Century-Old Math Problem Solved

An incredibly indirect proof resolves an old problem and links two seemingly unrelated areas of mathematics

An outstanding problem in number theory that has challenged mathematicians for more than a century has now been solved. The problem involves families of number systems, and what is surprising and significant about the proof is that it uses elliptic curves, an entirely different type of mathematical object. In the end, the solution to this problem may be a major step toward linking the analysis of elliptic curves and number theory of these curves.

The proof was recently announced by Don Zagier of the University of Maryland and the Max Planck Institute in Bonn and Benedict Gross of Brown University. The two mathematicians have published a brief note announcing their result but are still in the process of writing their 300-page manuscript describing the details of their proof. Mathematicians have complained that such long proofs can be nearly impossible to check because they frequently require that the reader somehow assimilate enormous amounts of information and verify complicated logical connections. But, despite the unwieldy size of their proof, Gross believes that it is understandable and, he says, he has "absolutely no doubt" that it is correct. "It is more explicit than most mathematical proofs and less prone to error," he remarks. Other mathematicians agree. "I believe it," says Dorian Goldfeld of the University of Texas at Austin, who is visiting this semester at Harvard University.

Zagier and Gross worked for several years to get this result, but they felt after they got started that success was inevitable. "Results in arithmetic are so tight that it can be very hard to make progress," says Gross. "But once you are on the right track, you know it will work." Gross says he and Zagier are "delighted" that they proved the theorem.

The theorem that Gross and Zagier proved dates back to Karl Fredrich Gauss, the 19-century mathematician who was one of the giants in the field of number theory. Gauss began by generalizing the notion of a whole number. His idea was to look at numbers of the form $a + b\sqrt{-1}$, where a and b are integers. Those numbers, which are called Gaussian integers, form a grid in the complex plane and when two Gaussian integers are added together you get a third. You also can multiply Gaussian integers and get as a product another Gaussian integer. But, an essential question was, Are the usual laws of number theory valid in the Gaussian integers? For example, in the ordinary integers there is the notion of a prime, meaning a number that is divisible only by itself and 1, and the unique factorization theorem which states that any number can be expressed uniquely as a product of primes. The number 10, for example, can be expressed as a product of 2 times 5. The answer to the number theory question—and Gauss himself proved it—is that there are "primes" and a unique factorization theorem in the Gaussian integers.

One reason this sort of work in systems like the Gaussian integers is significant, says Barry Mazur of Harvard University, is that many difficult questions about ordinary integers are easier to solve if they are first rephrased in terms of Gaussian integers. For example, it is easy to find which prime numbers can be expressed as a sum of two squares if you first translate the problem into one involving the Gaussian integers.

> "It is more explicit than most mathematical proofs and less prone to error."

Gauss also generalized the idea of Gaussian integers by looking at the system of all numbers of the form $a + b\sqrt{-d}$, where a and b are fixed integers and d can vary through all the integers. (The only slight complication to this rule, mathematicians have discovered, occurs when d has a remainder of 3 when divided by 4. Then the number systems are impoverished and must be slightly enlarged by allowing a and b to be half integers as well as whole numbers.) When d is 1, you are back to the Gaussian integers. But when d is not 1, you have other number systems. Can you do number theory comfortably in any one of these? Is there, for example, a unique factorization theorem?

A major problem, then, became one of deciding for which values of d a unique factorization theorem holds. It was known in Gauss's time that it holds for d equal to 1, 2, 3, 7, 11, 19, 43, 67, and 163. But no one knew if there were other values of d that worked. By the 1920's mathematicians made some progress on the problem. They knew that there was no more than one case in addition to the nine already discovered and that this additional d, if it existed, must be astronomically large.

About 15 years ago, Harold Stark of the Massachusetts Institute of Technology and Alan Baker of Trinity College in Cambridge, England, working independently and with entirely different methods, proved that there is no tenth d. Then they decided to look back in the literature to see what else had been done with this problem. They found a paper, written in the 1950's, by Kurt Heegner, a retired Swiss scientist who did math as a hobby. In this paper, Heegner purported to prove that there can only be nine d's for which unique factorization holds, but the consensus in the mathematical community was that Heegner was wrong. "It's a hard paper to read," says Stark. "It's written in the most horrible style that you can think of." Nonetheless, when Stark and Baker went back and examined Heegner's paper, they decided that his proof was correct and that it was an absolutely wonderful proof.

The next question was, if you don't have prime factorization in one of these number systems, how close to prime factorization can you get? Here, once again, Gauss had a theory. He proposed something called the class number that can be associated with any of the number systems derived from the d's. "The class number," says Mazur, "is a measure of by how wide a margin the unique factorization theorem fails." If the class number is 1, then there is unique factorization. If it is 2, then the system just misses having unique factorization. Class numbers can go all the way up to but not include infinity, and the larger they are, the more ways there are to factor numbers in the system into primes.

With the nine d's, mathematicians had a complete list of all the class 1 number fields. In addition, Baker and Stark were able to list all the fields with class number 2. But what about the rest? Mathematicians were stumped by this problem which had first been posed by Gauss: For any number k, find the largest d whose number system has class number k.

About 6 years ago, Goldfeld thought

he nearly had the answer. "I was working on the class number problem for 4 or 5 years," he says, "and I thought I was almost there." What Goldfeld found was that he could provide the class number list to anyone who could provide him with a particular mathematical object—an elliptic curve with certain properties.

It sounded easy. Everyone, including Goldfeld, thought they would polish off the problem in short order. "It seemed very simple, but we soon realized it was way beyond our knowledge," says Gross. The mathematical object they were looking for has to do with the theory of elliptic curves, which are expressed by cubic equations of the form $x^3 + y^3 = z^3$.

Mathematicians associate a function, called an L-function, to elliptic curves and these L-functions are conjectured to tell how many rational points the curves have. Mathematicians look for what is known as the order of vanishing of these L-functions at a specific point in the complex plane to determine how many rational points are on the elliptic curves. Goldfeld proposed that if anyone can find an elliptic curve whose L-function has an order of vanishing that is greater than or equal to 3, he can solve the class number problem.

For 6 years, mathematicians worked on the problem. "Not only did it sound easy, but, if our conjectures were right, we thought we knew some elliptic curves that had that order of vanishing," says Mazur. "We thought we had gone from an easier theory, the order of vanishing, to a harder one, the class number problem. But the theory of vanishing turned out to be much harder than anyone expected."

What Gross and Zagier finally did was to link the arithmetic of elliptic curves to the theory of vanishing. They found that special points on elliptic curves have the property that if they are nonzero, the order of vanishing is precisely 1. If they are 0, the order of vanishing is greater than 1. They also know whether the order of vanishing is even or odd. Thus they can find curves with orders of vanishing greater than or equal to 3 by finding curves that have odd orders of vanishing and whose special points have zero values. Gross and Zagier call these special points H, in honor of Heegner who used them in his long-neglected proof that there are only nine d's.

The proof itself, says Gross, consists of a horrendous equation. "To calculate both sides of the equation takes 100 pages. Then you have to pair up terms on each side of the equation and prove the two sides of the equation are the same. It's a mess." The proof, then is by no means elegant. "I still have hope that it will be tremendously simplified," says Stark.

But what truly impresses mathematicians is the idea behind the proof. "The proof is surprisingly indirect. What they are doing is using an elliptic curve to somehow govern the structure of this infinite family of number systems," says Mazur. "The full gamut of these number systems is governed by a single mathematical object." Mathematicians might naïvely think there is no connection between an elliptic curve and these families of number systems. But the recent proof shows instead, Mazur remarks, that "here there is every connection." Gross agrees, adding, "that connection is really quite extraordinary."—**GINA KOLATA**

A Step Toward Artificial Chromosomes

In their continuing efforts to relate the behavior of chromosomes during cell division to their structure investigators have turned to the construction of artificial chromosomes. For example, in the 15 September issue of *Nature*, Andrew Murray and Jack Szostak of the Dana-Farber Cancer Institute of Harvard Medical School report that they have made artificial chromosomes that behave in yeast much like the natural ones do, although not perfectly so.

Over the past few years, investigators from several laboratories have made considerable progress in isolating and characterizing sequences from the yeast genome that appear to be needed for chromosome activities. These functional elements include, in addition to the genes themselves, the centromeres, to which the fibers that pull the chromosomes apart during mitosis and meiosis are attached; the autonomously replicating sequences, which may be the origins for chromosome replication; and the telomeres, the chromosome ends that are needed to complete chromosome replication.

Murray and Szostak wanted to know whether these elements are sufficient for chromosome function. "If these are the only elements required for chromosome function it should be possible to assemble them artificially and show that the products act like a real chromosome," Murray explains.

In their first efforts, the Harvard workers constructed artificial chromosomes that were only 10,000 to 15,000 base pairs (bp) in length. For comparison, the smallest yeast chromosome is about 150,000 bp in length. When the short synthetic chromosomes were transferred into yeast cells, they did not behave like the natural chromosomes, Murray says. There were too many copies per cell, and they were lost very quickly when the cells divided.

In a paper that was published earlier this summer,* Ginger Martin Dani and Virginia Zakian of the Hutchinson Cancer Research Center in Seattle, reported similar findings for small linear chromosomes that they had constructed.

Larger artificial chromosomes work better. Murray and Szostak went on to test constructs containing about 50,000 bp. "These show some of the properties of normal chromosomes," Murray says. "They were more stably inherited, passed through meiosis, and were present in only a few copies per cell. But they are still quite a long way from behaving like real chromosomes." In particular, although they are inherited in a more stable fashion than the smaller artificial chromosomes, they are still lost about two orders of magnitude faster than natural chromosomes.

The problems may be caused by incorrect spacing between the different functional elements or because even the longer artificial chromosomes are not long enough. Alternatively, all the structural elements needed for normal chromosome function may not yet have been identified. Nevertheless, when investigators can make synthetic chromosomes that behave generally as the natural ones do, they have come a long way toward understanding how chromosomes work.—**JEAN L. MARX**

*G. M. Dani and V. A. Zakian, *Proc. Natl. Acad. Sci. U.S.A.* **80**, 3406 (1983).