Prime Number: An integer $n > 1$ is prime if its only factors are 1 and n.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

How many primes are there? **Infinitely many.**

proof: Assume there are finitely many primes: $2, 3, 5, 7, \ldots, p$ (list of all primes)

Let $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$ (product of all primes)

Is n divisible by 2? No.
.. ... by 3? No.
.. by p? No

n is not divisible by any prime

So n must be prime, but n is not in our list of all primes. Contradiction.

Thus, there are infinitely many primes.

CURRENT RECORDS:

- Largest known prime: $2^{82\,589\,933} - 1$, which has 24,862,048 decimal digits
- Arbitrary numbers up to about 15000 digits can be proved prime.
- Arbitrary numbers up to 200 digits can be factored.
- Feb. 2020: RSA-250 factored (250 decimal digits)

Question: How to determine if an integer n is prime?

WANT: isPrime[n]

returns True if n is prime,
False otherwise

useful functions: Divisible[n, k] — returns True if k divides n,
False otherwise

Mod[n, k] — returns the remainder of n divided by k

Plan: test whether $2, 3, 4, 5, 6, \ldots, \frac{n}{2}$ divides n

pseudocode

```
isPrime[n]:
    i=2
    while i < n/2:
        if i divides n, then return False
        i += 1
    return True
```