

Prime Numbers

[Read this note online](#)

A prime number is a positive integer greater than 1 whose only positive divisors are 1 and itself. The primes, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ..., are the building blocks of the integers: every positive integer can be factored into primes in exactly one way (up to order). Primes are central to number theory, cryptography, and surprisingly to the random-looking statistics of complex systems. The study of their distribution is one of the oldest open problems in mathematics.

Primality is about divisibility of integers greater than 1. A useful test should explain why checking can stop at the square root.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

A prime number has exactly two divisors: 1 and itself

A prime number has exactly two positive divisors: 1 and itself. Primes are the building blocks of the integers.

Definition

A natural number $p > 1$ is prime if its only positive divisors are 1 and p itself. A natural number greater than 1 that is not prime is **composite**: it has at least one divisor other than 1 and itself. The number 1 is neither prime nor composite (by convention, to make the Fundamental Theorem of Arithmetic clean).

First 25 primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

The Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be written as a product of primes in essentially one way:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$$

where the p_i are distinct primes and the a_i are positive integers. The factorization is unique up to the order of the factors. Example: $360 = 2^3 \cdot 3^2 \cdot 5$. No other prime factorization of 360 exists.

Euclid's Theorem: Infinitely Many Primes

There are infinitely many primes. Euclid proved this around 300 BCE.

Proof sketch. Suppose only finitely many primes exist: $p_1, p_2, \dots, p_k$. Consider $N = p_1 p_2 \cdots p_k + 1$. Either N is itself prime (a new prime not in the list), or N has a prime factor, but that factor cannot be any of $p_1, \dots, p_k$ (because N leaves a remainder of 1 when divided by any of them). Either way, we have a prime not in the original list. Contradiction. So no finite list captures all the primes.

Distribution of Primes

Primes thin out as numbers get larger, but they never stop. The **Prime Number Theorem** (Hadamard and de la Vallée Poussin, 1896) makes the thinning precise:

$$\pi(x) \sim \frac{x}{\ln x}$$

where $\pi(x)$ is the number of primes $\leq x$. So among the first 10^9 numbers, about $10^9 / \ln(10^9) \approx 4.83 \times 10^7$ are prime, roughly 1 in 21.

The largest known prime as of 2026 is a Mersenne prime with over 41 million digits. Finding huge primes is a popular distributed-computing pursuit (GIMPS, Great Internet Mersenne Prime Search).

Sieve of Eratosthenes

The classic way to find primes up to N :

1. Write down all integers from 2 to N .
2. Cross out all multiples of 2 except 2 itself.
3. Move to the next number not crossed out (3) and cross out all its multiples except itself.
4. Repeat until the next number to check exceeds $\sqrt{N}$. All remaining numbers are prime.

Eratosthenes (3rd century BCE) gave this method; it's still the fastest way to find *all* primes up to a moderate bound.

Primality Tests vs. Factoring

Testing whether a number is prime is computationally *easy*: the AKS algorithm (2002) runs in polynomial time. The Miller-Rabin probabilistic test is fast and gives near-certainty of primality very quickly. Factoring a composite number into its prime factors, on the other hand, is computationally *hard*, no polynomial-time classical algorithm is known. This asymmetry is exactly what makes RSA encryption work.

Applications

- **RSA cryptography.** Pick two large primes p and q , multiply them to get $n = pq$. The product n is the public key; the primes are the private key. Factoring n to recover p and q is computationally infeasible at typical key sizes (~2048 bits), which makes RSA secure.
- **Hashing.** Hash table sizes are typically prime to spread keys evenly; prime moduli reduce clustering.
- **Random number generation.** Many pseudo-random generators use prime moduli to maximize period length.
- **Pure number theory.** The Riemann Hypothesis, the most famous open problem in mathematics, concerns the distribution of primes. A million-dollar Clay Millennium Prize is offered for a proof.
- **Coding theory.** Reed-Solomon codes and other error-correcting codes operate over finite fields, which have prime (or prime power) sizes.

Related study notes: [Modular Arithmetic](#), [Fundamental Theorem of Algebra](#), Cryptography, Euclidean Algorithm.

The related [OpenStax mathematics textbooks](#) provide additional explanations and exercises for the mathematical definitions used here.

Testing for a Factor

To test 97, checking prime divisors no greater than its square root is sufficient. Since the square root is less than 10, the candidates are 2, 3, 5 and 7. None divides 97, so 97 is prime.

If a composite number factors as ab , both factors cannot exceed its square root: their product would then exceed the number. At least 1 factor is therefore small enough to be found by the test. For 91, divisibility by 7 reveals $91 = 7 \times 13$.

The points to check in this example are:

- 1 is neither prime nor composite.
- 2 is the only even prime.
- A composite integer has a prime divisor no greater than its square root.

Check Your Understanding

Try the questions before reading the answers.

Question 1. Is 121 prime?

Answer. No. It is 11×11 .

Question 2. Does a number ending in 5 have to be composite?

Answer. Every such positive integer greater than 5 is composite; 5 itself is prime.

Frequently Asked Questions

What is a prime number?

A positive integer greater than 1 whose only positive divisors are 1 and itself. The primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29... A number greater than 1 that isn't prime is called composite (e.g., $4 = 2 \times 2$, $6 = 2 \times 3$).

Why isn't 1 considered a prime?

By convention. If we allowed 1 to be prime, the Fundamental Theorem of Arithmetic (unique factorization) would break, because we could insert any number of 1s into any factorization. Excluding 1 keeps the statement clean: every integer > 1 has exactly one prime factorization.

Are there infinitely many primes?

Yes. Euclid proved this around 300 BCE. The argument: assume only finitely many primes exist, multiply them all together, add 1. The result isn't divisible by any of the original primes, so it has a new prime factor, contradicting the assumption that the list was complete. So no finite list contains all primes.

How rare are primes among large numbers?

By the Prime Number Theorem, the density of primes near a number N is approximately $1/\ln(N)$. So roughly 1 in 23 of the 10-digit numbers is prime, and roughly 1 in 230 of the 100-digit numbers is prime. They thin out, but they never stop appearing.

Why are primes important in cryptography?

Because multiplying two large primes is easy but factoring the result is hard. RSA encryption picks two ~1024-bit primes and multiplies them to get a ~2048-bit public key. To break RSA, you'd need to factor that number, and no classical algorithm can do this in reasonable time for keys of this size. Quantum computers (Shor's algorithm) can, which is why post-quantum cryptography is now an active field.

What is the largest known prime?

As of 2026, the largest known prime is a Mersenne prime (a prime of the form $2^p - 1$) with over 41 million digits. The GIMPS (Great Internet Mersenne Prime Search) project finds these using distributed computing. New Mersenne primes are discovered every few years, each becoming the new record.