Example 99. 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 generic residue).

Example 100. (bonus challenge) If $a^{n-1} \equiv 1 \pmod n$ but $a^{(n-1)/2} \not\equiv \pm 1 \pmod n$, then we can find a factor of n! How?!

For instance. $a = 38$ and $n = 221$ in Example 97.

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...]

Send in a solution by next week for a bonus point!

How many primes are there?

Theorem 101. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there are only finitely many primes: $p_1, p_2, \ldots, p_n$.
Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
None of the p_i divide N (because division of N by any p_i leaves remainder 1).
Thus any prime dividing N is not on our list. Contradiction.

Just being silly. Similarly, there are infinitely many composite numbers.

Indeed, assume (for contradiction) there are only finitely many composites: $m_1, m_2, \ldots, m_n$.
Consider the number $N = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ (don't add 1).
N is not on our list. Contradiction.

Historical note. This is not necessarily a proof by contradiction, and Euclid (300BC) himself didn't state it as such. Instead, one can think of it as a constructive machinery of producing more primes, starting from any finite collection of primes. □

The following famous and deep result quantifies the infinitude of primes.

Theorem 102. (prime number theorem) Let $\pi(x)$ be the number of primes $\leqslant x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

In other words: Up to x, there are roughly $x/\ln(x)$ many primes.

Examples.

proportion of primes up to 10^6: $\frac{78,498}{10^6} = 7.85\%$ vs the estimate $\frac{1}{\ln(10^6)} = \frac{1}{6\ln(10)} = 7.24\%$

proportion of primes up to 10^{12}: $\frac{37,607,912,018}{10^{12}} = 3.76\%$ vs the estimate $\frac{1}{\ln(10^{12})} = \frac{1}{12\ln(10)} = 3.62\%$

An example of huge relevance for crypto.

By the PNT, the proportion of primes up to 2^{2048} is about $\frac{1}{\ln(2^{2048})} = 0.0704\%$.

That means, roughly, 1 in 1500 numbers of this magnitude are prime. That means we (i.e. our computer) can efficiently generate large random primes by just repeatedly generating large random numbers and discarding those that are not prime.

Comment. Here, $\ln(x)$ is the logarithm with base e. Isn't it wonderful how Euler's number $e \approx 2.71828$ is sneaking up on the primes?

Historical comment. Despite progress by Chebyshev (who succeeded in 1852 in showing that the quotient in the above limit is bounded, for large x, by constants close to 1), the PNT was not proved until 1896 by Hadamard and, independently, de la Vallée Poussin, who both used new ideas due to Riemann.

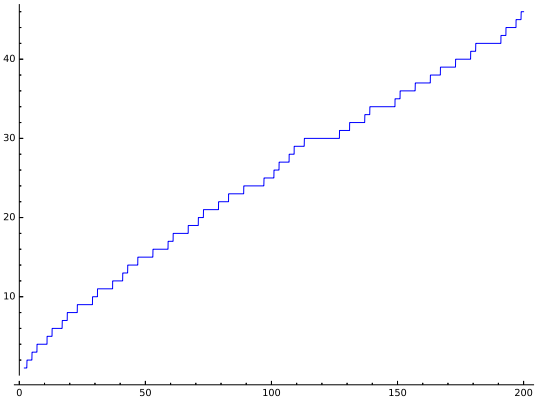
Armin Straub
straub@southalabama.edu

Example 103. Playing with the prime number theorem in Sage:

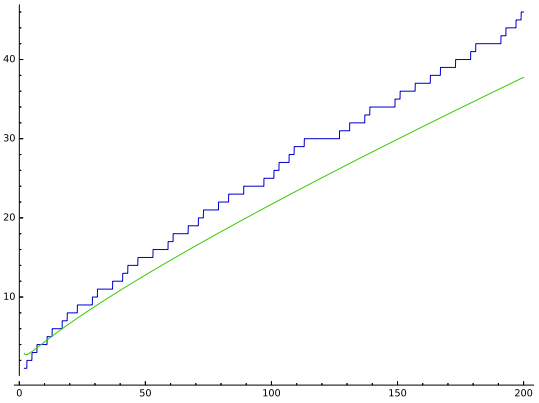
```
Sage] prime_pi(10)
```

```
4
```

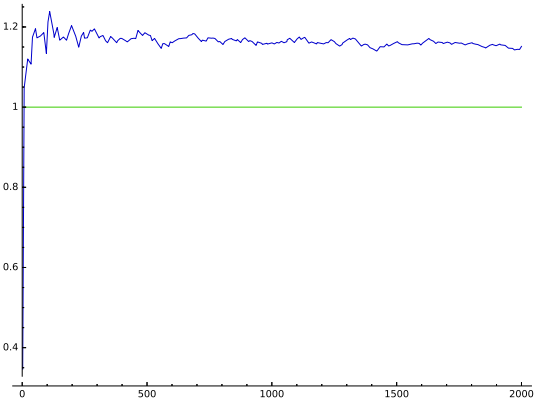
```
Sage] plot(prime_pi(x), 2, 200)
```




```
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).

Example 104. In 12/2018, a new largest (proven) prime was found: $2^{82,589,933}-1$.

https://www.mersenne.org/primes/?press=M82589933

This is a **Mersenne prime** (like the last 17 record primes). It has a bit over 24.8 million (decimal) digits (versus 23.2 for the previous record). The prime was found as part of GIMPS (Great Internet Mersenne Prime Search), which offers a $3,000 award for each new Mersenne prime discovered.

The EFF (Electronic Frontier Foundation) is offering $150,000 (donated anonymously for that specific purpose) for the discovery of the first prime with at least 100 million decimal digits.

https://www.eff.org/awards/coop

[Prizes of $50,000 and $100,000 for primes with 1 and 10 million digits have been claimed in 2000 and 2009.]

Definition 105. A **Mersenne prime** is a prime of the form 2^n-1.

For instance. The first few Mersenne primes have exponents $2,3,5,7,13,17,19,31,61,89,107,\ldots$ All of these exponents are primes (but not all primes work: for instance, $2^{11}-1=23\cdot 89$). See below.

Anecdote. Euler proved in 1772 that $2^{31}-1$ is prime (then, and until 1867, the largest known prime).
"$2^{31}-1$ is probably the greatest [Mersenne prime] that ever will be discovered; for as they are merely curious, without being useful, it is not likely that any person will attempt to find one beyond it." — P. Barlow, 1811

https://en.wikipedia.org/wiki/2,147,483,647

Mersenne primes give rise precisely to all even perfect numbers (numbers whose proper divisors sum to the number itself; for instance, 6 is perfect because $6=1+2+3$). Indeed, Euclid showed that, if 2^p-1 is prime, then $2^{p-1}(2^p-1)$ is perfect [$p=2$: $2\cdot 3=6$, $p=3$: $4\cdot 7=28=1+2+4+7+14$, $p=5$: $16\cdot 33=528$, ...]. It is not known whether odd perfect numbers exist.

Example 106. (geometric sum) Evaluate $1+x+x^2+\ldots+x^n$.

Solution. $(1+x+x^2+\ldots+x^n)(x-1)=x^{n+1}-1$, so that $1+x+x^2+\ldots+x^n=\frac{x^{n+1}-1}{x-1}$.

Geometric series. In particular, $\sum_{k=1}^{\infty} x^k=\lim_{n\to\infty}\frac{x^{n+1}-1}{x-1}=\frac{1}{1-x}$, provided that $|x|<1$.

Lemma 107. If $r \mid n$, then $x^r-1 \mid x^n-1$.

Proof. Write $n=rs$. It follows from $x^s-1=(x-1)(1+x+x^2+\ldots+x^{s-1})$ that
$x^{rs}-1=(x^r-1)(1+x^r+x^{2r}+\ldots+x^{r(s-1)})$. □

Corollary 108. 2^n-1 can only be prime if n is prime.

Proof. It follows from the previous lemma that, if $n=rs$ is composite, then 2^n-1 is divisible by 2^r-1 (as well as 2^s-1). □

For instance. $2^6-1=63$ is divisible by both $2^2-1=3$ and $2^3-1=7$.

Armin Straub
straub@southalabama.edu