

บทที่ 3

จำนวนเฉพาะ

ประมาณ 400 ปีก่อนคริสต์ศักราช อริสโตเติล(Aristotle) และยุคลิด(Euclid) ได้แบ่งจำนวนออกเป็นสองกลุ่ม กลุ่มแรกได้แก่ 2,3,5,7,11,13,... ซึ่งเรียกว่าจำนวนเฉพาะและอีกกลุ่มได้แก่ 4,6,8,9,10,12,14,... เรียกว่าจำนวนประกอบ ในวิชาทฤษฎีจำนวนการศึกษาจำนวนเฉพาะเป็นเรื่องหนึ่งที่มีบทบาทและสำคัญยิ่งเนื่องจากจำนวนเต็มบวกสามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะซึ่งแสดงว่าโมโนภาพเกี่ยวกับจำนวนเฉพาะจะสอดคล้องกันในทุก ๆ หัวข้อที่เกี่ยวข้องกับจำนวนเต็มรวมทั้งยังมีข้อคาดเดามากมายเกี่ยวกับจำนวนเฉพาะ ในการศึกษาจำนวนเฉพาะจะเป็นการศึกษาคุณสมบัติรวมทั้งการพิสูจน์ข้อความเกี่ยวกับจำนวนเฉพาะ วิวัฒนาการของจำนวนเฉพาะที่นักคณิตศาสตร์ในอดีตได้ทุ่มเทความรู้ ความสามารถ เพื่อสร้างงานทางทฤษฎีจำนวน และยังสามารถทำให้ผู้ศึกษาได้นำความรู้ที่ได้รับจากการศึกษาดังกล่าวไปใช้ในการแก้ปัญหาต่าง ๆ รวมทั้งหาแนวทางในการคาดเดาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเฉพาะ ซึ่งในบทนี้จะนำเสนอเนื้อหาที่สำคัญในการศึกษาจำนวนเฉพาะดังนี้ นิยามและสมบัติบางประการของจำนวนเฉพาะ ทฤษฎีบทหลักมูลเลขคณิต(Fundamental Theorem of Arithmetic) การค้นหาจำนวนเฉพาะ จำนวนเฉพาะแฟร์มา(Fermat Prime) และจำนวนเฉพาะเมอร์แซน(Mersenne Prime)

3.1 นิยามและสมบัติบางประการของจำนวนเฉพาะ

1 เป็นจำนวนเต็มบวกที่มีตัวหารเป็นบวกเพียงแค่นึงตัวเท่านั้น ก็คือตัวมันเอง ส่วนจำนวนเต็มอื่น ๆ มีตัวหารที่เป็นบวกอย่างน้อยสองจำนวนนั่นคือ 1 และตัวมันเอง สำหรับจำนวนเต็มที่มีตัวหารเพียงสองตัวนั้นเรียกว่าจำนวนเฉพาะ และจำนวนเต็มที่มีตัวหารมากกว่าสองตัวนั้นเรียกว่าจำนวนประกอบ โดยมีบทนิยามดังต่อไปนี้

บทนิยาม 3.1

จำนวนเต็ม p เรียกว่า **จำนวนเฉพาะ** ก็ต่อเมื่อ $p \neq \pm 1$ และ ถ้า $a, b \in \mathbb{Z}$ และ $p = ab$ แล้ว $a = \pm 1$ หรือ $b = \pm 1$ จำนวนเต็มที่มีค่ามากกว่า 1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่าจำนวนประกอบ กล่าวคือ n เป็น**จำนวนประกอบ** ก็ต่อเมื่อ มี $a, b \in \mathbb{N}$ ซึ่ง $1 < a \leq b < n$ ที่ทำให้ $n = ab$

จากบทนิยามของจำนวนเฉพาะ พบว่า

1. $-2, 2$ เป็นจำนวนเฉพาะที่เป็นจำนวนเต็มคู่ ส่วนจำนวนเฉพาะอื่น ๆ จะเป็นจำนวนคี่
2. ถ้า p เป็นจำนวนเฉพาะแล้ว $-p$ เป็นจำนวนเฉพาะ

3. ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ ถ้า $a|p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$
4. ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ ถ้า $p \nmid a$ แล้ว $(p, a) = 1$
5. ให้ p เป็นจำนวนเฉพาะและ $a \in \mathbb{Z}$ จะได้ว่า $p|a$ ก็ต่อเมื่อ $(p, a) = |p|$
6. ถ้า p และ q เป็นจำนวนเฉพาะและ $q|p$ แล้ว $p = q$

หมายเหตุ 3.1

จำนวนเฉพาะที่จะศึกษาในหัวข้อต่อไปจะกล่าวถึงจำนวนเฉพาะที่เป็นบวกเท่านั้น

ตัวอย่าง 3.1

จำนวนเฉพาะที่น้อยกว่า 20 มีดังนี้

2, 3, 5, 7, 11, 13 และ 19

จำนวนประกอบที่น้อยกว่า 20 มีดังนี้

4, 6, 8, 9, 10, 12, 14, 15, 16 และ 18

ตัวอย่าง 3.2 จงแสดงว่าถ้า n เป็นจำนวนประกอบแล้ว $2^n - 1$ เป็นจำนวนประกอบ

วิธีทำ ให้ n เป็นจำนวนประกอบ จะแสดงว่า $2^n - 1$ เป็นจำนวนประกอบ

เนื่องจาก n เป็นจำนวนประกอบแสดงว่ามีจำนวนเต็มบวก a, b ที่มากกว่า 1

จาก $x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + x^{b-3} + \dots + x + 1)$ เมื่อ $x, b \in \mathbb{N}$

จะได้ว่า $2^n - 1 = 2^{ab} - 1$

$$\begin{aligned} &= (2^a)^b - 1 \\ &= (2^a - 1) \left[(2^a)^{b-1} + (2^a)^{b-2} + (2^a)^{b-3} + \dots + (2^a) + 1 \right] \\ &= MN \end{aligned}$$

เมื่อ $M = (2^a - 1)$ และ $N = (2^a)^{b-1} + (2^a)^{b-2} + (2^a)^{b-3} + \dots + (2^a) + 1$

นั่นคือ M, N เป็นจำนวนเต็มที่มากกว่า 1

ดังนั้น $2^n - 1$ เป็นจำนวนประกอบ

ในตัวอย่าง 3.2 จากข้อความแย้งสลับที่พบว่า ถ้า $2^n - 1$ เป็นจำนวนเฉพาะแล้ว n เป็นจำนวนเฉพาะ ต่อไปจะเป็นการศึกษาทฤษฎีบทพื้นฐานที่เกี่ยวข้องกับจำนวนเฉพาะที่มีบทบาทสำคัญในการศึกษาทฤษฎีจำนวนขั้นสูงต่อไป

ทฤษฎีบท 3.1

ทุกจำนวนเต็ม $a > 1$ จะมีจำนวนเฉพาะ p ที่ $p|a$

พิสูจน์

ให้ a เป็นจำนวนเต็มที่มีมากกว่า 1 สมมติว่าไม่มีจำนวนเฉพาะ p ซึ่ง $p|a$ กำหนดให้

$$S = \{b \in \mathbb{N}, b > 1 \text{ และไม่มีจำนวนเฉพาะ } p \text{ ซึ่ง } p|b\}$$

โดยสมมติฐานจะได้ว่า $a \in S$ ดังนั้น $S \subseteq \mathbb{N}$ และ $s \neq \emptyset$ โดยหลักการจัดอันดับอย่างดี

จะได้ว่า S มีสมาชิกตัวเล็กที่สุดเรียกว่า m ดังนั้น m ไม่เป็นจำนวนเฉพาะ

(เนื่องจาก $m|m$) จะได้ว่ามี $1 < d < m$ ที่ทำให้ $d|m$ จะได้ว่า $d \notin S$

ดังนั้นจะมีจำนวน $p|d$ ทำให้ได้ว่า $p|m$ ซึ่งขัดแย้งกับเงื่อนไข $m \in S$

ทฤษฎีบท 3.2

ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ จะได้ว่าถ้า $p|ab$ แล้ว $p|a$ หรือ $p|b$

พิสูจน์

ให้ $a, b \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ

สมมติ ว่า $p|ab$ และ $p \nmid a$ จะได้ว่า $(p, a) = 1$

จะได้ว่า $p|b$

ตัวอย่าง 3.3 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไข $p|(p+1)175$

วิธีทำ กำหนดให้ $p|(p+1)175$

เนื่องจาก $p \nmid (p+1)$ ดังนั้น $p|175$

และ $175 = 5^2 \cdot 7$

ดังนั้น $p = 5, 7$

Burton D.M. (2011 : 40) ได้แสดงการขยายทฤษฎีบท 3.2 ในกรณีที่เป็นผลคูณของจำนวนที่มากกว่าสองจำนวน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.3

ให้ p เป็นจำนวนเฉพาะ และ $a, b, a_1, a_2, \dots, a_n \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ จะได้ว่า

ถ้า $p|(a_1 a_2 \cdots a_n)$ แล้ว $p|a_i$ สำหรับบางจำนวน $i \in \{1, 2, \dots, n\}$

พิสูจน์

สำหรับการพิสูจน์ทฤษฎีบทจะใช้หลักอุปนัยเชิงคณิตศาสตร์ดังนี้

ให้ p เป็นจำนวนเฉพาะ และ $P(n)$ แทนข้อความ

ถ้า $p \mid (a_1 a_2 \cdots a_n)$ แล้ว $p \mid a_i$ สำหรับบางจำนวน $i \in \{1, 2, \dots, n\}$

ขั้นฐาน

กรณี $n = 1$ จะได้ว่า $p \mid a_1$ นั่นคือ $P(1)$

ขั้นอุปนัย

สมมติว่า $P(k)$ เป็นจริงสำหรับ $k \in \mathbb{N}$

จะได้ว่าถ้า $p \mid (a_1 a_2 \cdots a_k)$ แล้ว $p \mid a_i$ สำหรับบางจำนวน $i \in \{1, 2, \dots, k\}$

เนื่องจาก $p \mid (a_1 a_2 \cdots a_k) a_{k+1}$

จะได้ว่า $p \mid (a_1 a_2 \cdots a_k)$ หรือ $p \mid a_{k+1}$

กรณี $p \mid a_{k+1}$ จะได้ว่ามี $i = k + 1$ ซึ่ง $p \mid a_i$

กรณี $p \mid (a_1 a_2 \cdots a_k)$ จากสมมติฐานจะได้ว่ามี a_i ที่ $i \in \{1, 2, \dots, k\}$ ซึ่ง $p \mid a_i$

ดังนั้น มี a_i ที่ $i \in \{1, 2, \dots, k + 1\}$ ซึ่ง $p \mid a_i$ นั่นคือ $P(k + 1)$ เป็นจริง

บทแทรก 3.1

ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ แล้ว สำหรับจำนวนนับ n ถ้า $p \mid a^n$ แล้ว $p \mid a$

พิสูจน์ จากทฤษฎีบท 3.3 โดยเลือก $a_i = a$ ทุก ๆ $i \in \{1, 2, 3, \dots, n\}$

ตัวอย่าง 3.4 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไขต่อไปนี้

1. $p \mid 735^8$
2. $p \mid 4004^{19}$
3. $p \mid (130 + p)^{12}$

วิธีทำ

1. $p \mid 735^8$

จะได้ว่า $p \mid 735$ เนื่องจาก $735 = 3 \cdot 5 \cdot 7^2$ ดังนั้น $p = 3, 5, 7$

2. $p \mid 4004^{19}$

จะได้ว่า $p \mid 4004$ เนื่องจาก $4004 = 2^2 \cdot 7 \cdot 11 \cdot 13$ ดังนั้น $p = 2, 7, 11, 13$

3. $p \mid (130 + p)^{12}$

จะได้ว่า $p \mid (130 + p)$ เนื่องจาก $p \mid p$ และ $130 = 2 \cdot 5 \cdot 13$

ดังนั้น $p = 2, 5, 13$

$$4. \ p \mid (37570 - 2p)^p$$

จะได้ว่า $p \mid (37570 - 2p)$ เนื่องจาก $p \mid 2p$ และ $37570 = 2 \cdot 5 \cdot 13 \cdot 17^2$

ดังนั้น $p = 2, 5, 13, 17$

ตัวอย่าง 3.5 จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไข $(p+1) \mid (p^2 + 2p + 195)^2$

$$\begin{aligned} \text{วิธีทำ} \quad (p^2 + 2p + 195) &= (p^2 + 2p + 1 + 194)^2 \\ &= \left[(p+1)^2 + 194 \right]^2 \end{aligned}$$

$$\text{แสดงว่า } (p+1) \mid \left[(p+1)^2 + 194 \right]^2$$

$$\text{เนื่องจาก } (p+1) \mid (p+1)^2$$

$$\text{พิจารณา } (p+1) \mid (194)^2$$

$$\text{เนื่องจาก } 194^2 = 2^2 \cdot 97^2$$

นั่นคือ $(p+1)$ หารจำนวนต่อไปนี้ลงตัว

1	2	$2^2 = 4$
97	$97^2 = 9409$	$2 \cdot 97 = 194$
$2 \cdot 97^2 = 18818$	$2^2 \cdot 97 = 18818$	$2^2 \cdot 97^2 = 37636$

$$\text{เนื่องจาก } (p+1) \mid (194)^2 \quad \text{จะได้ว่า}$$

$p+1 = 1$	$p = 1 - 1 = 0$
$p+1 = 2$	$p = 2 - 1 = 1$
$p+1 = 2^2 = 4$	$p = 4 - 1 = 3$
$p+1 = 97$	$p = 98 - 1 = 2^5 \cdot 3$
$p+1 = 97^2 = 9409$	$p = 9408 - 1 = 2^6 \cdot 3 \cdot 7^2$
$p+1 = 2 \cdot 97 = 194$	$p = 194 - 1 = 193$
$p+1 = 2 \cdot 97^2 = 18818$	$p = 18818 - 1 = 1887 = 3 \cdot 129$
$p+1 = 2^2 \cdot 97 = 18818$	$p = 18818 - 1 = 31 \cdot 607$
$p+1 = 2^2 \cdot 97^2 = 37636$	$p = 37636 - 1 = 37565 = 5 \cdot 7527$

ดังนั้น จำนวนเฉพาะ p ที่เป็นไปได้ทั้งหมดคือ 3 และ 193

3.2 ทฤษฎีบทหลักมูลเลขคณิต

จำนวนเต็มที่มากกว่า 1 สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ และถ้าไม่คิดลำดับเป็นสำคัญแล้วการเขียนนี้ทำได้เพียงวิธีเดียวเท่านั้น ซึ่งข้อความนี้มีบทบาทในการนำไปใช้ เป็นเครื่องมือที่เกี่ยวข้องกับจำนวนเต็มที่เป็นพื้นฐานที่สำคัญในการศึกษาทฤษฎีจำนวน โดยยุคลิดได้เขียนไว้ในหนังสือ Euclid's Elements Book IX : Proposition 14 ในรูปทฤษฎีบทดังต่อไปนี้

ทฤษฎีบท 3.4 (ทฤษฎีบทหลักมูลเลขคณิต)

จำนวนเต็ม $n > 1$ สามารถเขียนในรูป

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

โดยที่ $p_1, p_2, p_3, \dots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$

และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, \dots, k$ และเขียน n ในรูปแบบดังกล่าวได้เพียงรูปแบบเดียวเท่านั้น และเรียกว่า **รูปแบบบัญญัติ(Canonical Form)** ของ n

พิสูจน์ สำหรับการพิสูจน์ทฤษฎีบทจะแบ่งออกเป็น 2 ตอน ดังนี้

- (1) จะแสดงว่าทุก ๆ จำนวนเต็ม $n > 1$ สามารถเขียนให้อยู่ในรูปผลคูณของจำนวนเฉพาะ พิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ดังนี้

ให้ $P(k)$ แทนข้อความ $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$ สำหรับทุกจำนวนเต็ม $n > 1$

ขั้นฐาน

กรณี $n = 2$ จะได้ $2 = 2^1$

นั่นคือ $p_1 = 2$ และ $a_1 = 1$ แสดงว่า $P(1)$ เป็นจริง

ขั้นอุปนัย

สมมติว่า $m + 1$ เป็นจำนวนประกอบจะได้ว่า $m + 1 = ab$ ซึ่ง $a, b \in \mathbb{N}$ และ

$$1 < a < m + 1 \text{ และ } 1 < b < m + 1$$

โดยสมมติฐานจะมีจำนวนเฉพาะ

$$p_1, p_2, p_3, \dots, p_j \text{ และ } q_1, q_2, q_3, \dots, q_l$$

ซึ่ง $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_j^{a_j}$ และ $b = q_1^{b_1} q_2^{b_2} q_3^{b_3} \cdots q_l^{b_l}$ ทำให้ได้ว่า

$$m + 1 = ab = \left(p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_j^{a_j} \right) \left(q_1^{b_1} q_2^{b_2} q_3^{b_3} \cdots q_l^{b_l} \right)$$

นั่นคือ $m + 1$ เขียนได้ในรูปของผลคูณของจำนวนเฉพาะให้ $k = j + l$

และภายใต้การจัดลำดับการคูณที่เหมาะสม จะได้ว่า

$$m + 1 = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k} \text{ ซึ่ง } p_1 < p_2 < p_3 < \cdots < p_k$$

ดังนั้น ผลลัพธ์เป็นจริง สำหรับทุก $n = m + 1$

- (2) จะแสดงว่าทุก ๆ จำนวนเต็มบวกที่มากกว่า สามารถเขียนให้อยู่ในรูปผลคูณของจำนวนเฉพาะได้เพียงชุดเดียว ดังต่อไปนี้
สมมติว่า n เขียนได้สองแบบดังนี้

$$n = p_1 p_2 p_3 \cdots p_r \quad \text{เมื่อ } p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$$

$$n = q_1 q_2 q_3 \cdots q_s \quad \text{เมื่อ } q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$$

ดังนั้น $p_1 \mid (q_1 q_2 q_3 \cdots q_s)$ โดยทฤษฎีบท 3.3

จะได้ว่า $p_1 \mid q_i$ สำหรับบางค่า i

นั่นคือ $p_1 = q_i$ แสดงว่า $p_1 \geq q_1$

ในทำนองเดียวกันพิสูจน์ได้ว่า $q_1 \geq p_1$ แสดงว่า $p_1 = q_1$

จาก

$$p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$$

จะได้

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

พิสูจน์ในทำนองเดียวกันก็จะได้ $p_2 = q_2, p_3 = q_3, \dots$

ถ้า $r < s$ จะได้ว่า $1 = q_{r+1} q_{r+2} \cdots q_s > 1$ เป็นไปไม่ได้

ถ้า $r > s$ จะได้ว่า $1 = p_{s+1} p_{s+2} \cdots p_r > 1$ เป็นไปไม่ได้

ดังนั้นจะได้ว่า $r = s$ และ $p_2 = q_2, p_3 = q_3, \dots, p_r = q_s$

แสดงได้ว่า n สามารถเขียนในรูปของผลคูณของจำนวนเฉพาะได้เพียงแบบเดียว

ตัวอย่าง 3.6 ตัวอย่างจำนวนที่เขียนในรูปแบบบัญญัติ

1. $12 = 2^2 \cdot 3$
2. $58 = 2 \cdot 29$
3. $150 = 2 \cdot 3 \cdot 5^2$
4. $1225 = 5^2 \cdot 7^2$
5. $7425 = 3^3 \cdot 5^2 \cdot 11$
6. $15750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$
7. $10750 = 2 \cdot 5^3 \cdot 83$

จากตัวอย่าง 3.6 สามารถใช้ Wolfram Alpha ในการหารูปแบบบัญญัติในที่นี้จะยกตัวอย่างเพียงข้อเดียวส่วนข้ออื่น ๆ ก็ทำคล้ายกัน ดังภาพประกอบ 3.1



ภาพประกอบ 3.1 ใช้ Wolfram Alpha เพื่อแสดง 15750 ในรูปแบบบัญญัติ

ทฤษฎีบท 3.4 เป็นเครื่องมือที่สำคัญในการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับจำนวนเต็ม เพราะสามารถทำได้โดยการพิจารณาว่าจำนวนเต็มนั้นเป็นจำนวนเฉพาะหรือผลคูณของจำนวนเฉพาะและยังสามารถหาจำนวนตัวหารทั้งหมดของจำนวนใด ๆ ได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.7 จงหาตัวหารทั้งหมดของ 504

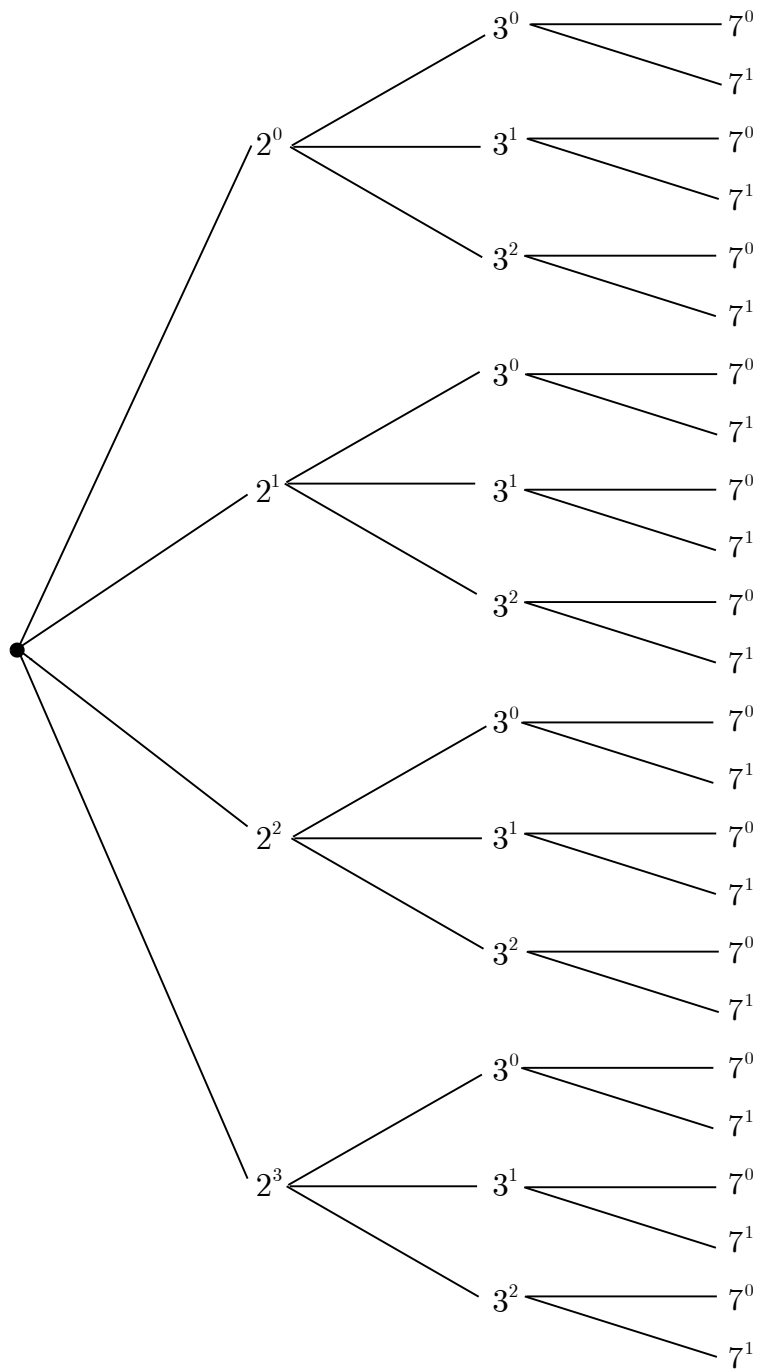
วิธีทำ เนื่องจาก $504 = 2^3 \cdot 3^2 \cdot 7$

พิจารณา

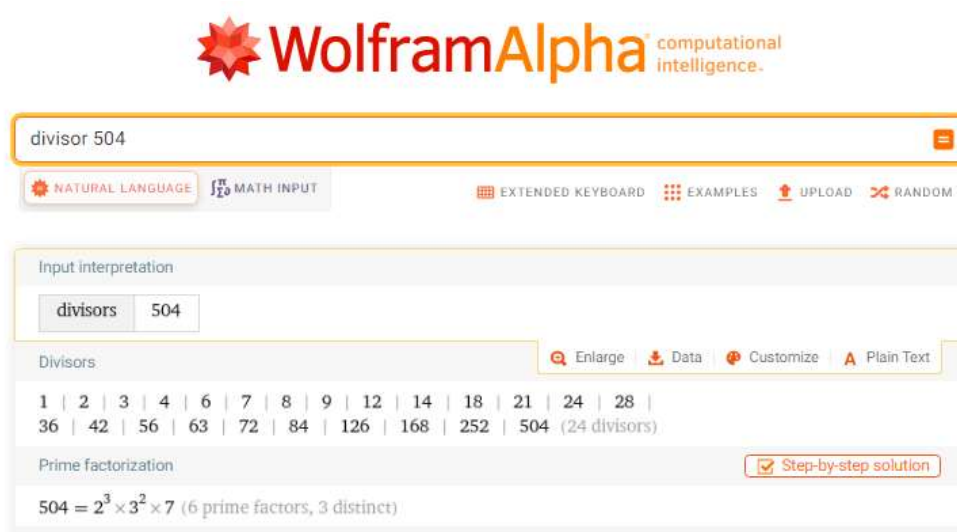
$2^0 \cdot 3^0 \cdot 7^0$	$2^0 \cdot 3^0 \cdot 7^1$	$2^0 \cdot 3^1 \cdot 7^0$
$2^1 \cdot 3^0 \cdot 7^0$	$2^1 \cdot 3^0 \cdot 7^1$	$2^1 \cdot 3^1 \cdot 7^0$
$2^2 \cdot 3^0 \cdot 7^0$	$2^2 \cdot 3^0 \cdot 7^1$	$2^2 \cdot 3^1 \cdot 7^0$
$2^3 \cdot 3^0 \cdot 7^0$	$2^3 \cdot 3^0 \cdot 7^1$	$2^3 \cdot 3^1 \cdot 7^0$
$2^0 \cdot 3^1 \cdot 7^1$	$2^0 \cdot 3^2 \cdot 7^0$	$2^0 \cdot 3^2 \cdot 7^1$
$2^1 \cdot 3^1 \cdot 7^1$	$2^1 \cdot 3^2 \cdot 7^0$	$2^1 \cdot 3^2 \cdot 7^1$
$2^2 \cdot 3^1 \cdot 7^1$	$2^2 \cdot 3^2 \cdot 7^0$	$2^2 \cdot 3^2 \cdot 7^1$
$2^3 \cdot 3^1 \cdot 7^1$	$2^3 \cdot 3^2 \cdot 7^0$	$2^3 \cdot 3^2 \cdot 7^1$

จะเห็นว่าตัวหารของ 504 มีทั้งหมด 24 ตัว ได้แก่ 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 18, 21, 24, 28, 36 และ 42

เขียนแผนภาพต้นไม้(Tree Diagram)ได้ดังนี้



จากตัวอย่าง 3.7 ใช้ Wolfram Alpha หาตัวหารทั้งหมดของ 504 ดังภาพประกอบ 3.2



ภาพประกอบ 3.2 ใช้ Wolfram Alpha เพื่อหาตัวหารทั้งหมดของ 504

การพิจารณาจากแผนภาพต้นไม้โดยใช้กฎการนับ(Multiplication Principle) สรุปได้ว่าจำนวนตัวหารทั้งหมดของ 504 มีทั้งหมด $(3 + 1)(2 + 1)(1 + 1)$ จำนวน ซึ่งสามารถสรุปเป็นทฤษฎีบทได้ดังต่อไปนี้

ทฤษฎีบท 3.5

ให้ $n \in \mathbb{N}$ ซึ่ง $n > 1$ มีรูปแบบบัญญัติคือ

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

เมื่อ $a_i \in \mathbb{N}$ ทุก ๆ i แล้วจำนวนตัวประกอบทั้งหมดของ n มีทั้งหมด

$$(a_1 + 1)(a_2 + 1)(a_3 + 1) \cdots (a_k + 1)$$

ทฤษฎีบทหลักมูลเลขคณิตสามารถนำมาประยุกต์ใช้เพื่อหาตัวหารร่วมมาก และตัวคูณร่วมน้อยได้ดังนี้

กำหนดให้ n และ m เป็นจำนวนเต็มที่ $n > 1$ และ $m > 1$ เขียนในรูปแบบบัญญัติได้ดังนี้

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k} \text{ และ } m = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_k^{b_k}$$

เมื่อแต่ละจำนวนเต็ม $a_i \geq 0$ และ $b_i \geq 0$ โดยที่ไม่เป็นศูนย์พร้อมกันจะได้ว่า

$$(n, m) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} p_3^{\min\{a_3, b_3\}} \cdots p_k^{\min\{a_k, b_k\}}$$

$$[n, m] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} p_3^{\max\{a_3, b_3\}} \cdots p_k^{\max\{a_k, b_k\}}$$

จากการหาตัวหารร่วมมากและตัวคูณร่วมน้อยจากการใช้ทฤษฎีบทหลักมูลเลขคณิตทำให้ข้อสรุปอีกว่า $(n, m)[n, m] = mn$

ตัวอย่าง 3.8 จงใช้ทฤษฎีบทหลักมูลเลขคณิตเพื่อหาค่า $(308, 1176)$ และ $[308, 1176]$

วิธีทำ เนื่องจาก $308 = 2^2 \cdot 7 \cdot 11$ และ $1176 = 2^3 \cdot 3 \cdot 7^2$
 หรือ $308 = 2^2 \cdot 3^0 \cdot 7 \cdot 11$ และ $1176 = 2^3 \cdot 3 \cdot 7^2 \cdot 11^0$
 จะได้ $(308, 1176) = 2^{\min\{2,3\}} \cdot 3^{\min\{0,1\}} \cdot 7^{\min\{1,2\}} \cdot 11^{\min\{1,0\}}$
 $= 2^2 \cdot 3^0 \cdot 7^1 \cdot 11^0$
 $= 28$
 และ $[308, 1176] = 2^{\max\{2,3\}} \cdot 3^{\max\{0,1\}} \cdot 7^{\max\{1,2\}} \cdot 11^{\max\{1,0\}}$
 $= 2^3 \cdot 3^1 \cdot 7^2 \cdot 11^1$
 $= 12936$
 ดังนั้น $(308, 1176) = 28$ และ $[308, 1176] = 12936$

ทฤษฎีบทหลักมูลยังสามารถหาตัวหารร่วมมาก และตัวคูณร่วมน้อยของจำนวนเต็มที่มีมากกว่าสองจำนวนได้ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.9 จงใช้ทฤษฎีบทหลักมูลเลขคณิตเพื่อหาค่า $(18, 42, 64)$ และ $[18, 42, 64]$

วิธีทำ เนื่องจาก $18 = 2 \cdot 3^2 \cdot 7^0$
 $42 = 2 \cdot 3 \cdot 7$
 $64 = 2^6 \cdot 3^0 \cdot 7^0$
 จะได้ $(18, 42, 64) = 2^{\min\{1,1,6\}} \cdot 3^{\min\{2,1,0\}} \cdot 7^{\min\{0,1,0\}}$
 $= 2^1 \cdot 3^0 \cdot 7^0$
 $= 2$
 และ $[18, 42, 64] = 2^{\max\{1,1,6\}} \cdot 3^{\max\{2,1,0\}} \cdot 7^{\max\{0,1,0\}}$
 $= 2^6 \cdot 3^2 \cdot 7$
 $= 4032$
 ดังนั้น $(18, 42, 64) = 2$ และ $[18, 42, 64] = 4032$

3.3 การค้นหาจำนวนเฉพาะ

จากที่ทราบอยู่แล้วว่าจำนวนเฉพาะคือจำนวนเต็มบวกที่มีตัวหารที่เป็นบวกอยู่สองจำนวนคือ 1 กับตัวมันเอง สำหรับการจะตรวจสอบว่าจำนวนเต็มบวกใดเป็นจำนวนเฉพาะนั้นอาจทำได้โดยการแยกตัวประกอบถ้าจำนวนนั้นสามารถแยกเป็นตัวประกอบสองตัวที่ไม่ใช่ 1 กับตัวมันเอง จำนวนนั้นก็จะไม่ใช่จำนวนเฉพาะซึ่งวิธีดังกล่าวนี้เหมาะสำหรับการตรวจสอบจำนวนเฉพาะที่มีค่าไม่มาก สำหรับทฤษฎีบทต่อไปนี้จะเป็นอีกหนึ่งวิธีสำหรับนำไปใช้ในการตรวจสอบจำนวนเฉพาะที่มีประสิทธิภาพ และลดขั้นตอนการตรวจสอบได้

ตัวอย่าง 3.10

$15 = 5 \times 3$ แสดงว่า 15 ไม่เป็นจำนวนเฉพาะ

$13 = 13 \times 1$ แสดงว่า 13 เป็นจำนวนเฉพาะ

ทฤษฎีบท 3.6

ถ้า n เป็นจำนวนประกอบ แล้วจะมีจำนวนเฉพาะ p ที่ $p \leq \sqrt{n}$ และ $p|n$

พิสูจน์

ให้ a เป็นจำนวนประกอบจะได้ว่ามี $1 < n \leq m < a$ ซึ่งทำให้ $a = nm$

ดังนั้น $m|a$ และ $n|a$

แสดงว่ามี $1 < n^2 \leq mn = a$

ดังนั้น $n \leq \sqrt{a}$ จากทฤษฎีบท 3.1

จะได้ว่ามีจำนวนเฉพาะ p ซึ่ง $p|n$ ทำให้ได้ว่า $p|a$ และ $p \leq \sqrt{a}$

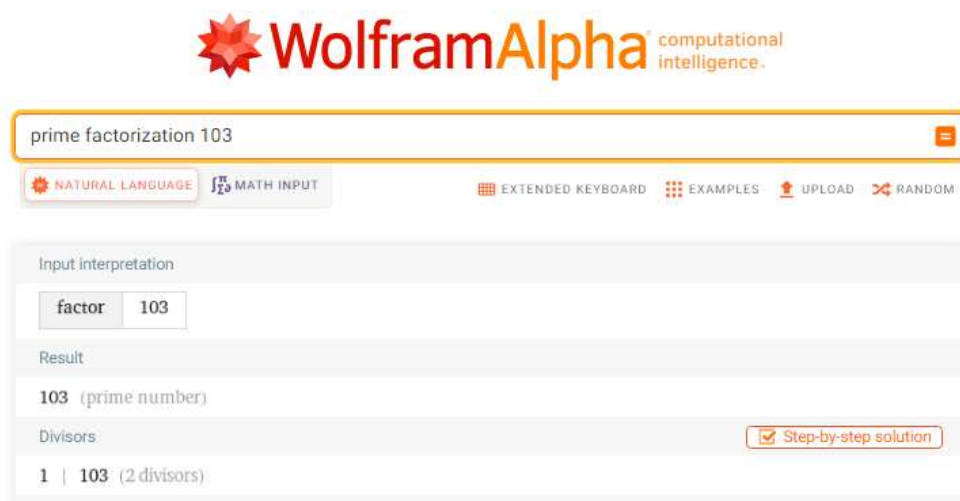
ตัวอย่าง 3.11 จงตรวจสอบว่า 103 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{103} < 11$

จำนวนเฉพาะที่น้อยกว่า 11 คือ 2, 3, 5, 7 ซึ่งไม่มีจำนวนใดหาร 103 ลงตัว

ดังนั้น 103 เป็นจำนวนเฉพาะ

จากตัวอย่าง 3.11 ใช้ Wolfram Alpha ตรวจสอบว่า 103 เป็นจำนวนเฉพาะหรือไม่
ดังภาพประกอบ 3.3



ภาพประกอบ 3.3 ใช้ Wolfram Alpha เพื่อแสดงว่า 103 เป็นจำนวนเฉพาะ

ตัวอย่าง 3.12 จงตรวจสอบว่า 2807 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เนื่องจาก $\sqrt{2807} < 53$

จำนวนเฉพาะที่น้อยกว่า 53 คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

เนื่องจาก $7 \nmid 2807$

ดังนั้น 2807 ไม่เป็นจำนวนเฉพาะ

จากตัวอย่าง 3.12 ใช้ Wolfram Alpha ตรวจสอบว่า 2807 เป็นจำนวนเฉพาะหรือไม่

ดังภาพประกอบ 3.4



ภาพประกอบ 3.4 ใช้ Wolfram Alpha เพื่อแสดงว่า 2807 ไม่เป็นจำนวนเฉพาะ

วิธีการตรวจสอบจำนวนเฉพาะตามทฤษฎีบท 3.6 เรียกว่า ตะแกรงเอราทอสเทนีส(Sieve of Eratosthenes) ซึ่งวิธีดังกล่าวนี้ยังสามารถนำไปใช้ในการหาจำนวนเฉพาะทั้งหมดที่น้อยกว่าจำนวนเต็มบวก n ที่กำหนดให้โดยมีหลักเกณฑ์ดังนี้

1. เขียนจำนวนเฉพาะทั้งหมดตั้งแต่ 2 ถึง n
2. ตัดจำนวนคู่หรือพหุคูณของ 2 ทั้งหมดทิ้งไป ยกเว้น 2 แล้ววงล้อมรอบ 2 ไว้
3. ตัดพหุคูณของ 3 ทิ้งไป แล้ววงล้อมรอบ 3 ไว้
4. ตัดพหุคูณของ 5 ทิ้งไป แล้ววงล้อมรอบ 5 ไว้
5. ทำเช่นนี้ไปเรื่อย ๆ จนถึงจำนวนเฉพาะ p มีค่ามากที่สุด และ $p \leq \sqrt{n}$ แล้วจึงหยุดทำ

ตัวอย่าง 3.13 จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 50

วิธีทำ $n = 50$ และ $p \leq \sqrt{50}$ คือ 2, 3, 5, 7 โดยมีหลักเกณฑ์ดังนี้

1. เขียนจำนวนเฉพาะทั้งหมดตั้งแต่ 2 ถึง 50
2. ตัดจำนวนคู่หรือพหุคูณของ 2 ทั้งหมดทิ้งไป ยกเว้น 2 แล้ววงล้อมรอบ 2 ไว้

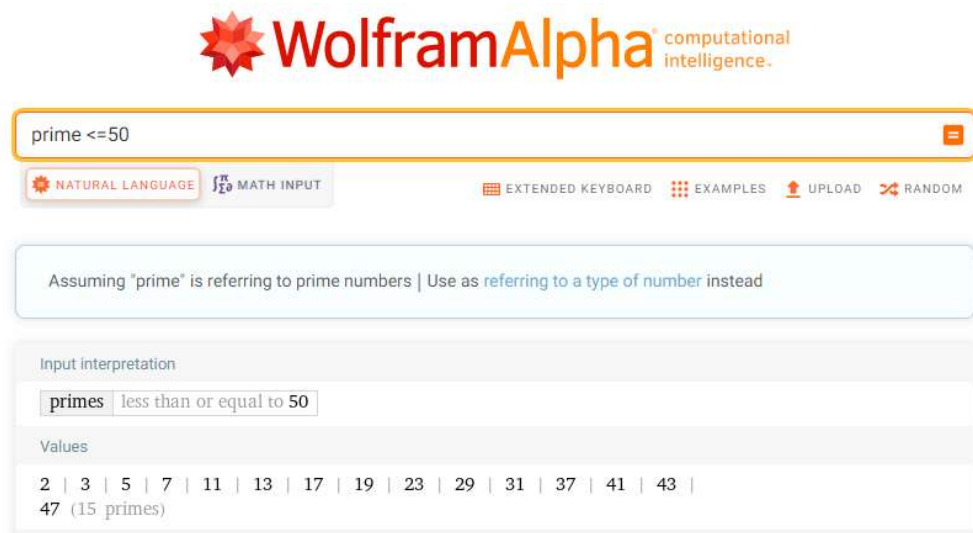
3. ตัดพหุคูณของ 3 ทิ้งไป แล้ววงล้อมรอบ 3 ไว้
4. ตัดพหุคูณของ 5 ทิ้งไป แล้ววงล้อมรอบ 5 ไว้
5. ตัดพหุคูณของ 7 ทิ้งไป แล้ววงล้อมรอบ 7 ไว้

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

จำนวนที่เหลือจะเป็นจำนวนเฉพาะ

ดังนั้น จำนวนเฉพาะที่น้อยกว่า 50 คือ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

จากตัวอย่าง 3.13 ใช้ Wolfram Alpha หาคำนวณเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 50
ดังภาพประกอบ 3.5



ภาพประกอบ 3.5 ใช้ Wolfram Alpha เพื่อหาคำนวณเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 50

ทฤษฎีบทหนึ่งที่สำคัญของจำนวนเฉพาะที่จะกล่าวต่อไป คือ “มีจำนวนเฉพาะอยู่ในจำนวนอนันต์” โดยยุคลิด ได้รับการยกย่องว่าเป็นนักคณิตศาสตร์คนแรกที่พิสูจน์ว่า “มีจำนวนเฉพาะอยู่ในจำนวนอนันต์” ซึ่งบทพิสูจน์นั้นปรากฏในหนังสือ Euclid’s Elements

ทฤษฎีบท 3.7

มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ (หรือไม่มีจำนวนเฉพาะที่มีค่ามากที่สุด)

พิสูจน์

สมมติว่ามีจำนวนเฉพาะอยู่เป็นจำนวนจำกัด

นั่นคือ ให้ $p_1, p_2, p_3, \dots, p_n$ เป็นลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปหามาก

และ p_n เป็นจำนวนเฉพาะที่มีค่ามากที่สุด

ให้ $N = (p_1 p_2 p_3 \cdots p_n) + 1$ จะได้ว่า $N > p_n$ แสดงว่า N เป็นจำนวนประกอบ

โดยทฤษฎีบท 3.1 จะมีจำนวนเฉพาะ p ซึ่ง $p \mid N$

และจากสมมติฐานจะได้ว่า $p \in \{p_1, p_2, \dots, p_n\}$

ดังนั้น $p \mid p_1 p_2 \cdots p_n$ แสดงว่า $p \mid 1$ ซึ่งเป็นไปไม่ได้

นั่นคือ มีจำนวนเฉพาะอยู่เป็นจำนวนอนันต์

ณรงค์ ปันนิม และนิตยา ปภาพจน์ (2553 : 73-74) กล่าวว่าบทพิสูจน์ว่าจำนวนเฉพาะมีจำนวนอนันต์ของยุคลิดนั้น ได้รับการยอมรับกว่า 2000 ปีมาแล้ว ต่อมานักคณิตศาสตร์รุ่นหลังได้พยายามที่จะหาแนวทางการพิสูจน์ใหม่ของทฤษฎีบทดังกล่าวโดยอย่างน้อยที่เห็นปรากฏในหนังสือ Proofs from THE BOOK (Aigner M. and Ziegler G.M. 1998) ได้กล่าวถึงบทพิสูจน์ของทฤษฎีบทดังกล่าวนี้ที่แตกต่างกันไว้ถึง 6 แบบด้วยกัน ทฤษฎีบทนี้ ถือว่ามีความสำคัญยิ่งของการนำไปสู่ข้อคาดเดาต่างๆ มากมาย

บทตั้ง 3.1

ให้ $p_1, p_2, p_3, \dots, p_n, p_{n+1}, \dots$ เป็นลำดับของจำนวนเฉพาะที่เรียงจากน้อยไปมาก

จะได้ว่า $p_{n+1} \leq (p_1 p_2 p_3 \cdots p_n) + 1$

ทฤษฎีบท 3.8

ให้ $p_1, p_2, p_3, \dots, p_n, \dots$ แทนลำดับของจำนวนเฉพาะทั้งหมดที่เรียงจากน้อยไปมาก

จะได้ว่า $p_n \leq 2^{2^{n-1}}$ สำหรับทุกจำนวนเต็มบวก n

พิสูจน์ พิสูจน์โดยใช้หลักอุปนัยเชิงคณิตศาสตร์ดังนี้

ให้ $P(n)$ แทนข้อความ $p_n \leq 2^{2^{n-1}}$

ขั้นฐาน

$$2 \leq 2^{2^0} = 2 \text{ เป็นจริง แสดงว่า } P(1)$$

ขั้นอุปนัย

สมมติให้ $P(k)$ เป็นจริง

นั่นคือ $p_k \leq 2^{2^{k-1}}$ เป็นจริงสำหรับทุก $k \leq n$

จะต้องพิสูจน์ว่า $p_{k+1} \leq 2^{2^k}$

$$\text{จาก } p_1 \leq 2^{2^{1-1}}, p_2 \leq 2^{2^{2-1}}, p_3 \leq 2^{2^{3-1}}, \dots, p_n \leq 2^{2^{n-1}}$$

$$\text{จะได้ } p_1 p_2 p_3 \cdots p_n \leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{k-1}}$$

$$= 2^{2^0 + 2^1 + 2^2 + \dots + 2^{k-1}}$$

$$= 2^{2^k - 1}$$

$$\text{ดังนั้น } p_1 p_2 p_3 \cdots p_k + 1 \leq 2^{2^k - 1} + 2^{2^k - 1} = 2^{2^k}$$

$$\text{นั่นคือ } p_1 p_2 p_3 \cdots p_n + 1 \leq 2^{2^k}$$

$$\text{โดยบทตั้ง 3.1 จะได้ว่า } p_{k+1} \leq 2^{2^k}$$

$$\text{แสดงว่า } p_n \leq 2^{2^{n-1}} \text{ สำหรับทุก } n \in \mathbb{N}$$

ตัวอย่าง 3.14

$$1. p_{30} = 113 \leq 2^{2^{30-1}}$$

$$2. p_{100} = 541 \leq 2^{2^{100-1}}$$

บทแทรก 3.1

สำหรับจำนวนเต็มบวก n จะมีจำนวนเฉพาะอย่างน้อยที่สุด $n + 1$ จำนวน
ที่มีค่าน้อยกว่า 2^{2^n}

ในปี ค.ศ. 1845 โจเซฟ เบร์ทรานด์ (Joseph Bertrand ค.ศ. 1822 – 1900) ได้ตั้งข้อคาดเดาว่า “จะมีจำนวนเฉพาะหนึ่งจำนวนที่อยู่ระหว่าง n กับ $2n$ เมื่อ $n \geq 2$ ” ซึ่งเขามีความเชื่อมั่นว่าข้อคาดเดาที่ตั้งขึ้นเป็นจริง โดยการแสดงให้เห็นจริงได้เมื่อ $n \leq 3,000,000$ โดยพบจำนวนเฉพาะที่อยู่ระหว่าง n กับ $2n$ คือ 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159389, ... ต่อมาในปี ค.ศ. 1850 พัพนุติ ลีโววิช เซบีเชฟ (Pafnuti

Lvovich Tschebychev ค.ศ. 1821 – 1894) นักคณิตศาสตร์ชาวรัสเซีย สามารถพิสูจน์ข้อคาดเดาของเบอร์ทรานได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.9

ให้ $n \in \mathbb{N}$ และ $n \geq 2$ จะได้ว่า มีจำนวนเฉพาะอย่างน้อยหนึ่งจำนวนในลำดับ $n, n+1, n+2, \dots, 2n$

บทพิสูจน์ของทฤษฎีบท 3.9 นี้ เซปีเซฟ ได้ใช้ความรู้สึกที่ลึกซึ้งและยาวมาก ต่อมาในปี ค.ศ. 1932 พอล เออร์ดอส (Paul Erdos ค.ศ. 1913 – 1996) นักคณิตศาสตร์ชาวฮังการี ได้แสดงการพิสูจน์ทฤษฎีบทนี้ที่ง่ายกว่าของเซปีเซ ซึ่งในขณะนั้นเขามีอายุเพียง 19 ปี และผลงานชิ้นนี้ถือว่าเป็นผลงานชิ้นแรกของเขาที่ได้รับการตีพิมพ์ สำหรับบทพิสูจน์ของทฤษฎีบทนี้ สามารถศึกษาได้จากหนังสือ Proofs from THE BOOK (Aigner M. and Ziegler G.M. 2013 : 7-10)

Silverman J.H. (2006 : 91-92) ได้กล่าวถึงทฤษฎีบทที่สำคัญอีกทฤษฎีบทหนึ่งซึ่งมีชื่อว่า ทฤษฎีบทของจำนวนเฉพาะ ซึ่งเกิดขึ้นจากการตั้งข้อคาดเดาของเกาส์ในปี ค.ศ. 1792 แต่ยังไม่มีการพิสูจน์ที่สมบูรณ์ ต่อมาในปี ค.ศ. 1896 ทฤษฎีบทนี้สามารถพิสูจน์ได้โดย อาตามาร์ด (Hadamard J.S. ค.ศ. 1865 – 1963) และ ปูแซง (Poussin C.V ค.ศ. 1866 – 1962) ให้การพิสูจน์ที่แตกต่างกัน แต่ใช้ความรู้ด้านการวิเคราะห์เชิงซ้อนเหมือนกัน ต่อมาในปี ค.ศ. 1949 อาเทิล เซลเบอร์ก และ เออร์ดอส ได้พิสูจน์ทฤษฎีบทนี้โดยใช้ความรู้ทางเลขคณิตเท่านั้น จากผลงานของเซลเบอร์กในครั้งนี้ ทำให้เขาได้รับรางวัลสูงสุดคือ Fields Medal ซึ่งเทียบเท่ากับรางวัลโนเบล ปี ค.ศ. 1950 ในงาน International Congress of Mathematics ซึ่งจะจัดประจำปีทุก 4 ปี และสำหรับนักคณิตศาสตร์ที่อายุต่ำกว่า 40 ปี

ทฤษฎีบท 3.10 (ทฤษฎีบทของจำนวนเฉพาะ)

ให้ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p ซึ่ง $p \leq n$ จะได้ว่า

$\pi(n)$ มีค่าประมาณ $\frac{n}{\log n}$ เมื่อ n มีค่ามาก ๆ และ $\log n$ หมายถึงลอการิทึม

ฐานธรรมชาติของ n นั่นคือ $\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1$

Burton D.M. (2011 : 375-383) ได้แสดงการพิสูจน์ของทฤษฎีบทดังกล่าวนี้ ในหนังสือ Elementary Number Theory

บทตั้ง 3.2

ผลคูณของจำนวนเต็มที่เขียนอยู่ในรูป $4k + 1$ ตั้งแต่สองจำนวนขึ้นไป
จะเป็นจำนวนเต็มที่เขียนอยู่ในรูป $4k + 1$

พิสูจน์

ให้ $n_1 = 4k_1 + 1$ และ $n_2 = 4k_2 + 1$ เมื่อ k_1 และ k_2 เป็นจำนวนเต็ม

$$\text{ดังนั้น } n_1 n_2 = (4k_1 + 1)(4k_2 + 1)$$

$$= 4(4k_1 k_2 + k_1 + k_2) + 1$$

$$= 4k + 1 \text{ เมื่อ } k = 4k_1 k_2 + k_1 + k_2 \text{ เป็นจำนวนเต็ม}$$

ทฤษฎีบท 3.11

มีจำนวนเฉพาะที่เขียนอยู่ $4k + 3$ เป็นจำนวนอนันต์

พิสูจน์

สมมติว่ามีจำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 3$ เป็นจำนวนจำกัด

นั่นคือ ให้ $p_1, p_2, \dots, p_n$ เป็นจำนวนเฉพาะที่เขียนอยู่ในรูป $4k + 3$ ทั้งหมด

ที่เรียงจากน้อยไปหามากและ p_n มีค่ามากที่สุด

$$\text{ให้ } N = 4p_1 p_2 \cdots p_n - 1 = 4(p_1 p_2 \cdots p_n - 1) + 3$$

จะได้ว่า $N > 1$ และ $N > p_n$

แสดงว่า N เป็นจำนวนประกอบ จะได้ว่า

N สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

นั่นคือ $N = q_1 q_2 \cdots q_t$ เมื่อ $q_1, q_2, \dots, q_t$ เป็นจำนวนเฉพาะ

เนื่องจาก N เป็นจำนวนคี่

ดังนั้น q_i จะเขียนอยู่ในรูป $4k + 1$ หรือ $4k + 3$

ถ้าทุก q_i อยู่ในรูป $4k + 1$ โดยบทตั้ง 3.2 จะได้ว่า N จะเขียนอยู่ในรูป $4k + 1$ ซึ่งไม่จริง

ดังนั้น จะมี $q_r \in \{q_1, q_2, \dots, q_t\}$ ซึ่งเขียนอยู่ในรูป $4k + 3$

เพราะฉะนั้นมี $j \in \{1, 2, \dots, n\}$ ซึ่ง $q_r = p_j$

นั่นคือ $p_j \mid N$ แต่ $p_j \nmid p_1 p_2 \cdots p_n$ ดังนั้น $p_j \nmid 1$ ซึ่งเป็นไปไม่ได้

สรุปได้ว่ามีจำนวนเฉพาะที่อยู่ในรูป $4k + 3$ อยู่เป็นจำนวนอนันต์

ใน ค.ศ. 1837 ดีริชเลต์ เป็นผู้นำเสนอทฤษฎีรูปแบบของจำนวนเฉพาะที่เป็นจำนวนอนันต์ สำหรับรายละเอียดของการพิสูจน์ปัญหานี้มีรายละเอียดและขั้นตอนที่ซับซ้อน ผู้เขียนจึงแสดงเฉพาะทฤษฎีบทเท่านั้นซึ่งมีรายละเอียดดังต่อไปนี้

ทฤษฎีบท 3.12

ถ้า $a, b \in \mathbb{N}$ และ $(a, b) = 1$ แล้วจะมีจำนวนเฉพาะปรากฏอยู่ในลำดับเลขคณิตอนันต์ $a, a + b, a + 2b, a + 3b, \dots$ เป็นจำนวนอนันต์

สำหรับทฤษฎีบทดังกล่าวนี้ ถ้าเลือก $a = 999$ และ $b = 1000$ จะพบว่าจำนวนเฉพาะอยู่เป็นจำนวนอนันต์ที่ลงท้ายด้วย 999 เช่น 1999, 100999, 1000999, ... ปรากฏอยู่ในลำดับเลขคณิตอนันต์ที่มีพจน์ที่ n คือ $1000n + 999$ ในทางกลับกันไม่มีลำดับเลขคณิตอนันต์ใดที่จะทำให้สมาชิกในลำดับนั้นทุกตัวเป็นจำนวนเฉพาะ ให้ $a, a + b, a + 2b, \dots$ เป็นลำดับเลขคณิตอนันต์ โดยที่ $a, b \in \mathbb{N}$ จะได้ว่า พจน์ที่ $a + 1$ คือ $a + ab = a(1 + b)$ ดังนั้น ถ้า $a > 1$ แล้ว $a(1 + b)$ ไม่เป็นจำนวนเฉพาะ

3.4 จำนวนเฉพาะแฟร์มาและจำนวนเฉพาะแมร์แซน

นับตั้งแต่อดีตจนถึงในปัจจุบันได้มีคณิตศาสตร์ที่ศึกษาจำนวนเต็มในรูปแบบต่าง ๆ เพื่อนำไปอธิบายเกี่ยวกับจำนวนเฉพาะ โดยในปี ค.ศ. 1640 แฟร์มาได้ศึกษาจำนวนเต็มที่อยู่ในรูป $2^{2^n} + 1$ มีรายละเอียดดังบทนิยามต่อไปนี้

บทนิยาม 3.2

จำนวนแฟร์มา คือจำนวนเต็มที่อยู่ในรูป $F_n = 2^{2^n} + 1$ เมื่อ $n \geq 0$
ถ้า F_n เป็นจำนวนเฉพาะ จะเรียก F_n ว่า จำนวนเฉพาะแฟร์มา

ตัวอย่าง 3.15 จงหาจำนวนเฉพาะแฟร์มา $F_n = 2^{2^n} + 1$ เมื่อ $n = 0, 1, 2, 3, 4$

วิธีทำ เมื่อ $n = 0$ จำนวนเฉพาะแฟร์มาคือ $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$

เมื่อ $n = 1$ จำนวนเฉพาะแฟร์มาคือ $F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$

เมื่อ $n = 2$ จำนวนเฉพาะแฟร์มาคือ $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$

เมื่อ $n = 3$ จำนวนเฉพาะแฟร์มาคือ $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$

เมื่อ $n = 4$ จำนวนเฉพาะแฟร์มาคือ $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$

Childs (1995:57) ได้กล่าวว่า แฟร์มาพบว่าจำนวนเต็ม $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ ต่างก็เป็นจำนวนเฉพาะ และเขายังตั้งข้อคาดเดาต่ออีกว่า $2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1, \dots$ เป็นจำนวนเฉพาะทุกจำนวน แต่ต่อมาในปี ค.ศ. 1732 ออยเลอร์ ได้พบว่า

$$F_5 = 2^{2^5} + 1 = 4,294,967,297 = (641)(6700417)$$

เป็นจำนวนตัวประกอบซึ่งทำให้ข้อคาดเดาของแฟร์มาไม่เป็นจริง ต่อมาในช่วง ค.ศ. 1878 ลูคัส (Edouard Lucas ค.ศ. 1842 - 1891) นักคณิตศาสตร์ชาวฝรั่งเศส ได้พิสูจน์ว่า F_6 เป็นจำนวนประกอบด้วยเช่นกัน เนื่องจาก

$$F_6 = 2^{2^6} + 1 = (274177)(67280421310721)$$

จากการศึกษาค้นคว้าต่อมาพบว่า F_n เป็นจำนวนประกอบ สำหรับ $5 \leq n \leq 20$ และมีผู้พิสูจน์ได้ว่า F_{23472} เป็นจำนวนประกอบ อย่างไรก็ตาม ยังไม่มีผู้ใดพิสูจน์ได้ว่า มีจำนวนเฉพาะที่อยู่ในรูป $2^{2^n} + 1$ มีเป็นจำนวนอนันต์หรือไม่ แต่ยังไม่มีการค้นพบจำนวนเฉพาะแฟร์มาตัวอื่น ๆ อีกเลย ดังนั้นอาจกล่าวได้ว่า จำนวนเฉพาะแฟร์มาที่ค้นพบในปัจจุบัน ตัวที่ใหญ่ที่สุดคือ $F_4 = 65537$ และข้อคาดเดาที่ดีที่สุดคือ จำนวนแฟร์มา $F_n > F_4$ เป็นจำนวนประกอบ ถ้าข้อคาดเดานี้เป็นจริง แสดงว่าจำนวนเฉพาะแฟร์มาจะได้จำกัดเพียง 5 จำนวนเท่านั้น และมีผู้พยายามที่จะค้นหาคุณลักษณะของ F_n ในกรณีที่ n มีค่าน้อย ๆ เช่น

$$F_7 = 2^{2^7} + 1 = (59,649,589,127,497,217)(5,704,689,200,685,129,654,721)$$

$$F_8 = 2^{2^8} + 1 = (1,238,926,361,552,897)M \text{ เมื่อ } M \text{ เป็นจำนวนเต็มบวกที่มี 62 หลัก}$$

$$F_{17} = 2^{2^{17}} + 1 = (31,065,037,602,817)N \text{ เมื่อ } N \in \mathbb{N}$$

สมบัติที่สำคัญอีกประการของจำนวนแฟร์มาคือ จำนวนแฟร์มาจะเป็นจำนวนเฉพาะสัมพัทธ์ซึ่งกันและกัน แสดงไว้ในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.13

ให้ F_m และ F_n เป็นจำนวนแฟร์มาโดยที่ $m > n \geq 0$ จะได้ว่า $(F_m, F_n) = 1$

พิสูจน์

ให้ $d = (F_m, F_n)$ เนื่องจากจำนวนแฟร์มาเป็นจำนวนคี่

ดังนั้น d จะต้องเป็นจำนวนคี่ด้วย

ให้ $x = 2^{2^n}$ และ $k = 2^{m-n}$ จะได้ว่า

$$\frac{F_m - 2}{F_n} = \frac{(2^{2n})^{2m-n} - 1}{2^{2n} - 1}$$

ดังนั้น

$$\frac{F_m - 2}{F_n} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \dots + x - 1$$

แสดงว่า $F_n \mid (F_m - 2)$

จาก $d \mid F_n$ จะได้ $d \mid (F_m - 2)$

และจาก $d \mid F_n$ และ $d \mid (F_m - 2)$ แสดงว่า $d \mid 2$

แต่ d เป็นจำนวนคี่

ดังนั้น $d = 1$ เพราะฉะนั้น $(F_m, F_n) = 1$

ตัวอย่าง 3.16

$F_0 = 3$ และ $F_1 = 5$ จากทฤษฎีบท 3.13 จะได้ว่า $(3, 5) = 1$

$F_1 = 5$ และ $F_2 = 17$ จากทฤษฎีบท 3.13 จะได้ว่า $(5, 17) = 1$

สำหรับทฤษฎีบทต่อไปเป็นทฤษฎีบทที่นำมาพิจารณาตัวประกอบหรือตัวหารของจำนวนแฟร์มา โดยในช่วงปี ค.ศ. 1747 ออยเลอร์ ได้กล่าวว่า ตัวประกอบเฉพาะทุกตัวของ F_n สามารถเขียนให้อยู่ในรูปแบบ $k \cdot 2^{n+2} + 1$ และในอีก 100 ปีถัดมาได้มีนักคณิตศาสตร์ชาวฝรั่งเศส เอดูอาร์ด ลูคัส (Francois Edouard Anatole, ค.ศ. 1842 - 1891) ได้แสดงว่า k สามารถเป็นจำนวนคู่ได้ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.14

ตัวหารเฉพาะ p ของจำนวนแฟร์มา $F_n = 2^{2^n} + 1$ เมื่อ $n \geq 2$ สามารถเขียนได้ในรูป $p = k \cdot 2^{n+2} + 1$

สำหรับในทฤษฎีบทนี้จะช่วยในการศึกษา $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$ ได้ง่ายมากยิ่งขึ้น ซึ่งตัวหารเฉพาะของ F_4 จะต้องอยู่ในรูปแบบ $k \cdot 2^{4+2} + 1 = 64k + 1$ ซึ่งมีจำนวนเฉพาะเพียงจำนวนเดียวเท่านั้นที่น้อยกว่าหรือเท่ากับ $\sqrt{F_4}$ คือ จำนวนเฉพาะ 193 สรุปได้ว่า F_4 เป็นจำนวนเฉพาะเช่นเดียวกัน แต่ในปัจจุบันนี้ความสามารถทางด้านเทคโนโลยี มีเพิ่มมากขึ้นทำให้สามารถหาตัวประกอบเฉพาะของจำนวนแฟร์มาได้สะดวกยิ่งขึ้นโดยสามารถแสดงลักษณะการค้นพบจำนวน F_n เมื่อ $0 \leq n \leq 35$ ซึ่งแสดงไว้ดังตาราง 3.1

ตาราง 3.1 ลักษณะการค้นพบของจำนวนแฟร์มา F_n เมื่อ $0 \leq n \leq 30$

n	ลักษณะของ F_n
0,1,2,3,4	เป็นจำนวนเฉพาะ
5,6,7,8,9,11	แยกเป็นผลคูณของจำนวนเฉพาะได้
10,12,13,19,30	ทราบตัวประกอบเพียง 2 หรือ 4 ตัวประกอบ
15,16,17,18,21,23,25,26,27	ทราบเพียง 1 ตัวประกอบที่เป็นจำนวนเฉพาะ
14,20	เป็นจำนวนประกอบแต่ไม่ทราบว่ามีส่วนประกอบอะไรบ้าง
22,24,28,29	ไม่ทราบลักษณะใด ๆ เลย

ที่มา : Burton D. M. (2011 : 242)

มาริน แมร์แซน (Marin Mersenne ค.ศ. 1588 – 1648) บาทหลวงชาวฝรั่งเศส เป็นนักคณิตศาสตร์คนหนึ่งที่มีความสนใจในการสร้างลำดับของจำนวนเต็มที่จะเป็นลำดับของจำนวนเฉพาะ โดยเขาศึกษาลำดับของจำนวนเต็มที่อยู่ในรูป $M_n = 2^n - 1$ เมื่อ $n \in \mathbb{N}$ จึงได้ตั้งชื่อเพื่อเป็นเกียรติแก่แมร์แซนดังบทนิยามต่อไปนี้

บทนิยาม 3.3

จำนวนเต็มที่อยู่ในรูป $M_n = 2^n - 1$ โดยที่ $n \geq 1$ เรียกว่า **จำนวนแมร์แซน** (Mersenne numbers) และถ้า M_n เป็นจำนวนเฉพาะ เรียก M_n นี้ว่า **จำนวนเฉพาะแมร์แซน** (Mersenne numbers)

ตัวอย่าง 3.17 จำนวนแมร์แซน $M_n = 2^n - 1$ เมื่อ $n = 0,1,2,3,4$ จำนวนใดบ้างเป็นจำนวนเฉพาะแมร์แซน

วิธีทำ $M_1 = 2^1 - 1 = 1$

$$M_2 = 2^2 - 1 = 3$$

$$M_3 = 2^3 - 1 = 7$$

$$M_4 = 2^4 - 1 = 15$$

ดังนั้น M_2 และ M_3 เป็นจำนวนเฉพาะแมร์แซน

จากตัวอย่าง M_2 และ M_3 เป็นจำนวนเฉพาะ แต่ M_4 เป็นจำนวนประกอบ พบว่า 2 และ 3 เป็นจำนวนเฉพาะ ส่วน 4 นั้นเป็นจำนวนประกอบ ซึ่งสอดคล้องทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.15

ถ้า M_n เป็นจำนวนเฉพาะแล้ว n เป็นจำนวนเฉพาะ

จากทฤษฎีบท 3.15 จะได้ว่าจำนวน M_p จะเป็นจำนวนเฉพาะแมร์แซนได้ ก็ต่อเมื่อ มีจำนวนเฉพาะ p ที่ทำให้ M_p เป็นจำนวนเฉพาะ เช่น

$$M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, M_{11} = 8191,$$

แมร์แซนได้ตั้งข้อสังเกตว่า มีเพียง M_p ที่เป็นจำนวนเฉพาะเมื่อ $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ และ 257 เท่านั้น และเป็นจำนวนประกอบสำหรับจำนวนเฉพาะ p อื่น ๆ ที่น้อยกว่า 257 นักคณิตศาสตร์คนอื่น ๆ ในสมัยนั้นเชื่อว่าแมร์แซนไม่ได้ทดสอบความเป็นจำนวนเฉพาะของจำนวนเหล่านั้นทุกจำนวน ต่อมาในปี ค.ศ. 1772 ออยเลอร์ได้พิสูจน์ว่า M_{31} เป็นจำนวนเฉพาะ โดยทดสอบกับตัวหารที่เป็นจำนวนเฉพาะจนถึง 46339 แต่ M_{67}, M_{127} และ M_{257} เป็นจำนวนที่มีค่ามากเกินไปที่จะตรวจสอบได้ การค้นคว้าต่อมาได้มีผู้พยายามตรวจสอบ M_p สำหรับจำนวนเฉพาะ p ซึ่งมีทั้งหมด 55 จำนวนที่น้อยกว่า 257 พบว่าข้อสังเกตของแมร์แซนผิดพลาดไป กล่าวคือ

$$M_{67} \text{ และ } M_{257} \text{ เป็นจำนวนประกอบ}$$

$$M_{61}, M_{89} \text{ และ } M_{107} \text{ เป็นจำนวนเฉพาะ}$$

เมื่อนำจำนวนเฉพาะแมร์แซน 4 ตัวแรก คือ 3, 7, 31 และ 127 ไปแทน n ในสูตร $2^n - 1$ จะได้จำนวนแมร์แซนตัวใหม่ขึ้นมาจากการแทนค่านี้ นักคณิตศาสตร์ได้พากันคาดหวังว่าวิธีนี้อาจทำให้ได้ว่ามีจำนวนเฉพาะแมร์แซนอยู่จำนวนอนันต์ จึงได้มีข้อคาดเดาว่า ถ้า M_p เป็นจำนวนเฉพาะแล้ว M_{M_p} เป็นจำนวนเฉพาะด้วยแต่ความคาดหวังก็ดับลง ในปี ค.ศ. 1953 เมื่อพบว่า

$$M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$$

เป็นจำนวนประกอบ (มีเลขโดด 2466 หลัก)

ในปี ค.ศ. 2001 พบว่า $M_{13466917}$ เป็นจำนวนเฉพาะแมร์แซนที่มีค่ามากที่สุด ปัญหาที่น่าสนใจขณะนี้คือจำนวนเฉพาะ $M_p = 2^p - 1$ มีอยู่จำนวนอนันต์หรือไม่ ซึ่งปัญหานี้ยังเป็นปัญหาที่มีชื่อเสียงระดับโลกที่ยังไม่มีใครตอบได้ ในการพิจารณาว่าจำนวนแมร์แซนเป็นจำนวนเฉพาะหรือจำนวนประกอบมีมากมายหลายวิธี สำหรับทฤษฎีบทต่อไปนี้เป็นอีกหนึ่งวิธีที่ใช้การตรวจสอบ

ทฤษฎีบท 3.16

ถ้า p และ $q = 2p + 1$ เป็นจำนวนเฉพาะ แล้ว $q \mid M_p$ หรือ $q \mid (M_p + 2)$

อย่างใดอย่างหนึ่งเพียงอย่างเดียวเท่านั้น

พิสูจน์ จากทฤษฎีบทแฟร์มาจะได้ว่า

$$2^{q-1} - 1 \equiv 0 \pmod{q}$$

แยกตัวประกอบทางด้านซ้าย จะได้

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0 \pmod{q}$$

$$M_p(M_p + 2) \equiv 0 \pmod{q}$$

แต่ไม่สามารถมี $q \mid M_p$ หรือ $q \mid (M_p + 2)$ พร้อมกันได้ เมื่อ $q \mid 2$ ซึ่งเป็นไปไม่ได้

ทฤษฎีบท 3.17

ถ้า p เป็นจำนวนเฉพาะคี่ แล้วตัวหารของ M_p จะต้องเขียนอยู่ในรูป $2kp + 1$

ตัวอย่าง 3.18

$$M_{17} = 2^{17} - 1 = 131071$$

พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{17} จะต้องเขียนอยู่ในรูป $2k(17) + 1 = 34k + 1$

$$M_{23} = 2^{23} - 1$$

พบว่าจำนวนเต็มที่เป็นตัวหารของ M_{23} จะต้องเขียนอยู่ในรูป $2k(23) + 1 = 46k + 1$

ตัวอย่าง 3.19 จงแสดงว่าจำนวนเฉพาะเมอร์แซน M_{13} เป็นจำนวนเฉพาะ

วิธีทำ เนื่องจาก $M_{13} = 2^{13} - 1 = 8191$ และ $\sqrt{8191} \leq 91$

ดังนั้น ตัวหารของ M_{13} ที่เขียนอยู่ในรูป $2kp + 1 = 2k(13) + 1 = 26k + 1$

ซึ่งมีค่าน้อยกว่า 91 คือ 53 และ 79 ซึ่งพบว่า $53 \nmid 8191$ และ $79 \nmid 8191$

เพราะฉะนั้น M_{13} เป็นจำนวนเฉพาะ

นอกจากจำนวนเฉพาะเมอร์แซน ยังมีจำนวนเฉพาะอีกรูปแบบหนึ่งที่อยู่ในรูป $2^{p-1}(2^p - 1)$ เรียกจำนวนที่อยู่ในรูปแบบดังกล่าวว่าจำนวนสมบูรณ์ โดยมีบทนิยามดังต่อไปนี้

บทนิยาม 3.4

ให้ p เป็นจำนวนเฉพาะที่ทำให้ $M_p = 2^p - 1$ เป็นจำนวนเฉพาะ เรียกจำนวน p_p ซึ่ง $p_p = 2^{p-1}(2^p - 1)$ ว่าเป็น จำนวนสมบูรณ์

สำหรับจำนวนเฉพาะแมร์แซนและจำนวนสมบูรณ์เท่าที่ทราบในปัจจุบันรวมทั้งผู้ที่ค้นพบปี
ค้นพบได้แสดงไว้ในตารางต่อไปนี้

ตาราง 3.2 แสดงจำนวนเฉพาะแมร์แซน

ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ
1	2	-	-
2	3	-	-
3	5	-	-
4	7	-	-
5	13	1456	Anonymous
6	17	1588	Cataldi
7	19	1588	Cataldi
8	31	1772	Euler
9	61	1883	Pervushin
10	89	1911	Powers
11	107	1914	Powers
12	127	1876	Lucas
13	521	1952	Robinson
14	607	1952	Robinson
15	1279	1952	Robinson
16	2203	1952	Robinson
17	2281	1952	Robinson
18	3217	1957	Riesel
19	4253	1961	Herwitz
20	4423	1961	Herwitz
21	9689	1963	Gillies
22	9941	1963	Gillies
23	11213	1963	Gillies
24	19937	1971	Tuckerman
25	21701	1978	Noll & Nickel
26	23209	1979	Noll
27	44497	1979	Nelson & Slowinski
28	86243	1982	Slowinski
29	110503	1988	Colquilt&Welsh

ตาราง 3.2 (ต่อ)

ลำดับที่	จำนวนเฉพาะ (p)	ปีที่ค้นพบ (ค.ศ.)	ผู้ค้นพบ
30	132046	1983	Slowinski
31	216091	1985	Slowinski
32	756839	1992	Slowinski&Gage
33	859433	1994	Slowinski&Gage
34	1257787	1996	Slowinski&Gage
35	1398269	1996	Armenguad,et.al.
36	2976221	1997	Spence,et.al
37	3021377	1998	Claekson,et.al.
38	6972593	1999	Hajaratwala,et.al.
39	13466917	2001	Kurowski,et.al.
40	20996011	2003	Shafer,et.al

ที่มา : ฌ็องส์ ป็อนนิม และ นิติยา ปภาพจน์ (2552 : 86)

3.5 สรุปท้ายบทที่ 3

จำนวนเต็มบวกที่มากกว่า 1 จะเรียกว่าจำนวนเฉพาะนั้นตัวหารที่เป็นบวกของจำนวนเฉพาะมีเพียง 2 ตัว คือ 1 และตัวมันเอง สำหรับจำนวนเต็มบวกที่มากกว่า 1 ที่ไม่เป็น จำนวนเฉพาะเรียกว่า จำนวนประกอบ แสดงว่า 1 ไม่ใช่จำนวนเฉพาะและไม่ใช่จำนวนประกอบ 2 เป็นจำนวนเฉพาะที่เป็นจำนวนคู่เพียงจำนวนเดียว ส่วนจำนวนเฉพาะตัวอื่น ๆ นั้นจะเป็นจำนวนคี่ นอกจากนี้ยังพบว่าจำนวนเฉพาะนั้นมีอยู่อนันต์ตัว จากข้อคาดการณ์ของนักคณิตศาสตร์หลายท่าน และยุคคิดเป็น คนพิสูจน์ข้อความดังกล่าว สำหรับตรวจสอบการเป็นจำนวนเฉพาะมีวิธีการตรวจสอบได้หลากหลายวิธี เช่น ใช้ตะแกรงเอราทอสเทนีส (The Sieve of Eratosthenes) นอกจากนี้ยังสามารถใช้ Wolfram Alpha ในการค้นหาจำนวนเฉพาะได้อีกด้วย สำหรับทฤษฎีบทที่สำคัญ และเป็นพื้นฐานในการพัฒนาไปสู่ทฤษฎีบทอื่น ๆ คือ ทฤษฎีบทหลักมูลเลขคณิตซึ่งกล่าวไว้ว่าสำหรับจำนวนเต็ม $n > 1$ สามารถเขียนในรูปแบบ

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

โดยที่ $p_1, p_2, p_3, \dots, p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < \cdots < p_k$ และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, \dots, k$ และเขียน n ในรูปแบบดังกล่าวได้เพียงรูปแบบเดียวเท่านั้น และเรียกว่ารูปแบบบัญญัติของ n

แบบฝึกหัดท้ายบทที่ 3

1. จงตรวจสอบว่ามีจำนวนเฉพาะที่อยู่ระหว่าง 701 และ 1009 กี่จำนวนและมีจำนวนใดบ้าง
2. จงแสดงว่า มีจำนวนเฉพาะ p ซึ่ง $2^p - 1$ ไม่เป็นจำนวนเฉพาะ
3. จงหาจำนวนเฉพาะ p ทั้งหมดที่สอดคล้องกับเงื่อนไขต่อไปนี้

3.1 $p \mid (p+1)840$

3.2 $p \mid (240)^{500}$

3.3 $p \mid (160+p)^5$

3.4 $p \mid (p^2 + 2p + 195)^2$

3.5 $(p+3) \mid \left[(p+3)^2 + 15 \right]^{11}$

3.6 $(p-1) \mid \left[2(p-1)^3 + (p-1) + 36 \right]$

4. จงเขียนจำนวนต่อไปนี้ให้อยู่ในรูปแบบบัญญัติ

4.1 2,535

4.2 1,500

4.3 9,261

4.4 1,323

5. จงหาตัวหารทั้งหมดของ 588 และ 6,861

6. จงใช้ทฤษฎีบทหลักมูลเลขคณิตเพื่อหาค่าต่อไปนี้

6.1 $[18, 63]$

6.2 $[84, 24]$

6.3 $[3, 11, 24]$

6.4 $[3, 14, 21, 33]$

6.5 $(18, 81)$

6.6 $(17, 289)$

6.7 $(120, 540, 450)$

6.8 $(84, 24, 108)$

7. จงตรวจสอบว่าจำนวนต่อไปนี้เป็นจำนวนเฉพาะหรือไม่

7.1 377

7.2 131

7.3 297

7.4 357

7.5 211

7.6 263

8. จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่า 88

9. ให้ $n \in \mathbb{N}$ จงแสดงว่ามีจำนวนประกอบเรียงต่อเนื่องกัน n จำนวน

10. ให้ F_n และ F_m เป็นจำนวนแฟร์มาโดยที่ $m > n \geq 0$ ยกตัวอย่าง F_m และ F_n ที่

$$(F_m, F_n) = 1$$

11. จำนวนเมอร์แซน $M_n = 2^n - 1$ เมื่อ $n = 0, 1, 2, 3, 4$ จำนวนใดบ้างเป็นจำนวนเมอร์แซน
12. จำนวนแฟร์มา $F_n = 2^{2^n} + 1$ เมื่อ $n = 0, 1, 2, 3, 4, 5, 6, 7$ จำนวนใดบ้างเป็นจำนวนประกอบ