Example 139. 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 $a \in \{1, 2, ..., n-1\}$

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 $\neg B \Longrightarrow \neg A$.

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 $\{2, 3, ..., n-2\}$.
  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 called a **Fermat liar** modulo n.

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

Flaw. There exist certain composite numbers n (see Definition 141) 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.

There do exist extensions of the Fermat primality test which solve these issues.

[For instance, Miller-Rabin, which checks whether $a^{n-1} \equiv 1 \pmod{n}$ but also checks whether values like $a^{(n-1)/2}$ are congruent to ± 1.]

Advanced comment. If n is composite but not an absolute pseudoprime (see Definition 141), 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.

Example 140. 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 $\{2, 3, ..., 219\}$.
  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 $\{2, 3, ..., 219\}$.
  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. (To wit, $221 = 13 \cdot 17$.)

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 221 is a **pseudoprime** to the base 38.

On the other hand, we say that 24 was a **Fermat witness** modulo 221.

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.

Armin Straub
straub@southalabama.edu

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:

Definition 141. A composite positive integer n is an **absolute pseudoprime** (or Carmichael number) if $a^{n-1}\equiv 1 \pmod n$ holds for any integer a with $\gcd(a,n)=1$.

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 142. Show that 561 is an absolute pseudoprime.

Solution. We need to show that $a^{560}\equiv 1 \pmod{561}$ for all invertible residues a modulo 561.

Since $561=3\cdot 11\cdot 17$, $a^{560}\equiv 1 \pmod{561}$ is eqivalent to $a^{560}\equiv 1 \pmod p$ for each of $p=3,11,17$.

By Fermat's little theorem, we have $a^2\equiv 1 \pmod 3$, $a^{10}\equiv 1 \pmod{11}$, $a^{16}\equiv 1 \pmod{17}$. Since $2, 10, 16$ each divide 560, it follows that indeed $a^{560}\equiv 1 \pmod p$ for $p=3,11,17$.

Comment. Korselt's criterion (1899) states that what we just observed in fact characterizes absolute pseudoprimes. Namely, a composite number n is an absolute pseudoprime if and only if n is squarefree, and for all primes p dividing n, we also have $p-1|n-1$.

Theorem 143. (Korselt's Criterion) A composite positive integer n is an absolute pseudoprime if and only if n is squarefree and $(p-1)|(n-1)$ for any prime divisor p of n.

Proof. Here, we will only consider the "if" part (the "only if" part is also not hard to show but the typical proof requires a little more insight into primitive roots than we currently have).

To that end, assume that n is **squarefree** and that $(p-1)|(n-1)$ for any prime divisor p of n. Let a be any integer with $\gcd(a,n)=1$. We will show that $a^{n-1}\equiv 1 \pmod n$.

n being squarefree means that its prime factorization is of the form $n=p_1\cdot p_2\cdots p_d$ for distinct primes p_i (this is equivalent to saying that there is no integer $m>1$ such that $m^2|n$). By Fermat's little theorem $a^{p_i-1}\equiv 1 \pmod{p_i}$ and, since $(p_i-1)|(n-1)$, we have $a^{n-1}\equiv 1 \pmod{p_i}$ for all p_i. It therefore follows from the Chinese remainder theorem that $a^{n-1}\equiv 1 \pmod n$. □

Comment. Modulo a prime p, Fermat's little theorem implies that $a^p\equiv a \pmod p$ for any integer a. (Why?!) It therefore follows from the above argument that, for an absolute pseudoprime n, we have $a^n\equiv a \pmod n$ for any integer a (and this property characterizes absolute pseudoprimes).

Example 144. Using Sage, determine all numbers n up to 5000, for which 2 is a Fermat liar.

```
Sage] def is_fermat_liar(x, n):
          return not is_prime(n) and power_mod(x, n-1, n) == 1

Sage] [ n for n in [1..5000] if is_fermat_liar(2, n) ]
```

$$[341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681]$$

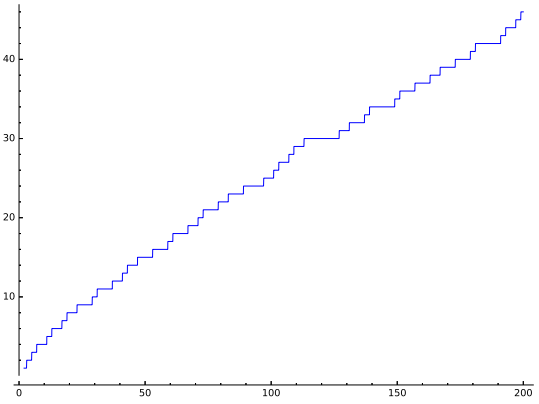
Even if you have never written any code, you can surely figure out what's going on!

Example 145. Playing with the prime number theorem in Sage:

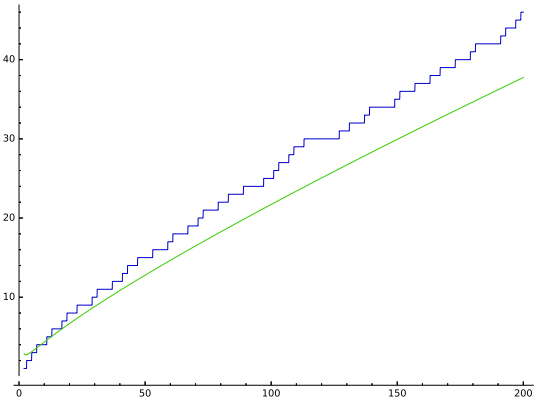
```
Sage] prime_pi(10)
```

$$4$$

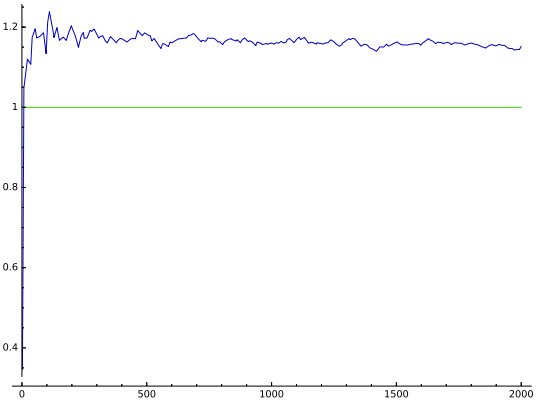
```
Sage] plot(prime_pi(x), 2, 200)
```




```
Sage] plot([prime_pi(x),x/ln(x)], 2, 200)
```




```
Sage] plot([prime_pi(x)/(x/ln(x)), 1], 2, 2000)
```



Comment. As the final plot suggests, the quotient of $\pi(x)$ and $x/\ln(x)$ indeed approaches 1 from above. This is slightly stronger than the PNT, which only claims that the quotient approaches 1.

In particular, as the previous plot suggests, for large x, $x/\ln(x)$ is always an underestimate for $\pi(x)$ (though looking at a plot like this can be very misleading).