Elliptic divisibility sequences in Lean

British Mathematical Colloquium and British Applied Mathematics Colloquium

David Kurniadi Angdinata (with Junyan Xu)

London School of Geometry and Number Theory

Wednesday, 25 June 2025

Formalising mathematics

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.

Throughout my PhD, I have been formalising the algebraic foundations of elliptic curves in the **Lean 4 theorem prover** as a side project.

In the process, we accidentally discovered a novel purely algebraic proof of the group law on the points of an elliptic curve over a field.

Two years ago, I was stuck trying to formalise a result on division points simply because the standard literature turned out to be incomplete.

Since this is a joint session, *there will be no Lean in this talk*!

Elliptic divisibility sequences

Let $W := \{W_n\}_{n\in\mathbb{Z}}$ be a sequence of elements in a commutative ring R.

Then W is

- a **divisibility sequence** if for all $m, n \in \mathbb{Z}$,

$$m \mid n \qquad \Longrightarrow \qquad W_m \mid W_n,$$

- an **elliptic sequence** if for all $p, q, r \in \mathbb{Z}$,

$$W_{p+q}W_{p-q}W_r^2 + W_{q+r}W_{q-r}W_p^2 + W_{r+p}W_{r-p}W_q^2 = 0,$$

- an **elliptic divisibility sequence (EDS)** if it is simply a divisibility sequence that is elliptic.

EDSs were first introduced by Morgan Ward (1948), where he studied their arithmetic properties in relation to elliptic curves.

Examples in nature

There are many examples of EDSs in nature with integer values.

Examples

- The constant sequence $W_n = 0$ for all $n \in \mathbb{Z}$ is an EDS.
- The identity sequence $W_n = n$ for all $n \in \mathbb{Z}$ is an EDS.
- If W is an EDS, then $\{cW_n\}_{n\in\mathbb{Z}}$ is an EDS for any $c \in \mathbb{Z}$.
- The subsequence of even terms of the Fibonacci sequence is an EDS:

$$1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, 17711, 46368, 121393, \ldots.$$

- Certain subsequences of Lucas sequences $L := \{L_n\}_{n\in\mathbb{Z}}$ given by $L_1 = 1$, $L_2 = \ell$, and $L_{n+2} = \ell \cdot L_{n+1} - L_n$ for all $n > 2$ are EDSs.
- Certain generalised Somos-4 sequences $a := \{a_n\}_{n\in\mathbb{Z}}$ given by $a_n a_{n-4} = a_{n-1}a_{n-3} + a_{n-2}^2$ are EDSs. For instance, the generalised Somos-4 sequence with $(a_1, a_2, a_3, a_4) = (1, 1, -1, 2)$ is an EDS:

$$0, 1, 1, -1, 2, 3, 1, -11, -16, 35, -129, -299, -386, 3977, 8063, \ldots.$$

Division polynomials

Perhaps the most important example of an EDS is the sequence arising from division points on an elliptic curve E over a field F.

Exercise (The Arithmetic of Elliptic Curves, 3.7(d))

Prove that for any point $(x : y : 1)$ *on* E *we have for all* $n \in \mathbb{Z}$,

$$[n](x : y : 1) = (\phi_{E,n}(x,y)\psi_{E,n}(x,y) : \omega_{E,n}(x,y) : \psi_{E,n}(x,y)^3).$$

Here, $\phi_{E,n}, \omega_{E,n} \in F[X,Y]$ are defined in terms of **division polynomials** $\psi_{E,n} \in F[X,Y]$. Then the sequence $\psi_E := \{\psi_{E,n}\}_{n\in\mathbb{Z}}$ is an EDS.

This is *one path* to formalising the isomorphism of Galois representations

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

which is useful for Buzzard's formalisation of Fermat's last theorem.

Special cases

EDSs can be generated easily by inspecting special cases of $(p, q, r) \in \mathbb{Z}^3$.

Let $p, q \in \mathbb{Z}$ be arbitrary, and let $r = 0$. Then

$$W_{p+q} W_{p-q} W_0^2 + W_q W_q W_p^2 + W_p W_{-p} W_q^2 = 0.$$

Since $W_0 \nmid W_n$ for any $n \in \mathbb{Z}$, it is *sensible* to set $W_0 = 0$. This forces $W_p W_{-p} W_q^2 = -W_p^2 W_q^2$, so it is *sensible* to set $W_{-p} = -W_p$.

If two of $p, q, r > 0$ are the same, say $q = r$, then

$$W_{p+q} W_{p-q} W_q^2 + W_{2q} W_0 W_p^2 + W_{q+p} W_{q-p} W_q^2 = 0.$$

This is trivial, so assume that $p > q > r > 1$.

- If $(p, q, r) = (3, 2, 1)$, then $W_5 W_1^3 + W_3^3 W_1 - W_4 W_2^3 = 0$.
- If $(p, q, r) = (4, 2, 1)$, then $W_6 W_2 W_1^2 + W_3 W_1 W_4^2 - W_5 W_3 W_2^2 = 0$.

It turns out that all non-trivial relations can be generated this way.

Recursive cases

If $(p, q, r) = (n+1, n, 1)$ for some $n > 0$, then

$$W_{2n+1} W_1^3 + W_{n+1}^3 W_{n-1} - W_{n+2} W_n^3 = 0.$$

If W_1 is not a zero divisor, then this gives a non-trivial relation

$$W_{2n+1} = \frac{W_{n+2} W_n^3 - W_{n+1}^3 W_{n-1}}{W_1^3} \qquad \text{for all } n > 1.$$

If $(p, q, r) = (n+1, n-1, 1)$ for some $n > 0$, then

$$W_{2n} W_2 W_1^2 + W_n W_{n-2} W_{n+1}^2 - W_{n+2} W_n W_{n-1}^2 = 0.$$

If W_1 and W_2 are not zero divisors, then this gives a non-trivial relation

$$W_{2n} = \frac{W_{n+2} W_n W_{n-1}^2 - W_n W_{n-2} W_{n+1}^2}{W_2 W_1^2} \qquad \text{for all } n > 2.$$

Thus a sensible EDS is *completely determined* by its first four values.

The canonical EDS

Let $a, b, c, d \in R$ such that a and b are not zero divisors. The **canonical EDS defined by** (a, b, c, d) is the sequence $C := \{C_n\}_{n\in\mathbb{Z}}$ given by

$$
\begin{aligned}
C_0 &:= 0, \\
C_1 &:= a, \\
C_2 &:= ab, \\
C_3 &:= ac, \\
C_4 &:= abd, \\
C_{-n} &:= -C_n && \text{for all } n < 0, \\
C_{2n+1} &:= \frac{C_{n+2}C_n^3 - C_{n+1}^3 C_{n-1}}{C_1^3} && \text{for all } n > 1, \\
C_{2n} &:= \frac{C_{n+2}C_n C_{n-1}^2 - C_n C_{n-2} C_{n+1}^2}{C_2 C_1^2} && \text{for all } n > 2.
\end{aligned}
$$

Now ψ_E is simply defined as C, with parameters a, b, c, d given in terms of the coefficients of E, but the fact that C is an EDS is *not obvious*!

An infamous exercise

Exercise (The Arithmetic of Elliptic Curves, 3.34(a))

Prove that a sequence $W := \{W_n\}_{n\in\mathbb{Z}}$ *of elements of a field with* $W_1W_2W_3 \neq 0$ *is an EDS if and only if it satisfies the two conditions*

$$W_{2n+1}W_1^3 = W_{n+2}W_n^3 - W_{n+1}^3W_{n-1} \qquad \text{for all } n > 1,$$
$$W_{2n}W_2W_1^2 = W_{n+2}W_nW_{n-1}^2 - W_nW_{n-2}W_{n+1}^2 \qquad \text{for all } n > 2.$$

In the literature, *every* complete argument I could find only proves this for $W = \psi_E$ using complex analysis, but this is not covered until Chapter 6!

An interesting conversation in Math Stack Exchange (paraphrased):

- Question (2013): how can this be done without elliptic functions?
- Answer (2013): you can use the addition formulae and some algebra
- Comment (2020): has anyone actually done the algebraic approach?
- Reply (2020): I expect the answer is yes but I do not know who

Elliptic nets

It turns out that you cannot solve Exercise 3.34(a) with direct induction: the inductive hypothesis is *too weak* to establish the inductive step.

Instead, it turns out that a canonical EDS C also satisfies the stronger relation of an **elliptic net**, that for all $p, q, r, s \in \mathbb{Z}$,

$$\begin{aligned} \mathrm{EN}(p,q,r,s) \ : \ C_{p+q}C_{p-q}C_{r+s}C_{r-s} &= C_{p+r}C_{p-r}C_{q+s}C_{q-s} \\ &- C_{q+r}C_{q-r}C_{p+s}C_{p-s}. \end{aligned}$$

Elliptic nets were first introduced and studied by Katherine Stange (2008), which generalise elliptic sequences by setting $s = 0$.

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

Theorem (Xu, 2024)

A canonical EDS is an elliptic net, and hence an elliptic sequence.

I will now briefly describe his inductive argument on four variables.

Xu's argument

By $C_{-n} = -C_n$, it suffices to prove $\mathrm{EN}(p,q,r,s)$ by strong induction on p assuming that $p,q,r,s > 0$. Firstly,

$$\mathrm{EN}(p,q,1,0) = \mathrm{EN}(\tfrac{p+q+1}{2}, \tfrac{p+q-1}{2}, \tfrac{p-q+1}{2}, \tfrac{p-q-1}{2}).$$

If $p = q+1$, then $\mathrm{EN}(q+1,q,1,0)$ holds by definition of C_{2q+1}. Otherwise $p > q+1$, then inductive hypothesis applies since $\frac{p+q+1}{2} < p$. This gives $\mathrm{EN}(p,q,1,0)$ for all $p,q > 1$. Furthermore,

$$\begin{aligned}
\mathrm{EN}(p,q,r,0) &= C_r^2\cdot\mathrm{EN}(p,q,1,0) - C_q^2\cdot\mathrm{EN}(p,r,1,0) + C_p^2\cdot\mathrm{EN}(q,r,1,0),\\
\mathrm{EN}(p,q,r,1) &= C_{r+1}C_{r-1}\cdot\mathrm{EN}(p,q,1,0) - C_{q+1}C_{q-1}\cdot\mathrm{EN}(p,r,1,0) + C_{p+1}C_{p-1}\cdot\mathrm{EN}(q,r,1,0).
\end{aligned}$$

This gives $\mathrm{EN}(p,q,r,0)$ and $\mathrm{EN}(p,q,r,1)$ for all $p,q,r > 1$. Finally,

$$\begin{aligned}
\mathrm{EN}(p,q,r,s) = {} & C_q^2\cdot\mathrm{EN}(p,r,s,1) + C_{q+1}C_{q-1}\cdot\mathrm{EN}(p,r,s,0) + C_{q+r}C_{q-r}\cdot\mathrm{EN}(p,s,1,0)\\
& - C_r^2\cdot\mathrm{EN}(p,q,s,1) - C_{r+1}C_{r-1}\cdot\mathrm{EN}(p,q,s,0) - C_{q+s}C_{q-s}\cdot\mathrm{EN}(p,r,1,0)\\
& + C_s^2\cdot\mathrm{EN}(p,q,r,1) + C_{s+1}C_{s-1}\cdot\mathrm{EN}(p,q,r,0) + C_{r+s}C_{r-s}\cdot\mathrm{EN}(p,q,1,0)\\
& - 2C_p^2\cdot\mathrm{EN}(q,r,s,1) \quad .
\end{aligned}$$

This gives $\mathrm{EN}(p,q,r,s)$ for all $p,q,r,s > 1$.

Final remarks

Note that the complete argument also needs the case when p, q, r, s are all half-integers, so that $\mathrm{EN}(\frac{p+q+1}{2}, \frac{p+q-1}{2}, \frac{p-q+1}{2}, \frac{p-q-1}{2})$ is well-defined when p and q have the same parity, and this uses the definition of C_{2q}.

Xu's result also allows for the construction of an explicit **complement sequence** $C^c := \{C^c_{m,n}\}_{m,n\in\mathbb{Z}}$ such that for all $m, n \in \mathbb{Z}$,

$$C_m \cdot C^c_{m,n} = C_{mn},$$

which proves that C is a divisibility sequence, and hence an EDS.

Finally, the fact that ω_E is a sequence of *polynomials* turned out to be highly non-trivial! Xu showed this by establishing the invariant

$$\mathcal{I}_W(n) := \frac{W_{n-1}^2 W_{n+2} + W_{n-2} W_{n+1}^2 + W_2^2 W_n^3}{W_{n+1} W_n W_{n-1}}, \qquad n \in \mathbb{Z},$$

for any EDS W, which holds for C and in particular for ψ_E.