The Miller–Rabin primality test

The Fermat primality test picks a and checks whether $a^{n-1} \equiv 1 \pmod{n}$.

- If $a^{n-1} \not\equiv 1 \pmod{n}$, then we are done because n is definitely not a prime.

- If $a^{n-1} \equiv 1 \pmod{n}$, then either n is prime or a is a Fermat liar.
  But instead of leaving off here, we can dig a little deeper:
  Note that $a^{(n-1)/2}$ satisfies $x^2 \equiv 1 \pmod{n}$. If n is prime, then $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.
  [Recall that, if n is composite (and odd), then $x^2 \equiv 1 \pmod{n}$ has additional solutions!]

    - Hence, if $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, then we again know for sure that n is not a prime.
      In fact, we can now factor n! See bonus challenge below.

    - If $a^{(n-1)/2} \equiv 1 \pmod{n}$ and $\frac{n-1}{2}$ is divisible by 2, we continue and look at $a^{(n-1)/4} \pmod{n}$.

    - If $a^{(n-1)/2} \equiv -1 \pmod{n}$, then n is a prime or a is a **strong liar** modulo n.

Write $n - 1 = 2^s \cdot m$ with m odd. In conclusion, if n is a prime, then

$$a^m \equiv 1 \quad \text{or, for some } r = 0, 1, ..., s - 1, \quad a^{2^r m} \equiv -1 \pmod{n}.$$

In other words, if n is a prime, then the values $a^m, a^{2m}, ..., a^{2^s m}$ must be of the form $1, 1, ..., 1$ or $..., -1, 1, 1, ..., 1$. If the values are of this form even though n is composite, then a is a **strong liar** modulo n.

This gives rise to the following improved primality test:

Miller–Rabin primality test

Input: number n and parameter k indicating the number of tests to run
Output: "not prime" or "likely prime"
Algorithm:

> Write $n - 1 = 2^s \cdot m$ with m odd.
> Repeat k times:
> > Pick a random number a from $\{2, 3, ..., n - 2\}$.
> > If $a^m \not\equiv 1 \pmod{n}$ and $a^{2^r m} \not\equiv -1 \pmod{n}$ for all $r = 0, 1, ..., s - 1$, then
> > > stop and output "not prime".
> Output "likely prime".

Comment. If n is composite, then less than a quarter of the values for a could possibly be strong liars. In other words, for any composite number, the odds that the Miller–Rabin test returns "likely prime" are less than 4^{-k}.

Comment. Note that, though it looks more involved, the Miller–Rabin test is essentially as fast as the Fermat primality test (recall that, to compute a^{n-1}, we proceed using binary exponentiation).

Advanced comments. This is usually implemented as a probabilistic test. However, assuming GRH (the generalized Riemann hypothesis), it becomes a deterministic algorithm if we check $a = 2, 3, ..., \lfloor 2(\log n)^2 \rfloor$. This is mostly of interest for theoretical applications. For instance, this then becomes a polynomial time algorithm for checking whether a number is prime.

More recently, in 2002, the AKS primality test was devised. This test is polynomial time (without relying on outstanding conjectures like GRH).

Example 92. Suppose we want to determine whether $n = 221$ is a prime. Simulate the Miller–Rabin primality test for the choices $a = 24$, $a = 38$ and $a = 47$.

Solution. $n - 1 = 4 \cdot 55 = 2^s \cdot m$ with $s = 2$ and $m = 55$.

- For $a = 24$, we compute $a^m = 24^{55} \equiv 80 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 80^2 \equiv 212 \not\equiv -1$, and conclude that n is not a prime.

  Note. We do not actually need to compute that $a^{n-1} = a^{4m} \equiv 81$, which features in the Fermat test and which would also lead us to conclude that n is not prime.

- For $a = 38$, we compute $a^m = 38^{55} \equiv 64 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 64^2 \equiv 118 \not\equiv -1$ and conclude that n is not a prime.

  Note. This case is somewhat different from the previous in that 38 is a Fermat liar. Indeed, $a^{4m} \equiv 118^2 \equiv 1 \pmod{221}$. This means that we have found a nontrivial sqareroot of 1. In this case, the Fermat test would have failed us while the Miller–Rabin test would have succeeded.

- For $a = 47$, we compute $a^m = 47^{55} \equiv 174 \not\equiv \pm 1 \pmod{221}$. We continue with $a^{2m} \equiv 174^2 \equiv -1$. We conclude that n is a prime or a is a strong liar. In other words, we are not sure but are (incorrectly) leaning towards thinking that 221 was a prime.

Comment. In this example, only 4 of the 218 residues $2, 3, \ldots, 219$ are strong liars (namely $21, 47, 174, 200$). On the other hand, there are 14 Fermat liars (namely $18, 21, 38, 47, 64, 86, 103, 118, 135, 157, 174, 183, 200, 203$).

Example 93. (bonus challenge) If $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, then we can factor n! How?!

Comment. However, note that this only happens if a is a Fermat liar modulo n, and these are typically very rare. So, unfortunately, we have not discovered an efficient factorization algorithm.

But we have run into an idea, which is used for some of the best known factorization algorithms. If time permits, more on that later...

Example 94. (bonus challenge) In Example 90, we saw that all $\phi(561) = 320$ invertible residues a modulo 561 are Fermat liars (that is, they all satisfy $a^{560} \equiv 1 \pmod{561}$). How many of them are strong liars?