THE MILLER–RABIN PRIMALITY TEST

1. Fast Modular Exponentiation

Given positive integers a, e, and n, the following algorithm quickly computes the reduced power $a^e \,\%\, n$.

- (*Initialize*) Set $(x, y, f) = (1, a, e)$.
- (*Loop*) While $f > 1$, do as follows:
  - If $f\%2 = 0$ then replace (x, y, f) by $(x, y^2 \,\%\, n, f/2)$,
  - otherwise replace (x, y, f) by $(xy \,\%\, n, y, f - 1)$.
- (*Terminate*) Return x.

The algorithm is strikingly efficient both in speed and in space.

To see that it works, represent the exponent e in binary, say

$$e = 2^f + 2^g + 2^h, \quad 0 \le f < g < h.$$

The algorithm successively computes

$$\begin{aligned}
&(1,\ a,\ 2^f + 2^g + 2^h)\\
&(1,\ a^{2^f},\ 1 + 2^{g-f} + 2^{h-f})\\
&(a^{2^f},\ a^{2^f},\ 2^{g-f} + 2^{h-f})\\
&(a^{2^f},\ a^{2^g},\ 1 + 2^{h-g})\\
&(a^{2^f+2^g},\ a^{2^g},\ 2^{h-g})\\
&(a^{2^f+2^g},\ a^{2^h},\ 1)\\
&(a^{2^f+2^g+2^h},\ a^{2^h},\ 0),
\end{aligned}$$

and then it returns the first entry, which is indeed a^e.

2. The Fermat Test and Fermat Pseudoprimes

Fermat's Little Theorem states that for any positive integer n,

$$\textit{if } n \textit{ is prime then } b^n \bmod n = b \textit{ for } b = 1, \ldots, n-1.$$

In the other direction, all we can say is that

$$\textit{if } b^n \bmod n = b \textit{ for } b = 1, \ldots, n-1 \textit{ then } n \textit{ might be prime.}$$

If $b^n \bmod n = b$ where $b \in \{1, \ldots, n-1\}$ then n is called a **Fermat pseudoprime base** b.

There are 669 primes under 5000, but only five values of n (561, 1105, 1729, 2465, and 2821) that are Fermat pseudoprimes base b for $b = 2, 3, 5$ without being prime. This is a false positive rate of less than 1%. The false positive rate under 500,000 just for $b = 2, 3$ is 0.118%.

On the other hand, the bad news is that checking more bases b doesn't reduce the false positive rate much further. There are infinitely many **Carmichael numbers**,

numbers n that are Fermat pseudoprimes base b for all $b \in \{1, \ldots, n-1\}$ but are not prime.

In sum, Fermat pseudoprimes are reasonable candidates to be prime. More specifically, given any *base* $b \in \{1, \cdots, n-1\}$, one can quickly compute two informative quantities:

- If $\gcd(b, n) > 1$ then n is composite.
- If $b^{n-1} \,\%\, n \neq 1$ then a is a *Fermat witness* that n is composite; otherwise n passes the *Fermat test* for the base b, telling us that n might be prime.

If n passes the Fermat test for many bases b (where "many" is a vague term) then almost certainly either n is prime or n is a product of distinct primes.

Lemma. *Let p be an odd prime. Let n be a positive integer divisible by p^2. Let x, y be integers such that $x = y \bmod p$ and $x^{n-1} = y^{n-1} = 1 \bmod n$. Then $x = y \bmod p^2$.*

First we note that $x^p = y^p \bmod p^2$. This follows quickly from the relation

$$x^p - y^p = (x - y)(x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}),$$

because the condition $x = y \bmod p$ makes each of the multiplicands on the right side a multiple of p. Second, raise both sides of the relation $x^p = y^p \bmod p^2$ to the power n/p to get $x^n = y^n \bmod p^2$. But since $x^n = x \bmod n$, certainly $x^n = x \bmod p^2$, and similarly for y. The result follows.

Proposition. *Let p be an odd prime. Let n be a positive integer divisible by p^2. Let B denote the set of bases b between 1 and $n-1$ such that n is a Fermat pseudoprime base b, i.e.,*

$$B = \{b : 1 \leq b \leq n-1 \text{ and } b^{n-1} \bmod n = 1\}.$$

Then

$$|B| \leq \frac{p-1}{p^2} n \leq \frac{1}{4}(n-1).$$

To see this, decompose B according to the values of its elements modulo p,

$$B = \bigcup_{d=1}^{p-1} B_d$$

where

$$B_d = \{b \in B : b \bmod p = d\}, \quad 1 \leq d \leq p-1.$$

For any d such that $1 \leq d \leq p-1$, if $b_1, b_2 \in B_d$ then we know that $b_1 = b_2 \bmod p^2$. It follows that $|B_d| \leq n/p^2$, and the result follows.

3. Strong Pseudoprimes

The **Miller–Rabin test** on a positive odd integer n and a positive test base b in $\{1, \ldots, n-1\}$ proceeds as follows.

- Factor $n - 1$ as $2^s m$ where m is odd.
- Replace b by $b^m \bmod n$.
- If $b = 1$ then return the result that n could be prime, and terminate.
- Do the following s times: If $b = n - 1$ then return the result that n could be prime, and terminate; otherwise replace b by $b^2 \bmod n$.

- If the algorithm has not yet terminated then return the result that n is composite, and terminate.

(Slight speedups here: (1) If the same n is to be tested with various bases b then there is no need to factor $n-1 = 2^s m$ each time; (2) there is no need to compute b^2 mod n on the sth time through the step in the fourth bullet.)

In carrying out the Miller–Rabin test we keep an intelligent eye on the process of raising the test base b to the $(n-1)$st power modulo n by first taking b^m and then repeatedly squaring. If the process reaches 1 without passing through a square root of 1 then we have learned nothing; if the process reaches 1 by finding the square root -1 of 1 a moment earlier then also we have learned nothing; however, if the process reaches the last bullet in the description then either b^{n-1} has reached 1 by passing through a square root of 1 other than -1 or $b^{n-1} \neq 1$, and n is composite in both cases. When n is composite, the Miller–Rabin test for only one base b isn't so informative (the chance of a false suggestion that n is prime could be as high as 25% though in practice it is far lower), but the likelihood of *repeatedly* squaring our way to 1 without ever finding a square root of 1 other than -1 is exponentially small. For example, the chance of twenty false positive is in practice far less than $1/4^{20} = 1/2^{40} \approx 1/1000^4 = 10^{-12}$.

A positive integer n that passes the Miller–Rabin test for some b is a **strong pseudoprime base** b.

For any n, at least 3/4 of the b-values in $\{1, \dots, n-1\}$ have the property that if n is a strong pseudoprime base b then n is really prime. But according to the theory, up to 1/4 of the b-values have the property that n could be a strong pseudoprime base b but not be prime. In practice, the percentage of such b's is much lower. For n up to 500,000, if n is a strong pseudoprime base 2 and base 3 then n is prime.

Here is a rough argument that the Miller–Rabin method works well. Consider an odd composite positive integer,

$$n = \prod_{p|n} q_p, \quad \text{each } q_p = p^{e_p} \text{ with } e_p \geq 1.$$

By the Sun-Ze Theorem, the multiplicative group modulo n is, structurally,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{p|n} (\mathbb{Z}/q_p\mathbb{Z})^\times.$$

Each factor on the right side, being cyclic of even order, contains the unique nontrivial square root -1 mod q_p of its 1. So altogether, letting f denote the number of distinct prime factors of n, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ contains 2^f distinct square roots of 1 (two of which are ± 1). Assume that since we are applying the Miller–Rabin test to n, it is a Fermat pseudoprime to the base b of the test. (Alternatively, we may simply verify that this is so before Rabin–Miller.) The test replaces b by b^m and then repeatedly squares, exiting if the squaring produces -1 and running all the way to the end if the squaring produces 1 without passing through -1. Thus:

> *If n is composite and a Fermat pseudoprime to base b, and if the Miller–Rabin test returns the result that n could be prime, then either the repeated squaring process has inadvertantly started at 1 or it has proceeded to 1 via -1. The probability of the latter occurrence is heuristically $1/2^f$.*

Even in the simplest composite case that isn't a prime power, $n = p\tilde{p}$, the Miller–Rabin test should misleadingly suggest that n is prime at most roughly $1/4$ of the time.

No longer assuming that n is composite, if the test repeatedly suggests that n is prime as the base b varies, then the probability that the suggestion is false decreases exponentially in the number of tests.

To understand the Miller–Rabin test more precisely, consider a positive odd integer n and a base b, and reason as follows.

- Factor $n - 1 = 2^s \cdot m$ where m is odd.
- If n is prime then $b^{n-1} = 1$ (here and throughout this discussion, all arithmetic is being carried out modulo n). So by contraposition, if $b^{n-1} \neq 1$ then n is composite.
- Hence we continue reasoning only if $b^{n-1} = 1$. In this case we know a square root of 1: it is $b^{(n-1)/2}$.
- If $b^{(n-1)/2} \neq \pm 1$ then too many square roots of 1 exist mod n for n to be prime, and so n is composite.
- If $b^{(n-1)/2} = -1$ then we have no evidence that n is composite, nor can we proceed, since we have no new square roots of 1 to study. The algorithm terminates, reporting that n could be prime.
- But if $b^{(n-1)/2} = 1$ then we do have a new square root of 1 at hand: it is $b^{(n-1)/4}$.
- This process can continue until $b^{2m} = 1$, so that b^m is a square root of 1. If $b^m \neq \pm 1$ then n is composite. Otherwise, n could be prime.

The only wrinkle in encoding the algorithm efficiently as above is to compute the powers of b from low to high, even though the analysis here considered them from high to low. Inspecting the highest power b^{n-1} turns out to be redundant.

For another way to think about the Miller–Rabin test, again let $n - 1 = 2^s \cdot m$. Then

$$\begin{aligned} X^{2^s m} - 1 &= (X^{2^{s-1} m} + 1)(X^{2^{s-1} m} - 1) \\ &= (X^{2^{s-1} m} + 1)(X^{2^{s-2} m} + 1)(X^{2^{s-2} m} - 1) \\ &= (X^{2^{s-1} m} + 1)(X^{2^{s-2} m} + 1)(X^{2^{s-3} m} + 1)(X^{2^{s-3} m} - 1) \\ &\vdots \\ &= (X^{2^{s-1} m} + 1)(X^{2^{s-2} m} + 1)(X^{2^{s-3} m} + 1) \cdots (X^m + 1)(X^m - 1). \end{aligned}$$

That is, rewriting the left side and reversing the order of the factors of the right side,

$$X^{n-1} - 1 = (X^m - 1) \cdot \prod_{r=0}^{s-1} (X^{2^r m} + 1).$$

It follows that

$$b^{n-1} - 1 = (b^m - 1) \cdot \prod_{r=0}^{s-1} (b^{2^r m} + 1) \bmod n, \quad \text{for } b = 1, \ldots, n-1.$$

If n is prime then $b^{n-1} - 1 = 0 \bmod n$ for $b = 1, \ldots, n$, and also $\mathbb{Z}/n\mathbb{Z}$ is a field, so that necessarily one of the factors on the right side vanishes modulo n as well.

That is, given any base $b \in \{1, \ldots, n-1\}$, if n is prime then at least one of the factors

$$b^m - 1, \quad \{b^{2^r m} + 1 : 0 \le r \le s-1\}$$

vanishes modulo n. So conversely, given any base $b \in \{1, \ldots, n-1\}$, if none of the factors vanishes modulo n then n is composite. This analysis shows that the Miller–Rabin test can be phrased as earlier in this writeup.

4. Generating Candidate Large Primes

Given n, a simple approach to finding a candidate prime above $2n$ is as follows. Take the first of $N = 2n+1$, $N = 2n+3$, $N = 2n+5$, ... to pass the following test.

(1) Try trial division for a few small primes. If N passes, continue.
(2) Check whether N is a Fermat pseudoprime base 2. If N passes, continue.
(3) Check whether N is a strong pseudoprime base b as b runs through the first 20 primes.

Any N that passes the test is extremely likely to be prime. And such an N should appear quickly. Indeed, using only the first *three* primes in step (3) of the previous test finds the following correct candidate primes:

The first candidate prime after	10^{50}	is	$10^{50} + 151$.
The first candidate prime after	10^{100}	is	$10^{100} + 267$.
The first candidate prime after	10^{200}	is	$10^{200} + 357$.
The first candidate prime after	10^{300}	is	$10^{300} + 331$.
The first candidate prime after	10^{1000}	is	$10^{1000} + 453$.