**Example 115.** How can you check whether a huge randomly selected number $N$ is prime?

**Solution.** Compute $2^{N-1} \pmod N$ using binary exponentiation. If this is $\not\equiv 1 \pmod N$, then $N$ is not a prime. Otherwise, $N$ is a prime or $2$ is a Fermat liar modulo $N$ (but the latter is exceedingly unlikely for a huge randomly selected number $N$; the bonus challenge below indicates that this is almost as unlikely as randomly running into a factor of $N$).

**Comment.** There is nothing special about $2$ here (you could also choose $3$ or any other residue).

**Comment.** Just for giggles, let us emphasize once more the need to compute $2^{N-1} \pmod N$ without actually computing $2^{N-1}$. Take, for instance, the 1024 bit RSA challenge number $N = 135...563$ from Example 78. In Example 109, we did compute $2^{N-1} \pmod N$, observed that it was $\not\equiv 1$ and concluded that $N$ is not prime. The number $2^{N-1}$ itself has $N-1 \approx 2^{1024} \approx 10^{308.3}$ binary digits. It is often quoted that the number of particles in the visible universe is estimated to be between $10^{80}$ and $10^{100}$. Whatever these estimates are worth, our number has WAY more digits (!) than that. Good luck writing it out!

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**.

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, when computing $a^m, a^{2m}, ..., a^{2^s m}$, we must see the value $-1$ before the value $1$ (unless $a^m$ is already $1$).

**Example 116. (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...

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 $\{2,3,\ldots,n-2\}$.
    If $a^m\not\equiv 1 \pmod n$ and $a^{2^r m}\not\equiv -1 \pmod n$ for all $r=0,1,\ldots,s-1$, 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 $4^{-k}$.

**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 $a=2,3,\ldots,\lfloor 2(\log n)^2\rfloor$. 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 117.** 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 $a^{n-1}=a^{4m}$, which features in the Fermat test.

- 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 $1$.

- 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 liars (namely $21,47,174,200$).