1. Euler function

$$\varphi(n) = \operatorname{len}(\{1, 2, 3..n\}, \gcd(k, n) = 1)$$

Phi is multiplicative function

$$\varphi(ab) = \varphi(a)\varphi(b)$$

$\varphi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1)$... Where p is prime number from factorization n.

Example

$$\varphi(54) = \varphi(2 * 3^3) = \varphi(2) * \varphi(3^3)$$

2. Euler theorem

a, n are coprime

$$\alpha^{\varphi(n)} \equiv 1 \bmod n$$

x coprime with n, a coprime wuth n -> x a coprime with n (there no gcd>1)

3. Modular arithmetics

3.1. Congruence

We say that 3 is congruent to 15 by modulo 12, written $15 \equiv 3 (\bmod 12)$

Coprime two integers GCD is 1.

3.2. Fermat's little theorem

Special case of euler theorem.

Theorem If p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p

$$a^p \equiv a \bmod p$$

If a is coprime to p.

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

3.3. Primitive root modulo

$a|b$ a divides b=> b/a = 0

Primitive root modulo n g is called primitive root modulo p if every a coprime number to n is congruent to a power of g modulo p.

$$\forall a \in Z : \gcd(a, p) = 1, \exists n : g^n = a \longrightarrow g \text{ is primitive root modulo}$$

N is not required to be prime. G is a *primitive root modulo n* if and only if g is a generator of the multiplicative group of integers modulo n.

3.4. P Group

3.4.1. How to check that group is cyclic

3.4.2. Theorem to check generator in p group

$\alpha \in Z_p^*$ is a generator of Z_p^* if and only if

$$\alpha^{\frac{p-1}{q}} \neg \equiv 1 \bmod p$$

For all primes q such that $q|(p-1)$

Task

Task find the all generators of Z_{11}^*

Let's begin with $p - 1 = 10$, 10 = 2*5.

Generator check condition for each divider of $(p - 1)$:

- $\alpha^5 \neg \equiv 1 \bmod 11$
- $\alpha^2 \neg \equiv 1 \bmod 11$

Solution is to check each element in group to match conditions.

3.4.3. How to count generators in group

Theorem let p be prime, that Z_p^* contains exactly $\varphi(p-1)$ generators.

3.4.4. How to find generator

3.4.5. Discrete logarithm in p

If $\mathrm{B} \in Z_p^*$, then $\mathrm{B} = g^x$ for some unique $0 \leq x \leq p - 2$. X is called the discrete logarithm of B to base g.

$g^x = \mathrm{B} \Rightarrow \log_g \mathrm{B} = x$ in Z

Problem find the integer x, such that

$$\log_g \mathrm{B} \text{ in } Z_p^*$$

The naive approach is exhaustive search: compute $g^x, g^2x, ...$ until B is obtained.

3.5. N Group

3.5.1. Theorem to check generator in n group

For $n \geq 1$, we consider Z_n^*

$$Z_n^* = \{k \in \{1, ..., n\} / \gcd(k, n) = 1\}$$

$$\operatorname{len}(Z_n^*) = \varphi(n)$$

Z_n^* **is cyclic**(has at least one generator) when:

1. n=2 or 4
2. $n = p^x, x \in \{1, 2...\}$
3. $n = 2p^x, x \in \{1, 2...\}$

Theorem to check generator

Assume Z_n^* is cyclic. $\alpha \in Z_n^*$ is a generator if and only if

$$\alpha^{\frac{\varphi(n)}{p}} \neg \equiv 1 \bmod n$$

For each prime p divisor of $\varphi(n)$

3.5.2. How to count generators in group

Theorem if Z_n^* is cyclic, then it has $\pi(\pi(n))$ generators.

3.5.3. Discrete logarithm in n

If $\mathrm{B} \in Z_n^*$, then $\mathrm{B} = g^x$ for some unique $0 \leq x \leq p - 2$. X is called the discrete logarithm of B to base g.

Example

Find $\log_{13} 47$ in Z_{50}^*

1. Check Z_{50}^* is cyclic(e.g. has generators)
2. Check g 13 is generator.(requires find $\varphi(n)$)
3. Start to calculate elements.(exhaustive search)

4. Algorithms for computing discrete algorithms

1. Brute force
2. Shank's baby-step giant-step method

4.1. Some equations

$$3\mathrm{B} \bmod 13 = 1 \Rightarrow 3B \equiv 1 \bmod 13$$

$$(ab) \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$$

4.2. Core Equation for DH

$$y_1 = (a^{x_1} \bmod p)^{x_2} \bmod p = a^{x_1 x_2} \bmod p$$

Some modular arithmetics to proof:

$$y_1 = (a^{x_1} \bmod p)^{x_2} \bmod p = ((a \bmod p)^{x_1} \bmod p)^{x_2} \bmod p =$$

Reduce extra modulo due to modulo properties:

$$(a \bmod p)^{x_1} \bmod p = a^{x_1} \bmod p$$

Continue:

$$= (a \bmod p)^{x_1 x_2} \bmod p$$

$$= a^{x_1 x_2} \bmod p$$

4.3. Factorization problem

For example RSA relies on difficulty of factoring the product of two large prime numbers.

But for this need to determine or find large prime number.

Determine if number is prime:

1. Simple methods(advanced brute force, without 2,3 and maybe some memoization,etc)
2. Probabilistic tests(all primes + some non primes - never FN, but sometimes FP)

4.4. Modular multiplicative inverse

Algorithm Modular Inverse using Extended Euclidean Algorithm

check why it works

If a is coprime to n

Problem: $ax \equiv 1 \bmod n$

$ax + my = \gcd(a, m)$

$$x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1$$

While $a > 1$:

$$q = \left[\frac{a}{n}\right]$$

$$(a, n) = (n, a \bmod n)$$

$$(x_0, x_1) = (x_1, x_0 - qx_1)$$

$(y_0, y_1) = (y_1, y_0 - qy_1)$ (may be omitted when find modular multiplicative inverse)

Next: if $x_0 < 0$, then $x_0 = x_0 + n$

4.5. Bezout equality

$$\exists m, n \in Z : md + nd = d$$

$$(m + n) = 1$$

$$\exists \gcd(a, b) = d \longrightarrow \exists x, y : md = ax; nd = by;$$

Why x and y do exist?

$$ax + by = \gcd(a, b)$$

$$\exists k, l : a = kd, b = ld$$

Let's divide equation by d:

$$kdx + ldy = d \longrightarrow kx + ly = 1$$

we know k and l

$$k = \frac{a}{d}; l = \frac{b}{d};$$

$$kx + ly = 1 \longrightarrow y = \frac{1 - kx}{l}$$

$$l \neq 0; k, x \in Z : kx \in Z \longrightarrow y \text{ can be solved}$$

In the end we have endless count of solutions with formula:

$$y\left(\frac{b}{d}\right) = \left(1 - \left(\frac{a}{d}\right)x\right); ax + by = \gcd(a, b)$$

If one pair of (x,y) was found:

$$\left(x - k\left(\frac{b}{d}\right), y + k\left(\frac{a}{d}\right)\right)$$

For case of gcd = 1:

$$ax + by = 1$$

4.6. Proof of gcd equality

$$S \neg \emptyset \rightarrow \exists \min(n) \in S$$

x, y - are Bezout's coefficients

Having a, b with $\gcd(a, b) = d$ and $ax + by = d$

Prove that x, y exists and $ax + by = d$, d is min positive integer of this combination

Proof Suppose that we have set S with smallest element d.

1. Prove that d is a divisor of a,b and
2. for any common divisor c $c \leq d$

1. Let's divide a on d: $a = dq + r, 0 \leq r < d$

$$r = a - dq$$

$$r = a - (ax + by)q$$

$$r = a(1 - x) - b(yq)$$

Thus:

$$r = an + bm, \text{ where: } n = 1 - x, m = -(yq)$$

This implies that $r \in S, S : \{ax + by = d; \exists x, y \in Z\}$

Now we have

$$0 \leq r < d; r \in S; d \text{ is min in} S$$

Contradiction. Min element d from S is divisor of a, b (b by analog proof).

2. For any common divisor c $c \leq d$

Let c be divisor of a, b -> $ax + by = d$ a = c k b = c l

$$cxk + cyl = d$$

$$c(xK + yl) = d; (xK + yl) \geq 1 \rightarrow d \geq c \rightarrow d \text{ is the greatest divisor}$$

5. Find gcd

GCD - greatest common divisor

5.1. Euclidean algorithm

Based on the principle

$$\gcd(a, b) = \gcd(a - b, b), \text{if a} > \text{b}$$

Example:

$$\gcd(112, 256) = \gcd(112, 144) = \gcd(32, 112) = \gcd(32, 80)$$

$$= \gcd(48, 32) = \gcd(16, 32) = \gcd(16, 16) = 16$$

Proof let's assume:

$$\exists m : a = d * m$$

$$\exists n : b = d * n$$

$$a - b = d(m - n) \longrightarrow a - b \equiv d$$

A more efficient way is to use modulo operation for bigger element by smaller.

Proof let's assume:

$$\exists m : a = d * m$$

$$\exists n : b = d * n$$

$$\gcd(a, b) = \gcd(bk + a \bmod b, b)$$

As we know $\gcd(a, b) = \gcd(a - b, b)$, applying recursively we obtain equation:

$$\gcd(a, b) = \gcd(a - (kb), b) = \gcd(a \bmod b, b)$$

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

But that's not enough. Need to proof:

1. r_{n-1} is a common divisor of a,b
2. r_{n-1} is a gcd

Proof:

1. Is proved above. $r_{n-1} = c; c \leq \gcd \rightarrow r_{n-1} \leq \gcd$
2. Suppose we have common divisor c, which divides a, b; a -b = $kc - lc$ -> c divides a-b, divides each r_n.

Thus $r_n = (k - l)c$. Therefore $\forall c, c|a; c|b : c|r_n$(c<=r_n) -> r_n is gcd

5.2. Extended euclidean algorithm

a is coprime to b

$$ax + by = \gcd(a, b)$$

Why a and b should have gcd = 1; Because if not: a cannot have inverse.

Suppose that gcd is not 1:

$$ab \equiv 1 \bmod m$$

$$ab - 1 \equiv 0 \bmod m$$

$$a = gk; m = gl;$$

$$(gk)b \equiv 1 \bmod (gl)$$

$$kb \equiv \frac{1}{g} \bmod l$$

$$\frac{1}{g} \neg \in Z * . \Rightarrow \neg \exists b$$

6. Other

6.1.1. Division theorem

For every natural number m and positive natural number n, there exists a unique pair of integers q and r such that

$q \geq 0, 0 \leq r < n$, and $m = q \cdot n + r$

6.2. Fundamental arithmetics theorem

$$N = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$$