Generation of Prime Numbers

AK Bhateja

Generation of large primes & primality test

- The sieve of Eratosthenes
- General method to generate a prime
  - Generate a random odd number n of appropriate size.
  - Test n for primality.
  - If n is composite, return to the first step.

Probabilistic primality tests

- Probable prime
  - believed to be prime on the basis of a probabilistic primality test
  - an integer that satisfies a specific condition that is satisfied by all prime numbers, but which is not satisfied by most composite numbers
- Witnesses to the compositeness of *n*
  - Let *n* be an odd composite integer. An integer *a*, $1 \leq a < n - 1$ is witness of *n*, if The probabilistic test outputs composite.

Algorithm: Fermat primality testing

for $i = 1$ to t

do choose a random integer a, $2 \leq a \leq n - 2$.

compute $r = a^{(n-1)} \bmod n$

if $r \neq 1$ then return ("composite")

return("prime")

- If n is prime, then the Fermat primality test always outputs prime. If n is composite, then the algorithm outputs prime with probability at most 2^{-t}

Fermat’s Test : When will it give error?

- If the number is prime the algorithm will always give the output as “PRIME”.
- If the input number is composite, the algorithm might claim that the number is prime. [Hence, give an error]
- Why is this error generated? Due to the presence of F-Liars
- For an odd composite number n, an element a, $1 \leq a \leq n - 1$, is F-liar if $a^{(n-1)} \bmod n \equiv 1$

Fermat's Test : Error Probability

- If $n \geq 3$ is an odd composite number such that there is at least one F-witness a in Z^*_n , then the Fermat test applied to n gives answer 1 with probability more than 1/2 .
- Carmichael number
  - a composite number which satisfies the relation $a^{(n-1)} \equiv 1 \bmod n$ for all integers a satisfying gcd(a, n) = 1.
  - The converse of Fermat's little theorem is not generally true, as it fails for Carmichael numbers.

Example: $n = 341$ ($= 11 \times 31$) is a pseudoprime to the base 2 since $2^{340} \equiv 1 \pmod{341}$.

Legendre symbol

- **Legendre symbol:** Let p be an odd prime and a an integer. The Legendre symbol is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & if\ \ p \mid a \\ 1 & if\ a \in Q_p \\ -1 & if\ a \in \overline{Q}_p \end{cases}$$

i.e. $\left(\frac{a}{p}\right) \equiv a^{\,(p-1)}$ (mod p) and $\left(\frac{a}{p}\right) \in$ {-1, 0, 1}

- **Fact:** Let p be an odd prime and a, $b \in$ Z. Then

(i) $\left(\frac{a}{p}\right) = 1$ iff a is a quadratic residue modulo p

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

(iii) $If\ \ a \equiv b \,(\text{mod}\ p)$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Jacobi Symbol

- Jacobi symbol is generalization of Legendre symbol .
- Definition Let $n \geq 2$ be odd integer and $n = p_1^{e_1} . p_2^{e_2} \ldots p_k^{e_k}$ then Jacobi symbol of a & b is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

- If m is composite and the Jacobi symbol (a/m) = -1, then a is quadratic non residue modulo m.
- If a is residue modulo m then (a/m) = 1, but if (a/m) = 1 then a may be quadratic residue or non-residue modulo m.
- Example: (2/15) = 1 and (4/15) = 1, but 2 N 15 and 4 R 15.

Solovay-Strassen test

- Fact (Euler's criterion) Let n be an odd prime. Then $a^{(n\text{-}1)/2} \equiv \left(\frac{a}{n}\right)$(mod n) for all integers a which satisfy gcd(a, n) = 1.
- If gcd(a, n) = 1 and $a^{(n\text{-}1)/2} \equiv \left(\frac{a}{n}\right)$ (mod n) then n is said to be an Euler pseudoprime to the base a.

Algorithm Solovay-Strassen probabilistic primality test

INPUT: an odd integer $n > 3$ and security parameter $t \geq 1$.

for i from 1 to t

do choose a random integer a, $2 \leq a \leq n - 2$

compute $r = a^{(n-1)/2} \bmod n$

if $r \neq 1$ and $r \neq n - 1$ then return("composite")

compute the Jacobi symbol $s = (a/n)$

if $r \neq s \pmod{n}$ then return ("composite")

return("prime")

Solovay-Strassen error-probability bound

- Fact: Let n be an odd composite integer. The probability that Solovay-Strassen algorithm declares n to be "prime" is less than $(1/2)^t$.
- Example: (Euler pseudoprime) The composite integer 91 ($= 7 \times 13$) is an Euler pseudoprime to the base 9
  since $9^{45} = 1 \pmod{91}$ and $\left(\frac{9}{91}\right) = 1$.
- Fact: Let n be an odd composite integer. Then at most $\varphi(n)/2$ of all the numbers a, $1 \le a \le n - 1$, are Euler liars for n

Properties of Jacobi symbol

1. $(a/n) = (b/n)$ if $a = b \bmod n$.

2. $(1/n) = 1$ and $(0/n) = 0$.

3. $(2m/n) = (m/n)$ if $n = \pm 1 \bmod 8$.

   $(2m/n) = -(m/n)$ otherwise

4. (**Quadratic reciprocity**) If m and n are both odd, then

   $(m/n) = -(n/m)$ if both m and n are congruent to 3 mod 4

   $(m/n) = (n/m)$ otherwise.