# Formal Proof of the Group Law for Edwards Elliptic Curves

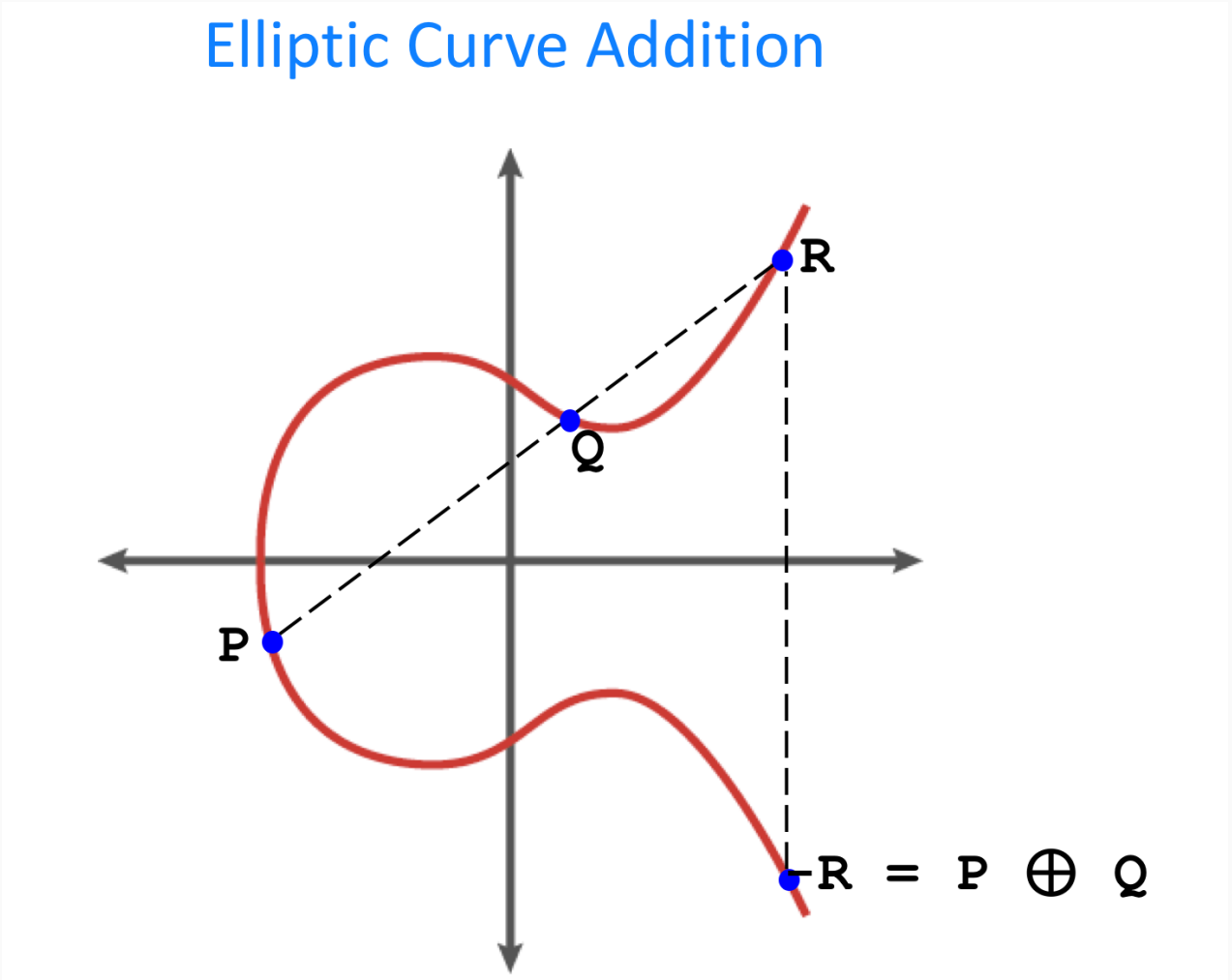
Thomas Hales and Rodrigo Raya

July 3, 2020

IJCAR 2020

# Motivation

# Weierstrass



# Easy to prove?

- Silvermann and Tate: Rational points on elliptic curves, 1992

  *Of course, there are an awful lot of special cases to consider, such as when one of the points is the negative of the other or two of the points coincide. But in a few days, you will be able to check associativity using these formulas. So we need say nothing more about the proof of the associative law!*

- Russinoff: A Computationally Surveyable Proof of the Group Properties of an Elliptic Curve (2017).

  *Expanding the resulting polynomial equation into monomials would involve some* $10^{25}$ *terms...*

Théry, Proving the group law of elliptic curves formally (2007):

> *To translate this 7 page long paper proof in a theorem prover was a real challenge. In fact, the proof relies on some non-trivial computations that the author advises to check using a computer algebra system such as CoCoA. The main difficulty has been to find an effective way to cope with these computations inside our proof system.*

# Affine Edwards curves

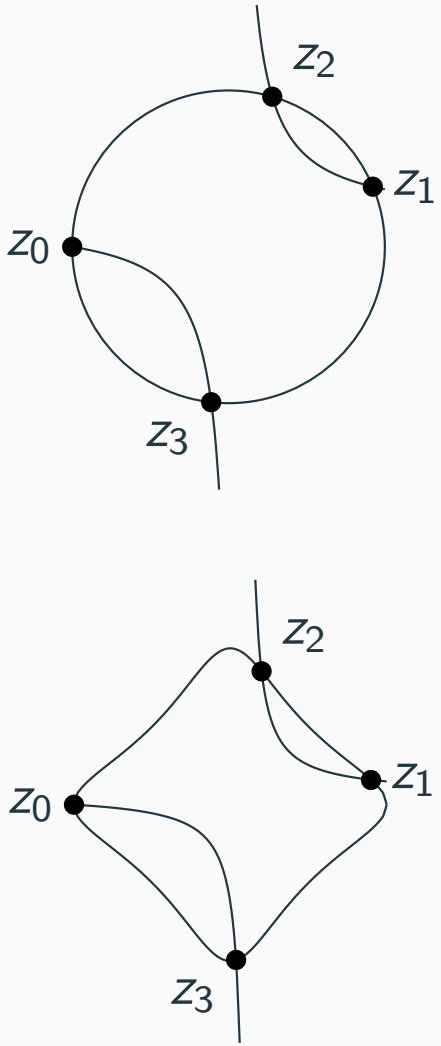
# Affine Edwards curves

- Let $k$ be an arbitrary field and $c, d, x, y \in k$ with $c, d$ fixed.

- An affine Edwards curve is given by the set of zeros of the polynomial:
$$e(x, y) = x^2 + cy^2 - 1 - dx^2y^2$$

- The following addition determines a group law on the curve:
$$(x_1, y_1) \oplus_0 (x_2, y_2) = \left( \frac{x_1x_2 - cy_1y_2}{1 - dx_1x_2y_1y_1}, \frac{x_1y_2 + y_1y_2}{1 + dx_1x_2y_1y_2} \right)$$

# Geometric interpretation




Source: Thomas Hales, The Group Law for Edwards Curves (2016)

# Affine statement

**Theorem (group law)**

*If $c$ is a square and $d \neq 0$ is not a square, then:*

$$C = \{(x, y) \in k^2 \mid e(x, y) = 0\}$$

*is an abelian group with binary operation $\oplus_0$.*

# The group law in Isabelle/HOL

- Associativity is the hardest to prove.
- $e_i = x_i^2 + c * y_i^2 - 1 - d * x_i^2 * y_i^2 = 0$
- Normalized associativity equation:
  $\text{gxpoly} = ((p_1 \oplus_0 p_2) \oplus_0 p_3 - p_1 \oplus_0 (p_2 \oplus_0 p_3))_1 * \Delta_x$

```
have "∃ r1 r2 r3. gxpoly = r1 * e1 + r2 * e2 + r3 * e3"
  unfolding gxpoly_def Delta_x_def
  apply(simp add: assms(1,2))
  apply(rewrite in "_ / ⌑" delta_minus_def[symmetric])+
  apply(simp add: divide_simps assms(9,11))
  apply(rewrite left_diff_distrib)
  apply(simp add: simp1gx simp2gx)
  unfolding delta_plus_def delta_minus_def
            e1_def e2_def e3_def e_def
  by algebra
```

- Like Mathematica but without explicitly computing $r_i$.

# Key tools

- The *rewrite* tactic: rewrites in subterms specified by a pattern.
- The *algebra* method: given $e_i(x),\ p_{ij}(x),\ a_i(x) \in R[x_1, \ldots, x_n]$, where $R$ is a commutative ring and $x = (x_1, \ldots, x_n)$, the method checks formulas:

$$\forall x.\ \bigwedge_{i=1}^{L} e_i(x) = 0 \rightarrow \exists y.\ \bigwedge_{i=1}^{M} \left( a_i(x) = \sum_{j=1}^{N} p_{ij}(x) y_j \right)$$

  The method is complete for formulas holding over all commutative rings with unit.
- In particular, ideal membership problems fit in this formula.

# Projective Edwards Curves

# Projective Edwards curves

- Bypass restriction: $d$ not a non-null square.
- Assume $c \neq 0$ and $c, d$ are squares.
- Set $t^2 = \frac{d}{c}$ and change variables $y \mapsto \frac{y}{c}$ to get:

$$e(x, y) = x^2 + y^2 - 1 - t^2 x^2 y^2$$

- Define a second addition $\oplus_1$:

$$(x_1, y_1) \oplus_1 (x_2, y_2) = \left( \frac{x_1 y_1 - x_2 y_2}{x_2 y_1 - x_1 y_2}, \frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2} \right)$$

# Projective Edwards curves

- Bypass restriction: $d$ not a non-null square.
- Assume $c \neq 0$ and $c, d$ are squares.
- Set $t^2 = \frac{d}{c}$ and change variables $y \mapsto \frac{y}{c}$ to get:

$$e(x, y) = x^2 + y^2 - 1 - t^2 x^2 y^2$$

- Define a second addition $\oplus_1$:

$$(x_1, y_1) \oplus_1 (x_2, y_2) = \left( \frac{x_1 y_1 - x_2 y_2}{x_2 y_1 - x_1 y_2}, \frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2} \right)$$

- Define $E_{\text{aff}}$ (points on curve) and $E^\circ$ (non-zero coordinates)
- Make two copies of $E_{aff}$. $(P, i)$ is representative of $P$ on i-th copy.
- For $P \in E^\circ$, identify $(P, i) \sim (\tau P, i + 1)$.
- Let $E = E_{aff}^2 / \sim$ be the quotient set with elements $[P, i]$.
- Define addition on $E$ as:

$$[P, i] \oplus [Q, j] = [P \oplus_I Q, i + j]$$

if $\delta_I(P, Q) \neq 0, I \in \mathbb{F}_2 = \{0, 1\}$.

# Projective addition in Isabelle/HOL

- Definition as usual:
  1. Basic operation: add $((x_1, y_1), i)$ and $((x_2, y_2), j)$.
  2. Apply basic operation to all pairs from two classes $c_1, c_2$.
  3. Apply the equivalence relation $\sim$.
  4. Extract the resulting class $c_1 \oplus c_2$.

# Projective addition in Isabelle/HOL

- Definition as usual:
  1. Basic operation: add $((x_1, y_1), i)$ and $((x_2, y_2), j)$.
  2. Apply basic operation to all pairs from two classes $c_1, c_2$.
  3. Apply the equivalence relation $\sim$.
  4. Extract the resulting class $c_1 \oplus c_2$.

- This uses Isabelle's ability to encode **partial functions**.
- The resulting definition is **easy to compute**. The equivalence classes are:

$$[(x, y), i] = \begin{cases} \{((x, y), i)\} & x = 0 \vee y = 0 \\ \{((x, y), i), (\tau(x, y), i + 1)\} & x \neq 0 \wedge y \neq 0 \end{cases}$$

  for $(x, y) \in E_{aff}$.
- But! Prove the **independence of the representative**.

# Using Isabelle's Gröbner basis

- **Dichotomy:** if $P, Q \in E_{aff}$ then
  - $P \in E^\circ$ and $Q = giP$ for some $g \in \tau\langle\rho\rangle$, or
  - $(P, Q) \in E_{aff,i}$ for some $i$.
- **Proof:** solve particular ideal membership problems.
- Formalization caught some **misinterpretation of computer algebra calculations**:

$$\exists r_1\ r_2\ r_3\ r_4.\ y_0^2 - x_1^2 = r_1 e(x_0, y_0) + r_2 e(x_1, y_1) + r_3\delta' + r_4\delta_-$$

  corrected to:

$$\exists r_1\ r_2\ r_3\ r_4.\ 2x_0y_0(y_0^2 - x_1^2) = r_1 e(x_0, y_0) + r_2 e(x_1, y_1) + r_3\delta' + r_4\delta_-$$

- In other case, some **strengthening of the hypothesis** needed: $\delta_+ = 0$ to $\delta_- \neq 0$
- We also produced a proof without Gröbner basis.

# When the assistant shows you the proof ($\delta$-relations)

First findings, used for the independence of class representative:

$$\begin{array}{rrcl}
 & \delta\ \tau P_1\ \tau P_2 \neq 0 & \Longrightarrow & \delta\ P_1\ P_2 \neq 0 \\
 & \delta'\ \tau P_1\ \tau P_2 \neq 0 & \Longrightarrow & \delta'\ P_1\ P_2 \neq 0 \\
\delta\ P_1\ P_2 \neq 0, & \delta\ P_1\ \tau P_2 \neq 0 & \Longrightarrow & \delta'\ P_1\ P_2 \neq 0 \\
\delta'\ P_1\ P_2 \neq 0, & \delta'\ P_1\ \tau P_2 \neq 0 & \Longrightarrow & \delta\ P_1\ P_2 \neq 0
\end{array}$$

Natural to ask about sums. Crucial to establish associativity:

$$\begin{array}{rrcl}
 & \delta'\ (P_1 \oplus_1 P_2)\ \tau\iota P_2 \neq 0 & \Longrightarrow & \delta\ (P_1 \oplus_1 P_2)\ \iota P_2 \neq 0 \\
\delta\ P_1\ P_2 \neq 0, & \delta\ (P_1 \oplus_0 P_2)\ \tau\iota P_2 \neq 0 & \Longrightarrow & \delta'(P_1 \oplus_0 P_2)\ \iota P_2 \neq 0 \\
\delta\ P_1\ P_2 \neq 0, & \delta'\ (P_0 \oplus_0 P_1)\ \tau\iota P_2 \neq 0 & \Longrightarrow & \delta\ (P_0 \oplus_0 P_1)\ \iota P_2 \neq 0 \\
\delta'\ P_1\ P_2 \neq 0, & \delta\ (P_0 \oplus_1 P_1)\ \tau\iota P_2 \neq 0 & \Longrightarrow & \delta'\ (P_0 \oplus_1 P_1)\ \iota P_2 \neq 0
\end{array}$$

# Use of $\delta$-relations

**Goal:** show $([P,0] \oplus [Q,0]) \oplus [iQ,0] = [P,0]$

- After applying dichotomy three times, we arrive to:
  $([P,0] \oplus [Q,0]) \oplus [\tau\iota Q,0] = [(P \oplus Q) \oplus \tau\iota Q,0]$
- We are stuck since $Q$ and $\tau iQ$ are not summable.
- **Sledgehammer** finds a contradiction using $\delta$-relations on $\oplus$ and hypothesis of second dichotomy.

# Final thoughts

- How to address the **maintainability** and **interoperability** of proof methods in proof-assistants (recall the *algebra* method) to make the next generation **usable for mathematicians**.

- Further elliptic curve formalizations: Schoof's algorithm, Hasse's theorem, elliptic curve primality testing, connection of elliptic curves and modular forms...

# Acknowledgements


- Manuel Eberl (TUM)
- Prof. Thomas Hales (University of Pittsburgh)
- Prof. Viktor Kunčak (EPFL)
- Prof. Tobias Nipkow (TUM)