Miller-Rabin Primality test

Miller – Rabin primality test is based on two properties. First property states that there are no nontrivial square roots modulo prime.

Let us understand the significance of this first property. 1 and −1 always satisfy the equation $a^2 \equiv 1(mod\ n)$, for any n. So they are called trivial square roots of $1(mod\ n)$. But, in case of congruences modulo theory, it is possible to have square roots other than 1 or −1. For example, if $n = 8$, $\boldsymbol{a^2 \equiv 1(mod\ 8)}$ has 1, 3, 5, 7 as solutions $\leq \mathbf{7}$. 1, 3, 5, 7 satisfy $\boldsymbol{a^2 \equiv 1(mod\ 8)}$, because, $\mathbf{1^2} = 1 \equiv 1(mod\ 8)$, $\mathbf{3^2} = 9 \equiv 1(mod\ 8)$, $\mathbf{5^2} = 25 \equiv 1(mod\ 8)$, and $\mathbf{7^2} = 49 \equiv 1(mod\ 8)$. So, this equation has 4 square roots namely 1, 3, 5, 7, each mod 8, two of them different from 1or $\boldsymbol{-1(mod\ 8)}$. On the other hand, if $n = 5$, $\boldsymbol{a^2 \equiv 1(mod\ 5)}$ is satisfied only by 1 and 4 . This means, there are no nontrivial square roots for modulo 5. Let us state and prove this property.

Property 1: Square roots of $\boldsymbol{1(mod\ p)}$; $\boldsymbol{p}$ prime:

Statement: For $1 \leq a \leq p-1$, with p prime, $a^2 \equiv 1(mod\ p)$, iff $a = \pm 1(mod\ p)$, that is, $a = 1$ or $p-1$.

Proof: If, $a^2 \equiv 1(mod\ p)$, then $(a^2 - 1) \equiv 0(mod\ p)$, that is, $((a+1)(a-1)) \equiv 0(mod\ p)$. Therefore, $p|((a+1)(a-1))$, giving $p|(a+1)$ or $p|(a-1)$ as p is prime. Thus, $(a+1) \equiv 0(mod\ p)$ or $(a-1) \equiv 0(mod\ p)$. So, $a \equiv -1(mod\ p)$ or $a \equiv 1(mod\ p)$, which can be written as $a \equiv \pm 1(mod\ p)$.

Conversely, let $a \equiv \pm 1(mod\ p)$, that is, $a \equiv 1(mod\ p)$ or $a \equiv -1(mod\ p)$. This gives, $p|(a-1)$ or $p|(a+1)$. So, $p\big|\big((a+1)(a-1)\big) \Rightarrow p\big|(a^2-1)$. This can be written as $(a^2-1) \equiv 0(mod\ p)$. $a^2 \equiv 1(mod\ p)$. This proves the property 1.

Second property states that sequence of successive square roots of $a^{p-1} \equiv 1(mod\ p)$; p prime has all 1's or the first element which is different from 1 in the sequence is −1 $(mod\ p)$, that is $p-1$. Miller-Rabin Primality test makes use of this property. Let us state and prove this property.

Property 2: Sequence of successive square roots of $\boldsymbol{a^{p-1} \equiv 1(mod\ p)}$; $\boldsymbol{p}$ prime:

Statement: Let p be prime and odd, 2^s be the largest power of 2 which divides $(p-1)$, with $p - 1 = 2^s \cdot q$ (q is odd). Let $1 < a < p-1$. Then, either every element of the sequence: $a^{p-1}, a^{(p-1)/2}, a^{(p-1)/4}, \ldots, a^q$ is $1(mod\ p)$ is 1 or the first element which is different from 1 in the sequence is −1 $(mod\ p)$, that is $p-1$.

Proof: As p is prime and odd, p is ≥ 3. So, $p-1$ is even. 2^s be the largest number power of 2 which divides $p-1$, we can say that $p-1 = 2^s \cdot q$, where q is odd. Now, consider the sequence $a^{p-1}, a^{(p-1)/2}, a^{(p-1)/4}, \ldots, a^q$, that is, $a^{2^s \cdot q}, a^{2^{s-1} \cdot q}, a^{2^{s-2} \cdot q}, \ldots, a^q$. The first number in the sequence is a^{p-1} and each successive number in this sequence is square root of the preceding number. p being prime, by Fermat's theorem, (https://www.savitagandhi.com/articles/fermats-little-theorem) $a^{p-1} \equiv 1(mod\ p)$. As first element in the sequence is a^{p-1}, it is $1(mod\ p)$. By property 1: *Square roots of* $1(mod\ p); p\ prime$), the only square roots of $1(mod\ p)$ are $\pm 1(mod\ p)$. Next element being square root of the preceding element is $\pm 1(mod\ p)$, (as long as preceding element is 1), that is either $1(mod\ p)$ or $-1(mod\ p)$. So, every element of the sequence: $a^{p-1}, a^{(p-1)/2}, a^{(p-1)/4}, \ldots, a^q$ is either $1(mod\ p)$, that is is 1, or the first element which is different from 1 in the sequence is $-1\ (mod\ p)$, that is $p-1$. Let us have one illustration.

Example 1: Determine sequence of successive square roots of $a^{p-1} \equiv 1(mod\ p);\ p$ prime with $p = 17$ and $a = 2$.

Solution: $p-1 = 16$, expressing 16 as $2^s \cdot q$, with q odd gives, $16 = 2^4 \cdot 1$, here $s = 4$, $q = 1$. The sequence is $2^{16}, 2^8, 2^4, 2^2, 2^1$. The backward sequence is $2^1, 2^2, 2^4, 2^8, 2^{16}$. For convenience, let us calculate backwards:

$$2^1 = 2 \equiv 2\ (mod\ 17),\ \ 2^2 = 4 \equiv 4\ (mod\ 17)$$

$$2^4 = (2^2)^2 = 4^2 = 16 \equiv 16\ (mod\ 17) \equiv -1\ (mod\ 17)$$

$$2^8 = (2^4)^2 = 16^2 \equiv (-1)^2\ (mod\ 17) \equiv 1\ (mod\ 17)$$

$$2^{16} = (2^8)^2 \equiv (1)^2\ (mod\ 17) \equiv 1\ (mod\ 17)$$

So the sequence is 1, 1, −1, 4, 2 confirming first element in the sequence to be different from 1 as −1.

For more illustrations and Miller Rabin test and the algorithm, one may refer book: …….. (*section 4.6.2: Miller-Rabin primality test*).

****