = 5 \text{ หรือ } 7$$

$$\Rightarrow a_1 + a_2 + a_3 + a_4 + a_5 = 23 \text{ หรือ } 21 \quad (\text{จาก (1) และ (2)})$$

$$\Rightarrow a_1 + a_2 + a_3 + a_4 + a_5 \text{ เป็นเลขคี่}$$

$$\text{และ } a = 420 \Rightarrow xy = \frac{5040}{420} = 12$$

$$\Rightarrow \{x, y\} = \{2, 6\} \text{ หรือ } \{x, y\} = \{3, 4\} \quad (\text{จาก (7)})$$

$$\Rightarrow x + y = 7 \text{ หรือ } 8$$

$$\Rightarrow a_1 + a_2 + a_3 + a_4 + a_5 = 21 \text{ หรือ } 20 \quad (\text{จาก (1) และ (2)})$$

เพราะฉะนั้น $a = 420$ จะทำให้ไม่สามารถบอกได้ว่าผลบวกของจำนวนที่เหลือเป็นเลขคู่หรือเลขคี่ $\square$

16. แนวคิด เพราะว่ $3^{(2^n)}$ เป็นเลขคี่ เพราะฉะนั้น $3^{(2^n)} + 1$ เป็นเลขคู่ เพราะฉะนั้น $2 \mid (3^{(2^n)} + 1)$

$$\text{เพราะว่ } 3^{(2^n)} = 3^{2^{(2^{n-1})}} = 9^{(2^{n-1})} = (8 + 1)^{(2^{n-1})} = \sum_{r=0}^{2^{n-1}-1} \binom{2^{n-1}-1}{r} 8^r = 1 + \sum_{r=1}^{2^{n-1}-1} \binom{2^{n-1}-1}{r} 8^r$$

$$\text{เพราะฉะนั้น } 3^{(2^n)} + 1 = 2 + \sum_{r=1}^{2^{n-1}} \binom{2^{n-1}}{r} 8^r \quad \dots (1)$$

$$\text{เพราะว่า } 4 \mid \binom{2^{n-1}}{r} 8^r \text{ ทุกค่า } r = 1, 2, \dots, 2^{n-1} \text{ เพราะฉะนั้น } 4 \mid \sum_{r=1}^{2^{n-1}} \binom{2^{n-1}}{r} 8^r$$

$$\text{เพราะฉะนั้น } 4 \nmid (2 + \sum_{r=1}^{2^{n-1}} \binom{2^{n-1}}{r} 8^r) \quad \dots (2)$$

$$\text{จาก (1) และ (2) จะได้ } 4 \nmid (3^{(2^n)} + 1)$$

หมายเหตุ การแสดงว่า $4 \nmid (3^{(2^n)} + 1)$ แบบที่ 2 โดยใช้ความรู้จากบทที่ 6

$$3^2 \equiv 1 \pmod{4}$$

$$(3^2)^{2^{n-1}} \equiv 1 \pmod{4}$$

$$(3^2)^{2^{n-1}} + 1 \equiv 2 \pmod{4}$$

$$3^{(2^n)} + 1 \equiv 2 \pmod{4} \neq 0 \pmod{4}$$

$$\text{เพราะฉะนั้น } 4 \nmid (3^{(2^n)} + 1)$$

□

$$\mathbf{17. แนวคิด} \quad 1001001001 = 1001 \times 10^6 + 1001 = 1001(10^6 + 1) = (7 \cdot 11 \cdot 13)(10^6 + 1)$$

$$\text{เพราะว่า } x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

$$\text{เพราะฉะนั้น } 10^6 + 1 = (100 + 1)(10000 - 100 + 1) = 101 \cdot 9901$$

$$\text{เพราะฉะนั้น } 1001001001 = 7 \cdot 11 \cdot 13 \cdot 101 \cdot 9901$$

$$\text{เพราะว่า } 7 \cdot 11 \cdot 13 \cdot 101 = 101101 > 10000$$

$$11 \cdot 13 \cdot 101 = 14443 > 10000$$

$$7 \cdot 13 \cdot 101 = 9191 < 9901$$

เพราะฉะนั้นไม่มีสับเซต A ของ $\{7, 11, 13, 101\}$ ที่ทำให้ผลคูณของสมาชิกใน A มีค่ามากกว่า 9901 และน้อยกว่า 10000

เพราะฉะนั้นตัวหารที่ใหญ่ที่สุดของ 1001001001 และตัวหารนั้นมีค่าน้อยกว่า 10000 คือ 9901

หมายเหตุ ตัวหารที่เป็นบวกของ 1001001001 คือ

$$1, 7, 11, 13, 77, 91, 101, 143, 707, 1001, 1111, 1313, 7777, 9191, 9901, 14443,$$

$$69307, 101101, 108911, 128713, 762377, 900991, 1000001, 1415843, 7000007,$$

$$9910901, 11000011, 13000013, 77000077, 91000091, 143000143, 1001001001$$

□

18. แนวคิด ให้ $(a, f), (b, d), (c, e)$ เป็นคู่ของจำนวนที่กำหนดให้กับหน้าของลูกบาศก์ที่ตรงข้ามกัน

$$\text{เพราะฉะนั้น } 2013 = abc + abe + acd + ade + bcf + bef + cdf + def$$

$$= (a + f)(b + d)(c + e)$$

$$\text{เพราะว่า } 2013 = (3)(11)(61) \text{ เพราะฉะนั้น } \{(a + f), (b + d), (c + e)\} = \{3, 11, 61\}$$

$$\text{เพราะฉะนั้น } (a + f) + (b + d) + (c + e) = 75 \text{ เพราะฉะนั้น } a + b + c + d + e + f = 75$$

□

19. แนวคิด $a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 79$ และ $a_1 < a_2 < a_3 < a_4 < a_5 < a_6$... (1)

เพราะว่า $a_i \mid a_{i+1}$ ทุกค่า $i = 1, 2, 3, 4, 5$ และ $a_1 < a_2 < a_3 < a_4 < a_5 < a_6$

เพราะฉะนั้น $a_6 \geq 2a_5, a_5 \geq 2a_4, a_4 \geq 2a_3, a_3 \geq 2a_2, a_2 \geq 2a_1$... (2)

เพราะฉะนั้น $a_6 \geq 2a_5 \geq 4a_4 \geq 8a_3 \geq 16a_2 \geq 32a_1$... (3)

$$a_5 \geq 2a_4 \geq 4a_3 \geq 8a_2 \geq 16a_1 \quad \dots (4)$$

$$a_4 \geq 2a_3 \geq 4a_2 \geq 8a_1 \quad \dots (5)$$

$$a_3 \geq 2a_2 \geq 4a_1 \quad \dots (6)$$

$$a_2 \geq 2a_1 \quad \dots (7)$$

เพราะว่า $79 = a_1 + a_2 + a_3 + a_4 + a_5 + a_6$ (จาก (1))

$$\geq a_1 + 2a_1 + 4a_1 + 8a_1 + 16a_1 + 32a_1 \quad \text{(จาก (2) - (7))}$$

$$= 63a_1$$

เพราะฉะนั้น $1.25 \geq a_1$

เพราะฉะนั้น $a_1 = 1$ เพราะฉะนั้นจาก (1) จะได้ $a_2 + a_3 + a_4 + a_5 + a_6 = 78$... (8)

จาก (2) และ (8) จะได้ $78 = a_2 + a_3 + a_4 + a_5 + a_6 \geq a_2 + 2a_2 + 4a_2 + 8a_2 + 16a_2 = 31a_2$

เพราะฉะนั้น $2.5 \geq a_2$ เพราะว่า $a_1 = 1$ และ $a_1 < a_2$ และ $2.5 \geq a_2$

เพราะฉะนั้น $a_2 = 2$ เพราะฉะนั้นจาก (8) จะได้ $a_3 + a_4 + a_5 + a_6 = 76$... (9)

จาก (2) และ (9) จะได้ $76 = a_3 + a_4 + a_5 + a_6 \geq a_3 + 2a_3 + 4a_3 + 8a_3 = 15a_3$

เพราะฉะนั้น $5.06 \geq a_3$

เพราะว่า $a_2 \mid a_3$ และ $5.06 \geq a_3$ เพราะฉะนั้น $2 \mid a_3$ และ $5.06 \geq a_3$

เพราะฉะนั้น $a_3 = 4$ เพราะฉะนั้นจาก (9) จะได้ $a_4 + a_5 + a_6 = 72$... (10)

จาก (2) และ (10) จะได้ $72 = a_4 + a_5 + a_6 \geq a_4 + 2a_4 + 4a_4 = 7a_4$ เพราะฉะนั้น $10.28 \geq a_4$

เพราะว่า $a_3 \mid a_4$ และ $10.28 \geq a_4$ เพราะฉะนั้น $4 \mid a_4$ และ $10.28 \geq a_4$

เพราะฉะนั้น $a_4 = 8$ เพราะฉะนั้นจาก (10) จะได้ $a_5 + a_6 = 64$... (11)

จาก (2) และ (11) จะได้ $64 = a_5 + a_6 \geq a_5 + 2a_5 = 3a_5$ เพราะฉะนั้น $21.33 \geq a_5$

เพราะว่า $a_4 \mid a_5$ และ $21.33 \geq a_5$ เพราะฉะนั้น $8 \mid a_5$ และ $21.33 \geq a_5$

เพราะฉะนั้น $a_5 = 16$ เพราะฉะนั้นจาก (11) จะได้ $a_6 = 64 - 16 = 48$ □

20. แนวคิด $(n + 10) \mid (n^3 + 100) \Rightarrow (n + 10) \mid (n^3 + 1000 - 900)$

$$\Rightarrow (n + 10) \mid ((n + 10)(n^2 - 10n + 100) - 900)$$

$$\Rightarrow (n + 10) \mid ((n + 10)(n^2 - 10n + 100) - 900)$$

$$\Rightarrow (n + 10) \mid 900$$

เพราะฉะนั้น $n = 890$ □

21. แนวคิด โดยการย่อขยายเราสามารถเริ่มต้นพิจารณาลูกบาศก์ ABCDEFGH ที่มีพิกัดดังนี้

$A(0, 0, 0)$, $B(0, 0, 1)$, $C(0, 1, 0)$, $D(0, 1, 1)$, $E(1, 0, 0)$, $F(1, 0, 1)$, $G(1, 1, 0)$, $H(1, 1, 1)$

เพราะฉะนั้น A, B, C, D, E, F, G, H สมนัยกับเลขฐานสองดังนี้

$$A(0, 0, 0) \sim (000)_2 = (0)2^2 + (0)2^1 + (0)2^0 = 0$$

$$B(0, 0, 1) \sim (001)_2 = (0)2^2 + (0)2^1 + (1)2^0 = 1$$

$$C(0, 1, 0) \sim (010)_2 = (0)2^2 + (1)2^1 + (0)2^0 = 2$$

$$D(0, 1, 1) \sim (011)_2 = (0)2^2 + (1)2^1 + (1)2^0 = 3$$

$$E(1, 0, 0) \sim (100)_2 = (1)2^2 + (0)2^1 + (0)2^0 = 4$$

$$F(1, 0, 1) \sim (101)_2 = (1)2^2 + (0)2^1 + (1)2^0 = 5$$

$$G(1, 1, 0) \sim (110)_2 = (1)2^2 + (1)2^1 + (0)2^0 = 6$$

$$H(1, 1, 1) \sim (111)_2 = (1)2^2 + (1)2^1 + (1)2^0 = 7$$

หมายเหตุ ระยะทางจาก (x_0, y_0, z_0) กับระนาบ $ax + by + cz = d$ คือ $\frac{|ax_0 + by_0 + cz_0 - d|}{\sqrt{a^2 + b^2 + c^2}}$

เพราะฉะนั้น A, B, C, D, E, F, G, H ห่างจากระนาบ $M : 2^2x + 2^1y + 2^0z = 0$

เป็นระยะทาง $\frac{0}{\sqrt{16+4+1}}, \frac{1}{\sqrt{16+4+1}}, \frac{2}{\sqrt{16+4+1}}, \dots, \frac{7}{\sqrt{16+4+1}}$ ตามลำดับ

เพราะฉะนั้น $A'(0, 0, 0)$, $B'(0, 0, \sqrt{21})$, $C'(0, \sqrt{21}, 0)$, $D'(0, \sqrt{21}, \sqrt{21})$, $E'(\sqrt{21}, 0, 0)$,

$F'(\sqrt{21}, 0, \sqrt{21})$, $G'(\sqrt{21}, \sqrt{21}, 0)$, $H'(\sqrt{21}, \sqrt{21}, \sqrt{21})$ ห่างจากระนาบ $M : 4x + 2y + z = 0$

เป็นระยะทาง $0, 1, 2, \dots, 7$ ตามลำดับ

22. แนวคิด $1 = 4^2 + 7^2 - 8^2$, $2 = 6^2 + 7^2 - 8^2$, $3 = 4^2 + 6^2 - 7^2$, $4 = 5^2 + 10^2 - 11^2$,

$5 = 4^2 + 5^2 - 6^2$, $6 = 5^2 + 9^2 - 10^2$, $7 = 6^2 + 14^2 - 15^2$, $8 = 5^2 + 8^2 - 9^2$

แบบที่ 1 ให้ k เป็นจำนวนเต็มบวก พิจารณาค่า a, b, c จากเงื่อนไข $k = a^2 + b^2 - c^2$

เพราะว่าเราต้องการ $a < b < c$ เพราะฉะนั้นเราสามารถลดตัวแปรโดยให้ $c = b + 1$... (1)

เพราะฉะนั้น $k = a^2 + b^2 - (b + 1)^2 = a^2 + b^2 - (b^2 + 2b + 1) = a^2 - (2b + 1)$

เพราะฉะนั้น $b = \frac{a^2 - (k + 1)}{2} = \frac{(a^2 - k) - 1}{2}$... (2)

เพราะว่า b เป็นจำนวนเต็ม เพราะฉะนั้น $2 \mid ((a^2 - k) - 1)$ เพราะฉะนั้น $a^2 - k$ เป็นเลขคี่

เพราะฉะนั้น a^2 เป็นเลขคู่ ก็ต่อเมื่อ k เป็นเลขคี่

เพราะฉะนั้น a เป็นเลขคู่ ก็ต่อเมื่อ k เป็นเลขคี่

เพราะฉะนั้น a และ k มีภาวะการเป็นเลขคู่หรือเลขคี่ต่างกัน ... (3)

พิจารณาเงื่อนไข $a < b \Leftrightarrow a < \frac{a^2 - (k + 1)}{2} \Leftrightarrow 2a < a^2 - (k + 1) \Leftrightarrow k + 1 < a^2 - 2a$

$$\Leftrightarrow k + 2 < a^2 - 2a + 1 \Leftrightarrow k + 2 < (a - 1)^2 \Leftrightarrow \sqrt{k + 2} < a - 1 \Leftrightarrow 1 + \sqrt{k + 2} < a$$

เพราะฉะนั้น $a < b \Leftrightarrow 1 + \sqrt{k + 2} < a$... (4)

เพราะฉะนั้นเงื่อนไขในการเลือก a, b, c ที่ทำให้ $k = a^2 + b^2 - c^2$

พิจารณาจากค่าของจำนวนเต็มบวก k ดังนี้

1. เลือก a ให้มีภาวะการเป็นเลขคู่หรือเลขคี่ต่างจาก k (จาก (3))
2. เลือก a ที่ทำให้ $1 + \sqrt{k+2} < a$ (จาก (4))
3. เลือก $b = \frac{a^2 - (k+1)}{2}$ (จาก (2))
4. เลือก $c = b + 1$ (จาก (1))

เพราะฉะนั้น a, b, c สอดคล้องเงื่อนไข $k = a^2 + b^2 - c^2$ และ $a < b < c$

แบบที่ 2 ให้ k เป็นจำนวนเต็มบวกและ $k \geq 9$

กรณีที่ 1 k เป็นเลขคู่ เพราะฉะนั้น $k \geq 10$

ให้ n เป็นจำนวนเต็มบวกที่ทำให้ $k = 2n$

เพราะว่า $(3n)^2 + (4n - 1)^2 - (5n - 1)^2 = 2n$ และ $3n < 4n - 1 < 5n - 1$ เมื่อ $n \geq 5$

เพราะฉะนั้น $a = 3n, b = 4n - 1, c = 5n - 1$ สอดคล้องเงื่อนไข $k = a^2 + b^2 - c^2$ และ $a < b < c$

กรณีที่ 2 k เป็นเลขคี่ เพราะฉะนั้น $k \geq 9$

ให้ n เป็นจำนวนเต็มบวกที่ทำให้ $k = 2n + 3$

เพราะว่า $(3n + 2)^2 + (4n)^2 - (5n + 1)^2 = 2n + 3$ และ $3n + 2 < 4n < 5n + 1$ เมื่อ $n \geq 3$

เพราะฉะนั้น $a = 3n + 2, b = 4n, c = 5n + 1$ สอดคล้องเงื่อนไข $k = a^2 + b^2 - c^2$ และ $a < b < c$ $\square$

23. แนวคิด ให้ $P(n)$ แทนข้อความ “ด้วยการเปลี่ยนเครื่องหมาย + หรือ - จะทำให้ผลบวก

$\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4n + 1)$ เกิดค่าของเลขคี่บวกทุกค่าที่มีค่าน้อยกว่าหรือเท่ากับ $(2n + 1)(4n + 1)$ ”

(1) การแสดงว่า $P(1)$ เป็นจริง

$$\begin{array}{lll} \text{เพราะว่า} & 1 - 2 + 3 + 4 - 5 = 1 & -1 + 2 + 3 + 4 - 5 = 3 & -1 + 2 + 3 - 4 + 5 = 5 \\ & -1 + 2 - 3 + 4 + 5 = 7 & -1 - 2 + 3 + 4 + 5 = 9 & 1 - 2 + 3 + 4 + 5 = 11 \\ & -1 + 2 + 3 + 4 + 5 = 13 & 1 + 2 + 3 + 4 + 5 = 15 & \end{array}$$

และ $(2(1) + 1)(4(1) + 1) = 15$ เพราะฉะนั้น $P(1)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(k)$ เป็นจริง เมื่อ $k \geq 1$ แล้ว $P(k + 1)$ เป็นจริง

สมมติ $P(k)$ เป็นจริง เมื่อ $k \geq 1$

เพราะว่า $P(k)$ เป็นจริง

เพราะฉะนั้นด้วยการเปลี่ยนเครื่องหมาย + หรือ - จะทำให้ผลบวก $\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4k + 1)$

เกิดค่าของเลขคี่บวกทุกค่าที่มีค่าน้อยกว่าหรือเท่ากับ $(2k + 1)(4k + 1)$... (1)

เพราะว่า $-(4k + 2) + (4k + 3) + (4k + 4) - (4k + 5) = 0$ และจาก (1)

เพราะฉะนั้นด้วยการเปลี่ยนเครื่องหมาย + หรือ - จะทำให้ผลบวก

$$\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4k + 1) \pm (4k + 2) \pm (4k + 3) \pm (4k + 4) \pm (4k + 5)$$

เกิดค่าของเลขคี่บวกทุกค่าที่มีค่าน้อยกว่าหรือเท่ากับ $(2k + 1)(4k + 1)$... (2)

การแสดงว่า ทุกเลขคี่ m ในช่วง $(2k + 1)(4k + 1) + 2$ ถึง $(2k + 3)(4k + 5)$

มีการเปลี่ยนเครื่องหมาย + หรือ - ที่ทำให้

$$\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4k + 1) \pm (4k + 2) \pm (4k + 3) \pm (4k + 4) \pm (4k + 5) = m$$

โดยการจัดรูปพีชคณิตจะได้

$$(2k + 3)(4k + 5) = \left(\frac{4k + 5}{2}\right)(1 + (4k + 5)) = 1 + 2 + 3 + \dots + (4k + 5)$$

$$(2k + 3)(4k + 5) - 2 = 1 + 2 + 3 + \dots + (4k + 4) + (4k + 5) - 2 = -1 + 2 + 3 + \dots + (4k + 4) + (4k + 5)$$

$$(2k + 3)(4k + 5) - 4 = 1 + 2 + 3 + \dots + (4k + 4) + (4k + 5) - 4 = 1 - 2 + 3 + \dots + (4k + 4) + (4k + 5)$$

$$(2k + 3)(4k + 5) - 6 = 1 + 2 + 3 + \dots + (4k + 4) + (4k + 5) - 6 = 1 + 2 - 3 + \dots + (4k + 4) + (4k + 5)$$

:

$$(2k + 3)(4k + 5) - 2(4k + 5) = 1 + 2 + 3 + \dots + (4k + 4) + (4k + 5) - 2(4k + 5)$$

$$= 1 + 2 - 3 + \dots + (4k + 4) - (4k + 5)$$

$$\text{เพราะว่า } 1 + 2 + 3 + \dots + (4k + 4) - (4k + 5) = 8k^2 + 14k + 3$$

$$\text{เพราะฉะนั้น } (2k + 1)(4k + 1) + 2(4k + 1) = 8k^2 + 14k + 3$$

$$(2k + 1)(4k + 1) + 2(4k) = 8k^2 + 14k + 1$$

$$= (8k^2 + 14k + 3) - 2(1)$$

$$= -1 + 2 + 3 + \dots + (4k + 4) - (4k + 5)$$

$$(2k + 1)(4k + 1) + 2(4k - 1) = 8k^2 + 14k - 1$$

$$= (8k^2 + 14k + 3) - 2(2)$$

$$= 1 - 2 + 3 + \dots + (4k + 4) - (4k + 5)$$

:

$$(2k + 1)(4k + 1) + 4 = 8k^2 + 6k + 5$$

$$= 8k^2 + 14k + 3 - 2(4k - 1)$$

$$= ((1 + 2 + 3 + \dots + (4k - 2) + (4k - 1) + (4k) + \dots + (4k + 4) - (4k + 5)) - 2(4k - 1)$$

$$= (1 + 2 + 3 + \dots + (4k - 2) - (4k - 1) + (4k) + \dots + (4k + 4) - (4k + 5))$$

$$(2k + 1)(4k + 1) + 2 = 8k^2 + 6k + 3$$

$$= 8k^2 + 14k + 3 - 2(4k)$$

$$= ((1 + 2 + 3 + \dots + (4k - 1) + (4k) + (4k + 1) + (4k + 4) - (4k + 5)) - 2(4k)$$

$$= 1 + 2 + 3 + \dots + (4k - 1) - (4k) + (4k + 1) + (4k + 4) - (4k + 5)$$

เพราะฉะนั้น $P(k + 1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n = 1, 2, 3, \dots$

เพราะฉะนั้นการเปลี่ยนเครื่องหมาย + หรือ - จะทำให้ผลบวก $\pm 1 \pm 2 \pm 3 \pm 4 \pm \dots \pm (4n + 1)$

เกิดค่าของเลขคี่บวกทุกค่าที่มีค่าน้อยกว่าหรือเท่ากับ $(2n + 1)(4n + 1)$



24. แนวคิด m เป็นจำนวนเต็มบวกและ $p(m)$ = จำนวนเต็มบวกที่ค่ามากที่สุดที่เป็นตัวหารของ m

ตัวอย่างเช่น $p(1) = 1, p(2) = 1, p(3) = 3, p(4) = 1, p(5) = 5, p(6) = 3$

เพราะฉะนั้น $\frac{p(n)}{n} \leq 1$ ทุกค่า n และ $p(n) = 1$ ทุกเลขคี่ n ... (1)

ให้ $t = p(2m)$

เพราะฉะนั้น $t \mid (2m)$ และ t เป็นเลขคี่ เพราะว่า t เป็นเลขคี่ เพราะฉะนั้น $\gcd(t, 2) = 1$

เพราะว่า $\gcd(t, 2) = 1$ และ $t \mid (2m)$ เพราะฉะนั้น $t \mid m$

เพราะฉะนั้น $p(m) \geq t$ เพราะฉะนั้น $p(m) \geq p(2m)$

ให้ $u = p(m)$

เพราะฉะนั้น $u \mid m$ และ u เป็นเลขคี่ เพราะฉะนั้น $u \mid (2m)$

เพราะว่า $p(2m)$ เป็นจำนวนเต็มบวกที่ค่ามากที่สุดที่เป็นตัวหารของ $2m$ และ $u \mid (2m)$

เพราะฉะนั้น $p(2m) \geq u$ เพราะฉะนั้น $p(2m) \geq p(m)$

เพราะฉะนั้น $p(m) = p(2m)$... (2)

ให้ $s(n) = \frac{p(1)}{1} + \frac{p(2)}{2} + \dots + \frac{p(n)}{n}$

เพราะฉะนั้น $s(1) = \frac{p(1)}{1} = \frac{1}{1} = 1, s(2) = \frac{p(1)}{1} + \frac{p(2)}{2} = \frac{1}{1} + \frac{1}{2} = \frac{3}{2}$

ให้ $P(n)$ แทนข้อความ “ $\frac{2n}{3} < s(n) < \frac{2(n+1)}{3}$ ”

(1) การแสดงว่า $P(1), P(2)$ เป็นจริง

เพราะว่า $\frac{2(1)}{3} < 1 = s(1) < \frac{4}{3} = \frac{2(1+1)}{3}$ เพราะฉะนั้น $P(1)$ เป็นจริง

เพราะว่า $\frac{2(2)}{3} = \frac{4}{3} < \frac{3}{2} = s(2) < 2 = \frac{2(2+1)}{3}$ เพราะฉะนั้น $P(2)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(1), P(2), \dots, P(k)$ เป็นจริง เมื่อ $k \geq 2$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(1), P(2), \dots, P(k)$ เป็นจริง เมื่อ $k \geq 2$... (3)

กรณีที่ 1 k เป็นเลขคู่

ให้ m เป็นจำนวนเต็มบวกที่ทำให้ $k = 2m$ เพราะฉะนั้น $1 \leq m < k$ และ $k+1 = 2m+1$... (4)

จาก (3) จะได้ $\frac{2m}{3} < s(m) < \frac{2(m+1)}{3}$... (5)

$s(k+1) = s(2m+1)$ (จาก (4))

$$\begin{aligned} &= \frac{p(1)}{1} + \frac{p(2)}{2} + \frac{p(3)}{3} + \frac{p(4)}{4} + \frac{p(5)}{5} + \frac{p(6)}{6} + \dots + \frac{p(2m)}{2m} + \frac{p(2m+1)}{2m+1} \\ &= \left(\frac{p(1)}{1} + \frac{p(3)}{3} + \frac{p(5)}{5} + \dots + \frac{p(2m+1)}{2m+1} \right) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m)}{2m} \right) \\ &\leq (1 + 1 + 1 + \dots + 1) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m)}{2m} \right) \end{aligned} \quad \text{(จาก (1))}$$

$$= (m+1) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m)}{2m} \right)$$

$$= (m+1) + \left(\frac{p(1)}{2} + \frac{p(2)}{4} + \frac{p(3)}{6} + \dots + \frac{p(m)}{2m} \right) \quad \text{(จาก (2))}$$

$$\begin{aligned}
 &= (m + 1) + \frac{1}{2} \left(\frac{p(1)}{1} + \frac{p(2)}{2} + \frac{p(3)}{3} + \dots + \frac{p(m)}{m} \right) \\
 &= (m + 1) + \frac{1}{2} s(m) \quad \dots (6)
 \end{aligned}$$

จาก (5) จะได้ $\frac{m}{3} < \frac{1}{2} s(m) < \frac{m+1}{3}$

$$\begin{aligned}
 (m + 1) + \frac{m}{3} &< (m + 1) + \frac{1}{2} s(m) < (m + 1) + \frac{m+1}{3} \\
 \frac{4m+3}{3} &< s(k+1) < \frac{4m+4}{3} \quad \text{(จาก (6))} \quad \dots (7)
 \end{aligned}$$

$$\frac{2(k+1)}{3} = \frac{2(2m+1)}{3} = \frac{4m+2}{3} < \frac{4m+3}{3} \quad \dots (8)$$

$$\frac{4m+4}{3} = \frac{2(2m+1+1)}{3} = \frac{2(k+1+1)}{3} \quad \dots (9)$$

จาก (7), (8) และ (9) จะได้ $\frac{2(k+1)}{3} < s(k+1) < \frac{2(k+2)}{3}$

กรณีที่ 2 k เป็นเลขคี่

ให้ m เป็นจำนวนเต็มบวกที่ทำให้ $k = 2m + 1$

เพราะฉะนั้น $1 \leq m < k$ และ $k + 1 = 2m + 2$... (10)

$$k = 2m + 1 \Rightarrow k + 1 = 2m + 2 \Rightarrow m + 1 = \frac{k+1}{2} \Rightarrow m + 1 = \frac{k+1}{2} < k$$

จาก (3) จะได้ $\frac{2(m+1)}{3} < s(m+1) < \frac{2(m+2)}{3}$... (11)

$$s(k+1) = s(2m+2) \quad \text{(จาก (10))}$$

$$= \frac{p(1)}{1} + \frac{p(2)}{2} + \frac{p(3)}{3} + \frac{p(4)}{4} + \frac{p(5)}{5} + \frac{p(6)}{6} + \dots + \frac{p(2m)}{2m} + \frac{p(2m+1)}{2m+1} + \frac{p(2m+2)}{2m+2}$$

$$= \left(\frac{p(1)}{1} + \frac{p(3)}{3} + \frac{p(5)}{5} + \dots + \frac{p(2m+1)}{2m+1} \right) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m+2)}{2m+2} \right)$$

$$\leq (1 + 1 + 1 + \dots + 1) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m+2)}{2m+2} \right) \quad \text{(จาก (1))}$$

$$= (m + 1) + \left(\frac{p(2)}{2} + \frac{p(4)}{4} + \frac{p(6)}{6} + \dots + \frac{p(2m+2)}{2m+2} \right)$$

$$= (m + 1) + \left(\frac{p(1)}{2} + \frac{p(2)}{4} + \frac{p(3)}{6} + \dots + \frac{p(m+1)}{m+1} \right) \quad \text{(จาก (2))}$$

$$= (m + 1) + \frac{1}{2} \left(\frac{p(1)}{1} + \frac{p(2)}{2} + \frac{p(3)}{3} + \dots + \frac{p(m+1)}{m+1} \right)$$

$$= (m + 1) + \frac{1}{2} s(m+1) \quad \dots (12)$$

จาก (11) จะได้ $\frac{2(m+1)}{3} < s(m+1) < \frac{2(m+2)}{3}$

$$\frac{m+1}{3} < \frac{1}{2} s(m+1) < \frac{m+2}{3}$$

$$(m + 1) + \frac{m+1}{3} < (m + 1) + \frac{1}{2} s(m+1) < (m + 1) + \frac{m+2}{3}$$

$$(m + 1) + \frac{m+1}{3} < s(k+1) < (m + 1) + \frac{m+2}{3} \quad \text{(จาก (12))}$$

$$\frac{4m+4}{3} < s(k+1) < \frac{4m+5}{3} \quad \dots (13)$$

$$\frac{2(k+1)}{3} = \frac{2(2m+2)}{3} = \frac{4m+4}{3} \quad \dots (14)$$

$$\frac{4m+5}{3} < \frac{4m+4}{3} = \frac{2(2m+2)}{3} = \frac{2(k+1)}{3} < \frac{2(k+2)}{3} \quad \dots (15)$$

$$\text{จาก (13), (14) และ (15) จะได้ } \frac{2(k+1)}{3} < s(k+1) < \frac{2(k+2)}{3}$$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n = 1, 2, 3, \dots$ □

25. แนวคิด ให้ p เป็นผลคูณของจำนวน 14 ตัว

$$\text{เพราะฉะนั้น } p = (a!)^{bcd+1} (b!)^{acd+1} (c!)^{abd+1} (d!)^{abc+1} ((ab)!)^{cd+1} ((ac)!)^{bd+1} ((ad)!)^{bc+1} ((bc)!)^{ad+1} \\ \times ((bd)!)^{ac+1} ((cd)!)^{ab+1} ((abc)!)^{d+1} ((abd)!)^{c+1} ((acd)!)^{b+1} ((bcd)!)^{a+1}$$

$$\text{กรณี } b = c = d = 1 \text{ จะได้ } p = (a!)^{1+1} ((a!)^{1+1})^3 ((a!)^{1+1})^3 = (a!)^{2+6+6} = (a!)^{14}$$

$$\text{เพราะว่า } p \mid ((abcd)!)^r \text{ เพราะฉะนั้น } (a!)^{14} \mid (a!)^r \text{ เพราะฉะนั้น } 14 \leq r \quad \dots (1)$$

เพราะว่า

$$1. (a!)^{bcd+1} ((bcd)!)^{a+1} = (((bcd)!)^1 (a!)^{bcd}) ((a!)^1 ((bcd)!)^a) = ((bcd)!) (a!)^{bcd} (a! ((bcd)!)^a)$$

$$2. \text{จำนวนวิธีแบ่งสิ่งของต่างกัน } abcd \text{ สิ่ง ออกเป็น } bcd \text{ กลุ่มๆ ละ } a \text{ ทำได้ } \frac{(abcd)!}{(a!)^{bcd} (bcd)!} \text{ วิธี}$$

$$\text{เพราะว่า } \frac{(abcd)!}{(a!)^{bcd} (bcd)!} \text{ เป็นจำนวนเต็ม เพราะฉะนั้น } ((bcd)!) (a!)^{bcd} \mid ((abcd)!) \quad \dots (i)$$

$$3. \text{จำนวนวิธีแบ่งสิ่งของต่างกัน } abcd \text{ สิ่ง ออกเป็น } a \text{ กลุ่มๆ ละ } bcd \text{ ทำได้ } \frac{(abcd)!}{((bcd)!)^a a!} \text{ วิธี}$$

$$\text{เพราะว่า } \frac{(abcd)!}{((bcd)!)^a a!} \text{ เป็นจำนวนเต็ม เพราะฉะนั้น } (a! ((bcd)!)^a) \mid ((abcd)!) \quad \dots (ii)$$

หมายเหตุ ดูสูตรการนับจำนวนวิธีได้จาก คณิตศาสตร์ปริยาย เล่มที่ 36 โลกคอมบินาทอริก หน้า 85

$$\text{เพราะฉะนั้น } ((a!)^{bcd+1} ((bcd)!)^{a+1}) \mid ((abcd)!)^2 \quad \dots (2)$$

$$\text{ในทำนองเดียวกัน } ((b!)^{acd+1} ((acd)!)^{b+1}) \mid ((abcd)!)^2 \quad \dots (3)$$

$$((c!)^{abd+1} ((abd)!)^{c+1}) \mid ((abcd)!)^2 \quad \dots (4)$$

$$((d!)^{abc+1} ((abc)!)^{d+1}) \mid ((abcd)!)^2 \quad \dots (5)$$

$$\text{เพราะว่า } 1. ((ab)!)^{cd+1} ((cd)!)^{ab+1} = ((ab)!) ((cd)!)^{ab} ((cd)!) ((ab)!)^{cd}$$

$$2. ((ab)!) ((cd)!)^{ab} \mid ((abcd)!) \quad (\text{ใช้เหตุผลเหมือน (i)})$$

$$3. ((cd)!) ((ab)!)^{cd} \mid ((abcd)!) \quad (\text{ใช้เหตุผลเหมือน (i)})$$

$$\text{เพราะฉะนั้น } (((ab)!)^{cd+1} ((cd)!)^{ab+1}) \mid ((abcd)!)^2 \quad \dots (6)$$

$$\text{ในทำนองเดียวกัน } (((ac)!)^{bd+1} ((bd)!)^{ac+1}) \mid ((abcd)!)^2 \quad \dots (7)$$

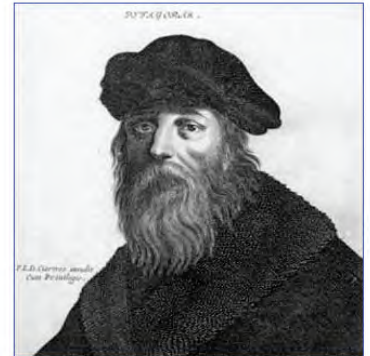
$$(((ad)!)^{bc+1} ((bc)!)^{ad+1}) \mid ((abcd)!)^2 \quad \dots (8)$$

$$\text{จาก (2), (3), ... , (8) จะได้ } p \mid ((abcd)!)^{14} \quad \dots (9)$$

$$\text{จาก (1) และ (9) จะได้ } r = 14 \quad \square$$

บทที่ 2

ตัวหารร่วมมากและตัวคูณร่วมน้อย



Pythagoras of Samos
about 569 BC - about 475 BC

2.1 ตัวหารร่วมมาก (greatest common divisor)

บทนิยาม 2.1.1 ให้ a และ b เป็นจำนวนเต็ม

d เป็น ตัวหารร่วม (common divisor) ของ a และ b ก็ต่อเมื่อ $d \mid a$ และ $d \mid b$

ตัวอย่างเช่น 2 เป็นตัวหารร่วมของ 4 และ 12

ข้อสังเกต

1. ถ้า $a = 0$ และ $b = 0$ แล้วจำนวนเต็มที่ไม่นับศูนย์ทุกตัวจะเป็นตัวหารร่วมของ a และ b
2. ถ้า $a \neq 0$ หรือ $b \neq 0$ แล้วตัวหารร่วมของ a และ b มีจำนวนจำกัด
3. เพราะว่า (d เป็นตัวหารร่วมของ a และ b ก็ต่อเมื่อ $-d$ เป็นตัวหารร่วมของ a และ b)
เพราะฉะนั้นเราสามารถพิจารณาเฉพาะตัวหารร่วมที่เป็นบวกของ a และ b ได้
4. ถ้า (d เป็นตัวหารร่วมของ a และ b) และ $d' \mid d$ แล้ว d' เป็นตัวหารร่วมของ a และ b
เพราะฉะนั้น ถ้ารู้ตัวหารร่วมค่ามากที่สุดของ a และ b แล้วจะได้ตัวหารร่วมทั้งหมดของ a และ b

บทนิยาม 2.1.2 ให้ a และ b เป็นจำนวนเต็ม $a \neq 0$ หรือ $b \neq 0$ และ d เป็นจำนวนเต็มบวก

d เป็น ตัวหารร่วมมาก (greatest common divisor) ของ a และ b

ก็ต่อเมื่อ 1. $d \mid a$ และ $d \mid b$

และ 2. $\forall c \in \mathbb{Z}^+$ ถ้า $(c \mid a \text{ และ } c \mid b)$ แล้ว $c \leq d$

เพราะฉะนั้น ถ้า c เป็นตัวหารร่วมของ a และ b แล้ว $c \leq d$

ข้อตกลง ตัวหารร่วมมากของ a และ b ใช้สัญลักษณ์แทนด้วย (a, b) หรือ $\gcd(a, b)$

ตัวอย่างเช่น $\gcd(12, 15) = 3$, $\gcd(20, 35) = 5$, $\gcd(4, 22) = 2$, $\gcd(5, 15) = 5$, $\gcd(24, 32) = 8$
 $\gcd(40, 220) = 20$, $\gcd(125, 625) = 125$, $\gcd(42, 56) = 14$

บทนิยาม 2.1.3 ให้ $a_1, a_2, \dots, a_n$ เป็นจำนวนเต็มบวก

ผลบวก $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$ เมื่อ $\alpha_1, \alpha_2, \dots, \alpha_n$ เป็นจำนวนเต็ม

เรียกว่า **ผลรวมเชิงเส้น** (linear combination) ของ $a_1, a_2, \dots, a_n$

เพราะฉะนั้นสำหรับจำนวนเต็ม a, b จะได้ $ax + by$ เป็นผลรวมเชิงเส้นของ a, b เมื่อ x, y เป็นจำนวนเต็ม

ทฤษฎีบทต่อไปจะแสดงให้เห็นว่า

$\gcd(a, b)$ เป็นจำนวนเต็มบวกค่าน้อยที่สุดที่อยู่ในรูป $ax + by$ เมื่อ x, y เป็นจำนวนเต็ม

กล่าวคือ $\gcd(a, b)$ เป็นผลรวมเชิงเส้นของ a, b ที่เป็นบวกค่าน้อยที่สุด

ทฤษฎีบท 2.1.1 ให้ a, b เป็นจำนวนเต็มและ a, b ไม่เป็นศูนย์พร้อมกัน จะได้

1. ถ้า $d = \gcd(a, b)$ แล้วมีจำนวนเต็ม x, y ที่ทำให้ $d = ax + by$

2. $d = \gcd(a, b) = \min \{ am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0 \}$

ข้อพิสูจน์ โดยไม่สูญเสียสาระสำคัญของกรณีทั่วไปเราสามารถสมมติให้ $a \geq b$

ให้ $S = \{ am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0 \}$ เพราะฉะนั้น $S \subset \mathbb{N}$

กรณีที่ 1 $a > 0$ เพราะฉะนั้น $a \cdot 1 + b \cdot 0 = a > 0$ เพราะฉะนั้น $a \cdot 1 + b \cdot 0 \in S$

กรณีที่ 2 $a = 0$

เพราะว่า a, b ไม่เป็นศูนย์พร้อมกัน เพราะฉะนั้น $b \neq 0$

กรณีที่ 2.1 $b > 0$ เพราะฉะนั้น $a \cdot 0 + b \cdot 1 = b > 0$ เพราะฉะนั้น $a \cdot 0 + b \cdot 1 \in S$

กรณีที่ 2.2 $b < 0$ เพราะฉะนั้น $a \cdot 0 + b \cdot (-1) = -b > 0$ เพราะฉะนั้น $a \cdot 0 + b \cdot (-1) \in S$

กรณีที่ 3 $a < 0$ เพราะฉะนั้น $a \cdot (-1) + b \cdot 0 = -a > 0$ เพราะฉะนั้น $a \cdot (-1) + b \cdot 0 \in S$

จากทั้ง 3 กรณีจะได้ $S \neq \emptyset$

เพราะว่า $S \subset \mathbb{N}$ และ $S \neq \emptyset$ เพราะฉะนั้นโดยหลักการจัดอันดับดีจะได้ S จะมีสมาชิกค่าน้อยสุด

ให้ $d \in S$ และ d เป็นสมาชิกค่าน้อยสุดของ S

... (1)

เพราะว่า $d \in S$ เพราะฉะนั้นมี $x, y \in \mathbb{Z}$ ที่ทำให้ $d = ax + by$ และ $d > 0$

... (2)

การแสดงว่า $d = \gcd(a, b)$

การแสดงว่า $d \mid a$

โดยขั้นตอนวิธีการหารให้ q, r เป็นจำนวนเต็มที่ทำให้ $a = dq + r$ และ $0 \leq r < d$

... (3)

สมมติ $r > 0$

... (4)

จาก (2) และ (3) จะได้ $a = (ax + by)q + r$

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

$= a(1 - xq) + b(-yq)$

... (5)

จาก (4) และ (5) จะได้ $a(1 - xq) + b(-yq) = r > 0$

เพราะฉะนั้น $r = a(1 - xq) + b(-yq) \in S$

... (6)

จาก (3) และ (6) จะได้ $r < d$ และ $r \in S$

เพราะฉะนั้นเกิดข้อขัดแย้งกับ (1) ซึ่งกล่าวว่า d เป็นสมาชิกค่าน้อยสุดของ S

เพราะฉะนั้นที่สมมติ (4) $r > 0$ ไม่จริง

เพราะฉะนั้น $r \leq 0$

... (6)

จาก (3) $0 \leq r < d$ และ (6) $r \leq 0$ เพราะฉะนั้น $r = 0$

เพราะว่า $r = 0$ จาก (3) จะได้ $a = dq$ เพราะฉะนั้น $d \mid a$

ในทำนองเดียวกัน $d \mid b$

การแสดงว่า ทุกค่าของจำนวนเต็มบวก c ถ้า $(c \mid a$ และ $c \mid b)$ แล้ว $c \leq d$

ให้ c เป็นจำนวนเต็มบวกและ $c \mid a$ และ $c \mid b$

เพราะฉะนั้น $c \mid ax$ และ $c \mid by$ เพราะฉะนั้น $c \mid (ax + by)$

จาก (2) $d = ax + by$ เพราะฉะนั้น $c \mid d$ โดยผลของทฤษฎีบท 1.4.1 จะได้ $|c| \leq |d|$

เพราะว่า c, d เป็นจำนวนเต็มบวก เพราะฉะนั้น $c \leq d$

เพราะว่า 1. $d \mid a$ และ $d \mid b$

และ 2. ทุกค่า c ที่เป็นจำนวนเต็มบวก ถ้า $(c \mid a$ และ $c \mid b)$ แล้ว $c \leq d$

เพราะฉะนั้น $d = \gcd(a, b)$

เพราะฉะนั้นจาก (2) จึงสรุปได้ว่ามี x, y เป็นจำนวนเต็มที่ทำให้ $d = ax + by$

2. จาก (1) จะได้ $d = \gcd(a, b) = \min \{ am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0 \}$

□

หมายเหตุ ถ้ามีจำนวนเต็ม x, y ที่ทำให้ $d = ax + by$ เป็นจำนวนเต็มบวก แล้ว $d = \gcd(a, b)$ ไม่จริง

ตัวอย่างเช่น $a = 4, b = 6$ และ $d = 10 = (4)(1) + (6)(1)$ แต่ $(4, 6) = 2 \neq 10$

ทฤษฎีบท 2.1.2 ให้ a, b เป็นจำนวนเต็มและ a, b ไม่เป็นศูนย์พร้อมกัน ให้ $d = \gcd(a, b)$

จะได้ $\{ am + bn \mid m, n \in \mathbb{Z} \} = \{ x \in \mathbb{Z} \mid d \mid x \}$

ข้อพิสูจน์ ให้ $S = \{ am + bn \mid m, n \in \mathbb{Z} \}$ และ $T = \{ x \in \mathbb{Z} \mid d \mid x \}$

ให้ $s \in S$

เพราะฉะนั้นมี $m, n \in \mathbb{Z}$ ที่ทำให้ $s = am + bn$

เพราะว่า $d = \gcd(a, b)$ เพราะฉะนั้น $d \mid a$ และ $d \mid b$ เพราะฉะนั้น $d \mid (am + bn)$ เพราะฉะนั้น $d \mid s$

เพราะว่า $d \mid s$ เพราะฉะนั้น $s \in T$

เพราะฉะนั้น $S \subset T$

... (1)

ให้ $t \in T$

เพราะฉะนั้น $d \mid t$

เพราะฉะนั้นมีจำนวนเต็ม n ที่ทำให้ $t = nd$

เพราะว่า $d = \gcd(a, b)$

เพราะฉะนั้นโดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x_0, y_0 ที่ทำให้ $d = ax_0 + by_0$

เพราะฉะนั้น $t = nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0)$ และ $nx_0, ny_0 \in \mathbb{Z}$

เพราะฉะนั้น $t \in S$

เพราะฉะนั้น $T \subset S$

... (2)

จาก (1) และ (2) จะได้ $T = S$

□

บทนิยาม 2.1.4 ให้ p เป็นจำนวนเต็มบวกและ $p > 1$

p เป็น จำนวนเฉพาะ (prime number) ก็ต่อเมื่อ p มีตัวหารที่เป็นบวก 2 ตัวคือ 1 และ p

ถ้า p ไม่เป็นจำนวนเฉพาะ แล้ว p เป็น จำนวนประกอบ (composite number)

เพราะฉะนั้น ถ้า n เป็นจำนวนประกอบ แล้ว มีจำนวนเต็ม a, b ที่ทำให้ $n = ab$ โดยที่ $1 < a, b < n$

หมายเหตุ จำนวนเต็มบวก $p > 1$ เป็นจำนวนเฉพาะ ก็ต่อเมื่อ p มีตัวหาร 4 ตัวคือ 1, -1 , p , $-p$

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

บทนิยาม 2.1.5 a และ b เป็น จำนวนเฉพาะสัมพัทธ์ (relatively prime) ก็ต่อเมื่อ $\gcd(a, b) = 1$

ตัวอย่าง เพราะว่า $\gcd(14, 25) = 1$ เพราะฉะนั้น 14 และ 25 เป็นจำนวนเฉพาะสัมพัทธ์

เพราะว่า $\gcd(20, 33) = 1$ เพราะฉะนั้น 20 และ 33 เป็นจำนวนเฉพาะสัมพัทธ์

เพราะว่า $\gcd(12, 15) = 3$ เพราะฉะนั้น 12 และ 15 ไม่เป็นจำนวนเฉพาะสัมพัทธ์

ทฤษฎีบท 2.1.3 ให้ a, b เป็นจำนวนเต็มและ a, b ไม่เป็นศูนย์พร้อมกัน จะได้

$\gcd(a, b) = 1$ ก็ต่อเมื่อ มีจำนวนเต็ม x, y ที่ทำให้ $ax + by = 1$

ข้อพิสูจน์ ($\Rightarrow$) ให้ $\gcd(a, b) = 1$ โดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x, y ที่ทำให้ $ax + by = 1$

($\Leftarrow$) มีจำนวนเต็ม x, y ที่ทำให้ $ax + by = 1$

... (1)

ให้ $d = \gcd(a, b)$

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

จาก (1) มีจำนวนเต็ม x, y ที่ทำให้ $ax + by = 1$ เพราะฉะนั้น $1 \in S$

... (2)

โดยทฤษฎีบท 2.1.1 จะได้ $d = \min\{am + bn \mid m, n \in \mathbb{Z} \text{ และ } am + bn > 0\}$ และ $d > 0$

... (3)

จาก (2) และ (3) จะได้ $d \leq 1$ และ $d > 0$ เพราะฉะนั้น $d = 1$

เพราะฉะนั้น $\gcd(a, b) = 1$

□

ทฤษฎีบท 2.1.4 ให้ a, b เป็นจำนวนเต็มและ a, b ไม่เป็นศูนย์พร้อมกัน

จะได้ $\gcd(a, b) \mid (ax + by)$ ทุกค่า x, y ที่เป็นจำนวนเต็ม

ข้อพิสูจน์ ให้ x, y เป็นจำนวนเต็ม

เพราะว่า $\gcd(a, b) \mid a$ และ $\gcd(a, b) \mid b$ เพราะฉะนั้น $\gcd(a, b) \mid ax$ และ $\gcd(a, b) \mid by$

เพราะฉะนั้น $\gcd(a, b) \mid ax + by$ (โดยทฤษฎีบท 1.4.1)

□

ทฤษฎีบท 2.1.5 ให้ a และ b เป็นจำนวนเต็ม $a \neq 0$ และ $b \neq 0$ จะได้

1. $\gcd(a, b) = \gcd(b, a)$ และ $\gcd(a, 0) = |a|$ และ $\gcd(a, 1) = 1$

2. $\gcd(a, b) \leq \gcd(a, bc)$ ทุกจำนวนเต็มบวก c

3. ถ้า p เป็นจำนวนเฉพาะและ $p \nmid a$ แล้ว $\gcd(a, p) = 1$
4. ถ้า $a \mid bc$ และ $\gcd(a, b) = 1$ แล้ว $a \mid c$
5. $(\gcd(a, b) = 1 \text{ และ } \gcd(a, c) = 1)$ ก็ต่อเมื่อ $\gcd(a, bc) = 1$
6. $(\gcd(a, b_1) = \gcd(a, b_2) = \dots = \gcd(a, b_n) = 1)$ ก็ต่อเมื่อ $\gcd(a, b_1 b_2 \dots b_n) = 1$
7. ถ้า $a \mid c$ และ $b \mid c$ และ $\gcd(a, b) = 1$ แล้ว $ab \mid c$
8. ถ้า $d = \gcd(a, b)$ แล้ว $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

เพราะฉะนั้น ถ้า $d = \gcd(a, b)$ แล้ว $\frac{a}{d}$ และ $\frac{b}{d}$ เป็นจำนวนเต็มที่เป็นจำนวนเฉพาะสัมพัทธ์

9. ให้ a เป็นจำนวนเต็มบวก จะได้ $\gcd(a, b) = a$ ก็ต่อเมื่อ $a \mid b$
10. ถ้า $\gcd(a, b) = 1$ และ $c \mid (a + b)$ แล้ว $\gcd(c, a) = 1 = \gcd(c, b)$
11. ถ้า $\gcd(a, c) = 1$ และ $b \mid c$ แล้ว $\gcd(a, b) = 1$
12. ถ้ามีจำนวนเต็ม x, y ที่ทำให้ $ax + by = \gcd(a, b)$ แล้ว $\gcd(x, y) = 1$
13. $\gcd(a, a + n) \mid n$ ทุกจำนวนเต็ม n
14. ให้ p เป็นจำนวนเฉพาะและ k เป็นจำนวนเต็มและ $1 \leq k < p$ จะได้ $p \mid \binom{p}{k}$
15. $\gcd(a, b) = \gcd(-a, -b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(|a|, |b|)$
16. ให้ m, n เป็นจำนวนเต็มบวก ถ้า $\gcd(a^m, b^n) = 1$ แล้ว $\gcd(a, b) = 1$

ข้อพิสูจน์ 1. โดยบทนิยามจะได้ $\gcd(a, b) = \gcd(b, a)$

$$x = \gcd(a, 0) \Rightarrow x \mid a \Rightarrow x \mid |a| \Rightarrow x \leq |a| \Rightarrow \gcd(a, 0) \leq |a| \quad \dots (1)$$

$$\text{เพราะว่า } |a| \mid a \text{ และ } |a| \mid 0 \text{ เพราะฉะนั้น } |a| \leq \gcd(a, 0) \quad \dots (2)$$

$$\text{จาก (1) และ (2) จะได้ } \gcd(a, 0) = |a|$$

$$\text{โดยบทนิยามของตัวหารร่วมมากจะได้ } \gcd(a, 1) \geq 1 \quad \dots (3)$$

$$\text{เพราะว่า } \gcd(a, 1) \mid 1 \text{ เพราะฉะนั้น } \gcd(a, 1) \leq 1 \quad \dots (4)$$

$$\text{จาก (3) และ (4) จะได้ } \gcd(a, 1) = 1$$

$$2. \ d = \gcd(a, b) \Rightarrow d \mid a \text{ และ } d \mid b \Rightarrow d \mid a \text{ และ } d \mid bc$$

$$\Rightarrow d \text{ เป็นตัวหารร่วมของ } a \text{ และ } bc$$

$$\Rightarrow d \leq \gcd(a, bc)$$

$$\text{เพราะฉะนั้น } \gcd(a, b) \leq \gcd(a, bc)$$

$$3. \text{ ให้ } p \text{ เป็นจำนวนเฉพาะและ } p \nmid a \text{ ให้ } d = \gcd(a, p) \quad \dots (1)$$

$$\text{สมมติ } d > 1 \quad \dots (2)$$

$$\text{เพราะฉะนั้น } d \mid p \text{ และ } d \mid a$$

$$\text{เพราะว่า } p \text{ เป็นจำนวนเฉพาะและ } d \mid p \text{ เพราะฉะนั้น } d = p$$

$$\text{เพราะว่า } d \mid a \text{ และ } d = p \text{ เพราะฉะนั้น } p \mid a \text{ เกิดข้อขัดแย้งกับ } p \nmid a \text{ (จาก (1))}$$

เพราะฉะนั้นที่สมมติ (2) $d > 1$ ไม่จริง

เพราะฉะนั้น $d = 1$ เพราะฉะนั้น $\gcd(a, p) = 1$

4. ให้ $a \mid bc$ และ $\gcd(a, b) = 1$... (1)

กรณีที่ 1 $c = 0$ เพราะฉะนั้น ถ้า $a \mid bc$ และ $\gcd(a, b) = 1$ แล้ว $a \mid c$ เป็นจริง

กรณีที่ 2 $c \neq 0$ เพราะว่าจาก (1) $\gcd(a, b) = 1$ เพราะฉะนั้นมีจำนวนเต็ม x, y ที่ทำให้ $ax + by = 1$

เพราะฉะนั้น $acx + bcy = c$... (2)

จาก (1) จะได้ $a \mid bcy$ เพราะว่า $a \mid acx$ และ $a \mid bcy$ เพราะฉะนั้น $a \mid (acx + bcy)$... (3)

เพราะฉะนั้นจาก (2) และ (3) จะได้ $a \mid c$

5. ($\Rightarrow$) ให้ $\gcd(a, b) = 1$ และ $\gcd(a, c) = 1$... (1)

แบบที่ 1 โดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x_0, y_0 ที่ทำให้ $ax_0 + by_0 = 1$

โดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x_1, y_1 ที่ทำให้ $ax_1 + cy_1 = 1$

เพราะฉะนั้น $1 = (ax_0 + by_0)(ax_1 + cy_1)$

$$= a(ax_0x_1 + x_0cy_1 + by_0x_1) + bc(y_0y_1)$$

เพราะฉะนั้น $\gcd(a, bc) = 1$ (ทฤษฎีบท 2.1.3)

แบบที่ 2 ให้ $d = \gcd(a, bc)$

สมมติ $d = \gcd(a, bc) > 1$... (2)

เพราะฉะนั้นมี p เป็นจำนวนเฉพาะและ $p \mid d$... (3)

เพราะว่า $d = \gcd(a, bc)$ เพราะฉะนั้น $d \mid a$ และ $d \mid bc$... (4)

จาก (3) และ (4) จะได้ $p \mid a$ และ $p \mid bc$ (ทฤษฎีบท 1.4.1) ... (5)

กรณีที่ 1 $p \mid b$ เพราะฉะนั้น $p \mid b$ หรือ $p \mid c$

กรณีที่ 2 $p \nmid b$ เพราะฉะนั้นผลจากข้อ 3 จะได้ $\gcd(b, p) = 1$

เพราะว่า $p \mid bc$ และ $\gcd(b, p) = 1$ และผลจากข้อ 4 เพราะฉะนั้น $p \mid c$

จากทั้งสองกรณีจะได้ $p \mid b$ หรือ $p \mid c$ เป็นจริง ... (6)

(5) และ (6) $\Rightarrow p \mid a$ และ ($p \mid b$ หรือ $p \mid c$)

$$\Rightarrow (p \mid a \text{ และ } p \mid b) \text{ หรือ } (p \mid a \text{ และ } p \mid c)$$

$$\Rightarrow (p \mid \gcd(a, b)) \text{ หรือ } (p \mid \gcd(a, c))$$

$$\Rightarrow (p \mid \gcd(a, b)) \text{ หรือ } (p \mid \gcd(a, c))$$

$$\Rightarrow (p \mid 1) \text{ หรือ } (p \mid 1) \quad (\text{จาก (1)})$$

เพราะฉะนั้น $p = 1$ เกิดข้อขัดแย้งกับ (3) p เป็นจำนวนเฉพาะ เพราะฉะนั้นที่สมมติ (2) $d > 1$ ไม่จริง

เพราะฉะนั้น $d = 1$ เพราะฉะนั้น $\gcd(a, bc) = 1$

($\Leftarrow$) ให้ $\gcd(a, bc) = 1$

จากข้อ 2 จะได้ $\gcd(a, b) \leq \gcd(a, bc)$ เพราะฉะนั้น $1 \leq \gcd(a, b) \leq 1$ เพราะฉะนั้น $\gcd(a, b) = 1$

ในทำนองเดียวกัน $\gcd(a, c) = 1$

6. ($\Rightarrow$) ให้ $P(n)$ แทนข้อความ

“ ถ้า $\gcd(a, b_1) = \gcd(a, b_2) = \dots = \gcd(a, b_n) = 1$ แล้ว $\gcd(a, b_1 b_2 \dots b_n) = 1$ ”

(1) การแสดงว่า $P(2)$ เป็นจริง

เพราะว่า ถ้า $\gcd(a, b) = \gcd(a, c) = 1$ แล้ว $\gcd(a, bc) = 1$ (จากข้อ 5) เพราะฉะนั้น $P(2)$ เป็นจริง

(2) การแสดงว่า ถ้า $P(2), P(3), \dots, P(k)$ เป็นจริง เมื่อ $k \geq 2$ แล้ว $P(k+1)$ เป็นจริง

สมมติ $P(2), P(3), \dots, P(k)$ เป็นจริง เมื่อ $k \geq 2$

ให้ $\gcd(a, b_1) = \gcd(a, b_2) = \dots = \gcd(a, b_k) = \gcd(a, b_{k+1}) = 1$

เพราะว่า $P(k)$ เป็นจริง เพราะฉะนั้น $\gcd(a, b_1 b_2 \dots b_k) = 1$

เพราะว่า $\gcd(a, b_1 b_2 \dots b_k) = 1$ และ $\gcd(a, b_{k+1}) = 1$

เพราะว่า $P(2)$ เป็นจริง เพราะฉะนั้น $\gcd(a, b_1 b_2 \dots b_k b_{k+1}) = 1$

เพราะฉะนั้น $P(k+1)$ เป็นจริง

โดยอุปนัยเชิงคณิตศาสตร์ จะได้ $P(n)$ เป็นจริง ทุกค่า $n = 2, 3, 4, \dots$

($\Leftarrow$) ให้ $\gcd(a, b_1 b_2 \dots b_n) = 1$

ให้ $i \in \{1, 2, \dots, n\}$

จากข้อ 2 จะได้ $\gcd(a, b_i) \leq \gcd(a, b_1 b_2 \dots b_n)$ เพราะฉะนั้น $1 \leq \gcd(a, b_i) \leq 1$

เพราะฉะนั้น $\gcd(a, b_i) = 1$

เพราะฉะนั้น $\gcd(a, b_i) = 1$ ทุกค่า $i = 1, 2, \dots, n$

7. ให้ $a \mid c$ และ $b \mid c$ และ $\gcd(a, b) = 1$

เพราะว่า $a \mid c$ และ $b \mid c$ เพราะฉะนั้นมีจำนวนเต็ม d และ e ที่ $c = ad$ และ $c = be$... (1)

เพราะว่า $\gcd(a, b) = 1$ เพราะฉะนั้นมีจำนวนเต็ม x, y ที่ $ax + by = 1$ (ทฤษฎีบท 2.1.3) ... (2)

เพราะฉะนั้น $c = cax + cby$ (จาก (2))

$= (be)ax + (ad)by$ (จาก (1))

$= ab(ex + dy)$

เพราะฉะนั้น $ab \mid c$

8. ให้ $d = \gcd(a, b)$... (1)

เพราะฉะนั้น $d \mid a$ และ $d \mid b$ เพราะฉะนั้น $\frac{a}{d}$ และ $\frac{b}{d}$ เป็นจำนวนเต็ม

โดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x, y ที่ทำให้ $d = ax + yb$... (2)

จาก (2) $d = ax + yb \Rightarrow 1 = (\frac{a}{d})x + (\frac{b}{d})y$

$\Rightarrow \gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (ทฤษฎีบท 2.1.3)

9. ให้ a เป็นจำนวนเต็มบวก

$(\Rightarrow)$ ให้ $\gcd(a, b) = a$ เพราะว่า $\gcd(a, b) \mid b$ เพราะฉะนั้น $a \mid b$

$(\Leftarrow)$ ให้ $a \mid b$

ให้ c เป็นจำนวนเต็มบวกและ $c \mid a$ และ $c \mid b$

เพราะว่า a, c เป็นจำนวนเต็มบวกและ $c \mid a$ เพราะฉะนั้น $c \leq a$

เพราะว่า 1. $a \mid a$ และ $a \mid b$

และ 2. ทุกค่า c ที่เป็นจำนวนเต็มบวก ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq a$

เพราะฉะนั้น $a = \gcd(a, b)$

10. ให้ $\gcd(a, b) = 1$ และ $c \mid (a + b)$... (1)

ให้ $d = \gcd(c, a)$... (2)

เพราะฉะนั้น $d \mid c$ และ $d \mid a$... (3)

เพราะว่า $c \mid (a + b)$ เพราะฉะนั้นมีจำนวนเต็ม t ที่ทำให้ $a + b = ct$... (4)

เพราะฉะนั้น $b = a - ct$... (5)

จาก (3) $d \mid c$ และ $d \mid a$ เพราะฉะนั้น $d \mid (a - ct)$ เพราะฉะนั้น $d \mid b$ (จาก (5))

เพราะฉะนั้น $d \mid a$ และ $d \mid b$ เพราะฉะนั้น $d \leq \gcd(a, b)$

จาก (1) $\gcd(a, b) = 1$ และ $d \leq \gcd(a, b)$ เพราะฉะนั้น $d \leq 1$

เพราะว่า $d = \gcd(c, a) \geq 1$ เพราะฉะนั้น $d = 1$ เพราะฉะนั้น $\gcd(c, a) = 1$

ในทำนองเดียวกันจะได้ $\gcd(c, b) = 1$

11. ให้ $\gcd(a, c) = 1$ และ $b \mid c$... (1)

ให้ $d = \gcd(a, b)$... (2)

เพราะฉะนั้น $d \mid a$ และ $d \mid b$... (3)

เพราะว่า $d \mid b$ (จาก (3)) และ $b \mid c$ (จาก (1)) เพราะฉะนั้น $d \mid c$... (4)

เพราะว่า $d \mid a$ (จาก (3)) และ $d \mid c$ (จาก (4)) เพราะฉะนั้น $d \leq \gcd(a, c)$ (บทนิยาม 2.1.2)

เพราะว่า $\gcd(a, c) = 1$ (จาก (1)) เพราะฉะนั้น $d \leq 1$

เพราะว่า $d = \gcd(a, b) \geq 1$ เพราะฉะนั้น $d = 1$ เพราะฉะนั้น $\gcd(a, b) = 1$

12. ให้ x, y เป็นจำนวนเต็มที่ทำให้ $ax + by = \gcd(a, b)$

เพราะว่า $\gcd(a, b) \mid a$ และ $\gcd(a, b) \mid b$ เพราะฉะนั้น $\frac{a}{\gcd(a, b)}$ และ $\frac{b}{\gcd(a, b)}$ เป็นจำนวนเต็ม

เพราะว่า $ax + by = \gcd(a, b)$ เพราะฉะนั้น $\frac{a}{\gcd(a, b)}x + \frac{b}{\gcd(a, b)}y = 1$

โดยทฤษฎีบท 2.1.3 จะได้ $\gcd(x, y) = 1$

13. ให้ n เป็นจำนวนเต็มบวก ให้ $d = \gcd(a, a + n)$

$d = \gcd(a, a + n) \Rightarrow d \mid (a + n)$ และ $d \mid a \Rightarrow d \mid ((a + n) - (a)) \Rightarrow d \mid n \Rightarrow \gcd(a, a + n) \mid n$

14. ให้ p เป็นจำนวนเฉพาะและ k เป็นจำนวนเต็มและ $1 \leq k < p$

เพราะว่า p เป็นจำนวนเฉพาะ เพราะฉะนั้น $\gcd(p, k) = 1$

เพราะว่า $k \binom{p}{k} = k \frac{p!}{k!(p-k)!} = p \frac{(p-1)!}{(k-1)!(p-k)!} = p \binom{p-1}{k-1}$ เพราะฉะนั้น $p \mid k \binom{p}{k}$

เพราะว่า $\gcd(p, k) = 1$ และ $p \mid k \binom{p}{k}$ เพราะฉะนั้น $p \mid \binom{p}{k}$

15. ให้ $d = \gcd(a, b)$ และ $d' = \gcd(-a, -b)$

เพราะว่า $d = \gcd(a, b)$ เพราะฉะนั้น $d \mid a$ และ $d \mid b$

เพราะฉะนั้น $d \mid (-a)$ และ $d \mid (-b)$ เพราะฉะนั้น $d \leq d'$... (1)

เพราะว่า $d' = \gcd(-a, -b)$ เพราะฉะนั้น $d' \mid (-a)$ และ $d' \mid (-b)$

เพราะฉะนั้น $d' \mid a$ และ $d' \mid b$ เพราะฉะนั้น $d' \leq d$... (2)

จาก (1) และ (2) จะได้ $d = d'$ เพราะฉะนั้น $\gcd(a, b) = \gcd(-a, -b)$

ในทำนองเดียวกันจะได้ $\gcd(a, b) = \gcd(-a, -b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(|a|, |b|)$

16. ให้ $\gcd(a^m, b^n) = 1$

ให้ $t = \gcd(a, b) \Rightarrow t \mid a$ และ $t \mid b \Rightarrow t \mid a^m$ และ $t \mid b^n \Rightarrow t \mid \gcd(a^m, b^n) \Rightarrow t \mid 1 \Rightarrow t = 1$

เพราะฉะนั้น $\gcd(a, b) = 1$ □

ทฤษฎีบท 2.1.6 ให้ a, b เป็นจำนวนเต็มและ a, b ไม่เป็นศูนย์พร้อมกัน ให้ d เป็นจำนวนเต็มบวก จะได้

$d = \gcd(a, b)$ ก็ต่อเมื่อ 1. $d \mid a$ และ $d \mid b$

และ 2. ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$

ข้อพิสูจน์ ($\Leftarrow$) ให้ 1. $d \mid a$ และ $d \mid b$... (1)

และ 2. ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$... (2)

ให้ c เป็นจำนวนเต็มบวกและ $c \mid a$ และ $c \mid b$ เพราะฉะนั้นจาก (2) จะได้ $c \mid d$

โดยทฤษฎีบท 1.4.1 จะได้ $|c| \leq |d|$

เพราะว่า c, d เป็นจำนวนเต็มบวกและ $|c| \leq |d|$ เพราะฉะนั้น $c \leq d$

เพราะฉะนั้น ถ้า c เป็นจำนวนเต็มบวกและ $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$... (3)

จาก (1) และ (3) จะได้ $d = \gcd(a, b)$

($\Rightarrow$) ให้ $d = \gcd(a, b)$ เพราะฉะนั้น $d \mid a$ และ $d \mid b$... (4)

ให้ $c \mid a$ และ $c \mid b$... (5)

เพราะว่า $d = \gcd(a, b)$ เพราะฉะนั้นโดยทฤษฎีบท 2.1.1 จะมีจำนวนเต็ม x, y ที่ทำให้ $d = ax + by$

เพราะว่า $c \mid a$ และ $c \mid b \Rightarrow c \mid ax$ และ $c \mid by \Rightarrow c \mid (ax + by) \Rightarrow c \mid d$

เพราะฉะนั้น ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$ □

แนวคิดอีกแบบหนึ่งในการหาตัวหารร่วมมาก

ให้ D_a แทนเซตของตัวหารที่เป็นบวกทั้งหมดของ a เพราะฉะนั้น $D_a = \{x \in \mathbb{Z}^+ \mid x \mid a\}$
 เพราะฉะนั้น $D_a \cap D_b$ เป็นเซตของตัวหารร่วมของ a และ b ทฤษฎีบทต่อไปพิสูจน์ได้ว่า
 $\gcd(a, b) =$ สมาชิกค่ามากที่สุดของ $D_a \cap D_b = \max(D_a \cap D_b)$

ทฤษฎีบท 2.1.7 ให้ a และ b เป็นจำนวนเต็ม $a \neq 0$ และ $b \neq 0$ จะได้ $\gcd(a, b) = \max(D_a \cap D_b)$

ข้อพิสูจน์ $d = \gcd(a, b) \Rightarrow d \mid a$ และ $d \mid b$

$$\Rightarrow d \in D_a \text{ และ } d \in D_b$$

$$\Rightarrow d \in D_a \cap D_b$$

$$\Rightarrow d \leq \max(D_a \cap D_b)$$

... (1)

$$x \in D_a \cap D_b \Rightarrow x \in D_a \text{ และ } x \in D_b$$

$$\Rightarrow x \mid a \text{ และ } x \mid b$$

$$\Rightarrow x \leq \gcd(a, b)$$

เพราะฉะนั้น $x \leq \gcd(a, b)$ ทุกค่า $x \in D_a \cap D_b$ เพราะฉะนั้น $\max(D_a \cap D_b) \leq \gcd(a, b)$... (2)

จาก (1) และ (2) จะได้ $\gcd(a, b) = \max(D_a \cap D_b)$ □

ตัวอย่างเช่น $a = 12, b = 15$ จะได้ $D_a = \{1, 2, 3, 4, 6, 12\}$ และ $D_b = \{1, 3, 5, 15\}$

เพราะฉะนั้น $D_a \cap D_b = \{1, 3\}$ และ $\gcd(a, b) = 3$

ทฤษฎีบท 2.1.8 $D_k = D_{-k}$ ทุกจำนวนเต็ม k

ข้อพิสูจน์ $a \in D_k \Leftrightarrow a \mid k$

$$\Leftrightarrow a \mid (-k)$$

$$\Leftrightarrow a \in D_{-k}$$

เพราะฉะนั้น $D_k = D_{-k}$ □

ข้อสังเกต 1. ถ้า $a \mid b$ แล้ว $D_a \subset D_b$

2. ถ้า $D_a \cap D_b \subset D_x \cap D_y$ แล้ว $\gcd(a, b) \leq \gcd(x, y)$

เพราะฉะนั้น $D_a \cap D_b = D_x \cap D_y$ แล้ว $\gcd(a, b) = \gcd(x, y)$

ทฤษฎีบท 2.1.9 ให้ a, b, c เป็นจำนวนเต็ม จะได้

$$1. \gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b) = \gcd(|a|, |b|)$$

$$2. \text{ ถ้า } b \mid c \text{ แล้ว } \gcd(b, c) = |b|$$

$$3. \text{ ถ้า } b \mid c \text{ แล้ว } \gcd(a, b) \leq \gcd(a, c)$$

$$4. \gcd(a, b) = \gcd(a, b + ca)$$

ข้อพิสูจน์ 1. $D_a \cap D_b = D_a \cap D_{-b}$ (ทฤษฎีบท 2.1.8)

$$= D_{-a} \cap D_b \quad (\text{ทฤษฎีบท 2.1.8})$$

$$= D_{-a} \cap D_{-b} \quad (\text{ทฤษฎีบท 2.1.8})$$

$$= D_{|a|} \cap D_{|b|} \quad (\text{ทฤษฎีบท 2.1.8})$$

$$\begin{aligned} \text{เพราะฉะนั้น } \max(D_a \cap D_b) &= \max(D_a \cap D_{-b}) = \max(D_{-a} \cap D_{-b}) \\ &= \max(D_{-a} \cap D_b) = \max(D_{|a|} \cap D_{|b|}) \end{aligned}$$

$$\text{เพราะฉะนั้น } \gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b) = \gcd(|a|, |b|)$$

2. ให้ $b \mid c$ เพราะฉะนั้น $D_b \subset D_c$

$$\begin{aligned} D_b \subset D_c &\Rightarrow D_b \cap D_c = D_b \\ &\Rightarrow \max(D_b \cap D_c) = \max(D_b) \\ &\Rightarrow \gcd(b, c) = |b| \end{aligned} \quad \dots (1)$$

3. ให้ $b \mid c$ เพราะฉะนั้น $D_b \subset D_c$

$$\begin{aligned} D_b \subset D_c &\Rightarrow D_a \cap D_b \subset D_a \cap D_c \\ &\Rightarrow \max(D_a \cap D_b) \leq \max(D_a \cap D_c) \\ &\Rightarrow \gcd(a, b) \leq \gcd(a, c) \end{aligned} \quad \dots (2)$$

4. ให้ $d = \gcd(a, b)$ และ $d' = \gcd(a, b + ca)$

$$\begin{aligned} d = \gcd(a, b) &\Rightarrow d \mid a \text{ และ } d \mid b \\ &\Rightarrow d \mid a \text{ และ } d \mid b \text{ และ } d \mid ca \\ &\Rightarrow d \mid a \text{ และ } d \mid (b + ca) \\ &\Rightarrow d \leq \gcd(a, b + ca) \\ &\Rightarrow d \leq d' \end{aligned} \quad \dots (1)$$

$$\begin{aligned} d' = \gcd(a, b + ca) &\Rightarrow d' \mid a \text{ และ } d' \mid (b + ca) \\ &\Rightarrow d' \mid a \text{ และ } d' \mid (-ca) \text{ และ } d' \mid (b + ca) \\ &\Rightarrow d' \mid a \text{ และ } d' \mid ((b + ca) + (-ca)) \\ &\Rightarrow d' \mid a \text{ และ } d' \mid b \\ &\Rightarrow d' \leq \gcd(a, b) \\ &\Rightarrow d' \leq d \end{aligned} \quad \dots (2)$$

จาก (1) และ (2) จะได้ $d' = d$ เพราะฉะนั้น $\gcd(a, b) = \gcd(a, b + ca)$ □

ทฤษฎีบท 2.1.10 ถ้า $a = qb + r$ แล้ว $\gcd(a, b) = \gcd(b, r)$

ข้อพิสูจน์ ให้ $a = qb + r$ เพราะฉะนั้น $r = a - qb$... (1)

ให้ $d = \gcd(a, b)$

เพราะฉะนั้น $d \mid a$ และ $d \mid b$ เพราะฉะนั้น $d \mid (a - qb)$... (2)

จาก (1) และ (2) จะได้ $d \mid r$... (3)

ให้ c เป็นจำนวนเต็มบวกและ $c \mid r$ และ $c \mid b$

เพราะฉะนั้น $c \mid (qb + r)$... (4)

จาก (1) และ (4) จะได้ $c \mid a$ เพราะฉะนั้น $c \mid a$ และ $c \mid b$ เพราะฉะนั้น $c \leq \gcd(a, b)$

เพราะฉะนั้น $c \leq d$... (5)

เพราะว่า 1. $d \mid b$ และ $d \mid r$ (จาก (2) และ (3))

และ 2. ถ้า c เป็นจำนวนเต็มบวกและ $c \mid r$ และ $c \mid b$ แล้ว $c \leq d$ (จาก (5))

เพราะฉะนั้น $\gcd(b, r) = d$ เพราะฉะนั้น $\gcd(a, b) = \gcd(b, r)$ □

ทฤษฎีบท 2.1.11 ถ้า $b \mid a$ แล้ว $\gcd(a, b) = |b|$

ข้อพิสูจน์ ให้ $b \mid a$ เพราะฉะนั้นมีจำนวนเต็ม q ที่ทำให้ $a = qb$ เพราะฉะนั้น $a = qb + 0$

โดยทฤษฎีบท 2.1.10 จะได้ $\gcd(a, b) = \gcd(qb + 0, b) = \gcd(b, 0) = b$

กรณีที่ 1 $b > 0$ เพราะฉะนั้น $\gcd(a, b) = b = |b|$

กรณีที่ 2 $b < 0$ เพราะฉะนั้น $\gcd(a, b) = -b = |b|$

เพราะฉะนั้น ถ้า $b \mid a$ แล้ว $\gcd(a, b) = |b|$ □

ทฤษฎีบท 2.1.12 $\gcd(n, n + 1) = 1$ ทุกจำนวนเต็มบวก n

ข้อพิสูจน์ แบบที่ 1 $\gcd(n, n + 1) = \gcd(n, n + 1 + (-n))$ (ทฤษฎีบท 2.1.9)

$$= \gcd(n, 1)$$

$$= 1 \quad \text{(ทฤษฎีบท 2.1.9)}$$

แบบที่ 2 จากทฤษฎีบท 2.1.6 จะได้ $\gcd(n, n + 1) \mid 1$ เพราะฉะนั้น $\gcd(n, n + 1) = 1$ □

ตัวอย่าง 2.1.1 ให้ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่า $\gcd(n! + 1, (n + 1)! + 1) = 1$

แนวคิด $\gcd(n! + 1, (n + 1)! + 1) = \gcd(n! + 1, (n + 1)! + 1 - (n! + 1)(n + 1))$ (ทฤษฎีบท 2.1.9)

$$= \gcd(n! + 1, -n)$$

$$= \gcd(-n, n! + 1) \quad \text{(ทฤษฎีบท 2.1.5)}$$

$$= \gcd(-n, n! + 1 - n(n - 1)!) \quad \text{(ทฤษฎีบท 2.1.9)}$$

$$= \gcd(-n, 1)$$

$$= 1 \quad \text{(ทฤษฎีบท 2.1.5)} \quad \square$$

ตัวอย่าง 2.1.2 จงแสดงว่า $\frac{21n + 4}{14n + 3}$ เป็นเศษส่วนอย่างต่ำ ทุกจำนวนเต็มบวก n

แนวคิด $\gcd(14n + 3, 21n + 4) = \gcd(14n + 3, 21n + 4 - (14n + 1))$ (ทฤษฎีบท 2.1.9)

$$= \gcd(14n + 3, 7n + 1) = \gcd(7n + 1, 14n + 3)$$

$$= \gcd(7n + 1, 14n + 3 - 2(7n + 1)) \quad \text{(ทฤษฎีบท 2.1.9)}$$

$$= \gcd(7n + 1, 1)$$

$$= 1 \quad \text{(ทฤษฎีบท 2.1.9)}$$

เพราะฉะนั้น $14n + 3, 21n + 4$ ไม่มีตัวประกอบร่วม เพราะฉะนั้น $\frac{21n + 4}{14n + 3}$ เป็นเศษส่วนอย่างต่ำ □

ทฤษฎีบท 2.1.13 ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a, b เป็นจำนวนเต็มบวก โดยที่

$$a = bq_1 + r_1, \quad 0 < r_1 < b \quad \dots (1)$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \quad \dots (2)$$

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \quad \dots (3)$$

:

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \quad \dots (4)$$

$$r_{n-1} = r_n q_{n+1} \quad \dots (5)$$

จะได้ $r_n = \gcd(a, b)$

ข้อพิสูจน์ $\gcd(a, b) = \gcd(bq_1 + r_1, b)$

(จาก (1))

$$= \gcd(r_1, b) \quad (\text{ทฤษฎีบท 2.1.10})$$

$$= \gcd(r_1, r_1 q_2 + r_2) \quad (\text{จาก (2)})$$

$$= \gcd(r_1, r_2) \quad (\text{ทฤษฎีบท 2.1.10})$$

$$= \gcd(r_2 q_3 + r_3, r_2) \quad (\text{จาก (3)})$$

$$= \gcd(r_3, r_2) \quad (\text{ทฤษฎีบท 2.1.10})$$

:

$$= \gcd(r_{n-1}, r_n)$$

$$= \gcd(r_n q_{n+1}, r_n) \quad (\text{จาก (5)})$$

$$= r_n \quad (\text{ทฤษฎีบท 2.1.9}) \quad \square$$

ผลของขั้นตอนวิธีการหารจะช่วยให้หาจำนวนเต็ม x, y ที่ทำให้ $ax + by = \gcd(a, b)$

กำหนดให้ขั้นตอนวิธีการหารคือ

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b \quad \dots (1)$$

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \quad \dots (2)$$

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2 \quad \dots (3)$$

$$r_2 = r_3 q_4 + r_4, \quad 0 \leq r_4 < r_3 \quad \dots (4)$$

:

$$r_{k-2} = r_{k-1} q_k + r_k, \quad 0 \leq r_k < r_{k-1} \quad \dots (5)$$

$$r_{k-1} = r_k q_{k+1} \quad \dots (6)$$

เพราะฉะนั้น $r_k = \gcd(a, b)$

โดยใช้การแทนค่าย้อนกลับ

จาก (1) จะได้ $r_1 = a - bq_1 \quad \dots (7)$

$$= a\alpha_1 + b\beta_1$$

เมื่อ $\alpha_1 = 1$ และ $\beta_1 = -q_1$

จาก (2) จะได้ $r_2 = b - q_2 r_1$

$$= b - q_2 (a\alpha_1 + b\beta_1) \quad (\text{จาก (7)})$$

$$= -aq_2\alpha_1 + b(1 - q_2\beta_1) \quad \dots (8)$$

$$= a\alpha_2 + b\beta_2$$

เมื่อ $\alpha_2 = -q_2\alpha_1$ และ $\beta_2 = 1 - q_2\beta_1$

จาก (2) จะได้ $r_3 = r_1 - r_2 q_3$

$$= a\alpha_1 + b\beta_1 - q_3(a\alpha_2 + b\beta_2) \quad (\text{จาก (7) และ (8)})$$

$$= a(\alpha_1 - q_3\alpha_2) + b(\beta_1 - q_3\beta_2)$$

$$= a\alpha_3 + b\beta_3$$

เมื่อ $\alpha_3 = \alpha_1 - q_3\alpha_2$ และ $\beta_3 = \beta_1 - q_3\beta_2$

ในทำนองเดียวกันจะได้ $r_i = a\alpha_i + b\beta_i$ ทุกค่า $i = 1, 2, \dots, k$

เมื่อ $\alpha_{i+1} = \alpha_{i-1} - q_{i+1}\alpha_i$ ทุกค่า $i = 2, 3, \dots, k$

$$\beta_{i+1} = \beta_{i-1} - q_{i+1}\beta_i \quad \text{ทุกค่า } i = 2, 3, \dots, k$$

เพราะฉะนั้น $d = \gcd(a, b) = r_k = a\alpha_k + b\beta_k$

เพราะฉะนั้นมีจำนวนเต็ม $x = \alpha_k$ และ $y = \beta_k$ ที่ทำให้ $ax + by = d$

ตัวอย่าง 2.1.3 จงหา $\gcd(216, 84)$ และหาจำนวนเต็ม x, y ที่ทำให้ $\gcd(216, 84) = 216x + 84y$

$$\text{แนวคิด } 216 = (84)(2) + 48 \quad \dots (1)$$

$$84 = (48)(1) + 36 \quad \dots (2)$$

$$48 = (36)(1) + 12 \quad \dots (3)$$

$$36 = (12)(3)$$

เพราะฉะนั้น $\gcd(216, 84) = 12$

โดยการแทนค่าย้อนกลับจะได้

$$12 = 48 - (36)(1) \quad (\text{จาก (3)})$$

$$= 48 - 36$$

$$= 48 - (84 - (48)(1)) \quad (\text{จาก (2)})$$

$$= 2(48) - 84$$

$$= 2(216 - (84)(2)) - 84 \quad (\text{จาก (1)})$$

$$= (216)(2) + (84)(-5)$$

เพราะฉะนั้นมี $x = 2$ และ $y = -5$ ที่ทำให้ $12 = 216x + 84y$