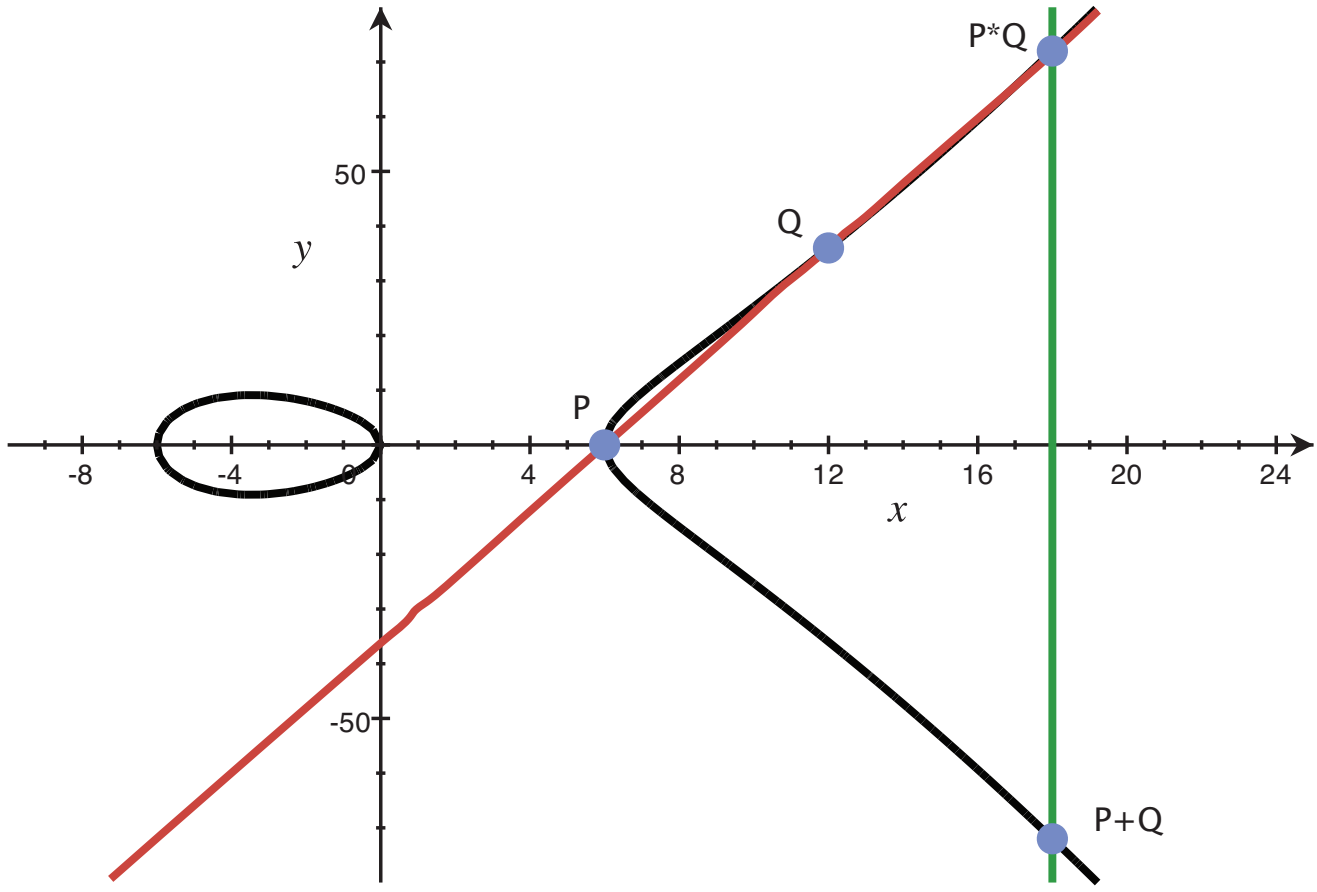
The Ubiquity of Elliptic Curves



Edray Herber Goins

Elliptic Curves appear in many branches of mathematics and science: Algebraic Geometry, Abstract Algebra, and even Computer Science. In this article, I provide a gentle introduction to the subject, and explore the many ways elliptic curves are used to answer questions from a variety of fields.

An elliptic curve is a non-singular projective curve of genus one having a specified base point. For the inspired, we can say this in fancier terms: Fix a field k, such as the rational numbers $\mathbb{Q}$ or a finite field $\mathbb{F}_q$ or even a function field $\mathbb{C}(t)$. We say that *an elliptic curve E defined over k* is that functor which associates fields K containing k to an algebraic set of the form

$$E(K) = \left\{ (x : y : z) \in \mathbb{P}^2(K) \;\middle|\; \begin{array}{l} y^2 z + a_1 x y z + a_3 y z^2 \\ \qquad = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3 \end{array} \right\}$$

where (i) the coefficients $a_1, \ldots, a_6$ lie in k and (ii) each point $P = (x : y : z)$ in $E(K)$ has a well-defined tangent line. The so-called *point at infinity* $\mathcal{O} = (0 : 1 : 0)$ is our specified base point; it is always an element of $E(K)$. Here we employ notation which allows us to express our points in *projective space*: we write $(x : y : z)$ to denote the equivalence class of points in the form $(\lambda x, \lambda y, \lambda z)$ for nonzero scalars λ. We say that elements P of $E(K)$ are *K-rational points on E*.

If k is not of characteristic 2 or 3, it is equivalent to say that an elliptic curve is represented by a cubic equation of the form $y^2 = x^3 + A x + B$ for some $A, B \in k$ satisfying $4A^3 + 27B^2 \neq 0$ because we can make a linear change of variables. Indeed, $\mathcal{O} = (0 : 1 : 0)$ is the only projective point $P = (x : y : z)$ on the curve with $z = 0$, so for

Edray Herber Goins is a professor of mathematics at Pomona College. His email address is edray.goins@pomona.edu.

Communicated by Notices *Associate Editor Daniel Krashen.*

DOI: https://doi.org/10.1090/noti1789

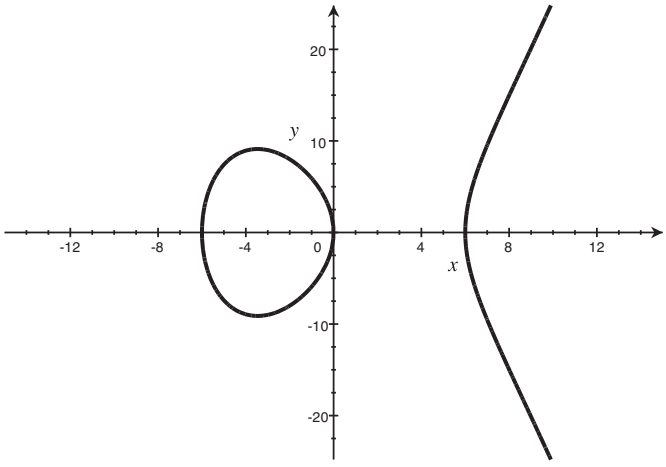


Figure 1. Graph of an elliptic curve over $K = \mathbb{R}$.

all other projective points we can scale by $\lambda = 1/z$ and assume that $P = (x : y : 1)$. We typically identify this as an affine point (x, y) in the usual sense. An example of a graph of the set $E(K)$ when $K = \mathbb{R}$ can be found in Figure 1. More information can be found in the standard texts [7] and [32].

Elliptic Curves in Algebraic Geometry

It is not always obvious that a given set of equations defines an elliptic curve. Here are some examples.

Fermat curves. First, consider the curve $a^3 + b^3 = c^3$ over the field $k = \mathbb{Q}$. Using the substitutions $a = 32 - 8\,y$, $b = 40 + 8\,y$, and $c = 24\,x$, we find the elliptic curve $y^2 + y = x^3 - 7$. On the other hand, the curve $3\,a^3 + 4\,b^3 = 5\,c^3$ is not an elliptic curve over $\mathbb{Q}$ because this equation has no $\mathbb{Q}$-rational solutions other than the degenerate one, namely $a = b = c = 0$. This equation does however define a projective curve of genus one. This example and a larger class are discussed in some detail in [31].

There has been considerable interest in the curve $a^n + b^n = c^n$ over $\mathbb{Q}$ for various exponents n. Such an equation defines a *Fermat curve* because Pierre de Fermat wondered whether there were any nonzero $\mathbb{Q}$-rational solutions when n is a sufficiently large integer. When $n = 2$, it is clear that any *Pythagorean Triple*, such as $(a, b, c) = (3, 4, 5)$, will suffice as a desired solution. We have seen that elliptic curves appear when $n = 3$, but this is not the only exponent where this happens. Curiously, when $n = 7$, any solution (a, b, c) yields a point $P = (x : y : 1)$ on the elliptic curve $E : y^2 + x\,y = x^3 - x^2 - 107\,x + 552$ through the unwieldly – and nontrivial – substitution

$$x = 49\,\frac{(a^2+b^2+c^2+a\,b+a\,c+b\,c)^2 + a\,b\,c\,(a+b+c)}{(a+b+c)^4} - 12,$$

$$y = \frac{7\,(x+12)\,(a^2+b^2+c^2) - x\,(a+b+c)^2}{2\,(a+b+c)^2}.$$

Hence one can find all $\mathbb{Q}$-rational solutions to $a^7 + b^7 = c^7$ by focusing on $\mathbb{Q}$-rational points P on E. The reader may wish to compare with the discussion of elliptic curves with conductor 49 in [12].

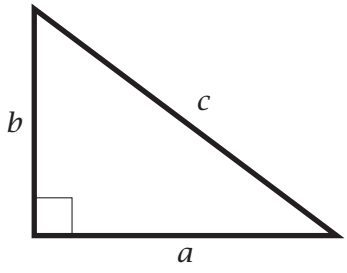
Congruent numbers. As another example, say that we are given a positive integer n. When can this integer be expressed as the area of a right triangle having rational sides of lengths a, b, and c? (See Figure 2.) Such n is said to be *congruent* because there exists a rational number d such that the arithmetic progression $\{d-n,\ d,\ d+n\}$ consists of three squares, namely $\{(a-b)^2/4,\ c^2/4,\ (a+b)^2/4\}$; see [33]. This question is equivalent to asking whether there is a $\mathbb{Q}$-rational solution (a, b, c) to the simultaneous equations $a^2 + b^2 = c^2$ and $(1/2)\,a\,b = n$. Using the substitutions $a = (x^2 - n^2)/y$, $b = 2\,n\,x/y$ and $c = (x^2+n^2)/y$, we find the elliptic curve $y^2 = x^3 - n^2\,x$. We see immediately that $n = 6$ is a congruent number because the elliptic curve has a $\mathbb{Q}$-rational point $(x : y : 1) = (12 : 36 : 1)$ which corresponds to the familiar 3–4–5 triangle. More interestingly, $n = 5$ is also a congruent number because the elliptic curve has a $\mathbb{Q}$-rational point $(x : y : 1) = (50 : 75 : 8)$ which corresponds to the less obvious $(9/6)$–$(40/6)$–$(41/6)$ triangle.

Quadric intersections. It may seem surprising that two quadratic equations—such as $a^2 + b^2 = c^2$ and $(1/2)\,a\,b = n$—yield an elliptic curve, but this is part of a more general phenomenon. A typical number theory course discusses how to find $\mathbb{Q}$-rational solutions (v, w) to a quadratic equation, such as the *Pell equation* $v^2 - d\,w^2 = 1$. More generally, say that d_1 and d_2 are distinct nonzero $\mathbb{Q}$-rational numbers. The collection of simultaneous Pell equations $u^2 - d_1\,w^2 = 1$ and $v^2 - d_2\,w^2 = 1$ is known as a *quadric intersection*. (These are closely related to *concordant quadratic forms*; see [2] and [26].) Using the substitutions

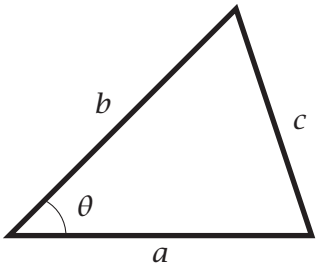
$$u = (x^2 + 2\,d_1\,x + d_1\,d_2)/(x^2 - d_1\,d_2)$$
$$v = (x^2 + 2\,d_2\,x + d_1\,d_2)/(x^2 - d_1\,d_2)$$
$$w = 2\,y/(x^2 - d_1\,d_2)$$

we find the elliptic curve $y^2 = x\,(x + d_1)\,(x + d_2)$. In general, given a set of equations, it is easy to determine whether it has genus one, but it is difficult to determine whether there is a K-rational solution which we could assign as our base point.

Heron triangles and θ-congruent numbers. It is only natural to wonder whether the geometric construction of congruent numbers as the area of a $\mathbb{Q}$-rational right triangle can be generalized to other types of triangles. For example, if a, b, and c are the lengths of a triangle with an angle



(a) Right Triangle



(b) Triangle with Angle θ

Figure 2. Triangles with sides of lengths a, b, and c.

$\theta = 90^\circ$, then $a^2+b^2 = c^2$; but if we have a triangle with an angle $\theta = 106.26^\circ$, then $a^2 + (14/25)\,a\,b + b^2 = c^2$. Indeed, this concept can be generalized.

Say that we are given a positive integer n. When can this integer be expressed as the area of some triangle having rational sides of lengths a, b, and c? (See Figure 2.) Such a triangle is called a *Heron triangle* because Heron of Alexandria found a formula which relates these quantities, although a slightly more general formula was known much earlier to Brahmagupta: $n^2 = s\,(s-a)\,(s-b)\,(s-c)$ where $s = (a+b+c)/2$ is the *semi-perimeter*. If θ is the angle opposite of the side of length c, the Law of Cosines and the Law of Sines together assert that

$$\cos\theta = \frac{m^2-1}{m^2+1} \quad \text{and} \quad \sin\theta = \frac{2\,m}{m^2+1}$$
$$\text{where} \quad m = \frac{(a+b)^2-c^2}{4\,n}.$$

Using the substitutions $a = y/x$, $b = (d_1-d_2)\,x/y$, and $c = (x^2 - d_1\,d_2)/y$, we find the elliptic curve $E : y^2 = x\,(x+d_1)\,(x+d_2)$ in terms of $d_1 = n\,m$ and $d_2 = -n/m$. For example, if $\theta = 90^\circ$ then $m = 1$ and we find the curve $y^2 = x^3 - n^2\,x$; and if $\theta = 106.26^\circ$ then $m = 3/4$ and we find the curve $y^2 = x^3 - (7/12)\,n\,x - n^2\,x$. In other words, once we fix an area n and an angle θ in terms of m as above, then we can use $\mathbb{Q}$-rational points $P = (x : y : 1)$ to find Heron triangles with sides of lengths a, b, and c. As a generalization of congruent numbers, we say n is a *θ-congruent number*; see [14].

Elliptic Curves in Abstract Algebra

Chord tangent construction. We have seen that there are many questions one can ask about $\mathbb{Q}$-rational solutions to systems of polynomial equations. Such questions were of primary interest to Diophantus of Alexandria—the namesake of the so-called *Diophantine Equations*. In fact, Diophantus gave a general geometric trick to finding $\mathbb{Q}$-rational solutions.

The non-singularity of elliptic curves allows us to start with a few known K-rational points and construct more. For example, let $y = \lambda\,x + \nu$ be a line through two affine points $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ in $E(K)$; we choose this to be the line tangent to E at P if $P = Q$. This line must intersect the curve as a third point in $E(K)$ which we denote by $P * Q = (x_3 : y_3 : 1)$. Rather explicitly, $x_3 = \lambda^2 + a_1\,\lambda - a_2 - x_1 - x_2$ and $y_3 = \lambda\,x_3 + \nu$. This is known as the *chord tangent construction*.

As an example, consider the $\mathbb{Q}$-rational point $P = (12 : 36 : 1)$ on the curve $E : y^2 = x^3 - 36\,x$. The line tangent to E at P is $y = (11/2)\,x - 30$, so we find the new $\mathbb{Q}$-rational point $P * P = (50 : 35 : 8)$. That is, the triangle $(49/70)$–$(1200/70)$–$(1201/70)$ also has area $n = 6$; hopefully you can see how to construct many more. As another example, consider the curve $y^2 + y = x^3 - 7$. Some $\mathbb{Q}$-rational points are $P = (3 : 4 : 1)$ and $Q = (3 : -5 : 1)$. The line tangent to E at P is $y = 3\,x - 5$, so we find that $P * P = P$. The line through P and Q is the vertical line $x = 3$, so we find that $P * Q = \mathcal{O}$. That is, the chord-tangent construction does not help much in this case to find more $\mathbb{Q}$-rational points.

Group law. The chord tangent construction yields a way to turn $E(K)$ into a group. Indeed, given two points P and Q in $E(K)$, define $P \oplus Q = (P * Q) * \mathcal{O}$, where the point $P * Q = (x : y : z)$ is found as described above, and the point $P \oplus Q = (x : -y - a_1\,x - a_3\,z : z)$ is that reflection of $P * Q$ about the line $2\,y + a_1\,x + a_3 = 0$. A graph of these lines and their intersections can be found in Figure 3. It is easy to check that $E(K)$ forms an abelian group under $\oplus$, where the point at infinity $\mathcal{O} = (0 : 1 : 0)$ is the identity and $[-1]P = P * \mathcal{O}$ is the inverse of a given point P. The difficulty in proving that this is indeed an abelian group comes down to showing associativity, namely that $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. One typically does this via the famous Riemann-Roch Theorem; see [32].

The Mordell–Weil group. A natural question is to ask about the structure of the abelian group $E(K)$. A celebrated theorem of Louis Mordell [24], for $K = \mathbb{Q}$, generalized by André Weil [34] for finite extensions K of $\mathbb{Q}$, states that $E(K)$ is finitely generated, that is $E(K) = E(K)_{\text{tors}} \oplus \mathbb{Z}^r$ for some finite group $E(K)_{\text{tors}}$ consisting of the torsion elements, and some nonnegative integer r called the

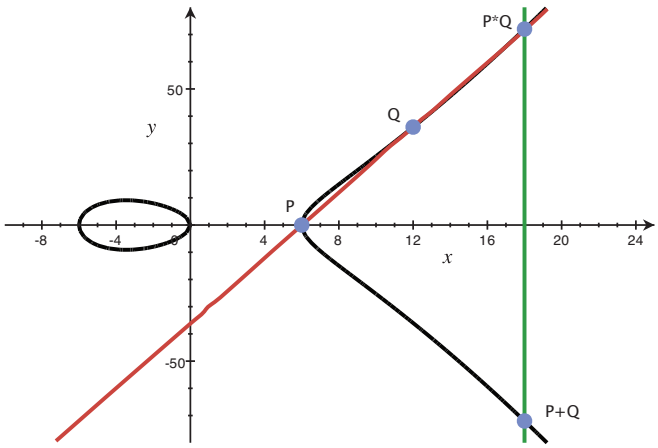


Figure 3. The group law of an elliptic curve.

rank. The group $E(K)$ is called the Mordell–Weil group in these cases. This result asserts there is a finite set of generators $\{T_1, \ldots, T_s, P_1, \ldots, P_r\} \subseteq E(K)$ such that any K-rational point $P \in E(K)$ can be expressed in the form $P = [m_1]T_1 \oplus \cdots \oplus [m_s]T_s \oplus [n_1]P_1 \oplus \cdots \oplus [n_r]P_r$ for some integers m_i and n_j, where we employ the notation $[n]P = P \oplus P \oplus \cdots \oplus P$ as a sum n times. For example, when $y^2 + y = x^3 - 7$ we have $E(\mathbb{Q}) \simeq (\mathbb{Z}/3\,\mathbb{Z})$ as generated by $T_1 = (3 : 4 : 1)$ because $T_1 * T_1 = T_1$, and so $T_1 \oplus T_1 = [-1]T$. Incidentally, this also explains why the there are only three rational solutions $(a : b : c)$ to $a^3 + b^3 = c^3$, and they each satisfy $a\,b\,c = 0$.

There has been a lot of work done in understanding the group $E(K)$ when $K = \mathbb{Q}$. Barry Mazur [22] [23], proving conjectures of Beppo Levi [30] and Andrew Ogg [25], showed that there are only 15 possible types of torsion subgroup, namely either $E(\mathbb{Q})_{\text{tors}} \simeq (\mathbb{Z}/n\,\mathbb{Z})$ for $n = 1, 2, \ldots, 10, 12$; or $E(\mathbb{Q})_{\text{tors}} \simeq (\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/2\,m\,\mathbb{Z})$ for $m = 1, 2, 3, 4$. (There are similar classifications when K is a finite extension of $\mathbb{Q}$; see [16], [17], [18], and [19].) Not a lot is known about the rank r. Work of Manjul Bhargava [4] and others [1] suggest that the average value of r is $1/2$— meaning roughly half of elliptic curves have rank $r = 0$ while the other half have rank $r = 1$. An example of Noam Elkies shows that the rank can be as large as $r = 28$, but recent work of Bjorn Poonen et al. [27] [28] suggests that there is a uniform upper bound on r.

Computing the Mordell–Weil group. Computing $E(K)$ is a difficult task—even when $K = \mathbb{Q}$. One can ask two questions for a given elliptic curve E defined over $\mathbb{Q}$: (i) What are the torsion subgroup $E(K)_{\text{tors}}$ and the rank r? (ii) What is a generating set $\{T_1, \ldots, T_s, P_1, \ldots, P_r\}$ for the Mordell–Weil group? We give a method for determining the answers to these questions by focusing on a specific family of elliptic curves. Fix distinct nonzero $\mathbb{Q}$-rational numbers d_1 and d_2, and consider the elliptic curve $E : y^2 = x\,(x + d_1)\,(x + d_2)$. The torsion subgroup is relatively easy to compute: Mazur's Theorem states that $E(\mathbb{Q})_{\text{tors}} \simeq (\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/2\,m\,\mathbb{Z})$ for some $m = 1, 2, 3$, or 4. We can choose $T_1 = (0 : 0 : 1)$ as a generator of order 2, so it remains to find some $\mathbb{Q}$-rational point T_2 as a generator of order $2\,m$. The rank is considerably more difficult to determine: Following an idea of Mordell, there is an injective group homomorphism

$$\begin{array}{ccc} \dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})} \simeq \left(\dfrac{\mathbb{Z}}{2\,\mathbb{Z}}\right)^{r+2} & \hookrightarrow & \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \times \dfrac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2} \\ P = (x : y : 1) & \longmapsto & (x + d_1,\ x + d_2) \end{array}$$

One can determine the image of this map by other means—such as looking at certain homogeneous spaces as torsors for E—then use this to determine the rank r. See [8], [9], and [10] for the state of the art on this topic.

Heron triangles revisited. Recall earlier that we introduced the elliptic curve $y^2 = x\,(x + d_1)\,(x + d_2)$ in terms of the distinct nonzero $\mathbb{Q}$-rational numbers $d_1 = n\,m$ and $d_2 = -n/m$; $\mathbb{Q}$-rational points on this curve correspond to a triangle with area n and rational sides of lengths a, b, and c. What can we say about the Mordell–Weil group of this elliptic curve? For example, take $n = 12$. This is the area of an isosceles triangle with sides of lengths $a = b = 5$ and $c = 8$. We find that $m = ((a + b)^2 - c^2)/(4\,n) = 3/4$, and hence the elliptic curve $E : y^2 = x^3 - (7/12)\,n\,x - n^2\,x$. One shows that $E(\mathbb{Q}) \simeq (\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/4\,\mathbb{Z})$ as generated by $T_1 = (0 : 0 : 1)$ and $T_2 = (18 : 45 : 2)$. In general for $d_1 = n\,m$ and $d_2 = -n/m$, the torsion subgroup of the elliptic curve $E : y^2 = x\,(x + d_1)\,(x + d_2)$ contains $(\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/4\,\mathbb{Z})$ if and only if n is the area of an isosceles triangle; and $E(\mathbb{Q})_{\text{tors}} \simeq (\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/2\,\mathbb{Z})$ otherwise. Note that the torsion subgroup can never be $(\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/6\,\mathbb{Z})$! For more information, see [15] and [29].

This elliptic curve is not the only one which yields Heron triangles. Fix a $\mathbb{Q}$-rational number t different from 0 or ± 1. It is easy to check that $\mathbb{Q}$-rational points $P = (x : y : 1)$ on the elliptic curve $E : y^2 = x\,(x + d_1)\,(x + d_2)$ yield a Heron triangle with area n and sides of lengths a, b, and c, all in terms of

$$a = \left[\frac{1}{2}\,\frac{x-1}{x+1} + \frac{t^3 - t}{t^4 - 6\,t^2 + 1}\,\frac{y}{x}\right] c$$

$$b = \left[\frac{1}{2}\,\frac{x-1}{x+1} - \frac{t^3 - t}{t^4 - 6\,t^2 + 1}\,\frac{y}{x}\right] c$$

$$n = \frac{t^3 - t}{t^4 - 6\,t^2 + 1}\,c^2$$

and

$$d_1 = \left(\frac{t^2 - 1}{2\,t}\right)^2 \qquad d_2 = \left(\frac{2\,t}{t^2 - 1}\right)^2$$

It is also easy to check that this elliptic curve has torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq (\mathbb{Z}/2\,\mathbb{Z}) \oplus (\mathbb{Z}/8\,\mathbb{Z})$. In fact, every

elliptic curve defined over $\mathbb{Q}$ with this torsion subgroup is in the form of this E for some $\mathbb{Q}$-rational number t. We find an elliptic curve with rank $r = 3$ if we choose $t = 15/76$. This is the largest known rank among all elliptic curves E defined over $\mathbb{Q}$ having this torsion subgroup! For more information, see [6] and [11].

Elliptic Curves in Computer Science

We have seen how elliptic curves play a large role in finding K-rational solutions to collections of polynomial equations. Surprisingly, elliptic curves can be used to factor very large numbers, or even make it difficult for people to decode secret messages.

Elliptic curve factorization methods. Say that n is a large integer which we know is the product of two large primes roughly equal in size, but we don't know what those primes are. We outline a method using elliptic curves to determine these primes.

Pick an elliptic curve E defined over $K = k = \mathbb{Z}/n\mathbb{Z}$—even though we know that k is certainly not a field because it contains zero divisors. We will use this to our advantage. Also pick two points $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ in $E(K)$; we will try to compute $P \oplus Q$. This would involve first constructing a line $y = \lambda x + \nu$. Since the slope $\lambda = (y_1 - y_2)/(x_1 - x_2)$ and the y-intercept is $\nu = (y_2 x_1 - y_1 x_2)/(x_1 - x_2)$, we consider the greatest common divisor $d = \gcd(n, x_1 - x_2)$. If $d = 1$, then we can compute $P \oplus Q$; but if $d \neq 1$ then d should be a nontrivial divisor of n. In this way, we expect to eventually find enough points to be able to factor n. This is known as the *elliptic curve factorization method (ECM)*; see [21].

The largest factor d found to date using ECM corresponds to the integer $n = 7^{337} + 1$; this divisor d has 83 digits! See [35].

Elliptic curve discrete logarithm problem. Say that we have two individuals, Shuri and T'Challa, who want to send each other a private message. First they must make sure that each is who they claim. Here is a protocol to explain how to do this.

Both individuals agree upon three items publicly: (i) a finite field $K = k = \mathbb{F}_q$, (ii) an elliptic curve E defined over k, and (iii) a point $P \in E(K)$ with a large order n, that is $[n]P = \mathcal{O}$. Shuri chooses some private information—such as a PIN—as a positive integer s less than n; T'Challa chooses the same as a positive integer t. Both Shuri and T'Challa publicly list $[s]P$ and $[t]P$ as their *public keys*—perhaps as the signature in an e-mail. If Shuri and T'Challa compute the same *shared key* $[st]P = [s]([t]P) = [t]([s]P)$, then Shuri and T'Challa can feel confident that they are indeed who they say they are. This public key agreement exchange is known as the *elliptic curve Diffie–Hellman (ECDH)* protocol; see [5].

The question becomes this: If an eavesdropper, say Killmonger, sees the public keys P, $[s]P$, $[t]P$, and $[st]P$, can he recover the private keys s and t? There is widespread belief that the answer is "no"—at least in a world where quantum computers do not exist. This is known as the *elliptic curve discrete logarithm problem (ECDLP)*; see [20].

Apple HomeKit and Curve25519. We give one last application of elliptic curves which is causing something of a controversy. Apple Computers has software which developers are slow to use because the software uses elliptic curves. Apple has created *HomeKit*, a platform for connecting your smartphones with WiFi and Bluetooth enabled accessories such as lights, cameras, and thermostats. Apple wishes to have strong security in this platform, so it has decided to employ 3072-bit encryption—much, much stronger than the 256-bit key Advanced Encryption Standard (AES).

To this end, Apple has asked developers to use elliptic curve cryptography for digital signatures and encrypted keys; the most secure seems to be an elliptic curve called `Curve25519`. Rather concretely, this is the curve $E : y^2 = x^3 + 486662\,x^2 + x$ defined over the field $k = \mathbb{F}_q$, where $q = (2^{255} - 19)^2$ is the square of a prime number. Daniel J. Bernstein et al. [3] showed that the abelian group $E(\mathbb{F}_q)$ has a subgroup $(\mathbb{Z}/n\mathbb{Z})$ of order

$$n = 2^{252} + 27742317777372353535851937790883648493$$

as generated by a K-rational point $P = (x_1 : y_1 : 1)$ having coordinate $x_1 = 9$. It is thought that elliptic curve cryptography is to blame for the slow rollout of *HomeKit*-ready devices for the market: developers are finding the mathematics behind this implementation to be... unusual.

References

[1] Jennifer S. Balakrishnan, Wei Ho, Nathan Kaplan, Simon Spicer, William Stein, and James Weigandt. Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks. *LMS J. Comput. Math.*, 19(suppl. A):351–370, 2016. MR3540965

[2] Eric Temple Bell. The problems of congruent numbers and concordant forms. *Proc. Nat. Acad. Sci. U. S. A.*, 33:326–328, 1947. MR0022228

[3] Daniel J. Bernstein. Curve25519: new Diffie-Hellman speed records. In *Public key cryptography—PKC 2006*, volume 3958 of *Lecture Notes in Comput. Sci.*, pages 207–228. Springer, Berlin, 2006. MR2423191

[4] Manjul Bhargava and Christopher Skinner. A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one. *J. Ramanujan Math. Soc.*, 29(2):221–242, 2014. MR3237733

[5] Dan Boneh and Igor E. Shparlinski. On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme. In *Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA)*, volume 2139 of Lecture Notes in Comput. Sci., pages 201–212. Springer, Berlin, 2001. MR1931423

[6] Garikai Campbell and Edray Herber Goins. Heron Triangles, Diophantine Problems, and Elliptic Curves. *Preprint*, pages 1–15, 2003.

[7] J. W. S. Cassels, *Lectures on elliptic curves*, Volume 24 of London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991. MR1144763

[8] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155, 2008. MR2384334

[9] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. II. Geometry. *J. Reine Angew. Math.*, 632:63–84, 2009. MR2544143

[10] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves III. Algorithms. *Math. Comp.*, 84(292):895–922, 2015. MR3290968

[11] Andrej Dujella, Juan Carlos Peral, and Petra Tadić. Elliptic curves with torsion group $\mathbb{Z}/6\mathbb{Z}$. *Glas. Mat. Ser. III*, 51(71)(2):321–333, 2016. MR3580201

[12] Noam Elkies. Elliptic curves in nature. www.math.harvard.edu/~elkies/nature.html

[13] Noam Elkies On $A^4 + B^4 + C^4 = D^4$. *Mathematics of Computation*, 51 (184): 825–835, 1988. MR930224

[14] Masahiko Fujiwara. θ-congruent numbers. In *Number theory (Eger, 1996)*, pages 235–241. de Gruyter, Berlin, 1998. MR1628845

[15] Edray Herber Goins and Davin Maddox. Heron triangles via elliptic curves. *Rocky Mountain J. Math.*, 36(5):1511–1526, 2006. MR2285297

[16] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(273):579–591, 2011. MR2728995

[17] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over quartic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(276):2395–2410, 2011. MR2813367

[18] Sheldon Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Math. J.*, 53(1):157–162, 1986. MR835802

[19] Sheldon Kamienny. Torsion points on elliptic curves over all quadratic fields. II. *Bull. Soc. Math. France*, 114(1):119–122, 1986. MR860654

[20] Neal Koblitz. *A course in number theory and cryptography*, Volume 114 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994. MR1302169

[21] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987. MR916721

[22] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. MR488287

[23] Barry Mazur. Rational points on modular curves. pages 107–148. *Lecture Notes in Math.*, Vol. 601, 1977. MR0450283

[24] Louis J. Mordell On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophical Society*, 21: 179-192, 1922-23.

[25] Andrew P. Ogg. Rational points of finite order on elliptic curves. *Inventiones Mathematicae*, 12: 105–111, 1971. MR0291084

[26] Ken Ono. Euler's concordant forms. *Acta Arith.*, 78(2):101–123, 1996. MR1424534

[27] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. https://arxiv.org/abs/1602.01431, February 2016.

[28] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012. MR2833483

[29] David J. Rusin. Rational triangles with equal area. *New York J. Math.*, 4:1–15, 1998. MR1489407

[30] Norbert Schappacher and René Schoof. Beppo Levi and the arithmetic of elliptic curves. *The Mathematical Intelligencer*, 18 (1): 57–69, 1996. MR1381581

[31] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85: 203–362, 1951. MR0041871

[32] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, Volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986. MR0817210

[33] Jerrold B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983. MR700775

[34] André Weil. L'arithmetique sur les courbes algébriques. *Acta Mathematica*, 52 (1): 281–315, 1929. MR1555278

[35] Paul Zimmermann. Top 50 factors found by ECM. https://members.loria.fr/PZimmermann/records/top50.html

Edray Herber Goins

Credits

All article figures and the author photo are courtesy of Edray Herber Goins.