Formalising division polynomials in Lean

Lean 形式化数学学习强化和实践交流研讨会

David Ang (洪鼎赐)

University of East Anglia

Monday, 26 January 2026

The weak Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve over a number field K.

Conjecture (weak Birch and Swinnerton-Dyer)

The rank of E is the order of vanishing of its L-function $L(E, s)$ at $s = 1$.

Here, the *L-function* of E is given by

$$L(E, s) := \prod_{p} \frac{1}{L_p(E, s)},$$

where p runs over all primes of K, and the Euler factor $L_p(E, s)$ is defined in terms of the *ℓ-adic Galois representation* $\rho_{E,\ell}$ for any prime ℓ with $p \nmid \ell$. This is the action of the absolute Galois group of K_p on the *ℓ-adic Tate module* $T_\ell E$, which is the inverse limit of *ℓ^n-torsion subgroups*

$$E(\overline{K_p})[\ell^n] := \{P \in E(\overline{K_p}) : [\ell^n](P) = 0\},$$

with respect to the multiplication-by-ℓ maps $[\ell] : E(\overline{K_p}) \to E(\overline{K_p})$.

The n-torsion subgroup and the ℓ-adic Tate module

Let E be an elliptic curve over a perfect field F.

Theorem (main)

$\#E(\overline{F})[n] = n^2$ for any $n \in \mathbb{N}$ with $\mathrm{char}(F) \nmid n$.

If G is an abelian group such that $\#G[n] = n^d$ for all $n \in \mathbb{N}$, then $G[n] \cong (\mathbb{Z}/n)^d$ by the structure theorem of finite abelian groups. In particular, $E(\overline{F})[n] \cong (\mathbb{Z}/n)^2$ for any $n \in \mathbb{N}$ with $\mathrm{char}(F) \nmid n$, so

$$\begin{array}{ccccccccc}
T_\ell E := \varprojlim \Big(\dots & \xrightarrow{[\ell]} & E(\overline{F})[\ell^3] & \xrightarrow{[\ell]} & E(\overline{F})[\ell^2] & \xrightarrow{[\ell]} & E(\overline{F})[\ell] \Big) \\
\downarrow \sim & & \downarrow \sim & & \downarrow \sim & & \downarrow \sim \\
\mathbb{Z}_\ell^2 := \varprojlim \Big(\dots & \xrightarrow{\bmod \ell^3} & (\mathbb{Z}/\ell^3)^2 & \xrightarrow{\bmod \ell^2} & (\mathbb{Z}/\ell^2)^2 & \xrightarrow{\bmod \ell} & (\mathbb{Z}/\ell)^2 \Big).
\end{array}$$

吴培然 formalised the reduction of $\rho_{E,\ell}$ to the main theorem.

An infamous exercise

The Arithmetic of Elliptic Curves by Silverman gives several approaches to the main theorem (see Theorem III.6.4(b) and Theorem VI.6.1(a)).

Exercise (3.7(d))

Let $n \in \mathbb{Z}$. Prove that for any point $(x, y) \in E(F)$,

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

Silverman gives definitions for $\phi_n, \omega_n \in F[X, Y]$ in terms of certain *division polynomials* $\psi_n \in F[X, Y]$, which feature in Schoof's algorithm.

Conjecture (洪)

No one has done Exercise 3.7 purely algebraically.

许俊彦 formalised a complete solution to Exercise 3.7(d).

The polynomials ψ_n

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

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

In `mathlib`, ψ_n is defined in terms of $\Psi_n \in R[X]$.

The polynomials Ψ_n

The polynomial $\Psi_n \in R[X]$ is given by

$$\begin{aligned}
\Psi_0 &:= 0, \\
\Psi_1 &:= 1, \\
\Psi_2 &:= 1, \\
\Psi_3 &:= \bigcirc, \\
\Psi_4 &:= \triangle, \\
\Psi_{2n+1} &:= \begin{cases} \Psi_{n+2}\Psi_n^3 - \square^2\Psi_{n-1}\Psi_{n+1}^3 & \text{if } n \text{ is odd,} \\ \square^2\Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3 & \text{if } n \text{ is even,} \end{cases} \\
&\quad \text{where } \square := 4X^3 + b_2X^2 + 2b_4X + b_6, \\
\Psi_{2n} &:= \Psi_{n-1}^2\Psi_n\Psi_{n+2} - \Psi_{n-2}\Psi_n\Psi_{n+1}^2, \\
\Psi_{-n} &:= -\Psi_n.
\end{aligned}$$

Then $\psi_n = \Psi_n$ when n is odd and $\psi_n = \psi_2\Psi_n$ when n is even.

The polynomials ϕ_n and Φ_n

Modulo the Weierstrass equation $E(X, Y)$ defining E,

$$\begin{aligned}\psi_2^2 &= (2Y + a_1X + a_3)^2 \\ &= 4(Y^2 + a_1XY + a_3Y) + a_1^2X^2 + 2a_1a_3X + a_3^2 \\ &\equiv \underbrace{4X^3 + b_2X^2 + 2b_4X + b_6}_{\square} \mod E(X, Y).\end{aligned}$$

In particular, ψ_n^2 and $\psi_{n+1}\psi_{n-1}$ are congruent to polynomials in $R[X]$.

The polynomial $\phi_n \in R[X, Y]$ is given by

$$\phi_n := X\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

so that $\phi_n \equiv \Phi_n \mod E(X, Y)$, where $\Phi_n \in R[X]$ is given by

$$\Phi_n := \begin{cases} X\Psi_n^2 - \square\Psi_{n+1}\Psi_{n-1} & \text{if } n \text{ is odd,} \\ X\square\Psi_n^2 - \Psi_{n+1}\Psi_{n-1} & \text{if } n \text{ is even.} \end{cases}$$

The polynomials ω_n

The polynomial $\omega_n \in R[X, Y]$ is given by

$$\omega_n := \frac{1}{2}\left(\frac{\psi_{2n}}{\psi_n} - a_1\phi_n\psi_n - a_3\psi_n^3\right).$$

Lemma (许)

Let $n \in \mathbb{Z}$. Then $\psi_{2n}/\psi_n - a_1\phi_n\psi_n - a_3\psi_n^3$ is divisible by 2 in $\mathbb{Z}[a_i, X, Y]$.

Example ($a_1 = a_3 = 0$)

$$\omega_2 = \frac{\Psi_4}{2} = \frac{2X^6+4a_2X^5+10a_4X^4+40a_6X^3+10b_8X^2+(4a_2b_8-8a_4a_6)X+(2a_4b_8-16a_6^2)}{2}.$$

Define ω_n as the image of the quotient under $\mathbb{Z}[a_i, X, Y] \to R[X, Y]$.

When $n = 4$, this quotient has 15,049 terms.

Elliptic divisibility sequences and elliptic nets

Integrality relies on the fact that ψ_n is an **elliptic divisibility sequence**.

Exercise (3.7(g))

For all $n, m, r \in \mathbb{Z}$, prove that $\psi_n \mid \psi_{nm}$ and

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

Note that this generalises the recursive definitions of ψ_{2n+1} and ψ_{2n}.

Surprisingly, this needs the stronger result that ψ_n is an **elliptic net**.

Theorem (许)

Let $n, m, r, s \in \mathbb{Z}$. Then

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

Elliptic divisibility sequences were first introduced by Morgan Ward (1948) and generalised to elliptic nets by Katherine Stange (2008).

Other formalised results

The polynomial $\Psi_n^{(2)} \in R[X]$ is given by

$$\Psi_n^{(2)} := \begin{cases} \Psi_n^2 & \text{if } n \text{ is odd,} \\ \Box\Psi_n^2 & \text{if } n \text{ is even,} \end{cases}$$

so that $\Psi_2^{(2)} = \Box$ and $\Psi_n^{(2)} \equiv \psi_n^2 \mod E(X, Y)$.

Exercise (3.7(b))

Show that $\Phi_n = X^{n^2} + \ldots$ *and* $\Psi_n^{(2)} = n^2 X^{n^2-1} + \ldots$.

This is an inductive computation of `natDegree` and `leadingCoeff`.

Exercise (3.7(c))

Prove that Φ_n *and* $\Psi_n^{(2)}$ *are relatively prime.*

Surprisingly, this needs Exercise 3.7(d) and the assumption that $\Delta \neq 0$.

A blueprint for the ℓ-adic Tate module