บทที่ 4

คอนกรูเอนซ์
Congruences

4.1 นิยามและคุณสมบัติเบื้องต้น

หลายปัญหาในทฤษฎีจำนวนนำไปสู่การพิจารณาเซ็ตของจำนวนเต็ม ซึ่งจำนวนเต็มคงที่จำนวนหนึ่งจะหารผลต่างของสมาชิกสองตัวใด ๆ ในเซ็ตได้ลงตัว เช่น การแก้สมการไดโอแฟนไทน์ $14x + 10y = 12$ จะได้คำตอบทั่วไปดังนี้ $x = -2 + 5k$, $y = 4 - 7k$ แสดงว่าค่าของ x จะต้องมาจากเซ็ตของจำนวนเต็มซึ่งอยู่ในรูป $-2 + 5k$ คือเซ็ต

$$\{ \ldots, -12, -7, -2, 3, 8, 13, \ldots \}$$

และค่าของ y จะมาจากเซ็ตของจำนวนเต็มในรูป $4 - 7k$ คือเซ็ต

$$\{ \ldots, -10, -3, 4, 11, 18, 25, \ldots \}$$

จะเห็นว่าในเซ็ตแรก 5 จะหารผลต่างของสมาชิกคู่ใด ๆ ในเซ็ตได้ลงตัว และในเซ็ตที่สอง 7จะหารผลต่างของสมาชิกคู่ใด ๆ ได้ลงตัว

C.F. Gauss เป็นผู้นำความคิดเรื่องคอนกรูเอนซ์มาทำให้การศึกษาเซ็ตแบบนี้ง่ายขึ้น

ในบทนี้เราจะศึกษาเรื่องของคอนกรูเอนซ์ (Congruences) คุณสมบัติต่าง ๆ ตลอดจนการใช้คอนกรูเอนซ์มาช่วยในการแก้สมการไดโอแฟนไทน์

นิยาม 4.1

ให้ a และ b เป็นจำนวนเต็ม m เป็นจำนวนเต็มบวก ถ้า m หาร $(a - b)$ ลงตัวแล้ว เราจะเรียกว่า "a คอนกรูเอนซ์กับ b มอดุโล m" **(modulo m)**

จะเขียนแทนด้วย $a \equiv b \pmod{m}$

ถ้า m หาร $(a - b)$ ไม่ลงตัวแล้วจะเรียกว่า a ไม่คอนกรูเอนซ์กับ b **(mod m)**

และเขียนแทนด้วย $a \not\equiv b \pmod{m}$

ขอให้จำไว้เสมอว่าเมื่อเราเขียน $a \equiv b \pmod{m}$ นั้น หมายถึงว่า $m|(a - b)$ และถ้าเราทราบว่า $m|(a - b)$ ก็หมายความว่า $a \equiv b \pmod{m}$

ตัวอย่าง 4.1

$10 \equiv 1 \pmod{9}$ $\quad$ $10 \equiv 20 \pmod{5}$

$7 \equiv -5 \pmod{6}$ $\quad$ $14 \equiv 0 \pmod{7}$

$-2 \not\equiv -6 \pmod{8}$ $\quad$ $-5 \equiv 13 \pmod{9}$

$10 \not\equiv 1 \pmod{4}$ $\quad$ $-1 \not\equiv -11 \pmod{13}$

$20 \not\equiv -2 \pmod{10}$ $\quad$ $-6 \not\equiv 0 \pmod{5}$

เนื่องจากว่า ถ้า $m|(a-b)$ แล้วจะต้องมีจำนวนเต็ม q ซึ่งทำให้ $a-b=mq$ หรือ $a=b+mq$ เราจึงได้นิยามของคอนกรูเอนซ์อีกอย่างหนึ่งว่า

$a \equiv b \pmod{m}$ ก็ต่อเมื่อจะต้องมีจำนวนเต็ม q ซึ่งทำให้

$$a = b + mq$$

$a \not\equiv b \pmod{m}$ ก็ต่อเมื่อ สำหรับจำนวนเต็มทุกจำนวน q

$$a \neq b + mq$$

ทฤษฎี 4.1

ให้ a, b, c เป็นจำนวนเต็มใด ๆ และ m เป็นจำนวนเต็มบวก

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 เพราะว่า $m|(a-a)$

เพราะฉะนั้น $a \equiv a \pmod{m}$

ถ้า $a \equiv b \pmod{m}$

ตามนิยาม $m|(a-b)$

ดังนั้น $m|(b-a)$

นั่นคือ $b \equiv a \pmod{m}$ ตามนิยาม

ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว $m|(a-b)$ และ $m|(b-c)$

เพราะฉะนั้น $m|[(a-b)+(b-c)]$

นั่นคือ $m|(a-c)$

ดังนั้น $a \equiv c \pmod{m}$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.2

ให้ d และ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ และ $d|m$ แล้ว $a \equiv b \pmod{d}$

พิสูจน์ เพราะว่า $d|m$ และ $m|(a-b)$ เพราะ $a \equiv b \pmod{m}$

เพราะฉะนั้น $d|(a-b)$

นั่นคือ $a \equiv b \pmod{d}$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.3

ให้ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$

แล้ว $a \pm c \equiv b \pm d \pmod m$

และ $ac \equiv bd \pmod m$

พิสูจน์ ถ้า $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว

จะต้องมีจำนวนเต็ม q_1 และ q_2 ซึ่งทำให้

$a = b + mq_1$ และ $c = d + mq_2$

เพราะฉะนั้น $a \pm c = b \pm d + m(q_1 \pm q_2)$

นั่นคือ $a \pm c \equiv b \pm d \pmod m$

และ $ac = bd + m(q_1 d + q_2 b + mq_1 q_2)$

ดังนั้น $ac \equiv bd \pmod m$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.2 $18 \equiv 10 \pmod 4 \quad 6 \equiv 2 \pmod 4$

$24 \equiv 18 + 6 \equiv 10 + 2 \equiv 12 \pmod 4$

$12 \equiv 18 - 6 \equiv 10 - 2 \equiv 8 \pmod 4$

$108 \equiv 18 \cdot 6 \equiv 10 \cdot 2 \equiv 20 \pmod 4$

แต่ $3 \equiv \frac{18}{6} \not\equiv \frac{10}{2} \equiv 5 \pmod 4$

ทฤษฎี 4.4

ให้ m เป็นจำนวนเต็มบวก ถ้า $a_i \equiv b_i \pmod m$ สำหรับ $i = 1, 2, \ldots, n$ แล้ว

1. $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m$

2. $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m$

พิสูจน์ 1) เพราะว่า $a_i \equiv b_i \pmod m$ ดังนั้นจะต้องมีจำนวนเต็ม q_i ซึ่ง

ทำให้ $a_i - b_i = mq_i$ สำหรับแต่ละ $i = 1, 2, \ldots, n$

เพราะฉะนั้น $m \cdot \sum_{i=1}^{n} q_i = \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i$

แสดงว่า $m \mid \left(\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i \right)$

นั่นคือ $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m$

2. $\prod_{i=1}^{n} \equiv \prod_{i=1}^{n} b_i \pmod m$

เป็นจริงเมื่อ $n = 1$

สมมุติว่าข้อความนี้เป็นจริงเมื่อ $n = k$ และ $a_i \equiv b_i \pmod m$

เมื่อ $i = 1, 2,\ldots,k+1$

นั่นคือ $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod m$

ถ้า $n = k+1$

$$a_{k+1} \equiv b_{k+1} \pmod m$$

เพราะฉะนั้นตามทฤษฎี 4.3

$$a_{k+1} \prod_{i=1}^{k} a_i \equiv b_{k+1} \prod_{i=1}^{k} b_i \pmod m$$

นั่นคือ $\prod_{i=1}^{k+1} a_i \equiv \prod_{i=1}^{k+1} b_i \pmod m$

ดังนั้นโดยการอุปนัยทางคณิตศาสตร์สรุปได้ว่า

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.5

ให้ m เป็นจำนวนเต็มบวก k เป็นจำนวนเต็มใด ๆ และ $n \geq 0$ ถ้า $a \equiv b \pmod m$

แล้ว 1. $ka \equiv kb \pmod m$

2. $a^n \equiv b^n \pmod m$

พิสูจน์ เพราะว่า $k \equiv k \pmod m$ และ $a \equiv b \pmod m$

ดังนั้นตามทฤษฎี 4.3 $ka \equiv kb \pmod m$

สำหรับการพิสูจน์ $a^n \equiv b^n \pmod m$

จากข้อ 2 ของทฤษฎี 4.4 ให้ $a_i = a$ และ $b_i = b$ สำหรับ

$i = 1, 2,\ldots,n$ เมื่อ $n > 0$ จะได้ว่า $a^n \equiv b^n \pmod m$

ถ้า $n = 0$, $1 \equiv a^0 \equiv b^0 \equiv 1 \pmod m$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

เรามาพิจารณาคอนกรูเอนซ์ต่อไปนี้ $15 \equiv 3 \pmod 6$ และ $5 \not\equiv 1 \pmod 6$ จากตัวอย่างนี้จะพบว่า ถ้า $ac \equiv bc \pmod m$ แล้วไม่จำเป็นว่า $a \equiv b \pmod m$ เพราะว่า ถ้า $ac \equiv bc \pmod m$ แล้ว $m|ac - bc$ หรือ $m|(a - b)c$ ซึ่งไม่จำเป็นว่า $m|(a - b)$ และ $a \equiv b \pmod m$

อาจจะเป็นว่าส่วนหนึ่งของ m หาร c ลงตัวและอีกส่วนหนึ่งของ m หาร (a – b) ลงตัว หรือแม้แต่ m หาร c ลงตัวก็สรุปไม่ได้ว่า m หาร (a – b) ลงตัว ทฤษฎีและบทแทรกต่อไปนี้จะบอกให้ทราบว่าเราจะสรุปได้อย่างไร ถ้า $ac \equiv bc \pmod{m}$

ทฤษฎี 4.6

ให้ m เป็นจำนวนเต็มบวก และ ห.ร.ม. ของ m และ c เท่ากับ d แล้ว $ac \equiv bc \pmod{m}$ ก็ต่อเมื่อ $a \equiv b \pmod{m/d}$

พิสูจน์ ถ้า $ac \equiv bc \pmod{m}$ แล้วจะต้องมีจำนวนเต็ม q ซึ่งทำให้

$ac - bc = mq$ หรือ $ac = bc + mq$

เพราะฉะนั้น $a \cdot \frac{c}{d} = b \cdot \frac{c}{d} + \frac{m}{d} \cdot q$

ซึ่ง $\frac{c}{d}$ เป็นจำนวนเต็ม เพราะ $d = (m, c)$

แสดงว่า $\frac{c}{d} \mid \frac{m}{d} \cdot q$

แต่ $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$

เพราะฉะนั้น $\frac{c}{d} \mid q$ ตามทฤษฎี 2.7

นั่นคือ $a = b + \frac{m}{d} \cdot \frac{qd}{c}$ เมื่อ $\frac{m}{d}$ และ $\frac{qd}{c}$ เป็นจำนวนเต็ม

เพราะฉะนั้น $a \equiv b \left(\mod \frac{m}{d}\right)$

ในทางกลับกันถ้า $a \equiv b \left(\mod \frac{m}{d}\right)$

$$a = b + \frac{m}{d} \cdot t \text{ สำหรับ t เป็นจำนวนเต็ม}$$

$$ac = bc + m \cdot t \cdot \frac{c}{d} \text{ เมื่อ } \frac{c}{d} \text{ เป็นจำนวนเต็ม}$$

เพราะฉะนั้น $ac \equiv bc \pmod{m}$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

บทแทรก 4.1

ถ้า $ac \equiv bc \pmod{m}$ และ $(m, c) = 1$ แล้ว $a \equiv b \pmod{m}$

พิสูจน์ ตามทฤษฎี 4.6 เพราะ $(m, c) = 1 = d$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.7

ถ้า $c \neq 0$ และ $ac \equiv bc \pmod{mc}$ แล้ว $a \equiv b \pmod{m}$

พิสูจน์ เพราะว่า $ac \equiv bc \pmod{mc}$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม q ซึ่งทำให้

$$ac - bc = q\,mc$$
$$c(a - b) = q\,mc$$
$$a - b = q\,m$$

ดังนั้น $a \equiv b \pmod{m}$ ตามนิยาม

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 4.1

1. จงหาว่าจำนวนต่อไปนี้คู่ไหนบ้างที่คอนกรูเอนซ์กัน มอดุโล 7,

   $-6, -4, -1, 1, 3, 6, 8, 10, 13$

2. ให้ $S_a^m = \{ a \pm mk \}_{k=0}^{\infty}$ และ $S_a^m = S_b^m$ ก็ต่อเมื่อ $a \in S_b^m$ ก็ต่อเมื่อ $b \in S_a^m$ จงพิสูจน์ว่า $S_a^m = S_b^m$ ก็ต่อเมื่อ $a \equiv b \pmod{m}$

3. จงพิสูจน์ว่า $ab \equiv 0 \pmod{p}$ ก็ต่อเมื่อ $a \equiv 0 \pmod{p}$ หรือ $b \equiv 0 \pmod{p}$ สำหรับ p เป็นจำนวนเฉพาะ

4. จงพิสูจน์ว่า ถ้า $a^2 \equiv 1 \pmod{p}$ แล้ว $a \equiv \pm 1 \pmod{p}$ สำหรับ p เป็นจำนวนเฉพาะ

5. จงพิสูจน์ว่า 17 หาร $5n^2 + 15$ ไม่ลงตัวสำหรับ n เป็นจำนวนเต็ม

6. จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ และ $n \mid m$ แล้ว $a \equiv b \pmod{n}$

7. ถ้า $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ และ $(m, n) = 1$ จงพิสูจน์ว่า $a \equiv b \pmod{mn}$ (แนะนำ : ใช้ทฤษฎี 2.8)

8. ถ้า $a \equiv b \pmod{m_i}$ สำหรับ $i = 1, 2, \ldots, k$ และ $(m_i, m_j) = 1$ เมื่อ $i \neq j$ แล้วจงพิสูจน์ว่า $a \equiv b \pmod{m}$ เมื่อ $m = \prod_{i=1}^{k} m_i$

9. จงพิสูจน์ว่า $a^3 \equiv a \pmod{3}$ และ $a^5 \equiv a \pmod{5}$ สำหรับ a เป็นจำนวนเต็มใด ๆ

10. จงพิสูจน์ว่า $a^5 \equiv a \pmod{15}$

11. ให้ m, n เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ และ $a \equiv b \pmod{n}$ แล้วจงพิสูจน์ว่า $a \equiv b \; [\text{mod ค.ร.น.}(m, n)]$

4.2 กฎเกณฑ์การหารชนิดพิเศษ (Special Divisibility Criteria)

ดังที่ทราบแล้วว่า จำนวนเต็มที่ 2 หารลงตัวจะต้องเป็นจำนวนคู่ หรือหลักหน่วยของจำนวนนั้นเป็นจำนวนเต็มคู่นั่นเอง ดังนั้นสำหรับจำนวนเต็ม n ใด ๆ ที่อยู่ในรูป $n = 10k + u$ ซึ่ง u เป็นเลขในหลักหน่วยของ n แล้ว 2 หาร n ลงตัวก็ต่อเมื่อ 2 หาร u ได้ลงตัว ในทำนองเดียวกัน 5 จะหารจำนวนเต็มใดได้ลงตัวก็ต่อเมื่อเลขหลักหน่วยของจำนวนนั้นต้องเป็น 5 หรือ 0 สำหรับการหารด้วย 3 หรือ 9 หรือ 11 ก็มีวิธีการคิดอย่างเดียวกัน ซึ่งจะพบในทฤษฎีต่อไป โดยเริ่มแรกจะพิสูจน์ทฤษฎีสำหรับโพลิโนเมียลคอนกรูเอนซ์เสียก่อน

ทฤษฎี 4.8

ให้ $f(x) = \sum_{k=0}^{n} c_k x^k$ เมื่อ $c_0, c_1, \ldots, c_n$ เป็นจำนวนเต็ม ถ้า $\pmod m$

แล้ว $f(a) \equiv f(b) \pmod m$

พิสูจน์ เพราะว่า $a \equiv b \pmod m$

เพราะฉะนั้นจากทฤษฎี 4.5 ข้อ 2 จะได้ว่า

$$a^k \equiv b^k \pmod m \text{ เมื่อ } k = 0, 1, \ldots, n$$

ดังนั้น $c_k a^k \equiv c_k b^k \pmod m$ ตามทฤษฎี 4.5 ข้อ 1

และตามทฤษฎี 4.4 จะได้ว่า

$$\sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod m$$

นั่นคือ $f(a) \equiv f(b) \pmod m$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.3 ให้ $f(x) = x^2 + 2x + 1 \quad m = 5$

$$\left.\begin{array}{ll} f(0) = 1 \equiv 1 & 1 \equiv 36 = f(5) \\ f(1) = 4 \equiv 4 & 4 \equiv 49 = f(6) \\ f(2) = 9 \equiv 4 & 4 \equiv 64 = f(7) \\ f(3) = 16 \equiv 1 & 1 \equiv 81 = f(8) \\ f(4) = 25 \equiv 0 & 0 \equiv 100 = f(9) \end{array}\right\} \pmod 5$$

$$\left.\begin{array}{l} f(0) \equiv f(5) \\ f(1) \equiv f(6) \\ f(2) \equiv f(7) \\ f(3) \equiv f(8) \\ f(4) \equiv f(9) \end{array}\right\} \pmod 5$$

ตัวอย่าง 4.4 จะแสดงให้เห็นว่าทฤษฎี 4.8 ไม่เป็นจริง ถ้าสัมประสิทธิ์ใน f(x) ไม่ใช่จำนวนเต็ม

เช่น $g(x) = \frac{(x-1)x}{6}$ $m = 3$

$10 \equiv 4 \pmod 3$

แต่ $g(10) = 15 \not\equiv 2 = g(4) \pmod 3$

ทฤษฎี 4.9

ให้ $a = \sum_{k=0}^{n} a_k 10^k$, $s = \sum_{k=0}^{n} a_k$ และให้ $t = \sum_{k=0}^{n} (-1)^k a_k$ แล้ว

1. $9|a$ ก็ต่อเมื่อ $9|s$
2. $3|a$ ก็ต่อเมื่อ $3|s$
3. $11|a$ ก็ต่อเมื่อ $11|t$

พิสูจน์ 1. $a = \sum_{k=0}^{n} a_k 10^k = f(10)$ เมื่อ $f(x) = \sum_{k=0}^{n} a_k x^k$ และ

$s = \sum_{k=0}^{n} a_k = f(1)$

เมื่อ $10 \equiv 1 \pmod 9$

ดังนั้นจากทฤษฎี 4.8 $f(10) \equiv f(1) \pmod 9$

หรือ $a \equiv s \pmod 9$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม q ซึ่งทำให้

$a - s = 9q$

แสดงว่า $9|a$ ก็ต่อเมื่อ $9|s$

2. $3|a$ ก็ต่อเมื่อ $3|s$ พิสูจน์เหมือนข้อ 1

3. $a = f(10)$ และ $t = \sum_{k=0}^{n} a_k(-1)^k = f(-1)$

และเพราะว่า $10 \equiv -1 \pmod{11}$

ดังนั้นจากทฤษฎี 4.8 $f(10) \equiv f(-1) \pmod{11}$

แสดงว่า $a \equiv t \pmod{11}$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม r ซึ่งทำให้

$a - t = 11r$

แสดงว่า $11|a$ ก็ต่อเมื่อ $11|t$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.5 พิจารณาว่า 9 หาร 340722 ลงตัวหรือไม่

จากทฤษฎีเราทราบว่า $9|340722$ เพราะ

$9|3+4+0+7+2+2$

$3|41811$ เพราะ $3|4+1+8+1+1$

$11|304161$ เพราะ $11|-3+0-4+1-6+1$

แต่ 3, 9 และ 11 หาร 357266 ไม่ลงตัวเพราะ

3 และ 9 หาร $3+5+7+2+6+6 = 29$ ไม่ลงตัว

และ 11 หาร $-3+5-7+2-6+6 = -3$ ไม่ลงตัว

แบบฝึกหัด 4.2

1. จงพิจารณาดูว่า 3, 9, 11 หารเลขต่อไปนี้ลงตัวหรือไม่

   1) 37,686 2) 113,058 3) 20,004

2. $10^3 \equiv -1 \pmod 7$ จงหาเงื่อนไขสำหรับ 7 หารลงตัว

3. ให้ $a = \sum_{k=0}^{n} a_k 10^k$ จงพิสูจน์ว่า

   1) $6|a$ ก็ต่อเมื่อ $3|a$ และ $2|a$

   2) $4|a$ ก็ต่อเมื่อ $4|(10a_1 + a_0)$

4. ให้ a และ b เป็นจำนวนเต็มบวก และ $f(x) = 2^x$ ถ้า $a \equiv b \pmod 3$ แล้ว $f(a) \equiv f(b) \pmod 3$ เป็นจริงเสมอหรือไม่

5. ให้ m เป็นจำนวนเต็มบวก $g(x_1, x_2,\ldots,x_n) \in Z[x_1, x_2,\ldots x_n]$ จงพิสูจน์ว่า ถ้า $a_i \equiv b_i \pmod m$ สำหรับ $i = 1, 2,\ldots,n$ แล้ว $g(a_1, a_2,\ldots,a_n) \equiv g(b_1, b_2,\ldots,b_n) \pmod m$

4.3 คอนกรูเอนซ์เชิงเส้น (Linear Congruences)

ในการพิจารณาคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{m}$ เพื่อที่จะหาคำตอบของคอนกรูเอนซ์นี้ เราหมายถึงว่าจะต้องหาจำนวนเต็มตัวหนึ่ง สมมุติ x_0 ซึ่งทำให้ $ax_0 \equiv b \pmod{m}$ ปัญหาในตอนนี้ก็คือคอนกรูเอนซ์ดังกล่าวข้างต้นนี้จะมีคำตอบเป็นจำนวนเต็มเมื่อใด และจะหาคำตอบทั้งหมดอย่างไร

สมมุติว่า x_0 เป็นคำตอบของคอนกรูเอนซ์ $ax \equiv b \pmod{m}$ แล้วจะต้องมีจำนวนเต็ม y_0 ซึ่งทำให้ $ax_0 - b = my_0$

หรือ $ax_0 - my_0 = b$

ดังนั้น x_0, y_0 ก็เป็นคำตอบของสมการไดโอแฟนไทน์เชิงเส้น

$$ax - my = b$$

หรือจะกล่าวอีกนัยหนึ่งว่า ถ้าสมการไดโอแฟนไทน์เชิงเส้น $ax - my = b$ มีคำตอบชุดหนึ่งเป็น x_0, y_0 แล้ว

$$ax_0 - my_0 = b$$

ดังนั้น

$$ax_0 \equiv b \pmod{m}$$

ทฤษฎี 4.10 คอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{m}$ จะมีคำตอบก็ต่อเมื่อ ห.ร.ม. ของ a และ m หาร b ได้ลงตัว และถ้าคอนกรูเอนซ์นี้มีคำตอบแล้ว จำนวนคำตอบจะเท่ากับ ห.ร.ม. ของ a และ m คำตอบที่ไม่คอนกรูเอนซ์ กัน (incongruent solution)

พิสูจน์ ให้ $(a, m) = d$ สมมุติว่า $d|b$

ดังนั้นจะต้องมีจำนวนเต็ม k ซึ่งทำให้ $b = dk$

แต่ $d = (a, m)$ ดังนั้นตามทฤษฎี 2.5

จะต้องมีจำนวนเต็ม q และ r ซึ่งทำให้

$$d = aq + mr$$

เพราะฉะนั้น $b = kd = akq + mkr$

หรือ $b - akq = mkr$

แสดงว่า $akq \equiv b \pmod{m}$

นั่นคือ kq เป็นคำตอบของคอนกรูเอนซ์ $ax \equiv b \pmod{m}$

ในทางกลับกันสมมุติว่า x_0 เป็นคำตอบหนึ่งของคอนกรูเอนซ์นี้

ดังนั้น $ax_0 \equiv b \pmod{m}$ และจะต้องมีจำนวนเต็ม t ซึ่ง

ทำให้ $ax_0 - b = mt$

หรือ $ax_0 - mt = b$

แต่ $d|a$ และ $d|m$ เพราะ $d = (a, m)$

ดังนั้น $d|b$ ตามทฤษฎี 2.1 ข้อ 5

ขั้นต่อไปจะแสดงว่าคำตอบทั้งหมดมีอะไรบ้าง

ถ้า x_0 เป็นคำตอบหนึ่งของคอนกรูเอนซ์ $ax \equiv b \pmod m$

แล้วจะต้องมีจำนวนเต็ม y_0 ซึ่งทำให้ $ax_0 - b = my_0$

ซึ่งคำตอบทั่วไปของสมการนี้คือ $x_t = x_0 + \frac{m}{d}t$

แสดงว่า $x_0 + \frac{m}{d}t$ เป็นคำตอบของคอนกรูเอนซ์ข้างบนนี้

สำหรับ t เป็นจำนวนเต็มใด ๆ เพราะ

$$a\left(x_0 + \frac{m}{d}t\right) = ax_0 + mt \cdot \frac{a}{d} \equiv ax_0 \equiv b \pmod m$$

ถ้า x_1 เป็นอีกคำตอบหนึ่งของ $ax \equiv b \pmod m$ แล้ว

$$ax_1 \equiv b \equiv ax_0 \pmod m$$

ดังนั้นตามทฤษฎี 4.6

$$x_1 \equiv x_0 \left(\mod \frac{m}{d}\right)$$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม t ซึ่งทำให้

$$x_1 = x_0 + \frac{m}{d}t$$

แสดงว่า ถ้า x_0 เป็นคำตอบหนึ่งของคอนกรูเอนซ์เชิงเส้นแล้ว คำตอบอื่นจะอยู่ในรูป

$x_0 + \frac{m}{d}t$ เมื่อ t เป็นจำนวนเต็ม ซึ่งจะมีทั้งหมด d คำตอบที่ไม่คอนกรูเอนซ์กันมอดุโล **m**

และคำตอบเหล่านั้นน้อยกว่า m

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.6 $49x \equiv 30 \pmod{35}$ ไม่มีคำตอบเพราะ $(49, 35) = 7$ ซึ่ง $7 \nmid 30$

ตัวอย่าง 4.7 จงหาค่าของ x ซึ่งสอดคล้องกับ $51x \equiv 21 \pmod{36}$

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

ดังนั้นคอนกรูเอนซ์นี้มี 3 คำตอบที่ไม่คอนกรูเอนซ์กันมอดุโล 36

เนื่องจาก $51 \equiv 15 \pmod{36}$

ดังนั้น $51x \equiv 15x \pmod{36}$

แทนที่ 51x ด้วย 15x จะได้

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

จากทฤษฎี 4.7 ลดทอนโดยใช้ 3 หารจะได้

$$5x \equiv 7 \pmod{12}$$

หาจำนวนเต็มมาคูณกับ 5 แล้วให้ได้ผลลัพธ์คอนกรูเอนซ์กับ 1
มอดุโล 12 ซึ่งในที่นี้คือ 5 แล้วนำ 5 มาคูณทั้งสองข้างคอนกรูเอนซ์จะได้

$$5.5x \equiv 5.7 \pmod{12}$$

แต่ $25 \equiv 1 \pmod{12}$

และ $35 \equiv 11 \pmod{12}$

เพราะฉะนั้น $x \equiv 11 \pmod{12}$

ดังนั้น 3 คำตอบของ $51x \equiv 21 \pmod{36}$

จะอยู่ในรูป $x \equiv 11+12t$ เมื่อ $t = 0, 1, 2$

ก็คือ $x \equiv 11 \pmod{36}$

$x \equiv 23 \pmod{36}$

$x \equiv 35 \pmod{36}$

ตัวอย่าง 4.8 จงหาค่าของ x ซึ่งสอดคล้องกับ $22x \equiv 4 \pmod{30}$

วิธีทำ

$$22x \equiv 4 \pmod{30}$$
$$11x \equiv 2 \pmod{15}$$
$$-4x \equiv 2 \pmod{15} \text{ เพราะ } 11 \equiv -4 \pmod{15}$$
$$-16x \equiv 8 \pmod{15}$$
$$-x \equiv 8 \pmod{15}$$
$$x \equiv -8 \pmod{15}$$

ดังนั้น 2 คำตอบซึ่งมากกว่า 0 และน้อยกว่า 30 คือ

$-8+15 = 7$ และ $-8+30 = 22$

เราสามารถใช้วิธีการแก้คอนกรูเอนซ์เชิงเส้นมาใช้ในการแก้สมการไดโอแฟนไทน์เชิงเส้น ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.9 จงแก้สมการ $7x + 11y = 100$ ต้องการคำตอบเป็นจำนวนเต็มบวก

วิธีทำ สมมุติว่า x_0, y_0 เป็นคำตอบของสมการนี้ แล้ว x_0, y_0 จะสอดคล้องกับคอนกรูเอนซ์

$7x_0 \equiv 100 \pmod{11}$ และ $11y_0 \equiv 100 \pmod{7}$

ดังนั้นคำตอบของ $7x + 11y = 100$ ก็คือคำตอบของ $7x \equiv 100 \pmod{11}$

หรือ $11y \equiv 100 \pmod{7}$

จาก $11y \equiv 100 \pmod{7}$

$4y \equiv 2 \pmod{7}$

$8y \equiv 4 \pmod{7}$

$y \equiv 4 \pmod{7}$

ดังนั้นค่า y ซึ่งเป็นจำนวนเต็มบวกซึ่งคล้องตามสมการนี้คือ 4, 11, 18,...

สำหรับค่าของ x ซึ่งสมนัยกับ y ในสมการนี้คือ 8, -3, -14,...

ดังนั้นคำตอบที่เป็นจำนวนเต็มบวกก็คือ $x = 8$, $y = 4$

แบบฝึกหัด 4.3

ข้อ 1 ถึง 9 จงหาค่าของ x ซึ่งสอดคล้องกับคอนกรูเอนซ์ต่อไปนี้

1. $25x \equiv 4 \pmod{11}$
2. $15x \equiv 3 \pmod{9}$
3. $23x \equiv 41 \pmod{52}$
4. $42x \equiv 37 \pmod{63}$
5. $42x \equiv 50 \pmod{76}$
6. $70x \equiv 50 \pmod{90}$
7. $34x \equiv 60 \pmod{98}$
8. $68x \equiv 100 \pmod{120}$
9. $35x \equiv 15 \pmod{182}$
10. จงหาคำตอบที่เป็นจำนวนเต็มบวกทั้งหมดของ
    1) $5x + 7y = 110$
    2) $23x + 37y = 212$
    3) $17x - 11y = 272$
11. ผ้าตัดเสื้อราคาเมตรละ 25 บาท ผ้าตัดกางเกงราคาเมตรละ 50 บาท มีเงิน 2,000 บาท จะซื้อผ้าทั้งสองอย่างได้อย่างละกี่เมตร

4.4 ชั้นเรซิดิว (Residue Classes)

นิยาม 4.2 เซ็ตของจำนวนเต็มซึ่งคอนกรูเอนซ์กับจำนวนเต็มตัวหนึ่ง มอดุโล m เรียกว่า ชั้นเรซิดิว (Residue Class) มอดุโล m

ตัวอย่าง 4.10 เซ็ตตอไปนี้คือชั้นเรซิดิว มอดุโล 7

$$\{ \ldots, -14, -7, 0, 7, 14, 21, \ldots \}$$
$$\{ \ldots, -13, -6, 1, 8, 15, 22, \ldots \}$$
$$\{ \ldots, -12, -5, 2, 9, 16, 23, \ldots \}$$
$$\{ \ldots, -11, -4, 3, 10, 17, 24, \ldots \}$$
$$\{ \ldots, -10, -3, 4, 11, 18, 25, \ldots \}$$
$$\{ \ldots, -9, -2, 5, 12, 19, 26, \ldots \}$$
$$\{ \ldots, -8, -1, 6, 13, 20, 27, \ldots \}$$

เซ็ตแรกคือเซ็ตของจำนวนเต็มซึ่งคอนกรูเอนซ์กับศูนย์ มอดุโล 7

เซ็ตที่สองคือเซ็ตของจำนวนเต็มซึ่งคอนกรูเอนซ์กับ 1 มอดุโล 7

จนกระทั่งเซ็ตที่ 7 คือเซ็ตของจำนวนเต็มคอนกรูเอนซ์กับ 6 มอดุโล 7

เราจะพบว่าจำนวนเต็มในแต่ละเซ็ตจะคอนกรูเอนซ์กัน มอดุโล 7 แต่จะไม่คอนกรูเอนซ์ มอดุโล 7 กับสมาชิกในต่างเซ็ตเลย เช่น ในเซ็ตแรกกับเซ็ตที่สอง สมาชิกทุกตัวในเซ็ตแรกจะไม่คอนกรูเอนซ์มอดุโล 7 กับสมาชิกทุกตัวในเซ็ตที่สองเลย

เราจะใช้ $R_a \pmod m$ แทนชั้นเรซิดิว มอดุโล m ดังนั้น $R_a \pmod m$ ก็คือเซ็ตของจำนวนเต็มซึ่งคอนกรูเอนซ์กับ a มอดุโล m แต่ชั้นเรซิดิวสามารถใช้สัญลักษณ์แทนได้มากมายนับไม่ถ้วน เช่น ในตัวอย่างเซ็ตแรกอาจเขียนแทนด้วย $R_{-14}, R_{-7}, R_0, R_7, R_{14}, \ldots$

ทฤษฎี 4.11 ให้ m เป็นจำนวนเต็มบวกแล้ว

1. $R_a = R_b$ ก็ต่อเมื่อ $a \equiv b \pmod m$
2. $R_a = R_b$ หรือ $R_a \cap R_b = \phi$ สำหรับ R_a และ R_b เป็นชั้นเรซิดิวมอดุโล m
3. ชั้นเรซิดิวมอดูโล m จะมีจำนวนทั้งหมด m ชั้น และทุก ๆ ชั้นเรซิดิวรวมกันก็คือจำนวนเต็มทั้งหมด

พิสูจน์ 1. ถ้า $a \equiv b \pmod m$ แล้วจากทฤษฎี 4.1

จำนวนเต็ม $c \equiv a \pmod m$ ก็ต่อเมื่อ

$$c \equiv b \pmod m$$

ดังนั้น $R_a = R_b$

2. สมมุติว่า R_a และ R_b มีสมาชิกร่วมกันคือ c

แสดงว่า $c \equiv a \pmod m$ และ $c \equiv b \pmod m$

จากทฤษฎี 4.1 จะได้ว่า

$$a \equiv b \pmod m$$

ดังนั้นจากข้อ 1. ที่พิสูจน์มาแล้ว $R_a = R_b$

นั่นคือ $R_a \cap R_b = \phi$ หรือ $R_a = R_b$

3. ถ้า a เป็นจำนวนเต็ม เราสามารถจะนำ m มาหาร a ได้ดังนี้

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

เพราะฉะนั้น $a \equiv r \pmod m$

จากข้อ 1. ข้างต้น $R_a = R_r$

แสดงว่า a เป็นสมาชิกของชั้นเรซิดิวชั้นหนึ่งชั้นใดต่อไปนี้

$R_0, R_1, R_2, \ldots, R_{m-1}$

เพราะจำนวนเต็ม 0, 1, 2,..., m - 1 ไม่มีคู่ใดคอนกรูเอนซ์ มอดุโล m กันเลย

แสดงว่าจะมีชั้นเรซิดิว มอดุโล m ทั้งหมด m ชั้น

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 4.4

1. จงเขียนสมาชิกของชั้นเรซิดิว มอดุโล 17 ต่อไปนี้มาชั้นละ 7 ตัว

   $R_7, R_{29}, R_{72}, R_5, R_{-47}, R_{-80}, R_{-101}$

2. จงบอกว่ามีชั้นไหนที่เท่ากัน

4.5 ระบบคอนกรูเอนซ์เชิงเส้น (System of Linear Congruences)

พิจารณาระบบคอนกรูเอนซ์ต่อไปนี้

$$a_1x \equiv b_1 \pmod{m_1}$$
$$a_2x \equiv b_2 \pmod{m_2}$$
$$\cdots$$
$$a_nx \equiv b_n \pmod{m_n}$$

ในการหาคำตอบสำหรับระบบคอนกรูเอนซ์นี้ก็คือจะต้องหาจำนวนเต็ม x_0 ซึ่งเป็นคำตอบของทุก ๆ คอนกรูเอนซ์ในระบบ

ทฤษฎี 4.12 ให้ m_1, m_2 เป็นจำนวนเต็มบวก ระบบคอนกรูเอนซ์

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$

จะมีคำตอบก็ต่อเมื่อ $(m_1, m_2)|(b_1 - b_2)$ ถ้ามีคำตอบ และ x_0 เป็นคำตอบหนึ่งแล้ว คำตอบอื่น ๆ จะคอนกรูเอนซ์กับ x_0 มอดุโล $[m_1, m_2]$ หรือคอนกรูเอนซ์นี้มีคำตอบเดียวในมอดุโล $[m_1, m_2]$ ที่เป็นจำนวนเต็มบวกน้อยกว่า $[m_1, m_2]$

พิสูจน์ (ตอนที่ 1) จำนวนเต็ม x_0 เป็นคำตอบของระบบคอนกรูเอนซ์ก็ต่อเมื่อ จะต้องมีจำนวนเต็ม k ซึ่งทำให้

$$x_0 = b_1 + km_1$$

และ $b_1 + km_1 \equiv b_2 \pmod{m_2}$

หรือ $m_1k \equiv b_2 - b_1 \pmod{m_2}$

ดังนั้นจากทฤษฎี 4.10 จะมีจำนวนเต็ม k ก็ต่อเมื่อ $(m_1, m_2)|(b_1 - b_2)$

(ตอนที่ 2) สมมุติว่า $(m_1, m_2)|(b_1 - b_2)$ และ x_0 เป็นคำตอบหนึ่งของระบบคอนกรูเอนซ์ ถ้า x_1 เป็นคำตอบอีกคำตอบหนึ่งแล้ว

$$x_1 \equiv b_1 \equiv x_0 \pmod{m_1}$$

และ $x_1 \equiv b_2 \equiv x_0 \pmod{m_2}$

เพราะฉะนั้น $m_1|x_1 - x_0$ และ $m_2|x_1 - x_0$

แสดงว่า $x_1 - x_0$ เป็นตัวคูณร่วมของ m_1 และ m_2

ดังนั้นจากนิยามของ ค.ร.น. $[m_1, m_2]|x_1 - x_0$

นั่นคือ $x_1 \equiv x_0 \pmod{[m_1, m_2]}$ ตามนิยาม

ในทางกลับกัน ถ้า $x_1 \equiv x_0 \pmod{[m_1, m_2]}$ แล้ว

$$x_1 \equiv x_0 \equiv b_1 \pmod{m_1}$$

และ $x_1 \equiv x_0 \equiv b_2 \pmod{m_2}$

ดังนั้น x_1 เป็นคำตอบของระบบคอนกรูเอนซ์

นั่นคือคำตอบทั่วไปของระบบคอนกรูเอนซ์นี้คือ $x \equiv x_0 \pmod{[m_1, m_2]}$

หรือกล่าวอีกอย่างหนึ่งว่าระบบคอนกรูเอนซ์นี้มีคำตอบที่เป็นจำนวนเต็มบวกและน้อยกว่า $[m_1, m_2]$ เพียงคำตอบเดียว

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

บทแทรก 4.2 ระบบคอนกรูเอนซ์เชิงเส้น

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_n \pmod{m_n}$$

จะมีคำตอบก็ต่อเมื่อ $(m_i, m_j) | (a_i - a_j)$

ถ้าคอนกรูเอนซ์นี้มีคำตอบ และถ้าคำตอบหนึ่งเป็น x_0

แล้วคำตอบทั่วไปคือ $x \equiv x_0 \pmod{[m_1, m_2, \ldots, m_n]}$

หรือจะมีคำตอบเพียงคำตอบเดียวที่เป็นจำนวนเต็มบวก

และน้อยกว่า $[m_1, m_2, \ldots, m_n]$

พิสูจน์ ให้ผู้อ่านทำเป็นแบบฝึกหัด

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.11 จงหาคำตอบของระบบคอนกรูเอนซ์ $x \equiv 1 \pmod{3}$

$$x \equiv 2 \pmod{5}$$

วิธีทำ $[3, 5] = 15$ และ $(3, 5) | (1 - 2)$

ดังนั้นเราจะต้องหาคำตอบในมอดุโล 15 ซึ่งอาจจะหาได้โดยหาคำตอบจากแต่ละคอนกรูเอนซ์ มอดุโล 15

ให้ S เป็นเซ็ตของจำนวนเต็ม x ซึ่ง $x \equiv 1 \pmod{3}$ ในมอดุโล 15

$$S = \{ 1, 4, 7, 10, 13 \}$$

ให้ T เป็นเซ็ตของจำนวนเต็ม x ซึ่ง $x \equiv 2 \pmod{5}$ ในมอดุโล 15

$$T = \{ 2, 7, 12 \}$$
$$S \cap T = \{ 7 \}$$

ดังนั้น 7 เป็นคำตอบสำหรับ $x \equiv 1 \pmod 3$ และ $x \equiv 2 \pmod 5$ ในมอดุโล

อาจจะทำอีกวิธีหนึ่งได้ดังนี้

จาก $x \equiv 1 \pmod 3$ จะมีจำนวนเต็ม t ซึ่งทำให้

$$x = 1 + 3t$$

ดังนั้น $1 + 3t \equiv 2 \pmod 5$

$$3t \equiv 1 \pmod 5$$

$$t \equiv 7 \equiv 2 \pmod 5$$

แสดงว่ามีจำนวนเต็ม k ซึ่งทำให้ $t = 2 + 5k$

$$x = 1 + 3t = 1 + 3(2 + 5k)$$

$$x = 7 + 15k$$

ดังนั้น $x \equiv 7 \pmod{15}$ เป็นคำตอบที่ต้องการ

ทฤษฎี 4.13 (Chinese Remainder Theorem)

ให้ $m_1, m_2, \ldots, m_n$ เป็นจำนวนเต็มบวก ถ้า $(m_i, m_j) = 1$

สำหรับ $i \neq j$ แล้วระบบคอนกรูเอนซ์

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$$\cdots$$

$$x \equiv c_n \pmod{m_n}$$

จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $m = \prod_{i=1}^{n} m_i$

พิสูจน์ จากทฤษฎี 4.12 เราทราบว่าคอนกรูเอนซ์สองอันแรกมีคำตอบเพียงคำตอบเดียวในมอดุโล m_1m_2 แสดงว่า

$$x \equiv a_2 \pmod{m_1m_2} \qquad \text{(A)}$$

จากคอนกรูเอนซ์ที่ 3 $\quad x \equiv c_3 \pmod{m_3} \qquad$ (B)

แต่ $(m_1, m_3) = 1 = (m_2, m_3)$ ดังนั้นตามทฤษฎี 2.12

$$(m_1m_2, m_3) = 1$$

จากทฤษฎี 4.12 สำหรับคอนกรูเอนซ์ (A) กับ (B) จะมีคำตอบเพียงคำตอบเดียวในมอดุโล $m_1m_2m_3$

แสดงว่าสามคอนกรูเอนซ์แรกมีคำตอบร่วมกันเพียงคำตอบเดียวในมอดุโล $m_1m_2m_3$

เขียนได้เป็น

$$x \equiv b_3 \pmod{m_1m_2m_3} \quad (C)$$

จากคอนกรูเอนซ์ที่สี่ $x \equiv c_4 \pmod{m_4}$ (D)

ในทำนองเดียวกันกับที่พิสูจน์คอนกรูเอนซ์ (A) และ (B) จะได้ว่า คอนกรูเอนซ์ (C) กับ (D) มีคำตอบร่วมกันเพียงคำตอบเดียวใน มอดุโล $m_1m_2m_3m_4$

ทำดังนี้ไปเรื่อย ๆ จำนวน n-1 ครั้ง จะได้ว่าระบบคอนกรูเอนซ์นี้มีคำตอบเพียงคำตอบเดียวใน มอดุโล $m = \prod_{i=1}^{n} m_i$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.12 จงหาคำตอบของระบบสมการ $x \equiv 5 \pmod{15}$

$x \equiv 1 \pmod{21}$

วิธีทำ จะเห็นว่าถ้า $x \equiv 5 \pmod{15}$ แล้ว

$x \equiv 5 \pmod{3}$

และ $x \equiv 2 \pmod{3}$ แต่ $x \equiv 1 \pmod{21}$

ดังนั้น $x \equiv 1 \pmod{3}$

ถ้าระบบคอนกรูเอนซ์นี้มีคำตอบแล้ว คำตอบนั้นจะต้องคอนกรูเอนซ์กับ 2 มอดุโล 3 และคอนกรูเอนซ์กับ 1 มอดุโล 3 ด้วย ซึ่งเป็นไปไม่ได้

ดังนั้นระบบคอนกรูเอนซ์นี้ไม่มีคำตอบ

ถ้าเราทดสอบตั้งแต่แรกก็จะทราบเพราะ $(15, 21) \nmid (5 - 1)$

ตัวอย่าง 4.13 จงหาคำตอบของระบบคอนกรูเอนซ์

$x \equiv 1 \pmod{2}$ $x \equiv 2 \pmod{3}$

$x \equiv 1 \pmod{5}$ $x \equiv 5 \pmod{7}$

วิธีทำ จาก $x \equiv 1 \pmod{2}$ และ $x \equiv 1 \pmod{5}$

จะได้ $x \equiv 1 \pmod{10}$

ดังนั้นจะต้องมีจำนวนเต็ม t ซึ่งทำให้

$$x = 1 + 10t$$

เพราะฉะนั้น $1 + 10t \equiv 2 \pmod{3}$

$10t \equiv 1 \pmod{3}$

$t \equiv 1 \pmod{3}$

แสดงว่าจะต้องมีจำนวนเต็ม k ซึ่งทำให้ $t = 1 + 3k$

$x = 1 + 10t = 1 + 10(1 + 3k) = 11 + 30k$

นั่นคือ $x = 11 + 30k \equiv 5 \pmod 7$

$30k \equiv -6 \pmod 7$

$2k \equiv -6 \pmod 7$

$k \equiv -3 \equiv 4 \pmod 7$

แสดงว่าจะต้องมีจำนวนเต็ม ℓ ซึ่งทำให้ $k = 4 + 7\ell$

$x = 11 + 30k = 11 + 30(4 + 7\ell)$

$x = 131 + 210\ell$

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

แบบฝึกหัด 4.5

ข้อ 1. - 7. จงหาคำตอบของระบบคอนกรูเอนซ์ที่เป็นจำนวนเต็มบวกที่น้อยที่สุด หรือแสดงว่าไม่มีรากที่เป็นจำนวนเต็มอยู่เลย

1. $x \equiv 3 \pmod 9$, $x \equiv 1 \pmod 8$
2. $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$
3. $x \equiv 1 \pmod 5$, $x \equiv 4 \pmod 7$
4. $x \equiv 5 \pmod 7$, $x \equiv 8 \pmod{19}$
5. $x \equiv 2 \pmod 2$, $x \equiv 5 \pmod{19}$
6. $x \equiv 7 \pmod 9$, $x \equiv 13 \pmod{23}$, $x \equiv 1 \pmod 2$
7. $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$
   $x \equiv 5 \pmod 7$, $x \equiv 2 \pmod 9$
8. จงหาจำนวนเต็มบวกที่น้อยที่สุดซึ่งเมื่อหารด้วย 3 เหลือเศษ 2 เมื่อหารด้วย 5 เหลือเศษ 3 และเมื่อหารด้วย 7 เหลือเศษ 2
9. จงหาจำนวนเต็มบวกที่น้อยที่สุด ซึ่งเมื่อหารด้วย 2, 3, 4 และ 5 แล้วเหลือเศษ 1, 2, 3 และ 4 ตามลำดับ
10. ตะกร้าใบหนึ่งใส่ไข่ไว้เต็มซึ่งไม่ทราบว่ามีกี่ฟอง แต่ถ้าหยิบไข่ออกครั้งละ 2 ฟองจะเหลือเศษ 1 ฟอง ถ้าหยิบไข่ออกครั้งละ 3 ฟอง, 4 ฟอง, 5 ฟอง และ 6 ฟอง จะเหลือเศษ 2 ฟอง, 3 ฟอง, 4 ฟอง และ 5 ฟองตามลำดับ ถ้าหยิบออกครั้งละ 7 ฟอง จะไม่มีไข่เหลืออยู่เลย จงหาว่ามีไข่อยู่อย่างน้อยกี่ฟองในตะกร้า
11. จงพิสูจน์บทแทรก 4.2

4.6 รีดิวซ์ เรซิดิว ซิสเท็ม และออยเลอร์ไฟ ฟังก์ชัน
(Reduced Residue System and Euler Phi Eunction)

นิยาม 4.3 ให้ a เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก แล้วจะต้องมีจำนวนเต็ม q และ r ซึ่งทำให้

$$a = mq + r \quad \text{เมื่อ } 0 \leqslant r < m$$

แล้วเราจะเรียก r ว่าเป็น "ลีส เรซิดิว (least residue) ของ a มอดุโล m"

โดยทั่วไป ถ้า $a \equiv b \pmod m$ เราเรียก b ว่าเรซิดิวของ a มอดุโล m

ตัวอย่าง 4.14 ให้ $a = 17, m = 5$

$$17 = 5 \cdot 3 + 2 \qquad 0 < 2 < 5$$

ดังนั้น 2 เป็นลีสเรซิดิวของ 17 มอดุโล 5

ทฤษฎี 4.14 ให้ m เป็นจำนวนเต็มบวก $a \equiv b \pmod m$ ก็ต่อเมื่อ a และ b มีลีสเรซิดิว มอดุโล m เป็นค่าเดียวกัน

พิสูจน์ ให้ r_1 เป็นลีสเรซิดิวของ a มอดุโล m

และ r_2 เป็นลีสเรซิดิวของ b มอดุโล m

เพราะฉะนั้นจะต้องมีจำนวนเต็ม q_1 และ q_2 ซึ่งทำให้

$a = mq_1 + r_1$ และ $b = mq_2 + r_2$

เมื่อ $0 \leqslant r_1 < m$ และ $0 \leqslant r_2 < m$

ถ้า $a \equiv b \pmod m$ แล้ว

$$r_1 + mq_1 \equiv r_2 + mq_2 \pmod m$$

เพราะฉะนั้น $m | r_1 - r_2$

แต่ $0 \leqslant r_1 < m$ และ $-m < -r_2 \leqslant 0$

ดังนั้น $-m < r_1 - r_2 < m$

นั่นคือ $|r_1 - r_2| < m$

แต่ $m | (r_1 - r_2)$

เพราะฉะนั้น $r_1 - r_2 = 0$

นั่นคือ $r_1 = r_2$ แสดงว่า a และ b มีลีสเรซิดิว มอดุโล m เป็นค่าเดียวกัน

ในทางกลับกัน ถ้า a และ b มีลีสเรซิดิว เดียวกันคือ r

เพราะฉะนั้น $a \equiv r \pmod m$

และ $b \equiv r \pmod m$

ดังนั้นตามทฤษฎี 4.1 $a \equiv b \pmod m$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.15 จงหาลีสเรซิดิวของ 5^{296} มอดุโล 7

วิธีทำ การที่เราจะหาค่าของ 5^{296} แล้วหารด้วย 7 เพื่อจะหาลีส เรซิดิว เหมือนตัวอย่างที่แล้วนั้น เราหาได้ยาก แต่เรายังมีวิธีที่จะหาได้โดยไม่ต้องคำนวณ คือการใช้คอนกรูเอนซ์

$$5^3 = 125 \equiv -1 \pmod 7$$
$$5^6 = (5^3)^2 \equiv (-1)^2 \equiv 1 \pmod 7$$
$$296 = 6 \cdot 49 + 2$$
$$5^{296} = 5^{6 \cdot 49+2} = (5^6)^{49} \cdot 5^2 \equiv (1)^{49} \cdot 5^2$$
$$\equiv 25 \equiv 4 \pmod 7$$

นั่นคือลีสเรซิดิวของ 5^{296} มอดุโล 7 คือ 4

ตัวอย่าง 4.16 จงแสดงว่า $83|(3^{41}-1)$

วิธีทำ เนื่องจากว่า $3^{41} - 1$ เป็นจำนวนที่มีค่ามาก เราอาจจะหาค่าได้ถ้าใช้ความพยายาม และมีความละเอียดถี่ถ้วนพอ ซึ่งจะหาได้ดังนี้

$3^{41} - 1 \equiv 36472996377170786402$

ถ้านำ 83 ไปหารจำนวนนี้จะได้ผลลัพธ์เป็น 4394336912912194 และเศษเป็นศูนย์ แสดงว่า 83 หารลงตัว

แต่กว่าจะได้ผลลัพธ์ออกมาก็ต้องใช้เวลามากและยังไม่แน่ใจว่าการคูณและการหารของเราถูกต้องหรือไม่ ซึ่งวิธีการที่จะแสดงให้เห็นได้โดยง่าย และแน่ใจว่าไม่ผิดพลาด คือใช้คอนกรูเอนซ์เข้ามาช่วยเพื่อหาลีสเรซิดิวของ $3^{41} - 1$ มอดุโล 83

$3^4 \equiv 81 \equiv -2 \pmod{83}$

$3^8 \equiv (3^4)^2 \equiv (-2)^4 \equiv 4 \pmod{83}$

$3^{32} \equiv (3^8)^4 \equiv (4)^4 \equiv 256 \equiv 7 \pmod{83}$

$3^{40} \equiv 3^{32} \cdot 3^8 \equiv 7 \cdot 4 \equiv 28 \pmod{83}$

$3^{41} \equiv 3^{40} \cdot 3 \equiv 28 \cdot 3 \equiv 84 \equiv 1 \pmod{83}$

$3^{41} - 1 \equiv 0 \pmod{83}$

แสดงว่า $83|3^{41} - 1$

นิยาม 4.4 ให้ m เป็นจำนวนเต็มบวก แล้วเซ็ต $\{ 0, 1, 2, \ldots, (m - 1) \}$ เรียกว่า "ลีส เรซิดิว ซิสเท็ม" มอดุโล m และเขียนแทนเซ็ตนี้ด้วย Z_m

เซ็ตของจำนวนเต็มใด ๆ m ตัวซึ่งไม่มีคู่ใดเลย คอนกรูเอนซ์กัน มอดุโล m แล้วเรียกเซ็ตนี้ว่า "คอมพลีท เรซิดิว ซิสเท็ม" มอดุโล m (complete residue system)

ข้อสังเกต ลีส เรซิดิว ซิสเท็ม ก็คือคอมพลีท เรซิดิว ซิสเท็ม และคอมพลีท เรซิดิว ซิสเท็ม ก็คือเซ็ตที่ประกอบด้วยสมาชิกในแต่ละชั้นเรซิดิว มอดุโล m ชั้นละ 1 ตัวเท่านั้น

ตัวอย่าง 4.17 $Z_1 = \{ 0 \}$

$Z_2 = \{ 0, 1 \}$

$Z_3 = \{ 0, 1, 2 \}$

$Z_4 = \{ 0, 1, 2, 3 \}$

$Z_5 = \{ 0, 1, 2, 3, 4 \}$

$Z_6 = \{ 0, 1, 2, 3, 4, 5 \}$

$Z_7 = \{ 0, 1, 2, 3, 4, 5, 6 \}$

ทั้งหมดนี้ต่างก็เป็นลีส เรซิดิว ซิสเท็ม มอดุโลต่าง ๆ กัน

ตัวอย่าง 4.18 ให้ $m = 7$ เพราะว่า 1 อยู่ใน R_1, 16 อยู่ใน R_2, -11 อยู่ใน R_3, 55 อยู่ใน R_4, -44 อยู่ใน R_5, 69 อยู่ใน R_6 และ -77 อยู่ใน R_7

ดังนั้น $\{ 1, 16, -11, 55, -44, 69, -77 \}$ เป็นคอมพลีท เรซิดิว ซิสเท็ม มอดุโล 7

ทฤษฎี 4.15 ให้ m เป็นจำนวนเต็มบวก ถ้า $a \equiv b \pmod{m}$ แล้ว

$$(a, m) = (b, m)$$

พิสูจน์ การพิสูจน์ให้ผู้อ่านทำเป็นแบบฝึกหัด

นิยาม 4.5 ให้ m เป็นจำนวนเต็มบวก $\phi(m)$ ก็คือจำนวนชั้นเรซิดิว มอดูโล m ที่เป็นรีเลทีบลีไพรม์กับ m หรือจำนวนของจำนวนเต็มบวกที่ไม่เกิน m และเป็นรีเลทีบลีไพรม์กับ m เรียก $\phi(m)$ ว่า ออยเลอร์ ไฟ ฟังก์ชัน (Euler Phi Function)

นิยาม 4.6 ให้ m เป็นจำนวนเต็มบวก แล้วเซ็ต $\{ a : a \in Z^+, a \leqslant m, (a, m) = 1 \}$ เรียกว่า "ลีส รีดิวซ์ เรซิดิว ซิสเท็ม" มอดุโล m (least reduced residue system) และจะเขียนแทนเซ็ตนี้ด้วย Z_m^* และให้ $\phi(m)$ แทนจำนวนสมาชิกใน Z_m^* เซ็ตของจำนวนเต็มบวกที่เป็นรีเลทีบลีไพรม์กับ m ทั้งหมด $\phi(m)$ จำนวนและไม่มีคู่ใดคอนกรูเอนซ์มอดุโล m กันเลย เรียกเซ็ตนี้ว่า "คอมพลีท รีดิวซ์ เรซิดิว ซิสเท็ม" (Complete reduced residue system) มอดุโล m

ตัวอย่าง 4.19 $Z_1^* = \{ 1 \}$

$Z_2^* = \{ 1 \}$

$Z_3^* = \{ 1, 2 \}$

$Z_4^* = \{ 1, 3 \}$

$Z_5 = \{ 1, 2, 3, 4 \}$

$Z_6^* = \{ 1, 5 \}$

$Z_7^* = \{ 1, 2, 3, 4, 5, 6 \}$

$Z_8^* = \{ 1, 3, 5, 7 \}$

$Z_9^* = \{ 1, 2, 4, 5, 7, 8 \}$

$Z_{10}^* = \{ 1, 3, 7, 9 \}$

จะพบว่า ถ้า $m > n$ แล้ว $\phi(m)$ ไม่จำเป็นจะต้องมากกว่า $\phi(n)$

เช่น $\phi(10) = 4 < 6 = \phi(9)$

$\phi(8) = 4$ และ $\{ 1, 3, 5, 7 \}$ เรียกว่าลีส รีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล 8

ส่วน $\{ 9, -5, 21, 7 \}$ เรียกว่าคอมพลีท รีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล 8

สำหรับ $m > 1$ แล้ว $Z_m^* \in Z_m$

ในกรณีที่เราต้องการหาค่าของ $\phi(m)$ เราไม่จำเป็นจะต้องเขียนเซ็ต Z^*_m ก็ได้เพราะถ้าเป็นกรณีที่ m มีค่ามาก ๆ การเขียน Z_m^* ก็ไม่สะดวก ซึ่งทฤษฎีต่อไปนี้จะช่วยให้เราหาค่าของ $\phi(m)$ ได้โดยง่าย

ทฤษฎี 4.16 ให้ a, b, n เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะบวก แล้ว

1. $\phi(p) = p - 1$
2. $\phi(p^{n+1}) = p^n\phi(p)$
3. ถ้า $(a, b) = 1$ แล้ว $\phi(ab) = \phi(a) \cdot \phi(b)$

พิสูจน์ 1. เพราะว่า p เป็นจำนวนเฉพาะบวกดังนั้น

$Z_p^* = \{ 1, 2, 3, \ldots, (p - 1) \}$ แสดงว่า

$\phi(p) = p - 1$

2. เลขจำนวนเต็มบวกที่มีค่าน้อยกว่าหรือเท่ากับ p^{n+1} ซึ่ง ห.ร.ม. ระหว่างเลขนั้น กับ p^{n+1} ไม่เท่ากับ 1 ก็คือจำนวนที่เป็นพหุคูณของ p มีดังนี้คือ

$1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p \cdot p, \ldots, p^2 \cdot p, \ldots, (p^n - 1) \cdot p, p^n \cdot p$ ซึ่งมีทั้งหมด p^n จำนวน

ซึ่งจำนวนเต็มบวกซึ่งน้อยกว่าหรือเท่ากับ p^{n+1} มีทั้งสิ้น p^{n+1} จำนวน

ดังนั้น $\phi(p^{n+1}) = p^{n+1} - p^n$

$= p^n(p - 1)$

$= p^n\phi(p)$

3. จะแสดงว่าถ้า (a, b) = 1 แล้ว $\phi(ab) = \phi(a)\phi(b)$

ให้ $\phi(a) = j$ และให้ $\{ r_1, r_2,\ldots,r_j \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล **a**

ให้ $\phi(b) = k$ และให้ $\{ s_1, s_2,\ldots,s_k \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล **b**

ถ้า x อยู่ในรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล ab แล้ว (x, ab) = 1

และจากทฤษฎี 2.12 (x, a) = 1 = (x, b)

ดังนั้น $x \equiv r_h \pmod a$ และ $x \equiv s_i \pmod b$

สำหรับ h, i บางตัว

ในทางกลับกัน ถ้า $x \equiv r_h \pmod a$ และ $x \equiv s_i \pmod b$ แล้ว (x, ab) = 1

ดังนั้นรีดิวซ์ เรซิดิว ซิสเต็ม มอดุโล ab ก็คือเซ็ตของ x ทั้งหมด ซึ่ง $x \equiv r_h \pmod a$

และ $x \equiv s_i \pmod b$

สำหรับ h, i บางตัว

จากทฤษฎี 4.12 สำหรับแต่ละคู่ของ h, i จะให้ค่า x เพียงค่าเดียวใน มอดุโล ab

สำหรับ h, i แต่ละคู่ที่แตกต่างกันก็จะได้ค่า x มอดูโล ab แตกต่างกัน

ซึ่งมีทั้งหมด jk คู่

ดังนั้นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล ab จะมีสมาชิก jk ตัว

แสดงว่า $\phi(ab) = \phi(a) \cdot \phi(b)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.20 $\phi(16) = \phi(2^4) = 2^3\phi(2) = 8 \cdot 1 = 8$

$\phi(15) = \phi(3 \cdot 5) = \phi(3)\phi(5) = 2 \cdot 4 = 8$

$4 = \phi(12) \neq \phi(6) \cdot \phi(2) = 2 \cdot 1 = 2$

เพราะ $(6, 2) \neq 1$

$\phi(16) = \phi(4^2) \neq 4\phi(4)$ เพราะ 4 ไม่ใช่จำนวนเฉพาะ

หรือ $\phi(6) \neq 5$ เพราะ 6 ไม่ใช่จำนวนเฉพาะ

ข้อสังเกต ในการหาค่า $\phi(m)$ โดยใช้ทฤษฎี 4.16 จะต้องพิจารณาให้ดี ต้องแน่ใจว่าการหานั้นสอดคล้องตามเงื่อนไขของทฤษฎี ดังตัวอย่างที่กล่าวแล้ว

ทฤษฎี 4.17 ถ้า $\{ a_1, a_2,\ldots,a_{\phi(m)} \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m และ (k, m) = 1 แล้ว $\{ ka_1, ka_2,\ldots,ka_{\phi(m)} \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m ด้วย

พิสูจน์ เพราะว่าจำนวนสมาชิกในเซ็ต $\{ ka_1, ka_2,\ldots,ka_{\phi(m)} \}$ มีเท่ากับ $\phi(m)$ แล้วเหลือเพียงแสดงว่าสมาชิกในเซ็ตไม่มีคู่ใดคอนกรูเอนซ์กัน มอดุโล m และสมาชิกแต่ละจำนวนเป็นรีเลทีบลีไพรม์กับ m

เพราะว่า $\{ a_1, a_2,\ldots,a_{\phi(m)} \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m

เพราะฉะนั้น $(a_i, m) = 1$ สำหรับ $i = 1, 2,\ldots,\phi(m)$

และ $a_i \not\equiv a_j \pmod m$ ถ้า $i \neq j$

1. เพราะ $(a_i, m) = 1$ สำหรับ $i = 1, 2,\ldots,\phi(m)$

   และ $(k, m) = 1$ จากที่กำหนดให้

   ดังนั้นจากทฤษฎี 2.12 $(ka_i, m) = 1$ สำหรับ $i = 1, 2,\ldots,\phi(m)$

2. สมมุติว่า $ka_i \equiv ka_j \pmod m$ เมื่อ $i \neq j$

   แต่ $(k, m) = 1$

   เพราะฉะนั้นตามบทแทรก 4.1

   $$a_i \equiv a_j \pmod m$$ ซึ่งเป็นไปไม่ได้

   ดังนั้น $ka_i \not\equiv ka_j \pmod m$ ถ้า $i \neq j$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.18 (The Euler - Fermat Theorem)

ถ้า $(b, m) = 1$ แล้ว $b^{\phi(m)} \equiv 1 \pmod m$

พิสูจน์ จากทฤษฎี 4.17 จะได้ว่าถ้า $\{ a_1, a_2,\ldots,a_{\phi(m)} \}$ เป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m และ $(b, m) = 1$ แล้ว $\{ ba_1, ba_2,\ldots,ba_{\phi(m)} \}$ เป็นรีดิวซ์เรซิดิว ซิสเท็ม มอดุโล m

แสดงว่าสำหรับ ba_j แต่ละตัวใน $\{ ba_1, ba_2,\ldots,ba_{\phi(m)} \}$

จะต้องมี a_k บางตัวใน $\{ a_1, a_2,\ldots,a_{\phi(m)} \}$ ซึ่งทำให้

$$ba_j \equiv a_k \pmod m$$

เพราะฉะนั้น $$\prod_{j=1}^{\phi(m)} ba_j \equiv \prod_{k=1}^{\phi(m)} a_k \pmod m$$

$$b^{\phi(m)} \prod_{j=1}^{\phi(m)} a_j \equiv \prod_{k=1}^{\phi(m)} a_k \pmod m$$

เพราะว่า $(a_i, m) = 1$ สำหรับ $i = 1, 2,\ldots,\phi(m)$

เพราะฉะนั้น $\left(\prod_{i=1}^{\phi(m)} a_i, m \right) = 1$

ดังนั้นจากบทแทรก 4.1 จะได้ว่า

$$b^{\phi(m)} \equiv 1 \pmod m$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.21 ให้ $m = 10$ แล้ว $Z_{10}^{*} = \{ 1, 3, 7, 9 \}$

$\phi(10) = 4$

ถ้า $b = 3$

แล้ว $3^4 \equiv 81 \equiv 1 \pmod{10}$

หรือ $b = 7$

$7^4 \equiv 2401 \equiv 1 \pmod{10}$

แต่ถ้าให้ $b = 2$

$2^4 \equiv 16 \equiv 6 \not\equiv 1 \pmod{10}$ เพราะอะไร

เพราะว่า $(2, 10) = 2 \neq 1$ จึงไม่เป็นตามทฤษฎี

ทฤษฎี 4.19 **(Fermat's Theorem)**

ถ้า p เป็นจำนวนเฉพาะแล้ว $a^p \equiv a \pmod{p}$ สำหรับ a เป็นจำนวนเต็ม

พิสูจน์ ถ้า $p \nmid a$ แล้ว $a^{p-1} \equiv 1 \pmod{p}$ ตามทฤษฎี 4.18

ดังนั้นตามทฤษฎี 4.5 ข้อ 1 จะได้ว่า

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

ถ้า $p|a$ แล้ว $a \equiv 0 \pmod{p}$ และตามทฤษฎี 4.5 ข้อ 2

$a^p \equiv 0 \pmod{p}$

ดังนั้นตามทฤษฎี 4.1 ข้อ 3

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

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

จากทฤษฎี Euler-Fermat เราสามารถนำไปช่วยหาลีส เรซิดิว ของจำนวนทีมีค่ามาก ๆ ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.22 จงหาลีสเรซิดิวของ 7^{1015} มอดุโล 31

วิธีทำ เพราะว่า $\phi(31) = 30$ และ $(7, 31) = 1$

ดังนั้นจากทฤษฎี 4.18

$7^{30} \equiv 1 \pmod{31}$

แต่ $1015 = 30 \cdot 33 + 25$

$7^{1015} \equiv 7^{30 \cdot 33+25} \equiv 1^{33} \cdot 7^{25} \equiv 7^{25} \pmod{31}$

$7^2 \equiv 49 \equiv -13 \pmod{31}$

$7^4 \equiv 169 \equiv 14 \pmod{31}$

$7^8 \equiv 196 \equiv 10 \pmod{31}$

$7^{16} \equiv 100 \equiv 7 \pmod{31}$

$7^{25} \equiv 7 \cdot 7^8 \cdot 7^{16} \equiv 7 \cdot 10 \cdot 7 \equiv 490 \equiv 25 \pmod{31}$

แสดงว่า $7^{1015} \equiv 25 \pmod{31}$

นั่นคือลีส เรซิดิว มอดูโล 31 ของ 7^{1015} คือ 25

แบบฝึกหัด 4.6

1. จงหาเซ็ตของ Z_{14}^*, Z_{15}^*, Z_{16}^*
2. จงแสดงว่า -30, -19, -15, -4, 15 และ 39 อยู่ในรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล 7
3. จงแสดงว่า 3, 3^2, 3^3, 3^4, 3^5, 3^6 อยู่ในรีดิวซ์ เรซิดิว ซิสเท็มมอดุโล 7
4. จำนวนไหนที่ 61 หารลงตัว $2^{30}-1$ และ $2^{30}+1$
5. จำนวนไหนที่ 61 หารลงตัว $3^{30}-1$ และ $3^{30}+1$
6. จำนวนไหนที่ 61 หารลงตัว $6^{30}-1$ และ $6^{30}+1$
7. จำนวนใดต่อไปนี้ที่ 13 หารลงตัว

   2^4-1 2^4-3 2^4-3^2

   5^4-1 5^4-3 5^4-3^2

   7^4-1 7^4-3 7^4-3^2
8. จงหาลีส เรซิดิวของ 3^{1000} มอดูโล 7
9. จงหาค่าของ $\phi(221)$, $\phi(441)$, $\phi(873)$

   $\phi(9702)$, $\phi(7^2 \cdot 13^4 \cdot 19)$
10. จงพิสูจน์ทฤษฎี 4.15
11. ถ้า p เป็นจำนวนเฉพาะแล้วจงพิสูจน์ว่า $(a \pm b)^p \equiv a^p \pm b^p \pmod p$
12. จงพิสูจน์ว่า $a^5 \equiv a \pmod{15}$ และ $a^{21} \equiv a \pmod{15}$

4.7 โพลิโนเมียล คอนกรูเอนซ์ (Polynomial Congruences)

เราจะใช้ f(x) แทนโพลิโนเมียล ซึ่งมีดีกรี $n \geq 2$ และสัมประสิทธิ์เป็นจำนวนเต็ม ในหัวข้อนี้จะกล่าวถึงการหาคำตอบของโพลิโนเมียล คอนกรูเอนซ์ $f(x) \equiv 0 \pmod{m}$ ว่าจะมีคำตอบได้กี่คำตอบ ซึ่งในตอนแรกนี้ เรายังไม่มีวิธีการอื่นใด นอกจากวิธีการแทนค่า เช่น ถ้าเราให้ $x = a$ แล้ว แทนใน f(x) ทำให้ $f(a) \equiv 0 \pmod{m}$ แล้วเรากล่าวว่า a เป็นคำตอบหนึ่งและจำนวนเต็มใดก็ตามที่คอนกรูเอนซ์กับ a มอดุโล m ก็จะเป็นคำตอบของ $f(x) \equiv 0 \pmod{m}$ ด้วย แต่เราถือว่าเป็นคำตอบเดียวกัน ปัญหาของเราตอนนี้ก็คือต้องหาคำตอบซึ่งไม่คอนกรูเอนซ์กัน มอดุโล m

ตัวอย่าง 4.23 จงหาคำตอบของคอนกรูเอนซ์

$$f(x) = x^2 + 1 \equiv 0 \pmod{5}$$

วิธีทำ แทนค่าx ด้วย 0, 1, 2, 3 และ 4 ใน f(x) ได้ดังนี้

$$\left.\begin{aligned} f(0) &= 1 \equiv 1 \\ f(1) &= 2 \equiv 2 \\ f(2) &= 5 \equiv 0 \\ f(3) &= 10 \equiv 0 \\ f(4) &= 17 \equiv 2 \end{aligned}\right\} \pmod{5}$$

ดังนั้น $x = 2$ และ $x = 3$ เป็นคำตอบของคอนกรูเอนซ์นี้

ตัวอย่าง 4.24 จงหาคำตอบของคอนกรูเอนซ์ $x^2 + 1 \equiv 0 \pmod{3}$

วิธีทำ แทนค่า x ด้วย 0, 1, 2 ปรากฏว่า

$$\left.\begin{aligned} f(0) &= 1 \equiv 1 \\ f(1) &= 2 \equiv 2 \\ f(2) &= 5 \equiv 2 \end{aligned}\right\} \pmod{3}$$

ดังนั้นคอนกรูเอนซ์นี้ไม่มีคำตอบ

ทฤษฎี 4.20 (Lagrange's Theorem)

ให้ p เป็นจำนวนเฉพาะ และ f(x) เป็นโพลิโนเมียลดีกรี n ซึ่งมีสัมประสิทธิ์เป็นจำนวนเต็ม และ $a_n \not\equiv 0 \pmod{p}$ แล้ว $f(x) \equiv 0 \pmod{p}$ จะมีคำตอบไม่เกิน n คำตอบที่ไม่คอนกรูเอนซ์กัน มอดุโล p

พิสูจน์ ให้ $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

ถ้า $n = 1$ เราจะได้ $f(x) = a_1 x + a_0$ ซึ่ง $a_1 \not\equiv 0 \pmod p$

ดังนั้น $f(x) \equiv 0 \pmod p$ จะมีคำตอบหนึ่งคำตอบตามทฤษฎี 4.10

สมมุติว่าทฤษฎีนี้เป็นจริง สำหรับทุก n ซึ่ง $1 \leqslant n < k$ (A)

พิจารณา $f(x) = a_k x^k + \ldots + a_1 x + a_0$ ซึ่ง $a_k \not\equiv 0 \pmod p$

ถ้า $f(x) \equiv 0 \pmod p$ มีคำตอบเพียง 1 คำตอบหรือไม่มีเลย แล้วทฤษฎีนี้เป็นจริง

แต่ถ้า $f(x) \equiv 0 \pmod p$ มีคำตอบอย่างน้อยสองคำตอบที่ไม่คอนกรูเอนซ์กัน มอดุโล p

สมมุติคำตอบนั้นคือ b และ c

ดังนั้น $f(b) \equiv 0 \pmod p$ หรือ $p \mid f(b)$

จากทฤษฎีเศษ (Remainder Theorem) เราจะได้

$$g(x) = \frac{f(x) - f(b)}{x - b}$$

เป็นโพลิโนเมียลดีกรี $(k - 1)$ ซึ่งสัมประสิทธิ์เป็นจำนวนเต็ม

ดังนั้น $f(x) = (x - b)\, g(x) + f(b)$

$f(x) \equiv (x - b)g(x) + f(b) \pmod p$

ดังนั้นจะได้ $f(x) \equiv (x - b)g(x) \pmod p$

เพราะว่า c เป็นอีกคำตอบหนึ่งของ $f(x) \equiv 0 \pmod p$

ซึ่ง $c \not\equiv b \pmod p$ ดังนั้น $f(c) \equiv 0 \pmod p$

แล้ว $0 \equiv f(c) \equiv (c - b)g(c) \pmod p$

เนื่องจาก $(c - b)g(c) \equiv 0 \pmod p$ และ $c \not\equiv b \pmod p$

แล้ว $g(c) \equiv 0 \pmod p$ และดีกรีของ $g(x)$ คือ $n = k - 1 < k$

ดังนั้นถ้า $f(x) \equiv 0 \pmod p$ มีคำตอบอย่างน้อยที่สุด $k + 1$ คำตอบ

แล้ว $g(x) \equiv 0 \pmod p$ จะต้องมีคำตอบอย่างน้อย k คำตอบ เมื่อดีกรีของ $g(x)$

เท่ากับ $k - 1$ ซึ่งขัดแย้งกับที่สมมุติไว้ (A)

เพราะฉะนั้น $f(x) \equiv 0 \pmod p$ จะมีคำตอบไม่เกิน k

ดังนั้นทฤษฎีนี้เป็นจริงสำหรับ $n = k$ และสำหรับทุกค่าของ n ซึ่งเป็นจำนวนเต็ม

ตัวอย่าง 4.25 จงหาคำตอบของ $x^2+3x+2 \equiv 0 \pmod 7$

วิธีทำ แยกตัวประกอบได้ $x^2+3x+2 = (x+2)(x+1) \equiv 0 \pmod 7$

ดังนั้น $(x+2) \equiv 0 \pmod 7$ หรือ $(x+1) \equiv 0 \pmod 7$

จะได้ $x \equiv -2 \equiv 5 \pmod 7$ และ $x \equiv -1 \equiv 6 \pmod 7$

แสดงว่าเป็นจริงตามทฤษฎีคือมีคำตอบไม่เกิน 2 คำตอบ

ตัวอย่าง 4.26 ถ้าเอคุลัสไม่ใช่จำนวนเฉพาะเราอาจจะหาคำตอบได้มากกว่าดีกรีของโพลิโนเมียล เช่น $x^2 - 1 \equiv 0 \pmod 8$

จะได้ $x \equiv 1 \pmod 8$ $x \equiv 3 \pmod 8$

$x \equiv 5 \pmod 8$ $x \equiv 7 \pmod 8$

จะเห็นว่าได้คำตอบถึง 4 คำตอบในขณะที่ดีกรีของโพลิโนเมียลเป็น 2

ทฤษฎี 4.21 ให้ $m = \prod_{i=1}^{n} m_i$ ซึ่ง $(m_i, m_j) = 1$ เมื่อ $i \neq j$ แล้ว a จะเป็นคำตอบของ $f(x) \equiv 0 \pmod m$ ก็ต่อเมื่อ a เป็นคำตอบของระบบคอนกรูเอนซ์

$$f(x) \equiv 0 \pmod{m_1}$$
$$f(x) \equiv 0 \pmod{m_2}$$
$$\cdots$$
$$f(x) \equiv 0 \pmod{m_n}$$

พิสูจน์ ถ้า a เป็นคำตอบของ $f(x) \equiv 0 \pmod m$ แล้ว $f(a) \equiv 0 \pmod m$

แต่ $m = \prod_{i=1}^{n} m_i$ ดังนั้น ถ้า $m \mid f(a)$ แล้ว $m_i \mid f(a)$

สำหรับแต่ละ $i = 1, 2, \ldots, n$

นั่นคือ $f(a) \equiv 0 \pmod{m_i}$

แสดงว่า a เป็นคำตอบของ ระบบคอนกรูเอนซ์

$f(x) \equiv 0 \pmod{m_i}$

ในทางกลับกันสมมุติ a เป็นคำตอบของระบบคอนกรูเอนซ์

$f(x) \equiv 0 \pmod{m_i}$ สำหรับ $i = 1, 2, \ldots, n$

แล้ว f(a) เป็นคำตอบของระบบคอนกรูเอนซ์

$$y \equiv 0 \pmod{m_1}$$
$$y \equiv 0 \pmod{m_2}$$
$$\cdots$$
$$y \equiv 0 \pmod{m_n}$$

และตามทฤษฎี Chinese Remainder จะได้ $f(a) \equiv 0 \pmod{m}$

ดังนั้น a เป็นคำตอบของ $f(x) \equiv 0 \pmod{m}$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.27 จงหาคำตอบของ $f(x) \equiv 0 \pmod{165}$ เมื่อ $f(x) = x^5 - 3x^4 + 7x^3 - 2x^2 - 9x + 6$

วิธีทำ เพราะว่า $165 = 11 \cdot 5 \cdot 3$

ดังนั้นเราต้องหาคำตอบทั้งหมดของ $f(x) \equiv 0 \pmod{11}$

$f(x) \equiv 0 \pmod{5}$ และ $f(x) \equiv 0 \pmod{3}$

โดยวิธีการแทนค่า $x = 0, 1, 2, \ldots, 10$ เราได้

$x \equiv 1$ $x \equiv 6$ และ $x \equiv 8 \pmod{11}$

ในทำนองเดียวกันคำตอบสำหรับ $f(x) \equiv 0 \pmod{5}$

คือ $x \equiv 1$ $x \equiv 2$ และ $x \equiv 3 \pmod{5}$

และคำตอบของ $f(x) \equiv 0 \pmod{3}$ คือ

$x \equiv 0$ และ $x \equiv 1 \pmod{3}$

จากคำตอบทั้งหมดนี้ เราสามารถจัดระบบคอนกรูเอนซ์เชิงเส้น มอดูโล ทั้ง 3 คือ 11, 5 และ 3 ได้ทั้งหมด 18 ระบบ

ดังนั้นก็จะได้คำตอบ 18 คำตอบ ต่อไปเป็นตัวอย่างจากระบบที่จัดได้

$$\left\{\begin{array}{l} x \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{3} \end{array}\right\} \quad \text{และ} \quad \left\{\begin{array}{l} x \equiv 8 \pmod{11} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3} \end{array}\right\}$$

จากทั้ง 2 ระบบคอนกรูเอนซ์นี้เราหาคำตอบตามที่เคยทำมาแล้วในหัวข้อ 4.5 จะได้

$x \equiv 111 \pmod{165}$ และ $x \equiv 52 \pmod{165}$

ส่วนคำตอบอื่น ๆ จากอีก 16 ระบบคอนกรูเอนซ์ให้ไว้เป็นแบบฝึกหัด

แบบฝึกหัด 4.7

1. จงหาคำตอบที่เหลือในตัวอย่าง 4.27
2. จงหาคำตอบของ $x^3 - 2x^2 - 5x + 10 \equiv 0 \pmod{17}$
3. จงหาคำตอบของ $x^2 + x + 1 \equiv 0 \pmod{11}$
4. จงหาคำตอบของ $x^5 - x \equiv 0 \pmod{5}$
5. จงหาคำตอบของ $x^2 - 11 \equiv 0 \pmod{23}$
6. จงหาคำตอบของ $x^2 + 11 \equiv 0 \pmod{23}$
7. จงหาคำตอบของ $2x^3 - 25x^2 + 9x + 1 \equiv 0 \pmod{715}$
8. จงหาคำตอบของ $x^2 + 3x + 2 \equiv 0 \pmod{385}$

4.8 เอกซ์โพเนนท์ และรากปฐมฐาน(Exponents and Primitive Roots)

ให้ m เป็นจำนวนเต็มบวก และ b เป็นจำนวนเต็ม ซึ่ง (b, m) = 1 แล้ว เราทราบว่า $\phi(m)$ เป็นคำตอบหนึ่งของคอนกรูเอนซ์ $b^x \equiv 1 \pmod{m}$ เพราะจากทฤษฎีออยเลอร์-เฟอร์แมท $b^{\phi(m)} \equiv 1 \pmod{m}$ ดังนั้นคอนกรูเอนซ์นี้จะต้องมีคำตอบ ซึ่งเป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุด นั่นคือถ้า k เป็นคำตอบดังกล่าวแล้ว k ต้องเป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่งทำให้ $b^k \equiv 1 \pmod{m}$

นิยาม 4.7 ถ้า k_0 เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่งทำให้ $b^k \equiv 1 \pmod{m}$ แล้วเราเรียก k ว่าเป็นออเดอร์ (order) ของ b มอดุโล m และเรียกว่า b เป็นของเอกซ์โพเนนท์ (belong to exponent) k มอดุโล m

จะใช้ $\text{ord}_m(b) = k$ แทนออเดอร์ของ b มอดุโล m

หมายเหตุ นิยามนี้จะไม่มีความหมาย นอกจาก (b, m) = 1 ดังนั้นเมื่อเรากล่าวว่า ออเดอร์ของ b มอดุโล m เท่ากับ k เราหมายถึง (b, m) = 1 ด้วย

ตัวอย่าง 4.28 สำหรับ m = 7, b = 2 ถ้าเรายกกำลังของ 2 จะได้ดังนี้

$$2^1 \equiv 2 \pmod{7}$$
$$2^2 \equiv 4 \pmod{7}$$
$$2^3 \equiv 8 \equiv 1 \pmod{7}$$
$$2^4 \equiv 16 \equiv 2 \pmod{7}$$
$$2^5 \equiv 32 \equiv 4 \pmod{7}$$
$$2^6 \equiv 64 \equiv 1 \pmod{7}$$

จะเป็นอย่างนี้ไปเรื่อย ๆ ซึ่ง 3 เป็นจำนวนเต็มบวกที่น้อยที่สุด

ซึ่งทำให้ $2^3 \equiv 1 \pmod{7}$

ดังนั้น $\text{ord}_7(2) = 3$

ถ้าให้ m = 8, b = 3

$$3^1 \equiv 3 \pmod{8}$$
$$3^2 \equiv 9 \equiv 1 \pmod{8}$$

แสดงว่า 2 เป็นจำนวนเต็มบวกที่น้อยที่สุดซึ่งทำให้

$$3^2 \equiv 1 \pmod{8}$$

ดังนั้น $\text{ord}_8(3) = 2$

ถ้าให้ $m = 8$ และ $b = 4$

$$4^1 \equiv 4 \pmod 8$$

$$4^2 \equiv 16 \equiv 0 \pmod 8$$

$$4^3 \equiv 64 \equiv 0 \pmod 8$$

จะเป็นอย่างนี้ไปเรื่อย ๆ เพราะ $(4, 8) \neq 1$

จากตัวอย่างนี้ดูเหมือนว่าไม่มีวิธีที่จะหาออเดอร์ของจำนวนใด ๆ ได้ง่าย ๆ นอกจากวิธีทดลองยกกำลังของจำนวนนั้น ๆ แล้วดูว่าคอนกรูเอนซ์กับหนึ่งหรือไม่ แต่ทฤษฎีต่อไปนี้จะช่วยให้เราหาออเดอร์ของจำนวนเต็มได้ง่ายขึ้น

ทฤษฎี 4.22 ให้ m เป็นจำนวนเต็มบวก b เป็นจำนวนเต็ม ซึ่ง $(b, m) = 1$ แล้ว $b^n \equiv 1 \pmod m$ ก็ต่อเมื่อ $\text{ord}_m(b) | n$

พิสูจน์ ให้ $\text{ord}_m(b) = k$

สมมุติให้ $b^n \equiv 1 \pmod m$

ดังนั้นจะต้องมีจำนวนเต็ม q และ r ซึ่งทำให้

$$n = kq + r \quad 0 \leqslant r < k$$

เพราะฉะนั้น $1 \equiv b^n \equiv b^{kq+r} \equiv (b^k)^q \cdot b^r \equiv b^r \pmod m$

เพราะว่า $b^k \equiv 1 \pmod m$

แสดงว่า $b^r \equiv 1 \pmod m$ สำหรับ $0 \leqslant r < k$

แต่ k เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่ง $b^k \equiv 1 \pmod m$

ดังนั้น r ต้องเท่ากับศูนย์

นั่นคือ $n = kq$

แสดงว่า $k | n$ หรือ $\text{ord}_m(b) | n$

ในทางกลับกันสมมุติให้ $\text{ord}_m(b) | n$ หรือ $k | n$

เพราะฉะนั้นจะต้องมีจำนวนเต็ม q ซึ่งทำให้

$$n = kq$$

เพราะฉะนั้น $b^n \equiv b^{kq} \equiv (b^k)^q \equiv 1 \pmod m$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.23 ให้ m เป็นจำนวนเต็มบวก สำหรับ b เป็นจำนวนเต็มใด ๆ ซึ่ง $(b, m) = 1$ แล้ว $\text{ord}_m(b) | \phi(m)$

พิสูจน์ จากทฤษฎีออยเลอร์-เฟอร์แมท เราทราบว่า ถ้า (b, m) = 1

แล้ว $b^{\phi(m)} \equiv 1 \pmod{m}$

ดังนั้นจากทฤษฎี 4.22 $\text{ord}_m(b) | \phi(m)$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ตัวอย่าง 4.29 ให้ m = 13, b = 5

$\phi(13) = 12$ จำนวนที่หาร 12 ลงตัวคือ 1, 2, 3, 4, 6, 12

$5^1 \equiv 5 \pmod{13}$

$5^2 \equiv 25 \equiv -1 \pmod{13}$

$5^4 \equiv 1 \pmod{13}$

$\text{ord}_{13}(5) = 4$ และ $\text{ord}_{13}(5) | \phi(13)$

ถ้า m = 41, b = 3

$\phi(41) = 40$ จำนวนที่หาร 40 ลงตัวคือ 1, 2, 4, 5, 8, 10, 20, 40

$3^1 \equiv 3 \pmod{41}$

$3^2 \equiv 9 \pmod{41}$

$3^4 \equiv 81 \equiv -1 \pmod{41}$

$3^8 \equiv 1 \pmod{41}$

$\text{ord}_{41}(3) = 8$

ทฤษฎี 4.24 ให้ m เป็นจำนวนเต็มบวก และ $\text{ord}_m(b) = k$ แล้ว $b^c \equiv b^d \pmod{m}$ ก็ต่อเมื่อ $c \equiv d \pmod{k}$

พิสูจน์ เพราะว่า $\text{ord}_m(b) = k$

เพราะฉะนั้น $b^k \equiv 1 \pmod{m}$

สมมุติว่า $b^c \equiv b^d \pmod{m}$

ให้ $d \leqslant c$

เพราะว่า $\text{ord}_m(b) = k$ และ (b, m) = 1

ดังนั้น $(b^d, m) = 1$

เพราะฉะนั้น ตามบทแทรก 4.1

$b^{c-d} \equiv 1 \pmod{m}$ จาก $b^c \equiv b^d \pmod{m}$

ดังนั้นตามทฤษฎี 4.22

$$\text{ord}_m(b) | c - d \quad \text{หรือ} \quad k | c - d$$

นั่นคือ $c \equiv d \pmod{k}$

ในทางกลับกัน ถ้า $c \equiv d \pmod{k}$ แล้วจะมีจำนวนเต็ม q ซึ่งทำให้

$$c = d + kq$$

$$b^c = b^{d+kq} = b^d \cdot (b^k)^q \equiv b^d(1)^q \equiv b^d \pmod{m}$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.25 ถ้า k เป็นจำนวนเต็มบวก และ $\text{ord}_m(b) = hk$ แล้ว $\text{ord}_m(b^h) = k$

พิสูจน์ ถ้า $\text{ord}_m(b) = hk$ แล้วแสดงว่า

$$(b^h)^k \equiv 1 \pmod{m}$$

สมมุติว่า $\text{ord}_m(b^h) = i$

ดังนั้นตามทฤษฎี 4.22 $\text{ord}_m(b^h) | k$ หรือ $i | k$ (1)

และ $b^{hi} \equiv 1 \pmod{m}$ เพราะ $\text{ord}_m(b^h) = i$

ดังนั้นตามทฤษฎี 4.22 $\text{ord}_m(b) | hi$ หรือ $hk | hi$

นั่นคือ $k | i$ (2)

ดังนั้นจาก (1) และ (2) $k = i$

นั่นคือ $\text{ord}_m(b^h) = k$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 4.26 ให้ $\text{ord}_m(a) = j$ และ $\text{ord}_m(b) = k$ ถ้า $(j, k) = 1$
แล้ว $\text{ord}_m(ab) = jk$

พิสูจน์ สมมุติว่า $\text{ord}_m(ab) = i$

เพราะฉะนั้น $(ab)^i \equiv 1 \pmod{m}$

และ $a^{ji} \cdot b^{ji} \equiv 1 \pmod{m}$

แต่ $\text{ord}_m(a) = j$ แล้ว $a^{ji} \equiv 1^i \equiv 1 \pmod{m}$

ดังนั้น $b^{ji} \equiv 1 \pmod{m}$

แต่ $\text{ord}_m(b) = k$

ดังนั้นตามทฤษฎี 4.22 $k | ji$

เนื่องจาก $(j, k) = 1$

ดังนั้นตามทฤษฎี 2.7 $k|i$

ในทำนองเดียวกันจะพิสูจน์ได้ว่า $j|i$

เพราะฉะนั้นตามทฤษฎี 2.8

$$jk|i \qquad (A)$$

จาก $(ab)^{jk} = (a^j)^k(b^k)^j \equiv 1^k \cdot 1^j \equiv 1 \pmod{m}$

แสดงว่า $i|jk$ ตามทฤษฎี 4.22 (B)

ดังนั้นจาก (A) และ (B) สรุปได้ว่า

$$jk = i = \text{ord}_m(ab)$$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

นิยาม 4.8 ถ้าให้ m เป็นจำนวนเต็มบวกที่ $(g, m) = 1$ และ $\text{ord}_m(g) = \phi(m)$ แล้วเรียก g ว่า **รากปฐมฐาน มอดุโล** m

ตัวอย่าง 4.30 ให้ $m = 7, \quad (2, 7) = 1$

$$\phi(7) = 6$$

$$2^1 \equiv 2 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$2^3 \equiv 1 \pmod{7}$$

$$\text{ord}_7(2) = 3 \neq \phi(7)$$

ดังนั้น 2 ไม่เป็น**รากปฐมฐาน ของ** 7

แต่ 5 เป็น**รากปฐมฐาน ของ** 7

เพราะ $\text{ord}_7(5) = 6 = \phi(7)$

ต่อไปลองพิจารณา $m = 10$

เนื่องจาก $\phi(10) = 4$ และ $(3, 10) = 1$

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

$$3^2 \equiv 9 \equiv -1 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

ดังนั้น 3 เป็น**รากปฐมฐาน** ของ 10

จำนวนเต็มบวกบางตัวอาจไม่มีรากปฐมฐานก็ได้ เช่น

$\phi(8) = 4$ และจำนวนเต็มที่เป็นรีเลทีฟไพรม์กับ 8

ก็คือ 1, 3, 5, 7

$\text{ord}_8(1) = 1$ $\text{ord}_8(3) = 2$

$\text{ord}_8(5) = 2$ $\text{ord}_8(7) = 2$

ดังนั้น 8 ไม่มี**รากปฐมฐาน**

ทฤษฎี 4.27 ให้ m เป็นจำนวนเต็มบวก ถ้า g เป็น**รากปฐมฐาน ของ** m แล้ว $\{ g, g^2, g^3, \ldots, g^{\phi(m)} \}$ จะเป็นรีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m

พิสูจน์ เพราะว่ารีดิวซ์ เรซิดิว ซิสเท็ม มอดุโล m มีจำนวน $\phi(m)$

เพราะฉะนั้นเราต้องแสดงเพียงว่าเซ็ต $\{ g, g^2, \ldots, g^{\phi(m)} \}$

ไม่มีสมาชิกคู่ใดคอนกรูเอนซ์ มอดูโล m กันเลย

สมมุติว่า มี i และ j ซึ่ง $1 \leqslant i < j \leqslant \phi(m)$ ซึ่งทำให้

$$g^i \equiv g^j \pmod{m}$$

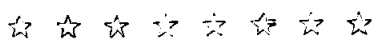
ดังนั้นจากทฤษฎี 4.24 $i \equiv j \pmod{\phi(m)}$

แสดงว่า $\phi(m) | j - i$

ซึ่งเป็นไปไม่ได้เพราะ $0 < j - i < \phi(m)$

เพราะฉะนั้น $g^i \not\equiv g^j \pmod{m}$

สำหรับ $1 \leqslant i < j \leqslant \phi(m)$



แบบฝึกหัด 4.8

1. จงหา $\text{ord}_{10}(7)$, $\text{ord}_{11}(6)$, $\text{ord}_{23}(3)$ และ $\text{ord}_{31}(3)$
2. จงแสดงว่า 2 เป็นรากปฐมฐาน ของ 29 และ 5 ไม่เป็น
3. จงพิสูจน์ว่า ถ้า $a \equiv b \pmod{m}$ แล้ว $\text{ord}_m(a) = \text{ord}_m(b)$
4. จงพิสูจน์ว่า ถ้า $ab \equiv 1 \pmod{m}$ แล้ว $\text{ord}_m(a) = \text{ord}_m(b)$
5. ถ้า $\text{ord}_m(a) = h$ และ $\text{ord}_n(a) = k$ และถ้า $(m, n) = 1$ แล้วจงพิสูจน์ว่า $\text{ord}_{mn}(a) = [h, k]$
6. ถ้า $\text{ord}_m(b) = k$ แล้ว จงพิสูจน์ว่า $\text{ord}_m(b^h) = k/d$ เมื่อ $h > 0$ และ $d = (h, k)$

4.9 อินดิซีส (Indices)

นิยาม 4.9 ให้ p เป็นจำนวนเฉพาะ และให้ g เป็นรากปฐมฐาน มอดุโล p

ให้ (a, p) = 1 ให้ k เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่ง $g^k \equiv a \pmod p$ แล้วเรียก k ว่าเป็นอินเดกซ์ (index) ของ a (ฐาน g มอดุโล p) และเขียนแทนด้วย

$$k = \text{ind}_g(a) = \text{ind}(a)$$

ตัวอย่าง 4.31 จงสร้างตารางของอินดิซีสสำหรับ p = 13

วิธีทำ เพราะว่า 2 เป็นพริมิทีบ รูทของ 13

$$\left.\begin{aligned} 2^1 &\equiv 2 \\ 2^2 &\equiv 4 \\ 2^3 &\equiv 8 \\ 2^4 &\equiv 3 \\ 2^5 &\equiv 6 \\ 2^6 &\equiv 12 \end{aligned}\right\} \pmod{13} \qquad \left.\begin{aligned} 2^7 &\equiv 11 \\ 2^8 &\equiv 9 \\ 2^9 &\equiv 5 \\ 2^{10} &\equiv 10 \\ 2^{11} &\equiv 7 \\ 2^{12} &\equiv 1 \end{aligned}\right\} \pmod{13}$$

เขียนเป็นตารางได้ดังนี้

a	1	2	3	4	5	6	7	8	9	10	11	12
ind (a)	12	1	4	2	9	5	11	3	8	10	7	6

ทฤษฎีต่อไปแสดงว่า อินดิซีส มีคุณสมบัติคล้ายกับ ลอการิธึม (logarithm) แต่โปรดจำไว้ว่าไม่เหมือนกันเพียงแต่คล้ายเท่านั้น

ทฤษฎี 4.28 ให้ p เป็นจำนวนเฉพาะและ g เป็นรากปฐมฐานมอดุโล p และ a, b เป็นจำนวนเต็มซึ่ง (a, p) = (b, p) = 1 และ n เป็นจำนวนเต็มบวกแล้ว

1. $\text{ind}(ab) \equiv \text{ind}(a) + \text{ind}(b) \pmod{p-1}$
2. $\text{ind}(a^n) \equiv n \cdot \text{ind}(a) \pmod{p-1}$

พิสูจน์ 1. เพราะว่า $g^{ind(a)} \equiv a \pmod p$

ดังนั้น $g^{ind(ab)} \equiv ab \equiv g^{ind(a)} \cdot g^{ind(b)} \equiv g^{ind(a)+ind(b)} \pmod p$

มอดุโล p

แสดงว่า $1 \equiv g^{ind(a)+ind(b)\ -\ ind\ (ab)} \pmod p$

เพราะฉะนั้น ตามทฤษฎี 4.22

$$\text{ord}_p(g) \mid [\text{ ind (a)} + \text{ind (b)} - \text{ind (ab) }]$$

นั่นคือ $\text{ind (a)} + \text{ind (b)} \equiv \text{ind (ab)} \pmod{p-1}$

2. ให้ผู้อ่านทำเป็นแบบฝึกหัด

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

เราสามารถนำอินดิซีสมาใช้ในการหาคำตอบของคอนกรูเอนซ์ได้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.32 จงหาคำตอบทั้งหมดของ $5x^{10} \equiv 7 \pmod{13}$

วิธีทำ ใช้ทฤษฎี 4.28 และตารางของอินดิซีสสำหรับ 13 เราได้

$$5x^{10} \equiv 7 \pmod{13}$$

$$\text{ind}\,(5x^{10}) = \text{ind}\,(7)$$

$$\text{ind}\,(5) + 10\,\text{ind}\,(x) \equiv \text{ind}\,(7) \pmod{12}$$

$$10\,\text{ind}\,(x) \equiv \text{ind}\,(7) - \text{ind}\,(5) \pmod{12}$$

แต่ $\text{ind}\,(7) = 11$ และ $\text{ind}\,(5) = 9$

เพราะฉะนั้น $10\,\text{ind}\,(x) \equiv 11 - 9 \equiv 2 \pmod{12}$

ใช้ทฤษฎี 4.6 จะได้ $5\,\text{ind}\,(x) \equiv 1 \pmod{6}$

$$5 \cdot 5\,\text{ind}\,(x) \equiv 5 \pmod{6}$$

$$\text{ind}\,(x) \equiv 5 \pmod{6}$$

ดังนั้น $\text{ind}\,(x) = 5$ หรือ $\text{ind}\,(x) = 11$

จึงจะทำให้ $\text{ind}\,(x) \equiv 5 \pmod{6}$

จากตารางเราทราบว่า $\text{ind}\,(6) = 5$ และ $\text{ind}\,(7) = 11$

ดังนั้นคำตอบที่ต้องการคือ $x \equiv 6 \pmod{13}$

$$x \equiv 7 \pmod{13}$$

ตัวอย่าง 4.33 จงหาคำตอบของคอนกรูเอนซ์

$$x^5 \equiv 3 \pmod{13}$$

วิธีทำ $5\,\text{ind}\,(x) \equiv \text{ind}\,(x^5) \equiv \text{ind}\,(3) \pmod{12}$

จากตาราง $\text{ind}\,(3) = 4$

เพราะฉะนั้น $5\,\text{ind}\,(x) \equiv 4 \pmod{12}$

$$5 \cdot 5\,\text{ind}\,(x) \equiv 5 \cdot 4 \equiv 8 \pmod{12}$$

$$\text{ind}\,(x) \equiv 8 \pmod{12}$$

ดังนั้น $\text{ind}\,(x) = 8$ ได้อย่างเดียวเท่านั้น

จากตารางเราทราบว่า $\text{ind}\,(9) = 8$

ดังนั้น $x \equiv 9 \pmod{13}$ เป็นคำตอบที่ต้องการ

ตัวอย่าง 4.34 จงหาคำตอบของ $x^3 \equiv 4 \pmod{13}$

$$3 \text{ ind}(x) \equiv \text{ind}(4) \equiv 2 \pmod{12}$$

เพราะว่า $(3, 12) \nmid 2$ ดังนั้น

$$3 \cdot \text{ind}(x) \equiv 2 \pmod{12}$$

ไม่มีคำตอบในมอดุโล 12

ดังนั้น $x^3 \equiv 4 \pmod{13}$

ก็ไม่มีคำตอบด้วย

ตัวอย่าง 4.35 จงหาคำตอบของ $23 \cdot 5^x \equiv 33 \pmod{71}$

วิธีทำ $\text{ind}(23) + x \text{ ind}(5) \equiv \text{ind}(33) \pmod{70}$

$$x \text{ ind}(5) \equiv \text{ind}(33) - \text{ind}(23) \pmod{70}$$

จากตารางท้ายเล่มหาอินเดกซ์ของจำนวนต่าง ๆ ได้ดังนี้

$\text{ind}(5) = 28$, $\text{ind}(33) = 57$, $\text{ind}(23) = 15$

ดังนั้น

$$\begin{aligned} 28x &\equiv 57 - 15 \pmod{70} \\ 28x &\equiv 42 \pmod{70} \\ 2x &\equiv 3 \pmod{5} \\ 3 \cdot 2x &\equiv 3 \cdot 3 \pmod{5} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

แบบฝึกหัด 4.9

1. จงหาคำตอบของ $x^4 \equiv 31 \pmod{41}$
2. จงหาคำตอบของ $x^5 \equiv 7 \pmod{29}$
3. จงหาคำตอบของ $x^3 \equiv 6 \pmod{19}$
4. จงหาคำตอบของ $14x^{72} \equiv 81 \pmod{97}$
5. จงหาคำตอบของ $8 \cdot 50^x \equiv 41 \pmod{59}$
6. จงพิสูจน์ข้อ 2 ของทฤษฎี 4.28
7. จงพิสูจน์ว่า ถ้า $t \equiv \text{ind}_g(a) \pmod{p-1}$ แล้ว $g^t \equiv a \pmod{p}$ เมื่อ g เป็นรากปฐมฐานมอดุโล จำนวนเฉพาะ p และ $(a, p) = 1$