

Elliptic Curves: An Introduction

Adam Block

December 2016

1 Introduction

The goal of the following paper will be to explain some of the history of and motivation for elliptic curves, to provide examples and applications of the same, and to prove and discuss the Mordell theorem. As [1] mentions, the motivation for developing a theory of elliptic curves comes from the attempts at finding solutions to elementary problems in number theory. One such problem is the congruent numbers problem. We have

Definition 1. *An natural number $n \in \mathbb{N}$ is called congruent if it is the area of a right triangle with rational side lengths, i.e. there exist $x, y, z \in \mathbb{Q}$ such that $x^2 + y^2 = z^2$ and $\frac{1}{2}xy = n$.*

For example, we note that 6 is congruent because the triangle of sides (3, 4, 5) has area 6. On the other hand, it can be proven easily by the method of infinite descent that 1 is not a congruent number. A natural question that arises is to classify which natural numbers n are congruent. As it turns out, this problem can be translated into the language of elliptic curves, and a solution resting upon the still open conjecture of Birch and Swinnerton-Dyer has been presented.

Our other motivating example of how elliptic curves are useful tools comes to us from Fermat. Popularly known as "Fermat's Last Theorem" the following conjecture was finally proven by Andrew Wiles and Richard Taylor in the late 20th century.

Theorem 1 (Fermat's Last Theorem). *There are no nontrivial solutions to the equation $x^n + y^n = z^n$ over the integers for $n > 2$, i.e., for $n > 2$ there do not exist $x, y, z \in \mathbb{Z}$ such that $x^n + y^n = z^n$ and $xyz \neq 0$.*

The proof of this goes far beyond the scope of the present paper but we consider the following special case:

Proposition 1. *There are no nontrivial solutions over the integers to the equation $x^4 + y^4 = z^4$*

While this proof is actually quite easy by elementary means, it serves as an example of the power of elliptic curves to solve problems from elementary number theory. First, though, we need to define elliptic curves.

2 Elliptic Curves: Elementary Definitions

Elliptic curves can be defined over any field k but in general we will be considering them over \mathbb{Q} because that is where the elementary applications of the theory are coming from. We will take the approach of [2] because it seems more natural than that of [1] as a result of it being slightly more geometric. We begin with the definition of a plane curve.

Definition 2. *Let $f \in K[x, y]$. We let the plane curve of f over K be*

$$C_f(K) = \{(a, b) \in K^2 \mid f(a, b) = 0\}$$

We say the curve $C_f(K)$ is irreducible if f is irreducible; similarly, the degree of the curve is the degree of the polynomial defining it.

There is much theory to be built up around plane curves, including the theory of resultants, intersection numbers, and genus, with results such as Riemann-Roch and Bezout's theorem that are required for a more advanced treatment of the subject. In the interest of brevity, we will skip much of this in order to get to the heart of the matter. One thing that needs to be mentioned, though, is projective space. Let $(x_0, x_1, \dots, x_n) \in \mathbb{A}^{n+1}$ and we define an equivalence relation on $\mathbb{A}^{n+1} - \{0\}$, such that $(x_0, x_1, \dots, x_n) \sim (\lambda x_0, \lambda x_1, \dots, \lambda x_n)$ where $\lambda \in K^\times$. Now we are prepared to define projective space.

Definition 3. Over some field K with the equivalence relation defined above, we let $\mathbb{P}^n = (\mathbb{A}^{n+1} - \{0\}) / \sim$. Because ratios are all that is important in projective space, we often use the notation $(x_0 : x_1 : \dots : x_n)$ to denote the equivalence class of (x_0, x_1, \dots, x_n)

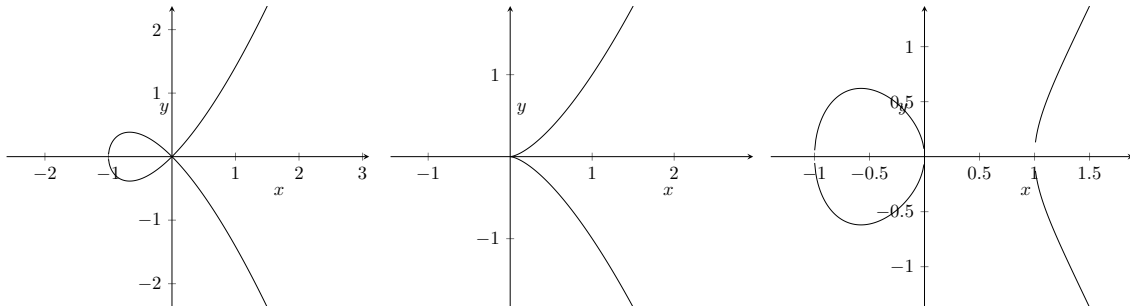
Note that any polynomial in $K[x, y]$ can be turned into a homogeneous polynomial in $K[x, y, z]$ simply by multiplying by powers of z on each term to equalize total degree. Also, while polynomials are not in general well-defined functions over projective space, homogeneous polynomials have well-defined zeroes because if f is homogeneous of degree d and $X = (x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n) = X'$ then $f(X') = \lambda^d f(X)$. Also, we can identify any point $(x, y) \in \mathbb{A}^2$ with a point in \mathbb{P}^2 by sending $(x, y) \mapsto (x : y : 1)$; thus it makes sense to define plane curves over \mathbb{P}^2 by simply homogenizing the function that defines a plane curve over \mathbb{A}^2 . We will frequently make use of this ability to switch between affine and projective space. We are now prepared to define elliptic curves, combining the definitions of [1] and [2].

Definition 4. For K a field, an elliptic curve is a nonsingular cubic curve of genus 1, or, equivalently, is the set of solutions over K to the following

$$y^2 = ax^3 + bx^2 + cx + d$$

where $a \neq 0$ and the polynomial in x does not have a multiple root.

Below are two examples of cubic curves that are not elliptic curves, the first being $y^2 = x^3 + x^2$ and the second being $y^2 = x^3$ and one example of an elliptic curve defined by $y^2 = x^3 - x$.



Note that the two are not elliptic because they are both singular, but that $x^3 - x = x(x^2 - 1) = x(x-1)(x+1)$ has no multiple root so does define an elliptic curve. As cited in [1], it is a theorem of Mordell and Siegal that elliptic curves over \mathbb{Q} have finitely many integral points. Thus, one can show that the latter curve is not elliptic by noting that if $n \in \mathbb{Z}$, then $(n^2, n^3) \in E(\mathbb{Q}) \cap \mathbb{Z}^2$ so there are infinitely many integral points, violating the above theorem of Mordell and Siegal. An example of an elliptic curve is the zero set of $y^2 = x^3 + x$ over \mathbb{Q} . We are now ready to develop some of the theory, in particular the all important group law.

3 Elliptic Curves as Abelian Groups

One of the reasons that we choose degree 3 curves is that we can introduce a binary operation that turns each elliptic curve into an Abelian group. With this group structure, we can translate many elementary number theory problems into more abstract language and bring in insight from group theory to provide solutions. In order to do this, we first have to define a group law. We first introduce the point O , heuristically a point "at infinity," and let $E(K) = \{(x, y) \in K^2 | f(x, y) = 0\} \cup \{O\}$. This is the affine description, but it will be easier

to follow [2] and translate into projective space, because then we get a better picture of what O is. Using the results from above about projective space, and letting f be the homogenized polynomial that defines a nonsingular cubic curve, we can also consider the elliptic curve in projective space.

$$E(K) = \{(x : y : 1) \in \mathbb{P}^2 \mid f(x : y : 1) = 0\} \cup \{(0 : 1 : 0)\}$$

We are now ready to define the group law. It is natural to let O be the identity, and if we consider points on the actual curve, a natural generalization from the case $K = \mathbb{Q}$ will occur. When $K = \mathbb{Q}$, we can consider the curve embedded in \mathbb{R}^2 and a natural operation would be to take any two points, $P, Q \in E(\mathbb{Q})$ that have different abscissae and draw the secant line between them, \overline{PQ} and then see where this line intersects the elliptic curve a third time. If they are the same point, then the natural change is to use the tangent line. Doing this, we note that the line \overline{PQ} has an equation $y = mx + r$ where $m, r \in \mathbb{Q}$ so we are solving a system of equations

$$\begin{aligned} y &= mx + r \\ y^2 &= ax^3 + bx^2 + cx + d \end{aligned}$$

Substituting in for y we get some $g(x) \in \mathbb{Q}[x]$ of degree 3. We know that two roots of $g(x)$ are the abscissae of P and Q and it is a well known fact that a cubic polynomial with two roots in the field must have its third root in the field as well. But if the abscissa of a line with rational slope and intercept is rational then so is the ordinate, so we get a third point, that we will, after the convention of [2], call PQ . We then call $PQ = Q$ where Q has the opposite ordinate as P for all points P . Finally, if the line \overline{PQ} is vertical, we let $PQ = O$. We might naively try to assert that this operation defines a group, but, alas, it fails associativity. In order to get associativity, let $P+Q = O(PQ)$. We will show that this addition turns $E(K)$ into an abelian group. Note that it is in this construction that the benefits of introducing projective space are warranted. In \mathbb{P}^2 , all lines intersect, so instead of using casework, we simply define PQ as the other intersection of the line \overline{PQ} with $E(K)$, thus making our new operation far more natural. We now show that under addition, we do indeed have a group, but first, we need a lemma.

Lemma 1. *If two cubic curves in \mathbb{P}^2 intersect in exactly nine points, then every cubic curve in \mathbb{P}^2 that passes in eight of the points also passes through the ninth.*

Proof. The proof of this is not difficult, and, though interesting, is tangential at best to the topic of this exposition, so we omit it and refer the reader to [2][pp. 27-28]. ■

We now prove the main result of the section.

Theorem 2. *With the above binary operation, with K a field, $(E(K), +)$ is an abelian group with identity O .*

Proof. We proceed as in [2]. Note first that if $E(K)$ is a group then it is clearly abelian because nowhere above did the order of the points matter. We first show that O is the identity; this is obvious though because $O \cdot : E(K) \rightarrow E(K)$ takes $P(x : y : 1)$ to $P'(x : -y : 1)$ which is an involution so $O + P = O(OP) = P$. Also we note that OP is an inverse for P , i.e. $OP + P = O$, which is clear by construction. Thus it suffices to show that this addition is associative. To do this, we follow [2] and consider addition in projective space. We wish to show that for any points $P, Q, R \in E(K)$, we have $(P + Q) + R = P + (Q + R)$. Let $S = (P + Q)R$ and $T = P(Q + R)$. Then we have $(P + Q) + R = OS$ and $P + (Q + R) = OT$ by definition, so it will suffice to show that $S = T$. Viewing lines as homogeneous polynomials, it makes sense to define multiplication of lines by multiplication of their defining functions in $K[x, y, z]$, so we consider the following three equations:

$$\begin{aligned} f(x : y : z) &= 0 \\ \overline{PQ} \cdot \overline{R(P+Q)} \cdot \overline{(QR)O} &= 0 \\ \overline{P(QR)} \cdot \overline{QR} \cdot \overline{PO} &= 0 \end{aligned}$$

Note that they are all cubic over \mathbb{P}^2 and all pass through the eight points $O, P, Q, R, PQ, QR, P+Q, Q+R$ and that the last two also pass through $T' = \overline{P(Q+R)} \cap \overline{(P+Q)R}$ which is a point because we are working in projective space. By Lemma 1, then, we have $S = T = T'$ and associativity holds. ■

The above proof of associativity was not terrible in that it had some geometric motivation, but much of the technical problem of the intersection theory in projective space was omitted by citing Lemma 1. Another proof follows directly from the Riemann-Roch theorem, but again, this is outside the scope of this paper. The interested reader should direct his attention to [2][pp. 34-35].

4 Abelian Group Structure

From the above discussion, we know that $E(K)$ is an abelian group, but the natural next question is one of structure. The remarkable theorem of Mordell says that this group is actually finitely generated, a theorem that will be proven below. From the classification of finitely generated abelian groups, if $T = \text{Tor}(E(\mathbb{Q}))$ is the torsion subgroup, which is finite, then we have $E(K) = \mathbb{Z}^r \oplus T$ for some $r \geq 0$. Little is known about the rank of the group of a general elliptic curve, but the conjecture of Birch and Swinnerton-Dyer involves the determination of this rank. Much more is known about T , and in fact, as [1] mentions, Mazur proved that T is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$ or to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for $n \in \{2, 4, 6, 8\}$ and, indeed, that each of these occurs as the torsion subgroup of some elliptic curve. This section will be devoted to proving the theorem of Mordell. We need the notion of height to do this.

Definition 5. Let $q = \frac{m}{n} \in \mathbb{Q}$ be a fraction in lowest terms. We let the height of q be $H(q) = \max(|m|, |n|)$ where $\gcd(m, n) = 1$ by q being reduced. If $P(x : y : 1)$ is some point, then we define $H(P) = H(x)$.

We now follow [1] and prove the following theorem:

Theorem 3 (Mordell). If $E(\mathbb{Q})$ is an elliptic curve then the abelian group $(E(\mathbb{Q}), +)$ is finitely generated.

The above proof rests on a few facts that will be proven independently. First is the weak Mordell theorem that states that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Second is certain properties of how the height function interacts with the group composition. In particular, we note that

$$S_C = \{P \in E(\mathbb{Q}) \mid H(P) \leq C\}$$

is finite for all C , which follows because the set of rationals with bounded height is finite and S_C is just a subset of this. Secondly, we assert the existence of some real number C that satisfies for all $P, Q \in E(\mathbb{Q})$:

$$C \cdot H(P) \geq H(P)^4 \tag{1}$$

$$C \cdot H(P) \cdot H(Q) \geq \min(H(P+Q), H(P-Q)) \tag{2}$$

Given the above two facts, we can prove Mordell's theorem with some ease as follows. The key here is that if $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, then we can choose $Q_1, \dots, Q_n \in E(\mathbb{Q})$ such that $\{Q_1, \dots, Q_n\}$ surjects onto $E(\mathbb{Q})/2E(\mathbb{Q})$ by the projection map. We let M be the maximum height of any of the Q_i and claim that S_M generates $E(\mathbb{Q})$. Note that by the observation above, S_M is finite, so this suffices to prove the theorem. To show this, suppose there were some $P_0 \in E(\mathbb{Q})$ that is not generated by the elements in S_M such that the height of P_0 is minimal. Then clearly $H(P_0) > M$ because otherwise $P_0 \in S_M$. Because $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, we can take some i such that P_0 and Q_i agree in $E(\mathbb{Q})/2E(\mathbb{Q})$. But then we have that $P_0 - Q_i \in 2E(\mathbb{Q})$ and so $P_0 - Q_i + 2Q_i = P_0 + Q_i \in 2E(\mathbb{Q})$. Let Q be the one of $P_0 + Q_i$ and $P_0 - Q_i$ such that the height of Q is smaller and let $P_1 \in E(\mathbb{Q})$ such that $2P_1 = Q$. By part (1) of the height relations we have $H(P_1)^4 \leq CH(Q) \leq MH(Q)$ and we also have $H(Q) \leq CH(P_0)H(Q) \leq M^3H(P_0)$. Combining we get $H(P_1)^4 \leq M^3H(P_0)^4 < H(P_0)^4$ because $H(P_0) > M$, so $H(P_1) < H(P_0)$. But by minimality of P_0 we get that P_1 can be generated by elements in S_M and solving for P_0 in terms of P_1 we see that then P_0 can be generated by elements from S_M so we have a contradiction and Mordell's theorem holds.

Thus it remains to prove the above assertions. The proof of existence of such a C is quite technical and involved and is hardly germane in anything but its conclusion; for this reason, we refer the interested reader to [1][pp. 35-42] for a clear exposition on the proof and simply take the result on faith. Similarly, the weak Mordell theorem for general elliptic curves is more subtle than we are prepared to deal with in this paper, so we prove it for a special case.

Proposition 2 (Weak Mordell). *If we have distinct $a, b, c \in \mathbb{Q}$, we have an elliptic curve, E , defined by*

$$y^2 = (x - a)(x - b)(x - c)$$

Then, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Unfortunately, the following proof, after [1], is rather unintuitive, particularly in the definition of δ . It does hold, however, and we can use this to get an idea of how to prove the general case.

Proof. The goal of this proof is to define a morphism $\delta : E(\mathbb{Q}) \rightarrow (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \times (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \times (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)$ with kernel $2E(\mathbb{Q})$ and finite image. We let $\bar{}$ denote passage to the quotient by $(\mathbb{Q}^\times)^2$. If $P \neq O$ is some point on $E(\mathbb{Q})$, let x be the abscissa. Then we define δ as follows:

$$\delta(P) = \begin{cases} (\overline{(x-a, x-b, x-c)}) & P \notin \{O, (a, 0), (b, 0), (c, 0)\} \\ (\overline{((a-b)(a-c), a-b, a-c)}) & P = (a, 0) \\ (\overline{(b-a, (b-a)(b-c), b-c)}) & P = (b, 0) \\ (\overline{(c-a, c-b, (c-a)(c-b))}) & P = (c, 0) \\ (1, 1, 1) & P = O \end{cases}$$

We claim that δ is a homomorphism with kernel $2E(\mathbb{Q})$ and that, moreover, the image of δ is contained in $G \times G \times G$, where G is the subgroup of $(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)$ that is generated by all prime factors of $a-b, b-c, c-a$ and -1 . Note in particular that G is finite so if the above claim holds then so does the proposition by the first isomorphism theorem. To show that δ is a homomorphism is easy but involves casework. It also involves solving for an explicit formula for $P + Q$ in terms of the coordinates of P and Q , which is, again, easy but technical. As a result of this, we will leave it as an exercise for the reader to check that δ is indeed a homomorphism.

The fact that the kernel of δ is $2E(\mathbb{Q})$ follows directly from a result in our subsequent discussion of the congruent numbers problem, but the basic idea is that for any field K , if the cubic polynomial in x splits over K then the image of the multiplication by 2 map of $E(\mathbb{Q})$ consists of those points whose x coordinates differ from squares in K by the roots of the cubic. The actual proof involves the fact that a determined bijection between the following two sets

$$B = \{(x, y, z) \in K^3 \mid x^2 + a = y^2 + b = z^2 + c\}$$

$$C = \{(x, y) \in K^2 \mid y^2 = (x - a)(x - b)(x - c)\} - \{(a, 0), (b, 0), (c, 0)\}$$

appears as the multiplication by 2 map on the abelian group but the explicit construction of this map is technical and not particularly illuminating. The interested reader should refer to [1][p. 21].

To prove the last part, we let $ord_p(\frac{m}{n})$ be the p -adic valuation of $\frac{m}{n}$. It suffices to show that for any prime p that divides none of $a-b, b-c, c-a$, $_p(x-a)$, $_p(x-b)$, and $_p(x-c)$ are all even because then their image under δ is 1. By $y^2 = (x-a)(x-b)(x-c)$ we have that $ord_p(x-a) + ord_p(x-b) + ord_p(x-c) = 2ord_p(y)$ is even. If one of these orders is negative then because the order of the difference of any two of them is 0 because p does not divide any of $a-b, b-c, c-a$, then they are all the same. But then $3 \cdot ord_p(x-a)$ is even so $ord_p(x-a) = ord_p(x-b) = ord_p(x-c)$ must all be even. Now suppose that one of the orders is positive. By the same argument of the differences of the order being zero and applying the fact that $ord(r-s) = \min(ord(r), ord(s))$ if $ord(r) \neq ord(s)$ we get that the other two orders are zero and again they are all even. Thus in the quotient by perfect squares these elements go to the identity and we get that the image of δ is inside of $G^{\times 3}$ as desired. ■

We have only briefly touched on the group structure of elliptic curves, but many more results are known and it is still an area of active research. In particular, the conjecture of Birch and Swinnerton-Dyer relating the rank of the group to the growth order of a certain function remains open and one of the most important problems in modern number theory. Many other results come by way of algebraic geometry and the study of more general abelian varieties, as hinted at by our mention of the theorem of Riemann and Roch, but this is far beyond the scope of this paper. To conclude, we return to the two motivating problems and describe the way in which elliptic curves have helped in the search for their answers.

5 Motivating Problems: A Second Look

5.1 Fermat's Last Theorem

We first examine the special case of Fermat's last theorem for $n = 4$. The first step is to translate the problem into the language of elliptic curves. Let us suppose that there exists some solution $x^4 + y^4 = z^4$ in the integers with $y \neq 0$. Then we can move y^4 to the other side and multiply by $\frac{z^2}{y^6}$ to get

$$\begin{aligned}\frac{z^2}{y^6}x^4 &= \frac{z^2}{y^6}z^4 - \frac{z^2}{y^6}y^4 \\ \left(\frac{x^2z}{y^3}\right)^2 &= \left(\frac{z^2}{y^2}\right)^2 - \frac{z^2}{y^2} \\ y'^2 &= x'^3 - x'\end{aligned}$$

Where

$$\begin{aligned}x' &= \frac{z^2}{y^2} \\ y' &= \frac{x^3z}{y^3}\end{aligned}$$

Note that all of the above steps are reversible so we have a solution over the integers to $x^4 + y^4 = z^4$ with not all $x, y, z = 0$ if and only if we have a solution to $y'^2 = x'^3 - x'$ over \mathbb{Q} . It is now a relatively easy proof by the method of infinite descent to show that the only rational points on this curve are $(0, 0)$ and $(\pm 1, 0)$, the exposition of which we leave to [1][pp. 22-24]. The more general case is obviously much more difficult, but follows from the proof of a conjecture of Taniyama and Shimura by Andrew Wiles and Richard Taylor.

5.2 Congruent Numbers

We conclude with a brief discussion of the congruent numbers problem introduced in the introduction. The problem is still unsolved because the solution rests upon the conjecture of Birch and Swinnerton-Dyer. We first wish to translate the problem into one involving elliptic curves. To do this, we introduce three sets, letting $d \in \mathbb{Q}$:

$$\begin{aligned}A_d &= \{(x, y, z) \in \mathbb{Q}^3 \mid x^2 + y^2 = z^2, \frac{1}{2}xy = d\} \\ B_d &= \{(u, v, w) \in \mathbb{Q}^3 \mid u^2 + d = v^2, v^2 + d = w^2\} \\ C_d &= \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - d^2x, y \neq 0\}\end{aligned}$$

The observant reader will note that C_d determines an elliptic curve. We note, as [1] does, that the three sets are in bijection with $f : A_d \rightarrow B_d$, and $g : B_d \rightarrow C_d$. The fact mentioned in the proof of the second part of Proposition 2 follows directly from the proof that there exists such a bijection g and can be found in [1][p. 21]. Thus, we have transformed the elementary problem of congruent numbers into one of finding nontrivial rational points on the elliptic curve $y^2 = x^3 - d^2x$. While not easy, the group structure of the curve gives the mathematician much more material to work with. Indeed, we have the following result, the proof of which, alas, far exceeds the current scope.

Theorem 4 (Tunnell). *Assuming the conjecture of Birch and Swinnerton-Dyer, the odd squarefree integer n is congruent if and only if the number of triples $(x, y, z) \in \mathbb{Z}^3$ such that $2x^2 + y^2 + 8z^2 = n$ is exactly twice the number of triples that satisfy $2x^2 + y^2 + 32z^2 = n$.*

Thus the problem of congruent numbers that has seeming little to do with elliptic curves entirely rests upon one of the foremost open problems in the subject.

The above has hopefully given the reader a brief and enjoyable introduction to the basics of elliptic curves. Further reading is recommended, especially the notes of [2] because his exposition is both very clear and very comprehensive.

References

- [1] KAZUYA KATO, N. K., AND SAITO, T. *Number Theory: Fermat's Dream*. American Mathematical Society, 2000.
- [2] MILNE, J. *Elliptic Curves*. BookSurge Publishers, 2006.