Integers

$a \mid b$ a divides b

$\exists c \in \mathbb{Z}\ b = ac$

Primes positive integers ≥ 2

$p \geq 2$ is prime if $\underset{a \geq 1}{a \mid p} \Rightarrow a = 1 \lor a = p$

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7 \ldots$

Fundamental Theorem of Arithmetic

Every positive integer ≥ 2 (or 1) can be written uniquely as a product of primes.

$$n = \prod_{i \geq 1} p_i^{e_i}$$

$e_i \in \mathbb{N}$

$9 = 2^0 \cdot 3^2 \cdot 5^0 \cdots$

Proof (excluding uniqueness)

basis $1 = 2^0 \cdot 3^0 \cdot 5^0 \cdots$

$2 = 2^1 \cdot 3^0 \cdot 5^0 \cdots$

$n+1$:

case 1, $n+1$ is prime p_j

$$n+1 = p_1^0 \cdot p_2^0 \cdots p_j^1 \, p_{j+1}^0 \cdots$$

case 2 $n+1$ is composite

$$n+1 = a \cdot b \text{ , s.t. } a \neq 1, b \neq 1$$

$$a = p_1^{a_1} \, p_2^{a_2} \, p_3^{a_3} \cdots$$

$$b = p_1^{b_1} \, p_2^{b_2} \cdots$$

$$n+1 = p_1^{(a_1+b_1)} \cdot p_2^{(a_2+b_2)} \cdots$$

$a, b \geq 1$

$\gcd(a, b)$

c is a common divisor of a & b
if $c \mid a$ & $c \mid b$

$\gcd(a, b) = \max\{c \mid c$ is a common divisor of a & b $\}$

<u>Theorem</u> $d \mid a$

$d = \prod p_i^{d_i}$ $\quad a = \prod p_i^{a_i}$

$\forall i \quad d_i \leq a_i$

$a = 24 = 2^3 \cdot 3^1$

$2^0 3^0 = 1$	$2^0 3^1$ 3
$2^1 3^0 = 2$	$2^1 3^1$ 6
$2^2 3^0 = 4$	$2^2 3^1$ 12
$2^3 3^0 = 8$	$2^3 3^1$ 24

$d \mid a$

$\exists c \quad a = d \cdot c$

$c = \prod p_i^{c_i}$

$a = \prod p_i^{a_i} = d \cdot c$

$= \prod p_i^{d_i} \cdot \prod p_i^{c_i}$

$= \prod p_i^{d_i + c_i} = \prod p_i^{a_i}$

$\forall i \quad d_i + c_i = a_i$

by uniqueness

and so $\forall i \; d_i \leq a_i$

(since $c_i \geq 0$)