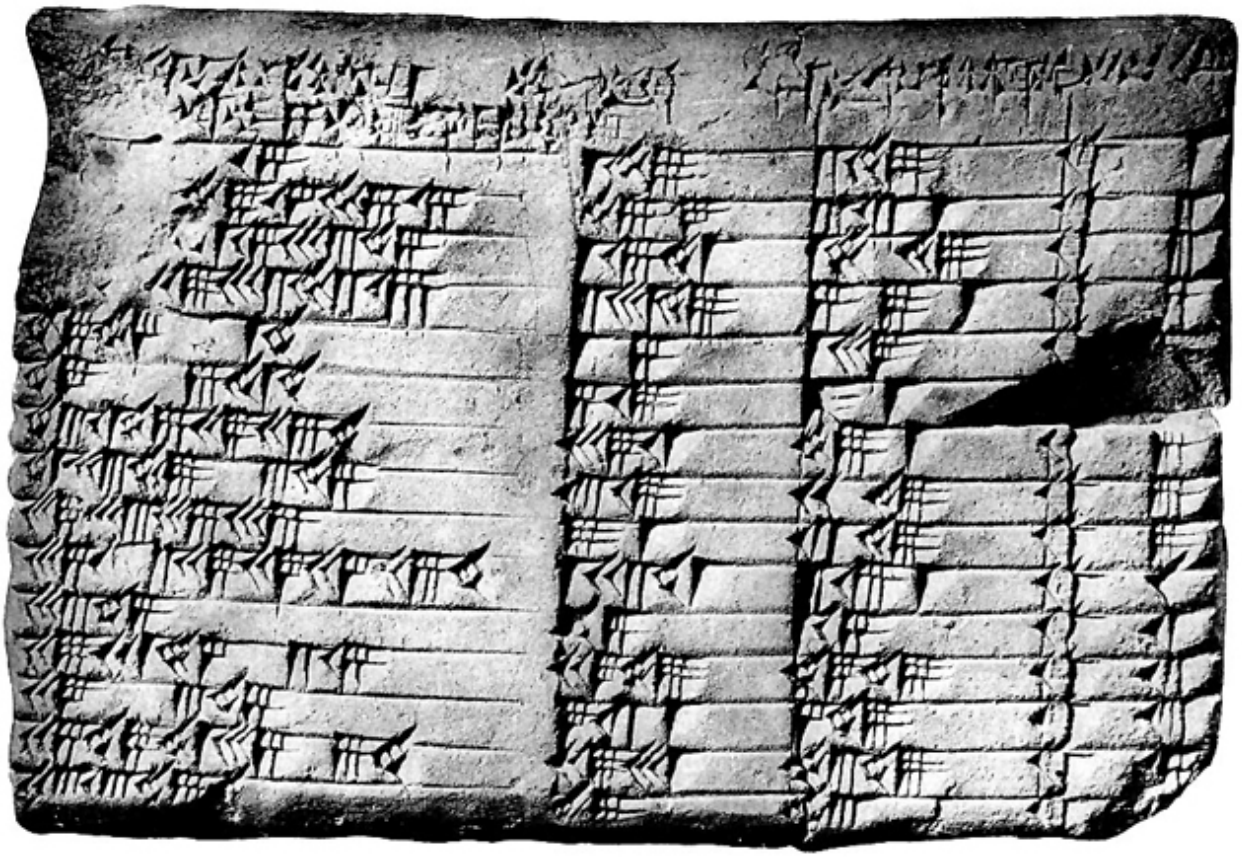
Mathematicians Shed Light on Minimalist Conjecture



This Babylonian clay tablet, believed to be from 1,800 B.C., lists Pythagorean triples – whole numbers a, b and c that satisfy the polynomial equation $a^2 + b^2 = c^2$. To this day, finding rational and whole number solutions to polynomial equations continues to challenge mathematicians.

By Erica Klarreich

In the fifth century B.C., a Greek mathematician made a discovery that shattered the foundations of mathematics and, according to legend, cost him his life. The mathematician, who some historians believe was Hippasus of Metapontum, belonged to the Pythagorean school of mathematics, which took as a central tenet that every physical phenomenon could be expressed in terms of whole numbers and their ratios (what we now call rational numbers). This presumption, however, fell apart, many historians believe, when Hippasus considered the lengths of the sides of a right triangle, which he knew must satisfy the "Pythagorean theorem" — the famous $a^2 + b^2 = c^2$ relationship. If the two legs of a right triangle each have the same rational length, Hippasus is said to have shown, its hypotenuse cannot have a rational length.

According to one version of the story, Hippasus made this discovery at sea, and his appalled fellow Pythagoreans threw him overboard.

Modern mathematicians have overcome the Greeks' discomfiture with irrational numbers (and have

discovered, in fact, that there are far more irrational numbers than rational ones). But the Pythagorean love affair with rational solutions to equations continues to inform mathematics. It lies at the heart of number theory, a traditionally pure branch of mathematics that, in our integer-centric digital era, has suddenly found many applications.

Now two young mathematicians are illuminating a frontier in the study of rational solutions to polynomial equations: the cubics (equations involving variables with a highest exponent of 3). Polynomial equations, which involve variables raised to powers, such as $y = 3x^3 + 4$, or $x^2 + y^2 = 1$, are among the most fundamental objects mathematicians study, underlying a host of different applications and branches of mathematics.

Polynomial Universe

It's easy to see that a polynomial equation whose highest exponent is 1, such as $y = 3x + 4$, has an infinite collection of rational solutions: Any rational value for x produces a rational value for y, and vice versa.

Rational solutions to polynomials whose highest exponent is 2, such as $x^2 + y^2 = 1$ or $y = 3x^2 + 2x - 7$, have been understood for millennia and have either no solutions or infinitely many. The graphs of such curves are the conic sections — circles, parabolas, ellipses and hyperbolas. Given one rational point P on such a graph, there is an elegant way to find all the other rational points: Simply take each line that passes through P with a rational slope, and calculate the line's second intersection point with the conic section.

In 1983, Gerd Faltings, now a director of the Max Planck Institute for Mathematics in Bonn, dealt with the polynomial equations with exponents higher than 3; most of them can have only finitely many rational solutions, he showed. That leaves cubics, the stubborn holdouts of the polynomial universe.

Millennia ago, mathematicians explicated the rational solutions to polynomials whose highest exponent is less than 3. And 30 years ago, Gerd Faltings, now of the Max Planck Institute for Mathematics in Bonn, showed that most polynomial equations whose highest exponent is greater than 3 can have at most a finite sprinkling of solutions.

But cubic equations have defied mathematicians' attempts to classify their solutions, though not for lack of trying. Attempting to classify the rational solutions to cubics — more specifically, to a family of cubics called elliptic curves which are, with a few exceptions, the only cubics that can have any rational solutions — has occupied all the great number theorists of the modern age, starting with the 17th-century French mathematician Pierre de Fermat, said Benedict Gross of Harvard University.

Elliptic curves can have zero, finitely many or infinitely many solutions. Mathematicians have only been able to guess how often these different possibilities arise.

Elliptic curves have an uncanny tendency to pop up in unexpected places, in both pure and applied mathematics. Understanding them was a key element in the 1995 proof of Fermat's Last Theorem, even though elliptic curves seem to have nothing to do with the statement of the theorem. Operations using elliptic curves have become a core component of many of the cryptographic protocols that encode credit card numbers in online transactions. And rational solutions to elliptic curves are at the heart of certain geometry problems in the Pythagorean style, such as figuring out which right triangles have both rational side lengths and rational area.

"Intellectual stimulation, beautiful structure, applications — elliptic curves have it all," said Manjul Bhargava of Princeton University.

Bhargava, 38, and Arul Shankar, 26, of the Institute for Advanced Study in Princeton, have now taken one of the biggest steps forward in decades toward understanding rational solutions to elliptic curves.

Their work offers no recipe for figuring out the rational solutions to a particular elliptic curve; instead, it gives insight into what the most likely scenarios are for the number of rational solutions, if you pick an elliptic curve at random. Their work is awaiting publication in Annals of Mathematics, one of the discipline's leading publications.

Bhargava and Shankar's findings are "starting to illuminate a large area of our ignorance," Gross said. "The whole field looks different after their work."

A Wild Ride

Elliptic Security

Given two rational points on an elliptic curve, the line through them will almost always intersect the curve at one additional point, which will again have rational coordinates. It's easy to use two rational points to generate a third, but it's hard to do the reverse — to take one rational point and find two rational points that would generate it via the straight-line method. This is what makes elliptic curves so useful for cryptography: Operations that are easy to do but hard to undo are fundamental to cryptographic security.

"Elliptic curves have been at the heart of many exciting things," said Peter Sarnak, of Princeton University. "They are complicated enough to carry a lot of juicy information, but simple enough to be able to study in depth."

Finding rational solutions to an elliptic curve boils down to finding the points on its graph in the xy-plane whose x– and y-coordinates are both rational numbers — often no easy matter. Once you've found some rational points, however, it becomes possible to generate more using a few simple connect-the-dots procedures first explored nearly two millennia ago, historians believe, by the Alexandrian mathematician Diophantus. For example, if you draw a line through two rational points, it usually intersects the curve at exactly one more point, which is again a rational point.

This connect-the-dots process is "a very rich structure, something special about cubics that makes them very deep," Bhargava said.

In 1922, Louis Mordell proved something remarkable: For any given elliptic curve, even one with infinitely many rational points, it's possible to generate all the rational points by starting with just a finite handful of them and then connecting the dots again and again. When the number of rational points of an elliptic curve is infinite, the number of points in the smallest handful that can generate essentially all the rational points is called the curve's rank. (When the number of rational points is finite, mathematicians say that the curve has rank 0.)

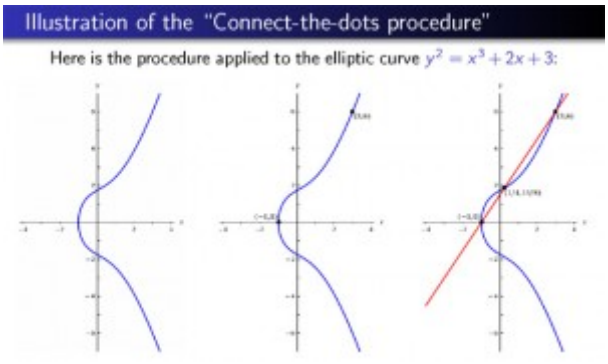


Illustration by Manjul Bhargava

Given two rational points on the graph of an elliptic curve (in this case, the curve corresponding to the polynomial equation $y^2 = x^3 + 2x + 3$), the line through those two points will usually intersect the curve at one more point, which is guaranteed to again be a rational point. This process, along with a couple of similar connect-the-dots procedures, creates the means to generate all of an elliptic curve's rational points starting from a finite handful.

For decades, mathematicians have tossed around the so-called minimalist conjecture, a proposition about the rank of elliptic curves for which the evidence is decidedly mixed. The conjecture speculates that, statistically speaking, half of all elliptic curves have rank 0 (meaning that they have either finitely many rational points or none at all) and half have rank 1 (meaning that their infinite set of rational points can be generated essentially from just one point). According to the conjecture, all other possibilities are vanishingly rare. That doesn't mean that exceptions never occur, or even that there are finitely many of them — just that as you look at bigger and bigger collections of elliptic curves, the ones that fall into other categories are a smaller and smaller percentage of the whole, approaching 0 percent.

This proposition, initially formulated in 1979 by Dorian Goldfeld of Columbia University for a particular class of elliptic curves, "has been a folklore conjecture forever," said Barry Mazur of Harvard University.

Support for the minimalist conjecture comes in part from the widely held belief that it's hard for elliptic curves to have many rational points. After all, rational numbers are a decided minority on the number line.

"Rational points of elliptic curves are accidental gems of mathematics, and it is hard to imagine that there could be bulk occurrence of these precious accidents," wrote Mazur and three co-authors in 2007 in the Bulletin of the American Mathematical Society.

At first glance, this would suggest that most elliptic curves should have rank 0. But many mathematicians also believe in something called the parity conjecture, which proposes that there's a 50-50 split between even- and odd-rank elliptic curves. Combine the parity conjecture with the idea that rational points are rare, and you end up with the minimalist conjecture — a 50-50 split between the two lowest possible ranks, 0 and 1.

The minimalist conjecture has been bolstered by experimental evidence that suggests that it is

indeed hard for elliptic curves to have high rank. Mathematicians versed in the art of elliptic-curve construction have used computers to contrive examples with fairly high rank — the current record-setter has at least rank 28 — but such curves are rare and tend to have enormous coefficients.

Other computational evidence has been far less encouraging. Mathematicians have calculated the ranks of hundreds of thousands of elliptic curves, and so far, around 20 percent of the computed examples have rank 2; a smaller but nontrivial percent have rank 3. According to the minimalist conjecture, these percentages should come out to 0, when all elliptic curves are taken into account.

“The data seem to be at war with the conjecture,” Mazur said.

Normally, when data fail to bear out a hypothesis, the proper course is to discard the hypothesis. But many mathematicians have clung to the minimalist conjecture. Although computers have churned out many examples, mathematicians point out that these calculations are only the tip of the iceberg.

“It may very well be that until we actually prove our conjectures, no data that we can accumulate, however massive it may appear, will give even lukewarm comfort to the conjecturers,” wrote Mazur and his co-authors in the Bulletin.

The substantial proportion of computed elliptic curves with rank higher than 1 is somewhat analogous to dark matter in physics, they added. “This large mass of rational points … is palpably there. We aren’t in the dark about that,” they wrote. “We are merely in the dark about how to give a satisfactory account of it being there.”

Because of this conflict between data and theory, they write, over the decades the minimalist conjecture “has had a wild ride in terms of its being believed, and doubted.”

New Methods

Until a few years ago, one of the doubters was Manjul Bhargava, a rising star in the mathematical world. Named one of Popular Science magazine’s “Brilliant 10” in 2002, the following year Bhargava became one of the youngest people ever to become a full professor at Princeton University, at age 28. His colleagues enthuse not just about his mathematical attainments but also about his kindly nature and deep creativity.

Manjul Bhargava

Manjul Bhargava, 38, Princeton University.

“Manjul is a highly original guy,” Gross said. “He looks at things in ways most people don’t — that’s

his genius."

Bhargava, a number theorist, was intrigued by the stark contrast between the computed data and the minimalist conjecture. "It tells you that there is something interesting going on," he said.

"I went to my colleague, Peter Sarnak, and asked him, 'How can you believe this conjecture?'" Bhargava recalled. "The conjecture looked ridiculous to me."

But Sarnak maintained that the data were eventually going to turn around, when elliptic curves with larger coefficients could be calculated in substantial numbers. "He had high confidence in the conjecture," Bhargava said.

Bhargava became determined to figure out something definitive, one way or the other, as to whether the minimalist conjecture is true. "It seemed like time to actually prove something," he said.

He started examining a collection of algorithms for calculating the rank of an elliptic curve that trace their origin to a procedure introduced by Fermat in the 17th century. Called the "descent" algorithms, this family of algorithms — there's one for each whole number from 2 onward — seems adept at finding the generators of an elliptic curve's rational points. But despite many efforts, no one has been able to prove that these algorithms always work.

Bhargava decided to try a different tack. "The idea I had was to try to do the descent procedure on all elliptic curves simultaneously and then prove that it's going to work most of the time," Bhargava said. After all, to tackle the minimalist conjecture, it's not necessary to know what every single elliptic curve looks like, just what they tend to look like.

The descent-algorithms problem involved a topic called the geometry of numbers, which studies how to count the lattice points inside different shapes (a lattice point is a point with whole-number coordinates). For a simple shape such as a circle or rectangle, the number of lattice points tallies closely with the shape's volume. But the problem Bhargava needed to solve involved more complex shapes, and when a shape has complicated features, such as tentacles, it may encompass many more or fewer lattice points than its volume predicts.

Ashley Gardner

Arul Shankar, 26, Institute for Advanced Study.

Before tackling such shapes, Bhargava tested the waters by assigning an easier but related problem to Arul Shankar, his doctoral student at the time. Graduate students often wrestle with their dissertation problems for years, but Shankar came back with a solution to his in just three months. So, Bhargava said, "I asked him if he'd like to join me on this."

Bhargava and Shankar developed a collection of new techniques whose importance is likely to extend far beyond the original problem the pair was trying to solve, Mazur said. "The geometry of numbers has always been a very deep, powerful method, and now they have made it vastly more powerful." He added that the brilliance of their techniques "opens up a new wedge into number theory."

These new techniques "are going to influence number theory for years and years," agreed Gross.

A Clear Pattern

If the minimalist conjecture is true, the average rank of all elliptic curves should be ½, but before Bhargava and Shankar's work, mathematicians had not even been able to prove that the average is finite.

Using the 2-descent algorithm, Bhargava and Shankar were able to show that the average rank of all elliptic curves is at most 1.5. By using 3-descent, 4-descent and 5-descent to handle some of the curves that 2-descent didn't elucidate, they were later able to bring this bound down to about 0.88.

While there's still a gulf between this bound and the minimalist conjecture's average, Bhargava and Shankar's definitive finding represents a quantum leap forward.

"It's just the first step, but it's a massive first step," Sarnak said. "It's nice to see two such young people hit a home run."

What's more, by showing that the average rank is less than 1, Bhargava and Shankar have proved that a sizable chunk of elliptic curves — at least 12 percent — must have rank 0 (since otherwise the average would have to be higher). The pair used this fact to show that the same proportion of curves satisfies a famous hypothesis called the Birch and Swinnerton-Dyer conjecture, a long-standing question about elliptic curves with a million-dollar bounty, courtesy of the Clay Mathematics Institute in Providence, Rhode Island.

At a lecture Bhargava presented at the Clay institute, one audience member inquired jokingly whether Bhargava and Shankar are now entitled to 12 percent of the million-dollar prize. "The Clay institute people were there, and they answered right away that no, it doesn't mean that," Bhargava said ruefully.

Bhargava and Shankar's findings have galvanized number theorists, many of whom were not expecting progress on the average rank any time soon. "If you had asked me one month before Manjul told me about his work," Gross said, "I would have said it's hopeless."

Now the minimalist conjecture is starting to look more and more promising, he said. "I'd put money on it."

One potential path forward — which may require another influx of new ideas, several mathematicians said — is to try to use the descent algorithms higher than 5 to get better and better bounds on the average rank.

"A clear pattern has emerged with 2-, 3-, 4- and 5-descent, and it seems likely that it continues,"

Bhargava said.

Far from feeling proprietary about his new approach, Bhargava hopes that his work with Shankar will serve as a spark that will inspire young mathematicians to work on understanding rational points on elliptic curves.

“The minimalist conjecture isn’t the end in itself,” he said. “Every time you open a door, it seems as if there are more doors to open. The more people get involved, the more doors we can open.”

Editor’s Note: Manjul Bhargava receives funding from the Simons Foundation as a Simons Investigator. Barry Mazur is a member of the foundation’s Scientific Advisory Board.