Ch 1.2.1 Theory of Divisibility (Y)

Let a and b be integers with $a \neq 0$. We say a divides b, denoted by $a \mid b$, if there exists an integer c such that $b = ac$. When a divides b, we say that a is a *divisor* (or *factor*) of b, and b is a *multiple* of a. If a does not divide b, we write $a \nmid b$. If $a \mid b$ and $0 < a < b$, then a is called a *proper divisor* of b.

- $a \mid b \rightarrow b$ is divisible by a.
- $a^\alpha \mid\mid b$ is sometimes used to indicate that $a^\alpha \mid b$ but $a^{\alpha+1} \nmid b$.

▼ Example

The integer 200 has the following positive divisors: $1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200$.

Thus, for example, we can write $8 \mid 200,\ 50 \mid 200,\ 7 \nmid 200,\ 35 \nmid 200$.

A divisor of n is called a *trivial divisor* of n if it is either 1 or n itself. A divisor of n is called a *nontrivial divisor* if it is a divisor of n, but is neither 1, nor n.

▼ Example

For the integer 18, 1 and 18 are the trivial divisors, whereas 2, 3, 6, 9 are the nontrivial divisors. The integer 191 has only two trivial divisors and does not have any nontrivial divisors.

Theorem Let a, b, c be integers. Then
1. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. if $a \mid b$, then $a \mid bc$, for any integer c.
3. if $a \mid b$ and $b \mid c$, then $a \mid c$.

Theorem (Division algorithm) For any integer a and any positive integer b, there exist unique integers q and r such that $a = bw + r,\ 0 \leq r < b$.

- a is called *dividend*, q the *quotient*, and r the *remainder*.

Consider the following equation $a = 2q + r,\ a, q, r \in \mathbb{Z},\ 0 \leq r < q$.
Then if $r = 0$, then a is *even*, whereas if $r = 1$, then a is *odd*.

A positive integer n greater than 1 is called *prime* if it only divisors are n and 1. A positive integer n that is greater than 1 and is not prime is called *composite*.

Theorem (Euclid) There are infinitely many primes.

Theorem If n is an integer ≥ 1, then there is a prime p such that $n < p \leq n! + 1$.

Theorem Given any real number $x \geq 1$, there exists a prime between x and $2x$.

If n is an integer ≥ 2, then there are no primes between $n! + 2$ and $n! + n$.

If n is a composite, then n has a prime divisor p such that $p \leq \sqrt{n}$.

Algorithm (The Sieve of Eratosthenes)

Given a positive integer $n > 1$, this algorithm will find all prime numbers up to n.

1. Create a list of integers from 2 to n.
2. For prime numbers p_i $(i = 1, 2, \ldots)$ from 2, 3, 5 up to $\lfloor \sqrt{n} \rfloor$, delete all the multiples $p_i < p_i m \leq n$ from the list.
3. Print the integers remaining in the list.