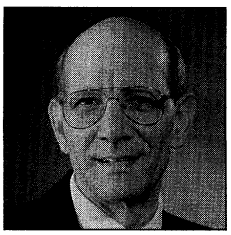
Three Fermat Trails to Elliptic Curves

Ezra Brown



Ezra (Bud) Brown (brown@math.vt.edu) professes mathematics at Virginia Tech, where he has been since 1969. The elliptic curve bug first bit him while he was in graduate school at Louisiana State, and has never really gone away. Although his main research has been in quadratic forms and algebraic number theory, he once wrote a paper with a sociologist. He loves to talk about mathematics and its history with anyone, especially students. He occasionally sings in operas, plays jazz piano just for fun, and bakes biscuits for his classes. He and his mathematical grandfather, L. E. Dickson, have the same birthday.

1 Mysterious Curves and Distinguished Visitors

You may have wondered, as I once did, what lies beyond quadratic equations within mathematics. In geometry, we meet the Pythagorean Theorem; in algebra, the quadratic formula; in analytic geometry, the conic sections—ellipses, parabolas, and hyperbolas; and eventually, in multivariable calculus, the quadric surfaces—ellipsoids, hyperboloids, paraboloids, hyperbolic paraboloids. All of these involve quadratic equations in one or more variables.

Beyond quadratics... what? In the first semester of calculus, we find extreme values of cubics and polynomials of higher degree, but no special names are attached to those curves. A course in number theory will include mention of Fermat's Last Theorem, and if you're lucky, you might learn about Tartaglia, Fior, Cardano, and Ferrari, the sixteenth-century Italians who figured out the third- and fourth-degree analogs of the quadratic formula. But what then?

One day in graduate school, I found out "what then" in a book lying open on a desk in the coffee room. I picked it up and saw the two graphs in Figure 1.

I was struck by their interesting shapes and began to read. These were, I learned, the graphs of the equations $y^2 = x^3 - 7x + 6$ and $y^2 = x^3 - 2x + 4$, respectively. Both their pictures and their names intrigued me. For these were, I learned, two

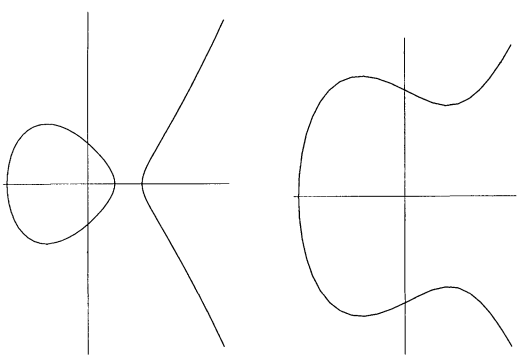


Figure 1

examples of elliptic curves—curves that were graphs of cubic equations of the form $y^2 = ax^3 + bx^2 + cx + d$, in which the right-hand side has three distinct complex roots. I wondered about their names... they certainly didn't look like ellipses.

My next encounter with elliptic curves was in 1968. Picture the scene: a visiting speaker was talking with some graduate students after his lecture, and the topic of doctoral dissertations arose. The speaker reeled off a list of fields that were not currently fashionable in mathematics and, in his opinion, that graduate students should avoid as dissertation topics. At one point, he mentioned elliptic curves—and I pounced.

"What are elliptic curves? Anything like ellipses?"

The speaker became thoughtful. "Oh, they're part of algebraic geometry... not too much in vogue these days... mostly studied at really high-powered institutions, especially in Japan and Britain... questions are hard... not much future in studying them... better do something within your grasp. Oh, the name? Something to do with elliptic integrals—that's where the name comes from. Still interested? Tell me your background in complex analysis, algebraic geometry and analytic number theory. Oh... in that case, you'd better stick to your quadratic forms, young man."

So I did. But I was curious enough to read up on elliptic integrals. Here's what I found:

- Elliptic integrals are definite integrals of several different types, including ones of the form

$$w = w(v) = \int_0^v \frac{1}{\sqrt{(1-u^2)(1-k^2u^2)}}\,du. \tag{1}$$

- Such great mathematicians as Euler and Legendre (eighteenth century) and Abel and Jacobi (1820s and 1830s) made major studies of elliptic integrals. Just why these integrals were important, the source did not say.
- Abel transformed the study of elliptic integrals into the study of their inverse functions—that is, the functions you get from the integral in (1) by viewing v as a function of w—that he called elliptic functions. Just why he did this, the source did not say.
- An elliptic function, according to one source, is a function f of a complex variable z that is doubly periodic—that is, there exist complex numbers α and β such that for all complex z, $f(z) = f(z+\alpha) = f(z+\beta)$ and such that the ratio α/β is not a real number. Just what they had to do with ellipses, curves, or elliptic integrals, the source did not say.

Not terribly enlightening, I thought, and not much of a source, either. Not only that, but the source was totally silent regarding the mysterious elliptic curves. Oh, well... I tucked the subject of elliptic curves quietly away and "stuck to my quadratic forms." But I wondered....

2 Reviews and Rejections

One day in the mid 1980s, after discovering that a particular reference located in a certain reviewing journal was not quite what I needed, I hid my disappointment by idly leafing through the volume, hoping to turn up something of interest. Did I ever!

What "turned up" was a review of an article **[16]** about an old problem in elementary number theory called Euler's Congruent Numbers problem. Briefly, Euler asked for a characterization of congruent numbers, those rational numbers

that are the areas of right triangles with rational sides. For example, 6 is a congruent number, since 6 is the area of the 3-4-5 right triangle. What caught my eye was a statement by the reviewer that the author, Jerrold Tunnell, had recast the entire congruent numbers problem into a problem involving *elliptic curves*—and then proceeded, essentially, to solve it.

Elliptic curves, again.

Maybe I should look at this paper... but the next day I got an inspiration for a problem I was working on, and once again elliptic curves slid quietly back into their customary comfortable corner... waiting.

They did not have long to wait. Several years later, a thick package from a journal proved to contain a rejection of a paper I had submitted some months earlier. The referee said that the problem I was studying could easily be solved, because "... a simple change of variables transforms any question about solutions of the equations at hand into a problem about *elliptic curves* [my emphasis]..."—at which point I dropped the letter on the floor.

Not only had elliptic curves resurfaced, but they had jumped out of the water and swatted me in the face. Now I was truly curious about these creatures, and this curiosity heightened over the next few years. For these innocent-looking cubic polynomials have turned up in a powerful method, due to Lenstra, for factoring large integers **[9]**, in the Goldwasser-Kilian Primality Test **[4]**, in public key cryptography **[8]**, **[10]**, in Tunnell's resolution of the congruent numbers problem **[16]**, and finally, in Gerhard Frey's transformation of Fermat's Last Theorem into a problem about elliptic curves **[3]**, ultimately solved in spectacular fashion (with an assist from Richard Taylor **[15]**) by Andrew Wiles **[17]**. In a word, elliptic curves are the latest silver bullets in the world of mathematics.

I'd like to take you on a brief tour of the world of elliptic curves, so that you can learn what they are, where they came from and how they got their name. Then, we'll look at three problems that illustrate their attraction. These three have an added attraction: they're all associated with Fermat.

Oh, yes: about that rejected paper—tell you later.

3 The Arc Length of an Ellipse

The story of how elliptic curves got their name begins with the work of G. C. Fagnano (1682–1766) who showed that computing the arc length of an ellipse leads to the integals mentioned in the previous section. (The story of elliptic curves begins, as do many mathematical stories, with the ancient Greeks and Alexandrians —but we'll get to that later.)

An ellipse centered at the origin and having the ends of its major and minor axes at $(\pm a, 0)$ and $(0, \pm b)$, respectively, is the graph of the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Fagngno knew that to get a very nice parametrization of this ellipse, just set $x = x(t) = a\cos t$ and $y = y(t) = b\sin t$; as t varies from 0 to 2π, the point $(x(t), y(t))$ traces out the entire ellipse.

For a curve parametrized by functions $x(t)$ and $y(t)$ for t between t_0 and t_1, the arc length of the curve is given by the integral

$$L = \int_{t_0}^{t_1} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}\, dt.$$

Because of symmetry, we obtain the arc length of the entire ellipse by calculating the arc length in the first quadrant and multiplying by 4. You can check that this means t varies from 0 to $\pi/2$. Hence,

$$L = 4\int_0^{\pi/2} \sqrt{a^2 \cos^2 t + b^2 \sin^2 t}\, dt = 4b\int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 t}\, dt,$$

where k is some constant involving a and b.

Now set $\sin t = u$, and so

$$\cos t = \frac{1}{\sqrt{1-u^2}}, \qquad \text{and} \qquad du = \cos t\, dt.$$

Thus,

$$L = 4b\int_0^1 \frac{\sqrt{1-k^2u^2}}{\sqrt{1-u^2}}\, du = 4b\int_0^1 \frac{1-k^2u^2}{\sqrt{(1-u^2)(1-k^2u^2)}}\, du.$$

In order to find the arc length of the ellipse, we must evaluate

$$I(u) = \int \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}},$$

which is known as an elliptic integral.

If the change of variables

$$v^2 = g(u) = (1-u^2)(1-k^2u^2) = 1 - (1+k^2)u^2 + k^2u^4 \tag{2}$$

would allow us to evaluate the integral, we'd do it. Now that's a quartic polynomial, and elliptic curves are of the form $y^2 = f(x)$, where f is a cubic polynomial—and elliptic curves are supposed to have something to do with elliptic integrals. Notice that since $k \neq \pm 1$, g has the four distinct roots ± 1 and $\pm k$. This allows us to transform $v^2 = g(u)$ to $y^2 = f(x)$, where f is a cubic polynomial, as follows:

If g is a quartic polynomial with four distinct roots α, β, γ, and δ, then we have that

$$v^2 = (u-\alpha)(u-\beta)(u-\gamma)(u-\delta).$$

Dividing both sides by $(u-\alpha)^4$ and doing a little algebra leads to

$$\left(\frac{v}{(u-\alpha)^2}\right)^2 = \left(1 + (\alpha-\beta)\frac{1}{u-\alpha}\right)\left(1 + (\alpha-\gamma)\frac{1}{u-\alpha}\right)\left(1 + (\alpha-\delta)\frac{1}{u-\alpha}\right).$$

Since the roots are distinct, none of the factors on the right collapses to 1. It follows that if we set

$$x = \frac{1}{u-\alpha}, \qquad y = \frac{v}{(u-\alpha)^2},$$

then we have constructed a birational transformation between $v^2 = g(u)$ and

$$y^2 = f(x) = (1 + (\alpha-\beta)x)(1 + (\alpha-\gamma)x)(1 + (\alpha-\delta)x)$$

where $f(x)$ is a cubic polynomial in x—with three distinct roots, by the way. Thus, to find the arc length of an ellipse, we must evaluate

$$I(x) = \int \frac{dx}{\sqrt{x^3 + ax^2 + bx + c}},$$

and that is why $y^2 = x^3 + ax^2 + bx + c$ is called an elliptic curve.

Unfortunately, the change of variables (2) does not lead to an evaluation of the integral. You can't have everything.

4 Chord and Tangent Addition

Before we get to the problems, there's one more thing you need to know about elliptic curves—something that explains how Diophantus, Bachet, and Fermat were able to produce rational points (that is, points with rational coordinates) on curves, seemingly out of thin air.

It took the work of several giants of mathematics to show that the air wasn't as thin as all that. In the late seventeenth century, Newton (see [6, pp. 9–12] for details) deduced that each new point lay on the intersection of the given curve with a line that was either (a) tangent to the curve at some other point, or (b) a chord joining two points already on the curve (see Figure 2). In the nineteenth century, Jacobi tied the chord-and-tangent method in with elliptic integrals, and Weierstrass made a beautiful connection between an addition formula for elliptic functions and this chord-and-tangent way of producing new points from old on an elliptic curve. Finally, in 1901, Poincaré combined all of these ideas in a landmark paper on the arithmetical properties of algebraic curves.

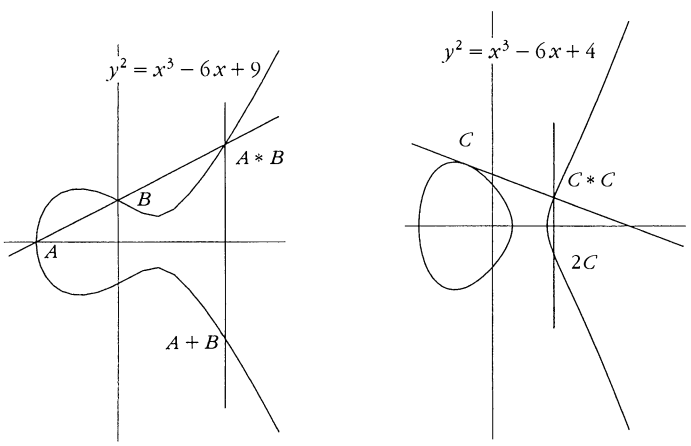


Figure 2

What these outstanding mathematicians showed was that the chord-and-tangent construction can be used to define a way of "adding" points on an elliptic curve. That is, given two points A and B on an elliptic curve, there's a third point on the curve called $A + B$, and this "addition" satisfies the group laws of closure, associativity, existence of an identity element, and existence of inverses.

Here are two examples. In Figure 2, the curve on the left, $y^2 = x^3 - 6x + 9$, contains the points $A = (-3, 0)$ and $B = (0, 3)$, and the chord joining A and B

meets the curve at a third point $A * B = (4, 7)$. Instead of this third point being $A + B$, it turns out that $A + B$ is the reflection $(4, -7)$ of $A * B$ in the x-axis. Similarly, the curve on the right, $y^2 = x^2 - 6x + 4$, contains the point $C = (-1, 3)$, and the tangent line at C meets the curve at the point $C * C = (9/4, 21/8)$. We call the reflection $(9/4, -21/8)$ of $C * C$ in the x-axis the double $2C = C + C$ of C. (Just why the operation is defined this way is another story.)

The upshot is that the set of all points on an elliptic curve forms a group under this addition, and the rational points on the curve form a subgroup. It is this subgroup of rational points that has been extensively studied, and whose properties can be brought to bear on many ancient problems. And that is perhaps the most magical aspect of this area of mathematics: we can do arithmetic with the points on an elliptic curve, and that this arithmetic comes directly out of the geometry of the curve!

And now, as promised, for three of those problems.

5 Congruent Numbers and Elliptic Curves

A right triangle with rational sides is called a rational right triangle; the area of such a triangle, which equals half the product of the legs, is clearly rational. But suppose we specified the area in advance; is there, for example, a rational right triangle with area 1? with area 5? with area, say, 157?

Commenting on an old problem of Diophantus, Pierre de Fermat proved, in a marginal note—not *the* marginal note—in his copy of Bachet's edition of Diophantus' *Arithmetica*, that the difference of two fourth powers is never a square. Now, if x, y, and z are the sides of a rational right triangle area $xy/2 = w^2$, a little algebra shows that

$$\left(x^2 - y^2\right)^2 = z^4 - (2w)^4,$$

contrary to Fermat's result. Hence, the area of a rational right triangle is never a square; in particular, no rational right triangle exists with area 1. This was the first theorem on what became known as the Congruent Numbers problem.

Leonhard Euler defined a congruent number to be a rational number that is the area of some right triangle with rational sides. As I mentioned earlier, the area of the 3-4-5 right triangle is 6; therefore, 6 is a congruent number. The 5-12-13 and 7-24-25 triangles have areas 30 and 84, respectively, so 30 and 84 are also congruent numbers. You should be able to find a rational right triangle with area 5 (start with the 9-40-41 triangle) and, with a bit more work, one with area 7. Euler conjectured, but could not prove, that if n is a squarefree integer of the form $8k + 5$, $8k + 6$, or $8k + 7$, then n is a congruent number. If he was right, then $157 = 8 \cdot 19 + 5$ should be a congruent number—and it is. More about that later.

There's another characterization of congruent numbers, which turns out to be useful:

Theorem. *Let n be a positive rational number. Then n is a congruent number if and only if there exist three rational squares in an arithmetic progression with common difference n.*

Proof. If n is the area of the rational right triangle with legs X and Y and hypotenuse Z, then we have $n = XY/2$; since $X^2 + Y^2 = Z^2$, a little algebra shows

that

$$\left(\frac{X+Y}{2}\right)^2 = \frac{X^2=Y^2}{4} + \frac{XY}{2} = \left(\frac{Z}{2}\right)^2 + n, \text{ and similarly}$$

$$\left(\frac{X-Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - n.$$

If we let $u = Z/2$, then $u^2 - n, u^2$ and $u^2 + n$ are three rational squares (rational since Z is rational) in an arithmetic progression (AP) with common difference n.

Conversely, if we have three such squares $u^2 - n, u^2$ and $u^2 + n$, just set $X = \sqrt{u^2+n} - \sqrt{u^2-n}$, $Y = \sqrt{u^2+n} + \sqrt{u^2-n}$, and $Z = 2u$. Again, a little algebra shows that $X^2 + Y^2 = Z^2$, so that we do have a right triangle (rational, since $u^2 - n, u^2$ and $u^2 + n$ are rational squares); a little more algebra shows that this triangle has area n, and so n is a congruent number. We're done.

For example, $\{1/4, 25/4, 49/4\}$ is an AP of rational squares with common difference $n = 6$, and the $(3, 4, 5)$ right triangle has area 6. On the other hand, the $(9, 40, 41)$ right triangle has area 180, and so the $(9/6, 40/6, 41/6)$ right triangle has area 5. Sure enough, $\{(31/12)^2, (41/12)^2, (49/12)^2\}$ is an AP of rational squares with common difference $n = 5$.

Euclid characterized all integral right triangles (X, Y, Z) with $\gcd(x, y, z) = 1$ as being of the form

$$X = r^2 - s^2, Y = 2rs, Z = r^2 + s^2$$

where r and s are relatively prime integers of opposite parity. Noting that the area of this triangle is $s(r^2 - s^2)$, a systematic way to generate squarefree congruent numbers goes something like this. For each odd k, list all products $rs(r^2 - s^2)$ with $r + s = k$. If $rs(r^2 - s^2)$ is divisible by a square m^2, so are both X and Y (try it!); so if we write $rs(r^2 - s^2) = m^2 n$ with n squarefree, then

$$\{(r^2 - s^2)/m, 2rs/m, (r^2 + s^2)/m\}$$

is a rational right triangle with area n. Here's a short list:

Pythagorean Triple	Area	Squarefree Congruent Number
$(3, 4, 5)$	6	6
$(5, 12, 13)$	30	30
$(7, 24, 25)$	84	21
$(8, 15, 17)$	60	15
$(9, 40, 41)$	180	5
$(25, 312, 313)$	3900	39

Well, this is fine, but where do elliptic curves come in?

Right here. If we take the product of three rational squares $u^2 - n, u^2$ and $u^2 + n$ in an arithmetic progression, this product is certainly a rational square v^2—but of a very particular form, namely

$$v^2 = (u^2 - n)u^2(u^2 + n) = u^6 - n^2u^2 = (u^2)^3 - n^2(u^2).$$

That is, if n is a congruent number, then the point $(x = u^2, y = v)$ is a rational point on the elliptic curve $y^2 = x^3 - n^2x$. From our example with $n = 6$, we saw that $u = 5/2$, and a little algebra again shows that $(25/4, 35/8)$ is a point on the elliptic

curve $y^2 = x^3 - 36x$. We observe that $25/4$ is a rational square with even denominator, which turns out to be the key to the whole business, though we won't prove the

Key Lemma. *n is a congruent number if and only if there exists a rational point (x, y) on the elliptic curve $y^2 = x^3 - n^2x$ such that x is a rational square with even denominator.*

So, even though $(25, 120)$ is a point on $y^2 = x^3 - 49x$ with x a rational square, its denominator is odd, and that's not enough to prove that 7 is a congruent number. But 7 *is* a congruent number, and the procedure outlined above should not take too long to produce both the relevant triangle and the rational point on $y^2 = x^3 - 49x$. Try it!

The Congruent Numbers trail wound from Diophantus through Fermat and Euler and came to (pretty much) an end in 1983 with the work of Jerrold Tunnell [**16**]. It was Tunnell who finally resolved the Congruent Numbers problem by tackling the equivalent problem involving the group of rational points on the elliptic curves $y^2 = x^3 - n^2x$. In part, he found the following necessary condition for n to be a congruent number—and it's fairly easy to check:

Tunnell's Criterion. Suppose that n is a square-free positive integer which is a congruent number. (a) If n is odd, then the number of integer triples (x, y, z) satisfying $n = 2x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $n = 2x^2 + y^2 + 32z^2$. (b) If n is even, then the number of integer triples (x, y, z) satisfying $\frac{n}{2} = 4x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $\frac{n}{2} = 4x^2 + y^2 + 32z^2$.

You can use this criterion to verify that a particular number is not a congruent number—try it on 11, 26, and 43, for example. It's almost true that if the criterion holds, then n is a congruent number. (The "almost" part is deep; if you want to pursue the matter, Koblitz' book [**7**] contains a wealth of information, is very well written, and will take you as far as you'd care to go.)

Oh, yes; 157 is a congruent number, but the denominator of a side of a right triangle with rational sides and area 157 has 22 digits. The two legs of this triangle are

$$x = \frac{6803298487826435051217540}{411340519227716149383203} \quad \text{and} \quad y = \frac{411340519227716149383203}{21666555693714761309610}.$$

I'll leave it as an exercise for you to find the hypotenuse!

6 A Truly Marvelous Proof—via Elliptic Curves

Fermat's Last Theorem states that if n is an integer greater than 2, then the equation $x^n + y^n = z^n$ has no solutions in which x, y, and z are all nonzero integers. This statement is one of the major milestones on the longest trail in mathematics. This trail begins almost 4000 years ago in ancient Mesopotamia, with a clay tablet known as Plimpton 322 (see [**13**, p. 3]), containing a table of integer triples (x, y, z) for which $x^2 + y^2 = z^2$, whose authors are unknown. It ends in 1995 in Princeton, with a mathematics journal known as the *Annals of Mathematics*, containing two papers [**17**], [**15**] which provide a proof of Fermat's Last Theorem, whose authors are Andrew Wiles and Richard Taylor. Many singular and notable events stand along

that trail, especially an obscure day, probably in 1637, when Fermat wrote down "that theorem" in the margin of his copy of Bachet's translation of Diophantus' *Arithmetica*, and that heart-stopping moment in June 1993 when Andrew Wiles announced a proof. Many mathematicians, including Euler, Legendre, Dirichlet, Germain, and Kummer, labored in vain to that end, and a good bit of modern number theory was developed in these attempts. Singh's book **[12]** is a highly readable and mathematically unsophisticated account of this most famous of mathematical puzzles from its genesis to its resolution. For a mathematically more technical account, a good place to begin is with David Cox's article **[2]**.

What is interesting for us is that the home stretch of the trail passes right through the world of elliptic curves, and that Fermat's Last Theorem (FLT, for short) was finally proved by, in essence, grafting the whole problem onto an elliptic curve.

Previous attempts at a proof of FLT usually begin by assuming, to the contrary, that nonzero integers a, b, c exist for which $a^n + b^n = c^n$ with $n > 2$ an integer. The attempt would proceed by analyzing the curve $x^n + y^n = z^n$ directly. One example was Gabriel Lamé's work in the 1840s; he began by writing

$$y^n = z^n - x^n = \prod_{k=0}^{n-1} (z - \zeta^k x),$$

where $\zeta = e^{2\pi i/n}$ satisfies $\zeta^n = 1$. He thought that he had proved that each factor on the right is a perfect nth power, and this led him to a desired contradiction. But Ernst Kummer pointed out a flaw in Lamé's argument, which he, Kummer, did his best to patch. The patch didn't always work, however, and the problem remained unsolved.

It was Gerhard Frey **[3]** who completely transformed FLT into a problem about elliptic curves. In essence, Frey said this: if I have a solution $a^n + b^n = c^n$ to the Fermat equation for some exponent $n > 2$, then I'll use it to construct the following elliptic curve:

$$\mathbf{E}\colon\ y^2 = x(x - a^n)(x + b^n) = g(x).$$

Now if f is a polynomial of degree k and if $r_1, r_2, \ldots, r_k$ are all of its roots, then the discriminant $\Delta(f)$ of f is defined by

$$\Delta(f) = \prod_{1 \le i < j \le k} (r_i - r_j)^2.$$

If f is monic with integer coefficients, it turns out that $\Delta(f)$ is an integer. The three roots of the polynomial $g(x)$ on the right-hand side of the Frey curve are 0, a^n, and $-b^n$; using the fact that $a^n - (-b^n) = a^n + b^n = c^n$ and a little algebra, we find that $\Delta(g) = (abc)^{2n}$.

Frey said that an elliptic curve with such a discriminant must be really strange. In particular, such a curve cannot possibly be what is called modular (never mind what that means). Now here's a thought, said he; what if you could manage to prove two things: first, that a large class of elliptic curves *is* modular, and second, that the Frey curve is always a member of that class of curves? Why, you'd have a contradiction —from which you could conclude that there is no such curve. That is, there is no such solution to the Fermat equation... that there is no counterexample to Fermat's Last Theorem... and so Fermat's Last Theorem is true.

And *that* is exactly what Andrew Wiles **[17]**—with a last-minute assist from Richard Taylor **[15]**—did.

7 $x^4 + dx^2y^2 + y^4 = z^2$ and Elliptic Curves

A solution of

$$x^4 + dx^2y^2 + y^4 = z^2 \tag{3}$$

with x, y, and z nonnegative integers is called trivial either if $xy = 0$ or if $d = n^2 - 2$ and $x = y = 1$. The first mention of this equation was made by Fermat, who proved that if $d = 0$, then (3) has only trivial solutions. His proof appeared in —yes—1637 as a marginal note in his copy of—you guessed it—Bachet's edition of Diophantus' *Arithmetica*. Over the years, many mathematicians tackled this problem, including Leibniz, who showed that the case $d = 6$ has only trivial solutions, and Euler, who gave several elegant methods for generating nontrivial solutions of (3).

As a result of reading a review in *Mathematical Reviews*, I got interested in this problem. In particular, it seemed curious that there were 23 values of d between 0 and 100 about which it was unknown whether nontrivial solutions to (3) exist. I was able to show that in 22 of these cases, there are indeed only trivial solutions to (3). The exceptional case is $d = 85$—apparently a solution Euler missed, since it is a solution he might have found, namely

$$1287^4 + 85 \cdot 1287^2 \cdot 4340^2 + 4340^4 = 54858119^2.$$

I wrote up what I'd done and sent it off to a journal, only to receive the aforementioned bad news that the entire problem could be transformed into a problem about elliptic curves, whose solution, I was assured by the referee, was routine.

Here's how the transformation works. Suppose that $X^4 + dX^2Y^2 + Y^4 = Z^2$; if we multiply both sides of this equation by X^2/Y^6, we are led to

$$\left(\frac{X}{Y}\right)^6 + d\left(\frac{X}{Y}\right)^4 + \left(\frac{X}{Y}\right)^2 = \left(\frac{zx^3}{y^3}\right)^2.$$

If we now let $y = ZX^3/Y^3$ and $x = (X/Y)^2$, we obtain

$$y^2 = x^3 + dx^2 + x; \tag{4}$$

since the roots of the right hand side are distinct if $d \neq \pm 2$, (4) is the equation of an elliptic curve.

Hence, if there is a nontrivial solution to (3), then the elliptic curve (4) will have a rational point (x, y) such that x is a perfect square. If this sounds familiar, it should; it's almost the same thing that happens when the Congruent Numbers problem is transformed to the world of elliptic curves. To take another example, since $(25, 245)$ is a rational point on the elliptic curve $y^2 = x^3 + 71x^2 + x$ in which the x-coordinate is a perfect square, it follows that $X^4 + 71X^2Y^2 + Y^4 = Z^2$ has a nontrivial solution—namely, $(X, Y, Z) = (5, 1, 49)$.

Resolving the problem at hand, however, while not nearly as hard or deep as the resolution of the Congruent Numbers problem, is still not entirely as routine as all that; furthermore, at the time, my knowledge of elliptic curves was practically nil.

Then I got an idea. I sent the paper off to a different journal, explaining in the cover letter that my approach to the problem was completely elementary and avoided the complicated machinery of elliptic curves. They accepted the paper [**1**].

8 Now What?

The future looks bright for the world of elliptic curves. Research in the area is booming, and there are many old problems in number theory that have been around for a long time and just might yield to the elliptic curve approach. In fact, ... oh, yes, of course you have questions.

- *You've said that elliptic curves are cubics of the form $y^2 = x^3 + ax^2 + bx + c$, in which the cubic polynomial in x has distinct roots. What do you get if the polynomial has repeated roots, such as x^3 or $x^3 + x^2$?* Those curves are called singular cubics, and they aren't studied as much as elliptic curves are, mainly because they don't have anything comparable to the chord-and-tangent addition of points on an elliptic curve.
- *Is there a special name for curves that involve polynomials of degree greater than 3?* For some of them, yes. In Section 3, we saw that an equation of the form $y^2 = f(x)$ with f a polynomial of degree 4 can be transformed into an elliptic curve, provided f has distinct roots. Curves of the form $y^2 = g(x)$, with g a polynomial of degree ≥ 5, are called *hyperelliptic curves*, and a goodly bit is known about them. But that's another story. Maybe some other time.
- *You said something back in Section 4 about addition of points on an elliptic curve being defined in a peculiar way for a particular reason. What's the reason?* Now *that's* a story I'd love to tell—but the margin of this paper is not large enough to contain it. As my grandmother used to say, "Tell you tomorrow!"

References

1. Ezra Brown, $x^4 + dx^2y^2 + y^4 = z^2$: Some cases with only trivial solutions—and a solution Euler missed, *Glasgow Math. J.* 31 (1989), 297–307.
2. David A. Cox, Introduction to Fermat's Last Theorem, *Amer. Math. Monthly* 101 (1994), 3–14.
3. Gerhard Frey, Links between stable elliptic curves and certain Diophantine equations, *Ann. Univ. Saraviensis*, Series Mathematicae 1 (1986), 1–40.
4. Shafi Goldwasser and J. Kilian, Almost all primes can be quickly certified, *Proc. 18th Annual ACM Symposium on Theory of Computing* (1986), 316–329.
5. Thomas L. Heath, *Diophantus of Alexandria*, Cambridge University Press, 1910.
6. Anthony W. Knapp, *Elliptic Curves*, Princeton University Press, 1992.
7. Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.
8. Neal Koblitz, Elliptic curve cryptosystems, *Math. Comp.* 48 (1987), 203–209.
9. Hendrik W. Lenstra, Factoring integers with elliptic curves, *Annals of Mathematics* 126 (1987), 649–673.
10. Victor S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology—CRYPTO '85*, Lecture Notes in Computer Science 218 (1986), 417–426.
11. Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.
12. Simon Singh, *Fermat's Enigma*, Walker Publishing Co., 1997.
13. John Stillwell, *Mathematics and its History*, Springer-Verlag, 1989.
14. John Stillwell, The evolution of elliptic curves, *Amer. Math. Monthly* 102 (1995), 831–837.
15. Richard Taylor and Andrew Wiles, Ring-theoretic aspects of certain Hecke algebras, *Annals of Mathematics* 142 (1995), 553–572.
16. Jerrold Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Inventiones Math.* 72 (1983), 323–334.
17. Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics* 142 (1995), 443–551.