PRIME NUMBERS: A number p is prime if its only factors are 1 and p.

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

How many primes are there? infinitely many

Assume there are finitely many primes: $2, 3, 5, \ldots, p$ (the biggest prime)

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

Is n prime? No, since it was not in our list of all primes.

But n is not divisible by 2, or 3, or 5, etc...

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

CURRENT RECORDS:

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

Question: How would you determine if a positive integer n is prime?

want: isPrime[n] returns True if n is prime; False otherwise

useful functions: Divisible[n, k] returns True iff k divides n

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

Idea: check whether n is divisible by $2, 3, 4, \ldots, n-1$

$\sqrt{n}$

For big n, $\sqrt{n} < \frac{n}{2}$

Lemma: If n is composite, then it has a factor $1 < m \leq \sqrt{n}$.

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

pseudocode: isPrime[n]:

Do for $k = 2, 3, \ldots, \sqrt{n}$:
does k divide n?
Yes: return ~~True~~ False
(No: keep dividing)
return ~~False~~ True

Return[False]
↑
quits the Module