Finding the Torsion Subgroup of an Elliptic Curve

Michael Logal

April 5, 2023

1 Introduction

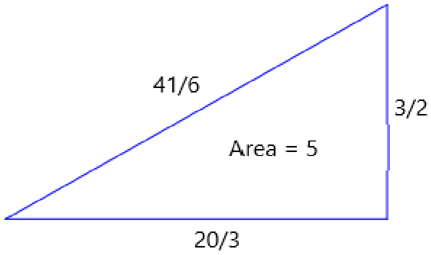
There are many algebraic problems that have roots in certain types of algebraic structures called elliptic curves. One of the more popular problemss is the congruent number problem, which asks for the area of right triangles with rational side lengths. This paper will describe elliptic curves starting from their definition in the projective space (Section 2). The group law and group structure will be defined with the help of examples and some important theorems discovered by Mazur, Nagell, Lutz, and more (Sections 3,4). We will bring the congruent number problem with us along the way and end with proving an interesting fact about these numbers (Section 5).

2 Defining Elliptic Curves

We introduce elliptic curves with examples of some of the seemingly unrelated algebraic problems. First, can you find three (non-zero) rational numbers in an arithmetic sequence whose product is a perfect square? An arithmetic sequence is a sequence of numbers with a common difference. For example, consider the triple $(-9, -4, 1)$. Here, the common difference and product are

$$d = 1 - (-4) = (-4) - (-9) = 5 \qquad \text{and} \qquad p = (1)(-4)(-9) = 36 = 6^2.$$

The second problem is the congruent number problem: suppose the value of d was fixed from the beginning, and try to find a right triangle with rational side lengths and area d. Here is one, with legs a, b and hypotenuse c: $(a, b, c) = \left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$



We have $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = 5$, satisfying all conditions. It may not look like it, but these questions are exactly the same! If we fix d at some value, whenever we have a triangle (a, b, c) with area d, we can generate the pair

$$(x, y) = \left(\frac{db}{c-a}, \frac{2d^2}{c-a}\right),$$

where the arithmetic sequence is $x - d, x, x + d$ and the product is $p = x^3 - d^2x = y^2$. This map is invertible, so for the pair (x, y) with $y \neq 0$ as before,

$$(a, b, c) = \left(\frac{x^2 - d^2}{y}, \frac{2dx}{y}, \frac{x^2 + d^2}{y}\right).$$

Thus, if we want to learn more about one, we automatically gain knowledge about the other.

If we had to choose one of these to study, we would most likely prefer to work with the single equation

$$y^2 = x^3 - d^2x.$$

This is an example of an elliptic curve. We will define exactly what an elliptic curve is soon, but first we need some background information on the projective space.

Definition 2.1 ([1]). *The projective space of degree n over the rationals $\mathbf{Q}$, denoted $\mathbb{P}^n(\mathbf{Q})$ is the set of points $(x_0, x_1, \cdots, x_n)$, not all 0, where two points $(x_0, \cdots, x_n)$ and $(y_0, \cdots, y_n)$ are considered equivalent if there is some $\lambda \neq 0$ such that $x_i = \lambda y_i$ for all i.*

Let's take this piece by piece. For our purposes, it will always be the case that $n = 2$, the projective plane. First, we include all rational triples like $(1, 0, 1)$ and $\left(-\frac{19}{47}, \frac{12}{5}, 1000\right)$, but we exclude $(0, 0, 0)$. Then, we say

$$(x, y, z) \sim (X, Y, Z) \qquad \text{if} \qquad x = \lambda X,\ y = \lambda Y, \text{ and } z = \lambda Z \qquad \text{for some } \lambda.$$

For example, $(1, 0, 1) \sim (3, 0, 3)$ with $\lambda = \frac{1}{3}$, but $(1, 0, 1) \not\sim (1, 1, 0)$. Notice that we can partition the points by whether $z = 0$: we have the points $(x, y, 0)$ and $(x/z, y/z, 1)$ by setting $\lambda = 1/z$. We will use this later.

Definition 2.2 ([1]). *An elliptic curve E defined over a field K is given by an equation in the projective plane of the form*

$$\begin{aligned} E/K : F(X, Y, Z) =& c_0X^3 + c_1X^2Y + c_2XY^2 + c_3Y^3 + c_4X^2Z \\ &+ c_5XYZ + c_6Y^2Z + c_7XZ^2 + c_8YZ^2 + c_9Z^3 = 0 \end{aligned}$$

with each $c_i \in K$ and no singular points. A singular point P is a point where $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$.

There is a lot going on here, but thanks to the Riemann-Roch Theorem (from algebraic geometry), there is a change of variables that allows us to study the equations

$$E : zy^2 = x^3 + Axz^2 + Bz^3$$

We will only use $K = \mathbf{Q}$ the rational numbers. Here, we use the categorization of $z = 0$ and $z = 1$. If $z = 0$, we get $0 = x^3$, so our solutions are $(x, y, z) = (0, y, 0) \sim (0, 1, 0)$ in the projective plane. This will be our "point at infinity." If $z = 1$, we get the curve $y^2 = x^3 + Ax + B$. Generally, when defining E, this is the equation we refer to; the point at infinity is understood to be a solution.

Example 2.3. *The curve $E : y^2 = x^3$ has a singular point, and is thus not an elliptic curve.*

Proof. Here, $F(x, y, z) = y^2z - x^3$. However, $P = (0, 0, 1)$ is on the curve, as $F(P) = 0$, and $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$, so E has a singular point P. □

Remember that we cannot use $P = (0, 0, 0)$ because this point is excluded from the projective plane. Here is a simpler way of finding singular points:

Theorem 2.4 ([1]). *Let $E : y^2 = x^3 + Ax + B = f(x)$ be a curve. There is a singular point P on $F(x, y, z) = y^2 z - x^3 - Axz^2 - Bz^3 = 0$ if and only if there is some x such that $f(x) = f'(x) = 0$.*

Example 2.5. *For any $d \neq 0$, the curve $E : y^2 = x^3 - d^2 x = f(x)$ is an elliptic curve.*

Proof. Here, $f'(x) = 3x^2 - d^2$. Suppose $f'(x) = 0$. Then, $x = \pm \frac{d}{\sqrt{3}}$. In either case, $f(x) = \pm \frac{2d^3}{3\sqrt{3}} \neq 0$. Thus, for any $d \neq 0$, the curve $E : y^2 = x^3 - d^2 x$ is an elliptic curve. □

The form that is used most often for checking if a curve is singular is as follows:

Theorem 2.6 ([1]). *Let $E : y^2 = x^3 + Ax + B$ be a curve. Then E is singular if and only if the value of the discriminant $\Delta_E = 4A^3 + 27B^2 = 0$.*

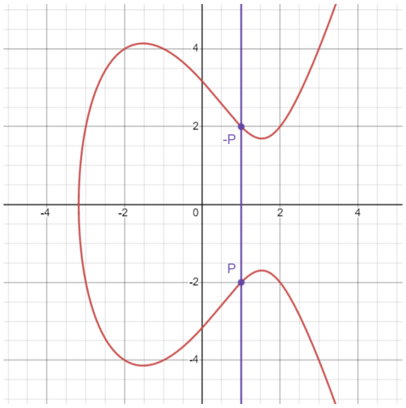
Example 2.7. *The curve $E : y^2 = x^3 - 3x + 2$ contains a singular point.*

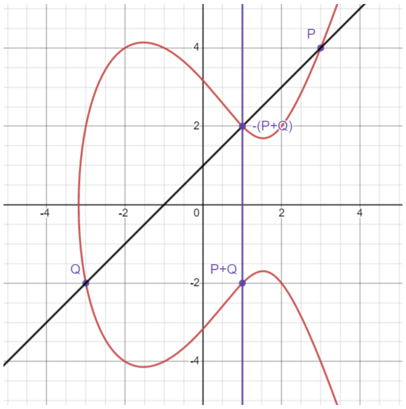
Proof. For this example, $\Delta_E = 4A^3 + 27B^2 = 4(-3)^3 + 27(2)^2 = 0$, so E has a singularity, and is thus not an elliptic curve. □

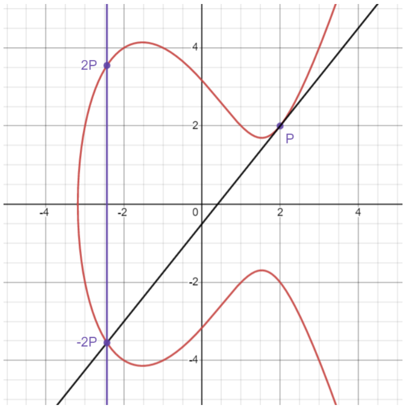
3 Elliptic Curves Group Law

For the rest of this paper, let x and y be functions of points that return the $x-$ and $y-$ coordinates, respectively, so $x(P)$ is the x-coordinate of P and likewise for $y(P)$. We are going to define the group structure on the elliptic curve $E : y^2 = x^3 + Ax + B$. Let P and Q be points on E. Define the inverse $-P = (x(P), -y(P))$, which is also on E. If $P = -Q$, then $P + Q$ is the point at infinity $\mathcal{O}$. Otherwise, let $-(P + Q)$ be the point other than P or Q that the line through P and Q intersects E, counted with multiplicity (i.e., tangents are double counted and inflection points are triple counted). Here are some examples of different scenarios for P and Q, graphed using

Desmos.







These formulas create an abelian group. To formalize this, we rely on the resulting algebraic formulas detailed here.

Theorem 3.1 ([2]). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve, P, Q be points on E, $d = \frac{3x(P)^2+A}{2y(P)}$, $\lambda = \frac{y(P)-y(Q)}{x(P)-x(Q)}$, and $\delta = \frac{y(Q)x(P)-y(P)x(Q)}{x(P)-x(Q)}$. Then, the points of E with the operations*

$$\begin{aligned} -P =&(x(P), -y(P)) \\ P + (-P) =&\mathcal{O} \\ P + P =&(d^2 - 2x(P), -y(P) - d(d^2 - 3x(P))) && \textit{if } P \neq -P \\ P + Q =&\big(\lambda^2 - x(P) - x(Q), -\lambda(\lambda^2 - x(P) - x(Q)) - \delta\big) && \textit{if } x(P) \neq x(Q) \end{aligned}$$

form an abelian group.

Given that the outputs of the function all lie on E, we can confirm that the operations are well-defined because $P = -P$ exactly when $y(P) = 0$, and $x(P) = x(Q)$ exactly when $P = \pm Q$.

Furthermore, it should be clear from the geometric description that the group is abelian because the lines $\overline{PQ} = \overline{QP}$.

Example 3.2. *Let $E : y^2 = x^3 - 1$ and $P = (1, 0)$. Then $-P = (1, 0) = P$, so $2P = \mathcal{O}$.*

Example 3.3. *Let $E : y^2 = x^3 - 2$ and $P = (3, 5)$. Then $d = \frac{27}{10}$ and*

$$2P = \left(\left(\frac{27}{10}\right)^2 - 2(3), -5 - \frac{27}{10}\left(\left(\frac{27}{10}\right)^2 - 3(3)\right)\right) = \left(\frac{129}{100}, -\frac{33683}{1000}\right)$$

Example 3.4. *Let $E : y^2 = x^3 - 5x$, $P = (5, 10)$, and $Q = (0, 0)$. Then $\lambda = 2$, $\delta = 0$, and*

$$P + Q = \left(2^2 - 5 - 0, -2\left(2^2 - 5 - 0\right) - 0\right) = (-1, -2)$$

Example 3.5. *Let $E : y^2 = x^3 - 25x$ ad $P = (-4, 6)$. Then $d = \frac{23}{12}$, so*

$$2P = \left(\frac{1681}{144}, -\frac{62279}{1728}\right)$$

If we go back to the map from section 1, we find a right triangle with area 5 given by the side lengths

$$(a, b, c) = \left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$$

4 Elliptic Curves Group Structure

One of the most natural question to ask when a family of groups is discovered is that of their structures. There are many open questions about the group structure of a general elliptic curve over **Q**, and many more if we allow look at any field. Fortunately, many of these questions have been answered. We will start with arguably the most important one.

Theorem 4.1 (Mordell-Weil, [2])**.** *The group over an elliptic curve E is finitely generated*

As a refresher, a finitely generated abelian group E is an abelian group such that there is a finite set $\{P_1, P_2, \cdots, P_m\}$ of elements of E where any $Q \in E$ can be written as $Q = n_1P_1 + \cdots + n_mP_m$ for integers n_i.

Corollary 4.2. *For any finitely generated abelian group E, there is a finite group E_{tors} and a non-negative integer r such that*

$$E \cong E_{tors} \times \mathbb{Z}^r.$$

The integer r is called the rank of E. The group E_{tors} is called the torsion subgroup of E. The points of finite order in E are called the torsion points.

Most of the open problems regarding elliptic curves have to do with rank. For example,

Exercise 4.3. *For any non-negative integer r, is there an elliptic curve E such that the rank of E is equal to r? If not, which values of r can be achieved?*

The largest known rank of an elliptic curve is 28.

Although the possibilities for the rank of elliptic curves is not completely known, the list of possibilities for the torsion subgroup is known.

Theorem 4.4. *If P and Q are torsion points on E, then $P + Q$ is also a torsion point.*

Proof. Since P is a torsion point, there is some integer a such that $aP = \mathcal{O}$. Similarly, there is b such that $bQ = \mathcal{O}$. Then, since E is abelian,

$$\begin{aligned} ab(P+Q) =& abP + abQ \\ =& b(aP) + a(bQ) \\ =& b\mathcal{O} + a\mathcal{O} \\ =& \mathcal{O} \end{aligned}$$

Thus $P + Q$ is a torsion point, as well. □

Corollary 4.5. *For a torsion point P on E and an integer n, nP is also a torsion point.*

Proof. Since P is torsion, $-P$ is also, with the same order as P. Since $nP = P + P + \cdots P$ or $nP = -(P + P + \cdots + P)$, the corollary follows from Theorem 3.3. □

Theorem 4.6 (Mazur, [1])**.** *For an elliptic curve $E/\mathbf{Q}$, the torsion subgroup of E is one of the following*

$$\mathbb{Z}/m\mathbb{Z} \qquad \textit{for some } 1 \leq m \leq 10 \textit{ or } m = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \qquad \textit{for some } 1 \leq m \leq 4$$

Note that if $E_{tors} \cong \mathbb{Z}/1\mathbb{Z}$, then E is made up of only $\mathcal{O}$ and points in the rank, since $\mathbb{Z}/1\mathbb{Z}$ is a trivial group.

Example 4.7 ([1])**.** *The following is a table of elliptic curves with every possible torsion.*

Curve	*Torsion*
$y^2 = x^3 - 2$	$\{\mathcal{O}\}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$y^2 + 5xy - 6x = x^3 - 3x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

5 Finding the Torsion Subgroup

There are many ways of discovering the torsion subgroup for a specific elliptic curve. A straightforward algorithm to do this is due to T. Nagell and E. Lutz:

Theorem 5.1 (Nagell-Lutz, [1]). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with A and B integers. Suppose P is a torsion point of E other than $\mathcal{O}$. We have*

1. *The coordinates $x(P)$ and $y(P)$ are integers.*

2. *If P has order 2, then $y(P) = 0$ and $x(P)^3 + Ax(P) + B = 0$.*

3. *If P has order greater than or equal to 3, then $y(P)^2$ divides $\Delta_E = 4A^3 + 27B^2$*

However, if $4A^3 + 27B^2$ is large, this theorem loses practicality due to the computational difficulty of factoring large numbers. Proofs about families of elliptic curves using this theorem often utilize number theory, as in examples 4.2 and 4.3.

Example 5.2 ([1]). *Let $E : y^2 = x^3 - 2$. The only torsion point on E is $\mathcal{O}$.*

Proof. We have $A = 0$ and $B = -2$, so $\Delta_E = 4 \cdot 27$. Suppose P is a torsion point of order 2. Then $x(P)^3 - 2 = 0$. However, $\sqrt[3]{2}$ is not an integer, so such a P cannot exist. Now, suppose P is a torsion point of order greater than 2. Then $y(P)^2$ divides 54, so $y(P)^2$ is one of 1, 4, 9, or 36. Since $y(P)^2 = x(P)^3 - 2$, this means $x(P)^3$ is one of 3, 6, 11, or 38. Since none of these is a cube number, there cannot be a torsion point P on E other than $\mathcal{O}$. □

We could have immediately seen that the point $(3, 5)$ on E was not a torsion point because $(3, 5) + (3, 5) = (\frac{129}{100}, -\frac{33683}{1000})$, which is not a torsion point because the coefficients are not integers.

Example 5.3. *Let $p \geq 2$ be a prime number, and let $E_p : y^2 = x^3 + px$. Then $E_{tors} \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. In this example, $\Delta_p = 4p^3$. If Q is a point of order 2, then $x(Q)^3 + x(Q)p = 0$, which only has solution $x(Q) = 0$. Thus the point $(0, 0)$ is the only torsion point of order 2. Now, suppose Q is a point of order larger than 2. Then $y(Q)^2$ divides $4p^3$, so $y(Q)^2$ is one of 1, 4, p, $4p$. Note that if $x(Q) < 0$, then $y(Q)^2 = x(Q)^3 + px(Q) = x(Q)(x(Q)^2 + p) < 0$, so we must have $x(Q) \geq 0$. We check these one at a time:

- Suppose $y(Q)^2 = 1$. Then $x(Q)(x(Q)^2 + p) = 1$, so $x(Q) = 1$ and $x(Q)^2 + p = 1$. However, this means $p = 0$, so we have a contradiction.

- Suppose $y(Q)^2 = 4$. Then $x(Q)(x(Q)^2 + p) = 4$, so we have one of the following.
    - ○ $x(Q) = 1$ and $x(Q)^2 + p = 4$
    - ○ $x(Q) = 2$ and $x(Q)^2 + p = 2$
    - ○ $x(Q) = 4$ and $x(Q)^2 + p = 1$

  In the last two cases, p is an imaginary value, which is a contradiction. In the first case, we have a solution with $p = 3$, so E_3 contains the integer points $(1, \pm 2)$.

- Suppose $y(Q)^2 = p^2$. Then $x(Q)^3 + px(Q) = p^2$. Since p divides both p^2 and $px(Q)$, we must have p dividing $x(Q)^3$, so p also divides $x(Q)$. We then have $x(Q) \geq p$, so $x(Q)^3 + px(Q) \geq p^3 + p^2 > p^2$. This is another contradiction.

- Finally, suppose $y(Q)^2 = 4p^2$. Then $x(Q)^3 + px(Q) = 4p^2$. By the same argument, $x(Q) \geq p$. Then for $p \geq 5$, $x(Q)^3 + px(Q) \geq p^3 + p^2 > 4p^2$, which is a contradiction. We check $p = 2$ and $p = 3$ individually. If $p = 2$, then we have $x(Q)^3 + 2x(Q) = 16$, which has no solutions. If $p = 3$, then $x(Q)^3 + 3x(Q) = 36$, which has solution $x(Q) = 3$. Thus when $p = 3$, there are integer points $(3, \pm 6)$.

Thus for $p \neq 3$, we can conclude E_p has torsion subgroup $\mathbb{Z}/2\mathbb{Z}$. What about $p = 3$? Here, we notice that Theorem 5.1 is not an if and only if statement. We still need to check that $(1, \pm 2)$ and $(3, \pm 6)$ are torsion points. To do this, we calculate

$$\begin{aligned} 2(1,2) =& (0.25, -0.875) \\ 2(1,-2) =& (0.25, 0.875) \\ 2(3,6) =& (0.25, 0.875) \\ 2(3,-6) =& (0.25, -0.875) \end{aligned}$$

If the integer points were torsion, then doubling them would only provide torsion points by Theorem 4.2. However, since the doubled values are not integer values, they are not torsion. Thus none of the potential points for $p = 3$ are actually torsion. Thus, for any value of p, the torsion subgroup of E_p is $\mathbb{Z}/2\mathbb{Z}$. □

Theorem 5.4. *For any positive integer d, the curve $E : y^2 = x^3 - d^2x$ has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*

Proof. We can see that $(0, 0)$ and $(\pm d, 0)$ are torsion points of order 2 because applying the doubling formula returns $\mathcal{O}$, so the torsion subgroup E_{tors} has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus the only options are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ for $m = 1, 2, 3, 4$. We first show $m = 3$ is not possible.

Suppose P is a point of order 3. If $m = 3$, then one must exist. Then $3P = \mathcal{O}$, so $y(2P) = y(-P)$. Applying the formulas gives

$$-y(P) - \frac{3x(P)^2 - d^2}{2y(P)}\left(\left(\frac{3x(P)^2 - d^2}{2y(P)}\right)^2 - 3x(P)\right) = -y(P)$$

After canceling the $-y(P)$, we conclude one of the following

- $3x(P)^2 - d^2 = 0$
- $\left(\frac{3x(P)^2 - d^2}{2y(P)}\right)^2 - 3x(P) = 0$

In the first case, we get $\frac{d}{x(P)} = \sqrt{3}$, which cannot happen since $\sqrt{3}$ is irrational. In the second case, we expand to get

$$(3x(P)^2 - d^2)^2 = 12x(P)y^2(P)$$

Since $(x(P), y(P))$ is on E, we have $y(P)^2 = x(P)^3 - d^2x(P)$. Substituting this back in, we get

$$\begin{aligned} 9x(P)^2 - 6x(P)^2d^2 + d^4 =& 12x(P)^2(x(P)^2 - d^2) \\ -3x(P)^4 + 6x(P)^2d^2 - d^4 =& 0 \\ (3x(P)^2 + d^2)^2 =& 3(2x(P)^2)^2 \end{aligned}$$

Since $\sqrt{3}$ is still irrational, this is also a contradiction.

We move onto the cases $m = 2$ and $m = 4$. In either case, there is a point P of order 4, so $2P$ has order 2, so $y(2P) = 0$. We expand with the doubling formula to get

$$-y(P) - \frac{3x(P)^2 - d^2}{2y(P)}\left(\left(\frac{3x(P)^2 - d^2}{2y(P)}\right)^2 - 3x(P)\right) = 0$$

After clearing the fractions and substituting $y(P)^2 = x(P)^3 - d^2x(P)$, we find

$$-(3x(P)^2 - d^2)\left((3x(P)^2 - d^2)^2 - 12x(P)^2(x(P)^2 - d^2)\right) = 2x(P)^2(x(P)^2 - d^2)^2$$

Let $n = x(P)^2 - d^2$ and $t = x(P)^2$. Then

$$-(n + 2t)((n + 2t)^2 - 12nt) = 2n^2t$$

In mod 2, we get $n^3 \equiv 0$, so n is even. Let $n = 2k$. After some algebra, we can find

$$t^3 - 3t^2k - 2tk^2 + k^3 = 0$$

We can rearrange this to $(t - k)^3 = k^2(5t - 2k)$. Suppose $t \neq k \mod 2$. Then either $t \equiv 0$ or $k \equiv 0$, so $k^2(5t - 2k) \equiv 0$. Then $t - k \equiv 0$, and $t \equiv k$, which is a contradiction. Thus, $t \equiv k$. If $t \equiv k \equiv 1$, then we have $(t - k)^3 \equiv 0$, but $k^2(5t - 2k) \equiv 1$, so $t \equiv k \equiv 0$. If we let $t = 2t_0$ and $t = 2t_0$, and substitute, we again have $(t_0 - k_0)^3 = k_0^2(5t_0 - 2k_0)$. However, this means t_0 and k_0 are even. This can go on forever, so every power of 2 divides t and k. This only happens when $t = k = 0$. Going back in substitutions, we find $d = 0$, which is a contradiction, since d was assumed to be positive. Thus $m = 2$ and $m = 4$ lead to contradictions, so we have $m = 1$. Thus the torsion subgroup $E_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Corollary 5.5 (The Boss). *If the area of a rational right triangle with side lengths (a, b, c) is d, as in section 1, then there is an infinite family of rational right triangles that also have area d.*

Proof. Suppose P is the solution to $E : y^2 = x^3 - d^2x$ corresponding to the triangle (a, b, c). We know $y(P) \neq 0$, since the degenerate solutions are excluded. Since the torsion subgroup of E is exactly $\{\mathcal{O}, (0, 0), (\pm d, 0)\}$, we know P is not a torsion point of E. Thus, there are triangles corresponding to the points $P, 2P, 3P, \cdots$. □

6 Conclusion

We started with a question about triangles, and through some quite abstract mathematics, ended with a sizable claim about the existence of such triangles. Along the way, we defined an elliptic curve, found a group law attached to it, defined the rank and torsion of a curve, and did many examples of finding the torsion subgroup.

References

[1] Álvaro Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. Student mathematical library. IAS/Park City mathematical subseries; v. 58. American Mathematical Society, Providence, R.I, 2011.

[2] Joseph H. Silverman. *The arithmetic of elliptic curves*. Graduate texts in mathematics ; 106. Springer-Verlag, New York, 1986.