บทที่ 3

ตัวหารแบบยูนิแทรี

ในบทนี้จะเป็นการศึกษาบทความของ Leonard G. Swanson และ Rodney T. Hansen ซึ่งลงพิมพ์ในวารสาร Mathematics Magazine ปี 1979 ในหัวข้อ Unitary Divisor โดยการศึกษาจะแบ่งเป็นหัวข้อดังต่อไปนี้

3.1 นิยามของตัวหารแบบยูนิแทรี

3.2 เปรียบเทียบคุณสมบัติเบื้องต้นของการหารแบบยูนิแทรีและการหารแบบธรรมดา

3.3 คุณสมบัติของตัวหารแบบยูนิแทรี

3.4 นิยามของตัวหารแบบยูนิแทรีร่วมมาก

3.5 ความสัมพันธ์ของตัวหารแบบยูนิแทรีร่วมมากและตัวหารร่วมมาก

3.6 นิยามของจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี

3.1 นิยามของตัวหารแบบยูนิแทรี

นิยาม 3.1.1 ถ้า $n, d \in Z^+$ แล้วจะเรียก d ว่า ตัวหารแบบยูนิแทรีของ n ก็ต่อเมื่อ

ก. d/n และ

ข. $(d, \frac{n}{d}) = 1$

d เป็นตัวหารแบบยูนิแทรีของ n เขียนแทนด้วย $d/^*n$

และ d ไม่เป็นตัวหารแบบยูนิแทรีของ n เขียนแทนด้วย $d\not/^*n$

ตัวอย่าง 3.1.1 (แสดงการเป็นตัวหารแบบยูนิแทรี)

1. ให้ $n = 12$

จะได้ $d = 1, 3, 4, 12$ เป็นตัวหารแบบยูนิแทรีของ n

2. ให้ $n = 16$

จะได้ $d = 1, 16$ เป็นตัวหารแบบยูนิแทรีของ n □

3.2 เปรียบเทียบคุณสมบัติเบื้องต้นของการหารแบบยูนิแทรีและการหารแบบธรรมดา

ในหัวข้อนี้จะเป็นการเปรียบเทียบคุณสมบัติเบื้องต้นของการหารแบบยูนิแทรีและการหารแบบธรรมดา ซึ่งจะเริ่มจากทฤษฎีดังต่อไปนี้

ทฤษฎี 3.2.1 (คุณสมบัติเบื้องต้นของการหารแบบยูนิแทรีที่เหมือนกับการหารแบบธรรมดา)

ถ้า $a, b, c \in Z^+$ แล้ว

ก. $a/^*a$

ข. $1/^*a$

ค. ถ้า $a/^*b$ แล้ว $\frac{b}{a}/^*b$

ง. ถ้า $a/^*b$ แล้ว $a \leq b$

จ. ถ้า $a/^*b$ และ $b/^*a$ แล้ว $a = b$

ฉ. ถ้า $a/^*b$ และ $b/^*c$ แล้ว $a/^*c$

ช. ถ้า $ab/^*ac$ แล้ว $b/^*c$

ซ. ถ้า p เป็นจำนวนเฉพาะและ $p/^*ab$ แล้ว $p/^*a$ หรือ $p/^*b$

พิสูจน์ ก. พิจารณา $a \in Z^+$ โดยทฤษฎี 2.2.1 (ก) จะได้

$$a/a \text{ ----------(1)}$$

พิจารณา $(a, \frac{a}{a})$ โดยทฤษฎี 2.3.3 (ก) และนิยาม 2.2.3 จะได้

$$(a, \tfrac{a}{a}) = (a, 1) = 1 \text{ ----------(2)}$$

จาก (1) และ (2) โดยนิยาม 3.1.1 จึงได้

$$a /^* a$$ □

พิสูจน์ ข. พิจารณา $a \in Z^+$ โดยทฤษฎี 2.2.1 (ข) จะได้

$$1/a \text{ ----------(1)}$$

พิจารณา $(1, \frac{a}{1})$ โดยนิยาม 2.2.3 จะได้

$$(1, \tfrac{a}{1}) = (1, a) = 1 \text{ ----------(2)}$$

จาก (1) และ (2) โดยนิยาม 3.1.1 จึงได้

$$1 /^* a$$ □

พิสูจน์ ค. จากกำหนดให้ $a /^* b$ โดยนิยาม 3.1.1 จึงได้

$$a/b \text{ และ } (a, \tfrac{b}{a}) = 1 \text{ ---------(1)}$$

จาก (1) a/b โดยนิยาม 2.2.1 จะได้ว่ามี $c \in Z^+$ ซึ่ง

$b = ac$ จะได้ $c = \frac{b}{a}$ และ $a = \frac{b}{c}$ --(2)

จาก (1) และ (2) โดยทฤษฎี 2.2.1 (ค) จะได้

$$c/b \text{ ----------(3)}$$

จาก (1) $(a, \frac{b}{a}) = 1$ และจาก (2) $c = \frac{b}{a}$ จะได้

$(a, \frac{b}{a}) = (a, c) = 1$ พิจารณา $(c, \frac{b}{c})$

จาก (2) $a = \frac{b}{c}$ จะได้ $(c, \frac{b}{c}) = (c, a) = (a, c)$

นั่นคือ

$$(c, \frac{b}{c}) = 1 \quad \text{----------(4)}$$

จาก (3) และ (4) โดยนิยาม 3.1.1 จึงได้

$c /^* b$ นั่นคือ $\frac{b}{a} /^* b$ □

พิสูจน์ ง. จากกำหนดให้ $a /^* b$ โดยนิยาม 3.1.1 จะได้

$$a/b \quad \text{----------(1)}$$

จาก (1) และทฤษฎี 2.2.1 (ฉ) จึงได้

$$a \leq b$$

พิสูจน์ จ. จากกำหนดให้ $a /^* b$ โดยทฤษฎี 3.2.1 (ง) จะได้

$$a \leq b \quad \text{----------(1)}$$

จากกำหนดให้ $b /^* a$ โดยทฤษฎี 3.2.1 (ง) จะได้

$$b \leq a \quad \text{----------(2)}$$

จาก (1) และ (2) จึงได้ $a = b$ □

<u>พิสูจน์</u> ฉ. จากกำหนดให้ $a/^{*}b$ โดยนิยาม 3.1.1 จึงได้

$$a/b \quad \text{และ} \quad (a, \frac{b}{a}) = 1 \text{ -------(1)}$$

จากกำหนดให้ $b/^{*}c$ โดยนิยาม 3.1.1 จึงได้

$$b/c \quad \text{และ} \quad (b, \frac{c}{b}) = 1 \text{ -------(2)}$$

จาก (1) a/b และ (2) b/c โดยทฤษฎี 2.2.1 (จ) จะได้

$$a/c \text{ ----------(3)}$$

จาก (1) a/b โดยนิยาม 2.2.1 จะมี $m \in Z^{+}$ ที่ทำให้

$$b = am \text{ จะได้ } m = \frac{b}{a} \text{ ----------(4)}$$

จาก (2) b/c โดยนิยาม 2.2.1 จะมี $n \in Z^{+}$ ที่ทำให้

$$c = bn \text{ จะได้ } n = \frac{c}{b} \text{ ----------(5)}$$

จาก (1) $(a, \frac{b}{a}) = 1$ และ (4) จะได้ว่า

$$(a, \frac{b}{a}) = (a, m) = 1 \text{ ----------(6)}$$

จาก (2) $(b, \frac{c}{b}) = 1$ และ (4), (5) จะได้

$$(b, \frac{c}{b}) = (b, n) = (am, n) = 1 \text{ ---(7)}$$

จาก (7) และทฤษฎี 2.2.8 จึงได้

$$(a, n) = 1 \text{ ----------(8)}$$

จาก (6) และ (8) โดยทฤษฎี 2.2.9 จึงได้

$(a,mn) = 1$ ----------(9)

จาก (4), (5) และ (9) โดยทฤษฎี 2.3.3 (ก) จึงได้

$$(a, \frac{c}{a}) = (a, \frac{cb}{ba}) = (a, \frac{bnm}{b}) = (a, mn)$$

$$= 1 \text{ ----------(10)}$$

จาก (3) และ(10) โดยนิยาม 3.1.1 จึงได้

$a/^{*}c$ □

พิสูจน์ ช. จากกำหนดให้ $ab/^{*}ac$ โดยนิยาม 3.1.1 จึงได้

ab/ac และ $(ab, \frac{ac}{ab}) = 1$ ----------(1)

จาก (1) ab/ac โดยทฤษฎี 2.2.1 (ช) จึงได้

b/c ----------(2)

จาก (1) $(ab, \frac{ac}{ab}) = 1$ พิจารณาร่วมกับทฤษฎี 2.3.3(ก) จะได้

$(ab, \frac{ac}{ab}) = (ab, \frac{c}{b}) = 1$ ----------(3)

จาก (3) และโดยทฤษฎี 2.2.8 จะได้

$(b, \frac{c}{b}) = 1$ ----------(4)

จาก (2) และ (4) โดยนิยาม 3.1.1 จึงได้

$b/^{*}c$ □

พิสูจน์ ซ. จากกำหนดให้ $p/^*ab$ โดยนิยาม 3.1.1 จึงได้

$$p/ab \text{ และ } (p, \frac{ab}{p}) = 1 \text{ ----------(1)}$$

จาก (1) p/ab โดยที่ p เป็นจำนวนเฉพาะ โดยทฤษฎี 2.2.12 จึงได้

$$p/a \text{ หรือ } p/b \text{ ----------(2)}$$

จาก (1) $(p, \frac{ab}{p}) = 1$ และจาก (2) ถ้า p/a โดยทฤษฎี 2.2.8 จะได้

$$(p, \frac{a}{p}) = 1 \text{ ----------(3)}$$

หรือจาก (1) $(p, \frac{ab}{p}) = 1$ และ (2) ถ้า p/b โดยทฤษฎี 2.2.8 จะได้

$$(p, \frac{b}{p}) = 1 \text{ ----------(4)}$$

จาก (2), (3) และ (4) โดยนิยาม 3.1.1 จึงได้

$$p/^*a \text{ หรือ } p/^*b$$ □

ทฤษฎี 3.2.2 (คุณสมบัติเบื้องต้นของการหารแบบยูนิแทรีที่แตกต่างกับการหารแบบธรรมดา)

ถ้า $a, b, c \in Z^+$ โดยที่ $a \geq 2$ และ $a/^*b$, $a/^*c$ แล้วจะมี $x, y \in Z^+$ ซึ่งทำให้ $a/^*(bx + cy)$

ข. ถ้า $a, b \in Z^+$ ซึ่ง $a \neq b$ และ $a \not/^* b$ แล้วจะมี $m \in Z^+$ โดยที่ $m > 1$ ซึ่งทำให้ $am \not/^* bm$

<u>พิสูจน์</u> ก. จากกำหนดให้ $a \in Z^+$ โดยที่ $a \geq 2$ พิจารณา a^2 จะได้

$$a^2 \in Z^+ \text{ ----------(1)}$$

พิจารณา $(a, \frac{ba^2 + ca^2}{a}) = (a, \frac{a^2(b+c)}{a})$

โดยทฤษฎี 2.3.2 จะได้

$$(a, \frac{a^2(b+c)}{a}) = (a, a(b+c) = a \text{ ----(2)}$$

จาก (2) และ $a \geq 2$ โดยนิยาม 3.1.1 จึงได้

$$a \not/^* (ba^2 + ca^2) \text{ ----------(3)}$$

จาก (1), (3) และให้ $x = y = a^2$ จะได้ว่ามี $x, y \in Z^+$ ซึ่ง

$$a \not/^* (bx + cy)$$ □

<u>พิสูจน์</u> ข. จากกำหนดให้ $a/^* b$ โดยนิยาม 3.1.1 จึงได้

$$a/b \text{ ----------(1)}$$

จาก (1) โดยนิยาม 2.2.1 จะมี $c \in Z^+$ โดยที่ $c = \frac{b}{a}$ นั่นคือ $\frac{b}{a} \in Z^+$ และจากกำหนดให้ $a \neq b$ จึงได้

$$\frac{b}{a} > 1 \text{ ----------(2)}$$

จาก (1) โดยทฤษฎี 2.2.1 (ฌ) จะได้ $a \cdot \frac{b}{a} / b \cdot \frac{b}{a}$

โดยทฤษฎี 2.3.3 (ก) จะได้ $a \cdot \frac{b}{a} = b$ และโดยทฤษฎี 2.3.1 (ก) จะได้ $b \cdot \frac{b}{a} = \frac{b^2}{a}$ นั่นคือ

$$a \cdot \frac{b}{a} / b \cdot \frac{b}{a} \text{ จะได้ } b / \frac{b^2}{a} \quad \text{-----(3)}$$

พิจารณา $(b, \frac{b^2}{ab})$ จาก (2) และทฤษฎี 2.3.2 จะได้

$$(b, \frac{b^2}{ab}) = (b, \frac{b}{a}) = \frac{b}{a} > 1 \quad \text{----------(4)}$$

จาก (3), (4) และนิยาม 3.1.1 จึงได้ $b \not/^* \frac{b^2}{a}$

โดยทฤษฎี 2.3.3 (ก) และนิยาม 2.3.1 จึงได้

$$a \cdot \frac{b}{a} \not/^* b \cdot \frac{b}{a} \quad \text{----------(5)}$$

จาก (5) ให้ $m = \frac{b}{a}$ จะได้ว่า $m \in Z^+$ โดยที่ $m > 1$ ซึ่ง

$am \not/^* bm$ □

3.3 คุณสมบัติของตัวหารแบบยูนิแทรี

ในหัวข้อนี้จะศึกษาคุณสมบัติของตัวหารแบบยูนิแทรีของจำนวนเต็มบวกที่เป็นจำนวนเฉพาะและจำนวนเต็มบวกที่เป็นผลคูณของจำนวนเฉพาะที่แตกต่างกัน ซึ่งการแสดงคุณสมบัติดังกล่าวจะเริ่มจากตัวอย่างและทฤษฎีดังต่อไปนี้

ตัวอย่าง 3.3.1 พิจารณา 2, 3, 5, 17 จะพบว่า

ตัวหารแบบยูนิแทรีของ 2 ได้แก่ 1, 2
ตัวหารแบบยูนิแทรีของ 3 ได้แก่ 1, 3
ตัวหารแบบยูนิแทรีของ 5 ได้แก่ 1, 5
ตัวหารแบบยูนิแทรีของ 17 ได้แก่ 1, 17 □

ตัวอย่าง 3.3.2 พิจารณา 6, 15, 30 จะพบว่า

ตัวหารแบบยูนิแทรีของ 6 ได้แก่ 1, 2, 3, 6
ตัวหารแบบยูนิแทรีของ 15 ได้แก่ 1, 3, 5, 15
ตัวหารแบบยูนิแทรีของ 30 ได้แก่ 1, 2, 3, 5, 6, 10, 15, 30 □

จากตัวอย่างข้างต้นทำให้ได้ข้อสังเกตซึ่งพิสูจน์ได้ตามทฤษฎีต่อไปนี้

ทฤษฎี 3.3.1 ถ้า p เป็นจำนวนเฉพาะแล้ว ตัวหารแบบยูนิแทรีของ p จะมีเพียง 2 ตัว คือ 1 และ p

พิสูจน์ จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยนิยาม 2.2.4 จะได้ว่ามีจำนวนเต็มบวกเพียง 2 ตัวเท่านั้นที่หาร p ลงตัว คือ 1 และ p และโดยทฤษฎี 3.2.1 ข้อ ก. และ ข. จะได้ $1/^{*}p$ และ $p/^{*}p$ นั่นคือ

จำนวนตัวหารแบบยูนิแทรีของ p มีเพียง 1 และ p □

<u>ทฤษฎี 3.3.2</u> ถ้า $m, a_i, d \in Z^+$ โดยที่ $i = 1, 2, \ldots, m$

และ $p_1, p_2, \ldots, p_m$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ

$a = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ และ d/a แล้ว $(d, \frac{a}{d}) = 1$

ก็ต่อเมื่อ $d = p_1^{d_1} p_2^{d_2} \ldots p_m^{d_m}$ โดยที่ $d_i = 0, a_i$

<u>พิสูจน์</u> <---) ให้ S(m) แทนข้อความ "ถ้า $d = p_1^{d_1} p_2^{d_2} \ldots p_m^{d_m}$

โดยที่ $d_i = 0, a_i$ และ $a = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ โดยที่ $m, a_i \in Z^+$,

$i = 1, 2, \ldots, m$ และ p_i เป็นจำนวนเฉพาะที่แตกต่างกันแล้ว $(d, \frac{a}{d}) = 1$

(ก) พิจารณา S(1) ถ้า $a = p_1^{a_1}$ และ $d = p_1^0, p_1^{a_1}$ ------(1)

ถ้า $d = p_1^0$ จะได้ $(d, \frac{a}{p}) = (1, \frac{p_1^{a_1}}{1}) = (1, p_1^{a_1}) = 1$

ถ้า $d = p_1^{a_1}$ จะได้ $(d, \frac{a}{d}) = (p_1^{a_1}, \frac{p_1^{a_1}}{a_1})$ โดยทฤษฎี 2.3.3 (ก)

จึงได้ $(p_1^{a_1}, \frac{p_1^{a_1}}{a_1}) = (p_1^{a_1}, 1) = p_1^1 = 1$ ----------(2)

จาก (1) และ (2) จะได้ S(1) เป็นจริง

(ข) ให้ S(k) เป็นจริง นั่นคือ ถ้า $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$

และ $d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$ โดยที่ $d_i = 0, a_i$

แล้ว $(d, \frac{a}{d}) = 1$

(ค) พิจารณา $S(k+1)$ จะได้ $a = p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}$

และ $d = p_1^{d_1} p_2^{d_2} \ldots p_{k+1}^{d_{k+1}}$

โดยที่ $d_i = 0, a_i$ และ $i = 1, 2, \ldots, k+1$

พิจารณาค่า d จาก $d_i = 0, a_i$

จะได้ $d_{k+1} = 0, a_{k+1}$

ดังนั้น

$$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{0}, \; p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}} \quad --(1)$$

พิจารณา $\left(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{0}, \dfrac{p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{0}}\right)$

$$= \left(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}}\right)$$

จาก (ข) จะได้

$$\left(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}}\right) = 1 \quad ----(2)$$

พิจารณา $\left(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, p_{k+1}^{a_{k+1}}\right)$ จากกำหนดให้ p_i แตกต่างกันทั้งหมด

จะได้ $\left(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, p_{k+1}^{a_{k+1}}\right) = 1 \quad -------(3)$

จาก (2) และ (3) โดยทฤษฎี 2.2.9 จะได้

$$(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}}) = 1 \quad \text{-----(4)}$$

พิจารณา

$$(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}}})$$

โดยทฤษฎี 2.3.3 (ก)

จะได้

$$(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_{k+1}^{a_{k+1}}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}}})$$

$$= (p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} p_{k+1}^{a_{k+1}}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}})$$

จาก (ข) จะได้

$$(p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}}) = 1 \quad \text{----(5)}$$

พิจารณา $(p_{k+1}^{a_{k+1}}, \frac{p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}}{p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}})$

จากกำหนดให้ p_i เป็นจำนวนเฉพาะที่แตกต่างกันทั้งหมด

ดังนั้นจะได้

$$\left(p_{k+1}^{a_{k+1}}\ ,\ \frac{p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}{p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}}\right) = 1 \quad \text{----------(6)}$$

จาก (5), (6) และโดยทฤษฎี 2.2.9 จึงได้

$$\left(p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}p_{k+1}^{a_{k+1}}\ ,\ \frac{p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}{p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}}\right) = 1 \quad \text{---(7)}$$

จาก (1), (4) และ (7) จึงได้ $(d, \frac{a}{d}) = 1$

นั่นคือ $S(k+1)$ เป็นจริง

จาก (ก), (ข) และ (ค) โดยทฤษฎี 2.6.2 จึงได้ว่า

$(d, \frac{a}{d}) = 1$ เมื่อ d และ a นิยามตามกำหนดให้ □

<u>พิสูจน์</u> --->) จากกำหนดให้ d/a โดยทฤษฎี 2.4.2 จะได้

$$d = p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m} \quad \text{โดยที่}$$

$$0 \le d_i \le a_i \quad \text{----------(1)}$$

ถ้ามี $k \in Z^+$ โดยที่ $1 \le k \le m$ ที่ทำให้ $0 < d_k < a_k$

พิจารณา $(d, \frac{a}{d}) = \left(p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m}\ ,\ \frac{p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}}{p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m}}\right)$

โดยทฤษฎี 2.4.3 จึงได้

$$\left(p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m},\ \frac{p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}}{p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m}}\right) \geq p_k^{\min\{d_k,a_k-d_k\}} \quad \text{-----(2)}$$

จาก (2) พิจารณา d_k และ $a_k - d_k$ จาก $d_k > 0$

และจาก $d_k < a_k$ ดังนั้น $d_k \geq 1$ และ $a_k - d_k \geq 1$

จะได้

$$\min\{d_k,\ a_k - d_k\} \geq 1 \quad \text{----------(3)}$$

จาก (2) และ (3) จึงได้

$$\left(p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m},\ \frac{p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}}{p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m}}\right) \geq p_k > 1 \quad \text{------(4)}$$

นั่นคือ ถ้ามี $k \in Z^+$ โดยที่ $1 \leq k \leq m$

ที่ทำให้ $0 < d_k < a_k$ แล้ว $(d, \frac{a}{d}) > 1$ ขัดแย้งกับ

กำหนดให้ และจาก (1) จึงได้

$$d = p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m} \quad \text{โดยที่} \quad d_i = 0,\ a_i \ \square$$

<u>ทฤษฎี 3.3.3</u> ถ้า $a, k \in Z^+$ และ $p_1, p_2, \ldots, p_k$ เป็น

จำนวนเฉพาะที่แตกต่างกันและ $n = p_1p_2\cdots p_k$ และ a/n

แล้ว $a /^* n$

พิสูจน์ จากกำหนดให้ $n = p_1 p_2 \cdots p_k$ และ a/n

โดยทฤษฎี 2.4.2 จะได้

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{โดยที่} \quad a_i = 0, 1 \text{ -----(1)}$$

จาก (1) และโดยทฤษฎี 3.3.2 จะได้

$$(a, \frac{n}{a}) = 1 \text{ ----------(2)}$$

จากกำหนดให้ a/n และ (2) โดยนิยาม 3.1.1 จึงได้

$a/^* n$ □

3.4 **นิยามของตัวหารแบบยูนิแทรีร่วมมาก** (Greatest Common Unitary Divisor)

นิยาม 3.4.1 ตัวหารแบบยูนิแทรีร่วม (Common Unitary Divisor)

ถ้า $a, b, d \in Z^+$ แล้ว จะเรียก d ว่า ตัวหารแบบยูนิแทรีร่วมของ a และ b ก็ต่อเมื่อ $d/^* a$ และ $d/^* b$

<u>ทฤษฎี 3.4.1</u> ถ้า $a_i, b_i, k \in W$ โดยที่ $i = 1, 2, \ldots, k$ และ $k > 0$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ และ $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ แล้ว d จะเป็นตัวหารแบบยูนิแทรีร่วมของ a และ b ก็ต่อเมื่อ

$$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} \quad \text{โดยที่}$$

$d_i = 0, a_i$ ถ้า $a_i = b_i$

และ $d_i = 0$ ถ้า $a_i \neq b_i$

<u>พิสูจน์</u> --->) จากกำหนดให้ $d /^* a$ และ $d /^* b$ โดยนิยาม 3.1.1

จะได้ d/a และ $(d, \frac{a}{d}) = 1$ ----------(1)

และ d/b และ $(d, \frac{b}{d}) = 1$ ----------(2)

จาก (1) โดยทฤษฎี 3.3.2 จะได้

$$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} \quad \text{โดยที่}$$

$$d_i = 0, a_i \text{ ----------(3)}$$

จาก (2) โดยทฤษฎี 3.3.2 จะได้

$$d = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \quad \text{โดยที่} \quad e_i = 0, b_i \text{ --(4)}$$

จาก (3), (4) จะได้

$$d = p_1^{d_1} p_1^{d_2} \cdots p_k^{d_k} \quad \text{โดยที่}$$

$d_i = 0$, a_i ถ้า $a_i = b_i$

และ $d_i =$ 0 ถ้า $a_i \neq b_i$ □

พิสูจน์ <--) จากกำหนดให้และทฤษฎี 2.4.2 จะได้

d/a และ d/b ----------(1)

พิจารณา $(d, \frac{a}{d})$ และ $(d, \frac{b}{d})$

จากกำหนดให้และทฤษฎี 3.3.2 จะได้

$(d, \frac{a}{d}) = 1$ และ $(d, \frac{b}{d}) = 1$ ----------(2)

จาก (1) และ (2) และนิยาม 3.1.1 จะได้

$d /^* a$ และ $d /^* b$ □

ทฤษฎี 3.4.2 ถ้า $a, b \in Z^+$ แล้ว จะมี $d \in Z^+$ ซึ่ง

ก) $d /^* a$ และ $d /^* b$,

ข) ถ้า $c \in Z^+$ และ $c /^* a$, $c /^* b$ แล้ว $c \leq d$

พิสูจน์ พิจารณา $K = \{x \in Z^+ / x /^* a \text{ และ } x /^* b\}$

$A = \{1, 2, \ldots, \min\{a,b\}\}$

จะได้ A เป็นเซตจำกัด และ $K \subseteq A \subseteq Z^+$ โดยทฤษฎี 2.1.4.1 จะได้

K เป็นเซตจำกัด ----------(1)

จากทฤษฎี 3.2.1 (ข) จะได้ $1 /^* a$ และ $1 /^* b$

นั่นคือ $1 \in K$ จะได้

$K \neq \emptyset$ ----------(2)

จาก (1), (2) และทฤษฎี 2.6.1 จะได้ K มีสมาชิกที่มากที่สุด

ให้ d เป็นสมาชิกที่มากที่สุดของ K ----------(3)

จากนิยาม K และนิยาม 2.6.1 จะได้

$d /^* a$ และ $d /^* b$ ----------(4)

พิจารณา $c \in Z^+$ โดยที่ $c /^* a$ และ $c /^* b$ โดยนิยาม K จะได้ $c \in K$ จาก (3) และนิยาม 2.6.1 จึงได้

$c \leq d$

จาก (3), (4) และ (5) จะได้ผลของการพิสูจน์ □

นิยาม 3.4.2 ตัวหารแบบยูนิแทรีร่วมมาก (Greatest Common Unitary Divisor)

ถ้า $a, b, d \in Z^+$ จะเรียก d ว่า ตัวหารแบบยูนิแทรีร่วมมาก ของ a และ b ก็ต่อเมื่อ

ก. $d /^* a$ และ $d /^* b$,

ข. ถ้า $c \in Z^+$ โดยที่ $c /^* a$ และ $c /^* b$ แล้ว $c \leq d$

d เป็นตัวหารแบบยูนิแทรีร่วมมากของ a และ b เขียนแทนด้วย $d = (a, b)^*$

ตัวอย่างของตัวหารแบบยูนิแทรีร่วมมาก

ตัวอย่าง 3.4.1 พิจารณา 12, 15

ตัวหารแบบยูนิแทรีของ 12 คือ 1, 3, 4, 12
ตัวหารแบบยูนิแทรีของ 15 คือ 1, 3, 5, 12
จะได้ตัวหารแบบยูนิแทรีร่วมของ 12, 15 คือ 1, 3
นั่นคือ $(12, 15)^* = 3$ □

ตัวอย่าง 3.4.2 พิจารณา 7, 10

ตัวหารแบบยูนิแทรีของ 7 คือ 1, 7
ตัวหารแบบยูนิแทรีของ 10 คือ 1, 2, 5, 10
จะได้ตัวหารแบบยูนิแทรีร่วมของ 7, 10 คือ 1
นั่นคือ $(7, 10)^* = 1$ □

ตัวอย่าง 3.4.3 พิจารณา 12, 16

ตัวหารแบบยูนิแทรีของ 12 คือ 1, 3, 4, 12

ตัวหารแบบยูนิแทรีของ 16 คือ 1, 16

จะได้ตัวหารแบบยูนิแทรีร่วมของ 12, 16, คือ 1

นั่นคือ $(12, 16)^* = 1$ □

ทฤษฎี 3.4.3 ถ้า $a, b \in Z^+$ แล้ว $(a, b)^* = (b, a)^*$

พิสูจน์ เป็นผลจากนิยาม 3.4.2 □

ทฤษฎี 3.4.4 ถ้า $a_i, b_i, k \in W$ โดยที่ $i = 1, 2, \ldots, k$

และ $k > 0$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่

แตกต่างกัน และ $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$

แล้ว d จะเป็นตัวหารแบบยูนิแทรีร่วมมากของ a และ b

ก็ต่อเมื่อ

$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$ โดยที่ $d_i = a_i$ ถ้า $a_i = b_i$

และ $d_i = 0$ ถ้า $a_i \neq b_i$

<u>พิสูจน์</u> -->) จากกำหนดให้ $d = (a, b)^*$ โดยนิยาม 3.4.2 (ก)

จะได้

$$d/^* a \quad \text{และ} \quad d/^* b \qquad \text{----------(1)}$$

จาก (1) และทฤษฎี 3.4.1 จะได้

$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$ โดยที่ $d_i = 0, a_i$ ถ้า $a_i = b_i$

และ $d_i = 0$ ถ้า $a_i \neq b_i$

โดยนิยาม 3.4.2 (ข) จึงได้

$d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$ โดยที่ $d_i = a_i$ ถ้า $a_i = b_i$

และ $d_i = 0$ ถ้า $a_i \neq b_i$ □

<u>พิสูจน์</u> <--) จากกำหนดให้และทฤษฎี 3.4.1 จะได้

$$d/^* a \quad \text{และ} \quad d/^* b \qquad \text{----------(1)}$$

พิจารณา $c \in Z^+$ โดยที่ $c/^* a$ และ $c/^* b$

โดยทฤษฎี 3.4.1 จะได้

$c = p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}$ โดยที่ $c_i = 0, a_i$ ถ้า $a_i = b_i$

และ $c_i = 0$ ถ้า $a_i \neq b_i$ ---(2)

จากกำหนดให้ และ (2) จึงได้

$c \leq d$ ----------(3)

จาก (1) และ (3) จึงได้

$d = (a, b)^*$ □

<u>ทฤษฎี 3.4.5</u> ถ้า $a, b, d \in Z^+$ แล้ว $d = (a, b)^*$ ก็ต่อเมื่อ

ก. $d /^* a$ และ $d /^* b$,

ข. ถ้า $c \in Z^+$ โดยที่ $c /^* a$ และ $c /^* b$ แล้ว $c /^* d$

<u>พิสูจน์</u> $\rightarrow$) จากกำหนดให้ $d = (a, b)^*$ โดยนิยาม 3.4.2 จึงได้

$d /^* a$ และ $d /^* b$ ----------(1)

พิจารณา $c \in Z^+$ โดยที่ $c /^* a$ และ $c /^* b$

ให้ $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ และ $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

โดยที่ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน

และ $k, a_i, b_i \in W$ และ $k > 0, i = 1, 2, \ldots, k$

โดยทฤษฎี 3.4.1 จะได้

$c = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$ โดยที่ $c_i = 0, a_i$ ถ้า $a_i = b_i$

และ $c_i = 0$ ถ้า $a_i \neq b_i$--(2)

จาก $d = (a, b)^*$ โดยทฤษฎี 3.4.4 จะได้

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \quad \text{โดยที่} \quad d_i = a_i \text{ ถ้า } a_i = b_i$$
$$\text{และ} \quad d_i = 0 \text{ ถ้า } a_i \neq b_i \text{--(3)}$$

จาก (2), (3) โดยทฤษฎี 2.4.2 จะได้

$$c/d \text{ ----------(4)}$$

จาก (2), (4) โดยทฤษฎี 3.3.2 จะได้

$$(c, \frac{d}{c}) = 1 \text{ ----------(5)}$$

จาก (4), (5) และนิยาม 3.1.1 จะได้

$$c /\!\!^* d \text{ ----------(6)}$$

จาก (1), (2) และ (6) จะได้ผลของการพิสูจน์ □

<u>พิสูจน์</u> <--) จาก (ก) $d \in Z^+$ และ $d /\!\!^* a$, $d /\!\!^* b$ พิจารณา $c \in Z^+$

โดยที่ $c /\!\!^* a$ และ $c /\!\!^* b$ โดยข้อ (ข) จะได้

$$c /\!\!^* d \text{ ----------(1)}$$

จาก (1) โดยทฤษฎี 3.2.1 (ง) จะได้

$$c \leq d \text{ ----------(2)}$$

จากกำหนดให้ (ก) และ (2) โดยนิยาม 3.4.2 จึงได้

$$d = (a, b)^* \quad \square$$

3.5 ความสัมพันธ์ของตัวหารแบบยูนิแทรีร่วมมากและตัวหารร่วมมาก

ในหัวข้อนี้จะศึกษาความสัมพันธ์ของตัวหารแบบยูนิแทรีร่วมมากและตัวหารร่วมมาก ซึ่งเริ่มจากตัวอย่างและทฤษฎีต่อไปนี้

ตัวอย่าง 3.5.1 พิจารณา 12, 15

จากตัวอย่าง 3.4.1 จะได้ $(12, 15)^* = 3$

และจาก $(12, 15) = 3$

จะพบว่า $(12, 15)^* = (12, 15)$ □

ตัวอย่าง 3.5.2 พิจารณา 7, 10

จากตัวอย่าง 3.4.2 จะได้ $(7, 10)^* = 1$

และจาก $(7, 10) = 1$

จะพบว่า $(7, 10)^* = (7, 10)$ □

ตัวอย่าง 3.5.3 พิจารณา 12, 16

จากตัวอย่าง 3.4.3 จะได้ $(12, 16)^* = 1$

และจาก $(12, 16) = 4$

จะพบว่า $(12, 16)^* < (12, 16)$ □

จากตัวอย่างทำให้ได้ข้อสังเกตซึ่งแสดงโดยทฤษฎีต่อไปนี้

ทฤษฎี 3.5.1 ถ้า $a, b \in \mathbb{Z}^+$ แล้ว $(a, b)^* \leq (a, b)$

<u>พิสูจน์</u> จากกำหนดให้ $a, b \in Z^+$ จะได้ $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$

และ $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ โดยที่ $a_i, b_i, k \in W$

ซึ่ง $i = 1, 2, \ldots, k$ และ $k > 0$ และ $p_1, p_2, \ldots, p_k$

เป็นจำนวนเฉพาะที่แตกต่างกัน โดยทฤษฎี 3.4.4 จะได้

$$(a, b)^* = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} \text{ โดยที่ } d_i = a_i \text{ ถ้า } a_i = b_i$$

และ $d_i = 0$ ถ้า $a_i \neq b_i$ ---(1)

จาก (1) พิจารณา ถ้า $a_i = b_i$ จะได้

$$d_i = a_i = \min\{a_i, b_i\} \text{ ----------(2)}$$

จาก (1) พิจารณา ถ้า $a_i \neq b_i$ จะได้

$$d_i = 0 \leq \min\{a_i, b_i\} \text{ ----------(3)}$$

จาก (1), (2), (3) โดยทฤษฎี 2.4.3 จะได้

$$(a, b)^* = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} \leq p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \ldots p_k^{\min\{a_k,b_k\}}$$

$$= (a, b)$$ □

<u>ทฤษฎี 3.5.2</u> ถ้า $a, b \in Z^+$ แล้ว $(a, b)^* = (a, b) = 1$

ก็ต่อเมื่อ a และ b ไม่มีตัวหารร่วมที่เป็นจำนวนเฉพาะ

พิสูจน์ ---->) จากกำหนดให้ $(a, b) = 1$ โดยนิยาม 2.2.3 จะได้ว่า

a และ b ไม่มีตัวหารร่วมอื่นนอกจาก 1 นั่นคือ

a และ b ไม่มีตัวหารร่วมที่เป็นจำนวนเฉพาะ □

พิสูจน์ <----) จากกำหนดให้ a และ b ไม่มีตัวหารร่วมที่เป็นจำนวนเฉพาะ

โดยนิยาม 2.2.3 จะได้

$$(a, b) = 1 \quad \text{----------(1)}$$

จาก (1) โดยทฤษฎี 3.5.1 และนิยาม 3.4.2 จะได้

$$1 \leq (a, b)^* \leq (a, b) = 1 \quad \text{----------(2)}$$

จาก (2) จะได้

$$(a, b)^* = 1 \quad \text{----------(3)}$$

จาก (1) และ (3) จึงได้ $(a, b)^* = (a, b) = 1$ □

ทฤษฎี 3.5.3 ถ้า $k, a_i, b_i \in W$ โดยที่ $i=1, 2, \ldots, k$

และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกันและ

$a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ แล้ว

$(a, b)^* = (a, b) > 1$ ก็ต่อเมื่อ มี $m \in Z^+$ โดยที่ $1 \leq m \leq k$

ที่ทำให้ $a_m = b_m > 1$ และ

ก. ถ้า $a_i > 0$ แล้ว $b_i = a_i$ หรือ $b_i = 0$

หรือ ข. ถ้า $b_i > 0$ แล้ว $a_i = b_i$ หรือ $a_i = 0$

<u>พิสูจน์</u> $\dashrightarrow$)

จากกำหนดให้ $(a, b)^* > 1$ โดยทฤษฎี 3.4.4 จะได้

$$(a, b)^* = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k} \quad \text{โดยที่} \quad d_i = a_i \text{ ถ้า } a_i = b_i$$

และ $d_i = 0$ ถ้า $a_i \neq b_i$--(1)

พิจารณา ถ้า $a_i \neq b_i$ ทุก $i = 1, 2, \ldots, k$ จะได้ $d_i = 0$

นั่นคือ

$$(a, b)^* = p_1^0 p_2^0 \ldots p_k^0 = 1 \quad \text{ขัดแย้งกับ} \quad (a, b)^* > 1$$

ดังนั้นจะได้มี $m \in Z^+$ โดยที่ $1 \leq m \leq k$ ที่ทำให้ $a_m \neq b_m$ และ $a_m > 1$

$$a_m = b_m \geq 1 \text{ ----------(2)}$$

จากกำหนดให้ $(a, b) > 1$ โดยทฤษฎี 2.4.3 จะได้

$$(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \ldots p_k^{\min\{a_k, b_k\}} \text{ --------(3)}$$

จาก (1), (3) และจากกำหนดให้ $(a, b)^* = (a, b)$ จึงได้

$$d_i = \min\{a_i, b_i\} \text{ ----------(4)}$$

ก. จากกำหนดให้ $a_i > 0$ พิจารณา

ถ้า $b_i \neq a_i$ จาก (1) และ (4) จะได้

$d_i = 0 = \min\{a_i, b_i\}$ นั่นคือ $b_i = 0$

ข. จากกำหนดให้ $b_i > 0$ พิจารณา

ถ้า $a_i \neq b_i$ จาก (1) และ (4) จะได้

$d_i = 0 = \min\{a_i, b_i\}$ นั่นคือ $a_i = 0$ □

พิสูจน์ (<--)

พิจารณา $(a, b)^*$ และ (a, b) จากกำหนดให้ มี $m \in Z^+$

โดยที่ $1 \leq m \leq k$ ที่ทำให้ $a_m = b_m > 1$ โดยทฤษฎี 2.4.3 จะได้

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \ldots p_k^{\min\{a_k,b_k\}} \geq p_m^{a_m} \quad ---(1)$$

และโดยทฤษฎี 3.4.4 จะได้

$$(a,b)^* = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$$ โดยที่ $d_i = a_i$ ถ้า $a_i = b_i$

และ $d_i = 0$ ถ้า $a_i \neq b_i$ --(2)

จาก (2) และกำหนดให้ จะได้

$$(a, b)^* \geq p_m^{a_m} \quad ----------(3)$$

จาก $a_m \geq 1$ และ p_m เป็นจำนวนเฉพาะ จะได้

$$p_m^{a_m} > 1 \quad \text{----------(4)}$$

จาก (1), (3) และ (4) จึงได้

$$(a, b), (a, b)^* > 1 \quad \text{----------(5)}$$

พิจารณา (a, b) ถ้า $a_i > 0$ จาก ข้อ (ก) จะได้ว่า

$a_i = b_i$ จะได้ $\min\{a_i, b_i\} = a_i$ ----------(6)

หรือถ้า $a_i \neq b_i$ แล้ว $b_i = 0$ จะได้ $\min\{a_i, b_i\} = 0$ ---(7)

พิจารณา ถ้า $a_i = 0$ จะได้

$$\min\{a_i, b_i\} = 0 \quad \text{----------(8)}$$

จาก (2), (5), (6), (7), (8) และ ทฤษฎี 2.4.3 จะได้

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \ldots p_k^{\min\{a_k,b_k\}}$$

$$= p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} \quad \text{โดยที่} \quad m_i = a_i \text{ ถ้า } a_i = b_i$$

และ $m_i = 0$ ถ้า $a_i \neq b_i$ ---(9)

จาก (5), (9) และ ทฤษฎี 3.4.4 จะได้

$$(a,b) = (a,b)^* > 1 \qquad \square$$

3.6 นิยามจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี (Unitary Relatively Prime)

นิยาม 3.6.1 ถ้า $a, b \in Z^+$ จะเรียก a และ b ว่าเป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี ก็ต่อเมื่อ $(a, b)^* = 1$

ตัวอย่าง 3.6.1

ก. 4 และ 6 เป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี

ข. 5 และ 7 เป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี

ค. 15 และ 18 เป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี

ง. 10 และ 25 เป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรี □