5. Introduction to Number Theory

5.1 Divisor and Multiple(약수와 배수)

Def. 5.1.1 *Let $m \in \mathbf{Z}$ and $d \in \mathbf{Z}-\{0\}$. Then*

*we say d **divides** m, if $\exists q \in \mathbf{Z}$.ə. $m = dq$.*

*We say q the **quotient**(몫) of m,*

*d the **divisor**(약수) or **factor** of m, and*

*m the **multiple**(배수) of d and/or q.*

*We write $d \mid m$, if d **divides** m. and $a \nmid b$ to denote a **does not divides** b.*

Since $\mid \subseteq \mathbf{Z}-\{0\} \times \mathbf{Z} \subseteq \mathbf{Z} \times \mathbf{Z}$, $\mid$ is a binary relations on $\mathbf{Z}$.

Thm. 5.1.3 *Let $m, n, d \in \mathbf{Z}$. Then*

(a) $(d \mid m) \wedge (d \mid n) \Rightarrow (d \mid (m+n))$

(b) $(d \mid m) \wedge (d \mid n) \Rightarrow (d \mid mn)$

(c) $(d \mid m) \Rightarrow (d \mid mn)$

(d) $(d \mid n) \wedge (n \mid m) \Rightarrow (d \mid m)$

Def. 5.1.4 *Let* $n \in \aleph_2$. *We call the number n is the* ***prime****(* 소수 *),*
iff whose positive divisors of n are ***only*** *1 or n.*
Otherwise n is ***composite****(* 합성수 *).*

Thm. 5.1.7 *Let* $n \geq 2$. *n is* ***composite*** $\Leftrightarrow 2 \leq {}^{\exists}d \leq sqrt(n)$.ə. $d \mid n$.

Alg. 5.1.8 function Is_prime*?(n: integer):* **B**;
for $d := 2$ ***to*** $\lfloor \sqrt{n} \rfloor$ ***do if*** $(d \mid n) \rightarrow$ ***return*** **F** $\mid \neg(d \mid n) \rightarrow$ ***skip fi od***
return **T**

Thm. 5.1.11 Fundamental Theorem of Arithatics

Let $n \in \aleph_1$. *Then* $^{\exists}i \in \aleph$: $^{\forall}k \in \mathbf{N}_i$: $p_j \in$ *Prime and*

$n = p_1p_2\ldots p_i$ *where* $^{\forall}k \in \mathbf{N}_{i-1}$: $p_k \leq p_{k+1}$.*)*

Furthermore if $^{\exists}j \in \aleph$: $^{\forall}k \in \mathbf{N}_j$: $p_j' \in$ *Prime and*

$n = p_1'p_2'\ldots p_j'$ *where* $^{\forall}k \in \mathbf{N}_{j-1}$: $p_k' \leq p_{k+1}'$, *then*

$i = j \wedge {}^{\forall}k \in \mathbf{N}_i$: $p_k = p_k'$.

proof basis *if* $n = 1$, $i = 1$ *and* $p_1 = 1$.

induction *Assume Thm. 5.1.11 is valid for* $n \in \aleph_2$ *where* $n = p_1p_2\ldots p_i$.

Consider n +1. 1) If n+1 is ***prime****,* $i = 1$ *and* $p_1 = n$.

2) If n+1 is ***composite****,* $^{\exists}a, b \leq n$, *.э.* $n+1 = ab$ *where* $a \leq b$.

$\therefore a = p_1p_2\ldots p_i$ *and* $b = q_1q_2\ldots q_k$.

$\therefore n+1 = p_1p_2\ldots p_i \cdot q_1q_2\ldots q_k = p_1'p_2'\ldots p_j'$ *where* $^{\forall}k \in \mathbf{N}_{j-1}$: $p_k' \leq p_{k+1}'$.

Thm. 5.1.12 The number of primes is infinite

proof *proof by* ***contradiction***

Assume there are ***only finitelt many*** *primes,* $p_1, p_2, \ldots p_n$.

Consider $Q = p_1p_2\ldots p_n + 1$.

Q is prime or product of two or more primes.

If $p_j \mid Q$, $p_j \mid Q - p_1p_2\ldots p_n = p_j \mid 1$. ***Contradiction****!*

$\therefore \neg\exists j: 1 < j < n, p_j \mid Q$.

$\therefore$ *There exist* ***other prime*** *not in the list* $p_1, p_2, \ldots p_n$ *or Q is a* ***prime****.*

$\therefore$ *There are* ***infinitely many*** *primes.*

Def. 5.1.14 Common Divisors** and **Greatest Common Divisor

*Let $u, v \in \aleph_1$ and $u \neq v$. We define **common divisors** of u and v, as*

$$cd(u, v) = \{d \in \aleph_1 | \ d \mid u \wedge d \mid v\}$$ 공약수

*We define **greatest common divisors** of u and v, as*

$$gcd(u, v) = max(cd(u, v)).$$ 최대공약수

***greatest lower bound** of max*

Def. 5.1.19 Common Multiples** and **Least Common Multiple

*Let $u, v \in \aleph_1$ and $u \neq v$. We define **common multiples** of u and v, as*

$$cm(u, v) = \{m \in \aleph_1 | \ u \mid m \wedge v \mid m\}$$ 공배수

*We define **least common divisors** of u and v, as*

$$lcm(u, v) = min(cm(u, v)).$$ 최소공배수

***least upper bound** of min*

Def. 5.1.17 Prime Factorization

Let $n \in \aleph_1$. *Then where* $^{\exists} i \in \aleph$: $^{\forall} j \in \mathbf{N}_i$: $p_j \in$ *Prime:* $^{\forall} l \in \mathbf{N}_i$ *and*

***Thm. 5.1.17; 22 GCD** and **LCM**.*

Let $m, n \in \aleph_1$, $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ *and* $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ *are* ***prime factorizations****. Then*

$$gcd(m, n) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \ldots p_k^{min(a_k, b_k)}.$$

$$lcm(m, n) = p_1^{max(a_1, b_1)} p_2^{max(a_2, b_2)} \ldots p_k^{max(a_k, b_k)}.$$

Thm. 5.1.25 *Let* $m, n \in \aleph_1$. *Then* $gcd(m, n) \cdot lcm(m, n) = mn$.

proof *Mathematical induction on m and n. Left for homework!*

Definition *3 The integers a and b are* ***relatively prime(coprime)*** *if gcd(a, b) = 1.*

Definition *4 The integers* $a_1, a_2, \ldots a_n$ *are* ***pairwise relatively prime****, if* $gcd(a_i, a_j) = 1$ *whenever* $1 \leq i < j \leq n$.

Theorem *5 Let a and b be positive integer.*

$ab = gcd(a, b)\ lcm(a, b)$

Lemma *1 Let* $a = bq + r$, $a, b, q, r \in \mathbf{Z}$. *Then* $gcd(a, b) = gcd(b, r)$

proof $\forall d, d \mid a \wedge d \mid b$, *then* $d \mid a - bq = r$.*(Corollary 1)*

$\forall d, d \mid b \wedge d \mid r$, *then* $d \mid bq + r = a$.

Modular Arithmetic

Thm 1 The Division Algorithm

Let $n \in \mathbf{Z}$ *and* $d \in \aleph_2$. *Then* $\exists_1 q \in \mathbf{Z}, \exists_1 r \in \mathbf{N}_{0,d-1}: n = dq + r$.

d is called the ***divisor****, n is called* ***dividened****,*
q is called the ***quotient****, and r is called the* ***remainder****.*
$q = n$ ***div*** d, $r = n$ ***mod*** d.

Definition *3 Let* $a, b \in \mathbf{Z}, m \in \aleph_2$. *Then a is* ***congruent*** *to b modulo m,*
written $a \equiv b \pmod m$ *or* $b \in [a]_{mod\ m}$, *if* $m \mid (a - b)$.

Theorem *3* $a \equiv b \pmod m$, *iff* $a \bmod m = b \bmod m$.
or $(a - b) \bmod m = 0$.

Theorem *4* $a \equiv b \pmod m$, *iff* $\exists k \in \mathbf{Z}: a = b + km$.

Theorem *5 If* $a \equiv b \pmod m \wedge c \equiv d \pmod m$, *then*
$a + c \equiv b + d \pmod m$ $\quad$ $ac \equiv bd \pmod m$.

5.2 Representation of Integer and Integer Algorithms

Thm. 5.2.0 *Let* $B \in \aleph_2$ *and* $n \in \aleph_0$. *Then*

$^{\exists}k \geq 0$: $^{\forall}j \in \mathbf{N}_{0,k}$: $0 \leq a_k < B$, $a_k \neq 0$.э.

$n = a_k B^k + a_{k-1} B^{k-1} + \ldots + a_1 B + a_0$.

unique *repesentation*

base*(B)* ***expansion*** *of n*

written $n = (a_k a_{k-1} \ldots a_1 a_0)_B$.

$B = 10$	*Decimal*	*0, 1, 2, …, 9.*
$B = 2$	*Binary*	*0, 1.*
$B = 16$	*Hexadecimal*	*0, 1, 2, …, 9, A, B, …, F.*

5.3 The Euclidean Algorithms

Algorithm *6 Euclid algorithm*
procedure *gcd(a, b: positive integer)*
    do $b \neq 0 \rightarrow r := a \bmod b;\ a := b;\ b := r$ ***od***;
    return a

procedure *gcd(a, b: positive integer) Euclid's algorithm*
    do $a > b \rightarrow a := a - b$
     | $a < b \rightarrow b := b - a$
    od;
    return a

5.4 The PSA Public-Key Criptosystem