Basic Number Theory

Cryptography - CS 411 / CS 507

Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

September 27, 2019

Number Theory

Concerned with the properties of integers

Basic Notions

- Divisibility (of integers)
  - Let a and b be integers with $a \neq 0$. We say that a divides b, if there is an integer k s.t. $b = a \times k$
  - Denoted as $a|b$.
  - b is a multiple of a.
- Propositions
  - For every $a \neq 0$, $a|0$ and $a|a$. Also $1|b$ for every b.
  - If $a|b$ and $b|c$, then $a|c$
  - If $a|b$ and $a|c$, then $a|(s \times b + t \times c)$ for all s and t.

Prime Numbers

- A number $p > 1$ that is divisible only by 1 and itself is called a prime number.
- An integer that is not a prime number is called a composite number.
- Prime Number Theorem: Let $\pi(x)$ be the $\#$ of primes less than x. Then
  $$\pi(x) \to x/\ln x \text{ as } x \to \infty (\text{i.e. } \pi(x) \approx x/\ln x)$$
- Theorem: Every positive integer is a product of primes. This factorization is unique.
- Lemma: If p is a prime and it divides a product of integers $a \cdot b$, then either $p|a$ or $p|b$.

Greatest Common Divisor (GCD)

- GCD of a and b is the largest positive integer that divides both integers.
  - Denoted as $\text{gcd}(a, b)$.
- Computation gcd of a and b can be done
  1. by factoring a and b into primes
     - Example: $\text{gcd}(576, 135)$
     - $576 = 2^6 \times 3^2$ and $135 = 3^3 \times 5 \Rightarrow$
     - $\text{gcd}s(576, 135) = 3^2 = 9$.
  2. by using Euclidean algorithm
     - Utilizes division by remainder.

Example: Euclidean algorithm

- $\text{gcd}(482, 1180)$

$\text{gcd}(c + k \times b, b) = \text{gcd}(c, b)$

$$1180 = 2 \cdot 482 + 216$$

$$482 = 2 \cdot 216 + 50$$

$$216 = 4 \cdot 50 + 16$$

$$50 = 3 \cdot 16 + 2$$

$$16 = 8 \cdot 2 + 0$$

The last nonzero remainder is the gcd

GCD

- Theorem: Let a and b be two integers, with at least one of them nonzero, and let $d = \text{gcd}(a, b)$.
  Then there exist integers x, y such that

  $$a \times x + b \times y = d$$

  In particular, if a and b are relatively prime (i.e. $\text{gcd}(a, b) = 1$) then $a \times x + b \times y = 1$.
- In the last case, x is called the multiplicative inverse of a with respect to b since $a \times x \equiv 1 \bmod b$.

Solving $a \times x + b \times y = d$

Algorithm 1 Solving $a \cdot x + b \cdot y = d$

Input: $a > b > 0$
Output: $d = gcd(a, b)$ and $x, y \ni a \cdot x + b \cdot y = d$

```
x_2 := 1, x_1 := 0, y_2 := 0, y_1 := 1
while b > 0 do
    q := ⌊a/b⌋, r := a − q · b, x := x_2 − q x_1, y := y_2 − q y_1
    a := b, b := r, x_2 := x_1, x_1 := x, y_2 := y_1 and y_1 := y
end while
d := a, x := x_2, y := y_2
return d, x, y
```

Example: EEA $a = 4864$ and $b = 3451$

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3451	1	0	0	1
1	1413	1	-1	3451	1413	0	1	1	-1
2	625	-2	3	1413	625	1	-2	-1	3
2	163	5	-7	625	163	-2	5	3	-7
3	136	-17	24	163	136	5	-17	-7	24
1	27	22	-31	136	27	-17	22	24	-31
5	1	-127	179	27	1	22	-127	-31	179
57	0	3451	-4864	1	0	-127	3451	179	-4864

Congruence Classes

- Let a, b, and n be integers with $n \neq 0$. We say that
  - $a \equiv b \bmod n$
    (a is congruent to $b \bmod n$) if $a - b$ is a (positive or negative) multiple of n.
    Thus, $a = b + k \times n$ for some integer k (positive or negative)
  - Proposition: a, b, c, d, n integers with $n \neq 0$ and $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then
    - $a + c \equiv b + d \bmod n$,
    - $a - c \equiv b - d \bmod n$,
    - $a \times c \equiv b \times d \bmod n$

Division in Congruence Classes

- We can divide by "a" $(\text{mod} n)$ when $\gcd(a, n) = 1$
- Proposition: Suppose $\gcd(a, n) = 1$. Let s and t be integers s.t. $a \times s + n \times t = 1$. Then
  $a \cdot s \equiv 1 \pmod{n}$
  s is called the multiplicative inverse of $a \bmod n$
- Extended Euclidean algorithm is a fairly efficient method of computing multiplicative inverses in congruence classes.
- Example: Solve $2x + 7 \equiv 3 \pmod{17}$
- Example: Solve $5x + 6 \equiv 13 \pmod{15}$.

Solution to $ax \equiv b \pmod{n}$

- If $\gcd(a, n) = 1$
  - There is exactly one solution
  - $x \equiv ba^{-1} \pmod{n}$
- If $\gcd(a, n) = d \neq 1$
  - There "may" be solutions
  - If there exist solutions,there are exactly "d" solutions
  - If $d \nmid b$ then there is no solution
  - Otherwise solutions are obtained as follows

$$\frac{a}{d}\tilde{x} \equiv \frac{b}{d} \bmod \frac{n}{d} \qquad gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \qquad \tilde{x} \equiv \left(\frac{a}{d}\right)^{-1} \frac{b}{d} \bmod \frac{n}{d}$$

$$x = \left\{\tilde{x}, \tilde{x} + \frac{n}{d}, \tilde{x} + 2\frac{n}{d}, \cdots, \tilde{x} + (d-1)\frac{n}{d}\right\}$$

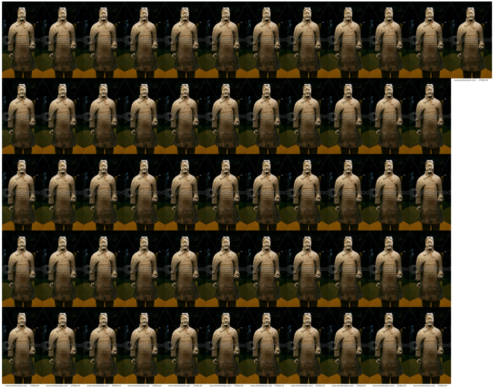
Solution to $ax \equiv b \bmod n$

- Example 1
  - $12x \equiv 15 \bmod 39$
  - Is there a solution to this equation?
- Example 2
  - $12x \equiv 17 \bmod 39$
  - Is there a solution to this equation?

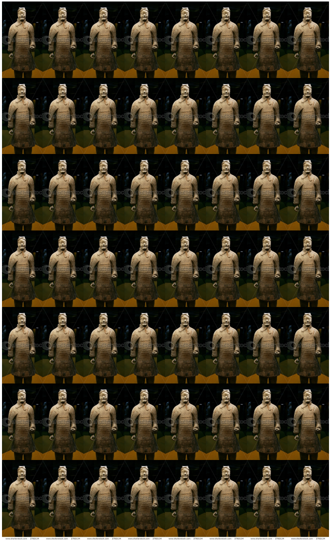
Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem (CRT)



Chinese Remainder Theorem (CRT)



Chinese Remainder Theorem (CRT)

- Suppose gcd$(n_1, n_2) =$ gcd$(n_1, n_3) =$ gcd$(n_2, n_3) = 1$.
  Given $x \equiv a \bmod n_1$, $x \equiv b \bmod n_2$, and $x \equiv c \bmod n_3$
  There exists exactly one solution to $x \bmod n_1 \times n_2 \times n_3$
  Example: Given $x \equiv 2 \bmod 3$, $x \equiv 1 \bmod 5$, and $x \equiv 0 \bmod 7 \rightarrow$ Solve $x \bmod 105$
- Solution: (works only for small numbers).
  - Congruence class $0 \bmod 7$:

$$
\begin{array}{cccccccccccc}
7, & 14, & 21, & 28, & 35, & 42, & 49, & 56, & 63, & 70, & 77, & \ldots \\
1, & 2, & 0, & 1, & 2, & 0, & 1, & 2, & 0, & 1, & 2, & \ldots \\
2, & 4, & 1, & 3, & 0, & 2, & 4, & 1, & 3, & 0, & 2, & \ldots
\end{array}
$$

Gauss' Algorithm for CRT

- Simultaneous congruences for general case
  - $x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, …, $x \equiv a_k \bmod n_k$ has a unique solution modulo $n_1 \times n_2 \times \ldots \times n_k$
  - $x \mod (n = n_1 \times n_2 \times \ldots \times n_k)$
- Gauss' algorithm:

$x = \sum_{i=1}^{k} a_i N_i M_i \bmod n$, where

$N_i = n/n_i$ and $M_i = {N_i}^{-1} \bmod n_i$

Example 1/2

- Solve
  - $x \equiv 2 \bmod 3$, $x \equiv 1 \bmod 5$, and $x \equiv 0 \bmod 7$
  - $a_1 = 2$, $a_2 = 1$, $a_3 = 0$
  - $n_1 = 3$, $n_2 = 5$, $n_3 = 7$
  - $n = 3 \times 5 \times 7 = 105$
- N_i for $i = 1, 2, 3$
  - $N_1 = n/n_1 = 105/3 = 35$
  - $N_2 = n/n_2 = 105/5 = 21$
  - $N_3 = n/n_3 = 105/7 = 15$
- M_i for $i = 1, 2, 3$

Example 2/2

- M_i for $i = 1, 2, 3$
  - $M_i = {N_i}^{-1} \bmod n_i$
  - $n_1 = 3,\ n_2 = 5,\ n_3 = 7$
  - $N_1 = 35,\ N_2 = 21,\ N_3 = 15$
  - $M_1 = {N_1}^{-1} \bmod n_1 = 35^{-1} \bmod 3 = 2$
  - $M_2 = {N_2}^{-1} \bmod n_2 = 21^{-1} \bmod 5 = 1$
  - $M_3 = {N_3}^{-1} \bmod n_3 = 15^{-1} \bmod 7 = 1$
- $x = a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3$
  - $a_1 = 2,\ a_2 = 1,\ a_3 = 0$
  - $x = 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 0 \cdot 15 \cdot 1 \bmod 105$
  - $x = 161 \bmod 105 = 56.$

CRT has a very important application in RSA cryptography

Think of performing $m^d \bmod n$ where
$n = p \times q$

Modular Exponentiation

- $m^e \bmod n$
- Example: $2^{1234} \bmod 789$,
- Naïve method:
  - Compute 2^{1234} first
  - $(2.95811224608098629060044695716 1 \times 10^{371})$
  - then reduce the result modulo 789.
  - Is it practical (possible)?
- Practical method: Use binary expansion of the exponent.
- $1234 = (10011010010)_2$

Binary Left-to-Right Algorithm

Algorithm 2 Binary Left-to-Right Algorithm

Input: $1 < a < n$ and $e \geq 1 (e = e_{k-1}, \ldots, e_1, e_0)$
Output: $x \equiv a^e \bmod n$

```
x := 1
for i = k − 1 downto 0 do
    x := x × x mod n
    if e_i = 1 then
        x := x × a mod n
    end if
end for
return x mod p
```

Modular Exponentiation Example

$2^{1234} \bmod 789$, $1234 = (10011010010)_2$, $x = 1$

i	e_i	Squaring $x \cdot x$	Multiplication $2 \times x$
10	1	$x = 1 \cdot 1 = 1$	$x = 1 \cdot 2 = 2$
9	0	$x = 2 \cdot 2 = 4$	–
8	0	$x = 4 \cdot 4 = 16$	–
7	1	$x = 16 \cdot 16 = 256$	$x = 256 \cdot 2 = 512$
6	1	$x = 512 \cdot 512 = 196$	$x = 196 \cdot 2 = 392$
5	0	$x = 392 \cdot 392 = 598$	–
4	1	$x = 598 \cdot 598 = 187$	$x = 187 \cdot 2 = 374$
3	0	$x = 374 \cdot 374 = 223$	–
2	0	$x = 223 \cdot 223 = 22$	–
1	1	$x = 22 \cdot 22 = 484$	$x = 484 \cdot 2 = 179$
0	0	$x = 179 \cdot 179 = 481$	–

Binary Right-to-Left Algorithm

Algorithm 3 Binary Right-to-Left Algorithm

Input: $1 < a < n$ and $e \geq 1$
Output: $x \equiv a^e \mod n$

$x := 1$, $y := a$
while $e \neq 0$ **do**
    if e is odd **then**
        $x := x \times y \mod n$
    end if
    $y := y \times y \mod n$
    $e := e >> 1$
end while
return $x \mod p$

- If p is a prime and p does not divide a, then

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

Pierre de Fermat (1601 or 1607 or 1608 - 12 January 1665)

Euler's Theorem

- If $gcd(a, n) = 1$, then

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

  where $\phi(n)$ is defined as the number of integers $1 \leq a \leq n$ such that $gcd(a, n) = 1$ and called as Euler's ϕ-function.
- $\phi(p) = (p - 1)$

Leonhard Paul Euler
(15 April 1707 -
18 September 1783)

Euler's Totient Function

- If $n = p \cdot q$ then $\phi(n) = (p-1) \cdot (q-1)$ (prove this)
- If p is prime and $n = p^r$, then:

$$\phi(p^r) = \left(1 - \frac{1}{p}\right) p^r$$

we must remove every p^{th} number in order to get the list of a's with $gcd(a, n) = 1$
In general case any integer can be written as

$$n = \prod_{i=1}^{t} {p_i}^{a_i} \qquad \phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Examples

- Example 1: $2^{10} \bmod 11$
  - $2^{10} \equiv ? \mod 11$
- Example 2: Compute $5^{-1} \bmod 11$
  $5^{10} = 5 \times 5^9 \equiv 1 \bmod 11$
  $5^{-1} \equiv 5^9 \bmod 11 \equiv 9 \bmod 11.$
- Example 3: $\phi(10) = ?$
- Example 4: Compute $2^{43210} \bmod 101$
  We know $2^{100} \equiv 1 \bmod 101 \rightarrow$
  $2^{43210} \mod 101 \equiv$

Important Principle

- Let a, n, x, y be integers with $n \geq 1$ and $gcd(a, n) = 1$.
  If $x \equiv y \bmod \phi(n)$ then
  $$a^x \equiv a^y \bmod n.$$
  Proof: $x = y + k \times \phi(n)$ from congruence relation.
  Then
  $a^x = a^{y+\phi(n)k} \equiv a^y \left(a^{\phi(n)}\right)^k \equiv a^y 1^k \equiv a^y \bmod n$
  In other words, if you work $\mathrm{mod} n$ in the base, you should work $\mathrm{mod} \phi(n)$ in the exponent.

Example

- Compute $3^{4012} \bmod 100$.
- Solution 1:
  $3^{4012} \equiv 41 \bmod 100$.
- Solution 2:
  $\phi(100) = 100 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{5}) = 40$.
  $4012 \equiv 12 \bmod 40$
  $3^{4012} \equiv 2^{4012 \bmod 40} \bmod 100$
  $\equiv 3^{12} \bmod 100$
  $\equiv 41 \bmod 100$.

Group

- An algebraic structure consisting of
  - a set together with one operation
  - A set of axioms should hold
    - closure, associativity, identity and invertibility.
- Example:
  - The set of integers $\mathbb{Z}$ which consists of the numbers
    - $\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$
    - Operation is addition, "$+$".
    - Prove that axioms hold
  - Set of numbers $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$
    - Operation is the modular multiplication (with prime p)
- The number of elements in a finite group is the *order* of the group; e.g., $|\mathbb{Z}_p^*| = p - 1$

Primitive (Roots) Elements

- Consider powers of $3 \bmod 7$:
  $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$
- Powers of 3 generate all nonzero elements of the congruence class $\bmod 7$.
- Such elements are called primitive elements or multiplicative generators in the congruence class.
- If p is a prime, there are $\phi(p-1)$ primitive elements $\bmod p$.
- Let g be a primitive element for the prime p. Then if n is an integer, then $g^n \equiv 1 \bmod p$ if and only if $n \equiv 0 \bmod p-1$.

Primitive Root Modulo n

- If n is a positive integer
  - the congrunce classes coprime to n form a group with multiplication modulo n as the operation;
  - denoted by $\mathbb{Z}_n^*$.
  - Also called as the group of primitive classes $\mathrm{mod} n$.
- A primitive root modulo n is any number g
  - with the property that any number coprime to n is congruent to a power of $g \bmod n$.
  - If g is a primitive root $\mathrm{mod} n$ and $gcd(a, n) = 1$, then there is an integer k such that $g^k \equiv a \bmod n$.
  - k is called the **index** of a.

Square Roots Modulo n

- Suppose $y = x^2 \bmod n$, where $n = p \times q$, has a solution.
- If the factorization of n is known, the equation can be solved quite easily.
  - Conversely, if we know all the solutions, then it is easy to factor n.
- Proposition: Let $p \equiv 3 \bmod 4$ be prime and let y be an integer. Let $x = y^{(p+1)/4} \bmod p$.
  1. If y has square roots $\bmod p$, then the square roots of $y \bmod p$ are $\pm x$.
  2. If y has no square root $\bmod p$, then $-y$ has a square root $\bmod p$, and the square roots of $-y \bmod p$ are $\pm x$.

Examples: Square Roots Modulo n

- Example: Find the square root of $5 \bmod 11$.
  $\frac{(p+1)}{4} = 3 \rightarrow 5^3 \bmod 11 = 4$.
  Then ± 4 are square roots of $5 \bmod 11$.
- Example: Find the square roots of $2 \bmod 11$.
- Square roots for composite modulus.
- Example: $x^2 \equiv 71 \bmod 77$
  $77 = 7 \times 11 \rightarrow x^2 \equiv 1 \bmod 7$ and $x^2 \equiv 5 \bmod 11$
  $\rightarrow x \equiv \pm 1 \bmod 7$ and $x \equiv \pm 4 \bmod 11$
  Solve the rest using CRT.

Square Roots Modulo n

- Four solutions:
  1. $x \equiv 1 \bmod 7$ and $x \equiv 4 \bmod 11$
     $\rightarrow x \equiv 15 \bmod 77$
  2. $x \equiv 1 \bmod 7$ and $x \equiv -4 \bmod 11$
     $\rightarrow x \equiv 29 \bmod 77$
  3. $x \equiv -15 \bmod 77$ and
  4. $x \equiv -29 \bmod 77$
- An important property
  - $x = \pm a, \pm b$ of $y = x^2 \bmod n$ where $n = p \times q$
  - $a \equiv b \bmod p$ and $a \equiv -b \bmod q$.

Important Question

- Can we factor n if we know all four solutions?
- Let $n = p \times q$ be the product of two primes and we know the four solutions $x = \pm a, \pm b$ of $x^2 \equiv y \bmod n$.
- We know that $a \equiv b \bmod p$ and $a \equiv -b \bmod q$. Thus, $p|(a-b)$ and $q \nmid (a-b)$. This means that $gcd(a-b, n) = p$. This is a nontrivial factor of n.
- Result:
  - Computing square root modulo n (where $n = p \times q$) is as hard as factorization

Subgroup

- A subset $\mathbb{H}$ of a group $\mathbb{G}$ can form a subgroup under the same operation
- **Lagrange Theorem**: The order of a subgroup divides the order of the group
- Example: $\mathbb{Z}_{11}^{*} = \{1, \ldots, 10\}$, where $|\mathbb{Z}_{11}^{*}| = 10$
  - $\mathbb{H} = \{1, 3, 4, 5, 9\}$ is a subgroup of $\mathbb{Z}_{11}^{*}$.

$\times \mod 11$	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

;

Finite Fields

- Two operations defined in a field:
  - addition (subtraction) and multiplication.
  - Since every non-zero element has a multiplicative inverse we can also define the division operation.
- If p is a prime, $\{0, 1, \ldots, p-1\}$ forms a finite field.
- $\mathbb{F}_p$ or $GF(p)$ to denote prime finite fields.
- GF is read as Galois field after a famous French Mathematician, Évariste Galois.
- Is set of integers a field?
- Give an example of infinite field

Évariste Galois
1811 - 1832

A Special Class of Finite Field (Binary Extension Field)

- Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ be an irreducible binary polynomial (i.e., $a_i \in \{0, 1\}$ $0 \leq i \leq n-1$).
- No binary polynomial of degree $n-1$ or less divides $f(x)$
- Using $f(x)$, we can construct *binary extension field* $GF(2^n)$ or $\mathbb{F}_{2^n}$.

Binary Extension Fields

- Example: Irreducible polynomial $x^3 + x + 1$ can be used to construct $GF(2^3)$.
- A simple method to construct this field is to find all the binary polynomials whose degrees are smaller than the degree of the irreducible polynomial $(n = 3)$.
- $GF(2^3) = \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$
- In computer we can use binary strings to represent these elements as
  $GF(2^3) = \{000, 001, 010, 011, 100, 101, 110, 111\}$

Operations in $GF(2^n)$

- Addition is an operation that act on the corresponding coefficients of the two polynomials when the polynomial representation is used.
- Example: $(x+1)+(x^2+1) = x^2+x$
- Subtraction is identical to the addition.
- Multiplication is done by using polynomial arithmetic when the polynomial representation is used. Two steps are involved:
  1. Polynomial multiplication
  2. Reduction with irreducible polynomial

- Example: $(x+1) \times (x^2+1)$ in $GF(2^3)$ with x^3+x+1

  Step 1: x^3+x^2+x+1 which is not the element of $GF(2^3)$ then a reduction step is necessary

  Step 2: The remainder of the following division is the result:

  $\frac{x^3+x^2+x+1}{x^3+x+1} \to x^2$.

Division in $GF(2^n)$

- Every non-zero element has a multiplicative inverse.
- i.e. for every element of $GF(2^n)$, $a(x)$, there exists $b(x)$ such that $a(x) \times b(x) \equiv 1 \bmod f(x)$.
- Thus the division by a non-zero element of $GF(2^n)$ is defined.

Primitive Polynomials and Elements

- The root of some of the irreducible polynomials can be used to construct the binary extension field.
  - Namely, its powers generate all nonzero elements of the field.
- Example: $f(x) = x^4 + x + 1$
- Let $f(\alpha) = 0$
- Then $\alpha^4 + \alpha + 1 = 0 \rightarrow \alpha^4 = \alpha + 1$.

Primitive Polynomials and Elements

$$f(x) = x^4 + x + 1 \to \alpha^4 + \alpha + 1 = 0 \to \alpha^4 = \alpha + 1.$$

0	$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$
$\alpha^0 = 1$	$\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 1$
α	$\alpha^9 = \alpha^3 + \alpha$
α^2	$\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$
α^3	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 = \alpha + 1$	$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$
$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha$
	$\alpha^{15} = \alpha^4 + \alpha = \alpha + 1 + \alpha = 1$

Primitive Polynomials and Elements

- Such polynomials are called primitive polynomials while the root of a primitive polynomial is called primitive element.
- Example: $f(x) = x^4 + x^3 + x^2 + x + 1$ is not a primitive polynomial.