A prime number (or a prime) is a natural number greater than 1 that has no positive divisors other than 1 and itself. A natural number greater than 1 that is not a prime number is called a composite number. For example, 5 is prime because 1 and 5 are its only positive integer factors, whereas 6 is composite because it has the divisors 2 and 3 in addition to 1 and 6. The fundamental theorem of arithmetic establishes the central role of primes in number theory: any integer greater than 1 can be expressed as a product of primes that is unique up to ordering. The uniqueness in this theorem requires excluding 1 as a prime because one can include arbitrarily many instances of 1 in any factorization, e.g., 3, $1 \cdot 3$, $1 \cdot 1 \cdot 3$, etc. are all valid factorizations of 3.

The property of being prime (or not) is called primality. A simple but slow method of verifying the primality of a given number n is known as trial division. It consists of testing whether n is a multiple of any integer between 2 and . Algorithms much more efficient than trial division have been devised to test the primality of large numbers. These include the Miller–Rabin primality test, which is fast but has a small probability 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 January 2016[update], the largest known prime number has 22,338,618 decimal digits.

There are infinitely many primes, as demonstrated by Euclid around 300 BC. There is no known simple formula that separates prime numbers from composite numbers. However, the distribution of primes, that is to say, the statistical behaviour of primes in the large, can be 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 that a given, randomly chosen number n is prime is inversely proportional to its number of digits, or to the logarithm of n.

Many questions regarding prime numbers remain open, such as 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 whose difference is 2). Such questions spurred the development of various branches of number theory, focusing on analytic or algebraic aspects of numbers. Primes are used in several routines in information technology, such as public-key cryptography, which makes use of properties such as the difficulty of factoring large numbers into their prime factors. Prime numbers give rise to various generalizations in other mathematical domains, mainly algebra, such as prime elements and prime ideals.

Hence, 6 is not prime. The image at the right illustrates that 12 is not prime: $12 = 3 \cdot 4$. No even number greater than 2 is prime because by definition, any such number n has at least three distinct divisors, namely 1, 2, and n. This implies that n is not prime. Accordingly, the term odd prime refers to any prime number greater than 2. Similarly, when written in the usual decimal system, all prime numbers larger than 5 end in 1, 3, 7, or 9, since even numbers are multiples of 2 and numbers ending in 0 or 5 are multiples of 5.

Most early Greeks did not even consider 1 to be a number, so they could not consider it to be a prime. By the Middle Ages and Renaissance many mathematicians included 1 as the first prime number. In the mid-18th century Christian Goldbach listed 1 as the first prime in his famous correspondence with Leonhard Euler -- who did not agree. In the 19th century many mathematicians still considered the number 1 to be a prime. For example, Derrick Norman Lehmer's list of primes up to 10,006,721, reprinted as late as 1956, started with 1 as its first prime. Henri Lebesgue is said to be the last professional mathematician to call 1 prime. By the early 20th century, mathematicians began to accept that 1 is not a prime number, but rather forms its own special category as a "unit".

A large body of mathematical work would still be valid when calling 1 a prime, but Euclid's fundamental theorem of arithmetic (mentioned above) would not hold as stated. For example, the number 15 can be factored as $3 \cdot 5$ and $1 \cdot 3 \cdot 5$; if 1 were admitted as a prime, these two presentations would be

considered different factorizations of 15 into prime numbers, so the statement of that theorem would have to be modified. Similarly, the sieve of Eratosthenes would not work correctly if 1 were considered a prime: a modified version of the sieve that considers 1 as prime would eliminate all multiples of 1 (that is, all other numbers) and produce as output only the single number 1. Furthermore, the prime numbers have several properties that the number 1 lacks, such as the relationship of the number to its corresponding value of Euler's totient function or the sum of divisors function.

There are hints in the surviving records of the ancient Egyptians that they had some knowledge of prime numbers: the Egyptian fraction expansions in the Rhind papyrus, for instance, have quite different forms for primes and for composites. However, the earliest surviving records of the explicit study of prime numbers come from the Ancient Greeks. Euclid's Elements (circa 300 BC) contain important theorems about primes, including the infinitude of primes and the fundamental theorem of arithmetic. Euclid also showed how to construct a perfect number from a Mersenne prime. The Sieve of Eratosthenes, attributed to Eratosthenes, is a simple method to compute primes, although the large primes found today with computers are not generated this way.

After the Greeks, little happened with the study of prime numbers until the 17th century. In 1640 Pierre de Fermat stated (without proof) Fermat's little theorem (later proved by Leibniz and Euler). Fermat also conjectured that all numbers of the form $22n + 1$ are prime (they are called Fermat numbers) and he verified this up to $n = 4$ (or $216 + 1$). However, the very next Fermat number $232 + 1$ is composite (one of its prime factors is 641), as Euler discovered later, and in fact no further Fermat numbers are known to be prime. The French monk Marin Mersenne looked at primes of the form $2p – 1$, with p a prime. They are called Mersenne primes in his honor.

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

Modern primality tests for general numbers n can be divided into two main classes, probabilistic (or "Monte Carlo") and deterministic algorithms. Deterministic algorithms provide a way to tell for sure whether a given number is prime or not. For example, trial division is a deterministic algorithm because, if performed correctly, it will always identify a prime number as prime and a composite number as composite. Probabilistic algorithms are normally faster, but do not completely prove that a number is prime. These tests rely on testing a given number in a partly random way. For example, a given test might pass all the time if applied to a prime number, but pass only with probability p if applied to a composite number. If we repeat the test n times and pass every time, then the probability that our number is composite is $1/(1-p)n$, which decreases exponentially with the number of tests, so we can be as sure as we like (though never perfectly sure) that the number is prime. On the other hand, if the test ever fails, then we know that the number is composite.

A particularly simple example of a probabilistic test is the Fermat primality test, which relies on the fact (Fermat's little theorem) that $np \equiv n \pmod p$ for any n if p is a prime number. If we have a number b that we want to test for primality, then we work out $nb \pmod b$ for a random value of n as our test. A flaw with this test is that there are some composite numbers (the Carmichael numbers) that satisfy the Fermat identity even though they are not prime, so the test has no way of distinguishing between prime numbers and Carmichael numbers. Carmichael numbers are substantially rarer than prime numbers, though, so this test can be useful for practical purposes. More powerful extensions of the Fermat

primality test, such as the Baillie-PSW, Miller-Rabin, and Solovay-Strassen tests, are guaranteed to fail at least some of the time when applied to a composite number.

are prime. Prime numbers of this form are known as factorial primes. Other primes where either $p + 1$ or $p – 1$ is of a particular shape include the Sophie Germain primes (primes of the form $2p + 1$ with p prime), primorial primes, Fermat primes and Mersenne primes, that is, prime numbers that are of the form $2p – 1$, where p is an arbitrary prime. The Lucas–Lehmer test is particularly fast for numbers of this form. This is why the largest known prime has almost always been a Mersenne prime since the dawn of electronic computers.

The following table gives the largest known primes of the mentioned 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. The Electronic Frontier Foundation also offers $150,000 and $250,000 for primes with at least 100 million digits and 1 billion digits, respectively. Some of the largest primes not known to have any particular form (that is, no simple formula such as that of Mersenne primes) have been found by taking a piece of semi-random binary data, converting it to a number n, multiplying it by $256k$ for some positive integer k, and searching for possible primes within the interval $[256kn + 1, 256k(n + 1) – 1]$.[citation needed]

are prime for any natural number n. Here represents the floor function, i.e., largest integer not greater than the number in question. The latter formula can be shown using Bertrand's postulate (proven first by Chebyshev), which states that there always exists at least one prime number p with $n < p < 2n – 2$, for any natural number $n > 3$. However, computing A or μ requires the knowledge of infinitely many primes to begin with. Another formula is based on Wilson's theorem and generates the number 2 many times and all other primes exactly once.

can have infinitely many primes only when a and q are coprime, i.e., their greatest common divisor is one. If this necessary condition is satisfied, Dirichlet's theorem on arithmetic progressions asserts that the progression contains infinitely many primes. The picture below illustrates this with $q = 9$: the numbers are "wrapped around" as soon as a multiple of 9 is passed. Primes are highlighted in red. The rows (=progressions) starting with $a = 3$, 6, or 9 contain at most one prime number. In all other rows ($a = 1$, 2, 4, 5, 7, and 8) there are infinitely many prime numbers. What is more, the primes are distributed equally among those rows in the long run—the density of all primes congruent a modulo 9 is 1/6.

The zeta function is closely related to prime numbers. For example, the aforementioned fact that there are infinitely many primes can also be seen using the zeta function: if there were only finitely many primes then $\zeta(1)$ would have a finite value. However, the harmonic series $1 + 1/2 + 1/3 + 1/4 + ...$ diverges (i.e., exceeds any given number), so there must be infinitely many primes. Another example of the richness of the zeta function and a glimpse of modern algebraic number theory is the following identity (Basel problem), due to Euler,

The unproven Riemann hypothesis, dating from 1859, states that except for $s = –2, –4, ...$, all zeroes of the ζ-function have real part equal to 1/2. The connection to prime numbers is that it essentially says that the primes are as regularly distributed as possible.[clarification needed] From a physical viewpoint, it roughly states that the irregularity in the distribution of primes only comes from random noise. From a mathematical viewpoint, it roughly states that the asymptotic distribution of primes (about $x/\log x$ of numbers less than x are primes, the prime number theorem) also holds for much shorter intervals of length about the square root of x (for intervals near x). This hypothesis is generally believed to be correct. In particular, the simplest assumption is that primes should have no significant irregularities without good reason.

In addition to the Riemann hypothesis, many more conjectures revolving about primes have been posed. Often having an elementary formulation, many of these conjectures have withstood a proof for

decades: all four of Landau's problems from 1912 are still unsolved. 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. As of February 2011[update], this conjecture has been verified for all numbers up to $n = 2 \cdot 1017$. 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. 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. Also, any even integer can be written as the sum of six primes. The branch of number theory studying such questions is called additive number theory.

A third type of conjectures concerns aspects of the distribution of primes. It is conjectured that there are infinitely many twin primes, pairs of primes with difference 2 (twin prime conjecture). Polignac's conjecture is a strengthening of that conjecture, it states that for every positive integer n, there are infinitely many pairs of consecutive primes that differ by 2n. It is conjectured there are infinitely many primes of the form $n2 + 1$. These conjectures are special cases of the broad Schinzel's hypothesis H. Brocard's conjecture says that there are always at least four primes between the squares of consecutive primes greater than 2. Legendre's conjecture states that there is a prime number between $n2$ and $(n + 1)2$ for every positive integer n. It is implied by the stronger Cramér's conjecture.

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

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

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

The evolutionary strategy used by cicadas of the genus Magicicada make use of prime numbers. 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. The logic for this is believed to be that the prime number intervals between emergences make it very difficult for predators to evolve that could specialize as predators on Magicicadas. If Magicicadas appeared at a non-prime number intervals, say every 12 years, then predators appearing every 2, 3, 4, 6, or 12 years would be sure to meet them. Over a 200-year period, average predator populations during hypothetical outbreaks of 14- and 15-year cicadas would be up to 2% higher than during outbreaks of 13- and 17-year cicadas. Though small, this advantage appears to have been enough to drive natural selection in favour of a prime-numbered life-cycle for these insects.

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 is the smallest subfield of a field F containing both 0 and 1. It is either Q or the finite field with p elements, whence the name. 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 knot sum of two nontrivial knots. Any knot can be uniquely expressed as a connected sum of prime knots. Prime models and prime 3-manifolds are other examples of this type.

Prime numbers give rise to two more general concepts that apply to elements of any commutative ring R, an algebraic structure where addition, subtraction and multiplication are defined: prime elements and irreducible elements. An element p of R is called prime element if it is neither zero nor a unit (i.e., does not have a multiplicative inverse) and satisfies the following requirement: given x and y in R such that p divides the product xy, then p divides x or y. An element is irreducible if it is not a unit and cannot be written as a product of two ring elements that are not units. In the ring Z of integers, the set of prime elements equals the set of irreducible elements, which is

The fundamental theorem of arithmetic continues to hold in unique factorization domains. An example of such a domain is the Gaussian integers Z[i], that is, the set 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 prime (in Z) is a Gaussian prime: in the bigger ring Z[i], 2 factors into the product of the two Gaussian primes (1 + i) and (1 – i). Rational primes (i.e. prime elements in Z) of the form 4k + 3 are Gaussian primes, whereas rational primes of the form 4k + 1 are not.

In ring theory, the notion of number is generally replaced with that of ideal. 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.

Prime ideals are the points of algebro-geometric objects, via the notion of the spectrum of a ring. 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. Such ramification questions occur even 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 solvability of quadratic equations

In particular, this norm gets smaller when a number is multiplied by p, in sharp contrast to the usual absolute value (also referred to as the infinite prime). While completing Q (roughly, filling the gaps) with respect to the absolute value yields the field of real numbers, completing with respect to the p-adic norm |–|p yields the field of p-adic numbers. These are essentially all possible ways to complete Q, by Ostrowski's theorem. Certain arithmetic questions related to Q or more general global fields may be transferred back and forth to the completed (or local) fields. This local-global principle again underlines the importance of primes to number theory.

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".