

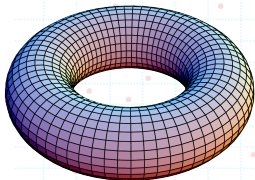
Elliptic Curves in Practice

Complex Tori, Cryptography, and Rational Points

Tyler Genao

Tennessee Tech University
Graduate Student Seminar

October 1, 2026



$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})[\text{tors}]$$

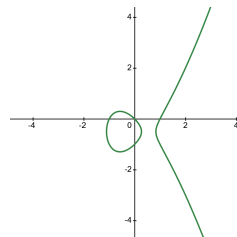
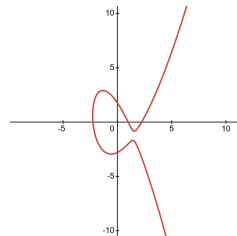
Where We Left Off

- Last time: we studied solutions to the Cannonball Problem, a classic problem of Diophantus, and Fermat's Last Theorem.
- Each example was connected to **elliptic curves**, which we defined as algebraic curves in $\mathbb{R}^2$ with a *group law*.

Today's question

What changes when we view elliptic curves over $\mathbb{C}$, finite fields, and $\mathbb{Q}$?

- Each of these topics could get a dedicated talk of their own!



What Is an Elliptic Curve, Again?

- Our primary definition for an **elliptic curve** is a curve, written as E or $E/\mathbb{R}$, defined by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{R}$ satisfy a nonsingularity condition.

- A shorter form of this is

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

where $A, B \in \mathbb{R}$ and $4A^3 + 27B^2 \neq 0$.

- These two forms are called **Weierstrass forms**.
- Elliptic curves $E/\mathbb{R}$ have a *group operation* on their elements, called the **Chord and Tangent Method**.

The Chord Method

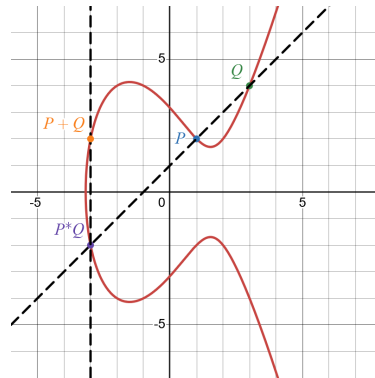
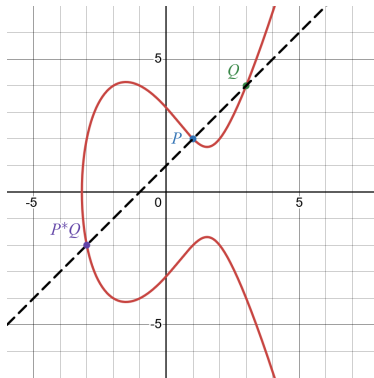
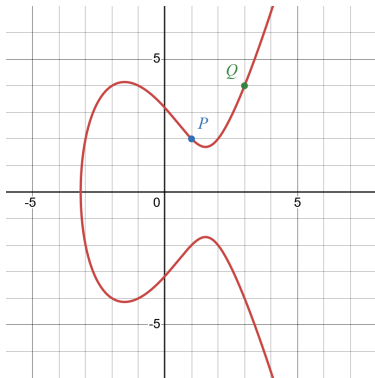


Figure: The addition law on E for adding two distinct points P and Q to get $P+Q$ (Chord Method + reflection).

The Tangent Method

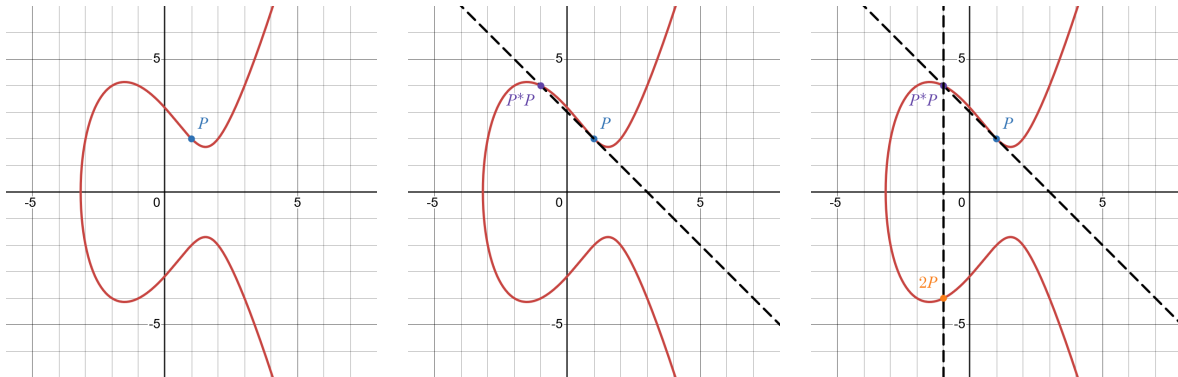


Figure: The addition law on E for adding P to itself to get $2P$ (Tangent Method + reflection).

The Chord and Tangent Method

$$+: E(\mathbb{R}) \times E(\mathbb{R}) \rightarrow E(\mathbb{R}), \quad (P, Q) \mapsto P + Q$$

① **Associative:**

$$\forall P, Q, R \in E(\mathbb{R}), \quad (P + Q) + R = P + (Q + R).$$

② **Has an identity:**

$$\exists O \in E(\mathbb{R}), \quad \forall P \in E(\mathbb{R}) \quad O + P = P + O = P.$$

③ **Closed under inverses:**

$$\forall P \in E(\mathbb{R}), \quad \exists Q \in E(\mathbb{R}) \quad P + Q = Q + P = O. \quad (\text{We write } -P := Q.)$$

④ **Commutative:**

$$\forall P, Q \in E(\mathbb{R}), \quad P + Q = Q + P.$$

- Therefore, $E(\mathbb{R})$ is an **abelian group**.

Addition Formulas for Weierstrass Form

- Given an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{R}$, for two points $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{R})$ which are not on the same vertical line, if m denotes the slope of the line between P and Q , one has

$$P + Q = (x_3, -a_1x_3 - a_3 - y_3)$$

where

$$(x_3, y_3) = P * Q = (m^2 + a_1m - a_2 - x_1 - x_2, m(x_3 - x_1) + y_1).$$

- For short Weierstrass form

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

one has the formula

$$P + Q = (x_3, y_3) = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1).$$

- When two distinct points are on the same vertical line, their sum is

$$P + Q = O,$$

no formula necessary.

- There are a few lingering questions about elliptic curves you might have...
- *What is the identity of the elliptic curve group?*
- *In the definition of an elliptic curve, we said the equation is nonsingular. What does that mean?*
- We will address these in the next few slides.

The Projective Plane

- The identity O of $E(\mathbb{R})$ satisfies

$$\forall P \in E(\mathbb{R}), \quad P + O = O + P = P.$$

- However, O cannot be seen in $\mathbb{R}^2$, but only in the *projective plane*...
- The **projective plane**, written $\mathbb{P}^2\mathbb{R}$, is defined as

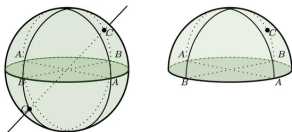
$$\mathbb{P}^2\mathbb{R} := (\mathbb{R}^3 \setminus \{(0, 0, 0)\}) / \sim, \quad (a, b, c) \sim (\lambda a, \lambda b, \lambda c) \quad \forall \lambda \neq 0 \in \mathbb{R}.$$

- Equivalence classes in $\mathbb{P}^2\mathbb{R}$ are written as $[a : b : c]$ instead of $\overline{(a, b, c)}$, and are called *projective points*.
- For example, $[1 : 2 : 3] \in \mathbb{P}^2\mathbb{R}$, and $[1 : 2 : 3] = [2 : 4 : 6] = [\pi : 2\pi : 3\pi] = \dots$
- The identity O is called the **point at infinity**, and has coordinates

$$O = [0 : 1 : 0].$$

Properties of $\mathbb{P}^2\mathbb{R}$

- Visualizing $\mathbb{P}^2\mathbb{R}$ is very tricky.
- Defining property of $\mathbb{P}^2$: **any two curves in projective space intersect at the right amount of points.** This is **Bézout's Theorem**.
- Over $\mathbb{C}$, Bézout's Theorem generalizes the Fundamental Theorem of Algebra: analyze intersection of $y = f(x)$ with $y = 0$.
- A key consequence of working in $\mathbb{P}^2\mathbb{R}$: *"Parallel lines in $\mathbb{R}^2$ intersect at a point in $\mathbb{P}^2\mathbb{R}$."*



Parallel railroad tracks appear to converge at the horizon.

Elliptic Curves in $\mathbb{P}^2\mathbb{R}$

- Every elliptic curve $E/\mathbb{R}$ in Weierstrass form

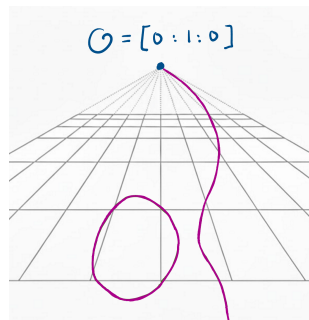
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

contains the point at infinity $O = [0 : 1 : 0]$ in $\mathbb{P}^2\mathbb{R}$.

- We can check this by *homogenizing* the equation:

$$E_H : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

- For a fun visualization, see Bill Shillito's YouTube video *Putting Algebraic Curves in Perspective*.



An elliptic curve in $\mathbb{RP}^2$, with its point at infinity O .

Nonsingular Curves

- An elliptic curve, by definition, must be *nonsingular*. What does this mean?
- A **singular point** on a curve is one with “extra multiplicity” at *all* lines through it. A curve with a singular point is called a **singular curve**.
- Singular points can be computed using partial derivatives of the curve equation.
- At a singular point, the usual Chord/Tangent Method fails. This prevents the Chord and Tangent group law from working for singular cubic curves.

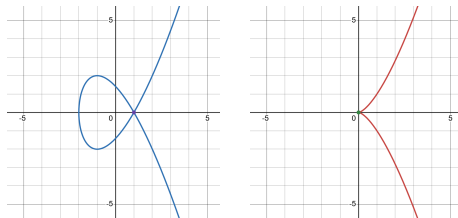


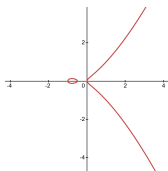
Figure: The singular curves $C : y^2 = x^3 - 3x + 2$ (nodal) and $D : y^2 = x^3$ (cuspidal).

Summarizing Elliptic Curves

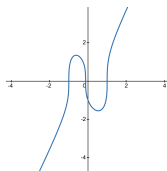
General Definition

An **elliptic curve** (over $\mathbb{R}$) is a nonsingular cubic plane curve with a fixed real point.

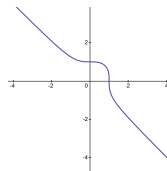
- Cubic is necessary, since otherwise our Chord/Tangent Method can fail to produce a third point over $\mathbb{R}$.
- We thus have more elliptic curves at our disposal:



Cannonball Curve
 $6y^2 = 2x^3 + 3x^2 + x$



Diophantus Curve
 $y^3 = (x^2 - 1)(8x + 1)$



Fermat Curve
 $x^3 + y^3 = 1$

Changing the Field

- We can work beyond $\mathbb{R}$:

More General Definition

An **elliptic curve** over a *field* F is a nonsingular cubic plane curve with a fixed point over F .

- Roughly speaking, a **field** is an algebraic structure where you can *add* and *multiply* elements, and take *fractions* of nonzero elements.
- Fields include: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ for prime numbers p .
- Fields do *not* include: $\mathbb{Z}$, $\mathbb{Q}[x]$, and $\mathbb{Z}/n\mathbb{Z}$ for composite n . (Can you find nonzero elements with no fractions in each of these rings?)

- We will study elliptic curves over the following fields.

Field	What its points look like	Question for today
$\mathbb{C}$	a continuous complex surface	Why a torus?
$\mathbb{F}_p$	finitely many coordinate pairs	How many points? DLP?
$\mathbb{Q}$	rational coordinate pairs	What is the group structure?

The Chord and Tangent Method still defines a group law in each setting!

Elliptic Curves over $\mathbb{C}$

Lattices in the Complex Plane

- Choose $\omega_1, \omega_2 \in \mathbb{C}$ that are linearly independent over $\mathbb{R}$. Their **lattice** is

$$\Lambda := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}.$$

Square lattice

If $\omega_1 = 1$ and $\omega_2 = i$, then

$$\Lambda = \mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i].$$

This is the *Gaussian integers*.

- A lattice Λ is always an additive subgroup of $\mathbb{C}$. The quotient group $\mathbb{C}/\Lambda$ has a special structure...

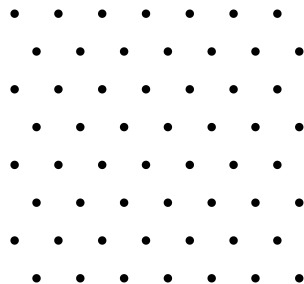
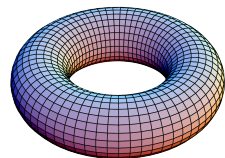
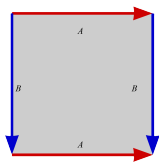
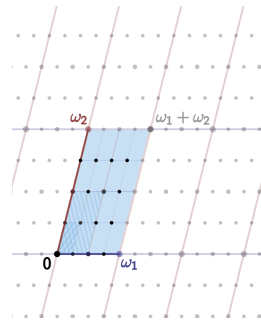


Figure: An example of a lattice in $\mathbb{C}$.

- In the quotient group $\mathbb{C}/\Lambda$, addition is

$$(z + \Lambda) + (w + \Lambda) = (z + w) + \Lambda.$$

- So e.g.
 $z + \Lambda = (z + \omega_1) + \Lambda = (z + \omega_2) + \Lambda.$
- Topologically, the opposite sides of the *fundamental parallelogram* of $\mathbb{C}/\Lambda$ are identified with each other.
- You can attach these sides together to form a **(complex) torus**.



The Weierstrass $\wp$ -Function

Every lattice Λ has an associated **Weierstrass $\wp$ -function**

$$\wp(z) := \wp_{\Lambda}(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

- $\wp(z + \omega) = \wp(z)$ for $\omega \in \Lambda$.
- Its derivative satisfies an algebraic equation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda).$$

The function and derivative are meromorphic on $\mathbb{C}$ and have poles at lattice points.

From a Torus to a Cubic

- Put $x = \wp(z)$ and $y = \wp'(z)/2$. Then the equation becomes

$$E_\Lambda : y^2 = x^3 - \frac{g_2(\Lambda)}{4}x - \frac{g_3(\Lambda)}{4}.$$

- This is an elliptic curve!

The map from $\mathbb{C}/\Lambda$ to E_Λ :

$$z + \Lambda \mapsto (x, y) = \left(\wp(z), \frac{\wp'(z)}{2} \right), \quad 0 + \Lambda \mapsto O.$$

- The analytic addition $[z] + [w] = [z + w]$ in $\mathbb{C}/\Lambda$ matches the Chord and Tangent group law in $E_\Lambda(\mathbb{C})$, so this map is a **group homomorphism**.

The Uniformization Theorem

For every elliptic curve $E/\mathbb{C}$, there is a lattice $\Lambda_E \subset \mathbb{C}$ such that

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda_E$$

as *complex Lie groups*. Conversely, every lattice Λ in $\mathbb{C}$ gives a complex elliptic curve $E_\Lambda/\mathbb{C}$, with $E_\Lambda(\mathbb{C}) \cong \mathbb{C}/\Lambda$.

- Therefore, **complex elliptic curves** are **tori**.

Elliptic Curves over $\mathbb{F}_p$

Points over $\mathbb{F}_p$

- If an elliptic curve over $\mathbb{C}$ is a torus, what is an elliptic curve over a finite field?
- For this talk, a *finite field* has the form

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

where $p \geq 5$ is a prime number.

- in $\mathbb{F}_p$, dividing by a nonzero denominator means multiplying by its inverse modulo p .
- To simplify matters, for this talk an **elliptic curve over $\mathbb{F}_p$** , written $E/\mathbb{F}_p$, has the form

$$E : y^2 \equiv x^3 + Ax + B \pmod{p}$$

where $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$.

- The points in $E(\mathbb{F}_p)$ include $O := [0 : 1 : 0]$, and $(x, y) \in \mathbb{F}_p^2$ where

$$y^2 \equiv x^3 + Ax + B \pmod{p}.$$

The Points on $E/\mathbb{F}_p$

- The Chord and Tangent Method still works for $E/\mathbb{F}_p$ *algebraically*.
- However, the picture of $E(\mathbb{F}_p)$ is quite different than over $\mathbb{R}$ and $\mathbb{C}$!
- $E(\mathbb{F}_p)$ is then a **finite abelian group**.
- Finding points on $E/\mathbb{F}_p$ amounts to solving the congruence condition

$$E : y^2 \equiv x^3 + Ax + B \pmod{p}.$$

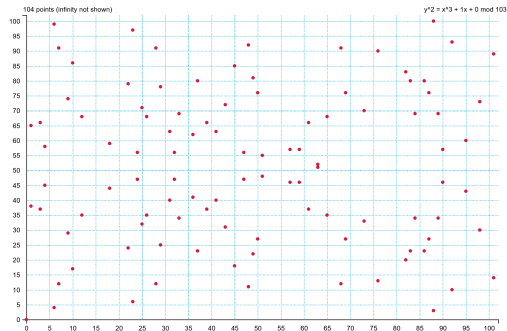


Figure: The elliptic curve $y^2 = x^3 + x$ over the finite field of size 103.

An Example

- Take the elliptic curve $E/\mathbb{F}_{11}$, given by

$$E : y^2 \equiv x^3 + x \pmod{11}.$$

- The values of x that give points are:

x	0	5	7	8	9	10
y	0	± 3	± 3	± 5	± 1	± 3

- Finding these points amounts to checking whether $x^3 + x$ is a *square* modulo 11.
- Therefore, there is one point (x, y) above $x = 0$, ten more which come in pairs, and O :

$$\therefore |E(\mathbb{F}_{11})| = 1 + 10 + 1 = 12.$$

For example, $(8, 5)$ lies on $E/\mathbb{F}_{11}$ because $5^2 \equiv 8^3 + 8 \equiv 3 \pmod{11}$.

Hasse's Bound

- If $E(\mathbb{F}_p)$ is always a finite abelian group, what do we know about $|E(\mathbb{F}_p)|$?
- Always have $|E(\mathbb{F}_p)| \leq p^2 + 1$.

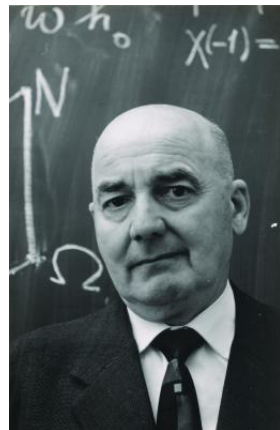
Hasse's Theorem

For any elliptic curve $E/\mathbb{F}_p$,

$$\left| |E(\mathbb{F}_p)| - (p + 1) \right| \leq 2\sqrt{p}.$$

- For our example curve $E : y^2 \equiv x^3 + x \pmod{11}$, we found $|E(\mathbb{F}_{11})| = 12$:

$$|12 - (11 + 1)| = 0 \leq 2\sqrt{11}. \checkmark$$



Helmut Hasse

Changing the Prime

- Let's count $|E(\mathbb{F}_p)|$ for our elliptic curve $E : y^2 \equiv x^3 + x \pmod{p}$ over *varying* p .

p	5	7	11	13	17	19
$ E(\mathbb{F}_p) $	4	8	12	20	16	20
$p + 1$	6	8	12	14	18	20

A pattern to investigate

The entries for $p = 7, 11, 19$ equal $p + 1$. What do these primes have in common?

Elliptic Curves in Cryptography

The Discrete Logarithm Problem

- In a cyclic group $G = \langle g \rangle$, repeated multiplication is easy:

$$a \mapsto g^a.$$

- The **discrete logarithm problem** runs this backwards:

DLP

Given generator g of G and an element $h \in G$, find the unique $0 \leq a < |G|$ for which

$$g^a = h.$$

- Some groups let us solve this quickly. Cryptography chooses groups where the inverse problem appears *hard* at appropriate sizes.

The Elliptic Curve Discrete Logarithm Problem

- Fix a prime p and an elliptic curve $E/\mathbb{F}_p$.
- Fix a point $P \in E(\mathbb{F}_p)$ of order large order n .



Neal Koblitz

$$aP = \underbrace{P + \cdots + P}_{a \text{ copies}} =: Q.$$

ECDLP

Given P and $Q \in \langle P \rangle$, find $0 \leq a < n$ such that

$$Q = aP.$$



Victor Miller

- Computing aP is efficient; reversing for a is believed to be hard for classical computers.

Miller and Koblitz independently proposed elliptic-curve cryptography in the 1980s.

Applying the ECDLP

- This is one way to implement the ECDLP towards sharing secrets on a public channel; specifically, it is *Elliptic Curve Diffie–Hellman*.
- Public information: $E/\mathbb{F}_p$, a large prime-order point $P \in E(\mathbb{F}_p)$, and its order.

Alice

Chooses secret a .

Publishes aP .

Computes $a(bP) = abP$ (privately).

Bob

Chooses secret b .

Publishes bP .

Computes $b(aP) = abP$ (privately).

Both obtain the same group element abP and derive a shared *secret* key from it using the same algorithm.

Why Use Elliptic Curves?

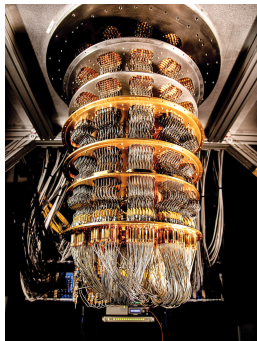
- For suitable elliptic curve choices, there are no known subexponential *index-calculus attacks*, unlike the DLP on $\mathbb{F}_p^\times$ (these attacks exploit factorization of the elements).
- The choice of E and generator P are important: special curves and weak parameters can defeat the intended security. (See: *anomalous curves*.)

To summarize:

Computing aP is efficient. Determining a from P and aP remains hard in the classical setting.

Quantum Attacks

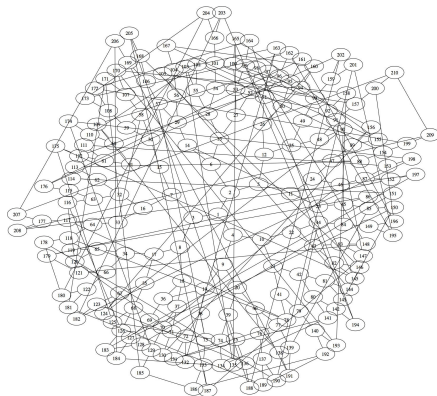
- A decade after the discovery of the ECDLP, **Shor's algorithm** was created: a **quantum** algorithm that, on a sufficiently accurate quantum computer, can solve DLP's in *polynomial time*.
- Thus, ECDLP is **quantum-vulnerable**.
- NIST, the *National Institute of Standards and Technology*, plans to move away from quantum-vulnerable cryptosystems by 2035.
- However, elliptic curves are still seeing use in post-quantum research...



A quantum computer. The actual computer is a small chip inside this refrigerator; the cords control/read the chip. From Google Quantum AI.

Supersingular Isogeny Graphs

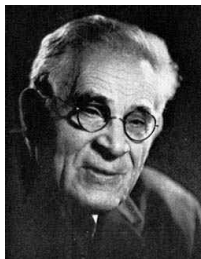
- A **vertex** represents a *supersingular elliptic curve*, up to isomorphism.
- An **edge** represents an *isogeny*, a structure-preserving map between curves.
- Some proposed cryptosystems use hard questions about paths and endomorphisms.



Example with $p = 2521$: Denis Charles, via Microsoft Research, *Where cryptography and quantum computing intersect* (2017).

Elliptic Curves over $\mathbb{Q}$

The Mordell–Weil Theorem



Louis Mordell

- For an elliptic curve $E/\mathbb{Q}$, the rational points form a **finitely generated abelian group**.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})[\text{tors}]$$

- The integer r is the **rank**. It counts the maximal number of linearly independent points of infinite order.
- $E(\mathbb{Q})[\text{tors}]$ is the **torsion subgroup**. It is the subgroup of $E(\mathbb{Q})$ of points with finite order.



André Weil

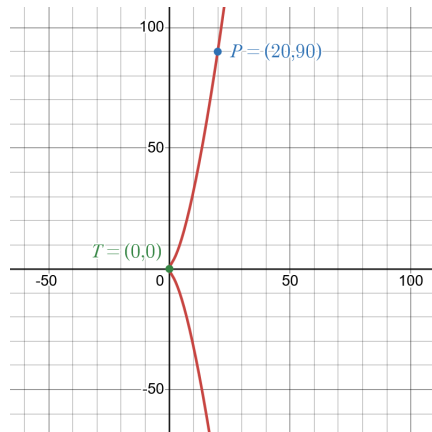
A Rational-Point Example

- Consider $E : y^2 = x^3 + 5x$.
- We can check that $P := (20, 90)$ and $T := (0, 0)$ are on E .
- $2T = O$, since $T = -T$.
- It turns out that P has *infinite* order.
- Thus,

$$\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle P, T \rangle \leq E(\mathbb{Q}).$$

- As it turns out, this is an equality:

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$



What Can $E(\mathbb{Q})[\text{tors}]$ Be?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})[\text{tors}]$$

Mazur's Torsion Theorem, 1977

For an elliptic curve $E/\mathbb{Q}$,

$$E(\mathbb{Q})[\text{tors}] \cong \begin{cases} \mathbb{Z}/N\mathbb{Z}, & N = 1, 2, \dots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, & N = 1, 2, 3, 4. \end{cases}$$

A different problem over number fields

If we replace $\mathbb{Q}$ by a *number field* F , which torsion groups can occur in $E(F)$? This is one theme in my research.

How Large Can the Rank Be?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})[\text{tors}]$$

- In contrast to the torsion subgroup, **it is unknown whether ranks of elliptic curves over $\mathbb{Q}$ are bounded.**

Year	Rank bound	Record credited to
1938	$r \geq 3$	Billing
		$\vdots$
2006	$r \geq 28$	Elkies
2024	$r \geq 29$	Elkies and Klagsbrun
2026	$r \geq 30$	Alpöge and Howell
2026	$r \geq 31$	Alpöge and Howell

Table source: A. Dujella, *History of elliptic curves rank records* (accessed September 2026).
<https://dujella.github.io/tors/rankhist.html>

- A *linear dependence* is a relation

$$n_1 P_1 + \dots + n_k P_k = O$$

where not all $n_i \in \mathbb{Z}$ are zero.

- A bound $r \geq k$ comes from k points with no such relation.

The 2026 Rank Record

A curve found in 2026 has **31 proven independent rational points**. Consequently, the curve's rank is ≥ 31 .

- This is a *lower bound*; it does not prove that the exact rank is 31.
- This result is from Levent Alpöge and Ava Howell, with the help of AI (Claude).

The Example for $r \geq 31$

$$y^2 + xy + y = x^3 + x^2 - 1284727764113567728281797636015784768866707681415849262157224232063x \\ + 560368321454261339256859338981915312332769858684945406858043869199456710681980958863306170127006181$$

Independent points of infinite order:

```
P1 = [-343746913367434053557936715792581, -31005994945795167281668477280091616990476695982462]
P2 = [739387066521976456185309925500635, 3830813927243125109605210052773411116315836476962]
P3 = [794918160232596023344129483097739, 6435806665987309972375508567418781686192466975138]
P4 = [55222982172554306445525103966115, -439432766051778936811414681478594663009127495638]
P5 = [621111741565922967463663441261795, 1421683191996488160880565213880200774834445145522]
P6 = [672709190481033101277453068263195, 739179814158401859498464392317452223287910224482]
P7 = [821399009280840681555588652225649, -7699942068198872209289633789793873375706107955662]
P8 = [765203485098820658379256355481245, -5034345308760298854369394902951465889284652680168]
P9 = [5399595603851507511243908479925915, 388654067273650918227195921742660550010310029109122]
P10 = [752668954339285868300409092384315, 44842956013172287133563039699897920170009189762]
P11 = [665267573831105472345147950403835, -339632380726246052348178275348181915170728600638]
P12 = [2348702476455858806523697264250795, 102466166054736815527265002032727452468648322658682]
P13 = [-4853012393400163999257025789080055, -3270399766787423263973934480265805294302785095518]
P14 = [1671562150318197588290891477490065, -55528472789639333688258829014227823359584879796238]
P15 = [533792265728561313885832952129951, -516587267603053509137532850965718653070997396662]
P16 = [8050101189939018648004785213625795/9, -304090504548899061983493167851611965128494136836666/27]
P17 = [641126276756517817380587191947425, 475393761225519880788251703870437551199359754892]
P18 = [-28607312564278696457116932283279229/25, 288349279894494822652093539160188543199459930509066/125]
P19 = [56549444812087071231733196839837255/4, 134055776981335578686240729300809297336164276021592851/8]
P20 = [1436747523773762964481823443661979, 40991896134294415817647888149334972652525806317538]
P21 = [-5064387018792502839844249474841045/9, 897570094862437631568619794896775730629735504169894/27]
P22 = [487104273264503806273608258117432335/484, -180314887995146178717423515157548125006198119570993099/10648]
P23 = [25599342024506626201702677512314955, 4091893764954118703319829997327215311497327967339042]
P24 = [980266989498097787981780089573917995/961, -525575897314714907955968908277850024344706090034709538/29791]
P25 = [5818507410725525932023407879789875/9, 1789182708478717961552943758166081786352797832214/27]
P26 = [19197683320190396803412613672365855/49, -371272445208849581845790009045877458707899890853974/343]
P27 = [887913128901643530184527456121547975/841, -47594899737181706228705904314984539154585989478008302/24389]
P28 = [1816718417495680977851120075801270195/1849, 1248545591609034704022269662335921779441905481482388694/79507]
P29 = [45289030981914257697743589493812866845795/3630906049, -6558125371552387528524400913253424783234119422079260125534495614/21878750794593]
P30 = [33880100347989327554317013369507240405/52441, -1625428840401701290033088199518465040555146308891387272/12008989]
P31 = [-11477003798992551861310315487329257253535/8922169, -24493977634318200818657636220539498535490153552116110249914/26650518803]
```

- We do **not** know whether ranks over $\mathbb{Q}$ are unbounded!

Elliptic Curves in Three Different Worlds

Field	Structure of the points	Main questions
$\mathbb{C}$	$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, a complex torus	How is a torus an elliptic curve?
$\mathbb{F}_p$	$E(\mathbb{F}_p)$, a finite abelian group	How many points are there? How are they used in cryptography?
$\mathbb{Q}$	$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})[\text{tors}]$	Which ranks and torsion subgroups occur?

The Chord and Tangent Method links geometry, complex analysis, finite arithmetic, cryptography, and Diophantine questions.

For More on Elliptic Curves

- The “gold standard” textbooks for learning elliptic curves:
 - at the undergraduate level: *Rational Points on Elliptic Curves*, by Silverman and Tate.
 - at the introductory graduate level: *The Arithmetic of Elliptic Curves*, by Silverman.
- Another great book for undergraduates is *Elliptic Curves: Number Theory and Cryptography*, by Washington.
- On my site, I also have several additional resources:
 - A set of notes that I wrote on *elementary number theory* in 2026, with the last chapter on *Diophantine equations and elliptic curves*. The only technical prerequisite is experience with introductory proofs.
 - I gave a talk at the University of Connecticut in 2026 on elliptic curve **Galois representations**, aimed at senior undergraduates and introductory graduate students. It has since been recorded and uploaded to YouTube.

A Summary

- The point at infinity O serves as the group identity on elliptic curves.
- Over $\mathbb{C}$, every elliptic curve is a quotient $\mathbb{C}/\Lambda$.
- Over $\mathbb{F}_p$, Hasse's Theorem controls the point count, and elliptic curves can be applied through cryptography via the discrete logarithm problem and supersingular isogeny graphs.
- Over $\mathbb{Q}$, the Mordell–Weil Theorem gives a rank and a finite torsion subgroup. Mazur classified these torsion groups over $\mathbb{Q}$; the possible ranks remain mysterious.

Thank you!

Select References

- ① J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009. (For theoretical material.)
- ② N. Koblitz, Elliptic Curve Cryptosystems, *Mathematics of Computation* **48** (1987), 203–209; V. S. Miller, Use of Elliptic Curves in Cryptography, CRYPTO '85 proceedings, 1986.
- ③ NIST, *Post-Quantum Cryptography* project and *NIST IR 8547*, Transition to Post-Quantum Cryptography Standards.
- ④ K. Lauter, Where cryptography and quantum computing intersect, Microsoft Research Blog, May 8, 2017 (graph by Denis Charles).
- ⑤ B. Mazur, Modular Curves and the Eisenstein Ideal, *Publications Mathématiques de l'IHÉS* **47** (1977), 33–186.
- ⑥ A. Dujella, History of elliptic curves rank records, <https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html>; ICARM, Elliptic Curve Rank Leaderboard, curve #302.