The Rabin-Miller Primality Test

Fermat Pseudoprimes; The Fermat Primality Test

Fermat's Little Theorem allows us to prove that a number is composite without actually factoring it.

Fermat's Little Theorem (alternate statement): If $a^{n-1} \not\equiv 1 \pmod{n}$ for some a with $a \not\equiv 0 \pmod{n}$, then n is composite.

This statement is absolute: There are no exceptions.

Unfortunately, the inverse statement is not always true.

*Inverse to Fermat's Little Theorem (**not always true**):* If $a^{n-1} \equiv 1 \pmod{n}$ for some a with $a \not\equiv 0 \pmod{n}$, then n is prime.

Some counterexamples:

$2^{340} \equiv 1 \pmod{341}$, but $341 = 11 \cdot 31$ is composite, and

$5^{560} \equiv 1 \pmod{561}$, but $561 = 3 \cdot 11 \cdot 17$ is composite.

We say that 341 is a Fermat pseudoprime (to the base 2), and 561 is a Fermat pseudoprime to the base 5.

It is even possible for $a^{n-1} \equiv 1 \pmod{n}$ to hold for ***every*** a with $\gcd(a,n) = 1$, and still have n be composite.

This occurs if n is a Carmichael number (also called an absolute Fermat pseudoprime). A Carmichael number is a Fermat pseudoprime to any base a with $\gcd(a,n) = 1$.

Carmichael numbers are fairly rare: There are only seven less than 10000: *561, 1105, 1729, 2465, 2821, 6601, 8911*

In fact, there are only 585,355 Carmichael numbers less than 10^{17}.

Given a randomly chosen odd integer n less than 10^{17}, the probability that n is a Carmichael number is only a little over 10^{-11} (about one in one hundred billion).

For a randomly chosen odd integer n with 100 to 300 digits, the probability that n is a Carmichael number appears to be exceedingly low (for practical purpose, zero).

If n is composite and not a Carmichael number, then there are at most $\varphi(n)/2$ values of a $(1 \le a < n)$ for which $a^{n-1} \equiv 1 \pmod{n}$.

Let n be any odd integer, other than a Carmichael number.

Say we choose 50 random integers a and compute that each satisfies $a^{n-1} \equiv 1 \pmod{n}$.

The probability that this would occur if n is composite is at most $2^{-50} \approx 10^{-15}$.

So we can say with reasonable certainty that n is prime.

If n is composite and not a Carmichael number, then it is actually possible to have $\varphi(n)/2$ values for which $a^{n-1} \equiv 1 \pmod{n}$.

For example, take $n = 91 = 7 \cdot 13$. $\varphi(n) = 6 \cdot 12 = 72$.

There are 36 values of a with $a^{72} \equiv 1 \pmod{91}$, namely a = 1, 3, 4, 9, 10, 12, 16, 17, 22, 23, 25, 27, 29, 30, 36, 38, 40, 43, 48, 51, 53, 55, 61, 62, 64, 66, 68, 69, 74, 75, 79, 81, 82, 87, 88, 90.

But this is unusual.

For nearly all odd composite integers n (other than Carmichael numbers), $a^{n-1} \equiv 1 \pmod{n}$ for far fewer than $\varphi(n)/2$ values of a.

For example, let us look at odd composite integers starting with 10001.

n	φ(n)	No of a with $a^{n-1} \equiv 1 (\text{mod } n)$
10001	9792	64
10003	8568	36
10005	4928	64
10011	6440	280
10013	8640	16
10015	8008	4
10017	5616	16
10019	9744	4
10021	9100	100
10023	6144	8
10025	8000	32
10027	9720	162
10029	6684	4
10031	8592	4
10033	9828	36
10035	5328	8
10041	6192	4
10043	9020	4

This means that far fewer than the 50 random values of a, mentioned earlier, are typically sufficient to show that an odd integer (not a Carmichael number) is prime, with near certainty.

For a randomly chosen odd integer n with 100 to 300 digits, it appears that if $a^{n-1} \equiv 1$ (mod n) for even a single randomly chosen a, then n is prime with probability very close to 1.

Fermat Test for Primality: To test whether n is prime or composite, choose a at random and compute $a^{n-1} \pmod{n}$.

i) If $a^{n-1} \equiv 1 \pmod{n}$, declare n a probable prime, and optionally repeat the test a few more times.

ii) If $a^{n-1} \not\equiv 1 \pmod{n}$, declare n composite, and stop.

We have seen that the Fermat test is really quite good for large numbers.

One limitation: If someone is supposed to provide us with a prime number, and sends a Carmichael number instead, we cannot detect the deception with the Fermat test.

In any case, we can improve upon the Fermat test at almost no cost.

Euler Pseudoprimes; The Euler Test

If n is an odd prime, we know that an integer can have at most two square roots, mod n. In particular, the only square roots of 1 (mod n) are ± 1.

If $a \not\equiv 0 \pmod{n}$, $a^{(n-1)/2}$ is a square root of $a^{(n-1)} \equiv 1 \pmod{n}$, so $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.

> If $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$ for some a with $a \not\equiv 0 \pmod{n}$, then n is composite.

Euler Test: For a randomly chosen a with $a \not\equiv 0 \pmod{n}$, compute $a^{(n-1)/2} \pmod{n}$.

i) If $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$, declare n a probable prime, and optionally repeat the test a few more times.

If n is large and chosen at random, the probability that n is prime is very close to 1.

ii) If $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, declare n composite.

This is always correct.

The Euler test is more powerful than the Fermat test.

If the Fermat test finds that n is composite, so does the Euler test.

But the Euler test may find n composite even when the Fermat test fails. Why?

If n is an odd composite integer (other than a prime power), 1 has at least 4 square roots mod n.

So we can have $a^{(n-1)/2} \equiv \beta \pmod{n}$, where $\beta \neq \pm 1$ is a square root of 1. Then $a^{n-1} \equiv 1 \pmod{n}$. In this situation, the Fermat Test (incorrectly) declares n a probable prime, but the Euler test (correctly) declares n composite.

We noted earlier that

$2^{340} \equiv 1 \pmod{341}$, even though 340 is composite, and

$5^{560} \equiv 1 \pmod{561}$, even though 561 is composite.

We can compute that

$2^{170} \equiv 1 \pmod{341}$, even though 340 is composite, but

$5^{280} \equiv 67 \not\equiv \pm 1 \pmod{561}$, showing that 561 is composite.

We call 341 an <u>Euler pseudoprime</u> to the base 2.

But note that 561 is not an Euler pseudoprime base 5, even though it is a Fermat pseudoprime base 5.

On the whole, there are only about half as many Euler pseudoprimes as Fermat pseudoprimes.

Consider the seven Carmichael numbers less than 10000.

The Euler test can show that 5 of the 7 numbers are composite.

n	$\varphi(n)$	**No of a with $a^{n-1} \equiv 1 \pmod{n}$**	**No of a with $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$**
561	320	320	160
1105	768	768	384
1729	1296	1296	1296
2465	1792	1792	1792
2881	2160	2160	1080
6601	5280	5280	2640
8911	7128	7128	1782

The integers 1729 and 2465 are called absolute Euler pseudoprimes (by analogy with the absolute Fermat pseudoprimes, i.e., Carmichael numbers).

These are composite odd integers such that $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$ for every a with $gcd(a,n) = 1$.

These number cannot be proven composite with the Euler test (unless we happen to choose an a with $gcd(a,n) > 1$, which is exceedingly unlikely if n is a large integer lacking small prime factors.

There are fewer absolute Euler pseudoprimes than there are Carmichael numbers, but unfortunately absolute Euler pseudoprimes do exist.

The Rabin-Miller Primality Test

The Euler test improves upon the Fermat test by taking advantage of the fact, if 1 has a square root other than $\pm 1 \pmod{n}$, then n must be composite.

If $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, where $gcd(a,n) = 1$, then n must be composite for one of two reasons:

i) If $a^{n-1} \not\equiv 1 \pmod{n}$, then n must be composite by Fermat's Little Theorem

ii) If $a^{n-1} \equiv 1 \pmod{n}$, then n must be composite because $a^{(n-1)/2}$ is a square root of $1 \pmod{n}$ different from ± 1.

The limitation of the Euler test is that is does not go to any special effort to find square roots of 1, different from ± 1. The Rabin-Miller test does do this.

For example, recall the Euler Test declares 341 a probable prime because $2^{170} \equiv 1 \pmod{341}$.

But if we compute $2^{85} \pmod{341}$, we find $2^{85} \equiv 32 \pmod{341}$. Thus 32 is a square root of $2^{2\cdot 85} \equiv 2^{170} \equiv 1 \pmod{341}$, different from ± 1, so we would find that 341 is composite.

In the Rabin-Miller test, we write $n - 1 = 2^s \cdot m$, with m odd and $s \geq 1$.

We then start by compute $a^m \pmod{n}$ using fast exponentiation.

If $a^m \equiv \pm 1 \pmod{n}$, we declare n a probable prime, and stop.

Why? We know that $a^{n-1} \equiv (a^m)^{2^s} \equiv 1 \pmod{n}$, and we will not find a square root of 1, other than ± 1, in repeated squaring of a^m to get a^{n-1}.

Otherwise, unless $s = 1$, we square $a^m \pmod{n}$ to obtain a^{2m}.

If $a^{2m} \equiv 1 \pmod{n}$, we declare n composite, and stop.

Why? a^m is a square root of $a^{2m} \equiv 1 \pmod{n}$, different from ± 1.

If $a^{2m} \equiv -1 \pmod{n}$, we declare n a probable prime, and stop.

Why? Just as above, we know that $a^{n-1} \equiv 1 \pmod{n}$, and we will not find a square root of 1, other than ± 1.

Otherwise, unless $s = 2$, we square $a^{2m} \pmod{n}$ to obtain $a^{2^2 m}$.

If $a^{2^2 m} \equiv 1 \pmod{n}$, we declare n composite, and stop.

Why? We have found a square root of 1 (mod n), different from ±1, just as above

If $a^{2m} \equiv -1 \pmod{n}$, we declare n a probable prime, and stop.

Why? Just above, we know that $a^{n-1} \equiv 1$ (mod n), and we will not find a square root of 1, other than ±1.

Otherwise we continue in this manner until either (a) we stop the test, or (b) we have computed $a^{2^{s-1}m}$, and stopped if $a^{2^{s-1}m} \equiv a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.

If we haven't stopped by this point, we declare n composite and stop.

Why? Exactly as with the Euler test.

Let us carry out the Rabin-Miller test on the absolute Euler pseudoprime 1729, using $a = 671$.

$1729 - 1 = 1728 = 2^6 \cdot 27$. So $s = 6$, $m = 27$.

$$
\begin{aligned}
671^{27} &\equiv 1084 && \pmod{1729}\\
671^{27\cdot 2} &\equiv 1084^2 \equiv 1065 && \pmod{1729}\\
671^{27\cdot 2^2} &\equiv 1065^2 \equiv 1 && \pmod{1729}
\end{aligned}
$$

The test declares n composite, and terminates.

Next we test a much larger integer, $n = 972133929835994161$ (also a Carmichael number), using $a = 2$.

$n - 1 = 2^4 \cdot 60758370614749635$.

$$
\begin{aligned}
2^{60758370614749635} &\equiv 338214802923303483 && \pmod{n}\\
2^{2\cdot 60758370614749635} &\equiv 338214802923303483^2 && \pmod{n}\\
&\equiv 332176174063516118 && \pmod{n}\\
2^{2^2\cdot 60758370614749635} &\equiv 332176174063516118^2 && \pmod{n}\\
&\equiv 779803551049098051 && \pmod{n}\\
2^{2^3\cdot 60758370614749635} &\equiv 779803551049098051^2 && \pmod{n}\\
&\equiv 1 && \pmod{n}
\end{aligned}
$$

The test declares n composite, and terminates.

Next we test an integer that is composite, but not a Carmichael number, $n = 2857191047211793$, using $a = 1003$.

$n - 1 = 2^4 \cdot 178574440450737$.

$$
\begin{aligned}
1003^{178574440450737} &\equiv 1135781085623492 && \pmod{n}\\
1003^{2\cdot 178574440450737} &\equiv 1135781085623492^2 && \pmod{n}\\
&\equiv 84313648747407 && \pmod{n}\\
1003^{2^2\cdot 178574440450737} &\equiv 84313648747407^2 && \pmod{n}\\
&\ 2321094267189023 && \pmod{n}\\
1003^{2^3\cdot 178574440450737} &\equiv 2321094267189023^2 && \pmod{n}\\
&\equiv 978857874792606 && \pmod{n}
\end{aligned}
$$

The test declares n composite, and terminates.

Finally we test an integer that is in fact prime, $n = 104513$, using $a = 3$.

$n - 1 = 2^6 \cdot 1633$.

$$
\begin{aligned}
3^{1633} &\equiv 88958 & & \pmod{n} \\
3^{2\cdot 1633} &\equiv 88958^2 &\equiv 10430 & \pmod{n} \\
3^{2^2\cdot 1633} &\equiv 10430^2 &\equiv 91380 & \pmod{n} \\
3^{2^3\cdot 1633} &\equiv 91380^2 &\equiv 29239 & \pmod{n} \\
3^{2^4\cdot 1633} &\equiv 29239^2 &\equiv 2781 & \pmod{n} \\
3^{2^5\cdot 1633} &\equiv 2781^2 &\equiv -1 & \pmod{n}
\end{aligned}
$$

The test concludes that n is a probable prime. We might perform a few more tests before we are convinced that n is in fact prime.

Like the Fermat and Euler tests, the Rabin-Miller test has psuedoprimes (choices of a for which the test declares a composite integer to be a probable prime).

Rabin-Miller pseudoprimes are called strong pseudoprimes.

There are fewer strong pseudoprimes than Fermat or Euler pseudoprimes.

More importantly, there are no Rabin-Miller absolute pseudoprimes (as we had absolute Fermat and Euler absolute pseudoprimes).

For any odd composite integer n, there are at most $\varphi(n)/4$ integers a ($1 \le a < n$, $gcd(a,n) = 1$) for which the Rabin-Miller test declares n prime.

In practice, the number of strong pseudoprimes is usually far, far less than $\varphi(n)/4$, if n is large.

There are a number of other primality tests, but the Rabin-Miller test is the one most commonly used.