THEOREM: There are infinitely many prime numbers.

proof: Assume there are finitely many prime numbers, namely

$$p_1, p_2, p_3, p_4, \dots, p_k$$

Multiply all the primes together and add 1:

Let $N = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_k + 1$

N cannot be prime, since it is larger than any prime in my original list.

So N must have some prime factor.

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

p_2 also cannot divide N

By the same reasoning, none of $p_1, p_2, \dots, p_k$ can divide N. This is a contradiction!

Therefore, there must be infinitely many primes.

Sieve of Eratosthenes

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~ = N

Python Implementation

- Start with a list
  2, 3, 4, ..., nMax
- deleting from lists is computationally problematic
- "cross off" numbers by replacing them with a different value, say $\emptyset$.
- No division or modulus is necessary – just addition!

If I want to find all primes up to N,
then I can stop crossing off after $\sqrt{N}$.

Why? If $N = a \cdot b$, then either $a \le \sqrt{N}$ or $b \le \sqrt{N}$.

Suppose not: $a > \sqrt{N}$ and $b > \sqrt{N}$

then $a \cdot b > \sqrt{N} \cdot \sqrt{N} = N$ contradiction,
since $ab = N$