Torsion subgroups of elliptic curves in Lean

SMS Spring Meeting: Formalization and Proof Assistants

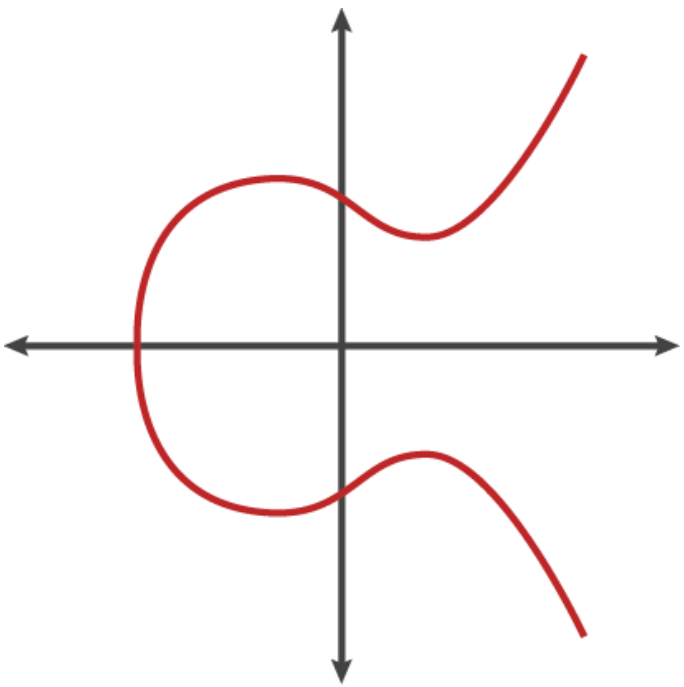
David Kurniadi Angdinata (with Chris Birkbeck)

University of East Anglia

Thursday, 26 March 2026

Elliptic curves

Elliptic curves are algebraic curves given by cubic equations, whose set of points can be endowed with the structure of an abelian group.



- Wiles's proof of Fermat's last theorem is a correspondence between elliptic curves and certain modular forms.
- The Birch and Swinnerton-Dyer conjecture predicts the rank of an elliptic curves in terms of L-functions.
- Intractability of the discrete logarithm problem forms the basis behind many public key cryptographic protocols.
- The Atkin–Morain primality test and Lenstra's factorisation method are two of the fastest known algorithms.

Weierstrass equations

Formally, an **elliptic curve** E **over a field** F is a smooth projective curve of genus one over F with a distinguished point O defined over F.

By the Riemann–Roch theorem, its set of points $E(F)$ is the zero locus of

$$f := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6),$$

for some $a_i \in F$ such that $\Delta \neq 0$, [1] with O being the point at infinity.

More specifically, there is an equivalence of categories

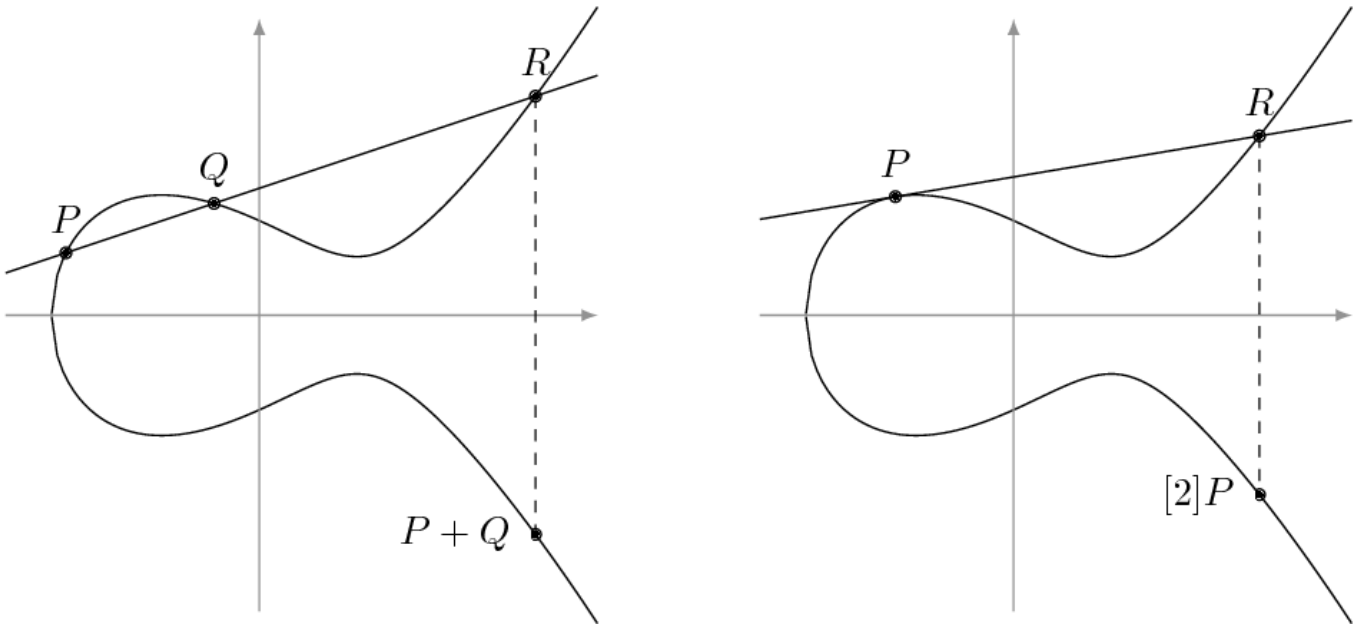
$$\{\text{elliptic curves over } F\} \cong \{(a_1, a_2, a_3, a_4, a_6) \in F^5 \text{ such that } \Delta \neq 0\}.$$

In `mathlib`, an **elliptic curve** E **over a ring** R is the data of a tuple $(a_1, a_2, a_3, a_4, a_6) \in R^5$ and a proof that $\Delta \in R^\times$. A **point** in $E(F)$ is either O or an **affine point** $(x, y) \in R^2$ such that $f(x, y) = 0$.

[1] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Group law

There is an **addition law** of points in $E(F)$ defined geometrically.



In `mathlib`, the addition law is given by explicit rational functions.

Formalisation (A.–Xu, 2022)

This addition law makes $E(F)$ an abelian group with identity O.

The n-torsion subgroup

For any $P \in E(F)$ and any $n \in \mathbb{Z}$, denote multiplication-by-n by

$$[n](P) := \underbrace{P + \cdots + P}_{n},$$

and define the n-**torsion subgroup** by $E(F)[n] := \ker[n]$.

Formalisation (A.–Xu, 2024)

If the characteristic of F does not divide n, then $\#E(\overline{F})[n] = n^2$.

Exercise (3.7(d) in *The Arithmetic of Elliptic Curves* by Silverman)

Prove that for any affine point $(x, y) \in E(F)$,

$$[n](x, y) = \left(\frac{\phi_n(x, y)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right).$$

Division polynomials

Assume $a_1 = a_2 = a_3 = 0$. Then $\phi_n, \omega_n, \psi_n \in F[X, Y]$ are defined by

$$\begin{aligned}
\psi_0 &:= 0,\\
\psi_1 &:= 1,\\
\psi_2 &:= 2Y,\\
\psi_3 &:= 3X^4 + 6a_4X^2 + 12a_6X - a_4^2,\\
\psi_4 &:= \psi_2 \cdot (2X^6 + 10a_4X^4 + 40a_6X^3\\
&\qquad - 10a_4^2X^2 - 8a_4a_6X - 4a_6^2 - 2a_4^3),
\end{aligned}$$

$$\begin{aligned}
\psi_{2n+1} &:= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3,\\
\psi_{2n} &:= \frac{\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2}{\psi_2},\\
\psi_{-n} &:= -\psi_n,\\
\phi_n &:= X\psi_n^2 - \psi_{n+1}\psi_{n-1},\\
\omega_n &:= \frac{\psi_{2n}}{2\psi_n}.
\end{aligned}$$

Observe that ϕ_n and ψ_n^2 can be viewed as polynomials in $F[X]$ modulo f.

Exercise (3.7(b) in *The Arithmetic of Elliptic Curves* by Silverman)

Prove that $\phi_n = X^{n^2} + \dots$ *and* $\psi_n^2 = n^2X^{n^2-1} + \dots$.

Arithmetic structure

Theorem (Mordell–Weil, 1929)

If K is a global field, then $E(K)$ is finitely generated.

By the structure theorem for finitely generated abelian groups,

$$E(K) \cong \mathrm{tor}(E/K) \oplus \mathbb{Z}^{\mathrm{rk}(E/K)},$$

where $\mathrm{rk}(E/K) \in \mathbb{N}$ is the **rank**, and the finite **torsion subgroup** is

$$\mathrm{tor}(E/K) := \bigcup_{n \in \mathbb{Z} \setminus \{0\}} E(K)[n] \leq E(K).$$

The proof of Mordell–Weil has two parts:

- Weak Mordell–Weil: $E(K)/nE(K)$ is finite for any $n \in \mathbb{Z} \setminus \{0\}$.
- Heights and descent: there is a height function on $E(K)$.

Michael Stoll formalised the latter a month ago.

The torsion subgroup

While $\mathrm{rk}(E/K)$ is mysterious, $\mathrm{tor}(E/K)$ is well-understood.

Theorem (Levin, 1968)

If K is the function field of a curve of genus g over a finite field, then $\#\,\mathrm{tor}(E/K)$ is bounded in terms of g.

Theorem (Merel, 1996)

If K is a number field, then $\#\,\mathrm{tor}(E/K)$ is bounded in terms of $[K:\mathbb{Q}]$.

Theorem (Mazur, 1978)

$$\mathrm{tor}(E/\mathbb{Q}) \cong \begin{cases} C_n, & \text{for } n = 1, \ldots, 10, 12, \\ C_2 \oplus C_{2n}, & \text{for } n = 1, \ldots, 4. \end{cases}$$

Computing torsion subgroups

Theorem (Lutz–Nagell, 1937)

Let E be an elliptic curve over $\mathbb{Q}$ with $a_1 = a_2 = a_3 = 0$ and $a_4, a_6 \in \mathbb{Z}$. If $(x, y) \in \mathrm{tor}(E/\mathbb{Q})$, then

1. *$x, y \in \mathbb{Z}$, and*
2. *either $y = 0$ or $y^2 \mid 4a_4^3 + 27a_6^2$.*

Note that $\Delta = -16(4a_4^3 + 27a_6^2)$, and

$$4a_4^3 + 27a_6^2 = 3(3y^2 + 4a_4x + 6a_6)y^2 - (3x^2 + 4a_4)\psi_3(x, y).$$

To compute $\mathrm{tor}(E/\mathbb{Q})$:

- Find all $y \in \mathbb{Z}$ such that $y^2 \mid 4a_4^3 + 27a_6^2$.
- For each such y, find all $x \in \mathbb{Z}$ such that $x^3 + a_4x + (a_6 - y^2) = 0$.
- For each such (x, y), check that it is in $\mathrm{tor}(E/\mathbb{Q})$.

An illustrative example

Let E be the elliptic curve $y^2 = x^3 + 8$ over $\mathbb{Q}$ and $(x, y) \in \mathrm{tor}(E/\mathbb{Q})$. Then $x, y \in \mathbb{Z}$, and either $y = 0$ or $y^2 \mid 1728 = 2^6 \cdot 3^3$. Hence,

$$y^2 \in \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, 64, 72, 96, 108, 144, 192, 216, 288, 432, 576, 864, 1728\}.$$

y^2	0	1	4	9	16	36	64	144	576
$8 - y^2$	8	7	4	-1	-8	-28	-56	-136	-568
x	-2	N/A	N/A	1	2	N/A	N/A	N/A	N/A
y	0	± 1	± 2	± 3	± 4	± 6	± 8	± 12	± 24

Therefore, $(x, y) \in \{(-2, 0), (1, \pm 3), (2, \pm 4)\}$. Now,

$$[2](-2, 0) = O, \quad [2](1, \pm 3) = (-\tfrac{7}{4}, \mp \tfrac{13}{8}), \quad [2](2, \pm 4) = (-\tfrac{7}{4}, \pm \tfrac{13}{8}).$$

Thus, $\mathrm{tor}(E/\mathbb{Q}) = \{O, (-2, 0)\}$. In fact, $\mathrm{tor}(E/\mathbb{Q}) = \langle (-2, 0) \rangle \cong C_2$.

An elementary proof

Let $(x, y) \in \mathrm{tor}(E/\mathbb{Q})$ such that $y^2 = x^3 + a_4x + a_6$. May write

$$x = \frac{b}{d^2}, \qquad y = \frac{c}{d^3}, \qquad (b, d) = (c, d) = 1.$$

If $[n](x, y) \in \mathbb{Z}^2$, then $(x, y) \in \mathbb{Z}^2$, since the X-coordinate of $[n](x, y)$ is

$$\frac{\phi_n(x, y)}{\psi_n(x, y)^2} = \frac{x^{n^2} + \dots}{n^2 x^{n^2-1} + \dots} = \frac{b^{n^2} + d^2(\dots)}{d^2(n^2 b^{n^2-1} + \dots)}.$$

May assume that $[p](x, y) = O$ for $p > 2$. Then $\psi_p(x, y) = 0$, so

$$0 = \psi_p(x, y)^2 = p^2 x^{p^2-1} + \dots = \frac{p^2 b^{p^2-1} + d^2(\dots)}{d^{2(p^2-1)}}.$$

Thus $(x, y) \in \mathbb{Z}^2$. Now the X-coordinate of $[2](x, y) \in \mathrm{tor}(E/\mathbb{Q})$ is $x - \psi_3(x, y)/4y^2$, so $y^2 \mid \psi_3(x, y)$, and hence $y^2 \mid 4a_4^3 + 27a_6^2$.

Lean formalisation

Chris, ChatGPT, and Claude Code (CCCC) formalised this in a day!

Theorem (CCCC, 2026)

Let E be an elliptic curve over a number field K of class number one with $a_1 = a_3 = 0$ and $a_2, a_4, a_6 \in \mathcal{O}_K$. If $(x, y) \in \mathrm{tor}(E/K)$, and the primes dividing the order of (x, y) do not ramify in K, then

- $x, y \in \mathcal{O}_K$, *and*
- *either* $y = 0$ *or* $y^2 \mid (4a_4^3 + 27a_6^2) + a_2(4a_2^2 a_6 - a_2 a_4^2 - 18a_4 a_6)$.

When $a_1 \neq 0$ or $a_3 \neq 0$, they proved an alternative statement with $y^2 \mid \Delta$.

I am automating the computations of $\mathrm{tor}(E/\mathbb{Q})$ using `simprocs`.

When $4a_4^3 + 27a_6^2$ is massive, its factorisation can be extracted from the LMFDB to circumvent divisor `dsimprocs`, which uses trial division.