PRIME: A integer $n \geq 2$ is prime if its only factors are 1 and n.

2, 3, 5, 7, 11, 13, 17, 19, ...

Current Records:

- Largest known prime: $2^{82,589,933} - 1$
  - has more than 24 million digits
- Arbitrary numbers of about 15,000 digits can be proven prime
- Factoring: in 2020, RSA-250 was factored into 2 primes
  this took 2700 core-years
- Arbitrary numbers of about 200 digits can be factored

Basic primality testing:

algorithm: isPrime(n)
input: integer $n \geq 2$
output: True if n is prime, False otherwise

```
def isPrime(n):
    for i in range(2, n):      # i counts 2, 3, 4, 5, 6, ..., n-1
        if n % i == 0:         # if i divides n
            print(n, "is divisible by", i)
            return False
    return True
```

- In $n = a \cdot b$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Why? if $a > \sqrt{n}$ and $b > \sqrt{n}$, then

$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction.