Prime number

A **prime number** (or a **prime**) is a natural number greater than 1 that has no positive divisors other than 1 and itself. A natural number greater than 1 that is not a prime number is called a composite number. For example 5 is prime, as only 1 and 5 divide it, whereas 6 is composite, since it has the divisors 2 and 3 in addition to 1 and 6. The fundamental theorem of arithmetic establishes the central role of primes in number theory: any integer greater than 1 can be expressed as a product of primes that is unique up to ordering. This theorem requires excluding 1 as a prime.

The property of being prime is called primality. A simple but slow method of verifying the primality of a given number n is known as trial division. It consists of testing whether n is a multiple of any integer between 2 and $\sqrt{n}$. Algorithms that are much more efficient than trial division have been devised to test the primality of large numbers. Particularly fast methods are available for primes of special forms, such as Mersenne primes. As of 2011, the largest known prime number has nearly 13 million decimal digits.

There are infinitely many primes, as demonstrated by Euclid around 300 BC. There is no known useful formula that yields all of the prime numbers and no composites. However, the distribution of primes, that is to say, the statistical behaviour of primes in the large, can be modeled. The first result in that direction is the prime number theorem, proven at the end of the 19th century, which says that the probability that a given, randomly chosen number n is prime is inversely proportional to its number of digits, or the logarithm of n.

Many questions around prime numbers remain open, such as Goldbach's conjecture, which asserts that every even integer greater than 2 can be expressed as the sum of two primes, and the twin prime conjecture, which says that there are infinitely many pairs of primes whose difference is 2. Such questions spurred the development of various branches of number theory, focusing on analytic or algebraic aspects of numbers. Primes are used in several routines in information technology, such as public-key cryptography, which makes use of properties such as the difficulty of factoring large numbers into their prime factors. Prime numbers give rise to various generalizations in other mathematical domains, mainly algebra, such as prime elements and prime ideals.

Definition and examples

A natural number

$$1, 2, 3, 4, 5, 6, \ldots$$

is called a **prime** or a **prime number** if it is greater than 1 and has exactly two divisors, 1 and the number itself. Natural numbers greater than 1 that are not prime are called *composite*.

Among the numbers 1 to 6, the numbers 2, 3, and 5 are the prime numbers, while 1, 4, and 6 are not prime. 1 is excluded as a prime number, for reasons explained below. 2 is a prime number, since the only natural numbers dividing it are 1 and 2. Next, 3 is prime, too: 1 and 3 do divide 3 without remainder, but 3 divided by 2 gives remainder 1. Thus, 3 is prime. However, 4 is composite, since 2 is another number (in addition to 1 and 4) dividing 4 without remainder:

$$4 = 2 \cdot 2.$$

5 is again prime: none of the numbers 2, 3, or 4 divide 5. Next, 6 is divisible by 2 or 3, since

$$6 = 2 \cdot 3.$$

Hence, 6 is not prime. The image at the right illustrates that 12 is not prime: $12 = 3 \cdot 4$. More generally, no even number greater than 2 is prime: any such number n has at least three distinct divisors, namely 1, 2, and n. This implies that n is not prime. Accordingly, the term *odd prime* refers to any prime number greater than 2. In a similar vein, all prime numbers bigger than 5, written in the usual decimal system, end in 1, 3, 7 or 9, since even numbers are multiples of 2 and numbers ending in 0 or 5 are multiples of 5.

If n is a natural number, then 1 and n divide n without remainder. Therefore, the condition of being a prime can also be restated as: a number is prime if it is greater than one and if none of

$$2, 3, ..., n - 1$$

divides n (without remainder). Yet another way to say the same is: a number $n > 1$ is prime if it cannot be written as a product of two integers a and b, both of which are larger than 1:

$$n = a \cdot b.$$

In other words, n is prime if n items can not be divided up into smaller equal-sized groups of more than one item.

The smallest 168 prime numbers (all the prime numbers under 1000) are:

> 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, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769,

773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997 (sequence A000040 in OEIS).

The set of all primes is often denoted **P**.

The fundamental theorem of arithmetic

The crucial importance of prime numbers to number theory and mathematics in general stems from the *fundamental theorem of arithmetic*, which states that every positive integer larger than 1 can be written as a product of one or more primes in a way which is unique except possibly for the order of the prime factors. Primes can thus be considered the “basic building blocks” of the natural numbers. For example:

$$\begin{aligned} 23244 &= 2 \cdot 2 \cdot 3 \cdot 13 \cdot 149 \\ &= 2^2 \cdot 3 \cdot 13 \cdot 149. \end{aligned}$$ (2^2 denotes the square or second power of 2.)

As in this example, the same prime factor may occur multiple times. A decomposition:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_t$$

of a number n into (finitely many) prime factors p_1, p_2, ... to p_t is called *prime factorization* of n. The fundamental theorem of arithmetic can be rephrased so as to say that any factorization into primes will be identical except for the order of the factors. So, albeit there are many prime factorization algorithms to do this in practice for larger numbers, they all have to yield the same result.

If p is a prime number and p divides a product ab of integers, then p divides a or p divides b. This proposition is known as Euclid's lemma. It is used in some proofs of the uniqueness of prime factorizations.

The number of prime numbers

There are infinitely many prime numbers. Another way of saying this is that the sequence

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

of prime numbers never ends. This statement is referred to as *Euclid's theorem* in honor of the ancient Greek mathematician Euclid, since the first known proof for this statement is attributed to him. Many more proofs of the infinitude of primes are known, including an analytical proof by Euler, Goldbach's proof based on Fermat numbers,[11] Fürstenberg's proof using general topology, and Kummer's elegant proof.[13]

Testing primality and integer factorization

There are various methods to determine whether a given number *n* is prime. The most basic routine, trial division is of little practical use because of its slowness. One group of modern primality tests is applicable to arbitrary numbers, while more efficient tests are available for particular numbers. Most such methods only tell whether *n* is prime or not. Routines also yielding one (or all) prime factors of *n* are called factorization algorithms.

Trial division

The most basic method of checking the primality of a given integer *n* is called *trial division*. This routine consists in dividing *n* by each integer *m* which is greater than 1 and less than or equal to the square root of *n*. If the result of any of these divisions is an integer, then *n* is not a prime, otherwise, it is a prime. Indeed, if $n = ab$ is composite (with a and $b \neq 1$) then one of the factors *a* or *b* is necessarily at most $\sqrt{n}$. For example, for $n = 37$, the trial divisions are by $m = 2, 3, 4, 5$, and 6. None of these numbers divides 37, so 37 is prime. This routine can be implemented more efficiently if a complete list of primes up to $\sqrt{n}$ is known—then trial divisions only need to be checked for those *m* that are prime. For example, to check the primality of 37, only three divisions are necessary ($m = 2, 3$, and 5), given that 4 and 6 are composite.

While a simple method, trial division quickly becomes impractical for testing large integers because the number of possible factors grows too rapidly as *n* increases. According to the prime number theorem explained below, the number of prime numbers less than $\sqrt{n}$ is approximately given by $\sqrt{n} / \ln(\sqrt{n})$, so the algorithm may need up to this number of trial divisions to check the primality of *n*. For $n = 10^{20}$, this number is 450 million—too large for many practical applications.

Sieves

An algorithm yielding all primes up to a given limit, such as required in the trial division method, is called a sieve. The oldest example, the sieve of Eratosthenes (see above) is useful for relatively small primes. The modern sieve of Atkin is more complicated, but faster when properly optimized. Before the advent of computers, lists of primes up to bounds like 10^7 were also used.

Primality testing vs. primality proving

Modern primality tests for general numbers *n* can be divided into two main classes, probabilistic (or "Monte Carlo") and deterministic algorithms. The former merely "test" whether *n* is prime in the sense that they declare *n* to be (definitely) composite or "probably prime", which latter means that *n* may or may not be a prime number. Composite numbers which do pass a given primality test are referred to as pseudoprimes. For example, Fermat's primality test relies on Fermat's little theorem. This theorem says for any prime number *p*, and any integer *a* not divisible by *p*, $a^{p-1} - 1$ is divisible by *p*. Thus, if $a^{n-1} - 1$ is not divisible by *n*, *n* cannot be prime. However, conversely, *n* may be composite even if this divisibility holds. In fact, there are infinitely many composite numbers *n* which pass the Fermat primality test for every choice of *a* that is coprime with *n* (Carmichael numbers), for example *n* = 561.

Applications

For a long time, number theory in general, and the study of prime numbers in particular, was seen as the canonical example of pure mathematics, with no applications outside of the self-interest of studying the topic. In particular, number theorists such as British mathematician G. H. Hardy prided themselves on doing work that had absolutely no military significance.[37] However, this vision was shattered in the 1970s, when it was publicly announced that prime numbers could be used as the basis for the creation of public key cryptography algorithms. Prime numbers are also used for hash tables and pseudorandom number generators.

Some rotor machines were designed with a different number of pins on each rotor, with the number of pins on any one rotor either prime, or coprime to the number of pins on any other rotor. This helped generate the full cycle of possible rotor positions before repeating any position.

The International Standard Book Numbers work with a check digit, which exploits the fact that 11 is a prime.

Arithmetic modulo a prime and finite fields

Modular arithmetic modifies usual arithmetic by only using the numbers

$$\{0, 1, 2, \dots, n-1\},$$

where *n* is a fixed natural number called modulus. Calculating sums, differences and products is done as usual, but whenever a negative number or a number greater than *n*−1 occurs, it gets replaced by the remainder after division by *n*. For instance, for *n* = 7, the sum 3 + 5 is 1 instead of 8, since 8 divided by 7 has remainder 1. This is referred to by saying "3 + 5 is congruent to 1 modulo 7" and is denoted

$$3 + 5 \equiv 1 \pmod 7.$$

Similarly, 6 + 1 ≡ 0 (mod 7), 2 − 5 ≡ 4 (mod 7), since −3 + 7 = 4, and 3 · 4 ≡ 5 (mod 7) as 12 has remainder 5. Standard properties of addition and multiplication familiar from the integers remain valid in modular arithmetic. In the parlance of abstract algebra, the above set of integers, which is also denoted **Z**/*n***Z**, is therefore a commutative ring for any *n*. Division, however, is not in general possible in this setting. For example, for *n* = 6, the equation

$$3 \cdot x \equiv 2 \pmod 6,$$

a solution x of which would be an analogue of 2/3, cannot be solved, as one can see by calculating $3 \cdot 0, ..., 3 \cdot 5$ modulo 6. The distinctive feature of prime numbers is the following: division *is* possible in modular arithmetic if and only if n is a prime. Equivalently, n is prime if and only if all integers m satisfying $2 \leq m \leq n - 1$ are *coprime* to n, i.e. their only common divisor is one. Indeed, for $n = 7$, the equation

$$3 \cdot x \equiv 2 \pmod{7},$$

has a unique solution, $x = 3$. Because of this, for any prime p, $\mathbf{Z}/p\mathbf{Z}$ (also denoted $\mathbf{F}_p$) is called a field or, more specifically, a finite field since it contains finitely many, namely p, elements.

A number of theorems can be derived from inspecting $\mathbf{F}_p$ in this abstract way. For example, Fermat's little theorem, stating

$$a^{p-1} \equiv 1 (\bmod\ p)$$

for any integer a not divisible by p, may be proved using these notions. This implies

$$\sum_{a=1}^{p-1} a^{p-1} \equiv (p-1) \cdot 1 \equiv -1 \pmod{p}.$$

Giuga's conjecture says that this equation is also a sufficient condition for p to be prime. Another consequence of Fermat's little theorem is the following: if p is a prime number other than 2 and 5, $^1/_p$ is always a recurring decimal, whose period is $p - 1$ or a divisor of $p - 1$. The fraction $^1/_p$ expressed likewise in base q (rather than base 10) has similar effect, provided that p is not a prime factor of q. Wilson's theorem says that an integer $p > 1$ is prime if and only if the factorial $(p - 1)! + 1$ is divisible by p. Moreover, an integer $n > 4$ is composite if and only if $(n - 1)!$ is divisible by n.

Other mathematical occurrences of primes

Many mathematical domains make great use of prime numbers. An example from the theory of finite groups are the Sylow theorems: if G is a finite group and p^n is the highest power of the prime p which divides the order of G, then G has a subgroup of order p^n. Also, any group of prime order is cyclic (Lagrange's theorem).

Public-key cryptography

Main article: Public key cryptography

Several public-key cryptography algorithms, such as RSA and the Diffie–Hellman key exchange, are based on large prime numbers (for example 512 bit primes are frequently used for RSA and 1024 bit primes are typical for Diffie–Hellman.). RSA relies on the fact that it is thought to be much easier (i.e., more efficient) to perform the multiplication of two (large) numbers *x* and *y* than to calculate *x* and *y* (assumed coprime) if only the product *xy* is known. The Diffie–Hellman key exchange relies on the fact that there are efficient algorithms for modular exponentiation, while the reverse operation the discrete logarithm is thought to be a hard problem.

Prime numbers in nature

Inevitably, some of the numbers that occur in nature are prime. There are, however, relatively few examples of numbers that appear in nature *because* they are prime.

One example of the use of prime numbers in nature is as an evolutionary strategy used by cicadas of the genus *Magicicada*. These insects spend most of their lives as grubs underground. They only pupate and then emerge from their burrows after 13 or 17 years, at which point they fly about, breed, and then die after a few weeks at most. The logic for this is believed to be that the prime number intervals between emergences make it very difficult for predators to evolve that could specialize as predators on *Magicicadas*. If *Magicicadas* appeared at a non-prime number intervals, say every 12 years, then predators appearing every 2, 3, 4, 6, or 12 years would be sure to meet them. Over a 200-year period, average predator populations during hypothetical outbreaks of 14- and 15-year cicadas would be up to 2% higher than during outbreaks of 13- and 17-year cicadas.[40] Though small, this advantage appears to have been enough to drive natural selection in favour of a prime-numbered life-cycle for these insects.

There is speculation that the zeros of the zeta function are connected to the energy levels of complex quantum systems