# บทที่ 3
# การลงรอยกัน
# (Congruences)

## 3.1 การลงรอยกัน (Congruences)

ถ้า $m$ เป็นจำนวนเต็มบวกใด ๆ และ $a$ เป็นจำนวนเต็ม จากขั้นตอนวิธีการหารจะมีจำนวนเต็ม $q$ และ $r$ โดยที่ $0 \leqslant r \leqslant m-1$ และ

$$a = qm + r$$

นั่นคือ เศษที่เกิดจากการหารจำนวนเต็มใด ๆ ด้วย $m$ ที่เป็นไปได้ คือ $0, 1, 2, \ldots, m-1$ เท่านั้น

ดังนั้น ถ้าให้ $a$ และ $b$ เป็นจำนวนเต็มใด ๆ ที่มีเศษที่เกิดจากการหารด้วย $m$ เท่ากัน เราจะได้ว่า

$$a = qm + r$$

และ $$b = q'm + r$$

โดยที่ $q, q'$ เป็นจำนวนเต็ม และ $r$ เป็นเศษ

ผลที่ตามมาก็คือ

$$a - qm = b - q'm$$

ซึ่งได้ว่า

$$a - b = (q - q')m$$

นั่นคือ $m|(a-b)$

ดังนั้น เราจึงจัดกลุ่มจำนวนเต็มที่มีเศษที่เกิดจากการหารด้วย $m$ เท่ากัน ดังนี้

**บทนิยาม 3.1** ให้ $a, b$ เป็นจำนวนเต็ม และ $m$ เป็นจำนวนเต็มบวก เรากล่าวว่า $a$ และ $b$ **เป็นจำนวนลงรอยกันมอดุโล** $m$ (a is congruent to b modulo m) ถ้า $m|(a-b)$ และเขียนแทนด้วย $a \equiv b \pmod{m}$

และในกรณีที่ $m \nmid (a-b)$ เรากล่าวว่า a และ b ไม่เป็นจำนวนลงรอยกันมอดุโล m (a and b are incongruent modulo m) เขียนแทนด้วย $a \not\equiv b \pmod{m}$

โดยทั่วไป ถ้า $a \equiv b \pmod{m}$ แล้ว เรากล่าวว่า b **เป็นเศษตกค้างของ** a **มอดุโล** m (b is a residue of a modulo m)

**ตัวอย่าง 3.1**

$22 \equiv 4 \pmod{9}$ เพราะว่า $9 \mid (22-4)$

$3 \equiv -9 \pmod{4}$ เพราะว่า $4 \mid (3-(-9))$ #

**ทฤษฎีบท 3.1** ให้ a, b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้ว $a \equiv b \pmod{m}$ ก็ต่อเมื่อมีจำนวนเต็ม k ที่ทำให้ $a = b + km$

**พิสูจน์** เห็นได้ชัดจากบทนิยาม 3.1 และบทนิยามการหารลงตัว #

ถ้า m เป็นจำนวนเต็มบวก และ a, q, r เป็นจำนวนเต็ม โดยที่ $0 \leqslant r < m$ และ

$$a = qm + r$$

แล้ว จะได้ว่า $a \equiv r \pmod{m}$ ด้วย เนื่องจาก $a - r = mq$

**บทนิยาม 3.2** ถ้า $a = mq + r$ โดยที่ $0 \leqslant r < m$ แล้ว เรียก r ว่าเป็น **เศษตกค้างที่เล็กที่สุดของ** a **มอดุโล** m (the least residue of a modulo m)

**ทฤษฎีบท 3.2** กำหนด a, b และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ แล้ว r เป็นเศษตกค้างที่เล็กที่สุดของ a และ b มอดุโล m ก็ต่อเมื่อ $a \equiv b \pmod{m}$

**พิสูจน์** สมมติ r เป็นเศษตกค้างที่เล็กที่สุดของ a และ b มอดุโล m

ดังนั้น มีจำนวนเต็ม q, q′ โดยที่

$$a = mq + r \qquad 0 \leqslant r < m$$

$$b = mq' + r \qquad 0 \leqslant r < m$$

เพราะฉะนั้น

$$a - b = m(q - q')$$

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

ในทางกลับกันสมมติ $a \equiv b \pmod{m}$

ให้ $r, r'$ เป็นเศษตกค้างที่เล็กที่สุดของ a และ b มอดุโล m ตามลำดับ
นั่นคือ มีจำนวนเต็ม $q, q'$ ที่ทำให้

$$a = mq + r \qquad 0 \leqslant r < m$$

$$b = mq' + r' \qquad 0 \leqslant r' < m$$

เพราะฉะนั้น $a - b = m(q - q') + (r - r')$

เพราะว่า $a \equiv b \pmod m$ จะได้ $m|(a-b)$ ผลที่ตามมาก็คือ $m|r - r'$

แต่ $|r - r'| < m$ จึงสรุปได้ว่า

$$|r - r'| = 0$$

นั่นคือ $r = r'$ #

**ทฤษฎีบท 3.3** ให้ m เป็นจำนวนเต็มบวก แล้วการลงรอยกันมอดุโล m สอดคล้องคุณสมบัติต่อไปนี้

ก. **คุณสมบัติการสะท้อน** (reflexive property)
กล่าวคือ ถ้า a เป็นจำนวนเต็ม แล้ว $a \equiv a \pmod m$

ข. **คุณสมบัติสมมาตร** (symmetric property)
กล่าวคือ ถ้า a และ b เป็นจำนวนเต็ม โดยที่ $a \equiv b \pmod m$ แล้ว $b \equiv a \pmod m$

ค. **คุณสมบัติการถ่ายทอด** (transitive property)
กล่าวคือ ถ้า a, b และ c เป็นจำนวนเต็ม โดยที่ $a \equiv b \pmod m$ และ $b \equiv c \pmod m$ แล้ว $a \equiv c \pmod m$

**พิสูจน์** ก. เนื่องจาก $a - a = 0$ และ $m|0$ จึงได้ว่า $a \equiv a \pmod m$

ข. สมมติ $a \equiv b \pmod m$ ดังนั้น จะมีจำนวนเต็ม k ที่ทำให้

$$a = b + km$$

นั่นคือ $a - b = km$

และได้ว่า

$$b - a = (-k)m$$

นั่นคือ $m|(b-a)$

เพราะฉะนั้น $b \equiv a \pmod m$

ค. เพราะว่า $a \equiv b \pmod m$ และ $b \equiv c \pmod m$
ดังนั้น จะมีจำนวนเต็ม $k, k'$ ที่ทำให้

$$a = b + km$$

$$b = c + k'm$$

นั่นคือ

$$a + b = (b + c) + (k + k')m$$

ซึ่งได้ว่า

$$a = c + (k + k')m$$

ผลที่ตามมาก็คือ

$$a \equiv c \pmod{m}$$ #

เนื่องจากเศษที่เป็นไปได้จากการหารจำนวนเต็มใด ๆ ด้วย m คือ 0, 1, 2, ..., m − 1 ดังนั้น จำนวนเต็มจะแบ่งออกเป็นเซตต่าง ๆ m เซต ตามค่าของเศษที่เกิดจากการหารด้วยจำนวนเต็มบวก m และผลจากทฤษฎีบท 3.3 จะพบว่า แต่ละ m เซตเหล่านั้นจะไม่มีสมาชิกร่วมกันเลย เซตทั้ง m เซตเรียกว่า **ชั้นของการลงรอยกันมอดุโล** m (congruence classes modulo m) และสมาชิกทุกคู่ในแต่ละชั้นจะเป็นจำนวนลงรอยกันมอดุโล m เสมอ

**ตัวอย่าง 3.2** พิจารณาในมอดุโล 4

เศษที่เป็นไปได้คือ 0, 1, 2 หรือ 3

ดังนั้น

$$\ldots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \ldots \equiv \ldots \pmod{4}$$
$$\ldots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \ldots \equiv \ldots \pmod{4}$$
$$\ldots \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots \equiv \ldots \pmod{4}$$
$$\ldots \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv \ldots \equiv \ldots \pmod{4}$$

และชั้นของการลงรอยกันมอดุโล 4 ทั้ง 4 ชั้น คือ

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$\{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$\{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$\{\ldots, -5, -1, 3, 7, 11, \ldots\}$$ #

ถ้าเลือกสมาชิกของแต่ละชั้นของการลงรอยกันมอดุโล m มาชั้นละ 1 ตัว เซตที่ประกอบด้วยแต่ละสมาชิกของแต่ละชั้นที่เลือกมาชั้นละ 1 ตัวนั้น เรียกว่า ระบบบริบูรณ์ของเศษตกค้างมอดุโล m

**บทนิยาม 3.3** เซตของจำนวนเต็ม m จำนวน ซึ่งมีคุณสมบัติว่า สำหรับจำนวนเต็ม a ใด ๆ a จะเป็นจำนวนลงรอยกับจำนวนเต็มในเซตนี้หนึ่งจำนวนเสมอ เรียกว่า **ระบบบริบูรณ์ของเศษตกค้างมอดุโล** m (a complete system of residues modulo m)

**ตัวอย่าง 3.3** พิจารณาในมอดุโล 4

$\{0, 1, 2, 3\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล 4

$\{-8, -3, -6, 3\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล 4 #

**ตัวอย่าง 3.4** สำหรับจำนวนเต็มบวก m ใด ๆ

$\{0, 1, 2, \ldots, m-1\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล m #

**บทนิยาม 3.4** สำหรับจำนวนเต็มบวก m เรียก $\{0, 1, 2, \ldots, m-1\}$ ว่า เป็น **เซตของเศษตกค้างที่ไม่เป็นลบที่เล็กที่สุดมอดุโล** m (the set of least nonnegative residues modulo m)

**ทฤษฎีบท 3.4** ให้ a, b, c และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $a \equiv b \pmod{m}$ แล้ว

ก. $a + c \equiv b + c \pmod{m}$

ข. $a - c \equiv b - c \pmod{m}$

ค. $ac \equiv bc \pmod{m}$

**พิสูจน์** ก. เพราะว่า $a \equiv b \pmod{m}$ ดังนั้น $m \mid (a - b)$

และเพราะว่า

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

ดังนั้น $m \mid |(a + c) - (b + c)|$

ผลที่ตามมาก็คือ

$$a + c \equiv b + c \pmod{m}$$

ข. เพราะว่า $a \equiv b \pmod{m}$ จะได้ว่า $m \mid (a - b)$

และเพราะว่า

$$(a - c) - (b - c) = a - b$$

ดังนั้น $m \mid |(a - c) - (b - c)|$

ผลที่ตามมาก็คือ

$$a - c \equiv b - c \pmod{m}$$

ค. เพราะว่า $ac - bc = (a-b)c$

และ $a \equiv b(\text{mod } m)$ จึงได้ว่า $m|(ac-bc)$

ผลที่ตามมาก็คือ

$$ac \equiv bc(\text{mod } m)$$ #

**ตัวอย่าง 3.5** กำหนด $19 \equiv 3(\text{mod } 8)$

จะได้ $26 \equiv 10(\text{mod } 8)$

เนื่องจาก $26 = 19+7$ และ $10 = 3+7$

และ $15 \equiv -1(\text{mod } 8)$

เนื่องจาก $15 = 19-4$ และ $-1 = 3-4$

นอกจากนั้นจะได้

$38 \equiv 6(\text{mod } 8)$

เนื่องจาก $38 = 19\cdot 2$ และ $6 = 3\cdot 2$ #

จากทฤษฎีบท 3.4 จะเห็นว่า คุณสมบัติการลงรอยกันนั้นยังคงยืนยงอยู่สำหรับการดำเนินการบวก ลบ และคูณ แต่สำหรับการหารนั้นไม่จริง กล่าวคือ ถ้า $ac \equiv bc(\text{mod } m)$ แล้วข้อความ $a \equiv b(\text{mod } m)$ ไม่จริง ดังตัวอย่างต่อไปนี้

**ตัวอย่าง 3.6** เพราะว่า $14 \equiv 8(\text{mod } 6)$ และ $14 = 7\cdot 2,\ 8 = 4\cdot 2$

นั่นคือ $7\cdot 2 \equiv 4\cdot 2(\text{mod } 6)$

แต่ $7 \not\equiv 4(\text{mod } 6)$ #

แต่เมื่อเพิ่มคุณสมบัติบางประการ ทฤษฎีบทต่อไปนี้จะแสดงว่า คุณสมบัติการลงรอยกันยังคงยืนยงอยู่สำหรับการหาร แต่จะเปลี่ยนมอดุโล m เป็นมอดุโลอื่น

**ทฤษฎีบท 3.5** กำหนด a, b, c และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $d = (c, m)$ ถ้า $ac \equiv bc(\text{mod } m)$ แล้ว $a \equiv b\left(\text{mod } \frac{m}{d}\right)$

**พิสูจน์** เพราะว่า $ac \equiv bc(\text{mod } m)$ ดังนั้น $m|(ac-bc)$

นั่นคือ จะมีจำนวนเต็ม k ที่ทำให้

$$ac - bc = km$$

ดังนั้น

$$(a-b)\frac{c}{d} = k\frac{m}{d}$$

เพราะว่า $d = (c, m)$ จึงได้ว่า $\frac{c}{d}$ และ $\frac{m}{d}$ เป็นจำนวนเต็ม และ $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$

ผลที่ตามมาก็คือ $\frac{m}{d} | (a-b)$ นั่นคือ $a \equiv b\left(\text{mod } \frac{m}{d}\right)$ #

**ตัวอย่าง 3.7** เพราะว่า $50 \equiv 10\cdot 5 \equiv 20 \equiv 10\cdot 2 (\text{mod } 15)$

และ $(10, 15) = 5$

ดังนั้น โดยทฤษฎีบท 3.5

$$5 \equiv 2\left(\text{mod } \frac{15}{5}\right)$$

นั่นคือ $5 \equiv 2(\text{mod } 3)$ #

**บทแทรก 3.6** ถ้า a, b, c และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ ; $(c, m) = 1$ และ $ac \equiv bc(\text{mod } m)$ แล้ว $a \equiv b(\text{mod } m)$

**พิสูจน์** ผลจากทฤษฎีบท 3.5 #

**ตัวอย่าง 3.8** เพราะว่า $42 \equiv 6\cdot 7 \equiv 7 \equiv 1\cdot 7 (\text{mod } 5)$ และ $(7, 5) = 1$

ดังนั้น โดยบทแทรก 3.6 จึงได้ว่า $6 \equiv 1(\text{mod } 5)$ #

ทฤษฎีบทต่อไปนี้จะเป็นบทขยายสำหรับทฤษฎีบท 3.4

**ทฤษฎีบท 3.7** ให้ a, b, c, d และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $a \equiv b(\text{mod } m)$ $c \equiv d(\text{mod } m)$ แล้ว

ก. $a + c \equiv b + d(\text{mod } m)$

ข. $a - c \equiv b - d(\text{mod } m)$

ค. $ac \equiv bd(\text{mod } m)$

**พิสูจน์** ก. เพราะว่า $a \equiv b(\text{mod } m)$ และ $c \equiv d(\text{mod } m)$

ดังนั้น จะมีจำนวนเต็ม $k, \ell$ ที่ทำให้

$$a - b = km$$

$$c - d = \ell m$$

ดังนั้น

$$(a+c)-(b+d) = (a-b)+(c-d) = (k+\ell)m$$

นั่นคือ $m \mid (a+c)-(b+d)$

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

ข. เพราะว่า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$

จึงมีจำนวนเต็ม $k, \ell$ ที่ทำให้

$$a - b = km$$

$$c - d = \ell m$$

ดังนั้น

$$(a-c)-(b-d) = (a-b)-(c-d) = (k-\ell)m$$

นั่นคือ $m \mid (a-c)-(b-d)$

เพราะฉะนั้น $a - b \equiv c - d \pmod{m}$

ค. เพราะว่า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$

จึงมีจำนวนเต็ม $k, \ell$ ที่ทำให้

$$a - b = km$$

$$c - d = \ell m$$

ดังนั้น

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + (c-d)b \\ &= kmc + \ell mb \\ &= (kc + \ell b)m \end{aligned}$$

นั่นคือ $m \mid (ac - bd)$

เพราะฉะนั้น $ac \equiv bd \pmod{m}$ #

**ตัวอย่าง 3.9** เพราะว่า $13 \equiv 8 \pmod{5}$ และ $7 \equiv 2 \pmod{5}$

ดังนั้น โดยทฤษฎีบท 3.7

$$20 \equiv 13+7 \equiv 10 \equiv 8+2 \pmod{5}$$

$$6 \equiv 13-7 \equiv 6 \equiv 8-2 \pmod{5}$$

และ $91 \equiv 13 \cdot 7 \equiv 16 \equiv 8.2 \pmod{5}$ #

**ทฤษฎีบท 3.8** ให้ $\{r_1, r_2, \ldots, r_m\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล m และถ้า a เป็นจำนวนเต็มบวก โดยที่ $(a, m) = 1$ และ b เป็นจำนวนเต็มใด ๆ แล้ว $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล m

**พิสูจน์** จะแสดงว่า $ar_j + b \not\equiv ar_k + b \pmod m$ ถ้า $j \neq k$

สมมติ $j \neq k$ และ $ar_j + b \equiv ar_k + b \pmod m$

โดยทฤษฎีบท 3.4 ได้ว่า

$$ar_j \equiv ar_k \pmod m$$

และเพราะว่า $(a, m) = 1$ ดังนั้น โดยบทแทรก 3.6

$$r_j \equiv r_k \pmod m$$

ซึ่งเป็นไปไม่ได้ เนื่องจาก $j \neq k$ และ $r_j, r_k$ เป็นสมาชิกของระบบบริบูรณ์ของเศษตกค้างมอดุโล m

นั่นคือ $ar_j + b \not\equiv ar_k + b \pmod m$ ถ้า $j \neq k$

และเพราะว่า $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ ประกอบด้วยจำนวนเต็ม m จำนวน ซึ่งไม่ลงรอยกันมอดุโล m ดังนั้น

$\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ จึงเป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล m #

**ตัวอย่าง 3.10** เพราะว่า $\{0, 1, 2, \ldots, 5\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล 6 เลือก $a = 5$, $b = -3$ เพราะว่า $(5, 6) = 1$ จะได้

$\{-3, 2, 7, 12, 17, 22\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล 6 #

**ทฤษฎีบท 3.9** ให้ a, b, k และ m เป็นจำนวนเต็ม โดยที่ $k > 0$ และ $m > 0$ และ $a \equiv b \pmod m$ แล้ว $a^k \equiv b^k \pmod m$

**พิสูจน์** เพราะว่า $a \equiv b \pmod m$ ดังนั้น $m \mid (a - b)$

เพราะว่า $(a - b) \mid (a^k - b^k)$ ทุกจำนวนเต็มบวก k จึงได้ว่า $m \mid (a^k - b^k)$

นั่นคือ

$$a^k \equiv b^k \pmod m$$ #

**ตัวอย่าง 3.11** เพราะว่า $8 \equiv 3 \pmod 5$

จะได้ $512 \equiv 8^3 \equiv 3^3 \equiv 27 \pmod 5$

และเพราะว่า $27 \equiv 2 \pmod 5$

จึงได้

$$512 \equiv 2 \pmod 5$$ #

**ทฤษฎีบท 3.10** ให้ $a, b, m_1, m_2, \ldots, m_k$ เป็นจำนวนเต็ม โดยที่ $m_1, m_2, \ldots, m_k$ เป็นจำนวนเต็มบวก ถ้า

$$a \equiv b \pmod{m_1}$$
$$a \equiv b \pmod{m_2}$$
$$\vdots$$
$$a \equiv b \pmod{m_k}$$

แล้ว $a \equiv b \left(\bmod |m_1, m_2, \ldots, m_k|\right)$

โดยที่ $|m_1, m_2, \ldots, m_k|$ เป็นตัวคูณร่วมน้อยของ $m_1, m_2, \ldots, m_k$

**พิสูจน์** เพราะว่า $a \equiv b \pmod{m_1}$

$$a \equiv b \pmod{m_2}$$
$$\vdots$$
$$a \equiv b \pmod{m_k}$$

จะได้ $m_1|(a-b),\ m_2|(a-b),\ \ldots,\ m_k|(a-b)$

นั่นคือ $a-b$ เป็นตัวคูณร่วมของ $m_1, m_2, \ldots, m_k$

ผลที่ตามมาก็คือ $|m_1, m_2, \ldots, m_k|\,|(a-b)$

นั่นคือ $a \equiv b \left(\bmod |m_1, m_2, \ldots, m_k|\right)$ #

**บทแทรก 3.11** ให้ $a, b, m_1, m_2, \ldots, m_k$ เป็นจำนวนเต็ม โดยที่ $m_1, m_2, \ldots, m_k$ เป็นจำนวนเต็มบวกที่เป็นจำนวนเฉพาะต่อกันทีละคู่ กล่าวคือ $(m_i, m_j) = 1,\ i \neq j$

ถ้า $a \equiv b \pmod{m_1}$

$$a \equiv b \pmod{m_2}$$
$$\vdots$$
$$a \equiv b \pmod{m_k}$$

แล้ว $a \equiv b \left(\bmod (m_1 m_2 \ldots m_k)\right)$

**พิสูจน์** เพราะว่า $(m_i, m_j) = 1$ ถ้า $i \neq j$

จะได้

$$|m_1, m_2, \ldots, m_k| = m_1 m_2 \ldots m_k$$

จากทฤษฎีบท 3.10 จึงได้ $a \equiv b(\text{mod}(m_1 m_2 \ldots m_k))$ #

**ตัวอย่าง 3.12** เพราะว่า $15 \equiv 5(\text{mod } 2)$

$15 \equiv 5(\text{mod } 5)$

และ $(2, 5) = 1$ จึงได้ว่า

$15 \equiv 5(\text{mod } 10)$ #

ตัวอย่างต่อไปนี้จะแสดงให้เห็นว่า สามารถหาเศษตกค้างที่เล็กที่สุดของ a มอดุโล m ได้ โดยใช้คุณสมบัติของการลงรอยกัน

**ตัวอย่าง 3.13** จงหาเศษตกค้างที่เล็กที่สุดของ $25 \cdot 34 + 9 \cdot 8^5$ มอดุโล 7

**วิธีทำ** เพราะว่า $8 \equiv 1(\text{mod } 7)$

ดังนั้น $8^5 \equiv 1^5 \equiv 1(\text{mod } 7)$

เพราะว่า $9 \equiv 2(\text{mod } 7)$

จึงได้ $9 \cdot 8^5 \equiv 2 \cdot 1 \equiv 2(\text{mod } 7)$

เพราะว่า $25 \equiv -3(\text{mod } 7)$ และ $34 \equiv -1(\text{mod } 7)$

จึงได้ $25 \cdot 34 \equiv (-3)(-1) \equiv 3(\text{mod } 7)$

เพราะฉะนั้น

$$25 \cdot 34 + 9 \cdot 8^5 \equiv 3 + 2 \equiv 5(\text{mod } 7)$$

เพราะว่า $0 \leqslant 5 < 7$

ดังนั้น 5 จึงเป็นเศษตกค้างที่เล็กที่สุดของ $25 \cdot 34 + 9 \cdot 8^5$ มอดุโล 7 #

**ตัวอย่าง 3.14** จงหาเศษตกค้างที่เล็กที่สุดของ $3^{472}$ มอดุโล 242

**วิธีทำ** เพราะว่า $3^5 \equiv 243 \equiv 1(\text{mod } 242)$

ดังนั้น $3^{472} \equiv (3^5)^{94} \cdot 3^2 \equiv 1^{94} \cdot 3^2 \equiv 9(\text{mod } 242)$

เพราะว่า $0 \leqslant 9 < 242$

ดังนั้น 9 จึงเป็นเศษตกค้างที่เล็กที่สุดของ $3^{472}$ มอดุโล 242 #

## แบบฝึกหัด 3.1

1. จงหาค่าจำนวนเต็มบวก m ที่ทำให้ข้อความต่อไปนี้เป็นจริง

   1.1 $27 \equiv 5 \pmod{m}$ 1.2 $1000 \equiv 1 \pmod{m}$

   1.3 $1331 \equiv 0 \pmod{m}$

2. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคู่แล้ว $a^2 \equiv 0 \pmod{m}$

   และ ถ้า a เป็นจำนวนเต็มคี่แล้ว $a^2 \equiv 1 \pmod{m}$

3. จงแสดงว่า ถ้า a เป็นจำนวนเต็มคี่แล้ว $a^2 \equiv 1 \pmod{8}$

4. จงหาเศษตกค้างที่ไม่เป็นลบที่เล็กที่สุดของจำนวนเต็มต่อไปนี้ มอดุโล 13

   4.1 22 4.2 100

   4.3 1001 4.4 $-1$

   4.5 $-100$ 4.6 $-1000$

5. ให้ a, b, m และ n เป็นจำนวนเต็ม โดยที่ $m > 0$, $n > 0$ และ $n|m$

   จงแสดงว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $a \equiv b \pmod{n}$

6. ให้ a, b, c และ m เป็นจำนวนเต็ม โดยที่ $c > 0$, $m > 0$

   จงแสดงว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $ac \equiv bc \pmod{mc}$

7. จงแสดงว่า ถ้า a, b และ c เป็นจำนวนเต็ม โดยที่ $c > 0$ และ $a \equiv b \pmod{c}$ แล้ว $(a, c) = (b, c)$

8. กำหนด $a_j$, $b_j$ เป็นจำนวนเต็มทุก $j = 1, 2, \ldots, n$ และ m เป็นจำนวนเต็มบวก และ $a_j \equiv b_j \pmod{m}$ ทุก $j = 1, 2, \ldots, n$ แล้ว

   8.1 $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m}$

   8.2 $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod{m}$

   เมื่อ $\prod_{j=1}^{n} a_j = a_1 a_2 \ldots a_n$

9. จงใช้คุณสมบัติของการลงรอยกันตอบคำถามต่อไปนี้

   9.1 29 ชั่วโมงหลังจากเวลา 11 นาฬิกา เป็นเวลาเท่าไร

   9.2 100 ชั่วโมงหลังจากเวลา 2 นาฬิกา เป็นเวลาเท่าไร

9.3 50 ชั่วโมงก่อนเวลา 6 นาฬิกา เป็นเวลาเท่าไร

10. จงแสดงว่า ถ้า n เป็นจำนวนเต็มบวกแล้ว จงแสดงว่า

10.1 $1+2+3+\ldots+(n-1) \equiv 0 \pmod{n}$

10.2 $1^3+2^3+3^3+\ldots+(n-1)^3 \equiv 0 \pmod{n}$

11. จำนวนเต็มบวก n ที่ทำให้

$1^2+2^2+3^2+\ldots+(n-1)^2 \equiv 0 \pmod{n}$

คือจำนวนอะไร

12. จงเขียนระบบบริบูรณ์ของเศษตกค้างมอดุโล 13

13. จงเขียนระบบบริบูรณ์ของเศษตกค้างมอดุโล 13 โดยกำหนดให้ทุกจำนวนเป็นจำนวนเต็มคี่

14. จงแสดงว่า ถ้า $n \equiv 3 \pmod{4}$ แล้ว n ไม่สามารถเขียนเป็นผลบวกของกำลังสองของจำนวนเต็มสองจำนวน

15. จงเขียนระบบบริบูรณ์ของเศษตกค้างมอดุโล 5 โดยกำหนดให้ทุกจำนวนเป็นพหุคูณของ 9

16. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $22 \cdot 51 + 698^5$ มอดุโล 7

17. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $3^{20}$ มอดุโล 5

18. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $10^{515}$ มอดุโล 7

19. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $2^{12}$ มอดุโล 13

20. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $5^{16}$ มอดุโล 17

21. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $3^{22}$ มอดุโล 23

22. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ 6! มอดุโล 7

23. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ 12! มอดุโล 13

## 3.2 การลงรอยกันเชิงเส้น (Linear Congruences)

การลงรอยกันในรูปแบบของ

$$ax \equiv b(\text{mod } m)$$

เมื่อ $x$ เป็นจำนวนเต็มไม่ทราบค่า เรียกว่า **การลงรอยกันเชิงเส้นในหนึ่งตัวแปร** (linear congruence in one variable)

ในหัวข้อนี้จะได้ศึกษาถึงวิธีการหาผลเฉลยของการลงรอยกันเชิงเส้นหนึ่งตัวแปร ซึ่งจะเห็นว่า การหาผลเฉลยนี้จะคล้ายกับการหาผลเฉลยของสมการดีโอฟานทีนเชิงเส้น

ก่อนอื่นขอให้สังเกตว่า ถ้า $x = x_0$ เป็นผลเฉลยของ $ax \equiv b(\text{mod } m)$ และถ้า $x_1 \equiv x_0(\text{mod } m)$ แล้ว $ax_1 \equiv ax_0 \equiv b(\text{mod } m)$ นั่นคือ $x_1$ เป็นผลเฉลยของ $ax \equiv b(\text{mod } m)$ ด้วย ดังนั้น ถ้าสมาชิกในชั้นของการลงรอยกันมอดุโล $m$ เป็นผลเฉลยของ $ax \equiv b(\text{mod } m)$ จะได้ทุกสมาชิกในชั้นเป็นผลเฉลยด้วย ดังนั้น สมาชิกทุกตัวในชั้นจะถือว่าเป็นเพียง 1 ผลเฉลยเท่านั้น และปัญหาที่เราจะพิจารณาต่อไปก็คือ จะมีกี่ชั้นที่เป็นผลเฉลย ซึ่งจะได้ศึกษาจากทฤษฎีบทต่อไปนี้ ซึ่งจากทฤษฎีบทถ้ากล่าวว่า มีผลเฉลย $d$ ผลเฉลย จะหมายถึงมี $d$ ชั้นในมอดุโล $m$ ที่เป็นผลเฉลย

**ทฤษฎีบท 3.12** ให้ $a, b, m$ เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $d = (a, m)$ ถ้า $d \nmid b$ แล้ว $ax \equiv b(\text{mod } m)$ ไม่มีผลเฉลย ถ้า $d|b$ แล้ว $ax \equiv b(\text{mod } m)$ มีผลเฉลย และมีแน่นอน $d$ ผลเฉลย

**พิสูจน์** พิจารณา $ax \equiv b(\text{mod } m)$

จะได้ $m|(ax - b)$

กล่าวคือ มีจำนวนเต็ม $y$ ที่ทำให้ $ax - my = b$

โดยทฤษฎีบท 2.20 ถ้า $d \nmid c$ แล้ว $ax - my = b$ ไม่มีผลเฉลยที่เป็นจำนวนเต็ม

นั่นคือ $ax \equiv b(\text{mod } m)$ ไม่มีผลเฉลยที่เป็นจำนวนเต็ม ถ้า $d \nmid c$

ถ้า $d|c$ แล้ว จากทฤษฎีบท 2.20 $ax - my = b$ มีผลเฉลยมากมายเป็นจำนวนอนันต์

ให้ $x = x_0$ และ $y = y_0$ เป็นผลเฉลยหนึ่งของ $ax - my = b$

จะได้

$$x = x_0 + \frac{m}{d}n$$

$$y = y_0 + \frac{a}{d}n$$

เมื่อ $n$ เป็นจำนวนเต็มใด ๆ เป็นผลเฉลยทั่วไปของ $ax - my = b$

นั่นคือ

$$x = x_0 + \frac{m}{d}n$$

เมื่อ $n$ เป็นจำนวนเต็มใด ๆ เป็นผลเฉลยของ $ax \equiv b(\text{mod } m)$

ต่อไปจะพิจารณาว่า มีกี่ผลเฉลยที่ไม่ลงรอยกันในมอดุโล $m$

สมมติให้ $x_1 = x_0 + \frac{(m)}{d}t_1$ และ $x_2 = x_0 + \frac{(m)}{d}t_2$ เป็นผลเฉลยที่ลงรอยกันในมอดุโล $m$

จะได้

$$x_0 + \frac{(m)}{d}t_1 \equiv x_0 + \frac{(m)}{d}t_2(\text{mod } m)$$

ผลที่ตามมาก็คือ

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2(\text{mod } m)$$

เพราะว่า $\left(m, \frac{m}{d}\right) = \frac{m}{d}$

จะได้ว่า $t_1 \equiv t_2(\text{mod } d)$

นั่นคือ ถ้า $t_1 \not\equiv t_2(\text{mod } d)$ แล้ว $x_1 \not\equiv x_2(\text{mod } m)$

จึงสรุปได้ว่า ผลเฉลยที่อยู่ต่างชั้นของการลงรอยกันมอดุโล $m$ จะขึ้นอยู่กับจำนวนเต็ม $t$ ที่อยู่ต่างชั้นของการลงรอยกันมอดุโล $d$ ซึ่งมีอยู่แน่นอน $d$ ชั้น เลือก $t = 0, 1, 2, \ldots, (d-1)$

เพราะฉะนั้น ผลเฉลยทั้งหมดในแต่ละชั้นคือ

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \ldots,\ x_0 + (d-1)\frac{m}{d} \qquad \#$$

**ตัวอย่าง 3.15** จงหาผลเฉลยของ $9x \equiv 12(\text{mod } 15)$

**วิธีทำ** เพราะว่า $(9, 15) = 3$ และ $3|12$

เพราะฉะนั้น $9x \equiv 12(\text{mod } 15)$ มีผลเฉลย และมีแน่นอน 3 ผลเฉลย

พิจารณา $9x - 15y = 12$

และเขียนขั้นตอนวิธีของยุคลิดสำหรับการหาค่าตัวหารร่วมมากของ 9 และ 15

$$15 = 1\cdot 9+6$$
$$9 = 1\cdot 6+3$$
$$6 = 2\cdot 3$$

ดังนั้น

$$3 = 9-1\cdot 6$$
$$= 9-1(15-1\cdot 9)$$
$$3 = 2\cdot 9-1\cdot 15$$

และ

$$12 = 3\cdot 4 = 8\cdot 9-4\cdot 15$$

นั่นคือ

$$x_0 = 8$$

จึงได้

$$x_0,\ x_0+\frac{m}{d},\ x_0+\frac{2m}{d} \text{ เป็นผลเฉลย}$$

ซึ่งคือ 8, 13, 18

เพราะฉะนั้น ผลเฉลยทั้งสามผลเฉลยคือ

$$x \equiv 8 \pmod{15}$$
$$x \equiv 13 \pmod{15}$$
$$x \equiv 18 \pmod{15}$$

#

**ตัวอย่าง 3.16** จงหาผลเฉลยของ $51x \equiv 21 \pmod{36}$

**วิธีทำ** เพราะว่า $(51, 36) = 3$ และ $3|21$

เพราะฉะนั้น $51x \equiv 21 \pmod{36}$ มีผลเฉลยและมีแน่นอน 3 ผลเฉลย

พิจารณาการหาผลเฉลยได้ดังนี้

เพราะว่า $51 \equiv 15 \pmod{36}$

จะได้

$$51x \equiv 15x \pmod{36}$$

จึงได้

$$51x \equiv 15x \equiv 21 \pmod{36}$$

นั่นคือ $15x \equiv 21 \pmod{36}$

เพราะว่า $(15, 21) = 3$

เพราะฉะนั้น

$$5x \equiv 7\left(\bmod \frac{36}{3}\right)$$

ซึ่งคือ $5x \equiv 7 \pmod{12}$

เพราะว่า

$$-5 \equiv 5(-1) \equiv 7 \pmod{12}$$

จึงได้ $-1$ เป็นผลเฉลยของ $5x \equiv 7 \pmod{12}$ และเป็นผลเฉลยของ $51x \equiv 21 \pmod{36}$ เพราะฉะนั้น จึงได้

$$-1,\ -1+\frac{m}{d},\ -1+\frac{2m}{d} \text{ เป็นผลเฉลย}$$

ซึ่งคือ $-1,\ 11,\ 23$

ดังนั้น ผลเฉลยทั้งสามผลเฉลย คือ

$$x \equiv -1 \equiv 35 \pmod{36}$$

$$x \equiv 11 \pmod{36}$$

$$x \equiv 23 \pmod{36}$$ #

**ตัวอย่าง 3.17** จงพิจารณาผลเฉลยของ $2x \equiv 3 \pmod 4$

**วิธีทำ** เพราะว่า $(2, 4) = 2$ และ $2 \nmid 3$

เพราะฉะนั้น $2x \equiv 3 \pmod 4$ ไม่มีผลเฉลย #

ต่อไปจะพิจารณาการลงรอยกันเชิงเส้น

$$ax \equiv 1 \pmod m$$

จะเห็นว่า การลงรอยกันเชิงเส้นดังกล่าวมีผลเฉลยก็ต่อเมื่อ $(a, m) = 1$ เท่านั้น และถ้ามีผลเฉลย จะมีผลเฉลยได้เพียงผลเฉลยเดียวเท่านั้น เราจึงให้บทนิยามต่อไปนี้

**บทนิยาม 3.5** ให้ a และ m เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $(a, m) = 1$ ถ้า $\bar{a}$ เป็นผลเฉลยของ $ax \equiv 1 \pmod m$ แล้ว เรียก $\bar{a}$ ว่า เป็น **ตัวผกผันของ** a (an inverse of a) มอดุโล m

**ตัวอย่าง 3.18** จงหาตัวผกผันของ 7 มอดุโล 31

**วิธีทำ** พิจารณาผลเฉลยของ $7x \equiv 1 \pmod{31}$

เพราะว่า $(7, 31) = 1$ และ $1|1$ จึงได้ว่า $7x \equiv 1 \pmod{31}$ มีผลเฉลยและมีแน่นอนผลเฉลยเดียวเท่านั้น

พิจารณาสมการดีโอฟานทีนเชิงเส้น

$$7x - 31y = 1$$

จาก

$$31 = 4 \cdot 7 + 3$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 3 \cdot 1$$

จะได้

$$1 = 7 - 2 \cdot 3$$
$$= 7 - 2(31 - 4 \cdot 7)$$
$$1 = 9 \cdot 7 - 2 \cdot 31$$

นั่นคือ $x_0 = 9$ เป็นผลเฉลยของ $7x \equiv 1 \pmod{31}$

เพราะฉะนั้น 9 เป็นตัวผกผันของ 7 มอดุโล 31 และทุกจำนวนที่ลงรอยกันกับ 9 มอดุโล 31 เป็นตัวผกผันของ 7 มอดุโล 31 ด้วย #

เราสามารถใช้ตัวผกผันสำหรับ a มอดุโล m ช่วยหาผลเฉลยของ $ax \equiv b \pmod{m}$ ได้ดังตัวอย่างต่อไปนี้

**ตัวอย่าง 3.19** จงหาผลเฉลยของ $7x \equiv 22 \pmod{31}$

**วิธีทำ** จากตัวอย่าง 3.18 9 เป็นตัวผกผันของ 7 มอดุโล 31

ดังนั้น $7 \cdot 9 \equiv 1 \pmod{31}$

จึงได้ว่า $7 \cdot 9x \equiv x \pmod{31}$

จาก $7x \equiv 22 \pmod{31}$

จะได้

$$7 \cdot 9x \equiv x \equiv 22 \cdot 9 \equiv 198 \pmod{31}$$

เพราะฉะนั้น

$$x \equiv 198 \equiv 12 \pmod{31}$$

เป็นผลเฉลยของ $7x \equiv 22 \pmod{31}$ และมีผลเฉลยเดียว เพราะว่า $(7, 31) = 1$ #

**ทฤษฎีบท 3.13** ให้ $p$ เป็นจำนวนเฉพาะ และ $a$ เป็นจำนวนเต็มบวกแล้ว ตัวผกผันของ $a$ ในมอดุโล $p$ คือ $a$ ก็ต่อเมื่อ $a \equiv 1 \pmod{p}$ หรือ $a \equiv -1 \pmod{p}$

**พิสูจน์** สมมติ $a \equiv 1 \pmod{p}$ หรือ $a \equiv -1 \pmod{p}$

จะได้ $a^2 \equiv 1 \pmod{p}$ หรือ $a^2 \equiv 1 \pmod{p}$

นั่นคือ $a$ เป็นตัวผกผันของ $a$ ในมอดุโล $p$

ต่อไปสมมติ $a$ เป็นตัวผกผันของ $a$ ในมอดุโล $p$

ดังนั้น จึงได้ $a^2 \equiv 1 \pmod{p}$ นั่นคือ $p|(a^2 - 1)$

เพราะว่า $a^2 - 1 = (a-1)(a+1)$

จึงได้ $p|(a-1)(a+1)$

นั่นคือ $p|(a-1)$ หรือ $p|(a+1)$

ผลที่ตามมาก็คือ

$$a \equiv 1 \pmod{p} \quad \text{หรือ} \quad a \equiv -1 \pmod{p}$$ #

**ตัวอย่าง 3.20** จงหาผลเฉลยของ $4x \equiv 2 \pmod{3}$

**วิธีทำ** เพราะว่า 3 เป็นจำนวนเฉพาะ และ $4 \equiv 1 \pmod{3}$

ดังนั้น 4 เป็นตัวผกผันของ 4 มอดุโล 3

นั่นคือ จาก $4x \equiv 2 \pmod{3}$

คูณทั้งสองข้างด้วยตัวผกผันของ 4 มอดุโล 3 จะได้

$$4 \cdot 4x \equiv x \equiv 4 \cdot 2 \equiv 8 \pmod{3}$$

นั่นคือ

$$x \equiv 8 \equiv 5 \pmod{3}$$

เป็นผลเฉลยของ $4x \equiv 2 \pmod{3}$ และมีผลเฉลยเดียว เนื่องจาก $(4, 3) = 1$ #

## แบบฝึกหัด 3.2

1. จงหาผลเฉลยต่อไปนี้

1.1 $3x \equiv 2 \pmod 7$

1.2 $6x \equiv 3 \pmod 9$

1.3 $17x \equiv 14 \pmod{21}$

1.4 $15x \equiv 9 \pmod{25}$

1.5 $128x \equiv 833 \pmod{1001}$

1.6 $987x \equiv 610 \pmod{1597}$

1.7 $25x \equiv 4 \pmod{11}$

1.8 $15x \equiv 3 \pmod 9$

1.9 $34x \equiv 60 \pmod{98}$

1.10 $35x \equiv 15 \pmod{182}$

2. จงหาค่าจำนวนเต็ม c โดยที่ $0 \leqslant c < 30$ ที่ทำให้ $12x \equiv c \pmod{30}$ มีผลเฉลย

3. จงหาตัวผกผันของจำนวนเต็มต่อไปนี้ มอดุโล 17

3.1 4

3.2 5

3.3 7

3.4 16

4. จงหาผลเฉลยต่อไปนี้

4.1 $4x \equiv 12 \pmod{17}$

4.2 $5x \equiv 6 \pmod{17}$

4.3 $7x \equiv 7 \pmod{17}$

4.4 $16x \equiv 5 \pmod{17}$

## 3.3 ทฤษฎีบทเศษเหลือของชาวจีน (The Chinese Remainder Theorem)

ในหัวข้อนี้จะได้ศึกษาระบบการลงรอยกันเชิงเส้นในหนึ่งตัวแปร ซึ่งระบบการลงรอยกันนี้ได้สร้างขึ้นจากปัญหาของชาวจีนโบราณ ซึ่งได้ตั้งปัญหาไว้ดังนี้

**"จงหาจำนวนเต็มตัวหนึ่งซึ่งมีเศษเป็น 1 เมื่อหารด้วย 3 มีเศษเป็น 2 เมื่อหารด้วย 5 และมีเศษเป็น 3 เมื่อหารด้วย 7"**

จากปัญหาของชาวจีนดังกล่าว นำมาเขียนเป็นระบบการลงรอยกันได้ดังนี้

จงหาผลเฉลยของระบบการลงรอยกัน

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

ซึ่งทฤษฎีบทดังกล่าวต่อไปนี้ เป็นทฤษฎีบทซึ่งใช้สำหรับตอบปัญหาในลักษณะดังกล่าวนี้ได้

**ทฤษฎีบท 3.14** *ทฤษฎีบทเศษเหลือของชาวจีน* (The Chinese Remainder Theorem)

ให้ $m_1, m_2, \ldots, m_k$ เป็นจำนวนเต็มบวก โดยที่ $(m_i, m_j) = 1$ ถ้า $i \neq j$ แล้วระบบการลงรอยกัน

$$(*) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \bmod m_2) \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

มีผลเฉลย และมีผลเฉลยเพียงผลเฉลยเดียว มอดุโล M เมื่อ $M = m_1 m_2 \ldots m_k$

**พิสูจน์** ให้ $M_i = \dfrac{M}{m_i} \quad i = 1, 2, \ldots, k$

จะได้ว่า $(M_i, m_i) = 1$ เนื่องจาก $(m_j, m_i) = 1$ ถ้า $j \neq i$

ดังนั้น จะมี $y_i$ ซึ่งทำให้

$$M_i y_i \equiv 1 \pmod{m_i}$$

ให้ $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k$

จะแสดงว่า $x$ เป็นผลเฉลยของ $(*)$ นั่นคือ จะแสดงว่า $x \equiv a_i \pmod{m_i}$

ทุก $i = 1, 2, \ldots, k$

เพราะว่า $m_i | M_j$ ถ้า $i \neq j$

จะได้ $M_j \equiv 0 (\text{mod } m_i)$

ผลที่ตามมาก็คือ

$$a_j M_j y_j \equiv 0 (\text{mod } m_i) \quad \text{ทุก} \quad j \neq i$$

และ $a_i M_i y_i \equiv a_i (\text{mod } m_i)$

เนื่องจาก $M_i y_i \equiv 1 (\text{mod } m_i)$

เพราะฉะนั้น

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k \equiv a_i (\text{mod } m_i)$$

นั่นคือ (*) มีผลเฉลย

ต่อไปจะแสดงว่า ผลเฉลยคู่ใดก็ตามของ (*) จะลงรอยกัน มอดุโล M

ให้ $x_0, x_1$ เป็นผลเฉลยของ (*)

ดังนั้น สำหรับแต่ละ i

$$x_0 \equiv x_1 \equiv a_i (\text{mod } m_i)$$

นั่นคือ $m_i | (x_0 - x_1)$ ทุก $i = 1, 2, \ldots, k$

ผลที่ตามมาก็คือ

$$M | (x_0 - x_1)$$

ซึ่งทำให้ $x_0 \equiv x_1 (\text{mod } M)$ #

**ตัวอย่าง 3.21** จงหาผลเฉลยของระบบการลงรอยกัน

$$x \equiv 1 (\text{mod } 3)$$

$$x \equiv 2 (\text{mod } 5)$$

$$x \equiv 3 (\text{mod } 7)$$

**วิธีทำ**

$$M = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = \frac{105}{3} = 35$$

$$M_2 = \frac{105}{5} = 21$$

$$M_3 = \frac{105}{7} = 15$$

ต่อไปหา $y_1$ ที่ทำให้

$$y_1 M_1 \equiv 1 (\text{mod } 3)$$

นั่นคือ $35y_1 \equiv 1 \pmod 3$

เพราะว่า $35 \equiv 2 \pmod 3$

ดังนั้น $35y_1 \equiv 2y_1 \equiv 1 \pmod 3$

ซึ่งได้ $y_1 \equiv -1 \pmod 3 \equiv 2 \pmod 3$

ต่อไปหา $y_2$ ซึ่งทำให้

$$M_2y_2 \equiv 1 \pmod{m_2}$$

พิจารณา $21y_2 \equiv 1 \pmod 5$

เพราะว่า $21 \equiv 1 \pmod 5$

ดังนั้น $y_2 \equiv 1 \pmod 5$

ต่อไปหา $y_3$ ซึ่งทำให้

$$M_3y_3 \equiv 1 \pmod{m_3}$$

พิจารณา $15y_3 \equiv 1 \pmod 7$

เพราะว่า $15 \equiv 1 \pmod 7$

ดังนั้น $y_3 \equiv 1 \pmod 7$

ให้ $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1$

$= 70 + 42 + 45 = 157$

นั่นคือ $x \equiv 157 \equiv 52 \pmod{105}$ #

**ตัวอย่าง 3.22** จงหาผลเฉลยของระบบการลงรอยกัน

$$19x \equiv 1 \pmod 4$$
$$19x \equiv 1 \pmod 5$$
$$19x \equiv 1 \pmod 7$$

**วิธีทำ** หาผลเฉลยของการลงรอยกันเชิงเส้นแต่ละอันดังนี้

หาผลเฉลยของ $19x \equiv 1 \pmod 4$

เพราะว่า $57 \equiv 19 \cdot 3 \equiv 1 \pmod 4$

จึงได้ $x \equiv 3 \pmod 4$

หาผลเฉลยของ $19x \equiv 1 \pmod 5$

เพราะว่า $19 \equiv -1 \pmod 5$

จึงได้ $x \equiv -1 \pmod 5 \equiv 4 \pmod 5$

หาผลเฉลยของ $19x \equiv 1 \pmod 7$

เพราะว่า $19 \equiv -2 \pmod 7$

จึงได้ $-2x \equiv 1 \pmod 7$

และผลที่ตามมาก็คือ $x \equiv 3 \pmod 7$

ดังนั้น ระบบการลงรอยกันดังกล่าวจึงสามารถเขียนใหม่ได้ดังนี้

$$(*) \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

ซึ่งจะได้ $M = 4 \cdot 5 \cdot 7 = 140$

$$M_1 = \frac{140}{4} = 35$$

$$M_2 = \frac{140}{5} = 28$$

$$M_3 = \frac{140}{7} = 20$$

หา $y_1$ ซึ่งทำให้

$$35y_1 \equiv 1 \pmod 4$$

เพราะว่า $35 \equiv -1 \pmod 4$

จึงได้ $y_1 \equiv -1 \equiv 3 \pmod 4$

หา $y_2$ ที่ทำให้

$$28y_2 \equiv 1 \pmod 5$$

เพราะว่า $28 \equiv 3 \pmod 5$

จึงได้ $3y_2 \equiv 1 \pmod 5$

และได้ $y_2 \equiv 2 \pmod 5$

หา $y_3$ ที่ทำให้

$$20y_3 \equiv 1 \pmod 7$$

เพราะว่า $-20 \equiv 1 \pmod 7$

จึงได้ $y_3 \equiv -1 \pmod 7$

ให้ $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$$= 3\cdot 35\cdot 3 + 4\cdot 28\cdot 2 + 3\cdot 20\cdot(-1)$$

$$= 315 + 224 - 60 = 479$$

นั่นคือ $x \equiv 479 \equiv 59 \pmod{140}$ เป็นผลเฉลย #

ตัวอย่างต่อไปจะแสดงการหาผลเฉลยของระบบการลงรอยกันโดยวิธีอื่น

**ตัวอย่าง 3.23** จงหาผลเฉลยของ

$$x \equiv 1 \pmod 5 \qquad \text{.....(1)}$$

$$x \equiv 2 \pmod 6 \qquad \text{.....(2)}$$

$$x \equiv 3 \pmod 7 \qquad \text{.....(3)}$$

**วิธีทำ** จาก (1) จะได้ว่า มีจำนวนเต็ม $t$ ที่ทำให้

$$x = 5t + 1$$

แทนค่า $x = 5t + 1$ ใน (2) จะได้

$$5t + 1 \equiv 2 \pmod 6$$

ซึ่งทำให้ $5t \equiv 1 \pmod 6$

และเพราะว่า $25 \equiv 5\cdot 5 \equiv 1 \pmod 6$

จึงได้ $t \equiv 5 \pmod 6$

นั่นคือ จะมีจำนวนเต็ม $u$ ที่ทำให้

$$t = 5 + 6u$$

เพราะฉะนั้น $x = 5t + 1 = 5(5 + 6u) + 1 = 30u + 26$

แทนค่า $x = 30u + 26$ ใน (3) จะได้

$$30u + 26 \equiv 3 \pmod 7$$

เพราะว่า $-26 \equiv 2 \pmod 7$

จึงได้ $30u \equiv 5 \pmod 7$

และเพราะว่า $(5, 7) = 1$

จึงได้ $6u \equiv 1 \pmod 7$

เพราะว่า $36 \equiv 6\cdot 6 \equiv 1 \pmod 7$

จึงได้ $u \equiv 6 \pmod 7$

นั่นคือ จะมีจำนวนเต็ม $v$ ที่ทำให้

$$u = 7v + 6$$

ดังนั้น $x = 30u + 26 = 30(7v + 6) + 26$

$= 210v + 206$

นั่นคือ $x \equiv 206 \pmod{210}$ เป็นผลเฉลยของระบบการลงรอยกันนี้ #

ทฤษฎีบทเศษเหลือของชาวจีนจะเป็นกรณีพิเศษของทฤษฎีบทต่อไปนี้

**ทฤษฎีบท 3.15** ระบบการลงรอยกัน

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

จะมีผลเฉลยก็ต่อเมื่อ $(m_1, m_2) | (a_1 - a_2)$

นอกจากนั้น ถ้าระบบมีผลเฉลยแล้ว จะมีเพียงผลเฉลยเดียวในมอดุโล M

เมื่อ $M = [m_1, m_2]$

**พิสูจน์** สมมติ

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

มีผลเฉลย

ให้ $x_0$ เป็นผลเฉลย

ดังนั้น $x_0 \equiv a_1 \pmod{m_1}$

$x_0 \equiv a_2 \pmod{m_2}$

เพราะฉะนั้น จะมีจำนวนเต็ม $t_1, t_2$ ที่ทำให้

$$x_0 = a_1 + m_1 t_1 = a_2 + m_2 t_2$$

ผลที่ตามมาก็คือ

$$a_1 - a_2 = m_2 t_2 - m_1 t_1$$

ให้ $d = (m_1, m_2)$ จะได้ $d | (m_2 t_2 - m_1 t_1)$ นั่นคือ $d | (a_1 - a_2)$

ในทางกลับกัน สมมติ $(m_1, m_2) | (a_1 - a_2)$

ให้ $d = (m_1, m_2)$

ดังนั้น จะมีจำนวนเต็ม $s, t$ ที่ทำให้

$$d = sm_1 + tm_2$$

และเพราะว่า $d | (a_1 - a_2)$ จึงมีจำนวนเต็ม $k$ ที่ทำให้ $a_1 - a_2 = kd$

ดังนั้น $a_1 - a_2 = kd = ksm_1 + ktm_2$

นั่นคือ $a_1 - ksm_1 = a_2 + ktm_2$

ให้ $x_0 = a_1 - ksm_1 = a_2 + ktm_2$

จะได้ $x_0 \equiv a_1 (\text{mod } m_1)$

และ $x_0 \equiv a_2 (\text{mod } m_2)$

นั่นคือ $x_0$ เป็นผลเฉลยของระบบการลงรอยกันนี้

ต่อไปจะพิสูจน์ว่า ถ้าระบบการลงรอยกันมีผลเฉลย จะมีผลเฉลยเพียงผลเฉลยเดียวในมอดุโล M เมื่อ $M = [m_1, m_2]$

สมมติ $x_1$ และ $x_2$ เป็นผลเฉลยของ

$$x \equiv a_1 (\text{mod } m_1)$$

$$x \equiv a_2 (\text{mod } m_2)$$

ดังนั้น

$$x_1 \equiv a_1 (\text{mod } m_1)$$

$$x_1 \equiv a_2 (\text{mod } m_2)$$

และ

$$x_2 \equiv a_1 (\text{mod } m_1)$$

$$x_2 \equiv a_2 (\text{mod } m_2)$$

จึงมีจำนวนเต็ม $t_1, t_2, k_1, k_2$ ที่ทำให้

$$x_1 = a_1 + m_1 t_1$$

$$x_1 = a_2 + m_2 t_2$$

และ

$$x_2 = a_1 + m_1 k_1$$

$$x_2 = a_2 + m_2 k_2$$

จึงได้ว่า

$$x_1 - x_2 = m_1(t_1 - k_1)$$

$$x_1 - x_2 = m_2(t_2 - k_2)$$

นั่นคือ $x_1 \equiv x_2 (\text{mod } m_1)$

และ $x_1 \equiv x_2 (\text{mod } m_2)$

ดังนั้น โดยทฤษฎีบท 3.10 $x_1 \equiv x_2 (\text{mod } M)$ เมื่อ $M = [m_1, m_2]$ #

**บทแทรก 3.16** ระบบการลงรอยกัน

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$\vdots$$
$$x \equiv a_k (\text{mod } m_k)$$

มีผลเฉลยก็ต่อเมื่อ ทุก ๆ $i \neq j$ $(m_i, m_j) | (a_i - a_j)$

นอกจากนั้น ถ้าระบบมีผลเฉลยแล้ว จะมีเพียงผลเฉลยเดียว

มอดุโล $M = |m_1, m_2, \ldots, m_k|$

**พิสูจน์** ให้นักศึกษาพิสูจน์เป็นแบบฝึกหัด #

**ตัวอย่าง 3.24** จงหาผลเฉลยของระบบการลงรอยกัน

$$x \equiv 1 (\text{mod } 2) \quad \ldots\ldots\ldots\ldots (1)$$
$$x \equiv 2 (\text{mod } 3) \quad \ldots\ldots\ldots\ldots (2)$$
$$x \equiv 1 (\text{mod } 5) \quad \ldots\ldots\ldots\ldots (3)$$
$$x \equiv 5 (\text{mod } 7) \quad \ldots\ldots\ldots\ldots (4)$$
$$x \equiv 2 (\text{mod } 9) \quad \ldots\ldots\ldots\ldots (5)$$

**วิธีทำ** พิจารณาเฉพาะการลงรอยกัน (1), (2), (3) และ (4) จะเห็นว่าสอดคล้องตามเงื่อนไขของทฤษฎีบทเศษเหลือของชาวจีน ดังนั้นจึงหาผลเฉลยของการลงรอยกัน (1), (2), (3) และ (4) เสียก่อน

พิจารณา $x \equiv 1 (\text{mod } 2)$

จะได้มีจำนวนเต็ม $t$ ที่ทำให้

$$x = 1 + 2t$$

แทนค่า $x = 1 + 2t$ ใน (2) จึงได้

$$1 + 2t \equiv 2 (\text{mod } 3)$$

นั่นคือ $2t \equiv 1 (\text{mod } 3)$

และได้ $t \equiv 2 (\text{mod } 3)$

นั่นคือ มีจำนวนเต็ม $u$ ที่ทำให้

$$t = 2 + 3u$$

ดังนั้น $x = 1 + 2t = 1 + 2(2 + 3u) = 5 + 6u$

แทนค่า $x = 5+6u$ ใน (3) จะได้

$$5+6u \equiv 1 \pmod 5$$

เพราะว่า

$$5 \equiv 0 \pmod 5$$

จึงได้ $6u \equiv 1 \pmod 5$

ผลที่ตามมาก็คือ $u \equiv 1 \pmod 5$

ดังนั้น จะมีจำนวนเต็ม v ที่ทำให้

$$u = 1+5v$$

เพราะฉะนั้น $x = 5+6u = 5+6(1+5v) = 11+30v$

แทนค่า $x = 11+30v$ ใน 4

$$11+30v \equiv 5 \pmod 7$$

เพราะว่า $11 \equiv 4 \pmod 7$

ดังนั้น $30v \equiv 1 \pmod 7$

และได้ $v \equiv 4 \pmod 7$

นั่นคือ มีจำนวนเต็ม w ที่ทำให้

$$v = 4+7w$$

ดังนั้น $x = 11+30v = 11+30(4+7w)$

$$x = 131+210w$$

นั่นคือ $x \equiv 131 \pmod{210}$ เป็นผลเฉลยของระบบ (1), (2), (3) และ (4)

พิจารณาระบบการลงรอยกัน

$$x \equiv 131 \pmod{210}$$

$$x \equiv 2 \pmod 9$$

เพราะว่า $(210, 9) = 3$ และ $3 \mid (131-2)$ ดังนั้น ระบบนี้มีผลเฉลย

จาก $x = 131+210w$ แทนค่า x ใน $x \equiv 2 \pmod 9$

ได้

$$131+210w \equiv 2 \pmod 9$$

เพราะว่า $131 \equiv 5 \pmod 9$

จึงได้ $210w \equiv -3 \pmod 9 \equiv 6 \pmod 9$

เพราะว่า $(6, 9) = 3$ จึงได้

$$35w \equiv 1\left(\bmod \frac{9}{3}\right) \equiv 1 \pmod 3$$

และได้ $w \equiv 2 \pmod 3$

นั่นคือ มีจำนวนเต็ม s ที่ทำให้

$$w = 2 + 3s$$

ดังนั้น $x = 131 + 210w = 131 + 210(2 + 3s)$

$$x = 551 + 630s$$

นั่นคือ $x \equiv 551 \pmod{630}$ เป็นผลเฉลยของการลงรอยกัน (1), (2), (3), (4) และ (5)

#

**ตัวอย่าง 3.25** จงหาผลเฉลยของระบบการลงรอยกัน

$5x \equiv 2 \pmod 3$ ..... (1)

$2x \equiv 4 \pmod{10}$ ..... (2)

$4x \equiv 7 \pmod 9$ ..... (3)

**วิธีทำ** พิจารณา (1) $5x \equiv 2 \pmod 3$

เพราะว่า $(3, 5) = 1$ และ $1|2$ ดังนั้น $5x \equiv 2 \pmod 3$ มีผลเฉลย 1 ผลเฉลย

และผลเฉลยคือ $x \equiv 1 \pmod 3$

พิจารณา (2) $2x \equiv 4 \pmod{10}$

เพราะว่า $(2, 10) = 2$ และ $2|4$ ดังนั้น $2x \equiv 4 \pmod{10}$ มี 2 ผลเฉลย

และผลเฉลยคือ $x \equiv 2 \pmod{10}$ และ $x \equiv 7 \pmod{10}$

พิจารณา (3) $4x \equiv 7 \pmod 9$

เพราะว่า $(4, 9) = 1$ และ $1|7$ ดังนั้น $4x \equiv 7 \pmod 9$ มี 1 ผลเฉลย

และผลเฉลยคือ $x \equiv 4 \pmod 9$

ดังนั้น พิจารณาระบบการลงรอยกันสองระบบคือ

$$\text{(I)}\quad \begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod{10} \\ x &\equiv 4 \pmod 9 \end{aligned} \qquad \text{และ} \qquad \text{(II)}\quad \begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 7 \pmod{10} \\ x &\equiv 4 \pmod 9 \end{aligned}$$

พิจารณา (I) จะได้ $(3, 10)|(1-2)$, $(10, 9)|(2-4)$, $(3, 9)|(1-4)$

ดังนั้น ระบบ (I) มีผลเฉลย

จาก $x \equiv 1 \pmod 3$

จะมีจำนวนเต็ม s ที่ทำให้

$$x = 1 + 3s$$

แทนค่า $x = 1+3s$ ใน $x \equiv 2 \pmod{10}$

จะได้ $x \equiv 1+3s \equiv 2 \pmod{10}$

ซึ่งทำให้ $3s \equiv 1 \pmod{10}$

และ $s \equiv 7 \pmod{10}$

นั่นคือ มีจำนวนเต็ม $t$ ที่ทำให้

$$s = 7+10t$$

ดังนั้น $x = 1+3s = 1+3(7+10t) = 22+30t$

แทนค่า $x = 22+30t$ ใน $x \equiv 4 \pmod{9}$

จะได้ $x \equiv 22+30t \equiv 4 \pmod{9}$

$$30t \equiv 18 \pmod{9}$$

เพราะว่า $(3, 9) = 3$ ดังนั้น จึงได้

$$10t \equiv 6 \pmod{3}$$

เพราะว่า $(2, 3) = 1$ จึงได้

$$5t \equiv 3 \pmod{3}$$

และ $t \equiv 3 \pmod{3}$

ดังนั้น จึงมีจำนวนเต็ม $u$ ที่ทำให้ $t = 3+3u$

นั่นคือ $x = 22+30t = 22+30(3+3u) = 112+90u$

เพราะฉะนั้น $x \equiv 112 \equiv 22 \pmod{90}$ เป็นผลเฉลยของ (I)

พิจารณา (II) จะได้ $(3, 10)|(1-7)$, $(10, 9)|(7-4)$, $(9, 3)|(4-1)$

ดังนั้น ระบบ (II) มีผลเฉลย

จาก $x \equiv 1 \pmod{3}$

จะมีจำนวนเต็ม $s$ ที่ทำให้

$$x = 1+3s$$

แทนค่า $x = 1+3s$ ใน $x \equiv 7 \pmod{10}$

จะได้ $1+3s \equiv 7 \pmod{10}$

และ $3s \equiv 6 \pmod{10}$

ผลที่ตามมาก็คือ $s \equiv -8 \pmod{10} \equiv 2 \pmod{10}$

นั่นคือ มีจำนวนเต็ม $k$ ที่ทำให้

$$s = 2+10k$$

ดังนั้น $x = 1+3s = 1+3(2+10k) = 7+30k$

แทนค่า $x = 7+30k$ ใน $x \equiv 4 \pmod 9$

$$7+30k \equiv 4 \pmod 9$$

$$30k \equiv -3 \pmod 9$$

เพราะว่า $(3, 9) = 3$ จึงได้

$$10k \equiv -1 \pmod 3$$

ดังนั้น $$k \equiv 2 \pmod 3$$

นั่นคือ มีจำนวนเต็ม $\ell$ ที่ทำให้

$$k = 2+3\ell$$

ดังนั้น $$x = 7+30k = 7+30(2+3\ell)$$

$$= 67+90\ell$$

นั่นคือ $$x \equiv 67 \pmod{90}$$

เพราะฉะนั้น $x \equiv 22 \pmod{90}$ และ $x \equiv 67 \pmod{90}$ เป็นผลเฉลยของ

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

$$2x \equiv 4 \pmod{10}$$

$$4x \equiv 7 \pmod 9$$

#

## แบบฝึกหัด 3.3

1. จงหาผลเฉลยของ

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

2. จงหาผลเฉลยของ

$$x \equiv 5 \pmod{11}$$
$$x \equiv 14 \pmod{29}$$
$$x \equiv 15 \pmod{31}$$

3. จงหาผลเฉลยของ

$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod{11}$$
$$x \equiv 3 \pmod{17}$$

4. จงหาผลเฉลยของ

$$2x \equiv 1 \pmod 5$$
$$3x \equiv 9 \pmod 6$$
$$4x \equiv 1 \pmod 7$$
$$5x \equiv 9 \pmod{11}$$

5. จงหาผลเฉลยของ $17x \equiv 3 \pmod{2\cdot 3\cdot 5\cdot 7}$ โดยหาผลเฉลยของระบบการลงรอยกัน

$$17x \equiv 3 \pmod 2$$
$$17x \equiv 3 \pmod 3$$
$$17x \equiv 3 \pmod 5$$
$$17x \equiv 3 \pmod 7$$

6. จงหาจำนวนเต็มบวก a ที่เล็กที่สุด โดยที่ $a > 2$ และ

$2 \mid a$, $3 \mid (a+1)$, $4 \mid (a+2)$, $5 \mid (a+3)$ และ $6 \mid (a+4)$

7. จงหาจำนวนเต็มบวก a ที่ทำให้ $2^2|a$, $3^2|(a+1)$ และ $5^2|(a+2)$

8. จงหาผลเฉลยของ

$$x \equiv 4 \pmod 6$$
$$x \equiv 13 \pmod{15}$$

9. จงหาผลเฉลยของ

$$x \equiv 7 \pmod{10}$$
$$x \equiv 4 \pmod{15}$$

10. จงหาผลเฉลยของ

$$x \equiv 5 \pmod 6$$
$$x \equiv 3 \pmod{10}$$
$$x \equiv 8 \pmod{15}$$

11. จงหาผลเฉลยของ

$$x \equiv 2 \pmod 6$$
$$x \equiv 4 \pmod 8$$
$$x \equiv 2 \pmod{14}$$
$$x \equiv 14 \pmod{15}$$

12. จงหาผลเฉลยของ

$$x \equiv 2 \pmod{14}$$
$$x \equiv 16 \pmod{21}$$
$$x \equiv 10 \pmod{30}$$

## 3.4 การทดสอบการหารลงตัว (Divisibility Tests)

ในหัวข้อนี้จะได้ศึกษาวิธีทดสอบการหารลงตัว โดยใช้คุณสมบัติการลงรอยกัน ดังนี้

*การทดสอบการหารลงตัวด้วย 2 หรือกำลังของ 2*

ให้ $n$ เป็นจำนวนเต็มบวกใด ๆ และ

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$$

โดยที่ $0 \leqslant a_j \leqslant 9$ ทุก $j = 0, 1, 2, \ldots, k$

เนื่องจาก $10 \equiv 0 \pmod 2$

และ $2^j | 10^j$ ทุกจำนวนเต็มบวก $j$

ดังนั้น $10^j \equiv 0 \pmod{2^j}$ ทุก $j = 0, 1, 2, \ldots, k$

เพราะว่า $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$

จะได้ว่า

$$n \equiv (a_0)_{10} \pmod 2$$

$$n \equiv (a_1 a_0)_{10} \pmod{2^2}$$

$$n \equiv (a_2 a_1 a_0)_{10} \pmod{2^3}$$

$$\vdots$$

$$n \equiv (a_{j-1} a_{j-2} \ldots a_2 a_1 a_0)_{10} \pmod{2^j}$$

ซึ่งสรุปได้ดังนี้

เราจะทดสอบว่า $2|n$ เพียงพอที่จะทดสอบว่า $2|(a_0)_{10}$

จะทดสอบว่า $4|n$ เพียงพอที่จะทดสอบว่า $4|(a_1 a_0)_{10}$

จะทดสอบว่า $8|n$ เพียงพอที่จะทดสอบว่า $8|(a_2 a_1 a_0)_{10}$

$$\vdots$$

จะทดสอบว่า $2^j|n$ เพียงพอที่จะทดสอบว่า $2^j|(a_{j-1} a_{j-2} \ldots a_2 a_1 a_0)_{10}$

**ตัวอย่าง 3.26** ให้ $n = 32688048$

จะได้ $a_7 = 3,\ a_6 = 2,\ a_5 = 6,\ a_4 = 8,\ a_3 = 8,\ a_2 = 0,\ a_1 = 4,\ a_0 = 8$

เพราะว่า $2|8$ จะได้ $2|n$

เพราะว่า $4|48$ จะได้ $4|n$

เพราะว่า $8|048$ จะได้ $8|n$

เพราะว่า $16|8048$ จะได้ $16|n$

เพราะว่า $32 \nmid 88048$ จะได้ $32 \nmid n$ #

*การทดสอบการหารลงตัวด้วย 5 หรือกำลังของ 5*

เนื่องจาก $10 \equiv 0 \pmod 5$

และ $5^j | 10^j$ ทุกจำนวนเต็มบวก j

ดังนั้น $10^j \equiv 0 \pmod{5^j}$ ทุกจำนวนเต็มบวก j

ดังนั้น ถ้า

$$n = (a_k a_{k-1} \ldots a_2 a_1 a_0)$$

จะได้

$$n \equiv (a_0)_{10} \pmod 5$$

$$n \equiv (a_1 a_0)_{10} \pmod{5^2}$$

$$\vdots$$

$$n \equiv (a_{j-1} a_{j-2} \ldots a_2 a_1 a_0)_{10} \pmod{5^j}$$

นั่นคือ การทดสอบว่า $5^j | n$ หรือไม่ เพียงพอที่จะทดสอบว่า $5^j | (a_{j-1} a_{j-2} \ldots a_1 a_0)_{10}$ หรือไม่

**ตัวอย่าง 3.27** ให้ $n = 15535375$

จะได้

$a_7 = 1,\ a_6 = 5,\ a_5 = 5,\ a_4 = 3,\ a_3 = 5,\ a_2 = 3,\ a_1 = 7,\ a_0 = 5$

เพราะว่า $5 | 5$ จึงได้ว่า $5 | n$

เพราะว่า $5^2 | 75$ จึงได้ว่า $25 | n$

เพราะว่า $5^3 | 375$ จึงได้ว่า $125 | n$

เพราะว่า $5^4 \nmid 5375$ จึงได้ว่า $625 \nmid n$ #

*การทดสอบการหารลงตัวด้วย 3 หรือ 9*

เพราะว่า $10 \equiv 1 \pmod 3$ และ $10 \equiv 1 \pmod 9$

จะได้ว่า $10^j \equiv 1 \pmod 3$ และ $10^j \equiv 1 \pmod 9$

ทุกจำนวนเต็มบวก j

ดังนั้น ถ้า

$$n = (a_k a_{k-1} \ldots a_2 a_1 a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$$

จะได้ $a_k 10^k \equiv a_k \pmod 3$

$$a_{k-1}10^{k-1} \equiv a_{k-1} \pmod 3$$
$$\vdots$$
$$a_1 10 \equiv a_1 \pmod 3$$
$$a_0 \equiv a_0 \pmod 3$$

ดังนั้น

$$n \equiv a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0 \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod 3$$

และในทำนองเดียวกันได้ว่า

$$n \equiv a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0 \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod 9$$

นั่นคือ การทดสอบว่า $3|n$ หรือ $9|n$ เพียงพอที่จะทดสอบว่า 3 หารผลบวกของเลขโดดของ $n$ ลงตัวหรือไม่ หรือทดสอบว่า 9 หารผลบวกของเลขโดดของ $n$ ลงตัวหรือไม่

**ตัวอย่าง 3.28** ให้ $n = 4127835$

ผลบวกของเลขโดดของ $n$ คือ

$$4+1+2+7+8+3+5 = 30$$

เพราะว่า $3|30$ เพราะฉะนั้น $3|4127835$

เพราะว่า $9\nmid 30$ เพราะฉะนั้น $9\nmid 4127835$ #

*การทดสอบการหารลงตัวด้วย* 11

เพราะว่า $10 \equiv -1 \pmod{11}$

จะได้ $10^j \equiv (-1)^j \pmod{11}$ ทุกจำนวนเต็มบวก $j$

ดังนั้น ถ้า

$$n = (a_k a_{k-1} \ldots a_2 a_1 a_0)_{10} = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0$$

จะได้

$$n \equiv (-1)^k a_k + (-1)^{k-1}a_{k-1} + \ldots + (-1)a_1 + (-1)^0 a_0 \pmod{11}$$

นั่นคือ $11|n$ ก็ต่อเมื่อ $11 \mid |(-1)^k a_k + (-1)^{k-1}a_{k-1} + \ldots + (-1)a_1 + (-1)^0 a_0|$

**ตัวอย่าง 3.29** ให้ $n = 723160823$

เพราะว่า

$$(-1)^8 a_8 + (-1)^7 a_7 + \ldots + (-1)a_1 + a_0 = 7-2+3-1+6-0+8-2+3 = 22$$

และ $11|22$ ดังนั้น $11|723160823$ #

## แบบฝึกหัด 3.4

1. จงพิจารณากำลังสูงสุดของ 2 ที่ทำให้หารจำนวนเต็มต่อไปนี้ลงตัว

   1.1 201984 1.2 1423408

   1.3 89375744 1.4 41578912246

2. จงพิจารณากำลังสูงสุดของ 5 ที่ทำให้หารจำนวนเต็มต่อไปนี้ลงตัว

   2.1 112250 2.2 4860625

   2.3 235555790 2.4 48126953125

3. จงทดสอบการหารลงตัวด้วย 3 และ 9 ของจำนวนเต็มต่อไปนี้

   3.1 18381 3.2 65412351

   3.3 987654321 3.4 78918239735

4. จำนวนเต็มต่อไปนี้จำนวนใดหารลงตัวด้วย 11

   4.1 10763732 4.2 1086320015

   4.3 674310976375 4.4 8924310064537

5. จงหาเงื่อนไขการหารลงตัวด้วย 1001

   (*แนะนำ* : $1001 = 7 \cdot 11 \cdot 13$)

## 3.5 ทฤษฎีบทของวิลสันและทฤษฎีบทเล็ก ๆ ของแฟร์มาต์ (Wilson's Theorem and Fermat's Little Theorem)

ในหัวข้อนี้จะได้ศึกษาถึงทฤษฎีบทที่เกี่ยวกับการลงรอยกันสองทฤษฎีบท ดังนี้

**ทฤษฎีบท 3.17** *ทฤษฎีบทของวิลสัน* (Wilson's Theorem)

ถ้า $p$ เป็นจำนวนเฉพาะแล้ว $(p-1)! \equiv -1 \pmod{p}$

**พิสูจน์** ถ้า $p = 2$ เราได้ว่า $(p-1)! \equiv 1 \equiv -1 \pmod{p}$

นั่นคือ ทฤษฎีบทเป็นจริงเมื่อ $p = 2$

ให้ $p$ เป็นจำนวนเฉพาะ โดยที่ $p > 2$

ดังนั้น สำหรับแต่ละจำนวนเต็มบวก $a$ ที่ $1 \leqslant a \leqslant p-1$ จะมีตัวผกผัน $\bar{a}$ สำหรับ $a$ ในมอดุโล $p$ โดยที่ $1 \leqslant \bar{a} \leqslant p-1$ และ $a\bar{a} \equiv 1 \pmod{p}$

จากทฤษฎีบทที่ 3.13 $a$ มี $a$ เป็นตัวผกผันมอดุโล $a$ ก็ต่อเมื่อ $a \equiv 1 \pmod{p}$ หรือ $a \equiv -1 \pmod{p}$ เท่านั้น

นั่นคือ จำนวนเต็มบวกที่น้อยกว่า $p$ ที่มีตัวเองเป็นตัวผกผันมอดุโล $p$ ก็คือ $1$ และ $p-1$ เท่านั้น

แบ่งจำนวนเต็ม $2, 3, 4, \ldots, (p-2)$ ออกเป็น $\frac{(p-3)}{2}$ คู่ ดังนี้

พิจารณา $2 \leqslant a \leqslant p-2$

จะได้ว่า $(a-1, p) = (a+1, p) = 1$

ดังนั้น $a^2 - 1 = (a-1)(a+1) \not\equiv 0 \pmod{p}$

เนื่องจาก ถ้า $a^2 - 1 \equiv 0 \pmod{p}$ แล้ว จะได้ $p|(a+1)$ หรือ $p|(a-1)$ ซึ่งเป็นไปไม่ได้

นั่นคือ แต่ละจำนวนเต็ม $a$ $2 \leqslant a \leqslant p-2$ $a$ จะไม่เป็นตัวผกผันของ $a$ ในมอดุโล $p$

จับคู่ $a, \bar{a}$ ใน $2, 3, \ldots, (p-2)$ โดยที่ $a\bar{a} \equiv 1 \pmod{p}$ และ $a \neq \bar{a}$

ดังนั้น จะได้

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$$

และเพราะว่า

$$1 \equiv 1 \pmod{p}$$

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

จึงได้

$$(p-1)! \equiv 1\cdot 2\cdot 3\cdot \ldots \cdot (p-2)(p-1) \equiv -1 \pmod p$$ #

ตัวอย่างต่อไปนี้จะทำให้เข้าใจการพิสูจน์ทฤษฎีบทของวิลสันมากขึ้น

**ตัวอย่าง 3.30** ให้ $p = 7$

จะได้ $(p-1)! = 6! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6$

เพราะว่า

$$1 \equiv 1 \pmod 7$$
$$2\cdot 4 \equiv 1 \pmod 7$$
$$3\cdot 5 \equiv 1 \pmod 7$$
$$6 \equiv -1 \pmod 7$$

จึงได้ $(p-1)! \equiv 6! \equiv 1\cdot 2\cdot 3\cdot \ldots \cdot 6 \equiv -1 \pmod 7$ #

สิ่งที่น่าสนใจคือ บทกลับของทฤษฎีบทของวิลสันเป็นจริง ซึ่งพิสูจน์ได้ดังนี้

**ทฤษฎีบท 3.18** ถ้า $n$ เป็นจำนวนเต็มบวก โดยที่ $(n-1)! \equiv -1 \pmod n$ แล้ว $n$ เป็นจำนวนเฉพาะ

**พิสูจน์** สมมติ $n$ ไม่ใช่จำนวนเฉพาะ ดังนั้น $n$ จะมีตัวหาร $d$ โดยที่ $1 < d \leqslant n-1$

เพราะว่า $d \leqslant n-1$ จึงได้ว่า $d|(n-1)!$

และเนื่องจาก $(n-1)! \equiv -1 \pmod n$

ผลที่ตามมาก็คือ $n|(n-1)!+1$ เพราะว่า $d|n$

ดังนั้น $d|(n-1)!+1$ และจึงได้ $d|1$ ซึ่งเป็นไปไม่ได้

นั่นคือ $n$ เป็นจำนวนเฉพาะ #

ต่อไปจะกล่าวถึงทฤษฎีบทที่สำคัญอีกทฤษฎีบทหนึ่ง คือ ทฤษฎีบทเล็ก ๆ ของแฟร์มาต์

**ทฤษฎีบท 3.19** ถ้า $p$ เป็นจำนวนเฉพาะ และ $a$ เป็นจำนวนเต็มบวก โดยที่ $p \nmid a$

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

**พิสูจน์** ให้ $p$ เป็นจำนวนเฉพาะ และ $a$ เป็นจำนวนเต็มบวก โดยที่ $p \nmid a$

พิจารณาจำนวนเต็ม $a, 2a, \ldots, (p-1)a$ ซึ่งมี $(p-1)$ จำนวน

จะได้ว่า $p \nmid ja$ ทุก ๆ $j = 1, 2, \ldots, p-1$

เนื่องจาก ถ้า $p|ja$ แล้ว จะได้ว่า $p|j$ หรือ $p|a$ ซึ่งเป็นไปไม่ได้

และทุกคู่ใด ๆ ใน $a, 2a, \ldots, (p-1)a$ จะไม่ลงรอยกันในมอดุโล $p$

เนื่องจาก ถ้า $ja \equiv ka \pmod p$ และ $(a, p) = 1$ แล้ว $j \equiv k \pmod p$ ซึ่งเป็นไปไม่ได้

นั่นคือ $a, 2a, \ldots, (p-1)a$ จะอยู่ในต่างชั้นของการลงรอยกันมอดุโล $p$

และเพราะว่า $a, 2a, \ldots, (p-1)a$ ไม่ลงรอยกันกับ 0 มอดุโล $p$ จึงได้ว่า เศษตกค้างที่เล็กที่สุดที่ไม่เป็นลบมอดุโล $p$ ที่อยู่ในชั้นเดียวกันกับ $a, 2a, \ldots, (p-1)a$ คือ $1, 2, \ldots, (p-1)$ เท่านั้น

นั่นคือ

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p$$

จึงได้ว่า

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$$

เพราะว่า $\quad ((p-1)!, p) = 1$

ดังนั้น

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

**ตัวอย่าง 3.31** ให้ $p = 7, \ a = 3$

เพราะว่า $7 \nmid 3$

โดยทฤษฎีบทเล็ก ๆ ของแฟร์มาต์ ได้ว่า

$$3^6 \equiv 1 \pmod 7$$ #

ทฤษฎีบทต่อไปนี้เป็นผลจากทฤษฎีบทเล็ก ๆ ของแฟร์มาต์

**ทฤษฎีบท 3.20** ถ้า $p$ เป็นจำนวนเฉพาะ และ $a$ เป็นจำนวนเต็มบวกใด ๆ แล้ว

$$a^p \equiv a \pmod p$$

**พิสูจน์** ถ้า $p \nmid a$ โดยทฤษฎีบท 3.19 ได้ว่า

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

ดังนั้น จึงได้ $\quad a^p \equiv a \pmod p$

ถ้า $p \mid a$ จะได้ว่า $p \mid a^p$

นั่นคือ $\quad a^p \equiv a \pmod p$ #

เราสามารถใช้ทฤษฎีบทเล็ก ๆ ของแฟร์มาต์หาเศษตกค้างที่ไม่เป็นลบที่เล็กที่สุดใน มอดุโล m ได้ดังตัวอย่างต่อไปนี้

**ตัวอย่าง 3.32** จงหาเศษตกค้างที่ไม่เป็นลบที่เล็กที่สุดของ $3^{201}$ มอดุโล 11

**วิธีทำ** เพราะว่า 11 เป็นจำนวนเฉพาะ และ $11 \nmid 3$

ดังนั้น โดยทฤษฎีบทเล็ก ๆ ของแฟร์มาต์

$$3^{10} \equiv 1 \pmod{11}$$

นั่นคือ

$$3^{201} \equiv (3^{10})^{20} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{11}$$

เพราะว่า $0 \leqslant 3 < 11$ ดังนั้น เศษตกค้างที่ไม่เป็นลบที่เล็กที่สุดของ $3^{201}$ มอดุโล 11 คือ 3

#

**ตัวอย่าง 3.33** จงแสดงว่า $5^{38} \equiv 4 \pmod{11}$

**วิธีทำ** เพราะว่า 11 เป็นจำนวนเฉพาะ และ $11 \nmid 5$

ดังนั้น $5^{10} \equiv 1 \pmod{11}$

และเพราะว่า $5^2 \equiv 25 \equiv 3 \pmod{11}$

$$5^{38} \equiv (5^{10})^3 \cdot (5^2)^4 \equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}$$

#

ตัวอย่างต่อไปนี้จะแสดงวิธีทดสอบจำนวนประกอบ โดยใช้ทฤษฎีบทเล็ก ๆ ของแฟร์มาต์

**ตัวอย่าง 3.34** จงพิจารณาว่า 117 เป็นจำนวนประกอบหรือจำนวนเฉพาะ

**วิธีทำ** เลือก $a = 2$

เพราะว่า

$$2^7 \equiv 128 \equiv 11 \pmod{117}$$

จึงได้ว่า

$$2^{117} \equiv 2^{7 \cdot 16+5} \equiv (2^7)^{16} \cdot 2^5 \equiv (11)^{16} \cdot 2^5 \pmod{117}$$

เพราะว่า

$$11^{16} \equiv (121)^8 \equiv 4^8 \pmod{117}$$

ดังนั้น

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv 4^8 \cdot 2^5 \pmod{117}$$

นั่นคือ

$$2^{117} \equiv 2^{16}\cdot 2^{5} \equiv 2^{21}(\text{mod } 117)$$

และเพราะว่า

$$2^{21} \equiv (2^{7})^{3} \equiv 11^{3} \equiv 11^{2}\cdot 11 \equiv 4\cdot 11 \equiv 44(\text{mod } 117)$$

จึงได้ว่า

$$2^{117} \equiv 44(\text{mod } 117) \not\equiv 2(\text{mod } 117)$$

นั่นคือ 117 ต้องเป็นจำนวนประกอบ เนื่องจากว่า ถ้า 117 เป็นจำนวนเฉพาะแล้ว โดยทฤษฎีบท 3.20 จะต้องได้ว่า

$$2^{117} \equiv 2(\text{mod } 117)$$ #

**ทฤษฎีบท 3.21** ถ้า p และ q เป็นจำนวนเฉพาะที่แตกต่างกัน และ a เป็นจำนวนเต็มบวก โดยที่ $a^{p} \equiv a(\text{mod } q)$ และ $a^{q} \equiv a(\text{mod } p)$ แล้ว $a^{pq} \equiv a(\text{mod } pq)$

**พิสูจน์** โดยทฤษฎีบท 3.20 ได้ว่า

$$a^{p} \equiv a(\text{mod } p)$$

ดังนั้น $(a^{p})^{q} \equiv a^{q}(\text{mod } p)$

โดยสมมติฐาน

$$a^{q} \equiv a(\text{mod } p)$$

ดังนั้น จึงได้ว่า

$$a^{pq} \equiv a(\text{mod } p)$$

และในทำนองเดียวกัน ก็พิสูจน์ได้ว่า

$$a^{pq} \equiv a(\text{mod } q)$$

เพราะว่า $p|a^{pq}-a$ และ $q|a^{pq}$ และ $(p, q) = 1$ จึงได้ว่า $pq|a^{pq}-a$

นั่นคือ $a^{pq} \equiv a(\text{mod } pq)$ #

**ตัวอย่าง 3.35** จงแสดงว่า $2^{340} \equiv 1(\text{mod } 341)$

**วิธีทำ** เพราะว่า $341 = 11\cdot 31$

และ $2^{10} \equiv 1024 \equiv 1(\text{mod } 31)$

เพราะฉะนั้น $2^{11} \equiv 2^{10}\cdot 2 \equiv 1\cdot 2 \equiv 2(\text{mod } 31)$

และเพราะว่า

$$2^{31} \equiv (2^{10})^{3}\cdot 2 \equiv 1^{3}\cdot 2 \equiv 2(\text{mod } 11)$$

จึงได้ว่า

$$2^{341} \equiv 2^{31\cdot 11} \equiv 2 \pmod{341}$$

และเพราะว่า $(2, 341) = 1$ จึงได้ว่า

$$2^{340} \equiv 1 \pmod{341}$$

#

ผลจากตัวอย่าง 3.35 แสดงให้เห็นว่า บทกลับของทฤษฎีบทของแฟร์มาต์ไม่จริง เนื่องจากมีจำนวนเต็ม $n = 341$ และจำนวนเต็มบวก $a = 2$ โดยที่ $n \nmid 2$ ที่ทำให้ $a^{n-1} \equiv 1 \pmod{n}$ แต่ $n$ ไม่ใช่จำนวนเฉพาะ

#

นอกจากนั้น ผลจากทฤษฎีบทเล็ก ๆ ของแฟร์มาต์จะทำให้การหาตัวผกผันของ $a$ มอดุโล $p$ ทำได้ง่ายขึ้น ดังนี้

**ทฤษฎีบท 3.22** ถ้า $p$ เป็นจำนวนเฉพาะ และ $a$ เป็นจำนวนเต็มบวก โดยที่ $p \nmid a$ แล้ว $a^{p-2}$ เป็นตัวผกผันของ $a$ มอดุโล $p$

**พิสูจน์** เพราะว่า $p \nmid a$ จึงได้ว่า

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

ดังนั้น

$$a^{p-1} \equiv a \cdot a^{p-2} \equiv 1 \pmod{p}$$

นั่นคือ $a^{p-2}$ เป็นตัวผกผันของ $a$ มอดุโล $p$

#

**ตัวอย่าง 3.36** จงหาตัวผกผันของ 2 มอดุโล 11

**วิธีทำ** เพราะว่า 11 เป็นจำนวนเฉพาะ และ $11 \nmid 2$ จึงได้ว่า

$$2^{10} = 2 \cdot 2^{9} \equiv 1 \pmod{11}$$

นั่นคือ $2^{9}$ เป็นตัวผกผันของ 2 มอดุโล 11

#