บทที่ 2

ความรู้พื้นฐาน

ในบทนี้จะกล่าวถึงความรู้พื้นฐานเฉพาะที่จำเป็น เพื่อนำไปใช้ในบทที่ 3 และบทที่ 4 โดยจะกล่าวถึง เซตและทฤษฎีเซต คุณสมบัติของจำนวนเต็ม การยกกำลังของจำนวนเต็ม ทฤษฎีพื้นฐานของเลขคณิต กอนกรูเอนซ์ คุณสมบัติของจำนวนเต็มบวก และ การจัดลำดับ

สำหรับทฤษฎีบทต่าง ๆ ในบทนี้ จะไม่พิสูจน์ไว้ ผู้ที่สนใจศึกษาได้จากเอกสารอ้างอิงท้ายเล่ม และข้อเสนอแนะที่กล่าวไว้

2.1 <u>เซตและทฤษฎีเซต</u>

ในหัวข้อนี้จะกล่าวถึง เซต คู่ลำดับ ความสัมพันธ์ ฟังก์ชัน และการเทียบเท่าของเซต

2.1.1 <u>เซต</u> (Set)

ความหมาย โดยปกติคำว่า เซต และ สมาชิกของเซตเป็นคำอนิยาม (Undefined Term) แต่ในที่นี้จะให้ความหมายของคำดังกล่าวเพื่อช่วยความเข้าใจดังนี้

เซต หมายถึง กลุ่มของสิ่งของหรือกลุ่มของจินตนาการ ซึ่งมีคุณสมบัติบางประการคล้ายกัน และสิ่งของหรือจินตนาการดังกล่าวนั้นเรียกว่า สมาชิกของเซต และใช้สัญลักษณ์ $\in$ แทนการเป็นสมาชิกของเซต ดังนั้นเมื่อเขียน

$a \in A$ หมายความว่า a เป็นสมาชิกของเซต A

$a \notin A$ หมายความว่า a ไม่เป็นสมาชิกของเซต A

<u>สัจพจน์ 2.1.1.1</u> (Existential Axiom)

มีเซตอย่างน้อยหนึ่งเซต

<u>สัจพจน์ 2.1.1.2</u> (Paradox Axiom)

ถ้า A เป็นเซตแล้ว $A \notin A$

<u>สัจพจน์ 2.1.1.3</u> (Axiom of Extension)

เซต A เท่ากับเซต B ก็ต่อเมื่อสมาชิกทุกตัวของ A เป็นสมาชิกของ B และสมาชิกทุกตัวของ B เป็นสมาชิกของ A

นั่นคือ เซตสองเซตจะเท่ากันก็ต่อเมื่อ เซตทั้งสองมีสมาชิกเหมือนกันทุกตัว

เขียนในรูปสัญลักษณ์ได้ $A = B \longleftrightarrow \forall x \left[x \in A \longleftrightarrow x \in B \right]$

จากสัจพจน์ข้างต้น จึงได้ว่า

$$A \neq B \longleftrightarrow \exists x \left[x \in A \wedge x \notin B \right] \vee \exists y \left[y \in B \wedge y \notin A \right]$$

<u>สัจพจน์ 2.1.1.4</u> (Axiom of Specification)

แต่ละเซต A และแต่ละเงื่อนไข P(x) จะมีเซต B ซึ่งประกอบด้วยสมาชิก x ทุกตัวของ A ซึ่ง P(x) เป็นจริง

นั่นคือ จะมี $B = \{x \in A \mid P(x)\}$ เรียกวิธีเขียนเซตแบบนี้ว่า วิธีกำหนดเงื่อนไข (Set builder notation)

<u>นิยาม 2.1.1.1</u> สับเซต (Subset)

เซต A เป็นสับเซต (Subset) ของเซต B ก็ต่อเมื่อสมาชิกทุกตัวของ A เป็นสมาชิกของ B

A เป็นสับเซตของ B เขียนแทนด้วย $A \subseteq B$ หรือ

$A \subseteq B \iff \forall x \; [x \in A \rightarrow x \in B]$

ถ้าสมาชิกบางตัวของ A ไม่เป็นสมาชิกของ B จะกล่าวว่า A ไม่เป็นสับเซตของ B และเขียนแทนด้วย $A \not\subseteq B$

นิยาม 2.1.1.2 สับเซตแท้ (Proper Subset)

เซต A เป็นสับเซตแท้ของเซต B ก็ต่อเมื่อ $A \subseteq B$ และ $A \neq B$

A เป็นสับเซตแท้ของ B เขียนแทนด้วย $A \subset B$

นิยาม 2.1.1.3 เซตว่าง (Empty Set)

เซตว่างคือ เซตที่ไม่มีสมาชิก **เขียนแทนด้วย** ϕ (phi อ่านว่า ฟาย) หรือ { }

2.1.2 คู่ลำดับ

นิยาม 2.1.2.1 คู่ลำดับ (Ordered pair)

คู่ลำดับ $(a,b) = \{\{a\}, \{a,b\}\}$ เรียก a ว่า พิกัดแรก และเรียก b ว่า พิกัดที่สอง

นิยาม 2.1.2.2 ผลคูณคาร์ทีเซียน (Cartesian Product)

ผลคูณคาร์ทีเซียนของ A และ B คือ เซตของคู่ลำดับ (a, b) ทุกตัวโดยที่ $a \in A$ และ $b \in B$

เขียนแทนผลคูณคาร์ทีเซียนของ A และ B ด้วย $A \times B$ เขียนในรูปสัญลักษณ์ได้

$$A \times B = \{x / x = (a, b),\ a \in A,\ b \in B\}$$

2.1.3 <u>ฟังก์ชัน</u> (Function)

<u>นิยาม 2.1.3.1</u> ฟังก์ชัน (Function)

f เป็นฟังก์ชันจาก A ไป B ก็ต่อเมื่อ

1. $f \subseteq A \times B$,
2. ถ้า $a \varepsilon A$ และ $B \neq \emptyset$ แล้ว จะมี $b \varepsilon B$ ที่ทำให้ $(a, b) \varepsilon f$,
3. ถ้า $(a, b), (a, c) \varepsilon f$ แล้ว $b = c$

f เป็นฟังก์ชันจาก A ไป B เขียนแทนด้วย $f : A \dashrightarrow B$

<u>นิยาม 2.1.3.2</u> ให้ $f : A \dashrightarrow B$ และ $(x, y) \varepsilon f$ จะกล่าวว่า y เป็นอิมเมจ (image) ของ x และ x เป็นพรีอิมเมจ (preimage) ของ y

เขียนแทนด้วย $y = f(x)$

<u>นิยาม 2.1.3.3</u> ให้ $f : A \dashrightarrow B$

ก. f เป็นฟังก์ชันแบบทั่วถึง ก็ต่อเมื่อ แต่ละ $b \varepsilon B$ จะมี $a \varepsilon A$ ที่ทำให้ $b = f(a)$

ข. f เป็นฟังก์ชันแบบหนึ่งต่อหนึ่ง ก็ต่อเมื่อ ถ้า $a, b \varepsilon A$ และ $f(a) = f(b)$ แล้ว $a = b$

ค. f เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่ง และ f เป็นฟังก์ชันแบบทั่วถึง

2.1.4 <u>การเทียบเท่าของเซต</u> (Equivalent)

<u>นิยาม 2.1.4.1</u> A เทียบเท่ากับ B ก็ต่อเมื่อมีฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก A ไป B

A เทียบเท่ากับ B เขียนแทนด้วย $A \sim B$

<u>นิยาม 2.1.4.2</u> เซตจำกัด (Finite set)

A จะเป็นเซตจำกัด ก็ต่อเมื่อ A เป็นเซตว่างหรือมี $k \in Z^+$ โดยที่ $N_k = \{1, 2, \ldots, k\}$ ที่ทำให้ $A \sim N_k$

<u>ทฤษฎี 2.1.4.1</u> ถ้า A เป็นเซตจำกัด และ $A \neq \emptyset$ และ $B \subset A$ แล้ว B จะเป็นเซตจำกัด

<u>พิสูจน์</u> ดูรายละเอียดจาก [2] หน้า 41

<u>นิยาม 2.1.4.3</u> จำนวนสมาชิก

ถ้า A เป็นเซตจำกัด และ $A \neq \emptyset$ แล้วจะเรียก $k \in Z^+$ ว่าเป็นจำนวนสมาชิกของ A ก็ต่อเมื่อ $A \sim N_k$

จำนวนสมาชิกของ A เขียนแทนด้วย $\|A\|$ ดังนั้นจะได้ $\|A\| = k$

ทฤษฎี 2.1.4.2 ถ้า A และ B เป็นเซตจำกัด โดยที่ $A, B \neq \emptyset$ และ $A \subseteq B$ แล้ว $\|A\| \leq \|B\|$

พิสูจน์ ดูรายละเอียดจาก [2] หน้า 52

ทฤษฎี 2.1.4.3 ถ้า A และ B เป็นเซตจำกัด โดยที่ $A, B \neq \emptyset$ และ $A \subset B$ แล้ว $\|A\| < \|B\|$

พิสูจน์ ดูรายละเอียดจาก [2] หน้า 52

2.2 คุณสมบัติของจำนวนเต็ม

นิยาม 2.2.1 (การหารลงตัว)

ถ้า $n, a \in Z$ โดยที่ $a \neq 0$ แล้ว จะกล่าวว่า a หาร n ลงตัว ก็ต่อเมื่อ มี $c \in Z$ ซึ่งทำให้ $ac = n$ และจะได้ $a = \frac{n}{c}$, $c = \frac{n}{a}$

เรียก a ว่าตัวหาร และ $\frac{n}{a}$ อ่านว่า a หาร n

a หาร n ลงตัว เขียนแทนด้วย a/n

a หาร n ไม่ลงตัว เขียนแทนด้วย $a \not/ n$

ทฤษฎี 2.2.1 (คุณสมบัติเบื้องต้นของการหารลงตัว)

ถ้า $a, b, c, x, y \in Z$ โดยที่ $a \neq 0$ แล้ว

ก. a/a

ข. $1/b$

ค. ถ้า a/b และ $b \neq 0$ แล้ว $\frac{b}{a}/b$

ง. ถ้า a/b และ b/a และ $b \neq 0$ แล้ว $|a| = |b|$

จ. ถ้า a/b และ b/c และ $b \neq 0$ แล้ว a/c

ฉ. ถ้า a/b และ $b \neq 0$ แล้ว $|a| \leq |b|$

ช. ถ้า ab/ac และ $b \neq 0$ แล้ว b/c

ซ. ถ้า a/b และ a/c แล้ว $a/(bx + cy)$

ฌ. ถ้า a/b และ $c \neq 0$ แล้ว ac/bc

<u>พิสูจน์</u> ดูรายละเอียดจาก [4] หน้า 96

<u>นิยาม 2.2.2</u> (ตัวหารร่วม)

ถ้า $a, b, d \in Z$ และ $d \neq 0$ แล้ว จะเรียก d ว่าเป็นตัวหารร่วมของ a และ b ก็ต่อเมื่อ d/a และ d/b

<u>ทฤษฎี 2.2.2</u> ถ้า $a, b \in Z$ โดยที่ a และ b ไม่เป็น 0 พร้อมกัน แล้วจะมี $d \in Z^+$ ซึ่ง

ก. d/a และ d/b,

ข. $d = ax + by$ โดยที่ $x, y \in Z$,

ค. ถ้า $c \in Z^+$ โดยที่ $c \neq 0$ และ c/a, c/b แล้ว c/d

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 15

<u>ทฤษฎี 2.2.3</u> ถ้า $a, b \in Z^+$ โดยที่ a และ b ไม่เป็น 0 พร้อมกัน แล้วจะมี $d \in Z^+$ เพียงตัวเดียวเท่านั้น ซึ่ง

ก. d/a และ d/b,

ข. ถ้า $c \in Z^+$ และ c/a, c/b แล้ว c/d

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 15

<u>นิยาม 2.2.3</u> ตัวหารร่วมมาก (Greatest Common Divisor)

ถ้า $a, b \in Z$ โดยที่ a และ b ไม่เป็น 0 พร้อมกันแล้ว จะเรียก $d \in Z^+$ ว่าเป็นตัวหารร่วมมากของ a และ b ก็ต่อเมื่อ

ก. d/a และ d/b,

ข. ถ้า $c \in Z^+$ และ c/a, c/b แล้ว c/d

d เป็นตัวหารร่วมมากของ a และ b

เขียนแทนด้วย $d = (a, b)$

<u>ทฤษฎี 2.2.4</u> ถ้า $a, b \in Z$ แล้ว $(a, b) = (b, a)$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 16

<u>ทฤษฎี 2.2.5</u> ถ้า $a, b \in Z$ และ $(a, b) = d$ แล้ว จะมี $x, y \in Z$ ที่ทำให้ $d = ax + by$

<u>พิสูจน์</u> ดูรายละเอียดจาก [10] หน้า 6

<u>ทฤษฎี 2.2.6</u> ถ้า $a, b \varepsilon Z$ แล้ว $(a, b) = 1$ ก็ต่อเมื่อ มี $x, y \varepsilon Z$ ที่ทำให้ $1 = ax + by$

<u>พิสูจน์</u> ดูรายละเอียดจาก [1] หน้า 12

<u>ทฤษฎี 2.2.7</u> ถ้า $a, b, c \varepsilon Z$ โดยที่ $a \neq 0$ และ a/bc และ $(a, b) = 1$ แล้ว a/c

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 16

<u>ทฤษฎี 2.2.8</u> ถ้า $a, m, n \varepsilon Z$ และ $(am, n) = 1$ แล้ว $(a, n) = 1$

<u>พิสูจน์</u> อาศัยทฤษฎี 2.2.6

<u>ทฤษฎี 2.2.9</u> ถ้า $a, m, n \varepsilon Z$ และ $(a, m) = 1 = (a, n)$ แล้ว $(a, mn) = 1$

<u>พิสูจน์</u> ดูรายละเอียดจาก [4] หน้า 115

<u>นิยาม 2.2.4</u> จำนวนเฉพาะ (prime)

ถ้า $p \varepsilon Z^{+}$ โดยที่ $p > 1$ แล้วจะเรียก p ว่าเป็นจำนวนเฉพาะ ก็ต่อเมื่อ มีเพียง ± 1 และ $\pm p$ เท่านั้นที่หาร p ลงตัว

<u>ทฤษฎี 2.2.10</u> ถ้า $n \in Z^+$ โดยที่ $n > 1$ แล้ว n จะเป็นจำนวนเฉพาะหรือเป็นผลคูณของจำนวนเฉพาะ

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 16

<u>ทฤษฎี 2.2.11</u> ถ้า $a \in Z$ และ $p \nmid a$ โดยที่ p เป็นจำนวนเฉพาะ แล้ว $(a, p) = 1$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 17

<u>ทฤษฎี 2.2.12</u> ถ้า $a, b \in Z$ และ p/ab โดยที่ p เป็นจำนวนเฉพาะ แล้ว p/a หรือ p/b

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 17

<u>นิยาม 2.2.5</u> จำนวนเฉพาะสัมพัทธ์ (Relatively prime)

ถ้า $a, b \in Z$ แล้ว จะเรียก a และ b ว่าเป็นจำนวนเฉพาะสัมพัทธ์ ก็ต่อเมื่อ $(a, b) = 1$

<u>ทฤษฎี 2.2.13</u> ถ้า $q, p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะโดยที่ $n \in Z^+$ และ $q/p_1 \cdot p_2 \cdots p_n$ แล้ว $q = p_k$ สำหรับบาง k ซึ่ง $1 \leq k \leq n$

<u>พิสูจน์</u> ดูรายละเอียดจาก [10] หน้า 14

2.3 การยกกำลังของจำนวนเต็ม

นิยาม 2.3.1 ถ้า $a \in Z^+$ และ $k \in Z^+$ แล้ว

ก. a เขียนย่อ ๆ เป็น a^1

$a.a$ เขียนย่อ ๆ เป็น a^2

$a.a...a$ (k จำนวน) เขียนย่อ ๆ เป็น a^k

ข. $a^k . a = a^{k+1}$

ทฤษฎี 2.3.1 ถ้า $m, n \in Z^+$ และ $a, b \in Z^+$ แล้ว

ก. $a^m . a^n = a^{m+n}$

ข. $(a^m)^n = a^{mn}$

ค. $(ab)^m = a^m b^m$

ง. $1^m = 1$

จ. $0^m = 0$

ฉ. $a^m \neq 0$

ช. $\frac{a^m}{b^n} = a^m . b^{-n}$

พิสูจน์ ดูรายละเอียดจาก [6] หน้า 7

ทฤษฎี 2.3.2 ถ้า $m, n \varepsilon Z^+$ และ $a \varepsilon Z^+$

แล้ว $\frac{a^m}{a^n} = a^{m-n}$

พิสูจน์ ดูรายละเอียดจาก [4] หน้า 66

ทฤษฎี 2.3.3 ถ้า $a, k \varepsilon Z^+$ แล้ว

ก. $\frac{k}{k} = 1$

ข. $\frac{1}{a} = a^{-1}$

พิสูจน์ เป็นผลจากทฤษฎี 2.3.2

2.4 ทฤษฎีพื้นฐานของเลขคณิต (The Fundamental Theorem of Arithmetic)

ทฤษฎี 2.4.1 ถ้า $n, k \varepsilon Z^+$ โดยที่ $n > 1$ แล้วจะมี $a_i \varepsilon Z^+$ โดยที่ $i = 1, 2, \ldots, k$ และ p_i เป็นจำนวนเฉพาะ ซึ่ง $p_1 < p_2 < \ldots < p_k$ ซึ่งทำให้ $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ และการเขียน n แบบนี้ เขียนได้เพียงแบบเดียว

พิสูจน์ ดูรายละเอียดจาก [9] หน้า 17

<u>ทฤษฎี 2.4.2</u> ถ้า $k, n, a_i \in Z^+$ และ $t_i \in W$ โดยที่

$0 \leq t_i \leq a_i$ และ $i = 1, 2, \ldots, k$ และ

$p_1, p_2, \ldots, p_k$ เป็นจำนวนเฉพาะที่แตกต่างกัน และ

$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ แล้ว $d \in Z^+$

จะเป็นตัวหารของ n ก็ต่อเมื่อ $d = p_1^{t_1} p_2^{t_2} \ldots p_k^{t_k}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [8] หน้า 28

<u>ทฤษฎี 2.4.3</u> ถ้า $a, b, k, d \in Z^+$ และ $a_i, b_i \in W$

โดยที่ $i = 1, 2, \ldots, k$ และ $p_1, p_2, \ldots, p_k$

เป็นจำนวนเฉพาะที่แตกต่างกัน และ $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$,

$b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ แล้ว $d = (a, b)$

ก็ต่อเมื่อ $d = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \ldots p_k^{\min\{a_k, b_k\}}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 18

<u>นิยาม 2.4.1</u> ออยเลอร์ ฟาย-ฟังก์ชัน (Euler ϕ-Function)

ถ้า $n \in Z^+$ แล้ว จำนวนของจำนวนเต็มบวกที่น้อยกว่าหรือเท่ากับ n และเป็นจำนวนเฉพาะสัมพัทธ์กับ n เรียกว่า ออยเลอร์ ฟาย-ฟังก์ชัน ของ n เขียนแทนด้วย $\phi(n)$ หรือ

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

แล้ว $||K|| = \emptyset(n)$

<u>สัญลักษณ์</u> ถ้า $d_i, n, k \in Z^+$ และ d_i/n โดยที่ $i = 1, 2, \ldots, k$ แล้ว $\sum_{i=1}^{k} \emptyset(d_i)$ หมายถึง $\emptyset(d_1) + \emptyset(d_2) + \ldots + \emptyset(d_k)$

<u>ทฤษฎี 2.4.4</u> ถ้า $d_i, n, k \in Z^+$ และ d_i / n โดยที่ $i = 1, 2, \ldots, k$ แล้ว $\sum_{i=1}^{k} \emptyset(d_i) = n$

<u>พิสูจน์</u> ดูรายละเอียดจาก [8] หน้า 35

<u>ทฤษฎี 2.4.5</u> ค่าของ $\emptyset(n)$

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

$$\emptyset(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 27

2.5 <u>คอนกรูเอนซ์</u> (Congruence)

<u>นิยาม 2.5.1</u> ถ้า $a, b \in Z$ และ $m \in Z^+$ เราจะกล่าวว่า a คอนกรูเอนซ์กับ b มอดุโล m ก็ต่อเมื่อ $m/(a-b)$

a คอนกรูเอนซ์กับ b มอดุโล m เขียนแทนด้วย $a \equiv b \pmod{m}$

<u>ทฤษฎี 2.5.1</u> ถ้า $a \equiv b \pmod{m}$ และ $c \equiv d \pmod{m}$ แล้ว $ac \equiv bd \pmod{m}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [8] หน้า 62

<u>ทฤษฎี 2.5.2</u> ถ้า $a \equiv b \pmod{m}$ และ $c \in Z$ แล้ว $ac \equiv bc \pmod{m}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [8] หน้า 62

<u>ทฤษฎี 2.5.3</u> ถ้า $a \equiv b \pmod{m}$ และ $c \in Z^+$ แล้ว $ac \equiv bc \pmod{mc}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 108

<u>ทฤษฎี 2.5.4</u> ถ้า $ac \equiv bc \pmod{m}$ และ $d = (m, c)$

แล้ว $a \equiv b \pmod{\frac{m}{d}}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 109

<u>ทฤษฎี 2.5.5</u> ถ้า $a \equiv b \pmod{m}$ และ $c \in Z^+$ แล้ว $a^c \equiv b^c \pmod{m}$

<u>พิสูจน์</u> ดูรายละเอียดจาก [8] หน้า 63

<u>ทฤษฎี 2.5.6</u> (Euler-Fermat Theorem)

ถ้า $a \in Z$, $m \in Z^+$ โดยที่ $(a, m) = 1$ แล้ว

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 113

<u>ทฤษฎี 2.5.7</u> ถ้า $m, n \in Z^+$ และ $d = (m, n)$ แล้ว

$$\phi(mn) = \phi(m)\,\phi(n)\left(\frac{d}{\phi(d)}\right)$$

<u>พิสูจน์</u> ดูรายละเอียดจาก [9] หน้า 28

2.6 คุณสมบัติของจำนวนเต็มบวก

นิยาม 2.6.1 สมาชิกที่มากที่สุดของเซต

ถ้า $A \subseteq Z^+$ และ $A \neq \emptyset$ แล้ว จะเรียก $x \in A$ ว่าเป็นสมาชิกที่มากที่สุดของ A ก็ต่อเมื่อ ถ้า $y \in A$ แล้ว $y \leq x$

ทฤษฎี 2.6.1 ถ้า $A \subseteq Z^+$ และ $A \neq \emptyset$ และ A เป็นเซตจำกัด แล้ว A มีสมาชิกที่มากที่สุด

พิสูจน์ ดูรายละเอียดจาก [3] หน้า 910

ทฤษฎี 2.6.2 ถ้า $n \in Z^+$ และ $p(n)$ แทนข้อความที่เกี่ยวกับ n และ

ก. $p(1)$ เป็นจริง ,

ข. ถ้า $k \in Z^+$ และ $p(k)$ เป็นจริงแล้ว $p(k+1)$ เป็นจริงด้วย

แล้วจะได้ว่า $p(n)$ เป็นจริงทุกค่าของ n

พิสูจน์ ดูรายละเอียดจาก [4] หน้า 83

2.7 การจัดลำดับ (Permutation)

กฎขั้นมูลฐาน 1 ถ้ามีการกระทำ 2 อย่างต่อเนื่องกัน โดยที่การกระทำอย่างหนึ่งมี n_1 วิธี และแต่ละวิธีนั้นทำให้การกระทำครั้งที่ 2 มี n_2 วิธี ดังนั้นการกระทำต่อเนื่องกันจะจัดกระทำได้ $n_1 \times n_2$ วิธี

หมายเหตุ ถ้ามีการกระทำหลายอย่างเกิดขึ้นต่อเนื่องกันไป การกระทำอย่างแรกมี n_1 วิธี และแต่ละวิธีของการกระทำอย่างแรกนั้น การกระทำอย่างที่ 2 เกิดได้ n_2 วิธี และแต่ละวิธีของการกระทำอย่างแรกและอย่างที่ 2 การกระทำอย่างที่ 3 เกิดได้ n_3 วิธี ดังนี้ต่อไปเรื่อย ๆ จนถึงการกระทำอย่างที่ k ซึ่งเกิดได้ n_k วิธี เพราะฉะนั้นการกระทำ k อย่างต่อเนื่องกันนี้ จะจัดกระทำได้ $n_1 \times n_2 \times \ldots \times n_k$ วิธี

กฎขั้นมูลฐาน 2 จากกฎที่ 1 ถ้าหากว่า $n_1 = n_2 = \ldots = n_k = n$ นั่นคือ มีการกระทำ k อย่าง ซึ่งกระทำต่อเนื่องหรือกระทำพร้อม ๆ กัน ถ้าแต่ละอย่างมีจำนวนวิธีที่จะทำได้ n วิธี ฉะนั้นการกระทำ k อย่างต่อเนื่องกัน หรือพร้อม ๆ กัน จะกระทำได้ n^k วิธี