

Problems

Sarawut Suebsang

July 23, 2021

§1 Number theory

Example 1.1

ให้ m, n เป็นจำนวนเต็มบวกโดยที่ $\gcd(m, n) = 1$, m เป็นจำนวนคู่ และ n เป็นจำนวนคี่ จงหาค่าของ

$$\frac{1}{2n} + \sum_{k=1}^{n-1} (-1)^{\lfloor \frac{km}{n} \rfloor} \left\{ \frac{km}{n} \right\}$$

Proof. ให้ $r_k = (km \bmod n)$ จะได้ $\left\{ \frac{km}{n} \right\} = \frac{r_k}{n}$ และ $\lfloor \frac{km}{n} \rfloor = \frac{km - r_k}{n}$ พิจารณา

$$\frac{km - r_k}{n} \equiv r_k \pmod{2}$$

จะได้ $(-1)^{\lfloor \frac{km}{n} \rfloor} = (-1)^{r_k}$ และจาก $\gcd(m, n) = 1$ แสดงว่า $(km \bmod n), k = 1, 2, \dots, n-1$ ต่างกันหมด ดังนั้นจากโจทย์จะเขียนใหม่ได้เป็น

$$\frac{1}{2n} + \frac{1}{n} \sum_{r=1}^{n-1} (-1)^r r = \frac{1}{2}$$

□

Example 1.2

จงหาจำนวนเฉพาะ p ทั้งหมด ซึ่ง $p = m^2 + n^2$ และ p หาร $m^3 + n^3 - 4$ ลงตัว สำหรับจำนวนเต็มบวก m, n บางค่า

Proof.

$$(m + n)^2 \equiv 2mn \pmod{p}$$

จะได้

$$\begin{aligned} (m + n)^3 &\equiv m^3 + n^3 + 3mn(m + n) \pmod{p} \\ m^3 + n^3 &\equiv (m + n)^3 - 3mn(m + n) \pmod{p} \\ 2(m^3 + n^3) &\equiv 2(m + n)^3 - 3(m + n)(2mn) \pmod{p} \\ 2(m^3 + n^3) &\equiv -(m + n)^3 \pmod{p} \end{aligned}$$

จาก $m^3 + n^3 - 4 \equiv 0 \pmod{p}$ จะได้ $(m+n)^3 + 8 \equiv 0 \pmod{p}$ นั่นคือ

$$p|(m+n+2)((m+n)^2 - 2(m+n) + 4)$$

จะได้

$$p|m+n+2 \text{ หรือ } p|2mn - 4(m+n) + 4$$

ในกรณี $p = 2, 5$ เห็นชัดว่าสอดคล้องกับที่โจทย์ต้องการ พิจารณา กรณี $p \geq 13$ จะได้

$$p|m+n+2 \text{ หรือ } p|mn - (m+n) + 2$$

จาก $p = m^2 + n^2$ จะได้ $\max\{m, n\} > \sqrt{\frac{13}{2}}$ นั่นคือ $\max\{m, n\} \geq 3$

ดังนั้น $m(m-1) + n(n-1) > 2$ หรือ $p > m+n+2$ จะได้ $p \nmid m+n+2$

จะได้ $p|mn - (m+n) + 2$ เท่านั้น , $mn - (m+n) + 2 = (m-1)(n-1) + 1 > 0$ เนื่องจาก $\max\{m, n\}^2 > (m-1)(n-1)$ จะได้ $p > (m-1)(n-1) + 1$ ดังนั้นกรณีนี้ไม่มีคำตอบ \square

Theorem (triangle inequality of floor function)

ให้ $a, b \in \mathbb{R}$

$$\lfloor a+b \rfloor \geq \lfloor a \rfloor + \lfloor b \rfloor$$

Theorem (Legendre's formula)

สำหรับ p เป็นจำนวนเฉพาะให้ $v_p(n)$ คือเลขชี้กำลังที่มากที่สุดของ p ซึ่งหาร n ลงตัว จะได้

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Example 1.3

ให้ a_1, a_2, \dots, a_k เป็นจำนวนเต็มบวก และ $d = \gcd(a_1, a_2, \dots, a_k)$ และ

$a_1 + a_2 + \dots + a_k = n$ จงแสดงว่า $\frac{d(n-1)!}{a_1!a_2!\dots a_k!}$ เป็นจำนวนเต็ม

Proof. ก่อนอื่นจะพิจารณาสมบัติที่ต้องใช้แก้โจทย์

Claim — ให้ $a, b \in \mathbb{Z}$ ถ้า $b \nmid a$ แล้ว $\lfloor \frac{a}{b} \rfloor = \lfloor \frac{a-1}{b} \rfloor$

เนื่องจาก $b \nmid a$ ให้ $a = bq + r$ เมื่อ $0 < r < b$ จะได้ $q = \lfloor \frac{a}{b} \rfloor = \lfloor \frac{a-1}{b} \rfloor$

ให้ p เป็นจำนวนเฉพาะใดๆ ต่อไปเราจะแสดงว่า $v_p(d(n-1)!) \geq \sum_{i=1}^k v_p(a_i!)$

เราจะใช้ triangle inequality of floor function และ Legendre's formula เพื่อแสดงอสมการข้างต้น
 $v_p(d(n-1)!) = v_p(d) + v_p((n-1)!) = v_p(d) + \sum_{i=1}^{\infty} \left\lfloor \frac{n-1}{p^i} \right\rfloor$ และ $\sum_{j=1}^k v_p(a_j) = \sum_{j=1}^k \sum_{i=1}^{\infty} \left\lfloor \frac{a_j}{p^i} \right\rfloor$
 จัดรูปอสมการใหม่จะได้

$$v_p(d) + \sum_{i=1}^{\infty} \left\lfloor \frac{n-1}{p^i} \right\rfloor \geq \sum_{j=1}^k \sum_{i=1}^{\infty} \left\lfloor \frac{a_j}{p^i} \right\rfloor$$

หรือ

$$v_p(d) + \sum_{i=1}^{\infty} \left(\left\lfloor \frac{n-1}{p^i} \right\rfloor - \sum_{j=1}^k \left\lfloor \frac{a_j}{p^i} \right\rfloor \right) \geq 0$$

ในกรณี $p \nmid d$ จะได้ $v_p(d) = 0$ และจะมี l ซึ่ง $p \nmid a_l$ จากที่ Claim ไว้จะได้ $\left\lfloor \frac{a_l}{p^i} \right\rfloor = \left\lfloor \frac{a_l-1}{p^i} \right\rfloor$ ดังนั้นเราสามารถเปลี่ยน a_l เป็น $a_l - 1$ และจาก triangle inequality of floor function ทำให้ได้

$$\left\lfloor \frac{n-1}{p^i} \right\rfloor \geq \sum_{j=1}^k \left\lfloor \frac{a_j}{p^i} \right\rfloor$$

ดังนั้นสมการที่เราต้องการแสดงเป็นจริงในกรณี $p \nmid d$
กรณี $p \mid d$ ถ้าหาก $i > v_p(d)$ ใช้เหตุผลคล้ายกรณีแรกจะได้

$$\left\lfloor \frac{n-1}{p^i} \right\rfloor \geq \sum_{j=1}^k \left\lfloor \frac{a_j}{p^i} \right\rfloor$$

ถ้าหาก $i \leq v_p(d)$ เราจะแบ่ง 1 จาก $v_p(i)$ ให้กับแต่ละวงเล็บ $i \leq v_d(p)$ ซึ่งเพียงพอที่จะพิสูจน์

$$1 + \left\lfloor \frac{n-1}{p^i} \right\rfloor \geq \sum_{j=1}^k \left\lfloor \frac{a_j}{p^i} \right\rfloor$$

ซึ่งเป็นจริงจาก $1 + \left\lfloor \frac{n-1}{p^i} \right\rfloor \geq \left\lfloor \frac{n}{p^i} \right\rfloor$ และ triangle inequality of floor function □

Theorem (primitive roots)

ให้ p เป็นจำนวนเฉพาะ จะมีจำนวนเต็ม g เรียกว่า **primitive root** ซึ่ง order ของ g ใน modulo p เท่ากับ $p-1$

Order ของ a ใน modulo $p = k$ หมายถึงจำนวนเฉพาะที่เล็กที่สุดที่ $a^k \equiv 1 \pmod{p}$

Example 1.4

ให้ $p \geq 2$ เป็นจำนวนเฉพาะ จงหาค่า k ทั้งหมดซึ่ง $S_k = 1^k + 2^k + \dots + (p-1)^k$ หารด้วย p ลงตัว

Proof. ให้ g เป็น primitive root ใน modulo p
จะได้ $\{1^k, 2^k, \dots, (p-1)^k\} = \{g^{1k}, g^{2k}, \dots, g^{(p-1)k}\}$ ใน modulo p
ในกรณี $p-1 \mid k$ จะได้ $S_k \equiv -1 \pmod{p}$
ในกรณี $p-1 \nmid k$ จะได้

$$\begin{aligned} S_k &\equiv g^{1k} + g^{2k} + \dots + g^{(p-1)k} \pmod{p} \\ &\equiv \frac{g^k(g^{k(p-1)} - 1)}{g^k - 1} \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

ทุก $k \in \mathbb{N}$ โดยที่ $p-1 \nmid k$ จะสอดคล้องกับที่โจทย์ต้องการ □

Example 1.5

ให้ $p \geq 3$ เป็นจำนวนเฉพาะ นิยาม

$$F(p) = \sum_{k=1}^{\frac{p-1}{2}} k^{120}, f(p) = \frac{1}{2} - \left\{ \frac{F(p)}{p} \right\} \text{ โดยที่ } x = x - [x]$$

จงหาค่าของ $f(p)$

Proof. จาก $i^2 \equiv (p-i)^2 \pmod{p}$ ดังนั้น $2F(p) \equiv 1^{120} + 2^{120} + \dots + (p-1)^{120} \pmod{p}$

จากข้อก่อนหน้าจะได้ $2F(p) \equiv \begin{cases} 0, & \text{if } p-1 \nmid 120 \\ p-1, & \text{otherwise} \end{cases}$ และ $\left\{ \frac{F(p)}{p} \right\} = \frac{F(p) \pmod{p}}{p}$

นั่นคือ $f(p) = \begin{cases} \frac{1}{2} & \text{if } p-1 \nmid 120 \\ \frac{1}{2} + \frac{1}{p}(2^{-1}(-1) \pmod{p}) & \text{otherwise} \end{cases}$

□

Example 1.6

ให้ $p \geq 3$ เป็นจำนวนเฉพาะ จงหาฟังก์ชัน $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ทั้งหมดซึ่ง สำหรับแต่ละ $m, n \in \mathbb{Z}$
 1. ถ้า $m \equiv n \pmod{p}$ แล้ว $f(m) = f(n)$ 2. $f(mn) = f(m)f(n)$

Proof. ให้ g เป็น primitive root ใน modulo p พิจารณา $f(0) = f(0)^2$

ดังนั้น $f(0) = 1$ หรือ $f(0) = 0$

กรณี $f(0) = 1$, $f(0) = f(n)f(0)$ จะได้ $f(n) = 1$ ทุก $n \in \mathbb{Z}$

กรณี $f(0) = 0$ พิจารณา $f(1) = f(1)^2$ ดังนั้น $f(1) = 1$ หรือ $f(1) = 0$

กรณี $f(1) = 0$ จะได้ $f(g)^{p-1} = f(1) = 0$ ดังนั้น $f(n) = 0$ ทุก $n \in \mathbb{Z}$

กรณี $f(1) = 1$ จะได้ $f(g)^{p-1} = 1$ นั่นคือ $f(g) = 1$ หรือ $f(g) = -1$ ถ้า $f(g) = 1$ จะได้ $f(n) = 1$ ทุก $n \in \mathbb{Z}/\{0\}$ ถ้า $f(g) = -1$ จะได้ $f(n) = (-1)^k$ เมื่อ $g^k \equiv n \pmod{p}$

□

Example 1.7

จงหาจำนวนเฉพาะ p ทั้งหมด ที่ทำให้ $\binom{100}{p} + 7$ หารด้วย p ลงตัว

Proof. พิจารณา ในกรณี $p \mid \binom{100}{p}$ จะได้ $p = 7$ ในกรณี $p \nmid \binom{100}{p}$ แสดงได้ไม่ยากว่า $50 < p < 100$

พิจารณา $\binom{100}{p} = \frac{100 \cdot 99 \cdot \dots \cdot p \cdot \dots \cdot (100 - (p-1))}{p(p-1)!} = \frac{S}{(p-1)!}$ สังเกตว่าเดิม S' ประกอบด้วย $\{100, 99, \dots, (100 -$

$(p-1)\} = \{0, 1, 2, \dots, p-1\}$ ใน \pmod{p} การตัด p ออกเหมือนเป็นการเอา ศูนย์ออกจะได้ S

ประกอบด้วย $\{1, 2, 3, \dots, p-1\}$ นั่นคือ $S \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}$ จาก Wilson's theorem

จะได้ $\binom{100}{p}((p-1)!) \equiv S \equiv -1 \pmod{p}$ จาก Wilson's theorem อีกรอบได้ $\binom{100}{p} + 7 \equiv 8$

\pmod{p} ดังนั้น $p = 7$

□

Example 1.8

จงหาจำนวนเต็มบวก N ทั้งหมดที่มีตัวประกอบเฉพาะอย่างน้อยสองจำนวนและ N มีค่าเท่ากับผลบวกของกำลังสองของตัวหารบวกที่มีค่าน้อยที่สุด 4 จำนวนแรก

Proof. ให้ตัวที่น้อยที่สุด 4 อันดับแรกเป็น $1, d_1, d_2, d_3$ โดย $1 < d_1 < d_2 < d_3$ และ $1^2 + d_1^2 + d_2^2 + d_3^2 = N$ พิจารณา $\pmod{2}$ สมมติ $2 \nmid N$ จะได้ $d_1^2 + d_2^2 + d_3^2 \equiv 0 \pmod{2}$ ขัดแย้ง ดังนั้น $2 \mid N$ เราจะได้ $d_1 = 2$ ต่อไป จะแสดง $4 \nmid N$ สมมติ $4 \mid N$ จะได้ $1^2 + 2^2 + d_2^2 + d_3^2 \equiv 0 \pmod{4}$ ซึ่งเป็นไปไม่ได้ ดังนั้น $2 \parallel N$ ต่อไปพิจารณา $\pmod{4}$ อีกครั้งจะได้ ซึ่งจะได้ d_2, d_3 ต้องมีตัวใดตัวหนึ่งหาร 2 เห็นได้ชัดว่า $d_2 = p$ บางจำนวนเฉพาะ p และ $d_3 = 2p$ จากโจทย์เขียนใหม่ได้เป็น $1^2 + 2^2 + p^2 + (2p)^2 = N$ จัดรูปจะได้ $5(p^2 + 1) = N$ ในกรณี $p = 3$ เห็นได้ชัดว่าเป็นไปไม่ได้ดังนั้น $p = 5$ จะได้ $N = 130$ ซึ่งตรวจสอบได้ไม่ยากว่าสอดคล้อง \square

Example 1.9

ให้ a และ b เป็นจำนวนเต็ม และ p เป็นจำนวนเฉพาะ สำหรับแต่ละจำนวนนับ k ใดๆ กำหนด $A_k = \{n \in \mathbb{N} : p^k \mid a^n - b^n\}$ จงแสดงว่าถ้า $A_1 \neq \emptyset$ แล้ว $A_k \neq \emptyset$ สำหรับทุก จำนวนนับ k

Proof. จากโจทย์เพียงพอที่จะแสดงทุก k จะมี n ซึ่ง $p^k \mid a^n - b^n$ จะพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ ให้ $P(n)$ แทนข้อความ $p^n \mid a^n - b^n$ เมื่อ n เป็นจำนวนนับ

ขั้นฐาน $P(1)$ จริงโดยกำหนด

ขั้นอุปนัย สมมติ $P(n)$ จริงเมื่อ $n \geq 1$ จะแสดง $P(n+1)$ เป็นจริง พิจารณา

$$a^{p^{n+1}} - b^{p^{n+1}} = (a^{p^n} - b^{p^n})(a^{p^n(p-1)} + a^{p^n(p-2)}b^{p^n} + \dots + b^{p^n(p-1)}) = (a^{p^n} - b^{p^n})(S)$$

เพียงพอที่จะแสดง $p \mid S$ และจากโจทย์กำหนดจะได้ $a \equiv b \pmod{p}$

$$S \equiv pa^{p^n(p-1)} \equiv 0 \pmod{p}$$

ดังนั้น $P(n+1)$ เป็นจริง จากหลักอุปนัยเชิงคณิตศาสตร์สรุปได้ว่า $P(n)$ เป็นจริงทุก $n \in \mathbb{Z}$ \square

Example 1.10

ให้ p เป็นจำนวนเฉพาะคี่ จงหาเศษจากการหาร $\sum_{k=0}^p k!(p-k)!$ ด้วย p

Proof.

$$\begin{aligned} k! &\equiv (-1)^{k-1}(-1)(-2) \dots (-(k-1))k \pmod{p} \\ &\equiv (-1)^{k-1}(p-1)(p-2) \dots (p-(k-1))k \pmod{p} \\ k!(p-k)! &\equiv k(-1)^{k-1}(p-1)! \pmod{p} \\ &\equiv k(-1)^k \pmod{p} \text{ จาก Wilson's theorem} \end{aligned}$$

$$\text{ดังนั้น } \sum_{k=0}^p k!(p-k)! \equiv \sum_{k=0}^p k(-1)^k \equiv \frac{p-1}{2} \pmod{p} \quad \square$$

Example 1.11

จงหา (a, b, c) ของจำนวนเต็มบวกทั้งหมดซึ่ง $(1 + \frac{1}{a})(1 + \frac{1}{b})(1 + \frac{1}{c}) = 2$

Proof. โดยไม่เสียสัณให้ $a \geq b \geq c$ สมมติ $c \geq 4$ ซึ่งจะได้ $2 > \frac{125}{64} \geq (1 + \frac{1}{a})(1 + \frac{1}{b})(1 + \frac{1}{c})$ ซึ่งเป็นไปไม่ได้ ดังนั้น $3 \geq c$ ต่อไปเราจะพิจารณา $c = 1, 2, 3$ ตามลำดับ

กรณี $c = 1$ จะได้ $(1 + \frac{1}{a})(1 + \frac{1}{b}) > 1$ ซึ่งเป็นไปไม่ได้

กรณี $c = 2$ จะได้ $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{4}{3}$ จัดรูปใหม่ได้ $(a-3)(b-3) = 12$ ซึ่งแยกกรณีหา a, b ได้ไม่ยาก

กรณี $c = 3$ จะได้ $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{3}{2}$ จัดรูปใหม่ได้ $(a-2)(b-2) = 3$ ซึ่งแยกกรณีหา a, b ได้ไม่ยาก

□

Example 1.12

จงหาจำนวนสองหลัก $n = 10a + b$ โดยที่ $a, b \in \{0, 1, 2, \dots, 9\}$ ซึ่ง ทุกจำนวนเต็ม k $n | k^a - k^b$

Proof. โอเคในการทำข้อนี้คือพิจารณาจำนวนเฉพาะที่หาร n แล้วเลือก k ที่เป็น primitive root ของจำนวนเฉพาะที่หาร n ลงตัว เห็นได้ชัดว่าถ้า $a = b$ จะเป็นจริงหมด ดังนั้นจะพิจารณา $a \neq b$ ถ้า a, b มีตัวใดตัวหนึ่งเป็นศูนย์เราสามารถเลือก $k = n$ เพื่อหาข้อขัดแย้งได้ยกเว้นกรณี $n = 1$ ดังนั้น n จะเป็นเลขสองหลักสมมติ n มีตัวประกอบจำนวนเฉพาะที่ ≥ 11 เลือก $k = g$ ซึ่งเป็น primitive root ของ p จะได้ $p | g^{\min\{a,b\}}(g^{|a-b|} - 1)$ ได้ $p | g^{|a-b|} - 1$ แต่ $|a-b| \leq 9$ ซึ่งขัดแย้งเพราะ $p-1$ จะต้องหาร $|a-b|$ ดังนั้น n จะต้องประกอบด้วยจำนวนเฉพาะ 2, 3, 5, 7 และมี 2 หลัก และถ้า p เป็นตัวประกอบของ n $p-1$ จะต้องหาร $|a-b|$ ซึ่งสามารถไล่กรณีได้ไม่ยาก

□

Example 1.13

กำหนดให้ x_1, x_2, \dots, x_k เป็นจำนวนเต็มซึ่ง $x_1 + x_2 + \dots + x_k = 1492$ จงแสดงว่า

$$x_1^7 + x_2^7 + \dots + x_k^7 \neq 1998$$

Proof. พิสูจน์ได้ไม่ยากว่า $x^7 \equiv x \pmod{3}$ ทุก $x \in \mathbb{Z}$

$$x_1 + x_2 + \dots + x_k \equiv x_1^7 + x_2^7 + \dots + x_k^7 \pmod{3}$$

ดังนั้น

$$x_1^7 + x_2^7 + \dots + x_k^7 \equiv 1492 \equiv 1 \pmod{3}$$

แต่ $1998 \equiv 0 \pmod{3}$ ดังนั้น $x_1^7 + x_2^7 + \dots + x_k^7 \neq 1998$

□

Example 1.14

กำหนดให้ $p_1 < p_2 < \dots < p_{31}$ เป็นจำนวนเฉพาะ ถ้า 30 หาร $p_1^4 + p_2^4 + \dots + p_{31}^4$ ลงตัว จงแสดงว่ามี k ซึ่ง p_k, p_{k+1}, p_{k+2} เป็นจำนวนเฉพาะที่เรียงติดกัน

Proof. ข้อนี้นี้เพียงพอที่จะแสดงว่า 2, 3, 5 อยู่ในอันดับ p_i สมมติไม่มี 2 ในลำดับ a_i จะได้ $p_i^4 \equiv 1 \pmod{2}$ จะได้ $\sum_{i=1}^{31} p_i^4 \equiv 1 \pmod{2}$ ซึ่งขัดแย้งกับที่โจทย์กำหนดดังนั้นมี 2 ในลำดับ ในทำนองเดียวกันกับ $\pmod{3}$ และ $\pmod{5}$ จะได้ 2, 3, 5 อยู่ในลำดับ p_i \square

Example 1.15

จงหาจำนวนเฉพาะ p ทั้งหมดที่ทำให้ $2p^2 - 3p - 1$ เป็นกำลังสามของจำนวนเต็มบวก

Proof. (TMO 2014) ให้ เห็นได้ชัดว่า $p = 2, 3$ สอดคล้องสมมติ $p \neq 2, 3$ ให้ $x^3 = 2p^2 - 3p - 1$ จัดรูปได้ $(x+1)(x^2-x+1) = p(2p-3)$ แสดงได้ไม่ยากว่า $\gcd(x+1, x^2-x+1) = \gcd(p, 2p-3) = 1$ และ $p > x$ เมื่อ $p > 3$

กรณี $p|x+1$ จะได้ $p \leq x+1$ ดังนั้น $p = x+1$ แทนค่ากลับได้ $p = 2, 3$ ขัดแย้ง

กรณี $p|x^2 - x + 1$ จะได้ $x+1|2p-3$ ได้ $2p-3 = (x+1)k$ แทนค่ากลับจะได้ $pk = x^2 - x + 1$ พิจารณา $\pmod{x+1}$ จะได้ $2p \equiv 3 \pmod{x+1}$ และ $x^2 - x + 1 \equiv 3 \equiv pk \pmod{x+1}$ ดังนั้น $2p \equiv pk \pmod{x+1} + 1$ นั่นคือ $x+1|k-2$ ถ้า $k = 2$ แทนค่ากลับแก้สมการแล้วจะขัดแย้ง ดังนั้น $x+1 \leq k-2$ และจาก $x+1 \leq p$ จะได้ $x^2 - x + 1 = pk \geq (x+1)(x+3)$ ขัดแย้ง \square

Example 1.16

จงหาพหุนาม $P(x)$ ทั้งหมดที่มีสัมประสิทธิ์เป็นจำนวนเต็ม ซึ่ง $2557^n + 213 \cdot 2014$ หารด้วย $P(n)$ ลงตัว สำหรับแต่ละจำนวนเต็มบวก n

Proof. (TMO 2014) ในกรณี $P(x)$ เป็นพหุนามคงตัวสามารถแก้หา $P(x)$ ได้ไม่ยากเราจะพิจารณา $P(x)$ ไม่เป็นพหุนามคงตัวแสดงได้ไม่ยากกว่าจะมีจำนวนเฉพาะ q ซึ่ง $q \neq 2557, q \nmid 2556$ และ $q|P(n_0)$ จะได้ $q|P(n_0+rp)$ สำหรับ r เป็นจำนวนเต็มใดๆ ดังนั้น $q|2557^{n_0} + 213 \cdot 2014$ และ $q|2557^{n_0+rp} + 213 \cdot 2014$ จะได้ $q|2557^{rp} - 1$ จาก Fermat's little theorem จะได้ $q|2557^{q-1} - 1$ จะได้ $q|2557^r - 1$ เลือก $r = 1$ จะได้ $q|2556$ ขัดแย้ง \square

Example 1.17

ให้ p เป็นจำนวนเฉพาะที่อยู่ในรูป $4k+3$ เมื่อ k เป็นจำนวนเต็มบวกหรือศูนย์ ถ้า m และ n เป็นจำนวนเต็มซึ่ง $p|m^2+n^2$ แล้ว $p^2|m^2+n^2$

Proof. ข้อนี้นี้เพียงพอที่จะแสดง $p|n$ และ $p|m$ สมมติ $p \nmid n$ เพื่อหาข้อขัดแย้งจะได้ $p \nmid n$ ด้วยดังนั้น $(m^{-1}n)^2 \equiv -1 \pmod{p}$ ให้ g เป็น primitive root ของ p จะมี $a \in \mathbb{N}$ ซึ่ง $g^a \equiv m^{-1}n \pmod{p}$ ดังนั้น $((g^a)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ ซึ่งได้ $1 \equiv -1 \pmod{p}$ ขัดแย้ง \square

Example 1.18

จงแสดงว่าไม่มีคู่อันดับ (x, y) ของจำนวนเต็ม ที่สอดคล้องกับสมการ $2560x^2 + 5x + 6 = y^5$

Proof. (TMO 2017)

$$5(512x^2 + 5x + 5 + 5) = (y-1)(y^4 + y^3 + y^2 + y + 1)$$

แสดงได้ไม่ยากว่า $y \equiv 1 \pmod{5}$ ทำให้ได้ $y^4 + y^3 + y^2 + y + 1 \equiv 5 \equiv 0 \pmod{5}$ ดังนั้น $5^2 \mid y^5 - 1$ พิจารณา $\pmod{5}$ จะได้ $512x^2 + 5x + 5 + 5 \not\equiv 0 \pmod{5}$ ดังนั้นขัดแย้ง \square

Example 1.19

สำหรับจำนวนเต็มบวก n กำหนดให้ $S(n)$ แทนผลรวมของเลขโดดใน n จงหาจำนวนเฉพาะ p ทั้งหมดซึ่ง $S(p^{p+2}) = S((p+2)^p)$

Proof. ถ้า $p = 2$ เห็นชัดว่าจริงจะพิจารณากรณีอื่น จาก $S(p^{p+2}) = S((p+2)^p)$ พิจารณา $\pmod{3}$ จะได้ $p^{p+2} \equiv (p+2)^p \pmod{3}$ แสดงได้ไม่ยากว่า $p \neq 3$ กรณี $p \equiv 1 \pmod{3}$ ได้ $p+2 \equiv 0 \pmod{3}$ ซึ่งเป็นไปไม่ได้ที่ $p^{p+2} \equiv (p+2)^p \pmod{3}$ ต่อไปจะพิจารณากรณี $p \equiv 2 \pmod{3}$ จะได้ $p+2 \equiv 1 \pmod{3}$ จะได้ $p^{p+2} \equiv 2 \pmod{3}$ และ $(p+2)^p \equiv 1 \pmod{3}$ ซึ่งขัดแย้ง \square

§2 Combinatorics

Example 2.1

ให้ $a_1 \leq a_2 \leq \dots \leq a_n = m$ เป็นจำนวนเต็มบวก ให้ b_k เป็นจำนวนของ a_i ซึ่ง $a_i \geq k$ จงแสดงว่า

$$a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_m$$

Example 2.2

กำหนดให้ $A = \{2010, 2011, 2012, \dots, 2553\}$ ให้หาจำนวนสมาชิกใน A ที่หารด้วยจำนวนเฉพาะน้อยกว่า 10 ลงตัว

Example 2.3

กระทรวงศึกษาธิการจัดกิจกรรมโดยสุ่มเลือกนักเรียน ชั้น ม.1 จำนวน 2010 คนจาก 5 ภูมิภาคทั่วประเทศ เพื่อให้นักเรียนคูใด ๆ เลือกถกปัญหาาร่วมกันจำนวน 1 หัวข้อ จากปัญหา 3 หัวข้อคือ ปัญหาด้านการเมือง ปัญหาด้านเศรษฐกิจ และปัญหาด้านสังคม ให้แสดงว่าจะมีนักเรียน 3 คนซึ่งเกิดเดือนเดียวกัน เป็นเพศเดียวกัน มาจากภูมิภาคเดียวกัน และนักเรียนทุก ๆ คนใน 3 คนนี้เลือกถกปัญหาร่วมกันในหัวข้อเดียวกันหมด

Example 2.4

ให้ (V, E) เป็นกราฟจงแสดงว่า

$$\sum_{v \in V} \deg(v)^2 = \sum_{xy \in E} (\deg(x) + \deg(y))$$

Example 2.5

ในบางบริษัท ลูกจ้างแต่ละคนจะทำงานแค่ 10 วันต่อเดือนเท่านั้น นอกจากนี้ ทุกๆ ลูกจ้าง 3 คน จะมีวันที่ทำงานร่วมกัน 1 วันเท่านั้น จงแสดงว่าบริษัทมีลูกจ้างอย่างมาก 19 คนเท่านั้น (สมมติให้ 1 เดือนมี 30 วัน)

Example 2.6

กำหนดให้ n จุดต่างกันบนระนาบหนึ่ง จงแสดงว่ามีน้อยกว่า $2n^{3/2}$ คู่อันดับซึ่งห่างกัน 1 หน่วย

Example 2.7

ในโรงละครสัตว์มีตัวตลก n คนโดยแต่งตัวและทาสีตัวเองโดยใช้สีต่างกัน 12 สีต่างกัน ตัวตลกแต่ละคนต้องการอย่างน้อย 5 สี วันหนึ่ง หัวหน้าละครสัตว์ออกคำสั่งให้ไม่มีตัวตลก 2 คนใด ๆ มีสีชุดเดียวกัน และไม่มี สีใดๆ ที่มีตัวตลกใช้อย่างน้อย 20 คน จงหาจำนวนตัวตลกที่มากที่สุดที่ทำให้คำสั่งของหัวหน้าละครสัตว์เป็นไปได้