บทที่ 3

ทฤษฎีเบื้องต้น

(THEORETICAL BACKGROUND)

3.1 สมการไดโอแฟนไทน์ (Diophantine Equation)

สมการไดโอแฟนไทน์ ตั้งขึ้นตามชื่อของนักคณิตศาสตร์ชาวกรีก ชื่อ ดีฟานโตส แห่งอะเล็กซานเดรีย และชื่อสมการไดโอแฟนไทน์นี้ถูกนำไปใช้เรียกสมการที่มีตัวแปรหนึ่งตัวหรือมากกว่าหนึ่งตัวและผลเฉลยเป็นจำนวนเต็มว่า สมการไดโอแฟนไทน์

3.2 ผลเฉลยของสมการไดโอแฟนไทน์ (Solution of Diophantine Equation)

เราเรียกจำนวนเต็มที่แทนค่าตัวแปรในสมการไดโอแฟนไทน์แล้วทำให้สมการนั้นเป็นจริงว่าผลเฉลย เรียกผลเฉลยที่ประกอบด้วยตัวคงค่าเลือกที่เป็นจำนวนเต็ม (integral arbitrary constant) ว่าผลเฉลยทั่วไป (general solution) และเรียกผลเฉลยที่มีค่าเป็นจำนวนเต็มที่แน่นอนหรือผลเฉลยที่ได้จากการแทนค่าของตัวคงค่าเลือกในผลเฉลยทั่วไปว่า ผลเฉลยเฉพาะ (particular solution)

3.3 ตัวอย่างสมการไดโอแฟนไทน์

1) $2x + y = 5$

2) $2x + 3y + 4z = 1$

3) $x^2 - 2y^2 = 1$

ซึ่งเราสนใจเฉพาะผลเฉลยที่ x, y, z เป็นจำนวนเต็ม

3.4 ทฤษฎีบท สมการไดโอแฟนไทน์ $ax + by = c$ จะมีผลเฉลยก็ต่อเมื่อ $(a,b)|c$ และถ้า (x_0, y_0) เป็นผลเฉลยหนึ่ง แล้วผลเฉลยทั้งหมดจะอยู่ใน

$$x = x_0 + \frac{b}{(a,b)}t$$

$$y = y_0 - \frac{a}{(a,b)}t$$

เมื่อ t เป็นจำนวนเต็มใด ๆ

3.5 ตัวอย่างการหาผลเฉลยสมการไดโอแฟนไทน์

1) สมการ $7x+16y=5$

หา ห.ร.ม. ของ 7 กับ 16 ด้วย ขั้นตอนของยูคลิด

$$16=7(2)+2$$
$$7=2(3)+1$$
$$2=1(2)$$

ทำย้อนกลับกระบวนการของยูคลิด

$$\begin{aligned}1&=7(1)-2(3)\\&=7(1)-(16-7\cdot 2)(3)\\&=7(7)-16(3)\end{aligned}$$

ดังนั้น $(7,16)=1$

เนื่องจาก $(7,16)|5$ สมการนี้จึงมีผลเฉลยนอกจากนี้

$$5=7(35)+16(-15)$$

จึงมี $x_0=35$ และ $y_0=-15$ ซึ่ง $7(x_0)+16(y_0)=5$

ดังนั้นผลเฉลยทั่วไปอยู่ในรูป

$$x=x_0+\frac{b}{(a,b)}t=35+16t$$
$$y=y_0-\frac{a}{(a,b)}t=-15-7t$$

2) ต้องการแลกเงิน 1000 บาท เป็นธนบัตรใบละ 20 บาท และธนบัตรใบละ 50 บาท จะแลกได้แตกต่างกัน ทั้งหมดกี่แบบ

ต้องการหาผลเฉลยของ $20x+50y=1000$

โดยที่ $x, y \in \{0,1,2,\ldots\}$

นั้นคือ $2x+5y=100$

เนื่องจาก $(2,5)|100$ สมการนี้จึงมีผลเฉลย

$$2(0)+5(20)=100$$

จึงได้ผลเฉลย $x_0=0$ และ $y_0=20$ เป็นผลเฉลยหนึ่งดังนั้น

$$x=0+5t$$
$$y=20-2t$$

แต่ $y \geq 0$ และ $t \leq 10$ ดังนั้นมีค่า t ที่เป็นไปได้ 11 ค่า คือ $t=0,1,\ldots,10$

จะได้ $(x,y)=(0,20),(5,18),(10,16),\ldots,(50,0)$

3.6 คอนกรูเอนซ์

ให้ n เป็นจำนวนเต็ม สำหรับจำนวนเต็ม a และ b เรากล่าวว่า a คอนกรูเอนซ์กับ b มอดุโล n ซึ่งเขียนแทนด้วย $a \equiv b \pmod{n}$ ก็ต่อเมื่อ n หาร $a-b$ ลงตัว และถ้า n หาร $a-b$ ไม่ลงตัว เราจะกล่าวว่า a ไม่คอนกรูเอนซ์กับ b มอดุโล n ซึ่งเขียนแทนด้วยสัญลักษณ์ $a \not\equiv b \pmod{n}$ ในที่นี้เรียกจำนวนเต็มบวก n ว่า มอดุลัส (modulus)

3.7 ทฤษฎีบท สำหรับจำนวนเต็ม a, b และจำนวนเต็มบวก n จะได้ว่า

1) $a \equiv b \pmod{n}$ ก็ต่อเมื่อ $n|(a-b)$

2) $a \not\equiv b \pmod{n}$ ก็ต่อเมื่อ $n \not| (a-b)$

3) $a \equiv b \pmod{1}$ และ $a \equiv a \pmod{n}$

3.8 ทฤษฎีบท สำหรับจำนวนเต็ม a และ b ใดๆ $a \equiv b \pmod{n}$ ก็ต่อเมื่อ a และ b มีเศษที่เหลือจากการหารด้วย n เท่ากัน

3.9 สมบัติของคอนกรูเอนซ์

กำหนดให้ $n \in N$ และ $a, b, c, d \in Z$ จะได้ว่า

1) ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
2) ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$
3) ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้ว $a + c \equiv b + d \pmod{n}$ และ $ac \equiv bd \pmod{n}$
4) ถ้า $a \equiv b \pmod{n}$ แล้ว $a^k \equiv b^k \pmod{n}$ สำหรับจำนวนเต็มบวก k

หมายเหตุ
1) $a \equiv a \pmod{n}$
2) ถ้า $a \equiv b \pmod{n}$ แล้ว $b \equiv a \pmod{n}$
3) ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$ แล้ว $a \equiv c \pmod{n}$

3.10 ทฤษฎีบท ให้ $a \in Z$ และ $n \in N$ จะมี $r \in Z$ ซึ่ง $0 \le r < n$ เพียงค่าเดียวที่ทำให้ $a \equiv r \pmod{n}$

จากทฤษฎีบทข้างต้น จะได้ว่า

1) ถ้า $r_1, r_2 \in \{0, 1, 2, \ldots, n-1\}$ โดยที่ $r_1 \equiv r_2 \pmod{n}$ แล้ว $r_1 = r_2$
2) สมาชิกในเซต $\{0, 1, 2, \ldots, n-1\}$ ที่ต่างกัน จะไม่คอนกรูเอ็นซ์กันในมอดุโล n
3) ทุกๆจำนวนเต็ม a จะมี $r \in \{0, 1, \ldots, n-1\}$ เพียงค่าเดียวที่ทำให้ $a \equiv r \pmod{n}$ และ ค่า r คือ เศษเหลือจากการหาร a ด้วย n

3.11 ทฤษฎีบท ให้ $a,b,n \in Z$ โดยที่ $n>0$ และ $(a,n)=d$ จะได้ว่า **สมการคอนกรูเอนซ์เชิงเส้น** (linear congruence equation) $ax \equiv b \pmod{n}$ มีคำตอบ $x \in Z$ ก็ต่อเมื่อ $d \mid b$

3.12 บทแทรก ถ้า $(a,n)=1$ แล้วสมการคอนกรูเอนซ์เชิงเส้น $ax \equiv b \pmod{n}$ มีคำตอบเพียงคำตอบเดียว กล่าวคือ ถ้า x_1 และ x_2 เป็นคำตอบของสมการ $ax \equiv b \pmod{n}$ แล้ว $x_1 \equiv x_2 \pmod{n}$

3.13 Catalan's conjecture

สำหรับจำนวนเต็ม $a>1, b>1, x>1, y>1$ ผลเฉลยของสมการ $a^x - b^y = 1$ จะมีเพียงผลเฉลยเดียวคือ $a = y = 3$ and $b = x = 2$.