§20 Square roots in modular arithmetics.

§20.1. The case of odd prime p.

Let p be an odd prime.

Definition. Let $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod p$. a is a <u>quadratic residue</u> (QR) modulo p if the equation

$$x^2 \equiv a \pmod p$$

has solutions. Otherwise it is called quadratic non-residue (NR) modulo p.

Note: If $a \equiv 0 \pmod p$ then it is neither QR nor NR mod p.

If a is a QR mod p then $x^2 \equiv a \pmod p$ has exactly two solutions:

$$x \equiv \pm b \pmod p.$$

Q: How to check whether $a \in \{1, 2, \dots, p-1\}$ is a QR or not?

We can solve it with help of prim. roots and discrete logs.

Let g be a prim. root mod p.

$x \equiv g^i \pmod p$, $a \equiv g^k \pmod p$

$$x^2 \equiv a \pmod p \iff \underset{\substack{\uparrow \\ \text{even}}}{2i} \equiv k \pmod{\underset{\substack{\uparrow \\ \text{even.}}}{p-1}}$$

If k is odd the equation does not have solutions $\Longrightarrow a \equiv g^k \pmod p$ is NR.

If $k=2m$ is even then

$$2i \equiv k \pmod{p-1} \Longleftrightarrow i \equiv m \pmod{\tfrac{p-1}{2}}$$

$\Longrightarrow x \equiv g^m$ or $g^{m+\frac{p-1}{2}} \pmod p$ are solutions

$\Longrightarrow a \equiv g^{2m} \pmod p$ is a ~~prim. root~~. QR.

Problem: this method involves finding a prim. root and solving the DLP - very hard and practically useless for big p.

Lemma: a is a QR mod $p \Longleftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$

a is a NR mod $p \Longleftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Proof.

a is a QR mod $p \Longleftrightarrow a \equiv g^{2m} \pmod p$ where g is a prim. root.

$$\Longrightarrow a^{\frac{p-1}{2}} \equiv (g^{2m})^{\frac{p-1}{2}} \equiv g^{m(p-1)} \equiv 1 \pmod p.$$

a is NR mod $p \Longleftrightarrow a \equiv g^k \pmod p$, k is odd

$$\Longrightarrow a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \equiv (\underbrace{g^{\frac{p-1}{2}}}_{\equiv -1 \text{ (Check-Ex)}})^k \equiv (-1)^k \equiv -1 \pmod p.$$

$\boxtimes$

Example: $p=7$. Is 3 a QR?

$$3^{\frac{p-1}{2}} \equiv 3^3 \equiv 6 \equiv -1 \pmod 7 \Rightarrow 3 \text{ is a NR}.$$

Q (Square Root Problem): Given $a \in \{1, \dots, p-1\}$ is a QR, solve the equation
$$x^2 \equiv a \pmod{p}.$$

As before we can solve it with help of prim. roots and discrete logs - too long. We want something faster.

Easy case: $p \equiv 3 \pmod 4$. Then $\frac{p+1}{4} \in \mathbb{Z}$.

Lemma: Let p be prime, $p \equiv 3 \pmod 4$ and a is a QR mod p. Then $a^{\frac{p+1}{4}}$ is a solution of
$$x^2 \equiv a \pmod{p}.$$

Proof: $\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} \cdot a \equiv [a \text{ is a QR}]$
$$\equiv a \pmod{p}.$$
$\boxtimes$

Example: $p = 11$. Solve $x^2 \equiv 3 \pmod{11}$. $11 \equiv 3 \pmod 4$

Check whethe 3 is a QR:

$3^{\frac{p-1}{2}} \equiv 3^5 \equiv 1 \pmod{11} \Rightarrow 3$ is QR.

~~The~~ One solution is: $3^{\frac{p+1}{4}} \equiv 3^3 \equiv 5 \pmod{11}$

$\Rightarrow 5$ is a square root of $3 \pmod{11}$.

The general solution is $x \equiv \pm 5 \pmod{11}$.

General case: Let $p - 1 = 2^k \cdot m$ where $k \in \mathbb{Z}^+$, $m \in \mathbb{Z}$ is odd

(Easy case is when $k = 1$).

Algorithm for finding of a square root of a modulo p:

<u>Step 0</u>: Check if a is QR by checking if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

<u>Step 1</u>: Find $b \in \{1, 2, \dots, p-1\}$ such that

$$ord_p(b) = 2^k.$$

Method: find a NR r modulo p by checking $r^{2^{k-1}m} \equiv -1 \pmod{p}$. Do this by random search.

There are $\frac{p-1}{2}$ NR's so we should find such r quickly.

Take $b \equiv r^m \pmod{p}$.

Check: $b^{2^k} \equiv r^{2^k m} \equiv r^{p-1} \equiv 1 \pmod{p}$

$$b^{2^{k-1}} \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$\Rightarrow ord_p(b) \mid 2^k$ but $ord_p(b) \nmid 2^{k-1}$

$\Rightarrow ord_p(b) = 2^k.$

<u>Step 2</u>: We have that the numbers

$b^0, b^2, b^4, \dots, b^{2^k-2}$ are (2^{k-1})th roots of 1.

$\Rightarrow$ they are <u>all</u> roots of 1 of degree 2^{k-1}.

On the other hand a^m is also (2^{k-1})th root of 1

$\Rightarrow \exists\, j$ s.t. $b^{2j} \equiv a^m \pmod{p}$, $j \in \{0, 1, \dots, 2^{k-1}-1\}$

In other words $j = \frac{1}{2} \log_{b,p}(a^m)$.

Find this j (By Pohling-Hellman.

This is easy because the order is 2^{k}).

Step 3:

$x \equiv \pm b^j \cdot a^{-(m-1)} \pmod{p}$.