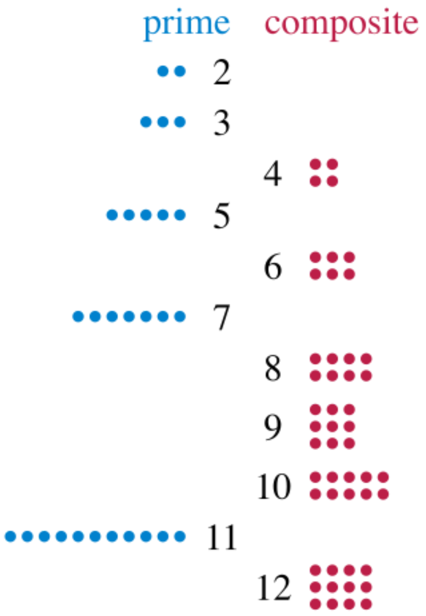
WIKIPEDIA

Prime number

A **prime number** (or a **prime**) is a natural number greater than 1 that is not a product of two smaller natural numbers. A natural number greater than 1 that is not prime is called a composite number. For example, 5 is prime because the only ways of writing it as a product, 1 × 5 or 5 × 1, involve 5 itself. However, 4 is composite because it is a product (2 × 2) in which both numbers are smaller than 4. Primes are central in number theory because of the fundamental theorem of arithmetic: every natural number greater than 1 is either a prime itself or can be factorized as a product of primes that is unique up to their order.



Composite numbers can be arranged into rectangles but prime numbers cannot

The property of being prime is called **primality**. A simple but slow method of checking the primality of a given number n, called trial division, tests whether n is a multiple of any integer between 2 and $\sqrt{n}$. Faster algorithms include the Miller–Rabin primality test, which is fast but has a small chance of error, and the AKS primality test, which always produces the correct answer in polynomial time but is too slow to be practical. Particularly fast methods are available for numbers of special forms, such as Mersenne numbers. As of December 2018 the largest known prime number is a Mersenne prime with 24,862,048 decimal digits.[1]

There are infinitely many primes, as demonstrated by Euclid around 300 BC. No known simple formula separates prime numbers from composite numbers. However, the distribution of primes within the natural numbers in the large can be statistically modelled. The first result in that direction is the prime number theorem, proven at the end of the 19th century, which says that the probability of a randomly chosen number being prime is inversely proportional to its number of digits, that is, to its logarithm.

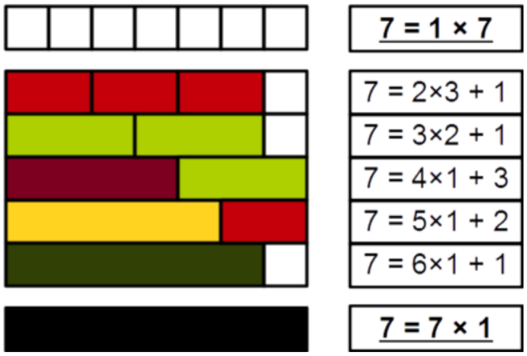
Several historical questions regarding prime numbers are still unsolved. These include Goldbach's conjecture, that every even integer greater than 2 can be expressed as the sum of two primes, and the twin prime conjecture, that there are infinitely many pairs of primes having just one even number between them. 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 relies on the difficulty of factoring large numbers into their prime factors. In abstract algebra, objects that behave in a generalized way like prime numbers include prime elements and prime ideals.

Contents

Definition and examples

A natural number (1, 2, 3, 4, 5, 6, etc.) is called a *prime number* (or a *prime*) if it is greater than 1 and cannot be written as the product of two smaller natural numbers. The numbers greater than 1 that are not prime are called composite numbers.[2] In other words, n is prime if n items cannot be divided up into smaller equal-size groups of more than one item,[3] or if it is not possible to arrange n dots into a rectangular grid that is more than one dot wide and more than one dot high.[4] For example, among the numbers 1 through 6, the numbers 2, 3, and 5 are the prime numbers,[5] as there are no other numbers that divide them evenly (without a remainder). 1 is not prime, as it is specifically excluded in the definition. 4 = 2 × 2 and 6 = 2 × 3 are both composite.

The divisors of a natural number n are the natural numbers that divide n evenly. Every natural number has both 1 and itself as a divisor. If it has any other divisor, it cannot be prime. This idea leads to a different but equivalent definition of the primes: they are the numbers with exactly two positive divisors, 1 and the number itself.[6] Yet another way to express the same thing is that a number n is prime if it is greater than one and if none of the numbers $2, 3, \dots, n-1$ divides n evenly.[7]



Demonstration, with Cuisenaire rods, that 7 is prime, because none of 2, 3, 4, 5, or 6 divide it evenly

The first 25 prime numbers (all the prime numbers less than 100) are:[8]

> 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 (sequence A000040 in the OEIS).

No even number n greater than 2 is prime because any such number can be expressed as the product $2 \times n/2$. Therefore, every prime number other than 2 is an odd number, and is called an *odd prime*.[9] Similarly, when written in the usual decimal system, all prime numbers larger than 5 end in 1, 3, 7, or 9. The numbers that end with other digits are all composite: decimal numbers that end in 0, 2, 4, 6, or 8 are even, and decimal numbers that end in 0 or 5 are divisible by 5.[10]

The set of all primes is sometimes denoted by $\mathbf{P}$ (a boldface capital *P*)[11] or by $\mathbb{P}$ (a blackboard bold capital P).[12]

History

The Rhind Mathematical Papyrus, from around 1550 BC, has Egyptian fraction expansions of different forms for prime and composite numbers.[13] However, the earliest surviving records of the explicit study of prime numbers come from ancient Greek mathematics. Euclid's *Elements* (c. 300 BC) proves the infinitude of primes and the fundamental theorem of arithmetic, and shows how to construct a perfect number from a Mersenne prime.[14] Another Greek invention, the Sieve of Eratosthenes, is still used to construct lists of primes.[15][16]

The Rhind Mathematical Papyrus

Around 1000 AD, the Islamic mathematician Ibn al-Haytham (Alhazen) found Wilson's theorem, characterizing the prime numbers as the numbers n that evenly divide $(n-1)!+1$. He also conjectured that all even perfect numbers come from Euclid's construction using Mersenne primes, but was unable to prove it.[17] Another Islamic mathematician, Ibn al-Banna' al-Marrakushi, observed that the sieve of Eratosthenes can be sped up by testing only the divisors up to the square root of the largest number to be tested. Fibonacci brought the innovations from Islamic mathematics back to Europe. His book *Liber Abaci* (1202) was the first to describe trial division for testing primality, again using divisors only up to the square root.[16]

In 1640 Pierre de Fermat stated (without proof) Fermat's little theorem (later proved by Leibniz and Euler).[18] Fermat also investigated the primality of the Fermat numbers $2^{2^n}+1$,[19] and Marin Mersenne studied the Mersenne primes, prime numbers of the form 2^p-1 with p itself a prime.[20] Christian Goldbach formulated Goldbach's conjecture, that every even number is the sum of two primes, in a 1742 letter to Euler.[21] Euler proved Alhazen's conjecture (now the Euclid–Euler theorem) that all even perfect numbers can be constructed from Mersenne primes.[14] He introduced methods from mathematical analysis to this area in his proofs of the infinitude of the primes and the divergence of the sum of the reciprocals of the primes $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\cdots$.[22] At the start of the 19th century, Legendre and Gauss conjectured that as x tends to infinity, the number of primes up to x is asymptotic to $x/\log x$, where $\log x$ is the natural logarithm of x. A weaker consequence of this high density of primes was Bertrand's postulate, that for every $n>1$ there is a prime between n and $2n$, proved in 1852 by Pafnuty Chebyshev.[23] Ideas of Bernhard Riemann in his 1859 paper on the zeta-function sketched an outline for proving the conjecture of Legendre and Gauss. Although the closely related Riemann hypothesis remains unproven, Riemann's outline was completed in 1896 by Hadamard and de la Vallée Poussin, and the result is now known as the prime number theorem.[24] Another important 19th century result was Dirichlet's theorem on arithmetic progressions, that certain arithmetic progressions contain infinitely many primes.[25]

Many mathematicians have worked on primality tests for numbers larger than those where trial division is practicably applicable. Methods that are restricted to specific number forms include Pépin's test for Fermat numbers (1877),[26] Proth's theorem (c. 1878),[27] the Lucas–Lehmer primality test (originated 1856), and the generalized Lucas primality test.[16]

Since 1951 all the largest known primes have been found using these tests on computers.[a] The search for ever larger primes has generated interest outside mathematical circles, through the Great Internet Mersenne Prime Search and other distributed computing projects.[8][29] The idea that prime numbers had few applications outside of pure mathematics[b] was shattered in the 1970s when public-key cryptography and the RSA cryptosystem were invented, using prime numbers as their basis.[32]

The increased practical importance of computerized primality testing and factorization led to the development of improved methods capable of handling large numbers of unrestricted form.[15][33][34] The mathematical theory of prime numbers also moved forward with the Green–Tao theorem (2004) that there are arbitrarily long arithmetic progressions of prime numbers, and Yitang Zhang's 2013 proof that there exist infinitely many prime gaps of bounded size.[35]

Primality of one

Most early Greeks did not even consider 1 to be a number,[36][37] so they could not consider its primality. A few mathematicians from this time also considered the prime numbers to be a subdivision of the odd numbers, so they also did not consider 2 to be prime. However, Euclid and a majority of the other Greek mathematicians considered 2 as prime. The medieval Islamic mathematicians largely followed the Greeks in viewing 1 as not being a number.[36] By the Middle Ages and Renaissance mathematicians began treating 1 as a number, and some of them included it as the first prime number.[38] In the mid-18th century Christian Goldbach listed 1 as prime in his correspondence with Leonhard Euler; however, Euler himself did not consider 1 to be prime.[39] In the 19th century many mathematicians still considered 1 to be prime,[40] and lists of primes that included 1 continued to be published as recently as 1956.[41][42]

If the definition of a prime number were changed to call 1 a prime, many statements involving prime numbers would need to be reworded in a more awkward way. For example, the fundamental theorem of arithmetic would need to be rephrased in terms of factorizations into primes greater than 1, because every number would have multiple factorizations with different numbers of copies of 1.[40] Similarly, the sieve of Eratosthenes would not work correctly if it handled 1 as a prime, because it would eliminate all multiples of 1 (that is, all other numbers) and output only the single number 1.[42] Some other more technical properties of prime numbers also do not hold for the number 1: for instance, the formulas for Euler's totient function or for the sum of divisors function are different for prime numbers than they are for 1.[43] By the early 20th century, mathematicians began to agree that 1 should not be listed as prime, but rather in its own special category as a "unit".[40]

Elementary properties

Unique factorization

Writing a number as a product of prime numbers is called a *prime factorization* of the number. For example:

$$\begin{aligned}34866 &= 2\cdot 3\cdot 3\cdot 13\cdot 149\\ &= 2\cdot 3^2\cdot 13\cdot 149.\end{aligned}$$

The terms in the product are called *prime factors*. The same prime factor may occur more than once; this example has two copies of the prime factor 3. When a prime occurs multiple times, exponentiation can be used to group together multiple copies of the same prime number: for example, in the second way of writing the product above, 3^2 denotes the square or second power of 3.

The central importance of prime numbers to number theory and mathematics in general stems from the *fundamental theorem of arithmetic*.[44] This theorem states that every integer larger than 1 can be written as a product of one or more primes. More strongly, this product is unique in the sense that any two prime factorizations of the same number will have the same numbers of copies of the same primes, although their ordering may differ.[45] So, although there are many different ways of finding a factorization using an integer factorization algorithm, they all must produce the same result. Primes can thus be considered the "basic building blocks" of the natural numbers.[46]

Some proofs of the uniqueness of prime factorizations are based on Euclid's lemma: If p is a prime number and p divides a product ab of integers a and b, then p divides a or p divides b (or both).[47] Conversely, if a number p has the property that when it divides a product it always divides at least one factor of the product, then p must be prime.[48]

Infinitude

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,[49] Furstenberg's proof using general topology,[50] and Kummer's elegant proof.[51]

Euclid's proof[52] shows that every finite list of primes is incomplete. The key idea is to multiply together the primes in any given list and add 1. If the list consists of the primes $p_1, p_2, \ldots, p_n$, this gives the number

$$N = 1 + p_1 \cdot p_2 \cdots p_n.$$

By the fundamental theorem, N has a prime factorization

$$N = p'_1 \cdot p'_2 \cdots p'_m$$

with one or more prime factors. N is evenly divisible by each of these factors, but N has a remainder of one when divided by any of the prime numbers in the given list, so none of the prime factors of N can be in the given list. Because there is no finite list of all the primes, there must be infinitely many primes.

The numbers formed by adding one to the products of the smallest primes are called Euclid numbers.[53] The first five of them are prime, but the sixth,

$$1 + \big(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13\big) = 30031 = 59 \cdot 509,$$

is a composite number.

Formulas for primes

There is no known efficient formula for primes. For example, there is no non-constant polynomial, even in several variables, that takes *only* prime values.[54] However, there are numerous expressions that do encode all primes, or only primes. One possible formula is based on Wilson's theorem and generates the number 2 many times and all other primes exactly once.[55] There is also a set of Diophantine equations in nine variables and one parameter with the following property: the parameter is prime if and only if the resulting system of equations has a solution over the natural numbers. This can be used to obtain a single formula with the property that all its *positive* values are prime.[54]

Other examples of prime-generating formulas come from Mills' theorem and a theorem of Wright. These assert that there are real constants $A > 1$ and μ such that

$$\left\lfloor A^{3^n} \right\rfloor \text{ and } \left\lfloor 2^{\cdots^{2^{2^\mu}}} \right\rfloor$$

are prime for any natural number n in the first formula, and any number of exponents in the second formula.[56] Here $\lfloor \cdot \rfloor$ represents the floor function, the largest integer less than or equal to the number in question. However, these are not useful for generating primes, as the primes must be generated first in order to compute the values of A or μ.[54]

Open questions

Many conjectures revolving about primes have been posed. Often having an elementary formulation, many of these conjectures have withstood proof for decades: all four of Landau's problems from 1912 are still unsolved.[57] One of them is Goldbach's conjecture, which asserts that every even integer n greater than 2 can be written as a sum of two primes.[58] As of 2014, this conjecture has been verified for all numbers up to $n = 4 \cdot 10^{18}$.[59] Weaker statements than this have been proven, for example, Vinogradov's theorem says that every sufficiently large odd integer can be written as a sum of three primes.[60] Chen's theorem says that every sufficiently large even number can be expressed as the sum of a prime and a semiprime (the product of two primes).[61] Also, any even integer greater than 10 can be written as the sum of six primes.[62] The branch of number theory studying such questions is called additive number theory.[63]

Another type of problem concerns prime gaps, the differences between consecutive primes. The existence of arbitrarily large prime gaps can be seen by noting that the sequence $n!+2, n!+3, \dots, n!+n$ consists of $n-1$ composite numbers, for any natural number n.[64] However, large prime gaps occur much earlier than this argument shows.[65] For example, the first prime gap of length 8 is between the primes 89 and 97,[66] much smaller than $8! = 40320$. It is conjectured that there are infinitely many twin primes, pairs of primes with difference 2; this is the twin prime conjecture. Polignac's conjecture states more generally that for every positive integer k, there are infinitely many pairs of consecutive primes that differ by $2k$.[67] Andrica's conjecture,[67] Brocard's conjecture,[68] Legendre's conjecture,[69] and Oppermann's conjecture[68] all suggest that the largest gaps between primes from 1 to n should be at most approximately $\sqrt{n}$, a result that is known to follow from the Riemann hypothesis, while the much stronger Cramér conjecture sets the largest gap size at $O((\log n)^2)$.[67] Prime gaps can be generalized to prime k-tuples, patterns in the differences between more than two prime numbers. Their infinitude and density are the subject of the first Hardy–Littlewood conjecture, which can be motivated by the heuristic that the prime numbers behave similarly to a random sequence of numbers with density given by the prime number theorem.[70]

Analytic properties

Analytic number theory studies number theory through the lens of continuous functions, limits, infinite series, and the related mathematics of the infinite and infinitesimal.

This area of study began with Leonhard Euler and his first major result, the solution to the Basel problem. The problem asked for the value of the infinite sum $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$, which today can be recognized as the value $\zeta(2)$ of the Riemann zeta function. This function is closely connected to the prime numbers and to one of the most significant unsolved problems in mathematics, the Riemann hypothesis. Euler showed that $\zeta(2) = \pi^2/6$.[71] The reciprocal of this number, $6/\pi^2$, is the limiting probability that two random numbers selected uniformly from a large range are relatively prime (have no factors in common).[72]

The distribution of primes in the large, such as the question how many primes are smaller than a given, large threshold, is described by the prime number theorem, but no efficient formula for the n-th prime is known. Dirichlet's theorem on arithmetic progressions, in its basic form, asserts that linear polynomials

$$p(n) = a + bn$$

with relatively prime integers a and b take infinitely many prime values. Stronger forms of the theorem state that the sum of the reciprocals of these prime values diverges, and that different linear polynomials with the same b have approximately the same proportions of primes. Although conjectures have been formulated about the proportions of primes in higher-degree polynomials, they remain unproven, and it is unknown whether there exists a quadratic polynomial that (for integer arguments) is prime infinitely often.

Analytical proof of Euclid's theorem

Euler's proof that there are infinitely many primes considers the sums of reciprocals of primes,

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots+\frac{1}{p}.$$

Euler showed that, for any arbitrary real number x, there exists a prime p for which this sum is bigger than x.[73] This shows that there are infinitely many primes, because if there were finitely many primes the sum would reach its maximum value at the biggest prime rather than growing past every x. The growth rate of this sum is described more precisely by Mertens' second theorem.[74] For comparison, the sum

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}$$

does not grow to infinity as n goes to infinity (see the Basel problem). In this sense, prime numbers occur more often than squares of natural numbers, although both sets are infinite.[75] Brun's theorem states that the sum of the reciprocals of twin primes,

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots,$$

is finite. Because of Brun's theorem, it is not possible to use Euler's method to solve the twin prime conjecture, that there exist infinitely many twin primes.[75]

Number of primes below a given bound

The prime counting function $\pi(n)$ is defined as the number of primes not greater than n.[76] For example, $\pi(11)=5$, since there are five primes less than or equal to 11. Methods such as the Meissel–Lehmer algorithm can compute exact values of $\pi(n)$ faster than it would be possible to list each prime up to n.[77] The prime number theorem states that $\pi(n)$ is asymptotic to $n/\log n$, which is denoted as

$$\pi(n)\sim\frac{n}{\log n},$$

and means that the ratio of $\pi(n)$ to the right-hand fraction approaches 1 as n grows to infinity.[78] This implies that the likelihood that a randomly chosen number less than n is prime is (approximately) inversely proportional to the number of digits in n.[79] It also implies that the nth prime number is proportional to $n\log n$[80] and therefore that the average size of a prime gap is proportional to $\log n$.[65] A more accurate estimate for $\pi(n)$ is given by the offset logarithmic integral[78]

$$\pi(n)\sim\operatorname{Li}(n)=\int_2^n\frac{dt}{\log t}.$$

Arithmetic progressions

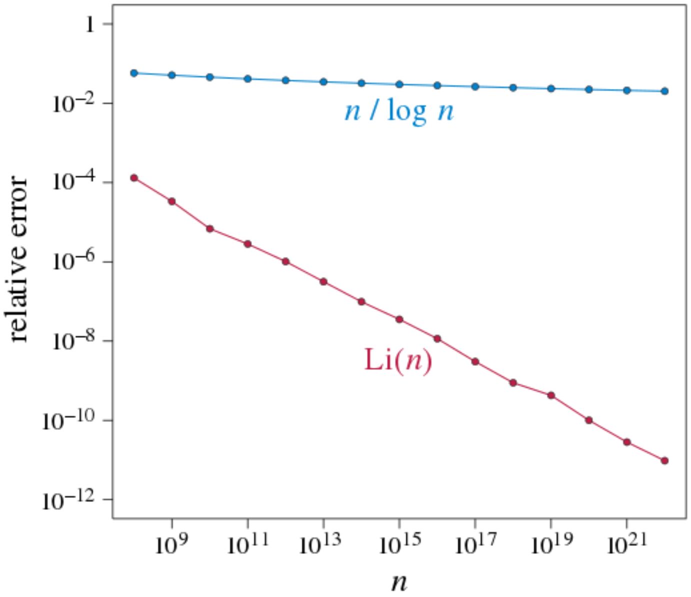
An arithmetic progression is a finite or infinite sequence of numbers such that consecutive numbers in the sequence all have the same difference.[81] This difference is called the modulus of the progression.[82] For example,

3, 12, 21, 30, 39, ...,

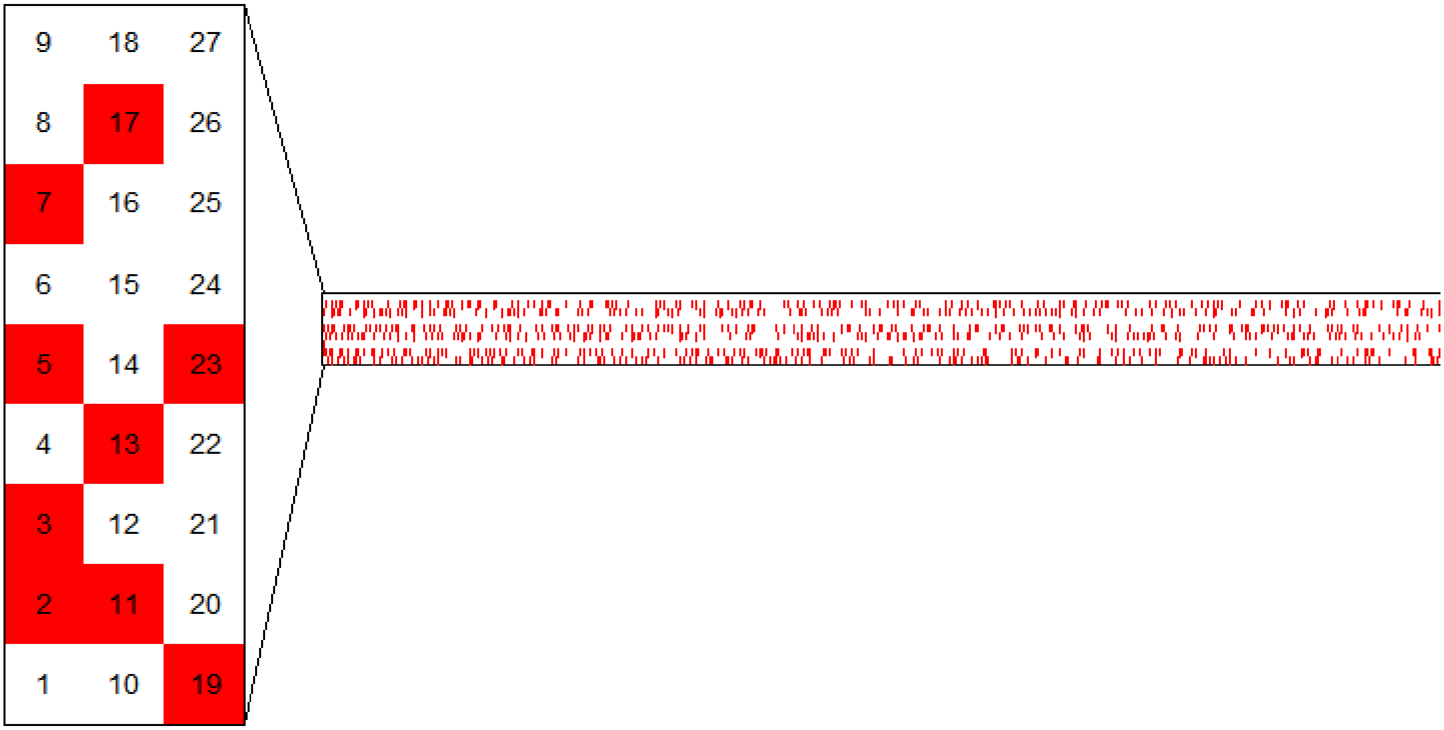
is an infinite arithmetic progression with modulus 9. In an arithmetic progression, all the numbers have the same remainder when divided by the modulus; in this example, the remainder is 3. Because both the modulus 9 and the remainder 3 are multiples of 3, so is every element in the sequence. Therefore, this progression contains only one prime number, 3 itself. In general, the infinite progression

$$a, a+q, a+2q, a+3q, \dots$$

can have more than one prime only when its remainder a and modulus q are relatively prime. If they are relatively prime, Dirichlet's theorem on arithmetic progressions asserts that the progression contains infinitely many primes.[83]



The relative error of $\frac{n}{\log n}$ and the logarithmic integral $\mathrm{Li}(n)$ as approximations to the prime-counting function. Both relative errors decrease to zero as n grows, but the convergence to zero is much more rapid for the logarithmic integral.



Primes in the arithmetic progressions modulo 9. Each row of the thin horizontal band shows one of the nine possible progressions mod 9, with prime numbers marked in red. The progressions of numbers that are 0, 3, or 6 mod 9 contain at most one prime number (the number 3); the remaining progressions of numbers that are 2, 4, 5, 7, and 8 mod 9 have infinitely many prime numbers, with similar numbers of primes in each progression

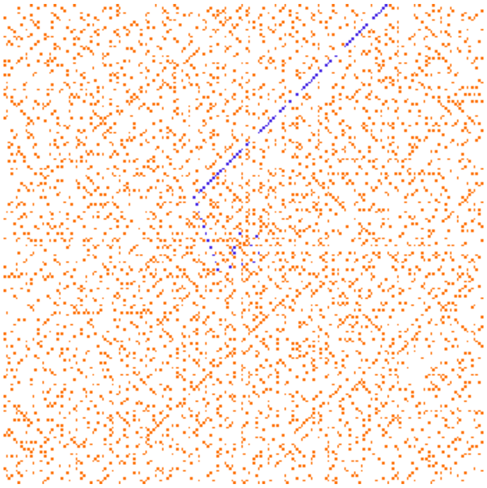
The Green–Tao theorem shows that there are arbitrarily long finite arithmetic progressions consisting only of primes.[35][84]

Prime values of quadratic polynomials

Euler noted that the function

$$n^2 - n + 41$$

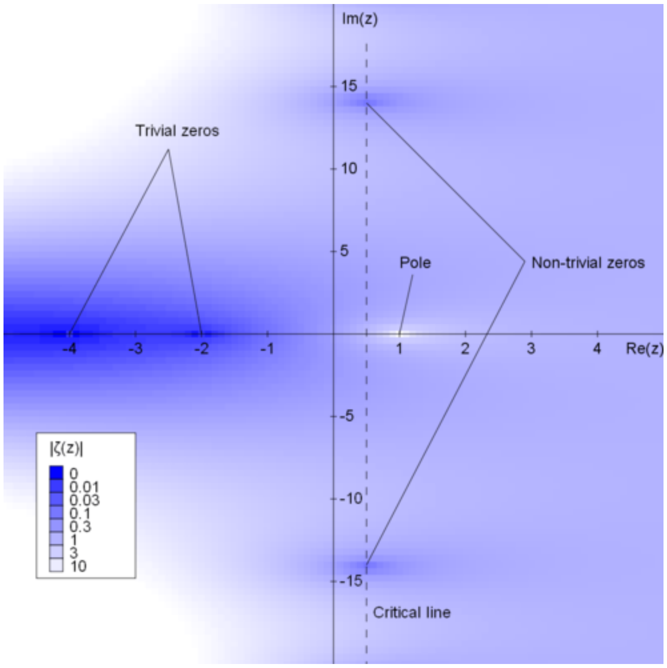
yields prime numbers for $1 \leq n \leq 40$, although composite numbers appear among its later values.[85][86] The search for an explanation for this phenomenon led to the deep algebraic number theory of Heegner numbers and the class number problem.[87] The Hardy-Littlewood conjecture F predicts the density of primes among the values of quadratic polynomials with integer coefficients in terms of the logarithmic integral and the polynomial coefficients. No quadratic polynomial has been proven to take infinitely many prime values.[88]



The Ulam spiral. Prime numbers (red) cluster on some diagonals and not others. Prime values of $4n^2 - 2n + 41$ are shown in blue.

The Ulam spiral arranges the natural numbers in a two-dimensional grid, spiraling in concentric squares surrounding the origin with the prime numbers highlighted. Visually, the primes appear to cluster on certain diagonals and not others, suggesting that some quadratic polynomials take prime values more often than others.[88]

Zeta function and the Riemann hypothesis



Plot of the absolute values of the zeta function, showing some of its features

One of the most famous unsolved questions in mathematics, dating from 1859, and one of the Millennium Prize Problems, is the Riemann hypothesis, which asks where the zeros of the Riemann zeta function $\zeta(s)$ are located. This function is an analytic function on the complex numbers. For complex numbers s with real part greater than one it equals both an infinite sum over all integers, and an infinite product over the prime numbers,

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}.$$

This equality between a sum and a product, discovered by Euler, is called an Euler product.[89] The Euler product can be derived from the fundamental theorem of arithmetic, and shows the close connection between the zeta function and the prime numbers.[90] It leads to another proof that there are infinitely many primes: if there were only finitely many, then the sum-product equality would also be valid at $s=1$, but the sum would diverge (it is the harmonic series $1+\frac{1}{2}+\frac{1}{3}+\ldots$) while the product would be finite, a contradiction.[91]

The Riemann hypothesis states that the zeros of the zeta-function are all either negative even numbers, or complex numbers with real part equal to 1/2.[92] The original proof of the prime number theorem was based on a weak form of this hypothesis, that there are no zeros with real part equal to 1,[93][94] although other more elementary proofs have been found.[95] The prime-counting function can be expressed by Riemann's explicit formula as a sum in which each term comes from one of the zeros of the zeta function; the main term of this sum is the logarithmic integral, and the remaining terms cause the sum to fluctuate above and below the main term.[96] In this sense, the zeros control how regularly the prime numbers are distributed. If the Riemann hypothesis is true, these fluctuations will be small, and the asymptotic distribution of primes given by the prime number theorem will also hold over much shorter intervals (of length about the square root of x for intervals near a number x).[94]

Abstract algebra

Modular arithmetic and finite fields

Modular arithmetic modifies usual arithmetic by only using the numbers $\{0,1,2,\dots,n-1\}$, for a natural number n called the modulus. Any other natural number can be mapped into this system by replacing it by its remainder after division by n.[97] Modular sums, differences and products are calculated by performing the same replacement by the remainder on the result of the usual sum, difference, or product of integers.[98] Equality of integers corresponds to *congruence* in modular arithmetic: x and y are congruent (written $x \equiv y$ mod n) when they have the same remainder after division by n.[99] However, in this system of numbers, division by all nonzero numbers is possible if and only if the modulus is prime. For instance, with the prime number 7 as modulus, division by 3 is possible: $2/3 \equiv 3 \bmod 7$, because clearing denominators by multiplying both sides by 3 gives the valid formula $2 \equiv 9 \bmod 7$. However, with the composite modulus 6, division by 3 is impossible. There is no valid solution to $2/3 \equiv x \bmod 6$: clearing denominators by multiplying by 3 causes the left-hand side to become 2 while the right-hand side becomes either 0 or 3. In the terminology of abstract algebra, the ability to perform division means that modular arithmetic modulo a prime number forms a field or, more specifically, a finite field, while other moduli only give a ring but not a field.[100]

Several theorems about primes can be formulated using modular arithmetic. For instance, Fermat's little theorem states that if $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.[101] Summing this over all choices of a gives the equation

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

valid whenever p is prime. Giuga's conjecture says that this equation is also a sufficient condition for p to be prime.[102] Wilson's theorem says that an integer $p > 1$ is prime if and only if the factorial $(p-1)!$ is congruent to -1 mod p. For a composite number $n = r \cdot s$ this cannot hold, since one of its factors divides both *n* and $(n-1)!$, and so $(n-1)! \equiv -1 \pmod{n}$ is impossible.[103]

p-adic numbers

The p-adic order $\nu_p(n)$ of an integer n is the number of copies of p in the prime factorization of n. The same concept can be extended from integers to rational numbers by defining the p-adic order of a fraction m/n to be $\nu_p(m) - \nu_p(n)$. The p-adic absolute value $|q|_p$ of any rational number q is then defined as $|q|_p = p^{-\nu_p(q)}$. Multiplying an integer by its p-adic absolute value cancels out the factors of p in its factorization, leaving only the other primes. Just as the distance between two real numbers can be measured by the absolute value of their distance, the distance between two rational numbers can be measured by their p-adic distance, the p-adic absolute value of their difference. For this definition of distance, two numbers are close together (they have a small distance) when their difference is divisible by a high power of p. In the same way that the real numbers can be formed from the rational numbers and their distances, by adding extra limiting values to form a complete field, the rational numbers with the p-adic distance can be extended to a different complete field, the p-adic numbers.[104][105]

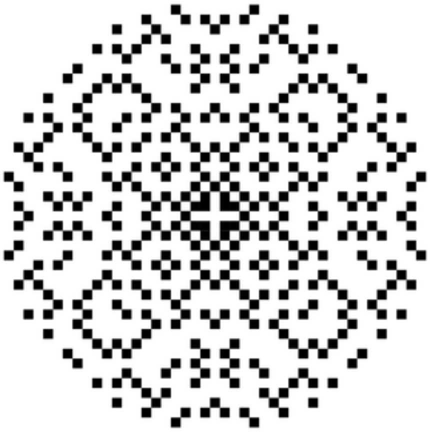
This picture of an order, absolute value, and complete field derived from them can be generalized to algebraic number fields and their valuations (certain mappings from the multiplicative group of the field to a totally ordered additive group, also called orders), absolute values (certain multiplicative mappings from the field to the real numbers, also called norms),[104] and places (extensions to complete fields in which the given field is a dense set, also called completions).[106] The extension from the rational numbers to the real numbers, for instance, is a place in which the distance between numbers is the usual absolute value of their difference. The corresponding mapping to an additive group would be the logarithm of the absolute value, although this does not meet all the requirements of a valuation. According to Ostrowski's theorem, up to a natural notion of equivalence, the real numbers and p-adic numbers, with their orders and absolute values, are the only valuations, absolute values, and places on the rational numbers.[104] The local-global principle allows certain problems over the rational numbers to be solved by piecing together solutions from each of their places, again underlining the importance of primes to number theory.[107]

Prime elements in rings

A commutative ring is an algebraic structure where addition, subtraction and multiplication are defined. The integers are a ring, and the prime numbers in the integers have been generalized to rings in two different ways, *prime elements* and *irreducible elements*. An element p of a ring R is called prime if it is nonzero, has no multiplicative inverse (that is, it is not a unit), and satisfies the following requirement: whenever p divides the product xy of two elements of R, it also divides at least one of x or y. An element is irreducible if it is neither a unit nor the product of two other non-unit elements. In the ring of integers, the prime and irreducible elements form the same set,

$$\{\ldots,-11,-7,-5,-3,-2,2,3,5,7,11,\ldots\}\,.$$

In an arbitrary ring, all prime elements are irreducible. The converse does not hold in general, but does hold for unique factorization domains.[108]



The Gaussian primes with norm less than 500

The fundamental theorem of arithmetic continues to hold (by definition) in unique factorization domains. An example of such a domain is the Gaussian integers $\mathbb{Z}[i]$, the ring of complex numbers of the form $a+bi$ where i denotes the imaginary unit and a and b are arbitrary integers. Its prime elements are known as Gaussian primes. Not every number that is prime among the integers remains prime in the Gaussian integers; for instance, the number 2 can be written as a product of the two Gaussian primes $1+i$ and $1-i$. Rational primes (the prime elements in the integers) congruent to 3 mod 4 are Gaussian primes, but rational primes congruent to 1 mod 4 are not.[109] This is a consequence of Fermat's theorem on sums of two squares, which states that an odd prime p is expressible as the sum of two squares, $p=x^2+y^2$, and therefore factorizable as $p=(x+iy)(x-iy)$, exactly when p is 1 mod 4.[110]

Prime ideals

Not every ring is a unique factorization domain. For instance, in the ring of numbers $a+b\sqrt{-5}$ (for integers a and b) the number 21 has two factorizations $21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})$, where neither of the four factors can be reduced any further, so it does not have a unique factorization. In order to extend unique factorization to a larger class of rings, the notion of a number can be replaced with that of an ideal, a subset of the elements of a ring that contains all sums of pairs of its elements, and all products of its elements with ring elements. *Prime ideals*, which generalize prime elements in the sense that the principal ideal generated by a prime element is a prime ideal, are an important tool and object of study in commutative algebra, algebraic number theory and algebraic geometry. The prime ideals of the ring of integers are the ideals (0), (2), (3), (5), (7), (11), ... The fundamental theorem of arithmetic generalizes to the Lasker–Noether theorem, which expresses every ideal in a Noetherian commutative ring as an intersection of primary ideals, which are the appropriate generalizations of prime powers.[111]

The spectrum of a ring is a geometric space whose points are the prime ideals of the ring.[112] Arithmetic geometry also benefits from this notion, and many concepts exist in both geometry and number theory. For example, factorization or ramification of prime ideals when lifted to an extension field, a basic problem of algebraic number theory, bears some resemblance with ramification in geometry. These concepts can even assist with in number-theoretic questions solely concerned with integers. For example, prime ideals in the ring of integers of quadratic number fields can be used in proving quadratic reciprocity, a statement that concerns the existence of square roots modulo integer prime numbers.[113] Early attempts to prove Fermat's Last Theorem led to Kummer's introduction of regular primes, integer prime numbers connected with the failure of unique factorization in the cyclotomic integers.[114] The question of how many integer prime numbers factor into a product of multiple prime ideals in an algebraic number field is addressed by Chebotarev's density theorem, which (when applied to the cyclotomic integers) has Dirichlet's theorem on primes in arithmetic progressions as a special case.[115]

Group theory

In the theory of finite groups the Sylow theorems imply that, if a power of a prime number p^n divides the order of a group, then the group has a subgroup of order p^n. By Lagrange's theorem, any group of prime order is a cyclic group, and by Burnside's theorem any group whose order is divisible by only two primes is solvable.[116]

Computational methods

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 mathematics[b] other than the use of prime numbered gear teeth to distribute wear evenly.[117] In particular, number theorists such as British mathematician G. H. Hardy prided themselves on doing work that had absolutely no military significance.[118]

The small gear in this piece of farm equipment has 13 teeth, a prime number, and the middle gear has 21, relatively prime to 13

This vision of the purity of number theory 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.[32] These applications have led to significant study of algorithms for computing with prime numbers, and in particular of primality testing, methods for determining whether a given number is prime. The most basic primality testing routine, trial division, is too slow to be useful for large numbers. One group of modern primality tests is applicable to arbitrary numbers, while more efficient tests are available for numbers of special types. Most primality tests only tell whether their argument is prime or not. Routines that also provide a prime factor of composite arguments (or all of its prime factors) are called factorization algorithms. Prime numbers are also used in computing for checksums, hash tables, and pseudorandom number generators.

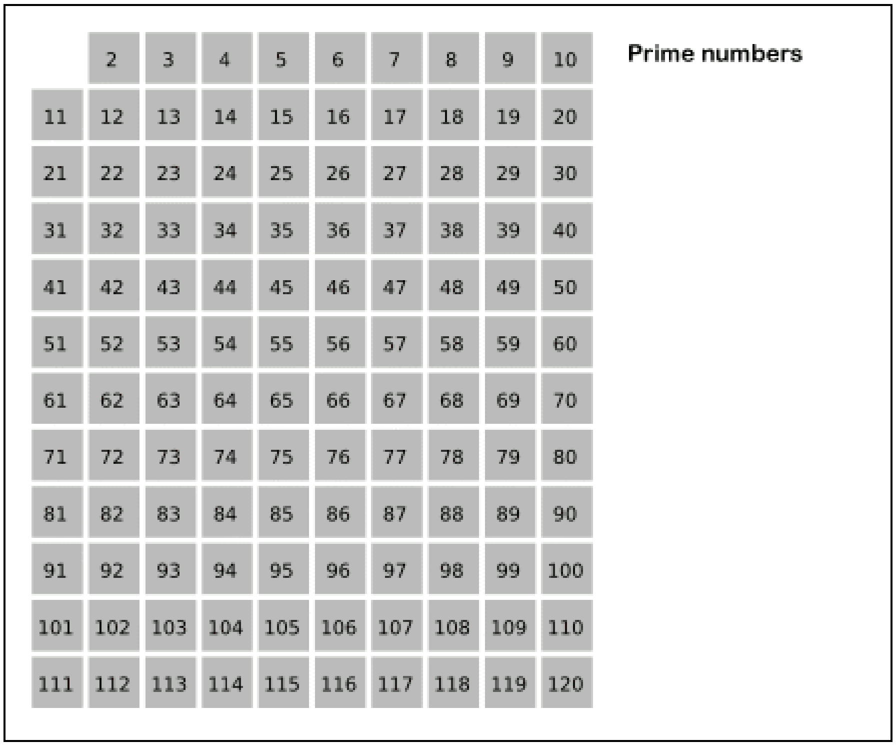
Trial division

The most basic method of checking the primality of a given integer n is called *trial division*. This method divides n by each integer from 2 up to the square root of n. Any such integer dividing n evenly establishes n as composite; otherwise it is prime. Integers larger than the square root do not need to be checked because, whenever $n = a \cdot b$, one of the two factors a and b is less than or equal to the square root of n. Another optimization is to check only primes as factors in this range.[119] For instance, to check whether 37 is prime, this method divides it by the primes in the range from 2 to $\sqrt{37}$, which are 2, 3, and 5. Each division produces a nonzero remainder, so 37 is indeed prime.

Although this method is simple to describe, it is impractical for testing the primality of large integers, because the number of tests that it performs grows exponentially as a function of the number of digits of these integers.[120] However, trial division is still used, with a smaller limit than the square root on the divisor size, to quickly discover composite numbers with small factors, before using more complicated methods on the numbers that pass this filter.[121]

Sieves

Before computers, mathematical tables listing all of the primes or prime factorizations up to a given limit were commonly printed.[122] The oldest method for generating a list of primes is called the sieve of Eratosthenes.[123] The animation shows an optimized variant of this method.[124] Another more asymptotically efficient sieving method for the same problem is the sieve of Atkin.[125] In advanced mathematics, sieve theory applies similar methods to other problems.[126]



	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

The sieve of Eratosthenes starts with all numbers unmarked (gray). It repeatedly finds the first unmarked number, marks it as prime (dark colors) and marks its square and all later multiples as composite (lighter colors). After marking the multiples of 2 (red), 3 (green), 5 (blue), and 7 (yellow), all primes up to the square root of the table size have been processed, and all remaining unmarked numbers (11, 13, etc.) are marked as primes (magenta).

Primality testing versus primality proving

Some of the fastest modern tests for whether an arbitrary given number n is prime are probabilistic (or Monte Carlo) algorithms, meaning that they have a small random chance of producing an incorrect answer.[127] For instance the Solovay–Strassen primality test on a given number p chooses a number a randomly from 2 through $p-2$ and uses modular exponentiation to check whether $a^{(p-1)/2} \pm 1$ is divisible by p.[c] If so, it answers yes and otherwise it answers no. If p really is prime, it will always answer yes, but if p is composite then it answers yes with probability at most 1/2 and no with probability at least 1/2.[128] If this test is repeated n times on the same number, the probability that a composite number could pass the test every time is at most $1/2^n$. Because this decreases exponentially with the number of tests, it provides high confidence (although not certainty) that a number that passes the repeated test is prime. On the other hand, if the test ever fails, then the number is certainly composite.[129] A composite number that passes such a test is called a pseudoprime.[128]

In contrast, some other algorithms guarantee that their answer will always be correct: primes will always be determined to be prime and composites will always be determined to be composite. For instance, this is true of trial division. The algorithms with guaranteed-correct output include both deterministic (non-random) algorithms, such as the AKS primality test,[130] and randomized Las Vegas algorithms where the random choices made by the algorithm do not affect its final answer, such as some variations of elliptic curve primality proving.[127] When the elliptic curve method concludes that a number is prime, it provides primality certificate that can be verified quickly.[131] The elliptic curve primality test is the fastest in practice of the guaranteed-correct primality tests, but its runtime analysis is based on heuristic arguments rather than rigorous proofs. The AKS primality test has mathematically proven time complexity, but is slower than elliptic curve primality proving in practice.[132] These methods can be used to generate large random prime numbers, by generating and testing random numbers until finding one that is prime; when doing this, a faster probabilistic test can quickly eliminate most composite numbers before a guaranteed-correct algorithm is used to verify that the remaining numbers are prime.[d]

The following table lists some of these tests. Their running time is given in terms of n, the number to be tested and, for probabilistic algorithms, the number k of tests performed. Moreover, ε is an arbitrarily small positive number, and log is the logarithm to an unspecified base. The big O notation means that each time bound should be multiplied by a constant factor to convert it from dimensionless units to units of time; this factor depends on implementation details such as the type of computer used to run the algorithm, but not on the input parameters n and k.

Test	Developed in	Type	Running time	Notes	References
AKS primality test	2002	deterministic	$O((\log n)^{6+\varepsilon})$		[130][133]
Elliptic curve primality proving	1986	Las Vegas	$O((\log n)^{4+\varepsilon})$ *heuristically*		[132]
Baillie-PSW primality test	1980	Monte Carlo	$O((\log n)^{2+\varepsilon})$		[134][135]
Miller–Rabin primality test	1980	Monte Carlo	$O(k(\log n)^{2+\varepsilon})$	error probability 4^{-k}	[136]
Solovay–Strassen primality test	1977	Monte Carlo	$O(k(\log n)^{2+\varepsilon})$	error probability 2^{-k}	[136]

Special-purpose algorithms and the largest known prime

In addition to the aforementioned tests that apply to any natural number, some numbers of a special form can be tested for primality more quickly. For example, the Lucas–Lehmer primality test can determine whether a Mersenne number (one less than a power of two) is prime, deterministically, in the same time as a single iteration of the Miller–Rabin test.[137] This is why since 1992 (as of December 2018) the largest *known* prime has always been a Mersenne prime.[138] It is conjectured that there are infinitely many Mersenne primes.[139]

The following table gives the largest known primes of various types. Some of these primes have been found using distributed computing. In 2009, the Great Internet Mersenne Prime Search project was awarded a US$100,000 prize for first discovering a prime with at least 10 million digits.[140] The Electronic Frontier Foundation also offers $150,000 and $250,000 for primes with at least 100 million digits and 1 billion digits, respectively.[141]

Type	Prime	Number of decimal digits	Date	Found by
Mersenne prime	$2^{82,589,933} - 1$	24,862,048	December 7, 2018[1]	Patrick Laroche, Great Internet Mersenne Prime Search
Proth prime	$10,223 \times 2^{31,172,165} + 1$	9,383,761	October 31, 2016[142]	Péter Szabolcs, PrimeGrid[143]
factorial prime	208,003! − 1	1,015,843	July 2016	Sou Fukui[144]
primorial prime[e]	1,098,133# − 1	476,311	March 2012	James P. Burt, PrimeGrid[146]
twin primes	$2,996,863,034,895 \times 2^{1,290,000} \pm 1$	388,342	September 2016	Tom Greer, PrimeGrid[147]

Integer factorization

Given a composite integer n, the task of providing one (or all) prime factors is referred to as *factorization* of n. It is significantly more difficult than primality testing,[148] and although many factorization algorithms are known, they are slower than the fastest primality testing methods. Trial division and Pollard's rho algorithm can be used to find very small factors of n,[121] and elliptic curve factorization can be effective when n has factors of moderate size.[149] Methods suitable for arbitrary large numbers that do not depend on the size of its factors include the quadratic sieve and general number field sieve. As with primality testing, there are also factorization algorithms that require their input to have a special form, including the special number field sieve.[150] As of December 2019 the largest number known to have been factored by a general-purpose algorithm is RSA-240, which has 240 decimal digits (795 bits) and is the product of two large primes.[151]

Shor's algorithm can factor any integer in a polynomial number of steps on a quantum computer.[152] However, current technology can only run this algorithm for very small numbers. As of October 2012 the largest number that has been factored by a quantum computer running Shor's algorithm is 21.[153]

Other computational applications

Several public-key cryptography algorithms, such as RSA and the Diffie–Hellman key exchange, are based on large prime numbers (2048-bit primes are common).[154] RSA relies on the assumption that it is much easier (that is, 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.[32] The Diffie–Hellman key exchange relies on the fact that there are efficient algorithms for modular exponentiation (computing $a^b \bmod c$), while the reverse operation (the discrete logarithm) is thought to be a hard problem.[155]

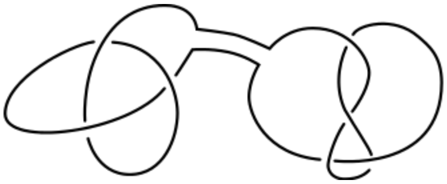
Prime numbers are frequently used for hash tables. For instance the original method of Carter and Wegman for universal hashing was based on computing hash functions by choosing random linear functions modulo large prime numbers. Carter and Wegman generalized this method to k-independent hashing by using higher-degree polynomials, again modulo large primes.[156] As well as in the hash function, prime numbers are used for the hash table size in quadratic probing based hash tables to ensure that the probe sequence covers the whole table.[157]

Some checksum methods are based on the mathematics of prime numbers. For instance the checksums used in International Standard Book Numbers are defined by taking the rest of the number modulo 11, a prime number. Because 11 is prime this method can detect both single-digit errors and transpositions of adjacent digits.[158] Another checksum method, Adler-32, uses arithmetic modulo 65521, the largest prime number less than 2^{16}.[159] Prime numbers are also used in pseudorandom number generators including linear congruential generators[160] and the Mersenne Twister.[161]

Other applications

Prime numbers are of central importance to number theory but also have many applications to other areas within mathematics, including abstract algebra and elementary geometry. For example, it is possible to place prime numbers of points in a two-dimensional grid so that no three are in a line, or so that every triangle formed by three of the points has large area.[162] Another example is Eisenstein's criterion, a test for whether a polynomial is irreducible based on divisibility of its coefficients by a prime number and its square.[163]

The concept of prime number is so important that it has been generalized in different ways in various branches of mathematics. Generally, "prime" indicates minimality or indecomposability, in an appropriate sense. For example, the prime field of a given field is its smallest subfield that contains both 0 and 1. It is either the field of rational numbers or a finite field with a prime number of elements, whence the name.[164] Often a second, additional meaning is intended by using the word prime, namely that any object can be, essentially uniquely, decomposed into its prime components. For example, in knot theory, a prime knot is a knot that is indecomposable in the sense that it cannot be written as the connected sum of two nontrivial knots. Any knot can be uniquely expressed as a connected sum of prime knots.[165] The prime decomposition of 3-manifolds is another example of this type.[166]


The connected sum of two prime knots

Beyond mathematics and computing, prime numbers have potential connections to quantum mechanics, and have been used metaphorically in the arts and literature. They have also been used in evolutionary biology to explain the life cycles of cicadas.

Constructible polygons and polygon partitions

Fermat primes are primes of the form

$$F_k = 2^{2^k} + 1,$$

with k a nonnegative integer.[167] They are named after Pierre de Fermat, who conjectured that all such numbers are prime. The first five of these numbers – 3, 5, 17, 257, and 65,537 – are prime,[168] but F_5 is composite and so are all other Fermat numbers that have been verified as of 2017.[169] A regular n-gon is constructible using straightedge and compass if and only if the odd prime factors of n (if any) are distinct Fermat primes.[168] Likewise, a regular n-gon may be constructed using straightedge, compass, and an angle trisector if and only if the prime factors of n are any number of copies of 2 or 3 together with a (possibly empty) set of distinct Pierpont primes, primes of the form $2^a 3^b + 1$.[170]

It is possible to partition any convex polygon into n smaller convex polygons of equal area and equal perimeter, when n is a power of a prime number, but this is not known for other values of n.[171]

Construction of a regular pentagon using straightedge and compass. This is only possible because 5 is a Fermat prime.

Quantum mechanics

Beginning with the work of Hugh Montgomery and Freeman Dyson in the 1970s, mathematicians and physicists have speculated that the zeros of the Riemann zeta function are connected to the energy levels of quantum systems.[172][173] Prime numbers are also significant in quantum information science, thanks to mathematical structures such as mutually unbiased bases and symmetric informationally complete positive-operator-valued measures.[174][175]

Biology

The evolutionary strategy used by cicadas of the genus *Magicicada* makes use of prime numbers.[176] These insects spend most of their lives as grubs underground. They only pupate and then emerge from their burrows after 7, 13 or 17 years, at which point they fly about, breed, and then die after a few weeks at most. Biologists theorize that these prime-numbered breeding cycle lengths have evolved in order to prevent predators from synchronizing with these cycles.[177][178] In contrast, the multi-year periods between flowering in bamboo plants are hypothesized to be smooth numbers, having only small prime numbers in their factorizations.[179]

Arts and literature

Prime numbers have influenced many artists and writers. The French composer Olivier Messiaen used prime numbers to create ametrical music through "natural phenomena". In works such as *La Nativité du Seigneur* (1935) and *Quatre études de rythme* (1949–50), he simultaneously employs motifs with lengths given by different prime numbers to create unpredictable rhythms: the primes 41, 43, 47 and 53 appear in the third étude, "Neumes rythmiques". According to Messiaen this way of composing was "inspired by the movements of nature, movements of free and unequal durations".[180]

In his science fiction novel *Contact*, scientist Carl Sagan suggested that prime factorization could be used as a means of establishing two-dimensional image planes in communications with aliens, an idea that he had first developed informally with American astronomer Frank Drake in 1975.[181] In the novel *The Curious Incident of the Dog in the Night-Time* by Mark Haddon, the narrator arranges the sections of the story by consecutive prime numbers as a way to convey the mental state of its main character, a mathematically gifted teen with Asperger syndrome.[182] Prime numbers are used as a metaphor for loneliness and isolation in the Paolo Giordano novel *The Solitude of Prime Numbers,* in which they are portrayed as "outsiders" among integers.[183]

Notes

a. A 44-digit prime number found in 1951 by Aimé Ferrier with a mechanical calculator remains the largest prime not to have been found with the aid of electronic computers.[28]

b. For instance, Beiler writes that number theorist Ernst Kummer loved his ideal numbers, closely related to the primes, "because they had not soiled themselves with any practical applications",[30] and Katz writes that Edmund Landau, known for his work on the distribution of primes, "loathed practical applications of mathematics", and for this reason avoided subjects such as geometry that had already shown themselves to be useful.[31]

c. In this test, the ± 1 term is negative if a is a square modulo the given (supposed) prime p, and positive otherwise. More generally, for non-prime values of p, the ± 1 term is the (negated) Jacobi symbol, which can be calculated using quadratic reciprocity.

d. Indeed, much of the analysis of elliptic curve primality proving is based on the assumption that the input to the algorithm has already passed a probabilistic test.[131]

e. The primorial function of n, denoted by $n\#$, yields the product of the prime numbers up to n, and a primorial prime is a prime of one of the forms $n\# \pm 1$.[145]

References

1. "GIMPS Project Discovers Largest Known Prime Number: $2^{82,589,933}$-1" (https://www.mersenne.org/primes/press/M82589933.html). *Mersenne Research, Inc*. 21 December 2018. Retrieved 21 December 2018.
2. Gardiner, Anthony (1997). *The Mathematical Olympiad Handbook: An Introduction to Problem Solving Based on the First 32 British Mathematical Olympiads 1965–1996* (https://archive.org/details/mathematicalolym1997gard). Oxford University Press. p. 26 (https://archive.org/details/mathematicalolym1997gard/page/26). ISBN 978-0-19-850105-3.
3. Henderson, Anne (2014). *Dyslexia, Dyscalculia and Mathematics: A practical guide* (https://books.google.com/books?id=uy-yGVRUilMC&pg=PA62) (2nd ed.). Routledge. p. 62. ISBN 978-1-136-63662-2.
4. Adler, Irving (1960). *The Giant Golden Book of Mathematics: Exploring the World of Numbers and Space* (https://archive.org/details/giantgoldenbooko00adle). Golden Press. p. 16 (https://archive.org/details/giantgoldenbooko00adle/page/16). OCLC 6975809 (https://www.worldcat.org/oclc/6975809).
5. Leff, Lawrence S. (2000). *Math Workbook for the SAT I* (https://archive.org/details/barronsmathworkb00leff_0). Barron's Educational Series. p. 360 (https://archive.org/details/barronsmathworkb00leff_0/page/360). ISBN 978-0-7641-0768-9.
6. Dudley, Underwood (1978). "Section 2: Unique factorization" (https://books.google.com/books?id=tr7SzBTsk1UC&pg=PA10). *Elementary number theory* (https://archive.org/details/elementarynumber00dudl_0/page/10) (2nd ed.). W.H. Freeman and Co. p. 10 (https://archive.org/details/elementarynumber00dudl_0/page/10). ISBN 978-0-7167-0076-0.
7. Sierpiński, Wacław (1988). *Elementary Theory of Numbers* (https://books.google.com/books?id=ktCZ2MvgN3MC&pg=PA113). North-Holland Mathematical Library. **31** (2nd ed.). Elsevier. p. 113. ISBN 978-0-08-096019-7.
8. Ziegler, Günter M. (2004). "The great prime number record races". *Notices of the American Mathematical Society*. **51** (4): 414–416. MR 2039814 (https://www.ams.org/mathscinet-getitem?mr=2039814).
9. Stillwell, John (1997). *Numbers and Geometry* (https://books.google.com/books?id=4elkHwVS0eUC&pg=PA9). Undergraduate Texts in Mathematics. Springer. p. 9. ISBN 978-0-387-98289-2.
10. Sierpiński, Wacław (1964). *A Selection of Problems in the Theory of Numbers* (https://archive.org/details/selectionproblem00sier). New York: Macmillan. p. 40 (https://archive.org/details/selectionproblem00sier/page/n37). MR 0170843 (https://www.ams.org/mathscinet-getitem?mr=0170843).

11. Nathanson, Melvyn B. (2000). "Notations and Conventions" (https://books.google.com/books?id=sE7lBwAAQBAJ&pg=PP10). *Elementary Methods in Number Theory*. Graduate Texts in Mathematics. **195**. Springer. ISBN 978-0-387-22738-2. MR 1732941 (https://www.ams.org/mathscinet-getitem?mr=1732941).
12. Faticoni, Theodore G. (2012). *The Mathematics of Infinity: A Guide to Great Ideas* (https://books.google.com/books?id=I433i_ZGxRsC&pg=PA44). Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. **111** (2nd ed.). John Wiley & Sons. p. 44. ISBN 978-1-118-24382-4.
13. Bruins, Evert Marie, review in *Mathematical Reviews* of Gillings, R.J. (1974). "The recto of the Rhind Mathematical Papyrus. How did the ancient Egyptian scribe prepare it?". *Archive for History of Exact Sciences*. **12** (4): 291–298. doi:10.1007/BF01307175 (https://doi.org/10.1007%2FBF01307175). MR 0497458 (https://www.ams.org/mathscinet-getitem?mr=0497458). S2CID 121046003 (https://api.semanticscholar.org/CorpusID:121046003).
14. Stillwell, John (2010). *Mathematics and Its History* (https://books.google.com/books?id=V7mxZqjs5yUC&pg=PA40). Undergraduate Texts in Mathematics (3rd ed.). Springer. p. 40. ISBN 978-1-4419-6052-8.
15. Pomerance, Carl (December 1982). "The Search for Prime Numbers". *Scientific American*. **247** (6): 136–147. Bibcode:1982SciAm.247f.136P (https://ui.adsabs.harvard.edu/abs/1982SciAm.247f.136P). doi:10.1038/scientificamerican1282-136 (https://doi.org/10.1038%2Fscientificamerican1282-136). JSTOR 24966751 (https://www.jstor.org/stable/24966751).
16. Mollin, Richard A. (2002). "A brief history of factoring and primality testing B. C. (before computers)". *Mathematics Magazine*. **75** (1): 18–29. doi:10.2307/3219180 (https://doi.org/10.2307%2F3219180). JSTOR 3219180 (https://www.jstor.org/stable/3219180). MR 2107288 (https://www.ams.org/mathscinet-getitem?mr=2107288).
17. O'Connor, John J.; Robertson, Edmund F. "Abu Ali al-Hasan ibn al-Haytham" (http://www-history.mcs.st-andrews.ac.uk/Biographies/Al-Haytham.html). *MacTutor History of Mathematics archive*. University of St Andrews..
18. Sandifer 2007, 8. Fermat's Little Theorem (November 2003), p. 45 (https://books.google.com/books?id=sohHs7ExOsYC&pg=PA45)
19. Sandifer, C. Edward (2014). *How Euler Did Even More* (https://books.google.com/books?id=3c6iBQAAQBAJ&pg=PA42). Mathematical Association of America. p. 42. ISBN 978-0-88385-584-3.
20. Koshy, Thomas (2002). *Elementary Number Theory with Applications* (https://books.google.com/books?id=-9pg-4Pa19IC&pg=PA369). Academic Press. p. 369. ISBN 978-0-12-421171-1.
21. Yuan, Wang (2002). *Goldbach Conjecture* (https://books.google.com/books?id=g4jVCgAAQBAJ&pg=PA21). Series In Pure Mathematics. **4** (2nd ed.). World Scientific. p. 21. ISBN 978-981-4487-52-8.
22. Narkiewicz, Wladyslaw (2000). "1.2 Sum of Reciprocals of Primes" (https://books.google.com/books?id=VVr3EuiHU0YC&pg=PA11). *The Development of Prime Number Theory: From Euclid to Hardy and Littlewood*. Springer Monographs in Mathematics. Springer. p. 11. ISBN 978-3-540-66289-1.
23. Tchebychev, P. (1852). "Mémoire sur les nombres premiers" (http://sites.mathdoc.fr/JMPA/PDF/JMPA_1852_1_17_A19_0.pdf) (PDF). *Journal de mathématiques pures et appliquées*. Série 1 (in French): 366–390.. (Proof of the postulate: 371-382). Also see Mémoires de l'Académie Impériale des Sciences de St. Pétersbourg, vol. 7, pp.15-33, 1854
24. Apostol, Tom M. (2000). "A centennial history of the prime number theorem" (https://books.google.com/books?id=aiDyBwAAQBAJ&pg=PA1). In Bambah, R.P.; Dumir, V.C.; Hans-Gill, R.J. (eds.). *Number Theory*. Trends in Mathematics. Basel: Birkhäuser. pp. 1–14. MR 1764793 (https://www.ams.org/mathscinet-getitem?mr=1764793).
25. Apostol, Tom M. (1976). "7. Dirichlet's Theorem on Primes in Arithmetical Progressions" (https://books.google.com/books?id=3yoBCAAAQBAJ&pg=PA146). *Introduction to Analytic Number Theory*. New York; Heidelberg: Springer-Verlag. pp. 146–156. MR 0434929 (https://www.ams.org/mathscinet-getitem?mr=0434929).

26. Chabert, Jean-Luc (2012). *A History of Algorithms: From the Pebble to the Microchip* (https://books.google.com/books?id=XcDqCAAAQBAJ&pg=PA261). Springer. p. 261. ISBN 978-3-642-18192-4.
27. Rosen, Kenneth H. (2000). "Theorem 9.20. Proth's Primality Test". *Elementary Number Theory and Its Applications* (4th ed.). Addison-Wesley. p. 342. ISBN 978-0-201-87073-2.
28. Cooper, S. Barry; Hodges, Andrew (2016). *The Once and Future Turing* (https://books.google.com/books?id=h12cCwAAQBAJ&pg=PA37). Cambridge University Press. pp. 37–38. ISBN 978-1-107-01083-3.
29. Rosen 2000, p. 245.
30. Beiler, Albert H. (1999) [1966]. *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains* (https://books.google.com/books?id=NbbbL9gMJ88C&pg=PA2). Dover. p. 2. ISBN 978-0-486-21096-4. OCLC 444171535 (https://www.worldcat.org/oclc/444171535).
31. Katz, Shaul (2004). "Berlin roots – Zionist incarnation: the ethos of pure mathematics and the beginnings of the Einstein Institute of Mathematics at the Hebrew University of Jerusalem". *Science in Context*. **17** (1–2): 199–234. doi:10.1017/S0269889704000092 (https://doi.org/10.1017%2FS0269889704000092). MR 2089305 (https://www.ams.org/mathscinet-getitem?mr=2089305).
32. Kraft, James S.; Washington, Lawrence C. (2014). *Elementary Number Theory* (https://books.google.com/books?id=4NAqBgAAQBAJ&pg=PA7). Textbooks in mathematics. CRC Press. p. 7. ISBN 978-1-4987-0269-0.
33. Bauer, Craig P. (2013). *Secret History: The Story of Cryptology* (https://books.google.com/books?id=EBkEGAOlCDsC&pg=PA468). Discrete Mathematics and Its Applications. CRC Press. p. 468. ISBN 978-1-4665-6186-1.
34. Klee, Victor; Wagon, Stan (1991). *Old and New Unsolved Problems in Plane Geometry and Number Theory* (https://books.google.com/books?id=tRdoIhHh3moC&pg=PA224). Dolciani mathematical expositions. **11**. Cambridge University Press. p. 224. ISBN 978-0-88385-315-3.
35. Neale 2017, pp. 18, 47.
36. Caldwell, Chris K.; Reddick, Angela; Xiong, Yeng; Keller, Wilfrid (2012). "The history of the primality of one: a selection of sources" (https://cs.uwaterloo.ca/journals/JIS/VOL15/Caldwell2/cald6.html). *Journal of Integer Sequences*. **15** (9): Article 12.9.8. MR 3005523 (https://www.ams.org/mathscinet-getitem?mr=3005523). For a selection of quotes from and about the ancient Greek positions on this issue, see in particular pp. 3–4. For the Islamic mathematicians, see p. 6.
37. Tarán, Leonardo (1981). *Speusippus of Athens: A Critical Study With a Collection of the Related Texts and Commentary* (https://books.google.com/books?id=cUPXqSb7V1wC&pg=PA35). Philosophia Antiqua : A Series of Monographs on Ancient Philosophy. **39**. Brill. pp. 35–38. ISBN 978-90-04-06505-5.
38. Caldwell et al. 2012, pp. 7–13. See in particular the entries for Stevin, Brancker, Wallis, and Prestet.
39. Caldwell et al. 2012, p. 15.
40. Caldwell, Chris K.; Xiong, Yeng (2012). "What is the smallest prime?" (https://cs.uwaterloo.ca/journals/JIS/VOL15/Caldwell1/cald5.pdf) (PDF). *Journal of Integer Sequences*. **15** (9): Article 12.9.7. MR 3005530 (https://www.ams.org/mathscinet-getitem?mr=3005530).
41. Riesel, Hans (1994). *Prime Numbers and Computer Methods for Factorization* (https://books.google.com/books?id=ITvaBwAAQBAJ&pg=PA36) (2nd ed.). Basel, Switzerland: Birkhäuser. p. 36. doi:10.1007/978-1-4612-0251-6 (https://doi.org/10.1007%2F978-1-4612-0251-6). ISBN 978-0-8176-3743-9. MR 1292250 (https://www.ams.org/mathscinet-getitem?mr=1292250).
42. Conway, John Horton; Guy, Richard K. (1996). *The Book of Numbers* (https://archive.org/details/bookofnumbers0000conw). New York: Copernicus. pp. 129–130 (https://archive.org/details/bookofnumbers0000conw/page/129). doi:10.1007/978-1-4612-4072-3 (https://doi.org/10.1007%2F978-1-4612-4072-3). ISBN 978-0-387-97993-9. MR 1411676 (https://www.ams.org/mathscinet-getitem?mr=1411676).

43. For the totient, see Sierpiński 1988, p. 245 (https://books.google.com/books?id=ktCZ2MvgN3MC&pg=PA245). For the sum of divisors, see Sandifer, C. Edward (2007). *How Euler Did It* (https://books.google.com/books?id=sohHs7ExOsYC&pg=PA59). MAA Spectrum. Mathematical Association of America. p. 59. ISBN 978-0-88385-563-8.
44. Smith, Karl J. (2011). *The Nature of Mathematics* (https://books.google.com/books?id=Di0HyCgDYq8C&pg=PA188) (12th ed.). Cengage Learning. p. 188. ISBN 978-0-538-73758-6.
45. Dudley 1978, Section 2, Theorem 2, p. 16 (https://books.google.com/books?id=tr7SzBTsk1UC&pg=PA16); Neale, Vicky (2017). *Closing the Gap: The Quest to Understand Prime Numbers*. Oxford University Press. p. 107 (https://books.google.com/books?id=T7Q1DwAAQBAJ&pg=PA107). ISBN 978-0-19-109243-5.
46. du Sautoy, Marcus (2003). *The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics* (https://archive.org/details/musicofprimessea00dusa). Harper Collins. p. 23 (https://archive.org/details/musicofprimessea00dusa/page/23). ISBN 978-0-06-093558-0.
47. Dudley 1978, Section 2, Lemma 5, p. 15 (https://books.google.com/books?id=tr7SzBTsk1UC&pg=PA15); Higgins, Peter M. (1998). *Mathematics for the Curious* (https://books.google.com/books?id=LeYH8P8S9oQC&pg=PA77). Oxford University Press. pp. 77–78. ISBN 978-0-19-150050-3.
48. Rotman, Joseph J. (2000). *A First Course in Abstract Algebra* (2nd ed.). Prentice Hall. Problem 1.40, p. 56. ISBN 978-0-13-011584-3.
49. Letter (http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0722.pdf) in Latin from Goldbach to Euler, July 1730.
50. Furstenberg, Harry (1955). "On the infinitude of primes". *American Mathematical Monthly*. **62** (5): 353. doi:10.2307/2307043 (https://doi.org/10.2307%2F2307043). JSTOR 2307043 (https://www.jstor.org/stable/2307043). MR 0068566 (https://www.ams.org/mathscinet-getitem?mr=0068566).
51. Ribenboim, Paulo (2004). *The little book of bigger primes* (https://books.google.com/books?id=SvnTBwAAQBAJ&pg=PA5). Berlin; New York: Springer-Verlag. p. 4. ISBN 978-0-387-20169-6.
52. Euclid's *Elements*, Book IX, Proposition 20. See David Joyce's English translation of Euclid's proof (http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html) or Williamson, James (1782). *The Elements of Euclid, With Dissertations* (https://babel.hathitrust.org/cgi/pt?id=umn.31951000084215o;view=1up;seq=95). Oxford: Clarendon Press. p. 63. OCLC 642232959 (https://www.worldcat.org/oclc/642232959).
53. Vardi, Ilan (1991). *Computational Recreations in Mathematica*. Addison-Wesley. pp. 82–89. ISBN 978-0-201-52989-0.
54. Matiyasevich, Yuri V. (1999). "Formulas for prime numbers" (https://books.google.com/books?id=oLKlk5o6WroC&pg=PA13). In Tabachnikov, Serge (ed.). *Kvant Selecta: Algebra and Analysis*. **II**. American Mathematical Society. pp. 13–24. ISBN 978-0-8218-1915-9.
55. Mackinnon, Nick (June 1987). "Prime number formulae". *The Mathematical Gazette*. **71** (456): 113–114. doi:10.2307/3616496 (https://doi.org/10.2307%2F3616496). JSTOR 3616496 (https://www.jstor.org/stable/3616496).
56. Wright, E.M. (1951). "A prime-representing function". *American Mathematical Monthly*. **58** (9): 616–618. doi:10.2307/2306356 (https://doi.org/10.2307%2F2306356). JSTOR 2306356 (https://www.jstor.org/stable/2306356).
57. Guy 2013, p. vii (https://books.google.com/books?id=EbLzBwAAQBAJ&pg=PR7).
58. Guy 2013, C1 Goldbach's conjecture, pp. 105–107 (https://books.google.com/books?id=EbLzBwAAQBAJ&pg=PA105).
59. Oliveira e Silva, Tomás; Herzog, Siegfried; Pardi, Silvio (2014). "Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$" (https://doi.org/10.1090%2FS0025-5718-2013-02787-1). *Mathematics of Computation*. **83** (288): 2033–2060. doi:10.1090/S0025-5718-2013-02787-1 (https://doi.org/10.1090%2FS0025-5718-2013-02787-1). MR 3194140 (https://www.ams.org/mathscinet-getitem?mr=3194140).

60. Tao 2009, 3.1 Structure and randomness in the prime numbers, pp. 239–247 (https://books.google.com/books?id=NxnVAwAAQBAJ&pg=PA239). See especially p. 239.
61. Guy 2013, p. 159.
62. Ramaré, Olivier (1995). "On Šnirel'man's constant" (https://www.numdam.org/item?id=ASNSP_1995_4_22_4_645_0). *Annali della Scuola Normale Superiore di Pisa*. **22** (4): 645–706. MR 1375315 (https://www.ams.org/mathscinet-getitem?mr=1375315).
63. Rassias, Michael Th. (2017). *Goldbach's Problem: Selected Topics* (https://books.google.com/books?id=ibwpDwAAQBAJ&pg=PP6). Cham: Springer. p. vii. doi:10.1007/978-3-319-57914-6 (https://doi.org/10.1007%2F978-3-319-57914-6). ISBN 978-3-319-57912-2. MR 3674356 (https://www.ams.org/mathscinet-getitem?mr=3674356).
64. Koshy 2002, Theorem 2.14, p. 109 (https://books.google.com/books?id=-9pg-4Pa19IC&pg=PA109). Riesel 1994 gives a similar argument using the primorial in place of the factorial.
65. Riesel 1994, "Large gaps between consecutive primes (https://books.google.com/books?id=ITvaBwAAQBAJ&pg=PA78)", pp. 78–79.
66. Sloane, N. J. A. (ed.). "Sequence A100964 (Smallest prime number that begins a prime gap of at least 2n)" (https://oeis.org/A100964). *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.
67. Ribenboim 2004, Gaps between primes, pp. 186–192.
68. Ribenboim 2004, p. 183.
69. Chan, Joel (February 1996). "Prime time!". *Math Horizons*. **3** (3): 23–25. doi:10.1080/10724117.1996.11974965 (https://doi.org/10.1080%2F10724117.1996.11974965). JSTOR 25678057 (https://www.jstor.org/stable/25678057). Note that Chan lists Legendre's conjecture as "Sierpinski's Postulate".
70. Ribenboim 2004, Prime k-tuples conjecture, pp. 201–202.
71. Sandifer 2007, Chapter 35, Estimating the Basel problem, pp. 205–208 (https://books.google.com/books?id=sohHs7ExOsYC&pg=PA205).
72. Ogilvy, C.S.; Anderson, J.T. (1988). *Excursions in Number Theory* (https://books.google.com/books?id=efbaDLITXvMC&pg=PA29). Dover Publications Inc. pp. 29–35. ISBN 978-0-486-25778-5.
73. Apostol 1976, Section 1.6, Theorem 1.13
74. Apostol 1976, Section 4.8, Theorem 4.12
75. Miller, Steven J.; Takloo-Bighash, Ramin (2006). *An Invitation to Modern Number Theory* (https://books.google.com/books?id=kLz4z8iwKiwC&pg=PA43). Princeton University Press. pp. 43–44. ISBN 978-0-691-12060-7.
76. Crandall & Pomerance 2005, p. 6 (https://books.google.com/books?id=RbEz-_D7sAUC&pg=PA6).
77. Crandall & Pomerance 2005, Section 3.7, Counting primes, pp. 152–162 (https://books.google.com/books?id=ZXjHKPS1LEAC&pg=PA152).
78. Crandall & Pomerance 2005, p. 10 (https://books.google.com/books?id=RbEz-_D7sAUC&pg=PA10).
79. du Sautoy, Marcus (2011). "What are the odds that your telephone number is prime?" (https://books.google.com/books?id=snaUbkIb8SEC&pg=PA50). *The Number Mysteries: A Mathematical Odyssey through Everyday Life*. St. Martin's Press. pp. 50–52. ISBN 978-0-230-12028-0.
80. Apostol 1976, Section 4.6, Theorem 4.7
81. Gelfand, I.M.; Shen, Alexander (2003). *Algebra* (https://books.google.com/books?id=Z9z7iliyFD0C&pg=PA37). Springer. p. 37. ISBN 978-0-8176-3677-7.
82. Mollin, Richard A. (1997). *Fundamental Number Theory with Applications* (https://books.google.com/books?id=Fsaa3MUUQYkC&pg=PA76). Discrete Mathematics and Its Applications. CRC Press. p. 76. ISBN 978-0-8493-3987-5.
83. Crandall & Pomerance 2005, Theorem 1.1.5, p. 12 (https://books.google.com/books?id=ZXjHKPS1LEAC&pg=PA).

84. Green, Ben; Tao, Terence (2008). "The primes contain arbitrarily long arithmetic progressions". *Annals of Mathematics*. **167** (2): 481–547. arXiv:math.NT/0404188 (https://arxiv.org/abs/math.NT/0404188). doi:10.4007/annals.2008.167.481 (https://doi.org/10.4007%2Fannals.2008.167.481). S2CID 1883951 (https://api.semanticscholar.org/CorpusID:1883951).

85. Hua, L.K. (2009) [1965]. *Additive Theory of Prime Numbers*. Translations of Mathematical Monographs. **13**. Providence, RI: American Mathematical Society. pp. 176–177. ISBN 978-0-8218-4942-2. MR 0194404 (https://www.ams.org/mathscinet-getitem?mr=0194404). OCLC 824812353 (https://www.worldcat.org/oclc/824812353).

86. The sequence of these primes, starting at $n = 1$ rather than $n = 0$, is listed by Lava, Paolo Pietro; Balzarotti, Giorgio (2010). "Chapter 33. Formule fortunate" (https://books.google.com/books?id=YfsSAAAAQBAJ&pg=PA133). *103 curiosità matematiche: Teoria dei numeri, delle cifre e delle relazioni nella matematica contemporanea* (in Italian). Ulrico Hoepli Editore S.p.A. p. 133. ISBN 978-88-203-5804-4.

87. Chamberland, Marc (2015). "The Heegner numbers" (https://books.google.com/books?id=n9iqBwAAQBAJ&pg=PA213). *Single Digits: In Praise of Small Numbers*. Princeton University Press. pp. 213–215. ISBN 978-1-4008-6569-7.

88. Guy, Richard (2013). "A1 Prime values of quadratic functions" (https://books.google.com/books?id=1BnoBwAAQBAJ&pg=PA7). *Unsolved Problems in Number Theory*. Problem Books in Mathematics (3rd ed.). Springer. pp. 7–10. ISBN 978-0-387-26677-0.

89. Patterson, S.J. (1988). *An introduction to the theory of the Riemann zeta-function* (https://books.google.com/books?id=IdHLCgAAQBAJ&pg=PA1). Cambridge Studies in Advanced Mathematics. **14**. Cambridge University Press, Cambridge. p. 1. doi:10.1017/CBO9780511623707 (https://doi.org/10.1017%2FCBO9780511623707). ISBN 978-0-521-33535-5. MR 0933558 (https://www.ams.org/mathscinet-getitem?mr=0933558).

90. Borwein, Peter; Choi, Stephen; Rooney, Brendan; Weirathmueller, Andrea (2008). *The Riemann hypothesis: A resource for the afficionado and virtuoso alike* (https://books.google.com/books?id=Qm1aZA-UwX4C&pg=PA10). CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. New York: Springer. pp. 10–11. doi:10.1007/978-0-387-72126-2 (https://doi.org/10.1007%2F978-0-387-72126-2). ISBN 978-0-387-72125-5. MR 2463715 (https://www.ams.org/mathscinet-getitem?mr=2463715).

91. Sandifer 2007, pp. 191–193 (https://books.google.com/books?id=sohHs7ExOsYC&pg=PA191).

92. Borwein et al. 2008, Conjecture 2.7 (the Riemann hypothesis), p. 15 (https://books.google.com/books?id=Qm1aZA-UwX4C&pg=PA15).

93. Patterson 1988, p. 7.

94. Borwein et al. 2008, p. 18. (https://books.google.com/books?id=Qm1aZA-UwX4C&pg=PA18)

95. Nathanson 2000, Chapter 9, The prime number theorem, pp. 289–324 (https://books.google.com/books?id=sE7lBwAAQBAJ&pg=PA289).

96. Zagier, Don (1977). "The first 50 million prime numbers". *The Mathematical Intelligencer*. **1** (S2): 7–19. doi:10.1007/bf03351556 (https://doi.org/10.1007%2Fbf03351556). S2CID 37866599 (https://api.semanticscholar.org/CorpusID:37866599). See especially pp. 14–16.

97. Kraft & Washington (2014), Proposition 5.3 (https://books.google.com/books?id=VG9YBQAAQBAJ&pg=PA96), p. 96.

98. Shahriari, Shahriar (2017). *Algebra in Action: A Course in Groups, Rings, and Fields* (https://books.google.com/books?id=GJwxDwAAQBAJ&pg=PA20). Pure and Applied Undergraduate Texts. **27**. American Mathematical Society. pp. 20–21. ISBN 978-1-4704-2849-5.

99. Dudley 1978, Theorem 3, p. 28 (https://books.google.com/books?id=tr7SzBTsk1UC&pg=PA28).

00. Shahriari 2017, pp. 27–28 (https://books.google.com/books?id=GJwxDwAAQBAJ&pg=PA27).

01. Ribenboim 2004, Fermat's little theorem and primitive roots modulo a prime, pp. 17–21.

02. Ribenboim 2004, The property of Giuga, pp. 21–22.

03. Ribenboim 2004, The theorem of Wilson, p. 21.

04. Childress, Nancy (2009). *Class Field Theory* (https://books.google.com/books?id=RYdy4PCJYosC&pg=PA8). Universitext. Springer, New York. pp. 8–11. doi:10.1007/978-0-387-72490-4 (https://doi.org/10.1007%2F978-0-387-72490-4). ISBN 978-0-387-72489-8. MR 2462595 (https://www.ams.org/mathscinet-getitem?mr=2462595). See also p. 64.
05. Erickson, Marty; Vazzana, Anthony; Garth, David (2016). *Introduction to Number Theory* (https://books.google.com/books?id=QpLwCgAAQBAJ&pg=PA200). Textbooks in Mathematics (2nd ed.). Boca Raton, FL: CRC Press. p. 200. ISBN 978-1-4987-1749-6. MR 3468748 (https://www.ams.org/mathscinet-getitem?mr=3468748).
06. Weil, André (1995). *Basic Number Theory* (https://archive.org/details/basicnumbertheor00weil_866). Classics in Mathematics. Berlin: Springer-Verlag. p. 43 (https://archive.org/details/basicnumbertheor00weil_866/page/n56). ISBN 978-3-540-58655-5. MR 1344916 (https://www.ams.org/mathscinet-getitem?mr=1344916). Note however that some authors such as Childress (2009) instead use "place" to mean an equivalence class of norms.
07. Koch, H. (1997). *Algebraic Number Theory* (https://books.google.com/books?id=wt1sCQAAQBAJ&pg=PA136). Berlin: Springer-Verlag. p. 136. CiteSeerX 10.1.1.309.8812 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.309.8812). doi:10.1007/978-3-642-58095-6 (https://doi.org/10.1007%2F978-3-642-58095-6). ISBN 978-3-540-63003-6. MR 1474965 (https://www.ams.org/mathscinet-getitem?mr=1474965).
08. Lauritzen, Niels (2003). *Concrete Abstract Algebra: From numbers to Gröbner bases* (https://books.google.com/books?id=BdAbcje-TZUC&pg=PA127). Cambridge: Cambridge University Press. p. 127. doi:10.1017/CBO9780511804229 (https://doi.org/10.1017%2FCBO9780511804229). ISBN 978-0-521-53410-9. MR 2014325 (https://www.ams.org/mathscinet-getitem?mr=2014325).
09. Lauritzen 2003, Corollary 3.5.14, p. 133; Lemma 3.5.18, p. 136.
10. Kraft & Washington 2014, Section 12.1, Sums of two squares, pp. 297–301 (https://books.google.com/books?id=4NAqBgAAQBAJ&pg=PA297).
11. Eisenbud, David (1995). *Commutative Algebra*. Graduate Texts in Mathematics. **150**. Berlin; New York: Springer-Verlag. Section 3.3. doi:10.1007/978-1-4612-5350-1 (https://doi.org/10.1007%2F978-1-4612-5350-1). ISBN 978-0-387-94268-1. MR 1322960 (https://www.ams.org/mathscinet-getitem?mr=1322960).
12. Shafarevich, Igor R. (2013). "Definition of $\operatorname{Spec} A$" (https://books.google.com/books?id=zDW8BAAAQBAJ&pg=PA5). *Basic Algebraic Geometry 2: Schemes and Complex Manifolds* (3rd ed.). Springer, Heidelberg. p. 5. doi:10.1007/978-3-642-38010-5 (https://doi.org/10.1007%2F978-3-642-38010-5). ISBN 978-3-642-38009-9. MR 3100288 (https://www.ams.org/mathscinet-getitem?mr=3100288).
13. Neukirch, Jürgen (1999). *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. **322**. Berlin: Springer-Verlag. Section I.8, p. 50. doi:10.1007/978-3-662-03983-0 (https://doi.org/10.1007%2F978-3-662-03983-0). ISBN 978-3-540-65399-8. MR 1697859 (https://www.ams.org/mathscinet-getitem?mr=1697859).
14. Neukirch 1999, Section I.7, p. 38
15. Stevenhagen, P.; Lenstra, H.W., Jr. (1996). "Chebotarëv and his density theorem". *The Mathematical Intelligencer*. **18** (2): 26–37. CiteSeerX 10.1.1.116.9409 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.116.9409). doi:10.1007/BF03027290 (https://doi.org/10.1007%2FBF03027290). MR 1395088 (https://www.ams.org/mathscinet-getitem?mr=1395088). S2CID 14089091 (https://api.semanticscholar.org/CorpusID:14089091).
16. Hall, Marshall (2018). *The Theory of Groups* (https://books.google.com/books?id=K8hEDwAAQBAJ). Dover Books on Mathematics. Courier Dover Publications. ISBN 978-0-486-81690-6. For the Sylow theorems see p. 43; for Lagrange's theorem, see p. 12; for Burnside's theorem see p. 143.
17. Bryant, John; Sangwin, Christopher J. (2008). *How Round is Your Circle?: Where Engineering and Mathematics Meet*. Princeton University Press. p. 178 (https://books.google.com/books?id=iIN_2WjBH1cC&pg=PA178). ISBN 978-0-691-13118-4.

18. Hardy, Godfrey Harold (2012) [1940]. *A Mathematician's Apology*. Cambridge University Press. p. 140 (https://books.google.com/books?id=EkY2im6xkVkC&pg=PA140). ISBN 978-0-521-42706-7. OCLC 922010634 (https://www.worldcat.org/oclc/922010634). "No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years."
19. Giblin, Peter (1993). *Primes and Programming* (https://archive.org/details/primesprogrammin0000gibl). Cambridge University Press. p. 39 (https://archive.org/details/primesprogrammin0000gibl/page/39). ISBN 978-0-521-40988-9.
20. Giblin 1993, p. 54 (https://archive.org/details/primesprogrammin0000gibl/page/54)
21. Riesel 1994, p. 220 (https://books.google.com/books?id=ITvaBwAAQBAJ&pg=PA220).
22. Bullynck, Maarten (2010). "A history of factor tables with notes on the birth of number theory 1657–1817" (https://hal-univ-paris8.archives-ouvertes.fr/hal-01103903/). *Revue d'Histoire des Mathématiques*. **16** (2): 133–216.
23. Wagstaff, Samuel S. Jr. (2013). *The Joy of Factoring* (https://books.google.com/books?id=rowCAQAAQBAJ&pg=PA191). Student mathematical library. **68**. American Mathematical Society. p. 191. ISBN 978-1-4704-1048-3.
24. Crandall, Richard; Pomerance, Carl (2005). *Prime Numbers: A Computational Perspective* (https://books.google.com/books?id=RbEz-_D7sAUC&pg=PA121) (2nd ed.). Springer. p. 121. ISBN 978-0-387-25282-7.
25. Farach-Colton, Martín; Tsai, Meng-Tsung (2015). "On the complexity of computing prime tables". In Elbassioni, Khaled; Makino, Kazuhisa (eds.). *Algorithms and Computation: 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings*. Lecture Notes in Computer Science. **9472**. Springer. pp. 677–688. arXiv:1504.05240 (https://arxiv.org/abs/1504.05240). doi:10.1007/978-3-662-48971-0_57 (https://doi.org/10.1007%2F978-3-662-48971-0_57).
26. Greaves, George (2013). *Sieves in Number Theory* (https://books.google.com/books?id=G0TtCAAAQBAJ&pg=PA1). Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge). **43**. Springer. p. 1. ISBN 978-3-662-04658-6.
27. Hromkovič, Juraj (2001). "5.5 Bibliographic Remarks" (https://books.google.com/books?id=nkeqCAAAQBAJ&pg=PA383). *Algorithmics for Hard Problems*. Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin. pp. 383–385. doi:10.1007/978-3-662-04616-6 (https://doi.org/10.1007%2F978-3-662-04616-6). ISBN 978-3-540-66860-2. MR 1843669 (https://www.ams.org/mathscinet-getitem?mr=1843669). S2CID 31159492 (https://api.semanticscholar.org/CorpusID:31159492).
28. Koblitz, Neal (1987). "Chapter V. Primality and Factoring". *A Course in Number Theory and Cryptography*. Graduate Texts in Mathematics. **114**. Springer-Verlag, New York. pp. 112–149. doi:10.1007/978-1-4684-0310-7_5 (https://doi.org/10.1007%2F978-1-4684-0310-7_5). ISBN 978-0-387-96576-5. MR 0910297 (https://www.ams.org/mathscinet-getitem?mr=0910297).
29. Pieprzyk, Josef; Hardjono, Thomas; Seberry, Jennifer (2013). "2.3.9 Probabilistic Computations" (https://books.google.com/books?id=BG2rCAAAQBAJ&pg=PA51). *Fundamentals of Computer Security*. Springer. pp. 51–52. ISBN 978-3-662-07324-7.
30. Tao, Terence (2010). "1.11 The AKS primality test" (https://terrytao.wordpress.com/2009/08/11/the-aks-primality-test/). *An epsilon of room, II: Pages from year three of a mathematical blog*. Graduate Studies in Mathematics. **117**. Providence, RI: American Mathematical Society. pp. 82–86. doi:10.1090/gsm/117 (https://doi.org/10.1090%2Fgsm%2F117). ISBN 978-0-8218-5280-4. MR 2780010 (https://www.ams.org/mathscinet-getitem?mr=2780010).
31. Atkin, A O.L.; Morain, F. (1993). "Elliptic curves and primality proving" (https://www.ams.org/mcom/1993-61-203/S0025-5718-1993-1199989-X/S0025-5718-1993-1199989-X.pdf) (PDF). *Mathematics of Computation*. **61** (203): 29–68. Bibcode:1993MaCom..61...29A (https://ui.adsabs.harvard.edu/abs/1993MaCom..61...29A). doi:10.1090/s0025-5718-1993-1199989-x (https://doi.org/10.1090%2Fs0025-5718-1993-1199989-x). JSTOR 2152935 (https://www.jstor.org/stable/2152935). MR 1199989 (https://www.ams.org/mathscinet-getitem?mr=1199989).

32. Morain, F. (2007). "Implementing the asymptotically fast version of the elliptic curve primality proving algorithm". *Mathematics of Computation*. **76** (257): 493–505. arXiv:math/0502097 (https://arxiv.org/abs/math/0502097). Bibcode:2007MaCom..76..493M (https://ui.adsabs.harvard.edu/abs/2007MaCom..76..493M). doi:10.1090/S0025-5718-06-01890-4 (https://doi.org/10.1090%2FS0025-5718-06-01890-4). MR 2261033 (https://www.ams.org/mathscinet-getitem?mr=2261033). S2CID 133193 (https://api.semanticscholar.org/CorpusID:133193).
33. Lenstra, H. W. Jr.; Pomerance, Carl (2019). "Primality testing with Gaussian periods" (https://math.dartmouth.edu/~carlp/aks111216.pdf) (PDF). *Journal of the European Mathematical Society*. **21** (4): 1229–1269. doi:10.4171/JEMS/861 (https://doi.org/10.4171%2FJEMS%2F861). MR 3941463 (https://www.ams.org/mathscinet-getitem?mr=3941463).
34. Carl Pomerance; John L. Selfridge; Samuel S. Wagstaff, Jr. (July 1980). "The pseudoprimes to $25\cdot 10^9$" (https://math.dartmouth.edu/~carlp/PDF/paper25.pdf) (PDF). *Mathematics of Computation*. **35** (151): 1003–1026. doi:10.1090/S0025-5718-1980-0572872-7 (https://doi.org/10.1090%2FS0025-5718-1980-0572872-7). JSTOR 2006210 (https://www.jstor.org/stable/2006210).
35. Robert Baillie; Samuel S. Wagstaff, Jr. (October 1980). "Lucas Pseudoprimes" (http://mpqs.free.fr/LucasPseudoprimes.pdf) (PDF). *Mathematics of Computation*. **35** (152): 1391–1417. doi:10.1090/S0025-5718-1980-0583518-6 (https://doi.org/10.1090%2FS0025-5718-1980-0583518-6). JSTOR 2006406 (https://www.jstor.org/stable/2006406). MR 0583518 (https://www.ams.org/mathscinet-getitem?mr=0583518).
36. Monier, Louis (1980). "Evaluation and comparison of two efficient probabilistic primality testing algorithms". *Theoretical Computer Science*. **12** (1): 97–108. doi:10.1016/0304-3975(80)90007-9 (https://doi.org/10.1016%2F0304-3975%2880%2990007-9). MR 0582244 (https://www.ams.org/mathscinet-getitem?mr=0582244).
37. Tao, Terence (2009). "1.7 The Lucas–Lehmer test for Mersenne primes" (https://terrytao.wordpress.com/2008/10/02/the-lucas-lehmer-test-for-mersenne-primes/). *Poincaré's legacies, pages from year two of a mathematical blog. Part I*. Providence, RI: American Mathematical Society. pp. 36–41. ISBN 978-0-8218-4883-8. MR 2523047 (https://www.ams.org/mathscinet-getitem?mr=2523047).
38. Kraft & Washington 2014, p. 41 (https://books.google.com/books?id=4NAqBgAAQBAJ&pg=PA41).
39. For instance see Guy 2013, A3 Mersenne primes. Repunits. Fermat numbers. Primes of shape $k \cdot 2^n + 1$. pp. 13–21 (https://books.google.com/books?id=1BnoBwAAQBAJ&pg=PA13).
40. "Record 12-Million-Digit Prime Number Nets $100,000 Prize" (https://www.eff.org/press/archives/2009/10/14-0). Electronic Frontier Foundation. October 14, 2009. Retrieved 2010-01-04.
41. "EFF Cooperative Computing Awards" (https://www.eff.org/awards/coop). Electronic Frontier Foundation. 2008-02-29. Retrieved 2010-01-04.
42. "PrimeGrid's Seventeen or Bust Subproject" (https://www.primegrid.com/download/SOB-31172165.pdf) (PDF). Retrieved 2017-01-03.
43. Caldwell, Chris K. "The Top Twenty: Largest Known Primes" (http://primes.utm.edu/top20/page.php?id=3). *The Prime Pages*. Retrieved 2017-01-03.
44. Caldwell, Chris K. "The Top Twenty: Factorial" (http://primes.utm.edu/top20/page.php?id=30). *The Prime Pages*. Retrieved 2017-01-03.
45. Ribenboim 2004, p. 4.
46. Caldwell, Chris K. "The Top Twenty: Primorial" (http://primes.utm.edu/top20/page.php?id=5). *The Prime Pages*. Retrieved 2017-01-03.
47. Caldwell, Chris K. "The Top Twenty: Twin Primes" (http://primes.utm.edu/top20/page.php?id=1). *The Prime Pages*. Retrieved 2017-01-03.
48. Kraft & Washington 2014, p. 275 (https://books.google.com/books?id=4NAqBgAAQBAJ&pg=PA275).
49. Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. (2014). *An Introduction to Mathematical Cryptography* (https://books.google.com/books?id=cbl_BAAAQBAJ&pg=PA329). Undergraduate Texts in Mathematics (2nd ed.). Springer. p. 329. ISBN 978-1-4939-1711-2.

50. Pomerance, Carl (1996). "A tale of two sieves". *Notices of the American Mathematical Society*. **43** (12): 1473–1485. MR 1416721 (https://www.ams.org/mathscinet-getitem?mr=1416721).
51. Emmanuel Thomé, "795-bit factoring and discrete logarithms," (https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;fd743373.1912) December 2, 2019.
52. Rieffel, Eleanor G.; Polak, Wolfgang H. (2011). "Chapter 8. Shor's Algorithm" (https://books.google.com/books?id=iYX6AQAAQBAJ&pg=PA163). *Quantum Computing: A Gentle Introduction*. MIT Press. pp. 163–176. ISBN 978-0-262-01506-6.
53. Martín-López, Enrique; Laing, Anthony; Lawson, Thomas; Alvarez, Roberto; Zhou, Xiao-Qi; O'Brien, Jeremy L. (12 October 2012). "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". *Nature Photonics*. **6** (11): 773–776. arXiv:1111.4147 (https://arxiv.org/abs/1111.4147). Bibcode:2012NaPho...6..773M (https://ui.adsabs.harvard.edu/abs/2012NaPho...6..773M). doi:10.1038/nphoton.2012.259 (https://doi.org/10.1038%2Fnphoton.2012.259). S2CID 46546101 (https://api.semanticscholar.org/CorpusID:46546101).
54. Chirgwin, Richard (October 9, 2016). "Crypto needs more transparency, researchers warn" (https://www.theregister.co.uk/2016/10/09/crypto_needs_more_transparency_researchers_warn/). *The Register*.
55. Hoffstein, Pipher & Silverman 2014, Section 2.3, Diffie–Hellman key exchange, pp. 65–67.
56. Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001) [1990]. "11.3 Universal hashing". *Introduction to Algorithms* (2nd ed.). MIT Press and McGraw-Hill. pp. 232–236. ISBN 0-262-03293-7. For k-independent hashing see problem 11–4, p. 251. For the credit to Carter and Wegman, see the chapter notes, p. 252.
57. Goodrich, Michael T.; Tamassia, Roberto (2006). *Data Structures & Algorithms in Java* (4th ed.). John Wiley & Sons. ISBN 978-0-471-73884-8. See "Quadratic probing", p. 382, and exercise C–9.9, p. 415.
58. Kirtland, Joseph (2001). *Identification Numbers and Check Digit Schemes* (https://books.google.com/books?id=Z8eka35WUb8C&pg=PA43). Classroom Resource Materials. **18**. Mathematical Association of America. pp. 43–44. ISBN 978-0-88385-720-5.
59. Deutsch, P. (1996). *ZLIB Compressed Data Format Specification version 3.3* (http://www.rfc-editor.org/rfc/rfc1950.txt). Request for Comments. **1950**. Network Working Group.
60. Knuth, Donald E. (1998). "3.2.1 The linear congruential model". *The Art of Computer Programming, Vol. 2: Seminumerical algorithms* (3rd ed.). Addison-Wesley. pp. 10–26. ISBN 978-0-201-89684-8.
61. Matsumoto, Makoto; Nishimura, Takuji (1998). "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator". *ACM Transactions on Modeling and Computer Simulation*. **8** (1): 3–30. CiteSeerX 10.1.1.215.1141 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.215.1141). doi:10.1145/272991.272995 (https://doi.org/10.1145%2F272991.272995). S2CID 3332028 (https://api.semanticscholar.org/CorpusID:3332028).
62. Roth, K.F. (1951). "On a problem of Heilbronn". *Journal of the London Mathematical Society*. Second Series. **26** (3): 198–204. doi:10.1112/jlms/s1-26.3.198 (https://doi.org/10.1112%2Fjlms%2Fs1-26.3.198). MR 0041889 (https://www.ams.org/mathscinet-getitem?mr=0041889).
63. Cox, David A. (2011). "Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first" (https://www.maa.org/sites/default/files/pdf/upload_library/22/Ford/Cox-2012.pdf) (PDF). *American Mathematical Monthly*. **118** (1): 3–31. CiteSeerX 10.1.1.398.3440 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.398.3440). doi:10.4169/amer.math.monthly.118.01.003 (https://doi.org/10.4169%2Famer.math.monthly.118.01.003). S2CID 15978494 (https://api.semanticscholar.org/CorpusID:15978494).
64. Lang, Serge (2002). *Algebra*. Graduate Texts in Mathematics. **211**. Berlin; New York: Springer-Verlag. doi:10.1007/978-1-4613-0041-0 (https://doi.org/10.1007%2F978-1-4613-0041-0). ISBN 978-0-387-95385-4. MR 1878556 (https://www.ams.org/mathscinet-getitem?mr=1878556)., Section II.1, p. 90

65. Schubert, Horst (1949). "Die eindeutige Zerlegbarkeit eines Knotens in Primknoten". *S.-B Heidelberger Akad. Wiss. Math.-Nat. Kl.* **1949** (3): 57–104. MR 0031733 (https://www.ams.org/mathscinet-getitem?mr=0031733).
66. Milnor, J. (1962). "A unique decomposition theorem for 3-manifolds". *American Journal of Mathematics*. **84** (1): 1–7. doi:10.2307/2372800 (https://doi.org/10.2307%2F2372800). JSTOR 2372800 (https://www.jstor.org/stable/2372800). MR 0142125 (https://www.ams.org/mathscinet-getitem?mr=0142125).
67. Boklan & Conway (2017) also include $2^0 + 1 = 2$, which is not of this form.
68. Křížek, Michal; Luca, Florian; Somer, Lawrence (2001). *17 Lectures on Fermat Numbers: From Number Theory to Geometry* (https://books.google.com/books?id=hgfSBwAAQBAJ&pg=PA1). CMS Books in Mathematics. **9**. New York: Springer-Verlag. pp. 1–2. doi:10.1007/978-0-387-21850-2 (https://doi.org/10.1007%2F978-0-387-21850-2). ISBN 978-0-387-95332-8. MR 1866957 (https://www.ams.org/mathscinet-getitem?mr=1866957).
69. Boklan, Kent D.; Conway, John H. (January 2017). "Expect at most one billionth of a new Fermat prime!". *The Mathematical Intelligencer*. **39** (1): 3–5. arXiv:1605.01371 (https://arxiv.org/abs/1605.01371). doi:10.1007/s00283-016-9644-3 (https://doi.org/10.1007%2Fs00283-016-9644-3). S2CID 119165671 (https://api.semanticscholar.org/CorpusID:119165671).
70. Gleason, Andrew M. (1988). "Angle trisection, the heptagon, and the triskaidecagon". *American Mathematical Monthly*. **95** (3): 185–194. doi:10.2307/2323624 (https://doi.org/10.2307%2F2323624). JSTOR 2323624 (https://www.jstor.org/stable/2323624). MR 0935432 (https://www.ams.org/mathscinet-getitem?mr=0935432).
71. Ziegler, Günter M. (2015). "Cannons at sparrows". *European Mathematical Society Newsletter* (95): 25–31. MR 3330472 (https://www.ams.org/mathscinet-getitem?mr=3330472).
72. Peterson, Ivars (June 28, 1999). "The Return of Zeta" (https://web.archive.org/web/20071020141624/http://maa.org/mathland/mathtrek_6_28_99.html). *MAA Online*. Archived from the original (http://www.maa.org/mathland/mathtrek_6_28_99.html) on October 20, 2007. Retrieved 2008-03-14.
73. Hayes, Brian (2003). "Computing science: The spectrum of Riemannium". *American Scientist*. **91** (4): 296–300. doi:10.1511/2003.26.3349 (https://doi.org/10.1511%2F2003.26.3349). JSTOR 27858239 (https://www.jstor.org/stable/27858239).
74. Bengtsson, Ingemar; Życzkowski, Karol (2017). *Geometry of quantum states : an introduction to quantum entanglement* (Second ed.). Cambridge: Cambridge University Press. pp. 313–354. ISBN 978-1-107-02625-4. OCLC 967938939 (https://www.worldcat.org/oclc/967938939).
75. Zhu, Huangjun (2010). "SIC POVMs and Clifford groups in prime dimensions" (http://stacks.iop.org/1751-8121/43/i=30/a=305305?key=crossref.45cb006b9f3c7e510461594ea8dfa7f7). *Journal of Physics A: Mathematical and Theoretical*. **43** (30): 305305. arXiv:1003.3591 (https://arxiv.org/abs/1003.3591). Bibcode:2010JPhA...43D5305Z (https://ui.adsabs.harvard.edu/abs/2010JPhA...43D5305Z). doi:10.1088/1751-8113/43/30/305305 (https://doi.org/10.1088%2F1751-8113%2F43%2F30%2F305305). S2CID 118363843 (https://api.semanticscholar.org/CorpusID:118363843).
76. Goles, E.; Schulz, O.; Markus, M. (2001). "Prime number selection of cycles in a predator-prey model". *Complexity*. **6** (4): 33–38. Bibcode:2001Cmplx...6d..33G (https://ui.adsabs.harvard.edu/abs/2001Cmplx...6d..33G). doi:10.1002/cplx.1040 (https://doi.org/10.1002%2Fcplx.1040).
77. Campos, Paulo R.A.; de Oliveira, Viviane M.; Giro, Ronaldo; Galvão, Douglas S. (2004). "Emergence of prime numbers as the result of evolutionary strategy". *Physical Review Letters*. **93** (9): 098107. arXiv:q-bio/0406017 (https://arxiv.org/abs/q-bio/0406017). Bibcode:2004PhRvL..93i8107C (https://ui.adsabs.harvard.edu/abs/2004PhRvL..93i8107C). doi:10.1103/PhysRevLett.93.098107 (https://doi.org/10.1103%2FPhysRevLett.93.098107). PMID 15447148 (https://pubmed.ncbi.nlm.nih.gov/15447148). S2CID 88332 (https://api.semanticscholar.org/CorpusID:88332).
78. "Invasion of the Brood" (http://economist.com/PrinterFriendly.cfm?Story_ID=2647052). *The Economist*. May 6, 2004. Retrieved 2006-11-26.

79. Zimmer, Carl (May 15, 2015). "Bamboo Mathematicians" (http://phenomena.nationalgeographic.com/2015/05/15/bamboo-mathematicians/). Phenomena: The Loom. *National Geographic*. Retrieved February 22, 2018.
80. Hill, Peter Jensen, ed. (1995). *The Messiaen companion* (https://books.google.com/books?id=7ag3ymWqvfgC&pg=PT225). Portland, OR: Amadeus Press. Ex. 13.2 *Messe de la Pentecôte* 1 'Entrée'. ISBN 978-0-931340-95-6.
81. Pomerance, Carl (2004). "Prime Numbers and the Search for Extraterrestrial Intelligence" (https://gauss.dartmouth.edu/~carlp/PDF/extraterrestrial.pdf) (PDF). In Hayes, David F.; Ross, Peter (eds.). *Mathematical Adventures for Students and Amateurs*. MAA Spectrum. Washington, DC: Mathematical Association of America. pp. 3–6. ISBN 978-0-88385-548-5. MR 2085842 (https://www.ams.org/mathscinet-getitem?mr=2085842).
82. GrrlScientist (September 16, 2010). "The Curious Incident of the Dog in the Night-Time" (https://www.theguardian.com/science/punctuated-equilibrium/2010/sep/16/curious-incident-dog-night-time). Science. *The Guardian*. Retrieved February 22, 2010.
83. Schillinger, Liesl (April 9, 2010). "Counting on Each Other" (https://www.nytimes.com/2010/04/11/books/review/Schillinger-t.html). Sunday Book Review. *The New York Times*.

External links

- "Prime number" (https://www.encyclopediaofmath.org/index.php?title=Prime_number). *Encyclopedia of Mathematics*. EMS Press. 2001 [1994].
- Caldwell, Chris, The Prime Pages at primes.utm.edu (http://primes.utm.edu/).
- Prime Numbers (https://www.bbc.co.uk/programmes/p003hyf5) on *In Our Time* at the BBC
- Plus teacher and student package: prime numbers (http://plus.maths.org/issue49/package/index.html) from Plus, the free online mathematics magazine produced by the Millennium Mathematics Project at the University of Cambridge.

Generators and calculators

- Prime Number Checker (http://www.archimedes-lab.org/primOmatic.html) identifies the smallest prime factor of a number.
- Fast Online primality test with factorization (https://www.alpertron.com.ar/ECM.HTM) makes use of the Elliptic Curve Method (up to thousand-digits numbers, requires Java).
- Huge database of prime numbers (http://www.bigprimes.net/)
- Prime Numbers up to 1 trillion (http://www.primos.mat.br/indexen.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Prime_number&oldid=1008728923"

This page was last edited on 24 February 2021, at 19:27 (UTC).