Miller Rabin Primality Test

Justin Wyss-Gallifent

February 27, 2022

0.1 What it Does

A probabilistic test for primality.

0.2 Preliminaries

Theorem:

If $a \mid bc$ and $\gcd(a,b)=1$ then $a \mid c$.

Proof:

We know there are integers x,y with $ax+by=1$ and then $acx+bcy=c$ then since $a \mid acx$ and $a \mid bcy$ we have $a \mid c$.

General Theorem (GT):

If $x^2 \equiv +1 \mod n$ then either $x \equiv \pm 1 \mod n$ or $x \not\equiv \pm 1 \mod n$ and n is composite with $\gcd(x-1,n)$ as a factor.

Proof:

If $x \equiv \pm 1 \mod n$ we are done, so suppose $x \not\equiv \pm 1 \mod n$.

Let $d=\gcd(x-1,n)$. If $d=n$ then $n \mid (x-1)$ and then $x \equiv 1 \mod n$, a contradiction.

If $d=1$ then $n \mid (x-1)(x+1)$ with $\gcd(x-1,n)=1$ implies that $n \mid (x+1)$ and then $x \equiv -1 \mod n$, a contradiction.

Thus $1<d<n$ and so n is composite and $\gcd(x-1,n)$ is a factor.

0.3 How to Apply

Suppose n is odd and we wish to know if it is prime. We write $n = 2^k m + 1$ with m odd. We choose some $1 < a < n - 1$ and set $b_0 \equiv a^m \mod n$.

- If $b_0 \equiv \pm 1 \mod m$ then STOP, n is probably prime.

Otherwise set $b_1 \equiv b_0^2 \mod n$. Note that $b_1 \equiv a^{2m} \mod n$.

- If $b_1 \equiv +1 \mod n$ then STOP, n is composite.
- If $b_1 \equiv -1 \mod n$ then STOP, n is probably prime.

Otherwise set $b_2 \equiv b_1^2 \mod n$. Note that $b_2 \equiv a^{4m} \mod n$.

- If $b_2 \equiv +1 \mod n$ then STOP, n is composite.
- If $b_2 \equiv -1 \mod n$ then STOP, n is probably prime.

Otherwise keep going ... note that in general $b_i \equiv a^{2^i m} \mod n$.

Keep going until we reach b_{k-1}. Note that $b_{k-1} \equiv a^{2^{k-1} m} \mod n$.

- If $b_{k-1} \equiv +1 \mod n$ then STOP, n is composite.
- If $b_{k-1} \equiv -1 \mod n$ then STOP, n is probably prime.

Otherwise if neither of these is true then STOP, n is composite.

0.4 Examples

Let $n = 561 = 2^4 35 + 1$ and $a = 2$

$$\begin{aligned} b_0 &\equiv 2^{35} \equiv 263 \mod 561 \\ b_1 &\equiv 263^2 \equiv 166 \mod 561 \\ b_2 &\equiv 166^2 \equiv 67 \mod 561 \\ b_3 &\equiv 67^2 \equiv 1 \mod 561 \end{aligned}$$

Composite.

Let $n = 74593 = 2^5 2331 + 1$ and $a = 3$

$$\begin{aligned} b_0 &\equiv 3^{2331} \equiv 74566 \mod 74593 \\ b_1 &\equiv 74566^2 \equiv 729 \mod 74593 \\ b_2 &\equiv 729^2 \equiv 9290 \mod 74593 \\ b_3 &\equiv 9290^2 \equiv -1 \mod 74593 \end{aligned}$$

Probably Prime. It actually isn't: $74593 = 97 \cdot 769$.

Let $n = 98762051 = 2^1 49381025 + 1$ and $a = 2$

$$b_0 \equiv 2^{49381025} \equiv -1 \mod 98762051$$

Probably Prime. It actually is.

Let $n = 10186669 = 2^2 2546667 + 1$ and $a = 2$

$$b_0 \equiv 2^{2546667} \equiv 9066525 \mod 10186669$$
$$b_1 \equiv 9066525^2 \equiv 10186668 \equiv -1 \mod 10186669$$

Probably Prime. It actually is.

Let $n = 10234283921 = 2^4 639642745 + 1$ and $a = 2$

$$b_0 \equiv 2^{639642745} \equiv 4179106498 \mod 10234283921$$
$$b_1 \equiv 4179106498^2 \equiv 5072761571 \mod 10234283921$$
$$b_2 \equiv 5072761571^2 \equiv 8004436438 \mod 10234283921$$
$$b_3 \equiv 8004436438^2 \equiv 5033398949 \mod 10234283921$$

Composite.

0.5 Why Does It Work?

0.5.1 Observation 1

Suppose $b_0 \equiv \pm 1 \mod n$, then observe that:

$$a^{n-1} \equiv a^{2^k m} \equiv (a^m)^{2^k} \equiv (b_0)^{2^k} \equiv (\pm 1)^{2^k} \equiv 1 \mod n$$

Then n is probably prime by FLIT.

0.5.2 Observation 2

Suppose we chug along until we hit the first $1 \leq j \leq k-1$ with $b_j \equiv \pm 1 \mod n$ and observe:

- If $b_j \equiv +1 \mod n$ then $b_{j-1}^2 \equiv b_j \equiv +1 \mod n$. We cannot have $b_{j-1} \equiv \pm 1 \mod n$, as this would contradict the fact that j was earliest, so by GT we must have $b_{j-1} \not\equiv \pm 1 \mod n$ and n is composite.
- If $b_j \equiv -1 \mod n$ then observe that since $k - j \geq 1$ we have:

  $$a^{n-1} \equiv a^{2^k m} \equiv \left(a^{2^j m}\right)^{2^{k-j}} \equiv (b_j)^{2^{k-j}} \equiv (-1)^{2^{k-j}} \equiv 1 \mod n$$

  Then n is probably prime by FLIT.

0.5.3 Observation 3

If we reach b_{k-1} and neither of these are true then we have $b_{k-1} \not\equiv \pm 1 \mod n$. We claim that n is composite. If n were prime then by FLIT we would have:

$$(b_{k-1})^2 \equiv \left(a^{2^{k-1} m}\right)^2 \equiv a^{2^k m} \equiv a^{n-1} \equiv 1 \mod n$$

Since $b_{k-1} \not\equiv \pm 1 \mod n$ by GT we then have n composite, a contradiction. Thus n is not prime and so it is composite.