4 Number Theory and Cryptography

4.1 Divisability and Modular Arithmetic

***Definition** 1 Let $a, b \in \mathbf{Z}$ but $a \neq 0$. We say a **divies** b, if $^{\exists}c \in \mathbf{Z}$.ə. $b = ac$.*
*We say a is a **factor(divisor** 약수) of b, and b is a **multiple(** 배수) of a.*
*$a \mid b$ denotes a **divides** b, and $a \nmid b$ to denote a **does not divide** b.*
약수 | 배수

***Thm** 1 $^{\forall}a, b, c \in \mathbf{Z}$ but $a \neq 0$.*
i) $(a \mid b) \wedge (a \mid c) \Rightarrow a \mid (b+c)$.
ii) $(a \mid b) \Rightarrow a \mid bc$.
iii) $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$.

***Col** 1 $^{\forall}a, b, c \in \mathbf{Z}$ but $a \neq 0$. (Extension of **Thm** 1)*
$(a \mid b) \wedge (a \mid c) \Rightarrow a \mid (mb+nc)$ $\forall m, n \in \mathbf{Z}$.

Thm** 2. **The Division Algorithm

Let $^{\forall}a \in \mathbf{N}, {}^{\forall}d \in \mathbf{N}^{+}, {}^{\exists 1}q \in \mathbf{N}, {}^{\exists 1}r \in \mathbf{N}: 0 \le r < d$.ə. $a = dq + r$.

***Def.** 2 d is called the **divisor**(젯수), a is called **dividened**(피젯수),*
*q is called the **quotient**(몫), and r is called the **remainder**(나머지).*

$q = a$ ***div*** d, $r = a$ ***mod*** d ($0 \le r < d$).

Modular Arithmetic

***Def.** 3 Let $a, b \in \mathbf{Z}, m \in \mathbf{N}^{+}$. Then a is **congruent** to b modulo m,*
*written $a \equiv b$ (**mod** m), if $(a - b) \mid m$.*

***Thm.** 3 Let $a, b \in \mathbf{Z}, m \in \mathbf{N}^{+}$.*
$a \equiv b$ (**mod** m), *iff* a ***mod*** $m = b$ ***mod*** m.

***Thm** 4. $a \equiv b$ (**mod** m), iff* $^{\exists}k \in \mathbf{Z}: a = b + km$.

***Thm** 5. Let $a, b \in \mathbf{Z}, m \in \mathbf{N}^{+}$. If $a \equiv b$ (**mod** m) $\wedge$ $c \equiv d$ (**mod** m), then*
$a + c \equiv b + d$ (**mod** m) $\quad$ $ac \equiv bd$ (**mod** m).

***Col**. 2 Let $a, b \in \mathbf{Z}, m \in \mathbf{N}^+$. then*

$(a + b)$ **mod** $m = ((a$ **mod** $m) + (b$ **mod** $m))$ **mod** m

$(a \cdot)$ **mod** $m = ((a$ **mod** $m) \cdot (b$ **mod** $m))$ **mod** m

Arithmetic Modulo m

***Def**. Let $\mathbf{Z}_m = \{0, 1, \ldots, m\text{-}1\}$*(m 의 나머지)

We define $+_m, \cdot_m: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}_m$

$a +_m b = (a + b)$ **mod** m $\quad$ $a \cdot_m b = (a \cdot b)$ **mod** m

***Ex**. $7 (7 +_{11} 9) = 16$ **mod** $11 = 5$ $\quad$ $(7 \cdot_{11} 9) = 63$ **mod** $11 = 8$*

Closure	$\mathbf{Z}_m$
Commutative	
Associativity	
Identity	*0 for $+_m$ and 1 for $\cdot_m$*
Additive inverse	*0 or (m-a): additive inverse of a*
Distributivity	

Observation *Let* $a \in \mathbf{Z}$ *and* $m \in \mathbf{N}^+$. *Then* $0 \le a$ **mod** $m < m$.

Definition 4 *Let* $a \in \mathbf{Z}$, $m \in \mathbf{N}^+$, *and* $0 \le r < m$.

We define $[a]_m^r = \{b \in \mathbf{Z} \mid a \equiv b \pmod m,\ r = a \bmod m\}$

Example 8 $[3]_2^1 = \{\ldots, -3, -1, 1, \ldots\} = [1]_2^1 = [-3]_2^1 = \ldots$ 홀수

$[2]_2^0 = \{\ldots, -2, 0, 2, \ldots\} = [0]_2^0 = [-2]_2^0 = \ldots$ 짝수

Example 9 $[0]_3^0 = \{\ldots, 0, 3, 6, \ldots\}$

$[1]_3^1 = \{\ldots, 1, 4, 7, \ldots\}$

$[2]_3^2 = \{\ldots, 2, 5, 8, \ldots\}$

Theorem 6 $\forall a \in \mathbf{Z}$, $\forall m \in \mathbf{N}^+$, *and* $0 \le r < m$:

$\cap_{r\in\{0,1,\cdots,m-1\}} [a]_m^r = \varnothing$ *and* $\cup_{r\in\{0,1,\cdots,m-1\}} [a]_m^r = \mathbf{Z}$.

mutually disjoint ***exhaustive***

***finite* partition(disjoint cover)** *of the set* **Z(integers)**

4.2 Integer Representation and Algorithms

Theorem 1 Let $b \in \mathbf{N}$, $b \geq 2$. Then $^{\forall}n \in \mathbf{N}$,

$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b^1 + a_0 b^0$.

$k \geq 0$, $0 \leq a_0, a_1, \ldots, a_k < b$, $a_k \neq 0$. $(n \geq 1)$

0 $(n = 0)$

unique repesentation **base expansion** of n

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

Alg. 1 Constructing Base b **expansion** of n

$q, k := n, 0;$

do $q \neq 0 \rightarrow a_k, q := q$ **mod** b, q **div** $b; ++k$ **od**

$(a_{k-1} a_{k-2} \ldots a_1 a_0)_b$. is the base b **expansion** of n

Alg. 2 **Addition** of integers $(a_k a_{k-1} \ldots a_1 a_0)_b + (b_k b_{k-1} \ldots b_1 b_0)_2$

$c:=0;$ **for** $i:=0$ **to** n **do**

***Alg**. 3 **Multiplication** of integers*
Alg**. 4 Computing **div** and **mod
***Alg**. 5 Moduler Exponential*

4.3 Primes and Greatest Common Divisors

Definition *1* $p \in \mathbf{N}^+$ *is* ***prime***, $\Leftrightarrow p > 1 \wedge \neg\exists a \in \mathbf{N}^+ : (1 < a < p) \wedge (a \mid p)$. *Otherwise* ***composite***.

Theorem *1* ***The Fundamental Theorem of Arithmetic***
Every positive integer has a ***unique*** *representation*
as the product of nondecreasing series of ***zero or more primes***.

Theorem *2 If n is* ***composite*** *integer, then n has a* ***prime divisor*** *less than or equal to SQRT(n).*

Theorem *3 There are* ***infinitely*** *many primes.*
proof *proof by contradiction*
Assume there are only finite primes, $p_1, p_2, \ldots p_n$.
Let $Q = p_1 p_2 \ldots p_n + 1$.

Q is either prime or product of two or more primes.
If $p_j \mid Q$, *then* $(p_j \mid Q - p_1p_2\ldots p_n) = (p_j \mid 1)$.
$\therefore \neg^{\exists} j: 1 \le j \le n, p_j \mid Q$.
$\therefore$ *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.*

Conjectures and Open Problems about Primes

Goldbach's conjecture

Every ***even*** *integer n, n > 2, is the* ***sum of two prime*** *numbers.*

$2 \cdot 10^{17}$.

The Twin Prime conjecture

primes that ***differs two***

$16{,}8699{,}8733{,}9975 \cdot 2^{17{,}1960} \pm 1$ *are* ***primes*** *with 5,1779 digits.*

Graetest common divisors and Least common multiples

Definition *2 Let* $a, b \in \mathbf{Z}$ *and not both zero.*

$$d = gcd(a, b) = max(d) \text{ .э. } (d \mid a) \wedge (d \mid b) \Leftrightarrow$$
$$[(d \mid a) \wedge (d \mid b) \wedge [\forall e \in \mathbf{Z}: (e \mid a) \wedge (e \mid b)] \Rightarrow (d \geq e).$$

Definition *3 The integers a and b are* ***relatively prime(coprime)***

$$\text{if } gcd(a, b) = 1.$$

Definition *4 The integers* $a_1, a_2, \ldots a_n$ *are* ***pairwise relatively prime****,*

$$\text{if } gcd(a_i, a_j) = 1 \text{ whenever } 1 \leq i < j \leq n.$$

Definition *5 Let* $a, b \in \mathbf{Z}$ *and not both zero.*

$$d = lcm(a, b) = min(m) \text{ .э. } (a \mid m) \wedge (b \mid m) \Leftrightarrow$$
$$[(a \mid m) \wedge (b \mid m) \wedge [\forall n \in \mathbf{Z}, (n \mid a) \wedge (n \mid b)] \Rightarrow (m \leq n).$$

Prime Factorization

Let $a = p_1^{a1} p_2^{a2} \dots p_n^{an}$ and $b = p_1^{b1} p_2^{b2} \dots p_n^{bn}$.

$$gcd(a, b) = p_1^{min(a1, b1)} p_2^{min(a2, b2)} \dots p_n^{min(an, bn)}.$$

$$lcm(a, b) = p_1^{max(a1, b1)} p_2^{max(a2, b2)} \dots p_n^{max(an, bn)}.$$

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

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

Euclidean Algorithm

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* $d \mid bq + r = a$.

Algorithm *1 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

4.4 Solving Congruences

Thm 1.B If a and m are ***releteivelt prime*** *(서로 소), m > 1.*

4.5 Application of Congruences

4.6 Cryptography