บทที่ 1
จำนวนเต็ม
(Integers)

จำนวน

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

เรียกว่า **จำนวนเต็ม** (integers)

$$0, 1, 2, 3, \ldots$$

เรียกว่า **จำนวนเต็มที่ไม่เป็นลบ** (non-negative integers)

$$1, 2, 3, \ldots$$

เรียกว่า **จำนวนเต็มบวก** (positive integers)

$$\ldots, -3, -2, -1$$

เรียกว่า **จำนวนเต็มลบ** (negative integers)

ในการศึกษาวิชาทฤษฎีจำนวนนี้ จะได้ศึกษาถึงคุณสมบัติของจำนวนเต็ม โดยเฉพาะคุณสมบัติของจำนวนเต็มบวก และในการศึกษาคุณสมบัติต่าง ๆ เหล่านี้ต้องอาศัยสัจพจน์และทฤษฎีบทต่าง ๆ เหล่านี้เสียก่อน ดังนี้

1.1 คุณสมบัติการเป็นอันดับที่ดี (The Well-Ordering Property)

คุณสมบัติการเป็นอันดับที่ดีกล่าวว่า **"ทุกเซตย่อยของจำนวนเต็มบวกที่ไม่ใช่เซตว่างต้องมีสมาชิกตัวที่เล็กที่สุด"**

ความหมายของคำกล่าวนี้ก็คือ ถ้าให้ S เป็นเซตย่อยของจำนวนเต็มบวกที่ไม่ใช่เซตว่าง จะต้องมี $s \in S$ ซึ่ง $s \leqslant x$ ทุก x ใน S

ตัวอย่าง 1.1 1 เป็นจำนวนเต็มบวกที่เล็กที่สุด

พิสูจน์ สมมติมีจำนวนเต็มบวก a โดยที่ $0 < a < 1$

ให้ $C = \{a|a$ เป็นจำนวนเต็มบวก และ $a < 1\}$

โดยสมมติฐาน $C \neq \phi$

ดังนั้น จากคุณสมบัติการเป็นอันดับที่ดี C มีสมาชิกตัวที่เล็กที่สุด

ให้ b เป็นสมาชิกตัวที่เล็กที่สุดของ C

นั่นคือ $0 < b < 1$

ซึ่งจะทำให้ $0 < b^2 < b < 1$

ดังนั้น b^2 เป็นสมาชิกของ C ที่น้อยกว่า b ซึ่งเป็นไปไม่ได้ เนื่องจาก b เป็นสมาชิกที่เล็กที่สุดของ C

นั่นคือ 1 เป็นจำนวนเต็มบวกที่น้อยที่สุด #

ตัวอย่าง 1.2 $\sqrt{2}$ เป็นจำนวนอตรรกยะ

พิสูจน์ สมมติ $\sqrt{2}$ เป็นจำนวนตรรกยะ

ดังนั้น $\sqrt{2} = \frac{m}{n}$ โดยที่ m, n เป็นจำนวนเต็ม และ $n \neq 0$

ให้ $C = \{n|n$ เป็นจำนวนเต็มบวก และมีจำนวนเต็ม m ที่ทำให้ $\sqrt{2} = \frac{m}{n}\}$

ดังนั้น $C \neq \phi$ โดยคุณสมบัติการเป็นอันดับที่ดี C มีสมาชิกที่เล็กที่สุด

ให้ b เป็นสมาชิกตัวที่เล็กที่สุดของ C และให้ a เป็นจำนวนเต็มที่ทำให้

$$\sqrt{2} = \frac{a}{b}$$

และเพราะว่า $1 < 2 < 4$ จะได้ว่า $1 < \sqrt{2} < 2$

นั่นคือ $1 < \frac{a}{b} < 2$

ผลที่ตามมาคือ $b < a < 2b$ และจึงได้ว่า $0 < a - b < b$

และเพราะว่า $\sqrt{2} = \frac{a}{b}$

ดังนั้น $2 = \frac{a^2}{b^2}$

ซึ่งทำให้ $2b^2 = a^2$

และ

$$2b^2 - ab = a^2 - ab$$

$$b(2b-a) = a(a-b)$$

ซึ่งได้ว่า

$$\sqrt{2} = \frac{a}{b} = \frac{2b-a}{a-b}$$

นั่นคือ $\sqrt{2}$ เขียนเป็นเศษส่วนของจำนวนเต็ม โดยที่ส่วนน้อยกว่า b ซึ่งเป็นไปไม่ได้

ดังนั้น $\sqrt{2}$ ต้องเป็นจำนวนอตรรกยะ #

ตัวอย่าง 1.3 ให้ k เป็นจำนวนเต็มบวกใด ๆ แล้วจะไม่มีจำนวนเต็มบวก n ที่ทำให้

$$k < n < k+1$$

พิสูจน์ สมมติมีจำนวนเต็มบวก n ที่ทำให้ $k < n < k+1$

ดังนั้น $0 < n-k < 1$ ซึ่งทำให้ $n-k$ เป็นจำนวนเต็มบวกที่น้อยกว่า 1 ซึ่งเป็นไปไม่ได้

#

คุณสมบัติการเป็นอันดับที่ดีสามารถพิสูจน์ทฤษฎีบทที่สำคัญยิ่งสำหรับจำนวนเต็มบวก ทฤษฎีบทหนึ่งคือ **ทฤษฎีบทอุปนัยทางคณิตศาสตร์** ดังนี้

ทฤษฎีบท 1.1 *ทฤษฎีบทอุปนัยทางคณิตศาสตร์แบบที่ 1* (Mathematical Induction : first form)

ให้ S เป็นเซตย่อยของเซตจำนวนเต็มบวก โดยที่ S ไม่ใช่เซตว่าง และ

1. $1 \in S$
2. สำหรับแต่ละจำนวนเต็มบวก k ถ้า $k \in S$ แล้ว $k+1 \in S$

แล้ว จะได้ว่า S คือ เซตของจำนวนเต็มบวก

พิสูจน์ ให้ S เป็นเซตย่อยของจำนวนเต็มบวก โดยที่ $S \neq \phi$ และมีคุณสมบัติ 1 และ 2

สมมติ S ไม่ใช่เซตของจำนวนเต็มบวก

ให้ $C = \{n | n$ เป็นจำนวนเต็มบวก และ $n \notin S\}$

โดยสมมติฐาน $C \neq \phi$ และโดยคุณสมบัติการเป็นอันดับที่ดี C มีสมาชิกตัวที่เล็กที่สุด

ให้ n เป็นสมาชิกตัวที่เล็กที่สุดของ C จะได้ว่า $1 < n$

เพราะว่า 1 เป็นสมาชิกของ S

เพราะว่า $0 < n-1 < n$

จะได้ว่า $n-1 \in S$

โดยคุณสมบัติ 2 ของ S

$$n = (n-1)+1 \in S$$

ซึ่งขัดแย้งกับคุณสมบัติของ n

ดังนั้น S ต้องเป็นเซตจำนวนเต็มบวก

ตัวอย่าง 1.4 สำหรับจำนวนเต็มบวก n ใด ๆ

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

วิธีทำ ให้ $C = \{n \mid n$ เป็นจำนวนเต็มบวก $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\}$

$1 \in C$ เนื่องจาก $1 = \frac{1(1+1)}{2}$

สมมติ $k \in C$

ดังนั้น $$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

นั่นคือ $$1+2+\ldots+k = \frac{k(k+1)}{2}$$

เพราะฉะนั้น

$$(1+2+\ldots+k)+(k+1) = \frac{k(k+1)}{2}+k+1$$

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

นั่นคือ $k+1 \in S$

ดังนั้น โดยทฤษฎีบทอุปนัยทางคณิตศาสตร์ C คือ เซตของจำนวนเต็มบวก #

ตัวอย่าง 1.5 ให้ a และ r เป็นจำนวนจริง โดยที่ $r \neq 1$ แล้ว

$$\sum_{j=0}^{n} ar^j = a+ar+ar^2+\ldots+ar^n = \frac{ar^{n+1}-a}{r-1}$$

พิสูจน์ ให้ $C = \{n \mid n$ เป็นจำนวนเต็มบวก $\sum_{j=0}^{n} ar^j = \frac{ar^{n+1}-a}{r-1}\}$

$1 \in C$ เนื่องจาก $a+ar = \frac{ar^2-a}{r-1}$

สมมติ $k \in C$

ดังนั้น $$\sum_{j=0}^{k} ar^j = \frac{ar^{k+1} - a}{r-1}$$

นั่นคือ

$$a + ar + ar^2 + \dots + ar^k = \frac{ar^{k+1} - a}{r-1}$$

เพราะฉะนั้น

$$\begin{aligned}(a + ar + ar^2 + \dots + ar^k) + ar^{k+1} &= \frac{ar^{k+1} - a}{r-1} + ar^{k+1} \\ &= \frac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r-1} \\ &= \frac{ar^{k+2} - a}{r-1}\end{aligned}$$

นั่นคือ $$\sum_{j=0}^{k+1} ar^j = \frac{ar^{k+2} - a}{r-1}$$

เพราะฉะนั้น $k+1 \in C$

ดังนั้น โดยทฤษฎีบทอุปนัยทางคณิตศาสตร์ C คือ เซตของจำนวนเต็มบวก #

ทฤษฎีบท 1.2 *ทฤษฎีบทอุปนัยทางคณิตศาสตร์ แบบที่ 2* (Mathematical Induction : second form)

ให้ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของเซตจำนวนเต็มบวก และ

1. $1 \in S$
2. สำหรับจำนวนเต็มบวก k ใด ๆ ถ้า $1, 2, 3, \dots, k$ เป็นสมาชิกของ S แล้ว $k+1$ เป็นสมาชิกของ S

แล้วจะได้ว่า S คือ เซตของจำนวนเต็มบวก

พิสูจน์ ให้ S เป็นเซตย่อยของเซตจำนวนเต็มบวกที่ไม่ใช่เซตว่าง และมีคุณสมบัติ 1, 2

สมมติ S ไม่ใช่เซตของจำนวนเต็มบวก

ให้ $C = \{n | n$ เป็นจำนวนเต็มบวก และ $n \notin S\}$

โดยสมมติฐาน $C \neq \phi$ ดังนั้น โดยคุณสมบัติการเป็นอันดับที่ดี

ให้ n_0 เป็นสมาชิกตัวที่น้อยที่สุดของ C

เนื่องจาก $1 \in S$ จะได้ว่า $1 < n_0$

และเพราะว่า n_0 เป็นสมาชิกตัวที่น้อยที่สุดของ C จะได้ว่า

$1, 2, \ldots, n_0 - 1$ เป็นสมาชิกของ S

ดังนั้น โดยคุณสมบัติของ S $n_0 = (n_0 - 1) + 1$ เป็นสมาชิกของ S จึงเกิดการขัดแย้ง

เพราะฉะนั้น S ต้องเป็นเซตจำนวนเต็มบวก #

ตัวอย่าง 1.6 กำหนด (a_n) เป็นลำดับ โดยที่

$$a_1 = 1$$

$$a_2 = 3$$

$$a_n = a_{n-1} + a_{n-2} \quad \text{สำหรับทุกจำนวนเต็มบวก } n \geqslant 3$$

ลำดับ (a_n) นี้เรียกว่า **ลำดับลูคัส** (Lucas Sequence)

จงแสดงว่า $a_n < \left(\frac{7}{4}\right)^n$ สำหรับทุกจำนวนเต็มบวก n

พิสูจน์ พิจารณา a_1 และ a_2

จะได้ $a_1 = 1 < \left(\frac{7}{4}\right)^1$

และ $a_2 = 3 < \left(\frac{7}{4}\right)^2$

นั่นคือ ข้อความ $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับ $n = 1, 2$

ให้ k เป็นจำนวนเต็มบวกใด ๆ และสมมติว่า

$$a_n < \left(\frac{7}{4}\right)^n \quad \text{ทุก } n = 1, 2, \ldots, k-1$$

เพราะว่า $a_k = a_{k-1} + a_{k-2}$

จะได้ว่า

$$\begin{aligned} a_k = a_{k-1} + a_{k-1} &< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} \\ &= \left(\frac{7}{4}\right)^{k-2}\left[\frac{7}{4} + 1\right] \\ &= \left(\frac{7}{4}\right)^{k-2}\left(\frac{11}{4}\right) \\ &< \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^k \end{aligned}$$

นั่นคือ ข้อความ $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับ $n = k$

เพราะฉะนั้น โดยทฤษฎีบทอุปนัยทางคณิตศาสตร์ แบบที่ 2 $a_n < \left(\frac{7}{4}\right)^n$ ทุกจำนวนเต็มบวก n #

แบบฝึกหัด 1.1

1 . จงแสดงว่า $1+3+5+\ldots+(2n-1) = n^2$ สำหรับทุกจำนวนเต็มบวก n

2 . จงแสดงว่า $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1) = \frac{n(n+1)(n+2)}{3}$ สำหรับทุกจำนวนเต็มบวก n

3. จงแสดงว่า $1^2+3^2+5^2+\ldots+(2n-1)^2 = \frac{n(4n^2-1)}{3}$ สำหรับทุกจำนวนเต็มบวก n

4. จงแสดงว่า $1^3+2^3+3^3+\ldots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$ สำหรับทุกจำนวนเต็มบวก n

5. โดยการใช้ทฤษฎีบทอุปนัยทางคณิตศาสตร์ แบบที่ 2 จงแสดงว่า

$$a^n-1 = (a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\ldots+a+1)$$

สำหรับทุกจำนวนเต็มบวก n

(*แนะนำ* : $a^{n+1}-1 = (a+1)(a^n-1)-a(a^{n-1}-1)$)

6. จงแสดงว่า กำลังสามของเลขจำนวนเต็มใด ๆ เขียนได้เป็นผลต่างของกำลังสองของจำนวนสองจำนวน

(*แนะนำ* : $n^3 = (1^3+2^3+\ldots+n^3) - (1^3+2^3+\ldots+(n-1)^3)$)

1.2 ทฤษฎีบททวินาม (The Binomial Theorem)

เราสามารถใช้วิธีอุปนัยทางคณิตศาสตร์มาให้นิยามของฟังก์ชันจำนวนเต็มได้ โดยให้นิยาม $f(1)$ และนิยาม $f(n+1)$ จาก $f(n)$ ฟังก์ชัน ซึ่งนิยามแบบนี้เรียกว่า **ฟังก์ชันนิยามแบบเวียนบังเกิด** (f is defined recursively)

บทนิยาม 1.1 *ฟังก์ชันแฟกทอเรียล* (factorial) นิยามโดย

$$f(0) = 1$$

$$f(1) = 1$$

$$f(n+1) = (n+1)\,f(n) \qquad \text{ทุกจำนวนเต็ม } n > 1$$

และโดยทั่วไปจะเขียนแทนด้วย $f(n) = n!$ (อ่านว่า n แฟกทอเรียล)

จากบทนิยามจะได้ว่า

$$0! = 1$$

$$1! = 1$$

$$2! = 2f(1) = 2\cdot 1$$

$$3! = 3f(2) = 3\cdot 2\cdot 1$$

$$\vdots$$

$$n! = nf(n-1) = n(n-1)(n-2)\ldots 2\cdot 1$$

เมื่อได้รู้จักกับฟังก์ชันแฟกทอเรียลแล้ว ต่อไปจะได้นำฟังก์ชันแฟกทอเรียลนี้มาให้บทนิยามของสัมประสิทธิ์ทวินาม (binomial coefficients)

บทนิยาม 1.2 ให้ m, k เป็นจำนวนเต็มบวก โดยที่ $k \leqslant m$ แล้ว สัมประสิทธิ์ทวินาม $\binom{m}{k}$ นิยามโดย

$$\binom{m}{k} = \frac{m!}{k!\,(m-k)!}$$

ตัวอย่าง 1.7 จงหาค่าสัมประสิทธิ์ทวินาม $\binom{7}{3}$

วิธีทำ

$$\binom{7}{3} = \frac{7!}{3!\,(7-3)!}$$

$$= \frac{7!}{3!\,4!}$$

$$= \frac{7\times6\times5}{3\times2\times1} = 35$$

ทฤษฎีบท 1.3 ให้ n, k เป็นจำนวนเต็มบวก โดยที่ $k \leqslant n$ แล้ว

ก. $\binom{n}{0} = \binom{n}{n} = 1$

ข. $\binom{n}{k} = \binom{n}{n-k}$

พิสูจน์ ก.
$$\binom{n}{0} = \frac{n!}{0!\ (n-0)!}$$
$$= \frac{n!}{1\cdot n!} = 1$$

และ
$$\binom{n}{n} = \frac{n!}{n!\ (n-n)!}$$
$$= \frac{n!}{n!\ 0!}$$
$$= \frac{n!}{n!\ 1} = 1$$

ข.
$$\binom{n}{k} = \frac{n!}{k!\ (n-k)!}$$
$$= \frac{n!}{(n-k)!\ \big(n-(n-k)\big)!}$$
$$= \binom{n}{n-k}$$ #

ต่อไปจะเป็นคุณสมบัติที่สำคัญของสัมประสิทธิ์ทวินาม ซึ่งเรียกว่า กฎของปาสคาล

ทฤษฎีบท 1.4 *กฎของปาสคาล* (Pascal's Rule)

ให้ n และ k เป็นจำนวนเต็มบวก โดยที่ $k \leqslant n$ แล้ว

$$\binom{n}{k}+\binom{n}{k-1} = \binom{n+1}{k}$$

พิสูจน์
$$\binom{n}{k}+\binom{n}{k-1} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!}$$
$$= \frac{n!}{(k-1)!\,(n-k)!}\left[\frac{1}{k} + \frac{1}{n-k+1}\right]$$

$$= \frac{n!}{(k-1)!\,(n-k)!}\left[\frac{n-k+1+k}{k(n-k+1)}\right]$$

$$= \frac{n!\,(n+1)}{(k-1)!\,(n-k)!\,k(n-k+1)}$$

$$= \frac{(n+1)!}{k!\,(n-k+1)!}$$

$$= \binom{n+1}{k} \qquad \#$$

จากกฎของปาสคาลนำไปสร้างสามเหลี่ยมปาสคาล (Pascal's triangle) ได้ดังนี้

ในสามเหลี่ยมปาสคาล สัมประสิทธิ์ทวินาม $\binom{n}{k}$ จะคือสมาชิกตัวที่ $k+1$ ในแถวที่ $n+1$

ดังนั้น สามเหลี่ยมปาสคาล 9 แถวแรก จะเป็นดังนี้

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

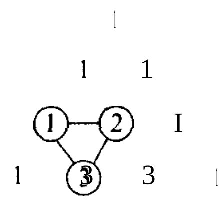
1 8 28 56 70 56 28 8 1

....

....

รูป 1.1 *สามเหลี่ยมปาสคาล*

จากสามเหลี่ยมปาสคาลจะเห็นว่า ตัวเลขที่อยู่ตามขอบของสามเหลี่ยมทั้งหมดเป็น 1 และสำหรับตัวเลขที่อยู่ภายในใด ๆ คือ ผลบวกของตัวเลขที่อยู่แถวบนในตำแหน่งใกล้ ๆ กัน 2 จำนวน เช่น พิจารณาจากแถวที่ 3 และ 4 ของสามเหลี่ยม



3 คือ ผลบวกของ 1 และ 2

รูป 1.2

ต่อไปจะได้กล่าวถึงทฤษฎีบททวินาม ซึ่งเป็นสูตรสำหรับการกระจาย $(a+b)^n$ เมื่อ $n \geqslant 1$ โดยการคำนวณโดยตรง จะได้สำหรับจำนวนจริง a, b ใด ๆ

$$
\begin{aligned}
(a+b)^1 &= a + b \\
(a+b)^2 &= a^2+2ab+b^2 \\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4 \\
&\ldots\ldots
\end{aligned}
$$

ซึ่งทฤษฎีบททวินามจะให้สูตรการกระจาย $(a+b)^n$ เมื่อ $n \geqslant 1$ ดังนี้

ทฤษฎีบท 1.5 *ทฤษฎีบททวินาม* (Binomial's Theorem)

ให้ a, b เป็นจำนวนจริงใด ๆ และ n เป็นจำนวนเต็มบวก จะได้ว่า

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

หรือเขียนสั้น ๆ จะได้ว่า

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j}a^{n-j}b^j$$

พิสูจน์ จะพิสูจน์โดยใช้ทฤษฎีบทอุปนัยทางคณิตศาสตร์

เมื่อ $n = 1$

จะได้ $a+b = \binom{1}{0}a + \binom{1}{1}b$

นั่นคือ ทฤษฎีบทเป็นจริง เมื่อ $n = 1$

สมมติว่าทฤษฎีบทเป็นจริงสำหรับจำนวนเต็มบวก k

นั่นคือ

$$(a+b)^k = \binom{k}{0}a^k + \binom{k}{1} a^{k-1}b + \binom{k}{2}a^{k-2}b^2 + \ldots + \binom{k}{k-1}ab^{k-1} + \binom{k}{k}b^k$$

เพราะว่า

$$(a+b)^{k+1} = (a+b)^k \, (a+b)$$

ดังนั้น

$$(a+b)^{k+1} = (a+b)^k \, (a+b)$$

$$= \left[\sum_{j=0}^{k} \binom{k}{j}\right] a^{k-j}b^j(a+b)$$

$$= \sum_{j=0}^{k} \binom{k}{j} a^{k-j+1}b^j + \sum_{j=0}^{k} \binom{k}{j} a^{k-j}b^{j+1}$$

เพราะว่า

$$\sum_{j=0}^{k} \binom{k}{j} a^{k-j+1}b^j = a^{k+1} + \sum_{j=1}^{k} \binom{k}{j} a^{k-j+1}b^j$$

และ

$$\sum_{j=0}^{k} \binom{k}{j} a^{k-j}b^{j+1} = \sum_{j=0}^{k-1} \binom{k}{j} a^{k-j}b^{j+1} + b^{k+1}$$

$$= \sum_{j=1}^{k} \binom{k}{j-1} a^{k-j+1}b^j + b^{k+1}$$

จะได้

$$(a+b)^{k+1} = a^{k+1} + \sum_{j=1}^{k} \binom{k}{j} a^{k-j+1}b^j + \sum_{j=1}^{k} \binom{k}{j-1} a^{k-j+1}b^j + b^{k+1}$$

$$= a^{k+1} + \sum_{j=1}^{k} \left[\binom{k}{j} + \binom{k}{j-1}\right] a^{k-j+1}b^j + b^{k+1}$$

และเพราะว่า

$$\binom{k}{j} + \binom{k}{j-1} = \binom{k+1}{j}$$

เพราะฉะนั้น

$$(a+b)^{k+1} = a^{k+1} + \sum_{j=1}^{k} \binom{k+1}{j} a^{k-j+1}b^j + b^{k+1}$$

$$= \sum_{j=0}^{k} \binom{k+1}{j} a^{k+1-j}b^j$$

นั่นคือ ทฤษฎีบทเป็นจริงเมื่อ $n = k+1$

ดังนั้น โดยทฤษฎีบทอุปนัยทางคณิตศาสตร์

$$(a + b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^n$$

ทุกจำนวนเต็มบวก n #

ตัวอย่าง 1.8 จงหาค่า 2^n เมื่อ n เป็นจำนวนเต็มบวกใด ๆ และเมื่อ $n = 5$

วิธีทำ เนื่องจาก $2^n = (1+1)^n$

ดังนั้น โดยทฤษฎีบททวินาม

$$2^n = (1+1)^n = \sum_{j=0}^{n} \binom{n}{j} 1^{n-j} 1^j$$

$$= \sum_{j=0}^{n} \binom{n}{j}$$

$$2^n = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

นั่นคือ 2^n คือ ผลบวกของจำนวนเลขในแถวที่ $n+1$ ของสามเหลี่ยมปาสคาล

พิจารณาค่า 2^5

$$2^5 = \binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5}$$

และเพราะว่า จำนวนเลขในแถวที่ 6 ของสามเหลี่ยมปาสคาล คือ

1 5 10 10 5 1

จะได้ว่า

$$2^5 = 1 + 5 + 10 + 10 + 5 + 1$$

$$= 32$$

แบบฝึกหัด 1.2

2. จงหาค่า $\binom{10}{0}, \binom{10}{3}, \binom{10}{5}, \binom{10}{7}$ และ $\binom{10}{10}$

3. จงหาค่าสัมประสิทธิ์ทวินาม $\binom{9}{3}, \binom{9}{4}$ และ $\binom{10}{4}$

   และจงแสดงโดยการคำนวณโดยตรงว่า $\binom{9}{3}+\binom{9}{4} = \binom{10}{4}$

4. ให้ n เป็นจำนวนเต็มบวก โดยการกระจาย $(1+(-1))^n$ โดยทฤษฎีบททวินาม จงแสดงว่า

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

5. ให้ n เป็นจำนวนเต็ม โดยที่ $n \geqslant 4$ และ $2 \leqslant k \leqslant n\cdot 2$ จงแสดงว่า

$$\binom{n}{k} = \binom{n\quad 2}{k\quad 2}+2\binom{n-2}{k-1}+\binom{n-2}{k}$$

6. สำหรับจำนวนเต็ม $n \geqslant 1$ จงแสดงว่า

$$\binom{n}{1}+2\binom{n}{2}+3\binom{n}{3}+\ldots+n\binom{n}{n} = n2^{n-1}$$

   (*แนะนำ* : กระจาย $n(1+b)^{n-1}$ โดยทฤษฎีบททวินาม และเลือกใช้ค่า $b = 1$ และ

$$n\binom{n}{k} = k+ \binom{n}{k+}$$

7. สำหรับจำนวนเต็มบวก $n \geqslant 1$ จงแสดงว่า

$$\binom{n}{0}+2\binom{n}{1}+2^2\binom{n}{2}+\ldots+2^n\binom{n}{n} = 3^n$$

8. สำหรับจำนวนเต็ม $n \geqslant 2$ จงพิสูจน์ว่า

$$\binom{2}{2}+\binom{3}{2}+\binom{4}{2}+\cdots+\binom{n}{2} = \binom{n+}{3}$$

9. จงหาจำนวนเต็มบวก x, y และ z ที่ทำให้ $x!+y! = z!$

10. **โดยไม่ใช้วิธีการคำนวณโดยตรง จงแสดงว่า**

10.1 $6!\ 7! = 10!$

10.2 $16! = 14!\ 5!\ 2!$

10.3 $10! = 7!\ 5!\ 3!$

10.4 $9! = 7!\ 3!\ 3!\ 2!$

1.3 **การหารลงตัว** (Divisibility)

พิจารณาการหารของจำนวนเต็มใด ๆ สองจำนวน เราจะพบว่า ผลหาร (quotient) อาจเป็นจำนวนเต็มหรืออาจไม่ใช่จำนวนเต็ม เช่น $\frac{24}{8}$ มีผลหารเป็นจำนวนเต็มคือ 3 แต่ $\frac{24}{5}$ มีผลหารเป็น 4.8 ซึ่งไม่ใช่จำนวนเต็ม ดังนั้น สำหรับจำนวนเต็ม a และ b ใด ๆ โดยที่ $a \neq 0$ เราจะกล่าวว่า a หาร b ลงตัว ถ้าผลหารของ $\frac{b}{a}$ เป็นจำนวนเต็ม ซึ่งเราสามารถให้บทนิยามได้ดังนี้

บทนิยาม 1.3 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ เรากล่าวว่า a **หาร** b **ลงตัว** (a divides b) เขียนแทนด้วย $a|b$ ถ้ามีจำนวนเต็ม c ที่ทำให้ $b = ac$

และถ้า a หาร b ลงตัว เรากล่าวว่า a **เป็นตัวหาร** (divisor) หรือ **แฟกเตอร์** (factor) ของ b เรียก b ว่า เป็น **พหุคูณ** (multiple) **ของ** a

ในกรณีที่ a หาร b ไม่ลงตัว จะเขียนแทนด้วย $a \nmid b$

ตัวอย่าง 1.9 $13|182$ เนื่องจาก

$$182 = 13 \cdot 14$$

เรียก 13 ว่า เป็นตัวหารของ 182 และ 182 คือ พหุคูณของ 13 #

ตัวอย่าง 1. $-5|30$ เนื่องจาก

$$30 = (-5)(-6)$$

เรียก -5 ว่า เป็นตัวหารของ 30 และ 30 คือ พหุคูณของ -5 #

ตัวอย่าง 1.11 $5 \nmid 37$ เนื่องจาก

$37 \neq 5k$ ทุกจำนวนเต็ม k #

สำหรับจำนวนเต็มใด ๆ อาจมีตัวหารได้มากมาย นอกจากนั้น ถ้า a เป็นตัวหารของ b แล้ว $-a$ ต้องเป็นตัวหารของ b ด้วย

ตัวอย่าง 1.12 **ตัวหารของ** 6 คือ $1, -1, 2, -2, 3, -3, 6$ และ -6

ตัวหารของ 7 คือ $1, -1, 7$ และ -7

ตัวหารของ 15 คือ $1, -1, 3, -3, 5, -5, 15$ และ -15 #

ทฤษฎีบท 1.6 ถ้า a, b และ c เป็นจำนวนเต็ม โดยที่ $a|b$ และ $b|c$ แล้ว $a|c$

พิสูจน์ เพราะว่า $a|b$ และ $b|c$ ดังนั้น จะมีจำนวนเต็ม e, f โดยที่

$$b = ae \qquad \text{และ} \qquad c = bf$$

ดังนั้น $c = bf = (ae)f = a(ef)$

นั่นคือ $a|c$ #

ตัวอย่าง 1.13 เนื่องจาก 11166 และ $66|198$

โดยทฤษฎีบท 1.6 111198 #

ทฤษฎีบท 1.7 ถ้า a, b, c, m และ n เป็นจำนวนเต็ม โดยที่ $c|a$ และ c / b แล้ว $c|(ma+nb)$

พิสูจน์ เพราะว่า c / a และ c/b ดังนั้น จะมีจำนวนเต็ม e, f โดยที่

$$a = ce \qquad \text{และ} \qquad b = cf$$

ดังนั้น

$$\begin{aligned} ma+nb &= m(ce)+n(cf) \\ &= c(me+nf) \end{aligned}$$

นั่นคือ $c|(ma+nb)$ #

ตัวอย่าง 1.14 เพราะว่า $3|21$ และ $3|33$ โดยทฤษฎีบท 1.7 จะได้ว่า

$$3|(5\cdot 21 - 3\cdot 33)$$

นั่นคือ 316 #

ทฤษฎีบท 1.8 ให้ a, b เป็นจำนวนเต็มใด ๆ โดยที่ $a \neq 0$

ก. $a|0$ และ $a|a$

ข. $1|b$

ค. ถ้า $a|b$ แล้ว $a|bc$ ทุกจำนวนเต็ม c

พิสูจน์ ก. เพราะว่า $0 = 0.a$

ดังนั้น $a|0$

และเพราะว่า $a = a\cdot 1$

ดังนั้น $a|a$

ข. เพราะว่า $b = 1 \cdot b$

เพราะฉะนั้น $1|b$

ค. เพราะว่า $a|b$ จะมีจำนวนเต็ม e ที่ทำให้

$$b = ae$$

ดังนั้น $bc = aec$

นั่นคือ $a|bc$

ทฤษฎีบท 1.9 ถ้า $a|b$ และ $b \neq 0$ แล้ว $|a| \leqslant |b|$

พิสูจน์ เพราะว่า $a|b$ และ $b \neq 0$ ดังนั้นจะมีจำนวนเต็ม e โดยที่ $e \neq 0$ และ

$$b = ae$$

ดังนั้นจะได้ว่า

$$|b| = |ae| = |a|\,|e|$$

เพราะว่า $e \neq 0$ จะได้ว่า $|e| \geqslant 1$

เพราะฉะนั้น

$$|b| = |a|\,|e| \geqslant |a|$$ #

บทแทรก 1.10 ถ้า a และ b เป็นจำนวนเต็มบวก โดยที่ $a|b$ และ $b|a$ แล้ว $a = b$

พิสูจน์ เพราะว่า $a|b$ และ $b|a$ ดังนั้น โดยทฤษฎีบท 1.9 จึงได้ว่า

$|a| \leqslant |b|$ และ $|b| \leqslant |a|$ ซึ่งทำให้ $|a| = |b|$

ผลที่ตามมาก็คือ $a = b$ เนื่องจากทั้ง a และ b เป็นจำนวนเต็มบวก #

ทฤษฎีบทต่อไปนี้จะเป็นทฤษฎีบทที่สำคัญสำหรับการหาร ซึ่งมีชื่อเรียกว่า **ขั้นตอนวิธีการหาร**

ทฤษฎีบท 1.11 ***ขั้นตอนวิธีการหาร*** (The Division Algorithm)

สำหรับจำนวนเต็ม a, b ใด ๆ โดยที่ $b > 0$ จะมีจำนวนเต็ม q และ r และมีอย่างละหนึ่งจำนวนเท่านั้น โดยที่ $0 \leqslant r < b$ และ $a = bq+r$

จำนวนเต็ม q เรียกว่า **ผลหาร** (quotient) r เรียกว่า **เศษ** (remainder)

พิสูจน์ ให้ $S = \{a-sb \mid s$ เป็นจำนวนเต็ม และ $a-sb \geqslant 0\}$

จะเห็นว่า ถ้า $a \geqslant 0$ แล้ว $a \in S$ เนื่องจาก $a = a-0(b)$

ถ้า $a < 0$ แล้ว จะได้ว่า $a-ab = a(1-b) \geqslant 0$

นั่นคือ $a-ab \in S$

ดังนั้น S เป็นเซตย่อยของเซตจำนวนเต็มบวกที่ไม่ใช่เซตว่าง

โดยคุณสมบัติการเป็นอันดับที่ดี S มีสมาชิกตัวที่น้อยที่สุด

ให้ r เป็นสมาชิกตัวที่น้อยที่สุดของ S และ q เป็นจำนวนเต็มที่ทำให้

$$r = a-qb$$

เนื่องจาก $r \in S$ จะได้ $r \geqslant 0$

และเพราะว่า

$$r-b = a-qb-b = a-(q+1)b$$

จะได้ว่า $a-(q+1)b < 0$

เนื่องจาก $r-b < r$ และ r เป็นสมาชิกตัวที่เล็กที่สุดของ S ผลที่ตามมาก็คือ

$$r-b < 0$$

นั่นคือ $0 \leqslant r < b$ และ $a = bq+r$

ต่อไปจะแสดงว่า r และ q มีได้อย่างละหนึ่งจำนวนเท่านั้น

สมมติ q' และ r' เป็นจำนวนเต็มที่ทำให้

$$a = bq'+r' \quad \text{โดยที่} \quad 0 \leqslant r' < q'$$

จะแสดงว่า $r = r'$ และ $q = q'$

สมมติ $q \neq q'$

กรณี 1 $q < q'$

จะได้ $q+1 \leqslant q'$

เพราะฉะนั้น

$$r' = a-bq' \leqslant a-b(q+1) = a-bq-b = r-b < 0$$

ซึ่งเป็นไปไม่ได้

กรณี 2 $q' < q$

จะได้ $q'+1 \leqslant q$

เพราะฉะนั้น

$$r = a-bq \leqslant a-b(q'+1) = a-bq'-b = r'-b < 0$$

ซึ่งเป็นไปไม่ได้

ดังนั้น $q = q'$

ผลที่ตามมาก็คือ

$$r \;=\; a-bq \;=\; a-bq' \;=\; r' \qquad \#$$

บทแทรก 1.12 ถ้า a และ b เป็นจำนวนเต็ม โดยที่ $b \neq 0$ แล้ว จะมีจำนวนเต็ม q และ r และมีอย่างละหนึ่งจำนวนเท่านั้น โดยที่

$$0 \leqslant r < |b| \qquad \text{และ} \qquad a = bq+r$$

พิสูจน์ เพราะว่า $b \neq 0$ **จะได้ว่า** $|b| > 0$

ดังนั้น โดยทฤษฎีบท 1.1 I **จะมีจำนวนเต็ม** q' **และ** r **และมีอย่างละหนึ่งจำนวนเท่านั้น** **โดยที่** $0 \leqslant r < |b|$ **และ** $a = |b|q'+r$

ถ้า $b > 0$ **จะได้** $a = bq'+r \qquad 0 \leqslant r < |b|$

ถ้า $b < 0$ **จะได้** $a = -bq'+r$

$$= b(-q')+r \qquad 0 \leqslant r < |b|$$

ให้ $q = -q'$ **จะได้** $a = bq+r,\ 0 \leqslant r < |b|$ #

ตัวอย่าง 1.15 กำหนด $a = 133$ และ $b = 21$ จงหา q, r โดยที่ $0 \leqslant r < b$ ที่ทำให้ $a = bq+r$

วิธีทำ $133 = 21 \cdot 6+7$ #

ตัวอย่าง 1.16 กำหนด $a = -50$ และ $b = 8$ จงหา q, r โดยที่ $0 \leqslant r < b$ ที่ทำให้ $a = bq+r$

วิธีทำ $-50 = 8(-7)+6$ #

ตัวอย่าง 1.17 กำหนด $a = 61$ และ $b = -7$ จงหา q, r โดยที่ $0 \leqslant r < |b|$ ที่ทำให้ $a = bq+r$

วิธีทำ $61 = (-7)(-8)+5$ #

หมายเหตุ กำหนด $b = 2$ และ a เป็นจำนวนเต็มใด ๆ จะพบว่า เศษที่เป็นไปได้คือ 0 และ 1 **ดังนั้น** $a = 2k$ **หรือ** $a = 2k+1$ **เมื่อ** k เป็นจำนวนเต็มเสมอ

นั่นคือ เราสามารถแบ่งแยกจำนวนเต็มได้เป็นสองพวก ดังนี้

ถ้าจำนวนเต็มใดอยู่ในรูปแบบ 2k เรียกจำนวนเต็มนั้นว่า **จำนวนเต็มคู่** (even integers) และถ้าจำนวนเต็มใด ๆ อยู่ในรูปแบบของ $2k+1$ เรียกจำนวนเต็มนั้นว่า **จำนวนเต็มคี่** (odd integers)

ตัวอย่าง 1.18 จงแสดงว่า กำลังสองของจำนวนเต็มใด ๆ เมื่อหารด้วย 4 จะมีเศษคือ 0 หรือ 1 เสมอ

พิสูจน์ ให้ a เป็นจำนวนเต็มใด ๆ

กรณี 1 a เป็นจำนวนเต็มคู่

นั่นคือ $a = 2k$ สำหรับจำนวนเต็ม k บางตัว

ดังนั้น $a^2 = 4k^2$

นั่นคือ เศษที่เกิดจากการหาร a^2 ด้วย 4 คือ 0

กรณี 2 a เป็นจำนวนเต็มคี่

นั่นคือ $a = 2k+1$ สำหรับจำนวนเต็ม k บางตัว

ดังนั้น
$$\begin{aligned} a^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ a^2 &= 4(k^2+k)+1 \end{aligned}$$

นั่นคือ เศษที่เกิดจากการหาร a^2 ด้วย 4 คือ 1 #

ฟังก์ชันจำนวนเต็มใหญ่ที่สุดใน x (The Greatest Integer Function in x)

บทนิยาม 1.4 ให้ x เป็นจำนวนจริง **จำนวนเต็มใหญ่ที่สุดใน** x (The greatest integer in x) เขียนแทนด้วย $[x]$ คือ จำนวนเต็มที่ใหญ่ที่สุดที่น้อยกว่าหรือเท่ากับ x

ตัวอย่าง 1.19
$$\begin{aligned} [2.3] &= 2 \\ [1.0003] &= 1 \\ [-1.23] &= -2 \end{aligned}$$
#

หมายเหตุ จากบทนิยาม 1.4 จะได้ว่า ถ้า x เป็นจำนวนจริงใด ๆ แล้ว

$$[x] \leq x < [x]+1$$

ทฤษฎีบท 1.13 ให้ x, y และ θ เป็นจำนวนจริง แล้ว

ก. $x-1 \leqslant \lfloor x \rfloor \leqslant x$

ข. ถ้า a เป็นจำนวนเต็ม โดยที่ $a \leqslant x$ แล้ว $a \leqslant \lfloor x \rfloor$

ค. ถ้า a เป็นจำนวนเต็ม โดยที่ $a > x$ แล้ว $a \geqslant \lfloor x \rfloor + 1 > \lfloor x \rfloor$

ง. ถ้า $x \leqslant y$ แล้ว $\lfloor x \rfloor \leqslant \lfloor y \rfloor$

จ. ถ้า $\theta = x - \lfloor x \rfloor$ แล้ว $0 \leqslant \theta < 1$

ฉ. ถ้า $x = n + \theta$ โดยที่ n เป็นจำนวนเต็ม และ $0 \leqslant \theta < 1$ แล้ว $\lfloor x \rfloor = n$

ช. สำหรับจำนวนเต็ม n ใด ๆ $\lfloor x+n \rfloor = \lfloor x \rfloor + n$

ฌ. ถ้า a, b, q และ r เป็นจำนวนเต็ม โดยที่

$$a = bq + r \qquad 0 \leqslant r < b$$

แล้ว $$q = \left\lfloor \frac{a}{b} \right\rfloor$$

พิสูจน์ ก. จากหมายเหตุข้างต้นได้

$$\lfloor x \rfloor \leqslant x \leqslant \lfloor x \rfloor + 1$$

นั่นคือ $$x - 1 \leqslant \lfloor x \rfloor \leqslant x$$

ข. กำหนด a เป็นจำนวนเต็ม และ $a \leqslant x$

กรณี 1 $a + 1 > x$

จะได้ $$a \leqslant x < a +$$

นั่นคือ $$\lfloor x \rfloor = a$$

กรณี 2 $a + 1 \not> x$

นั่นคือ $$a + \ \leq x$$

จะได้ $$a \leqslant x - 1 < \lfloor x \rfloor$$

ทั้งสองกรณีได้ว่า $a \leqslant \lfloor x \rfloor$

ค. กำหนด a เป็นจำนวนเต็ม และ $a > x$

เพราะว่า $$\lfloor x \rfloor \leqslant x$$

จะได้ $$\lfloor x \rfloor \leqslant x < a$$

เพราะฉะนั้น $$a \geqslant \lfloor x \rfloor + 1 > \lfloor x \rfloor$$

ง. กำหนด $x \leqslant y$

เพราะว่า $$\lfloor x \rfloor \leqslant x$$

เพราะฉะนั้น $[x] \leqslant x \leqslant Y$

ดังนั้น โดย ข. $[x] \leqslant [y]$

จ. กำหนด $\theta = x-[x]$

จาก ก. ได้ว่า $x-1 < [x] \leqslant x$

จะได้ $0 \leqslant x--(x]$

และเพราะว่า $x < [x]+1$

จะได้ $x-[x] < I$

นั่นคือ $0 \leqslant \theta < 1$

ฉ. ให้ $x = n + \theta$ โดยที่ n เป็นจำนวนเต็ม และ $0 \leqslant \theta < 1$

เพราะว่า $0 \leqslant \theta < 1$ และ $x = n+\theta$

จะได้ $n \leqslant x < n+l$

ดังนั้น โดยบทนิยาม 1.4 $[x] = n$

ช. ให้ $x = [x]+\theta$ $0 \leqslant \theta < 1$

เพราะว่า

$$x+n = [x]+\theta+n$$
$$= [x]+n+\theta$$

และเพราะว่า $0 \leqslant \theta < 1$ ดังนั้น โดย ฉ. ได้ว่า $[x+n] = [x]+n$

ฌ. ให้ $a = bq+r$ โดยที่ $0 \leqslant r < b$

จะได้ $\frac{a}{b} = q+\frac{r}{b}$

เพราะว่า $0 \leqslant r < b$ จะได้ $0 \leqslant \frac{r}{b} < 1$

ดังนั้น โดย ฉ. $\left[\frac{a}{b}\right] = q$ #

ทฤษฎีบท 1.14 สำหรับทุกจำนวนจริง x และจำนวนเต็มบวก n

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$$

พิสูจน์ โดยบทนิยาม 1.4

$$\left[\frac{x}{n}\right] \leqslant \frac{x}{n} < \left[\frac{x}{n}\right]+1$$

เพราะฉะนั้น

$$n\left[\frac{x}{n}\right] \leqslant x < n\left[\frac{x}{n}\right]+n$$

โดยทฤษฎีบท 1.13 ข. และ ค. จะได้ว่า

$$n\left[\frac{x}{n}\right] \leqslant [x] < n\left[\frac{x}{n}\right]+n$$

ผลที่ตามมาก็คือ

$$\left[\frac{x}{n}\right] \leqslant \frac{[x]}{n} < \left[\frac{x}{n}\right]+1$$

ดังนั้น โดยบทนิยาม 1.4

$$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$$ #

แบบฝึกหัด 1.3

1. จงแสดงว่า $3|99$, $5|145$, $7|343$ และ $889|0$
2. ถ้า $a|b$ จงแสดงว่า $(-a)|b$, $a|(-b)$ และ $(-a)|(-b)$
3. ถ้า $a|b$ และ $a|c$ จงแสดงว่า $a^2|bc$
4. ให้ c เป็นจำนวนเต็ม โดยที่ $c \neq 0$ จงพิสูจน์ว่า $a|b$ ก็ต่อเมื่อ $ac|bc$
5. จงพิจารณาว่า ข้อความต่อไปนี้จริงหรือเท็จ ถ้าจริงให้พิสูจน์ ถ้าเท็จให้ยกตัวอย่างมาให้ดู
   ถ้า $a|(b+c)$ แล้ว $a|b$ หรือ $a|c$ อย่างใดอย่างหนึ่ง
6. กำหนด a เป็นจำนวนเต็มใด ๆ จงแสดงว่า a, $a+2$, $a+4$ จำนวนใดจำนวนหนึ่งต้องหารด้วย 3 ลงตัว
   (*แนะนำ* : โดยขั้นตอนวิธีการหาร a ต้องอยู่ในรูปแบบของ $3k$, $3k+1$ หรือ $3k+2$)
7. จงแสดงว่า $4 \nmid (a^2+2)$ สำหรับทุกจำนวนเต็ม a
8. จงแสดงว่า ถ้า a เป็นจำนวนเต็ม โดยที่ $2 \nmid a$ และ $3 \nmid a$ แล้ว $24|(a^2-1)$
9. จงแสดงว่า กำลังสองของจำนวนเต็มคี่อยู่ในรูปแบบของ $8k+1$
10. จงแสดงว่า ถ้า a และ b เป็นจำนวนเต็มคี่แล้ว $8|(a^2-b^2)$
11. จงหาผลหารและเศษ เมื่อ
    - 11.1 $a = 100$ $b = 17$
    - 11.2 $a = 289$ $b = 17$
    - 11.3 $a = -44$ $b = 17$
    - 11.4 $a = -100$ $b = 17$
12. จงหาค่า
    - 12.1 $[2.7]$
    - 12.2 $[-3.5]$
    - 12.3 $[-\sqrt{2}]$
    - 12.4 $\left[\frac{75}{4}\right]$
    - 12.5 $[2.7+0.5]$
    - 12.6 $[-3.5+0.5]$
    - 12.7 $\left[\frac{75}{4}+\frac{1}{2}\right]$
13. จงแสดงว่า ถ้า x และ y เป็นจำนวนจริงแล้ว $[x+y] \geq [x]+[y]$
14. จงแสดงว่า ถ้า x และ y เป็นจำนวนจริงบวกแล้ว $[xy] \geq [x]\,[y]$

15. จงหาค่าของ $\lfloor x \rfloor + \lfloor -x \rfloor$ เมื่อ x เป็นจำนวนจริงใด ๆ

16. จงแสดงว่า จำนวนเต็ม n เป็นจำนวนเต็มคู่ก็ต่อเมื่อ $n - 2\left\lfloor \frac{n}{2} \right\rfloor = 0$

17. จงแสดงว่า ถ้า x เป็นจำนวนจริงแล้ว $\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$

1.4 รูปแบบของจำนวนเต็ม

เป็นการสะดวกที่จะเขียนจำนวนเต็มในรูปแบบของสัญกรณ์ทศนิยม (decimal notation) ซึ่งรูปแบบนี้เป็นการใช้เลขโดด (digits) แสดงพหุคูณ (multiples) ของกำลังของ 10 เช่น เมื่อเขียน 34769 หมายถึง

$$3\cdot 10^4 + 4\cdot 10^3 + 7\cdot 10^2 + 6\cdot 10^1 + 5\cdot 10^0$$

การใช้สัญกรณ์ทศนิยมแบบนี้เราหมายความว่า ใช้ 10 เป็นฐาน (base) และโดยทั่วไปการเขียนจำนวนเต็มนิยมใช้ฐาน 10 ทั้งสิ้น แต่เราสามารถพิสูจน์ได้ว่า จำนวนเต็มบวกทุกตัวที่มากกว่า 1 สามารถใช้เป็นฐานได้

ทฤษฎีบท 1.15 ให้ b เป็นจำนวนเต็มบวก โดยที่ $b > 1$ แล้วทุกจำนวนเต็มบวก n สามารถเขียนได้เป็น

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

โดยที่ a เป็นจำนวนเต็ม และ $0 \leqslant a_j \leqslant b-1$ ทุก $j = 1, 2, \ldots, k$ และ $a_k \neq 0$ นอกจากนั้น การเขียน

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

เขียนได้เพียงรูปแบบเดียวเท่านั้น

พิสูจน์ โดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q_0 และ a_0 ที่ทำให้

$$n = bq_0 + a_0 \qquad 0 \leqslant a_0 \leqslant b-1$$

ต่อไปหาร q_0 ด้วย b จะได้ว่ามีจำนวนเต็ม q_1 และ a_1 ที่ทำให้

$$q_0 = bq_1 + a_1 \qquad 0 \leqslant a_1 \leqslant b-1$$

ทำกระบวนการนี้ต่อไป จะได้

$$q_1 = bq_2 + a_2 \qquad 0 \leqslant a_2 \leqslant b-1$$

$$q_2 = bq_3 + a_3 \qquad 0 \leqslant a_3 \leqslant b-1$$

$$q_{k-2} = bq_{k-1} + a_{k-1} \qquad 0 \leqslant a_{k-1} \leqslant b-1$$

$$q_{k-1} = b\cdot 0 + a_k \qquad 0 \leqslant a_k \leqslant b-1$$

กระบวนการดังกล่าวข้างต้นต้องสิ้นสุด และมี k ที่ทำให้ $q_k = 0$ เนื่องจาก

$$n > q_0 > q_1 > q_2 > \ldots \geqslant 0$$

นอกจากนั้นจะได้ว่า a_k เป็นเศษตัวสุดท้าย และ $a_k \neq 0$

จากกระบวนการข้างต้นได้ว่า

$$\begin{aligned} n &= bq_0 + a_0 \\ &= b(bq_1 + a_1) + a_0 \\ &= b^2q_1 + ba_1 + a_0 \\ &= b^2(bq_2 + a_2) + ba_1 + a_0 \\ &= b^3q_2 + b^2a_2 + ba_1 + a_0 \end{aligned}$$

โดยการแทนค่า $q_1, q_2, \ldots, q_{k-1}$ ตามลำดับ จะได้

$$\begin{aligned} n &= b^3q_2 + b^2a_2 + ba_1 + a_0 \\ &= b^3(bq_3 + a_3) + b^2a_2 + ba_1 + a_0 \\ &= b^4q_3 + b^3a_3 + b^2a_2 + ba_1 + a_0 \\ &= \cdot \\ &= \cdot \quad \cdot \quad \cdot \\ &= \cdot \qquad \cdot \\ &= b^{k-1}q_{k-2} + a_{k-2}b^{k-2} + \ldots + a_1b + a_0 \\ &= b^{k-1}(bq_{k-1} + a_{k-1}) + a_{k-2}b^{k-2} + \ldots + a_1b + a_0 \\ &= b^kq_{k-1} + b^{k-1}a_{k-1} + a_{k-2}b^{k-2} + \ldots + a_1b + a_0 \\ n &= a_kb^k + a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1b + a_0 \end{aligned}$$

โดยที่ $0 \leqslant a_j \leqslant b-1$ ทุกค่า $j = 1, 2, \ldots, k$ และ $a_k \neq 0$

ต่อไปจะแสดงว่า การกระจายแบบนี้กระจายได้แบบเดียวเท่านั้น

สมมติ $n = a_kb^k + a_{k-1}b^{k-1} + \ldots + a_1b + a_0$

$= c_mb^m + c_{m-1}b^{m-1} + \ldots + c_1b + c_0$

โดยที่ $a_k \neq 0,\ c_m \neq 0 \quad 0 \leqslant a_j \leqslant b-1,\ 0 \leqslant c_j \leqslant b-1$ สำหรับทุก j

และสมมติว่า $m \geqslant k$

ดังนั้น $0 = c_mb^m + \ldots + c_{k+1}b^{k+1} + (c_k - a_k)b^k + \ldots + (c_1 - a_1)b + (c_0 - a_0)$

$0 = d_mb^m + \ldots + d_{k+1}b^{k+1} + \ldots + d_kb^k + \ldots + d_1b + d_0$

โดยที่ $d_j = \begin{cases} c_j & \text{ถ้า } j = k+1, \ldots, m \\ c_j - a_j & \text{ถ้า } j = 1, 2, \ldots, k \end{cases}$

นอกจากนั้น $-(b-1) \leqslant d_j \leqslant b-1$ ทุกค่า $j = 1, 2, \ldots, m$

ให้ ℓ เป็นจำนวนเต็มที่เล็กที่สุด ที่ $d_\ell \neq 0$ นั่นคือ $d_0, d_1, \ldots, d_{\ell-1}$ เป็นศูนย์หมด

เพราะฉะนั้น

$$\begin{aligned} d_m b^m + \ldots + d_\ell b^\ell &= 0 \\ b^\ell(d_m b^{m-\ell} + \ldots + d_{\ell+1} b + d_\ell) &= 0 \end{aligned}$$

เพราะว่า $b^\ell \neq 0$ จะได้ว่า

$$d_m b^{m-\ell} + \ldots + d_{\ell+1} b + d_\ell = 0$$

นั่นคือ

$$\begin{aligned} d_\ell &= -d_m b^{m-\ell} - \ldots - d_{\ell+1} b \\ &= b(-d_m b^{m-\ell-1} - \ldots - d_{\ell+1}) \end{aligned}$$

นั่นคือ $b|d_\ell$ ผลที่ตามมาก็คือ $|b| \leqslant |d_\ell|$ ซึ่งเป็นไปไม่ได้ เนื่องจาก

เพราะว่า $-(b-1) \leqslant d_j \leqslant b-1$ ทุกค่า j

จึงทำให้ $|d_j| \leqslant |b-1| < |b|$

ผลที่ตามมาก็คือ $d_j = 0$ ทุก $j = 1, 2, \ldots, m$ #

จากทฤษฎีบท 1.15 จะพบว่า จำนวนเต็มบวกทุกตัวสามารถเขียนเป็นผลบวกของกำลังของจำนวนเต็มบวก b โดยที่ $b > 1$ ได้เสมอ และ b นี้เราเรียกว่า **ฐาน** (base) ถ้าเราใช้ฐาน 10 จะเรียกการเขียนโดยใช้ฐาน 10 ว่า **สัญกรณ์ทศนิยม** (decimal notation) เรียกฐาน 2 ว่า **การกระจายทวิภาค** (binary expansions) ฐาน 8 เรียกว่า **การกระจายฐาน** 8 (octal expansions) และฐาน 16 เรียกว่า **การกระจายฐาน 16** (hexadecimal or hex)

และถ้า $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$ โดยที่ $a_k \neq 0$ และ $0 \leqslant a_j \leqslant b-1$ ทุก $j = 1, 2, \ldots, k$ แล้ว

แต่ละ a_j เรียก **เลขโดด** ของการกระจาย และโดยทั่วไปเขียนแทนด้วย

$$n = (a_k a_{k-1} \ldots a_1 a_0)_b$$

และเพื่อความสะดวก ถ้า $b = 10$ จะเขียนแทนด้วย $n = a_k a_{k-1} \ldots a_1 a_0$

ตัวอย่าง 1.20

$$\begin{aligned} (236)_7 &= 2 \cdot 7^2 + 3 \cdot 7 + 6 \cdot 7^0 \\ &= 125 \\ (10010011)_2 &= 1 \cdot 2^7 + 1 \cdot 2^4 + 1 \cdot 2 + 1 \cdot 2^0 \\ &= 147 \end{aligned}$$

#

จากการพิสูจน์ทฤษฎีบท 1.15 จะพบวิธีกระจายจำนวนเต็มเป็นเลขฐานอื่น ๆ ได้ โดยใช้ขั้นตอนวิธีการหาร ดังแสดงให้เห็นในตัวอย่างต่อไปนี้

ตัวอย่าง 1.21 จงกระจาย 1864 ให้เป็นฐาน 2 และฐาน 5

วิธีทำ

$$
\begin{aligned}
1864 &= 932\cdot 2+0\\
932 &= 466\cdot 2+0\\
466 &= 233\cdot 2+0\\
233 &= 116\cdot 2+1\\
116 &= 58\cdot 2+0\\
58 &= 49\cdot 2+0\\
49 &= 24\cdot 2+1\\
24 &= 12\cdot 2+0\\
12 &= 6\cdot 2+0\\
6 &= 3\cdot 2+0\\
3 &= 1\cdot 2+1\\
1 &= 0\cdot 2+1
\end{aligned}
$$

เพราะฉะนั้น

$$
\begin{aligned}
1864 &= 2\cdot 932+0\\
&= 2(2\cdot 466+0)+0\\
&= 2^2\cdot 466+0\\
&= 2^2(2\cdot 233+0)+0\\
&= 2^3\cdot 233+0\\
&= 2^3\cdot(2\cdot 116+1)+0\\
&= 2^4\cdot 116+2^3\\
&= 2^4\cdot(2\cdot 58+0)+2^3\\
&= 2^5\cdot 58+0+2^3\\
&= 2^5\cdot(2\cdot 29+0)+2^3\\
&= 2^6\cdot 29+0+2^3\\
&= 2^6\cdot(2\cdot 14+1)+2^3\\
&= 2^7\cdot 14+2^6+2^3
\end{aligned}
$$

$$
\begin{aligned}
&= 2^7(2\cdot 7+0)+2^6+2^3\\
&= 2^8\cdot 7+0+2^6+2^3\\
&= 2^8(2\cdot 3+1)+2^6+2^3\\
&= 2^9\cdot 3+2^8+2^6+2^3\\
&= 2^9(2\cdot 1+\ 1)+2^8+2^6+2^3\\
&= 2^{10}\cdot 1+2^9+2^8+2^6+2^3\\
&= 1\cdot 2^{10}+1\cdot 2^9+1\cdot 2^8+0\cdot 2^7+1\cdot 2^6+0\cdot 2^5+0\cdot 2^4+1\cdot 2^3+0\cdot 2^2+0\cdot 2+0\cdot 2^0
\end{aligned}
$$

นั่นคือ

$$1864 = (11101001000)_2$$

และ

$$
\begin{aligned}
1864 &= 5\cdot 372+4\\
372 &= 5\cdot 74 \quad +2\\
74 &= 5\cdot 14 \quad +4\\
14 &= 5\cdot 2 \quad +4\\
2 &= 5\cdot 0 \quad +2
\end{aligned}
$$

เพราะฉะนั้น

$$
\begin{aligned}
1864 &= 5\cdot 372+4\\
&= 5(5\cdot 74+2)+4\\
&= 5^2\cdot 74+5\cdot 2+4\\
&= 5^2(5\cdot 14+4)+5\cdot 2+4\\
&= 5^3\cdot 14+5^2\cdot 4+5\cdot 2+4\\
&= 5^3(5\cdot 2+4)+5^2\cdot 4+5\cdot 2+4\\
&= 5^4\cdot 2+5^3\cdot 4+5^2\cdot 4+5\cdot 2+4\\
&= 2\cdot 5^4+4\cdot 5^3+4\cdot 5^2+2\cdot 5+4\cdot 5^0
\end{aligned}
$$

นั่นคือ

$$1864 = (24424)_5$$ #

ในการกระจายฐาน 16 **เลขโดดของการกระจายคือ** 0, 1, 2, 3, ... 10, 11, 12, 13, 14 **และ** 15

เพื่อความสะดวกจึงใช้ A **แทน** 10

B **แทน** 11

c แทน 12

D แทน 13

E แทน 14

และ F แทน 15

ดังนั้น

$$(A35B0F)_{16} = 10\cdot16^5+3\cdot16^4+5\cdot10^3+11\cdot10^2+0\cdot10+15\cdot10^0$$

ตัวอย่าง 1.22 **จงเปลี่ยน** $(2FB3)_{16}$ **ให้เป็นฐาน** 2

วิธีทำ

$$\begin{aligned}(2FB3)_{16} &= 2\cdot16^3+15\cdot16^2+11\cdot16+3\cdot16^0\\ &= (12211)_{10}\\ &= (10111110110011)_2\end{aligned}$$

ตัวอย่าง 1.23 จงเปลี่ยน $(10111110110011)_2$ **ให้เป็นฐาน** 16

94
วิธีทำ เพราะว่า

$$\begin{aligned}(10111110110011)_2 = {} & 1\cdot2^{13}+0\cdot2^{12}+1\cdot2^{11}+1\cdot2^{10}+1\cdot2^9+1\cdot2^8+1\cdot2^7+0\cdot2^6+1\cdot2^5\\ & +1\cdot2^4+0\cdot2^3+0\cdot2^2+1\cdot2+1\cdot2^0\end{aligned}$$

และ $2^4 = 16$ **จึงพยายามจัดเทอมให้อยู่ในรูปผลบวกของกำลังของ** 2^4 **ได้ดังนี้**

$$\begin{aligned}(10111110110011)_2 &= (1\cdot2^{13}+0\cdot2^{12})+(1\cdot2^{11}+1\cdot2^{10}+1\cdot2^9+1\cdot2^8)\\ &\quad +(1\cdot2^7+0\cdot2^6+1\cdot2^5+1\cdot2^4)+(0\cdot2^3+0\cdot2^2+1\cdot2+1\cdot2^0)\\ &= 2\cdot2^{12}+(1\cdot2^3+1\cdot2^2+1\cdot2+1)2^8+(1\cdot2^3+0\cdot2^2+1\cdot2+1)2^4\\ &\quad +(0\cdot2^3+0\cdot2^2+1\cdot2+1\cdot2^0)\\ &= 2\cdot2^{12}+15\cdot2^8+11\cdot2^4+3\\ &= 2\cdot16^3+15\cdot16^2+11\cdot16+3\\ &= (2FB3)_{16}\end{aligned}$$

และจาก $(2FB3)_{16}$ **จะเปลี่ยนเป็นฐาน** 2 **เราสามารถทำง่าย ๆ ดังนี้**

แทนค่าเลขโดดในฐาน 16 **ด้วยชุด** 4 **ตัวของเลขโดดในฐาน** 2 **ดังนี้**

เพราะว่า

$$\begin{aligned}2 &= (0010)_2\\ F &= 15 = (1111)_2\\ B &= 11 = (1011)_2\\ 3 &= (0011)_2\end{aligned}$$

จะได้

$$(2FB3)_{16} = (10111110011)_2$$

ตัวอย่าง 1.24 **จงเปลี่ยน** $(10101011)_2$ **เป็นฐาน** 8 **และจงเปลี่ยน** $(253)_8$ **เป็นฐาน** 2

วิธีทำ เพราะว่า $8 = 2^3$ **จึงจัดเทอม** $(1010101\ 1)_2$ **เป็นผลบวกของกำลังของ** 2^3 **ดังนี้**

$$\begin{aligned}
(1010101\ 1)_2 &= 1\cdot 2^7 + 0\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1.2 + 1.2^0 \\
&\quad (1\cdot 2^7 + 0\cdot 2^6) + (1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3) + (0\cdot 2^2 + 1\cdot 2 + 1\cdot 2^0) \\
&= 2\cdot 2^6 + (1\cdot 2^2 + 0\cdot 2 + 1)2^3 + (0\cdot 2^2 + 1\cdot 2 + 1\cdot 2^0) \\
&= 2\cdot 8^2 + 5\cdot 8 + 3 \\
&= (253)_8
\end{aligned}$$

และจาก $(253)_8$ **จะเปลี่ยนเป็นฐาน** 2 **ทำได้โดยแทนค่าเลขโดดในฐาน** 8 **ด้วยชุด** 3 **ตัว ของเลขโดดในฐาน** 2 **ดังนี้**

เพราะว่า

$$\begin{aligned}
2 &= (10)_2 \\
5 &= (101)_2 \\
3 &= (011)_2
\end{aligned}$$

ดังนั้น

$$(253)_8 = (1010101\ 1)_2$$

แบบฝึกหัด 1.4

1. จงกระจาย $(247)_{10}$ ให้เป็น

   1.1 ฐาน 7   1.2 ฐาน 2

   1.3 ฐาน 8   1.4 ฐาน 16

2. จงกระจาย $(6105)_7$ ให้เป็นสัญกรณ์ทศนิยม

3. จงเปลี่ยนจำนวนต่อไปนี้ให้เป็นฐาน 10

   3.1 $(324)_8$ 3.2 $(324)_{16}$

   3.3 $(10)_7$ 3.4 (IO),

   3.5 $(100)_8$ 3.6 $(D9B)_{16}$

4. จงเปลี่ยน $(101001000)_2$ ให้เป็นฐาน 10

5. จงเปลี่ยน $(1984)_{10}$ ให้เป็นฐาน 2

6. จงเปลี่ยนจำนวนต่อไปนี้ให้เป็นฐาน 8 และฐาน 16

   6.1 $(111100101)_2$ 6.2 $(1100101)_2$

7. จงเปลี่ยนจำนวนต่อไปนี้ให้เป็นฐาน 2

   7.1 $(257)_8$ 7.2 $(301)_8$

   7.3 $(AF3)_{16}$ 7.4 $(10C)_{16}$

8. จงเปลี่ยน $(10001\ 11\ 10101)_2$ และ (11101001110)~ ให้เป็นฐาน 16

9. จงเปลี่ยน $(ABCDEF)_{16}$, $(DEFACDE)_{16}$ และ $(9A0B)_{16}$ ให้เป็นฐาน 2

1.5 **จำนวนเฉพาะ** (Prime Numbers)

บทนิยาม 1.5 ถ้า p เป็นจำนวนเต็มบวกที่มากกว่า 1 และ p มีตัวหารที่เป็นบวก (positive divisor) คือ 1 และ p เท่านั้น เรากล่าวว่า p เป็น **จำนวนเฉพาะ** (prime numbers)

และถ้า $p > 1$ ไม่ใช่จำนวนเฉพาะ เรากล่าวว่า p คือ **จำนวนประกอบ** (composite number)

ตัวอย่าง 1.25 2, 3, 5, 7 เป็นจำนวนเฉพาะ

4, 6, 10, 14 เป็นจำนวนประกอบ #

ทฤษฎีบทต่อไปจะแสดงให้เห็นว่า จำนวนประกอบสามารถเขียนให้อยู่ในรูปของผลคูณของจำนวนเฉพาะได้เสมอ

ทฤษฎีบท 1.16 ให้ n เป็นจำนวนเต็มบวก โดยที่ $n \geqslant 2$ แล้ว n ต้องเป็นจำนวนเฉพาะหรือผลคูณของจำนวนเฉพาะ

พิสูจน์ ทฤษฎีบทเป็นจริง เมื่อ $n = 2$ เนื่องจาก 2 เป็นจำนวนเฉพาะ

ให้ k เป็นจำนวนเต็มใด ๆ โดยที่ $k \geqslant 2$

และสมมติว่า ทฤษฎีบทเป็นจริงสำหรับจำนวนเต็มบวก n ซึ่ง $2 \leqslant n \leqslant k$

จะแสดงว่าทฤษฎีบทเป็นจริงสำหรับ $n = k+1$

ถ้า $k+1$ เป็นจำนวนเฉพาะแล้ว ทฤษฎีบทเป็นจริง ถ้า $k+1$ ไม่ใช่จำนวนเฉพาะ จะได้ว่า $k+1$ เป็นจำนวนประกอบ นั่นคือ มีจำนวนเต็ม r, s โดยที่ $2 \leqslant r \leqslant k$, $2 \leqslant s \leqslant k$ และ $k+1 = rs$

เพราะว่า $2 \leqslant r \leqslant k$ และ $2 \leqslant s \leqslant k$ โดยสมมติฐานจะได้ว่า r และ s ต่างก็เป็นผลคูณของจำนวนเฉพาะ

นั่นคือ ทฤษฎีบทเป็นจริงสำหรับ $n = k+1$

เพราะฉะนั้น โดยทฤษฎีบทอุปนัยทางคณิตศาสตร์ ทฤษฎีบทเป็นจริงสำหรับทุกจำนวนเต็ม $n \geqslant 2$ #

หมายเหตุ จากทฤษฎีบท 1.16 จำนวนเฉพาะซึ่งเป็นตัวประกอบ (factor) ของ n อาจจะซ้ำกันได้ ดังนั้นจึงอาจกล่าวได้ว่า สามารถเขียน

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

โดยที่ $p_1, p_2, \ldots, p_r$ เป็นจำนวนเฉพาะ และ $\alpha_1, \alpha_2, \ldots, \alpha_r$ เป็นจำนวนเต็มบวก

ตัวอย่าง 1.26 จงเขียน 576 เป็นผลคูณของจำนวนเฉพาะ

วิธีทำ

$$576 = 2\times2\times2\times2\times2\times2\times3\times3$$
$$= 2^6\times3^2 \qquad \#$$

ตัวอย่าง 1.27 จงเขียน 701 เป็นผลคูณของจำนวนเฉพาะ

วิธีทำ

$$701 = 1\times701 \qquad \#$$

ปัญหาที่น่าสนใจของเราในขณะนี้ก็คือ กำหนดจำนวนเต็มบวก n แล้วจะทราบได้อย่างไรว่า n เป็นจำนวนเฉพาะหรือเป็นจำนวนประกอบ ทฤษฎีบทต่อไปนี้จะช่วยให้ตัดสินใจได้ว่า n เป็นจำนวนเฉพาะหรือจำนวนประกอบ

ทฤษฎีบท 1.17 ถ้า n เป็นจำนวนประกอบแล้ว n จะต้องมีตัวประกอบที่เป็นจำนวนเฉพาะที่มีค่าไม่เกิน $\sqrt{n}$

พิสูจน์ เพราะว่า n เป็นจำนวนประกอบ

ดังนั้น จะต้องมีจำนวนเต็ม a, b โดยที่ $1 < a \leqslant b < n$

และ $n = ab$

จะต้องได้ว่า $a \leqslant \sqrt{n}$ เนื่องจากว่า ถ้า $a \nleqslant \sqrt{n}$ จะทำให้

$$b \geqslant a > \sqrt{n}$$

ผลที่ตามมาก็คือ

$$ab > \sqrt{n}\cdot\sqrt{n} = n$$

ซึ่งเป็นไปไม่ได้

ดังนั้น โดยทฤษฎีบท 1.16 a จะต้องมีตัวประกอบที่เป็นจำนวนเฉพาะ และจำนวนเฉพาะนี้มีค่าไม่เกิน $\sqrt{n}$ #

ดังนั้น ปัญหาต่อไปสำหรับการพิจารณาว่า n เป็นจำนวนเฉพาะหรือจำนวนประกอบก็คือ สามารถทราบจำนวนเฉพาะทุกตัวที่ไม่เกิน $\sqrt{n}$ หรือไม่

วิธีจะหาจำนวนเฉพาะที่มีค่าไม่เกินจำนวนเต็มบวก k มีวิธีที่เรียกว่า "Sieve of Erathosthenes" ซึ่งทำได้ดังนี้

ถ้าสมมติ $k = 200$

จากทฤษฎีบท 1.17 ทำให้ได้ว่า จำนวนประกอบที่น้อยกว่า 200 จะต้องมีตัวประกอบที่เป็นจำนวนเฉพาะที่มีค่าไม่เกิน $\sqrt{200} = 14.142$

ดังนั้น การหาจำนวนเฉพาะที่ไม่เกิน 200 ทำได้ดังนี้

เขียนตัวเลข 2 ถึง 200 ลงในตาราง

ตาราง 1.1

	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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

เนื่องจากจำนวนเฉพาะที่ไม่เกิน 14.14 คือ

2, 3, 5, 7, 11, 13

ดังนั้น ขั้นที่ 1 ตัด 2 และทุกตัวที่เป็นพหุคูณของ 2 ออก

ขั้นที่ 2 ตัด 3 และทุกตัวที่เป็นพหุคูณของ 3 ออก

ขั้นที่ 3 ตัด 5 และทุกตัวที่เป็นพหุคูณของ 5 ออก

ขั้นที่ 4 ตัด 7 และทุกตัวที่เป็นพหุคูณของ 7 ออก

ขั้นที่ 5 ตัด 11 และทุกตัวที่เป็นพหุคูณของ 11 ออก

ขั้นที่ 6 ตัด 13 และทุกตัวที่เป็นพหุคูณของ 13 ออก

ดังนั้น จำนวนที่เหลือจากการตัดทิ้งทั้ง 6 ขั้นตอนทั้งหมด ซึ่งก็คือจำนวนที่ล้อมรอบด้วยวงกลม คือจำนวนเฉพาะที่มีค่าไม่เกิน 200

และเมื่อทราบจำนวนเฉพาะที่มีค่าไม่เกินจำนวนเต็ม k ที่กำหนดให้แล้ว ทำให้สามารถจำแนกจำนวนเฉพาะและจำนวนประกอบได้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.28 จงพิจารณาว่า 503 เป็นจำนวนเฉพาะหรือจำนวนประกอบ

วิธีทำ เพราะว่า $\sqrt{503} = 22.42$

และจากตาราง 1.1 จำนวนเฉพาะที่ไม่เกิน 22.42 คือ

$$2, 3, 5, 7, 11, 13, 17, 19$$

และเพราะว่า

$$2 \nmid 503$$
$$3 \nmid 503$$
$$5 \nmid 503$$
$$7 \nmid 503$$
$$11 \nmid 503$$
$$13 \nmid 503$$
$$17 \nmid 503$$
$$19 \nmid 503$$

จึงสรุปได้ว่า 503 เป็นจำนวนเฉพาะ #

ตัวอย่าง 1.29 ให้ $n = 42833$ จงเขียน n ให้เป็นผลคูณของจำนวนเฉพาะ

วิธีทำ
$$42833 = 7 \text{x} 6119$$

และเพราะว่า $\sqrt{6119} = 78.224$

จำนวนเฉพาะที่ไม่เกิน 78.224 คือ

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73

และจะพบว่า 2916119

ดังนั้น

$$42833 = 7 \text{x} 6119$$
$$= 7 \times 29 \times 211$$

เพราะว่า $\sqrt{211} = 14.52$

และจำนวนเฉพาะที่ไม่เกิน 14.52 **คือ** 2, 3, 5, 7, 11, 13

และ $2 \nmid 211$

$3 \nmid 211$

$5 \nmid 211$

$7 \nmid 211$

$11 \nmid 211$

$13 \nmid 211$

จึงได้ว่า 211 **เป็นจำนวนเฉพาะ**

และจะได้

$$42833 = 7 \times 29 \times 211$$ #

นอกจากนั้น ยังสามารถพิสูจน์ได้ว่า มีจำนวนเฉพาะมากมายเป็นจำนวนอนันต์ ดังนี้

ทฤษฎีบท 1.18 มีจำนวนเฉพาะมากมายเป็นจำนวนอนันต์

พิสูจน์ สมมติมีจำนวนเฉพาะเป็นจำนวนจำกัด

ให้ $p_1, p_2, \ldots, p_r$ เป็นจำนวนเฉพาะทั้งหมด

และ $n = p_1p_2\ldots p_r + 1$

เนื่องจาก $n > p_i$ ทุก $i = 1, 2, \ldots, r$ จึงได้ว่า n เป็นจำนวนประกอบ

ดังนั้น n ต้องมีตัวหารที่เป็นจำนวนเฉพาะ

ให้ p_{i_0} เป็นตัวหารของ n

จะได้ว่า $p_{i_0} | p_1p_2\ldots p_r + 1$

ซึ่งทำให้ $p_{i_0} | 1$ ซึ่งเป็นไปไม่ได้

ดังนั้น จึงมีจำนวนเฉพาะมากมายเป็นจำนวนอนันต์ #

แบบฝึกหัด 1.5

1. จงพิจารณาว่า จำนวนต่อไปนี้เป็นจำนวนเฉพาะหรือจำนวนประกอบ

    1.1 101   1.2 103

    1.3 107   1.4 111

    1.5 113   1.6 121

    1.7 257   1.8 760

    1.9 1013   1.10 1259

2. จงเขียนจำนวนต่อไปนี้ให้อยู่ในรูปแบบของผลคูณของจำนวนเฉพาะ

    2.1 256   2.2 125

    2.3 449   2.4 662

    2.4 983   2.5 1238

    2.6 1019   2.7 1531

3. จงเขียนตารางแสดงจำนวนเฉพาะที่น้อยกว่า 300
4. จงแสดงว่า มีจำนวนเฉพาะมากมายเป็นจำนวนอนันต์ที่อยู่ในรูปแบบของ $4k-1$
5. ให้ p เป็นจำนวนเฉพาะที่ไม่ใช่ 2 หรือ 3 จงแสดงว่า p ต้องอยู่ในรูปแบบของ $6k+1$ หรือ $6k+5$
6. กำหนด p และ $p+2$ เป็นจำนวนเฉพาะ โดยที่ $p > 3$ จงแสดงว่า $6|(p+1)$