Theorem: There are infinitely many primes.

Proof: Suppose there are only finitely many primes:

$$p_1, p_2, p_3, \dots, p_k$$

Multiply the primes and add 1:

let $N = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$

Which primes divide N?

p_1 cannot divide N, since N is one more than a multiple of p_1

p_2 cannot dive N for the same reason

Similarly, $p_3, \dots, p_k$ cannot divide N

So N is not divisible by any prime.

Thus: either N is prime, or N has a prime factor that wasn't in our list.

Either option contradicts our assumption.

Therefore, there are infinitely many primes. ∎

Sieve of Eratosthenes

Implementing the sieve in Python

- Start with a list of integers
- Deleting from lists is computationally expensive
- Instead of deleting, simply mark composite numbers as not prime.

If I want to find primes up to N, I only have to consider factors up to $\sqrt{N}$.

Why? Suppose $N = a \cdot b$

If $a > \sqrt{N}$ and $b > \sqrt{N}$, then $a \cdot b > \sqrt{N} \cdot \sqrt{N} = N$, which is not possible since $N = a \cdot b$.

So if $N = a \cdot b$, then either a or b has to be $\leq \sqrt{N}$.