

PRIME NUMBERS

A positive integer $n \geq 2$ is prime if and only if its only divisors are 1 and n .

A positive integer $n \geq 2$ is composite if it has some divisor other than 1 and n .

Note: 1 is neither prime nor composite.

How do we determine whether n is prime?

Check for divisors $2, 3, 4, \dots, n-1$.

Example: $n = 2,931,133 = 1031 \times 2843$

CURRENT RECORDS

- Arbitrary numbers up to about 200 digits can be factored.
- Feb. 2020: RSA-250 (250 digits) was factored (2 primes)
2700 core-years of CPU time
- Currently: \$75,000 prize for factoring RSA 896 (270 digits)
- Arbitrary numbers of 15,000 digits can be proven prime.
- Largest known prime: $2^{136,279,841} - 1$ (41 million digits)
discovered Oct. 2024
- Currently: \$150,000 prize for discovery of a prime with
at least 100 million digits

function isPrime(^{argument}n):

input: a positive integer n

output: True if n is prime

False otherwise