Division polynomials of elliptic curves

Lean Together 2025

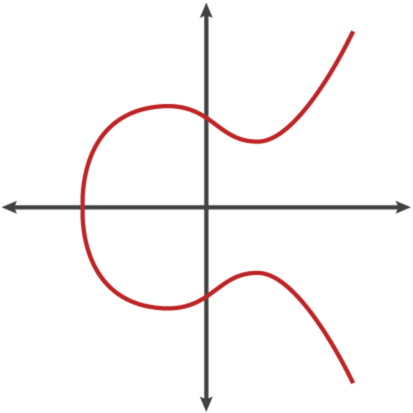
David Kurniadi Angdinata (with Junyan Xu)

London School of Geometry and Number Theory

Friday, 17 January 2025

Elliptic curves

An elliptic curve over a field F is a smooth projective curve E of genus one, equipped with a fixed point $\mathcal{O}$ defined over F.



They are one of the simplest non-trivial objects in arithmetic geometry.

Weierstrass equations

In `mathlib`, an **elliptic curve** E over an integral domain R is a tuple $(a_1, a_2, a_3, a_4, a_6) \in R^5$, with an extra condition that $\Delta \in R^\times$, where

$$
\begin{aligned}
b_2 &:= a_1^2 + 4a_2, \\
b_4 &:= 2a_4 + a_1 a_3, \\
b_6 &:= a_3^2 + 4a_6, \\
b_8 &:= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
\Delta &:= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.
\end{aligned}
$$

A **point** on E is either $\mathcal{O}$ or an **affine point** $(x, y)_a \in R^2$ such that

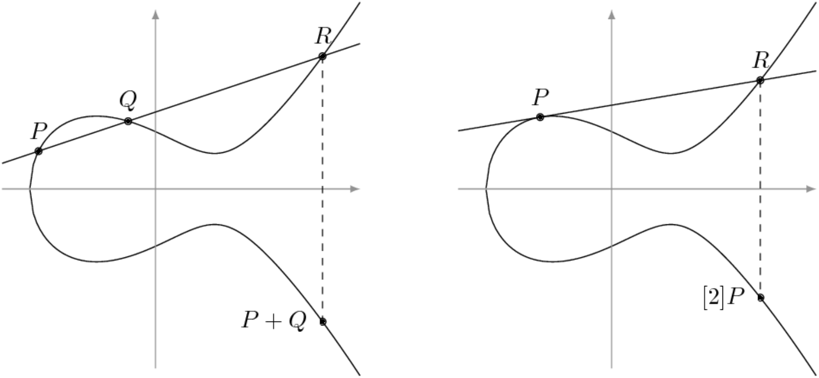
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^3 + a_6,$$

so the points on E vanish on the polynomial $\mathcal{E} \in R[X, Y]$ given by

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

Group law

The points on E can be endowed with a geometric addition law.



In 2023, we formalised a novel algebraic proof of the group law on E.

Is there an explicit formula for $[n]P$ in terms of P?

An impossible exercise

The Arithmetic of Elliptic Curves by Silverman gives an answer.

Exercise (3.7(d))

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

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

Silverman gives inductive definitions for $\phi_n, \omega_n, \psi_n \in F[X, Y]$.

This formula leads to a proof that

$$T_p E_{\overline{F}} \cong \begin{cases} \mathbb{Z}_p^2 & \text{if } \operatorname{char}(F) \neq p, \\ 0 \text{ or } \mathbb{Z}_p & \text{if } \operatorname{char}(F) = p. \end{cases}$$

These polynomials also feature in Schoof's algorithm.

Multiplication by 2

If $(x, y)_a$ is a generic affine point on E, then

$$[2](x, y)_a = \left(\frac{\phi_2(x, y)}{\psi_2(x, y)^2}, \frac{\omega_2(x, y)}{\psi_2(x, y)^3} \right)_a ,$$

where $\phi_2, \omega_2, \psi_2 \in F[X, Y]$ are given by

$$\begin{aligned} \psi_2 &:= 2Y + a_1 X + a_3, \\ \phi_2 &:= X\psi_2^2 - \bigcirc, \\ \omega_2 &:= \frac{1}{2}(\triangle - (a_1\phi_2 + a_3)\psi_2^3), \end{aligned}$$

for some $\bigcirc, \triangle \in F[X]$. If $(x, y)_a$ is a 2-torsion affine point on E, then

$$(x, y)_a = -(x, y)_a = (x, -y - a_1 x - a_3)_a,$$

so $\psi_2(x, y) = 2y + a_1 x + a_3 = 0$.

Projective coordinates

Let $(x, y)_a$ be an affine point on E. In **projective** coordinates,

$$[2](x, y)_a = (\phi_2(x, y)\psi_2(x, y) : \omega_2(x, y) : \psi_2(x, y)^3)_p.$$

In `mathlib`, a **projective point** on E is a class of $(x, y, z) \in F^3$ such that

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3.$$

The point at infinity on E is $(0 : 1 : 0)_p$.

More naturally, in **Jacobian** coordinates with weights $(2 : 3 : 1)$,

$$[2](x, y)_a = (\phi_2(x, y) : \omega_2(x, y) : \psi_2(x, y))_j.$$

In `mathlib`, a **Jacobian point** on E is a class of $(x, y, z) \in F^3$ such that

$$y^2 + a_1 xyz + a_3 yz^3 = x^3 + a_2 x^2 z^2 + a_4 xz^4 + a_6 z^6.$$

The point at infinity on E is $(1 : 1 : 0)_j$.

Multiplication by n

Exercise (3.7(d), corrected)

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

$$[n](x, y)_a = (\phi_n(x, y) : \omega_n(x, y) : \psi_n(x, y))_j.$$

If $(x : y : z)_j$ is a point on E, then $x = y = 1$ whenever $z = 0$, so

$$\ker[n] = \{\mathcal{O}\} \cup \{(x, y)_a : \psi_n(x, y) = 0\}.$$

Conjecture

No one has done Exercise 3.7(d) purely inductively.

Xu gave a complete answer to this exercise and formalised it in Lean.

I will define ϕ_n, ω_n, ψ_n, and their auxiliary polynomials.

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

In the coordinate ring of E,

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

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 $\phi_n \equiv \Phi_n \mod \mathcal{E}$, 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 (Xu)

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

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 (Xu)

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

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

Xu gave an elegant proof of this on Math Stack Exchange.

The Somos-4 invariant

As an elliptic sequence, ψ_n satisfies the **Somos-4 recurrence**

$$\psi_{n+2}\psi_{n-2} = \psi_2^2\psi_{n+1}\psi_{n-1} - \psi_3\psi_n^2.$$

An easy induction gives an invariant

$$\mathcal{I}(n) := \frac{\psi_{n-1}^2\psi_{n+2} + \psi_{n-2}\psi_{n+1}^2 + \psi_2^2\psi_n^3}{\psi_{n+1}\psi_n\psi_{n-1}}.$$

When $n = 2$, an explicit computation gives

$$\mathcal{I}(2) = \frac{\psi_4 + \psi_2^5}{\psi_3\psi_2} \equiv a_1\psi_2 \mod 2.$$

Being an invariant means that $\mathcal{I}(n) = \mathcal{I}(2)$, so

$$\frac{\psi_{n-1}^2\psi_{n+2} + \psi_{n-2}\psi_{n+1}^2 + \psi_2^2\psi_n^3}{\psi_2} \equiv a_1\psi_{n+1}\psi_n\psi_{n-1} \mod 2.$$

Integrality of ω_n

In particular,

$$\begin{aligned}\frac{\psi_{2n}}{\psi_n} &= \frac{\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2}{\psi_2} && \text{by definition of } \psi_{2n} \\ &\equiv \psi_2\psi_n^3 + a_1\psi_{n+1}\psi_n\psi_{n-1} \mod 2 && \text{by } \mathcal{I}(n) = \mathcal{I}(2) \\ &= 2Y\psi_n^3 + a_1\underbrace{(X\psi_n^2 + \psi_{n+1}\psi_{n-1})}_{\phi_n}\psi_n + a_3\psi_n^3 && \text{by definition of } \psi_2.\end{aligned}$$

Thus $\psi_{2n}/\psi_n - a_1\phi_n\psi_n - a_3\psi_n^3 \equiv 0 \mod 2$. In Lean,

$$\begin{aligned}\omega_n := \frac{\psi_{n+1}\psi_n\psi_{n-1}}{\psi_2\psi_3}(4\mathcal{E}(2\mathcal{E} + \square) + \psi_3(a_1\psi_2 - \tfrac{\partial\mathcal{E}}{\partial X})) \\ - \frac{\psi_{n-2}\psi_{n+1}^2}{\psi_2} + (Y - \psi_2)\psi_n^3,\end{aligned}$$

which is well-defined, since ψ_n is a divisibility sequence.

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 $\Psi_n^{(2)} \equiv \psi_n^2 \mod \mathcal{E}$.

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 $\Delta \neq 0$.