Example 77. How can we can compute the inverse of a modulo p via Fermat's little theorem?

Solution. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$.

Write $a^{p-1} = a \cdot a^{p-2}$ to see that it follows that $a^{-1} \equiv a^{p-2} \pmod{p}$.

For instance. Suppose we would like to compute $2^{-1} \pmod{7}$.

Since $2^6 \equiv 1 \pmod{7}$, by little Fermat, we conclude that $2^{-1} \equiv 2^5 = 32 \equiv 4 \pmod{7}$.

Comment. A similar approach (based on Euler's theorem, which we will discuss shortly) would work for computing inverses modulo composite numbers n. However, in that case, we essentially need to know the prime factorization of n, which is impractical for large n.

Example 78. (divisibility by 9) A number $n = (a_m a_{m-1} \cdots a_0)_{10}$ is divisible by 9 if and only if the sum of its decimal digits $a_m + a_{m-1} + \ldots + a_0$ is divisible by 9.

Why? Note that $10^r \equiv 1^r \equiv 1 \pmod{9}$ for any integer $r \geqslant 0$.

In particular, $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \pmod{9}$.

For instance. 1234567 is not divisible by 9 because $1 + 2 + 3 + \ldots + 7 = \frac{7(7+1)}{2} = 28$ is not divisible by 9. In fact, $1234567 \equiv 28 \equiv 10 \equiv 1 \pmod{9}$.

Example 79. (divisibility by 11) A number $n = (a_m a_{m-1} \cdots a_0)_{10}$ is divisible by 11 if and only if the alternating sum of its decimal digits $(-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots + a_0$ is divisible by 11.

Why? Note that $10^r \equiv (-1)^r \pmod{11}$ for any integer $r \geqslant 0$. In particular,

$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv (-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots - a_1 + a_0 \pmod{11}$.

For instance. 123456 is not divisible by 11 because $6 - 5 + 4 - 3 + 2 - 1 = 3$ is not divisible by 11. In fact, $123456 \equiv 3 \pmod{11}$.

Example 80. Bases 2, 8 and 16 (binary, octal and hexadecimal) are commonly used in computer applications.

For instance, in JavaScript or Python, $0\text{b}\ldots$ means $(\ldots)_2$, $0\text{o}\ldots$ means $(\ldots)_8$, and $0\text{x}\ldots$ means $(\ldots)_{16}$.

The digits $0, 1, \ldots, 15$ in hexadecimal are typically written as $0, 1, \ldots, 9, A, B, C, D, E, F$.

Problem. Which number is 0xD1?

Solution. $0\text{xD1} = 13 \cdot 16 + 1 = 209$.

The South Alabama Jaguar NCAA team color code is 0xD11241. That means $\text{RGB}(209, 18, 65)$, where each value (ranging from 0 to 255) quantifies the amount of red (R), green (G) and blue (B).

For instance, 0x000000 is black, and 0xFF0000 is red, and 0xFFFFFF is white.

We can thus see that the color 0xD11241 is close to a red (though not a pure one).

Example 81. (terrible jokes, parental guidance advised)

There is 10 types of people... those who understand binary, and those who don't.

Of course, you knew that. How about:

There are II types of people... those who understand Roman numerals, and those who don't.

It's not getting any better:

There are 10 types of people... those who understand hexadecimal, F the rest...

Example 82. (yet another joke) Why do mathematicians confuse Halloween and Christmas?

Because 31 Oct = 25 Dec.

Get it? $(31)_8 = 1 + 3 \cdot 8 = 25$ equals $(25)_{10} = 25$.

Fun borrowed from: `https://en.wikipedia.org/wiki/Mathematical_joke`

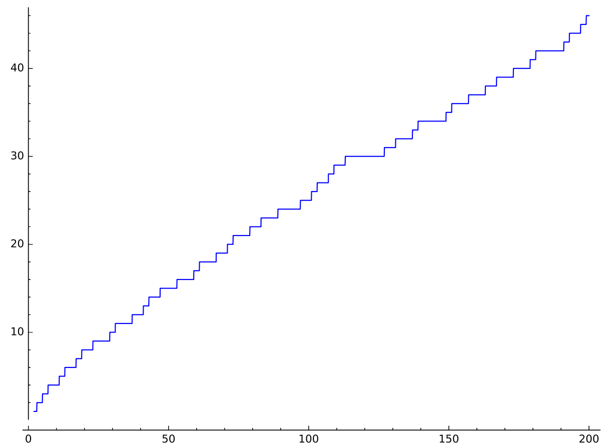
Armin Straub
straub@southalabama.edu

Example 83. Playing with the prime number theorem in Sage:

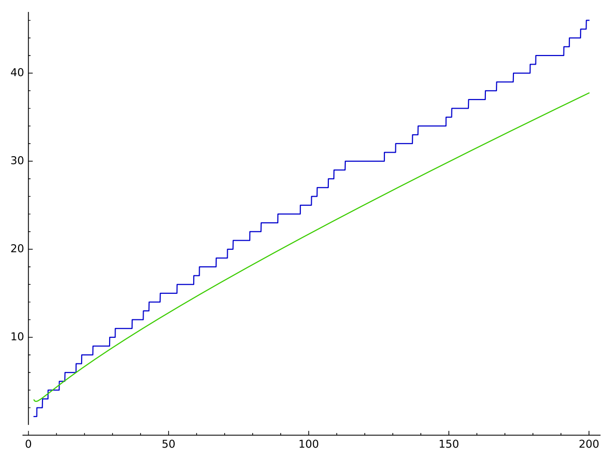
```
Sage] prime_pi(10)
```

4

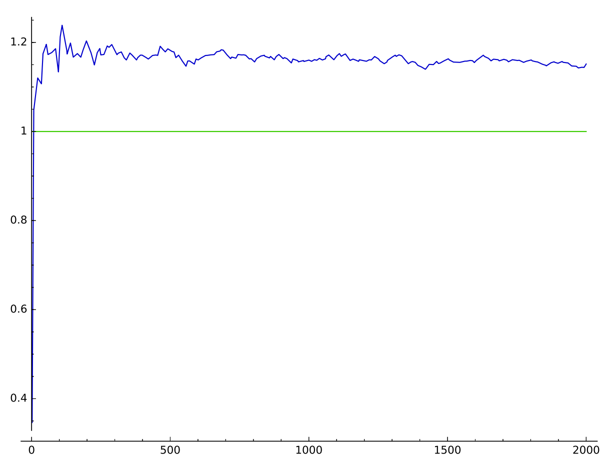
```
Sage] plot(prime_pi(x), 2, 200)
```




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




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



Armin Straub
straub@southalabama.edu