Example 55. The **sieve of Eratosthenes** is an efficient way to find all primes up to some n.

Write down all numbers $2, 3, 4, \ldots, n$. We begin with 2 as our first prime. We proceed by crossing out all multiples of 2, because these are not primes. The smallest number we didn't cross out is 3, our next prime. We again proceed by crossing out all multiples of 3, because these are not primes. The smallest number we didn't cross out is 5 (note that it has to be prime because, by construction, it is not divisible by any prime less than itself).

Problem. If $n = 10^6$, at which point can we stop crossing out numbers?

We can stop when our "new prime" exceeds $\sqrt{n} = 1000$. All remaining numbers have to be primes. Why?!

Theorem 56. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is 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. □

The following two famous results say a bit more about the infinitude of primes.

- **Bertrand's postulate**: for every $n > 1$, the interval $(n, 2n)$ contains at least one prime.
  conjectured by Bertrand in 1845 (he checked up to $n = 3 \cdot 10^6$), proved by Chebyshev in 1852
- **Prime number theorem**: up to x, there are roughly $x / \ln(x)$ many primes
  proportion of primes up to 10^6: $\frac{78,498}{10^6} = 7.850\%$ vs $\frac{1}{\ln(10^6)} = \frac{1}{6\ln(10)} = 7.238\%$
  proportion of primes up to 10^9: $\frac{50,847,534}{10^9} = 5.085\%$ vs $\frac{1}{\ln(10^9)} = 4.825\%$
  proportion of primes up to 10^{12}: $\frac{37,607,912,018}{10^{12}} = 3.761\%$ vs $\frac{1}{\ln(10^{12})} = 3.619\%$

Theorem 57. The gaps between primes can be arbitrarily large.

Proof. Indeed, for any integer $n > 1$,

$$n! + 2, \quad n! + 3, \quad \ldots, \quad n! + n$$

is a string of $n - 1$ composite numbers. Why are these numbers all composite!? □

Comment. Notice how astronomically huge the numbers brought up in the proof are!

5 Congruences

$$a \equiv b \pmod{n} \qquad \text{means} \qquad a = b + mn \quad (\text{for some } m \in \mathbb{Z})$$

In that case, we say that "a is congruent to b modulo n".

- In other words: $a \equiv b \pmod{n}$ if and only if $a - b$ is divisible by n.
- In even other words: $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when dividing by n.

Example 58. $17 \equiv 5 \pmod{12}$ as well as $17 \equiv 29 \equiv -7 \pmod{12}$

Example 59. We will discuss in more detail next time that we can calculate with congruences. Here is an appetizer: What is 2^{100} modulo 3? That is, what's the remainder upon division by 3?

Solution. $2 \equiv -1 \pmod{3}$. Hence, $2^{100} \equiv (-1)^{100} = 1 \pmod{3}$.

Armin Straub
straub@southalabama.edu