Introduction to Number Theory 2

Quadratic Residues

Definition: The numbers $0^2, 1^2, 2^2, \ldots, (n-1)^2 \bmod n$, are called **quadratic residues** modulo n. Numbers which are not quadratic residues modulo n are called **quadratic non-residues** modulo n.

Example: Modulo 11:

i	0	1	2	3	4	5	6	7	8	9	10
$i^2 \bmod 11$	0	1	4	9	5	3	3	5	9	4	1

There are six quadratic residues modulo 11: 0, 1, 3, 4, 5, and 9.

There are five quadratic non-residues modulo 11: 2, 6, 7, 8, 10.

Quadratic Residues (cont.)

Lemma: Let p be prime. Exactly half of the numbers in Z_p^* are quadratic residues. With 0, exactly $\frac{p+1}{2}$ numbers in Z_p are quadratic residues.

Proof: There are at most $\frac{p+1}{2}$ quadratic residues, since

$$\begin{aligned} & 0^2 \\ 1^2 &\equiv (p-1)^2 \pmod p \\ 2^2 &\equiv (p-2)^2 \pmod p \\ &\vdots \\ i^2 &\equiv (p-i)^2 \pmod p \qquad \forall i \\ &\vdots \end{aligned}$$

Thus, all the elements in Z_p span at most $\frac{p+1}{2}$ quadratic residues.

There are at least $\frac{p+1}{2}$ quadratic residues, otherwise, for some $i \neq j \leq \frac{p-1}{2}$ it holds that $i^2 = (p-i)^2 = j^2 = (p-j)^2$, in contrast to Lagrange theorem that states that the equation $x^2 - i^2 = 0$ has at most two solutions $\pmod p$.

Quadratic Residues (cont.)

Since Z_p^* is cyclic, there is a generator. Let g be a generator of Z_p^*.

1. g is a quadratic non-residue modulo p, since otherwise there is some b such that $b^2 \equiv g \pmod p$. Clearly, $b^{p-1} \equiv 1 \pmod p$, and thus $g^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$. However, the order of g is $p-1$. Contradiction.
2. $g^2, g^4, \ldots, g^{(p-1)} \bmod p$ are quadratic residues, and are distinct, therefore, there are at least $\frac{p-1}{2}$ quadratic residues.
3. $g, g^3, g^5, \ldots, g^{(p-2)} \bmod p$ are quadratic non-residues, since if any of them is a quadratic residue, g is also a quadratic residue.

QED

Euler's Criterion

Theorem: Let $p \neq 2$ be a prime, and let $a \in Z_p^*$. Then, a is a quadratic residue modulo p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Proof:

($\Rightarrow$) If a is a quadratic residue, there is some b such that $a \equiv b^2 \pmod p$. Thus,

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

Euler's Criterion (cont.)

($\Leftarrow$) If a is a quadratic non-residue: For any r there is a unique s such that $rs \equiv a \pmod p$, i.e., $s = ar^{-1}$, and there is no $r^* \neq r$ such that $s = ar^{*-1}$. Since a is a quadratic non-residue, $r \not\equiv s \pmod p$.

Thus, the numbers 1, 2, 3, $\ldots$, $p-1$ are divided into $\frac{p-1}{2}$ distinct pairs (r_1, s_1), (r_2, s_2), $\ldots$, $(r_{\frac{p-1}{2}}, s_{\frac{p-1}{2}})$, such that $r_i s_i = a$, and we get

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv r_1 s_1 r_2 s_2 \ldots r_{\frac{p-1}{2}} s_{\frac{p-1}{2}} \equiv \\ &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \pmod p \end{aligned}$$

by Wilson's theorem. QED

Quadratic Residues Modulo $n = pq$

Let p and q be large primes and let $n = pq$ (as in RSA).

Theorem: Let $m \in Z_n^*$. If m is a quadratic residue modulo n, then m has exactly **four** square roots modulo n in Z_n^*.

Proof: Assume $\alpha^2 \equiv m \pmod n$. Then

$\gcd(m, n) = 1 \Rightarrow \gcd(\alpha^2, n) = 1 \Rightarrow \gcd(\alpha, n) = 1 \Rightarrow \alpha \in Z_n^*$.

and since

$$m \equiv \alpha^2 \pmod n$$

then

$$\begin{aligned} m &\equiv \alpha^2 \pmod p \\ m &\equiv \alpha^2 \pmod q \end{aligned}$$

m has two square roots modulo p ($\alpha \bmod p$ and $-\alpha \bmod p$) and two square roots modulo q ($\alpha \bmod q$ and $-\alpha \bmod q$).

Quadratic Residues Modulo $n = pq$ (cont.)

Look at the systems of equations

$$\begin{aligned} x &\equiv \pm\alpha \pmod p \\ x &\equiv \pm\alpha \pmod q \end{aligned}$$

which represent four systems (one of each possible choice of $\pm$). Each system has an unique solution modulo n which satisfies

$$\begin{aligned} x^2 &\equiv m \pmod p \\ x^2 &\equiv m \pmod q \end{aligned}$$

and thus satisfies

$$x^2 \equiv m \pmod n$$

All the four solutions are roots of m modulo n.

These are all the roots. Otherwise there must be more than two roots either modulo p or modulo q.

QED

Quadratic Residues Modulo $n = pq$ (cont.)

Conclusion: Exactly a quarter of the numbers in Z_n^* are quadratic residues modulo n.

Legendre's Symbol

Definition: Let p be a prime such that $p \not| a$. **Legendre's symbol** of a over p is

$$\left(\frac{a}{p}\right) \triangleq \begin{cases} +1, & \text{if } a \text{ is a quadratic residue modulo } p; \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

By Euler:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Legendre's Symbol (cont.)

Properties of Legendre's symbol:

1. $a \equiv a' \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.
2. $\left(\frac{1}{p}\right) = \left(\frac{c^2}{p}\right) = 1 \qquad \forall c$.
3. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p = 4k+1; \\ -1, & \text{if } p = 4k+3. \end{cases}$

   Proof:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$
$$\equiv \begin{cases} (-1)^{\frac{4k+1-1}{2}} \equiv (-1)^{2k} \equiv 1, & \text{if } p = 4k+1; \\ (-1)^{\frac{4k+3-1}{2}} \equiv (-1)^{2k+1} \equiv -1, & \text{if } p = 4k+3. \end{cases}$$

Legendre's Symbol (cont.)

4. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

   (given without a proof).
5. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

   Proof:

   Let g be a generator modulo p. Then, $\exists i, a \equiv g^i \pmod{p}$ and $\exists j, b \equiv g^j \pmod{p}$. a is a quadratic residue iff i is even, b is a quadratic residue iff j is even, and ab is a quadratic residue iff $i+j$ is even. Thus, by Euler:

$$\left(\frac{ab}{p}\right) \equiv (-1)^{i+j} \equiv (-1)^i(-1)^j \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Legendre's Symbol (cont.)

6. The reciprocity law: if $p \neq q$ are both odd primes then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

   (given without a proof).

Jacobi's Symbol

Jacobi's symbol is a generalization of Legendre's symbol to composite numbers.

Definition: Let n be odd, and let $p_1, p_2, \ldots, p_k$ be the prime factors of n (not necessarily distinct) such that $n = p_1 p_2 \cdots p_k$. Let a be coprime to n. **Jacobi's symbol** of a over n is

$$\left(\frac{a}{n}\right) \triangleq \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

In particular, for $n = pq$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right).$$

Jacobi's Symbol (cont.)

Remarks:

1. $a \in Z_n^*$ is a quadratic residue modulo n iff the Legendre's symbols over all the prime factors are 1.
2. When Jacobi's symbol is 1, a is not necessarily a quadratic residue.
3. When Jacobi's symbol is -1, a is necessarily a quadratic non-residue.

Jacobi's Symbol (cont.)

Properties of Jacobi's symbol:

Let m and n be integers, and let a and b be coprime to m and n. Assume that n is odd and that the factorization of n is $n = p_1 p_2 \cdots p_k$.

1. $a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{1}{n}\right) = 1 \qquad \forall n$ (1 is a quadratic residue modulo any n).
3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

   Proof:

$$n = p_1 p_2 \cdots p_k$$
$$= ((p_1 - 1) + 1)((p_2 - 1) + 1) \cdots ((p_k - 1) + 1)$$

opening parentheses:

$$= \sum_{S \subseteq \{1,2,\ldots,k\}} \prod_{i \in S} (p_i - 1)$$

Jacobi's Symbol (cont.)

$$= \left[\sum_{\substack{S\subseteq\{1,2,\ldots,k\} \\ |S|\geq 2}} \prod_{i\in S} (p_i - 1) \right] + \sum_{i\in\{1,2,\ldots,k\}} (p_i - 1) + 1$$
$$= [(p_1 - 1)(p_2 - 1)\cdots(p_k - 1) + \ldots] + (p_1 - 1) + (p_2 - 1) + \ldots + (p_k - 1) + 1$$

where all the terms with $|S| \geq 2$ (in the brackets) are multiples of four, and all the $p_i - 1$ are even. Thus,

$$\frac{n-1}{2} \equiv \frac{(p_1-1)}{2} + \frac{(p_2-1)}{2} + \ldots + \frac{(p_k-1)}{2} \pmod 2,$$

and

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right)$$
$$= (-1)^{(p_1-1)/2}(-1)^{(p_2-1)/2}\cdots(-1)^{(p_k-1)/2}$$
$$= (-1)^{(p_1-1)/2+(p_2-1)/2+\ldots+(p_k-1)/2} = (-1)^{(n-1)/2}.$$

Jacobi's Symbol (cont.)

4. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Proof:

We saw that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, thus:

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right) = (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_k^2-1}{8}}$$

It remains to show that

$$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \cdots + \frac{p_k^2-1}{8} \pmod 2$$

$$q_1^2q_2^2 = (1+(q_1^2-1))(1+(q_2^2-1))$$
$$= 1 + (q_1^2-1) + (q_2^2-1) + (q_1^2-1)(q_2^2-1)$$

But $8|(q_1^2-1)$ and $8|(q_2^2-1)$, thus $64|(q_1^2-1)(q_2^2-1)$. Therefore,

$$q_1^2q_2^2 \equiv 1 + (q_1^2-1) + (q_2^2-1) \pmod{16}$$

Jacobi's Symbol (cont.)

And,

$$q_1^2q_2^2q_3^2 \equiv (1+(q_1^2-1))(1+(q_2^2-1))(1+(q_3^2-1)) \pmod{16}$$
$$\equiv 1 + (q_1^2-1) + (q_2^2-1) + (q_3^2-1) \pmod{16}$$

etc., thus,

$$n^2 \equiv 1 + (q_1^2-1) + (q_2^2-1) + \cdots + (q_k^2-1) \pmod{16}$$

$$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \cdots + \frac{p_k^2-1}{8} \pmod 2$$

Jacobi's Symbol (cont.)

5. The first multiplication property: $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

   (if a is coprime to mn it is coprime to m and to n; the rest is derived directly from the definition).

6. The second multiplication property: $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

   (if ab is coprime to n, the both a and b are coprime to n; the rest is derived since this property holds for Legendre's symbol).

Jacobi's Symbol (cont.)

7. The reciprocity law: if m, n are coprime and odd then

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right).$$

Proof:

First assume that $m = q$ is a prime, thus,

$$\left(\frac{n}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_k}{q}\right).$$

By the reciprocity law of Legendre's symbol we know that

$$\left(\frac{p_i}{q}\right) = (-1)^{\frac{p_i-1}{2}\frac{q-1}{2}}\left(\frac{q}{p_i}\right).$$

Thus,

$$\left(\frac{n}{q}\right) = (-1)^{\frac{q-1}{2}(\frac{p_1-1}{2}+\ldots+\frac{p_k-1}{2})}\underbrace{\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\cdots\left(\frac{q}{p_k}\right)}_{\left(\frac{q}{n}\right)}.$$

Jacobi's Symbol (cont.)

We saw in property 3 that,

$$\frac{n-1}{2} \equiv \frac{(p_1-1)}{2} + \frac{(p_2-1)}{2} + \ldots + \frac{(p_k-1)}{2} \pmod 2,$$

thus,

$$\left(\frac{n}{q}\right) = (-1)^{\frac{q-1}{2}\frac{n-1}{2}}\left(\frac{q}{n}\right).$$

Now for any odd m:

$$\left(\frac{n}{m}\right) = \left(\frac{n}{q_1}\right)\left(\frac{n}{q_2}\right)\cdots\left(\frac{n}{q_\ell}\right)$$
$$= \left(\frac{q_1}{n}\right)\left(\frac{q_2}{n}\right)\cdots\left(\frac{q_\ell}{n}\right)(-1)^{\frac{n-1}{2}(\frac{q_1-1}{2}+\ldots+\frac{q_\ell-1}{2})}$$
$$= (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right)$$

QED

Jacobi's Symbol (cont.)

Application of Jacobi's Symbol:

Using the properties of Jacobi's symbol, it is easy to calculate Legendre's symbols in polynomial time.

Example:

$$\left(\frac{117}{271}\right) \underset{7}{=} +1\cdot\left(\frac{271}{117}\right) \underset{1}{=} \left(\frac{37}{117}\right) \underset{7}{=} \left(\frac{117}{37}\right) \underset{1}{=} \left(\frac{6}{37}\right)$$
$$\underset{6}{=} \left(\frac{2}{37}\right)\left(\frac{3}{37}\right) \underset{4}{=} (-1)\left(\frac{3}{37}\right) \underset{7}{=} (-1)(+1)\left(\frac{37}{3}\right)$$
$$\underset{1}{=} (-1)(+1)\left(\frac{1}{3}\right) \underset{2}{=} (-1)(+1)1 = -1$$

271 is prime, therefore $\left(\frac{117}{271}\right)$ can also be computed by:

$$\left(\frac{117}{271}\right) \equiv 117^{\frac{271-1}{2}} \equiv 117^{135} \equiv -1 \pmod{271}.$$

Jacobi's Symbol (cont.)

Complexity:

The only required arithmetic operations are modular reductions and division by powers of two.

Clearly, a division (rule 6) reduces the "numerator" by a factor of two. A modular reduction (using rule 7 and then rule 1), reduces the number by at least two: as if $a > b$ then $a = qb + r \geq b + r > r + r$, thus $r < a/2$, i.e, $a \bmod b < a/2$.

Therefore, at most $O(\log n)$ modular reductions/divisions are performed, each of which takes $O((\log n)^2)$ time. This shows that the complexity is $O((\log n)^3)$, which is polynomial in $\log n$.

A more precise analysis of this algorithm shows that the complexity can be reduced to $O((\log n)^2)$.