บทที่ 2

ทฤษฎีพื้นฐานเกี่ยวกับการหาร
FUNDAMENTAL THEOREMS OF DIVISIBILITY

2.1 คุณสมบัติเบื้องต้น

นิยาม 2.1 ให้ a และ b เป็นจำนวนเต็มซึ่ง $a \neq 0$ และถ้ามีเลขจำนวนเต็ม m ซึ่งทำให้ $b = am$ แล้ว เรากล่าวว่า a หาร b ลงตัว และเขียนแทนด้วย $a|b$ เราอาจจะกล่าวอีกอย่างหนึ่งว่า a เป็นตัวหารหรือเป็นตัวประกอบของ b และ b เป็นพหุคูณของ a ถ้า a หาร b ไม่ลงตัวเขียนแทนด้วย $a \nmid b$

ตัวอย่าง 2.1 $2|4$ $3|21$ $5|0$ $2 \nmid 5$ $7 \nmid 20$ $5 \nmid 21$

ข้อสังเกต : สัญลักษณ์ที่ใช้ $a|b$ ระวังอย่าสับสนกับเลขตัวยะ a/b ซึ่งหมายถึงเศษ a ส่วน b

ทฤษฎี 2.1

1. ถ้า $a \neq 0$ แล้ว $a|0$ และ $a|a$ เมื่อ a เป็นจำนวนเต็มใด ๆ
2. $1|b$ สำหรับ b ซึ่งเป็นจำนวนเต็ม
3. ถ้า $a|b$ แล้ว $a|bc$ สำหรับ c เป็นจำนวนเต็มใด ๆ
4. ถ้า $a|b$ และ $b|c$ แล้ว $a|c$
5. ถ้า $a|b$ และ $a|c$ แล้ว $a|(bx+cy)$ สำหรับจำนวนเต็ม x, y

พิสูจน์

(1) เพราะว่า $a \cdot 0 = 0$
ดังนั้นตามนิยาม $a|0$ และ $a \cdot 1 = a$
ดังนั้นตามนิยาม $a|a$

(2) เช่นเดียวกันกับข้อ (1) เพราะ $1 \cdot b = b$
ดังนั้น $1|b$

(3) ถ้า $a|b$ แล้วจะต้องมีจำนวนเต็ม q ซึ่งทำให้ $b = aq$ และ $bc = aqc$ สำหรับ c เป็นจำนวนเต็ม
เพราะฉะนั้น $a|bc$ ตามนิยาม

(4) ถ้า $a|b$ และ $b|c$ แล้วจะต้องมีจำนวนเต็ม m และ n ซึ่งทำให้ $b = am$ และ $c = bn$
แทนค่า b จะได้ $c = amn = a(mn)$
เนื่องจาก mn เป็นจำนวนเต็ม ดังนั้น $a|c$ ตามนิยาม

(5) ถ้า $a|b$ และ $a|c$ แล้ว จะต้องมีจำนวนเต็ม m และ n ซึ่งทำให้ $b = am$ และ $c = an$

ดังนั้น $bx+cy = amx+any$ สำหรับ x, y เป็นจำนวนเต็ม

$= a(mx+ny)$

แต่ $mx+ny$ เป็นจำนวนเต็ม

เพราะฉะนั้น $a|(bx+cy)$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

บทแทรก 2.1

ถ้า $a|b_i$ สำหรับ $i = 1, 2, \ldots, n$ แล้ว $a|(b_1x_1+b_2x_2+ \ldots +b_nx_n)$ สำหรับจำนวนเต็ม $x_1, x_2, \ldots, x_n$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

จากทฤษฎีและบทแทรกนี้จะเป็นประโยชน์กับการพิสูจน์ทฤษฎีต่าง ๆ ให้หัวข้อต่อไปมาก ดังนั้นเราจะต้องทำความเข้าใจให้ดีเพื่อที่จะได้ทราบว่าเมื่อไรจะนำทฤษฎีนี้มาใช้ และจะใช้อย่างไร เมื่อเรามีสมการ

$$b_1c_1+b_2c_2 = d$$

ถ้าเราทราบว่า $a|b_1$ และ $a|b_2$ แล้ว เราจะต้องแยกตัวประกอบด้านซ้ายของสมการได้ดังการพิสูจน์ในทฤษฎีที่ผ่านมา และเขียนใหม่ได้เป็น

$$a(m_1c_1+m_2c_2) = d$$

จากนิยามการหารลงตัว แสดงว่า a ต้องหาร d ลงตัว นั่นแสดงว่าเมื่อ a หารแต่ละเทอมทางซ้ายของสมการได้แล้ว a ต้องหารจำนวนทางซ้ายของสมการได้ทั้งหมด และนั่นคือ a หารจำนวนทางขวาของสมการได้ด้วยนั่นเอง

ทฤษฎี 2.2

ให้ a เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ ถ้า $a|b$ และ $b \neq 0$ แล้ว $|a| \leqslant |b|$

พิสูจน์ ถ้า $a|b$ แล้วจะต้องมีจำนวนเต็ม m ซึ่งทำให้ $b = am$ แต่ $b \neq 0$

ดังนั้น $m \neq 0$

นั่นคือ $1 \leqslant |m|$ และ $1 \leqslant |b|$

เพราะฉะนั้น $|b| = |am| = |a| \cdot |m| \geqslant |a| \cdot 1$

หรือ $|a| \leqslant |b|$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

บทแทรก 2.2

ถ้า a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ และ $a|b$ และ $b|a$ แล้ว $a = \pm b$

พิสูจน์ จากทฤษฎี 2.2 เราทราบว่าถ้า $a|b$ แล้ว $|a| \leq |b|$ และถ้า $b|a$ แล้ว $|b| \leq |a|$

เพราะฉะนั้น $|a| = |b|$

นั่นคือ $a = \pm b$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.3

1. ให้ a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ ถ้า $b|c$ และ $a|\frac{c}{b}$ แล้ว $ab|c$
2. ให้ b และ c เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ ถ้า $b|c$ และ $\frac{c}{b}|a$ แล้ว $c|ab$

พิสูจน์ ถ้า $a|\frac{c}{b}$ แล้ว จะต้องมีจำนวนเต็ม m ซึ่งทำให้ $am = \frac{c}{b}$

ดังนั้น $abm = c$

เพราะฉะนั้น $ab|c$ ตามนิยาม

ถ้า $\frac{c}{b}|a$ แล้ว จะต้องมีจำนวนเต็ม n ซึ่งทำให้ $\frac{c}{b}n = a$

ดังนั้น $cn = ab$

เพราะฉะนั้น $c|ab$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.4 ดิวิชันอัลกอริธึม (Division Algorithm)

ถ้าให้ a และ b เป็นจำนวนเต็มซึ่ง $b \neq 0$ แล้วจะมีจำนวนเต็ม q และ r เพียงชุดเดียวเท่านั้น ซึ่งทำให้ $a = bq + r$ ที่ซึ่ง $0 \leq r < |b|$

(เรียก q ว่าเป็นผลหารและเรียก r ว่าเป็นเศษจากการหาร a ด้วย b)

พิสูจน์ ให้ S เป็นเซ็ตของจำนวนเต็มที่ไม่ใช่จำนวนลบ และอยู่ในรูป $a - kb$

$S = \{a - kb | k \in Z$ และ $(a - kb) \geq 0\}$

ถ้า $a \geq 0$ แล้ว $a - 0b$ จะอยู่ในเซ็ต S

ถ้า $a < 0$ แล้ว $a - |a|b > 0$ ถ้า $b < 0$

และ $a - ab > 0$ ถ้า $b > 0$

แสดงว่าเมื่อ a เป็นจำนวนเต็มใด ๆ แล้ว เซ็ต S ไม่ใช่เซ็ตว่าง

ดังนั้น จาก Well-Ordering Principle

S จะต้องมีจำนวนเต็มซึ่งมีค่าน้อยที่สุด สมมุติเป็น r และ $r \geq 0$

ดังนั้น $r = a - kb$ สำหรับ k ซึ่งเป็นจำนวนเต็มบางตัว

หรือ $a = qb + r$ เมื่อ $q = k$

ต่อไปจะแสดงว่า $r < |b|$

สมมุติว่า $r \geq |b|$

แล้ว $r - |b| = a - kb - |b|$ ซึ่งเป็นสมาชิกของ S

แต่ $r - |b| < r$ ซึ่งขัดแย้งกับที่สมมุติให้ r มีค่าน้อยที่สุดใน S

ดังนั้น $r \geq |b|$ เป็นไปไม่ได้

นั่นคือ $0 \leq r < |b|$

แสดงว่ามีจำนวนเต็ม q และ r ซึ่งทำให้ $a = bq + r$ ที่ซึ่ง $0 \leq r < |b|$

ขั้นต่อไปจะแสดงว่าจะมี q และ r เพียงชุดเดียว (unique) เท่านั้นที่มีคุณสมบัติดังกล่าวข้างต้น

สมมุติให้มี q_1 และ r_1 อีกชุดหนึ่งซึ่งทำให้ $a = bq_1 + r_1, 0 \leq r_1 < |b|$

แสดงว่า $a = bq + r = bq_1 + r_1$

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

แต่ $q_1 - q$ เป็นจำนวนเต็ม

เพราะฉะนั้น $b|(r - r_1)$ ตามนิยาม

ถ้า $r \neq r_1$ หรือ $(r - r_1) \neq 0$ แล้ว $|b| \leq |r - r_1|$ ซึ่งเป็นไปไม่ได้

เพราะ $-b < r - r_1 < b$ หรือ $|r - r_1| < |b|$

เพราะฉะนั้น $r = r_1$ หรือ $r - r_1 = 0$

นั่นคือ $b(q_1 - q) = r - r_1 = 0$

แต่ $b \neq 0$ ดังนั้น $q_1 - q = 0$ หรือ $q = q_1$

แสดงว่ามี q และ r เพียงชุดเดียวเท่านั้นที่มีคุณสมบัติดังกล่าวมาแล้ว

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.2 ให้ $a = 21, b = 5$

ดังนั้น $21 = (5)(4) + 1 \qquad 0 \leq 1 < |5|$

ให้ $a = -17, b = 5$

ดังนั้น $-17 = (5)(-4) + 3 \qquad 0 \leq 3 < |5|$

ให้ $a = 35, b = -6$

ดังนั้น $35 = (-6)(-5) + 5 \qquad 0 \leq 5 < |-6|$

นิยาม 2.2 จำนวนเต็ม p ซึ่ง $|p| > 1$ จะเรียกว่าเป็นจำนวนเฉพาะ (prime number) ถ้า p ไม่มีตัวหารอื่นนอกจาก ± 1 และ $\pm p$ เท่านั้น

จำนวนเต็มใดที่ไม่เท่ากับ 0 และไม่เท่ากับ ± 1 และไม่เป็นจำนวนเฉพาะเรียกว่าจำนวนประกอบ (Composite number)

นั่นคือ ถ้า a เป็นจำนวนประกอบแล้ว $a = b \cdot c$ ซึ่ง $|b| > 1$ และ $|c| > 1$

นิยาม 2.3 จำนวนเต็มที่หารด้วย ± 2 ลงตัว เรียกว่าจำนวนเต็มคู่ (even number)

จำนวนเต็มที่หารด้วย ± 2 ไม่ลงตัว เรียกว่า จำนวนเต็มคี่ (odd number)

จำนวนเต็มคู่จะเขียนได้ในรูป $2k$ และจำนวนเต็มคี่จะเขียนได้ในรูป $2k+1$ เมื่อ k เป็นจำนวนเต็มใด ๆ

แบบฝึกหัด 2.1

1. ถ้า $a|b$ และ $a+b = c$ แล้ว จงพิสูจน์ว่า $a|c$
2. ถ้า $a|c$ และ $a+b = c$ แล้ว จงพิสูจน์ว่า $a|b$
3. ถ้า $d|(35n+26)$, $d|(7n+3)$ และ $d > 1$ แล้ว จงแสดงว่า $d = 11$
4. ถ้า $a = bq+r$ เมื่อ $0 \leq r < b$ และ $b|a$ แล้ว จงแสดงว่า $r = 0$
5. จงหาจำนวนเต็ม a และ b ซึ่งทำให้ข้อความข้างล่างนี้เป็นจริง และบอกเงื่อนไขของ a และ b ด้วย
   1) $2|ab$ แต่ $2 \nmid (a+b)$
   2) $2 \nmid ab$ แต่ $2|(a+b)$
6. จงเขียน a ให้อยู่ในรูปของ $a = bq+r$, $0 \leq r < |b|$
   1) $a = 31$, $b = -7$
   2) $a = -39$, $b = -8$
7. จงพิสูจน์ว่า $2|(ab)$ หรือ $2|(a+b)$ อย่างหนึ่งอย่างใดเท่านั้น
8. ให้ k เป็นจำนวนเต็มบวก ถ้า $k|a$ และ $k|b$ และสำหรับจำนวนเต็ม x, y, $ax-by = 1$ จงพิสูจน์ว่า $k = 1$
9. ให้ $|a| > 1$ จงพิสูจน์ว่าถ้า $a|b$ แล้ว $a \nmid (b \pm 1)$

2.2 ตัวหารร่วมมาก (Greatest Common Divisor)

ถ้า $d|a$ และ $d|b$ แล้ว เราเรียก d ว่าเป็นตัวหารร่วมของ a และ b ถ้า a และ b เป็นศูนย์ทั้งคู่ก็จะมีตัวหารร่วมของ a และ b มากมายนับไม่ถ้วน แต่ถ้า a หรือ b ตัวหนึ่งตัวใดไม่เท่ากับศูนย์ ตัวหารร่วมของ a และ b จะมีจำนวนจำกัด และจะต้องมีตัวหารร่วมที่มีค่ามากที่สุดซึ่งเราจะเรียกว่า ตัวหารร่วมมากหรือเรียกย่อ ๆ ว่า ห.ร.ม. ดังนิยามต่อไปนี้

นิยาม 2.4 ให้ a และ b เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ทั้งคู่ และ d เป็นจำนวนเต็มบวกที่มีค่ามากที่สุด ซึ่งหาร a และ b ลงตัว เราเรียก d ว่าเป็น **"ตัวหารร่วมมาก"** (ห.ร.ม.) ของ a และ b และเขียนแทนด้วย $d = (a, b)$

นิยาม 2.4 อาจเขียนอีกแบบหนึ่งได้ดังนี้

ให้ a และ b เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ทั้งคู่ และ d เป็นจำนวนเต็มบวกที่มีคุณสมบัติต่อไปนี้

1. d เป็นตัวหารร่วมของ a และ b หรือ $d|a$ และ $d|b$
2. ถ้า c เป็นตัวหารร่วมใด ๆ ของ a และ b แล้ว c หาร d ลงตัว หรือถ้า $c|a$ และ $c|b$ แล้ว $c|d$ แล้ว เรียก d ว่าเป็น ห.ร.ม. ของ a และ b

ตัวอย่าง 2.3 $(3, 9) = 3$, $(0, -5) = 5$, $(-7, 21) = 7$, $(-4, -12) = 4$

ทฤษฎี 2.5

ถ้า ห.ร.ม. ของ a และ b เท่ากับ d แล้ว จะมีจำนวนเต็ม x_0, y_0 ซึ่งทำให้ $d = ax_0 + by_0$

พิสูจน์ ให้ C เป็นเซ็ตของจำนวนเต็มซึ่งเขียนอยู่ในรูป $ax + by$ ได้

เมื่อ x, y เป็นจำนวนเต็ม

เลือกจำนวนเต็ม x_0, y_0 ซึ่งทำให้ $ax_0 + by_0$ เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุดใน C

สมมติให้ $\ell = ax_0 + by_0$

ต้องการแสดงว่า $\ell|a$ และ $\ell|b$

สมมติว่า $\ell \nmid a$

ดังนั้นตามดิวิชันอัลกอริธึม จะต้องมีจำนวนเต็ม q และ r ซึ่งทำให้ $a = \ell q + r$, $0 \leq r < \ell$

นั่นคือ $r = a - \ell q = a - q(ax_0 + by_0)$

$= a(1 - qx_0) + b(-qy_0)$

แสดงว่า r อยู่ในเซ็ต C ซึ่งขัดแย้งกับที่สมมุติให้ ℓ มีค่าน้อยที่สุดใน C

ดังนั้น $\ell | a$

ในทำนองเดียวกันก็จะพิสูจน์ได้ว่า $\ell | b$

จากโจทย์ $d = (a, b)$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม A และ B ซึ่งทำให้ $a = dA$ และ $b = dB$

และ $\ell = ax_0 + by_0 = d(Ax_0 + By_0)$

แสดงว่า $d | \ell$

จากทฤษฎี 2.2 $d \leqslant \ell$

แต่ $d < \ell$ เป็นไปไม่ได้ เพราะ $d = (a, b)$

ดังนั้น $d = \ell = ax_0 + by_0$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

นิยาม 2.5 ให้ a และ b เป็นจำนวนเต็ม ถ้า ห.ร.ม. ของ a และ b เท่ากับ 1 แล้ว เราเรียก a และ b ว่าเป็นรีเลทีบลีไพรม์ (relatively prime)

จำนวนเต็มสองจำนวนใด ๆ ที่ไม่เท่ากับศูนย์จะเป็นรีเลทีบลีไพรม์ ถ้าจำนวนเต็มคู่นั้นไม่มีตัวหารร่วมอื่น ๆ นอกจาก 1

ถ้า p เป็นจำนวนเฉพาะ และ a เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์แล้ว a และ p จะเป็นรีเลทีบลีไพรม์ หรือ a จะเป็นพหุคูณของ p นั่นคือจำนวนเฉพาะคู่ใด ๆ ที่ไม่เท่ากันจะเป็นรีเลทีบลีไพรม์ และจำนวนเต็มคู่ใด ๆ ที่ไม่เท่ากับศูนย์ และไม่เป็นจำนวนเฉพาะ แต่เป็นรีเลทีบลีไพรม์ได้

ตัวอย่าง 2.4 3 และ 5 เป็นรีเลทีบลีไพรม์ เพราะ $(3, 5) = 1$

9 และ 10 เป็นรีเลทีบลีไพรม์ เพราะ $(9, 10) = 1$

8 และ 15 เป็นรีเลทีบลีไพรม์ เพราะ $(8, 15) = 1$

จะเห็นว่าทั้ง 8, 9, 10 และ 15 ต่างก็ไม่ใช่จำนวนเฉพาะ

ทฤษฎี 2.6

จำนวนเต็ม a และ b จะเป็นรีเลทีบลีไพรม์ ก็ต่อเมื่อมีจำนวนเต็ม m และ n ซึ่งทำให้ $am + bn = 1$

พิสูจน์ ให้ a และ b เป็นรีเลทีบลีไพรม์

เพราะฉะนั้น $(a, b) = 1$

ดังนั้นตามทฤษฎี 2.5 จะต้องมีจำนวนเต็ม m และ n ซึ่งทำให้

$$1 = am + bn$$

ในทางกลับกันสมมุติให้มีจำนวนเต็ม m และ n ซึ่งทำให้

$$1 = am + bn$$

สมมติให้ d เป็น ห.ร.ม. ของ a และ b
เพราะฉะนั้น $d|a$ และ $d|b$
ตามทฤษฎี 2.1 ข้อ 5 จะได้ว่า $d|am + bn$
นั่นคือ $d|1$
แสดงว่า $d = 1$ เพราะว่า $d > 0$
นั่นคือ a และ b เป็นรีเลทีบลีไพรม์

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.7

ถ้า $a|bc$ และ $(a, b) = 1$ แล้ว $a|c$ เมื่อ a เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์

พิสูจน์ เพราะว่า $(a, b) = 1$
ดังนั้นจากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x, y ซึ่งทำให้

$$ax + by = 1$$

ดังนั้น $acx + bcy = c$
แต่ $a|bc$ และ $a|ac$
ดังนั้น $a|acx + bcy$ ตามทฤษฎี 2.1 ข้อ 5
นั่นคือ $a|c$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.8

ให้ a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ ถ้า $(a, b) = 1$ และ $a|c$, $b|c$ แล้ว $ab|c$

พิสูจน์ เพราะว่า $a|c$ และ $b|c$
ดังนั้นจะต้องมีจำนวนเต็ม r และ s ซึ่งทำให้

$$c = ar = bs$$

แสดงว่า $b|ar$ แต่ $(a, b) = 1$
จากทฤษฎี 2.7 จะสรุปได้ว่า $b|r$
นั่นคือจะต้องมีจำนวนเต็ม t ซึ่งทำให้ $r = bt$

ดังนั้น $c = ar = abt$

แสดงว่า $ab|c$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.9

ให้ d เป็น ห.ร.ม. ของ a และ b สมการ $ax+by = c$ จะมีคำตอบเป็นจำนวนเต็ม (ทั้ง x และ y) ก็ต่อเมื่อ $d|c$

พิสูจน์ ให้ $(a, b) = d$ และสมมติว่า x_0, y_0 เป็นคำตอบที่เป็นจำนวนเต็มของสมการ $ax+by = c$

นั่นคือ $ax_0+by_0 = c$

ดังนั้นจากทฤษฎี 2.1 ข้อ 5 จะได้ว่า $d|ax_0+by_0$

นั่นคือ $d|c$

ในทางกลับกันถ้าสมมติให้ $d|c$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม q ซึ่งทำให้ $c = dq$

จากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x_1, y_1 ซึ่งทำให้

$$ax_1+by_1 = d$$
$$ax_1q+by_1q = dq = c$$
$$a(x_1q)+b(y_1q) = c$$

เพราะฉะนั้น $x = x_1q$ และ $y = y_1q$ เป็นคำตอบของสมการ $ax+by = c$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.5 พิจารณาสมการ $2x+6y = 3$ ไม่มีคำตอบเป็นจำนวนเต็ม

เพราะ $(2, 6) = 2$ และ $2 \nmid 3$

สมมุติว่าสมการนี้มีคำตอบเป็นจำนวนเต็มคือ x_1, y_1

แล้วให้ $x_1+3y_1 = m$ เมื่อ m เป็นจำนวนเต็ม

$$3 = 2x_1+6y_1 = 2m$$

แสดงว่า $2m = 3$ ซึ่งเป็นไปไม่ได้

นั่นคือสมการ $2x+6y = 3$ ไม่มีคำตอบเป็นจำนวนเต็ม

ทฤษฎี 2.10

ให้ m, a, b เป็นจำนวนเต็มแล้ว $(ma, mb) = |m|(a, b)$

พิสูจน์ ถ้า $a = 0$ หรือ $b = 0$ หรือ $m = 0$ แล้ว ทฤษฎีนี้จะเป็นจริง

ถ้า $a \neq 0$, $b \neq 0$ และ $m \neq 0$

จากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x_0, y_0 ซึ่งทำให้

$$max_0 + mby_0 = (ma, mb)$$

เพราะฉะนั้น $m|(ma, mb)$

ดังนั้น $ax_0 + by_0 = \frac{(ma, mb)}{m}$

จากทฤษฎี 2.9 $(a, b) | \frac{(ma, mb)}{m}$

ดังนั้นจากทฤษฎี 2.3 ข้อ 1 จะได้ว่า

$$m(a, b) | (ma, mb) \qquad \text{..... (1)}$$

จากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x_1, y_1 ซึ่งทำให้

$$ax_1 + by_1 = (a, b)$$

เพราะฉะนั้น $max_1 + mby_1 = m(a, b)$

ดังนั้นจากทฤษฎี 2.9

$$(ma, mb) | m(a, b) \qquad \text{..... (2)}$$

จาก (1) และ (2) และบทแทรก 2.2 แสดงว่า

$$(ma, mb) = \pm m(a, b)$$

นั่นคือ $(ma, mb) = |m|(a, b)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.11

ให้ d เป็น ห.ร.ม. ของ a และ b แล้ว $d|(ax_1 + by_1, ax_2 + by_2)$ เมื่อ x_1, y_1, x_2, y_2 เป็นจำนวนเต็ม

พิสูจน์ จาก $d = (a, b)$

เพราะฉะนั้น จากทฤษฎี 2.1 จะต้องมีจำนวนเต็ม x_1, y_1 และ x_2, y_2 ซึ่งทำให้

$d|(ax_1 + by_1)$ และ $d|(ax_2 + by_2)$

นั่นคือ $d|(ax_1 + by_1, ax_2 + by_2)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.12

ให้ a, b และ m เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์แล้ว $(m, ab) = 1$ ก็ต่อเมื่อ $(m, a) = 1 = (m, b)$

พิสูจน์ ให้ $(m, ab) = 1$

จากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x_1, y_1 ซึ่งทำให้ $mx_1 + aby_1 = 1$

ดังนั้นจากทฤษฎี 2.9 จะได้ว่า $(m, a) | 1$ และ $(m, b) | 1$

แต่จำนวนที่จะหาร 1 ได้ลงตัวมี 1 และ -1 ซึ่ง ห.ร.ม. จะต้องเป็นจำนวนเต็มบวก

ดังนั้น $(m, a) = 1$ และ $(m, b) = 1$

ในทางกลับกัน ถ้าให้ $(m, a) = 1 = (m, b)$ แล้ว

จากทฤษฎี 2.5 จะต้องมีจำนวนเต็ม x_2, y_2 และ x_3, y_3 ซึ่งทำให้ $mx_2 + ay_2 = 1$

และ $mx_3 + by_3 = 1$

$$(mx_2 + ay_2)(mx_3 + by_3) = 1$$

$$m(mx_2x_3 + ax_3y_2 + bx_2y_3) + ab(y_2y_3) = 1$$

ดังนั้นจากทฤษฎี 2.9

$$(m, ab) | 1$$

นั่นคือ $(m, ab) = 1$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

บทแทรก

$$(a_1a_2, b_1b_2) = 1 \text{ ก็ต่อเมื่อ } \begin{cases} (a_1, b_1) = 1 = (a_1, b_2) \\ (a_2, b_1) = 1 = (a_2, b_2) \end{cases}$$

พิสูจน์ โดยใช้ทฤษฎี 2.12

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

นิยาม 2.6 ให้ $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเต็ม จะเรียกว่า d เป็นตัวหารร่วมมากของจำนวนเหล่านี้ก็ต่อเมื่อ

1. $d | a_i$ สำหรับ $i = 1, 2, \ldots, n$
2. ถ้า $c | a_i$ แล้ว $c | d$

เขียนแทนด้วย $d = (a_1, a_2, \ldots, a_n)$

ตัวอย่าง 2.6 จงหา ห.ร.ม. ของ 12, 30, 42

วิธีทำ ตัวหารร่วมของ 12, 30 และ 42 ที่เป็นจำนวนบวก คือ 1, 2, 3, 6
ดังนั้น 6 เป็นตัวหารร่วมมาก เพราะ
1. $6|12$, $6|30$, $6|42$
2. $1|6$, $2|6$, $3|6$ และ $6|6$

ทฤษฎี 2.13

ถ้า $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มแล้ว

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

พิสูจน์ ให้ $d = (a_1, a_2, \ldots, a_n)$ และ

$$d_1 = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

จะต้องพิสูจน์ให้ได้ว่า $d|d_1$ และ $d_1|d$ จึงจะสรุปได้ว่า $d = d_1$

จาก $d = (a_1, a_2, \ldots, a_n)$

แสดงว่า $d|a_i$ สำหรับ $i = 1, 2, \ldots, n$

ดังนั้น $d|(a_1, a_2, \ldots, a_{n-1})$ และ $d|a_n$

เพราะฉะนั้นตามนิยามของ ห.ร.ม. $d|((a_1, a_2, \ldots, a_{n-1}), a_n)$ = ... (1)

ในทำนองเดียวกัน จาก $d_1 = ((a_1, a_2, \ldots, a_{n-1}), a_n)$

จะได้ว่า $d_1|(a_1, a_2, \ldots, a_{n-1})$ และ $d_1|a_n$

แสดงว่า $d_1|a_i$ สำหรับ $i = 1, 2, \ldots, n-1$ และ $d_1|a_n$

ดังนั้นตามนิยามของ ห.ร.ม. $d_1|(a_1, a_2, \ldots, a_n)$ ..... (2)

จาก (1) และ (2) สรุปได้ว่า $d = d_1$

หรือ $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 2.2

1. ถ้า $ad-bc = 1$ แล้ว จงพิสูจน์ว่า $(a+b, c+d) = 1$
2. ให้ a, b, m เป็นจำนวนเต็ม จงพิสูจน์ว่า $(a, b) = (a, am+b) = (a+bm, b)$
3. จงพิสูจน์ว่า $((a, b), c) = (a, (b, c)) = (a, b, c)$
4. จงพิสูจน์ว่า $(a, b, c) = ((a, b), (a, c)) = ((a, b), (b, c))$
5. ถ้า $d = (a, b)$, $a = Ad$ และ $b = Bd$ แล้ว จงพิสูจน์ว่า $(A, B) = 1$
6. ให้ k และ n เป็นจำนวนเต็มบวก จงพิสูจน์ว่า $(a, b) = 1$ ก็ต่อเมื่อ $(a^k, b^n) = 1$
7. ถ้า $d|mn$ และ $(m, n) = 1$ จงพิสูจน์ว่า $d = d_1d_2$ เมื่อ $d_1|m$, $d_2|n$ และ $(d_1, d_2) = 1$ (ข้อแนะนำ : ให้ $d_1 = (d, m)$)
8. ถ้า $(a, b) = 1$ จงพิสูจน์ว่า $(a+b, a-b) = 1$ หรือ 2
(ข้อแนะนำ : สมมติให้ $d = (a+b, a-b)$ แล้ว แสดงว่า $d|2b$, $d|2a$ และใช้ทฤษฎี 2.10
9. ถ้า $(a, b) = r$, $(a, c) = s$ และ $(b, c) = 1$ จงพิสูจน์ว่า $(a, bc) = rs$ และจงยกตัวอย่างแสดงว่าข้อความนี้ไม่เป็นจริงถ้า $(b, c) > 1$

2.3 ยูคลิเดียน อัลกอริธึม (Euclidean Algorithm)

เราได้ทราบมาจากทฤษฎีข้างต้นแล้วว่า ถ้าเรามีจำนวนเต็มสองจำนวน a กับ b ให้ $a > b > 0$ แล้ว จะต้องมีจำนวนเต็มอีกสองจำนวน q_1 และ r_1 ซึ่งทำให้ $a = bq_1 + r_1$ ซึ่ง $0 \leq r_1 < b$ ถ้า $r_1 = 0$ แล้ว แสดงว่า $b|a$ และ $(a, b) = b$ ถ้า $r_1 \neq 0$ แล้ว มาพิจารณา b กับ r_1 ย่อมจะต้องมีจำนวนเต็มอีกสองจำนวน q_2 และ r_2 ซึ่งทำให้ $b = r_1q_2 + r_2$ ซึ่ง $0 \leq r_2 < r_1$ ถ้า $r_2 = 0$ เราก็ยุติการหาร แต่ถ้า $r_2 \neq 0$ เราก็ดำเนินการหารต่อไปอีก จะได้ $r_1 = r_2q_3 + r_3$ ซึ่ง $0 \leq r_3 < r_2$ และดำเนินการกระทำนี้ไปเรื่อย ๆ จนกระทั่งได้เศษเป็นศูนย์ สมมุติว่าเศษที่เป็นศูนย์คือ r_{k+1} ดังนั้นเราก็จะได้สมการดังนี้

$$\left.\begin{aligned}
a &= bq_1 + r_1, && 0 \leq r_1 < b \\
b &= r_1q_2 + r_2, && 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, && 0 \leq r_3 < r_2 \\
&\vdots && \vdots \quad \vdots \\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, && 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= r_{k-1}q_k + r_k, && 0 \leq r_k < r_{k-1} \\
r_{k-1} &= r_kq_{k+1} + r_{k+1} \quad \text{ซึ่ง} && r_{k+1} = 0
\end{aligned}\right\} \text{A}$$

เราเรียกวิธีการกระทำนี้ว่ายูคลิเดียนอัลกอริธึมเป็นวิธีการที่ใช้หา ห.ร.ม. ของจำนวนเต็มสองจำนวนซึ่งไม่เท่ากับศูนย์ ซึ่งจะเป็นประโยชน์มากสำหรับการหา ห.ร.ม. ของจำนวนที่มีค่ามาก ๆ

ทฤษฎี 2.15

ถ้า a และ b เป็นจำนวนเต็มบวกสองจำนวนที่ทำให้หา r_k ได้ตามวิธีของระบบสมการ (A) แล้ว ห.ร.ม. ของ a และ b คือ r_k

พิสูจน์ จากสมการสุดท้ายเราทราบว่า $r_k|r_{k-1}$ และ $r_k|r_k$

ดังนั้นจากทฤษฎี 2.1 ข้อ 5 $r_k|r_{k-2}$

แต่ $r_k|r_{k-1}$ และ $r_k|r_{k-2}$

ดังนั้นจากทฤษฎี 2.1 ข้อ 5 $r_k|r_{k-3}$

ดำเนินการอย่างนี้ไปเรื่อย ๆ จะพบว่า $r_k|a$ และ $r_k|b$

สมมุติว่า f เป็นตัวหารร่วมใด ๆ ของ a และ b

ดังนั้น $f|a$ และ $f|b$

จากสมการแรกและทฤษฎี 2.1 ข้อ 5 จะพบว่า $f|r_1$

แต่ถ้า $f|b$ และ $f|r_1$

จากสมการถัดมาและทฤษฎี 2.1 ข้อ 5 จะพบว่า $f|r_2$

ดำเนินการกระทำนี้ไปเรื่อย ๆ จะพบว่า $f|r_k$

ดังนั้นตามนิยามของ ห.ร.ม. $r_k = (a, b)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.7 จงหา ห.ร.ม. ของ 351 กับ 183

วิธีทำ

$$\begin{aligned} 351 &= 183\cdot 1 + 168 \\ 183 &= 168\cdot 1 + 15 \\ 168 &= 15\cdot 11 + 3 \\ 15 &= 3\cdot 5 \\ (351, 183) &= 3 \end{aligned}$$

จากตัวอย่างจะพบว่าเราสามารถจะหาจำนวนเต็ม m และ n ซึ่งทำให้ $3 = 351m + 183n$ ได้ โดยเริ่มจากสมการถัดจากสมการสุดท้ายขึ้นมา แล้วแทนค่าเศษแต่ละสมการมาเรื่อย ๆ จนมาถึงสมการแรก ก็จะได้ค่า m, n ตามต้องการดังนี้คือ

$$\begin{aligned} 3 &= 168 - 15\cdot 11 \\ &= 168 - (183 - 168)11 \\ &= 168\cdot 12 - 183\cdot 11 \\ &= (351 - 183)12 - 183\cdot 11 \\ &= 351\cdot 12 + 183(-23) \end{aligned}$$

นั่นคือ $3 = 351m + 183n$ เมื่อ $m = 12$ และ $n = -23$

อย่างไรก็ตามสำหรับสมการ $3 = 351m + 183n$ นี้ไม่ได้มีค่า m, n เพียงคู่ที่หาได้เท่านั้น ดังตัวอย่างนี้

$$\begin{aligned} 3 &= 351\cdot 12 + 183(-23) \\ &= 351\cdot 12 + 351\cdot 183 - 351\cdot 183 + 183(-23) \\ &= 351\cdot 195 + 183(-374) \end{aligned}$$

นั่นคือ $m = 195$, $n = -374$

แบบฝึกหัด 2.3

1. จงหา (357, 629) และหาจำนวนเต็ม x และ y ซึ่งทำให้ (357, 629) = 357x + 629y
2. จงหา (−357, 629) และหาจำนวนเต็ม x และ y ซึ่งทำให้ (−357, 629) = −357x + 629y
3. จงหา (287, 203) และหาจำนวนเต็ม x และ y ซึ่งทำให้ (287, 203) = 287x + 203y
4. จงหา (1234, 234) และ (714, 2030, 2205)
5. จงหาจำนวนเต็ม x และ y ซึ่งทำให้ 394x + 500y = 2

2.4 ตัวคูณร่วมน้อย (Least Common Multiple)

ถ้า a, b และ m เป็นจำนวนเต็มซึ่ง a|m และ b|m แล้ว จะเรียก m ว่าเป็นตัวคูณร่วมของ a และ b เนื่องจากการหารด้วยศูนย์ไม่มีความหมาย ดังนั้น a และ b จะต้องไม่เท่ากับศูนย์ทั้งคู่ ในกรณีนี้จะพบว่าทั้ง ab และ $-ab$ ต่างก็เป็นตัวคูณร่วมของ a และ b ซึ่งตัวหนึ่งเป็นจำนวนบวก ดังนั้นจาก well-ordering principle จะต้องมีจำนวนเต็มบวกตัวที่น้อยที่สุดซึ่งเป็นตัวคูณร่วม

นิยาม 2.7 ถ้า m เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุดซึ่งเป็นตัวคูณร่วมของ a และ b แล้ว เรียก m ว่าเป็น **"ตัวคูณร่วมน้อย"** (ค.ร.น.) ของ a และ b เขียนแทนด้วย $[a, b] = m$

นิยาม 2.7 อาจเขียนได้อีกอย่างหนึ่งดังนี้

ให้ a, b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ c เป็นจำนวนเต็ม

ถ้า a|c และ b|c แล้ว เรียก c ว่าเป็นตัวคูณร่วมของ a และ b

ถ้า m เป็นจำนวนเต็มบวกและสอดคล้องกับเงื่อนไขต่อไปนี้

1. m เป็นตัวคูณร่วมของ a และ b $(a|m, b|m)$

2. ถ้า c เป็นตัวคูณร่วมใด ๆ ของ a และ b แล้ว m หาร c ได้ลงตัว (ถ้า a|c, b|c แล้ว m|c) แล้ว เรียก m ว่าเป็นตัวคูณร่วมน้อยของ a และ b

ตัวอย่าง 2.8 -60 เป็นตัวคูณร่วมของ -6 และ -15

แต่ $[-6, -15] = 30$

ทฤษฎี 2.16

ถ้า a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์แล้ว $[a, b](a, b) = |ab|$

พิสูจน์ เพราะว่า a และ b เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์

ดังนั้น ห.ร.ม. ของ a และ b ต้องไม่เท่ากับศูนย์ สมมุติว่าเท่ากับ d และ ค.ร.น. ของ a และ b เท่ากับ m

เพราะฉะนั้น $\frac{|ab|}{d}$ เป็นจำนวนเต็ม

แต่ $\frac{|ab|}{d} = a\cdot(\pm\frac{b}{d}) = b\cdot(\pm\frac{a}{d})$

เพราะฉะนั้น $\frac{|ab|}{d}$ เป็นตัวคูณร่วมของ a และ b ซึ่งมีค่าเป็นบวก

และ $\frac{|ab|}{d} \geqslant m$ **(A)**

เพราะว่า |ab| เป็นตัวคูณร่วมของ a และ b

ดังนั้น $\frac{|ab|}{m}$ เป็นจำนวนเต็มบวก ตามนิยามของ ค.ร.น.

แต่ m เป็นพหุคูณของ a ให้ $m = ka$ เมื่อ k เป็นจำนวนเต็ม

เพราะฉะนั้น $k \cdot \frac{|ab|}{m} = \pm \frac{k(ab)}{ka} = \pm b$

แสดงว่า $\frac{|ab|}{m} | b$

ในทำนองเดียวกันเราจะพิสูจน์ได้ว่า $\frac{|ab|}{m} | a$

เพราะฉะนั้น $\frac{|ab|}{m} \leqslant d = (a, b)$ **(B)**

จาก (A) และ (B) จะได้ว่า

$$|ab| = md = [a, b](a, b)$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.9 จากตัวอย่าง 2.7 เราทราบว่า $(351, 183) = 3$

ดังนั้น $[351, 183] = \frac{351 \cdot 183}{3} = 21411$

เราสามารถจะหา ค.ร.น. ของจำนวนเต็มซึ่งมีมากกว่าสองจำนวนได้ เช่นเดียวกันกับหา ห.ร.ม. ดังทฤษฎีต่อไปนี้

ทฤษฎี 2.17

ถ้า $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์แล้ว

$[a_1, a_2, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$

พิสูจน์ วิธีพิสูจน์เหมือนกับการพิสูจน์ทฤษฎี 2.13 ให้ผู้อ่านทำเป็นแบบฝึกหัด

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.10 จงหา ค.ร.น. ของ 108, 96, 90

วิธีทำ เริ่มแรกเราจะต้องหา ห.ร.ม. ของ 108, 96, 90 เสียก่อนโดยหาทีละคู่ตามวิธีการหาของยูคลิเดียนอัลกอริธึม

จะได้ $(108, 96) = 12$ และ $(12, 90) = 6$

ดังนั้นตามทฤษฎี 2.13 $(108, 96, 90) = 6$

จากทฤษฎี 2.16 จะได้ $[108, 96] = \frac{108 \cdot 96}{12} = 864$

ใช้ยูคลิเดียนอัลกอริธึมหา (864, 90) = 18

ดังนั้น $[864, 90] = \frac{864 \cdot 90}{18} = 4320$

เพราะฉะนั้น $[108, 96, 90] = [[108, 96], 90]$

$= [864, 90]$

$= 4320$

ทฤษฎี 2.18

ถ้า a, b และ m เป็นจำนวนเต็มแล้ว $[ma, mb] = |m|[a, b]$

พิสูจน์ ถ้า $a \neq 0, b \neq 0$ และ $m \neq 0$ แล้ว จะได้ว่า $(ma, mb) \neq 0$

ดังนั้นตามทฤษฎี 2.16

$(ma, mb)[ma, mb] = |mamb|$

$= |m||m||ab|$

แต่ $(a, b)[a, b] = |ab|$ ตามทฤษฎี 2.16

ดังนั้น $|m||m||ab| = |m||m|(a, b)[a, b]$

จากทฤษฎี 2.10 เราทราบว่า $|m|(a, b) = (ma, mb)$

เพราะฉะนั้น $|m||m|(a, b)[a, b] = (ma, mb)|m|[a, b]$

นั่นคือ $(ma, mb)[ma, mb] = (ma, mb)|m|[a, b]$

หรือ $[ma, mb] = |m|[a, b]$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 2.4

1. จงหา [108, 84], [756, 78], [357, 629], [−357, 629]
2. จงหา [357, 629, 221]
3. จงหา [299, 377, 403]
4. จงพิสูจน์ว่า a|b ก็ต่อเมื่อ [a, b] = |b|
5. จงหา $(12n^2+16n+6, 6n+5)$ และหา $[12n^2+16n+6, 6n+5]$ เมื่อ n เป็นจำนวนเต็ม
6. จงพิสูจน์ว่า $[9n+8, 6n+5] = 54n^2+93n+40$ สำหรับ n เป็นจำนวนเต็ม
7. จงพิสูจน์ว่า [a, b, c] = [[a, b], c]

2.5 สมการไดโอแฟนไทน์เชิงเส้น (Linear Diophantine Equations)

ถ้าให้ a, b, c เป็นจำนวนจริง ซึ่งทั้ง a และ b ไม่เท่ากับศูนย์แล้ว สมการ $ax+by=c$ เรียกว่าสมการเชิงเส้น เพราะว่ากราฟของสมการนี้จะเป็นเส้นตรงบนระนาบ xy

ในการแก้สมการชนิดนี้บางสมการก็มีคำตอบมากมาย แต่บางสมการก็ไม่มีคำตอบเป็นจำนวนเต็ม เช่น สมการ $x+y=1$ เราสามารถจะหาจำนวนเต็มมาแทนค่า x, y แล้วบวกกันเท่ากับ 1 ได้มากมายหลายชุด แต่สมการ $6x+8y=7$ ไม่มีคำตอบ เพราะถ้าเราแทนค่า x, y ด้วยจำนวนเต็มใดก็ตามจะทำให้ทางซ้ายของสมการเป็นจำนวนเต็มคู่ ซึ่งจะไม่มีโอกาสเท่ากับ 7 ซึ่งเป็นจำนวนเต็มคี่ได้เลย

นิยาม 2.8 สมการ $ax+by=c$ ซึ่ง a, b, c เป็นจำนวนเต็มและทั้ง a และ b ไม่เท่ากับศูนย์ จะเรียกว่าเป็นสมการ **"ไดโอแฟนไทน์เชิงเส้น" (linear diophantine equation)** ถ้าสมการนี้มีคำตอบเป็นจำนวนเต็ม

จากทฤษฎี 2.9 เราทราบว่าสมการ $ax+by=c$ จะมีคำตอบเป็นจำนวนเต็มก็ต่อเมื่อ $(a, b)|c$ สำหรับการแก้สมการหาค่า x, y นี้เราอาจจะพิจารณาจากการหาจุดต่าง ๆ บนเส้นตรง เพราะค่า x, y แต่ละคู่ที่ได้มาก็คือโคออร์ดิเนตของจุดบนระนาบ XY นั่นเอง จุดบนระนาบ XY จะเรียกว่า **"จุดแลททีซ" (lattice point)** ถ้าโคออร์ดิเนตของจุดนี้เป็นจำนวนเต็ม ดังนั้นในการแก้สมการไดโอแฟนไทน์ $ax+by=c$ นี้ก็คล้ายกับการหาจุดแลททีซทั้งหมดซึ่งอยู่บนเส้นตรงซึ่งมีสมการ $ax+by=c$ ในระนาบ XY นั่นเอง ซึ่งเส้นตรงนี้จะมีความชันเท่ากับ

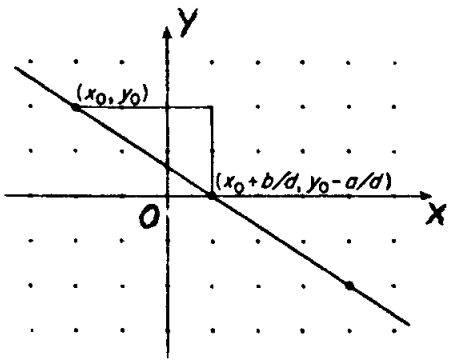
$$-\frac{a}{b}=\frac{-\frac{a}{d}}{\frac{b}{d}}$$

เมื่อ $d=(a, b)$ ดังนั้นถ้า x_0, y_0 เป็นคำตอบหนึ่งแล้ว

$$x_0+\frac{kb}{d},\ y_0-\frac{ka}{d}$$

จะเป็นคำตอบทั่วไปของสมการสำหรับ k ซึ่งเป็นจำนวนเต็มใด ๆ

รูปต่อไปนี้ คือกราฟของสมการไดโอแฟนไทน์ $2x+3y=2$



ทฤษฎี 2.19

ให้ ห.ร.ม. ของ a และ b เท่ากับ d ถ้า x_0, y_0 เป็นคำตอบหนึ่งของสมการไดโอแฟนไทน์ $ax+by = c$ แล้ว คำตอบทั่วไปของสมการนี้จะเป็น

$$x = x_0+\frac{kb}{d},\ y = y_0-\frac{ka}{d} \quad \text{เมื่อ k เป็นจำนวนเต็ม}$$

พิสูจน์ สมมติว่า x_1, y_1 เป็นคำตอบของสมการไดโอแฟนไทน์แล้ว

$$ax_1+by_1 = c = ax_0+by_0$$

$$a(x_1-x_0) = -b(y_1-y_0) \qquad \text{..... (A)}$$

แต่ $(a, b) = d$

ดังนั้นจะต้องมีจำนวนเต็ม a' และ b' ซึ่ง $(a', b') = 1$

และทำให้ $a = a'd$ และ $b = b'd$

แทนค่า a และ b ใน (A) และใช้ d หารทั้งสองข้างจะได้

$$a'(x_1-x_0) = -b'(y_1-y_0) \qquad \text{..... (B)}$$

แต่ (y_1-y_0) เป็นจำนวนเต็ม

แสดงว่า $b' | a'(x_1, -x_0)$ และ $(a', b') = 1$

ดังนั้น $b' | (x_1-x_0)$ ตามทฤษฎี 2.7

นั่นคือ $x_1-x_0 = kb'$ สำหรับ k ซึ่งเป็นจำนวนเต็ม

แทนค่าใน (B) และใช้ b' หารทั้งสองข้าง จะได้

$$a'k = -(y_1-y_0)$$

$$y_1-y_0 = -ka'$$

นั่นคือ

$$x_1 = x_0+kb' = x_0+\frac{kb}{d}$$

$$y_1 = y_0-ka' = y_0-\frac{ka}{d}$$

แต่ x_1, y_1 เป็นคำตอบใด ๆ ของสมการไดโอแฟนไทน์

$$ax+by = c$$

ดังนั้น $x = x_0+\frac{kb}{d},\ y = y_0-\frac{ka}{d}$

เป็นคำตอบทั่วไปของสมการไดโอแฟนไทน์นี้

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 2.11 จงแก้สมการ $288x + 51y = 3$ และหาคำตอบทั่วไปด้วย

วิธีทำ ใช้ยูคลิเดียนอัลกอริธึม หา ห.ร.ม. ของ 288 กับ 51 ได้ดังนี้

$$\begin{aligned} 288 &= 51 \cdot 5 + 33 \\ 51 &= 33 \cdot 1 + 18 \\ 33 &= 18 \cdot 1 + 15 \\ 18 &= 15 \cdot 1 + 3 \\ 15 &= 3 \cdot 5 \end{aligned}$$

แสดงว่า $(288, 51) = 3$ และ $(288, 51) | 3$ แสดงว่าสมการนี้มีคำตอบเป็นจำนวนเต็ม เราจะหาค่า x, y ได้โดยวิธีแทนค่าเศษซึ่งเริ่มจากบรรทัดสุดท้ายในขบวนการหา ห.ร.ม. โดยใช้ยูคลิเดียนอัลกอริธึมไปเรื่อย ๆ ดังนี้

$$\begin{aligned} 3 &= 18 \cdot 1 - 15 \\ &= 18 \cdot 1 - (33 - 18 \cdot 1) \\ &= 18 \cdot 2 - 33 \\ &= (51 - 33 \cdot 1)(2) - 33 \\ &= 51 \cdot 2 - 33 \cdot 3 \\ &= 51 \cdot 2 - (288 - 51 \cdot 5)(3) \\ &= 51 \cdot 17 - 288 \cdot 3 \\ 3 &= 288(-3) + 51 \cdot 17 \end{aligned}$$

นั่นคือ $3 = 288x + 51y$ เมื่อ $x = -3, y = 17$

แสดงว่า $x_0 = -3, y_0 = 17$

$$\begin{aligned} x &= -3 + 51\, k/3 = -3 + 17k \\ y &= 17 - 288\, k/3 = 17 - 96\, k \end{aligned}$$

ตัวอย่าง 2.12 จงแก้สมการ $30x + 42y = 12$

วิธีทำ ใช้ยูคลิเดียนอัลกอริธึม หา ห.ร.ม. ของ 30 กับ 42

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 \end{aligned}$$

ดังนั้น $(30, 42) = 6$ ซึ่ง $(30, 42) | 12$

แสดงว่าสมการนี้มีคำตอบเป็นจำนวนเต็ม

หาค่า x, y โดยวิธีแทนค่าเศษเช่นเดียวกับตัวอย่างแรก

$$6 = 30 - 12 \cdot 2$$
$$= 30 - (42 - 30)(2)$$
$$6 = 30 \cdot 3 + 42(-2)$$
$$12 = 30 \cdot 6 + 42(-4)$$

แต่ $12 = 30x + 42y$

ดังนั้น $x_0 = 6, y_0 = -4$

แล้ว $x = 6 + 7k$

$y = -4 - 5k$

ตัวอย่าง 2.13 จงหาคำตอบที่เป็นจำนวนเต็มบวกของสมการ $7x + 5y = 100$

วิธีทำ ห.ร.ม.ของ 7 และ 5 คือ 1 ซึ่งเขียนในรูปสมการได้ดังนี้คือ

$$7 \cdot 3 + 5(-4) = 1$$

ดังนั้น $7 \cdot 300 + 5(-400) = 100$

แสดงว่า $x_0 = 300$ และ $y_0 = -400$

นั่นคือ $x = 300 + 5k, y = -400 - 7k$

เราต้องการคำตอบที่เป็นจำนวนเต็มบวกเราจะต้องหาค่า k ให้สอดคล้องกับ

$$300 + 5k > 0$$

และ $-400 - 7k > 0$

ซึ่งจะได้ $-60 < k < -57\frac{1}{7}$ ดังนั้นสมการนี้มีคำตอบที่เป็นจำนวนเต็มบวกเพียงสอง

คำตอบเท่านั้นคือ เมื่อ $k = -59, k = -58$

$k = -59, \quad x = 5, \quad y = 13$

$k = -58, \quad x = 10, \quad y = 6$

แบบฝึกหัด 2.5

1. จงแก้สมการไดโอแฟนไทน์ต่อไปนี้ และหาคำตอบทั่วไป

   1.1 $5x + 11y = 92$

   1.2 $20x + 17y = 93$

   1.3 $738x + 621y = 45$

   1.4 $57x - 87y = 342$

   1.5 $1411x + 1547y = 224$

2. จงหาคำตอบซึ่งเป็นจำนวนเต็มบวกทั้งหมดของ $23x + 37y = 212$

3. ชายผู้หนึ่งมีเงินอยู่ 530 บาท ต้องการจะซื้อทุเรียน และส้มโอ ซึ่งทุเรียนราคาผลละ 70 บาท และส้มโอราคาผลละ 50 บาท อยากทราบว่าชายผู้นี้จะซื้อผลไม้ได้อย่างละกี่ผล (ทุเรียน 4 ผล, ส้มโอ 5 ผล)

4. หอพักแห่งหนึ่งมีห้องให้เช่าสองแบบ ห้องแบบ ก. ค่าเช่าเดือนละ 87 บาท แบบ ข. ค่าเช่าเดือนละ 123 บาท ปรากฏว่าแต่ละเดือนเจ้าของหอพักเก็บค่าเช่าได้เป็นเงินรวมทั้งสิ้น 8733 บาท อยากทราบว่าหอพักนี้มีห้องเช่าแบบละกี่ห้อง (82 แบบ ก. และ 13 แบบ ข. หรือ 41 แบบ ก. และ 42 แบบ ข.)

2.6 เกรทเทส อินทิเจคร์ ฟังก์ชัน (The Greatest Integer Function)

นิยาม 2.9 ถ้า x เป็นจำนวนจริง แล้ว [x] แทนจำนวนเต็มที่มีค่ามากที่สุดซึ่งน้อยกว่า หรือเท่ากับ x หรืออาจจะกล่าวอีกอย่างหนึ่งว่า

$$[x] \leqslant x < [x]+1$$

ตัวอย่าง 2.14 $[5\frac{1}{2}] = 5, \quad [-3\cdot 5] = -4, \quad [0] = 0$

$$[\sqrt{7}] = 2, \quad [\pi] = 3$$

ทฤษฎี 2.20

ให้ α, β, θ เป็นจำนวนจริง และ a, n เป็นจำนวนเต็ม

1. $\alpha - 1 < [\alpha] \leqslant \alpha$
2. ถ้า $a \leqslant \alpha$, แล้ว $a \leqslant [\alpha]$
3. ถ้า $a > \alpha$, แล้ว $a \geqslant [\alpha]+1 > [\alpha]$
4. ถ้า $\alpha \leqslant \beta$, แล้ว $[\alpha] \leqslant [\beta]$
5. ถ้า $\theta = \alpha - [\alpha]$, แล้ว $0 \leqslant \theta < 1$
6. ถ้า $\alpha = n+\theta$ ซึ่ง $0 \leqslant \theta < 1$, แล้ว $n = [\alpha]$
7. สำหรับ n เป็นจำนวนเต็ม $[\alpha+n] = [\alpha]+n$
8. ถ้า $a = bq+r$ ซึ่ง $0 \leqslant r < b$ แล้ว $q = [a/b]$

พิสูจน์ 1. $\alpha - 1 < [\alpha] \leqslant \alpha$ ก็คือการจัดรูปของนิยามของ $[\alpha]$

2. ถ้า $a+1 > \alpha$ แล้ว $a \leqslant \alpha < a+1$ และ $a = [\alpha]$ ตามนิยาม 2.9
   ถ้า $a+1 > \alpha$ แล้ว $a+1 \leqslant \alpha$ และ $a \leqslant \alpha - 1 < [\alpha]$ จากข้อ 1.
   ดังนั้นถ้า $a \leqslant \alpha$ แล้ว $a \leqslant [\alpha]$
3. จากนิยาม $[\alpha] \leqslant \alpha$ แต่ $a > \alpha$ ตามที่กำหนดให้
   ดังนั้น $a > [\alpha]$ แล้ว $a \geqslant [\alpha]+1$ เมื่อ a และ $[\alpha]$ เป็นจำนวนเต็ม
   สรุปว่าถ้า $a > \alpha$ แล้ว $a \geqslant [\alpha]+1 > [\alpha]$
4. เพราะว่า $\alpha \leqslant \beta$ แต่ $[\alpha] \leqslant \alpha$ ตามนิยาม
   เพราะฉะนั้น $[\alpha] \leqslant \beta$ แต่ $[\alpha]$ เป็นจำนวนเต็ม
   ดังนั้นจากข้อ 2 สรุปได้ว่า $[\alpha] \leqslant [\beta]$

5., 6., 7., ให้ผู้อ่านทำเป็นแบบฝึกหัด

8. เพราะว่า $a = bq + r$ ซึ่ง $0 \leq r < b$

ดังนั้น $\frac{a}{b} = q + \frac{r}{b}$

ซึ่ง $0 \leq r/b < 1$

เพราะฉะนั้น จากข้อ 6. จะสรุปได้ว่า $q = [\, a/b \,]$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 2.21

ให้ α เป็นจำนวนจริงใด ๆ และ n เป็นจำนวนเต็มซึ่งมากกว่าศูนย์แล้ว

$$[\, [\alpha]/n \,] = [\, \alpha/n \,]$$

พิสูจน์ จากนิยามเราทราบว่า $[\, \alpha/n \,] \leq \alpha/n < [\, \alpha/n \,] + 1$

เพราะฉะนั้น $n \cdot [\, \alpha/n \,] \leq \alpha < n \cdot [\, \alpha/n \,] + n$

จากข้อ 2. และข้อ 3. ของทฤษฎี 2.20 จะได้ว่า

$$n \cdot [\, \alpha/n \,] \leq [\, \alpha \,] < n \cdot [\, \alpha/n \,] + n$$

$$[\, \alpha/n \,] \leq [\, \alpha \,]/n < [\, \alpha/n \,] + 1$$

ดังนั้นตามนิยาม 2.9

$$[\, [\alpha]/n \,] = [\, \alpha/n \,] \text{ เพราะ } [\, \alpha/n \,] \text{ เป็นจำนวนเต็ม}$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 2.6

1. **จงพิสูจน์ข้อ** 5, 6, 7 ของทฤษฎี 2.20
2. จงหาค่าของจำนวนต่อไปนี้

   1) $[2 \cdot 7]$ 2) $-[3 \cdot 5]$ 3) $[-\sqrt{2}]$

   4) $-[\sqrt{2}]$ 5) $-[-2 \cdot 7]$ 6) $[-3 \cdot 5 + 0 \cdot 5]$

   7) $[-\sqrt{2} + 0 \cdot 5]$ 8) $-[-50/4]$ 9) $[50/4 + 1/2]$
3. **จงบอกเงื่อนไขที่ทำให้** $[\alpha] + [\alpha] = [2\alpha]$
4. **จงพิสูจน์ว่าจำนวนเต็มซึ่งมีค่าใกล้เคียงจำนวนจริง** α มากที่สุดคือ $[\alpha + 1/2]$
5. **จงพิสูจน์ว่า** $[\alpha] + [\beta] \leqslant [\alpha + \beta]$ สำหรับ α, β เป็นจำนวนจริง
   (**แนะให้ใช้ข้อ** 4 ของทฤษฎี 2.20)