Quadratic Residue Modulo $N = pq$, p and q are distinct odd primes

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ $\qquad \varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$

$QR_{15} = \{1, 4\}$

$\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$

$x \mapsto (x \bmod 3, x \bmod 5)$

$1 \mapsto (1, 1)$

$4 \mapsto (1, 4)$

$\mathbb{Z}_3^* = \{1, 2\}$

$QR_3 = \{1\}$

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$QR_5 = \{1, 4\}$

Theorem: $QR_N \cong QR_p \times QR_q$

let $x_p = x \bmod p$

$x_q = x \bmod q$

if $x_p \in QR_p$ and $x_q \in QR_q$, then $x = (x_p, x_q) \in QR_N$

if $x \in QR_N$ then $x_p \in QR_p$ and $x_q \in QR_q$

proof: If $x_p \in QR_p$ and $x_q \in QR_q$, there exists a and b s.t $a^2 = x_p \bmod p$ and $b^2 = x_q \bmod q$.

Hence $(x_p, x_q) = (a^2, b^2)$ is a QR_N.

If $(x_p, x_q) \in QR_N$, there exist a and b s.t $(a, b) \cdot (a, b) = (a^2, b^2) = (x_p, x_q)$, hence $x_p \in QR_p$ and $x_q \in QR_q$

Theorem: If $x \in QR_N$, then x has four square roots.

proof: $x = (x_p, x_q)$

Any square root of x is of form (a, b)

such that a is square root of x_p

b is square root of x_q

There are two square roots of x_p.

two square roots of x_q.

In total, four square roots of (x_p, x_q)

Example: What is square root of 4 mod $15 = 3 \cdot 5$

$4 \longrightarrow (1, 4)$

square roots of 1 in $\mathbb{Z}_3^*$ is 1, 2

square roots of 4 in $\mathbb{Z}_5^*$ is 2, 3

square root of $(1, 4)$ is

$7 \longleftarrow (1, 2)$

$13 \longleftarrow (1, 3)$

$2 \longleftarrow (2, 2)$

$8 \longleftarrow (2, 3)$

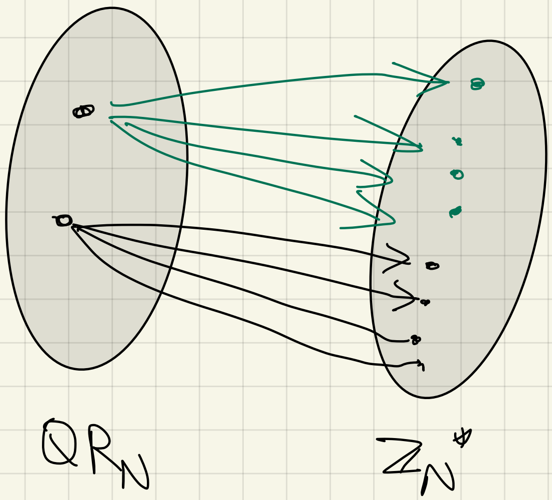
7, 13, 2, 8 are square roots of 4

none of these square roots are QR_N.

$p = 3$, $q = 5$ ($p \equiv 3 \bmod 4$ but $q \not\equiv 3 \bmod 4$)

In Homework 8, Question 5, when $p \equiv q \equiv 3 \bmod 4$, exactly one of the square root is a QR.

Corollary: $|QR_N| = \frac{1}{4} |\mathbb{Z}_N^*|$



Algorithm to check if an element is QR_N

Input: x, N

Output: QR is x is quadratic residue, QNR o/w.

Algorithm: Compute $J_p(x_p) = x_p^{\frac{p-1}{2}}$

$J_q(x_q) = x_q^{\frac{q-1}{2}}$

If $J_p(x_p) = J_q(x_q) = 1$ then output QR

o/w QNR.

Running Time: Polynomial

Algorithm to find square roots of QR_N

Input: N, x where $x \in QR_N$

Output: square roots of $x \bmod N$

Algorithm: Compute p and q such that $N = pq$

$$\boxed{\begin{array}{l} \text{Compute square roots of } x_p: \ a_1, a_2 \\ \text{Compute square roots of } x_q: \ b_1, b_2 \end{array}}$$

Output $(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)$

(after using CRT to convert (a, b) to $c \in \mathbb{Z}_N^*$)

$p \equiv 3 \bmod 4$, a_1, a_2 are $\pm x_p^{\frac{p+1}{4}} \bmod p$

$q \equiv 3 \bmod 4$, b_1, b_2 are $\pm x_q^{\frac{q+1}{4}} \bmod q$

Running Time: Polynomial if $p \equiv q \equiv 3 \bmod 4$.

Theorem

1. If factoring is easy, then it is easy to find square root modulo N.

2. If square root modulo N is easy, then it is easy to factor N.

---

2. Given N and x,

Suppose you can find all square roots of x mod N

x_1, x_2, x_3, x_4.

How to use these square roots to find p, q.

Example: $N = 15$

square roots of 4 is $7, -7, 2, -2$

Observation: Take the difference between two unrelated square roots:

$7 - 2 = 5$ has factor 5

$7 - (-2) = 9$ has factor 3

$2 - 7 = 10$ has factor 5

$2 - (-7) = 9$ has factor 3

Theorem: Let x_1, x_2 be the two square roots of x in $\mathbb{Z}_N^*$, such that

$x_1 \neq \pm x_2 \mod N$.

Either $\gcd(x_1 - x_2, N)$ or $\gcd(x_1 + x_2, N)$

is a prime divisor of N

proof: $x_1^2 = x_2^2 \mod N$

$N \mid (x_1^2 - x_2^2)$

$N \mid (x_1 - x_2)(x_1 + x_2)$

$pq \mid (x_1 - x_2)(x_1 + x_2)$

Since p is a prime, $p \mid x_1 - x_2$ or $p \mid x_1 + x_2$

case 1: $p \mid x_1 - x_2$.

If $q \mid x_1 - x_2$ then $pq \mid x_1 - x_2$ and hence $x_1 \equiv x_2 \mod N$

which contradics the orignal assumption.

so, $q \nmid x_1 - x_2$. Hence, $\gcd(N, x_1 - x_2) = p$

case 2: $p \mid x_1 + x_2$

If $q \mid x_1 + x_2$ then $pq \mid x_1 + x_2$ and hence $x_1 \equiv -x_2 \mod N$

which contradicts the orignal assumption.

so, $q \nmid x_1 + x_2$. Hence, $\gcd(N, x_1 + x_2) = p$

In fact, a little additional aguement will show that both $\gcd(x_1 - x_2, N)$ and $\gcd(x_1 + x_2, N)$ are prime divisors of N.