CH5. Introduction to Number Theory

※5.1 Divisors

< In this section, recalling the definition of "divide" >

- Def: Let n and d be integer, $d \neq 0$.
  - d : n is d divide n, there exist an integer q satisfying $n = dq$
    - d : divisor or factor
    - q : quotient

ex) Since $21 = 3 \cdot 7$. 3 divide 21 $= 3 \mid 21 = 7$

- features
  - If n and d are positive integers and $d \mid n$, then $d \leq n$.
    → The quotient can't be greater than the number of divisions.
  - whether an integer $d > 0$ divides an integer n or not, obtain a unique quotient q and remainder r with $n = dq + r \quad (0 \leq r < d)$

- prime number
  - Def: An integer greater than 1 whose only positive divisors are itself and 1
    ↔ composite number

- Discrimination
  1. If a positive integer n is composite, test whether any of the integers $2, 3, \cdots, n-1$ div n.
  2. A positive integer $n > 1$ is composite, if and only if n has a divisor d $(2 \leq d \leq \sqrt{n})$
     ⇒ If not, n is prime number.

     → proof) Let $1 < a \leq b < n$. $n = ab$.
     $n = ab \geq a^2 \rightarrow \sqrt{n} \geq a$.
     ① If a is prime, then $d \mid n$. $d \leq \sqrt{n}$
     ② else a is composite, there exists prime d satisfying $d \mid a$, then $d \leq a \leq \sqrt{n}$. so $d \leq \sqrt{n}$

- Fundamental Theorem of Arithmetic.
  - Def: Any integer n greater than 1 can be uniquely expressed as a product of different primes, except that the order of the prime factors is reversed.
    → Natural number can be factored into prime numbers.

$$n = p_1 p_2 \cdots p_i,$$
where the p_k are primes and $p_1 \leq p_2 \leq \cdots \leq p_i$, and
$$n = p'_1 p'_2 \cdots p'_j,$$
where the p'_k are primes and $p'_1 \leq p'_2 \leq \cdots \leq p'_j$, then $i = j$ and
$$p_k = p'_k \qquad \text{for all } k = 1, \ldots, i.$$

  - The number of primes is infinite.

- gcd and lcm
  - greater common divisor
    - Def: largest positive integer that divides both m and n
      $\gcd(m, n)$
    - when we check to see if fraction m/n is in lowest terms.
    - Let m, n be integer $(m > 1, n > 1)$, with prime factorizations $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$
      $\gcd(m, n) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$
      ex) $82320 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0$
      $95040 = 2^5 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^1$
      $\gcd(82320, 95040) = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0$
  - Least common multiple
    - Def: Smallest integer that is divisible by both m, n integer. $\operatorname{lcm}(m, n)$
    - Let m, n be integer $(m > 1, n > 1)$, with prime factorizations $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$
      $\operatorname{lcm}(m, n) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}$
      ex) $82320 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0$
      $95040 = 2^5 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^1$
      $\operatorname{lcm}(82320, 95040) = 2^5 \cdot 3^3 \cdot 5^1 \cdot 7^3 \cdot 11^1$
  - $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$