Solovay – Strassen primality test

This Solovay – Strassen primality test was published in 1977, little before publishing of Miller–Rabin test (https://www.savitagandhi.com/articles/miller-rabin-primality-test). Let us first understand the concepts required in Solovay – Strassen primality test.

Quadratic Residues

Let $n > 1$. An integer $1 \leq a \leq n$, is called a quadratic residue modulo n, if there exists integer b; $0 < b < n$, such that is $a \equiv b^2 (mod\ n)$. Otherwise, a is called a non quadratic residue modulo n. (a is a quadratic residue, if a is perfect square modulo n).

Example 1: Find quadratic residues modulo 10.

Solution: Let us find $b^2(mod\ 10)$ for $0 < b < 10$. The values of $b^2(mod\ 10)$are automatically in the range $0 \leq a \leq 10$. Following *table 1*, gives the values of $b^2(mod\ 10)$ for $0 < b < 10$.

b	$b^2(mod\ 10)$
1	1
2	4
3	9
4	6
5	5
6	6
7	9
8	4
9	1

Table 1

So, 1, 4, 5, 6, 9 are quadratic residues modulo 10 and 2, 3, 7, 8 are non-quadratic residues modulo 10.

In fact, as $(-b)^2 \equiv b^2(mod\ n)$, we need not work with the entire range $1 \leq b < n$, working with $1 \leq b \leq \left\lfloor \frac{n}{2} \right\rfloor$ only is sufficient. Let us see, how.

Example 2: Find quadratic residues modulo 11.

Solution: Construct table of $b^2(mod\ 11)$ for $1 \leq b \leq 5$. We need not try other remaining numbers, because of $(-b)^2 \equiv b^2(mod\ n)$.

b	$b^2(mod\ 11)$
1	1
2	4
3	9
4	5
5	3

Table 2

So, form *table 2*: 1, 3, 4, 5, 9 are quadratic residues modulo 11, whereas as remaining 2, 6, 7, 8, 10 are non-quadratic residues modulo 11.

We shall mainly be interested in quadratic residues modulo n, when n is prime. It can be shown that if p is an odd prime, then precisely $(p-1)/2$ of the numbers $1,2,\ldots,p-1$ are quadratic residues $mod\ p$, and the same number $(p-1)/2$ are quadratic non residues modulo p.

In above example, when $p = 11$, we got 1, 3, 4, 5, 9 ; five quadratic residues modulo 11 and same number of quadratic non residues modulo 11.

The following *table 3* of quadratic residues for $p \leq 20; p$ prime

p	Quadratic residues
2	1
3	1
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16
19	1, 4, 5, 6, 7, 9, 11, 16, 17

Table 3

Legendre Symbol

Let p be an odd prime and let $a \neq 0\ (mod\ p)$. The Legendre symbol denoted as $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1\ if\ a\ is\ a\ quadratic\ residue\ of\ p \\ -1 \qquad\qquad\qquad\qquad otherwise \end{cases}$$

Thus, from *table 2*, given in previous section, we can say that

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1;\ \text{where as}$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Euler's Criterion

Theorem: Let p be an odd prime and let $a \neq 0\ (mod\ p)$. Then,

$$a^{(p-1)/2}(mod\ p) \equiv \left(\frac{a}{p}\right) \text{ ; that is,}$$

$$a^{(p-1)/2}(mod\ p) \equiv \begin{cases} 1\ if\ a\ is\ a\ quadratic\ residue\ of\ p \\ -1 \qquad\qquad\qquad\qquad otherwise \end{cases}$$

This Criterion first appeared in 1748, in a paper by Euler. Euler's Criterion forms a basis for Solovay – Strassen primality test, discussed as follows: Proof is omitted here as it requires the knowledge of *Field Theory*.

Solovay – Strassen primality test

Let n be an odd integer. Choose several random integers a with $1 < a < n - 1$. If

$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2}(mod\ n)$, for some integer a with $1 < a < n - 1$, then n is composite.

$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2}(mod\ n)$, for all a with $1 < a < n - 1$, then n is probably prime.

Example 3: Let us apply Solovay-Strassen primality test to 15.

Solution: $n = 15$, choose $a = 2$, let us calculate $\left(\frac{2}{15}\right)$

x	$x^2(mod\ 15)$
1	1
2	4
3	9
4	1
5	10
6	6
7	4

Table 4

Rest of the numbers need not be tried as $(x)^2 \equiv (-x)^2(mod\ n)$. From *table 4*, it is clear that 2 is not a quadratic residue of 15, giving, $\left(\frac{2}{15}\right) = -1$.

Now, let us determine, $a^{(n-1)/2}(mod\ n)$ for $n = 15, a = 2$, and check whether it is equal to $\left(\frac{2}{15}\right)$. $a^{(15-1)/2}(mod\ 15) = 2^7(mod\ 15) \equiv 128(mod\ 15) = 8 \not\equiv -1(\text{mod } 15)$. Hence,15 is composite.

Example 4: Apply Solovay-Strassen primality test to 11.

Solution: $n = 11$, choose $a = 2$, let us calculate $\left(\frac{2}{11}\right)$. From *table 2*: $\left(\frac{2}{11}\right) = -1$. Next, let us determine $a^{(n-1)/2}(mod\ n)$ for $n = 11, and\ \ a = 2$. $a^{(11-1)/2}(mod\ 11) = 2^5(mod\ 11) = 32\ (mod\ 11) = -1(mod\ 11) = \left(\frac{2}{11}\right)$. Similiarly, on working with other remaining $a's$: $3 \leq a < 10$, it can be seen that condition is satisfied, yielding that 11 is probably prime.

There are very convenient formulas for calculating $\left(\frac{a}{n}\right)$. For the sake of brevity, they are omitted here. Interested readers can refer additional literature on Number Theory.

Both the tests Miller- Rabin test and Solovay-Strassen test run quickly, are quite efficient, but do not ensure 100% correctness, in case of prime number p. Results are probabilistic in nature. But they give the result with quite high probability. However, if we wish to compare these two methods against each other, Miller - Rabin test is more efficient then Solovay-Strassen test and at least as correct as Solovay-Strassen test. Miller – Rabin test was published in 1980. Nevertheless, if application demands 100% reliability on the result generated, deterministic primality algorithm like AKS primality test can be used, but the algorithm and its implementation variants known so far are not efficient.

****