5 April 2024

An integer $n \geq 2$ is **prime** if its only divisors are 1 and itself.

An integer $n \geq 2$ is **composite** if it has a divisor other than 1 and n

Note: 1 is neither prime nor composite (by definition).

How to determine whether a number is prime?

example: $n = 2,931,133 = 1031 \cdot 2843$

idea: check for divisors, but this might take a while

CURRENT RECORDS

- Arbitrary numbers up to 200 digits or so can be factored.
- Feb. 2020: RSA-250 (250 digits, 2 prime factors) was factored
  This took 2700 core-years of computing time.
- Arbitrary numbers of more than 15,000 digits can be proven prime.
- Largest known prime: $2^{82589933} - 1$ (Dec. 2018)
  this has 24,862,048 digits

Write a function: isPrime(n)

INPUT: integer $n \geq 2$

OUTPUT: True if n is prime,
False otherwise

Return value