Quadratic Residues

An element $a \in \mathbb{Z}_n^*$ is a **quadratic residue mod** n if there is an $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv a \pmod{n}$.

Let QR(n) denote the set of quadratic residues modulo n.

The *quadratic residue problem:* Given $a \in \mathbb{Z}_n^*$, determine whether $a \in \text{QR}(n)$.

Example: with $n = 15$

k:	1	2	4	7	8	11	13	14
k^2 :	1	4	1	4	4	1	4	1

So $\mathrm{QR}(15) = \{1, 4\}$

Prime moduli

Theorem: Let p be an odd prime, $a \in \mathbb{Z}_p^*$.

1. $a \in \mathrm{QR}(p) \iff a^{(p-1)/2} \equiv 1 \pmod{p}$.

2. a has either 0 or 2 square roots.

Thus the quadratic residue problem is easy to solve modulo a prime.

Suppose $p \equiv 3 \pmod 4$. Then for every $a \in \mathbb{Z}_p^*$,

$$a \in \mathrm{QR}(p) \iff -a \notin \mathrm{QR}(p).$$

Thus (when $p \equiv 3 \pmod 4$) every quadratic residue has a unique square root which is also a quadratic residue. **The principal square root**.

In fact, the principal square root of a is $a^{(p+1)/4}$

Composite moduli

Let p and q be distinct odd primes. $n = pq$.

$a \in \mathrm{QR}(n) \iff a \,\%\, p \in \mathrm{QR}(p)$ & $a \,\%\, q \in \mathrm{QR}(q)$.

Note that if $n = pq$ then every quadratic residue has 4 square roots.

More generally, if we know the factorization of n, then the quadratic residue problem is easy.

Converse?

Theorem: Let n be an odd integer. There is an easily computable quantity $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ such that

$$\left(\frac{a}{n}\right) = 0 \iff \gcd(a, n) \neq 1$$

$$\left(\frac{a}{n}\right) = -1 \implies a \notin \mathrm{QR}(n)$$

$$\left(\frac{a}{n}\right) = 1 \implies ???$$

The Jacobi symbol

When p is prime, $\left(\frac{a}{p}\right) = a^{(p-1)/2} \,\%\, p$.

For $n = p_1 \cdot p_2 \cdots p_k$ (not necessarily distinct) we define $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$.

Example:

$$\left(\frac{66}{175}\right) = \left(\frac{66}{5}\right) \cdot \left(\frac{66}{5}\right) \cdot \left(\frac{66}{7}\right) = [1^{(5-1)/2} \,\%\, 5]^2 \cdot \left[3^{(7-1)/2} \,\%\, 7\right] = -1.$$

Computing the Jacobi symbol

1. $\left(\frac{m}{n}\right) = \left(\frac{m \,\%\, n}{n}\right)$
2. $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod 8 \\ -1 & \text{if } n \equiv \pm 3 \pmod 8 \end{cases}$
3. $\left(\frac{uv}{n}\right) = \left(\frac{u}{n}\right)\left(\frac{v}{n}\right)$

Gauss' law of quadratic reciprocity:
if m is odd then

$$4.\ \left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod 4 \\ \left(\frac{n}{m}\right) & \text{otherwise} \end{cases}$$

Example:

$$\left(\frac{66}{175}\right) \overset{3}{=} \left(\frac{2}{175}\right)\left(\frac{33}{175}\right) \overset{2}{=} 1 \cdot \left(\frac{33}{175}\right)$$
$$\overset{4}{=} \left(\frac{175}{33}\right) \overset{1}{=} \left(\frac{10}{33}\right) \overset{3}{=} \left(\frac{2}{33}\right)\left(\frac{5}{33}\right) \overset{2}{=} 1\left(\frac{5}{33}\right) \overset{4}{=}$$
$$\left(\frac{33}{5}\right) \overset{1}{=} \left(\frac{3}{5}\right) \overset{4}{=} \left(\frac{5}{3}\right) \overset{1}{=} \left(\frac{2}{3}\right) \overset{2}{=} -1$$

Let

$$\widetilde{\mathrm{QR}}(n) = \left\{ a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = 1 \;\&\; a \notin \mathrm{QR}(n) \right\}$$

"pseudosquares modulo n".

Sharper statement of the quadratic residue problem:

Given an odd n with $\left(\frac{a}{n}\right) = 1$, determine whether $a \in \mathrm{QR}(n)$ or $a \in \widetilde{\mathrm{QR}}(n)$.

Open problem: Is the quadratic residue problem easier than factoring?

Assumption: No

Coin-tossing By Email

Alice and Bob communicate only by email. They wish to toss a coin. Assume they don't trust each other.

Alice picks primes p and q, $n = pq$, $m \in \widetilde{\mathrm{QR}}(n)$. Tells n, m to Bob.

1. Alice picks random $r \in \mathbb{Z}_n^*$ and tosses coin $c \in \{0, 1\}$. Sends $z = m^c r^2 \,\%\, n$ to Bob.
2. Bob calls "heads" (i.e. $c = 0$) or "tails" ($c = 1$)
3. Alice announces result and sends p, q, r, c to Bob.