UNBOUNDED FUNCTION: $f(x)$ is unbounded if, for any (big) number M, there exists some x such that $f(x) > M$.

For the Mean-Median project, $f(\vec{x})$ is the number of steps, starting with sequence $\vec{x}$, until the iterative process stabilizes (becomes constant).

Prime Numbers: 2, 3, 5, 7, 11, 13, 17, 19, ...

A prime number p is an integer greater than 1 that has only two factors: 1 and p.

How many primes are there? Infinitely many.

Why? Assume there are finitely many primes:

$$2, 3, 5, 7, \ldots, p$$

Then let $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p) + 1$.

Note: n is not divisible by 2, or 3, or 5, or 7, or by any prime.

So n itself must be prime, but it wasn't in our list of all primes.

This is a contradiction, so there must be infinitely many primes.

CURRENT RECORDS:

- Biggest known prime (Dec. 2018): $2^{82,589,933} - 1$, which has 24,862,048 digits
  (Mersenne Prime)
- RSA-250, a 250-digit number with exactly 2 prime factors, was factored (Feb. 2020)

This took roughly 2700 "core-years" of computing time.

- Arbitrary numbers up to about 200 digits can be factored.
- Arbitrary numbers of more than 15,000 digits can be proven prime.

Question: How would you determine if a positive integer n is prime or not?

Think and sketch an algorithm on paper before writing code.

want: `isPrime[n]`:

argument: n is a positive integer

return: True if n is prime, False otherwise

USEFUL FUNCTIONS:

`Divisible[n,k]` returns **True** if **n** is divisible by **k**, and **False** otherwise

`Mod[n,k]` returns the remainder when **n** is divided by **k**

LEMMA: If n is composite, then it has some factor m such that $1 < m \leq \sqrt{n}$.

proof: If $n = mk$, with $m > \sqrt{n}$ and $k > \sqrt{n}$, then $mk > n$, a contradiction.