Elliptic Curves from Mordell to Diophantus and Back

Ezra Brown and Bruce T. Myers

1. DIOPHANTUS, MORDELL, AND RATIONAL POINTS ON ELLIPTIC CURVES.

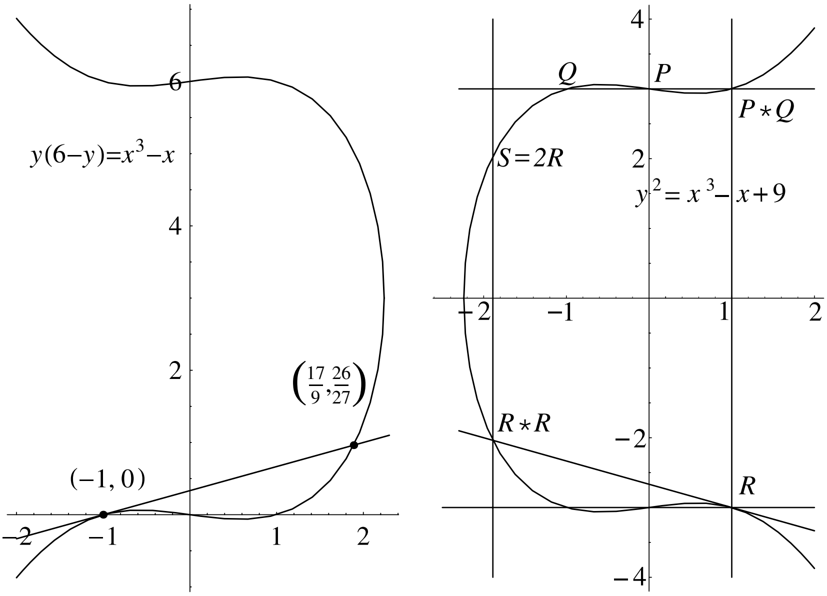

Figure 1. The First Elliptic Curve.

Many years ago, one of us was reading through L. J. Mordell's "Diophantine Equations" and was struck by a curious statement—namely, that the curve $C : y^2 = x^3 + 17$ contains exactly sixteen points (x, y) with x and y integers (see [**6**, p. 250]). A list of the points followed.

Many questions immediately came to mind. How did they find these points, called *integer points*? How did they prove that these were the only ones on that curve? Why do some curves have many integer points and others, such as the one with equation $y^2 = x^3 + 13$, have none? Are there curves with more integer points than C?

Many years later, we found some answers to these and other questions. The path on which our investigations took us began with Mordell's book and proceeded to Diophantus, to the "Arithmetica," to the first appearance of those wonders known as *elliptic curves*, to a certain family of elliptic curves, and back to Mordell. What we're going to do in this paper is to tell the story of what we found. In particular, we will:

- tell you what elliptic curves are (C is one, by the way)
- describe Diophantus' problem in which elliptic curves made their first appearance in the mathematical world

- exhibit a family of elliptic curves E_m, some of which have many more integer points than C
- tell about the rank of an elliptic curve (which was studied in great detail by Mordell, incidentally) and give a simple proof that if $m \geq 2$, then the rank of E_m is at least 2. By *simple*, we mean that—except for a couple of assumptions about ranks of curves—the proofs use nothing more complicated than congruences, the Least Integer Principle, elementary properties of finite groups, an old result of Fermat, and a formula for the double of a point on an elliptic curve
- prove that for infinitely many m the rank of E_m is at least 3.

And now, on to—yes? Oh. What are the eight integer points on C with positive y-coordinates? Well, the x-coordinate has one digit in five of them and two digits in two others. We'll talk about the eighth point later.

And now, on to Diophantus!

2. DIOPHANTUS AND ELLIPTIC CURVES. For us, an elliptic curve is a curve E defined over the rationals by an equation of the form

$$y^2 = x^3 + ax + b,$$

where a and b are rational and the cubic $x^3 + ax + b$ has distinct roots. They are among the most closely studied and fascinating objects in all of mathematics, and they make their mathematical debut in Diophantus of Alexandria's *Arithmetica* [**5**]. This book is a treasure trove for anyone interested in the early history of number theory, and I. G. Bashmakova [**1**] has written a particularly insightful presentation of this early gem for the modern reader. We first encounter elliptic curves in Problem 24 of Book IV, which reads as follows: "To divide a given number into two numbers such that their product is a cube minus its side."

If we call Diophantus' given number a, the task is to find x and y such that

$$y(a - y) = x^3 - x. \tag{1}$$

Diophantus solves the problem for $a = 6$ by substituting $x = ky - 1$ and choosing the value $k = 3$; this causes the resulting polynomial in y to have only a cubic and quadratic term. Ignoring the double root $y = 0$, he obtains $y = 26/27$ and thus $x = 17/9$.

A modern interpretation of Diophantus' solution goes like this: construct the tangent line to the curve at the point $(0, -1)$ and find the point $(17/9, 26/27)$ where the tangent re-intersects the curve. The solution to the problem is therefore $6 = 26/27 + 136/27$, and the product of those two numbers is $(17/9)^3 - (17/9)$.

Following Diophantus, set $a = 6$ in (1). If we subtract 9 from both sides and replace y by $y + 3$ and x by $-x$, we transform the curve corresponding to (1) into the curve E_3: $y^2 = x^3 - x + 9$ (we will explain the name shortly). Since the cubic $x^3 - x + 9$ has distinct roots, E_3 is an elliptic curve. The points $(-1, 0)$ and $(17/9, 26/27)$ correspond to $R = (1, -3)$ and $R * R = (-17/9, -55/27)$, respectively. (We define the operation $*$ in Section 3.) Reflecting R in the x-axis reveals the point $2R = (-17/9, 55/27)$, which—as we shall see—is the double of the point R in the group E_3 of points on this curve. This reveals that Diophantus really discovered the method of doubling points on elliptic curves—although he probably didn't know it at the time.

The points of E are the pairs (x, y) of algebraic numbers that are solutions to this cubic, together with a unique point at infinity, denoted $\mathbf{O}$. It is a fact that the points of E form an abelian group with $\mathbf{O}$ as the identity point, under an operation known as chord-and-tangent addition; we give a brief review of this operation in Section 3.

Before we go on, here is a bit of terminology we'll need. A point (x, y) on E is called a *rational* (respectively, *integer*) point if its coordinates x and y are in $\mathbf{Q}$ (respectively, in $\mathbf{Z}$); $\mathbf{O}$ is considered an integer (hence, a rational) point. This implies that our curve $C : y^2 = x^3 + 17$ has exactly 17 integer points. As noted, the set of points on E forms an abelian group, of which the rational points $E(\mathbf{Q})$ are a subgroup. A *torsion point* of E is a point of finite order in this group. The rational torsion points of E form a subgroup $E(\mathbf{Q})_{\mathrm{TORS}}$ of the group E_{TORS} of all torsion points of E.

One of the major results in the field is that $E(\mathbf{Q})$ is a finitely generated abelian group isomorphic to $\mathbf{Z}^r \oplus E(\mathbf{Q})_{\mathrm{TORS}}$ for some integer r; r is called the *rank* of E. Learning that this theorem is due to none other than L. J. Mordell was a revelation to one of us, as was the fact that $E(\mathbf{Q})$ is called the *Mordell–Weil group*.

Back to E_3: A bit of numerical experimentation revealed that E_3 has several obvious integer points, namely $P := (0, 3)$, $Q := (-1, 3)$, $R := (1, -3)$, and $(9, 27)$, as well as the nonobvious points $(35, 207)$ and $(37, 225)$ and the completely unanticipated point $(46584, 10054377)$. It turned out that in the group $E_m(\mathbf{Q})$ of rational points on E_m, $R = P + Q$, $(9, 27) = P + 2Q$, $(35, 207) = 2P + Q$, $(37, 225) = -P + Q$, and $(46584, 10054377) = 3P$.

Struck by this unexpected turn of events, we wondered if this is true in a more general setting, so we looked for integer points on the family of curves

$$E_m : y^2 = x^3 - x + m^2 \tag{2}$$

for m a nonnegative integer, which we call *Diophantine elliptic curves* in honor of their originator. We discovered that this pattern does persist. That is, E_m always has the following integer points:

$$\begin{aligned}
P &= (0, m),\\
Q &= (-1, m),\\
P + Q &= (1, -m),\\
P + 2Q &= (m^2, m^3),\\
2P + Q &= (4m^2 - 1, 8m^3 - 3m),\\
P - Q &= (4m^2 + 1, -8m^3 - 3m),\\
3P &= (64m^6 - 8m^2, 512m^9 - 96m^5 + 3m),
\end{aligned} \tag{3}$$

together with their negatives—the negative of (x, y) is $(x, -y)$—and the point at infinity $\mathbf{O}$, for a total of 15 integer points. Oddly enough, although $3P$ is always integral,

$$2P = \left(\frac{1}{4m^2}, -\frac{8m^4 - 1}{8m^3}\right)$$

is never integral.

But there's more: E_m often has many integer points besides these (Table 1).

In the elliptic curve world, an important problem is to determine the rank and rational torsion of a given curve. The rational torsion points are easy to determine, but in general, the rank is not. Using high-powered algorithms of Cremona, the rank can be computed in some cases [**4**, pp. 78–97]. It is unknown whether there exist elliptic curves of arbitrarily high rank.

TABLE 1. Numbers of integer points on $E_m : y^2 = x^3 - x + m^2$.

E_m	Integer points found
E_5	31
E_{25}	37
E_{113}	51
E_{337}	77
E_{8765}	85
E_{297779}	107
E_{765617}	181

We ran many experiments using MAGMA and PARI, and found another compelling aspect of the family of curves E_m. Namely, it appears that if $m > 1$, then their rank is always at least 2, and frequently much higher, as we can see from Table 2. In addition, if $m > 1$, then the points P and Q are always independent in $E_m(\mathbf{Q})$—that is, no nonzero integers n and k exist for which $nP + kQ = \mathbf{O}$.

TABLE 2. Minimal ranks of some $E_m : \ y^2 = x^3 - x + m^2$.

r	First few m such that $\mathrm{rank}(E_m(\mathbf{Q})) = r$
2	2, 3, 4, 6, 9, 10, 18, 21, 26, 30
3	5, 7, 8, 11, 12, 13, 14, 15, 16, 17
4	24, 25, 27, 31, 36, 41, 46, 58, 61, 63
5	113, 127, 163, 176, 181, 209, 215, 245, 283, 317
6	337, 599, 734, 853, 938, 1015, 1153, 1303, 1405, 1907
≥ 7	6310, 8765, 10327, 13411, 13777, 17207, 19013, 21937, 22361
≥ 8	78560, 83459, 146287, 170981, 265919, 297779, 420065, 464855, 466551, 467335
≥ 9	423515, 1395829, 1510627, 1533293, 1741033
≥ 10	765617

Intrigued, we investigated further and were able to prove the following theorem.

Theorem 1. *Let m be a nonnegative integer, and let E_m be the elliptic curve with equation $y^2 = x^3 - x + m^2$.*

(a) If $m \geq 1$, then $E_m(\mathbf{Q})_{\text{TORS}} = \{\mathbf{O}\}$.

(b) If $m \geq 2$, then rank$(E_m(\mathbf{Q})) \geq 2$, and P and Q are independent points.

(c) There are infinitely many values of m for which rank$(E_m(\mathbf{Q})) \geq 3$.

In contrast with many results in the elliptic curve world, this one has a fairly simple proof that uses very little heavy machinery. We present this proof in the remainder of this paper.

Before we do that, let's talk about how to add points on elliptic curves.

3. ADDITION OF POINTS ON AN ELLIPTIC CURVE. The exact nature of what Diophantus accomplished in the solution of his Problem 24, Book IV took over 1500 years to reveal itself completely. In the seventeenth century, Bachet and Fermat described algebraic formulas for, in essence, doubling a point, and Newton showed how the geometry of chords and tangents tied in with the formulas of Bachet and Fermat. In the nineteenth century, Jacobi and Weierstrass connected these efforts with elliptic integrals and elliptic functions, and in 1901 Poincaré unified and generalized this work to algebraic curves.

The point of this work is that if E is an elliptic curve, and if each of A and B is a point on E, then the chord joining A and B (or the tangent to the curve at A, if $A = B$) meets the curve in a unique third point called $A * B$. The reflection of $A * B$ in the x-axis yields a unique point, which we call $A + B$; if $A = B$, we call this reflection $2A$.

For example, in Figure 1 on the right we see the curve $E_3 : y^2 = x^3 - x + 9$. This contains the points $P = (0, 3)$, $Q = (-1, 3)$, and $R = (1, -3)$, R corresponding to the point where Diophantus drew his tangent line. The chord joining P and Q meets E_3 in $P * Q = (1, 3)$, and the reflection of $P * Q$ in the x-axis is the point $P + Q = (1, -3)$. This shows that $(0, 3) + (-1, 3) = (1, -3)$, i.e., $P + Q = R$. Furthermore, the line tangent to E_3 at R meets E_3 in $R * R = (-17/9, -55/27)$, and the reflection of this point in the x-axis is the point $2R = (-17/9, 55/27)$, the double of R.

The work of Poincaré showed that the set of points on an elliptic curve E is a group under this chord-and-tangent addition, the point at infinity $\mathbf{O}$ is its identity element, and the set $E(\mathbf{Q})$ of rational points is a subgroup. Among other curiosities, three points on the curve are collinear if and only if they sum to $\mathbf{O}$, and the hardest part about verifying the group axioms is proving associativity!

In Section 5 we make use of a formula for the x-coordinate of the double of a point, but for the sake of completeness, here are some general formulas for adding and doubling points on the curve E. Suppose that each of $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ is a point on $E : y^2 = x^3 + ax + b$. If $x_1 = x_2$ and either $y_1 \neq y_2$ or $y_1 = y_2 = 0$, then $P_1 + P_2 = \mathbf{O}$, and we write $P_2 = -P_1$. Otherwise, define k by

$$k = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\[2ex] \dfrac{3x_1^2 + a}{2y} & \text{if } x_1 = x_2. \end{cases} \tag{4}$$

Then $P_1 + P_2 = (x_3, y_3)$, where

$$\begin{aligned} x_3 &= k^2 - x_1 - x_2, \\ y_3 &= -(y_1 + k(x_3 - x_1)). \end{aligned} \tag{5}$$

As with addition of numbers, we write $2P = P + P$, $3P = P + 2P$, etc. For example, for that point $R = (1, -3)$ on E_3, you can show that

$$3R = \left(\frac{664}{169}, \frac{17811}{2197}\right), \quad 4R = \left(\frac{257299}{27225}, \frac{130479157}{4492125}\right).$$

Exercise. Use these formulas to verify the equalities in equation (3).

Notice that each of the rational points we've met so far is of the form $(u/r^2, v/r^3)$ for integers u, v, and r—for example,

$$4R = \left(\frac{257299}{165^2}, \frac{130479157}{165^3}\right).$$

In the next section, we prove that this always happens, along the way to showing that if $m > 0$, then E_m contains no rational points of finite order other than $\mathbf{O}$, the point at infinity.

4. RATIONAL TORSION AND CURVES OVER FINITE FIELDS. The following lemma greatly simplifies our work. The heaviest hammer in the proof is, appropriately, one of Fermat's theorems from the margin of his copy of Diophantus. We say that *a divides b* (or that *a is a divisor of b*) and write $a|b$ if a, b, and b/a are integers; if p is a prime, write $p^e\|a$ if $p^e|a$ and $p^{e+1}\nmid a$. Finally, $\mathrm{GCD}(a, b)$ refers to the greatest common divisor of a and b.

Lemma 2. *(a) If* (x, y) *is a rational point on the elliptic curve* $E : y^2 = x^3 + ax + b$*, then* $x = u/r^2$ *and* $y = v/r^3$ *for some integers* u, v, r *with* $\mathrm{GCD}(u, r) = \mathrm{GCD}(v, r) = 1$. *(b) The only rational points on* $E_0 : y^2 = x^3 - x$ *are* $(0, 0)$, $(1, 0)$, $(-1, 0)$*, and* $\mathbf{O}$.

Proof.

(a) Put $x = u/s$ and $y = v/t$ with $\mathrm{GCD}(u, s) = \mathrm{GCD}(v, t) = 1$. A little algebra yields

$$s^3v^2 = t^2(u^3 + aus^2 + bs^3).$$

If $p^e\|s$ then $p^{3e}|s^3v^2$. Since $p\nmid u$ and $p|aus^2 + bs^3$, it follows that $p^{3e}|t^2$. No higher power of p can divide t^2; otherwise $p|v$, contrary to the assumption that $\mathrm{GCD}(v, t) = 1$. Hence, $p^{3e}\|t^2$. If $p^f\|t$, then it follows that $3e = 2f$, i.e., $f = 3c$ and $e = 2c$ for some integer c. Thus, $p^{3c}\|t$ and $p^{2c}\|s$. Since this holds for each prime p, we conclude that $s = r^2$ and $t = r^3$ for some integer r.

(b) Now $\mathbf{O}$ is a rational point, by definition. Suppose (x, y) is a finite rational point of E_0; by (a), $x = u/r^2$ and $y = v/r^3$ for integers u, v, and r, with r relatively prime to u and v. Substituting and expanding, we find that

$$v^2 = u(u^2 - r^4).$$

If $u = 0$, 1, or -1, then $v = 0$, accounting for the points $(0, 0)$, $(1, 0)$, and $(-1, 0)$. Let $g = \mathrm{GCD}(u, v)$, so that $u = gu_1$, $v = gv_1$, and $\mathrm{GCD}(u_1, v_1) = 1$. We find that

$$gv_1^2 = u_1(g^2u_1^2 - r^4).$$

Since u_1 and v_1 have no common factors, it follows that $u_1|g$; writing $g = u_1u_2$ leads to the equation

$$u_2v_1^2 = u_1^4u_2^2 - r^4.$$

Hence $u_2|r^4$. But $\mathrm{GCD}(u, r) = 1$, so $u_2 = 1$ and we are led to the equation

$$v_1^2 = u_1^4 - r^4,$$

which, Fermat assures us, has no solutions in nonzero integers. Hence, the only rational points on E_0 are $(0, 0)$, $(1, 0)$, $(-1, 0)$, and $\mathbf{O}$. ■

Now, if $E : y^2 = x^3 + ax + b$ is an elliptic curve with a and b in $\mathbf{Z}$, and if p is a prime, then we may regard E as a "curve" over the p-element field $\mathbf{F}_p$, with a, b, x, and y elements of the field $\mathbf{F}_p$. If the discriminant $\Delta(E) = -16(4a^3 + 27b^2)$ is prime to p, then the cubic $x^3 + ax + b$ has distinct roots and E is an elliptic curve over $\mathbf{F}_p$. If this happens, E is said to have *good reduction* at p, and $E(\mathbf{F}_p)$ is called the group of F_p-points of E.

This matters because if E has good reduction at p, then the Reduction mod p Theorem ensures that there is an injection (i.e., a one-to-one mapping) of the group $E(\mathbf{Q})_{\text{TORS}}$ of rational torsion points into the group $E(\mathbf{F}_p)$ [**7**, p. 123]. This theorem makes it easy to prove the main result of this section.

Theorem 3. *If $m \geq 1$, then $E_m(\mathbf{Q})_{\text{TORS}} = \mathbf{O}$.*

Proof. The discriminant $\Delta(E_m) = -16(27m^4 - 4)$ is never divisible by 3 or 5, so E_m has good reduction at 3 and 5.

If $3|m$, then E_m reduces to $y^2 = x^3 - x$ over $\mathbf{F}_3$, and $E_m(\mathbf{F}_3) = \{\mathbf{O}, (0, 0), (1, 0), (-1, 0)\}$, the Klein Four Group. Since $E_m(\mathbf{Q})_{\text{TORS}}$ injects into $E_m(\mathbf{F}_3)$, it follows that $E_m(\mathbf{Q})_{\text{TORS}}$ is a subgroup of the rational points of order 2 of E_m. Such a point of E_m is necessarily of the form $(r, 0)$, where r is a rational root of $x^3 - x + m^2 = 0$, i.e., a rational solution to $m^2 = (-x)^3 - (-x)$. But there are no such rational roots, by Lemma 2. Hence $E(\mathbf{Q})_{\text{TORS}} = \{\mathbf{O}\}$.

If $3 \nmid m$, then $m^2 \equiv 1 \pmod 3$ and E_m reduces to $y^2 = x^3 - x + 1$ over $\mathbf{F}_3$. Here, $|E_m(\mathbf{F}_3)| = 7$, so that $|E(\mathbf{Q})_{\text{TORS}}| = 1$ or 7. In addition, E_m reduces over $\mathbf{F}_5$ to $y^2 = x^3 - x$, $y^2 = x^3 - x + 1$, or $y^2 = x^3 - x - 1$ according as $m \equiv 0, \pm 1$, or ± 2 (mod 5), respectively. In each case, $|E_m(\mathbf{F}_5)| = 8$. Hence, $|E(\mathbf{Q})_{\text{TORS}}| = 1, 2, 4$, or 8. Thus, $|E(\mathbf{Q})_{\text{TORS}}| = 1$, and we conclude that $E(\mathbf{Q})_{\text{TORS}} = \{\mathbf{O}\}$. ■

Keep an eye on this theorem: it reappears at a crucial moment.

5. COMPUTING THE RANK OF E_m.

There are several ways to find the rank of $E(\mathbf{Q})$, or at least a lower bound on the rank, but most of them are complicated and rely on lots of heavy machinery. The task is daunting, especially when the curve at hand has trivial rational torsion—as our curves do. So, we looked for, and found, a simple proof that $E_m(\mathbf{Q})$ has rank at least 2 for $m > 1$; it relies on only one piece of heavy machinery. We state the theorem for our special case; the full-blown result can be found in [**4**, p. 78]. Recall that an *elementary abelian* 2*-group* is an abelian group in which every nonidentity element has order 2.

Theorem 4. *Let $E(\mathbf{Q})$ (respectively, $2E(\mathbf{Q})$) be the group of rational points (respectively, doubles of rational points) on an elliptic curve E, and suppose that E has trivial rational torsion. Then the quotient group $E(\mathbf{Q})/2E(\mathbf{Q})$ is an elementary abelian 2-group of order 2^r, where r is the rank of $E(\mathbf{Q})$.*

Our strategy is to show that the points P, Q, and $P + Q$ from (3) are not doubles of rational points. This implies that the set of cosets $\{[\mathbf{O}], [P], [Q], [P + Q]\}$ is a four-element subgroup of $E_m(\mathbf{Q})/2E_m(\mathbf{Q})$ and, together with Theorem 3, that P and Q are independent. We begin by describing sufficient conditions for a rational point A not to be the double of a rational point B on E_m.

Theorem 5. *Let $A = (u/s^2, v/s^3)$ and $B = (w/t^2, z/t^3)$ be points on E_m, with* $\text{GCD}(uv, s) = \text{GCD}(wz, t) = 1$. *If either (a) u is even, (b) u and s are odd and*

m is even, (c) $u \equiv 1 \bmod 4$ and s and m are odd, or (d) $u = -1$, $s = 1$, and $m > 1$, then $A \neq 2B$.

Proof. If $B = (x, y)$ and $A = (x_0, y_0) = 2B$, then (4) and (5) imply that

$$x_0 = \frac{x^4 + 2x^2 + 1 - 8m^2x}{4(x^3 - x + m^2)}.$$

Substituting $x_0 = u/s^2$ and $x = w/t^2$ and expanding leads to the equation

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6). \tag{6}$$

The proofs in cases (a), (b), and (c) are straightforward; we leave them as exercises, along with these hints: look at (6) mod 8 for (a) and (b), and mod 16 for (c).

As for (d), let $u = -1$ and $s = 1$, i.e., $x_0 = -1$. Then (6) becomes

$$-4(wt^2(w^2 - t^4) + m^2t^8) = (w^2 + t^4)^2 - 8m^2wt^6,$$

which we can expand and rearrange, yielding

$$(w + t^2)^4 = 4t^4(w^2 + 2wt^2 + m^2t^2(2w - t^2)).$$

This implies that $t|(w + t^2)$, so that $t|w$. But t and w are relatively prime, and so $t = 1$. If we substitute $t = 1$, rearrange, and simplify, we are led to the equation

$$(w^2 + 2w - 1)^2 = 4m^2(2w - 1).$$

This implies that $(2w - 1)|(w^2 + 2w - 1)^2$, so that $(2w - 1)|w^2$. But again, $\mathrm{GCD}(2w - 1, w^2) = 1$, so we conclude that $w = 1$, and so $m = 1$. Thus, if $u = -1$, $s = 1$, and $m > 1$, then A is not the double of a rational point. ■

Remark. As a corollary, we know that if $m \geq 1$ then $P = (0, m) \notin 2E_m(\mathbf{Q})$ (by (a)) and $P + Q = (1, -m) \notin 2E_m(\mathbf{Q})$ (by (b) and (c)); and if $m > 1$, then $Q = (-1, m) \notin 2E_m(\mathbf{Q})$ (by (d)).

We're almost there.

Lemma 6. *Let $m > 1$, with $P = (0, m)$ and $Q = (-1, m)$. Then $H = \{[\mathbf{O}], [P], [Q], [P + Q]\}$ is a four-element subgroup of $E_m(\mathbf{Q})/2E_m(\mathbf{Q})$.*

Proof. By the preceding remark, we know that $[P] \neq [\mathbf{O}]$, $[Q] \neq [\mathbf{O}]$, and $[P + Q] \neq [\mathbf{O}]$. If $[P] = [Q]$, then $[P + Q] = [P] + [Q] = [P] + [P] = [2P] = [\mathbf{O}]$, which is impossible. In a similar way, we can show that $[P]$ and $[P + Q]$ are distinct (else $[Q] = [\mathbf{O}]$), and that $[Q]$ and $[P + Q]$ are distinct (else $[P] = [\mathbf{O}]$). We conclude that $[\mathbf{O}]$, $[P]$, $[Q]$, and $[P + Q]$ are distinct classes of $E_m(\mathbf{Q})/2E_m(\mathbf{Q})$, so H is a 4-element subgroup of $E_m(\mathbf{Q})/2E_m(\mathbf{Q})$.

■

The following lemma is the last piece of the puzzle.

Lemma 7. *P and Q are independent points in $E_m(\mathbf{Q})$ for $m \geq 2$.*

Proof. Suppose that, to the contrary, there exist integers n and k such that $nP + kQ = \mathbf{O}$. Without loss of generality, we may assume that n is positive and minimal among all such representations. If n is even and k is odd, then $[\mathbf{O}] = [nP + kQ] = [Q]$, contrary to Lemma 6. Similarly, n odd and k even imply that $[\mathbf{O}] = [P]$, and both n and k odd imply that $[\mathbf{O}] = [P + Q]$, both contrary to Lemma 6. Finally, if $n = 2n'$ and $k = 2k'$, then $2(n'P + k'Q) = \mathbf{O}$, which implies that $n'P + k'Q$ is a rational 2-torsion point. But E_m has trivial rational torsion by Theorem 3 (remember, we said to keep an eye on Theorem 3!), so that $n'P + k'Q = \mathbf{O}$, contrary to the minimality of n. ■

Theorem 1(b), which is the main result that $\operatorname{rank}(E_m(\mathbf{Q})) \geq 2$ for $m \geq 2$, now follows from Lemma 7 and the fact that the rank of $E_m(\mathbf{Q})$ is just the size of a maximal independent subset of $E_m(\mathbf{Q})$.

6. RANK 3 AND BEYOND.

The strategy for finding curves of rank at least 3 is based on the following generalization of Lemma 7.

Lemma 8. *Let R be a rational point on $E(\mathbf{Q})$, and let $\{P_1, \ldots, P_k\}$ be independent points in $E(\mathbf{Q})$. If $[R] \notin < [P_1], \ldots, [P_k] >$ in $E(\mathbf{Q})/2E(\mathbf{Q})$ and if E has trivial rational 2-torsion, then $P_1, \ldots, P_k$, and R are independent in $E(\mathbf{Q})$.*

Proof. Suppose that there exist integers $a_0, a_1, \ldots, a_k$, not all zero, such that

$$a_0R + a_1P_1 + \cdots + a_kP_k = \mathbf{O}; \tag{7}$$

without loss of generality, we may assume that a_0 is positive and minimal among all such representations.

If a_0 is odd, then $[a_0R] = [R]$ and (7) implies that $[R] = [a_1P_1 + \cdots + a_kP_k]$, contrary to assumption.

If a_0 is even, then $[a_0R] = [\mathbf{O}]$, and (7) implies that $[a_1P_1 + \cdots + a_kP_k] = [\mathbf{O}]$; since the P_i are independent, this means that all the a_i are even. Writing $a_i = 2b_i$, we see that (7) implies that

$$2(b_0R + b_1P_1 + \cdots + b_kP_k) = \mathbf{O}.$$

This means that $b_0R + \cdots + b_kP_k = \mathbf{O}$, since $E(\mathbf{Q})$ has only trivial 2-torsion; but this contradicts the minimality of a_0. ■

Since our curves E_m have trivial torsion for $m > 0$, Lemma 8 applies to these curves. All we need now is one more result, similar to Theorem 5, about certain points not being doubles of other points. Here it is:

Lemma 9. *Let $A = (u/s^2, v/s^3)$ and $B = (w/t^2, z/t^3)$ be points on E_m, with* $\operatorname{GCD}(uv, s) = \operatorname{GCD}(wz, t) = 1$. *If $m \equiv 0 \bmod 3$ and $s \not\equiv 0 \bmod 3$, then $A \neq 2B$.*

Proof. Putting $A = 2B$ and expanding leads, as in the proof of Theorem 5, to equation (6):

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6).$$

Considerations modulo 3 imply that if $m \equiv 0 \bmod 3$ and $s \not\equiv 0 \bmod 3$, then

$$4uwt^2(w^2 - t^4) \equiv (w^2 + t^4)^2 \pmod{3}. \tag{8}$$

Now w and t cannot both be divisible by 3, since they are relatively prime; hence, the right side of (8) is nonzero mod 3. But for all w and t, $wt^2(w^2 - t^4)$ is a multiple of 3. This is impossible, and so A is not the double of a rational point. ■

Finally, using Lemma 9 in conjunction with other results, we may construct some infinite families of curves with rank at least 3. For example, if $R = (36n + 17, 54n^2 + 267n + 114)$ and $m = 54n^2 - 165n - 90$, then R is a point on E_m with $m \equiv 0 \bmod 3$. It is not hard to show that none of the points R, $P + R$, $Q + R$, and $P + Q + R$ is in $2E_m$:

- R and $P + R = (-36n - 127, -54n^2 + 607n - 1434)$ are integer points, so $s = 1$; by Lemma 9, $R \notin 2E_m$ and $P + R \notin 2E_m$.
- The x-coordinate of $Q + R$ has even numerator and a denominator that is a divisor of $9(2n + 1)^2$, so u is even and s is odd. By Theorem 5, $Q + R \notin 2E_m$.
- The denominator of the x-coordinate of $P + Q + R$ is a divisor of $(36n + 16)^2$; hence, $s \not\equiv 0 \bmod 3$, and so by Lemma 9, $P + Q + R \notin 2E_m$.

Since P and Q are independent, E_m has trivial rational torsion, and $[R] \notin \langle [P], [Q] \rangle$ in $E(\mathbf{Q})/2E(\mathbf{Q})$,we may now apply Lemma 8 to see that P, Q, and R are independent points. This implies that for $m = 54n^2 - 165n - 90$, E_m has rank at least 3.

Hence there are infinitely many values of m such that E_m has rank at least 3.

7. QUESTIONS AND PROBLEMS.

- *How did you find the family of curves with rank at least 3?* We looked for values of x for which the points $R = (x, y)$, $P + R$, $Q + R$, and $P + Q + R$ satisfied at least one of the conditions of Theorem 5 and Lemma 9. We began with $x = 6n + 3$ and made adjustments where needed. For example, if the denominator of the x-coordinate of a point might be divisible by 3, we made sure that the denominator was odd and the numerator was even. There are probably many more such families. *Problem 1*: Find some.
- *Are there infinite families of curves E_m with rank at least 4, and if so, how do you prove it?* The tables suggest that there are infinitely many curves E_m of rank at least 4, 5, and even 6. Proving that a certain set of four points is independent amounts to showing that 15 distinct points are not doubles of rational points. Raising the rank by one, in short, doubles the work. *Problem 2*: Find some.
- *Are there families of elliptic curves other than E_m, all of which have high ranks?* No doubt about it. For example, the curves $C_m : y^2 = x^3 - m^2x + 1$ appear to have rank at least 3 for all $m \geq 4$, and they may be amenable to the elementary techniques we've described here. A bit of sleuthing should turn up others. *Problem 3*: Use the techniques of this paper to prove that the curves C_m have rank ≥ 3 for $m \geq 4$.

  An attempt to prove that the point $(m, 1)$ is not the double of a rational point failed—because it is false in a few cases. *Problem 4*: Prove that $(m, 1)$ is the double of a rational point on $C_m : y^2 = x^3 - m^2x + 1$ if and only if $m = 3, 7$, or 24. Equivalently, prove that the polynomial $x^4 - 4mx^3 + 2m^2x^2 + (4m^3 - 8)x + m^4 - 4m$ has a rational root if and only if $m = 3, 7$, or 24.
- *What about those eight points on $C : y^2 = x^3 + 17$ from Section 1?* A direct search turns up all eight points. It is more fun, however, to start with the two points $A = (-1, 4)$ and $B = (-2, 3)$ and generate the other six from linear combinations of A and B using the techniques of Section 3.

REFERENCES

1. I. G. Bashmakova, *Diophantus and Diophantine Equations* (trans. Abe Shenitzer), Dolciani Mathematical Expositions **20**, Mathematical Association of America, Washington, D.C., 1997.

2. B. J. Birch and H. P. Swinnerton-Dyer, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** (1963) 7–25.
3. J. E. Cremona, Classical invariants and 2-descent on elliptic curves, *J. Symbolic Comput.* **11** (1998) 1–17.
4. ———, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge University Press, New York, 1997.
5. Thomas L. Heath, *Diophantus of Alexandria*, Cambridge University Press, New York, 1910.
6. Louis J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
7. Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

EZRA (BUD) BROWN grew up in New Orleans, has degrees from Rice and LSU, and has been at Virginia Tech since 1969, with sabbatical visits to Washington, D.C., and Munich. His research interests include graph theory, the combinatorics of finite sets, and number theory—especially elliptic curves. He received the MAA MD-DC-VA Section's Teaching Award in 1999 and MAA Polya Awards for expository writing in 2000 and 2001. He enjoys singing in operas, playing jazz piano, gardening, talking about his granddaughter, and baking an occasional biscuit for his students.
Virginia Tech, Blacksburg, VA, 24061-0123
brown@math.vt.edu

BRUCE T. MYERS was born in Chicago at a time when violin cases had barely regained their respectability. As a youth, Bruce practiced enough to become employable as a violinist. He played for almost twenty-three years in the U.S. Air Force Orchestra and the U.S. Marine Chamber Orchestra, the latter as a concertmaster. However, Bruce had loved mathematics even before music, so he earned a Ph.D. in mathematics from University of Maryland in 1994. He took his military retirement and now works in the area of cryptographic design at the National Security Agency. He will neither confirm nor deny that he still plays the violin actively, has built and sold over 30 violins, violas, and cellos, and cooks an ornery bowl of chili.
9800 Savage Road, Suite 6511, Ft. George G. Meade, MD 20755-6511
btmyers@orion.ncsc.mil