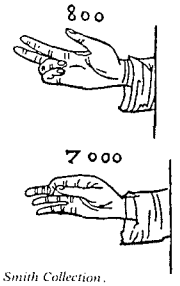
Mathematics:

MONSTERS AND MANIFOLDS

Izaak Walton once likened mathematics to fishing: Both are solitary pursuits that "can never be fully learnt." Yet mathematics has a loathsome reputation. It frightens many people and may bore the rest. In its highest reaches, it seems to defy common sense. There are 17,000 mathematicians in the United States today, almost all of them employed by universities or by flourishing "high-tech" corporations. Their ranks include brilliant theorists, yeoman problem-solvers, colorful eccentrics, classroom drones. The discipline has progressed by leaps and bounds since 1900; the past decade has been especially fruitful. But few Americans understand the achievements of modern mathematics or its contributions to the workings of an industrial society. The federal government is more appreciative; Washington plans to create two national mathematical "institutes," one at the University of Minnesota, the other at the University of California, Berkeley. Here, mathematician Rick Norwood explains some of the advances of recent years—and describes the unsolved problems that his colleagues seek to answer.



Smith Collection, Rare Books and Manuscripts Library, Columbia University.

by Rick Norwood

All mathematics is divided into three parts. Roughly, these parts are the study of number systems, called *algebra*; the study of geometrical spaces, called *topology*; and the study of functions, called *analysis*. There are also a few islands—number theory and set theory, for example — and two vast continents that have broken off from the mainland and are drifting out to sea: computer science and statistics.

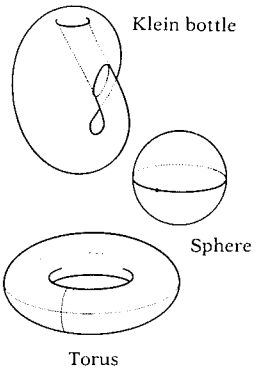
Most mathematicians identify with one or more of

these disciplines, and it is almost impossible to keep up with any but the most important results outside one's own area, a song of woe heard in other lands than mathematics.

The total amount of mathematics written in this century probably exceeds the total of all previous centuries taken together. In 1980, more than 64,000 pages of new mathematics were published. Not everyone in the field today (perhaps not anyone) is a Newton or a Gauss, but much of the mathematics now being done meets extremely high standards of originality and excellence. Much has been discovered that is startling and beautiful.

Most people think of mathematics as a dry, cobwebbed science, written by Euclid on tablets of stone and passed down through the ages from teacher to student until all are bent under the load—as the domain of hoary eccentrics at one extreme, and of fearsome schoolmasters at the other. It has long been the butt of jokes. "I have hardly ever met a mathematician capable of reasoning," Plato once said. To see mathematics exhibit grace and elegance, then, is as surprising as the sight, in *Shōgun,* of the warrior Toranaga dancing on the battlements. Nevertheless, it dances.

Topology is my own field. To me, the fascination of multidimensional geometric shapes is unending. One can easily visualize only the simplest of these things — the curious Klein bottle, for instance; the sphere; the doughnut-shaped torus. The rest one can never really "see"; they can be manipulated only in one's head. Or one can try (as I have tried) to convey their properties by employing seven colors of chalk while simultaneously using bodily gestures to simulate motion. I'll save topology for last. First, a brief word about computer science and statistics.



From Graduate Texts in Mathematics *by John Stillwell.*
© 1980 by Springer-Verlag, New York.

Statistics is the science that nearly got saccharin banned in 1977 on the basis of a study of 630 cancer patients by the National Cancer Institute of Canada. It is also the science used in the 1979 U.S. National Cancer Institute study of more than 3,000 patients that won saccharin a reprieve. When properly applied (e.g., by a life insurance company), statistics is as "true" and as useful as any other mathematics.

Computer science, meanwhile, has moved into our living rooms and seems there to stay. Already, computers build Toyotas and play games with us. Tomorrow, they may do housework. The day after tomorrow, they may tell us that they don't do windows.

Computers have revolutionized commerce, communications, government; they are an indispensable tool in engineering and in all of the physical sciences.

While mathematics gave birth to computer science and statistics (in the case of the former, electrical engineering was the father), both have largely packed up and moved out, perhaps because of mathematicians' schoolmarmish insistence on right answers.

Évariste Galois
(1811–32)

Courtesy of Bordas-Gauthier-Villars, Paris.

The problems with statistics are obvious. Given the real-world constraints of time, money, or a client's needs, there is a tendency to cut corners. Much of the statistical data published these days is quite misleading. Computer scientists, for their part, are primarily interested in programs that will be *reasonably* reliable. But no program is perfect, and a good mathematician can usually come up with some "input" that will overload a computer's memory. I can sometimes befuddle my own pocket calculator by asking it to perform certain chores that could quite easily be worked out with pencil and paper.

Does it sound as if I take a dim view of mathematics' glamorous offspring? I don't, really. I am impressed by the power of modern statistics and staggered by the advances in computers. If anything, I am a little envious. I wish simply to note a difference. Applied mathematics asks, "How can we accomplish such-and-such in a practical and efficient way?" Pure mathematics asks, "What is? What different kinds of mathematical objects can exist?"

Take "group theory."

Algebra, as I have mentioned, is a study of number systems. The algebra one learns in high school is an important example, but it bears the same relation to what a mathematician means by algebra as the study of lions bears to zoology. Mathematicians classify number systems according to their properties, just as zoologists classify animals. A warm-blooded animal that suckles its young is a mammal. A set with one operation that is *associative* and has *identity* and *inverses* is a *group*. (An example of an operation would be addition or multiplication.) The associative law is $(a+b)+c = a+(b+c)$. In other words, when adding

Rick Norwood, 39, is visiting assistant professor of mathematics at Lehigh University and recently completed a year at the Institute for Advanced Study in Princeton, N.J. He holds a B.A. (1966) and a Ph.D. (1979) from the University of Southwest Louisiana.

three or more numbers, you can drop the parentheses without being ambiguous. The law of identity is that $0 + a = a + 0 = a$. The law of inverses is that $a + (-a) = (-a) + a = 0$.

The whole numbers form a group, but so do matrices, polynomials, and functions. Quite a lot of things can play the role of numbers in abstract algebra, just as, in a court of law, the Interior Department, the Sierra Club, and Exxon may all be considered, legally, to be "individuals." If you find this troublesome, refer to Whitehead (below).

> "Now, it cannot be too clearly understood that, in science, technical terms are names arbitrarily assigned, like Christian names to children. There can be no question of the names being right or wrong. They may be judicious or injudicious. . . . The essential principle involved was quite clearly enunciated in Wonderland to Alice by Humpty Dumpty, when he told her, apropos of his use of words, 'I pay them extra and make them mean what I like.'"
>
> —Alfred North Whitehead,
> *An Introduction to Mathematics (1911)*

Groups occur in all branches of mathematics, and in theoretical physics as well, notably in the study of crystals and quarks. Many important mathematical problems come down to a question about the groups involved. For example, in the theory of "knots" (a branch of topology), we know that for every knot there is a group. If we can show that the group in question is the group of whole numbers, then we know that the "knot" can be pulled and stretched into a circle; that the "knot" was really untied to begin with.

For 150 years, since the days of Augustin-Louis Cauchy and Évariste Galois, mathematicians have been trying to answer these questions: "What different types of groups can there be? What are they like? How can we tell one from another?" This is called the classification problem.[1]

Let us concentrate on the finite groups, groups with a finite number of elements. The smallest finite group consists only of the number 0 and the operation +. It is a group with only one number; in math terminology, a group of order one. Once you know that $0 + 0 = 0$, you know everything you need to know about this group.

The next smallest group has order two. One way

[1]The term "group theory" itself can be traced back to a letter written in 1832 by Galois. The letter was composed on the eve of the duel in which the 20-year-old Galois was killed. For more information about Cauchy, Galois, and other prominent figures, see Eric Temple Bell's classic *Men of Mathematics* (Simon & Schuster, 1937).

to describe it is by using the numbers T (for True) and F (for False). When we "add" two numbers, we are asking for the truth value of the statement, "These numbers are the same." So $T + T = T$, $F + F = T$, but $T + F = F$ and so does $F + T$. The identity in this case is T, because T added to any number gives that number as an answer. Each number is also its own inverse, because a number added to itself gives the identity T. Another way of looking at the group of order two is by substituting "even" for T and "odd" for F. You might think this was a second group of order two, but mathematicians do not look at it that way. To a mathematician, the group of T and F is "isomorphic" to the group of even and odd, because the addition rules are the same for both groups. So we say that there is only one group of order two.[2]

There is also only one group of order three (i.e., with three elements), but there are two different groups of order four, and from then on there are often many groups of a given order.

By a technique known as the composition series, finite groups — groups with a finite number of elements—can always be broken up into smaller groups called simple groups, somewhat as a whole number like 15 can be broken into its prime factors, 3 and 5. Thus, mathematicians have been chiefly concerned with classifying the finite simple groups. And in 1980, the process of classification was completed.

The easiest examples of finite simple groups are the cyclic groups of prime order (e.g., a group of order three, since 3 is a prime, divisible only by itself and 1), and the so-called alternating groups of order 60 or more. These are groups one would study in an undergraduate course in abstract algebra. There are infinitely many of them, but they are completely classified and well understood.

Next, if you pursued abstract algebra at the graduate level, you would encounter finite simple groups of the *Lie* type, named for Norwegian mathematician Marius Sophus Lie (pronounced Lee). These are not easy to understand. Even so, finite simple groups of the Lie type are also completely classified.

Finite simple groups that are not of prime order, or alternating, or Lie, are called *sporadic*. They are the sports, the strange ones. They were the last type of finite simple group to be classified. We now know that there are exactly 26 of them.

Some of them have pet names like Monster and Baby Monster; these two, in fact, were the last to be

[2]Thus far, I have called the group operation "addition" and written it "+," and I will continue to do so, but I could just as well have called it "multiplication" or anything else. What's in a name? The rows, by any other name, would add as sweet.

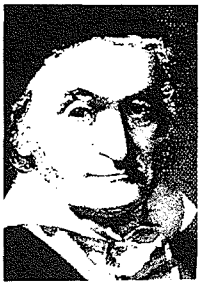
discovered. The order of Monster is 808,017,424,794, 512,875,886,459,904,961,710,757,005,754,368,000,000, 000. In other words, it has that many elements. Its discovery by Bernd Fischer of the University of Bielefeld in West Germany was one of the most important achievements in pure math in recent years.

Why have I led you over such murky terrain? To repeat: Groups are building blocks, like the elements of the periodic table. Some elements—hydrogen, say —are rather basic; we know pretty well what they can be used for, and we use them all the time. Other elements—lawrencium, for example, with its half-life of eight seconds—remain exotic. There is really no "use" for lawrencium. I expect it will likewise be a while before Monster gets much of a workout. But one never knows, for groups underlie many things: particle physics, chemistry, and, as Martin Gardner has pointed out, the theory behind any magic trick involving ropes and twisted handkerchiefs.

It would be a mistake to conclude that mathematicians necessarily care whether a new discovery has some practical application. Mathematicians do what they do because it is beautiful, interesting, challenging. What flares the nostrils is the prospect of a chase. A problem beckons: "Come, Watson. The game is afoot." Still, there are always surprises. Attempts by practical men to separate the pure from the applied are artificial concessions to the finiteness of human thought and time.

Number theory, for example, has always been considered the purest of pure math. It is the study of whole numbers, prime numbers in particular. Yet one of the most practical applications of mathematics in recent years came out of number theory: public key cryptography. The first method of public key cryptography was discovered by Whitfield Diffie and Martin Hellman of Stanford in 1976, but the system I am about to describe is the work of Ronald Rivest, Adi Shamir, and Leonard Adleman, all of MIT.

To understand public key cryptography, you must understand the word *modulo*, a concept introduced by Karl Friedrich Gauss in 1801 in his classic *Disquisitiones arithmeticae*. The integers modulo five (to give an example) are obtained by setting 5 equal to 0, so that you count 1,2,3,4,0, 1,2,3,4,0, and so on. Anything that is cyclic can be measured in modulo numbers. We tell time modulo 12. Numerous card tricks can be worked modulo 13. Because both the Earth and the moon follow a cyclic pattern, one can use modulo



Karl Friedrich Gauss (1777–1855)

From Carl Friedrich Gauss, 1777/1977 *by Karl Reich. © 1977 by Heinz Moos Verlag, Munich.*

arithmetic to determine the date on which Easter will fall in any year (the method below will work for any year between 1900 and 2099).

1. Call the year *Y*. Subtract 1900 from *Y* and call the difference *N*.
2. Divide *N* by 19. Call the remainder *A*.
3. Divide (7*A* + 1) by 19. Ignore the remainder and call the quotient *B*.
4. Divide (11*A* + 4 − *B*) by 29. Call the remainder *M*.
5. Divide *N* by 4. Ignore the remainder and call the quotient *Q*.
6. Divide (*N* + *Q* + 31 − *M*) by 7. Call the remainder *W*.
7. The date of Easter is 25 − *M* − *W*. If the result is positive, the month is April. If it is negative, the month is March (interpreting 0 as March 31, −1 as March 30, −2 as March 29 and so on to −9 for March 22.

From "Mathematical Games" by Martin Gardner.

Let us go back to modulo five. You can add and multiply modulo five (or any other number) provided you go back to zero every time you reach five. The easiest way to cast out fives is to divide by 5 and take the remainder. Thus, 4 + 3 = 2 (the remainder when you divide 7 by 5) and 4 × 4 = 1 (the remainder when you divide 16 by 5). This arithmetic may seem strange, but it obeys many of the laws of ordinary arithmetic.[3]

What does this have to do with cryptography? Well, you can see how easy it is, given a number, to find out what it equals modulo five. But what about going the other way? If I tell you what my number equals modulo five, you have no way of guessing what my original number is. I tell you my number is 3 modulo five. What is it? It might be 8. It might be 63. It might even be 3. A kind of one-way trap door has been set in place. This is the basis of public key cryptography, a tamper-free system whose applications range from ensuring the privacy of electronic mail to running a network of agents behind the Iron Curtain.

In practice, public key cryptography works modulo some very large number (one of 200 digits, say) that is the product of two very large prime numbers. To put a message into code, you first transform the message into a number (any schoolboy method for accomplishing this will do) and then raise that number to a power that anyone can know, modulo some very large number that is also open to anyone. Thus, *anybody* can encipher a message. But, once a number has been reduced modulo some other number, there is no way of getting the original number back.

Now the cyclic nature of modulo numbers comes

[3]Indeed, the integers modulo five with the operation of addition is an example of a cyclic group of prime order, which we encountered above. This is one of the nice things about mathematics. Even as things get "curiouser and curiouser," one finds old friends in unexpected places.

into play. There is another number, a secret number. When you raise the enciphered message to this secret power, it comes around to the original message.

Let's do an actual example. (So that we don't need a computer, I will use unrealistically small numbers.) The first step is to pick any two prime numbers. We pick 3 and 11. Multiply these numbers to get 33. We will work modulo 33. Subtract one from each prime to get 2 and 10. Multiply 2 times 10 to get 20. We calculate our public number and our secret number modulo 20 (since the standard abbreviation for modulo is *mod*, we say "mod 20"). First, list all the numbers that divide 20. Your list should read: 1, 2, 4, 5, 10, 20. For your public number, pick any number between 1 and 20 that is not divisible by any number on this list (except 1, of course). We pick 7. For your secret number, use your computer to find a number that, when multiplied by 7 and reduced mod 20, gives 1. The mathematics of modulo arithmetic guarantees that there will always be such a number, and in this case it is not hard to find. The number 3 will do the job, because $7 \times 3 = 21$ and 21 mod 20 equals 1. So, our secret number is 3, and we are ready to go.

A "cipher disc" invented by Giovanni Battista Porta (1535–1615).

David Kahn Collection.

Send your operatives in the field the public number, 7, and tell them all to work mod 33. Keep the number 3 so secret that not even you know it. The way to do this is to have your computer calculate it, with instructions to tell no one; but instruct it to raise any number entered to this secret power and then reduce mod 33.

Now, your operative is ready to send you a message. Because we are working with such small numbers, it must be a very short message. Suppose he decides to send the letter *B*. The easiest way to change letters to numbers is to let $A = 1, B = 2, C = 3$, and so on. So, he changes *B* to 2, raises it to the seventh power (7 is the public number, remember) and reduces mod 33. Two to the seventh power is 128. To reduce 128 mod 33 you divide 128 by 33 and take the remainder, which is 29. Your operative then sends you the number 29.

Back at the home office, you get the number. You feed 29 into your computer, which raises it to the secret power, 3, and reduces mod 33. That is, multiply 29 times 29 times 29, then divide by 33 and take the remainder. Do it and see what you get.[4]

With small numbers such as these, it is really very easy to find the secret number. Just factor 33 into 3×11, then find the secret number the same way we

[4]You should get 2, which yields the original message: *B*.

found it to begin with. The key to the success of this cipher lies in the fact that it is hard to factor *large* numbers. Mathematicians have been trying to find ways to do so for more than 100 years. It would take the fastest computer now in existence about 76 years to factor a 200-digit number.

Most mathematicians believe that the problem of factoring very large numbers will not be solved in the near future, but the U.S. National Security Agency (NSA) is taking no chances. The NSA has asked American mathematicians working in the area of cryptography to submit all new results to government experts in Washington prior to publication. Some mathematicians find this reasonable. Others feel it is an unwarranted intrusion into their lives and work. For arguments pro and con, see *Notices of the American Mathematical Society* (Oct. 1981). The debate may be academic. The NSA is powerless to prevent mathematicians in other countries from conducting research in cryptography and publishing their results in, say, the *Saskatchewan Journal of Number Theory*.

Let's turn now to analysis.

Analysis is the study of functions. A function is any rule that assigns a fixed output to any given input. The squaring function is a familiar example. Input 3, output 9. Input 5, output 25. Other well-known functions are the sine function and the exponential function. Calculus, discovered independently in the 17th century by both Isaac Newton and Gottfried Wilhelm Leibniz, is the greatest achievement of analysis.

Bernhard Riemann
(1826–66)

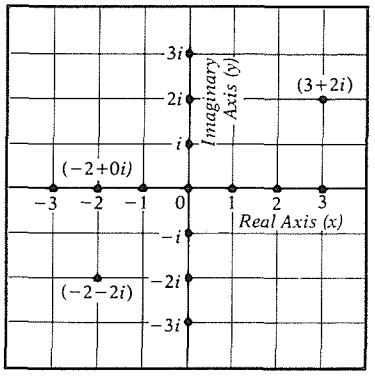
Courtesy of Archiv für Kunst und Geschichte, Berlin.

To understand the most significant recent result in analysis, we need to look at the Riemann zeta function, named for the German mathematician Bernhard Riemann. The Riemann zeta function has applications in algebra and algebraic geometry as well as analysis. It is used to estimate the number of primes in a given range (say, between 10 and 10 million), which is important in the theory of public key cryptography.

We begin with the number i, the elusive square root of -1. It was called imaginary (in "real life," you can't square anything and get a negative number), and its existence was denied until it proved too useful to ignore. Leibniz once called imaginary numbers "a wonderful flight of God's Spirit; they are almost an amphibian between being and not being." If we utilize these amphibians as in the graph on the facing page, then any number in the field—say, $3 + 2i$, or $-2 - 2i$, or even $-2 + 0i$—is known as a *complex number*. In trigonometry, we learn how to do arithmetic with

complex numbers.

The input of the Riemann zeta function is a complex number. So is the output. How is the Riemann function defined? To define a function, we need to know what to do with the input. The squaring function turns 3 (for example) into 9. The reciprocal function turns 3 into ⅓, 4 into ¼. If these simple functions are like light bulbs (input: electricity; output: light), then the Riemann zeta function is a whole factory (input: raw materials; output: finished product).



The Riemann zeta function inputs a complex number, z, then takes the series $1 + 2 + 3 + 4 + 5 + \ldots$ ("..." means: go on forever), takes its reciprocal term-by-term to get $1 + ½ + ⅓ + \ldots$, and then raises the whole thing, again term-by-term, to the z power. The sum of this infinite series is the output of the Riemann zeta function, and for any z which begins with a number greater than 1 (e.g., $3 + 2i$), the series converges.[5] This means that it adds up to a finite number. (The series $1 + ½ + ¼ + ⅛ + 1/16 \ldots$ also converges: It adds up to 2. While some people may wonder how one can actually add up an infinite number of terms—Will we ever *really* reach 2?—Isaac Newton discovered a method: calculus.)

Now, whenever you have a function, a natural question to ask is, "Where is the output zero?" This is what most of high school algebra was about. Where are the zeroes of $x^2 + 2x - 3$? Answer: $x = -3$, or $x = 1$. Where are the zeroes of the Riemann zeta function? To date, 3.5 million zeroes have been found by computer, not counting the zeroes (considered trivial) that lie along the horizontal axis. So far, all of the 3.5 million

[5]For z's that begin with a number less than or equal to 1, we must extend the zeta function by a process known as analytic continuation. Once this is done, then for every complex number except $1 + 0i$, the Riemann zeta function converges.

non-trivial zeroes lie on a vertical line through the point ½ + 0*i*. The question is: Do *all* of the zeroes in fact lie on this line? Riemann hypothesized that they did, but so far no one has been able to prove it.

When mathematicians cannot answer a question, they try to find a different question, one they *can* answer. If the Riemann hypothesis is too tough to crack, perhaps the problem can be solved for some important series other than 1 + ½ + ⅓. . . . It turns out that it can. The French mathematician Pierre Deligne has proved the Riemann hypothesis for a particular zeta function studied by André Weil of the Institute for Advanced Study at Princeton. And it has been proved, ironically, for a *harder* form than Riemann's original.[6]

[6]Deligne's solution has important applications. It allows us, for example, to achieve the best possible estimate of the number of whole-number solutions modulo *p* (*p* being any prime number) to a family of equations. Such "estimators" are invaluable in physics and engineering.

This is common in mathematics. Consider the Four-Color theorem, which asserts that no more than four colors are needed to color any map (such as the one below left) so that no two regions that touch are the same color. The conjecture was proved for maps drawn on all of the hard surfaces (e.g., the torus, the projective plane) long before it was proved in the "easy" case: maps on a flat surface. The breakthrough came in 1977 with the help of a computer (the computer just did the calculations), and the proof is too long for a human being to read.

The Zip Code districts of Mobile, Alabama

The Four-Color problem, along with the proofs of the Smith conjecture (a recent result in the unusual theory of knots) and the Complements conjecture, are some of the latest achievements in the field of topology. Here is another one, brand new, not even published yet.

To understand it, the first thing you must know is what is meant by the term *manifold*. The Euclidean spaces (e.g., the line, the plane, three-dimensional space) are all examples of manifolds, as are such non-Euclidean spaces as the torus and sphere. The Euclidean spaces can be given Cartesian coordinates, as on a graph, but these spaces do not stop with dimension three. Four coordinates represent a point in four dimensions, five coordinates a point in five-dimensional Euclidean space, and so on.

When we talk about a dimension, we simply mean a *direction* at right angles to each of our previous directions. One dimension is length, two dimensions length and breadth, three dimensions length, breadth, and height. Typically, mathematicians understand spaces of five or more dimensions better than they understand dimensions three and four. (The fourth dimension is not time, by the way, although Einstein-

ian space-time is an example of a space that has four dimensions.)

A one-dimensional manifold is a curve. A two-dimensional manifold is a surface. We might call a three-dimensional manifold a three-space, and a four-dimensional manifold a hyper-space. It is often easier to picture a manifold by putting it in a Euclidean space of higher dimension. A sphere, for example, is simply a surface: a two-manifold. But try to picture a sphere without picturing it in three-dimensional space. Mathematically, that three-dimensional space is unnecessary, but conceptually it is essential.[7]

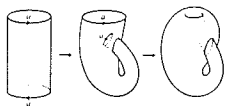
The question then arises: What is the smallest dimensional Euclidean space in which you can put a given manifold? In 1944, Hassler Whitney came up with a preliminary answer. He proved that any n-dimensional manifold (n-manifold, for short) can be put at least into $2n-1$ dimensional Euclidean space. So, we can always put a three-manifold into five-space. One- and two-manifolds are well understood, but there is a profusion of three-manifolds, and they are extremely hard to get a grip on. Seeing how they fit into Euclidean space is a big help.

When we put one space into another, we do not want to tear it or crease it. For example, we can flatten a sphere, but not without a sharp crease at the edge, so we cannot put a sphere into a plane. There are two legitimate ways of putting one space into another: *immersion* and *embedding*. An immersion allows the space to intersect itself, an embedding does not. A figure eight is an immersion of a circle in the plane: It intersects itself. The letter *O* is an embedding of a circle in the plane. To the right is a picture of a Klein bottle; it is an immersion because we construct it by passing the neck of the bottle through the bottle's side.

The new theorem, proved by Ralph Cohen of Stanford, and conveyed to me by Don Davis of Lehigh, shows that any n-manifold can be immersed in Euclidean space whose dimension is $2n$ minus the number of 1's in a binary expansion of n. The binary system is a way of expressing any number in terms of 1's and 0's, and the transformation of an ordinary number into binary form is easily accomplished (see box on next page). Thus, any five-manifold can be immersed in Euclidean eight-space because five in binary form has two ones in it.

A topological question that remains unsolved is the dimension of the smallest Euclidean space in

[7]There are three-dimensional spheres, four-dimensional spheres, and so on, but they are difficult to picture. If you had two balls and were able to glue their skins together so that one sphere was turned inside out over the other, then you would have a three-dimensional sphere.



From Graduate Texts in Mathematics *by John Stillwell.*

To change an ordinary number into a binary number, divide the number by 2 and write down the remainder. Keep dividing by two and writing the remainder. When your quotient is 0, stop. The remainders, written in reverse order, form the binary expansion. The binary expansion of 41 is achieved by:

$$\begin{array}{ccccccccccc} 20 & & 10 & & 5 & & 2 & & 1 & & 0 \\ 2\overline{)41} & \rightarrow & 2\overline{)20} & \rightarrow & 2\overline{)10} & \rightarrow & 2\overline{)5} & \rightarrow & 2\overline{)2} & \rightarrow & 2\overline{)1} \\ \underline{40} & & \underline{20} & & \underline{10} & & \underline{4} & & \underline{2} & & \underline{0} \\ 1 & & 0 & & 0 & & 1 & & 0 & & 1 \end{array}$$

Thus, 41 in binary form is 101001.

which every n-manifold can be *embedded.* The conjecture is that every n-manifold can be embedded in Euclidean space of dimension $2n$, minus the number of 1's in the binary expansion of n, plus 1. But this is just a conjecture.

During the past decade, many famous problems have fallen, but many more—like the embedding conjecture above—remain unsolved. One of the most obdurate conundrums of mathematics is the problem known as Fermat's last theorem, which involves solutions to the equation $x^n + y^n = z^n$, where x, y, z, and n are whole numbers. One easy solution is $3^2 + 4^2 = 5^2$, a familiar configuration to anyone who remembers the Pythagorean theorem. Indeed, solutions are a dime a dozen if $n = 1$ or $n = 2$. Fermat's last theorem states that the equation has no solutions that are whole numbers if n is 3 or larger. The trouble is proving it.

Pierre de Fermat
(1601–65)

Pierre de Fermat was a French jurist who lived in Toulouse and corresponded about mathematics—his hobby—with Descartes, Pascal, Leibniz, and Newton. He originated the conjecture that bears his name and in 1637 wrote in the margin of a book: "I have discovered a truly remarkable proof which this margin is too small to contain." However, he never wrote down the proof, even though he lived for 28 more years. Perhaps, he did not have a proof after all. After another 300 years, the theorem still has not been proved.

Some dents, of course, have been made. The Swiss Leonhard Euler proved it for $n = 3$ in 1770, Adrien-Marie Legendre of France proved it for $n = 5$ in 1823, and the German number theorist Ernst Edward Kummer proved it for almost all prime numbers in 1847. Modern computers have since proved it for any

n between 3 and 30,000. But such computer searches give no insight into a general solution to the problem. We may never know whether Fermat's last theorem is correct, but the efforts to prove or disprove it over the centuries have led to much useful and ingenious mathematics—a reward in itself.

The most important unsolved problem in mathematics may be the Poincaré conjecture, posed by the brilliant French astronomer-mathematician Jules-Henri Poincaré. To understand it, one must return to the topological spaces called manifolds.[8]

A manifold is termed "simply connected" if any loop of thread on its surface can be pulled in — by someone holding both ends of the loop firmly—while at the same time remaining in continuous contact with the manifold. A sphere is simply connected; try it with a piece of thread and a rubber ball. A torus is not simply connected. A loop of thread around it will lose contact with the surface as it is pulled in and passes over the hole; if the thread goes through the hole to begin with, one cannot pull it in at all. The Poincaré conjecture states that the only simply connected three-manifold is the three-dimensional sphere.

A version of the Poincaré conjecture has been proved for dimensions five and above (i.e., the only simply connected five-manifold is the five-dimensional sphere). The four-dimensional case has just been proved by Michael Freedman of the University of California, San Diego. (Another important new result.) The three-dimensional case remains unsolved.

But there are distant rumblings. Mathematician talks to mathematician. While nothing has yet appeared in print, the word is, to everyone's surprise, that the Poincaré conjecture may be false.

So it goes, new mathematics from old, curving back, folding and unfolding, old ideas in new guises, new theorems illuminating old problems. Doing mathematics is like wandering through a new countryside. We see a beautiful valley below us, but the way down is too steep, and so we take another path, which leads us far afield, until, by a sudden and unexpected turning, we find ourselves walking in the valley, admiring the trees and flowers.

Jules-Henri Poincaré (1854–1912)

From Major Prophets of Today *by Edwin E. Slossen. © 1914 by Little, Brown, and Company.*

[8]What follows concerns manifolds that are "finite" in a special technical sense of the word that we do not need to go into. A mathemetician would call them "closed, connected" manifolds.