Properties of integers

Divisibility

$a, b \in \mathbb{Z}$. We say that a divides b, denote $a \mid b$, if there exists an integer $k \in \mathbb{Z}$ such that

$$b = ak$$

Examples

$5 \mid 15$, $5 \mid -15$, $-5 \mid 15$, $-5 \mid -15$

Properties

(1) $1 \mid a$ for all $a \in \mathbb{Z}$

(2) $a \mid 0$ for all $a \in \mathbb{Z}$

(3) $a \mid b$ and $b \mid c$, then $a \mid c$

(4) $a \mid b \Rightarrow |a| \leq |b|$. $(b \neq 0)$

(5) $a \mid b$ and $b \mid a \Rightarrow b = \pm a$

(6) $a \mid b \Rightarrow a \mid bx$ for any $x \in \mathbb{Z}$

(7) $a \mid b_i$ for $i = 1, 2, \ldots, k$. Then for any integers $x_1, x_2, \ldots, x_k$, we have

$$a \mid b_1 x_1 + b_2 x_2 + \cdots + b_k x_k.$$

$n \in \mathbb{Z}^+$, $n > 1$

n is called prime, if

$a \mid n \Rightarrow a = 1$ or $a = n$.

If $n > 1$ is not prime, it is called composite.

A composite number n can be written as $n = n_1 n_2$ with

$1 < n_1 < n$ and

$1 < n_2 < n$.

Theorem: If $n > 1$ is composite, then n is divisible by a prime p.

Proof: (well-ordering principle)

Let $S \subseteq \mathbb{Z}^+$ be the set of integers > 1 that do not have prime divisors.

If $S \neq \emptyset$, then S contains a minimum n.

n is not prime. n is composite

$n = n_1 n_2$, $1 < n_1 < n$, $1 < n_2 < n$.

$n_1 \notin S$. $p \mid n_1$, $n_1 \mid n \Rightarrow p \mid n$

$S \neq \emptyset$

Theorem: There are infinitely many primes.

Proof: $p_1, p_2, \ldots, p_k$

$$n = p_1 p_2 \cdots p_k + 1$$

$\exists$ a prime p s.t. $p \mid n$.

But $p \neq p_1, p_2, \ldots, p_k$. $\lightning$

(Euclid's proof)

Greatest common divisors (gcd)

a, b (not both zero)

$a, b \in \mathbb{N}_0$.

$1 \mid a$, $1 \mid b$ $\Rightarrow$ 1 is a common divisor of a and b

$d = \gcd(a, b)$ if

(i) d is a common divisor of a and b

(ii) if c is a common divisor of a and b, then $c \mid d$ (or $c \leq d$)

How to compute $\gcd(a, b)$?

$\gcd(a, 0) = a$

$\gcd(0, 0)$ is undefined.

Euclidean division

Given any $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$,
there exist unique integers q and r
such that

(1) $a = qb + r$, and

(2) $0 \leq r < b$.

q - quotient

r - remainder

<u>Proof:</u> If $b \mid a$, $a = kb$

take $q = k$, $r = 0$.

So suppose $b \nmid a$.

$$S = \{ a - tb \mid t \in \mathbb{Z},\ a - tb > 0 \}$$

$S \neq \emptyset$ If $a > 0$, take $t = 0$

If $a = 0$, take $t = -1$

If $a < 0$, take $t = a$

$$a - ab = (1 - b)a \geq 0$$

S contains a minimum. Call it r.

If $r \geq b$,

$$r = a - tb \geq b$$

$$a - tb - b \geq 0$$

$$a - (t+1)b \geq 0$$

$$\underbrace{a - (t+1)b}_{\in S,} > 0$$

$r - b$ (smaller than r)

$\Rightarrow r < b.$

$$a = q_1 b + r_1 = q_2 b + r_2$$

$$0 \leq r_1 < b$$
$$0 \leq r_2 < b$$

$$(q_1 - q_2) b = r_2 - r_1$$

$$b \mid r_2 - r_1 \qquad -b < r_2 - r_1 < b$$

$$b \mid 0 \qquad r_2 - r_1 = 0$$

$$r_1 = r_2$$

$$q_1 = q_2$$

Euclidean gcd algorithm

$$\gcd(a, b) = \gcd(b, a \text{ rem } b)$$

$$a \% b$$

This terminates.

Theorem: Let $d = \gcd(a, b)$. Then d is the smallest positive integer that can be expressed as

$$ua + vb$$

with $u, v \in \mathbb{Z}$.

least common multiple (lcm)

$$\operatorname{lcm}(a,b) = \min\{m \in \mathbb{Z}^+ \mid a \mid m \text{ and } b \mid m\}$$

<u>Exercise:</u> $ab = \gcd(a,b) \times \operatorname{lcm}(a,b)$.

p prime and $p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$.

Theorem: p prime. $p \mid a_1 a_2 \cdots a_k$

$\Rightarrow p \mid a_i$ for some $i = 1, 2, \ldots, k$

Fundamental Theorem of Arithmetic

Every $n \in \mathbb{Z}^+$ can be factored uniquely into a product of primes.

Proof :

[Existence] n

$n = 1$ empty product

n is prime, ✓

n is composite.

n is divisible by some prime p.

$$\frac{n}{p} = p_1 p_2 \cdots p_r$$

$$n = p p_1 p_2 \cdots p_r$$

[Uniqueness]

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}$$

$$p_1 < p_2 < \cdots < p_s \qquad q_1 < q_2 < \cdots < q_t .$$

$$p_1 \mid n \qquad p_1 \mid q_j \qquad p_1 = q_j$$

$$q_1 \mid n \qquad q_1 \mid p_i \qquad q_1 = p_i$$

$$j > 1 \qquad p_1 = q_j > q_1 = p_i \geq p_1$$

$$j = 1$$

$p_1 = q_1$

$$\frac{n}{p_1} = p_1^{e_1-1} p_2^{e_2} \cdots p_s^{e_s}$$

$$= \frac{n}{q_1} = q_1^{f_1-1} q_2^{f_2} \cdots q_t^{f_t}$$

$s = t$, $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_s = q_t$

$e_1 - 1 = f_1 - 1$, $e_2 = f_2$, $\ldots$, $e_s = f_t$.

$n \in \mathbb{Z}^+$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

$\phi(n) = |\mathbb{Z}_n^*|$

= Euler totient function
(phi)

$\phi(20) = 8$

$n = 20$ $\quad \mathbb{Z}_{20} = \{0, 1, 2, \ldots, 19\}$

$\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + - \cdots$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

$$= n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

$$20 = 2^2 \times 5$$

$$\phi(20) = 20 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$$

$$= 8$$