บทที่ 3

จำนวนเฉพาะ
Prime Numbers

3.1 บทนำ

โดยปกติแล้วการศึกษาเรื่องจำนวนเฉพาะ (prime number) นั้น มักจะเริ่มด้วยปัญหาการพิจารณาว่าจำนวนเต็ม n ที่มีอยู่นั้นเป็นจำนวนประกอบ (composite number) หรือเป็นจำนวนเฉพาะ

นิยาม 3.1

ให้ $|m| > 1$ ถ้ามีจำนวนเต็ม b ซึ่ง $b \mid |m|$ เมื่อ $1 < b < |m|$ แล้วเรียก m ว่า "จำนวนประกอบ" ถ้า b เป็นจำนวนเต็มใด ๆ ซึ่ง $1 < b < |m|$ และ $b \nmid |m|$ แล้วเรียก m ว่าเป็น "จำนวนเฉพาะ"

โดยปกติทั่วไปแล้ว ถ้ากล่าวถึงจำนวนเฉพาะเราหมายถึง จำนวนเฉพาะที่เป็นจำนวนบวก (positive prime) ดังนั้น เราอาจจะให้นิยามได้อีกอย่างหนึ่งดังนี้

ถ้า p เป็นจำนวนเต็มซึ่งมีค่ามากกว่า 1 และมี 1 กับ p เท่านั้นที่หาร p ได้ลงตัวแล้วเราจะเรียก p ว่าเป็นจำนวนเฉพาะ และถ้า p มีค่ามากกว่า 1 และไม่ใช่จำนวนเฉพาะแล้วเราจะเรียก p ว่าเป็นจำนวนประกอบ

ตัวอย่าง 3.1 2 เป็นจำนวนเฉพาะ เนื่องจาก 2 เป็นจำนวนเต็มที่มากกว่า 1 และมี 2 กับ 1 เท่านั้นที่หาร 2 ได้ลงตัว

13 เป็นจำนวนเฉพาะ เนื่องจาก 13 เป็นจำนวนเต็มที่มากกว่า 1 และมี 13 กับ 1 เท่านั้นที่หาร 13 ได้ลงตัว

6 เป็นจำนวนประกอบ เพราะ 6 เป็นจำนวนเต็มที่มากกว่า 1 และมี 6, 3, 2 และ 1 ที่หาร 6 ได้ลงตัว

15 เป็นจำนวนประกอบ เพราะ 15 เป็นจำนวนเต็มที่มากกว่า 1 และมี 15, 5, 3 และ 1 ที่หาร 15 ได้ลงตัว

3.2 ซีฟ ออฟ อีเรโทสเธเนส (The Sieve of Eratosthenes)

วิธีการหาจำนวนเฉพาะทั้งหมดตั้งแต่ 2 ถึง n ซึ่ง n เป็นจำนวนเต็มที่ทราบค่า วิธีหนึ่งเรียกว่า Sieve of Eratosthenes ซึ่ง Eratosthenes เป็นนักคณิตศาสตร์ชาวกรีกซึ่งมีชีวิตอยู่ระหว่าง 276- 194 ก่อนคริสตศตวรรษ เป็นผู้หาวิธีเขียนตารางจำนวนเฉพาะแบบนี้ขึ้นมาโดยอาศัยหลักเกณฑ์ต่อไปนี้คือ

ถ้า n เป็นจำนวนประกอบแล้ว จำนวนเฉพาะที่เป็นตัวประกอบ (prime factor) ของ n จะต้องมีค่าน้อยกว่าหรือเท่ากับ $\sqrt{n}$ ถ้าข้อความนี้ไม่เป็นจริงแล้วเราสามารถเขียน $n = ab$ ซึ่ง $a > \sqrt{n}$ และ $b > \sqrt{n}$ ดังนั้น $n = ab > \sqrt{n}\sqrt{n} = n$ ซึ่งเป็นไปไม่ได้ อาศัยหลักนี้สร้างตารางได้ดังวิธีการต่อไปนี้

1. เขียนจำนวนเต็มทั้งหมดตั้งแต่ 2 ถึง n
2. ตัดจำนวนคู่ทั้งหมดยกเว้น 2 ออกเพราะ 2 เป็นจำนวนเฉพาะ
3. ตัดจำนวนที่เป็นพหุคูณของ 3 ออกหรือจำนวนที่ 3 หารลงตัวยกเว้น 3
4. ตัดจำนวนที่ 5 หารลงตัวยกเว้น 5
5. หาจำนวนเฉพาะตัวถัดจาก 5 สมมุติเป็น q แล้วเราก็ตัดจำนวนที่ q หารลงตัวออก
6. ทำดังนี้ไปเรื่อย ๆ จนถึงจำนวนเฉพาะ p ซึ่งมีค่ามากที่สุดและ $p \leqslant \sqrt{n}$ ก็ตัดจำนวนที่ p หารลงตัวออกยกเว้น p

จำนวนที่เหลือทั้งหมดก็คือจำนวนเฉพาะที่น้อยกว่าหรือเท่ากับ n

ตัวอย่าง 3.2 The Sicve of Eratosthencs สำหรับ $n = 100$

วิธีทำ เพราะว่า $\sqrt{100} = 10$

เพราะฉะนั้นจำนวนเฉพาะซึ่งน้อยกว่า $\sqrt{100}$ คือ 2, 3, 5, 7

เริ่มแรกเขียนจำนวนเต็มตั้งแต่ 2 ถึง 100 แล้วตัดจำนวนที่ 2 3 5 และ 7 หารลงตัวออกยกเว้นตัวของมันเองจะได้ดังนี้

	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~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

จำนวนที่มีวงกลมล้อมคือจำนวนเฉพาะทั้งหมดซึ่งน้อยกว่า 100

วิธีที่จะตรวจดูว่าจำนวนเต็มใดเป็นจำนวนเฉพาะหรือไม่นั้นเราอาจจะใช้วิธีหาจำนวนเฉพาะซึ่งน้อยกว่าหรือเท่ากับรากที่ 2 ของจำนวนเต็มนั้นมาหารดู ถ้าหารลงตัวจำนวนนั้นก็เป็นจำนวนประกอบ ถ้าไม่มีจำนวนเฉพาะใดหารลงตัวเลย จำนวนนั้นก็เป็นจำนวนเฉพาะดังตัวอย่าง

ตัวอย่าง 3.3 จงตรวจดูว่า 107 เป็นจำนวนเฉพาะหรือไม่

วิธีทำ เราจะต้องหาว่า 107 มีตัวประกอบซึ่งเป็นจำนวนเฉพาะและน้อยกว่า

หรือเท่ากับ $\sqrt{107} = 10.344\ldots$

ซึ่งพบว่า 2, 3, 5, 7 เป็นจำนวนเฉพาะซึ่งอาจเป็นตัวประกอบของ 107 ได้

ลองมาทดสอบดูปรากฏว่า

$$2 \nmid 107, \text{ และ } 5 \nmid 107$$

และ $107 = 3 \cdot 35 + 2$ แสดงว่า $3 \nmid 107$

$107 = 7 \cdot 15 + 2$ แสดงว่า $7 \nmid 107$

แสดงว่า 107 เป็นจำนวนเฉพาะ

ตัวอย่าง 3.4 จงตรวจดูว่า 119 เป็นจำนวนประกอบหรือจำนวนเฉพาะ

วิธีทำ จำนวนเฉพาะซึ่งน้อยกว่าหรือเท่ากับ $\sqrt{119} = 10.908\ldots$

คือ 2, 3, 5, 7

ซึ่ง $2 \nmid 119$ และ $5 \nmid 119$

$119 = 3 \cdot 39 + 2$ แสดงว่า 34119

$119 = 7.17$ แสดงว่า $7 | 119$

ดังนั้น 119 เป็นจำนวนประกอบ

ทฤษฎี 3.1

จำนวนเต็ม $n \geqslant 2$ จะต้องเป็นจำนวนเฉพาะหรือเป็นผลคูณของจำนวนเฉพาะ

พิสูจน์ ถ้า $n = 2$ ทฤษฎีนี้เป็นจริงเพราะ 2 เป็นจำนวนเฉพาะ

สมมุติว่าทฤษฎีนี้เป็นจริงสำหรับจำนวนเต็มทุกจำนวน n ซึ่ง $2 \leqslant n \leqslant k$ เมื่อ k คือจำนวนเต็มซึ่งไม่น้อยกว่า 2

จะแสดงว่าทฤษฎีนี้เป็นจริงเมื่อ $n = k + 1$

ถ้า $n = k+1$ เป็นจำนวนเฉพาะ ทฤษฎีนี้เป็นจริง

61 $n = k+1$ เป็นจำนวนประกอบ แล้วจะต้องมีจำนวนเต็ม r และ s

ซึ่งทำให้ $k + 1 = rs$ เมื่อ $2 \leqslant r \leqslant k$ และ $2 \leqslant s \leqslant k$

แต่เมื่อ r และ s อยู่ระหว่าง 2 กับ k ตามที่เราสมมุติ r และ s **จะต้องเป็นจำนวนเฉพาะ**
หรือผลคูณของจำนวนเฉพาะ
แสดงว่าทฤษฎีนี้เป็นจริงเมื่อ $n = k+1$
ดังนั้นตามการอุปนัยทางคณิตศาสตร์ ทฤษฎีนี้เป็นจริงสำหรับ**จำนวนเต็มทุกจำนวน**
$n \geqslant 2$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 3.2

ให้ p เป็นจำนวนเฉพาะ และ a, b เป็นจำนวนเต็ม
ถ้า $p|ab$ แล้ว $p|a$ หรือ $p|b$

พิสูจน์ ถ้า $p|b$ แล้วทฤษฎีนี้เป็นจริง
ถ้า $p\nmid b$ แล้ว $(p, b) = 1$ เพราะตัวประกอบของ p คือ ± 1 และ $\pm p$
ดังนั้นตามทฤษฎี 2.7 $p|a$

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ทฤษฎี 3.3

ให้ p เป็นจำนวนเฉพาะ ถ้า $p \mid \prod_{i=1}^{n} a_i$ แล้ว $p|a_i$ อย่างน้อยหนึ่ง a_i

พิสูจน์ ใช้ทฤษฎี 3.2 และการอุปมานทางคณิตศาสตร์

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

ถ้าเราศึกษาจากตารางของจำนวนเฉพาะจะพบว่าในห้ากลุ่มแรกของจำนวนเต็มแต่ละพัน คือช่วง 1 - 1,000, 1,001 - 2,000, 2,001 - 3,000, 3,001 - 4,000 และ 4,001 - 5,000 จะมีจำนวนเฉพาะอยู่ 168, 135, 127, 120 และ 119 จำนวนตามลำดับ ถ้าหาต่อไปก็จะพบว่าจำนวนเฉพาะนี้จะมีจำนวนลดลงเรื่อย ๆ ในกลุ่มของจำนวนเต็มที่มีค่ามาก ๆ คือในช่วง 9,995,000 ถึง 9,995,000 มีจำนวนเฉพาะอยู่ 62 จำนวน และในช่วง 9,999,000 ถึง 10,000,000 มีจำนวนเฉพาะอยู่ 53 จำนวน เราอาจจะสงสัยว่าจำนวนเฉพาะนี้มีทั้งหมดเท่าไร นับจำนวนได้ไหม หรือว่ามีมากมายจนนับไม่ได้ ทฤษฎีต่อไปนี้จะบอกให้ทราบ

ทฤษฎี 3.4

มีจำนวนเฉพาะอยู่เป็นจำนวนไม่จำกัด (infinitely many)

พิสูจน์ สมมุติว่ามีจำนวนเฉพาะอยู่เป็นจำนวน n คือ $p_1, p_2, \ldots p_n$

พิจารณาจำนวนเต็ม $m = p_1p_2\ldots p_n + 1$

แสดงว่า $m > p_i$ สำหรับ $i = 1, 2, \ldots, n$

ดังนั้น ถ้า m เป็นจำนวนประกอบแล้ว ตามทฤษฎี 3.1

m ต้องเป็นผลคูณของจำนวนเฉพาะ

เพราะฉะนั้น $p_i|m$ สำหรับ i บางตัว ดังนั้น $p_i|1$

ซึ่งเป็นไปไม่ได้

เพราะฉะนั้น m ต้องเป็นจำนวนเฉพาะ

แสดงว่าต้องมีจำนวนเฉพาะอยู่เป็นจำนวนไม่จำกัด

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

แบบฝึกหัด 3

1. ใช้ Sieve of Eratosthenes หาจำนวนเฉพาะที่น้อยกว่า 200
2. จงหาตัวประกอบเฉพาะทั้งหมดของ 1243 $(\sqrt{1243} = 35 \cdot 2562\ldots)$
3. จงหาตัวประกอบเฉพาะทั้งหมดของ 3059 $(\sqrt{3059} = 55 \cdot 3082\ldots)$
4. จงหาตัวประกอบเฉพาะทั้งหมดของ 1093 $(\sqrt{1093} = 33 \cdot 0605\ldots)$
5. ให้ $\pi(x)$ คือจำนวนของจำนวนเฉพาะซึ่งน้อยกว่าหรือเท่ากับ x เมื่อ x เป็นจำนวนจริง จงหา $\pi(\sqrt{210})$ และบอกด้วยว่ามีอะไรบ้าง
6. จงหาจำนวนเต็ม n ซึ่งมีค่ามากที่สุดซึ่ง $\pi(\sqrt{n}) = 6$
7. ให้ n เป็นจำนวนเต็มบวก และ $d > 1$ จงพิสูจน์ว่า ถ้า d เป็นจำนวนเต็มบวกที่มีค่าน้อยที่สุดซึ่งหาร n ลงตัวแล้ว d เป็นจำนวนเฉพาะ