แบบฝึกหัด 3.5

1. จงใช้ทฤษฎีบทของวิลสันหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 13$ มอดุโล 7
2. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $15!$ มอดุโล 17
3. จงหาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $2(26!)$ มอดุโล 29
4. จงพิจารณาว่า 17 เป็นจำนวนเฉพาะหรือไม่ โดยใช้ทฤษฎีบทของวิลสัน
5. จงแสดงว่า $18! \equiv -1 \pmod{437}$
6. ถ้า p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า

$$p \mid a^p + (p-1)!a \quad \text{และ} \quad p \mid (p-1)!a^p + a$$

สำหรับทุกจำนวนเต็ม a

(*แนะนำ* : โดยทฤษฎีบทของวิลสัน $a^p + (p-1)!a \equiv a^p - a \pmod{p}$)

7. จงแสดงว่า $3^{10} \equiv 1 \pmod{11^2}$
8. จงใช้ทฤษฎีบทเล็ก ๆ ของแฟร์มาต์หาผลเฉลยของ

8.1 $7x \equiv 12 \pmod{17}$

8.2 $4x \equiv 11 \pmod{19}$

8.3 $2x \equiv 1 \pmod{31}$

8.4 $6x \equiv 15 \pmod{11}$

9. จงแสดงว่า สำหรับจำนวนเต็ม n ใด ๆ

9.1 $2^{2n} \equiv 1 \pmod{3}$

9.2 $2^{3n} \equiv 1 \pmod{7}$

9.3 $2^{4n} \equiv 1 \pmod{15}$

10. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะคี่แล้ว $2(p-3)! \equiv -1 \pmod{p}$

3.6 ทฤษฎีบทของออยเลอร์ (Euler's Theorem)

ในหัวข้อนี้จะได้ขยายความรู้จากทฤษฎีบทเล็ก ๆ ของแฟร์มาต์ ซึ่งศึกษาเกี่ยวกับมอดุโล p เมื่อ p เป็นจำนวนเฉพาะ ไปยังมอดุโล n เมื่อ n เป็นจำนวนประกอบ ซึ่งก่อนอื่นจะได้แนะนำฟังก์ชันที่สำคัญฟังก์ชันหนึ่งเสียก่อน ดังนี้

บทนิยาม 3.6 ให้ n เป็นจำนวนเต็มบวก **ฟังก์ชันออยเลอร์ - ไฟ** (The Euler-phi function) $\phi(n)$ คือ จำนวนของจำนวนเต็มบวกที่ไม่เกิน n และเป็นจำนวนเฉพาะต่อกันกับ n

ตัวอย่าง 3.37 จงหาค่า $\phi(n)$ เมื่อ $1 \leqslant n \leqslant 12$

วิธีทำ *หาค่า* $\phi(1)$

จำนวนเต็มบวกที่ไม่เกิน 1 และเป็นจำนวนเฉพาะต่อกันกับ 1 คือ 1

ดังนั้น $\phi(1) = 1$

หาค่า $\phi(2)$

จำนวนเต็มบวกที่ไม่เกิน 2 และเป็นจำนวนเฉพาะต่อกันกับ 2 คือ 1

ดังนั้น $\phi(2) = 1$

หาค่า $\phi(3)$

จำนวนเต็มบวกที่ไม่เกิน 3 และเป็นจำนวนเฉพาะต่อกันกับ 3 คือ 1, 2

ดังนั้น $\phi(3) = 2$

หาค่า $\phi(4)$

จำนวนเต็มบวกที่ไม่เกิน 4 และเป็นจำนวนเฉพาะต่อกันกับ 4 คือ 1, 3

ดังนั้น $\phi(4) = 2$

หาค่า $\phi(5)$

จำนวนเต็มบวกที่ไม่เกิน 5 และเป็นจำนวนเฉพาะต่อกันกับ 5 คือ 1, 2, 3, 4

ดังนั้น $\phi(5) = 4$

หาค่า $\phi(6)$

จำนวนเต็มบวกที่ไม่เกิน 6 และเป็นจำนวนเฉพาะต่อกันกับ 6 คือ 1, 5

ดังนั้น $\phi(6) = 2$

หาค่า $\phi(7)$

จำนวนเต็มบวกที่ไม่เกิน 7 และเป็นจำนวนเฉพาะต่อกันกับ 7 คือ 1, 2, 3, 4, 5, 6

ดังนั้น $\phi(7) = 6$

หาค่า $\phi(8)$

จำนวนเต็มบวกที่ไม่เกิน 8 และเป็นจำนวนเฉพาะต่อกันกับ 8 คือ 1, 3, 5, 7

ดังนั้น $\phi(8) = 4$

หาค่า $\phi(9)$

จำนวนเต็มบวกที่ไม่เกิน 9 และเป็นจำนวนเฉพาะต่อกันกับ 9 คือ 1, 2, 4, 5, 7, 8

ดังนั้น $\phi(9) = 6$

หาค่า $\phi(10)$

จำนวนเต็มบวกที่ไม่เกิน 10 และเป็นจำนวนเฉพาะต่อกันกับ 10 คือ 1, 3, 7, 9

ดังนั้น $\phi(10) = 4$

หาค่า $\phi(11)$

จำนวนเต็มบวกที่ไม่เกิน 11 และเป็นจำนวนเฉพาะต่อกันกับ 11 คือ

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

ดังนั้น $\phi(11) = 10$

หาค่า $\phi(12)$

จำนวนเต็มบวกที่ไม่เกิน 12 และเป็นจำนวนเฉพาะต่อกันกับ 12 คือ 1, 5, 7, 11

ดังนั้น $\phi(12) = 4$ #

จากตัวอย่าง 3.37 สามารถนำมาสร้างตารางค่าฟังก์ชันออยเลอร์-ไฟ สำหรับ $1 \leqslant n \leqslant 12$ ได้ดังนี้

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

ตาราง 3.1 *ค่าฟังก์ชันออยเลอร์-ไฟ สำหรับ* $1 \leqslant n \leqslant 12$

จากตาราง 3.1 จะพบว่า ถ้า p เป็นจำนวนเฉพาะ และ $1 \leqslant p \leqslant 12$ จะได้ว่า

$$\phi(p) = p - 1$$

ซึ่งเราสามารถพิสูจน์ได้ว่า เป็นจริงสำหรับจำนวนเฉพาะโดยทั่วไปด้วย

ทฤษฎีบท 3.23 p เป็นจำนวนเฉพาะก็ต่อเมื่อ $\phi(p) = p-1$

พิสูจน์ สมมติ p เป็นจำนวนเฉพาะ

จะได้ว่า $(n, p) = 1$ ทุก $1 \leqslant n \leqslant p-1$

ดังนั้น $\phi(p) = p-1$

ในทางกลับกัน สมมติ $\phi(p) = p-1$

โดยที่ p เป็นจำนวนประกอบ ให้ d เป็นตัวหารของ p โดยที่ $1 < d < p$

ดังนั้น จะได้ว่า

$(d, p) \neq 1$ และ $(p, p) \neq 1$

นั่นคือ $\phi(p) \leqslant p-2$ ซึ่งเป็นไปไม่ได้

เพราะฉะนั้น p เป็นจำนวนเฉพาะ #

ทฤษฎีบท 3.24 ให้ p เป็นจำนวนเฉพาะ และ k เป็นจำนวนเต็มบวก แล้ว

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

พิสูจน์ เพราะว่า $(n, p^k) = 1$ ก็ต่อเมื่อ $p \nmid n$

และจำนวนเต็มที่อยู่ระหว่าง 1 ถึง p^k และหารด้วย p ลงตัวก็คือ

$$p, 2p, 3p, \ldots, p^{k-1}p$$

ซึ่งมีทั้งหมด p^{k-1} จำนวน

เพราะฉะนั้น จำนวนเต็ม $1, 2, 3, \ldots, p^k$ จะมีจำนวนเต็มที่เป็นจำนวนเฉพาะต่อกันกับ p^k อยู่ $p^k - p^{k-1}$ จำนวน

นั่นคือ $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ #

ตัวอย่าง 3.38

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 9 - 3 = 6$$

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$ #

ต่อไปจะแสดงว่า ถ้า m และ n เป็นจำนวนเฉพาะต่อกันแล้ว $\phi(mn) = \phi(m)\phi(n)$ แต่ก่อนที่จะได้พิสูจน์จะต้องอาศัยทฤษฎีบทประกอบต่อไปนี้เสียก่อน

ทฤษฎีบทประกอบ 3.25 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

$(a, bc) = 1$ ก็ต่อเมื่อ $(a, b) = 1$ และ $(a, c) = 1$

พิสูจน์ สมมติ $(a, bc) = 1$

ให้ $d = (a, b)$

จะได้ว่า $d|a$ และ $d|b$

ผลที่ตามมาก็คือ $d|a$ และ $d|bc$

นั่นคือ $d|1$ ซึ่งทำให้ $d = 1$

ในทำนองเดียวกัน ก็พิสูจน์ได้ว่า $(a, c) = 1$

ในทางกลับกัน สมมติ $(a, b) = 1$ และ $(a, c) = 1$

สมมติ $(a, bc) = d > 1$

ให้ p เป็นตัวหารของ d ที่เป็นจำนวนเฉพาะ

เพราะว่า $d|a$ และ $d|bc$

จะได้ว่า $p|a$ และ $p|bc$

และจาก $p|bc$

จะได้ว่า $p|b$ หรือ $p|c$

นั่นคือ ($p|a$ และ $p|b$) หรือ ($p|a$ และ $p|c$)

ผลที่ตามมาก็คือ $(a, b) \geq p$ หรือ $(a, c) \geq p$ ซึ่งเป็นไปไม่ได้ #

ทฤษฎีบทประกอบ 3.26 ให้ a, b และ n เป็นจำนวนเต็ม โดยที่ $n > 0$ และ $a \equiv b \pmod{n}$ แล้ว $(a, n) = 1$ ก็ต่อเมื่อ $(b, n) = 1$

พิสูจน์ สมมติ $(a, n) = 1$

และให้ $d = (b, n)$

จะได้ว่า $d|b$ และ $d|n$

เพราะว่า $a \equiv b \pmod{n}$

ดังนั้น จึงมีจำนวนเต็ม k ที่ทำให้ $a = b + kn$

เพราะว่า $d|b$ และ $d|n$ จึงได้ว่า $d|a$

ผลที่ตามมาก็คือ d เป็นตัวหารร่วมของ a และ n

ดังนั้น $d|1$ ซึ่งทำให้ $d = 1$

นั่นคือ $(b, n) = 1$

ในทำนองเดียวกัน ถ้า $(b, n) = 1$ ก็พิสูจน์ได้ว่า

$$(a, n) = 1$$

ทฤษฎีบท 3.27 ให้ m และ n เป็นจำนวนเต็มบวก โดยที่ $(m, n) = 1$ แล้ว

$$\phi(mn) = \phi(m)\phi(n)$$

พิสูจน์ เพราะว่า $\phi(1) = 1$ ดังนั้น ถ้า $m = 1$ หรือ $n = 1$ ทฤษฎีบทเป็นจริง จึงสมมติ $m > 1$ และ $n > 1$

เขียนจำนวนเต็ม $1, 2, 3, \ldots, mn$ เป็น m แถว และ n แนวตั้ง ดังนี้

1	$m+1$	$2m+1$	.....	$(n-1)m+1$
2	$m+2$	$2m+2$	.....	$(n-1)m+2$
3	$m+3$	$2m+3$	.....	$(n-1)m+3$
4	$m+4$	$2m+4$	.....	$(n-1)m+4$
m	$2m$	$3m$	.....	mn

พิจารณาจำนวนเต็มบวก r โดยที่ $1 \leqslant r \leqslant m$ และ $(m, r) = d > 1$ จำนวนเต็มในแถวที่ r จะอยู่ในรูปแบบของ $km + r$ โดยที่ $0 \leqslant k \leqslant n-1$

เพราะว่า $d|m$ และ $d|r$ จึงได้ว่า $d|km+r$ ทุก $0 \leqslant k \leqslant n-1$

นั่นคือ จำนวนเต็มทุกตัวในแถวที่ r โดยที่ r ไม่เป็นจำนวนเฉพาะต่อกันกับ m จะไม่เป็นจำนวนเฉพาะต่อกันกับ m ซึ่งส่งผลให้จำนวนเต็มทุกตัวในแถวที่ r จะไม่เป็นจำนวนเฉพาะต่อกันกับ mn ด้วย

ดังนั้น จำนวนเต็มที่จะเป็นจำนวนเฉพาะต่อกันกับ mn จะต้องอยู่ในแถวที่ r โดยที่ $(r, m) = 1$ ซึ่งมีอยู่ $\phi(m)$ แถว

พิจารณาสมาชิกแต่ละแถวจะอยู่ในรูปแบบของ

$$r \quad m+r \quad 2m+r \quad \ldots \quad (n-1)m+r$$

ซึ่งมี n จำนวน

จะพบว่า $km + r \not\equiv jm + r \pmod{n}$ ถ้า $k \neq j$

เนื่องจาก ถ้า $j \neq k$ และ

$$km + r \equiv jm + r \pmod{n}$$

แล้ว จะได้ว่า

$$km \equiv jm (\text{mod } n)$$

และเพราะว่า $(m, n) = 1$ จึงได้ว่า

$$k \equiv j (\text{mod } n)$$

ซึ่งเป็นไปไม่ได้ เพราะ $j \neq k$ และ $0 \leqslant k \leqslant n-1$, $0 \leqslant j \leqslant n-1$

นั่นคือ $r, m+r, 2m+r, \ldots, (n-1)m+r$ อยู่ในต่างชั้นของการลงรอยกัน มอดุโล n

และเพราะว่า จำนวนเต็มระหว่าง $1, 2, \ldots, n$ ซึ่งเป็นจำนวนเฉพาะต่อกันกับ n มีอยู่ $\phi(n)$ จำนวน จึงได้ว่า จำนวนเต็ม $r, m+r, 2m+r, \ldots, (n-1)m+r$ เป็นจำนวนเฉพาะต่อกันกับ n มีอยู่ $\phi(n)$ จำนวนด้วย

เพราะว่าจำนวนเต็มที่จะเป็นจำนวนเฉพาะต่อกันกับ m มี $\phi(m)$ แถว และแต่ละแถวจะมีจำนวนเต็มที่เป็นจำนวนเฉพาะต่อกันกับ n อยู่ $\phi(n)$ จำนวน ดังนั้น จึงได้

$$\phi(mn) = \phi(m)\phi(n) \qquad \#$$

ทฤษฎีบท 3.28 ให้ n เป็นจำนวนเต็มบวก และเขียนในรูปแบบบัญญัติได้เป็น

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$$

โดยที่ $p_1, p_2, \ldots, p_r$ เป็นจำนวนเฉพาะ และ $k_1, k_2, \ldots, k_r$ เป็นจำนวนเต็มบวกแล้ว

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

พิสูจน์ ถ้า $r = 1$ โดยทฤษฎีบท 3.25 $\phi(n) = n\left(1 - \frac{1}{p_1}\right)$

สมมติทฤษฎีบทเป็นจริง เมื่อ $r = i$

เพราะว่า $(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$

จึงได้ว่า

$$\begin{aligned}\phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i} p_{i+1}^{k_{i+1}}) &= \phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i})\phi(p_{i+1}^{k_{i+1}}) \\ &= \phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i})\, p_{i+1}^{k_{i+1}}\left(1 - \frac{1}{p_{i+1}}\right)\end{aligned}$$

เพราะว่า ทฤษฎีบทเป็นจริง เมื่อ $r = i$

จึงได้

$$\begin{aligned}\phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i} p_{i+1}^{k_{i+1}}) &= p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_i}\right) p_{i+1}^{k_{i+1}}\left(1 - \frac{1}{p_{i+1}}\right) \\ &= p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i} p_{i+1}^{k_{i+1}}\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_i}\right)\left(1 - \frac{1}{p_{i+1}}\right)\end{aligned}$$

นั่นคือ ทฤษฎีบทเป็นจริงเมื่อ $r = i+1$

ดังนั้น โดยทฤษฎีบทวิธีอุปนัยทางคณิตศาสตร์ ทฤษฎีบทเป็นจริงทุกจำนวนเต็มบวก r

#

ตัวอย่าง 3.39 จงหาค่า $\phi(360)$

วิธีทำ

$$\begin{aligned}\phi(360) &= \phi(2^3\cdot 3^2\cdot 5)\\ &= 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\ &= 360\times\frac{1}{2}\times\frac{2}{3}\times\frac{4}{5} = 96\end{aligned}$$

ตัวอย่าง 3.40 จงหาค่า $\phi(30030)$

94

วิธีทำ

$$\begin{aligned}\phi(30030) &= \phi(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13)\\ &= 30030\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\\ &= 30030\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdot\frac{10}{11}\cdot\frac{12}{13}\\ &= \mathbf{5760}\end{aligned}$$

#

ทฤษฎีบทต่อไปนี้จะแสดงให้เห็นว่า ถ้า $n > 2$ แล้ว $\phi(n)$ เป็นจำนวนเต็มคู่เสมอ

ทฤษฎีบท 3.29 สำหรับจำนวนเต็ม $n > 2$ $\phi(n)$ เป็นจำนวนเต็มคู่

พิสูจน์ *กรณี 1* n เป็นกำลังของ 2

กล่าวคือ มีจำนวนเต็ม k โดยที่ $k > 1$ ที่ทำให้ $n = 2^k$

จะได้

$$\begin{aligned}\phi(n) &= \phi(2^k)\\ &= 2^k\left(1-\frac{1}{2}\right) = 2^{k-1}\end{aligned}$$

นั่นคือ $\phi(n)$ เป็นจำนวนเต็มคู่

กรณี 2 n ไม่ใช่กำลังของ 2

จะได้ว่า มีจำนวนเฉพาะคี่ p ซึ่ง $p|n$

สมมติ $n = p^k m$ โดยที่ $k \geqslant 1$, m เป็นจำนวนเต็ม

และ $(p^k, m) = 1$

จะได้ $\phi(n) = \phi(p^k m)$

$$= \phi(p^k)\phi(m)$$

$$= p^k\left(1 - \frac{1}{p}\right)\phi(m)$$

$$= p^{k-1}(p-1)\phi(m)$$

เนื่องจาก $2|(p-1)$ จึงได้ว่า $\phi(n)$ เป็นจำนวนเต็มคู่ #

ทฤษฎีบท 3.30 *ทฤษฎีบทของเกาส์* (Gauss)

สำหรับจำนวนเต็มบวก $n \geqslant 1$

$$n = \sum_{d|n} \phi(d)$$

เมื่อ $\sum_{d|n} \phi(d)$ หมายถึง ผลบวกของ $\phi(d)$ ทุกค่า d ที่เป็นตัวหารบวกของ n

พิสูจน์ แบ่งจำนวนเต็ม $1, 2, 3, \ldots, n$ ออกเป็นชั้น ดังนี้

ให้ d เป็นตัวหารบวกของ n

$S_d = \{m | m$ เป็นจำนวนเต็ม $1 \leqslant m \leqslant n$ และ $(m, n) = d\}$

เพราะว่า $(m, n) = d$ ก็ต่อเมื่อ $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$

จึงได้ว่า

จำนวนของจำนวนเต็มใน S_d = จำนวนของจำนวนเต็มที่ไม่เกิน $\frac{n}{d}$ และเป็นจำนวนเฉพาะต่อกันกับ $\frac{n}{d}$

$$= \phi\left(\frac{n}{d}\right)$$

และเพราะว่าแต่ละจำนวนเต็มใน $\{1, 2, \ldots, n\}$ จะอยู่ใน S_d เพียง 1 เซตเท่านั้น

ดังนั้น $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$

เพราะว่า d แปรเปลี่ยนไปตามจำนวนเต็มบวกที่เป็นตัวหารของ n

$\frac{n}{d}$ ก็จะแปรเปลี่ยนไปตามตัวหารเหล่านี้ด้วย

นั่นคือ $n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$ #

ตัวอย่างต่อไปนี้จะช่วยให้เข้าใจการพิสูจน์ทฤษฎีบท 3.30 ยิ่งขึ้น

ตัวอย่าง 3.41 ให้ $n = 10$

จะได้ว่า ตัวหารบวกของ n คือ 1, 2, 5, 10

สำหรับตัวหารบวก d ใด ๆ ของ 10

ให้ $S_d = \{m \mid 1 \leqslant m \leqslant 10 \ (m, n) = d\}$

ดังนั้น

$$S_1 = \{1, 3, 7, 9\}$$

$$S_2 = \{2, 4, 6, 8\}$$

$$S_5 = \{5\}$$

$$S_{10} = \{10\}$$

พิจารณาค่า $\frac{n}{d}$ เมื่อ d แปรเปลี่ยนตามตัวหารบวกของ 10

จะได้ $\frac{n}{d}$ คือ 10, 5, 2, 1

และ

$$n = 10 = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \phi(10) + \phi(5) + \phi(2) + \phi(1)$$

$$= \sum_{d|n} \phi(d)$$

บทนิยาม 3.7 *ระบบลดทอนของเศษตกค้างมอดุโล* m (a reduced residue system modulo m) คือ เซตของจำนวนเต็ม $\phi(m)$ จำนวน โดยที่สมาชิกแต่ละจำนวนของเซตนี้เป็นจำนวนเฉพาะต่อกันกับ m และสมาชิกทุกคู่ในเซตนี้ไม่ลงรอยกันมอดุโล m

ตัวอย่าง 3.42 $\phi(8) = 4$

และ 1, 3, 5, 7 เป็นจำนวนเฉพาะต่อกันกับ 8 และทุกคู่ใน $\{1, 3, 5, 7\}$ ไม่ลงรอยกันมอดุโล 8 จึงได้

$\{1, 3, 5, 7\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล 8

นอกจากนั้น $-3, -1, 1, 3$ เป็นจำนวนเฉพาะต่อกันกับ 8 และทุกคู่ไม่ลงรอยกันมอดุโล 8 จึงได้

$\{-3, -1, 1, 3\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล 8 #

ทฤษฎีบท 3.31 ถ้า $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m และ a เป็นจำนวนเต็มบวก โดยที่ $(a, m) = 1$ แล้ว $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m ด้วย

พิสูจน์ จะแสดงว่าแต่ละจำนวนเต็ม ar_j เป็นจำนวนเฉพาะต่อกันกับ m

สมมติ $(ar_j, m) = d > 1$

เพราะว่า $d > 1$ d จึงมีตัวหารที่เป็นจำนวนเฉพาะ

ให้ p เป็นตัวหารของ d ที่เป็นจำนวนเฉพาะ

เพราะว่า $d|ar_j$ และ $d|m$ จึงได้ $p|ar_j$ และ $p|m$

ผลที่ตามมาก็คือ ($p|a$ และ $p|m$) หรือ ($p|r_j$ และ $p|m$)

เนื่องจาก $(r_j, m) = 1$ ดังนั้น จึงได้ว่า $p|a$ และ $p|m$

ซึ่งเป็นไปไม่ได้ เนื่องจาก $(a, m) = 1$

นั่นคือ $(ar_j, m) = 1$ ทุก $j = 1, 2, \ldots, \phi(m)$

ต่อไปจะพิสูจน์ว่า ถ้า $i \neq j$ แล้ว $ar_i \not\equiv ar_j (\text{mod } m)$

สมมติ $i \neq j$ และ $ar_i \equiv ar_j (\text{mod } m)$

เพราะว่า $(a, m) = 1$ จึงได้ว่า $r_i \equiv r_j (\text{mod } m)$ ซึ่งเป็นไปไม่ได้

นั่นคือ ถ้า $i \neq j$ แล้ว $ar_i \not\equiv ar_j (\text{mod } m)$

ผลที่ตามมาก็คือ $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m #

ตัวอย่าง 3.43 จากตัวอย่าง 3.42

$\{1, 3, 5, 7\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m

เพราะว่า $(3, 8) = 1$ จึงได้

$\{3\cdot 1, 3\cdot 3, 3\cdot 5, 3\cdot 7\} = \{3, 9, 15, 21\}$

เป็นระบบลดทอนของเศษตกค้างมอดุโล m ด้วย #

ทฤษฎีบท 3.32 *ทฤษฎีบทของออยเลอร์* (Euler's Theorem)

ถ้า m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็ม โดยที่ $(a, m) = 1$ แล้ว

$$a^{\phi(m)} \equiv 1 (\text{mod } m)$$

พิสูจน์ ให้ $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m โดยที่ $r_1, r_2, \ldots, r_{\phi(m)}$ เป็นจำนวนเต็มบวก

เพราะว่า $(a, m) = 1$ จึงได้ $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ เป็นระบบลดทอนของเศษตกค้างมอดุโล m ด้วย

นั่นคือ เซตของเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ $ar_1, ar_2, \ldots, ar_{\phi(m)}$ คือ

$$\{r_1, r_2, \ldots, r_{\phi(m)}\}$$

ซึ่งทำให้

$$ar_1ar_2\ldots ar_{\phi(m)} \equiv r_1r_2\ldots r_{\phi(m)} (\text{mod } m)$$

นั่นคือ

$$a^{\phi(m)}r_1r_2\ldots r_{\phi(m)} \equiv r_1r_2\ldots r_{\phi(m)} (\text{mod } m)$$

เพราะว่า $(r_1r_2\ldots r_{\phi(m)}, m) = 1$ จึงได้

$$a^{\phi(m)} \equiv 1 (\text{mod } m) \qquad \#$$

ทฤษฎีบทของออยเลอร์เป็นบทขยายของทฤษฎีบทเล็ก ๆ ของแฟร์มาต์ เนื่องจากถ้า p เป็นจำนวนเฉพาะ และ $(a, p) = 1$ แล้ว จะได้ $a^{\phi(p)} \equiv a^{p-1} \equiv 1 (\text{mod } p)$

ตัวอย่าง 3.44 จงแสดงว่า $3^{40} \equiv 1 (\text{mod } 100)$

และ $3^{256} \equiv 21 (\text{mod } 100)$

วิธีทำ เพราะว่า $(3, 100) = 1$

และ
$$\begin{aligned} \phi(100) &= \phi(2^2 \cdot 5^2) \\ &= 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \\ &= 40 \end{aligned}$$

ดังนั้น โดยทฤษฎีบทของออยเลอร์

$$3^{40} \equiv 1 (\text{mod } 100)$$

โดยขั้นตอนวิธีการหาร

$$256 = 6 \cdot 40 + 16$$

ดังนั้น

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 \cdot 3^{16} \equiv 3^{16} (\text{mod } 100)$$

และ

$$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (61)^2 \equiv 21 (\text{mod } 100)$$

นั่นคือ

$$3^{256} \equiv 21 (\text{mod } 100) \qquad \#$$

หมายเหตุ ถ้า a, m เป็นจำนวนเต็ม โดยที่ $m > 0$ และ $(a, m) = 1$ แล้ว โดยทฤษฎีบทของออยเลอร์ได้ว่า

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

นั่นคือ

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

จึงได้ว่า $a^{\phi(m)-1}$ เป็นตัวผกผันของ a มอดุโล m

ดังนั้น จึงสามารถใช้ทฤษฎีบทของออยเลอร์หาผลเฉลยของ $ax \equiv b \pmod{m}$ เมื่อ $(a, m) = 1$ ได้ดังนี้

เพราะว่า $a^{\phi(m)-1}$ เป็นตัวผกผันของ a มอดุโล m จึงได้

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

นั่นคือ $$x \equiv a^{\phi(m)-1}b \pmod{m}$$

ตัวอย่าง 3.45 จงหาผลเฉลยของ $3x \equiv 7 \pmod{10}$

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

จึงได้

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

ดังนั้น

$$3 \cdot 3^3 x \equiv 3^3 \cdot 7 \pmod{10}$$

จึงได้ $$x \equiv 3^3 \cdot 7 \equiv 9 \pmod{10}$$

แบบฝึกหัด 3.6

1. จงหาค่าฟังก์ชันออยเลอร์- ไฟของจำนวนเต็มต่อไปนี้

1.1 100	1.2 256
1.3 1001	1.4 10!
1.5 20!	1.6 5040
1.7 36000	

2. จงแสดงว่า ถ้า n เป็นจำนวนเต็มบวกแล้ว

$$\phi(2n) = \begin{cases} \phi(n) & n \text{ เป็นจำนวนคี่} \\ 2\phi(n) & n \text{ เป็นจำนวนคู่} \end{cases}$$

3. จงหาค่าจำนวนเต็มบวก n ที่ทำให้ $\phi(n)$ มีค่าเป็น

3.1 1	3.2 2
3.3 3	3.4 6
3.5 14	3.6 24

4. จงเขียนระบบลดทอนของเศษตกค้างมอดุโลต่อไปนี้

4.1 6	4.2 9
4.3 10	4.4 14
4.5 16	4.6 17

5. จงเขียนระบบลดทอนของเศษตกค้างมอดุโล 2^m เมื่อ m เป็นจำนวนเต็มบวก
6. จงใช้ทฤษฎีบทของออยเลอร์หาเศษตกค้างไม่เป็นลบที่เล็กที่สุดของ 3^{100000} มอดุโล 35
7. จงแสดงว่า ถ้า a เป็นจำนวนเต็มใด ๆ $a^7 \equiv a \pmod{63}$
8. จงแสดงว่า สำหรับจำนวนเต็ม a ใด ๆ

$$a^{37} \equiv a \pmod{1729}$$

(*แนะนำ* : $1729 = 7 \cdot 13 \cdot 19$)

9. จงแสดงว่า สำหรับจำนวนเต็ม a ใด ๆ

$$a^{13} \equiv a \pmod{2730}$$

(*แนะนำ* : $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$)

10. จงแสดงว่า สำหรับ a ที่เป็นจำนวนเต็มคี่

$$a^{33} \equiv a \pmod{4080}$$

(*แนะนำ* : $4080 = 15 \cdot 16 \cdot 17$)

11. **จงหาผลเฉลยของการลงรอยกันเชิงเส้นต่อไปนี้ โดยใช้ทฤษฎีบทของออยเลอร์**

11.1 $5x \equiv 3 \pmod{14}$

11.2 $4x \equiv 7 \pmod{15}$

11.3 $3x \equiv 5 \pmod{16}$

3.7 การลงรอยกันของพหุนาม (Polynomial Congruences)

ให้ $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ เป็นพหุนาม โดยที่ $a_n, a_{n-1}, \ldots, a_1, a_0$ เป็นจำนวนเต็ม เรากล่าวว่า จำนวนเต็ม c เป็นรากของ f(x) มอดุโล m ก็ต่อเมื่อ $f(c) \equiv 0 \pmod m$ และจะเห็นว่า ถ้า

$$c_0 \equiv c \pmod m$$

แล้วจะได้

$$f(c_0) \equiv f(c) \equiv 0 \pmod m \text{ ด้วย}$$

นั่นคือ ถ้า c เป็นรากของ f(x) มอดุโล m และ $c_0 \equiv c \pmod m$ แล้ว จะได้ว่า c_0 เป็นรากของ f(x) มอดุโล m ด้วย หรือกล่าวอีกนัยหนึ่งว่า ถ้าจำนวนเต็มจำนวนหนึ่งในชั้นของการลงรอยกันในมอดุโล m เป็นรากของ f(x) มอดุโล m แล้ว จำนวนเต็มทุกตัวในชั้นนั้นเป็นรากของ f(x) มอดุโล m ด้วย เราจึงถือว่า จำนวนเต็มทุกตัวในชั้นนี้เป็นหนึ่งรากของ f(x) มอดุโล m

ดังนั้น การพิจารณารากของ f(x) มอดุโล m จึงพิจารณาแค่ 0, 1, 2, ..., m − 1 ก็พอแล้ว

บทนิยาม 3.8 ให้ $\{r_1, r_2, \ldots, r_m\}$ เป็นระบบบริบูรณ์ของเศษตกค้างมอดุโล m จำนวนรากของ f(x) มอดุโล m คือ จำนวนของจำนวนเต็ม r_i ที่ทำให้ $f(r_i) \equiv 0 \pmod m$

ตัวอย่าง 3.46 ให้ $f(x) = x^2 + x + 1$ จงหารากของ f(x) มอดุโล 7

วิธีทำ

$f(0) = 1 \not\equiv 0 \pmod 7$

$f(1) = 3 \not\equiv 0 \pmod 7$

$f(2) = 7 \equiv 0 \pmod 7$

$f(3) = 13 \not\equiv 0 \pmod 7$

$f(4) = 21 \equiv 0 \pmod 7$

$f(5) = 31 \not\equiv 0 \pmod 7$

$f(6) = 43 \not\equiv 0 \pmod 7$

นั่นคือ $x \equiv 2 \pmod 7$ และ $x \equiv 4 \pmod 7$ เป็นราก 2 รากของ f(x) มอดุโล 7 #

ตัวอย่าง 3.47 ให้ $f(x) = x^2 + 2$ จงหารากของ f(x) มอดุโล 5

วิธีทำ

$f(0) = 2 \not\equiv 0 \pmod 5$

$f(1) = 3 \not\equiv 0 \pmod 5$

$f(2) = 6 \not\equiv 0 \pmod 5$

$f(3) = 11 \not\equiv 0 \pmod 5$

$f(4) = 18 \not\equiv 0 \pmod 5$

นั่นคือ $f(x)$ ไม่มีรากมอดุโล 5 #

ในกรณีที่ m เป็นจำนวนประกอบ ทฤษฎีบทต่อไปนี้จะทำให้การพิจารณารากของ $f(x)$ มอดุโล m ง่ายขึ้น

ทฤษฎีบท 3.33 ให้ $m = m_1 m_2 \ldots m_r$ เป็นจำนวนเต็มบวก โดยที่ $(m_i, m_j) = 1$ ทุก $i \neq j$ แล้ว จำนวนเต็ม c เป็นรากของ $f(x)$ มอดุโล m ก็ต่อเมื่อ c เป็นรากของ $f(x)$ มอดุโล m_i ทุก $i = 1, 2, \ldots, r$

พิสูจน์ ให้ c เป็นรากของ $f(x)$ มอดุโล m

จะได้ว่า $f(c) \equiv 0 \pmod m$

เพราะว่า ทุกค่า $i = 1, 2, \ldots, r$ $m_i | m$

ดังนั้น $f(c) \equiv 0 \pmod{m_i}$

นั่นคือ c เป็นรากของ $f(x)$ มอดุโล m_i ทุก $i = 1, 2, \ldots, r$

ในทางกลับกัน สมมติ c เป็นรากของ $f(x)$ มอดุโล m_i ทุก $i = 1, 2, \ldots, r$

ดังนั้น $f(c) \equiv 0 \pmod{m_i}$ ทุก $i = 1, 2, \ldots, r$

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

โดยบทแทรก 3.11 ได้ว่า

$$f(c) \equiv 0 \pmod{m_1 m_2 \ldots m_r}$$

ซึ่งก็คือ $f(c) \equiv 0 \pmod m$

นั่นคือ c เป็นรากของ $f(x)$ มอดุโล m #

ตัวอย่าง 3.43 ให้ $f(x) = x^2 + x + 7$ จงหารากของ $f(x)$ มอดุโล 15

วิธีทำ เนื่องจาก $15 = 3.5$ และ $(3, 5) = 1$

จึงพิจารณาหารากของ $f(x)$ มอดุโล 3 และมอดุโล 5

เพราะว่า

$f(0) = 7 \not\equiv 0 \pmod 3$

$$f(1) = 9 \equiv 0 \pmod 3$$

$$f(2) = 13 \not\equiv 0 \pmod 3$$

ดังนั้น 1 เป็นรากของ f(x) มอดุโล 3

และ

$$f(1) = 9 \not\equiv 0 \pmod 5$$

ดังนั้น จึงสรุปได้ว่า f(x) ไม่มีรากมอดุโล 15 #

ทฤษฎีบทประกอบ 3.34 ถ้า $f(x) = \sum_{k=0}^{n} a_k x^k$ เป็นพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็ม แล้ว

$$f(a+b) = f(a) + bf'(a) + b^2 q$$

โดยที่ a , b และ q เป็นจำนวนเต็ม และ

$$f'(a) = \sum_{k=1}^{n} ka_k a^{k-1}$$

พิสูจน์ โดยทฤษฎีบททวินาม สำหรับ $k > 1$

$$(a+b)^k = \binom{k}{0}a^k + \binom{k}{1}a^{k-1}b + \binom{k}{2}a^{k-2}b^2 + \ldots$$

$$+ \ldots + \binom{k}{k-1}a^2b^{k-2} + \binom{k}{k-2}ab^{k-1} + \binom{k}{k}b^k$$

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

เมื่อ $q_k = \sum_{i=2}^{k} \binom{k}{i} a^{k-1} b^{i-2}$

ดังนั้น

$$f(a+b) = \sum_{k=0}^{n} a_k (a+b)^k$$

$$= \sum_{k=2}^{n} a_k (a^k + kba^{k-1} + b^2 q_k) + a_1(a+b) + a_0$$

$$= \sum_{k=0}^{n} a_k a^k + b \sum_{k=1}^{n} ka_k a^{k-1} + b^2 \sum_{k=2}^{n} a_k q_k$$

$$= f(a) + bf'(a) + b^2 q$$

เมื่อ $q = \sum_{k=2}^{n} a_k b_k$ #

ทฤษฎีบท 3.35 ให้ $f(x)$ เป็นพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็ม p เป็นจำนวนเฉพาะ และ k เป็นจำนวนเต็ม โดยที่ $k \geqslant 2$ แล้ว

x_0 เป็นรากของ $f(x)$ มอดุโล p^k ก็ต่อเมื่อ $x_0 = a + y_0 p^{k-1}$

โดยที่ a เป็นรากของ $f(x)$ มอดุโล p^{k-1} และ y_0 เป็นรากของ $\frac{f(a)}{p^{k-1}} + yf'(a)$ มอดุโล p

พิสูจน์ สมมติ x_0 เป็นรากของ $f(x)$ มอดุโล p^k

เพราะว่า $p^{k-1} | p^k$ จึงได้ว่า x_0 เป็นรากของ $f(x)$ มอดุโล p^{k-1} ด้วย

โดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม a และ y_0 โดยที่

$$x_0 = y_0 p^{k-1} + a \qquad 0 \leqslant a < p^{k-1}$$

และเพราะว่า $x_0 \equiv a (\text{mod } p^{k-1})$ จึงได้ว่า a เป็นรากของ $f(x)$ มอดุโล p^{k-1} ด้วย

นั่นคือ รากของ $f(x)$ มอดุโล p^k สามารถเขียนในรูปแบบของ $a + y_0 p^{k-1}$

โดยที่ $0 \leqslant a < p^{k-1}$ เป็นรากของ $f(x)$ มอดุโล p^{k-1} และ y_0 เป็นจำนวนเต็ม

และถ้า $x_0 = y_0 p^{k-1} + a \;\; 0 \leqslant a < p^{k-1}$ เป็นรากของ $f(x)$ มอดุโล p^k แล้ว

จะได้ว่า

$$f(a + y_0 p^{k-1}) \equiv 0 (\text{mod } p^k)$$

และโดยทฤษฎีบทประกอบ 3.34

$$f(a + y_0 p^{k-1}) = f(a) + y_0 p^{k-1} f'(a) + q y_0^2 p^{2k-2}$$

โดยที่ q เป็นจำนวนเต็ม

และเพราะว่า $k \geqslant 2$ จึงได้ว่า $2k - 2 \geqslant k$ จึงได้ $p^{2k-2} \equiv 0 (\text{mod } p^k)$

และ

$$f(a) + y_0 p^{k-1} f'(a) + q y_0^2 p^{2k-2} \equiv 0 (\text{mod } p^k)$$

ดังนั้น

$$f(a) + y_0 p^{k-1} f'(a) \equiv 0 (\text{mod } p^k)$$

และเพราะว่า $f(a) \equiv 0 (\text{mod } p^{k-1})$ จึงได้ว่า $p^{k-1} | f(a)$

เนื่องจาก $(p^{k-1}, p^k) = p^{k-1}$ จึงทำให้

$$\frac{f(a)}{p^{k-1}} + y_0 f'(a) \equiv 0 (\text{mod } p)$$

นั่นคือ y_0 เป็นรากของ $\frac{f(a)}{p^{k-1}} + yf'(a)$ มอดุโล p

ในทางกลับกัน ให้ $x_0 = a + y_0 p^{k-1}$ โดยที่ $0 \leqslant a < p^{k-1}$

a เป็นรากของ f(x) มอดุโล p^{k-1} และ y_0 เป็นรากของ $\frac{f(a)}{p^{k-1}} + yf'(a)$ มอดุโล p

เนื่องจาก y_0 เป็นรากของ $\frac{f(a)}{p^{k-1}} + yf'(a)$ มอดุโล p

จึงได้

$$\frac{f(a)}{p^{k-1}} + y_0 f'(a) \equiv O(\text{mod } p)$$

เพราะฉะนั้น

$$f(a) + y_0 f'(a) p^{k-1} \equiv 0(\text{mod } p^k)$$

และเพราะว่า $p^{2k-2} \equiv O(\text{mod } p^k)$

จึงได้ว่า

$$f(a) + y_0 f'(a) p^{k-1} + q y_0^2 p^{2k-2} \equiv O(\text{mod } p^k)$$

เมื่อ q เป็นจำนวนเต็ม โดยที่

$$f(a + y_0 p^{k-1}) = f(a) + y_0 p^{k-1} f'(a) + q y_0^2 p^{2k-2}$$

นั่นคือ

$$f(x_0) \equiv O(\text{mod } p^k)$$

จึงสรุปได้ว่า x_0 เป็นรากของ f(x) มอดุโล p^k

ตัวอย่าง 5.49 ให้ $f(x) = x^3 - x^2 + 7x + 1$ จงหารากของ f(x) มอดุโล 8

วิธีทำ เนื่องจาก 8 = 23 จึงจะหารากของ f(x) มอดุโล 2^2

และถ้า a เป็นรากของ f(x) มอดุโล 2^2 แล้ว ขั้นต่อไปจะหารากของ

$$\frac{f(a)}{2^2} + yf'(a) \text{ มอดุโล } 2$$

การหารากของ f(x) มอดุโล 2^2 ทำได้โดยหารากของ f(x) มอดุโล 2 ก่อนดังนี้

เพราะว่า $f(0) = I \not\equiv 0(\text{mod } 2)$

$f(l) = 8 \equiv O(\text{mod } 2)$

จึงได้ว่า 1 เป็นรากเพียงค่าเดียวของ f(x) มอดุโล 2

ต่อไปจะหารากของ f(x) มอดุโล 2^2

โดยการใช้ทฤษฎีบท 3.35 โดยที่ p = 2, k = 2

เพราะว่า 1 เป็นรากของ f(x) มอดุโล 2 จึงได้ $a = 1$

เพราะฉะนั้น

$$x_0 = a + y_0 p^{k-1}$$
$$= 1 + y_0 \cdot 2 = 1 + 2y_0$$

เป็นรากของ f(x) มอดุโล p^2 เมื่อ y_0 เป็นรากของ $\frac{f(1)}{2} + yf'(1)$ มอดุโล p

เพราะว่า $f(1) = 8$ $f'(1) = 8$ จึงหาผลเฉลยของ

$$4 + 8y \equiv 0 \pmod 2$$

ซึ่งได้ว่า $y \equiv 0 \pmod 2$ และ $y \equiv 1 \pmod 2$ เป็นผลเฉลย

ดังนั้น $x_1 = 1 + 2(0) = 1$ และ $x_2 = 1 + (2)(1) = 3$

เป็นรากของ f(x) มอดุโล 2^2

ต่อไปจะหารากของ f(x) มอดุโล 2^3

โดยการใช้ทฤษฎีบท 3.35 โดยที่ $p = 2$, $k = 3$

จะได้ $a = 1$ หรือ $a = 3$

นั่นคือ $x = 1 + 4y_1$ และ $x_2 = 3 + 4y_2$

เป็นรากของ f(x) มอดุโล 2^3 เมื่อ y_1 คือรากของ $\frac{f(1)}{4} + yf'(1)$ มอดุโล 2

และ y_2 เป็นรากของ $\frac{f(3)}{4} + yf'(3)$ มอดุโล 2

กรณี $a = 1$

หาผลเฉลยของ

$$\frac{f(1)}{4} + yf'(1) \equiv 0 \pmod 2$$

หรือ $$2 + 8y \equiv 0 \pmod 2$$

จะได้ $y \equiv 0 \pmod 2$ และ $y \equiv 1 \pmod 2$ เป็นผลเฉลย

นั่นคือ จะได้ว่า 1 และ 5 เป็นรากของ f(x) มอดุโล 8

กรณี $a = 3$.

หาผลเฉลยของ

$$\frac{f(3)}{4} + yf'(3) \equiv 0 \pmod 2$$

ซึ่งก็คือ $$10 + 28y \equiv 0 \pmod 2$$

และได้ว่า $y = 0$ และ $y = 1$ เป็นผลเฉลย

นั่นคือ จะได้ว่า 3 และ 7 เป็นรากของ $f(x)$ มอดุโล 8

เพราะฉะนั้น รากทั้งหมดของ $f(x)$ มอดุโล 8 คือ 1, 3, 5 และ 7 #

ตัวอย่าง 3.50 ให้ $f(x) = x^3 - x^2 + 7x + 1$ จงหารากทั้งหมดของ $f(x)$ มอดุโล 200

วิธีทำ เพราะว่า $200 = 2^3 \cdot 5^2$ ดังนั้น การหารากของ $f(x)$ มอดุโล 200 จึงเพียงพอที่จะหาผลเฉลยของระบบการลงรอยกัน

$$f(x) \equiv 0 \pmod{8}$$

$$f(x) \equiv 0 \pmod{25}$$

โดยที่ $f(x) = x^3 - x^2 + 7x + 1$

จากตัวอย่าง 3.49 ได้ว่า 1, 3, 5 และ 7 เป็นรากของ $f(x)$ มอดุโล 8 ดังนั้น ต่อไปนี้จึงจะหารากของ $f(x)$ มอดุโล 25 ดังนี้

พิจารณาหารากของ $f(x)$ *มอดุโล* 5

เพราะว่า

$$f(0) = 1 \not\equiv 0 \pmod{5}$$

$$f(1) = 8 \not\equiv 0 \pmod{5}$$

$$f(2) = 19 \not\equiv 0 \pmod{5}$$

$$f(3) = 40 \equiv 0 \pmod{5}$$

$$f(4) = 77 \not\equiv 0 \pmod{5}$$

จึงได้ว่า 3 เป็นรากของ $f(x)$ มอดุโล 5

ต่อไปพิจารณาหารากของ $f(x)$ *มอดุโล* 5^2

โดยการใช้ทฤษฎีบท 3.35 เมื่อ $p = 5$, $k = 2$ และ $a = 3$

จะได้

$$x_0 = a + y_0 p^k = 3 + y_0 5^2$$

เป็นรากของ $f(x)$ มอดุโล 5^2 โดยที่ y_0 เป็นรากของ $\frac{f(3)}{5} + yf'(3)$ มอดุโล 5

เพราะว่า $f(3) = 40$ และ $f'(3) = 28$

จึงหาผลเฉลยของ

$$8 + 28y \equiv 0 \pmod{5}$$

เพราะว่า $28y \equiv -3 \pmod 5 \equiv 2 \pmod 5$

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

นั่นคือ $x_0 = 3 + 5(4) = 23$ เป็นรากของ $f(x)$ มอดุโล 5^2

เพราะว่ารากของ $f(x)$ มอดุโล 2^3 มี 4 ราก และรากของ $f(x)$ มอดุโล 5^2 มีเพียง 1 ราก จึงจะพิจารณาผลเฉลยของระบบการลงรอยกัน 4 ระบบ ดังนี้

$$\text{I} \quad \begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 23 \pmod{25} \end{cases}$$

$$\text{II} \quad \begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 23 \pmod{25} \end{cases}$$

$$\text{III} \quad \begin{cases} x \equiv 5 \pmod 8 \\ x \equiv 23 \pmod{25} \end{cases}$$

$$\text{IV} \quad \begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 23 \pmod{25} \end{cases}$$

โดยทฤษฎีบทเศษเหลือของชาวจีน หาผลเฉลยของ I, II, III และ IV ได้ดังนี้

ให้ $M = 8x25 = 200$

จะได้ $M_1 = \frac{200}{8} = 25$

$M_2 = \frac{200}{25} = 8$

หาค่า y_1 ที่ทำให้ $M_1 y_1 \equiv 1 \pmod 8$

นั่นคือ $25y_1 \equiv 1 \pmod 8$

ซึ่งได้ว่า $y_1 \equiv 1 \pmod 8$

หาค่า y_2 ที่ทำให้ $M_2 y_2 \equiv 1 \pmod{25}$

นั่นคือ $8y_2 \equiv 1 \pmod{25}$

ซึ่งได้ว่า $y_2 \equiv -3 \equiv 22 \pmod{25}$

ดังนั้น ผลเฉลยของ I คือ

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 \\ &= 1 \cdot 25 \cdot 1 + 23 \cdot 8 \cdot 22 \\ &= 4073 \end{aligned}$$

นั่นคือ $x \equiv 4073 \equiv 73 \pmod{200}$ เป็นผลเฉลยของ I

เพราะว่า ใน II มี $a_1 = 3$ และ $a_2 = 23$

ผลเฉลยของ II คือ

$$x = 3\cdot 25\cdot 1 + 23\cdot 8\cdot 22$$
$$= 75 + 4048 = 4123$$

ซึ่งได้ว่า $x \equiv 4123 \equiv 123 \pmod{200}$ เป็นผลเฉลยของ 11

เพราะว่าใน 111 มี $a_1 = 5$ และ $a_2 = 23$

ผลเฉลยของ 111 คือ

$$x = 5\cdot 25\cdot 1 + 23\cdot 8\cdot 22$$
$$= 125 + 4048$$
$$= 4173$$

ซึ่งได้ว่า $x \equiv 4173 \equiv 173 \pmod{200}$ เป็นผลเฉลยของ III

เพราะว่าใน IV มี $a_1 = 7$ และ $a_2 = 23$

ผลเฉลยของ IV คือ

$$x = 7\cdot 25\cdot 1 + 23\cdot 8\cdot 22$$
$$= 175 + 4048 = 4223$$

ซึ่งได้ว่า $x \equiv 4223 \equiv 23 \pmod{200}$ เป็นผลเฉลยของ IV

นั่นคือ รากทั้งหมดของ $f(x)$ มอดุโล 200 คือ 23, 73, 123 และ 173 #

จะสังเกตได้ว่า ในการหารากของ $f(x)$ มอดุโล m นั้น $f(x)$ อาจไม่มีรากมอดุโล m ดังเช่นตัวอย่าง 3.47 และ 3.48 หรือ $f(x)$ อาจมีรากมอดุโล m จำนวนมากกว่าดีกรีของ $f(x)$ ดังเช่นตัวอย่าง 3.49 $f(x) = x^3 - x^2 + 7x + 1$ เป็นพหุนามดีกรี 3 แต่ $f(x)$ มีรากมอดุโล 8 ถึง 4 ราก ทฤษฎีบทต่อไปนี้จะแสดงว่า ถ้า $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ โดยที่ $a_n \not\equiv 0 \pmod{p}$ เมื่อ p เป็นจำนวนเฉพาะแล้ว $f(x)$ มีรากมอดุโล p ไม่เกิน n ราก

ทฤษฎีบท 3.36 *ทฤษฎีบทของลากรองจ์* (Lagrange's Theorem)

ให้ p เป็นจำนวนเฉพาะ และ $f(x) = \sum_{i=0}^{n} a_ix^i$ เป็นพหุนามดีกรี $n \geq 1$

โดยที่ $a_0, a_1, \ldots, a_n$ เป็นจำนวนเต็ม และ $a_n \not\equiv 0 \pmod{p}$ แล้ว $f(x)$ มีรากมอดุโล p ได้อย่างมากที่สุดไม่เกิน n ราก

พิสูจน์ จะพิสูจน์โดยใช้วิธีอุปนัยทางคณิตศาสตร์บนดีกรีของพหุนาม

เมื่อ $n = 1$ $f(x) = a_1x + a_0$ และ $a_1 \not\equiv 0 \pmod p$

จะได้ว่า รากของ $f(x)$ มอดุโล p คือ ผลเฉลยของการลงรอยกันเชิงเส้น

$$a_1x \equiv -a_0 \pmod p$$

เพราะว่า $a_1 \not\equiv 0 \pmod p$ จึงได้ว่า $(a_1, p) = 1$ และ $1 | a_0$ จึงได้ว่า การลงรอยกันเชิงเส้น $a_1x \equiv -a_0 \pmod p$ มีผลเฉลยและมีเพียง 1 ผลเฉลยเท่านั้น

นั่นคือ ทฤษฎีบทเป็นจริง เมื่อ $n = 1$

ต่อไปสมมติว่าทฤษฎีบทเป็นจริงสำหรับพหุนามดีกรี $k-1$ เมื่อ k เป็นจำนวนเต็มมากกว่าหรือเท่ากับ 1

ให้ $f(x) = \sum_{i=0}^{k} a_ix^i$ โดยที่ $a_k \not\equiv 0 \pmod p$

สมมติ $f(x)$ มีราก $k+1$ รากมอดุโล p กล่าวคือ ให้ $c_0, c_1, \ldots, c_k$ เป็นรากของ $f(x)$ มอดุโล p ซึ่งไม่ลงรอยกัน

ดังนั้นจะได้ $f(c_i) \equiv 0 \pmod p$ ทุก $i = 0, 1, \ldots, k$

เราจะได้

$$\begin{aligned} f(x) - f(c_0) &= a_k(x^k - c_0^k) + a_{k-1}(x^{k-1} - c_0^{k-1}) + \ldots + a_1(x - c_0) \\ &= (x - c_0)\, g(x) \end{aligned}$$

เมื่อ $g(x)$ เป็นพหุนามดีกรี $k-1$ และมีสัมประสิทธิ์ของ x^{k-1} คือ a_k

จะแสดงว่า $c_1, c_2, \ldots, c_k$ เป็นรากของ $g(x)$ มอดุโล p

ให้ i เป็นจำนวนเต็มใด ๆ โดยที่ $1 \leqslant i \leqslant k$

เพราะว่า

$$f(c_i) \equiv f(c_0) \equiv 0 \pmod p$$

จะได้

$$f(c_i) - f(c_0) = (c_i - c_0)\, g(c_i) \equiv 0 \pmod p$$

ดังนั้นจึงได้ $g(c_i) \equiv 0 \pmod p$ เนื่องจาก $c_i - c_0 \not\equiv 0 \pmod p$

นั่นคือ c_i เป็นรากของ $g(x)$ มอดุโล p ทุก $i = 1, 2, \ldots, k$

ผลที่ตามมาก็คือ $g(x)$ ซึ่งมีดีกรี $k-1$ มีรากซึ่งไม่ลงรอยกันมอดุโล p ถึง k ราก ซึ่งขัดกับสมมติฐานของวิธีอุปนัย

ดังนั้น $f(x)$ จึงมีรากมอดุโล p ได้ไม่เกิน k ราก

นั่นคือ ทฤษฎีบทเป็นจริง #

ทฤษฎีบท 3.37 ให้ p เป็นจำนวนเฉพาะ และ d เป็นตัวหารของ $p-1$ ที่เป็นจำนวนเต็มบวก แล้ว x^d-1 จะมีรากมอดุโล p แน่นอน d ราก

พิสูจน์ เพราะว่า $d|(p-1)$ ดังนั้น จะมีจำนวนเต็ม e ที่ทำให้

$$p-1 = de$$

และ

$$x^{p-1}-1 = (x^d-1)\,g(x)$$

โดยที่ $g(x) = x^{d(e-1)}+x^{d(e-2)}+\ldots+x^d+1$

จากทฤษฎีบทเล็ก ๆ ของแฟร์มาต์ $x^{p-1}-1$ มีรากมอดุโล p แน่นอน $(p-1)$ ราก และเพราะว่ารากของ $x^{p-1}-1$ คือ รากของ x^d-1 หรือ $g(x)$ มอดุโล p

แต่ $g(x)$ มีรากได้ไม่เกิน $d(e-1) = de-d = p-1-d$ ราก และรากของ $x^{p-1}-1$ ที่ไม่ใช่รากของ $g(x)$ มอดุโล p จะคือรากของ x^d-1 มอดุโล p ดังนั้น x^d-1 จะมีรากอย่างน้อย $(p-1)-(p-1-d) = d$ ราก และจากทฤษฎีบทของลากรองจ์ x^d-1 มีรากมอดุโล p ไม่เกิน d ราก จึงสรุปได้ว่า

x^d-1 มีรากมอดุโล p แน่นอน d ราก #

แบบฝึกหัด 3.7

1. จงหารากของ $x^3 - 2x - 3$ มอดุโล 9
2. จงหารากของ $x^3 - 2x - 3$ มอดุโล 5
3. จงหารากของ $x^3 - 2x - 3$ มอดุโล 45
4. จงหารากของ $x^3 + 4x + 8$ มอดุโล 15
5. จงหารากของ $x^3 + 4x + 23x - 15$ มอดุโล 503

   (*แนะนำ* : $x^3 + 4x + 23x - 15 = (x-1)(x-3)(x-5)$)
6. จงหารากของ $x^3 - 9x^2 + 23x - 15$ มอดุโล 143
7. จงหารากของ $x^2 + x + 7$ มอดุโล 27
8. จงหารากของ $x^2 + x + 7$ มอดุโล 81
9. จงหารากของ $x^5 + x^4 + 1$ มอดุโล 3^4
10. จงหารากของ $x^3 + x + 57$ มอดุโล 5^3
11. จงหารากของ $x^2 + 5x + 24$ มอดุโล 36
12. จงหารากของ $x^3 + 10x^2 + x + 3$ มอดุโล 33
13. จงหารากของ $x^3 + x^2 - 4$ มอดุโล 7^3
14. จงหารากของ $x^3 + x^2 - 5$ มอดุโล 7^3
15. ให้ p เป็นจำนวนเฉพาะ และ $f(x) = \sum_{i=0}^{n} a_i x^i$

    ถ้า $f(x)$ มีรากมอดุโล p เกิน n ราก แล้ว จงแสดงว่า $p|a_i$ ทุก $i = 1, 2, \ldots, n$