Ch 5. Introduction to Number Theory

§5.1. Divisors.

Def) n, d : integers, $d \neq 0$.
We say that d divides n if
$n = dk$ for some integer k.

d divides $n \iff n$ is divisible by d
$\iff d$ is a divisor (또는 약수) of n
$\iff n$ is a multiple of d
$\iff d \mid n$

If d does not divide n, we write $d \nmid n$.

ex) 7 divides 84, $7 \mid 84$, $84 = 7 \cdot 12$
3 " -6, $3 \mid -6$, $-6 = 3 \cdot (-2)$
-3 " -6, $-3 \mid -6$, $-6 = (-3) \cdot 2$
5 " 0, $5 \mid 0$, $0 = 5 \cdot 0$.

Note : 0 is divisible by any nonzero integer. ($0 \mid d = 0$)

$d, m, n \in \mathbb{Z}$.

Thm ① $d \mid n, d \mid m \Rightarrow d \mid n+m$
② $d \mid n, d \mid m \Rightarrow d \mid n-m$
③ $d \mid m \Rightarrow d \mid mn \quad (n \in \mathbb{Z})$.

Pf) ① $n = d \cdot a$, $m = d \cdot b$ $(a, b \in \mathbb{Z})$.
$n+m = da + db = d(a+b)$
$\therefore d \mid n+m$.
②, ③ : similar. □

Def) An integer greater than or equal to 1 is called prime (소수) if 1 and itself are the only positive divisors. (1과 자기자신 / 양의 약수)
An integer greater than 1 is called composite if it is not prime.

ex) 7 is prime. $1 \mid 7$, $7 \mid 7$.
2 "
3 "
11 "
6 is composite. $6 = 2 \cdot 3$.

Q. How can we determine whether n is prime?

ex) 11 is prime because none of 2, 3, 4, 5, 6, 7, 8, 9, 10 divides 11.

If n is not divisible by any of $2, 3, \dots, n-1$ then n is prime.

Is 1037 prime?

Thm $n > 1$.
n is composite iff there is a divisor d of n s.t. $2 \le d \le \sqrt{n}$.

P if and only if Q = $P \leftrightarrow Q$ (P, Q 동시에 참/거짓이라는 의미)

$\neg P \leftrightarrow \neg Q$

Pf) ($\Leftarrow$) Clear. (d로 나눠지면 합성수)

($\Rightarrow$) Since n is composite, there is a divisor d of n s.t. $1 < d < n$.
Then $n = d \cdot k$, for some $k \in \mathbb{Z}$.
If $d \le k$, then $n = dk \ge d^2 \Rightarrow d \le \sqrt{n}$.
If $d > k$, then $n = dk > k^2$. Then $2 \le k < \sqrt{n}$ ☐.

$n = d \cdot k$ → 나도 divisor야

Cor (따름정리) Let $n > 1$. Then n is composite iff n has a divisor d such that d is prime and $2 \le d \le \sqrt{n}$.

↳ 더 작은 수로 쪼개지기 때문에

ex) Is 1037 prime?
sol) $\sqrt{1037} = 32.\times\times\times$
The primes at most 32 are
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots$ (*)
$1037 = 17 \cdot 61$. → composite. 합성수

ex) 1039 is prime?

sol) $\sqrt{1039} = 32.\times\times\times$
1039 is not divisible by any of (*).

$\therefore$ 1039 is prime.

Algorithm : Testing whether n is prime

Input : n $(n>1)$.

Output : True or False

```
is_prime (n) {
    for d = 2 to [√n]        // floor
        if d | n  ( n % d == 0 )
            return false
    return true.             // prime
}
```

Thm (Fundamental Theorem of Arithmetic).
Any integer greater than 1 can be written uniquely as a product of primes as follows :

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_1 < p_2 < \cdots < p_k \text{ : primes.}$$

(follows)

$e_i \geq 1$.

ex) $12 = 2^2 \cdot 3^1$, $18 = 2^1 \cdot 3^2$

$24 = 2^3 \cdot 3^1$, $60 = 2^2 \cdot 3^1 \cdot 5^1$

$17 = 17^1$

Thm There are infinitely many primes.

Pf) We will prove that if $p_1, \cdots, p_n$ are the first n primes, then there is a prime bigger than all of them.

Let $N = p_1 p_2 \cdots p_n + 1$.

Then N is not divisible by any of $p_1, \cdots, p_n$.

And, $N > p_n$.

If N is prime, we found a prime $> p_n$.

If N is not a prime, then there is a prime divisor $d \mid N$.

$p_1, \cdots p_n$은 N을 나눈기 못함

Since $p_1, \cdots, p_n \mid N$, we have $d \neq p_1, \cdots p_n$.

Then d is a prime $> p_n$. → smallest prime이기 때문에 p_n보다 큰 소수

Since there is always one more prime if we take the first n primes, there are infinitely many primes. □.

Note Twin primes are a pair of primes differ by 2.

$(3,5), (5,7), (11,13), (17,19), \ldots$ 차이가 2인

Conjecture There are infinitely many twin primes.

※ 증명

Def) n, m : integers, not both zero

The greatest common divisor of n and m is the largest integer that divides both n and m. 최대공약수

It is written as $\gcd(n,m)$ or (n,m).

ex) $\gcd(30,24) = 6$.

divisors of 30 : 1, 2, 3, 5, 6, 10, 15, 30.

" 24 : 1, 2, 3, 4, 6, 8, 12, 24.

Thm $m, n > 1$. Suppose m and n have prime factorizations

$$m = p_1^{a_1} \cdots p_k^{a_k}$$

$$n = p_1^{b_1} \cdots p_k^{b_k}$$

($p_1, \ldots p_k$ are distinct primes. $a_i, b_i \geq 0$) 0인 이유 : 두 수(m,n)를 비교해야해서

Then

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

ex) $\gcd(30,24)$.

$30 = 2^1 \cdot 3^1 \cdot 5^1$

$24 = 2^3 \cdot 3^1 \cdot 5^0$

$\gcd(30,24) = 2^{\min(1,3)} 3^{\min(1,1)} 5^{\min(1,0)}$

$= 2^1 \cdot 3^1 \cdot 5^0 = 6.$

Note $n > 0$. $\gcd(n,0) = n$. 왜냐하면 n은 0을 제외한 모든 소수나합성수로 나눌수 있기에

Def) $n, m \geq 1$. The least common multiple of n and m is the smallest positive integer that is divisible by both n and m. 최소공배수 small조건이붙어서 양수끼리 비교

It is written as $\operatorname{lcm}(n,m)$.

ex). $\operatorname{lcm}(30,24) = 120$.

multiples of 30 = 30, 60, 90, 120, 150, ...

" 24 = 24, 48, 72, 96, 120, ...

Thm $m, n \geq 1$.

$m = p_1^{a_1} \cdots p_k^{a_k}$, $n = p_1^{b_1} \cdots p_k^{b_k}$

($p_1, \ldots p_k$: distinct primes, $a_i, b_i \geq 0$).

Then

$$\operatorname{lcm}(m,n) = p_1^{\max(a_1,b_1)} \cdots p_k^{\max(a_k,b_k)}.$$

ex) $30 = 2^1 \cdot 3^1 \cdot 5^1$

$24 = 2^3 \cdot 3^1 \cdot 5^0$

$\operatorname{lcm}(30,24) = 2^{\max(1,3)} \cdot 3^{\max(1,1)} \cdot 5^{\max(1,0)}$

$= 2^3 \cdot 3^1 \cdot 5^1$

$= 120.$

Thm $m, n \geq 1$. (a_k, b_k 중 max)

$$mn = \operatorname{lcm}(m,n) \cdot \gcd(m,n).$$

(a_k, b_k 중 min)

pf) let $m = p_1^{a_1} \cdots p_k^{a_k}$

$n = p_1^{b_1} \cdots p_k^{b_k}$.

Then $\gcd(m,n) = p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$

$\operatorname{lcm}(m,n) = p_1^{\max(a_1,b_1)} \cdots p_k^{\max(a_k,b_k)}$

$\Rightarrow \operatorname{lcm}(m,n)\gcd(m,n)$

$= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdots$

We always have, for all $x, y \in \mathbb{R}$,

$\max(x,y) + \min(x,y) = x+y.$

Therefore,

$\operatorname{lcm}(m,n) \cdot \gcd(m,n)$

$= p_1^{a_1+b_1} \cdots p_k^{a_k+b_k}$ (곱셈)

$= p_1^{a_1} \cdots p_k^{a_k} \cdot p_1^{b_1} \cdots p_k^{b_k}$

$= m \cdot n.$ □

§5.2. Representations and integer algorithms

We use integers in the decimal number system.

$2107 = 2\cdot 10^3 + 1\cdot 10^2 + 0\cdot 10^1 + 7\cdot 10^0$
$= 2000 + 100 + 0 + 7$

10^3 10^2 10^1 10^0

자리

Each number in each position is in $\{0, 1, \ldots, 9\}$.

10개의 숫자

In general, we consider the number system with base b. (b is an integer ≥ 2).

base

Each number $n \geq 0$ can be written uniquely as

b진수

$$n = c_k \cdot b^k + c_{k-1} b^{k-1} + \cdots + c_1 b^1 + c_0 \cdot b^0,$$

where $c_i \in \{0, 1, \ldots, b-1\}$.

ex) The binary number system ($b=2$).

2진수

$11010_{(2)} = 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$
$= 16 + 8 + 0 + 2 + 0 = 26.$

10진수 → 2진수

How can we convert decimal → binary? (or any other base).

ex)

2 | 26		remainder
2 | 13	···	0
2 | 6	···	1
2 | 3	···	0
2 | 1	···	1
0	···	1

↑ 진수

$26 = 11010_{(2)}$.

아래부터 ↓

몫이 0이 될때까지 나누고 위로 읽음

ex) decimal → octal ($b=8$).

8진수

8 | 475		
8 | 59	···	3
8 | 7	···	3
0	···	7

↑

$475 = 733_{(8)}$.

* How to add two numbers in base b.

ex)
$$\begin{array}{r} 1\ \ 1 \\ 5\,7\,8\,3 \\ +\ \ 6\,4\,0\,9 \\ \hline 1\,2\,1\,9\,2 \end{array}$$

Carry

This came from $3+9=12>10$

$=10+2.$

ex) Addition in base 6.

$2+4=10_{(6)}$

$$\begin{array}{r} 1\ \ 1 \\ 3\,4\,0\,2_{(6)} \\ +\ \ 5\,4\,1\,4_{(6)} \\ \hline 1\,3\,2\,2\,0_{(6)} \end{array}$$

$8 = 12_{(6)}$

$9 = 13_{(6)}$

Def) a, b : integers, $b>0$.

If $a=bq+r$, $0\le r<b$, r, q : Integers,

then we say that r is the remainder of a when divided by b.

We write

$$a \bmod b = r$$

(In some programming laguages,)

$$a \,\%\, b = r.$$

ex) $10 \bmod 4 = 2$ $\quad 10 = 4\cdot 2+2$

$-5 \bmod 3 = 1$ $\quad -5 = 3\cdot(-2)+1$

$18 \bmod 6 = 0.$ $\quad 18 = 6\cdot 3+0.$

나머지가 음수가 될 수 없다

Question $2000^{10} \bmod 7 = ?$

Thm a, b: integers.
k: a positive integer.

※ $ab \bmod k = (a \bmod k)(b \bmod k) \bmod k$.
(안으로)

Pf) let $a \bmod k = r_1$, $b \bmod k = r_2$.
Then $a = kq_1 + r_1$, $b = kq_2 + r_2$.
let $ab \bmod k = r$.
Then $ab = kq + r$. $(0 \le r < k)$.
$ab = (kq_1 + r_1)(kq_2 + r_2)$
$= k^2 q_1 q_2 + kq_1 r_2 + kr_1 q_2 + r_1 r_2$. … ⊛
let $r_1 r_2 \bmod k = r_3$. $(0 \le r_3 < k)$.
Then $r_1 r_2 = kq_3 + r_3$.
By ⊛,
$ab = k(kq_1 q_2 + q_1 r_2 + r_1 q_2) + kq_3 + r_3$
$= k(kq_1 q_2 + q_1 r_2 + r_1 q_2 + q_3) + r_3$.
$\therefore ab \bmod k = r_3$
$= r_1 r_2 \bmod k$
$= (a \bmod k)(b \bmod k) \bmod k$.
(r_1, r_2) □

ex) $2000^{10} \bmod 7 = ?$
(안으로)

sol) $2000^{10} \bmod 7 = (2000 \bmod 7)^{10} \bmod 7$
$= 5^{10} \bmod 7$
$= 5^{2 \cdot 5} \bmod 7 = (5^2)^5 \bmod 7$
(기보다 크게 만든 것)
$= 25^5 \bmod 7$
$= (25 \bmod 7)^5 \bmod 7$.
$= 4^5 \bmod 7$
$= (4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \bmod 7$
$= 2 \cdot 2 \cdot 4 \bmod 7$
$= 16 \bmod 7$
$= \boxed{2}$.

$2000 = 7 \cdot 285 + 5$
$2000 \bmod 7 = 5$

§5.3. The Euclidean Algorithm (유클리드 알고리즘)

We learned a thm that allows us to compute gcd(n, m) using prime factorizations of n and m. (찾는 데 효율적이 아님 / 소인수분해)

Finding a prime factorization of a big integer is a challenging problem.

↳ RSA is a widely used cryptography system (암호화) that uses this fact.

Euclidean Algorithm is an effective way to compute gcd.

ex) gcd(2021, 2303) = 47.
(2021 = 43·47, 2303 = 47·49)

(이 정리를 사용)

Thm Suppose $a = bq + r$, $a \geq 0$, $b > 0$, $0 \leq r < b$.
Then $\gcd(a, b) = \gcd(b, r)$.

Pf) We will show that the common divisors of a, b = the common divisors of b, r.

($a > r$이라서 숫자가 작아져서)

$\Rightarrow$ $d \mid a, d \mid b \Rightarrow d \mid r = a - bq \Rightarrow d \mid b, d \mid r$.

$\Leftarrow$ $d \mid b, d \mid r \Rightarrow d \mid a = bq + r \Rightarrow d \mid a, d \mid b$.

(양을 나눌 수 있다)

Since a, b and b, r have the same common divisors their gcd must be equal. □.

2303 = 2021 + 282

Euclidean Algorithm

Input : a, b. (nonnegative, not both 0).
Output : $\gcd(a,b)$.

```
gcd (a,b) {
    if a < b
        swap (a,b)        // make a larger than b.
    while (b ≠ 0) {
        r = a mod b
        a = b
        b = r
    }
    return a
}
```

a를 b보다 더 크게

$\gcd(a,b) = \gcd(b,r)$

b=0 일 때까지

∴ remainder = 0

$\gcd(a,0) = a$

return

ex) $\gcd(2021, 2303) = ?$

$a = 2021$, $b = 2303$.

Since $a<b$, we swap a and b.

⇒ $a = 2303$, $b = 2021$.

$r = a \bmod b = 282$.

$a = 2021$, $b = 282$.

$r = 2021 \bmod 282 = 47$.

$a = 282$, $b = 47$.

$r = 282 \bmod 47 = 0$

$a = 47$, $b = 0$.

ans = 47

$\gcd(2021, 2303) = 47$.

(Recall $a \equiv b \bmod k \iff k \mid a-b$)

Thm Let $a, b \geq 0$ not both zero.
Then there are $s, t \in \mathbb{Z}$ such that
$$\gcd(a,b) = sa + tb.$$
gcd를 이렇게 표현할 수 있다.

ex) $\gcd(38, 52) = 2$
Let's find s, t satisfying $5 \cdot 38 + t \cdot 52 = 2$.

$52 = 1 \cdot 38 + 14$
$38 = 2 \cdot 14 + 10$
$14 = 1 \cdot 10 + 4$
$10 = 2 \cdot 4 + 2$ → gcd.
$4 = 2 \cdot 2 + 0$

$2 = 10 - 2 \cdot 4$
$= 1\,10 - 2(14 - 1 \cdot 10)$
$= (-2)\,14 + 3 \cdot 10$
$= (-2) \cdot 14 + 3\,(38 - 2 \cdot 14)$
$= 3 \cdot 38 - 8 \cdot 14$
$= 3 \cdot 38 - 8\,(52 - 1 \cdot 38)$
$= \underbrace{-8}_{t} \cdot 52 + \underbrace{11}_{s} \cdot 38$

역으로 대입하면

Def) $n > 0$, $k \geq 1$.
The inverse of $n \bmod k$ is the integer a
$0 < a < k$ with $a \cdot n \equiv 1 \bmod k$.
곱셈에 대한 역원
$a \cdot n \bmod k = 1$

Recall: In real numbers, the inverse of x is the number y such that $xy = 1$.
"$1/x$."

ex). The inverse of $7 \bmod 9$ is 4 because
$$4 \cdot 7 = 28 \equiv 1 \bmod 9.$$
$a \cdot 7 \bmod 9 = 1$ 을 만드는 a

Note There exists the inverse of $n \bmod k$
iff $\gcd(n, k) = 1$.
1이면 곱셈항

ex). There is no inverse of $10 \bmod 4$.
$10 \times a \bmod 4 = 1$
$a \cdot 10 \equiv 1 \bmod 4$.
even odd even
$a \cdot 10 - 1 = 4k$, Impossible.

ex). Find the inverse of 48 mod 13.

sol) We need to find $a \cdot 48 + b \cdot 13 = 1$.
(Then $a \cdot 48 \equiv 1 \mod 13$).

$48 = 3 \cdot 13 + 9$
$13 = 1 \cdot 9 + 4$.
$9 = 2 \cdot 4 + 1$

$1 = 9 - 2 \cdot 4$
$= 9 - 2(13 - 1 \cdot 9)$
$= -2 \cdot 13 + 3 \cdot 9$
$= -2 \cdot 13 + 3 \cdot (48 - 3 \cdot 13)$
$= 3 \cdot 48 + (-11) \cdot 13$.

So, $3 \cdot 48 \equiv 1 \mod 13$.
Therefore the inverse of 48 mod 13 is 3.

ex) Find the inverse of 13 mod 48.

sol)
we already know
$3 \cdot 48 + (-11) \cdot 13 = 1$.
$\Rightarrow (-11) \cdot 13 \equiv 1 \mod 48$.

$0 < a < 48$

The inverse of 13 mod 48 is -11?
No, because it's not between 0, 48.

$(-11+48) \cdot 13 \equiv (-11) \cdot 13 \mod 48$
$37 \cdot 13 \equiv 1$ "

So, 37 is the correct answer. □