Chapter 8
More Number Theory

정보보안

 $Z_p = \{0, 1, \cdots, p-1\}$

$a^{p-1} \bmod p = 1$ $\quad a^{b \bmod p-1} \bmod p$

- If p is prime and a is a positive integer not divisible by p, then a는 P의 배수가 아님

$$a^{p-1} \equiv 1 \pmod{p} \qquad (8.2)$$

- If p is prime and a is a positive integer, then

$$a^p \equiv a \pmod{p}$$

- Example

(Q) Find the least non-negative integer x in $2^{10} \equiv x \pmod{11}$.

(A) $x = 1$ 덧셈연산 X. 곱셈 연산만

$3^{52} = (\underbrace{3^{10}}_{1})^5 3^2 = 3^2 \pmod{11}$

(Q) Find the least non-negative integer x in $3^{52} \equiv x \pmod{11}$. mod(10)과 같다.

(A) $3^{52} \equiv (3^{10})^5 3^2 \equiv (1)^5 9 \equiv 9 \pmod{11}$ $\quad \therefore x = 9$ $\quad Z_n = \{0, 1, \cdots n-1\}$

$52/10 = 5 \cdots 2$ 페르마의 정리로 지수를 크지 않게 해줌

Fermat's Theorem

Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p - 1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka (\bmod p))$, where $1 \leq j < k \leq p - 1$. Because a is relatively prime to p, we can eliminate a from both sides of the equation [see Equation (4.3)] resulting in $j \equiv k (\bmod p)$. This last equality is impossible, because j and k are both positive integers less than p. Therefore, we know that the $(p - 1)$ elements of X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p - 1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \ldots \times (p - 1)a \equiv [(1 \times 2 \times \ldots \times (p - 1)] (\bmod p)$$
$$a^{p-1}(p - 1)! \equiv (p - 1)! (\bmod p)$$

We can cancel the $(p - 1)!$ term because it is relatively prime to p [see Equation (4.5)]. This yields Equation (8.2), which completes the proof.

Euler's Totient Function

- Euler's totient (or phi) function $\phi(n)$
  - $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n. 양의 정수, n보다 같거나 작은, 1, 2, … n 중에서 서로소인 것의 개수 : $\phi(n)$
  - Let p, q be prime numbers.

ex) $\phi 13 = 12$

$\phi(p) = p - 1$ prime 넘버니까

$\phi(p^k) = p^k - p^{k-1}$ p의 배수만 빼면됨 1~p^k 까지 p의 배수는

$\phi\ 21 = 3 \cdot 7$, $-1\ -1$, 12

$\phi(pq) = pq - p - q + 1 = (p - 1)(q - 1) = \phi(p)\,\phi(q)$ 소수에 지수승 꼴이 있을 때 서로소인 개수는 p^n 개 1~p^k p의 배수만 빼주면 된다. 배수를 빼는 것은 나누는 것. ∴ $p^k - p^{k-1}$

  - Example q의 배수, p의 배수 나누니까 빼줌.

3 $\phi(13) = 12, \quad \phi(21) = \phi(3)\,\phi(7) = 2 \times 6 = 12$

- Euler's product formula
  - For $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where $p_1 < p_2 < \cdots < p_r$ are primes,

$$\phi(n) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$$
$$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

  - Example

$\phi(36) = \phi(2^2 3^2) = (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$

$\phi(17640) = \phi(2^3 3^2 5^1 7^2) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0)(7^2 - 7^1) = 4032$

Euler's Theorem

a랑 n이 서로소, 공약수가 1이어야함

- For every a and n that are relatively prime (i.e., $a \in Z_n^*$),

$\phi(n)$ 오일러

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$a \in Z_p^*$ 소수들의 모임

n이랑 서로소인 개수를 지수로하면 1이된다.

- Example

Mod가 더 크면 ϕ 사용, 안하면 p-1 생각

(Q) Find the least non-negative integer x in $8^{82} \equiv x \pmod{165}$.

(A) $\phi(165) = \phi(3^1 5^1 11^1) = (3-1)(5-1)(11-1) = 2 \cdot 4 \cdot 10 = 80$

$8^{82} \equiv 8^{80} 8^2 \equiv 1 \cdot 64 \equiv 64 \pmod{165}$ $\quad \therefore x = 64$

$5 \,|\, 165$, $3 \,|\, 33$, 11

$8^{80} \equiv 1 \pmod{165}$

$a^{p-1} \equiv 1 \pmod{p}$

$8^{82} \equiv x \pmod{165}$

$\phi\ 165 = 3 \cdot 11 \cdot 5$

지수에 mod $\phi(n)$ 이 있는 것과 같다.

$2 \cdot 4 \cdot 10 = 80$.

$\underbrace{8^{80}}_{1} \cdot 8^2$

8^2

$64 \pmod{165}$

Primality Test

- The Miller-Rabin primality test
  - The MR test is an efficient probabilistic algorithm for determining if a given number is prime.

    합성수인가요? 네 → 100% 정답
  - A number which passes the test is not necessarily prime. If N multiple independent tests are performed on a composite number, then the probability that it passes each test is $1/4^N$ or less. 소수인가요? 네 → 25% 정답

    10번 물어봄 → n
- The Agrawal-Kayal-Saxena primality test
  - The AKS primality test is a deterministic polynomial-time primality-proving algorithm developed in 2002.
  - The AKS primality test is theoretically important but not very efficient.

    정확도↑. 속도↓

The Chinese Remainder Theorem

RSA . encryption . 전자서명　　　↳ 중국인의 나머지 정리

- Motivation

For example, consider the problem of finding an integer x such that

- $x \equiv 2 \pmod 3$　3으로 나누면 2　　3.4.5 가 서로소.
- $x \equiv 3 \pmod 4$　4로 나누면 3　　3×4×5=60
- $x \equiv 1 \pmod 5$　5로 나누면 1. x는 무엇일까요? x=11, 71, 131… +60 +60

A brute-force approach converts these congruences into sets and writes the elements out to the product of $3\times4\times5 = 60$ (the solutions modulo 60 for each congruence):

- $x \in \{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, \ldots\}$
- $x \in \{3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, \ldots\}$
- $x \in \{1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, \ldots\}$

To find an x that satisfies all three congruences, intersect the three sets to get:

- $x \in \{11, \ldots\}$ which can be expressed as $x \equiv 11 \pmod{60}$.

11은 교집합　3.4.5 서로 서로소　　11/3 = 3 나머지 2.

The Chinese Remainder Theorem

$$M = \prod_{i=1}^{k} m_i$$

where the m_i are pairwise relatively prime; that is, $\gcd(m_i, m_j) = 1$ for $1 \le i, j \le k$, and $i \ne j$. We can represent any integer A in Z_M by a k-tuple whose elements are in Z_{m_i} using the following correspondence:

$$A \leftrightarrow (a_1, a_2, \ldots, a_k) \qquad \textbf{(8.7)}$$

where $A \in Z_M$, $a_i \in Z_{m_i}$, and $a_i = A \bmod m_i$ for $1 \le i \le k$. The CRT makes two assertions.

1. The mapping of Equation (8.7) is a one-to-one correspondence (called a **bijection**) between Z_M and the Cartesian product $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}$.
2. Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each coordinate position in the appropriate system.

The Chinese Remainder Theorem

Let us demonstrate the **first assertion**. The transformation from A to $(a_1, a_2, \ldots, a_k)$, is obviously unique; that is, each a_i is uniquely calculated as $a_i = A \bmod m_i$. Computing A from $(a_1, a_2, \ldots, a_k)$ can be done as follows. Let $M_i = M/m_i$ for $1 \le i \le k$. Note that $M_i = m_1 \times m_2 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_k$, so that $M_i \equiv 0 \pmod{m_j}$ for all $j \neq i$. Then let

$$c_i = M_i \times \left(M_i^{-1} \bmod m_i\right) \qquad \text{for } 1 \le i \le k \tag{8.8}$$

By the definition of M_i, it is relatively prime to m_i and therefore has a unique multiplicative inverse mod m_i. So Equation (8.8) is well defined and produces a unique value c_i. We can now compute

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) \pmod{M} \tag{8.9}$$

To show that the value of A produced by Equation (8.9) is correct, we must show that $a_i = A \bmod m_i$ for $1 \le i \le k$. Note that $c_j \equiv M_j \equiv 0 \pmod{m_i}$ if $j \neq i$, and that $c_i \equiv 1 \pmod{m_i}$. It follows that $a_i = A \bmod m_i$.

The Chinese Remainder Theorem

The **second assertion** of the CRT, concerning arithmetic operations, follows from the rules for modular arithmetic. That is, the second assertion can be stated as follows: If

$$A \leftrightarrow (a_1, a_2, \ldots, a_k)$$

$$B \leftrightarrow (b_1, b_2, \ldots, b_k)$$

then

$$(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, \ldots, (a_k + b_k) \bmod m_k)$$

$$(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, \ldots, (a_k - b_k) \bmod m_k)$$

$$(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, \ldots, (a_k \times b_k) \bmod m_k)$$

The Chinese Remainder Theorem

To represent 973 mod 1813 as a pair of numbers mod 37 and 49, define

$$m_1 = 37$$

$$m_2 = 49$$

$$M = 1813$$

$$A = 973$$

We also have $M_1 = 49$ and $M_2 = 37$. Using the extended Euclidean algorithm, we compute $M_1^{-1} = 34 \bmod m_1$ and $M_2^{-1} = 4 \bmod m_2$. (Note that we only need to compute each M_i and each M_i^{-1} once.) Taking residues modulo 37 and 49, our representation of 973 is (11, 42), because 973 mod 37 = 11 and 973 mod 49 = 42.

Now suppose we want to add 678 to 973. What do we do to (11, 42)? First we compute $(678) \leftrightarrow (678 \bmod 37, 678 \bmod 49) = (12, 41)$. Then we add the tuples element-wise and reduce $(11 + 12 \bmod 37, 42 + 41 \bmod 49) = (23, 34)$. To verify that this has the correct effect, we compute

$$\begin{aligned}(23, 34) &\leftrightarrow a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \bmod M \\ &= [(23)(49)(34) + (34)(37)(4)] \bmod 1813 \\ &= 43350 \bmod 1813 \\ &= 1651\end{aligned}$$

and check that it is equal to (973 + 678) mod 1813 = 1651.

Z_n^* and Generators

Generator. ORDER

1이 되는 최소의 지수승 : ORDER

Generator

- Definitions 정의만 알기

  Z

  - The multiplicative group of Z_n is $Z_n^* = \{a \in Z_n \mid \gcd(a, n) = 1\}$. Note that $|Z_n^*| = \phi(n)$. → 1~n 가지중 n과 서로소의 개수 $\phi(14)$
  - If $a \in Z_n^*$ (i.e., a and n are relatively prime), the order of a is the least positive integer t such that $a^t \equiv 1 \pmod{n}$. t → a의 최소 지수승

  Z_8

  $Z_p^* = \{1, 2, \dots, p-1\}$

  $|Z_n^*| = \phi(n)$

  되 ofn

  - If $a \in Z_n^*$ and the order of a is $\phi(n)$, then a is said to be a generator or a primitive root of Z_n^*. If Z_n^* has a generator, then Z_n^* is said to be cyclic.

  2.3.10 13.14.15 → ORDER가 a^{18}이다.

- Theorem

  a^{18} 가장 커야만 ORDER를 Generator 라고함

  ORDER가 크면 다양한도가. 보안에서 사용

  - Z_n^* has a generator if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime and $k \geq 1$. In particular, if p is a prime, then Z_p^* has a generator.

  n이 2.4.p^k이면 Generator 가 있다.

  p^2

Table 8.3 Powers of Integers, Modulo 19

Z_{19}^* 각각 원소의 ORDER 그 전에 1이 될수도 있고 안될수도 있다.

32÷19 mod

반복

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Cyclic Group

CYCLIC GROUP We define exponentiation within a group as a repeated application of the group operator, so that $a^3 = a \bullet a \bullet a$. Furthermore, we define $a^0 = e$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group. A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.

> The additive group of integers is an infinite cyclic group generated by the element 1. In this case, powers are interpreted additively, so that n is the nth power of 1.

The Discrete Logarithm Problem (DLP)

Consider the equation 저번학기 RSA. 이산대수문제.

x를 주면 y계산 쉽고. y를 주면 힘듦

숫자가 뒤로 갈수록 커질수도, 작아질수도 있어서 잘 모른다

$$y = g^x \bmod p$$ p가 크다면. ↑

where p is a large prime number and $0 \le x \le p - 1$. Given g, x, and p, it is easy to calculate y. However, given y, g, and p, it is very difficult to calculate x ($= \mathrm{dlog}_{g,p}\, y$).

[(Generalized) Discrete Logarithm Problem]

Let G be a finite cyclic group of order n. Let g be a generator of G and let $h \in G$. The discrete logarithm of h to the base g, denoted $\log_g h$, is the unique integer x, $0 \le x \le n - 1$, such that $g^x = h$.