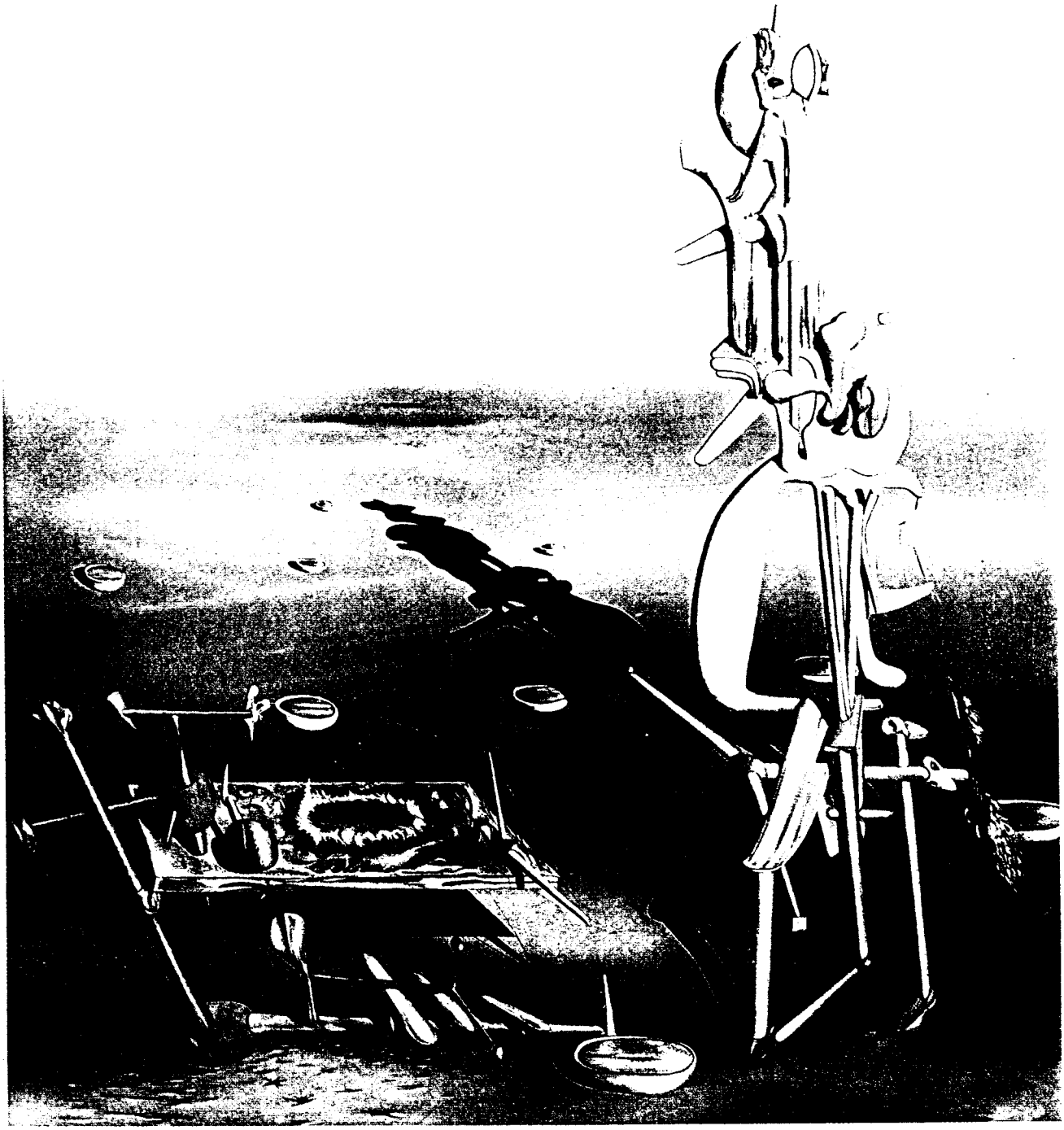
PRIME NUMBERS

PRIME TERRITORY

Exploring the Infinite Landscape at the Base of the Number System

by ENRICO BOMBIERI



Yves Tanguy, Indefinite Divisibility, *1942*

32(5)

IN HIS BOOK *The Man Who Mistook His Wife for a Hat,* the neurologist Oliver Sacks recounts a peculiar story of twin brothers, John and Michael, who had been diagnosed as autistic, psychotic and severely retarded. When Sacks met them in 1966, they were in their middle twenties and had been in various institutions since the age of seven. Although they seemed unable to make ordinary calculations, the twins had phenomenal memories for numbers and could instantly repeat a number with as many as 300 digits. On one occasion Sacks was watching as they sat in a corner, smiling and obviously very happy. They were carrying on a purely numerical conversation: John would mention a six-digit number; Michael would listen, nod, smile and then say another six-digit number, which would elicit the same response of appreciation from John. They seemed to enjoy contemplating the numbers. A bewildered Sacks went home trying to figure out what had given them such pleasure. Following a hunch, he checked and discovered that all the numbers the twins had exchanged were primes.

The next day Sacks returned and found the twins playing the same game. He joined them, and after a while ventured an eight-digit prime number, cribbed overnight from a table in a book. The twins turned toward him with an expression of intense concentration, and after a few seconds started smiling. They invited him to join in their game. After five minutes John mentioned a nine-digit prime number. So it went, as the twins continued to add digits until, incredibly, they reached a number that was twenty digits long. Sacks's prime number tables went up to only ten digits, but as far as he could determine, every number they mentioned was a prime.

It is hard for me to hear this story without feeling awe and astonishment at the workings of the brain. But I wonder: Do my nonmathematical friends have the same response? Do they have any inkling how bizarre, how prodigious and even otherworldly was the singular talent the twins so naturally enjoyed? Are they aware that mathematicians have been struggling for centuries to come up with a way to do what John and Michael did spontaneously: to generate and recognize prime numbers? Or can most people do little more than shrug and perhaps secretly imagine that a *real* mathematician would find what the twins did no more taxing or worthy of attention than performing long division in one's head?

For much of my career as a mathematician I have been fascinated by prime numbers, and my wife and my nonmathematical friends can see the excitement and enthusiasm I feel when I am on the trail of something new. But I would also like for them, and you, to share my enthusiasm—in some sense to "get" it. It turns out that investigations of prime numbers have led not only to some of the deepest, most beautiful and farthest-reaching mathematical connections of our age but also to applications in cryptography that affect banking and the national defense.

WHAT IS A PRIME NUMBER, and what makes it so special? A prime is any natural number, or integer, greater than 1, that can be divided exactly, without remainder, only by itself or by 1. Thus 5 is a prime, whereas 6 (= 2 × 3) is a composite (nonprime) number. The number 1 is considered neither prime nor composite, and it is better left apart.

The formal definition of a prime number is not terribly important here. What really matters is that primes are the building blocks of all the integers, in a sense already understood in 300 B.C., by the Greek geometer Euclid. Euclid proved a result that, loosely stated, implies the so-called fundamental theorem of arithmetic: There is only one way of expressing a number as a product of prime factors of increasing size. The number 24 is the product of 2 and 12, 3 and 8, or 6 and 4, yet the only way of factoring it into primes is $2 \times 2 \times 2 \times 3$.

Prime numbers stir curiosity. Is there a formula, a simple rule, that generates only primes—even if it does not get all of them? Is there a simple way of checking whether or not a given number is prime? And if the number is composite, can its factors be determined by means other than trial and error? Do prime numbers have hidden properties? Those questions are not unrelated, and they all lead onto the slippery slope of how to make the distinction between an interesting question and a merely antiquarian one. In other words, what properties of primes are worth serious attention, and what, in contrast, should be considered merely curios, destined to find their proper place gathering dust in a corner of the mathematical attic?

A CASE IN POINT is the history of "perfect" numbers. A perfect number is any number whose factors sum to that number. Six, for instance, is evenly divisible by 3, 2 and 1, and the sum of those factors is 6. Another perfect number is 28, whose proper parts are 14, 7, 4, 2 and 1. In ancient times perfect numbers were thought to have special and even magical significance. Euclid devised a rule for constructing them: if 2^n-1 is a prime p, then $p \times 2^n/2$ is a perfect number. For example, 2 raised to the third power minus 1 is the prime number 7; when 7 is multiplied by half of 8 (= 2^3), the answer is the perfect number 28.

So the question is: When does the formula 2^n-1 yield a prime? At the beginning of the seventeenth century only the first six exponents that generate perfect numbers were known: 2, 3, 5, 7, 13 and 19. In 1644 the French theologian and mathematician Marin Mersenne claimed to have found the next four: 31, 67, 127 and 257. Eventually it was discovered that he was mistaken and that the correct sequence is 31, 61, 89, 107, 127 and 521. Nevertheless, the primes of the form 2^n-1 are still known as Mersenne primes.

The Mersenne primes have achieved a kind of celebrity, partly because the numbers grow so fast with increasing values of n. The largest prime known today was discovered just a few months ago by David Slowinski on a Cray-2 supercomputer at the Harwell Laboratory of AEA Technology; the number is $2^{756,839}-1$, which takes forty-seven pages of dense type to write out in ordinary notation.

But in my view hunting for the largest perfect number today yields only trophies for the curio shop. Euclid showed that there are infinitely many primes; mathematicians believe the perfect numbers, too, go on forever, and so the goal of finding the largest one is doomed from the start. Still, some questions about perfect numbers remain unanswered. For example, no one has ever found an odd perfect number; if one exists, it must be truly gigantic, with many distinct prime factors. Is the nonexistence of odd perfect numbers an interesting problem? Here math-

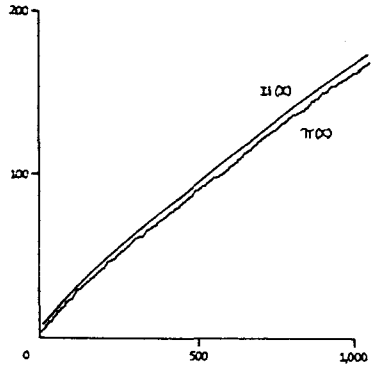
ematicians' opinions differ. A few years ago I ruffled some feathers when I stated in print that the interest for problems of this kind is "practically nil." In my opinion what would be of real interest would be to show that certain problems of that kind are truly undecidable, in the sense described in 1931 by the metamathematician Kurt Gödel: that they cannot be proved or disproved from the axioms of arithmetic.

IT IS APPARENT from a glance at a list of primes that the sequence is rather irregular, and that the list seems to thin out at a regular rate, even if it never ends:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59
61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 . . .

Plotting the number of primes as one progresses through the natural numbers gives a steplike graph with jumps, or discontinuities, of one unit at every prime number. But the function, usually written $\pi(x)$ (pi-of-x), also has a certain smoothness about its behavior. That smoothness requires explanation, and so mathematicians have tried fitting various curves such as parabolas to the graph. The function $x/\log(x)$ made a good fit, curving slowly downward much like the prime number function $\pi(x)$. (The number $\log(x)$ in the denominator is the natural logarithm of x.)

The German mathematician Carl Friedrich Gauss, who some people consider the greatest mathematician of all time, penetrated the meaning of $x/\log(x)$ to find an even better fit for $\pi(x)$. Gauss interpreted the empirical fact that $x/\log(x)$ is an approximation to $\pi(x)$ as evidence that $1/\log(x)$ is the probability that a given integer x is prime. If so, the sum of all those probabilities, at each number from 2 through x, should approximate the total number of primes from 2 to x. That sum, Gauss recognized, is close to what is known as the integral logarithm function, or $Li(x)$. It turns out that $Li(x)$ fits the prime number function $\pi(x)$ quite nicely, as the drawing at the left clearly shows.



THE PUBLICATION in 1748 of two volumes by the Swiss mathematician and physicist Leonhard Euler marked the beginning of the most fascinating development ever to come out of the theory of prime numbers. In his book *Introductio in analysin infinitorum* Euler presented for the first time a direct connection between the prime numbers and the integers, embodied in an explicit formula:

$$\frac{1}{1-2^{-n}} \times \frac{1}{1-3^{-n}} \times \frac{1}{1-5^{-n}} \times \cdots = \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \cdots$$

In the series on the left the denominators of the fractions progress through all the prime numbers, 2, 3, 5, 7 and so forth, whereas in the series on the right the denominators run through the natural numbers 1, 2, 3 and so forth. Mathematicians have studied the right side of the equation in the hope of learning more about the left side, thus gleaning clues to the distribution of prime numbers. The right side, now known as the zeta function, is easier to study simply because the distribution of the natural numbers is obvious.

One of the first by-products of Euler's equation was a better way of counting primes. Since sums are easier than products to study, mathematicians find it convenient to transform the left half of Euler's equation into a sum instead of a product. From that sum comes a new and much more manageable way of counting the number of primes less than or equal to some number x; the estimate is known as $\psi(x)$ (psi-of-x), and it counts each integer as follows: If the integer is a prime number p or the power of a prime p, it adds $\log(p)$ to the count; otherwise it adds 0. Suppose x is 10. Then to get $\psi(x)$, you begin with 2 by including its natural logarithm, log 2. You then come to 3, which contributes log 3 to the sum. Four is a power of 2, and so it adds a second log 2. Putting all of this together, you would find that

$$\psi(10) = \log 2 + \log 3 + \log 2 + \log 5 + \log 7 + \log 2 + \log 3 = 7.83 \ldots$$

The function $\psi(x)$ can be thought of as a novel way of counting primes. Instead of adding 1 every time a prime occurs, it gives a greater weight to the primes and their powers, namely the weight $\log(p)$. The beautiful outcome is that with such weights the "count" of primes becomes almost equal to the upper bound of the interval in which they are being counted. The count of primes less than or equal to, say 200, is roughly 200 and so on. The graph of the counting function $\psi(x)$ comes close to being a straight line that makes a forty-five-degree angle with the horizontal axis, especially for large numbers x.

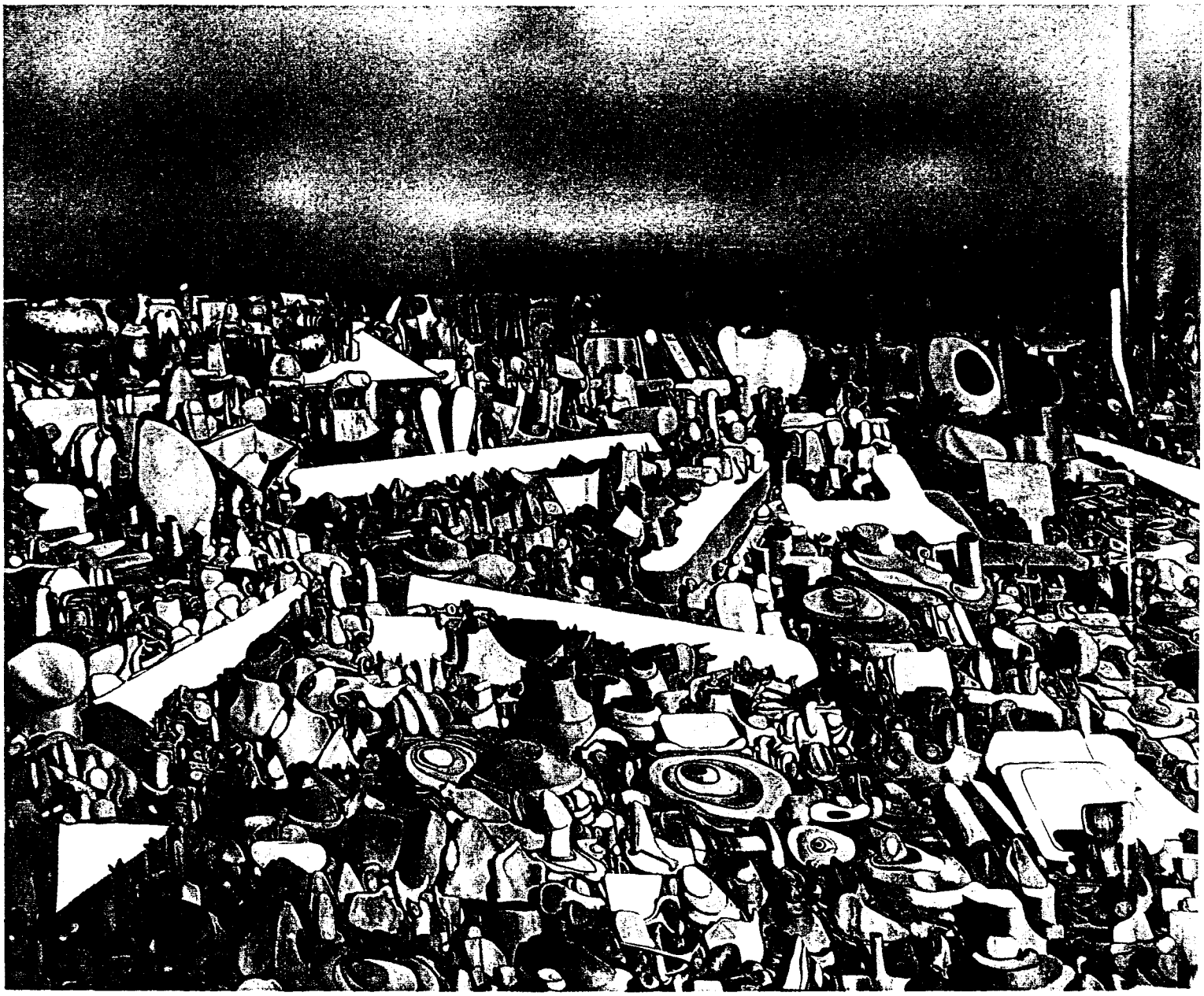
Such a result is cause for tremendous excitement among mathematicians, since it hints at an underlying rhythm in the placement of prime numbers. When I was in the eleventh grade, I studied several of the medieval philosophers. One of them, William of Occam, elevated to a method the idea that when one must choose between two explanations, one should always choose the simpler. Occam's razor, as the principle is called, cuts out the difficult and chooses the simple. When things get too complicated, it sometimes makes sense to stop and wonder: Have I asked the right question? Here the choice is between two functions that count primes: one is the function $\psi(x)$, approximated by a straight line, and the second is $\pi(x)$, approximated by the curving function $Li(x)$. Surely William of Occam would have chosen to study $\psi(x)$.

EULER'S EQUATION had made it clear that the right object to study—the relevant data for investigating prime numbers—is the function $\psi(x)$, which came from transforming the left side of the equation. But what about the zeta function on the right side? What light could it shed on the psi function? More than a hundred years were to pass before an answer to that question was forthcoming. Then, in 1859, the German mathematician Bernhard Riemann published his only paper in the theory of numbers, a truly astonishing tour de force on the distribution of primes.

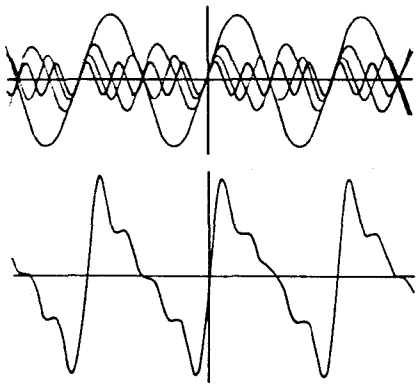
Riemann is a legendary figure in mathematics, in many minds the equal of Gauss; he shaped a century of mathematical work with ideas of tremendous depth and significance. Felix Klein, another towering figure in nineteenth-century German mathematics, was fond of saying that Riemann must have worked primarily by means of "great general ideas"—in other words, by intuition.

But another story contradicts Klein's assessment. In the late 1920s the German mathematician Carl Ludwig Siegel was studying the zeta function. After much thought he decided to send away for Riemann's unpublished notes, in the hope they would shed more light on the subject. André Weil, who is now a mathematician at the Institute for Advanced Study in Princeton, was visiting Siegel in Frankfurt at the time and accompanied him to pick up the package at the local public library. Siegel opened the package and found it full of loose sheets of paper, covered with complicated calculations in minute handwriting. Remembering Klein's comment, Siegel jokingly exclaimed: "Here are Riemann's great general thoughts!" Later, in a paper on the notes, Siegel wrote: "The legend that Riemann obtained his mathematical results by means of 'great general ideas,' without using the formal tools of analysis, is no longer so prevalent as it was in Klein's time." Today Riemann is viewed as a pragmatist who was never averse to taking the low road in order to get an important insight.

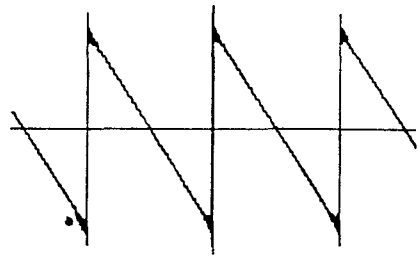
It was known by the time of Riemann's paper, through the work of the French mathematician Jean-Baptiste-Joseph Fourier, that every periodic wave can be expressed as the sum of sine waves of various frequencies and amplitudes. For example, if the heights of each of the four sine waves in the diagram at the top left of the opposite page are added at every point along the graph from left to right, the result is the wave just below them. You can think of each sine wave as a single instrument that



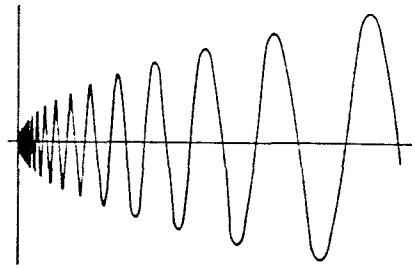
Yves Tanguy, Multiplication of the Arcs, 1954



produces a pure tone, which has a single frequency, or pitch, and a definite amplitude, or intensity. Any sound from an orchestra made up of such instruments would be the sum of all the pure tones at any given moment. Suppose, for instance, an orchestra played fifty pure tones all at once: an A in the first octave, plus an A at double the frequency of the first A but half its intensity, plus an E at three times the frequency but only one-third the intensity of the first A, and so on, with increasing frequency and decreasing intensity. Graphically, the notes would sum to resemble the shape of a sawtooth wave. The resulting sound would be most unpleasant, but the example illustrates the essence of harmonic analysis. The low-frequency, high-intensity A defines the general shape of the sawtooth sound, whereas the high-frequency, low-intensity notes define its sharp corners. Such sums only approximate the sawtooth shape, because wherever there is a sharp turn or discontinuity in a function, overshooting occurs.



Riemann discovered that prime numbers too could be studied by harmonic analysis, albeit of a slightly different kind. He realized that the psi function can be thought of as a sum of elementary waveforms; but instead of sine waves, the waveforms look like the wave at the right. Each waveform makes an infinite number of oscillations as it approaches the vertical axis from right to left toward the origin. Moving to the right, its amplitude increases according to a simple rule. The characteristics of the elementary waveforms can divulge a great deal about the psi function and, consequently, about the distribution of prime numbers. When plotted on a logarithmic scale, the waveforms are transformed into a function with a constant frequency. That frequency and the rate at which the amplitude grows are the two characteristics that define the shape of the elementary waveform.

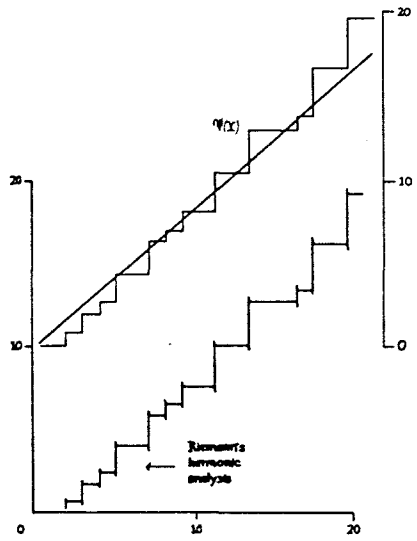


RIEMANN'S insight was that the frequencies of the basic waveforms that approximate the psi function are determined by the places where the zeta function is equal to zero. Thus one must solve the following equation for n:

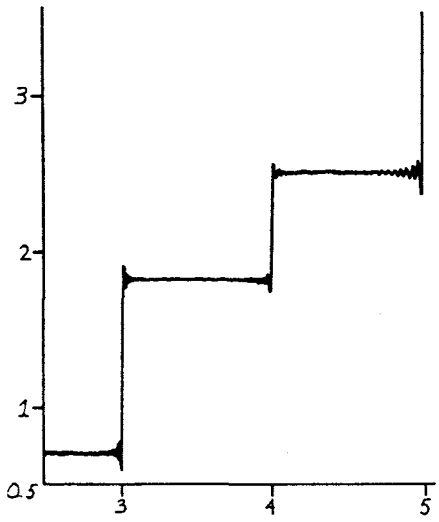
$$1 + 1/2^n + 1/3^n + 1/4^n + \ldots = 0$$

To make it possible to find values of n that will satisfy the equation, mathematicians apply certain tricks for handling infinite sums. For example, Euler multiplied the equation by the factor $1 - 2^{1-n}$, which transforms the series into one with alternating plus and minus signs. With that and other tricks, one can solve the transformed equation for n. Some of the solutions are trivial: -2, -4, -6, ... But the significant values for Riemann's analysis are not just ordinary numbers; rather they are complex numbers with two independent parts, one real and one imaginary. The complex numbers that make the Riemann zeta function equal to zero are the nontrivial zeros of the function. They occur in pairs, and there are infinitely many of them. Each one corresponds to an elementary waveform: the real part is the growth in its amplitude and the imaginary part is its frequency (logarithmically plotted).

In Riemann's analysis each complex number that acts as a zero of the zeta function gives two kinds of information about the psi function. The real part controls the large-scale behavior of the psi function—how quickly it ramps up. The imaginary part of each complex number controls the smaller-scale, oscillatory effects. Thus, the values of the imaginary parts determine precisely which of Riemann's elementary waveforms must be included in the "orchestra" to approximate the sharp steps taken by the psi function—just as high-frequency sine waves made it possible to approximate the sharp points of the sawtooth wave.



When the first 500 of Riemann's elementary waveforms are combined and the result is plotted, the curve fits almost precisely the plot of $\psi(x)$ [*see diagram at left*]. The only deviation is overshooting at the corners in the curve—the same effect one gets by trying to add sine waves to approximate the sawtooth wave. You can see the overshooting if the lower-left corner of the graph is enlarged, as it is at left. To me, that the distribution of prime numbers can be so accurately represented in a harmonic analysis is absolutely amazing and incredibly beautiful. It tells of an arcane music and a secret harmony composed by the prime numbers.



DID RIEMANN'S CELEBRATED paper solve the main problem: explaining the regularities and irregularities in the distribution of the prime numbers? The answer is no. Mathematicians still want to understand the fine distribution of the primes. Riemann's great accomplishment was transforming the problem of describing prime numbers into the problem of describing the zeros of the Riemann zeta function—which can be attacked directly.

But it is by no means trivial to solve. I am firmly convinced that the most important unsolved problem in mathematics today is the truth or falsity of a conjecture about the zeros of the zeta function, which was first made by Riemann himself. Suppose you plot the known zeros of the zeta function on a graph, the real part along the horizontal axis and the imaginary part along the vertical. In such a plot the complex zeros line up like soldiers along the vertical line that corresponds to the real value 1/2, the so-called critical line. Riemann conjectured that the real part is always equal to 1/2, for all the infinitely many zeroes.

Even a single exception to Riemann's conjecture would have enormously strange consequences for the distribution of prime numbers. The primes appear to follow a kind of random distribution, and experiments with computers for large numbers of primes bear that out. If the Riemann hypothesis turns out to be false, there will be huge oscillations in the distribution of primes. In an orchestra, that would be like one loud instrument that drowns out the others—an aesthetically distasteful situation. As a follower of William of Occam, I reject that conclusion, and so I accept the truth of the Riemann hypothesis.

AS RECENTLY AS two decades ago virtually all mathematicians would have concurred with the common perception about prime numbers: however worthy they may be of the most searching intellectual attention, they can have no utility or application in the "real" world. How that has changed! Prime numbers and the methods of factoring large composites are now at the heart of some of the most advanced methods of disguising data to prevent unauthorized access.

In the new methods security is guaranteed by two keys, one for encoding, the second for decoding. To avoid having to issue a key for each message or for every combination of sender and receiver, each user can be assigned a public encoding key; indeed, such keys might even be published in a kind of telephone book, next to the names of the users of the system. Each public key tells all potential senders of messages to, say, Jones how to encode messages for Jones. But the knowledge of the encoding key does not help at all in the decoding. To decode his messages Jones has a second key, known only to himself.

Among the most popular public-key systems are the ones based on large prime numbers. Two large primes of, say, a hundred digits each can be multiplied together with relative ease on a computer. Encoding a message to Jones is a matter of carrying out such a multiplication with the help of Jones's public key. Even with the help of the computer, however, reversing the multiplication, or in other words factoring a composite number whose factors are hundred-digit primes, has proved virtually impossible. That formidable difficulty is what protects Jones against eavesdroppers. The second, private key held only by Jones makes it possible for him alone to decode his messages without having to factor the large composite number.

BECAUSE the cryptographic technique requires large prime numbers, the ability to generate and recognize prime numbers is of great importance. Perhaps, then, it is a pity the peculiar talent of the twins of Oliver Sacks's story was never harnessed. Ten years after Sacks's encounter with them, the twins were separated; they were placed in halfway houses and taught to do menial jobs. Alas, the price of "normality" was that they forever lost their amazing numerical abilities. ●

ENRICO BOMBIERI is a professor of mathematics at the Institute for Advanced Study in Princeton.