Parabola Volume 62 Issue 2 (2026), Article 12

Into the endless world of elliptic curves

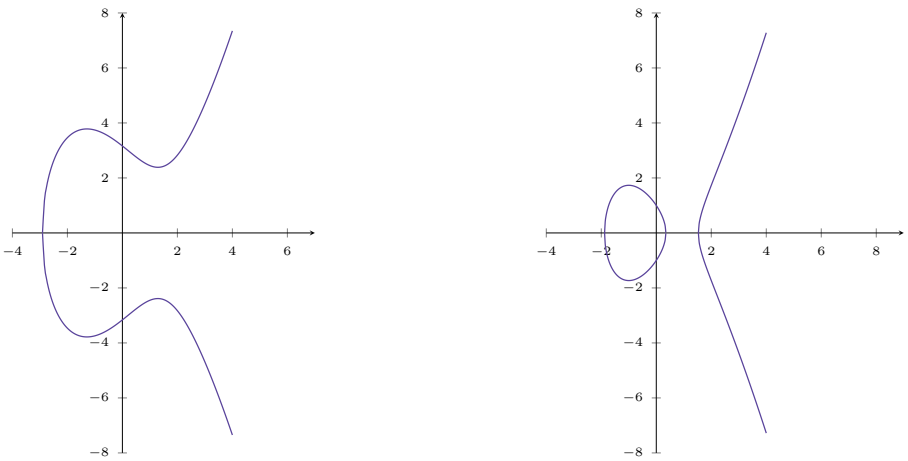
Candace Shi[1]

1 Introduction

> *"It is possible to write endlessly on elliptic curves. (This is not a threat.)"*
> *– Serge Lang, Elliptic Curves: Diophantine Analysis* [21]

There's little doubt that Serge Lang was exaggerating; in the process of editing, I realised there are many more things that I would have liked to ramble on about in great detail, but it would be best for me to not break this Overleaf document. Today, I merely hope to offer a glimpse into this endless world.

From verifying Bitcoin ownership to solving the congruent number problem, elliptic curves are beautifully puzzling yet practical mathematical objects that, from afar, hold an illusion of simplicity with their equation: $y^2 = x^3 + Ax + B$ [25, 29].



(a) $y^2 = x^3 - 5x + 10$ (b) $y^2 = x^3 - 3x + 1$

Figure 1: Elliptic curves over the real numbers

Before formally defining elliptic curves, we take a look at how they arose. Next, we zoom in on elliptic curves over prime fields and prove results that allow for simple point computation. Subsequently, arithmetic on elliptic curves satisfying Abelian

[1]Candace Shi is a second-year undergraduate studying Mathematics, and Discrete Mathematics and Algorithms, at the University of Sydney.

group laws will be established, which reveals its relevancy in cryptography. This naturally leads to exploration of cryptographic algorithms built on these curves: elliptic curve Diffie-Hellman key exchange, elliptic curve ElGamal encryption, and Elliptic Curve Digital Signature Algorithm. Moreover, the security and limitations of elliptic curve cryptography will be discussed, as well as future endeavours with the potential rise of quantum computers. Lastly, we shall appreciate the versatility of elliptic curves by examining their connection to the congruent number problem.

2 The birth of elliptic curves

> *"The history of mathematics is exhilarating, because it unfolds before us the vision of an endless series of victories of the human mind, victories without counterbalancing failures, that is, without dishonorable and humiliating ones, and without atrocities." – George Sarton* [27]

It all begins with Diophantus of Alexandria, a Greek mathematician who lived during the second century A.C. The first known appearance of an elliptic curve is scribed in his book *Arithmetica*, where he presented the problem as follows. [16, 25]

> *"To divide a given number into two numbers such that their product is a cube minus its side."*

In mathematical symbols, this translates to

$$Y(a-Y) = X^3 - X$$

which, after performing the change of variables $y := Y - a/2$ and $x := -X$, becomes $y^2 = x^3 - x + (a/2)^2$, satisfying the equation of an elliptic curve shown previously. Diophantus' solution to this problem for $a = 6$ involved substituting $X = 3Y - 1$ to obtain $27y^3 - 26y^2 = 0$. Disregarding the double root, he got $y = \frac{26}{27}$ and thus $x = \frac{17}{9}$.

Although the research remained near dormant for a thousand years, Diophantus' innovative work marked the beginning of what we now know as elliptic curves.

3 What is an elliptic curve?

> *"Mathematics is the art of giving the same name to different things."*
> *– Henri Poincaré* [33]

The "elliptic" curve did get its name from the ellipse, as these equations emerged in the process of computing elliptical arc lengths.[2] Despite this, elliptic curves are *almost* entirely unrelated to ellipses [25].

[2] I encourage the curious reader to see [25] for a comprehensive calculus demonstration of this.

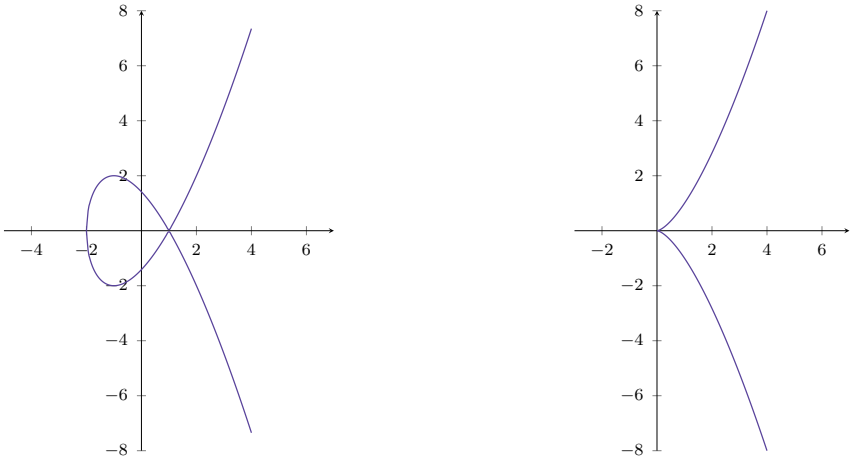
An elliptic curve E over the field K is the set of points $(x, y) \in K^2$ satisfying

$$E : y^2 = x^3 + Ax + B \tag{1}$$

for constants $A, B \in K$. To use this equation, it is necessary that the characteristic of K is not 2 or 3. [29]. Figure 1 shows how these curves may look over the real numbers.

If you are unfamiliar with fields, then think of them as sets of numbers that generally can be added, subtracted, multiplied and divided with each other – like the real numbers, as aforementioned.

An elliptic curve is *singular* if it has a self-intersection or cusp, as displayed in Figures 2a and 2b respectively. This occurs when the discriminant $\Delta = -16(4A^3 + 27B^2)$ is equal to zero. Otherwise, if the entire curve is "nice" and smooth, then it is nonsingular. See the Appendix for a more precise definition and proof.



(a) $y^2 = x^3 - 3x + 2$ (b) $y^2 = x^3$

Figure 2: Singular elliptic curves

For the remainder of this article, the sole focus will lie on the nonsingular elliptic curves, as singular ones hold dissimilar properties in comparison [29].

4 Elliptic curves over prime fields

> *"I think prime numbers are like life. They are very logical but you could never work out the rules, even if you spent all your time thinking about them."*
> *– Mark Haddon, The Curious Incident of the Dog in the Night-Time* [14]

A nice property of a given prime p is that the set $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$ forms a finite field where modular arithmetic is performed with respect to p; this happens to be very handy for cryptographic purposes. Let $\mathbb{F}_p^\times := \{1, \ldots, p-1\}$ for the sake of notation.

An elliptic curve over a finite field modulo $p \neq 2, 3$ is the set of points

$$E = \{(x, y) \in \mathbb{F}_p^2 : y^2 \equiv x^3 + Ax + B \pmod{p}\} \cup \{\mathcal{O}\} \tag{2}$$

with $A, B \in \mathbb{F}_p$ and $-16(4A^3 + 27B^2) \not\equiv 0 \pmod{p}$. We have $\mathcal{O}$ as the "point at infinity", which will be defined a couple sections later [15].

Elliptic curves over prime fields tend to look like a bunch of scattered points, especially for large values of p, as shown in Figure 3.

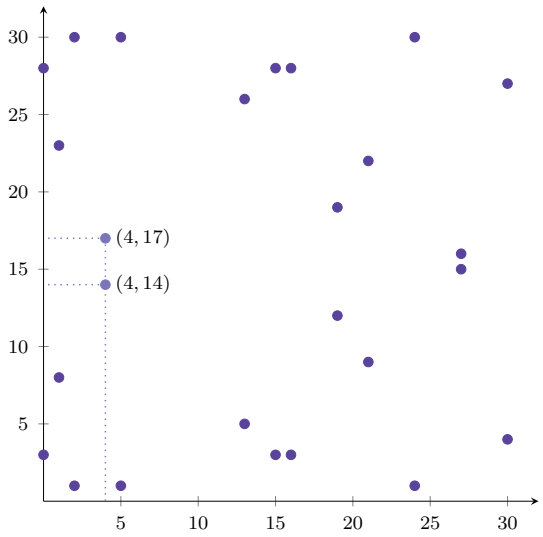


Figure 3: $E : y^2 \equiv x^3 - 8x + 9 \pmod{31}$

We now introduce a few convenient results that lead to the computation of points on elliptic curves over prime fields.

Fermat's Little Theorem

First, consider this particular case of the Euler-Fermat Theorem.

Fermat's Little Theorem. [19] *Suppose that p is prime and $\gcd(a, p) = 1$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. [19] Consider the sets $\mathbb{F}_p^\times$ and $S := \{a, 2a, \ldots, (p-1)a\}$.

First, we show that all elements of S are distinct modulo p. Suppose that $sa \equiv ta \pmod{p}$ for some $s, t \in \mathbb{F}_p^\times$. Then by coprime cancellation, we have $s \equiv t \pmod{p}$.

Because there are $p - 1$ distinct elements modulo p in both sets $\mathbb{F}_p^\times$ and S, each element in $\mathbb{F}_p^\times$ must be congruent modulo p to a unique element in S and vice versa. Hence,

$$a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdots \times (p-1) \pmod{p}.$$

Moreover, since all elements of $\mathbb{F}_p^\times$ are coprime to p, cancellation gives

$$a^{p-1} \equiv 1 \pmod{p}$$ □

Quadratic residues

Given an elliptic curve E as presented in Equation (2) and some $x \in \mathbb{F}_p$, does there necessarily exist $y \in \mathbb{F}_p$ such that (x, y) is a point on the curve? Spoiler alert, no.

Suppose that p is an odd prime and $a \in \mathbb{F}_p \setminus \{0\}$. If there exists $y \in \mathbb{F}_p \setminus \{0\}$ such that $y^2 \equiv a \pmod{p}$, then a is said to be a *quadratic residue modulo* p. Otherwise, a is a *quadratic nonresidue* [19].

We next introduce the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue}\,; \\ -1 \text{ if } a \text{ is a quadratic nonresidue}. \end{cases}$$

This has nothing to do with fractions! [19]

For $p = 7$, observe the following table.

x		1	2	3	4	5	6
x^2	$\pmod 7$	1	4	2	2	4	1

By this table, 1, 2 and 4 are quadratic residues modulo 7, while 3, 5 and 6 are quadratic nonresidues. Hence,

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = \quad 1 \qquad \text{and} \qquad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1\,.$$

Convince yourself that, for any distinct $y_1, y_2 \in \mathbb{F}_p^\times$, $y_1^2 \equiv y_2^2 \pmod{p}$ if and only if $y_1 = -y_2$. As a result, for any given p, precisely half the elements in the set $\mathbb{F}_p^\times$ are quadratic residues. Furthermore, it makes sense to say that roughly half of the x values on an elliptic curve have corresponding y values [19].

So after computing $x^3 + Ax + B \pmod{p}$ for some $x \in \mathbb{F}_p$, it is possible to search through all the quadratic residues without finding a value of y that allows the equation to hold. Well, this seems disappointing.

But there is in fact an easy way to check whether or not a number is a quadratic residue, known as Euler's Criterion [19].

Proposition 1. (Euler's Criterion)[19] *If p is an odd prime with $a \in \mathbb{F}_p^\times$, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}\,.$$

Before proving this, we present the concept of primitive roots. An integer g is a *primitive root modulo* p if, for every element $a \in \mathbb{F}_p^\times$, there exists a unique integer i such that $g^i \equiv a \pmod{p}$. Conversely, for every $i \in \mathbb{F}_p^\times$, $g^i \pmod{p}$ takes on a unique value in $\mathbb{F}_p \setminus \{0\}$. As a result, $g^i \equiv 1 \pmod{p}$ if and only if $i = p - 1$ for $i \in \mathbb{F}_p^\times$, by Fermat's Little Theorem. It can also be shown that every odd prime number has at least one primitive root [19].

Proof of Euler's Criterion. [19] If $a \in \mathbb{F}_p^\times$, then a is coprime to p. By Fermat's Little Theorem,

$$a^{p-1} \equiv \left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$$

and so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

Suppose that a is a quadratic residue. Then $\left(\frac{a}{p}\right) = 1$ and by definition there exists $y \in \mathbb{F}_p^\times$ such that $y^2 \equiv a \pmod{p}$. So, by Fermat's Little Theorem since y is nonzero,

$$a^{\frac{p-1}{2}} \equiv (y^2)^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Now suppose that a is a quadratic nonresidue and let g be a primitive root modulo p such that $g^i \equiv a \pmod{p}$ for some odd integer $i = 2k+1$ with $k \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) = -1$ and

$$a^{\frac{p-1}{2}} \equiv \left(g^{2k+1}\right)^{\frac{p-1}{2}} \equiv \left(g^k\right)^{p-1} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}.$$

We have that

$$\left(g^{\frac{p-1}{2}}\right)^2 \equiv g^{p-1} \equiv 1 \pmod{p}.$$

Under any prime modulus, 1 has just the two square roots ± 1, so since p is prime, $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Since g is a primitive root, we cannot have $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so

$$g^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}. \qquad \square$$

Computing points on elliptic curves over $\mathbb{F}_p$

In elliptic curve cryptography which shall be explored later, curves over prime fields $\mathbb{F}_p$ where $p+1$ is divisible by 4 are commonly used. We present the mathematics behind finding points on curves over such fields, although in practice, these calculations are performed by computer programs.

Firstly, for a given $x \in \mathbb{F}_p$, compute $x^3 + Ax + B \pmod{p}$ and use Euler's Criterion to check whether the result is a quadratic residue. If not, then clearly there is no need to continue. Otherwise, we have the following formula [19].

Proposition 2. [19] *If 4 divides $p+1$ and a is a quadratic residue modulo p, then the number y satisfying $y^2 \equiv a \pmod{p}$ is given by*

$$y \equiv \pm a^{\frac{p+1}{4}} \pmod{p}. \tag{3}$$

Proof. [19] By Fermat's Little Theorem and Euler's Criterion,

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} a \equiv 1a \equiv a \pmod{p}. \qquad \square$$

If a nonzero solution y to $y^2 \equiv a \pmod{p}$ exists, then there are exactly two of them [19].

It is time to run through an example with the elliptic curve

$$E : y^2 \equiv x^3 - 8x + 9 \pmod{31}$$

Given $x = 4$, find both corresponding values of y if they exist. We have that

$$x^3 - 8x + 9 = 4^3 - 4 \times 8 + 9 \equiv 10 \pmod{31}.$$

The next step is to check whether 10 is a quadratic residue using Euler's Criterion, and indeed it is: $\left(\frac{10}{31}\right) = 10^{\frac{31-1}{2}} \equiv 1 \pmod{31}$. Now the y values at these points can be computed from Equation (3):

$$y \equiv \pm 10^{\frac{31+1}{4}} \equiv \pm 14 \pmod{31}$$

and it follows that $(4, 14)$ and $(4, -14) = (4, 17)$ are points on the curve as shown in Figure 3.

5 Properties of elliptic curves

> *"It is not knowledge, but the act of learning, not possession, but the act of getting there, which grants the greatest enjoyment."*
> *– Carl Friedrich Gauss* [11]

We have seen that elliptic curves can look quite different, depending on the field over which they are defined. But regardless, all of them exhibit certain geometrical properties that allow the set of points on any given curve to form a group, which will be discussed in detail later below [29].

Firstly, as you may have already noticed, elliptic curves are horizontally symmetrical. This fact is useful as we will be reflecting points later on.

Now consider sketching a line between two points on the curve, extending both ends to infinity. Will the line hit the curve again?

Proposition 3. [29] *If a non-vertical line $L : y = mx + c$ with $m, c \in K$ intersects an elliptic curve $E : y^2 = x^3 + Ax + B$ over field K at two distinct points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then, counting with multiplicity, the line intersects the curve at a third point $P_3 = (x_3, y_3)$.*

Proof. [29] Suppose that the line L connects the distinct points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the elliptic curve E over field K. We claim that L intersects E at a third point. The intersection points are the solutions to the system of equations

$$\begin{aligned} y &= mx + c \\ y^2 &= x^3 + Ax + B \end{aligned}$$

or, equivalently, solutions of $(mx + c)^2 = x^3 + ax + b$. Rearranging gives the cubic polynomial equation $x^3 - m^2x^2 + (A - 2mc)x + (B - c^2) = 0$.

As $x_1, x_2 \in K$ are both solutions to this equation, Vieta's sum of roots formula implies that there exists a third root x_3 such that $x_1 + x_2 + x_3 = -(A - 2mc)$. Since $A, m, c \in K$, it follows that x_3 and $y_3 = mx_3 + c$ also belong to the field K.

Hence, the line L intersects E at a third point $P_3 = (x_3, y_3)$. □

As these points are counted with multiplicity, a non-vertical line tangent to a point on an elliptic curve will intersect the curve at exactly one other point.

These properties are quite special, as they give rise to defining point arithmetic.

6 Arithmetic with elliptic curves

"Groups, as men, will be known by their actions." – Guillermo Moreno

For the next part, it might help to forget some of the mathematics you've learnt in kindergarten. Here, elliptic curve arithmetic will be defined abstractly, and in way such that it follows a set of rules known as the group axioms.

Group axioms

If a non-empty set G with a defined binary operation $+$ satisfies the following axioms, then G is said to be a *group under* $+$.

(G1) Closure: $a + b \in G$ for all $a, b \in G$.

(G2) Associativity: $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

(G3) Identity: There is an element $e \in G$ such that $a + e = e + a = a$ for all $a \in G$.

(G4) Inverse: For each $a \in G$, there is an element $-a \in G$ such that $a + (-a) = e$.

A group is *Abelian* if its operation $+$ is *commutative*: $a + b = b + a$ for all $a, b \in G$ [19]. As a conventional example, the real numbers are an Abelian group under addition.

Groups are defined by the interactions between elements rather than the elements themselves, so the binary operation has quite an important job. A group of cats could form a perfectly valid group as long as all the group rules are followed, such as defining what an inverse cat is!

We now establish arithmetic in a particular way, so that elliptic curves form Abelian groups under point addition.

The point at infinity

To satisfy these axioms, elliptic curves are extended to the set

$$E = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is known as *the point at infinity* [29].

In order to see what this means, we operate in projective space. Consider an elliptic curve on a two-dimensional plane $z = 1$ over a unit sphere about the origin. A line is to be drawn from all points of the curve to the centre of the sphere, which gives rise to

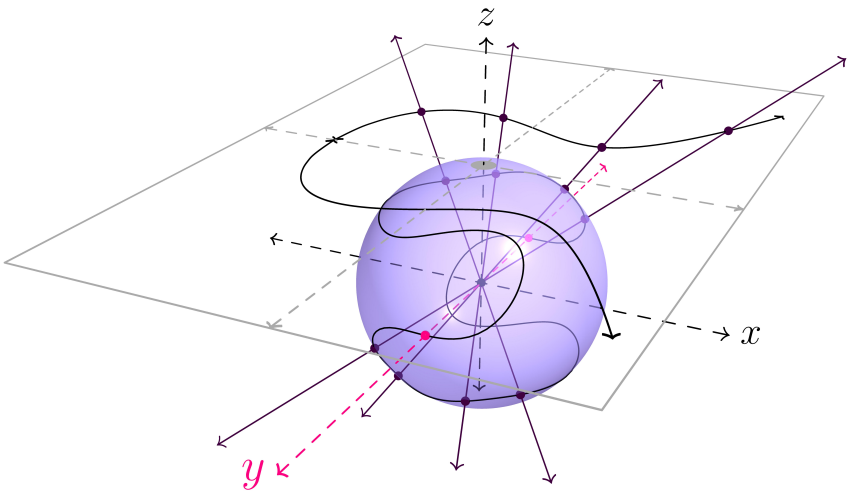


Figure 4: Schematic stereographic projection of an elliptic curve onto a sphere.

two points of intersection at the surface of the sphere. Taking these intersection points to form a new curve on the sphere, this process is called stereographic projection [29].

The surface intersection points make up the projected elliptic curve, which is the set

$$E_{\text{projection}} = \{(X : Y : Z) \in \mathbb{P}^2(K) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\} \tag{4}$$

where $\mathbb{P}^2(K)$ refers to the projected elements of the field K, and $(X : Y : Z)$ is the set of all ordered triples $(\lambda X, \lambda Y, \lambda Z)$ for $\lambda \in K$. In order to convert from projective coordinates back to Cartesian coordinates, the function $(X, Y, Z) \mapsto (X/Z, Y/Z)$ is to be applied. It makes sense that infinity occurs at $Z = 0$, and plugging it into Equation (4) requires $X^3 = 0$ and hence $X = 0$. However, there is no restriction on Y, so the set $(0 : 1 : 0)$ accounts for the point at infinity [29].

Geometrically, over the reals, as both sides of the Cartesian curve approach $\pm\infty$, the point projections get closer and closer to the y-axis $(0 : 1 : 0)$, as presented in Figure 4. This naturally gives rise to the point at infinity in two-dimensional space [29].

This point at infinity $\mathcal{O}$ is the identity element of the group E over "addition", established below. Funnily enough, the additive identity is also sometimes known as the zero element, but here the "zero element" happens to be the point at infinity!

Addition

In order to define addition $\oplus$ between two points on some elliptic curve E, we begin by drawing a line through two points P_1 and P_2 on the curve. If $P_1 = P_2$, then simply take the tangent. Either way, counting with multiplicity, if this line is not vertical, then it will intersect the curve at a third point, which we take and reflect across the axis of symmetry. It is this reflection that shall be defined as $P_1 \oplus P_2$, as shown in Figure 5 [29].

For now, we operate under the assumption that the line joining P_1 and P_2 is not vertical.

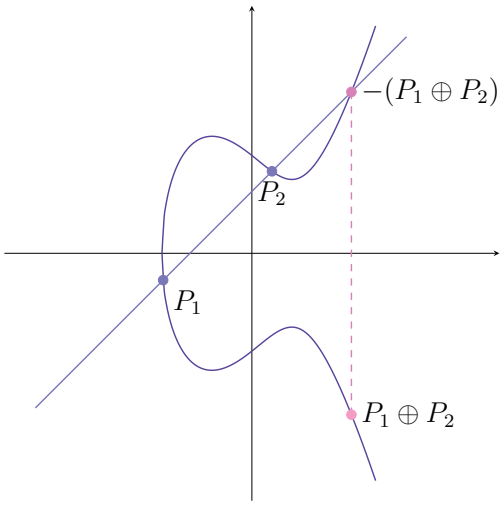


Figure 5: Point addition with elliptic curves over the real numbers

Over a finite field modulo p, the x and y values loop back to 0 right as they hit $p-1$, as presented in Figure 6 [15].

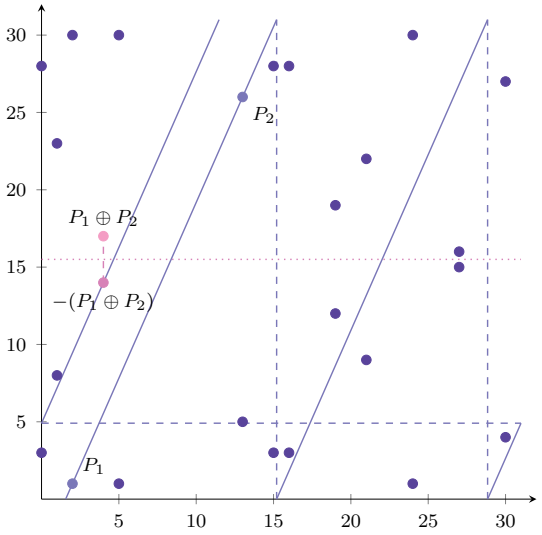


Figure 6: Point addition with elliptic curves over the prime field $\mathbb{F}_{31}$ [15]

A natural question to pose now would be of the necessity of reflecting the point across the horizontal line of symmetry. Why not simply define $P_1 \oplus P_2$ to be the third point of intersection when a line is drawn through the points? Suppose that point addition is to be defined as $P_1 \oplus P_2 = P_3$, the third point of intersection. Then geometrically, $P_2 \oplus P_3 = P_1$ and $P_1 \oplus P_3 = P_2$. Hence, $P_1 \oplus P_2 = P_1 \oplus P_1 \oplus P_3 = P_3$ and so $P_1 \oplus P_1 = \mathcal{O}$ implies $P_1 = -P_1$, which – as P_1 is arbitrary – is not true for most points [29].

Now the above definition of addition is to be made sense of algebraically, generalising to any arbitrary field K. Note that the inverse of $P = (x, y)$ is $-P = (x, -y)$.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be elements of $E = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$. The binary operation of point addition $\oplus$ between points P_1 and P_2 is defined as follows. If $P_1 \neq -P_2$, then $P_1 \oplus P_2 = (x_3, y_3)$ with

$$x_3 = m^2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = m(x_1 - x_3) - y_1\,, \tag{5}$$

where

$$m = \begin{cases} (y_1 - y_2)(x_1 - x_2)^{-1} & \text{if } P_1 \neq P\,; \\ (3x_1^2 + A)(2y_1)^{-1} & \text{if } P_1 = P_2\,. \end{cases} \tag{6}$$

Here, $^{-1}$ denotes the multiplicative inverse [15].

Observe that, for any $P \oplus P'$, the magnitude of m approaches infinity as P' approaches $-P$, so it is quite intuitive to let $P \oplus (-P) = \mathcal{O}$. Geometrically, this corresponds to a vertical line passing through the curve. Moreover, since $\mathcal{O}$ is the identity element, $P \oplus \mathcal{O} = P$ for all points on the curve [29].

We now offer the derivation of (5) for elliptic curves over the real numbers. Suppose that P_1 and P_2 are points on the elliptic curve $E = \{(x, y) \in \mathbb{R} : y^2 = x^3 + Ax + B\}$.

If $P_1 \neq P_2$, then the equation of the line connecting the points is

$$y - y_1 = m(x - x_1) \tag{7}$$

with $m = \frac{y_1 - y_2}{x_1 - x_2}$. Substituting into E yields

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

which expands to $x^3 - m^2x^2 + Cx + D = 0$ for some $C, D \in \mathbb{R}$. As x_1 and x_2 are solutions of the polynomial equation and a third solution x_3 exists by Proposition 3, the polynomial can be factorised as

$$\begin{aligned} x^3 - m^2x^2 + Cx + D &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3\,. \end{aligned}$$

Matching coefficients, we obtain that $x_1 + x_2 + x_3 = m^2$, and so $x_3 = m^2 - x_1 - x_2$. It follows from Equation (7) that the corresponding y value reflected across the x-axis is $y_3 = -(m(x_3 - x_1) + y_1) = m(x_1 - x_3) - y_1$ [29].

In the case $P_1 = P_2$, implicit differentiation yields $2yy' = 3x^2 + A$, and it follows that $m = (3x_1^2 + A)/2y_1$. Applying the same argument as above gives Equation (5) [15].

As an example, suppose that $E : y^2 \equiv x^3 - 8x + 9 \pmod{31}$. We shall compute $(1, 4) \oplus (7, 20) = (x_3, y_3)$ using Equation (5), as follows. First calculate

$$m = (4 - 20)(1 - 7)^{-1} = 16 \times 6^{-1} \equiv 16 \times 26 \equiv 13 \pmod{31}\,.$$

Note that $6^{-1} = 26$ since $6 \times 26 \equiv 1 \pmod{31}$. Then

$$\begin{aligned} x_3 &\equiv 13^2 - 1 - 7 \equiv 6 \pmod{31}\,; \\ y_3 &\equiv 13(1 - 6) - 4 \equiv 24 \pmod{31}\,. \end{aligned}$$

Hence, $(1, 4) \oplus (7, 20) = (6, 24)$.

Scalar multiplication

As is familiar, scalar point multiplication is merely repeated addition. For some point on the curve P and integer k, define as in [15] the product

$$kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ times}} .$$

A point P on an elliptic curve over a prime field repeatedly added to itself eventually yields $kP = \mathcal{O}$ for some integer k. Then the set $\{P, 2P, \ldots, kP\}$ generated by P forms a cyclic subgroup of E with k distinct elements, or order k. It is a literal cycle, since $\mathcal{O} \oplus P$ takes us back to P [15].

A generator G is a point on the curve such that all elements in the set E may be obtained by applying scalar multiplication to G. Moreover, if a generator exists on an elliptic curve over a prime field, all points on the curve form a cyclic group [15].

To see an example, take $E = \{(x, y) \in \mathbb{F}_{31} : y^2 \equiv x^3 - 8x + 9 \pmod{31}\} \cup \{\mathcal{O}\}$ and $P = (4, 14)$. Then

$$\begin{aligned} 2P &= (4, 14) \oplus (4, 14) = (1, 8) \\ 3P &= (1, 8) \oplus (4, 14) = (30, 27) \\ &\vdots \\ 8P &= (4, 17) = -P \\ 9P &= \mathcal{O} \end{aligned}$$

and so $P = (4, 14)$ generates a cyclic subgroup of E with order 9.

As it turns out, this seemingly odd way of defining addition and multiplication over elliptic curves works neatly in cryptography.

7 Top secret: elliptic curve cryptography

> *"One must acknowledge with cryptography no amount of violence will ever solve a math problem." – Jacob Appelbaum* [3]

Say hello to the characters central to any cryptography textbook: Alice, Bob and Eve the notorious eavesdropper, who we assume to be a basement hacker without a quantum computer. Alice and Bob wish to secretly converse with each other without their messages being intercepted by anyone, especially Eve. Assume all direct communication between Alice and Bob to made via an insecure channel.

Like Alice and Bob, people have necessitated confidential ways to communicate for thousands of years, so they made and developed cryptosystems – others have broken them, or at least tried to.

Elliptic-curve cryptography is now widely used in modern cryptographic protocols, so elliptic curves play an important role in practical cryptography [15, 7]. An

important precursor was Hendrik Lenstra's 1985 discovery of an integer-factorisation method based on elliptic curves, later published in 1987 [22]. In 1985, Neal Koblitz [20] and Victor Miller [23] independently proposed the use of elliptic curves in public-key cryptography. Their proposals initiated the modern development of elliptic-curve cryptography, which has since become standardised and widely deployed.

Hard problems

Elliptic curve cryptography is a form of public-key cryptography. Public-key schemes use public information together with private secret information; depending on the scheme, public keys are used for tasks such as encryption or signature verification, while private keys are used for decryption or signing. Their security is based on computational problems that are easy to evaluate in the forward direction but believed difficult to reverse without the secret information [10, 18].

But what does it mean for something to be computationally hard? Time complexity is a quantification of how quickly the number of required bit operations increase as the size of the input gets larger. An algorithm is said to be *polynomial time* if its bit operation growth rate is proportional to some polynomial function of the input size. If a problem is computationally hard, then there is no feasible polynomial time algorithm that can solve it. Moreover, if the number of necessary bit operations for an algorithm surges exponentially as the input size goes up, then it runs in exponential time. Sub-exponential time algorithms are those with greater time complexity than polynomial, but not quite exponential [30].

Scalar point multiplication on elliptic curves can be computed efficiently, whereas the inverse problem is believed to be computationally difficult for appropriately chosen groups. This asymmetry is what elliptic-curve cryptography exploits.

The Elliptic Curve Discrete Logarithm Problem. [15]
For an elliptic curve $E = \{(x, y) \in \mathbb{F}_p : y^2 \equiv x^3 + Ax + B \pmod{p}\}$ *with* $A, B \in \mathbb{F}_p$*, given a generator point* G *and another point* P*, find* x *such that* $xG = P$ *with scalar multiplication defined as above.*[6]

For appropriately chosen large parameters, this problem is believed to be computationally infeasible for classical attackers and serves as the foundation of the elliptic curve Diffie-Hellman protocol, ElGamal encryption, and the Elliptic Curve Digital Signature Algorithm [15].

Elliptic curve Diffie-Hellman

The Elliptic Curve Diffie-Hellman key exchange is a public-key key-agreement protocol that allows Alice and Bob to derive a shared secret over an insecure channel [10, 23, 15].

The first step is to publicly agree on a large prime p, an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, and a point $P \neq \mathcal{O}$ on the curve with substantial order n, ideally a generator. Thus, (E, p, P) is the public key.

Alice privately selects an integer $a \in \{1, \ldots, n-1\}$, computes aP and sends it to Bob, who does the same; Bob chooses $b \in \{1, \ldots, n-1\}$ and sends Alice bP.

Now Alice computes $a(bP)$ and Bob $b(aP)$, yielding the same result, as they are essentially both adding the point P to itself $ab = ba$ times. It follows that abP is their secret key, and they can easily create more keys by choosing new values of a and b.

Eve knows the prime p, the elliptic curve E, and the generator P. Suppose that she has also managed to find aP and bP. It is here the Elliptic Curve Discrete Logarithm Problem comes into play; given P, aP and bP, find a or b, and subsequently abP. For appropriately chosen parameters, known classical methods do not allow Eve to recover the shared secret feasibly from this public information [15].

Using $E : y^2 = x^3 + 129x + 23$, $p = 211$ and $P = (127, 24)$ with $n = 238$ as an example, suppose Alice and Bob privately choose $a = 121$ and $b = 99$, respectively. Now, Alice evaluates $121P = (60, 147)$ and sends it to Bob; he calculates $99P = (12, 150)$ and sends it to Alice. Finally, Alice and Bob use the numbers they each privately chose to compute $121(99P) = 121(12, 150)$ and $99(121P) = 99(60, 147)$ accordingly, yielding $(134, 194)$ as their shared secret. The point $P = (127, 24)$ is a generator for this particular curve E, making it a good choice for the public key.

Elliptic curve ElGamal encryption

In comparison with the above protocol, the elliptic curve ElGamal encryption method is more complicated as it requires extra steps. To aid with understanding, an example of elliptic-curve ElGamal encryption will be run simultaneously [12, 15].

Again, Bob chooses a prime p, an elliptic curve E over $\mathbb{F}_p$ and a point P with large order n. Moreover, he privately selects a positive integer $b \in \{1, \ldots, n-1\}$. He then computes $Q = bP$ and broadcasts the public key (E, p, P, Q). In our example, Bob chooses $E : y^2 = x^3 + 129x + 23$, $p = 211$ and a generator point $P = (127, 24)$ with $n = 238$. He then selects $b = 96$, which stays secret, and publicises $Q = bP = (187, 48)$.

If Alice wants to send a message, then she first encodes it as a sequence of points $M = (M_1, \ldots, M_h)$ on E[3], here, say, just a single point $M = (30, 64)$.

Next, Alice privately picks a positive number $a \in \{1, \ldots, n-1\}$, computes the points $R_i = M_i \oplus aQ$ for all $1 \leq i \leq h$ and sends the new sequence of points $R = (R_1, \ldots, R_h)$ to Bob. Suppose that she takes $a = 63$. Then

$$R = M \oplus aQ = (30, 64) \oplus 63(187, 48) = (190, 162)\,.$$

Lastly, Alice sends Bob aP, which in this case is $63(127, 24) = (181, 176)$.

Given that Bob kept his b secret, only he can decrypt Alice's message by computing

$$M_i = R_i \oplus (-aQ) = R_i \oplus (-a(bP)) = R_i \oplus (-b(aP))\ .$$

Here, Bob has the information $R = (190, 162)$, $aP = (181, 176)$ and $b = 96$, and hence obtains Alice's point:

$$M = R \oplus (-b(aP)) = (190, 162) \oplus (-96(181, 176)) = (190, 162) \oplus (86, 205) = (30, 64)\,.$$

[3]Methods of encoding points on elliptic curves are described in [20].

Bob subsequently reads her message.

Like everyone else, Eve knows Bob's public key (E, p, P, Q). With a little bit of digging, she can find R and aP, but she wants to know M. However, she cannot obtain any point $M_i = R_i \oplus (-aQ) = R_i \oplus (-b(aP))$ without knowing Alice's a or Bob's b, due to the difficulty of the Elliptic Curve Discrete Logarithm Problem once again.

Elliptic curve digital signature algorithm

A digital signature, which uses cryptographic methods to certify authenticity and integrity online, is a bit like the classic handwritten one, except it is unsurprisingly digital and is designed to make forgery computationally infeasible [24, 18].

As the name suggests, the Elliptic Curve Digital Signature Algorithm is used to generate digital signatures. Bitcoin has used ECDSA to authorise transactions controlled by ECDSA keys [2]. Once more, we go through an example of ECDSA [17, 24].

Suppose there is a curve E over $\mathbb{F}_p$ and a point P with a large prime order n, as well as another point $Q = kP$; all of this is public information, except for the number $k \in \{1, \ldots, n-1\}$ which is Alice's secret "password". The goal is for her to confirm her identity by proving that she knows k without revealing the private key itself. She does this by digitally signing a message, which anyone with access to it can verify. Let $E : y^2 = x^3 + 95x + 27$, $p = 211$ and $P = (2, 15)$ with $n = 227$. Suppose that $k = 187$ and hence $Q = 187(2, 15) = (13, 100)$.

Alice takes her message and applies a cryptographic hash function to get the corresponding message digest m. A cryptographic hash function maps an input of arbitrary length to a digest of fixed length. Distinct inputs can in principle have the same digest, but a secure hash function is designed to make finding such collisions, or recovering an input from its digest, computationally difficult. Small changes to the input typically produce apparently unrelated digests [18]. Here, presume that the message digest is $m = 121$.

Then Alice randomly chooses some private $a \in \{1, \ldots, n-1\}$, finds $R = aP \neq \mathcal{O}$ and takes its x-coordinate, denoted as r. She computes the identifying part of this signature $s = a^{-1}(m + rk) \bmod n$. Both r and s must be nonzero; otherwise, she needs to choose a different value of a. Now Alice sends off to Bob her original message, and its respective digital signature (r, s). If Alice takes $a = 133$, then $R = 133(2, 15) = (15, 117)$ and so $r = 15$. Subsequently, $s = 133^{-1}(121 + 15 \times 187) \bmod 227 = 22$ and hence $(r, s) = (15, 22)$.

To verify the signature, Bob uses the same hash function to obtain the message digest m, then evaluates $u_1 = m \times s^{-1} \bmod n$ and $u_2 = r \times s^{-1} \bmod n$. He next determines the point $S = u_1 P \oplus u_2 Q$ and deems the signature valid if and only if the x-coordinate of S is equal to r. In our case, Bob hashes the message to obtain $m = 121$ and finds $u_1 = 121 \times 22^{-1} \bmod 227 = 119$, $u_2 = 15 \times 22^{-1} \bmod 227 = 11$ and thus $S = 119(2, 15) \oplus 11(13, 100) = (15, 117)$. The x-coordinate of S is equal to $r = 15$, and so the legitimacy of Alice's identity is proven.

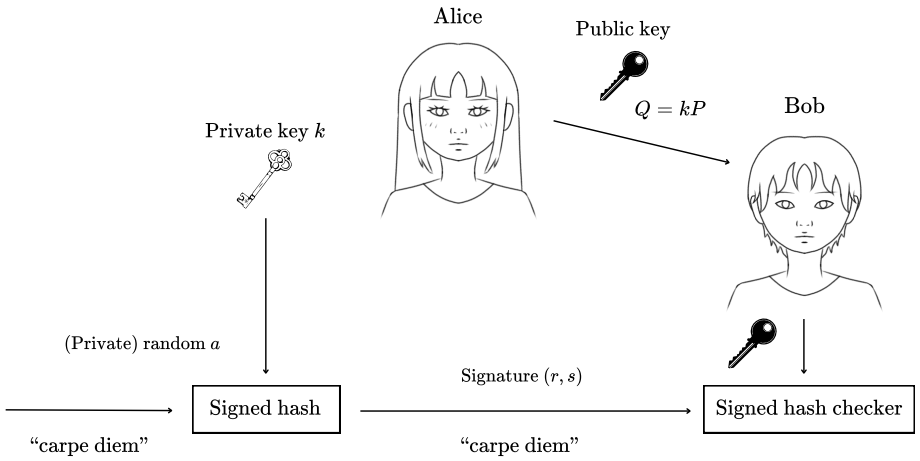


Figure 7: Visual summary of the Elliptic Curve Digital Signature Algorithm [17, 24]

Mathematically, why does this work? As $s \equiv a^{-1}(m + rk) \bmod n$,

$$a \equiv s^{-1}(m + rk) \equiv (m \times s^{-1}) + k(r \times s^{-1}) \equiv u_1 + u_2 k \pmod{n}.$$

and hence

$$R = aP = (u_1 + u_2 k)P = u_1 P \oplus u_2 kP = u_1 P \oplus u_2 Q = S.$$

Eve is up to no good as usual, and wants to forge Alice's signature. Eve, knowing $\{E, p, P, n, Q\}$, creates a message and hashes it to obtain m', then selects her $e \in \{1, \ldots, n-1\}$ and finds $R' = eP$ with x-coordinate r'. In order for Eve's plot to work, she needs to compute $s' = e^{-1}(m' + r'k) \bmod n$, which if done successfully, Bob would validate. Unluckily for Eve, she does not know k and the Elliptic Curve Discrete Logarithm Problem yet again stops her from finding it.

You really thought Eve would give up by now? Think again. She decides to use some random value k' in place of k. Taking $s' = e^{-1}(m' + r'k') \bmod n$, she sends (r', s') to Bob along with her original message. He obtains m' with the hash function, then computes $u'_1 = m' \times (s')^{-1} \bmod n$, $u'_2 = r' \times (s')^{-1} \bmod n$ and subsequently $S' = u'_1 P + u'_2 Q$ to check whether the x-coordinate of S' is equal to r'. However,

$$e \equiv (s')^{-1}(m' + r'k') \equiv (m' \times (s')^{-1}) + k'(r' \times (s')^{-1}) \equiv u'_1 + u'_2 k' \not\equiv u'_1 + u'_2 k \pmod{n}.$$

and so

$$R' = eP = (u'_1 + u'_2 k')P = u'_1 P \oplus u'_2 k' P \neq u'_1 P \oplus u'_2 Q = S'.$$

Thus, Eve's signed message is invalid.

The crux of this scheme is that Alice knowing k allows her to use it to create the s component of the signature, which confirms her identity.

Security and limitations

But 211 is a very small prime! In order for a cryptosystem to be secure, much larger parameters are needed. There are a number of standardised elliptic curves recommended by organisations such as the National Institute of Standards and Technology for cryptographic schemes [7].

The Elliptic Curve Discrete Logarithm Problem and integer factorisation, on which RSA is based, are distinct computational problems [26]. There exist sub-exponential classical algorithms for integer factorisation; however, for general well-chosen elliptic-curve groups, no sub-exponential classical algorithm for the Elliptic Curve Discrete Logarithm Problem is known. The best known generic attacks, such as Pollard's rho method, require on the order of $\sqrt{n}$ group operations for a group of order n [15].

Consequently, elliptic-curve cryptography can achieve a comparable classical security strength with substantially smaller keys than RSA:

RSA key size (bits)	Elliptic Curve Cryptography key size (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

Figure 8: RSA key sizes corresponding to required key sizes for elliptic curve schemes of equivalent cryptographic strength. [4]

To achieve a given classical security strength, the key sizes needed for elliptic-curve cryptography are significantly smaller. This can reduce storage and communication overhead and can be advantageous on resource-constrained devices [4].

However, elliptic curve cryptography has its own limitations.

Compared to other cryptosystems, those involving elliptic curves can be difficult to implement correctly, so implementation errors may compromise security. Sony's PlayStation 3, released in 2006, provides a famous example: in December 2010 the fail0verflow team publicly demonstrated that Sony's ECDSA implementation reused a fixed nonce, allowing the signing private key to be recovered [13, 17]. With a few algebraic manipulations, try to hack it yourself: given two signatures that use the same random integer a, find a, and subsequently the private key k.

Elliptic-curve cryptography can also be vulnerable to attacks when unsuitable curves, parameters, or implementations are used, which is why standardised parameter choices and careful implementation matter [15, 7].

You *really* thought Eve would have given up by now? You're right, the basement hacker gone. She's not the villain for ensuring safe secret keeping for us all anyway.

But the battle is still not over; unfortunately, elliptic-curve cryptography is not quantum-safe. In 1994, Peter Shor proposed polynomial-time quantum algorithms for integer factorisation and discrete logarithms. Consequently, a sufficiently large fault-tolerant quantum computer would break RSA and elliptic-curve systems based on the

discrete logarithm problem [28, 1]. No such quantum computer currently exists, and the timeline for one is uncertain; this threat is a principal motivation for the development and standardisation of post-quantum cryptography [1].

Isogeny-based cryptography

This is not a goodbye to elliptic curves though; isogeny-based cryptography is a proposed post-quantum scheme that involves functions sending these curves to one another [8].

Consider two elliptic curves E_1 and E_2. An isogeny $\phi : E_1 \to E_2$ is a function that maps an arbitrary point P_1 on E_1 to a new point P_2 on E_2 whilst maintaining structural properties. Isogeny-based cryptography relies on computational problems involving isogenies between elliptic curves [8].

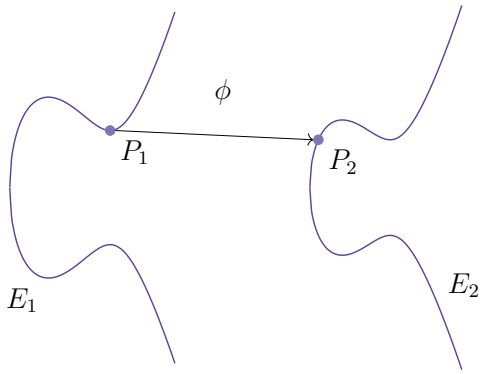


Figure 9: An isogeny mapping one elliptic curve to another

A prominent line of isogeny-based cryptography began with the supersingular-isogeny construction of Luca De Feo, David Jao and Jérôme Plût [8]. The later SIKE (*Supersingular Isogeny Key Encapsulation*) submission, which was based on SIDH, advanced to Round 4 of the National Institute of Standards and Technology's post-quantum cryptography process [1]. In 2022, Wouter Castryck and Thomas Decru found an efficient classical key-recovery attack on SIDH; their original implementation broke the SIKEp434 parameter set in roughly ten minutes on a single core [5]. The attack broke the SIDH/SIKE family, and the SIKE team now states that SIKE and SIDH are insecure and should not be used [1].

Despite this pitfall, research on other isogeny- and class-group-action-based constructions continues. Schemes such as CSIDH and SeaSign were proposed as post-quantum constructions [6, 9]. They are not based on SIDH and are not broken by the Castryck–Decru attack, but continued cryptanalysis is necessary before emerging constructions can be trusted for high-stakes real-world applications [1].

8 The Congruent Number Problem

"The definition of a good mathematical problem is the mathematics it generates rather than the problem itself."
– Andrew Wiles [35]

Dating back – as far as we know – to 10th century Arab manuscripts, the unsolved Congruent Number Problem is one of the oldest in the history of mathematics [32].

A positive integer n is said to be *congruent* if there exists a right triangle of area n with all sides having rational length. In other words, there are rational numbers a, b, c satisfying the simultaneous equations

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{1}{2}\, ab = n\,. \tag{8}$$

For example, 5 is a congruent number, as seen in Figure 10.

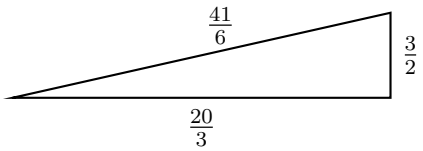


Figure 10: Area $= \frac{1}{2} \times \frac{3}{2} \times \frac{20}{3} = 5$

The Congruent Number Problem. [32] *Given a positive integer n, determine whether it is congruent; if so, find all right triangles of area n with only rational side lengths.*

We now explore its link to elliptic curves.

Proposition 4. [29, 32] *A positive integer n is congruent if and only if the elliptic curve $E : y^2 = x^3 - n^2 x$ has a rational point with $y \neq 0$.*

Proof. [29] Due to the restriction $y \neq 0$, if (x, y) is a rational point on an elliptic curve $E : y^2 = x^3 - n^2 x$, then $x \neq 0, \pm n$.

Suppose that there exist rational numbers a, b, c satisfying (8) for some positive number n. Then taking $x = n\,\frac{a+c}{b}$ and $y = 2n^2\,\frac{a+c}{b^2}$, we have that $x = \frac{1}{2}\,a(a+c)$ and $y = \frac{1}{2}\,a^2(a+c)$. Substituting this into E gives

$$\begin{aligned} y^2 = \frac{1}{4}\,a^4(a+c)^2 &= \frac{1}{2}\,a(a+c)\,\frac{1}{2}\,a^3(a+c) \\ &= x\Big(\frac{1}{4}\,a^2(a+c)^2 - \frac{1}{4}\,a^2b^2\Big) = x(x^2 - n^2) = x^3 - n^2 x\,. \end{aligned}$$

Hence, $(x, y) = (n\,\frac{a+c}{b}, 2n^2\,\frac{a+c}{b^2})$ is a point on the elliptic curve E and it is clear that $y \neq 0$.

Conversely, assume x, y are nonzero rational numbers with $y^2 = x^3 - n^2x$ for some positive integer n. Let

$$a = \frac{y}{x}\,, \quad b = \frac{2nx}{y} \quad \text{and} \quad c = \frac{2x^3 - y^2}{xy} = \frac{x^2 + n^2}{y}\,.$$

Then $\frac{1}{2}ab = n$, and

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

so $a^2 + b^2 = c^2$. Thus, n is congruent. □

It is highly likely that discovering this close association between the congruent number problem and elliptic curves has steered us in the right direction to finding an actual solution. In mathematics, it is not uncommon to see seemingly unrelated ideas synergize, building profound understanding and connections.

9 Finale

> *"The beauty of mathematics only shows itself to its more patient followers."*
> – *Maryam Mirzakhani* [31]

Elliptic curves are enigmatic objects that have undoubtedly revolutionised mathematics and cryptography. I am yet to scrape the tip of the iceberg, as there are always more questions to ask, new problems to solve, and further knowledge to gain. Like, have you ever wondered how large integers may be factorised with the help of elliptic curves? How one could find all the rational points on these curves? And how elliptic curves were involved Andrew Wiles's solution to the famous 300 year old problem, Fermat's Last Theorem [34]?

Our in-depth studying and research in mathematics is often rewarded by a revelation of its sometimes subtle, but never insignificant elegance, and it is through writing that this may be shared with others. So, if it is indeed possible to write endlessly on elliptic curves, then we certainly should.

Acknowledgements

I sincerely thank John Voight and Jonathan Spreer for making insightful comments and edit suggestions.

References

[1] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, H. Silberg, D. Smith-Tone and N. Waller, *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST Internal Report 8545, National Institute of Standards and Technology, Gaithersburg, 2025.

[2] A.M. Antonopoulos and D.A. Harding, *Mastering Bitcoin: Programming the Open Blockchain*, 3rd ed., O'Reilly Media, Sebastopol, CA, 2023.

[3] J. Assange, J. Appelbaum, A. Müller-Maguhn and J. Zimmermann, *Cypherpunks: Freedom and the Future of the Internet*, OR Books, New York, 2012,

[4] E.B. Barker, *Recommendation for Key Management: Part 1—General*, NIST Special Publication 800-57 Part 1 Revision 5, National Institute of Standards and Technology, Gaithersburg, MD, 2020.

[5] W. Castryck and T. Decru, An efficient key recovery attack on SIDH, in *Advances in Cryptology—EUROCRYPT 2023, Part V*, Lecture Notes in Computer Science **14008**, pp. 423–447, Springer, Cham, 2023.

[6] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes, CSIDH: An efficient post-quantum commutative group action, in *Advances in Cryptology—ASIACRYPT 2018, Part III*, Lecture Notes in Computer Science **11274**, pp. 395–427, Springer, Cham, 2018.

[7] L. Chen, D. Moody, K. Randall, A. Regenscheid and A. Robinson, *Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*, NIST Special Publication 800-186, National Institute of Standards and Technology, Gaithersburg, MD, 2023.

[8] L. De Feo, D. Jao and J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *Journal of Mathematical Cryptology* **8** (2014), 209–247.

[9] L. De Feo and S.D. Galbraith, SeaSign: Compact isogeny signatures from class group actions, in *Advances in Cryptology—EUROCRYPT 2019, Part III*, Lecture Notes in Computer Science **11478**, pp. 759–789, Springer, Cham, 2019.

[10] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), 644–654.

[11] G.W. Dunnington, *Carl Friedrich Gauss: Titan of Science*, Mathematical Association of America, Washington, DC, 2004.

[12] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory* **31** (1985), 469–472.

[13] fail0verflow, *Console Hacking 2010: PS3 Epic Fail*,
27th Chaos Communication Congress, 29 December 2010,
fahrplan.events.ccc.de/congress/2010/Fahrplan/events/4087.en.html,
last accessed on 2026-08-22.

[14] M. Haddon, *The Curious Incident of the Dog in the Night-Time*, Red Fox, London, 2014.

[15] D. Hankerson, A.J. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, New York, 2004.

[16] T.L. Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, 2nd ed., Cambridge University Press, Cambridge, 1910.

[17] D. Johnson, A. Menezes and S.A. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), *International Journal of Information Security* **1** (2001), 36–63.

[18] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Revised Third Edition*, CRC Press, Boca Raton, 2025.

[19] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994.

[20] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* **48** (1987), 203–209.

[21] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, Berlin, 1978.

[22] H.W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Mathematics* **126** (1987), 649–673.

[23] V. S. Miller, Use of elliptic curves in cryptography, in *Advances in Cryptology—CRYPTO '85*, Lecture Notes in Computer Science **218**, pp. 417–426, Springer, Berlin, 1986.

[24] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS PUB 186-5, National Institute of Standards and Technology, Gaithersburg, MD, 2023.

[25] A. Rice and E. Brown, Why Ellipses Are Not Elliptic Curves, *Mathematics Magazine* **85** (2012), 163–176.

[26] R.L. Rivest, A. Shamir and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21** (1978), 120–126.

[27] G. Sarton, *The Study of the History of Mathematics and The Study of the History of Science*, Dover Publications, New York, 1957.

[28] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, IEEE Computer Society Press, 1994.

[29] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer, Cham, 2015.

[30] M. Sipser, *Introduction to the Theory of Computation*, 3rd ed., Cengage Learning, Boston, MA, 2013.

[31] L. Taylor, The Guardian, *Maryam Mirzakhani: 'The more I spent time on maths, the more excited I got'* (2014), www.theguardian.com/science/2014/aug/13/interview-maryam-mirzakhani-fields-medal-winner-mathematician, last accessed on 2026-02-02.

[32] Y. Tian, Congruent Number Problem, *Notices of the International Consortium of Chinese Mathematicians* **5** (2017), 51–61.

[33] F. Verhulst, Mathematics is the art of giving the same name to different things, *Nieuw Archief voor Wiskunde, Series 5* **13** (2012), 154–158.

[34] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics* **141** (1995), 443–551.

[35] Nova, WGBH Educational Foundation, *Andrew Wiles on Solving Fermat* (2000), https://www.pbs.org/wgbh/nova/article/andrew-wiles-fermat/, last accessed on 2026-02-02.

Appendix: Singular and nonsingular elliptic curves

An elliptic curve E is *singular* if the polynomial $x^3 + Ax + B$ contains a repeated root; otherwise, it is *nonsingular* [29].

Proposition 5. [29] *An elliptic curve $E : y^2 = x^3 + Ax + B$ is singular if and only if its discriminant $\Delta = -16(4A^3 + 27B^2)$ equals zero.*

Proof. [29] The polynomial $x^3 + Ax + B$ contains a repeated root if and only if it has a shared root with its derivative $3x^2 + A$. Setting $3x^2 + A = 0$, we get $x^2 = -A/3$, and substituting this into the polynomial yields

$$0 = x^3 + Ax + B = x(x^2 + A) + B = x\Big(-\frac{A}{3} + A\Big) + B = \frac{2A}{3}\,x + B$$

and so $x = -\frac{3B}{2A}$. Now substituting this back into the derivative, we get

$$0 = 3x^2 + A = 3\Big(-\frac{3B}{2A}\Big)^2 + A = \frac{4A^3 + 27B^2}{24A^2}\,.$$

This implies $4A^3 + 27B^2 = 0$ and hence $-16(4A^3 + 27B^2) = 0$. □