บทที่ 2
ความรู้พื้นฐาน

ในบทนี้จะกล่าวถึงนิยามและทฤษฎีของจำนวนจริง เพื่อเป็นการทบทวนเฉพาะที่จะนำไปใช้ในการพิสูจน์คุณสมบัติของจำนวนฟิโบนักชี ตลอดถึงการนำไปช่วยในการพิสูจน์ทฤษฎีเกี่ยวกับการหาค่าจำนวนเฉพาะค่าใหญ่ ๆ

ในตอนแรกจะกล่าวถึงนิยามและทฤษฎีของการหาร การหาตัวหารร่วมมาก ต่อด้วยคอนกรูเอนซ์และซีเควนส์ของจำนวนเต็มบวก

ซึ่งในบทนี้ทฤษฎีบางทฤษฎีที่มีในหนังสือทั่วไปที่สามารถหาอ่านได้ง่าย จะเว้นการพิสูจน์ไว้ โดยบอกหนังสือที่ผู้สนใจสามารถหาอ่านได้

สัญลักษณ์.- ให้ I แทนเซตของจำนวนเต็ม

<u>นิยาม 2.1</u> ให้ $a,b \in I$ ที่ $b \neq 0$ จะกล่าวว่า b หาร a ลงตัว (b divides a) ซึ่งแทนด้วย $b \mid a$ ก็ต่อเมื่อมี $c \in I$ ที่ทำให้ $a = cb$

เราเรียก c และ b ว่าเป็นตัวหารของ a (divisor of a)

<u>หมายเหตุ</u> ถ้า b หาร a ไม่ลงตัว จะเขียนแทนด้วย $b \nmid a$

<u>ทฤษฎี 2.1</u> ถ้า $a, b, d \in I$ ซึ่ง $d \mid a$ และ $d \mid b$ แล้ว $d \mid ax + dy$ สำหรับทุก ๆ $x, y \in I$

<u>พิสูจน์</u> จากนิยาม 2.1 ถ้า $d \mid a$ แล้วจะมี $c \in I$ ที่ $a = cd$

ดังนั้น $ax = cdx$ ทุก ๆ $x \in I$

จากนิยาม 2.1 ถ้า $d \mid b$ แล้วจะมี $e \in I$ ที่ $b = ed$

ดังนั้น $by = edy$ ทุก ๆ $y \in I$

เพราะฉะนั้น $ax + by = cd\,x + edy$

$= d(cx + ey)$

เนื่องจาก $x, y, c, e \in I$ ดังนั้น $cx + ey \in I$

นั่นคือ $d \mid ax + by$.

<u>ทฤษฎี 2.2</u> ถ้า $a, b \in I$ และ $b \mid a$ แล้ว $b \mid xa$ สำหรับทุก ๆ $x \in I$

<u>พิสูจน์</u> จากนิยาม 2.1 ถ้า $b \mid a$ แล้วจะมี $c \in I$ ที่ $a = cb$

ดังนั้น $ax = cbx = bcx$ ทุก ๆ $x \in I$

เนื่องจาก $c, x \in I$ ดังนั้น $cx \in I$

นั่นคือ $b \mid xa$

<u>นิยาม 2.2</u> สำหรับทุก ๆ $a, b, d \in I$ ที่ a และ b ไม่เป็นศูนย์ พร้อมกัน จะเรียก d ว่าเป็นตัวหารร่วมมาก (greatest common divisor) หรือ ห.ร.ม.ของ a และ b ซึ่งแทนด้วย $d = (a,b)$ ก็ต่อเมื่อ

1) $d > 0$

2) $d \mid a$ และ $d \mid b$

และ 3) สำหรับทุก ๆ $c \in I$ ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \mid d$

<u>หมายเหตุ</u> 1) $(a, b) \geq 1$ สำหรับ $a, b \in I$

2) $(0,0)$ ไม่นิยาม

3) $(0,x) = |x|$ สำหรับทุก ๆ $x \in I$ และ $x \neq 0$

4) $(a,b) = (-a,b) = (a,-b) = (-a,-b)$

<u>ทฤษฎี 2.3</u> (Euclidean algorithm)

สำหรับทุก ๆ $a,b \in I$ ที่ $b > 0$ จะมี $q,r \in I$ เพียงคู่หนึ่งและคู่เดียวเท่านั้นที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

<u>ทฤษฎี 2.4</u> สำหรับทุก ๆ $a,b \in I$ ที่ a,b ไม่เป็นศูนย์พร้อม ๆ กันจะมี $d \in I$, $d > 0$ เพียงตัวหนึ่งและตัวเดียวเท่านั้นที่ $(a,b) = d$

<u>พิสูจน์</u> โดยหมายเหตุข้อ 4 หลังนิยาม 2.2 จะได้ $(a,b) = (a,-b)$ ดังนั้นในการพิสูจน์ จะพิสูจน์เฉพาะกรณีที่ $b > 0$ ดังนี้

จากทฤษฎี 2.3 จะได้สำหรับทุก ๆ $a,b \in I$ จะมีเพียงแต่ละคู่ของ q_i, r_i เมื่อ $i = 1,2,3,\ldots$ ที่

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$$

$$b = r_1q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{k-2} = r_{k-1}q_k + r_k \quad , \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1}$$

เนื่องจาก $b > r_1 > r_2 > \ldots$ จะมี r_k ซึ่งทำให้ $r_k \mid r_{k-1}$, โดยทฤษฎี 2.1 จะได้ $r_k \mid r_{k-2}$, $r_k \mid r_{k-3}$, $r_k \mid r_{k-4}$, ..., $r_k \mid b$ และ $r_k \mid a$

สำหรับ $d_1 \in I$ ที่ $d_1 \mid a$ และ $d_1 \mid b$ และโดยทฤษฎี 2.1 จะได้ $d_1 \mid r_1$ (จากสมการที่ 1)

และ $d_1 \mid r_2$ (จากสมการที่ 2)

.....

$d_1 \mid r_k$ (จากสมการสุดท้าย)

โดยนิยาม 2.2 จะได้ $r_k = (a,b)$

นั่นคือมี $d = r_k \in I$ และ $d > 0$ ที่ $d = (a,b)$

สมมุติว่ามี $d' \in I$ ที่ $d' = (a,b)$

โดยนิยาม 2.2 ข้อ 2 จะได้ $d' \mid a$ และ $d' \mid b$

และจาก $d = (a,b)$ โดยนิยาม 2.2 ข้อ 3 จะได้ $d' \mid d$

จาก $d \mid a$ และ $d \mid b$ และให้ $d' = (a,b)$

โดยนิยาม 2.2 ข้อ 3 จะได้ $d \mid d'$

ดังนั้น $d' = d = r_k$

นั่นคือจะมี $d \in I$, $d > 0$ เพียงตัวหนึ่งและตัวเดียวเท่านั้น

ที่ $d = (a,b)$

<u>ทฤษฎี 2.5</u> สำหรับทุก $a,b,c \in I$, $(a,b) \mid (a,bc)$

<u>พิสูจน์</u> ให้ $(a,b) = d$

โดยนิยาม 2.2 ข้อ 2 จะได้ $d \mid a$ และ $d \mid b$

โดยทฤษฎี 2.2 จะได้ว่า $d \mid bc$ สำหรับทุก ๆ $c \in I$,

ถ้าให้ $(a,bc) = e$

โดยนิยาม 2.2 ข้อ 2 จะได้ $e \mid a$ และ $e \mid bc$

และโดยนิยาม 2.2 ข้อ 3 จะได้ว่า $d \mid e$

นั่นคือ $(a,b) \mid (a,bc)$

<u>ทฤษฎี 2.6</u> สำหรับทุก ๆ $a,b,c \in I$, $(ac,bc) = (a,b)c$

<u>พิสูจน์</u> จากทฤษฎี 2.3 จะได้

$$a = bq_1 + r_1 , \quad 0 < r_1 < b$$

$$b = r_1q_2 + r_2 , \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 , \quad 0 < r_3 < r_2$$

$$\cdots\cdots\cdots\cdots$$

$$r_{k-2} = r_{k-1}q_k + r_k , \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k\, q_{k+1}$$

โดยทฤษฎี 2.4 จะได้ $r_k = (a,b)$

สำหรับทุก ๆ $c \in I$, $ac = bq_1c + r_1c$

$$bc = r_1cq_2 + r_2c$$

$$r_1c = r_2cq_3 + r_3c$$

$$\cdots\cdots\cdots\cdots$$

$$r_{k-1}c = r_kcq_{k+1}$$

โดยวิธีเดียวกับทฤษฎี 2.4 จะได้ $r_kc = (ac,bc)$

นั่นคือ $(a,b)c = (ac,bc)$

<u>ทฤษฎี 2.7</u> สำหรับทุก ๆ $a,b,c \in I$ ถ้า $(a,c) = 1$ แล้ว $(a,bc) = (a,b)$

<u>พิสูจน์</u> ให้ $(a,bc) = e$

โดยนิยาม 2.2 ข้อ 2 จะได้ $e \mid a$ และ $e \mid bc$

โดยทฤษฎี 2.2 จะได้ $e \mid ab$ ทุก ๆ $b \in I$

ให้ $(ab,bc) = t$

โดยนิยาม 2.2 ข้อ 2 จะได้ $t \mid ab$ และ $t \mid bc$

และโดยนิยาม 2.2 ข้อ 3 จะได้ $e \mid t$

ดังนั้น $(a,bc) \mid (ab,bc)$

จากทฤษฎี 2.6 จะได้ $(ab,bc) = (a,c)b$

เนื่องจาก $(a,c) = 1$

ดังนั้น $(ab,bc) = 1 \quad (b) = b$

เพราะฉะนั้น $(a,bc) \mid b$

และเนื่องจาก $(a,bc) \mid a$

โดยนิยาม 2.2 ข้อ 2 จะได้ $(a,b) \mid a$ และ $(a,b) \mid b$

และโดยนิยาม 2.2 ข้อ 3 จะได้ $(a,bc) \mid (a,b)$ .....(1)

โดยทฤษฎี 2.5 จะได้ $(a,b) \mid (a,bc)$ .....(2)

จาก(1) และ (2) จะได้ $(a,bc) = (a,b)$

นั่นคือ ถ้า $(a,c) = 1$ แล้ว $(a,bc) = (a,b)$

<u>ทฤษฎี 2.8</u> สำหรับทุก ๆ $a,b \in I$ และ $(a,b) = b$ ก็ต่อเมื่อ $b \mid a$

<u>พิสูจน์</u> ถ้า $(a,b) = b$ โดยนิยาม 2.2 ข้อ 2 จะได้ $b \mid a$

โดยนิยาม 2.2 ถ้า $b \mid a$ และสำหรับทุก ๆ $d \in I$ ที่ $d \mid b$, $d \mid a$ จะได้ $(a,b) = b$

นั่นคือ $(a,b) = b$ ก็ต่อเมื่อ $b \mid a$

<u>ทฤษฎี 2.9</u> สำหรับทุก ๆ $a,b,c \in I$ ถ้า $b \mid c$ แล้ว

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

<u>พิสูจน์</u> จากทฤษฎี 2.3 สามารถนำมาเขียนต่อไปได้ว่า

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$$

$$b = r_1q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{k-2} = r_{k-1}q_k + r_k \quad , \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_k$$

และโดยผลจากทฤษฎี 2.4 จะได้ $r_k = (a,b)$

จาก $b \mid c$ โดยนิยาม 2.1 จะมี $t \in I$ ที่ $c = tb$

และจากสมการแรก จะได้

$$a + c = bq_1 + tb + r_1$$

$$= b(q_1 + t) + r_1 \quad , \quad 0 < r_1 < b$$

และจะได้ $b = r_1q_2 + r_2 \quad , \quad 0 < r_2 < r_1$

$$r_1 = r_2q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{k-1} = r_kq_k$$

ทำนองเดียวกับตอนแรกจะได้ $r_k = (a + c,b)$

นั่นคือ $(a,b) = (a + c,b)$

นิยาม 2.3 จำนวนเต็มบวก p จะเรียกว่าจำนวนเฉพาะ (prime number) ก็ต่อเมื่อ

1) $p > 1$ และ

2) p มีตัวหารคือ ± 1 และ $\pm p$ เท่านั้น

นิยาม 2.4 จำนวนเต็มที่มากกว่า 1 และไม่ใช่จำนวนเฉพาะจะเรียกว่าจำนวนประกอบ (composite number)

ทฤษฎี 2.10 ถ้า m เป็นจำนวนประกอบแล้ว m สามารถเขียนได้ในรูป $m = p_1 p_2 p_3 \cdots$ เมื่อ p_i , $i = 1,2,3,\ldots$ เป็นจำนวนเฉพาะได้เพียงชุดหนึ่งและชุดเดียวเท่านั้น

การพิสูจน์ทฤษฎี 2.10 หาอ่านได้จากหนังสือ " Elementary Theory of Number" ของ Harriet Griffin.

นิยาม 2.5 สำหรับทุก ๆ $a \in I$ จะเรียกว่าจำนวนคู่ (even number) ก็ต่อเมื่อ $a = 2m$, ทุก ๆ $m \in I$
และจำนวนเต็มที่ไม่ใช่จำนวนคู่เรียกว่าจำนวนคี่ (odd number)

นิยาม 2.6 สำหรับทุก ๆ $a,b,m \in I$ ที่ $m > 0$ จะเรียกว่า a คอนกรูเอนซ์ b มอดูโล m (a congruence to b modulo m) ซึ่งแทนด้วย $a \equiv b \pmod m$ ก็ต่อเมื่อ $m \mid (a-b)$

ต่อไปนี้จะกล่าวถึงทฤษฎีของคอนกรูเอนซ์ ซึ่งนำมาใช้ในการพิสูจน์ทฤษฎีในบทต่อไป สำหรับผู้ที่สนใจการพิสูจน์ทฤษฎีเหล่านี้สามารถหาอ่านได้จากหนังสือที่ได้บอกไว้หลังทฤษฎีต่าง ๆ นี้

ทฤษฎี 2.11 ถ้า $a \equiv b \pmod m$ แล้ว สำหรับทุก ๆ $c \in I$

$$ac \equiv bc \pmod m$$

<u>ทฤษฎี 2.12</u> ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$
แล้ว $a \pm c \equiv b \pm d \pmod{m}$

<u>ทฤษฎี 2.13</u> ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$
แล้ว $ac \equiv bd \pmod{m}$

<u>ทฤษฎี 2.14</u> ถ้า $ac \equiv bc \pmod{m}$ และ $(c,m) = 1$
แล้ว $a \equiv b \pmod{m}$

<u>หมายเหตุ</u> การพิสูจน์ทฤษฎี 2.11 ถึงทฤษฎี 2.14 หาอ่านได้จากหนังสือ " Elementary Theory of Numbers" โดย William J. Leveque.

<u>ทฤษฎี 2.15</u> ถ้า $m = m_1 m_2 m_3 \cdots m_s$ และ $a \equiv b \pmod{m}$
แล้ว $a \equiv b \pmod{m_1}$
$a \equiv b \pmod{m_2}$
$a \equiv b \pmod{m_3}$
.....
$a \equiv b \pmod{m_s}$

<u>ทฤษฎี 2.16</u> ถ้า $a \equiv b \pmod{m}$ แล้วสำหรับทุก ๆ จำนวนเต็มบวก n, $a^n \equiv b^n \pmod{m}$

การพิสูจน์ทฤษฎี 2.15 และ 2.16 หาอ่านได้จากหนังสือ " Elementary Theory of Number" ของ Harriet Griffin.

<u>ทฤษฎี 2.17</u> ถ้า p เป็นจำนวนเฉพาะ และ $p \nmid a$ แล้ว

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

<u>ทฤษฎี 2.18</u> ถ้า p เป็นจำนวนเฉพาะ แล้ว

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

การพิสูจน์ทฤษฎี 2.17 และ 2.18 หาอ่านได้จากหนังสือ " The Theory of Algebraic Numbers" โดย Harry Polland

<u>ทฤษฎี 2.19</u> ถ้า q เป็นจำนวนเฉพาะที่ $q \equiv \pm 2 \pmod{5}$ แล้ว

$$5^{\frac{1}{2}(q-1)} \equiv -1 \pmod{q}$$

การพิสูจน์อ่านได้จากหนังสือ " An Introduction to the Theory of Number, Fourth Edition โดย G.H. Hardy and E.M. Wright.

<u>สัญลักษณ์</u> ให้ λ แทนจำนวนจริง $\frac{c + d\sqrt{5}}{2}$ เมื่อ $c,d \in I$

และให้ $\bar{\lambda}$ แทน $\frac{c - d\sqrt{5}}{2}$

ดังนั้น $\lambda\bar{\lambda} = (\frac{c + d\sqrt{5}}{2})(\frac{c - d\sqrt{5}}{2}) = \frac{c^2 - 5d^2}{4}$

<u>ตัวอย่าง</u> ถ้า $\lambda = \frac{1 + \sqrt{5}}{2}$ และ $\bar{\lambda} = \frac{1 - \sqrt{5}}{2}$

ดังนั้น $\lambda\bar{\lambda} = \frac{1 - 5}{4} = -1$

<u>ทฤษฎี 2.20</u> ถ้า q เป็นจำนวนเฉพาะในรูป $5m \pm 2$ เมื่อ $m \in I$

และ $m > 0$ แล้ว $\lambda^{q+1} \equiv \lambda\bar{\lambda} \pmod{q}$

<u>พิสูจน์</u> จาก $\lambda = \frac{c + d\sqrt{5}}{2}$ จะได้ $2\lambda = c + d\sqrt{5}$

ดังนั้น $(2\lambda)^q = (c + d\sqrt{5})^q$

โดยทฤษฎี 2.18 จะได้ $(c + d\sqrt{5})^q \equiv c^q + d^q\sqrt{5}^q \pmod{q}$

โดยทฤษฎี 2.17 จะได้

$$2^{q-1} \equiv 1 \pmod{q},\quad c^{q-1} \equiv 1 \pmod{q},\quad d^{q-1} \equiv 1 \pmod{q}$$

โดยทฤษฎี 2.11 จะได้

$$2^{q} \equiv 2 \pmod{q},\quad c^{q} \equiv c \pmod{q},\quad d^{q} \equiv d \pmod{q}$$

ดังนั้น $(2\lambda)^q \equiv 2\lambda^q \pmod{q}$

และ $(c + d\sqrt{5})^q \equiv c + d\,5^{\frac{1}{2}q} \pmod{q}$

ดังนั้น $2\lambda^q \equiv c + d\,5^{\frac{1}{2}q} \pmod{q}$

โดยทฤษฎี 2.19 จะได้ $5^{\frac{1}{2}(q-1)} \equiv -1 \pmod{q}$

โดยทฤษฎี 2.11 จะได้ $5^{\frac{1}{2}q} \equiv -5 \pmod{q}$

ดังนั้น $2\lambda^q \equiv c - d\sqrt{5} \pmod{q}$

จาก $2\bar{\lambda} = c - d\sqrt{5}$

จะได้ $2\lambda^q \equiv 2\bar{\lambda} \pmod{q}$

โดยทฤษฎี 2.14 จะได้ $\lambda^q \equiv \bar{\lambda} \pmod{q}$

โดยทฤษฎี 2.11 จะได้ $\lambda^{q+1} \equiv \lambda\bar{\lambda} \pmod{q}$

<u>นิยาม 2.7</u> ซีเควนส์ (Sequence)

ถ้า f เป็นฟังก์ชันบนเซตของจำนวนเต็มบวก โดยที่ $f(n) = u_n$, ทุก ๆ $n \in I$, $n > 0$ จะเรียก f ว่าเป็นซีเควนส์ ซึ่งเขียนแทนด้วย

$$u_1, u_2, u_3, \ldots, u_n, \ldots \quad \text{หรือ} \quad \{u_n\}$$

<u>ทฤษฎี 2.21</u> ถ้า $w_1', w_2', w_3', \ldots, w_n', \ldots$ และ $w_1'', w_2'', w_3'', \ldots, w_n'', \ldots$ เป็นซีเควนส์แล้ว

$$w_1' + w_1'',\ w_2' + w_2'',\ w_3' + w_3'', \ldots,\ w_n' + w_n'', \ldots$$

เป็นซีเควนส์ด้วย

<u>ทฤษฎี 2.22</u> ถ้า $w_1, w_2, w_3, \ldots, w_n, \ldots$ เป็นซีเควนส์ แล้ว

$cw_1, cw_2, cw_3, \ldots, cw_n, \ldots$ เมื่อ $c \in I$, $c > 0$

จะเป็นซีเควนส์ด้วย

<u>หมายเหตุ</u> สำหรับการพิสูจน์ทฤษฎี 2.21 และทฤษฎี 2.22 หาอ่านได้จากหนังสือ "A First Course in Mathematical Analysis" โดย J.C. Burkill.
