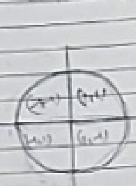
Jacobi Symbol

$$J\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(L\left(\frac{a}{p_i}\right)\right)^{e_i}$$

$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$

$\left(L\left(\frac{a}{p}\right), L\left(\frac{a}{q}\right)\right)$



$n = pq$

⇒ Jacobi Symbol Computation

(i) $M \equiv n \bmod N$ (odd)

$$J\left(\frac{M}{N}\right) = J\left(\frac{n}{N}\right)$$

(ii) $$J\left(\frac{2}{N}\right) = \begin{cases} +1 & 8k+1 = N \\ -1 & 8k+3 = N \end{cases}$$

(iii) $$J\left(\frac{a \cdot b}{N}\right) = J\left(\frac{a}{N}\right) \cdot J\left(\frac{b}{N}\right)$$

Gauss Quadratic Reciprocity formula

(iv) $$J\left(\frac{N}{M}\right) \times J\left(\frac{M}{N}\right) = (-1)^{\frac{(M-1)(N-1)}{4}}$$

1 2 3 4 5 (10)

001
010
011
100
101

$\boxed{a_i = 2^x + 2^y = 2}$

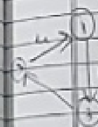
Group $(S, *)$

(i) closure $a, b \in S$ $a * b \in S$

(ii) associativity $a * (b * c) = (a * b) * c$

(iii) inverse $a \in S$, then $b \in S$

$a * b = e$



(iv) $e \in S$, $a * e = a$

Identity

$2^y(2^{x-y} - 1)$

(v) $a * b = b * a$ (Abelian group) If it holds at every $a, b \in S$

$Z_n^* = \{x \mid 1 \le x \le n-1 \quad \gcd(x, n) = 1\}$

op = multiplication

$|aZ_n^*| = |Z_n^*|$

$a\alpha \ne b\beta$ because a^{-1} exists for $\alpha \ne \beta$

$|aZ_n^*|$ would have 1 ⇒ inverse exists

$a(u_i - u_j) \equiv 0 \bmod n$

~~$a \mid n$~~

$a \nmid n$ or $n \mid u_i$ or $n \mid (u_i - u_j)$

Both are not possible

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

$\phi(n) = (p-1)(q-1)$ if $n = pq$

$n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ $\phi(n) - 1$

Date
Page

* $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$S = \{1, 2, 4\}$ is also valid group
subgroup

Lagrange's theorem
⇒ Cardinality of a subgroup divides the cardinality of a group

$\{a, a^2, a^3, \ldots, a^{k} = 1\}$

cyclic group generated by a
size = k

not possible
(because of a^{-1})

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

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

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

Randomly pick $a < n$

$\gcd(a, n) = 1$?

$a^{n-1} \bmod n = 1$? if not not prime.

$a^{n-1} \bmod n = 1$

Date
Page

1 2 4 5 1 2 4 5

k=1 ~~1~~ 2 ③ 4 5 6 7 8 9

k=2 ~~2~~ ~~5~~ 6 7 ~~8~~ ~~9~~

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

k=3 ~~7~~ ~~15~~ $\boxed{11}$ 12 13

$a^{2\frac{p-1}{2}} \bmod p = 1$

$a^{\frac{p-1}{2}} \bmod p = 1$ or -1

$+1 \rightarrow \left(\frac{a}{p}\right) = +1$

$-1 \rightarrow \left(\frac{a}{p}\right) = -1$

Prime number generation

$\boxed{1}$ . . . . $\boxed{1}$

fill middle digits randomly, check for primes if not repeat

$\pi(n) \approx c \cdot \frac{n}{\log_e n}$

no. of primes $< n$

How many primes $\left(\frac{2^{1024}}{1024} - \frac{2^{1023}}{1023}\right)$

$\approx \frac{2^{1023}}{2^{10}}$

* Public Key Cryptography (Asymmetric key crypto)

1976 Diffie & Martin Hellman
New dir in crypto

So far

$A \xrightarrow{f(m)} B$ $f^{-1}(m) = m$

* OWF

$x \xrightarrow{\text{easy}} f(x)$, $f(x) \xrightarrow{\text{hard}} x$

* OWF with trapdoor

$x \xrightarrow{\text{easy}} f(x)$, $f(x) \xrightarrow{\text{hard}} x$

easy if you know trapdoor

order of element

$g^{O(g)} = 1$

Cyclic Group $G = \langle g \rangle$ order of element $\lceil \frac{O(g)}{2} \rceil + 1$

$= (g, g^2, g^3, \ldots g^{O(g)})$

g^i will generate same G
if $\gcd(g^i, O(g)) = 1$

$\boxed{\text{Given } (G, g, g^i) \text{ find } i}$ Hard

given (g, i) g^i is easy

but (g, g^i) finding i is hard → Discrete Log Problem

(True for some cyclic grps only)

Alice	$G = \langle g \rangle$	Bob
chooses i randomly		chooses j randomly
g^i		g^j
$(g^j)^i$		
(Key)		$(g^i)^j$

Diffie Hellman key exchange

$(g, g^i, g^j) \xrightarrow{\text{DHP}} g^{ij}$ DHP $\leq_p$ DLP

CDH Computational DHP

$((g^i, g^j, g^{ij}), (g^i, g^j, g^k))$

Decide which tuple contains g^{ij}

DDH $\leq_p$ CDH $\leq_p$ DLP

(g^i, g^j, g^k)
$k = ij$? Decisional DHP

GCHQ

RSA (Rivest - Shamir - Adleman)

$Z_n^* = \{ x \mid 1 < x < n \quad \gcd(x, n) = 1 \}$

where $n = p \times q$, $\gcd(e, \phi(n)) = 1$

RSA permutation

$f(x) = x^e \bmod n$

Inverse permutation

secret $d = e^{-1} \bmod \phi(n)$

$ed \equiv 1 \bmod \phi(n)$

Public	Secret
$n = p \times q$	p, q
	$\phi(n)$
e	d

if $x \in Z_n^*$

$\boxed{\gcd(x, n)}$

Enc(x) = $x^e \bmod n$

Dec(c) = $c^d \bmod n$

$= (x^e \bmod n)^{d} \bmod n$

$= x^{ed} \bmod n$

$= x^{1 \bmod \phi(n)} \bmod n$

$= x^{k\phi(n)+1} \bmod n$

$= (x \bmod n)(x^{k\phi(n)} \bmod n)$

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

$\Pr(\text{Bad } x) = 1 - \frac{\phi(n)}{n}$

$= 1 - \frac{(p-1)(q-1)}{pq}$

$= \frac{p+q-1}{pq} \le \left(\frac{1}{2^{500}}\right)$

even if $x \notin Z_n^*$ $\quad p \cdot x_1 / q \cdot x_1$

$x^{ed} \bmod n = x$ $\quad x \in$ (Use CRT)

$(p \cdot x_1)^{ed} \bmod n \quad n = pq$

$(p \cdot x_1)^{ed} \bmod p = 0$

if $(x, p) = 1$ $\quad$ if $\gcd(x_1, p) = 1$

$x^{p-1} \bmod p = 1$

$x^{1 + k(p-1)(q-1)} \bmod p = x$

$x^{1 + k(p-1)(q-1)} \bmod q = 0$