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

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

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

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

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

- 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 $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ for all integers a which satisfy $\gcd(a, n) = 1$.
- If $\gcd(a, n) = 1$ and $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ 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, $2 \leq a \leq n - 2$

find gcd(a, n)

if gcd(a, n) >1 then return ("composite")

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 $9^{45} \equiv 1 \pmod{91}$ 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.

Jacobi symbol computation

Example: Compute Jacobi symbol (158/235)

$$\left(\frac{158}{235}\right) = -\left(\frac{79}{235}\right) \qquad \because\ n \neq \pm 1 \bmod 8$$

$$= \left(\frac{235}{79}\right) \qquad \because\ \text{both } m \,\&\, n \text{ are congruent to } 3 \bmod 4$$

$$= \left(\frac{10}{79}\right) \qquad \because\ 235 \equiv 10 \bmod 79$$

$$= -\left(\frac{5}{79}\right) = -\left(\frac{79}{5}\right)$$

$$= -\left(\frac{4}{5}\right) = -\left(\frac{1}{5}\right) = -1$$

Complexity of the Solovay-Strassen test

- GCD of two numbers can be calculated using the Euclidean algorithm having a complexity of $O(\log^2 n)$.
- Computing Jacobi symbol has the same complexity as the Euclidean algorithm.
- Multiplication of two numbers is always done modulo n and it takes $O(\log^2 n)$ time.
- For any a, we can compute a^n mod n in $O(\log n)$ multiplications, by repeated squaring.
- Thus this method of modular exponentiation can be done in $O(\log n \times \log^2 n) = \log^3 n$ for each value of a.
- The overall time-complexity of the Miller-Rabin algorithm is $O(t \cdot \log^3 n)$, t being the number of bases.

Miller-Rabin test

- It is a strong pseudoprime probabilistic test
- Fact: Let n be an odd prime, and let n - 1 = $2^s r$ where r is odd. Let a be any integer s.t. gcd(a, n) = 1. Then either $a^r \equiv 1$ (mod n) or $a^{2^j r} \equiv -1 (\bmod n)$ for some j, $0 \le j \le s$ -1.

Def: Let n be an odd composite integer, and let n - 1 = $2^s r$ where r is odd. Let a be any integer in [1, n -1]

(i) If $a^r \neq 1$ (mod n) & $a^{2^j r} \neq -1 \bmod n \ \forall j$, $0 \le j \le s$ -1. then a is said a strong witness (to compositeness) for n.

(ii) If $a^r \equiv 1$ (mod n) & $a^{2^j r} \equiv -1 \bmod n$ for some j, $0 \le j \le s$ -1. then n is said to be a strong pseudoprime to the base a (i.e. n acts like a prime). The integer a is called a strong liar for n.

Number of Strong liars

- Fact: If n is an odd composite integer, then at most 1/4 of all the numbers a, $1 \leq a \leq n - 1$, are strong liars for n. In fact, the number of strong liars for n is at most $\varphi(n)/4$.
- Example: Consider the composite integer $n = 91$ ($= 7 \times 13$).

  $91 - 1 = 90 = 2 \times 45$, $s = 1$ and $r = 45$.

  Let $a = 9$, $9^r = 9^{45} \equiv 1 \pmod{91}$

  Implies 91 is a strong pseudoprime to the base 9.

  The set of all strong liars for 91 is:

  {1, 9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90}.
- The number of strong liars for 91 is $18 = \varphi(91)/4$.

Algorithm: Miller-Rabin probabilistic primality test

INPUT: An odd integer $n > 2$ and security parameter $t \geq 1$

write n - 1 = $2^s r$ such that r is odd.

for i from 1 to t

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

    compute $y = a^r \bmod n$

    if $y \neq 1$ and $y \neq n - 1$

        then j = l.

        while $j < s - 1$ and $y \neq n - 1$

            compute $y = y^2 \bmod n$

            if $y = 1$ then return("composite")

            $j = j + 1$

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

return("prime")

Miller-Rabin error-probability bound

- For any odd composite integer n, the probability that Miller Rabin primality test algorithm declares n to be "prime" is less than $(1/4)^t$
- For most composite integers n, the number of strong liars for n is actually much smaller than the upper bound of $\varphi(n)/4$.

  Consequently, the Miller-Rabin error-probability bound is much smaller than $(1/4)^t$ for most positive integers n.
- Example: (some composite integers have very few strong liars) The only strong liars for the composite integer $n = 105$ $(= 3 \times 5 \times 7)$ are 1 and 104. More generally, if $k \geq 2$ and n is the product of the first k odd primes, there are only 2 strong liars for n, namely 1 and $n - 1$.

Time complexity

- Multiplication of two numbers is always done modulo n and it takes $O(\log^2 n)$ time.
- For any a, we can compute $a^n \bmod n$ in $O(\log n)$ multiplications (modular exponentiation).
- Thus this method of modular exponentiation can be done in $O(\log n \times \log^2 n) = \log^3 n$ for each value of a.
- The overall time-complexity of the Miller-Rabin algorithm is $O(t \cdot \log^3 n)$, t being the number of bases.

Comparison: Fermat, Solovay-Strassen and Miller-Rabin

- Fact: Let n be an odd composite integer.

  (i) If a is an Euler liar for n, then it is also a Fermat liar for n.

  (ii)If a is a strong liar for n, then it is also an Euler liar for n.

- Example: For composite integer $n = 65$ ($= 5 \times 13$)

  The Fermat liars for 65 are {1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64}.

  The Euler liars for 65 are {1, 8, 14, 18, 47, 51, 57, 64},

  while the strong liars for 65 are

  {1, 8, 18, 47, 57, 64}

Generation of Strong primes

Gordon's algorithm for generating a strong prime p

1. Generate two large random primes s and t of roughly equal bitlength
2. Select an integer i_0.

   Find the first prime in the sequence $2it + 1$, for $i = i_0, i_0 + 1, i_0 + 2, \ldots$ Denote this prime by $r = 2it + 1$.
3. Compute $p_0 = (2s^{r-2} \bmod r)s - 1$.
4. Select an integer j_0

   Find the first prime in the sequence $p_0 + 2jrs$, for $j = j_0, j_0 + 1, j_0 + 2, \ldots$ Denote this prime by $p = p_0 + 2jrs$.
5. Return(p).