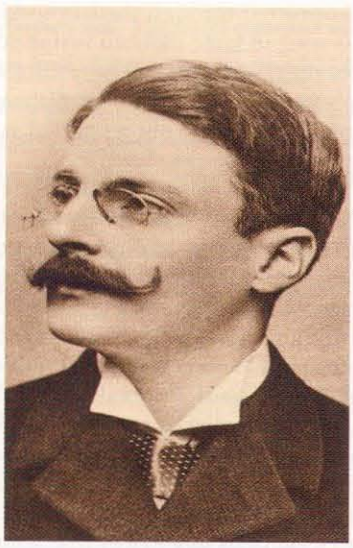
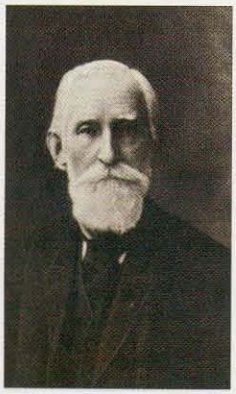
The emergence of number theory as a by-product of numerology is analogous to that of another great science, astronomy, which owes its origins to a pseudoscience, astrology.





A Centennial History of the Prime Number Theorem

By Tom M. Apostol

The prime number theorem was proved in 1896 by Charles-Jean de la Vallée Poussin and Jacques Salomon Hadamard, working independently of each other. Both de la Vallée Poussin (top left) and Hadamard (top right) built on the legacy of work by many previous mathematicians, including (in clockwise order from Hadamard) Carl Friedrich Gauss, Pafnuty Lvovich Chebyshev, Georg Friedrich Bernhard Riemann, and Leonhard Euler.

This year mathematicians all over the world are observing the 100th anniversary of the first proof of the prime number theorem, a landmark discovery in the history of mathematics. This famous theorem tells us what proportion of the positive integers are prime numbers. (The positive integers are the counting numbers: 1, 2, 3, 4, 5, and so on; a prime number is a positive integer greater than 1 that is divisible only by itself and by 1.) The prime number theorem is part of a branch of mathematics called number theory, which deals with properties of all the integers—positive, negative, and zero. The first proof was obtained independently in 1896 by two young mathematicians—Frenchman Jacques Salomon Hadamard, age 31, and Belgian Charles-Jean de la Vallée Poussin, age 30. Theirs was a remarkable achievement, the culmination of a century of efforts by an international collection of celebrated mathematicians.

The positive integers were undoubtedly humanity's first mathematical creation. It is hardly possible to imagine human beings without the ability to count, at least within a limited range. Numbers were used for record-keeping and commercial transactions for centuries before anyone thought of speculating about the nature and properties of the numbers themselves. This curiosity developed into a sort of number-mysticism or numerology, and even today numbers such as 3, 7, 11, and 13 are considered omens of good or bad luck. The emergence of number theory as a by-product of numerology is analogous to that of another great science, astronomy, which owes its origins to a pseudoscience, astrology.

The first scientific approach to the study of the integers, that is, the true origin of number theory (still intermixed with a good deal of number mysticism), is generally attributed to the ancient Greeks. Around 600 B.C. Pythagoras and his disciples classified the positive integers in various ways; examples include

Even numbers:
2, 4, 6, 8, 10, 12, 14, 16, 18, 20, ...
Odd numbers:
1, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...
Prime numbers:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, ...
Composite numbers:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...

Numbers that aren't prime are composite, except that the number 1 is neither prime nor composite. The Pythagoreans also linked numbers with geometry and with music—the latter by discovering the relationship between the length of a plucked string and its harmonic properties. (For example, a string that is one-half as long as another string under equal tension will sound an octave higher.)

The first systematic study of prime numbers appeared around 300 B.C., when Euclid wrote his *Elements*, a remarkable collection of 13 books that contained much of the mathematics known at that time. Books 7, 8, and 9 deal with properties of the integers and contain the early beginnings of number theory, a body of knowledge that has flourished ever since. It has grown into a vast and beautiful branch of mathematics that for centuries has attracted the attention of both amateur and professional mathematicians. It attracts amateurs because most of its problems are simple to state and easy to understand. It attracts professionals because these same problems are often difficult to solve, and reveal relations of great depth and elegance.

Prime numbers derive their importance from a theorem, called the fundamental theorem of arithmetic, which was first enunciated by the German mathematician Carl Friedrich Gauss. This theorem states that every integer n greater than 1 can

Courtesy of The Huntington Library, San Marino, California

Very little is known of the life of Euclid, who flourished around 300 B.C. and whose 13-volume Elements distills most of the mathematical wisdom of his day. He founded a school at Alexandria, in Egypt, and was a personal tutor to King Ptolemy I. When asked by Ptolemy if there was no shorter way to learn geometry than reading all 13 books, Euclid is said to have replied, "There is no royal road to geometry."

The largest known prime, as of September 3, 1996, is $2^{1,257,787} - 1$; it contains 378,632 digits, which, if printed in the *Los Angeles Times*, would fill 12 pages.

be factored as a product of prime numbers in one and only one way, if one ignores the order of the factors. For example, the number 12 has three different factorizations (1×12, 2×6, and 3×4) in which at least one factor is composite, but only one factorization ($2 \times 2 \times 3$) in which all the factors are primes. The fundamental theorem shows that the prime numbers are the building blocks of the mathematical world, just as the fundamental particles of physics are the building blocks of the physical world.

The fact that every positive integer is a product of prime numbers was known in Euclid's time, but the *uniqueness* of that factorization was first explicitly stated by Gauss in 1801 in his *Disquisitiones Arithmeticae*, one of the earliest books devoted exclusively to number theory. Gauss deduced the fundamental theorem from Proposition 30 in Book 7 of Euclid's *Elements*, which states that if a prime divides a product of two integers, then that prime must also divide at least one of the factors. Gauss, who is hailed as the greatest pure mathematician of all time, made enormous contributions to other branches of mathematics, as well as to astronomy and physics, but he considered the *Disquisitiones* to be his greatest work.

Proposition 20 in Book 9 of the *Elements* states that there are infinitely many primes. Many proofs of this theorem exist, but Euclid's original proof is the most elegant. It is a proof by contradiction that goes as follows. Suppose that there were only a finite number of primes, and let P denote their product. Look at the number $Q = P + 1$. Since Q is greater than 1 it must be divisible by some prime occurring in the product P, because P contains *all* the primes. However, such a prime would also divide their difference $Q - P$, because whenever two numbers (say, 35 and 20) have a common factor, their difference (in this case 15) also has that factor (5, in this example). But in the case of Q and P this is impossible, because $Q - P$ is equal to 1 and no prime divides 1.

A more sophisticated proof of Euclid's theorem was given many centuries later by the Swiss mathematician Leonhard Euler. In 1737, Euler showed that by adding the reciprocals of successive prime numbers you can attain a sum greater than any prescribed number. (This is written symbolically as

$$\tfrac{1}{2}+\tfrac{1}{3}+\tfrac{1}{5}+\tfrac{1}{7}+\tfrac{1}{11}+\tfrac{1}{13}+\tfrac{1}{17}+\tfrac{1}{19}+\cdots=\infty$$

where the ∞ represents infinity, and the $\cdots$ indicates that the sum is to be continued indefinitely.) Therefore, there must be infinitely many primes—otherwise the sum would be finite. Mathematicians describe this by saying that the infinite series of reciprocals of the primes diverges.

A question that presents itself at the very threshold of mathematics is this: How are the primes distributed among the positive integers? Detailed examination of a table of primes reveals great irregularities in their distribution.

Some primes are very close together, like 3 and 5; 11 and 13; 17 and 19; or 59 and 61—these are examples of pairs of twin primes, primes that differ by 2. Twin primes keep recurring as far as we can see, as the table below shows.

x	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}
number of twin prime pairs less than x	35	205	1,224	8,169	58,980	440,312	3,424,506	27,412,679	224,376,048

Leonhard Euler (1703–1783) lost the use of his right eye to overwork when only 28. When a friend attempted to commiserate, Euler is said to have remarked, "I shall now have fewer distractions." A cataract robbed him of his other eye at age 51, but his work continued undiminished with the assistance of his sons, an excellent memory, and a remarkable knack for mental computation.

The largest known pair of twin primes is $242{,}206{,}083 \times 2^{38{,}880}$ plus and minus 1. (The largest known prime, as of September 3, 1996, is $2^{1{,}257{,}787}-1$; it contains 378,632 digits, which, if printed in the *Los Angeles Times*, would fill 12 pages.) It would appear that there are infinitely many pairs of twin primes, but to date no one knows whether or not this is true. In 1919, the Norwegian mathematician Viggo Brun tried to use Euler's method to prove that there are infinitely many pairs of twin primes, but instead he found that the sum of the reciprocals of all the twin primes is not divergent but has a finite sum, now called Brun's constant B:

$$B=(\tfrac{1}{3}+\tfrac{1}{5})+(\tfrac{1}{5}+\tfrac{1}{7})+(\tfrac{1}{11}+\tfrac{1}{13})+(\tfrac{1}{17}+\tfrac{1}{19})+\cdots$$

Its value to five decimal places is 1.90216, which gives you some idea of the scarcity of twin primes, even if there are infinitely many of them.

But there are also large gaps between consecutive primes. For example, there are no primes between 20,831,323 and 20,831,533. In fact, it is easy to prove that arbitrarily large gaps must eventually exist between primes. Choose any integer n greater than 1 and look at the set of $n-1$ consecutive numbers $n!+2$, $n!+3$, $n!+4,\ldots, n!+n$. (The exclamation mark, called a factorial, indicates that the n in $n!$ is to be multiplied by all the positive integers less than it—for example, $5! = 5\times4\times3\times2\times1$.) All of the numbers in this set are composite ($n!+2$ is divisible by 2, $n!+3$ by 3, $n!+4$ by 4, etc.), and since n can be as large as you please, this means that there must eventually be arbitrarily long strings of consecutive composite numbers, and hence arbitrarily large gaps between consecutive primes. So we see that consecutive primes can be very close together, or very far apart. This irregular distribution is one of the difficulties inherent in the study of primes. Another difficulty is that no simple formula exists for producing all the primes.

Euclid's theorem on the infinitude of primes can be stated another way. Arrange the primes in increasing order and let p_n denote the nth prime, so that $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$. We can regard p_n as a function of n. Euclid's theorem states that p_n becomes as big as you want it to be as n increases without bound. Mathematicians describe this by saying that p_n tends to infinity as n tends to infinity; in symbols, $p_n \to \infty$ as $n \to \infty$. How fast does p_n go to infinity? Since not all positive integers are primes, p_n must grow more rapidly than n. But what is the actual growth rate of p_n for large n?

The prime number theorem—the title character of this tale—answers this question. The prime number theorem states that, for very large n, p_n is about the size of $n \log n$, where $\log n$ is the natural logarithm of n (the logarithm of n to the base e, sometimes written as $\log_e n$, or as $\ln n$; $e = 2.71828\ldots$). This is expressed symbolically as follows:

$$p_n \sim n \log n \quad \text{as } n \to \infty.$$

The symbol ~ is read as "is asymptotically equal to," which means that you can make the ratio $\frac{p_n}{n \log n}$ get as close to 1 as you like by pushing n farther and farther out toward infinity.

One can also turn the growth-rate question on its head and ask, how many primes are there that are less than or equal to any given positive value of x? This number depends on x and is denoted by $\pi(x)$. If a table of primes is available, $\pi(x)$ can be determined by simply counting the number of primes up to x. But don't panic if you can't find a table, or if the one you have isn't big enough—a second, logically equivalent version of the prime number theorem states that $\pi(x)$ is asymptotically equal to x divided by the natural logarithm of x. In symbols this is written as follows:

$$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty.$$

Again, this means that the ratio $\pi(x)/\frac{x}{\log x}$ approaches the limit 1 as x goes to infinity.

People began to speculate about the distribution of primes after extended tables of primes appeared in the 17th and 18th centuries. In 1791, the 14-year old Gauss examined a table (compiled by Johann Heinrich Lambert in 1770) that listed all the prime numbers less than 102,000. Gauss counted the primes in blocks of 100, 1,000, and 10,000 consecutive integers, and made a note in his diary that the function $1/\log n$ was a good approximation of the average density of distribution of primes in the interval from 2 to n. He offered no proof, only the numerical evidence he obtained by looking at the table. In 1797, when Georg Freiherr von Vega published an extended table of primes up to 400,031, Gauss substantiated his hypothesis further, and he kept returning to this work as new tables of primes appeared. Many years later, in 1849, he communicated his observations in a letter to the astronomer Johann Franz Encke, and the results were published posthumously in 1862. (Gauss died in 1855.) Based on tables listing primes up to 3 million, Gauss observed that $\pi(x)$ is closely approximated by the integral of the density function, $\int_2^x dn/\log n$. (This is called the logarithmic integral and is denoted by $\mathrm{Li}(x)$.) The table below is adapted from his letter to Encke. It shows $\pi(x)$ and $\mathrm{Li}(x)$ for x between $^1/_2$ million and 3 million. The agreement between $\pi(x)$ and $\mathrm{Li}(x)$ is striking—the error in each approximation is only about one-tenth of one percent.

Carl Friedrich Gauss (1777–1855) was a child prodigy who, he once said, "could count before he could talk." Gauss reveled in computations for their own sake. When Guiseppe Piazzi of the Palermo Observatory discovered the first asteroid, Ceres, on January 1, 1801, only to lose it again 40 days later as it appeared to approach the sun, Gauss sat himself down and computed its orbit from three of Piazzi's observations. Ceres was rediscovered within a year's time by several astronomers using Gauss's calculations.

x	$\pi(x)$	$\mathrm{Li}(x)$	% error
500,000	41,556	41,604.4	0.12
1,000,000	78,501	78,627.5	0.16
1,500,000	114,112	114,263.1	0.13
2,000,000	148,883	149,054.8	0.11
2,500,000	183,016	183,245.0	0.12
3,000,000	216,745	216,970.6	0.10

The first textbook devoted entirely to number theory was published in 1798 by a Frenchman, Adrien Marie Legendre. In the second edition of this text, published in 1808, Legendre also considered the problem of the distribution of primes. An appendix page from Legendre's second edition displays approximations to $\pi(x)$ for various x up to a million. Legendre asserted that $\pi(x)$ is closely approximated by the quotient

$$\frac{x}{\log x - 1.08366}.$$

On a later page Legendre states that $\pi(x)$ is approximately equal to the quotient

$$\frac{x}{\log x - A(x)}$$

where $A(x)$ is an unspecified function of x that approaches 1.08366 as x goes to infinity. It seems likely that Legendre introduced the number 1.08366 to make his formula approximate $\pi(x)$ more closely.

Neither Gauss nor Legendre revealed how they arrived at the appearance of the natural logarithm in their formulas. Nor did they make any explicit statement about how good they thought these approximations were outside the range of the existing prime number tables. It is generally understood that both intended to imply that the ratio of $\pi(x)$ to each approximating formula tends to the limit 1 as x tends to infinity. An elementary calculus exercise shows that Gauss's logarithmic integral $\mathrm{Li}(x)$ is asymptotically equal to $x/\log x$, so the conjectures of Gauss and Legendre are both equivalent to the statement now known as the prime number theorem:

$\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$, which means $\frac{\pi(x)}{(\frac{x}{\log x})} \to 1$ as $x \to \infty$.

This is one of the most astonishing results in all of mathematics. It describes a simple relation between the primes and the natural logarithm function—which, at first glance, has nothing to do with prime numbers.

It's natural to ask what led Gauss and Legendre to use the natural logarithm in their formulas. They did not leave any written clues; they simply recorded their formulas and the supporting data. Let's see how one might be led to conjecture the prime number theorem by examining a table of primes. Below are some values of $\pi(x)$. This table lists the number of primes less than successive even powers of 10. Gauss had access to tables that only went up to 3,000,000—the last four columns have been added from more modern tables.

x	10^2	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}
$\pi(x)$	25	1,229	78,498	5,761,455	455,052,512	37,607,912,018	3,204,941,750,802

What can we learn by looking at these numbers? Since we want to find how fast $\pi(x)$ grows with x, it's natural to look at the ratio $x/\pi(x)$, which compares the two quantities. The next table shows the corresponding ratios.

x	10^2	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}
$\pi(x)$	25	1,229	78,498	5,761,455	455,052,512	37,607,912,018	3,204,941,750,802
$x/\pi(x)$	4.000	8.137	12.739	17.357	21.975	26.590	31.202

Notice the differences between successive entries in that row of numbers: 4.137, 4.602, 4.618, 4.618, 4.615, 4.612. In each interval where the exponent of 10 increases by 2, we see that the ratio $x/\pi(x)$ increases by an almost constant amount, 4.6, which is 2.3 times the change in the exponent of 10. But if x is expressed as a power of 10, then the exponent of x is the logarithm of x to the base 10. So the table indicates that the change in the ratio $x/\pi(x)$ is approximately equal to 2.3 times the change in $\log_{10} x$. What about this strange factor 2.3? A bright 14-year-old such as Gauss would immediately realize that the factor 2.3 is very nearly the logarithm of 10 to the base e (in fact, $\log_e 10 = 2.3026\ldots$), so

$$2.3 \log_{10} x = (\log_e 10)(\log_{10} x) = \log_e x = \log x.$$

This suggests that we compare the ratio $x/\pi(x)$ with the natural logarithm of x. Our table now looks like this:

x	10^2	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}
$\pi(x)$	25	1,229	78,498	5,761,455	455,052,512	37,607,912,018	3,204,941,750,802
$x/\pi(x)$	4.000	8.137	12.739	17.357	21.975	26.590	31.202
$\log x$	4.605	9.210	13.816	18.421	23.026	27.361	32.236
$\log x / (x/\pi(x))$	1.151	1.132	1.085	1.061	1.048	1.039	1.033

Anyone looking at this last row of numbers would surely be tempted to conjecture that they approach 1 as x approaches infinity. Gauss, Legendre, and many other eminent mathematicians of the early 19th century apparently thought so, but they were unable to prove it. As far as we know, neither Gauss nor Legendre made any significant progress toward a proof.

Peter Gustav Lejeune Dirichlet (1805–1859) was deeply influenced by Gauss, and kept a much-thumbed, well-worn copy of the Disquisitiones Arithmeticae at his side at all times. Dirichlet was said to be one of the first people to actually understand this masterwork, and did much to make it accessible to others. In later years, Dirichlet became a friend of Gauss's as well as a disciple, eventually succeeding him to the professorship at Göttingen.

In the 1808 edition of his book, Legendre made another conjecture—on prime numbers in arithmetic progressions—that plays a tangential role in this story. An arithmetic progression is a sequence of numbers in which the difference between any number and its predecessor is a constant. So if the first term in the progression is b and the common difference is k, the progression consists of all numbers of the form $kn + b$ as n runs through all the nonnegative integers 0, 1, 2, 3, ... For example, if $b = 1$ and $k = 2$, the progression consists of all numbers of the form $2n + 1$; these are the odd numbers: 1, 3, 5, 7, 9, 11, 13, ... This particular progression contains infinitely many primes—in fact, it contains all of them except the prime number 2. The odd numbers, in turn, can be separated into two new progressions—those numbers of the form $4n + 1$,

$$1, 5, 9, 13, 17, 21, \ldots, 4n + 1, \ldots$$

and those of the form $4n + 3$,

$$3, 7, 11, 15, 19, 23, \ldots, 4n + 3, \ldots$$

Again, each of these progressions contains infinitely many primes.

Primes in the progression $4n + 1$ had already been investigated by the leading mathematician of the 17th century, the Frenchman Pierre de Fermat. He discovered the surprising result that every prime of the form $4n + 1$ is the sum of two squares. For example, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, and $29 = 2^2 + 5^2$. Although he never investigated the distribution of primes, Fermat was the first to discover really deep properties of the integers and is generally acknowledged to be the father of modern number theory.

But returning to the more general progression $kn + b$, you can see that if b and k have a common prime factor p, then each term of the progression is divisible by p and there can be no more than one prime in that progression. Legendre conjectured that there must be infinitely many primes in the progression $kn + b$ if b and k have no common prime factor, but he offered no proof.

In a celebrated paper published in 1837, the German mathematician Peter Gustav Lejeune Dirichlet

proved Legendre's conjecture. Inspired by Euler's proof of the infinitude of primes, Dirichlet used an ingenious argument to show that the sum of the reciprocals of all the primes in the progression $kn + h$ diverges, which implies that there are infinitely many primes in the progression. This result is now known as Dirichlet's theorem of the infinitude of primes in arithmetic progressions.

Dirichlet's proof was an incredible accomplishment. It marked the birth of a new branch of mathematics called analytic number theory, in which problems pertaining only to the integers were attacked by going outside the realm of integers. By using concepts that depend on functions of a continuous variable, Dirichlet brought the methods of calculus to bear on problems concerning integers, and changed the way that everyone approached the prime number theorem thereafter. The ideas introduced in Dirichlet's paper laid the groundwork not only for analytic number theory, but also for algebraic number theory, in which the methods of abstract algebra are used to study the properties of the integers.

Dirichlet's proof was an incredible accomplishment. It marked the birth of a new branch of mathematics called analytic number theory, in which problems pertaining only to the integers were attacked by going outside the realm of integers.

But the first real step toward a proof of the prime number theorem itself was made in 1848 by the Russian mathematician, Pafnuty Lvovich Chebyshev. He proved that if the ratio $\pi(x)(\log x)/x$ has a limit as x goes to infinity, then this limit must equal 1. However, Chebyshev was unable to prove that this ratio actually tends to a limit. Then, in 1850, he proved that this ratio lies between 0.89 and 1.11 for all sufficiently large x. So, although he still couldn't make the ratio converge, as it were, he established that the ratio $x/\log x$ does, indeed, represent the true order of magnitude of $\pi(x)$.

Chebyshev also introduced two new functions that are somewhat easier to deal with than $\pi(x)$, and that became the focus of nearly all subsequent work on the prime number theorem. One of these functions, denoted by $\theta(x)$, is defined to be the sum of the logarithms of all the primes not exceeding x. The other function, denoted by $\psi(x)$, is the sum $\psi(x) = \theta(x) + \theta(x^{\frac{1}{2}}) + \theta(x^{\frac{1}{3}}) + \cdots + \theta(x^{\frac{1}{m}})$, where m is the smallest positive integer for which x is less than 2^m. Chebyshev then showed that proving the prime number theorem is equivalent to proving that one of the ratios $\theta(x)/x$ or $\psi(x)/x$ approaches the limit 1 as x goes to infinity. When the prime number theorem was eventually proved in 1896, the argument was based on Chebyshev's functions.

Pafnuty Lvovich Chebyshev (1821–1894) was fascinated by mechanical toys as a boy. His quest to understand machinery led to an interest in geometry and ultimately to the rest of mathematics. He returned to mechanical problems time and again throughout his career, attempting to construct a machine that would draw a straight line when a crank was turned. Although Chebyshev failed to solve this problem (a student of his eventually did), in the attempt he invented the polynomials that bear his name.

A German named Georg Friedrich Bernhard Riemann made the next significant step in 1859, in a famous 8-page paper—the only one he wrote on number theory—that was remarkable for its brevity and for the wealth of its ideas. He attacked the problem with a new method, inspired by a discovery that Euler had made in 1732.

When Euler proved Euclid's theorem on the infinitude of primes by showing that the sum of the reciprocals of all the primes diverges, his argument was based on a formula he discovered that relates the prime numbers and the sum of the sth powers of the reciprocals of all the positive integers

$$1 + \tfrac{1}{2^s} + \tfrac{1}{3^s} + \tfrac{1}{4^s} + \tfrac{1}{5^s} + \cdots .$$

This infinite series is usually written more briefly as follows, using summation notation:

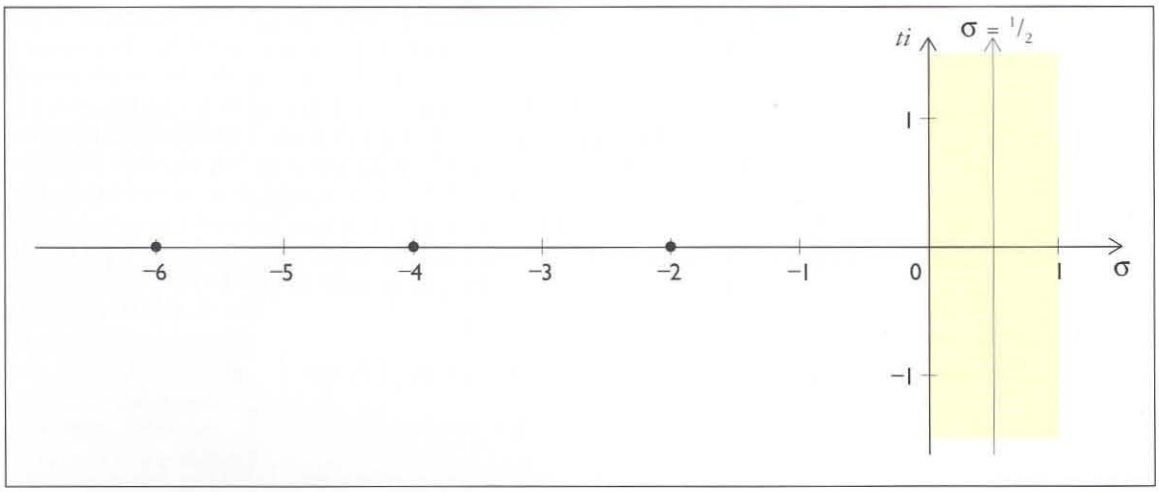
$$\sum_{n=1}^{\infty} \frac{1}{n^s} .$$

(The embellishments above and below the summation symbol Σ tell us to add up all the terms of the form $1/n^s$ as n goes from 1 to infinity.) Every beginning calculus student learns about this series while studying convergence tests. The series has a finite sum (converges) if the exponent s is greater than 1. For example, when $s = 2$, Euler discovered the striking result that the sum of the series is $\pi^2/6$:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} ,$$

where π is that famous number from geometry, 3.14159..., the ratio of the circumference of any circle to its diameter. He also showed that if the squares are replaced by fourth powers the result is $\pi^4/90$, and if they are replaced by sixth powers the result is $\pi^6/945$. However, if s is less than or equal to 1, the series has no finite sum—it diverges. Euler discovered that for s greater than 1 this series could also be expressed as an infinite product extended over all the primes. This relation is usually written as follows:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{p^s}{p^s - 1} .$$



Right: The complex-number plane maps all numbers of the form σ + ti. The integers lie on the σ axis; pure imaginary numbers lie on the ti axis. The trivial zeros of the Riemann zeta function are plotted; the non-trivial zeros lie somewhere in the critical strip, which is shown in yellow.

The infinite product symbol means that we are to multiply factors of this type for every prime p. For example, taking $s = 2$, we obtain a remarkable formula for expressing $\pi^2/6$ as an infinite product involving all the prime numbers:

$$\frac{\pi^2}{6} = \frac{2^2}{2^2-1} \times \frac{3^2}{3^2-1} \times \frac{5^2}{5^2-1} \times \frac{7^2}{7^2-1} \times \cdots$$

Georg Friedrich Bernhard Riemann (1826–1866) studied under Dirichlet, and upon his death succeeded him in the professorship that had once been Gauss's. He died of tuberculosis at age 39 while in Italy, on one of several trips he took to escape northern Germany's cold and damp. He borrowed a leaf from Pierre de Fermat when he wrote that the Riemann hypothesis "follow[s] from an expression for the function ζ(s) which I have not yet simplified enough to publish." Whether Riemann's hypothesis will require 357 years of effort to be settled, as Fermat's last theorem did, remains to be seen.

Euler's infinite product with the general exponent s is the analytic equivalent of the fundamental theorem of arithmetic, which, you recall, said that a positive integer can be divided into prime factors in one and only one way. The series on the left contains powers of all the positive integers, but the product on the right contains only powers of primes. Euler's product identity forms the basis for nearly all subsequent work on the distribution of primes.

Riemann suspected that Euler's product identity might hold the key to the proof of the prime number theorem, because the product on the right involves only primes. Riemann's main contribution was to replace the exponent s, which had heretofore always been a real number greater than 1, with a complex exponent that he also called s. Riemann used the notation $s = \sigma + ti$, where σ and t are real numbers, and i is the square root of -1. (Why Riemann mixed a Greek σ with a Roman t is unclear—he may have intended that it be a τ, but the printer set it as t, and t it has remained. And now, of course, it is enshrined in mathematical tradition.) Riemann then showed that the distribution of prime numbers is connected with properties of the function $\zeta(s)$, defined by the infinite series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} .$$

Because he did so much with the function $\zeta(s)$ it is now called the Riemann zeta function.

Riemann showed that the definition of the zeta function, originally valid only for σ greater than 1, could be extended (using integral calculus) to all complex values of s, and that the prime number theorem is intimately related to the location of the zeros of the zeta function, that is, those points in the complex plane for which $\zeta(s) = 0$. These zeros are of two categories, called trivial and nontrivial. The trivial zeros are the negative even integers, that is, the points $s = -2, -4, -6, \ldots$ along the negative real axis. The exact location of the nontrivial zeros is not known, except that they lie in an infinite strip of width 1 (called the critical strip) in which σ lies between 0 and 1. The critical strip is the region in the complex s plane that lies between the two vertical lines where $\sigma = 0$ and $\sigma = 1$, as shown above.

Riemann laid out an ingenious, highly creative plan for proving the prime number theorem. He showed that the prime number theorem would follow logically if one could prove that there were no zeros of the zeta function on the line where $\sigma = 1$. Unfortunately, despite his best efforts, Riemann could not carry out this crucial step in the plan. (He also conjectured a stronger statement—that all the nontrivial zeros were located on the critical strip's center line, now called the critical line, where $\sigma = 1/2$. This conjecture, called the Riemann hypothesis, is unproved to this day, and is considered to be the most famous unsolved problem in modern mathematics. If true, it has profound implications concerning the error made when $\pi(x)$ is approximated by $x/\log x$.)

Riemann, generally considered to be the intellectual successor of Gauss, came close to proving the

"I have discovered a truly remarkable proof, which this margin is too small to contain." Unfortunately, this truly remarkable proof—if indeed he had one—died with him, as he never wrote it down on anything wider.

prime number theorem, but did not succeed. Not enough was known during Riemann's lifetime about functions of a complex variable to carry out his ideas successfully. After his death, many mathematicians went to work to develop the tools needed to execute his plan. As a consequence of this research, French mathematician Jacques Salomon Hadamard developed in 1893 an important branch of mathematics—the theory of entire functions of finite order—to handle certain classes of previously intractable functions that had bested Riemann. (These functions have since taken on a life of their own in mathematical analysis.) In 1894, Hans Carl Friedrich von Mangoldt used Hadamard's theory to justify and simplify some of the steps in Riemann's method.

Jacques Salomon Hadamard (1865–1963) excelled in Latin and Greek as a child, but was last or nearly last in his arithmetic classes until the seventh grade, when he fell under the influence of a good mathematics teacher. Hadamard was a relative of Alfred Dreyfus (the army officer whose conviction of treason on the flimsiest of evidence began a 12-year controversy, known as the Dreyfus Affair, that rocked France to its foundations) and helped clear his name.

Charles-Jean de la Vallée Poussin (1866–1962) studied religion and engineering successively before turning to mathematics. A lifelong resident of Louvain, Belgium, the third edition of Volume 2 of his Cours d'analyse was lost when the German army overran the city.

By 1896 the necessary analytic tools were in hand. Working independently and almost simultaneously, Hadamard and Belgian Charles-Jean de la Vallée Poussin succeeded in proving the prime number theorem by following Riemann's strategy. In fact, de la Vallée Poussin published three papers on the subject that year—the first contains his proof of the prime number theorem, the second extends his method to obtain a prime number theorem for arithmetic progressions, and the third is on special types of primes.

Hadamard and de la Vallée Poussin each used a different method to prove that the zeta function has no zeros on the line $\sigma = 1$, the step upon which Riemann had foundered nearly 40 years earlier. Of the two proofs, Hadamard's is the simpler. In a two-page note at the end of his third paper, de la Vallée Poussin acknowledged this, and then showed how Hadamard's method could be simplified even further. In just a few lines de la Vallée Poussin showed that the lack of zeros on the line $\sigma = 1$ followed quite easily from an elementary trigonometric identity for the cosine of a double angle:

$$\cos 2\theta = 2\cos^2\theta - 1.$$

He then pointed out that this trigonometric identity can be used to shorten his original proof in the first paper by 24 pages, and that the same identity can be used to simplify the second and third papers as well.

These first proofs were later simplified by many other mathematicians, and new proofs discovered, all using sophisticated methods of calculus and complex analysis. Then, in 1949, Atle Selberg, at the Institute for Advanced Study in Princeton, and Paul Erdös, an itinerant Hungarian mathematician (who died on September 20 of this year, aged 83, while attending a conference in Warsaw), astounded the mathematical world by presenting a proof that makes no use of the Riemann zeta function or complex-function theory. But this so-called elementary proof is very intricate, and is more difficult to understand than the analytic proofs.

The prime number theorem is important, not only because it makes a fundamental, elegant statement about primes and has many applications within and beyond mathematics, but also because much new mathematics was created in the attempts to find a proof. This is typical in number theory. Some problems, very simple to state, are often extremely difficult to solve, and mathematicians working on these problems often create new areas of mathematics of independent interest. Another such example is Fermat's last theorem, which asserts that there are no positive integers x, y, z, and n satisfying the equation

$$x^n + y^n = z^n \text{ if } n \text{ is greater than or equal to } 3.$$

In 1637, Pierre de Fermat jotted that equation in the margin of his copy of Diophantus's *Arithmetica*, along with the note, "I have discovered a truly remarkable proof, which this margin is too small to

contain." Unfortunately, this truly remarkable proof—if indeed he had one—died with him, as he never wrote it down on anything wider. The theorem was proved only recently—in 1994!—by Andrew Wiles of Princeton University. The proof of Fermat's last theorem has received more publicity than any other result in mathematics, but Gauss himself considered Fermat's last theorem to be of only minor importance and refused to work on it.

The prime number theorem and Fermat's last theorem are two outstanding examples of problems that have attracted the intellectual curiosity of many individuals but resisted efforts at solution. Repeated failure by eminent mathematicians to settle these problems by known procedures stimulates the invention of new methods, approaches, and ideas that, in time, become part of the mainstream of mathematics, and even change the way mathematicians think about their subject. This is certainly true of the prime number theorem. Early attempts to prove it stimulated the development of the theory of functions of a complex variable—a branch of mathematics that is the lifeblood of mathematical analysis. And efforts to prove Fermat's last theorem led to the development of algebraic number theory—one of the most active areas of modern mathematical research, with ramifications far beyond the Fermat equation. One unexpected application of algebraic number theory is in designing security systems for computers.

There are hundreds of unsolved problems in number theory alone. New problems arise more rapidly than the old ones are solved, and many of the old ones have remained unsolved for centuries. Our knowledge of numbers is advanced, not only by what we already know about them, but also by realizing that there is much that we do *not* know about them. Here are a few of the great unsolved problems from the realm of prime numbers:

- Is there an even number greater than 2 that cannot be written as the sum of two primes? (Goldbach's problem.)
- Is there an even number greater than 2 that cannot be written as the difference of two primes?
- Are there infinitely many twin primes?
- Are there infinitely many primes of the form $2^p - 1$, where p is prime?
- Are there infinitely many primes of the form $2^{2^n} + 1$?
- Are there infinitely many primes of the form $x^2 + 1$, where x is an integer?
- Is there always a prime between n^2 and $(n + 1)^2$ for every positive integer n?
- Is there always a prime between n^2 and $n^2 + n$ for every integer n greater than 1?

Solve any of the above, and your name, too, shall live forever in the mathematical hall of fame! □

Professor of Mathematics, Emeritus, Tom M. Apostol earned his BS in chemical engineering from the University of Washington in 1944, and his MS in mathematics in 1946. He moved south to UC Berkeley for his PhD, which he got in 1948. The southward trend continued when he arrived at Caltech as an assistant professor in 1950, after a side trip to MIT. He became an associate professor in 1956, a full professor in 1962, and emeritus in 1992. His two-volume calculus textbook, written nearly 40 years ago and known to generations of Caltech undergrads as "Tommy 1" and "Tommy 2," is still used to teach freshman math. Apostol has kept up with the times, going electronic in the 1980s as part of the team that created The Mechanical Universe... and Beyond, *a 52-episode college-level physics telecourse. Apostol is currently creator, director, and producer of* Project MATHEMATICS!, *a series of computer-animated videotapes explaining math concepts.*