บทที่ 4

ตัวหารแบบยูนิแทรีและออยเลอร์ ฟาย-ฟังก์ชัน

ในบทนี้จะแสดงถึงจำนวนของตัวหารแบบยูแทรีของจำนวนเต็มบวก นอกเหนือจากบทที่ 3 และศึกษาตัวหารแบบยูนิแทรีร่วมกับออยเลอร์ ฟาย-ฟังก์ชัน นอกจากนี้ยังได้นิยาม ออยเลอร์ ฟาย-ฟังก์ชัน แบบยูนิแทรี และหาความสัมพันธ์ของออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรี และออยเลอร์ ฟาย-ฟังก์ชันแบบธรรมดา จากนั้นได้ขยายทฤษฎีของออยเลอร์-แฟร์มาต์ โดยใช้คุณสมบัติของตัวหารแบบยูนิแทรี สำหรับบทนี้ได้แบ่งการศึกษาเป็นหัวข้อดังนี้

4.1 จำนวนของตัวหารแบบยูนิแทรีของจำนวนเต็มบวก

4.2 ตัวหารแบบยูนิแทรีและออยเลอร์ ฟาย-ฟังก์ชัน

4.3 นิยามออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรี

4.4 ความสัมพันธ์ของออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรีและออยเลอร์ ฟาย-ฟังก์ชันแบบธรรมดา

4.5 ขยายทฤษฎีของ ออยเลอร์-แฟร์มาต์

4.1 จำนวนของตัวหารแบบยูนิแทรีของจำนวนเต็มบวก

ในหัวข้อนี้ จะเป็นการแสดงจำนวนของตัวหารแบบยูนิแทรีของจำนวนเต็มบวก โดยการแสดงจะเริ่มจากทฤษฎีต่อไปนี้

<u>ทฤษฎี 4.1.1</u> ถ้า $n \in Z^+$ แล้ว จำนวนตัวหารแบบยูนิแทรีของ n จะมีจำนวนน้อยกว่าหรือเท่ากับจำนวนตัวหารของ n

<u>พิสูจน์</u> พิจารณา $S = \{1, 2, \ldots, n\}$

$$A = \{x \in Z^+ / x / n\}$$

$$B = \{x \in Z^+ / x /^* n\}$$

จากทฤษฎี 2.2.1 (ข) $1/n$ และโดยนิยาม A จึงได้ $1 \varepsilon A$ นั่นคือ

$A \neq \emptyset$ --------------------------------------(1)

จากนิยาม A และ S จึงได้ $A \subseteq S$ และโดยทฤษฎี 2.1.4.1 จึงได้

A เป็นเซตจำกัด ----------------------------------(2)

จากทฤษฎี 3.2.1 (ข) $1/^{*}n$ และโดยนิยาม B จึงได้

$1 \varepsilon B$ นั่นคือ

$B \neq \emptyset$ --------------------------------------(3)

จากนิยาม B และ S จึงได้ $B \subseteq S$ และโดยทฤษฎี 2.1.4.1 จึงได้

B เป็นเซตจำกัด ----------------------------------(4)

พิจารณา $y \varepsilon B$ โดยนิยาม B จะได้ $y \varepsilon Z^{+}$ และ $y/^{*}n$

โดยนิยาม 3.1.1 จึงได้ y/n นั่นคือ $y \varepsilon A$ โดยนิยาม 2.1.1.1 จึงได้

$B \subseteq A$ --------------------------------------(5)

จาก (1), (2), (3), (4) และ (5) โดยทฤษฎี 2.1.4.2 จึงได้

$||B|| \leq ||A||$ ----------------------------------(6)

จากนิยาม A, B และจาก (6) จึงได้ว่า จำนวนตัวหารแบบยูนิแทรีของ n มีน้อยกว่าหรือเท่ากับจำนวนตัวหารของ n □

<u>ทฤษฎี 4.1.2</u> ถ้า p เป็นจำนวนเฉพาะแล้ว จำนวนตัวหารแบบยูนิแทรีและจำนวนตัวหารของ p มีจำนวนเท่ากัน

<u>พิสูจน์</u>

1. จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยนิยาม 2.2.4 จะได้ จำนวนเต็มบวกที่เป็นตัวหารของ p มี 2 ตัวคือ 1 และ p
2. จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยทฤษฎี 3.3.1 p จะมีตัวหารแบบยูนิแทรีเพียง 2 ตัวคือ 1 และ p

จาก 1. และ 2. จึงได้ว่า จำนวนตัวหารแบบยูนิแทรีและจำนวนตัวหารของ p มีจำนวนเท่ากัน □

<u>ทฤษฎี 4.1.3</u> ถ้า $n \varepsilon Z^+$ โดยที่ n เป็นผลคูณของจำนวนเฉพาะที่แตกต่างกัน แล้ว จำนวนตัวหารแบบยูนิแทรีและจำนวนตัวหารของ n จะมีจำนวนเท่ากัน

<u>พิสูจน์</u> พิจารณา $A = \{x \varepsilon Z^+ / x / n\}$

$B = \{x \varepsilon Z^+ / x /^* n\}$

จากการพิสูจน์ในทฤษฎี 4.1.1 จะได้ A, B เป็นเซตจำกัด โดยที่ $A, B \neq \emptyset$ และ

$$B \subseteq A \quad \text{---} (1)$$

พิจารณา ถ้า $y \varepsilon A$ จะได้ y/n โดยทฤษฎี 3.3.3

จะได้ $y/^{*}n$ นั่นคือ $y \varepsilon B$ โดยนิยาม 2.1.1.1 จึงได้

$$A \subseteq B \text{ ---(2)}$$

จาก (1), (2) และโดยสัจพจน์ 2.1.1.3 จึงได้

$$A = B \text{ ---(3)}$$

จาก (3) และนิยาม A, B จึงได้ว่า จำนวนตัวหารแบบยูนิแทรี และจำนวนตัวหารของ n มีจำนวนเท่ากัน □

<u>ทฤษฎี 4.1.4</u> ถ้า $n, r \varepsilon Z^+$ และ $n = p^r$ โดยที่ p เป็นจำนวนเฉพาะ และ $r \geq 2$ แล้ว ตัวหารแบบยูนิแทรีของ n จะมีเพียง 2 ตัว คือ 1 และ n

<u>พิสูจน์</u> พิจารณา $q \varepsilon Z^+$ โดยที่ $1 < q < n$ และ q/n จากกำหนดให้ $n = p^r$ และจาก q/n โดยทฤษฎี 2.4.2 จึงได้ว่ามี $m \varepsilon Z^+$ โดยที่ $1 \leq m < r$ ซึ่งทำให้

$$q = p^m \text{ ---(1)}$$

พิจารณา $(q, \frac{n}{q})$ และจาก (1) โดยทฤษฎี 2.3.2 และทฤษฎี 2.4.3 จะได้

$$(q, \frac{n}{q}) = (p^m, \frac{p^r}{p^m}) = p^{\min\{m,\ r-m\}} \text{ -------------(2)}$$

จาก $m \geq 1$ และ $r > m$ จึงได้ว่า

$$\min\{m, r-m\} \geq 1 \quad \text{------------------------(3)}$$

จาก (2) และ (3) จึงได้

$$(q, \frac{n}{q}) = p^{\min\{m, r-m\}} \geq p \neq 1 \quad \text{-------------(4)}$$

จาก (4) และโดยนิยาม 3.1.1 จึงได้

$$q \nmid^* n \quad \text{----------------------------------(5)}$$

จาก (1), (5) และโดยทฤษฎี 3.2.1 ข้อ ก.และ ข. คือ

$n/^* n$ และ $1/^* n$ จึงได้ว่า

n มีตัวหารแบบยูนิแทรีเพียง 2 ตัว คือ 1 และ n □

<u>ทฤษฎี 4.1.5</u> (รูปแบบของตัวหารแบบยูนิแทรี)

ถ้า $a_i, k \in Z^+$ โดยที่ $i = 1, 2, \ldots, k$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ แล้ว $d/^* n$ ก็ต่อเมื่อ

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

<u>พิสูจน์</u> --->) จาก $d/^{*} n$ โดยนิยาม 3.1.1 จะได้

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

จาก (1) และทฤษฎี 3.3.2 จะได้

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

<---) จาก $d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$ โดยที่ $d_i = 0, a_i$

โดยทฤษฎี 2.4.2 จะได้

d/n --(1)

จาก (1) โดยทฤษฎี 3.3.2 จะได้

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

จาก (1), (2) และนิยาม 3.1.1 จะได้

$d/^{*} n$ □

<u>ทฤษฎี 4.1.6</u> ถ้า $a_i, k \in Z^+$ โดยที่ $i = 1, 2, \ldots, k$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ แล้ว จำนวนตัวหารแบบยูนิแทรีของ n จะมี 2^k จำนวน

พิสูจน์ จากกำหนดให้ $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ โดยที่ $a_i \in Z^+$

จะได้ว่ามีจำนวนเฉพาะที่แตกต่างกัน k จำนวน

โดยทฤษฎี 4.1.5 ถ้า $d/^* n$ จะได้

$$d = p_1^{d_1}p_2^{d_2}\dots p_k^{d_k} \quad \text{โดยที่} \quad d_i = 0, a_i$$

นั่นคือ เลขยกกำลังของจำนวนเฉพาะแต่ละตัวจะเป็นไปได้ 2 กรณีคือ 0 และ a_i และจากที่จำนวนเฉพาะที่แตกต่างกันมี k จำนวน โดยกฎขั้นมูลฐาน 2 ของการจัดลำดับ จึงได้จำนวนตัวหารแบบยูนิแทรีมี 2^k จำนวน □

4.2 ตัวหารแบบยูนิแทรีและออยเลอร์ ฟาย-ฟังก์ชัน (Unitary Divisor and Euler Ø-Function)

ในหัวข้อนี้จะนำตัวหารแบบยูนิแทรีและออยเลอร์ ฟาย-ฟังก์ชัน มาพิจารณาร่วมกัน โดยหาผลบวกของออยเลอร์ ฟาย-ฟังก์ชัน ของตัวหารแบบยูนิแทรี ซึ่งจะเริ่มจากตัวอย่างและทฤษฎีต่อไปนี้

ตัวอย่าง 4.2.1 ให้ $n = 12$

พิจารณา d_i ซึ่ง $d_i/^* n$ จะได้

$d_1 = 1,\ d_2 = 3,\ d_3 = 4,\ d_4 = 12$

ดังนั้น จะได้ $\sum_{i=1}^{4} \phi(d_i) = \phi(1) + \phi(3) + \phi(4) + \phi(12)$

$= 9$ □

<u>ตัวอย่าง 4.2.2</u> ให้ $n = 7$

พิจารณา d_i ซึ่ง $d_i /^{*} n$ จะได้

$d_1 = 1,\ d_2 = 7$

ดังนั้น จะได้ $\sum_{i=1}^{2} \phi(d_i) = \phi(1) + \phi(7)$

$= 7$ □

<u>ตัวอย่าง 4.2.3</u> ให้ $n = 6$

พิจารณา d_i ซึ่ง $d_i /^{*} n$ จะได้

$d_1 = 1,\ d_2 = 2,\ d_3 = 3,\ d_4 = 6$

ดังนั้นจะได้ $\sum_{i=1}^{4} \phi(d_i) = \phi(1) + \phi(2) + \phi(3) + \phi(6)$

$= 6$ □

<u>ทฤษฎี 4.2.1</u> ถ้า $n, d_i, k \in Z^+$ โดยที่ $d_i /^{*} n$ เมื่อ $i = 1,2,\ldots,k$ แล้ว $\sum_{i=1}^{k} \phi(d_i) \leq n$

<u>พิสูจน์</u> พิจารณา $A = \{x \in Z^+ / x / n\}$

$B = \{x \in Z^+ / x /^{*} n\}$

จากการพิสูจน์ในทฤษฎี 4.1.1 จะได้ A, B เป็นเซตจำกัด

โดยที่ $A, B \neq \emptyset$ และ $B \subsetneq A$ ------------------------(1)

นั่นคือ ถ้า $d_1, d_2, \ldots, d_k \in B$ จะได้

$d_1, d_2, \ldots, d_k, d_{k+1}, \ldots, d_r \in A$ และ $k \leq r$ ------(2)

พิจารณา $\sum_{i=1}^{k} \phi(d_i)$ และ $\sum_{i=1}^{r} \phi(d_i)$ จากทฤษฎี 2.4.4

จะได้ $\sum_{i=1}^{r} \phi(d_i) = n$ และจาก (1), (2)

จะได้

$$\sum_{i=1}^{k} \phi(d_i) \leq \sum_{i=1}^{r} \phi(d_i) = n \qquad \square$$

<u>หมายเหตุ</u> จากข้อความในทฤษฎี 4.2.1 ถ้าเปลี่ยนจาก $d_i /^* n$ เป็น d_i / n

แล้วผลจะได้ $\sum_{i=1}^{k} \phi(d_i) = n$

<u>ทฤษฎี 4.2.2</u> ถ้า $d_i, k \in Z^+$ และ p เป็นจำนวนเฉพาะ และ $d_i /^* p$

โดยที่ $i = 1, 2, \ldots, k$ แล้ว $\sum_{i=1}^{k} \phi(d_i) = p$

<u>พิสูจน์</u> จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยทฤษฎี 3.3.1 จะได้

ตัวหารแบบยูนิแทรีของ p มีเพียง 1 และ p ---------------(1)

พิจารณา $\sum_{i=1}^{k} \phi(d_i)$ และจาก (1) จะได้

$$\sum_{i=1}^{2} \phi(d_i) = \phi(1) + \phi(p) \text{ ----------------------(2)}$$

จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยทฤษฎี 2.4.5

จึงได้ $\phi(p) = p-1$ และ $\phi(1) = 1$ พิจารณาร่วมกับ (2) จึงได้

$$\sum_{i=1}^{2} \phi(d_i) = 1 + p-1 = p \qquad \square$$

หมายเหตุ จากข้อความในทฤษฎี 4.2.2 ถ้าเปลี่ยนจาก $d_i /^{*} p$ เป็น d_i/p แล้วผลที่ได้ยังคงเป็นเช่นเดิม

ทฤษฎี 4.2.3 ถ้า $n, k, m, d_j \in Z^+$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $n = p_1 p_2 \ldots p_k$ และ $d_j /^{*} n$ โดยที่ $j = 1, 2, \ldots, m$ แล้ว $\sum_{j=1}^{m} \phi(d_j) = n$

พิสูจน์ จากกำหนดให้ $n = p_1 p_2 \ldots p_k$ โดยที่ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ $k \in Z^+$ พิจารณา

$$A = \{x \in Z^+ / x/n\}$$

$$B = \{x \in Z^+ / x/^{*} n\}$$

จากการพิสูจน์ในทฤษฎี 4.1.3 จะได้ว่า

$$A = B \text{ --(1)}$$

นั่นคือ ถ้า $A = \{d_1, d_2, \ldots, d_m\}$ แล้ว จะได้

$$B = \{d_1, d_2, \ldots, d_m\}$$

ดังนั้น โดยทฤษฎี 2.4.4

จึงได้

$$\sum_{j=1}^{m} \phi(d_j) = n$$ □

<u>หมายเหตุ</u> จากทฤษฎี 4.2.3 ถ้าเปลี่ยนข้อความจาก $d_j /^{*} n$ เป็น d_j/n แล้ว ผลที่ได้ยังคงเป็นเช่นเดิม

<u>ทฤษฎี 4.2.4</u> ถ้า $k, n, m, d_j \in Z^+$ และ $m \geq 2$, $n = p^m$ โดยที่ p เป็นจำนวนเฉพาะ และ $d_j /^{*} n$ โดยที่ $j = 1, 2, \ldots, k$ แล้ว $\sum_{j=1}^{k} \phi(d_j) < n$

<u>พิสูจน์</u> จากกำหนดให้ $n = p^m$ โดยที่ $m \in Z^+$ และ $m \geq 2$, p เป็นจำนวนเฉพาะ โดยทฤษฎี 4.1.4 จะได้

n มีตัวหารแบบยูนิแทรี 2 ตัวคือ 1 และ n ---------------(1)

จาก (1) พิจารณา $d_j /^{*} n$, $1 \leq d_j \leq n$ และ $j = 1, 2, \ldots, k$

และ $\sum_{j=1}^{k} \phi(d_j)$ จะได้

$$\sum_{j=1}^{2} \phi(d_j) = \phi(1) + \phi(n) \quad \text{------------------(2)}$$

จากกำหนดให้ $n = p^m$ และ $m \geq 2$ จะได้ว่า n ไม่เป็นจำนวนเฉพาะ

ดังนั้น

$$\phi(n) < n - 1 \quad \text{------------------------------(3)}$$

จาก (2) และ (3) จะได้

$$\sum_{j=1}^{2} \phi(d_j) < 1 + n - 1 = n \qquad \square$$

<u>หมายเหตุ</u> จากทฤษฎี 4.2.4 ถ้าเปลี่ยนข้อความจาก $d_j /^* n$ เป็น d_j / n แล้ว

ผลที่ได้จะเป็น $\sum_{j=1}^{k} \phi(d_j) = n$

<u>บทแทรก 4.2.1</u> ถ้า n เป็นจำนวนเต็มตามเงื่อนไขในทฤษฎี 4.2.4

แล้ว $\sum_{j=1}^{k} \phi(d_j) = 1 + (n - \frac{n}{p})$

<u>พิสูจน์</u> จากทฤษฎี 4.2.4 จะได้

$$\sum_{j=1}^{k} \phi(d_j) = \phi(1) + \phi(n) \quad \text{------------------(1)}$$

พิจารณา $K = \{x \in Z^+ / x \leq n$ และ $p / x\}$ จะได้

$$K = \{p, 2p, 3p, \ldots, kp\} \quad \text{------------------(2)}$$

จากนิยาม K จะได้ p^m เป็นสมาชิกที่มากที่สุดของ K นั่นคือ

$$kp = p^m \text{ ---------------------------------- (3)}$$

จาก (3) จะได้

$$k = \frac{p^m}{p} \text{ หรือ } \frac{n}{p} \text{ ---------------------------------- (4)}$$

จาก (2), (4) และนิยาม 2.1.4.3 จึงได้

$$||K|| = k = \frac{n}{p} \text{ ---------------------------------- (5)}$$

จาก (5) และนิยาม K จะได้ว่า จำนวนเต็ม x ซึ่ง $1 \leq x \leq n$

และ $(x, p) > 1$ จะมีทั้งหมด $\frac{n}{p}$ จำนวน

ดังนั้นโดยนิยาม 2.4.1 จึงได้

$$\emptyset(n) = n - \frac{n}{p} \text{ ---------------------------------- (6)}$$

จาก (1), (6) จึงได้ $\sum_{j=1}^{k} \emptyset(d_j) = 1 + (n - \frac{n}{p})$ □

4.3 <u>นิยามออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรี</u>

<u>นิยาม 4.3.1</u> ถ้า $n \in Z^+$ จำนวนของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ n และเป็นจำนวนเฉพาะสัมพัทธ์แบบยูนิแทรีกับ n เรียกว่า ออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรีของ n และเขียนแทนด้วย $\emptyset^*(n)$ หรือ

ถ้า $K = \{x \in Z^+/(x, n)^* = 1$ และ $x \leq n\}$ แล้ว

$$\emptyset^*(n) = ||K||$$

<u>ตัวอย่าง 4.3.1</u> ให้ $n = 12$

พิจารณา $d \in Z^+$ โดยที่ $d \leq 12$ และ $(d, 12)^* = 1$

จะได้ $d = 1, 2, 5, 7, 8, 9, 10, 11$

ดังนั้น จะได้ $\phi^*(12) = 8$ □

<u>ตัวอย่าง 4.3.2</u> ให้ $n = 7$

พิจารณา $d \in Z^+$ โดยที่ $d \leq 7$ และ $(d, 7)^* = 1$

จะได้ $d = 1, 2,3,4,5,6$

ดังนั้น จะได้ $\phi^*(7) = 6$ □

<u>ตัวอย่าง 4.3.3</u> ให้ $n = 4$

พิจารณา $d \in Z^+$ โดยที่ $d \leq 4$ และ $(d, 4)^* = 1$

จะได้ $d = 1, 2, 3$

ดังนั้น จะได้ $\phi^*(4) = 3$ □

4.4 <u>ความสัมพันธ์ของออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรีและแบบธรรมดา</u>

ในหัวข้อนี้ จะแสดงความสัมพันธ์ระหว่าง ออยเลอร์ ฟาย-ฟังก์ชันแบบยูนิแทรี และออยเลอร์ ฟาย-ฟังก์ชันแบบธรรมดาของจำนวนเต็มบวก ซึ่งจะแสดงโดยตัวอย่างและทฤษฎีต่อไปนี้

<u>ตัวอย่าง 4.4.1</u> ให้ $n = 12$

จากตัวอย่าง 4.3.1 จะได้

$$\phi^*(12) = 8$$

พิจารณา $\phi(12) = 4$

จะพบว่า $\phi^*(12) > \phi(12)$ $\square$

<u>ตัวอย่าง 4.4.2</u> ให้ $n = 7$

จากตัวอย่าง 4.3.2 จะได้

$$\phi^*(7) = 6$$

พิจารณา $\phi(7) = 6$

จะพบว่า $\phi^*(7) = \phi(7)$ $\square$

<u>ตัวอย่าง 4.4.3</u> ให้ $n = 4$

จากตัวอย่าง 4.3.3 จะได้

$$\phi^*(4) = 3$$

พิจารณา $\phi(4) = 2$

จะพบว่า $\phi^*(4) > \phi(4)$ $\square$

จากตัวอย่างทำให้ได้ข้อสังเกตซึ่งแสดงโดยทฤษฎีต่อไปนี้

<u>ทฤษฎี 4.4.1</u> ถ้า p เป็นจำนวนเฉพาะแล้ว $\emptyset^{*}(p) = p-1$

<u>พิสูจน์</u> จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยทฤษฎี 2.4.5

จะได้ $\emptyset(p) = p - 1$ นั่นคือ

ถ้า $a \in Z^{+}$ โดยที่ $1 \leq a \leq p-1$ แล้ว $(a,p) = 1$ ---(1)

จาก (1) โดยทฤษฎี 3.5.1 จะได้

$(a, p)^{*} \leq (a, p) = 1$ ----------------------------(2)

จาก (2) และนิยาม 3.4.2 จะได้

$1 \leq (a, p)^{*} \leq (a, p) = 1$ ----------------------------(3)

จาก (1) และ (3) จะได้ว่า

ถ้า $a \in Z^{+}$ โดยที่ $1 \leq a \leq p-1$ แล้ว

$(a, p)^{*} = 1$ ----------------------------------(4)

จาก (4) และนิยาม 4.3.1 จึงได้

$\emptyset^{*}(p) = p - 1$ □

<u>หมายเหตุ</u> จากทฤษฎี 4.4.1 ถ้าเปลี่ยนข้อความจาก $\emptyset^{*}(p)$ เป็น $\emptyset(p)$ ผลที่ได้ยังคงเป็นเช่นเดิม

<u>ทฤษฎี 4.4.2</u> ถ้า $m \varepsilon Z^{+}$ และ $m \geq 2$ และ $n = p^{m}$ โดยที่ p เป็นจำนวนเฉพาะ แล้ว $\phi^{*}(n) = n - 1$

<u>พิสูจน์</u> จากกำหนดให้ $n = p^{m}$ โดยที่ p เป็นจำนวนเฉพาะ, $m \geq 2$

พิจารณา $(a, n)^{*}$ โดยที่ $a \varepsilon Z^{+}$ และ $a \leq n$

ถ้า $a = n$ จะได้ $(a, n)^{*} = n$ ----------------(1)

ถ้า $a < n$ พิจารณา $(a, n)^{*} = (a, p^{m})^{*}$

ถ้า p หาร a ลงตัว โดยทฤษฎี 2.4.2 จะได้

$a = p^{r}$ โดยที่ $0 \leq r < m$ และ $r \varepsilon Z$ --------(2)

โดยทฤษฎี 3.4.2 จะได้

$(a, n)^{*} = (p^{r}, p^{m})^{*} = p^{0} = 1$ ------------(3)

ถ้า p หาร a ไม่ลงตัว โดยทฤษฎี 3.5.2 จะได้

$(a, n)^{*} = (a, p^{m})^{*} = 1$ ------------(4)

จาก (1), (3) และ(4) จึงได้ว่า ถ้า $a \varepsilon Z^{+}$ โดยที่ $1 \leq a < n$

แล้ว $(a, n)^{*} = 1$ โดยนิยาม 3.4.2 จึงได้ $\phi^{*}(n) = n - 1$ □

<u>ทฤษฎี 4.4.3</u> ถ้า p เป็นจำนวนเฉพาะแล้ว $\phi^*(p) = \phi(p)$

<u>พิสูจน์</u> จากกำหนดให้ p เป็นจำนวนเฉพาะ โดยทฤษฎี 4.4.1 จะได้

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

จากกำหนดให้ p เป็นจำนวนเฉพาะโดยทฤษฎี 2.4.5 จะได้

$\phi(p) = p - 1$ ---------------------------------(2)

จาก (1) และ (2) จึงได้ว่า

$\phi^*(p) = \phi(p)$ $\square$

<u>ทฤษฎี 4.4.4</u> ถ้า $m \varepsilon Z^+$ และ $n = p^m$ โดยที่ p เป็นจำนวนเฉพาะ และ $m \geq 2$ แล้ว $\phi^*(n) > \phi(n)$

<u>พิสูจน์</u> จากกำหนดให้ $n = p^m$ โดยที่ $m \varepsilon Z^+$ และ $m \geq 2$ และ p เป็นจำนวนเฉพาะ โดยทฤษฎี 4.4.2 จะได้

$\phi^*(n) = n - 1$ ---------------------------------(1)

พิจารณา p จะได้ $1 < p < n$ และ $(n, p) = p$

นั่นคือ มี $q \varepsilon Z^+$ โดยที่ $1 \leq q \leq n-1$ และ $(n, q) \neq 1$

โดยนิยาม 2.4.1 จะได้

$\phi(n) < n - 1$ ---------------------------------(2)

จาก (1) และ (2) จึงได้

$$\phi^*(n) > \phi(n)$$ □

<u>ทฤษฎี 4.4.5</u> ถ้า $n, k \in Z^+$ โดยที่ $k \geq 2$; $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < \ldots < p_k$ และ $n = p_1p_2\ldots p_k$ แล้ว $\phi^*(n) > \phi(n)$

<u>พิสูจน์</u> จากกำหนดให้ $n = p_1p_2 \ldots p_k$ โดยที่ $k \in Z^+$ และ $k \geq 2$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < \ldots < p_k$

พิจารณา

$$S = \{1, 2, \ldots, n\}$$

$$A = \{x \in Z^+/ (x, n) = 1 \text{ และ } x \leq n\}$$

$$B = \{x \in Z^+/ (x, n)^* = 1 \text{ และ } x \leq n\}$$

จาก $(1, n) = 1$ และ $(1, n)^* = 1$ จะได้ว่า $1 \in A$ และ $1 \in B$ นั่นคือ

$$A, B \neq \emptyset \text{ ------------------------------------(1)}$$

จากนิยาม A, B จะได้ $A \subsetneq S$ และ $B \subsetneq S$ โดยทฤษฎี 2.1.4.1 จะได้

$$A, B \text{ เป็นเซตจำกัด ---------------------------(2)}$$

พิจารณา ถ้า $y \in A$ จะได้ $(y, n) = 1$ โดยทฤษฎี 3.5.1

จะได้ $(y, n)^* \leq (y, n) = 1$ นั่นคือ $(y, n)^* = 1$

จะได้ $y \in B$ โดยนิยาม 2.1.1.1 จะได้

$\therefore A \subseteq B$ ---------------------------------------(3)

พิจารณา p_1^2 จาก $n = p_1p_2 \ldots p_k$ และ $k \geq 2$

และ $p_1 < p_2 < \ldots < p_k$

จะได้ $p_1^2 = p_1p_1 < p_1p_2 \leq n$ นั่นคือ $p_1^2 < n$ โดยทฤษฎี 3.4.4

จะได้

$(n, p_1^2)^* = p^0 = 1$ ----------------------------(4)

จาก (4) และนิยาม B จะได้

$p_1^2 \in B$ ---------------------------------------(5)

พิจารณา (n, p_1^2) จากกำหนดให้ $n = p_1p_2 \ldots p_k$ และโดย

นิยาม 2.2.3 จะได้

$(n, p_1^2) = p_1 \neq 1$ ----------------------------(6)

จาก (6) และนิยาม A จะได้

$p_1^2 \notin A$ ---------------------------------------(7)

จาก (3), (5) และ (7) โดยนิยาม 2.1.1.2 จึงได้

$A \subset B$ ---------------------------------------(8)

จาก (1), (2), (8) และโดยทฤษฎี 2.1.4.3 จึงได้ว่า

$\|A\| < \|B\|$ จึงเป็นไปตามนิยาม 2.4.1 และ 4.3.1 คือ

$\phi^*(n) > \phi(n)$ □

<u>ทฤษฎี 4.4.6</u> ให้ $k, n, a_i \in Z^+$ โดยที่ $k \geq 2$ และ $p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน ถ้า $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ โดยที่มี $a_i \neq 1$ สำหรับบาง i เมื่อ $i = 1, 2, \ldots, k$ แล้ว

$\phi^*(n) > \phi(n)$

<u>พิสูจน์</u> พิจารณา $A = \{x \in Z^+ / (x, n) = 1$ และ $x \leq n\}$

$B = \{x \in Z^+ / (x, n)^* = 1$ และ $x \leq n\}$

โดยทฤษฎี 3.5.1 พิสูจน์ทำนองเดียวกับทฤษฎี 4.4.5 จะได้

$A, B \neq \emptyset$ และ A, B เป็นเซตจำกัด ----------------(1)

และ $A \subsetneq B$ ---------------------------------(2)

จาก $a_i \neq 1$ ทุก i พิจารณา $p_m^{a_m - 1}$ ซึ่ง $1 \leq m \leq k$

และ $a_m > 1$ โดยทฤษฎี 3.4.4 และนิยาม $\square$ จะได้

$(p_m^{a_m - 1}, n)^* = 1$ ---------------------------(3)

โดยนิยาม 2.2.3 และนิยาม 2.2.4 จึงได้

$$(p_m^{a_m-1}, n) \geq p_m \neq 1 \quad \text{-----------------------------(4)}$$

จาก (3) และนิยาม B จึงได้

$$p_m^{a_m-1} \in B \quad \text{-----------------------------(5)}$$

จาก (4) และนิยาม A จะได้

$$p_m^{a_m-1} \notin A \quad \text{-----------------------------(6)}$$

จาก (2), (5) และ (6) โดยนิยาม 2.1.1.2 จึงทำให้

$$A \subset B \quad \text{-----------------------------(7)}$$

จาก (1), (6) และทฤษฎี 2.1.4.3 จะได้ $\|A\| < \|B\|$

และโดยนิยาม 2.4.1 และนิยาม 4.3.1 จึงได้

$$\emptyset^*(n) > \emptyset(n)$$ □

<u>ทฤษฎี 4.4.7</u> ถ้า $n \in Z^+$ แล้ว $\emptyset^*(n) \geq \emptyset(n)$

<u>พิสูจน์</u> ผลจากทฤษฎี 4.4.3, 4.4.4, 4.4.5, 4.4.6

□

4.5 <u>ขยายทฤษฎีของ ออยเลอร์-แฟร์มาต์</u>

ในหัวข้อนี้เป็นการนำคุณสมบัติของตัวหารแบบยูนิแทรีไปขยายทฤษฎีของ ออยเลอร์-แฟร์มาต์ ซึ่งจะเริ่มด้วย

การพิจารณา $n, a \in Z^+$ โดยที่ $a /^* n$ แล้ว

หา $k \in Z^+$ ที่ทำให้ $a^k \equiv a \pmod{n}$

<u>ตัวอย่างที่ 1</u> ให้ $n = 3$

จะได้ $a = 1, 3$

ถ้า $a = 1$ จะได้ $k = 1, 2, 3, \ldots$

ถ้า $a = 3$ จะได้ $k = 1, 2, 3, \ldots$

<u>ตัวอย่างที่ 2</u> ให้ $n = 4$

จะได้ $a = 1, 4$

ถ้า $a = 1$ จะได้ $k = 1, 2, 3, \ldots$

ถ้า $a = 4$ จะได้ $k = 1, 2, 3, \ldots$

<u>ตัวอย่างที่ 3</u> ให้ $n = 6$

จะได้ $a = 1, 2, 3, 6$

ถ้า $a = 1$ จะได้ $k = 1, 2, 3, \ldots$

ถ้า $a = 2$ จะได้ $k = 1, 3, 5, \ldots$

ถ้า $a = 3$ จะได้ $k = 1, 2, 3, \ldots$

ถ้า $a = 6$ จะได้ $k = 1, 2, 3, \ldots$

จากตัวอย่างข้างต้นจะพบว่า ถ้า $1 \leq a < n$ และ $(a,n) = 1$ หรือ $a/^{*}n$ แล้วจะมี $k \varepsilon Z$ โดยที่ $k \geq 2$ ที่ทำให้ $a^{k} \equiv a(\text{mod } n)$

และ ถ้า n เป็นผลคูณของจำนวนเฉพาะที่แตกต่างกันแล้ว จะได้ว่า ถ้า $1 \leq a < n$ แล้ว $a^{\emptyset(n)+1} \equiv a(\text{mod } n)$

ข้อสังเกตจากตัวอย่างทำให้ได้ทฤษฎีดังต่อไปนี้

<u>ทฤษฎี 4.5.1</u> ถ้า $a, n \varepsilon Z^{+}$ โดยที่ $a/^{*}n$ แล้ว จะมี $k \varepsilon Z^{+}$ โดยที่ $k \geq 2$ ที่ทำให้ $a^{k} \equiv a(\text{mod } n)$

<u>พิสูจน์</u> ก. กรณี $n = 1$ จาก $1/(a^{k} - a)$ จึงได้ว่า

ถ้า $k \varepsilon Z^{+}$ แล้ว $a^{k} \equiv a(\text{mod } n)$

ข. กรณี $n > 1$ โดยที่ $a/^{*}n$ จากนิยาม 3.1.1 จะได้

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

จาก (1) และทฤษฎี 2.5.6 จะได้

$$a^{\emptyset(\frac{n}{a})} \equiv 1(\text{mod } \tfrac{n}{a}) \quad \text{-----------------------------} (2)$$

พิจารณา $\emptyset(n)$ จาก $(a, \frac{n}{a}) = 1$ โดยทฤษฎี 2.5.7

จึงได้ $\emptyset(n) = \emptyset(a. \frac{n}{a}) = \emptyset(a) . \emptyset(\frac{n}{a})$

นั่นคือ

$$\frac{\emptyset(n)}{\emptyset(a)} = \emptyset(\tfrac{n}{a}) \quad \text{-----------------------------} (3)$$

จาก (2) และ (3) จึงได้

$$a^{\frac{\phi(n)}{\phi(a)}} \equiv 1 \pmod{\frac{n}{a}} \quad \text{------------------------(4)}$$

จาก (4) และทฤษฎี 2.5.5 จะได้

$$a^{\phi(n)} \equiv 1 \pmod{\frac{n}{a}} \quad \text{------------------------(5)}$$

จาก (5) และทฤษฎี 2.5.3 จะได้

$$a^{\phi(n)+1} \equiv a \pmod{n} \quad \text{------------------------(6)}$$

จาก $n > 1$ จึงได้ $\phi(n) \geq 1$ ดังนั้น $\phi(n) + 1 \geq 2$

นั่นคือ ถ้าให้ $k = \phi(n) + 1$ จะได้ว่ามี $k \in Z^+$ โดยที่ $k \geq 2$

ที่ทำให้ $a^k \equiv a \pmod{n}$ □

<u>ทฤษฎี 4.5.2</u> ถ้า $a, n \in Z^+$ โดยที่ n เป็นผลคูณของจำนวนเฉพาะที่แตกต่างกัน และ $1 \leq a \leq n$ แล้ว $a^{\phi(n)+1} \equiv a \pmod{n}$

<u>พิสูจน์</u> ถ้า $1 \leq a \leq n$

จะได้ $a = p_1p_2\cdots p_k$ โดยที่ p_i เป็น

จำนวนเฉพาะ

พิจารณา p_i โดยที่ $i = 1, 2, \ldots, k$ จะได้ p_i เป็นไปได้ 2 กรณี คือ p_i/n หรือ $p_i \nmid n$ โดยทฤษฎี 3.3.3 และทฤษฎี 2.2.11 จึงได้

$$p_i/^{*}n \quad \text{หรือ} \quad (p_i, n) = 1 \text{ ---------------------(1)}$$

จาก (1) ถ้า $p_i/^{*}n$ โดยทฤษฎี 4.5.1 จะได้

$$p_i^{\emptyset(n)+1} \equiv p_i \pmod{n} \text{ ----------------------(2)}$$

จาก (1) ถ้า $(p_i, n) = 1$ โดยทฤษฎี 2.5.6 จะได้

$$p_i^{\emptyset(n)+1} \equiv p_i \pmod{n} \text{ ----------------------(3)}$$

จาก (2) และ (3) จะได้ว่า ถ้า $a = p_1p_2\ldots p_k$ แล้ว

$$p_1^{\emptyset(n)+1} \equiv p_1 \pmod{n},\ p_2^{\emptyset(n)+1} \equiv p_2 \pmod{n},$$

$$\ldots,\ p_k^{\emptyset(n)+1} \equiv p_k \pmod{n} \text{ ----------------------(4)}$$

จาก (4) โดยทฤษฎี 2.5.2 จะได้

$$p_1^{\emptyset(n)+1} \cdot p_1^{\emptyset(n)+1} \ldots p_k^{\emptyset(n)+1} \equiv p_1p_2 \ldots p_k \pmod{n}$$

โดยทฤษฎี 2.3.1 (ข) จึงได้

$$(p_1p_2 \ldots p_k)^{\emptyset(n)+1} \equiv p_1p_2\ldots p_k \pmod{n}$$

นั่นคือ $a^{\emptyset(n)+1} \equiv a \pmod{n}$ $\square$