Quadratic Residues

Theorem 1 *For a prime p the equation*

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0 \pmod p$$

has at most n solutions.

Note that an equation may have no solution at all

$$x^2 = 2 \mod 5$$

$$1^1 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1$$

Definition: We say that a is a *quadratic residue* mod p if

$$x^2 - a = 0 \mod p$$

has a solution x.

Quadratic Residues

Denote the set of quadratic residues by the symbol

$$QR[p] = \left\{ x^2 \bmod p \mid x \in \{1, 2, \ldots p - 1\} \right\}.$$

Example

1. $p = 11$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

$$QR[11] = \{1, 4, 9, 5, 3\}.$$

2. $p = 13$

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

$$QR[13] = \{1, 4, 9, 3, 12, 10\}.$$

Theorem 2 *Precisely 1/2 of the integers in* $\{1, 2, \ldots, p-1\}$ *are quadratic residues mod* p.

Proof.

Clearly,

$$QR[p] = \{1^2, 2^2, 3^2, \ldots, (p-1)^2\}.$$

Notice that

$$(p-i)^2 = p^2 - 2\,p\,i + i^2 = i^2 \pmod{p}$$

Therefore

$$QR[p] = \{1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2\}.$$

These numbers are all distinct mod p since

$$i^2 - j^2 = (i-j)(i+j)$$

gives that we cannot have $i^2 = j^2$ mod p without p dividing one of the two numbers $i-j$ or $i+j$. However, if both i and j are no larger than $(p-1)/2$, p cannot divide $i+j$. Thus $i^2 = j^2$ forces $i = j$ in this case.

Theorem 3 *For any prime $p > 2$ and any integer a not equal to $0 \pmod p$ we have*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases}$$

Proof.

If $a = x^2$ with $x \neq 0 \bmod p$ then Fermat's theorem gives

$$a^{(p-1)/2} = x^{p-1} = 1 \pmod p$$

Thus the first part of our assertion holds true. To prove the second part, note that the equation

$$x^{p-1} - 1 = 0 \pmod p$$

has exactly $p-1$ solutions in $\{1, 2, \ldots, p-1\}$ and for $p > 2$ we have the factorization

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1).$$

All $(p-1)/2$ elements of $QR[p]$ satisfy the first factor. Therefore the other $(p-1)/2$ solutions must satisfy

$$x^{(p-1)/2} + 1 = 0.$$

Legendre Symbol

For a prime p

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \\ 0 & \text{if } gcd(a,p) > 1 \end{cases}$$

Then for a relatively prime to p, we have

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

Hence

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Theorem 4 (Quadratic Reciprocity) *For any two primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Jacobi Symbol

We start with the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases}$$

and for

$$n = p_1 p_2 \cdots p_k$$

we set

$$J(a,n) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

However, for n odd, we have

$$J(a,n) = \begin{cases} 1 & \text{if } a = 1 \\ J(a/2,n)(-1)^{(n^2-1)/8} & \text{if } a \text{ is even} \\ J(n \mod a, a)(-1)^{(n-1)(a-1)/4} & \text{if } a > 1 \text{ and odd} \end{cases}$$

Primality Testing

The Jacobi symbol allows us to test for primality of n without carrying out its factorization.

If n is prime then

$$J(a, n) = a^{(n-1)/2} \mod n$$

Thus if this identity fails to hold for any value of a in $[1, n-1]$ we can certainly conclude that n is not a prime!

Theorem 5 *If n is not a prime then for more than one half the integers in $\{1, \ldots, n-1\}$ one of the following two tests will fail*

$$J(a, n) = a^{(n-1)/2} \qquad \gcd(a, n) = 1$$

To select a prime at random in a given range, we proceed as follows.

1. We first pick an (odd) integer n at random in the given range.

2. We next pick at random a certain (previously agreed upon) number k of integers $a_1, a_2, \ldots, a_k$ in the interval $\{1, \ldots, n-1\}$.

3. For each number, check that

$$gcd(a_i, n) = 1 \quad \text{and} \quad J(a_i, n) = a^{(n-1)/2} \mod n$$

If n happened to be prime then it will pass all of these tests. On the other hand, if n is not a prime, it will pass all of these tests with probability less than $(1/2)^k$.