# Rational points on elliptic curves in Lean

Rational Points 2025

David Ang

London School of Geometry and Number Theory

Thursday, 31 July 2025

# Introduction

The process of formalising mathematics is interesting for many reasons. One important reason is to ensure that a mathematical argument is sound and complete, as the standard literature may sometimes be hazy.

Alongside my PhD, I have been developing the *algebraic* foundations of elliptic curves in the Lean 4 theorem prover, mostly in joint work with **Junyan Xu (Heidelberg)**, but with important contributions by Jinzhao Pan (Tongji), Kevin Buzzard and Andrew Yang (Imperial), Michael Stoll (Bayreuth), Peiran Wu (Leuven), Kenny Lau (unaffiliated), and others.

In my case, due to limitations of the algebraic geometry in Lean's mathematical library `mathlib`, we were forced to think outside the box. In the process, we could generalise existing definitions to suit our needs, and inadvertently discovered novel proofs of ancient results.

# Weierstrass curves

In 2021, Buzzard formalised a *working* definition of an elliptic curve in terms of its Weierstrass model that is amenable for computation.

## Definition

A **Weierstrass curve** $C_R$ over a commutative ring $R$ with unity is a tuple $(a_1, a_2, a_3, a_4, a_6) \in R^5$. Given $C_R$, define

$$b_2 := a_1^2 + 4a_2, \qquad b_4 := 2a_4 + a_1 a_3, \qquad b_6 := a_3^2 + 4a_6,$$

$$b_8 := a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \qquad c_4 := b_2^2 - 24 b_4,$$

$$c_6 := -b_2^3 + 36 b_2 b_4 - 216 b_6, \qquad \Delta := -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6.$$

If $\Delta \in R^\times$, then $C_R$ is **elliptic**, and define $j := c_4^3 / \Delta$.

This recovers all elliptic curves over $\mathrm{Spec}(R)$ when $\mathrm{Pic}(R) = 0$.

# Changes of variables

Any two Weierstrass equations of an elliptic curve are related by $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ for some $u \in R^\times$ and some $r, s, t \in R$.

## Definition

A **variable change** is a tuple $v = (u, r, s, t) \in R^\times \times R^3$. Given $C_R$, define

$$v \cdot C_R := \Big(\frac{a_1+2s}{u}, \frac{a_2-sa_1+3r-s^2}{u^2}, \frac{a_3+ra_1+2t}{u^3}, \frac{a_4-sa_3+2ra_2-(t+rs)a_1+3r^2-2st}{u^4}, \frac{a_6+ra_4+r^2a_2+r^3-ta_3-t^2-rta_1}{u^6}\Big).$$

If $C'_R = v \cdot C_R$ for some $v \in R^\times \times R^3$, then $C_R$ and $C'_R$ are **isomorphic**.

Pan formalised Silverman's normal forms of $C_R$ when $\mathrm{char}(R) = 2, 3$, as well as a proof that $C_{F^s}$ and $C'_{F^s}$ are isomorphic over the *separable closure $F^s$ of a field $F$* iff they have the same $j$. Recently, Lau formalised the Tate normal form of $C_F$ when it has a point of order at least four.

# Affine coordinates

For an $R$-algebra $A$, the $A$-points on $C_R$ are given in affine coordinates.

## Definition

An **affine** $A$**-point** on $C_R$ is a tuple $(x, y) \in A^2$ that vanishes on

$$f_{C_R} := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6).$$

It is **nonsingular** if its two partial derivatives generate $A$. A **nonsingular** $A$**-point** on $C_R$ is either $\mathcal{O}_{C_R}$ or a nonsingular affine $A$-point on $C_R$.

Note that when $C_R$ is elliptic, all $A$-points on $C_R$ are nonsingular.

In this case, Stoll, Xu, and I formalised in 2024 the fact that the functor of *affine* points $\mathbf{AffSch}_R^{\mathrm{op}} \to \mathbf{Set}$ is representable by $\mathrm{Spec}(R[X, Y]/\langle f_{C_R} \rangle)$.

# The group law

Addition on nonsingular $F$-points is given by explicit rational functions, where associativity is known to be *computationally difficult*: generic associativity involves an equality of polynomials with 26,082 terms!

**Formalisation (A.–Xu, 2022)**

*The type of nonsingular $F$-points $C_F(F)$ forms an additive abelian group.*

It suffices to show that the homomorphism $C_F(F) \to \mathrm{Cl}(F[X, Y]/\langle f_{C_F} \rangle)$ mapping $(x, y)$ to $[\langle X - x, Y - y \rangle]$ is injective. If it were not, then there are polynomials $f, g \in F[X]$ such that $\langle X - x, Y - y \rangle = \langle f + gY \rangle$. Then

$$\deg(\mathrm{Nm}(f + gY)) = \begin{cases} \max(2\deg(f), 2\deg(g) + 3) \\ \dim_F(F[X, Y]/\langle f_{C_F}, f + gY \rangle) \end{cases},$$

which is a contradiction.

# Miscellaneous results

I formalised some basic results for $C_F(F)$:

- $C_F(F) \cong C'_F(F)$ as additive groups when $C_F$ and $C'_F$ are isomorphic
- the torsion subgroup $C_F(F)_{\mathrm{tors}}$, including the statement of Mazur's torsion theorem, and the $n$-torsion subgroup $C_F(F)[n]$
- for a tower of finite Galois extensions $L/K/F$,

$$C_F(L)^{\mathrm{Gal}(L/K)} \cong C_F(K), \qquad C_F(L)[n]^{\mathrm{Gal}(L/K)} \cong C_F(K)[n]$$

Recently, Yang formalised a basic interface of singular Weierstrass curves.

**Question (Yang, 2025)**

*Is there a clean description of $C_F(F)$ when $C_F$ is not elliptic?*

Silverman gives a complete description of $C_F$ *when $F$ is perfect*.

# The $n$-torsion subgroup

In 2023, I attempted to formalise the isomorphism $C_F(F^s)[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

**Formalisation (A.–Wu–Xu, 2025?)**

*If $C_F$ is elliptic and $\mathrm{char}(F) \neq \ell$, then $T_\ell C_{F^s} \cong \mathbb{Z}_\ell^2$ as $\mathbb{Z}_\ell[G_F]$-modules.*

Silverman defines polynomials $\psi_n, \phi_n, \omega_n \in F^s[X, Y]$ and *claims* that there is a computational proof for the multiplication-by-$n$ formula

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

Computing $\deg(\phi_n) = n^2$ and $\deg(\psi_n^2) = n^2 - 1$, and proving that $(\phi_n, \psi_n^2) = 1$, imply that $\# \ker[n] = n^2$, and the result follows formally.

The complete argument also recovers $T_\ell C_{F^s}$ when $\mathrm{char}(F) = \ell$.

# Projective coordinates

## Definition

The **weighted projective space** $\mathbb{P}_R^w$ with weights $w = (w_0, \ldots, w_n)$ is

$$\{(x_0, \ldots, x_n) \in R^{n+1} : \langle x_0, \ldots, x_n \rangle = R\} / R^\times,$$

with an $R^\times$-action given by $u \cdot (x_0, \ldots, x_n) = (u^{w_0} x_0, \ldots, u^{w_n} x_n)$.

This is precisely $\operatorname{Proj} R[X_0, \ldots, X_n]^w$ when $\operatorname{Pic}(R) = 0$, and the natural injection $\mathbb{P}_R^w \to \mathbb{P}_{\operatorname{Frac}(R)}^w$ is bijective when $R$ is a discrete valuation ring.

## Definition

A **nonsingular Jacobian $A$-point** on $C_R$ is an element of $\mathbb{P}_A^{(2,3,1)}$ that vanishes in the $(2, 3, 1)$-weighted homogenisation $f_{C_R}^{(2,3,1)} \in R[X, Y, Z]$ of $f_{C_R}$, such that its three partial derivatives generate $A$.

# Division polynomials

## Definition

Given $C_R$, the *n*-**th division polynomial** $\psi_n \in R[X, Y]$ is given by

$$\begin{aligned}
\psi_0 &:= 0, \\
\psi_1 &:= 1, \\
\psi_2 &:= 2Y + a_1 X + a_3, \\
\psi_3 &:= 3X^4 + b_2 X^3 + 3b_4 X^2 + 3b_6 X + b_8, \\
\psi_4 &:= \psi_2 \cdot \left(2X^6 + b_2 X^5 + 5b_4 X^4 + 10b_6 X^3 + 10b_8 X^2 + (b_2 b_8 - b_4 b_6)X + (b_4 b_8 - b_6^2)\right), \\
\psi_{2n+1} &:= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \\
\psi_{2n} &:= \frac{\psi_{n-1}^2 \psi_n \psi_{n+2} - \psi_{n-2}\psi_n \psi_{n+1}^2}{\psi_2}, \\
\psi_{-n} &:= -\psi_n.
\end{aligned}$$

# Numerator polynomials

Given $\psi_n$, the polynomials $\phi_n, \omega_n \in R[X, Y]$ are given by

$$\phi_n := X\psi_n^2 - \psi_{n-1}\psi_{n+1}, \qquad \omega_n := \tfrac{1}{2}(\psi_{2n}/\psi_n - a_1\phi_n\psi_n - a_3\psi_n^3).$$

*It is not obvious that* $\omega_n \in R[X, Y]$! In 2024, Xu showed that this reduces to proving that $\psi_n$ forms an **elliptic sequence**: for all $n, m, r \in \mathbb{Z}$,

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2.$$

I think this is still not directly provable. Instead, Xu proved that $\psi_n$ forms an **elliptic net** in the sense of Stange: for all $n, m, r, s \in \mathbb{Z}$,

$$\psi_{n+m}\psi_{n-m}\psi_{r+s}\psi_{r-s} = \psi_{n+r}\psi_{n-r}\psi_{m+s}\psi_{m-s} - \psi_{m+r}\psi_{m-r}\psi_{n+s}\psi_{n-s}.$$

Later, Xu gave a complete proof of the multiplication-by-$n$ formula.

# The local theory

I believe it is possible to formalise much of the *arithmetic* foundations of elliptic curves while the algebraic geometry in `mathlib` catches up.

When $K$ is a global field, reduction modulo $\mathfrak{p}$ is the homomorphism

$$C_K(K) \hookrightarrow C_K(K_\mathfrak{p}) \xleftarrow{\sim} C_K(\mathcal{O}_\mathfrak{p}) \twoheadrightarrow C_K(\kappa_\mathfrak{p}).$$

Upon developing a theory of formal groups, it should be possible to compute torsion subgroups via the Lutz–Nagell theorem, classify reduction types, define the conductor for $\mathrm{char}(\kappa_\mathfrak{p}) \neq 2, 3$, prove the Néron–Ogg–Shafarevich criterion, state Szpiro's conjecture, etc.

Note that Tate's algorithm was implemented by Best, Dahmen, and Huriot-Tattegrain in 2023 before elliptic curves existed in Lean 4!

# The global theory

Much of the theory over a global field $K$ now becomes accessible!

- Isogenies can be defined in terms of their standard form when $\mathrm{char}(F) \neq 2, 3$, which opens the door to formalising basic facts about $\mathrm{Hom}_F(C_F, C'_F)$, $\mathrm{End}_F(C_F)$, and $\mathrm{Aut}_F(C_F)$.
- The $\ell$-adic representations $G_K \to \mathrm{Aut}(T_\ell C_{K^s})$ can be glued together to give an adelic representation $G_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$.
- Assuming modularity, the L-function and the Tamagawa number can both be defined as products of local factors.
- In 2022, I formalised a skeleton of the full Mordell–Weil theorem over $\mathbb{Q}$ in Lean 3 via complete 2-descent, including explicit Galois cohomology and naïve heights. Formalising this properly in Lean 4 naturally leads to the definitions of $\text{Ш}(C_K)$, $\mathrm{rk}(C_K)$, and $\mathrm{Reg}(C_K)$.

*All of these are part of the Birch and Swinnerton-Dyer conjecture*!

# The Birch and Swinnerton-Dyer conjecture

Here is my blueprint for the Birch and Swinnerton-Dyer conjecture.