Example 110. Fermat's little theorem can be stated in the slightly stronger form:

n is a prime $\iff$ $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \{1, 2, \ldots, n-1\}$

Why? Fermat's little theorem covers the "$\Longrightarrow$" part. The "$\Longleftarrow$" part is a direct consequence of the fact that, if n is composite with divisor d, then $d^{n-1} \not\equiv 1 \pmod{n}$. (Why?!)

Review. In the second part, we used that the **contrapositive** of $A \Longrightarrow B$ is the logically equivalent statement $\neg B \Longrightarrow \neg A$.

3.5 Primality testing

Recall that it is extremely difficult to factor large integers (this is the starting point for many cryptosystems). Surprisingly, it is much simpler to tell if a number is prime (without trying to factor it). The following is a first indication of how this can be done.

Example 111. Is 35 a prime? (Of course, not.)

Solution. If 35 was a prime, then $2^{34} \equiv 1 \pmod{35}$. Let's check!

$2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^8 = 16^2 \equiv 11$, $2^{16} \equiv 11^2 \equiv 16$, $2^{32} \equiv 16^2 \equiv 11$.

Hence, $2^{34} \equiv 2^{32} \cdot 2^2 \equiv 11 \cdot 4 \equiv 9 \not\equiv 1 \pmod{35}$. This implies that 35 is not a prime!

Note. We showed that 35 is not a prime without factoring it! Our method here certainly seems more complicated than trying to find these factors, but the situation is the opposite when the numbers get large.

Also note. If 2^{34} had worked out to be congruent to 1 modulo 35, then we wouldn't have learned anything for certain: 35 might be a prime, or it might not. However, we would have gathered some evidence leaning towards it being prime. Repeating this test with a number different from 2 we can build more and more confidence that our number is a prime. This uncertainty is a common feature of the most efficient primality tests, which are heuristic: they either prove that our number is not a prime or conclude that it "very likely" is a prime.

Comment. Note that it would be dishonest to simplify our computation above using Euler's theorem and $\phi(35) = 24$. Namely, recall that computing $\phi(n)$ is essentially as hard as factoring n. But, if we knew how to factor n, we wouldn't be asking whether n is a prime or not.

Fermat primality test

Input: number n and parameter k indicating the number of tests to run

Output: "not prime" or "likely prime"

Algorithm:

Repeat k times:
  Pick a random number a from $\{2, 3, \ldots, n-2\}$.
  If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "likely prime".

If $a^{n-1} \equiv 1 \pmod{n}$ although n is composite, then a is often called a **Fermat liar**.

On the other hand, if $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite and a is called a **Fermat witness**.

Flaw. There exist certain composite numbers n (see Example 113) for which every a is a Fermat liar (or reveals a factor of n). For this reason, the Fermat primality test should not be used as a general test for primality. That being said, for very large random numbers, it is exceedingly unlikely to meet one of these troublesome numbers, and so the Fermat test is indeed used for the purpose of randomly generating huge primes (for instance in PGP). In fact, in that case, we can even always choose $a = 2$ and $k = 1$ with virtual certainty of not messing up.

Below, we will discuss an extension of the Fermat primality test which solve these issues (and is just mildly slower).

Advanced comment. If n is composite but not an absolute pseudoprime (see Example 113), then at least half of the values for a satisfy $a^{n-1} \not\equiv 1 \pmod{n}$ and so reveal that n is not a prime. This is more of a theoretical result: for most large composite n, almost every a (not just half) will be a Fermat witness.

Armin Straub
straub@southalabama.edu

Example 112. Suppose we want to determine whether $n=221$ is a prime. Simulate the Fermat primality test for the choices $a=38$ and $a=24$.

Solution.

- First, maybe we pick $a=38$ randomly from $\{2,3,\ldots,219\}$.
  We then calculate that $38^{220} \equiv 1 \pmod{221}$. So far, 221 is behaving like a prime.
- Next, we might pick $a=24$ randomly from $\{2,3,\ldots,219\}$.
  We then calculate that $24^{220} \equiv 81 \not\equiv 1 \pmod{221}$. We stop and conclude that 221 is not a prime.

Important comment. We have done so without finding a factor of n! (Indeed, $221=13\cdot 17$.)

Comment. Since 38 was giving us a false impression regarding the primality of n, it is called a **Fermat liar** modulo 221. Similarly, we say that 24 was a **Fermat witness** modulo 221.

On the other hand, we say that 221 is a **pseudoprime** to the base 38.

Comment. In this example, we were actually unlucky that our first "random" pick was a Fermat liar: only 14 of the 218 numbers (about 6.4%) are liars. As indicated above, for most large composite numbers, the proportion of liars will be exceedingly small.

Example 113. Somewhat suprisingly, there exist composite numbers n with the following disturbing property: every residue a is a Fermat liar or $\gcd(a,n)>1$.

This means that the Fermat primality test is unable to distinguish n from a prime, unless the randomly picked number a happens to reveal a factor (namely, $\gcd(a,n)$) of n (which is exceedingly unlikely for large numbers).
[Recall that, for large numbers, we do not know how to find factors even if that was our primary goal.]

Such numbers are called **absolute pseudoprimes** or Carmichael numbers.

The first few are $561, 1105, 1729, 2465, \ldots$ (it was only shown in 1994 that there are infinitely many of them).
These are very rare, however: there are 43 absolute pseudoprimes less than 10^6. (Versus $78,498$ primes.)

Example 114. (bonus challenge) Show that $561=3\cdot 11\cdot 17$ is an absolute pseudoprime.

Hint. Proceed using the Chinese remainder theorem.

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.
  - 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**.

To be continued...