บทที่ 3

จำนวนเฉพาะและการแยกตัวประกอบของจำนวนธรรมชาติ

3.1 เงื่อนไขที่จำเป็นและเพียงพอในการเป็นจำนวนเฉพาะ และทฤษฎีบทเกี่ยวกับจำนวนธรรมชาติที่มีจำนวนเฉพาะเป็นตัวประกอบ (The Primes and Factorization of a Natural Number m into Primes)

นิยาม 1 จำนวนธรรมชาติใด ๆที่มากกว่า 1 และไม่มีตัวหารลงตัวที่เป็นจำนวนธรรมชาตินอกจากตัวมันเอง และ 1 เรียกว่า จำนวนเฉพาะ (prime number)

เงื่อนไขที่จำเป็นและเพียงพอ สำหรับจำนวนธรรมชาติ $m > 1$ ที่จะเป็นจำนวนเฉพาะ คือ m ต้องไม่อยู่ในรูปผลคูณของสองจำนวนธรรมชาติที่น้อยกว่า m

ดังนั้น เราจะแสดงการพิสูจน์เงื่อนไขที่จำเป็นก่อน คือ

ถ้า m เป็นจำนวนเฉพาะ แล้ว $m \neq a \cdot b$, $a, b \in N$ โดยที่ $a, b < m$

เพราะว่า ถ้า $m = a \cdot b$, $a, b \in N$ โดยที่ $a, b < m$ ดังนั้น $a, b > 1$

นั่นคือ m จะมีตัวหารลงตัวที่มากกว่า 1 และน้อยกว่า m ซึ่งเกิดข้อขัดแย้งกับนิยามของจำนวนเฉพาะ

ต่อไป ในส่วนที่เหลือก็เป็นการพิสูจน์เงื่อนไขที่เพียงพอในการเป็นจำนวนเฉพาะ คือ

ถ้า m ไม่เป็นจำนวนเฉพาะ แล้ว m จะมีตัวหารลงตัว คือ a โดยที่ $1 < a < m$

ดังนั้น จะได้ $m = a \cdot b$ โดยที่ $b \in N$

แต่เนื่องจาก $a > 1$ ดังนั้น $b < m$

นั่นคือ m สามารถเขียนเป็นผลคูณของสองจำนวนธรรมชาติ โดยที่แต่ละจำนวนน้อยกว่า m

จากนิยามของจำนวนเฉพาะได้ขยายสู่วิธีที่เราจะตัดสินว่า จำนวนธรรมชาติ $n > 1$ ที่กำหนดให้จะเป็นจำนวนเฉพาะหรือไม่ ที่จริงแล้วจากเงื่อนไขที่เพียงพอ ก็ประสบความสำเร็จอย่างเพียงพอที่จะหาร n ด้วย 2, 3, 4, ..., n-1 และถ้าไม่มีจำนวนใดใน 2, 3, 4, ... , n-1 หาร n ได้เลย แล้ว n จะเป็นจำนวนเฉพาะเท่านั้น

นิยาม 2 จำนวนธรรมชาติที่ไม่เท่ากับ 1 และไม่เป็นจำนวนเฉพาะ จะเรียกว่า จำนวนประกอบ (composite number) นั่นคือ ถ้า n เป็นจำนวนประกอบ, $n = ab$, $a, b \in N$ โดยที่ $a, b < n$ แล้วเกิดผลที่ติดตามมา คือ $a, b > 1$

ทฤษฎีบท 3 ถ้าจำนวนธรรมชาติ n เป็นจำนวนประกอบ แล้ว n มีตัวหารลงตัวคือ a โดยที่ $1 < a \leq \sqrt{n}$

พิสูจน์ ให้จำนวนธรรมชาติ n เป็นจำนวนประกอบ

ดังนั้น $n = ab$, $a, b \in N$ โดยที่ $a, b < n$

จะได้ว่า $a, b > 1$

สมมติว่า $a \leq b$

$1 < a^2 \leq ab = n$

$a^2 - n \leq 0$

$(a - \sqrt{n})(a + \sqrt{n}) \leq 0$

นั่นคือ $-\sqrt{n} \leq a \leq \sqrt{n}$ แต่ $a > 1$

ดังนั้น $1 < a \leq \sqrt{n}$

n มีตัวหารลงตัว คือ a โดยที่ $1 < a \leq \sqrt{n}$ #

ทฤษฎีบท 4 ทุกจำนวนธรรมชาติ $n > 1$ มีตัวหารลงตัวที่เป็นจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวน

พิสูจน์ ให้ n เป็นจำนวนธรรมชาติที่มากกว่า 1
เนื่องจาก $n \mid n$, $\forall n \in N$ และ $n > 1$
ดังนั้น n มีตัวหารลงตัวที่มากกว่า 1
สมมติให้ ตัวหารลงตัวที่น้อยที่สุดของ n คือ p
จะต้องแสดงให้ได้ว่า p เป็นจำนวนเฉพาะ
สมมติว่า ถ้า p ไม่เป็นจำนวนเฉพาะ ดังนั้น p เป็นจำนวนประกอบ
และจะได้ $p = ab$, $a, b \in N$ โดยที่ $1 < a, b < p$
ทำให้ a เป็นตัวหารลงตัวของ n โดยที่ $1 < a < p$ เกิดข้อขัดแย้งกับ p ที่เป็นตัวหารลงตัวที่น้อยที่สุดของ n
นั่นคือ p เป็นจำนวนเฉพาะ #

ผลที่ติดตามมาจากทฤษฎีบท 3 และทฤษฎีบท 4 เกิดเป็นบทแทรกต่อไปนี้ คือ

บทแทรก 5 ทุก ๆจำนวนประกอบ n มีตัวหารลงตัวที่เป็นจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวนที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$

พิสูจน์ ให้ n เป็นจำนวนประกอบ
ดังนั้น n เป็นจำนวนธรรมชาติที่ไม่เป็นจำนวนเฉพาะ และ $n > 1$
โดยทฤษฎีบท 3 n มีตัวหารลงตัวคือ a โดยที่ $1 < a \leq \sqrt{n}$
โดยทฤษฎีบท 4 n มีตัวหารลงตัวที่เป็นจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวน
นั่นคือ n มีตัวหารลงตัวที่เป็นจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวนที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$ #

บทแทรก 6 ทุก ๆจำนวนธรรมชาติที่มากกว่า 1 จะเป็นผลคูณอย่างจำกัดของตัวประกอบเฉพาะ (รวมไปถึงผลคูณของ 1 กับจำนวนเฉพาะ)

พิสูจน์ จะพิสูจน์แบบขัดแย้ง โดยสมมติว่า บทแทรก 6 ไม่เป็นจริง

ดังนั้น จะมีจำนวนธรรมชาติที่น้อยที่สุด คือ $n > 1$ ที่ไม่เป็นผลคูณของจำนวนเฉพาะ

โดยทฤษฎีบท 4 n มีตัวหารลงตัวที่เป็นจำนวนเฉพาะ สมมติให้เป็น p

ดังนั้น $n = pn_1$ โดยที่ $n_1 \in N$

พิจารณา ถ้า $n_1 = 1$ จะทำให้ $n = p$ นั่นคือ บทแทรก 6 เป็นจริง ซึ่งขัดแย้งกับที่สมมติไว้

ดังนั้น $n_1 \neq 1$ จะได้ $n_1 > 1$ และได้ว่า $n = pn_1 > n_1$

นั่นคือ $n_1 < n$ และจากนิยามของ n เราสรุปว่า n_1 เป็นผลคูณของจำนวนเฉพาะ แล้วจะได้ว่า $n = pn_1$ ก็เป็นผลคูณของจำนวนเฉพาะด้วย เกิดข้อขัดแย้งกับนิยามของ n ที่ว่าไม่เป็นผลคูณของจำนวนเฉพาะ

ดังนั้น ที่สมมติไว้ก็ไม่เป็นจริง

นั่นคือ บทแทรก 6 เป็นจริง #

เมื่อถึงตรงนี้ ก็เกิดคำถามขึ้นตามมาว่า จะมีวิธีซึ่งทำให้เราแทนจำนวนธรรมชาติที่กำหนดให้ในรูปผลคูณของจำนวนเฉพาะได้หรือไม่ คำตอบก็คือ วิธีนั้นมีจริง ๆ ถึงแม้ว่าวิธีการจะยาวมาก

นอกจากนี้ ยังเพียงพอที่จะพิสูจน์ว่า สำหรับจำนวนธรรมชาติ ที่กำหนดให้ เราสามารถหาตัวประกอบที่ต้องการสำหรับจำนวน n หรือไม่ก็ลดปัญหาการหาตัวประกอบของจำนวน ๆหนึ่งที่น้อยกว่า n

ทฤษฎีบท 7 จำนวนธรรมชาติใด ๆ สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะเพียงแบบเดียวเท่านั้น (โดยไม่คิดถึงลำดับของแต่ละจำนวนในผลคูณ)

พิสูจน์ ให้ n เป็นจำนวนธรรมชาติ โดยที่ $n > 1$

โดยทฤษฎีบท 4 n จะมีตัวหารลงตัวที่เป็นจำนวนเฉพาะ

สมมติให้ตัวหารลงตัวที่เป็นจำนวนเฉพาะที่น้อยที่สุดของ n คือ p

ดังนั้น $n = pn_1$ โดยที่ $n_1 \in N$

ต่อไป พิจารณาค่า n_1 ออกเป็น 2 กรณี คือ

<u>กรณี 1</u> ถ้า $n_1 = 1$ จะได้ $n = p$ นั่นคือ ทฤษฎีบท 7 เป็นจริง

<u>กรณี 2</u> ถ้า $n_1 > 1$ แล้ว $n = pn_1 > n_1$

นั่นคือ $n_1 < n$

แต่เพราะว่า $n_1 \in N$ โดยบทแทรก 6 จะได้ n_1 เป็นผลคูณอย่างจำกัดของจำนวนเฉพาะ

แล้วแทนค่า n_1 ใน n ทำเช่นนี้ไปเรื่อยๆ น้อยกว่า n ครั้ง

ดังนั้น จะได้ $n = p \cdot p' \cdot p'' \cdot \ldots \cdot p^{(k-1)}$

โดยที่ $p, p', p'', \ldots, p^{(k-1)}$ เป็นจำนวนเฉพาะ, $k \in N$, $k < n$

ถ้ามี $p, p', p'', \ldots, p^{(k-1)}$ ซ้ำกัน เราจะเขียน n ในรูปของเลขยกกำลัง คือ

$n = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$ โดยที่ $q_1, q_2, \ldots, q_s$ เป็นจำนวนเฉพาะที่แตกต่างกันทั้งหมด และให้ $q_1 < q_2 < \cdots < q_s$ และ $a_i \in N$, $i = 1, 2, 3, \ldots, s$

[การเขียนจำนวนธรรมชาติ n ในรูปผลคูณนี้ เรียกว่า การแยกตัวประกอบของ n ในรูปผลคูณของจำนวนเฉพาะ (factorization of n into prime numbers) และเรียกตัวประกอบทั้งหมดของ n: $q_1, q_2, \ldots, q_s$ ว่าตัวหารลงตัวเฉพาะของ n]

นั่นคือ จำนวนธรรมชาติใดๆ สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

ต่อไป เราจะต้องแสดงให้ได้ว่า รูปผลคูณของจำนวนเฉพาะนั้นมีเพียงแบบเดียวเท่านั้น โดยแยกแสดงเป็น 2 ส่วน คือ

ส่วนที่ 1 จะต้องอธิบาย n ได้ด้วยจำนวนเฉพาะ $q_1, q_2, \ldots, q_s$ เพียงแบบเดียวเท่านั้น

ส่วนที่ 2 จะต้องอธิบาย n ได้ด้วยเลขชี้กำลัง $a_1, a_2, \ldots, a_s$ เพียงแบบเดียวเท่านั้น

<u>ส่วนที่ 1</u> ถ้า n ถูกหารลงตัวได้ด้วยจำนวนเฉพาะอีกจำนวนหนึ่งคือ q ที่ไม่เท่ากับ $q_1, q_2, \ldots, q_s$

และเนื่องจาก จำนวนเฉพาะ q มีตัวหารลงตัวเพียง 2 จำนวนเท่านั้น คือ q และ 1

แล้วจะได้ $(q,q_i) = 1$ สำหรับ i = 1, 2, 3, ..., s

ดังนั้น $(q,q_i^{a_i}) = 1$ สำหรับ i = 1, 2, 3, ... s (โดยทฤษฎีบท 9 ในบทที่ 2)

นั่นคือ จะได้ว่า $(q,q_1^{a_1}q_2^{a_2} \cdots q_s^{a_s}) = 1$ (โดยทฤษฎีบท 9 ในบทที่ 2)

หรือ $(q,n) = 1$ เกิดข้อขัดแย้งกับที่ $q \mid n$

ดังนั้น จะได้ว่า n อธิบายได้ด้วย q_i, i = 1, 2, 3, ..., s เพียงแบบเดียวเท่านั้น

<u>ส่วนที่ 2</u> โดยปกติ a_1 สามารถนิยามให้เป็นจำนวนธรรมชาติที่มากที่สุดที่ $q_1^{a_1} \mid n$

แต่เนื่องจากในกรณี $q_1^{a_1+1} \mid n$ เราจะมี $q_1 \mid q_2^{a_2}q_3^{a_3} \cdots q_s^{a_s}$ ซึ่งเป็นไปไม่ได้

เพราะว่า เราสมมติให้ $q_1 < q_2 < \cdots < q_s$

ดังนั้นจะได้ว่า n อธิบายได้ด้วย a_i, i = 1, 2, 3, ... , s เพียงแบบเดียวเท่านั้น

นั่นคือ ทั้ง 2 กรณี จะสรุปได้ว่า n สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ

เพียงแบบเดียวเท่านั้น #

ทฤษฎีบท 8 ถ้าจำนวนธรรมชาติ $n > 2$ แล้ว มีจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวน ที่อยู่ระหว่าง n และ n!

พิสูจน์ ให้จำนวนธรรมชาติ n โดยที่ $n > 2$

และให้ $N = n! - 1$ ดังนั้น $N > 1$

จากทฤษฎีบท 4 N มีตัวหารลงตัวที่เป็นจำนวนเฉพาะ

สมมติให้เป็น p ดังนั้น $p \mid n! - 1$

แต่เนื่องจาก ถ้า $p \leq n$ นั่นคือ $p \mid 1$ ซึ่งเป็นไปไม่ได้

ดังนั้น $p > n$

จาก N มีตัวหารลงตัว คือ p จะได้ว่า $p \leq N$

ดังนั้น $n < p \leq N$

$n < p \leq n! - 1 < n!$

นั่นคือ มีจำนวนเฉพาะอย่างน้อยที่สุดหนึ่งจำนวน ที่อยู่ระหว่าง n และ n! #

จากทฤษฎีบท 8 จะได้ว่า สำหรับแต่ละจำนวนธรรมชาติ n มีจำนวนเฉพาะที่มากกว่า n หรือกล่าวง่าย ๆว่า มีจำนวนเฉพาะมากมายไม่จำกัด โดยเฉพาะอย่างยิ่งจะมีจำนวนเฉพาะที่อย่างน้อยที่สุดเป็นแสนหลักแต่เราไม่รู้ว่าเป็นจำนวนอะไรบ้างจำนวนเฉพาะที่มากที่สุดที่รู้กันในปัจจุบันนี้ คือ $2^{216091}-1$ ซึ่งเป็นจำนวนที่มี 65050 หลัก และได้พิสูจน์ว่าเป็นจำนวนเฉพาะในปี ค.ศ. 1985

3.2 ตะแกรง Eratosthenes (The Eratosthenes Sieve)

ผลที่ติดตามมาทันทีจากบทแทรก 5 ในหัวข้อ 3.1 คือ ถ้าจำนวนธรรมชาติ n จำนวนหนึ่งที่ $n > 1$ ไม่สามารถหารได้ด้วยจำนวนเฉพาะใด ๆที่น้อยกว่าหรือเท่ากับ $\sqrt{n}$ แล้ว n เป็นจำนวนเฉพาะ

นั่นคือ เมื่อต้องการเลือกจำนวนเฉพาะทั้งหมดจากลำดับ 2, 3, 4, ..., m เมื่อ m เป็นจำนวนธรรมชาติที่กำหนดให้ ก็ให้ตัดจำนวนทั้งหมดที่อยู่ในรูป kp, p เป็นจำนวนเฉพาะ โดยที่ $p \leq \sqrt{m}$ และ $k > 1$ ออกไปจากลำดับเช่น ลำดับ 2, 3, 4, 5,..., 25 จะมีจำนวนเฉพาะ p โดยที่ $p \leq \sqrt{25}$ คือ 2, 3, 5 ดังนั้นจะตัดจำนวนทั้งหมดที่มากกว่าและหารได้ด้วยอย่างน้อย 1 จำนวนจาก 2, 3, 5 ออกไปจากลำดับ 2, 3, 4, 5, ..., 25 แล้วจำนวนที่เหลือทั้งหมดเป็นจำนวนเฉพาะ ได้แก่ 2, 3, 5, 7, 11, 13, 17, 19, 23

นักคณิตศาสตร์ชาวกรีก ชื่อ Eratosthenes เป็นผู้คิดวิธีการดังกล่าวข้างต้นนั้น ดังนั้น เราจะพิจารณาลำดับ 2, 3, 4, ... ได้ตามขั้นตอนดังนี้

1. เนื่องจากจำนวนเฉพาะตัวแรก $p_1 = 2$ ก็ให้ตัดจำนวนทั้งหมดที่มากกว่า p_1 และหารได้ด้วย 2 ออกไปจากลำดับ 2, 3, 4, ...

2. จำนวนเฉพาะตัวที่สอง $p_2 = 3$ ก็ให้ตัดจำนวนทั้งหมดที่มากกว่า p_2 และหารได้ด้วย 3 ออกไปจากลำดับ 2, 3, 4, ...

3. จำนวนเฉพาะตัวที่สาม $p_3 = 5$ ก็ให้ตัดจำนวนทั้งหมดที่มากกว่า p_3 และหารได้ด้วย 5 ออกไปจากลำดับ 2, 3, 4, ...

4. ทำเช่นนี้ไปเรื่อย ๆ จนกระทั่งถึง จำนวนเฉพาะตัวที่ n, p_n ก็ให้ตัดจำนวนทั้งหมดที่มากกว่า p_n และหารได้ด้วย p_n ออกไปจากลำดับ 2, 3, 4, ... และจำนวนที่น้อยที่สุดที่ยังไม่ได้ตัดออกไป จะเป็นจำนวนเฉพาะจำนวนที่ n+1

นั่นคือ ถ้ามีลำดับของจำนวนธรรมชาติตั้งแต่ 2 ถูกแทนด้วยลำดับของจำนวนธรรมชาติ 2, 3, 4, 5, ..., N แล้วในกระบวนการสุดท้ายของวิธีดังกล่าวข้างต้น หลังจากสิ้นสุดขั้นตอนที่ k, จะได้ p_k คือ จำนวนเฉพาะตัวที่มากที่สุด $p_k \leq \sqrt{N}$

ดังนั้น เราจะได้ $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$, $p_{25} = 97$, ... , $p_{100} = 541$, $p_{200} = 1223$, $p_{1000} = 7917$, $p_{1229} = 9973$, $p_{1230} = 10007$, และเมื่อเร็ว ๆนี้ก็มีการคำนวณได้ว่า $p_{6000000} = 104395301$

D. Blanusa ได้แปลความหมายทางเรขาคณิตแบบพื้นฐานของตะแกรงอีราโทสทีเนส ในระบบพิกัดฉาก ไว้ดังนี้ ถ้า $A = \{(0,\frac{1}{m}) \mid m \in N\}$ และ $B = \{(n+1,0) \mid n \in N\}$ จะพบว่าสมการเส้นตรงที่เชื่อมระหว่างจุด $(0,\frac{1}{m})$ และ $(n+1,0)$ คือ $\frac{x}{n+1} + my = 1$

สมการเส้นตรง $\frac{x}{n+1} + my = 1$ จะตัดกับเส้นตรง $y = -1$ ที่จุดซึ่งมีค่าของ $x = (m+1)(n+1)$ แต่เนื่องจาก $m, n \in N$ นั่นคือ ค่า x เป็นจำนวนประกอบ

ในทางกลับกัน ถ้า x เป็นจำนวนประกอบ แล้วจะได้ $x = (m+1)(n+1)$, $m, n \in N$ นั่นคือ $x = (m+1)(n+1)$ เป็นค่าแอ็บซิสซาของจุดที่เกิดจากการตัดกันของเส้นที่เชื่อมระหว่างจุด $(0,\frac{1}{m})$ และ $(n+1,0)$ กับเส้น $y = -1$

นั่นคือ D. Blanusa ได้เสนอว่า เซตของค่าแอ็บซิสซาของจุดที่เกิดจากการตัดกันของเส้นที่เชื่อมระหว่างจุด $(0,\frac{1}{m})$ และ $(n+1,0)$ กับเส้น $y = -1$ เป็นเซตของจำนวนประกอบ

3.3 ผลต่างระหว่างจำนวนเฉพาะที่เรียงกัน (The Difference between Consecutive Prime Numbers)

จากหัวข้อ 3.2 เราทราบแล้วว่า p_n คือ จำนวนเฉพาะจำนวนที่ n เรื่องที่จะกล่าวต่อไปจะเป็นคำถามอันเกิดจากผลต่างระหว่างจำนวนเฉพาะที่เรียงกัน

โดยให้ $d_n = p_{n+1} - p_n$, $n = 1, 2, 3, \ldots$

เราจะได้ 100 พจน์แรกของลำดับ $d_1, d_2, d_3, \ldots$ ดังนี้ คือ

1	2	2	4	2	4	2	4	6	2
6	4	2	4	6	6	2	6	4	2
6	4	6	8	4	2	4	2	4	14
4	6	2	10	2	6	6	4	6	6
2	10	2	4	2	12	12	4	2	4
6	2	10	6	6	6	2	6	4	2
10	14	4	2	4	14	6	10	2	4
6	8	6	6	4	6	8	4	8	10
2	10	2	6	4	6	8	4	2	4
12	8	4	8	4	6	12	2	18	6

เนื่องจาก จำนวนคู่ที่มากกว่า 2 สามารถหารลงตัวได้ด้วย 2 ดังนั้นจึงเป็นจำนวนประกอบ ดังนั้นจึงมี จำนวนคู่ 2 เพียงจำนวนเดียวเท่านั้นที่เป็นจำนวนเฉพาะ

นั่นคือ เราสามารถสรุปได้ว่า สำหรับ $n > 1$ แล้ว p_n เป็นจำนวนคี่ แล้ว $d_n = p_{n+1} - p_n$ เป็นจำนวนคู่

จากตารางข้างต้น เราอาจจะตั้งคำถามขึ้นมาว่า

สำหรับแต่ละจำนวนธรรมชาติ k จะมี n อย่างน้อยหนึ่งจำนวน ที่ $d_n = 2k$ หรือไม่ ซึ่งเราไม่ทราบคำตอบของคำถามนี้ แต่จะมีตัวอย่างตารางของจำนวนธรรมชาติ n ที่น้อยที่สุด โดยที่ $d_n = 2k$, สำหรับ $2k \leq 30$ พร้อมด้วย p_{n+1}, p_n โดยที่ $p_{n+1} - p_n = 2k$

2k	n	p_n	p_{n+1}
2	2	3	5
4	4	7	11
6	9	23	29
8	24	89	97
10	34	139	149

2k	n	p_n	p_{n+1}
12	46	199	211
14	30	113	127
16	282	1831	1847
18	99	523	541
20	154	887	907

2k	n	p_n	p_{n+1}
22	189	1129	1151
24	263	1669	1693
26	367	2477	2503
28	429	2971	2999
30	590	4297	4327

และยังพบว่า จำนวนเฉพาะเรียงกันที่น้อยที่สุดที่มีผลต่างเท่ากับ 100 คือ จำนวนเฉพาะ 396733, 396833 เป็นต้น

เมื่อหลายร้อยปีมาแล้ว มีคอนเจคเจอร์ที่เกิดขึ้น เช่น

1. คอนเจคเจอร์ของ de Polignac : สำหรับทุก ๆจำนวนคู่ 2k จะมีจำนวนธรรมชาติ n มากมายอย่างไม่จำกัด ที่ $d_n = 2k$

สำหรับ 2k = 2 คอนเจคเจอร์ดังกล่าวจะสมมูลกับคอนเจคเจอร์ที่ว่ามีจำนวนเฉพาะคี่สองจำนวนเรียงกันอย่างไม่จำกัด (จำนวนเฉพาะคี่สองจำนวนที่เรียงกัน 10 ชุดแรก ได้แก่)

3 กับ 5 5 กับ 7 11 กับ 13 17 กับ 19 29 กับ 31

41กับ 43 59 กับ 61 71 กับ 73 101 กับ 103 107 กับ 109

นักคณิตศาสตร์ชื่อ H. Tietze ผู้สร้างตารางของจำนวนเฉพาะคี่สองจำนวนเรียงกันที่น้อยกว่า 300000 โดยเสนอในรูปของจำนวนมากที่สุดของแต่ละคู่ของจำนวนเฉพาะคี่สองจำนวนเรียงกันทั้งหมด 2994 จำนวน นอกจากนั้นยังมี Selmer และ Nesheim ผู้เสนอจำนวนเฉพาะคี่สองจำนวนเรียงกัน โดยนำเสนอในรูป 6n + 1 และ 6n - 1 ที่น้อยกว่า 200000 ในขณะที่ของ Sexton และ Brent ผู้พบว่ามี 152892 จำนวน ของจำนวนเฉพาะคี่สองจำนวนเรียงกันที่น้อยกว่า 10^{11} และจำนวนเฉพาะคี่สองจำนวนเรียงกันที่มากที่สุดที่รู้กันในเวลานี้ คือ 260497545 ± 1

2. คอนเจคเจอร์ : มีจำนวนธรรมชาติ n มากมายไม่จำกัด ที่ $n^2 - 1$ มีตัวหารลงตัวที่เป็นจำนวนธรรมชาติเพียง 4 จำนวนเท่านั้น เช่น เมื่อ n = 3 จะได้ $n^2 - 1 = 8$ มีตัวหารลงตัวที่เป็นจำนวนธรรมชาติเพียง 4 จำนวนเท่านั้น คือ 1, 2, 4, 8 เมื่อ n = 4 จะได้ $n^2 - 1 = 15$ มีตัวหารลงตัวที่เป็นจำนวนธรรมชาติเพียง 4 จำนวนเท่านั้น คือ 1, 3, 5, 15 และเมื่อ n = 6 จะได้ $n^2 - 1 = 35$ มีตัวหารลงตัวที่เป็นจำนวนธรรมชาติเพียง 4 จำนวนเท่านั้น คือ 1, 5, 7, 35 เป็นต้น

3. คอนเจคเจอร์ : สำหรับจำนวนธรรมชาติ n มีอย่างน้อยที่สุดจำนวนเฉพาะคี่สองจำนวนเรียงกันที่อยู่ระหว่าง n^3 กับ $(n+1)^3$ เช่น เมื่อ n = 2 มีจำนวนเฉพาะคือ 11,13, 17,19 อยู่ระหว่าง n^3 กับ $(n+1)^3$ และเมื่อ n = 3 มีจำนวนเฉพาะ คือ 29,31, 41,43, 59,61 ที่อยู่ระหว่าง n^3 กับ $(n+1)^3$ เป็นต้น

4. คอนเจคเจอร์ : มีจำนวนเฉพาะ p อย่างไม่จำกัด ที่ p, p+2, p+6 และ p+8 ต่างเป็นจำนวนเฉพาะ เราเรียกจำนวนเฉพาะทั้งสี่จำนวนข้างต้นนี้ว่า quadruplet เช่น

p = 5 quadruplet ได้แก่ 5, 7, 11, 13
p = 11 quadruplet ได้แก่ 11, 13, 17, 19
p = 101 quadruplet ได้แก่ 101, 103, 107, 109
p = 191 quadruplet ได้แก่ 191, 193, 197, 199
p = 821 quadruplet ได้แก่ 821, 823, 827, 829
p = 1481 quadruplet ได้แก่ 1481, 1483, 1487, 1489

3.4 ลำดับเลขคณิตที่แต่ละเทอมเป็นจำนวนเฉพาะ (Arithmetical Progressions Whose Terms are Prime Numbers)

ลำดับเลขคณิตที่ประกอบด้วยจำนวนเฉพาะที่แตกต่างกัน 18 จำนวน ที่เป็นที่แพร่หลาย ได้แก่ $4808316343 + 71777060\,k$ สำหรับ $k = 0, 1, 2, \ldots, 17$

P.A. Pritchard ผู้พบลำดับเลขคณิต $4180566390\,k + 8297644387$ สำหรับ $k = 0, 1, 2, \ldots, 18$ ที่ให้จำนวนเฉพาะที่แตกต่างกัน 19 จำนวน แต่อย่างไรก็ตาม เราไม่รู้ว่ามีลำดับเลขคณิตที่ประกอบด้วยจำนวนเฉพาะที่แตกต่างกัน 100 จำนวนหรือไม่ เราจะพิสูจน์ว่าถ้ามีลำดับเลขคณิตที่ประกอบด้วยจำนวนเฉพาะที่แตกต่างกัน 100 จำนวน แล้ว ผลต่างของลำดับเลขคณิตจะต้องมีค่ามากกว่า 30 หลัก

ทฤษฎีบทต่อไปนี้จะแสดงข้อความข้างต้นดังกล่าว

ทฤษฎีบท 1 ถ้า n และ r เป็นจำนวนธรรมชาติ โดยที่ $n > 1$ และถ้า n เทอมของลำดับเลขคณิตคือ $m, m+r, \ldots, m+(n-1)r$ เป็นจำนวนเฉพาะคี่ แล้วผลต่าง r จะถูกหารลงตัวได้ด้วยทุกจำนวนเฉพาะที่น้อยกว่า n

พิสูจน์ สมมติให้ m, n และ r เป็นจำนวนธรรมชาติที่กำหนดให้ โดยที่ $m, n > 1$

ให้ $m, m+r, \ldots, m+(n-1)r$ เป็นลำดับเลขคณิตที่มีแต่ละเทอมเป็นจำนวนเฉพาะคี่

ดังนั้นเราจะได้ว่า $m \geq n$ เนื่องจากถ้า $m < n$ แล้วจะมีจำนวนประกอบ $m+mr = m(1+r)$ เป็นสมาชิกหนึ่งของลำดับเลขคณิตข้างต้น

ให้ p เป็นจำนวนเฉพาะจำนวนหนึ่ง ที่น้อยกว่า n

และให้ $r_0, r_1, \ldots, r_{p-1}$ (1)

เป็นเศษเหลือที่ได้จากการหาร $m, m+r, \ldots, m+(p-1)r$ (2)

ด้วยจำนวนเฉพาะ p ตามลำดับ ดังนั้นทุกสมาชิกใน (1) ต้องไม่เท่ากับศูนย์ เพราะว่าถ้ามีบางสมาชิกใน (1) มีค่าเท่ากับศูนย์แล้ว จะมีสมาชิกใน (2)หารลงตัวได้ด้วย p ซึ่งเป็นไปไม่ได้

นั่นคือ เศษเหลือสามารถเป็นได้จากค่าเหล่านี้คือ $1,2,3,\ldots,p-1$ ซึ่งมี $p-1$ จำนวน

จากนี้เราสรุปได้ว่าสำหรับบางจำนวนเต็ม k และ j โดยที่ $0 \leq k < j \leq p-1$ เราจะมี $r_k = r_j$

นั่นคือ p ไปหาร $m+kr$ ได้เศษเหลือ r_k และ p ไปหาร $m+jr$ ได้เศษเหลือ r_j

$m + kr = ap + r_k$ โดยที่ $a \in N$ และ $m + jr = bp + r_j$ โดยที่ $b \in N$

จะได้ว่า $(m + jr) - (m + kr) = (b - a)p + (r_j - r_k) = (b - a)p$

ดังนั้น $p \mid (m+jr) - (m+kr)$

$p \mid (j - k)r$

แต่ $0 < j-k \leq p-1 < p$

จะได้ว่า $p \mid r$

แต่เนื่องจาก p เป็นจำนวนเฉพาะที่น้อยกว่า n

ดังนั้น ทฤษฎีบท 1 ก็เป็นจริง #

บทแทรก 2 ถ้ามีลำดับเลขคณิตค่าเพิ่ม ที่ประกอบด้วยจำนวนเฉพาะ n จำนวนที่มากกว่า 2 แล้วผลต่างของลำดับเลขคณิตถูกหารได้ด้วยผลคูณ P_n ของจำนวนเฉพาะทั้งหมดที่น้อยกว่า n และผลต่างของลำดับเลขคณิตนี้มากกว่าหรือเท่ากับ P_n

พิสูจน์ เป็นผลโดยตรงจากทฤษฎีบท 1 ในหัวข้อ 3.4 #

3.5 จำนวนเฉพาะในลำดับเลขคณิตที่กำหนดให้ (Primes in a Given Arithmetical Progression)

หัวข้อนี้จะกล่าวถึงปัญหาของจำนวนเฉพาะในลำดับเลขคณิตซึ่งแตกต่างจากหัวข้อที่แล้วมา คือ หัวข้อนี้จะต้องหาจำนวนธรรมชาติ a และ b ที่ทำให้ลำดับเลขคณิต $ak + b$, $k = 1,2,3, \ldots$ ประกอบด้วยจำนวนเฉพาะเป็นจำนวนอนันต์พจน์

พิจารณา ถ้า $(a,b) = d > 1$ แล้ว $d \mid a$ และ $d \mid b$
นั่นคือ จะไม่มีจำนวนเฉพาะในลำดับเลขคณิต $ak + b$, $k = 1,2,3, \ldots$
เพราะว่า สำหรับ k ใด ๆ, $ak + b = d\left(\frac{ka}{d} + \frac{b}{d}\right)$ เป็นจำนวนประกอบ

ดังนั้น เงื่อนไขที่จำเป็น สำหรับการมีลำดับเลขคณิต $ak + b$ ที่ประกอบด้วยจำนวนเฉพาะเป็นจำนวนไม่จำกัด คือ $(a,b) = 1$

ในปี ค.ศ. 1837 นักคณิตศาสตร์ชื่อ Lejeune Dirichlet ได้พิสูจน์ว่า เงื่อนไขที่จำเป็นข้างต้นนี้เป็นเงื่อนไขที่เพียงพอด้วยเช่นกัน การพิสูจน์ของ Lejeune Dirichlet ไม่เป็นแบบที่ง่าย ต่อมาการพิสูจน์จึงได้ถูกปรับปรุงให้เป็นแบบที่ง่ายขึ้น แต่ก็ยังซับซ้อนอยู่

ต่อไปจะเป็นสองทฤษฎีบทที่สมมูลกัน

ทฤษฎีบท 1 ถ้าให้ a, b เป็นจำนวนธรรมชาติ โดยที่ $(a,b) = 1$ แล้วจะมีจำนวนเฉพาะเป็นจำนวนไม่จำกัดในรูปของ $ak + b$ สำหรับ k ที่เป็นจำนวนธรรมชาติ

ทฤษฎีบท 2 ถ้าให้ a, b เป็นจำนวนธรรมชาติ โดยที่ $(a,b) = 1$ แล้วจะมีจำนวนเฉพาะ p อย่างน้อยที่สุดหนึ่งจำนวนที่อยู่ในรูปของ $ak + b$ สำหรับ k ที่เป็นจำนวนธรรมชาติ

พิสูจน์ เห็นได้ชัดว่า ทฤษฎีบท 1 $\longrightarrow$ ทฤษฎีบท 2

ต่อไปเราจะต้องแสดงว่า ทฤษฎีบท 2 $\longrightarrow$ ทฤษฎีบท 1

พิจารณา ถ้า $a = 1$ การพิจารณาจะตามจากความจริงที่ว่า ทฤษฎีบท 1 เป็นจริง

ดังนั้น เราสมมติให้ $a > 1$

โจทย์กำหนดให้ a, b เป็นจำนวนธรรมชาติ โดยที่ $(a,b) = 1$

ดังนั้น $(a^m,b) = 1$

นั่นคือโดยทฤษฎีบท 2 จะมีจำนวนเฉพาะ p ที่ $p = a^m k + b$ สำหรับ k เป็นจำนวนธรรมชาติ

เนื่องจาก $a > 1$, $a^m \geq 2^m > m$ ดังนั้น $p > m$

นั่นคือ เราได้พิสูจน์แล้วว่า สำหรับจำนวนธรรมชาติ m ใด ๆ จะมีจำนวนเฉพาะซึ่งอยู่ในรูป $ak + b$ ที่มีค่ามากกว่า m

นั่นคือ ได้พิสูจน์แล้วว่า มีจำนวนเฉพาะเป็นจำนวนไม่จำกัด ซึ่งอยู่ในรูป $ak + b$ สำหรับ k เป็นจำนวนธรรมชาติ #