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* $^{\exists}c \in \mathbf{Z}$.ㅇ. $b = ac$.
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) $(a \mid b) \Rightarrow {}^{\forall}k \in \mathbf{Z}: a \mid kb$.

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.ii)*

$(a \mid b) \wedge (a \mid c) \Rightarrow a \mid {}^{\forall}m, n \in \mathbf{Z}: (mb+nc) \in \mathbf{Z}$.

Thm** 2. **The Division Algorithm

Let $^{\forall}a \in \mathbf{Z}, {}^{\forall}d \in \mathbf{Z}^{+}, {}^{\exists 1}q \in \mathbf{Z}, {}^{\exists 1}r \in \mathbf{Z}^{+}: 0 \le r < d$.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 ($0 \le r < d$). $a \div d = q \ldots r$

Modular Arithmetic

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

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

***Thm** 4. $a \equiv_m b$, iff $^{\exists}k \in \mathbf{Z}: a = b + km$.*

***Thm** 5. Let $a, b \in \mathbf{Z}, m \in \mathbf{Z}^{+}$. If $a \equiv_m b$ and $c \equiv_m d$ (**mod** m), then*

$a + c \equiv_m b + d$ $ac \equiv_m bd$.

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

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

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

Arithmetic Modulo m

***Def**. Let $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$(나누기 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	

Def. 4 Let $a \in \mathbf{Z}, m \in \mathbf{Z}^+$. We define

$[a]_{\mathbf{mod}\ m} = [a]_m = \{b \in \mathbf{Z} | a \equiv_m b\} \subseteq \mathbf{Z} = [a]_m$ for short.

Ex. 8 $[3]_2 = \{\ldots, -3, -1, 1, \ldots\} = [1]_{\mathbf{mod}\ 2} = [-3]_{\mathbf{mod}\ 2} = \ldots$ 홀수

$[2]_2 = \{\ldots, -2, 0, 2, \ldots\} = [0]_{\mathbf{mod}\ 2} = [-2]_{\mathbf{mod}\ 2} = \ldots$ 짝수

Ex. 9 $[0]_3 = \{\ldots, 0, 3, \ldots\}$ $[1]_3 = \{\ldots, 1, 4, \ldots\}$ $[2]_3 = \{\ldots, 2, 5, \ldots\}$

Col. 3 Let $a \in \mathbf{Z}, m \in \mathbf{Z}^+$. Then

$[a]_{\mathbf{mod}\ m} = [b]_{\mathbf{mod}\ m}$, iff a **mod** $m = b$ **mod** m.

$[a]_{\mathbf{mod}\ m} \cap [b]_{\mathbf{mod}\ m} = \varnothing$, iff a **mod** $m \neq b$ **mod** m. ***mutually disjoint***

$\cup_{a \in \mathbf{Z}} [a]_{\mathbf{mod}\ m} = \mathbf{Z}$. ***exhaustive***

Def. 4 $Par_{\mathbf{mod}\ m}(\mathbf{Z}) = \{[a]_{\mathbf{mod}\ m} \subseteq \mathbf{Z} | a \in Z\}$

finite(m) ***congruent*** m***-modulo partition*** *of* ***infinite integers(Z)***

Col. 4 $Par_{\mathbf{mod}\ m}(\mathbf{Z}) = \mathbf{Z}$ and $|Par_{\mathbf{mod}\ m}(\mathbf{Z})| = m$ for $m \geq 2$.

What is the cardinality of $Par_{\mathbf{mod}\ m}(\mathbf{Z})$ *when* $n = 1$*???*

Algebra*, *Semingroup*, and *Monoid *(12.2 p783~)*

Let A be a set and $\oplus$ be an operation on A; i.e. $A \times A \to A$. Then

*1. If $\oplus$ is **closed** on A, i.e., $^{\forall}a, b \in A, a \oplus b \in A$, then*

*$(A, \oplus)$ is an **algebra**(**algebraic system**).*

*2. $(A, \oplus)$ is an **algebra** and the operation $\oplus$ is **associative**, i.e.,*

*$(a \oplus b) \oplus c = a \oplus (b \oplus c)$. Then $(A, \oplus)$ is called as a **semigroup**.*

Furthermore $\oplus$ bacomes an n-ary operation on A.

$A \times A \times \ldots \times A \to A$ or $A^n \to A$.

Note indexed set notation: $\oplus_{i \in I} a_i$ where $a_i \in A$.

*3. $(A, \oplus)$ is a **semigroup** and $e \in A$ is an **identity** element, i.e,*

*$^{\forall}a \in A, a \oplus e = e \oplus a = e$. Then $(A, \oplus, e)$ is called a **monoid**.*

*Let $(A, \oplus)$ be an **algebra** and $h: A \to B$. Then we **define homomorphic image** of the algebra $(A, \oplus)$ **under** h as an algebra $(B, \otimes)$.ə.*

if $h(a \oplus b) = h(a) \otimes h(b)$.

Consider two ***algebra*** $(\mathbf{Z}, +)$ *and* $(\mathbf{Par}_m(\mathbf{Z}), \oplus_m)$, *a ftn* h_m *and an op* $\oplus_m$.

$h_m: \mathbf{Z} \to \mathbf{Par}_m(\mathbf{Z})$ $\quad h_m(a) \equiv [a]_m$ *and*

$\oplus_m: \mathbf{Par}_m(\mathbf{Z}) \times \mathbf{Par}_m(\mathbf{Z}) \to \mathbf{Par}_m(\mathbf{Z})$ $\quad [a]_m \oplus_m [b]_m \equiv [a + b]_m$.

Since $h_m(a) \oplus_m h_m(b) = [a]_m{}^r \oplus_m [b]_m{}^r = [a + b]_m = h_m(a + b)$,

$(\mathbf{Par}_m(\mathbf{Z}), \oplus_m)$ *is a* ***homomorphic image*** *of* $(\mathbf{Z}, +)$ *under* h_m.

Col. 5 ***Monoids*** $(\mathbf{Z}_m, +, 0)$ *and* $(\mathbf{Par}_m(\mathbf{Z}), \oplus_m, [0]_m)$ *are* ***isomorphic***.

$i_m: \mathbf{Z}_m \to \mathbf{Par}_m(\mathbf{Z})$ $\quad i_m(a) \equiv [a]_m$ $\quad 0 \le a < m$

$i_m{}^{-1}: \mathbf{Par}_m(\mathbf{Z}) \to \mathbf{Z}_m$ $\quad i_m{}^{-1}([a]_m) = a$ $\quad 0 \le a < m$

Ex. Consider a ***monoid*** 홀짝 $= (\{$ 홀 , 짝 $\}$,

$\{$홀$\oplus_2$홀 = 짝 , 홀$\oplus_2$짝 = 홀 , 짝$\oplus_2$홀 = 홀 , 짝$\oplus_2$짝 = 짝 $\}$. 짝 $)$

Monoid 홀짝 *is an* ***abstract interpretation*** *of* $(\mathbf{Z}, +, 0)$.

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

Ex. 2 $(7106)_8 = 7 \cdot 8^3 + 1 \cdot 8^2 + 0 \cdot 8^1 + 6 \cdot 8^0 = 3654$.

$3654 \div 8 = (456, 6)$, $456 \div 8 = (57, 0)$, $57 \div 8 = (7, 1)$, $7 \div 8 = (0, 7)$.

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

$q, k := n, 0;$

do $q \neq 0 \rightarrow a_k, q, k := q$ **mod** b, q **div** b; $k+1$ **od**/* $q \div b = a_k \ldots q$ */

$(q, a_k, k) := (q \div b), k+1$ /* $q \div b = (q, a_k)$ */

$(a_{k-1}a_{k-2} \ldots a_1a_0)_b$. *is the base* b ***expansion*** *of* n

Alg. *2* ***Addition*** *of integers* $(a_ka_{k-1} \ldots a_1a_0)_b + (b_kb_{k-1} \ldots b_1b_0)_2$

c:=0; ***for*** *i:=0* ***to*** *n-1* ***do*** $\rightarrow$

Alg. *3* ***Multiplication*** *of integers*

Alg. *4 Computing* ***div*** *and* ***mod***

function *division(a, d: positive integer):*

q:=0, ***do*** $(a \geq d) \rightarrow (a, q) := (a\text{-}d, q+1)$ ***od return*** (q, a)

Alg. *5 Moduler Exponential*

4.3 Primes and Greatest Common Divisors

Definition *1* $p \in \mathbf{N}^+ \wedge p > 1$ *is* ***prime****, if only factor of p are 1 and 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)*

The Sieve of Eratosthenes
Try ***prime*** *numbers from 2 to prime number* $\leq$ *SQRT(n)*
Ex*. If n = 100, Try 2, 3, 5, 7 is enough!*

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 $Q = p_1p_2\ldots p_n + 1$.
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)***
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* $1 \leq i < j \leq n$.

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* $a = bq + r$, $a \geq b$. *Then* $\gcd(a, b) = \gcd(b, r)$, $b \geq r$.

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* $d \mid bq + r = a$. $a \div b = (q, r)$

Alg. *1 Euclid algorithm*

function *gcd(a, b: positive integer): integer;*

do $b \neq 0 \rightarrow r := a$ **mod** b; $a := b$; $b := r$ /* $a \geq b$ */ **od**; **return** a.

$(a, b) := (b, a$ **mod** $b)$ $b \geq a$ **mod** b

return a

Ex. 16 $\gcd(662, 414)$	*i.* $662 \div 414 = (1 \ldots \underline{248})$	$(414, 248)$
$= \gcd(414, 248)$	*ii.* $414 \div \underline{248} = (1 \ldots \underline{166})$	$(248, 166)$
$= \gcd(166, 82)$	*iii.* $248 \div \underline{166} = (1 \ldots \underline{82})$	$(166, 82)$
$= \gcd(166, 82)$	*iv.* $166 \div \underline{82} = (2 \ldots \underline{2})$	$(82, 2)$
$= \gcd(82, 2)$	*v.* $82 \div \underline{2} = (41 \ldots 0)$	$(2, 0)$
$= \gcd(2, 0)$	*X*	$= 2$

function slow_gcd(a, b: positive integer):integer; /* no division! */

do $a > b \rightarrow a := a - b$

| $a < b \rightarrow b := b - a$

od; **return** a.

Ex. 16' gcd(662, 414)	i.1 662 – 414 = 248	(414, 248)
= gcd(414, 248)	ii.1 414 – 248 = 166	(166, 248)
= gcd(166, 248)	iii.1 248 – 166 = 82	(166, 82)
= gcd(166, 82)	iv.1 166 – 82 = 84	(84, 82)
= gcd(84, 82)	iv.2 84 – 82 = 2	(2, 82)
= gcd(2, 82)	v.1 82 – 2 = 80	(2, 80)
= gcd(2, 80)	v.2 80 – 2 = 78	(2, 78)
=	…	
= gcd(2, 4)	v.40 4 – 2 = 2	(2, 2)
= gcd(2, 2)	v.41 2 – 2 = 0	(2, 0)
	X	= 2

4.4 Solving Congruences
4.5 Application of Congruences
4.6 Cryptography