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

$$m \equiv \alpha^2 \pmod{p}$$
$$m \equiv \alpha^2 \pmod{q}$$

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

$$x \equiv \pm\alpha \pmod{p}$$
$$x \equiv \pm\alpha \pmod{q}$$

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

$$x^2 \equiv m \pmod{p}$$
$$x^2 \equiv m \pmod{q}$$

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

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

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

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

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:

$$\begin{aligned} n &= p_1 p_2 \cdots p_k \\ &= ((p_1 - 1) + 1)((p_2 - 1) + 1) \cdots ((p_k - 1) + 1) \end{aligned}$$

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,

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

Jacobi's Symbol (cont.)

We conclude that

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

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:

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

It remains to show that

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

$$\begin{aligned} q_1^2 q_2^2 &= (1+(q_1^2-1))(1+(q_2^2-1)) \\ &= 1+(q_1^2-1)+(q_2^2-1)+(q_1^2-1)(q_2^2-1) \end{aligned}$$

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

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

Jacobi's Symbol (cont.)

And,

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

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

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

Jacobi's Symbol (cont.)

Thus,

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

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:

$$\left(\frac{n}{m}\right) = \left(\frac{n}{q_1}\right)\left(\frac{n}{q_2}\right)\cdots\left(\frac{n}{q_\ell}\right)$$

Jacobi's Symbol (cont.)

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

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

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:

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

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 $O((\log n)^2)$.

Algorithms for Public Key Cryptography

Computing Square Roots Modulo a Prime

We have already seen how to compute square roots modulo primes of the form $p = 4k + 3$:
Let α be a quadratic residue modulo p. Then

$$\beta \equiv \alpha^{\frac{p+1}{4}} \equiv \alpha^{k+1} \pmod{p}$$

is a square root of α:

$$\beta^2 \equiv \alpha^{\frac{p+1}{2}} \equiv \alpha\alpha^{\frac{p-1}{2}} \equiv \alpha 1 \equiv \alpha \pmod{p}.$$

Note that $-\beta$ is also a square root of α.

Example: Compute the square root of $\alpha = 3$ modulo $p = 11$.

$$\beta \equiv \alpha^{\frac{p+1}{4}} \equiv 3^3 \equiv 27 \equiv 5 \pmod{11}$$

Computing Square Roots Modulo a Prime (cont.)

We now show a probabilistic algorithm to compute square roots modulo primes of the form $p = 4k + 1$.

Theorem: -1 is a quadratic residue modulo $p = 4k + 1$.

Proof: (already given in the course) The Legendre symbol $\left(\frac{-1}{p}\right)$ is

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \equiv (-1)^{(4k+1-1)/2} \equiv$$
$$\equiv (-1)^{2k} \equiv 1^k \equiv 1 \pmod{p}$$

QED

Computing Square Roots Modulo a Prime (cont.)

Claim: For any a, both a and $-a$ have the same Legendre symbol modulo $p = 4k + 1$ (thus they are both quadratic residues or both quadratic non-residues).

Proof: By Legendre we get

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right) = 1 \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right).$$

QED

Computing Square Roots Modulo a Prime (cont.)

Let m be a quadratic residue modulo p and let $r^2 \equiv m \pmod{p}$.
Assume WLG that $m \not\equiv 0 \pmod{p}$ (otherwise $r \equiv 0 \pmod{p}$). Then, $r \not\equiv 0 \pmod{p}$.
The solutions of $x^2 \equiv m \pmod{p}$ are $x \equiv \pm r \pmod{p}$.

Computing Square Roots Modulo a Prime (cont.)

Fact: Let $0 \leq \delta < p,\ \delta \not\equiv r$. Then $\delta + r$ and $\delta - r$ have the same Legendre symbol iff

$$(\delta + r)/(\delta - r) \stackrel{\Delta}{=} (\delta + r)(\delta - r)^{-1}$$

is a quadratic residue modulo p.

Claim: When δ gets all its possible values $0 \leq \delta < p$, except $\delta \equiv r$, the ratio $(\delta + r)/(\delta - r)$ gets all the values $0 \leq \gamma < p$, except for $\gamma \equiv 1$.

Computing Square Roots Modulo a Prime (cont.)

Proof:

(a) Assume that some γ is received from two distinct δ's: $\delta_1 \not\equiv \delta_2 \pmod{p}$. Then,

$$(\delta_1 + r)/(\delta_1 - r) \equiv (\delta_2 + r)/(\delta_2 - r) \pmod{p}$$

From which the following equations are derived:

$$\begin{aligned}
(\delta_1 + r)(\delta_2 - r) &\equiv (\delta_2 + r)(\delta_1 - r) \pmod{p} \\
\delta_1\delta_2 + r\delta_2 - r\delta_1 - r^2 &\equiv \delta_1\delta_2 + r\delta_1 - r\delta_2 - r^2 \pmod{p} \\
r(\delta_2 - \delta_1) &\equiv -r(\delta_2 - \delta_1) \pmod{p} \\
2r(\delta_2 - \delta_1) &\equiv 0 \pmod{p}
\end{aligned}$$

Since $r \not\equiv 0 \pmod{p}$, we get:

$$\delta_1 \equiv \delta_2 \pmod{p}.$$

Contradiction. Thus, all the received γ's are distinct.

Computing Square Roots Modulo a Prime (cont.)

(b) It remains only to show that $\gamma \not\equiv 1 \pmod{p}$:

But, if $(\delta + r)/(\delta - r) \equiv 1 \pmod{p}$ then $(\delta + r) \equiv (\delta - r) \pmod{p}$, and thus $r \equiv 0 \pmod{p}$. Contradiction.

QED

Computing Square Roots Modulo a Prime (cont.)

Conclusion: Exactly half of the values of δ satisfy that $(\delta + r)$ and $(\delta - r)$ have the same Legendre symbol.

Proof: Exactly half of the values $\gamma = 1, \ldots, p-1$ are quadratic residues, and all of them, except 1 are received by various δ's. The value 1 is a quadratic residue that is not received, but instead the quadratic residue 0 is received. QED

Computing Square Roots Modulo a Prime (cont.)

The Algorithm:
Concentrate on the polynomial

$$f(x) \equiv x^2 - m \equiv (x + r)(x - r) \pmod{p}.$$

Then

$$f(x - \delta) \equiv (x + r - \delta)(x - r - \delta) \equiv (x - (\delta - r))(x - (\delta + r)) \pmod{p}.$$

Exactly for half of the values of δ, only one of $\delta + r$ and $\delta - r$ is a quadratic residue, and the other is a quadratic non-residue. From now on, we concentrate only on these values of δ. Thus, only one of the roots $\delta + r$ and $\delta - r$ of $f(x - \delta)$ is a quadratic residue.

Computing Square Roots Modulo a Prime (cont.)

The polynomial $x^{(p-1)/2} - 1 \pmod p$ is of degree $(p-1)/2$, and whose roots are exactly all the quadratic residues modulo p. By denoting all the quadratic residues by $\rho_1, \rho_2, \ldots, \rho_{(p-1)/2}$, we get

$$x^{(p-1)/2} - 1 \equiv (x - \rho_1)(x - \rho_2) \ldots (x - \rho_{(p-1)/2}) \pmod p.$$

Since only one of the roots of $f(x - \delta)$ is a quadratic residue, only this root is also a root of $x^{(p-1)/2} - 1 \pmod p$ — thus only one of $\delta \pm r$ is one of the ρ_i's.

We can find it by computing gcd of polynomials:

$$\gcd(x^{(p-1)/2} - 1, f(x - \delta)) = x - \rho_i = x + r - \delta \text{ or } x - r - \delta.$$

On average, two trials of δ are required to find the square root.

Computing Square Roots Modulo a Prime (cont.)

Example: Compute the square root of 3 modulo 13.

- Choose $\delta = 7$: Then

$$\begin{aligned} f(x-\delta) &\equiv (x-7)^2 - 3 \equiv x^2 - 14x + 49 - 3 \equiv \\ &\equiv x^2 - x + 7 \pmod{13} \\ x^{(p-1)/2} - 1 &\equiv x^6 - 1 \pmod{13} \end{aligned}$$

By computing the gcd we get:

$$\gcd(x^2 - x + 7, x^6 - 1) = x - 3$$

Thus,

$$\begin{aligned} x - \delta \pm r &\equiv x - 3 \\ \pm r &\equiv -3 + \delta \equiv 4 \pmod{13} \\ r &\equiv \pm 4 \pmod{13} \end{aligned}$$

Computing Square Roots Modulo a Prime (cont.)

- If we choose $\delta = 5$ we get

$$\begin{aligned} f(x-\delta) &\equiv (x-5)^2 - 3 \equiv x^2 - 10x + 25 - 3 \equiv \\ &\equiv x^2 - 10x - 4 \pmod{13} \end{aligned}$$

By computing the gcd we get:

$$\gcd(x^2 - 10x - 4, x^6 - 1) = x^2 - 10x - 4$$

so that both roots are quadratic residues, and really $5+r = 9$ and $5-r = 1$ (we already found that $r = \pm 4$).

Computing Square Roots Modulo a Prime (cont.)

- If we choose $\delta = 2$ we get

$$\begin{aligned} f(x-\delta) &\equiv (x-2)^2 - 3 \equiv x^2 - 4x + 4 - 3 \equiv \\ &\equiv x^2 - 4x + 1 \pmod{13} \end{aligned}$$

By computing the gcd we get:

$$\gcd(x^2 - 4x + 1, x^6 - 1) = 1$$

and thus both roots are quadratic non-residues.

Computing Square Roots Modulo $n = pq$

Example: Compute the square root of 3 modulo $11 \cdot 13$.
We have seen that:

- ± 5 are the square roots of 3 (mod 11).
- ± 4 are the square roots of 3 (mod 13).

The 4 solutions of:

$$\begin{cases} u \equiv \pm 5 \pmod{11} \\ u \equiv \pm 4 \pmod{13} \end{cases}$$

are the square roots of 3 modulo $11 \cdot 13$.

Computing Square Roots Modulo $n = pq$ (cont.)

by using the Chinese remainder theorem:

$$\begin{aligned}
u_1 &\equiv 4 \cdot 6 \cdot 11 + 5 \cdot 6 \cdot 13 \equiv 82 \pmod{11 \cdot 13} \\
u_2 &\equiv -4 \cdot 6 \cdot 11 + 5 \cdot 6 \cdot 13 \equiv 126 \pmod{11 \cdot 13} \\
u_3 \equiv -u_2 &\equiv 4 \cdot 6 \cdot 11 - 5 \cdot 6 \cdot 13 \equiv 17 \pmod{11 \cdot 13} \\
u_4 \equiv -u_1 &\equiv -4 \cdot 6 \cdot 11 - 5 \cdot 6 \cdot 13 \equiv 61 \pmod{11 \cdot 13}
\end{aligned}$$

Note that:

$$\begin{aligned}
13^{-1} &\equiv 6 \pmod{11} \\
11^{-1} &\equiv 6 \pmod{13}
\end{aligned}$$

The Density of Prime Numbers

For many applications, we need to find large "random" primes. Fortunately, large primes are not too rare, so it is not too time consuming to test random integers of the appropriate size until a prime is found.

The **prime number function** $\pi(n)$ specifies the number of primes that are less than or equal n.

Examples: $\pi(10) = 4$.

The Density of Prime Numbers (cont.)

Prime Number Theorem:

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$$

We can use the prime number theorem to estimate the probability that a randomly chosen integer n is a prime as $\frac{1}{\ln n}$. Thus, we need to examine approximately $\ln n$ integers chosen randomly near n in order to find a prime that is of the same length as n (this figure can be cut in half by choosing only odd integers).

Primality Tests

We want to know whether a given number n is prime.

$$\text{Primes} = \{n : n \text{ is a prime number in binary representation}\}$$

- It is easy to show that Primes $\in$ coNP.
  Primes $\in$ NP (Pratt 75).
- Primes $\in$ coRP (Solovay-Strassen 77, Rabin 80).
  Primes $\in$ RP.
  Thus, Primes $\in$ ZPP $=$ RP $\bigcap$ coRP.

In 2002, Agrawal, Kayal and Saxena have shown that Primes $\in P$. However, the time complexity of their algorithm is $O(log^{12}(n))$.

Note:
Monte Carlo algorithms - BPP (RP,coRP $\subseteq$ BPP).
Las Vegas algorithms - ZPP.

Primality Tests (cont.)

The following is a simple primality test, based on Euler's theorem.
Choose some $0 < a < n$, and test whether

$$a^{n-1} \equiv 1 \pmod{n}.$$

By Fermat's theorem, the equation holds for any prime number n, and for any a.
Thus, if this equation does not hold: n is composite. If the equations holds: try another a.

Primality Tests (cont.)

Does such a test suffice? Can we conclude that if we even tried many a's in $0 < a < n$, and the equations hold, then n is a prime?

No!

There are composite numbers for which for any a coprime to n, $a^{n-1} \equiv 1 \pmod{n}$. These numbers are called **Carmichael numbers**.

The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$, for which

$$\text{lcm}(3-1, 11-1, 17-1) = 80 | 560 = 561 - 1.$$

Indeed,

$$\begin{cases} a^{560} \equiv 1 \pmod{3} \\ a^{560} \equiv 1 \pmod{11} \\ a^{560} \equiv 1 \pmod{17} \end{cases}$$

Solovay-Strassen Primality Test

Ref: A Fast Monte-Carlo Test for Primality, SIAM Journal of Computing, V. 6, No. 1, March 1977. Correction in V. 7, No. 1, February 1978.

The Algorithm:

1. Let n be some odd number. We wish to test whether n is prime.
2. Choose some random number a, $1 < a < n$. If $\gcd(a, n) \neq 1$ then n is not prime.
3. Compute the values

$$\epsilon \equiv a^{(n-1)/2} \pmod{n}$$
$$\delta \equiv \left(\frac{a}{n}\right) \qquad \text{(Jacobi symbol)}$$

4. If $\gcd(a, n) > 1$ or $\epsilon \neq \delta$ then n is necessarily composite.
5. Otherwise n is probably a prime with probability $\geq 1/2$.

Solovay-Strassen Primality Test (cont.)

6. Execute the above test m times:

   (a) If the algorithm outputs 'Composite' at least once: output 'Composite'.

   (b) If the algorithm output 'Possibly Prime' in all the m trials: output 'Prime'.

Solovay-Strassen Primality Test (cont.)

Theorem: If n is an odd prime, the algorithm always outputs 'Prime', i.e., for any a

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

Proof: By Euler's criterion and the definition of Legendre's symbol. QED

Solovay-Strassen Primality Test (cont.)

The following theorem states that at least half of the a's are witnesses to the fact that n is composite.

Theorem: If n is an odd composite, at most half of the numbers $a \in Z_n^*$ satisfy

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

Proof: First we show that there exists some b such that

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Solovay-Strassen Primality Test (cont.)

1. If n is divisible by some prime power p^e ($p > 2$, $e \geq 2$, $p^{e+1} \not| n$), we choose

$$b = 1 + \frac{n}{p}.$$

Note that $p|\varphi(n)$ because $\varphi(p^e) = (p-1)p^{e-1}$.

Also note that $\gcd(b, \frac{n}{p}) = 1$, which implies $\gcd(b, n) = 1$.

Denote $n = p^e q_1 q_2 \ldots q_k$, where the q_i's are not necessarily distinct.

Then,

$$\left(\frac{b}{n}\right) = \left(\frac{b}{n/p^e}\right)\left(\frac{b}{p}\right)^e = \left(\frac{b}{q_1}\right)\left(\frac{b}{q_2}\right)\ldots\left(\frac{b}{q_k}\right)\left(\frac{b}{p}\right)^e$$

but $b \equiv 1 \pmod{q_i}$ for any q_i, and $b \equiv 1 \pmod{p}$. Thus,

$$\left(\frac{b}{n}\right) = 1.$$

Solovay-Strassen Primality Test (cont.)

On the other hand,

$$b^{(n-1)/2} \not\equiv 1 \pmod{n}$$

since if we assume the contrary, and denote the order of b modulo p^e by d ($b^d \equiv 1 \pmod{p^e}$), then $d|\frac{(n-1)}{2}$, and

$$d|n-1.$$

Denoting $b \equiv 1 + kp^{e-1} \pmod{p^e}$, for $k = n/p^e$, we get by the Binom that

$$1 \equiv b^d \equiv 1 + dkp^{e-1} + \text{Some multiple of } p^e \pmod{p^e}.$$

Therefore, $dkp^{e-1} \equiv 0 \pmod{p^e}$, from which we get $p|dk$. Since $gcd(k,p) = 1$, we conclude that $p|d$. Recall that $d|n-1$, therefore,

$$p|n-1$$

Solovay-Strassen Primality Test (cont.)

But

$$p|n.$$

Therefore, $p|1$, i.e., $p = 1$. Contradiction.

Solovay-Strassen Primality Test (cont.)

2. If n is a product of distinct primes, and is not divisible by any square of a prime:

   Let p be any prime factor of n, and denote $n = pq_1q_2 \ldots q_k$, where p and the q_i's are all distinct.

   Choose a quadratic non-residue s modulo p, and choose b by the Chinese remainder theorem:

$$\begin{aligned} b &\equiv s \pmod{p} \\ b &\equiv 1 \pmod{n/p} \end{aligned}$$

   Then,

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{q_1}\right)\left(\frac{b}{q_2}\right)\ldots\left(\frac{b}{q_k}\right) = (-1)\cdot 1\cdot 1\ldots\cdot 1 = -1$$

Solovay-Strassen Primality Test (cont.)

On the other hand:

$$b^{(n-1)/2} \equiv 1 \pmod{n/p}$$

and thus

$$b^{(n-1)/2} \not\equiv -1 \pmod{n/p}$$
$$b^{(n-1)/2} \not\equiv -1 \pmod{n}$$

We conclude that for any modulo n there is some b for which the equation does not hold, and

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Solovay-Strassen Primality Test (cont.)

3. We now show that at least half of the numbers do not satisfy the equation.

Let $w_1, w_2, \ldots, w_t$ all the numbers in Z_n^* that satisfy

$$w_i^{(n-1)/2} \equiv \left(\frac{w_i}{n}\right) \pmod{n}.$$

Define $u_1, u_2, \ldots, u_t$ by

$$u_i \equiv b w_i \bmod n, \qquad i = 1, \ldots, t.$$

All the numbers $u_1, u_2, \ldots, u_t$ are distinct, and all of them are coprime to n and in the range $0 < u_i < n$.

We claim that all the u_i's do not satisfy the equation, i.e., for any u_i:

$$u_i^{(n-1)/2} \not\equiv \left(\frac{u_i}{n}\right) \pmod{n}.$$

Solovay-Strassen Primality Test (cont.)

Assume the contrary that the equation holds for some u_i:

$$u_i^{(n-1)/2} \equiv \left(\frac{u_i}{n}\right) \pmod{n}.$$

Then,

$$b^{(n-1)/2} w_i^{(n-1)/2} \equiv \left(\frac{b}{n}\right)\left(\frac{w_i}{n}\right) \pmod{n}.$$

But

$$w_i^{(n-1)/2} \equiv \left(\frac{w_i}{n}\right) \pmod{n}.$$

and thus

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Contradiction for the choice of b.

Solovay-Strassen Primality Test (cont.)

Thus, all the u_i's do not satisfy the equation. Since they are all distinct, for any number w_i which satisfy the equation, there is at least one other number which do not satisfy the equation. Thus, the probability that a random a do not satisfy the equation is at least half.
QED

Solovay-Strassen Primality Test (cont.)

Complexity of the Primality Test:

- gcd computation: $O(\log n)$ divisions.
- ϵ: $O(\log n)$ modular operations.
- δ: $O(\log n)$ divisions.
- In total: $O(\log n)$ for any choice of a.
- In order to get probability 2^{-m} for an error (output 'Prime' for a composite number) the algorithm tries m a's. The total complexity is thus $O(m \log n)$.
- If n is a composite, it is identified on average after trying two a's. The complexity in this case is $O(2 \log n) = O(\log n)$.