บทที่ 2
จำนวนเต็ม (Integers)

วิวัฒนาการของจำนวนเต็มมาจากความพยายามที่จะหาคำตอบของสมการที่อยู่ในรูป $a = b+x$ โดยที่ a และ b เป็นจำนวนนับหรือจำนวนธรรมชาติ (natural number) ซึ่งจะพบว่า ถ้า $a > b$ แล้ว เราสามารถหาคำตอบของสมการ (x) เป็นจำนวนนับได้ แต่ถ้า $a \leqslant b$ เราไม่สามารถจะหาคำตอบของสมการที่เป็นจำนวนนับได้ เหตุนี้เองเราจึงพยายามที่จะสร้างจำนวนใหม่ขึ้นเพื่อที่จะหาคำตอบของสมการข้างต้น ซึ่งจะพบว่าคำตอบ (คือ x) ขึ้นกับจำนวนนับ a และ b เราจึงแทน x ด้วยคู่ลำดับ (a, b) และเรียกว่า เป็นจำนวนเต็ม

ตัวอย่าง 1) (7, 5) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $7 = 5+x$

2) (3, 8) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $3 = 8+x$

3) (8, 3) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $8 = 3+x$

4) (4, 4) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $4 = 4+x$

หมายเหตุ จากสมการ $a = b+x$ ตามที่เคยเรียนในชั้นประถมและมัธยม เราคุ้นเคยกับความหมายของ $x = a-b$

ดังนั้น เราอาจคิดว่า คู่ลำดับ (a, b) คือ $a-b$

พิจารณาตัวอย่างต่อไปนี้

(7, 5) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $7 = 5+x$

(6, 4) แทนจำนวนเต็มซึ่งสอดคล้องสมการ $6 = 4+x$

จะพบว่า คู่ลำดับ (7, 5) และ (6, 4) แทนจำนวนเต็มเดียวกัน คือ 2 แสดงว่าจำนวนเต็มหนึ่ง ๆ สามารถแทนด้วยคู่ลำดับมากมาย และเมื่อพิจารณา (7, 5) และ (6, 4)

จะเห็นว่า $7+4 = 5+6$

นั่นคือ สำหรับ (a, b) และ (c, d) แทนจำนวนเต็มเดียวกัน ก็ต่อเมื่อ

$$a+d = b+c$$

หมายเหตุ ถ้าเราคิดว่า (7, 5) แทนจำนวนเต็ม $7-5$ และ (6, 4) แทนจำนวนเต็ม $6-4$ ซึ่งต่างก็แทนจำนวนเต็มเดียวกัน แล้ว

$$7-5 = 6-4$$

หรือ $$7+4 = 5+6$$

ทำนองเดียวกัน ถ้า (a, b) และ (c, d) แทนจำนวนเต็มเดียวกันแล้ว

$$a-b = c-d$$

หรือ $$a+d = b+c$$

2.1 การบวกและการคูณจำนวนเต็ม

นิยาม 2.1.1 กำหนดให้ $K = [(a, b)/a, b \in N\}$ นิยามความสัมพันธ์ "$\sim$" บน K โดย $(a, b) \sim (c, d)$ ก็ต่อเมื่อ $a+d = b+c$ สำหรับทุก ๆ $(a, b), (c, d) \in K$ นั่นคือ

$$(a, b) \sim (c, d) \quad \text{ก็ต่อเมื่อ} \quad a+d = b+c$$

เราจะพบว่า $(9, 3) \sim (10, 4)$ เพราะว่า $9+4 = 3+10$

และ $(10, 4) \sim (200, 194)$ เพราะว่า $10+194 = 4+200$

นอกจากนี้เรายังได้ว่า

$(1, 1) \sim (2, 2) \sim (3, 3) \sim$

$(2, 1) \sim (3, 2) \sim (4, 3) \sim \ldots$

$(3, 1) \sim (4, 2) \sim (5, 3) \sim \ldots$

$(4, 1) \sim (5, 2) \sim (6, 3) \sim \ldots$

ข้อสังเกต

1. $(a, b) = (c, d)$ ตามนิยามคู่ลำดับ หมายถึง $a = c$ และ $b = d$

2. เราใช้ $(a, b) \sim (c, d)$ แทนความหมายถึง คู่ลำดับทั้งสองแทนจำนวนเต็มเดียวกัน (นั่นคือ $a+d = b+c$)

3. เนื่องจาก $K = \{(a, b)/a, b \in N\}$ ดังนั้น K จึงสามารถเขียนในรูปผลคูณคาร์ทีเซียน (Cartesian product) ได้

$$K = N \times N = \{(1,1), (1,2), (1,3), \ldots, (2,1), (2,2), (2,3), \ldots, (3,1), (3,2), (3,3), \ldots\}$$

ทฤษฎีบท 2.1.1 "$\sim$" เป็นความสัมพันธ์สมมูล (equivalence relation) บน K

พิสูจน์ เนื่องจากความสัมพันธ์สมมูล ต้องมีคุณสมบัติ 3 ข้อ คือ สำหรับ (a, b), (c, d) และ (e, f) $\in$ K

1. การสะท้อน (Reflexive) : (a, b) $\sim$ (a, b)
2. การสมมาตร (Symmetric) : (a, b) $\sim$ (c, d) $\rightarrow$ (c, d) $\sim$ (a, b)
3. การถ่ายทอด (Transitive) : (a, b) $\sim$ (c, d) $\wedge$ (c, d) $\sim$ (e, f) $\rightarrow$ (a, b) $\sim$ (e, f)

ดังนั้น เราจึงต้องพิสูจน์ให้ครบทั้ง 3 ข้อ

1. เพราะว่า $a+b = b+a$ กฎการสลับที่ของจำนวนนับ
   เพราะฉะนั้น (a, b) $\sim$ (a, b) นิยาม 2.1.1

2. ให้ (a, b) $\sim$ (a, b)
   ดังนั้น $a+d = b+c$ นิยาม 2.1.1
   หรือ $b+c = a+d$
   เพราะฉะนั้น $c+b = d+a$ กฎการสลับที่การบวกของจำนวนนับ
   นั่นคือ (c, d) $\sim$ (a, b) นิยาม 2.1.1

3. ให้ (a, b) $\sim$ (c, d) และ (c, d) $\sim$ (e, f)
   ดังนั้น $a+d = b+c$
   และ $c+f = d+e$ นิยาม 2.1.1
   เราจะได้ว่า $(a+d)+(c+f) = (b+c)+(d+e)$
   เพราะฉะนั้น $(a+f)+(d+c) = (b+e)+(d+c)$ กฎการจัดหมู่และกฎการสลับที่การบวกของจำนวนนับ
   นั่นคือ $a+f = b+e$ กฎการตัดออกของจำนวนนับ
   (a, b) $\sim$ (e, f) นิยาม 2.1.1

#

เนื่องจาก $K = N \times N$ และเท่ากับ

ดังนั้น $K = \{(1, 1), (1, 2), (1, 3), \ldots, (2, 1), (2, 2), (2, 3), \ldots, (3, 1), (3, 2), (3, 3), \ldots\}$

เราพบว่า สมาชิกของ K สามารถแยกเป็นพวก ๆ ที่แทนจำนวนเต็มเดียวกันได้ เช่น

$A = \{(2, 1), (3, 2), (4, 3), \ldots\}$

$B = \{(3, 1), (4, 2), (5, 3), \ldots\}$

ดังนั้น เราสามารถนิยามจำนวนเต็มใหม่ให้กะทัดรัดขึ้น

นิยาม 2.1.2 ให้ $\sim$ เป็นความสัมพันธ์สมมูลบน K สำหรับแต่ละ $(a, b) \in K$,

$$[a, b] = \{(m, n)/(m, n) \sim (a, b)\}$$

เรียก $[a, b]$ ว่า เป็นพวกสมมูลของ (a, b) (equivalence class of (a, b)) และเรียก (a, b) ว่า เป็นตัวแทนของพวกสมมูล $[a, b]$

ทฤษฎีบท 2.1.2 สำหรับแต่ละ $(a, b), (c, d) \in K$

1) $(a, b) \in [a, b]$
2) ถ้า $(a, b) \in [c, d]$ แล้ว $[a, b] = [c, d]$
3) $[a, b] = [c, d]$ ก็ต่อเมื่อ $(a, b) \sim (c, d)$

พิสูจน์ 1) เนื่องจาก $(a, b) \sim (a, b)$ (คุณสมบัติการสะท้อน)
ดังนั้น $(a, b) \in [a, b]$ นิยาม2.1.2

2) กำหนด $(a, b) \in [c, d]$ จะต้องพิสูจน์ว่า $[a, b] \subseteq [c, d]$
และ $[c, d] \subseteq [a, b]$
เนื่องจาก $(a, b) \in [c, d]$ ดังนั้น $(a, b) \sim (c, d)$
จะพิสูจน์ $[a, b] \subseteq [c, d]$
ให้ $(m, n) \in [a, b]$ ดังนั้น $(m, n) \sim (a, b)$
นั่นคือ $(m, n) \sim (c, d)$ (คุณสมบัติการถ่ายทอด)
เพราะฉะนั้น $(m, n) \in [c, d]$
ดังนั้น $[a, b] \subseteq [c, d]$
จะพิสูจน์ $[c, d] \subseteq [a, b]$
ให้ $(m, n) \in [c, d]$ ดังนั้น $(m, n) \sim (c, d)$
แต่ $(a, b) \sim (c, d)$
เพราะฉะนั้น $(c, d) \sim (a, b)$ คุณสมบัติการสมมาตร
นั่นคือ $(m, n) \sim (a, b)$ คุณสมบัติการถ่ายทอด
แสดงว่า $(m, n) \in [a, b]$
ดังนั้น $[c, d] \subseteq [a, b]$ #

3) ให้ทำเป็นแบบฝึกหัด

นิยาม 2.1.3 ให้ $[m, n]$ เป็นพวกสมมูลของ $(m, n) \in K$, เรานิยามจำนวนเต็มเป็นเซตของพวกสมมูล และแทนด้วยสัญลักษณ์ "Z" ดังนั้น

$$Z = \{[m, n] / m, n \in N\}$$

ก่อนที่จะนิยามการบวก และการคูณในเซตจำนวนเต็ม ขอให้พิจารณาตัวอย่างต่อไปนี้

เนื่องจาก $(2, 1)$ แทนจำนวนเต็ม 1

$(5, 3)$ แทนจำนวนเต็ม 2

$(7, 4)$ แทนจำนวนเต็ม $3 = 1+2$

$(13, 11)$ แทนจำนวนเต็ม $2 = 1 \cdot 2$

ซึ่งจะพบว่า $(7, 4)$ เกิดจาก $(2+5, 1+3)$

และ $(13, 11)$ เกิดจาก $(2 \cdot 5 + 1 \cdot 3, 2 \cdot 3 + 1 \cdot 5)$

หมายเหตุ ถ้าเราคิดว่าคู่ลำดับเป็นผลต่าง

$$\begin{aligned}(2, 1) + (5, 3) &= (2-1) + (5-3) \\ &= (2+5) - (1+3) \\ &= (2+5, 1+3) \\ &= (7, 4)\end{aligned}$$

$$\begin{aligned}(2, 1)(5, 3) &= (2-1)(5-3) \\ &= (2 \cdot 5 + 1 \cdot 3) - (2 \cdot 3 + 1 \cdot 5) \\ &= (2 \cdot 5 + 1 \cdot 3,\ 2 \cdot 3 + 1 \cdot 5) \\ &= (13,\ 11)\end{aligned}$$

นิยาม 2.1.4 การบวกและการคูณในเซต z นิยามดังนี้

สำหรับ $[a, b], [c, d] \in Z$

$$[a, b] + [c, d] = [a+c, b+d]$$

และ $$[a, b] \cdot [c, d] = [ac+bd,\ bc+ad]$$

ตัวอย่าง 2.1.1 กำหนดให้ $3 = [11, 8]$ และ $2 = [7, 5]$

ดังนั้น

$$\begin{aligned}3+2 &= [11, 8] + [7, 5] \\ &= [11+7, 8+5] \\ &= [18, 13] \\ &= 5\end{aligned}$$

และ $3.2 = [11, 8][7, 5]$

$= [11\cdot 7+8\cdot 5, 8\cdot 7+11\cdot 5]$

$= [117, 111]$

$= 6$

เนื่องจากการบวกและการคูณ ถูกนิยามบนเซตของพวกสมมูล ดังนั้นเราจะแสดงว่าไม่ว่าจะเลือกสมาชิกใดในพวกสมมูล ผลบวกและผลคูณยังคงเหมือนเดิม

ทฤษฎีบท 2.1.3 คุณสมบัติแจ่มชัด (Well-defined properties)

สำหรับ $[a, b], [a', b'], [c, d], [c'. d'] \in \mathbb{Z}$

ถ้า $[a, b] = [a', b']$ และ $[c, d] = [c', d']$ แล้ว

1. $[a, b]+[c, d] = [a', b']+[c', d']$
2. $[a, b]\cdot[c, d] = [a', b']\cdot[c', d']$

พิสูจน์ ในที่นี้จะพิสูจน์คุณสมบัติสำหรับการบวกเท่านั้น ส่วนการคูณให้เป็นแบบฝึกหัด

จะพิสูจน์ว่า $[a, b] + [c, d] = [a', b'] + [c', d']$

ต้องแสดงว่า $[a+c, b+d] = [a' +c', b' +d']$

นั่นคือ $(a+c, b+d) \sim (a' +c', b' +d')$

หรือ $(a+c)+(b'+d') = (b+d)+(a'+c')$

เนื่องจาก $[a, b] = [a', b']$ ดังนั้น $(a, b) \sim (a', b')$ ทฤษฎีบท 2.1.2 ข้อ 3

และ $[c, d] = [c', d']$ ดังนั้น $(c, d) \sim (c', d')$ ทฤษฎีบท 2.1.2 ข้อ 3

เพราะฉะนั้น $a + b' = b + a'$ นิยาม 2 . 1 . 1

และ $c + d' = d + c'$ นิยาม 2.1.1

จึงทำให้ได้ $(a+b')+(c+d') = (b+a')+(d+c')$

นั่นคือ $(a+c)+(b'+d') = (b+d)+(a'+c')$ กฎการสลับที่ และจัดหมู่สำหรับจำนวนเต็ม

เพื่อให้เกิดความเข้าใจทฤษฎีบทนี้ยิ่งขึ้น พิจารณาคำอธิบายเพิ่มเติมดังนี้

$[a, b] = [a', b']$ หมายถึง $(a, b) \sim (a', b')$ นั่นคือ คู่ลำดับทั้งสองแทนจำนวนเต็มเดียวกัน และ

$[c, d] = [c', d']$ หมายถึง $(c, d) \sim (c', d')$ นั่นคือ คู่ลำดับทั้งสองแทนจำนวนเต็มอีกจำนวนหนึ่งเหมือนกัน

ตามทฤษฎีบทกล่าวว่า ถ้า (a, b). (a', b') แทนจำนวนเต็มเดียวกัน และ (c, d), (c' , d') แทนจำนวนเต็มอีกจำนวนหนึ่ง แล้ว

$[a, b] + [c, d]$ เท่ากับ $[a', b'] + [c', d']$

$[a+c, b+d]$ เท่ากับ $[a' + c', b' + d']$

นั่นคือ $(a + c, b + d)$ กับ $(a' + c', b' + d')$ แทนจำนวนเต็มเดียวกัน #

ตัวอย่าง 2.1.2 ให้ $[1, 2] = [3, 4]$ และ $[5, 2] = [9, 6]$

พิจารณา $[1, 2] + [5, 2] = [1+5, 2+2] = [6, 4]$

และ $[3, 4] + [9, 6] = [3+9, 4+6] = [12, 10]$

ซึ่งจะพบว่า $[1, 2] + [5, 2] = [3, 4] + [9, 6]$

หรือ $(6, 4) \sim (12, 10)$

ต่อไปจะเป็นคุณสมบัติการบวกและการคูณใน Z

ทฤษฎีบท 2.1.4 คุณสมบัติปิดสำหรับการบวกและการคูณ

สำหรับแต่ละ $[a, b], [c, d] \in Z$

1 . $[a, b] + [c, d] \in Z$

2 . $[a, b] \cdot [c, d] \in Z$

พิสูจน์ 1) เพราะว่า $[a, b] + [c, d] = [a+c, b+d]$ นิยาม 2.1.4

เนื่องจาก a, b, c, d เป็นจำนวนนับ นิยาม 2.1.1

ดังนั้น $a + c$ และ $b + d$ เป็นจำนวนนับ คุณสมบัติปิดสำหรับการบวกของจำนวนนับ

นั่นคือ $[a+c, b+d] \in Z$ นิยาม 2.1.1

แต่ $[a, b] + [c, d] = [a+c, b+d]$

เพราะฉะนั้น $[a, b] + [c, d] \in Z$

2) ให้ทำเป็นแบบฝึกหัด

ทฤษฎีบท 2.1.5 คุณสมบัติสลับที่สำหรับการบวก และการคูณ

สำหรับแต่ละ $[a, b] [c, d] \in Z$

1. $[a, b] + [c, d] = [c, d] + [a, b]$
2. $[a, b] \cdot [c, d] = [c, d] \cdot [a, b]$

พิสูจน์ 1. ให้ทำเป็นแบบฝึกหัด

2. เพราะว่า $[a, b]\,[c, d] = [ac+bd, bc+ad]$ นิยาม 2.1.4

เนื่องจาก a, b, c และ $ac+bd, bc+ad$ ต่างก็เป็นจำนวนนับ (นิยาม 2.1.1 และคุณสมบัติปิดของจำนวนนับ)

เนื่องจาก $ac+bd = ca+db$ คุณสมบัติการสลับที่

และ $bc+ad = da+cb$ ทั้งการบวกและการคูณของจำนวนนับ

ดังนั้น $[ac+bd, bc+ad] = [ca+db, da+cb]$

แต่ $[c, d]\,[a, b] = [ca+db, da+cb]$ นิยาม 2.1.4

นั่นคือ $[a, b]\,[c, d] = [c, d]\,[a, b]$ คุณสมบัติการถ่ายทอด

#

ทฤษฎีบท 2.1.6 คุณสมบัติการจัดหมู่สำหรับการบวก และการคูณ

สำหรับแต่ละ $[a, b], [c, d], [e, f] \in Z$

1. $[a,b]+([c,d]+[e,f]) = ([a, b]+[c, d])+[e, f]$
2. $[a, b]\cdot([c, d]\cdot[e, f]) = ([a, b]\cdot[c, d])\cdot[e, f]$

พิสูจน์ 1. เนื่องจาก

$$\begin{aligned}
[a, b]+([c, d]+[e, f]) &= [a, b]+[c+e, d+f] && \text{นิยาม 2.1.4}\\
&= [a+(c+e), b+(d+f)] && \text{นิยาม 2.1.4}\\
&= [(a+c)+e, (b+d)+f] && \text{คุณสมบัติการจัดหมู่สำหรับการบวกของจำนวนนับ}\\
&= [a+c, b+d]+[e, f] && \text{นิยาม 2.1.4}\\
&= ([a+b]+[c, d])+[e, f] && \text{นิยาม 2.1.4}
\end{aligned}$$

#

2. ให้ทำเป็นแบบฝึกหัด

ทฤษฎีบท 2.1.7 คุณสมบัติการมีเอกลักษณ์สำหรับการบวก

สำหรับแต่ละ $[a, b] \in Z$ จะต้องมี $[m, m] \in Z$ เพียงแบบเดียว ซึ่งทำให้

$$[a, b]+[m, m] = [a, b]$$

พิสูจน์ ให้ทำเป็นแบบฝึกหัด

ตัวอย่าง 2.1.3 ให้ $[a, b] = [2, 3]$ และให้ $m = 4$

ดังนั้น $[2, 3]+[4, 4] = [2+4, 3+4]$

$= [6, 7]$

แต่ $(6, 7) \sim (2, 3)$ นั่นคือ $[6, 7] = [2, 3]$

จึงทำให้ได้ว่า $[2, 3] + [4, 4] = [2, 3]$

ทฤษฎีบท 2.1.8 คุณสมบัติการมีผกผันสำหรับการบวก

สำหรับแต่ละ $[a, b] \in Z$ จะมี $[b, a] \in Z$ เพียงแบบเดียว ซึ่งทำให้

$$[a, b] + [b, a] = [m, m]$$

พิสูจน์ เราต้องพิสูจน์ว่ามี $[b, a]$ เพียงแบบเดียวเท่านั้น

และต้องพิสูจน์ว่า $[a, b] + [b, a] = [m, m]$

ตอนแรกเราจะพิสูจน์ว่า $[a, b] + [b, a] = [m, m]$ ก่อน

เนื่องจาก $[a, b] + [b, a] = [a + b, b + a]$ นิยาม 2.1.4

$= [a + b, a + b]$ คุณสมบัติสลับที่การบวกของจำนวนนับ

$= [m, m]$ นิยาม 2.1.1

ตอนต่อไปจะแสดงว่า มี $[b, a] \in Z$ เพียงแบบเดียว ที่มีคุณสมบัติดังกล่าว

สมมติว่ามี $[c, d] \in Z$ ซึ่งแต่ละ $[a, b]$ ใด ๆ

$$[a, b] + [c, d] = [m, m]$$

เนื่องจาก $[a, b] + [b, a] = [m, m]$ จากคุณสมบัติ $[m, m]$

และจาก $[a, b] + [c, d] = [m, m]$ จากคุณสมบัติ $[c, d]$

ดังนั้น $[a, b] + [b, a] = [a, b] + [c, d]$

หรือ $[a + b, b + a] = [a + c, b + d]$ นิยาม 2.1.4

นั่นคือ $(a + b, b + a) \sim (a + c, b + d)$ ทฤษฎีบท 2.1.2 ข้อ 3

$(a + b) + (b + d) = (b + a) + (a + c)$ นิยาม 2.1.1

$b + d = a + c$ คุณสมบัติการตัดออก

$(b, a) \sim (c, d)$ นิยาม 2.1.1

$[b, a] = [c, d]$ ทฤษฎีบท 2.1.2 ข้อ 3

นั่นคือ มี $[b, a]$ เพียงแบบเดียว #

ตัวอย่าง 2.1.4 ให้ $[a, b] = [4, 8]$

ดังนั้น $[4, 8] + [8, 4] = [4 + 8, 8 + 4]$

$= [12, 12]$

$= [m, m]$, โดย $m = 12$

ทฤษฎีบท 2.1.9 คุณสมบัติการมีเอกลักษณ์สำหรับการคูณ

สำหรับแต่ละ $[a, b] \in Z$ จะมี $[c+1, c] \in Z$ เพียงแบบเดียว ซึ่งทำให้

$$[a, b]\cdot[c+1, c] = [a, b]$$

พิสูจน์ เนื่องจาก $[a, b]\cdot[c+1, c] = [a(c+1)+bc, b(c+1)+ac]$ นิยาม 2.1.4

$= [ac+bc+a, ac+bc+b]$ คุณสมบัติการกระจาย สลับที่และจัดหมู่

$= [a, b]$ นิยาม 2.1.1

ต่อไปจะแสดงว่า มี $[c+1, c] \in Z$ เพียงแบบเดียว

สมมติว่า มี $[e, f] \in Z$ ซึ่งสำหรับแต่ละ $[a, b]$ ทำให้

$$[a, b]\cdot[e, f] = [a, b]$$

เนื่องจาก $[e, f]\cdot[c+1, c] = [e, f]$ คุณสมบัติ $[c+1, c]$

และจาก $[c+1, c]\cdot[e, f] = [c+1, c]$ คุณสมบัติ $[e, f]$

แต่ $[e, f]\cdot[c+1, c] = [c+1, c]\cdot[e, f]$ คุณสมบัติการสลับที่การคูณของจำนวนเต็ม

ดังนั้น $[e, f] = [c+1, c]$

ตัวอย่าง 2.1.5 ให้ $[a, b] = [3, 5]$ และ $c = 9$

ดังนั้น $[3, 5]\cdot[9+1, 9] = [3, 5]\cdot[10, 9]$

$= [30+45, 50+27]$

$= [75, 77]$

ซึ่ง $(75.77) \sim (3, 5)$

หรือ $[75, 77] = [3, 5]$

เพราะฉะนั้น $[3, 5]\cdot[9+1, 9] = [3, 5]$ #

ทฤษฎีบท 2.1.10 คุณสมบัติการกระจาย

สำหรับแต่ละ $[a, b], [c, d], [e, f] \in Z$

$$[a, b]\cdot([c, d]+[e, f]) = ([a, b]\cdot[c, d])+([a, b]\cdot[e, f])$$

พิสูจน์ พิจารณาซ้ายมือ

$[a, b]\cdot([c, d]+[e, f]) = [a, b]\cdot([c+e, d+f])$ นิยาม 2.1.4

$= [a(c+e)+b(d+f), b(c+e)+a(d+f)]$ นิยาม 2.1.4

$= [(ac + ae) + (bd + bf), (bc + be) + (ad + af)]$

คุณสมบัติการกระจายของจำนวนนับ

พิจารณาขวามือ

$[a, b]\cdot[c, d] + [a, b]\cdot[e, f]$

$= [ac + bd, bc + ad] + [ae + bf, be + af]$ นิยาม 2.1.4

$= [(ac + bd) + (ae + bf), (bc + ad) + (be + af)$ นิยาม 2.1.4

$= [(ac + ae) + (bd + bf), (bc + be) + (ad + af)]$ คุณสมบัติการจัดหมู่และสลับที่ของจำนวนนับ

ในเรื่องของจำนวนธรรมชาติหรือจำนวนนับ มีการเรียงลำดับทำนองเดียวกันสำหรับจำนวนเต็ม $[a, b]$ และ $[c, d]$ ซึ่งถ้าเราคิดว่าอยู่ในรูปผลต่างก็คือ $a-b$ และ $c-d$ ก็สามารถเรียงลำดับได้ ถ้าเรากล่าวว่า จำนวนเต็ม $[a, b]$ น้อยกว่า $[c, d]$ ก็หมายความว่า $a-b$ น้อยกว่า $c-d$ นั่นคือ

$$a-b < c-d$$

หรือ $$a+d < b+c$$

นิยาม 2.1.5 เรากล่าวว่า $[a, b]$ น้อยกว่า $[c, d]$ ก็ต่อเมื่อ $a+d < b+c$ สำหรับ $[a, b], [c, d] \in Z$

ตัวอย่าง 2.1.6 $[4, 3] < [7, 2]$ เนื่องจาก $4+2 < 3+7$

$[2, 1]$ c $[8, -9]$ เนื่องจาก $2\text{-}9 < 1+8$

ทฤษฎีบท 2.1.11 สำหรับ $[a, b], [c, d] \in Z$ จะได้ว่า

$[a, b] < [c, d]$ ก็ต่อเมื่อมี $[e, f] \in Z$ โดยที่ $e > f$ ซึ่งทำให้

$$[c, d] = [a, b] + [e, f]$$

พิสูจน์ ให้ $[a, b], [c, d] \in Z$

เนื่องจาก $[a, b] < [c, d]$

ก็ต่อเมื่อ $a + d < b + c$ นิยาม 2.1.5

ก็ต่อเมื่อ $b + c = (a+d)+g$ สำหรับบาง $g \in N$

ก็ต่อเมื่อ $(b + c) + f = (a+d)+(g+f)$ โดย $f \in N$

ก็ต่อเมื่อ $c+(b+f) = d+a+(g+f)$

ก็ต่อเมื่อ $c+(b+f) = d+(a+e)$ (ให้ $e = g+f$)

ก็ต่อเมื่อ $(c, d) \sim (a+e, b+f)$ นิยาม 2.1.1

ก็ต่อเมื่อ $[c, d] = [a+e, b+f]$ ทฤษฎีบท 2.1.2 ข้อ 3

ก็ต่อเมื่อ $[c, d] = [a, b] + [e, f]$ นิยาม 2.1.3

เพราะฉะนั้น $[a, b] < [c, d]$ ก็ต่อเมื่อ $[c, d] = [a, b] + [e, f]$ โดยที่ $e > f$ #

ทฤษฎีบท 2.1.12 สำหรับ $[a, b], [c, d] \in Z$ จะได้ว่า กรณีต่อไปนี้เป็นจริงเพียงกรณีเดียว คือ

1. $[a, b] < [c, d]$
2. $[a, b] = [c, d]$
3. $[c, d] < [a, b]$

พิสูจน์ ให้ $[a, b], [c, d] \in Z$

ดังนั้น a, b, c และ $d \in N$

นั่นคือ $a+d$ และ $b+c$ ต่างก็เป็นจำนวนนับ

จากคุณสมบัติของจำนวนนับ แสดงว่ากรณีต่อไปนี้เป็นจริงกรณีเดียว

1. $a+d < b+c$
2. $a+d = b+c$
3. $b+c > a+d$

ซึ่งหมายความว่า กรณีต่อไปนี้เป็นจริงกรณีเดียว

1. $[a, d] < [c, d]$ นิยาม 2.1.5
2. $[a, b] = [c, d]$
3. $[c, d] < [a, b]$

เราเรียกทฤษฎีบทข้างต้นนี้ว่า กฎไตรวิภาค (Trichotomy law) #

ทฤษฎีบท 2.1.13 สำหรับ $[a, b], [c, d], [e, f], [g, h] \in Z$

ถ้า $[a, b] < [c, d]$ และ $[e, f] < [g, h]$ แล้ว

$$[a, b] + [e, f] < [c, d] + [g, h]$$

พิสูจน์ ให้ทำเป็นแบบฝึกหัด

ทฤษฎีบท 2.1.14 สำหรับ $[a, b], [c, d], [e, f] \in Z$ จะได้ว่า ข้อความต่อไปนี้เป็นจริง

1. $[a, b] < [c, d]$ ก็ต่อเมื่อ $[a, b] + [e, f] < [e, d] + [e, f]$
2. $[a, b] < [c, d]$ ก็ต่อเมื่อ $[a, b] \cdot [e, f] < [c, d] \cdot [e, f]$ โดยที่ $e > f$
3. $[a, b] < [c, d]$ ก็ต่อเมื่อ $[c, d] \cdot [e, f] < [a, b] \cdot [e, f]$ โดยที่ $e < f$

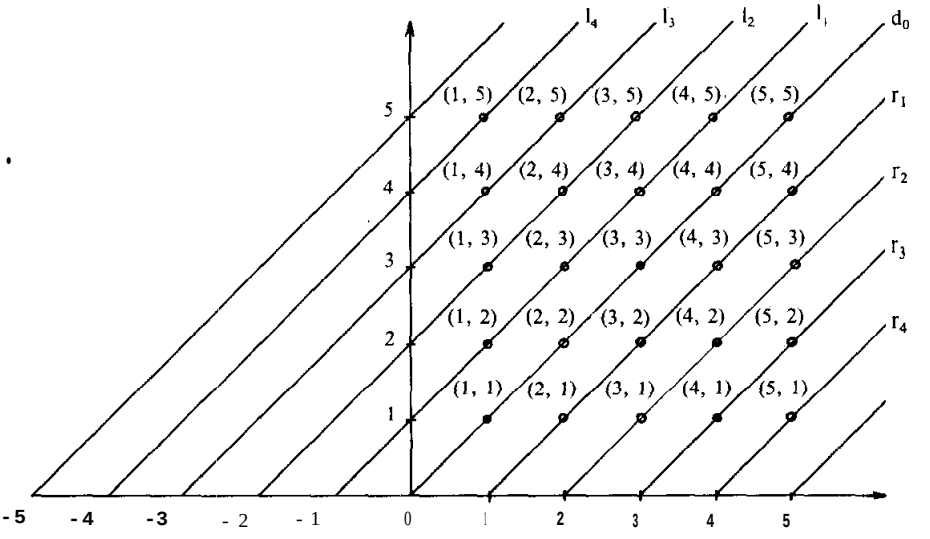
พิสูจน์ ให้ทำเป็นแบบฝึกหัด

หมายเหตุ เมื่อกล่าวถึงจำนวนเต็มจำนวนใดจำนวนหนึ่ง (สมาชิกของ Z) เราคุ้นเคยกับการใช้อักษรตัวเดียวแทนสมาชิกดังกล่าว นั่นคือเราใช้ $x \in Z$ ซึ่งหมายความว่า x เป็นตัวแทนของ equivalence class ซึ่งอยู่ในรูป $[a, b]$ สำหรับ $a, b \in N$ ตัวอย่างเช่น

$$\{(1, 1), (2, 2), (3, 3), \ldots\} = \{(a, a)/a \in N\} = 0$$
$$\{(2, 1), (3, 2), (4, 3), \ldots\} = \{(a+1, a)/a \in N\} = 1$$
$$\{(3, 1), (4, 2), (5, 3), \ldots\} = \{(a+2, a)/a \in N\} = 2$$
$$\{(4, 1), (5, 2), (6, 3), \ldots\} = \{(a+3, a)/a \in N\} = 3$$

$$\{(1, 2), (2, 3), (3, 4), \ldots\} = \{(a, a+1)/a \in N\} = -1$$
$$\{(1, 3), (2, 4), (3, 5), \ldots\} = \{a, a+2/a \in N\} = -2$$

ซึ่งเราเขียนแทนด้วยกราฟได้ดังนี้



นั่นคือ

เส้นแนวทแยงมุม d_0 แทน

$\{(1, 1), (2, 2), (3, 3), \ldots\}$

เส้นแนวทแยงมุม r_1 แทน

$\{(2, 1), (3, 2), (4, 3), \ldots\}$.

เส้นแนวทแยงมุม r_2 แทน

$\{(3, 1), (4, 2), (5, 3), \ldots\}$

เส้นแนวทแยงมุม l_1 แทน

$\{(1, 2), (2, 3), (3, 4), \ldots\}$

เส้นแนวทแยงมุม l_2 แทน

$\{(1, 3), (2, 4), (3, 5), \ldots$I

เราจะแทนจำนวนเต็มตามแนวทแยงมุม d_0 ด้วยจำนวนเต็ม 0 (ศูนย์)

แทนจำนวนเต็มแนวทแยงมุม $r_1, r_2, r_3, \ldots$ ด้วย 1, 2, 3, ... ตามลำดับ

แทนจำนวนเต็มแนวทแยงมุม $l_1, l_2, l_3, \ldots$ ด้วย $-1, -2, -3, \ldots$ ตามลำดับ

และเรียกจำนวนเต็มที่อยู่ใต้เส้น d_0 ว่า จำนวนเต็มบวก (positive integers) หรือจำนวนนับ แทนด้วยสัญลักษณ์ Z^+

เรียกจำนวนเต็มที่อยู่เหนือเส้น d_0 ว่า จำนวนเต็มลบ (negative integers) แทนด้วย Z^-

แบบฝึกหัดที่ 2.1

1. จงพิจารณาว่า คู่ลำดับต่อไปนี้ แทนจำนวนเต็มเดียวกันหรือไม่

   1.1 (6, 4) และ (5, 2)

   1.2 (9, 9) และ (17, 17)

   1.3 (35, 67) และ (67, 35)

   1.4 (23, 27), (27, 31)

   1.5 $(a+3c, a)$ และ $(a, a+4c)$ ซึ่ง $a, c \in N$

2. จงเขียนจำนวนเต็มในรูปของคู่ลำดับแบบอื่น ๆ อีก 3 แบบ

   2.1 (15, 4)

   2.2 (7, 11)

   2.3 (6, 6)

   2.4 (91, 23)

3. จงหาผลบวกและผลคูณของจำนวนเต็มต่อไปนี้

   3.1 $[9, 2]$ และ $[13, 10]$

   3.2 $[70, 100]$ และ $[2, 7]$

   3.3 $[37, 46]$ และ $[28, 14]$

   3.4 $[a+3c, a]$ และ $[a, a+4c]$

4. จงพิสูจน์ทฤษฎีบท 2.1.3 ข้อ 2
5. จงพิสูจน์ทฤษฎีบท 2.1.4 ข้อ 2
6. จงพิสูจน์ทฤษฎีบท 2.1.5 ข้อ 1
7. จงพิสูจน์ทฤษฎีบท 2.1.6 ข้อ 2
8. จงพิสูจน์ทฤษฎีบท 2.1.7
9. จงพิสูจน์ทฤษฎีบท 2.1.13
10. จงพิสูจน์ทฤษฎีบท 2.1.14

2.2 ห.ร.ม. และ ค.ร.น.

ในหัวข้อ 2.1 เรานิยามการบวกและการคูณของจำนวนเต็มมาแล้ว ดังนั้นเราสามารถนำการคูณมาใช้นิยามบางสิ่งบางอย่างได้ กล่าวคือ สำหรับ $a, b \in Z$ ถ้าสามารถหา $n \in Z$ ซึ่งทำให้ $b = na$ แล้ว เรากล่าวว่า a หาร b ลงตัว และเรียก n ว่าเป็นผลหาร ซึ่งการหารได้นำไปสู่คุณสมบัติต่าง ๆ ที่เราจะศึกษาอีกมากมาย

นิยาม 2.2.1 สำหรับแต่ละ $a, b \in Z$ เราจะกล่าวว่า a หาร b ลงตัว (แทนด้วยสัญลักษณ์ $a|b$) ก็ต่อเมื่อมีจำนวนเต็ม n จำนวนเดียว ซึ่งทำให้ $b = na$
เราจะใช้สัญลักษณ์ $\nmid$ แทนการหารไม่ลงตัว

พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง 2.2.1

$2|6$ เพราะว่ามี $3 \in Z$ ซึ่งทำให้ $6 = (3), (2)$
$-5|30$ เพราะว่ามี $6 \in Z$ ซึ่งทำให้ $30 = (-6)(-5)$
$7|-56$ เพราะว่ามี $-8 \in Z$ ซึ่งทำให้ $-56 = (-8)(7)$
$3 \nmid 4$ เพราะว่าไม่มี $n \in Z$ ซึ่งทำให้ $4 = n(3)$

ถ้าเราใช้คู่ลำดับแทนจำนวนเต็ม จากนิยาม 2.2.1 จะได้ว่า

สำหรับแต่ละ $[a, b], [c, d] \in Z$
$[a, b] \| [c, d]$ ก็ต่อเมื่อมี $[e, f]$ ซึ่งทำให้

$$[c, d] = [e, f] \cdot [a, b]$$

จากตัวอย่าง 2.2.1 $2|6$ โดยเขียนเป็นพวกของคู่ลำดับ จะได้ว่า

$[4, 2] \| [12, 6]$ ก็ต่อเมื่อมี $[e, f]$ ซึ่ง

$$[12, 6] = [e, f] \cdot [4, 2]$$
$$= [4e + 2f, 2e + 4f]$$
$$(12, 6) \sim (4e + 2f, 2e + 4f)$$

นั่นคือ $12 + 2e + 4f = 6 + 4e + 2f$
ทำให้ได้ $6 + 2f = 2e$
ถ้าสังเกตจะพบว่า $c = 6$ และ $f = 3$ เป็นคำตอบหนึ่งของสมการข้างต้น ฉะนั้น

$$[12, 6] = [6, 3] \cdot [4, 2]$$

แต่เรามีคำตอบอื่นอีก เช่น $e = 7$ และ $f = 4$ หรือ $[7, 4]$ ซึ่ง $[6, 3] = [7, 4]$ คือแทน

จำนวนเต็มเดียวกัน

เพราะฉะนั้น $[4, 2]|[12, 6]$ เพราะมี $[e, f]$ (โดยที่ $6+2f = 2e$)

ซึ่งทำให้ $[12, 6] = [e, f]\cdot[4, 2$

จากตัวอย่างข้างต้นจะพบว่า การใช้อักษรตัวเดียวแทนจำนวนเต็ม จะสะดวกและกะทัดรัดกว่าใช้พวกของคู่ลำดับ

ก่อนจะกล่าวถึงคุณสมบัติของการหาร ขอให้พิจารณาตัวอย่างต่อไปนี้

ตัวอย่าง 2.2.2. ถ้า $a \neq 0$ จงพิจารณาความเป็นไปได้ของ

1) $a|0$ 2) $0|a$ 3) $0|0$

วิธีทำ 1) เนื่องจาก $a|0$ ก็ต่อเมื่อ $0 = na$ โดยที่ $a \neq 0$ นั่นคือมี $n = 0$ เพราะฉะนั้น $a|0$ มีความหมายได้

2) พิจารณา $0|a$ ก็ต่อเมื่อ $a = n\cdot 0$ จะพบว่า $n\cdot 0 + 0$ สำหรับทุก $n \in Z$ แต่ $a \neq 0$ ซึ่งเป็นไปไม่ได้ เพราะฉะนั้น $0|a$ เป็นอนิยาม (undefined) หรือไม่นิยาม

3) พิจารณา $0|0$ ก็ต่อเมื่อ $0 = n\cdot 0$ ซึ่งเราพบว่า สมการ $0 = n\cdot 0$ เป็นจริงทุก $n\in Z$ ดังนั้น $0|0$ เป็นอนิยาม

ต่อไปจะเป็นคุณสมบัติเบื้องต้นของการหาร ซึ่งเป็นผลโดยตรงมาจากนิยาม

ทฤษฎีบท 2.2.1 สำหรับแต่ละ $a \in Z$

1) $a|a$ 2) $1|a$ และ 3) $a|0$

พิสูจน์ 1) เนื่องจาก $a = 1\cdot a$

ดังนั้นจากนิยาม เราสรุปว่า $a|a$ (ได้โดยที่ $n = 1$)

2) เนื่องจาก $a = a\cdot 1$

ดังนั้นจากนิยาม เราได้ว่า $1|a$ (โดย $n = a$)

3) เนื่องจาก $a = 0\cdot a$

ดังนั้นจากนิยาม เราได้ว่า $a|0$ (โดย $n = 0$)

ตัวอย่าง 2.2.2

$5|5,\ -3|-3,\ 1|6,\ 1|-7,\ 2|0$ และ $-6|0$

ทฤษฎีบท 2.2.2 ถ้า $ab \in Z$ และ a/b แล้ว

1) $-a/b$ 2) $a/-b$ 3) $-a|-b$

พิสูจน์ I) เนื่องจาก a|b

เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

$= (-n)(-a)$

$b = (-n)(-a)$ สำหรับ $-n \in Z$

นั่นคือ $-a|b$ นิยาม 2.2.1

2) เนื่องจาก a|b

เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

หรือ $-b = -na$

$= (-n)(a)$ สำหรับ $-n \in Z$

นั่นคือ a l -b นิยาม 2.2.1

3) เนื่องจาก a|b

เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

หรือ $-b = -na$

$= n(-a)$ สำหรับ $n \in Z$

นั่นคือ -a l -b #

ตัวอย่าง 2.2.3 เนื่องจาก 3|6 ดังนั้น เราได้ว่า

1) $-3|6$ 2) $3|-6$ 3) $-3|-6$

ทฤษฎีบท 2 . 2 . 3 ถ้า a|b และ b|c แล้ว a|c

(นั่นคือ การหารมีคุณสมบัติการถ่ายทอด)

พิสูจน์ เนื่องจาก a|b เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

และ b|c ดังนั้น $c = mb$ สำหรับ $m \in Z$

จากสองสมการข้างต้น ทำให้ได้ว่า

$c = m(na)$

$= (mn)a$ สำหรับ $mn \in Z$

นั่นคือ a|c นิยาม 2.1.1

ตัวอย่าง 2.2.4 เนื่องจาก 3|6 และ 6|24 ดังนั้น 3124

ทฤษฎีบท 2.2.4 ac|bc ก็ต่อเมื่อ a|b

พิสูจน์ จากนิยามการหาร, $ac \neq 0$

เพราะฉะนั้น $a \neq 0$ และ $c \neq 0$

เนื่องจาก $ac|bc$

เพราะฉะนั้น $bc = nac$ สำหรับ $n \in Z$

หรือ $b = na$

นั่นคือ $a|b$

ตัวอย่าง 2.2.5 $6|24$ $(3 \cdot 2|12 \cdot 2)$ ก็ต่อเมื่อ $3|12$

ทฤษฎีบท 2.2.5 ถ้า $a|b$ แล้ว $a|bx$, $x \in Z$

พิสูจน์ เนื่องจาก $a|b$

เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

$bx = nax$

$= (nx)a$ สำหรับ $nx \in Z$

นั่นคือ $a|bx$

ตัวอย่าง 2.2.6 ถ้า $4|12$ แล้ว $4|36$ (โดย $x = 3$)

ทฤษฎีบท 2.2.6 ถ้า $a|b$ และ a/c แล้ว

1) $a|(b+c)$ 2) $a|(b-c)$

พิสูจน์ 1) เนื่องจาก $a|b$ เพราะฉะนั้น $b = na$ สำหรับ $n \in Z$

และ $a|c$ เพราะฉะนั้น $c = ma$ สำหรับ $m \in z$

ทำให้ได้ว่า $b + c = na + ma$

$= (n+m)a$ สำหรับ $n+m \in Z$

นั่นคือ $a|(b+c)$

2) ให้ทำเป็นแบบฝึกหัด

ตัวอย่าง 2.2.7 เพราะว่า $2|8$ และ $2|16$ ดังนั้น $2|(8+16)$ และ $2|(8-16)$

ทฤษฎีบท 2.2.7 ถ้า a/b และ $a|c$ แล้ว $a|(bx+cy)$ สำหรับทุก $x, y \in Z$

พิสูจน์ ให้ทำเป็นแบบฝึกหัด

เราทราบว่า $2|6$ (2 หาร 6 ลงตัว) เพราะว่ามี $3 \in Z$ ซึ่ง $6 = 3.2$ แต่ $3 \nmid 4$ (3 หาร 4

ไม่ลงตัว) เนื่องจากไม่สามารถหา $n \in Z$ ซึ่งทำให้ $4 = n \cdot 3$ แต่เราสามารถเขียนให้อยู่ในรูป $4 = 1 \cdot 3 + 1$ ได้ โดยที่ $0 \leqslant 1 < 3$ ทำนองเดียวกัน $8 \nmid 42$ แต่เขียนได้ในรูป

$$42 = 5 \cdot 8 + 2 \qquad \text{โดยที่} \quad 0 \leqslant 2 < 8$$

หรือ

$$42 = 8 \cdot 5 + 2 \qquad \text{โดยที่} \quad 0 \leqslant 2 < 8$$

และสำหรับ $7 \nmid 48$ เขียนได้เป็น

$$48 = 7 \cdot 6 + 6 \ , \quad 0 \leqslant 6 < 7$$

สำหรับ $2 | 6$ เราก็สามารถเขียนได้เป็น

$$6 = 2 \cdot 3 + 0 \ , \quad 0 \leqslant 0 < 2$$

ทฤษฎีบท 2.2.8 ขั้นตอนวิธีหาร (Division Algorithm)

สำหรับแต่ละ $a, b \in Z^+$ ซึ่ง $a \neq 0$ จะได้ว่า มีจำนวนเต็ม q, r เพียงคู่เดียว ซึ่ง

$$b = aq + r \quad \text{โดย} \quad 0 \leqslant r < a$$

พิสูจน์ การพิสูจน์แบ่งเป็น 2 ขั้นตอน คือ

1) ต้องพิสูจน์ว่า มีจำนวนเต็ม q และ r ซึ่งสอดคล้องสมการ

$$b = aq + r \quad \text{โดย} \quad 0 \leqslant r < a$$

2) ต้องพิสูจน์ว่ามี q และ r เพียงคู่เดียว

1) ให้ $S = \{b - ax / x \in Z, b - ax \geqslant 0\}$

โดยที่ a และ b มีค่าแน่นอนไม่แปรเปลี่ยน ดังนั้น S เป็นเซตของจำนวนเต็มที่ไม่เป็นลบในรูป $b - ax$ โดย x มีค่าแปรเปลี่ยนไป สำหรับ $x = 0, b - ax - b > 0$ ดังนั้น $b \in S$

นั่นคือ S ไม่เป็นเซตว่าง

จากคุณสมบัติ well-ordering ของจำนวนเต็มที่ไม่เป็นลบ S ต้องมีสมาชิกที่มีค่าน้อยที่สุด, ให้เป็น r นั่นคือ $r \in S$ ฉะนั้นต้องมี $q \in Z$ ซึ่งทำให้ $b - aq = r$ หรือ $b = aq + r$ โดย $0 \leqslant r$

ต่อไปจะแสดงว่า $r < a$, โดยใช้วิธีการขัดแย้ง

สมมติ $r \geqslant a$ ดังนั้น $r - a \geqslant 0$

และ $r - a = (b - aq) - a$

$= b - a(q + 1)$, ซึ่งอยู่ในรูป $b - ax \geqslant 0$

แสดงว่า $r - a \in S$ แต่ a เป็นบวก, $r > r - a$ ซึ่งขัดแย้งกับที่ว่า r เป็นสมาชิกที่มีค่าน้อยที่สุดของ S

ดังนั้นสรุปได้ว่า $r < a$

2) สมมติว่ามีจำนวนเต็มอีกคู่หนึ่ง คือ q_1 และ r_1 ซึ่ง

$$b = aq_1 + r_1 \quad \text{โดย} \quad 0 \leq r_1 < a$$

ดังนั้น $aq_1 + r_1 = aq + r$

$$a(q_1 - q) = r - r_1$$

จะไม่มีการสูญเสียอะไร ถ้าเราจะให้ $q_1 \geq q$

(กรณี $q_1 < q$ เราสามารถเขียนสมการในรูป $a(q - q_1) = r_1 - r$ แล้วดำเนินการพิสูจน์เหมือนกับที่จะทำดังต่อไปนี้)

ดังนั้น $q_1 - q \geq 0$, ถ้า $q_1 - q \neq 0$ แล้ว $q_1 - q \geq 1$

ซึ่งทำให้ $r - r_1 = b - aq - (b_1 - aq_1)$

$= a(q_1 - q) \geq a$

แต่เนื่องจาก $r < a$ และ $r_1 < a$

นั่นคือ $r - r_1 < 0$

ฉะนั้นที่ได้ว่า $r - r_1 \geq a$ $(a \in Z^+)$ จึงเป็นไปไม่ได้

เพราะฉะนั้น $q_1 - q = 0$

ผลที่ตามมาคือ $r_1 - r = 0$

นั่นคือ $q_1 = q$ และ $r_1 = r$

หมายเหตุ

1) ทฤษฎีบทนี้สามารถขยายได้เป็น สำหรับ $a, b \in Z$ ซึ่ง $a \neq 0$ จะมีจำนวนเต็ม q, r เพียงคู่เดียวที่ทำให้

$$b = aq + r \quad \text{โดย} \quad 0 \leq r < |a|$$

หรืออาจเขียนอีกแบบว่า

สำหรับ $a > 0$, $b = aq + r$, $0 \leq r < a$

สำหรับ $a < 0$, $b = aq + r$, $0 \leq r < -a$

เราจะไม่พิสูจน์ในที่นี้

2) เราเรียก q ว่าผลหาร (quotient) และเรียก r ว่า เศษเหลือ (remainder)

ตัวอย่าง 2.2.8 จงหา q และ r ซึ่ง $b = aq + r$, $0 \leq r < |a|$

1) $a = 2$, $b = 13$

2) $a = 6$, $b = -31$

3) $a = -4$, $b = 34$

4) $a = 13$, $b = 0$

วิธีทำ 1) เนื่องจาก $13 = 2\cdot 6+1,\ 0 \leqslant 1 < 2$

ดังนั้น $q = 6$ และ $r = 1$

2) เนื่องจาก $-31 = 6(-6)+5,\ 0 \leqslant 5 < +6$

ดังนั้น $q = -6$ และ $r = 5$

3) เนื่องจาก $34 = (-4)(-8)+2,\ 0 \leqslant 2 < |-4|$

ดังนั้น $q = -8$ และ $r = 2$

4) เนื่องจาก $0 = (-13)\cdot 0+0,\ 0 \leqslant 0 < |-13|$

ดังนั้น $q = 0$ และ $r = 0$

นิยาม 2.2.2 จำนวนเต็มบวก d จะเรียกว่า เป็นตัวหารร่วมมาก (Greatest common division เขียนย่อว่า ห.ร.ม.) ของจำนวนเต็ม a และ b ก็ต่อเมื่อ

1. $d|a$ และ $d|b$
2. ถ้า $c|a$ และ $c|b$ แล้ว $c|d$

เราใช้สัญลักษณ์ (a, b) แทน ห.ร.ม. ของ a และ b

ดังนั้น $(a, b) = d$

และอย่าสับสนกับคู่ลำดับ (a, b)

ตัวอย่าง 2.2.9 กำหนด $a = 4$ และ $b = 20$

จำนวนเต็มที่หาร 4 และ 20 ลงตัว คือ $\pm 1, \pm 2$ และ ± 4 แต่ $\pm 1, \pm 2$ ต่างก็หาร ± 4 ลงตัว และ ห.ร.ม. ต้องเป็นจำนวนเต็มบวก

ดังนั้น ห.ร.ม. ของ 4 และ 20 คือ 4

$$(4, 20) = 4$$

ข้อสังเกต

1. เงื่อนไขของ ห.ร.ม. ข้อแรกบอกว่า d ต้องหาร a และ b ลงตัว ส่วนข้อสองบอกว่า ถ้ามีจำนวนเต็มอื่นที่หาร a และ b ลงตัวแล้ว จำนวนเต็มนั้นต้องหาร d ลงตัวด้วย นั่นคือ d ต้องมีค่ามากกว่าตัวหารอื่น ๆ (เป็นตัวหารที่มากที่สุดที่หาร a และ b ลงตัว)

2. ถ้าทั้ง $a = 0$ และ $b = 0$ แล้ว ห.ร.ม. ของ a และ b จะหาค่าไม่ได้ เพราะว่า $d|0$ เสมอ แต่ถ้ามี $c|0$ แล้ว $c|d$ อาจจะไม่จริง เช่น $5|0$ และ $3|0$ แต่ $3 \nmid 5$

3. ถ้า $b = 0$ แล้ว $(a, 0) = a$

4. ถ้า $a|b$ แล้ว $(a, b) = |a|$

5. $(a, b) = (b, a)$

6. $(a, b) = (-a, b) = (a, -b) = (-a, -b)$

ทฤษฎีบท 2.2.9 สำหรับจำนวนเต็ม a และ b ซึ่งไม่เป็นศูนย์พร้อมกัน จะมีจำนวนเต็มบวก d ซึ่ง $d = (a, b)$ และยังได้ว่า $d = am + bn$ สำหรับบาง $m, n \in Z$

พิสูจน์ ให้ $S = \{ax + by / x, y \in Z, ax + by > 0\}$

พิจารณา $x = a$ และ $y = b$ จะได้ว่า $a^2 + b^2 \in S$ โดยที่ $a^2 + b^2 > 0$

ดังนั้น $S \neq \phi$

จากคุณสมบัติ well-ordering ของจำนวนเต็มบวก แสดงว่า S มีสมาชิกที่มีค่าน้อยที่สุด, ให้เป็น d ดังนั้น $d = am + bn$ สำหรับบาง $m, n \in Z$

ต่อไปจะแสดงว่า d เป็น ห.ร.ม. ของ a และ b นั่นคือ ต้องสอดคล้องคุณสมบัติสองข้อตามนิยาม 2.2.2

1) จะต้องพิสูจน์ว่า $d|a$

จากขั้นตอนวิธีหารในทฤษฎีบท 2.2.8 สำหรับจำนวนเต็ม a และ d จะมีจำนวนเต็ม q และ r ซึ่ง

$$a = qd + r, \quad 0 \leq r < d$$
$$= q(am + bn) + r$$

หรือ $r = a - aqm - bqn$

$= a(1 - qm) + b(-qn)$ (ซึ่งอยู่ในรูป $ax + by$)

ถ้า $r \neq 0$ แล้ว $r \in S$, โดยที่ $r > d$ (เนื่องจาก d เป็นสมาชิกที่มีค่าน้อยที่สุด) ซึ่งเป็นไปไม่ได้ (เพราะว่า $r < d$)

เพราะฉะนั้น $r = 0$, ทำให้ $a = qd$ แสดงว่า $d|a$

ส่วนกรณี $d|b$ ก็พิสูจน์ทำนองเดียวกัน

2) ต้องพิสูจน์ว่า ถ้า $c|a$ และ $c|b$ แล้ว $c|d$

สมมติให้ $c|a$ และ $c|b$

จาก $c|a$ ดังนั้น มี $u \in Z$ ซึ่ง $a = uc$

และจาก $c|b$ ดังนั้น มี $v \in Z$ ซึ่ง $b = vc$

เนื่องจาก $d = am + bn$

$= (uc)m + (vc)n$

$$= c(um + vn)$$

นั่นคือ $c \mid d$ โดยที่ $um + vn \in Z$

จากทฤษฎีบทนี้ทำให้เราทราบว่า สำหรับจำนวนเต็มสองจำนวนที่ไม่เป็นศูนย์พร้อมกัน จะมี ห.ร.ม. แน่ ๆ แต่ไม่ได้กล่าวถึงวิธีหา ห.ร.ม. ถ้าเป็นจำนวนที่มีค่าน้อย ๆ เราสามารถพิจารณาหา ห.ร.ม. ตามนิยาม 2.2.2 ได้ แต่ถ้าจำนวนมีค่ามาก ๆ จะทำให้การหา ห.ร.ม. ลำบากขึ้น ดังนั้น เราจะมาพิจารณาขบวนการหา ห.ร.ม. ซึ่งเรียกว่า **ขั้นตอนวิธียูคลิด** (Euclidean Algorithm)

สำหรับจำนวนเต็ม a และ b ที่ไม่เป็นศูนย์พร้อมกัน

เนื่องจาก $(a, b) = (-a, b)$ ดังนั้นเราอาจสมมติว่า a เป็นจำนวนเต็มบวก โดยไม่สูญเสียอะไร จากขั้นตอนวิธีหาร ทำให้ได้ว่า ต้องมีจำนวนเต็ม q_1 และ r_1 ซึ่ง

$$a = bq_1 + r_1 , \quad 0 \leqslant r_1 < b$$

ถ้า $r_1 \neq 0$, พิจารณาเศษเหลือ r_1 และตัวหารเดิม b และจากขั้นตอนวิธีหารจะได้ว่า ต้องมีจำนวนเต็ม q_2 และ r_2 ซึ่ง

$$b = r_1q_2 + r_2 , \quad 0 \leqslant r_2 < r_1$$

ต่อไปพิจารณาเศษเหลือ r_2 และตัวหารในขั้นตอนที่แล้วคือ r_1 โดยขบวนการนี้ ทำต่อไปเรื่อย ๆ จนกระทั่งเศษเหลือเป็นศูนย์ ซึ่งเขียนขั้นตอนได้ดังนี้

(1)	$a = bq_1 + r_1$,		$0 < r_1 < b$
(2)	$b = r_1q_2 + r_2$,		$0 < r_2 < r_1$
(3)	$r_1 = r_2q_3 + r_3$,		$0 < r_3 < r_2$
$(k-1)$	$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$,		$0 < r_{k-1} < r_{k-2}$
(k)	$r_{k-2} = r_{k-1}q_k + r_k$,		$0 < r_k < r_{k-1}$
$(k+1)$	$r_{k-1} = r_kq_{k+1} + r_{k+1} + 0$		

เราต้องได้เศษเหลือเป็นศูนย์แน่นอนในขั้นตอนสุดท้าย เนื่องจาก $r_1, r_2, \ldots, r_k$ มีค่าเป็นจำนวนเต็มบวก และ $r_1 > r_2 > r_3 > \ldots > r_{k-1} > r_k$

ทฤษฎีบท 2.2.10 ขั้นตอนวิธียูคลิด

เศษเหลือตัวสุดท้ายที่ไม่เป็นศูนย์ในขั้นตอนวิธียูคลิด คือ ห.ร.ม. ของ a และ b

พิสูจน์ เราต้องแสดงว่า $r_k = (a, b)$ นั่นคือ ต้องพิสูจน์ว่า

1) $r_k|a$ และ $r_k|b$

2) ถ้า $c|a$ และ $c|b$ แล้ว $c|r_k$

1) จากขั้นตอนที่ $(k+1)$ แสดงว่า $r_k|r_{k-1}$

เนื่องจาก $r_{k-1}|r_{k-1}q_k$

ดังนั้น $r_k|r_{k-1}q_k$ (จากทฤษฎีบท 2.2.3)

และเราทราบว่า $r_k|r_k$

เพราะฉะนั้น $r_k|(r_{k-1}q_k + r_k)$ (จากทฤษฎีบท 2.2.6)

นั่นคือ $r_k|r_{k-2}$ (เนื่องจาก $r_{k-2} = r_{k-1}q_k + r_k$ ตามขั้นตอนที่ k)

ทำนองเดียวกัน เราสามารถแสดงว่า $r_k|r_{k-3}$ ได้ดังนี้

เนื่องจาก $r_k|r_{k-2}$ และ $r_{k-2}|r_{k-2}q_{k-1}$

ดังนั้น $r_k|r_{k-2}q_{k-1}$ (จากทฤษฎีบท 2.2.3)

และจากขั้นตอนที่ $(k+1)$, $r_k|r_{k-1}$

เพราะฉะนั้น $r_k|r_{k-2}q_{k-1} + r_{k-1}$ (ทฤษฎีบท 2.2.6)

นั่นคือ $r_k|r_{k-3}$ (จากขั้นตอนที่ $k-1$)

ด้วยวิธีการนี้ ทำย้อนขึ้นไปเรื่อย ๆ ในที่สุดจะได้ $r_k|r_2$ และ $r_k|r_1$

ดังนั้น $r_k|b$ (จากขั้นตอนที่ 2)

และ $r_k|a$ (จากขั้นตอนที่ 1)

2) สมมติว่า $c|a$ และ $c|b$

จากขั้นตอนที่ 1, $r_1 = a - bq_1$

แต่ $c|a$ และ $c|bq_1$ (เพราะว่า $c|b$)

ดังนั้น $c|(a - bq_1)$ หรือ $c|r_1$

จากขั้นตอนที่ 2, $r_2 = b - r_1q_2$

เนื่องจาก $c|r_1$ และ $r_1|r_1q_2$ ดังนั้น $c|r_1q_2$

และจาก $c|b$

เพราะฉะนั้น $c|(b - r_1q_2)$ หรือ $c|r_2$

ทำเช่นนี้ไปเรื่อย ๆ สุดท้ายจะได้ $c|r_k$

ตัวอย่าง 2.2.10 จงหา ห.ร.ม. ของ 422 และ 68

วิธีทำ เนื่องจาก $422 = 68 \cdot 6 + 14$

$68 = 14 \cdot 4 + 12$

$14 = 12 \cdot 1 + 3$

$12 = 2 \cdot 6 + 0$

ดังนั้น ห.ร.ม. ของ 422 และ 68 คือ 2

นั่นคือ $(422, 68) = 2$

จากนิยาม 2.2.1 เรานิยามการหารลงตัวว่า $a|b$ ก็ต่อเมื่อ $b = na$, $n \in Z$ ซึ่งกรณีเรากล่าวว่า a เป็นตัวหาร (divisor) ของ b และเรียก b ว่า เป็นพหุคูณ (multiple) ของ a

นั่นคือ สำหรับจำนวนเต็ม a และ b ใด ๆ เราเรียก b ว่า เป็นพหุคูณของ a ถ้ามีจำนวนเต็ม c ซึ่งทำให้ $b = ac$

นิยาม 2.2.3 จำนวนเต็มบวก m จะเรียกว่า เป็นตัวคูณร่วมน้อย (least common multiple, เขียนย่อว่า ค.ร.น.) ของจำนวนเต็ม a และ b ก็ต่อเมื่อสอดคล้องกับคุณสมบัติสองข้อ

1. m เป็นพหุคูณของ a และ m เป็นพหุคูณของ b
2. ถ้า n เป็นพหุคูณของ a และเป็นพหุคูณของ b แล้ว n ต้องเป็นพหุคูณของ m ด้วย

เราจะใช้สัญลักษณ์ $[a, b]$ แทน ค.ร.น.ของ a และ b

นั่นคือ $[a, b] = n$

และอย่าสับสนกับพวกของคู่ลำดับ

หมายเหตุ เนื่องจากเราคุ้นเคยกับการหารมามากแล้ว ฉะนั้นจากนิยามของ ค.ร.น. เราจึงใช้ $a|m$ แทนข้อความ m เป็นพหุคูณของ a เพราะฉะนั้น คุณสมบัติของ ค.ร.น. คือ

1. $a|m$ และ $b|m$
2. ถ้า $a|n$ และ $b|n$ แล้ว $m|n$

ซึ่งจะสังเกตเห็นว่า ค.ร.น. ก็คือ จำนวนเต็มบวกที่น้อยที่สุดที่ทั้ง a และ b หารลงตัว

ตัวอย่าง 2.2.11 จงหา ค.ร.น. ของ 4 และ 10

วิธีทำ ในที่นี้ $a = 4$ และ $b = 10$

เนื่องจาก $4|20$ และ $10|20$

$4|40$ และ $10|40$

$4|60$ และ $10|60$

นั่นคือ จำนวนเต็มบวกที่ทั้ง 4 และ 10 หารลงตัว คือ 20, 40, 60, ... แต่ $20|40$, $20|60$

ดังนั้น ค.ร.น. คือ 20 (จำนวนเต็มบวกที่น้อยที่สุดที่ a และ b หารลงตัว)

เพราะฉะนั้น $[4, 10] = 20$

และในทำนองเดียวกับ ห.ร.ม. จะได้ว่า

$$[a, b] = [-a, b] = [a, -b] = [-a, -b]$$

ทฤษฎีบท 2.2.11 สำหรับแต่ละ $a, b \in Z^+$ จะได้ว่า

$$[a, b] \cdot (a, b) = ab$$

โดยที่ (a, b) เป็น ห.ร.ม. ของ a และ b

ซึ่งเราจะไม่พิสูจน์ในที่นี้

ตัวอย่าง 2.2.11 จงหา ค.ร.น. ของ 128 และ 136 ถ้า ห.ร.ม. ของจำนวนทั้งสองคือ 8

วิธีทำ เนื่องจาก $[128, 136] \cdot (128, 136) = (128)(136)$

ดังนั้น $[128, 136] \cdot 8 = 128 \times 136$

นั่นคือ $(128, 136] = \frac{128.136}{8}$

$= 2,176$

แบบฝึกหัด 2.2

1. สำหรับแต่ละคู่ของจำนวนเต็มที่กำหนดให้ จงหา q และ r ซึ่งสอดคล้องขั้นตอนวิธีหาร

   1.1) 162, 49 1.2) 213, 114

   1.3) 1032, -25 1.4) -7, -40

2. จงพิสูจน์ทฤษฎีบท 2.2.6 ส่วนที่สอง
3. จงพิสูจน์ทฤษฎีบท 2.2.7
4. จงพิสูจน์ว่า ถ้า $a|b$ และ $b|a$ แล้ว $a = b$ หรือ $a = -b$
5. จงพิสูจน์ว่า ถ้า a/b และ $|b| < |a|$ แล้ว $b = 0$
6. จงหา ห.ร.ม. และ ค.ร.น. ของแต่ละคู่ของจำนวนเต็มที่กำหนดให้

   6.1) 103 และ 62 6.2) 201 และ -1014

   6.3) -478 และ 212 6.4) -1024 และ -361

7. จงพิสูจน์ว่า ถ้า $d = (a, b)$ แล้ว $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
8. จงพิสูจน์ว่า ถ้า $a|bc$ และ $(a, b) = 1$ แล้ว $a|c$ (Euclid Lemma)

2.3 สมการไดโอแฟนไทน์ (Diophantine Equation)

ในหัวข้อนี้จะพิจารณาปัญหาที่น่าสนใจปัญหาหนึ่งในเรื่องของทฤษฎีจำนวน ซึ่งลักษณะของปัญหาเป็นดังนี้ ชายคนหนึ่งซื้อของชนิดแรกราคาหน่วยละ 70 บาท และซื้อของชนิดที่สองราคาหน่วยละ 50 บาท ใช้เงินไปทั้งหมด 530 บาท อยากทราบว่าเขาซื้อของมาชนิดละกี่หน่วย ?

ถ้าเราสมมติว่า ซื้อของชนิดแรกมาทั้งหมด x หน่วย

และซื้อของชนิดที่สองมา y หน่วย

ดังนั้น เราตั้งสมการได้ในรูป

$$70x + 50y = 530$$

หรือ

$$7x + 5y = 53$$

ถ้าตัวไม่ทราบค่า (ทั้ง x และ y) ไม่จำกัดว่าต้องเป็นจำนวนเต็ม เราอาจสมมติค่า y แล้วแก้สมการหาค่า x ได้มากมาย แต่ลักษณะสมการนี้ต้องการคำตอบที่เป็นจำนวนเต็ม ซึ่งเราเรียกสมการประเภทนี้ว่า สมการไดโอแฟนไทน์ เช่น $ax + by = c$, $ax + by + cz + d = 0$, $x^2 + y^2 = z^2$ เป็นต้น สำหรับที่นี้เราจะพิจารณาเฉพาะแบบ $ax + by = c$ ซึ่งเป็นแบบเชิงเส้นสองตัวแปรเท่านั้น อนึ่ง สำหรับปัญหาข้างต้นเราจะกลับมาพิจารณาหาคำตอบอีก หลังจากเรารู้วิธีหาคำตอบแล้ว

ก่อนอื่นขอให้พิจารณาสมการ $2x + 3y = 18$ จะพบว่ามีคำตอบมากมายดังนี้

$$2(3) + 3(4) = 18$$
$$2(-3) + 3(8) = 18$$
$$2(12) + 3(-2) = 18$$

แต่ถ้าเราพิจารณาสมการอื่น เช่น $2x + 4y = 17$ จะพบว่าไม่สามารถหาคำตอบที่เป็นจำนวนเต็มได้เลย ทั้งนี้เนื่องจากว่าทางขวามือเป็นจำนวนคี่ ในขณะที่ซ้ายมือเป็นจำนวนคู่ ไม่ว่าจะแทน x และ y ด้วยจำนวนเต็มใดก็ตาม เพราะฉะนั้นเราจึงมาพิจารณาว่า เมื่อใดสมการในรูป $ax + by = c$ จึงจะมีคำตอบ และถ้ามีจะหาคำตอบได้อย่างไร

ทฤษฎีบท 2.3.1 สมการไดโอแฟนไทน์เชิงเส้น $ax + by = c$ มีคำตอบก็ต่อเมื่อ $d|c$ โดยที่ $d = (a, b)$ (d เป็น ห.ร.ม. ของ a และ b) และถ้า x_0, y_0 เป็นคำตอบหนึ่งของสมการแล้ว คำตอบรูปทั่วไปจะอยู่ในรูป

$$x = x_0 + \left(\frac{b}{d}\right)t \quad , \quad y = y_0 - \left(\frac{a}{d}\right)t$$

เมื่อ t เป็นจำนวนเต็มใด ๆ

พิสูจน์ เราจะแบ่งการพิสูจน์เป็น 2 ตอน คือ

1) จะพิสูจน์ว่า สมการมีคำตอบก็ต่อเมื่อ $d|c$

2) จะต้องพิสูจน์ว่า คำตอบทั่วไปอยู่ในรูป $x = x_0 + \left(\frac{b}{d}\right)t$ และ $y = y_0 - \left(\frac{a}{d}\right)t$ เมื่อ x_0, y_0 เป็นคำตอบหนึ่ง และ t เป็นจำนวนเต็มใด ๆ

1) เราจะพิสูจน์ทั้งสองทาง ,

1.1 ถ้า $ax + by = c$ แล้ว $d|c$

เนื่องจาก $d = (a, b)$ ดังนั้น $d|a$ และ $d|b$

เพราะฉะนั้น $d|(ax + by)$ (จากทฤษฎีบท 2.2.7)

แต่ $ax + by = c$ สำหรับบางจำนวนเต็ม x และ y

นั่นคือ $d|c$

1.2 ถ้า $d|c$ แล้ว $ax + by = c$

เนื่องจาก $d|c$ ดังนั้น $c = dt$, $t \in Z$

จากทฤษฎีบท 2.2.9 จะมีจำนวนเต็ม x_0 และ y_0 ซึ่ง

$$d = ax_0 + by_0$$

คูณด้วย t จะได้

$$\begin{aligned} c = dt &= ax_0t + by_0t \\ &= a(x_0t) + b(y_0t) \\ &= ax + by \end{aligned}$$

2) สมมติให้ x_0, y_0 เป็นคำตอบหนึ่งของสมการ $ax + by = c$

ดังนั้น $ax_0 + by_0 = c$

ทำให้ได้ว่า $a(x - x_0) + b(y - y_0) = 0$

หรือ $a(x - x_0) = -b(y - y_0)$ .....(1)

เนื่องจาก $d = (a, b)$ นั่นคือ $d|a$ และ $d|b$

แสดงว่าจะต้องมี r และ s ซึ่ง

$$a = dr \quad \text{และ} \quad b = ds$$

จาก (I), แทนค่า a และ b

$$dr(x - x_0) = -ds(y - y_0)$$

หรือ $r(x - x_0) = s(y_0 - y)$

นั่นคือ $r|s(y_0 - y)$

แต่ $\left(\frac{a}{d}, \frac{b}{d}\right) = (r, s) = 1$ จากแบบฝึกหัด 2.2 ข้อ 7

ดังนั้น $r|(y_0 - y)$ จากแบบฝึกหัด 2.2 ข้อ 8

นั่นคือ $y_0 - y = rt$ สำหรับ $t \in Z$

$$y = y_0 - rt$$

$$y = y_0 - \left(\frac{a}{d}\right)t$$

แทนค่า $y_0 - y$ ใน (1) จะได้

$$x - x_0 = st$$

$$x = x_0 + st$$

$$= x_0 + \left(\frac{b}{d}\right)t$$

ตัวอย่าง 2.3.1 จงหาคำตอบของสมการ $7x + 5y = 53$

วิธีทำ ในที่นี้ $a = 7$, $b = 5$ และ $c = 53$

ก่อนอื่นจะหา ห.ร.ม. ของ 7 และ 5 โดยใช้ขั้นตอนวิธีหาร

$$7 = 1 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

ดังนั้น ห.ร.ม. ของ 7 และ 5 คือ 1

และ $1|53$ ดังนั้น สมการนี้มีคำตอบแน่ ๆ

จะหาคำตอบหนึ่งของสมการนี้ได้โดยการย้อนขบวนการข้างต้น (เขียนให้อยู่ในรูปของ $7x + 5y = d$)

$$1 = 5 - 2 \cdot 2$$

$$= 5 - 2(7 - 5)$$

$$= 7(-2) + 5(3)$$

คูณตลอดด้วย 53

$$53 = 7(-106) + 5(159)$$

แสดงว่าคำตอบหนึ่งคือ $x_0 = -106$ และ $y_0 = 159$

ดังนั้น คำตอบทั่วไปคือ

$$x = x_0 + \frac{b}{d}t \quad , \qquad y = y_0 - \frac{a}{d}t$$

นั่นคือ $x = -106 + 5t$, $y = 159 - 7t$

แต่จากโจทย์ตอนต้น เราต้องการคำตอบที่เป็นจำนวนเต็ม

เพราะฉะนั้นเราต้องการ $-106 + 5t > 0$ และ $159 - 7t > 0$

หรือ $t > 21.2$ และ $t < 22.7$

ดังนั้น สำหรับคำตอบที่เป็นจำนวนเต็ม $21.2 < t < 22.7$

หรือ $t = 22$ นั่นเอง

จะได้ $x = -106 + 5(22)$ และ $y = 159 - 7(22)$

ทำให้ $x = 4$ และ $y = 5$

แบบฝึกหัด 2.3

1. จงหาคำตอบของสมการไดโอแฟนไทน์ต่อไปนี้

   1.1) $320x + 112y = 480$

   1.2) $2025x + 501y = 300$

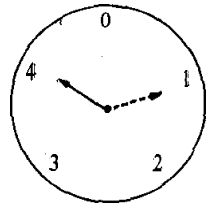
2. จงหาคำตอบที่เป็นบวก (ถ้ามี) ของสมการไดโอแฟนไทน์ต่อไปนี้

   2.1) $294x + 273y = 147$

   2.2) $54x + 21y = 900$

2.4 การลงรอยกัน (Congruence)

พิจารณานาฬิกาที่มี 5 ชั่วโมง ดังรูป



ถ้าขณะนี้เวลา 4 นาฬิกา อีก 3 ชั่วโมงต่อมาจะเป็นเวลา 2 นาฬิกา (ซึ่งอาจเขียนแทนได้ว่า $4+3 = 2$) ถ้าถามว่าอีก 17 ชั่วโมงถัดมา จะเป็นเวลาอะไร เรานับต่อไปเรื่อย ๆ ก็จะได้คำตอบเหมือนกัน แต่เรามีวิธีการที่ง่ายกว่า กล่าวคือ เนื่องจากจำนวน 17 บนหน้าปัดนาฬิกาไม่มี และนาฬิกาครบรอบครั้งละ 5 ชั่วโมง จึงพิจารณา $17 = 5+5+5+2 = 3(5)+2$ ดังนั้น เวลาที่ต้องการคือ $4+2 = 1$ หรือเวลา 1 นาฬิกา เราจะพบว่า 17 ทำหน้าที่เหมือน 2, โดยจำนวน 2 เป็นเศษเหลือที่เกิดจากการนำ 5 ไปหาร 17

$$17 = 3(5)+2$$

หรือ $$17-2 = 3(5)$$

คราวนี้ถ้ามาพิจารณานาฬิกาที่ใช้กันอยู่ทั่ว ๆ ไป คือ มี 12 ชั่วโมง ถ้าขณะนี้เวลา 2 นาฬิกา อีก 103 ชั่วโมงจะเป็นเวลาอะไร เรานำ 12 ไปหาร 103 เพื่อหาเศษเหลือ หรือขั้นตอนวิธีหารนั่นเอง

$$103 = 8(12)+7$$

หรือ $$103-7 = 8(12)$$

เพราะฉะนั้น เวลาที่ต้องการคือ $2+7 = 9$ นาฬิกา

(เนื่องจาก 103 ทำหน้าที่เหมือน 7)

การที่ 17 ทำหน้าที่เหมือน 2 ในระบบนาฬิกา 5 ชั่วโมง เราเรียกว่า 17 และ 2 ลงรอยกัน และใช้สัญลักษณ์ "$\equiv$" ดังนั้น เราใช้ว่า $17 \equiv 2 \pmod 5$ ซึ่งอ่านว่า "17 ลงรอยกับ 2 มอดูโล 5"

และทำนองเดียวกัน 103 ทำหน้าที่เหมือน 7 ในระบบนาฬิกา 12 ชั่วโมง เราได้ว่า

$$103 \equiv 7 \pmod{12}$$

นิยาม 2.4.1 สำหรับจำนวนเต็ม a และ b

$a \equiv b \pmod{m}$ โดยที่ $m \in Z^+$ ก็ต่อเมื่อมีจำนวนเต็ม k ซึ่งทำให้ $a = km + b$

ตัวอย่าง 2.4.1

$12 \equiv 2 \pmod{5}$, เพราะว่ามี $2 \in z$ ซึ่ง $12 = (2)(5) + 2$

$23 \equiv 2 \pmod{7}$, เพราะว่ามี $3 \in Z$ ซึ่ง $23 = (3)(1) + 2$

$-7 \equiv 11 \pmod{6}$, เพราะว่ามี $-3 \in Z$ ซึ่ง $-7 = (-3)(6) + 11$

$3 \equiv -1 \pmod{2}$, เพราะว่ามี $2 \in Z$ ซึ่ง $3 = (2)(2) + (-1)$

$12 \equiv 0 \pmod{4}$, เพราะว่ามี $3 \in z$ ซึ่ง $12 = (3)(4) + (0)$

ยังมีวิธีอื่น ๆ อีกที่จะอธิบายการลงรอยกัน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.4.1 a ลงรอยกันกับ b มอดูโล m ก็ต่อเมื่อ $m|(a-b)$

พิสูจน์ $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $a = km + b$

ก็ต่อเมื่อ $a - b = km$

ก็ต่อเมื่อ $m|(a-b)$

ตัวอย่าง 2.42 $12 \equiv 2 \pmod{5}$ เนื่องจาก $5|(12-2)$

ทฤษฎีบท 2.4.2 $a \equiv b \pmod{m}$ ก็ต่อเมื่อ m หาร a เหลือเศษเท่ากันกับ m หาร b

พิสูจน์ สำหรับ $a, m \in Z$ เราได้ว่า $a = qm + r,\ 0 \leqslant r < m$

สำหรับ $b, m \in Z$ เราได้ว่า $b = pm + s,\ 0 \leqslant s < m$

ดังนั้น $a - b = (qm + r) - (pm + s)$

$= (q - p)m + (r - s)$

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

ก็ต่อเมื่อ $m|(r-s)$, โดยที่ $r - s < m$

ก็ต่อเมื่อ $r - s = 0$ จากแบบฝึกหัด 2.2% 5

ก็ต่อเมื่อ $r = s$

ตัวอย่าง 2.4.3 $43 \equiv 58 \pmod{5}$ เนื่องจาก 5 หาร 43 และ 5 หาร 58 เหลือเศษเท่ากัน คือ 3

ต่อไปจะกล่าวถึงคุณสมบัติบางอย่างของการลงรอยกัน

ทฤษฎีบท 2.4.3 การลงรอยกันเป็นความสัมพันธ์สมภาค (equivalence relation) นั่นคือ

1) $a \equiv a \pmod{m}$

2) ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$

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

พิสูจน์ 1) เนื่องจาก $a - a = 0$

ทำให้ $m|(a-a)$

นั่นคือ $a \equiv a \pmod{m}$

2) เนื่องจาก $a \equiv b \pmod{m}$ ก็ต่อเมื่อ m หาร a เหลือเศษเท่ากับ m หาร b ดังนั้น ถ้า $a \equiv b \pmod{m}$ แล้ว m หาร a เหลือเศษเท่ากับ m หาร b ซึ่งมีความหมายว่า m หาร b เหลือเศษเท่ากับ m หาร a หรือ $b \equiv a \pmod{m}$ นั่นเอง เราอาจพิสูจน์ได้อีกแบบหนึ่ง ดังนี้

$a \equiv b \pmod{m}$ หมายความว่า $m|(a-b)$

นั่นคือ $m|-(a-b)$ จากทฤษฎีบท 2.2.2

หรือ $m|(b-a)$

ดังนั้น $b \equiv a \pmod{m}$

3) จาก $a \equiv b \pmod{m}$ เราได้ว่า $m|(a-b)$

และ $b \equiv c \pmod{m}$ เราได้ว่า $m|(b-c)$

ดังนั้น $m|[(a-b)+(b-c)]$ จากทฤษฎีบท 2.2.6

หรือ $m|(a-c)$

เพราะฉะนั้น $a \equiv c \pmod{m}$

ทฤษฎีบท 2.4.4 ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว

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

2) $a \cdot c \equiv bd \pmod{m}$

พิสูจน์ 1) เนื่องจาก $a \equiv b \pmod{m}$ นั่นคือ $m|(a-b)$

และ $c \equiv d \pmod{m}$ นั่นคือ $m|(c-d)$

เพราะฉะนั้น $m|[(a-b)+(c-d)]$

หรือ $m|[(a+c)-(b+d)]$

ทำให้ได้ว่า $a+c \equiv b+d \pmod{m}$

2) $a \equiv b \pmod{m}$ ก็ต่อเมื่อ $a = km + b,\ k \in I$ และ

$c \equiv d \pmod{m}$ ก็ต่อเมื่อ $c = nm + d,\ n \in I$

ดังนั้น $ac = (km + b)(nm + d)$

$= bd + bnm + kmnm + kmd$

$= bd + (bn + kmn + kd)m$

ซึ่ง $bn + kmn + kd$ เป็นจำนวนเต็ม

นั่นคือ $ac \equiv bd \pmod{m}$

ตัวอย่าง 2.2.4 $16 \equiv 7 \pmod 3$ และ $29 \equiv 17 \pmod 3$

เพราะฉะนั้น $16 + 29 \equiv 7 + 17 \pmod 3$

หรือ $45 \equiv 24 \pmod 3$

และยังได้ว่า $(16)(29) \equiv (7)(17) \pmod 3$

หรือ $464 \equiv 119 \pmod 3$

แบบฝึกหัด 2.4

1. จงหาจำนวนเต็มที่ลงรอยกันกับจำนวนต่อไปนี้ (มอดูโล 7)

   1.1) 8 1.2) -3 1.3) 39

   1.4) 0 1.5) 12 1.6) -12

2. ทำไมเราจึงไม่ยอมรับว่า 1 เป็นมอดูลัส (modulus)
3. จงพิสูจน์ว่า ถ้า a เป็นพหุคูณของ m แล้ว $a \equiv 0 \pmod{m}$ และพิสูจน์บทกลับด้วย
4. จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $a+c \equiv b+c \pmod{m}$
5. จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $ac \equiv bc \pmod{m}$
6. จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $a^2 \equiv b^2 \pmod{m}$