Outline

Theoretical complexity comparison

Quadratic Residues

Problems

Discrete logarithm: Group G, $g, h \in G$. Find x s.t.

$$g^x = h$$

Diffie-Hellman: Given $g \in \mathbb{Z}_p^*$ where p is odd prime and A, B such that

$$A = g^a \mod p$$

$$B = g^b \mod p.$$

Find g^{ab}.

Factoring: Given $N = pq$ where p and q are distinct odd primes. Find p, q

RSA problem: Given $N = pq$ where p and q are distinct odd primes, e such that $\gcd(e, (p-1)(q-1)) = 1$, and c. Find m such that

$$m^e \equiv c \mod N.$$

Square Root: Given $N = pq$, where p and q are distinct odd primes.

Find m such that

$$m^2 = C \mod N$$

Theoretical complexity comparison

$\boxed{\text{Problem A is no harder than problem B}}$

if an efficient algorithm to solve problem B can be used to solve problem A in polynomial time.

Reduce Problem A to Problem B

Examples.

① Diffie-Hellman is no harder than Discrete Logarithm

② RSA problem is no harder than Factoring.

Open question: Is Factoring no harder than RSA?

③ SquareRoot is no harder than Factoring

Factoring is no harder than SquareRoot.

Factoring and SquareRoot problems are polynomial-time equivalent.

Quadratic Residues

Definition: Given a group G, An element $y \in G$ is a quadratic residue (QR) if $y = x^2$ for some $x \in G$.

An element $y \in G$ that is not a quadratic residue is called quadratic non-residue. (QNR)

Example: $G = \mathbb{Z}_5^*$

$$QR = \{\underset{1^2}{\overset{\shortparallel}{1}}, \underset{2^2}{\overset{\shortparallel}{4}}\}$$

$$QNR = \{2, 3\}$$

Theorem: Given an abelian group G. The set of QR is a subgroup.

Notation: $G = \mathbb{Z}_n^*$

QR_n : set of quadratic residue modulo n

QNR_n : Set of quadratic non-residue modulo n.

Quadratic Residu Modulo prime $p > 2$

Observation : $|QR_p| = |QNR_p|$

$p = 5$
$p = 7$
$p = 11$

Theorem : For all $y \in QR_p$, there exists exactly two square roots.

proof : $\exists\, x$ s.t $y = x^2 \bmod p$.

So, x is a square root of y.

$(-x)^2 = x^2 = y \bmod p$,

so, $-x$ is a square root of y.

Is x is equal to $-x$? No. Because if $x = -x \bmod p$

then $2x \equiv 0 \bmod p$

but $2 \nmid p$ because p is odd prime.

We have shown that $x, -x$ are square roots of y.

could there be a third square root of y?

Suppose yes. Say x'.

$(x')^2 = y = x^2 \bmod p$

$p \mid x'^2 - x^2$

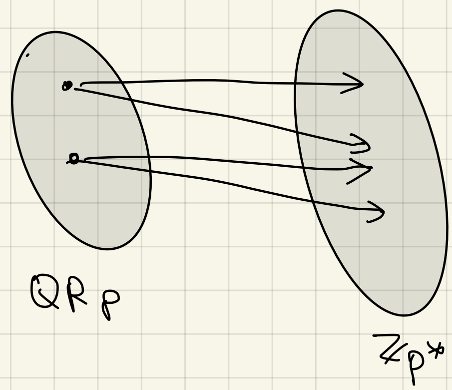
$p \mid (x' - x)(x' + x)$

$\rightarrow p \mid x' - x$ or $p \mid x' + x$

$\rightarrow x' \equiv x \bmod p$ $\quad \rightarrow x' \equiv -x \bmod p$

There can only be two square root of y.

Corollary: $|QR_p| = |QNR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$



Observation: Consider $\mathbb{Z}_p^* = \langle g \rangle$ where g is a generator.

$$\mathbb{Z}_p^* = \{ g^0, g^1, g^2, g^3, \dots, g^{\frac{p-1}{2}-1}, g^{\frac{p-1}{2}}, \dots, g^{p-2} \}$$

$$QR_p = \{ g^0, g^2, g^4, g^6, \dots g^{p-3}, g^0, \dots, g^{p-3} \}$$

multiply the exponent by 2 reduced modulo $p-1$.

Elements in QR_p is of the form g^i where i is even.

Elements in QNR_p is of the form g^i where i is odd.

Theorem: An element $x \in QR_p$ iff $x^{\frac{p-1}{2}} \equiv 1 \mod p$

An element $x \in QNR_p$ iff $x^{\frac{p-1}{2}} \equiv -1 \mod p$

---

proof: What could be the values of $x^{\frac{p-1}{2}} \mod p$?

$$\left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1 \mod p$$

$$x^{\frac{p-1}{2}} = 1, -1$$

Suppose $x \in QR_p$, $x = g^{2i} \mod p$ where $g \in \mathbb{Z}_p^*$

such that $ord(g) = p-1$

$$x^{\frac{p-1}{2}} = g^{2i\left(\frac{p-1}{2}\right)} = g^{(p-1)i} = 1 \mod p$$

Suppose $x^{\frac{p-1}{2}} \equiv 1 \mod p$.

Suppose $x = g^{2i+1}$

Since $x^{\frac{p-1}{2}} \equiv 1 \mod p$

then $g^{\frac{(2i+1)(p-1)}{2}} \equiv 1 \mod p$ ①

Because $ord(g) = p-1$, $g^{\frac{p-1}{2}} \not\equiv 1 \mod p$.

$g^{\frac{p-1}{2}} \equiv -1 \mod p$

$$\left(g^{\frac{p-1}{2}}\right)^{2i+1} \equiv -1 \mod p \quad ②$$

① contradicts ②.

Algorithm to check if $x \in QR_p$

Input: p, $x \in \mathbb{Z}_p^*$

compute $x^{\frac{p-1}{2}} \bmod p$.

If the result is 1, output x is QR_p

O/w, output x is QNR_p.

Running Time : polynomial.

Algorithm to compute square root of x given that $x \in QR_p$

$$x^{\frac{p-1}{2}} \equiv 1 \bmod p$$

$$x^{\frac{p-1}{2}} \cdot x \equiv x \bmod p$$

$$x^{\frac{p+1}{2}} \equiv x \bmod p$$

$$\left(x^{\frac{p+1}{4}}\right)^2 \equiv x \bmod p$$

So, $x^{\frac{p+1}{4}}$ is a square root of x

$-x^{\frac{p+1}{4}}$ is also a square root of x.

This only work when $\frac{p+1}{4}$ is an integer.

$p \equiv 3 \bmod 4$

When $p \equiv 3 \bmod 4$, if $x \in QR_p$, then $\pm x^{\frac{p+1}{4}} \bmod p$ are the square roots of x.

When $p \equiv 1 \bmod 4$, if $x \in QR_p$, no deterministic polynomial alg.

Jacobi Symbol

$$J_p(x) = \begin{cases} 1 & \text{if } x \in QR_p \\ -1 & \text{if } x \in QNR_p \end{cases}$$

An element $x \in QR_p$ iff $x^{\frac{p-1}{2}} \equiv 1 \mod p$

$\Updownarrow$

$J_p(x) = x^{\frac{p-1}{2}} \mod p$

Multiplicative property of $J_p(x)$

Theorem: $J_p(xy) = J_p(x) J_p(y)$

proof: $J_p(xy) = xy^{\frac{p-1}{2}} \mod p = J_p(x) J_p(y)$

$J_p(x) = x^{\frac{p-1}{2}} \mod p$

$J_p(y) = y^{\frac{p-1}{2}} \mod p$

Corollary: If $x, x' \in QR_p$, $y, y' \in QNR_p$

(a) $xx' \in QR_p$

(b) $yy' \in QR_p$ $\rightarrow$ $J_p(yy') = J_p(y) J_p(y')$

$= (-1)(-1)$

$= 1$

(c) $xy \in QNR_p$ $\rightarrow$ $J_p(xy) = J_p(x) J_p(y)$

$= (1)(-1)$

$= -1$