WHAT IS...

an Elliptic Curve?

Harris B. Daniels and Álvaro Lozano-Robledo

Communicated by Steven J. Miller and Cesar E. Silva

Elliptic curves are ubiquitous in number theory, algebraic geometry, complex analysis, cryptography, physics, and beyond. They lie at the forefront of arithmetic geometry, as shown in the feature on Andrew Wiles and his proof of Fermat's Last Theorem that appears in this issue of the *Notices*. The goal of arithmetic geometry, in general, is to determine the set of K-rational points on an algebraic variety C (e.g., a curve given by polynomial equations) defined over K, where K is a field, and the K-rational points, denoted by $C(K)$, are those points on C with coordinates in K. For instance, Fermat's Last Theorem states that the algebraic variety

$$X^n + Y^n = Z^n$$

has only trivial solutions (one with X, Y, or $Z = 0$) over $\mathbb{Q}$ when $n \geq 3$. Here we will concentrate on the case of a 1-dimensional algebraic variety, that is, a curve C, and a number field K (such as the rationals $\mathbb{Q}$ or the Gaussian rationals $\mathbb{Q}(i)$). Curves are classified by their geometric genus as complex Riemann surfaces. When the genus of C is 0, as for lines and conics, the classical methods of Euclid, Diophantus, Brahmagupta, Legendre, Gauss, Hasse, and Minkowski, among others, completely determine the K-rational points on C. For example,

$$C_1 : 37X + 39Y = 1 \quad \text{and} \quad C_2 : X^2 - 13Y^2 = 1$$

have infinitely many rational points that can be completely determined via elementary methods. However, when the genus of C is 1, we are in general not even able to decide whether C has K-rational points, much less determine all the points that belong to $C(K)$.

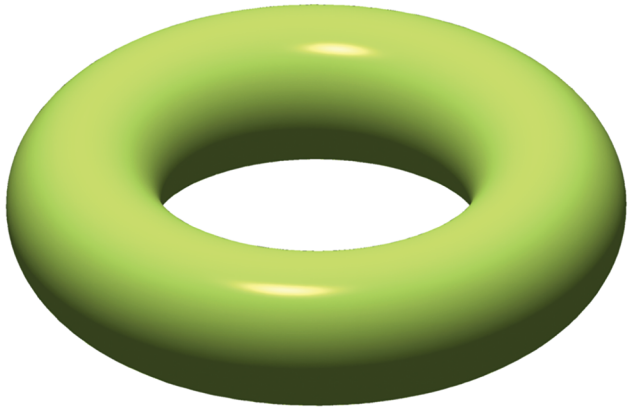


Figure 1. A curve of genus 1 over the complex numbers is a Riemann surface with one hole.

For example, the curve

$$C : 3X^3 + 4Y^3 = 5$$

has no $\mathbb{Q}$-rational points, but the local methods we use in the genus 0 case to rule out global points fail here.[1] A goal of the theory of elliptic curves is to find all the K-rational points on curves of genus one.

The study of elliptic curves grew in the 1980s.

An **elliptic curve** E is a smooth projective[2] curve of genus 1 defined over a field K, with at least one K-rational point (i.e., there is at least one point P on E with coordinates in K). If the field K is of characteristic 0 (e.g.,

Harris B. Daniels is assistant professor at Amherst College. His e-mail address is hdaniels@amherst.edu.

Álvaro Lozano-Robledo is associate professor at the University of Connecticut. His e-mail address is alvaro.lozano-robledo@uconn.edu.

DOI: http://dx.doi.org/10.1090/noti1490

[1] *$C : 3X^3 + 4Y^3 = 5$ is an example of Selmer where the local-to-global principle fails. This means that there are points on C over every completion of $\mathbb{Q}$—i.e., over $\mathbb{R}$ and the p-adics $\mathbb{Q}_p$ for every prime p—but not over $\mathbb{Q}$ itself.*

[2] *Curves are considered in projective space $\mathbb{P}^2(K)$, where, in addition to the affine points, there may be some points of the curve* at infinity.

number fields) or characteristic $p > 3$, then every elliptic curve can be given by a nice choice of coordinates, called a *short Weierstrass model*, of the form

$$E : y^2 = x^3 + Ax + B,$$

with A and B in K (and $4A^3 + 27B^2 \neq 0$ for smoothness). In this model there is only one K-rational point *at infinity*, denoted by $\mathcal{O}$. One aspect that makes the theory of elliptic curves so rich is that the set $E(K)$ can be equipped with an Abelian group structure, geometric in nature (see Figure 2), where $\mathcal{O}$ is the zero element (in other words, elliptic curves are 1-dimensional Abelian varieties).

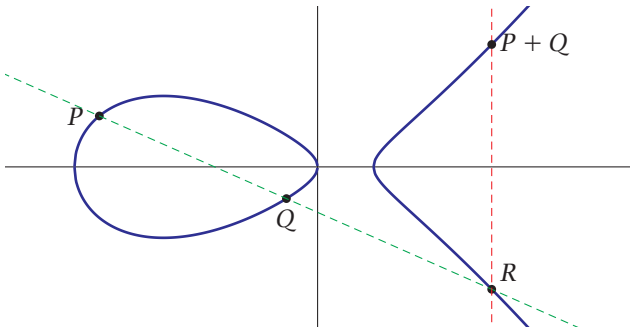


Figure 2. The addition law on an elliptic curve.

The Abelian group $E(K)$ was conjectured to be finitely generated by Poincaré in the early 1900s and proved to be so by Mordell for $K = \mathbb{Q}$ in 1922. The result was generalized to Abelian varieties over number fields by Weil in 1928 (a result widely known as the *Mordell–Weil Theorem*). The classification of finitely generated Abelian groups tells us that $E(K)$ is the direct sum of two groups: its torsion subgroup and a free Abelian group of rank $R \geq 0$, i.e.,

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^R.$$

We then call $R = R_{E/K}$ the *rank* of the elliptic curve E/K. For instance, for

$$E : y^2 + y = x^3 + x^2 - 10x + 10,$$

the group $E(\mathbb{Q})$ is generated by $P = (2, -2)$ and $Q = (-4, 1)$. Here P is a point of order 5 and Q is of infinite order, and so $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}$.

Which finitely generated Abelian groups can arise as the group structure of an elliptic curve over a fixed field K? The possible torsion subgroups $E(K)_{\text{tors}}$ that can occur have been determined only when $K = \mathbb{Q}$, or when K is a quadratic or cubic number field (e.g., $K = \mathbb{Q}(i)$, or $K = \mathbb{Q}(\sqrt[3]{2})$). For $K = \mathbb{Q}$, the list of torsion subgroups was conjectured by Levi in 1908, later reconjectured by Ogg in 1970, and finally proved in 1976 by Mazur:

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{for } 1 \leq N \leq 10, \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{for } 1 \leq 1M \leq 4. \end{cases}$$

In contrast, the list of possible ranks $R_{E/K}$ is completely unknown, even over $\mathbb{Q}$. We do not even know if this list is finite or infinite for any fixed number field. The largest rank known over $\mathbb{Q}$ is 28, for a curve found by Elkies.

The open questions about the rank of an elliptic curve are central to what makes the K-rational points on elliptic curves so hard to determine. The difficulty arises from the failure of the local-to-global principle (or Hasse principle) on curves of genus greater than or equal to 1 (see footnote 1). For an elliptic curve E/K, one defines the Tate–Shafarevich group $Ш = Ш(E/K)$ to measure the failure of the Hasse principle on E. In a sense, Ш plays the role of the ideal class group of a number field. However, we do not know that $Ш(E/K)$ is always a finite group.[3] If we knew that Ш is always finite, then a method Fermat inaugurated, called *descent*, would presumably yield an algorithm to determine all the K-rational points on E.

In the 1960s, Birch and Swinnerton-Dyer conjectured an analytic approach to computing the rank of an elliptic curve. Later, their conjecture was refined in terms of the Hasse–Weil L-function of an elliptic curve E (over $\mathbb{Q}$ for simplicity), which is defined by an Euler product:

$$L(E, s) = \prod_{p \text{ prime}} L_p(E, p^{-s})^{-1},$$

where $L_p(E, T) = 1 - a_p T + pT^2$ for all but finitely many primes, $a_p = p + 1 - \#E(\mathbb{F}_p)$, and $\#E(\mathbb{F}_p)$ is the number of points on E considered as a curve over $\mathbb{F}_p$. Thus defined, $L(E, s)$ converges as long as $\text{Re}(s) > 3/2$. In fact, Hasse conjectured more: any L-function of an elliptic curve over $\mathbb{Q}$ has an analytic continuation to the whole complex plane. This has now been proved as a consequence of the modularity theorem that we discuss below. The Birch and Swinnerton-Dyer conjecture (BSD) claims that the order of vanishing of $L(E, s)$ at $s = 1$ is equal to $R_{E/\mathbb{Q}}$, the rank of $E(\mathbb{Q})$. In fact, the conjecture also predicts the residue at $s = 1$ in terms of invariants of $E/\mathbb{Q}$. For instance, the curve $E : y^2 + y = x^3 - 7x + 6$ is of rank 3, with $E(\mathbb{Q}) \cong \mathbb{Z}^3$, and the graph of $L(E, x)$ for $0 \leq x \leq 3$ is displayed in Figure 3. The BSD conjecture is known to hold only in certain cases of elliptic curves of rank 0 and 1, by work of Coates and Wiles, Gross and Zagier, Kolyvagin, Rubin, Skinner and Urban, among others. However, Bhargava, Skinner, and Zhang have shown that BSD is true for at least 66 percent of all elliptic curves over the rationals.

An elliptic curve can be equipped with an Abelian group structure.

The study of elliptic curves grew in popularity in the 1980s when Hellegouarch, Frey, and Serre outlined a road map to prove Fermat's Last Theorem by proposing that a certain elliptic curve cannot exist. Roughly speaking, if $p \geq 11$ and $a^p + b^p = c^p$ is a nontrivial solution of Fermat's equation $X^p + Y^p = Z^p$, then the so-called Frey–Hellegouarch curve $y^2 = x(x - a^p)(x + b^p)$ would have two properties thought to be contradictory. First, the curve would be *semistable*, which is a mild technical

[3] *The finiteness of* Ш *is known only in certain cases with rank* ≤ 1, *by work of Kolyvagin and Rubin.*

condition about the type of curves $E/\mathbb{F}_p$ that we get by reducing the coefficients of E modulo p. Second, the curve would be *modular*, a property we explain in the next paragraph. The statement that the Frey–Hellegouarch curve is semistable but not modular was first formalized by Serre and then proved by Ribet. With Ribet's result, to prove Fermat's Last Theorem, one needed to prove "only" that all semistable elliptic curves over $\mathbb{Q}$ are modular. This statement emerged in the 1950s and is sometimes called the modularity conjecture, or Taniyama–Shimura–Weil conjecture.[4] The modularity conjecture relates two seemingly very distinct objects: elliptic curves and modular forms.

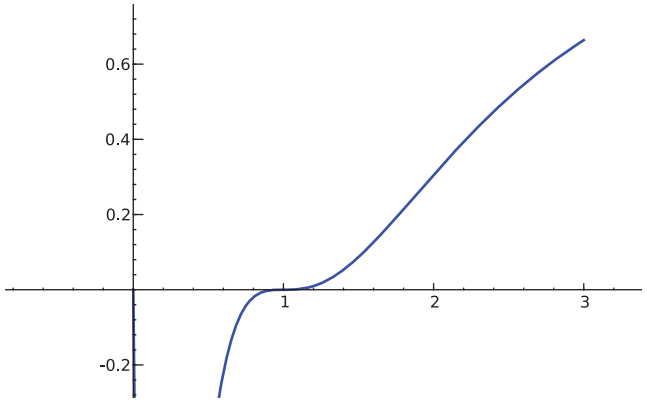


Figure 3. An L-function $L(E,x)$ with a zero of order 3 at $x = 1$.

A modular form is a complex-analytic function f on the upper-half complex plane that satisfies certain symmetries. In particular, $f(s)$ admits a Fourier series expansion $f(s) = \sum_{n\geq 0} a_n q^n$, where $q = e^{2\pi i s}$, and we can attach to the modular form f an L-function $L(f,s) = \sum_{n\geq 0} a_n/n^s$. The modularity conjecture says that every elliptic curve E is associated to a modular form f such that $L(E,s) = L(f,s)$; i.e., their L-functions coincide. In particular, this implies that $L(E,s)$ has an analytic continuation to $\mathbb{C}$, because $L(f,s)$ is known to have one. In 1993 Wiles [2] announced a proof of the modularity conjecture in the semistable case, but a flaw was found in the proof, which was fixed in 1995 by Taylor and Wiles. In 2001 the full conjecture was proved for all elliptic curves over $\mathbb{Q}$ by Brueil, Conrad, Diamond, and Taylor. In 2015 Freitas, Le Hung, and Siksek extended the modularity theorem to real quadratic fields. Modularity fits into a much larger context, together with the Langlands program and the Fontaine–Mazur conjecture, which was described in Mark Kisin's "What Is a Galois Representation?" (*Notices*, June/July 2007).

Modularity fits into a much larger context, together with the Langlands program and the Fontaine–Mazur conjecture.

The canonical starting point for a graduate student interested in learning more about elliptic curves is Silverman's *The Arithmetic of Elliptic Curves* [1]. A more elementary approach is Silverman and Tate's *Rational Points on Elliptic Curves*.

[4] *See Lang's article in the* Notices, *November 1995, for a detailed historical account of the modularity conjecture.*

References

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer-Verlag, New York, 2009. MR2514094

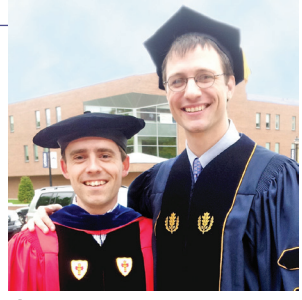
[2] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), no. 3, 443–551. MR1333035

Figure and Photo Credits

Figure 1/public domain, `https://commons.wikimedia.org/wiki/File:Torus_illustration.png`

Figure 3 was created by Àlvaro Lozano-Robledo with SageMath.

Photo of Harris B. Daniels and Àlvaro Lozano-Robledo is by Keith Conrad, courtesy of Àlvaro Lozano-Robledo.



Álvaro Lozano-Robledo and Harris B. Daniels

ABOUT THE AUTHORS

Harris B. Daniels (right) received his PhD in mathematics in 2013 from the University of Connecticut and is currently assistant professor at Amherst College in Massachusetts.

Álvaro Lozano-Robledo (left) is a father of two real children, one academic child, and is expecting a second (academic) descendent in spring 2017. He is the author of *Elliptic Curves, Modular Forms, and Their L-functions* (AMS, 2011) and has published over twenty-five research articles related to the theory of elliptic curves.