



# Formal Proof of the Group Law for Edwards Elliptic Curves

Thomas Hales<sup>1</sup>(✉) and Rodrigo Raya<sup>2</sup>

<sup>1</sup> University of Pittsburgh, Pittsburgh, USA  
hales@pitt.edu

<sup>2</sup> Technical University of Munich, Munich, Germany

**Abstract.** This article gives an elementary computational proof of the group law for Edwards elliptic curves. The associative law is expressed as a polynomial identity over the integers that is directly checked by polynomial division. Unlike other proofs, no preliminaries such as intersection numbers, Bézout’s theorem, projective geometry, divisors, or Riemann Roch are required. The proof of the group law has been formalized in the Isabelle/HOL proof assistant.

## 1 Introduction

Elliptic curve cryptography is a cornerstone of mathematical cryptography. Many cryptographic algorithms (such as the Diffie-Hellman key exchange algorithm which inaugurated public key cryptography) were first developed in the context of the arithmetic of finite fields. The preponderance of finite-field cryptographic algorithms have now been translated to an elliptic curve counterpart. Elliptic curve algorithms encompass many of the fundamental cryptographic primitives: pseudo-random number generation, digital signatures, integer factorization algorithms, and public key exchange.

One advantage of elliptic curve cryptography over finite-field cryptography is that elliptic curve algorithms typically obtain the same level of security with smaller keys than finite-field algorithms. This often means more efficient algorithms.

Elliptic curve cryptography is the subject of major international cryptographic standards (such as NIST). Elliptic curve cryptography has been implemented in widely distributed software such as NaCl [BLS12]. Elliptic curve algorithms appear in nearly ubiquitous software applications such as web browsers and digital currencies.

The same elliptic curve can be presented in different ways by polynomial equations. The different presentations are known variously as the Weierstrass curve ( $y^2 = \text{cubic in } x$ ), Jacobi curve ( $y^2 = \text{quartic in } x$ ), and Edwards curve (discussed below).

The set of points on an elliptic curve forms an abelian group. Explicit formulas for addition are given in detail below. The Weierstrass curve is the most familiar presentation of an elliptic curve, but it suffers from the shortcoming

that the group law is not given by a uniform formula on all inputs. For example, special treatment must be given to the point at infinity and to point doubling:  $P \mapsto 2P$ . Exceptional cases are bad; they are the source of hazards such as side-channel attacks (timing attacks) by adversaries and implementation bugs [BJ02].

Edwards curves have been widely promoted for cryptographic algorithms because their addition law avoids exceptional cases and their hazards. Every elliptic curve (in characteristic different from 2) is isomorphic to an elliptic curve in Edwards form (possibly after passing to a quadratic extension). Thus, there is little loss of generality in considering elliptic curves in Edwards form. For most cryptographic applications, Edwards curves suffice.

The original contributions of this article are both mathematical and formal. Our proof that elliptic curve addition satisfies the axioms of an abelian group is new (but see the literature survey below for prior work). Our proofs were designed with formalization specifically in mind. To our knowledge, our proof of associativity in Sect. 3.3 is the most elementary proof that exists anywhere in the published literature (in a large mathematical literature on elliptic curves extending back to Euler’s work on elliptic integrals). Our proof avoids the usual machinery found in proofs of associativity (such as intersection numbers, Bézout’s theorem, projective geometry, divisors, or Riemann Roch). Our algebraic manipulations require little more than multivariate polynomial division with remainders, even avoiding Gröbner bases in most places. Based on this elementary proof, we give a formal proof in the Isabelle/HOL proof assistant that every Edwards elliptic curve (in characteristic other than 2) satisfies the axioms of an abelian group.<sup>1</sup>

It is natural to ask whether the proof of the associative law also avoids exceptional cases (encountered in Weierstrass curves) when expressed in terms of Edwards curves. Indeed, this article gives a two-line proof of the associative law for so-called *complete* Edwards curves that avoids case splits and all the usual machinery.

By bringing significant simplification to the fundamental proofs in cryptography, our paper opens the way for the formalization of elliptic curve cryptography in many proof assistants. Because of its extreme simplicity, we hope that our approach might be widely replicated and translated into many different proof assistants.

## 2 Published Literature

A number of our calculations are reworkings of calculations found in Edwards, Bernstein, Lange et al. [Edw07], [BBJ+08], [BL07]. A geometric interpretation of addition for Edwards elliptic curves appears in [ALNR11].

<sup>1</sup> Mathematica calculations are available at [https://github.com/thalesant/publications-of-thomas-hales/tree/master/cryptography/group\\_law\\_edwards](https://github.com/thalesant/publications-of-thomas-hales/tree/master/cryptography/group_law_edwards). The Isabelle/HOL formalization is available at <https://github.com/rjraya/Isabelle/blob/master/curves/Hales.thy>.

Working with the Weierstrass form of the curve, Friedl was the first to give a proof of the associative law of elliptic curves in a computer algebra system (in Cocoa using Gröbner bases) [Fri98], [Fri17]. He writes, “The verification of some identities took several hours on a modern computer; this proof could not have been carried out before the 1980s.” These identities were later formalized in Coq with runtime one minute and 20s [The07]. A non-computational Coq formalization based on the Picard group appears in [BS14]. By shifting to Edwards curves, we have eliminated case splits and significantly improved the speed of the computational proof.

An earlier unpublished note contains more detailed motivation, geometric interpretation, pedagogical notes, and expanded proofs [Hal16]. The earlier version does not include formalization in Isabelle/HOL. Our formalization uncovered and corrected some errors in the ideal membership problems in [Hal16] (reaffirming the pervasive conclusion that formalization catches errors that mathematicians miss).

Other formalizations of elliptic curve cryptography are found in Coq and ACL2 by different methods [Rus17]. After we posted our work to the arXiv, another formalization was given in Coq along our same idea [Erb17, EPG+17]. It goes further by including formalization of implementation of code, but it falls short of our work by not including the far more challenging and interesting case of projective curves.

We do not attempt to survey the various formalizations of cryptographic algorithms built on top of elliptic curves. Because of the critical importance of cryptography to the security industry, the formalization of cryptographic algorithms is rightfully a priority within the formalization community.

### 3 Group Axioms

This section gives an elementary proof of the group axioms for addition on Edwards curves (Theorem 1). We include proofs, because our approach is not previously published.

Our definition of Edwards curve is more inclusive than definitions stated elsewhere. Most writers prefer to restrict to curves of genus one and generally call a curve with  $c \neq 1$  a twisted Edwards curve. We have interchanged the  $x$  and  $y$  coordinates on the Edwards curve to make it consistent with the group law on the circle.

#### 3.1 Rings and Homomorphisms

In this section, we work algebraically over an arbitrary field  $k$ . We assume a basic background in abstract algebra at the level of a first course (rings, fields, homomorphisms, and kernels). We set things up in a way that all of the main identities to be proved are identities of polynomials with integer coefficients.

All rings are assumed to be commutative with identity  $1 \neq 0$ . If  $R$  is an integral domain and if  $\delta \in R$ , then we write  $R[\frac{1}{\delta}]$  for the localization of  $R$  with

respect to the multiplicative set  $S = \{1, \delta, \delta^2, \dots\}$ ; that is, the set of fractions with numerators in  $R$  and denominators in  $S$ . We will need the well-known fact that if  $\phi : R \rightarrow A$  is a ring homomorphism sending  $\delta$  to a unit in  $A$ , then  $\phi$  extends uniquely to a map  $R[\frac{1}{\delta}] \rightarrow A$  that maps a fraction  $r/\delta^i$  to  $\phi(r)\phi(\delta^i)^{-1}$ .

**Lemma 1 (kernel property).** *Suppose that an identity  $r = r_1e_1 + r_2e_2 + \dots + r_k e_k$  holds in a commutative ring  $R$ . If  $\phi : R \rightarrow A$  is a ring homomorphism such that  $\phi(e_i) = 0$  for all  $i$ , then  $\phi(r) = 0$ .*

*Proof.*  $\phi(r) = \sum_{i=1}^k \phi(r_i)\phi(e_i) = 0. \quad \square$

We use the following rings:  $R_0 := \mathbb{Z}[c, d]$  and  $R_n := R_0[x_1, y_1, \dots, x_n, y_n]$ . We introduce the polynomial for the Edwards curve. Let

$$e(x, y) = x^2 + cy^2 - 1 - dx^2y^2 \in R_0[x, y]. \tag{1}$$

We write  $e_i = e(x_i, y_i)$  for the image of the polynomial in  $R_j$ , for  $i \leq j$ , under  $x \mapsto x_i$  and  $y \mapsto y_i$ . Set  $\delta_x = \delta^-$  and  $\delta_y = \delta^+$ , where

$$\delta^\pm(x_1, y_1, x_2, y_2) = 1 \pm dx_1y_1x_2y_2 \quad \text{and}$$

$$\delta(x_1, y_1, x_2, y_2) = \delta_x\delta_y \in R_2.$$

We write  $\delta_{ij}$  for its image of  $\delta$  under  $(x_1, y_1, x_2, y_2) \mapsto (x_i, y_i, x_j, y_j)$ . So,  $\delta = \delta_{12}$ .

### 3.2 Inverse and Closure

We write  $z_i = (x_i, y_i)$ . We define a pair of rational functions that we denote using the symbol  $\oplus_0$ :

$$z_1 \oplus_0 z_2 = \left( \frac{x_1x_2 - cy_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \right) \in R_2[\frac{1}{\delta}] \times R_2[\frac{1}{\delta}]. \tag{2}$$

When specialized to  $c = 1$  and  $d = 0$ , the polynomial  $e(x, y) = x^2 + y^2 - 1$  reduces to a circle, and (2) reduces to the standard group law on a circle. Commutativity is a consequence of the subscript symmetry  $1 \leftrightarrow 2$  evident in the pair of rational functions:

$$z_1 \oplus_0 z_2 = z_2 \oplus_0 z_1.$$

If  $\phi : R_2[\frac{1}{\delta}] \rightarrow A$  is a ring homomorphism, we also write  $P_1 \oplus_0 P_2 \in A^2$  for the image of  $z_1 \oplus_0 z_2$ . We write  $e(P_i) \in A$  for the image of  $e_i = e(z_i)$  under  $\phi$ . We often mark the image  $\bar{r} = \phi(r)$  of an element with a bar accent.

Let  $\iota(z_i) = \iota(x_i, y_i) = (x_i, -y_i)$ . The involution  $z_i \rightarrow \iota(z_i)$  gives us an inverse with properties developed below.

There is an obvious identity element  $(1, 0)$ , expressed as follows. Under a homomorphism  $\phi : R_2[\frac{1}{\delta}] \rightarrow A$ , mapping  $z_1 \mapsto P$  and  $z_2 \mapsto (1, 0)$ , we have

$$P \oplus_0 (1, 0) = P. \tag{3}$$

**Lemma 2 (inverse).** *Let  $\phi : R_2[\frac{1}{\delta}] \rightarrow A$ , with  $z_1 \mapsto P$ ,  $z_2 \mapsto \iota(P)$ . If  $e(P) = 0$ , then  $P \oplus_0 \iota(P) = (1, 0)$ .*

*Proof.* Plug  $P = (a, b)$  and  $\iota P = (a, -b)$  into (2) and use  $e(P) = 0$ . □

**Lemma 3 (closure under addition).** *Let  $\phi : R_2[\frac{1}{\delta}] \rightarrow A$  with  $z_i \mapsto P_i$ . If  $e(P_1) = e(P_2) = 0$ , then*

$$e(P_1 \oplus_0 P_2) = 0.$$

*Proof.* This proof serves as a model for several proofs that are based on multivariate polynomial division. We write

$$e(z_1 \oplus_0 z_2) = \frac{r}{\delta^2},$$

for some polynomial  $r \in R_2$ . It is enough to show that  $\phi(r) = 0$ . Polynomial division gives

$$r = r_1 e_1 + r_2 e_2, \tag{4}$$

for some polynomials  $r_i \in R_2$ . Concretely, the polynomials  $r_i$  are obtained as the output of the one-line Mathematica command

$$\text{PolynomialReduce}[r, \{e_1, e_2\}, \{x_1, x_2, y_1, y_2\}].$$

The result now follows from the kernel property and (4);  $e(P_1) = e(P_2) = 0$  implies  $\phi(r) = 0$ , giving  $e(P_1 \oplus_0 P_2) = 0$ . □

Mathematica’s `PolynomialReduce` is an implementation of a naive multivariate division algorithm [CLO92]. In particular, our approach does not require the use of Gröbner bases until Sect. 5.3. We write

$$r \equiv r' \pmod{S},$$

where  $r - r'$  is a rational function and  $S$  is a set of polynomials, to indicate that the numerator of  $r - r'$  has zero remainder when reduced by polynomial division with respect to  $S$  using `PolynomialReduce`. We also require the denominator of  $r - r'$  to be invertible in the localized polynomial ring. The zero remainder will give  $\phi(r) = \phi(r')$  in each application. We extend the notation to  $n$ -tuples

$$(r_1, \dots, r_n) \equiv (r'_1, \dots, r'_n) \pmod{S},$$

to mean  $r_i \equiv r'_i \pmod{S}$  for each  $i$ . Using this approach, most of the proofs in this article almost write themselves.

### 3.3 Associativity

This next step (associativity) is generally considered the hardest part of the verification of the group law on curves. Our proof is two lines and requires little more than polynomial division. The polynomials  $\delta_x, \delta_y$  appear as denominators in the addition rule. The polynomial denominators  $\Delta_x, \Delta_y$  that appear when we

add twice are more involved. Specifically, let  $(x'_3, y'_3) = (x_1, y_1) \oplus_0 (x_2, y_2)$ , let  $(x'_1, y'_1) = (x_2, y_2) \oplus_0 (x_3, y_3)$ , and set

$$\Delta_x = \delta_x(x'_3, y'_3, x_3, y_3)\delta_x(x_1, y_1, x'_1, y'_1)\delta_{12}\delta_{23} \in R_3.$$

Define  $\Delta_y$  analogously.

**Lemma 4 (generic associativity).** *Let  $\phi : R_3[\frac{1}{\Delta_x\Delta_y}] \rightarrow A$  be a homomorphism with  $z_i \mapsto P_i$ . If  $e(P_1) = e(P_2) = e(P_3) = 0$ , then*

$$(P_1 \oplus_0 P_2) \oplus_0 P_3 = P_1 \oplus_0 (P_2 \oplus_0 P_3).$$

*Proof.* By polynomial division in the ring  $R_3[\frac{1}{\Delta_x\Delta_y}]$

$$((x_1, y_1) \oplus_0 (x_2, y_2)) \oplus_0 (x_3, y_3) \equiv (x_1, y_1) \oplus_0 ((x_2, y_2) \oplus_0 (x_3, y_3)) \pmod{\{e_1, e_2, e_3\}}. \quad \square$$

### 3.4 Group Law for Affine Curves

**Lemma 5 (affine closure).** *Let  $\phi : R_2 \rightarrow k$  be a homomorphism into a field  $k$ . If  $\phi(\delta) = e(P_1) = e(P_2) = 0$ , then either  $\bar{d}$  or  $\bar{c}\bar{d}$  is a nonzero square in  $k$ .*

The lemma is sometimes called completeness, in conflict with the usual definition of *complete* varieties in algebraic geometry. To avoid possible confusion, we avoid this terminology. We use the lemma in contrapositive form to give conditions on  $\bar{d}$  and  $\bar{c}\bar{d}$  that imply  $\phi(\delta) \neq 0$ .

*Proof.* Let  $r = (1 - cdy_1^2y_2^2)(1 - dy_1^2x_2^2)$ . We have

$$r = d^2y_1^2y_2^2x_2^2e_1 + (1 - dy_1^2)\delta - dy_1^2e_2. \tag{5}$$

This forces  $\phi(r) = 0$ , which by the form of  $r$  implies that  $\bar{c}\bar{d}$  or  $\bar{d}$  is a nonzero square. □

We are ready to state and prove one of the main results of this article. This group law is expressed generally enough to include the group law on the circle and ellipse as a special case  $\bar{d} = 0$ .

**Theorem 1 (group law).** *Let  $k$  be a field, let  $\bar{c} \in k$  be a square, and let  $\bar{d} \notin k^{\times 2}$ . Then*

$$C = \{P \in k^2 \mid e(P) = 0\}$$

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

*Proof.* This follows directly from the earlier results. For example, to check associativity of  $P_1 \oplus_0 P_2 \oplus_0 P_3$ , where  $P_i \in C$ , we define a homomorphism  $\phi : R_3 \rightarrow k$  sending  $z_i \mapsto P_i$  and  $(c, d) \mapsto (\bar{c}, \bar{d})$ . By a repeated use of the affine closure lemma,  $\phi(\Delta_y\Delta_x)$  is nonzero and invertible in the field  $k$ . The universal property of localization extends  $\phi$  to a homomorphism  $\phi : R_3[\frac{1}{\Delta_y\Delta_x}] \rightarrow k$ . By the associativity lemma applied to  $\phi$ , we obtain the associativity for these three (arbitrary) elements of  $C$ . The other group axioms follow similarly from the lemmas on closure, inverse, and affine closure. □

The Mathematica calculations in this section are fast. For example, the associativity certificate takes about 0.12 s to compute on a 2.13 GHz processor.

## 4 Formalization in Isabelle/HOL

In this section, we describe the proof implementation in Isabelle/HOL. We have formalized the two main theorems (Theorem 1 and Theorem 2). Formalization uses two different locales: one for the affine and one for the projective case. (The projective case will be discussed in Sect. 5.)

Let  $k$  be the underlying curve field.  $k$  is introduced as the type class *field* with the assumption that  $2 \neq 0$  (characteristic different from 2). This is not included in the simplification set, but used when needed during the proof. The formalized theorem is slightly less general than the informal statement, because of this restriction.

### 4.1 Affine Edwards Curves

The formal proof fixes the curve parameters  $c, d \in k$  (dropping the bar accents from notation). The group addition  $\oplus_0$  (of Eq. 2) can be written as in Fig. 1. In Isabelle’s division ring theory, the result of division by zero is defined as zero. This has no impact on validity of final results, but gives cleaner simplifications in some proofs.

$$\begin{aligned} \text{add} &:: 'a \times 'a \Rightarrow 'a \times 'a \Rightarrow 'a \times 'a \\ \text{add } (x_1, y_1) (x_2, y_2) &= ((x_1 * x_2 - c * y_1 * y_2) \text{ div } (1 - d * x_1 * y_1 * x_2 * y_2), \\ &\quad (x_1 * y_2 + y_1 * x_2) \text{ div } (1 + d * x_1 * y_1 * x_2 * y_2)) \end{aligned}$$

**Fig. 1.** Definition of  $\oplus_0$  in Isabelle/HOL

Most of the proofs in this section are straight-forward. The only difficulty was to combine the Mathematica certificates of computation, into a single process in Isabelle.

In Fig. 2, we show an excerpt of the proof of associativity. We use the following abbreviations:

$$e_i = x_i^2 + c * y_i^2 - 1 - d * x_i^2 * y_i^2$$

where  $e_i = 0$ , since the involved points lie on the curve and

$$\text{gxpoly} = ((p_1 \oplus_0 p_2) \oplus_0 p_3 - p_1 \oplus_0 (p_2 \oplus_0 p_3))_1 * \Delta_x$$

which stands for a normalized version of the associativity law after clearing denominators. We say that points are *summable*, if the rational functions defining their sum have nonzero denominators. Since the points  $p_i$  are assumed to be summable,  $\Delta_x \neq 0$ . As a consequence, the property stated in Fig. 2 immediately implies that associativity holds in the first component of the addition.

Briefly, the proof unfolds the relevant definitions and then normalizes to clear denominators. The remaining terms of  $\Delta_x$  are then distributed over addends. The unfolding and normalization of addends is repeated in the lemmas *simp1gx* and

```

have "∃ r1 r2 r3. gxpoly = r1 * e1 + r2 * e2 + r3 * e3"
  unfolding gxpoly_def g_x_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

```

**Fig. 2.** An excerpt of the proof of associativity

*simp2gx*. Finally, the resulting polynomial identity is proved using the *algebra* method. Note that no computation was required from an external tool.

The *rewrite* tactic, which can modify a goal with various rewrite rules in various locations (specified with a pattern), is used to normalized terms [NT14]. Rewriting in the denominators is sufficient for our needs.

For proving the resulting polynomial expression, the *algebra* proof method is used [CW07, Cha08, Wen19]. Given  $e_i(x)$ ,  $p_{ij}(x)$ ,  $a_i(x) \in R[x_1, \dots, x_n]$ , where  $R$  is a commutative ring and  $x = (x_1, \dots, x_n)$ , the method verifies 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 such formulas that hold over all commutative rings with unit [Har07].

## 5 Group Law for Projective Edwards Curves

By proving the group laws for a large class of elliptic curves, Theorem 1 is sufficiently general for many applications to cryptography. Nevertheless, to achieve full generality, we push forward.

This section shows how to remove the restriction  $\bar{d} \notin k^{\times 2}$  that appears in the group law in the previous section. By removing this restriction, we obtain a new proof of the group law for all elliptic curves in characteristics different from 2. Unfortunately, in this section, some case-by-case arguments are needed, but no hard cases are hidden from the reader. The level of exposition here is less elementary than in the previous section. Again, we include proofs, because our approach is designed with formalization in mind and has not been previously published.

The basic idea of our construction is that the projective curve  $E$  is obtained by gluing two affine curves  $E_{\text{aff}}$  together. The associative property for  $E$  is a consequence of the associative property on affine pieces  $E_{\text{aff}}$ , which can be expressed as polynomial identities.

**5.1 Definitions**

In this section, we assume that  $c \neq 0$  and that  $c$  and  $d$  are both squares. Let  $t^2 = d/c$ . By a change of variable  $y \mapsto y/\sqrt{c}$ , the Edwards curve takes the form

$$e(x, y) = x^2 + y^2 - 1 - t^2 x^2 y^2. \tag{6}$$

We assume  $t^2 \neq 1$ . Note if  $t^2 = 1$ , then the curve degenerates to a product of intersecting lines, which cannot be a group. We also assume that  $t \neq 0$ , which only excludes the circle, which has already been fully treated. Shifting notation for this new setting, let

$$R_0 = \mathbb{Z}[t, \frac{1}{t^2 - 1}, \frac{1}{t}], \quad R_n = R_0[x_1, y_1, \dots, x_n, y_n].$$

As before, we write  $e_i = e(z_i)$ ,  $z_i = (x_i, y_i)$ , and  $e(P_i) = \phi(e_i)$  when a homomorphism  $\phi$  is given.

Define rotation by  $\rho(x, y) = (-y, x)$  and inversion  $\tau$  by

$$\tau(x, y) = (1/(tx), 1/(ty)).$$

Let  $G$  be the abelian group of order eight generated by  $\rho$  and  $\tau$ .

**5.2 Extended Addition**

We extend the binary operation  $\oplus_0$  using the automorphism  $\tau$ . We also write  $\delta_0$  for  $\delta$ ,  $\nu_0$  for  $\nu$  and so forth.

Set

$$z_1 \oplus_1 z_2 := \tau((\tau z_1) \oplus_0 z_2) = \left( \frac{x_1 y_1 - x_2 y_2}{x_2 y_1 - x_1 y_2}, \frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2} \right) = \left( \frac{\nu_{1x}}{\delta_{1x}}, \frac{\nu_{1y}}{\delta_{1y}} \right) \tag{7}$$

in  $R_2[\frac{1}{\delta_1}]^2$  where  $\delta_1 = \delta_{1x} \delta_{1y}$ .

We have the following easy identities of rational functions that are proved by simplification of rational functions:

$$\textit{inversion invariance:} \quad \tau(z_1) \oplus_i z_2 = z_1 \oplus_i \tau z_2; \tag{8}$$

$$\begin{aligned} \textit{rotation invariance:} \quad & \rho(z_1) \oplus_i z_2 = \rho(z_1 \oplus_i z_2); \\ & \delta_i(z_1, \rho z_2) = \pm \delta_i(z_1, z_2); \end{aligned} \tag{9}$$

$$\begin{aligned} \textit{inverses for } \sigma = \tau, \rho: \quad & \iota \sigma(z_1) = \sigma^{-1} \iota(z_1); \\ & \iota(z_1 \oplus_i z_2) = (\iota z_1) \oplus_i (\iota z_2). \end{aligned} \tag{10}$$

$$\begin{aligned} \textit{coherence:} \quad & z_1 \oplus_0 z_2 \equiv z_1 \oplus_1 z_2 \pmod{\{e_1, e_2\}}; \\ & e(z_1 \oplus_1 z_2) \equiv 0 \pmod{\{e_1, e_2\}}. \end{aligned} \tag{11}$$

The first identity of (11) inverts  $\delta_0 \delta_1$ , and the second inverts  $\delta_1$ . Proofs of (11) use polynomial division.

### 5.3 Projective Curve and Dichotomy

Let  $k$  be a field of characteristic different from two. We let  $E_{\text{aff}}$  be the set of zeros of Eq. (6) in  $k^2$ . Let  $E^\circ \subset E_{\text{aff}}$  be the subset of  $E_{\text{aff}}$  with nonzero coordinates  $x, y \neq 0$ .

We construct the projective Edwards curve  $E$  by taking two copies of  $E_{\text{aff}}$ , glued along  $E^\circ$  by isomorphism  $\tau$ . We write  $[P, i] \in E$ , with  $i \in \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ , for the image of  $P \in E_{\text{aff}}$  in  $E$  using the  $i$ th copy of  $E_{\text{aff}}$ . The gluing condition gives for  $P \in E^\circ$ :

$$[P, i] = [\tau P, i + 1]. \tag{12}$$

The group  $G$  acts on the set  $E$ , specified on generators  $\rho, \tau$  by  $\rho[P, i] = [\rho(P), i]$  and  $\tau[P, i] = [P, i + 1]$ .

We define addition on  $E$  by

$$[P, i] \oplus [Q, j] = [P \oplus_\ell Q, i + j], \quad \text{if } \delta_\ell(P, Q) \neq 0, \quad \ell \in \mathbb{F}_2 \tag{13}$$

We will show that the addition is well-defined, is defined for all pairs of points in  $E$ , and that it gives a group law with identity element  $[(1, 0), 0]$ . The inverse is  $[P, i] \mapsto [\iota P, i]$ , which is well-defined by the inverse rules (10).

**Lemma 6.**  *$G$  acts without fixed point on  $E^\circ$ . That is,  $gP = P$  implies that  $g = 1_G \in G$ .*

*Proof.* Write  $P = (x, y)$ . If  $g = \rho^k \neq 1_G$ , then  $gP = P$  implies that  $2x = 2y = 0$  and  $x = y = 0$  (if the characteristic is not two), which is not a point on the curve. If  $g = \tau\rho^k$ , then the fixed-point condition  $gP = P$  leads to  $2txy = 0$  or  $tx^2 = ty^2 = \pm 1$ . Then  $e(x, y) = 2(\pm 1 - t)/t \neq 0$ , and again  $P$  is not a point on the curve. □

The domain of  $\oplus_i$  is

$$E_{\text{aff},i} := \{(P, Q) \in E_{\text{aff}}^2 \mid \delta_i(P, Q) \neq 0\}.$$

Whenever we write  $P \oplus_i Q$ , it is always accompanied by the implicit assertion of summability; that is,  $(P, Q) \in E_{\text{aff},i}$ .

There is a group isomorphism  $\langle \rho \rangle \rightarrow E_{\text{aff}} \setminus E^\circ$  given by

$$g \mapsto g(1, 0) \in \{\pm(1, 0), \pm(0, 1)\} = E_{\text{aff}} \setminus E^\circ.$$

**Lemma 7 (dichotomy).** *Let  $P, Q \in E_{\text{aff}}$ . Then either  $P \in E^\circ$  and  $Q = g\iota P$  for some  $g \in \tau\langle \rho \rangle$ , or  $(P, Q) \in E_{\text{aff},i}$  for some  $i$ . Moreover, assume that  $P \oplus_i Q = (1, 0)$  for some  $i$ , then  $Q = \iota P$ .*

*Proof.* We start with the first claim. We analyze the denominators in the formulas for  $\oplus_i$ . We have  $(P, Q) \in E_{\text{aff},0}$  for all  $P$  or  $Q \in E_{\text{aff}} \setminus E^\circ$ . That case completed, we may assume that  $P, Q \in E^\circ$ . Assuming

$$\delta_0(P, Q) = \delta_{0x}(P, Q)\delta_{0y}(P, Q) = 0, \quad \text{and} \quad \delta_1(P, Q) = \delta_{1x}(P, Q)\delta_{1y}(P, Q) = 0,$$

we show that  $Q = g\iota P$  for some  $g \in \tau\langle\rho\rangle$ . Replacing  $Q$  by  $\rho Q$  if needed, which exchanges  $\delta_{0x} \leftrightarrow \delta_{0y}$ , we may assume that  $\delta_{0x}(P, Q) = 0$ . Set  $\tau Q = Q_0 = (a_0, b_0)$  and  $P = (a_1, b_1)$ .

We claim that

$$(a_0, b_0) \in \{\pm(b_1, a_1)\} \subset \langle\rho\rangle\iota P. \tag{14}$$

We describe the main polynomial identity that must be verified. Write  $\delta', \delta_+, \delta_-$  for  $x_0y_0\delta_{0x}, tx_0y_0\delta_{1x}$ , and  $tx_0y_0\delta_{1y}$  respectively, each evaluated at  $(P, \tau(Q_0)) = (x_1, y_1, 1/(tx_0), 1/(ty_0))$ . The nonzero factors  $x_0y_0$  and  $tx_0y_0$  have been included to clear denominators, leaving us with polynomials.

We have two cases  $\pm$ , according to  $\delta_{\pm} = 0$ . In each case, let

$$S_{\pm} = \text{Gröbner basis of } \{e_1, e_2, \delta', \delta_{\pm}\}.$$

We have

$$\begin{aligned} (x_0^2 - y_1^2, y_0^2 - x_1^2, x_0y_0 - x_1y_1) &\equiv (0, 0, 0) \pmod{S_+} \\ (2x_0y_0(x_0^2 - y_1^2), 2(1 - t^2)x_0y_0(y_0^2 - x_1^2), x_0y_0 - x_1y_1) &\equiv (0, 0, 0) \pmod{S_-}. \end{aligned} \tag{15}$$

In fact,  $\delta' = x_0y_0 - x_1y_1$ , so that the ideal membership for this polynomial is immediate. The factors 2,  $1 - t^2$ , and  $x_0y_0$  are nonzero and can be removed from the left-hand side. These equations then immediately yield  $(a_0, b_0) = \pm(b_1, a_1)$ . This gives the needed identity:  $\tau Q = Q_0 = (a_0, b_0) = g\iota P$ , for some  $g \in \langle\rho\rangle$ . Then  $Q = \tau g\iota P$ .

The second statement of the lemma has a similar proof. Polynomial division gives for  $i \in \mathbb{F}_2$ :

$$(x_1 - x_2, y_1 + y_2) \equiv (0, 0) \pmod{\text{Gröbner}\{e_1, e_2, q_x\delta_{ix} - 1, q_y\delta_{iy} - 1, \nu_{iy}, \nu_{ix} - \delta_{ix}\}}.$$

In fact, both  $x_1 - x_2$  and  $y_1 + y_2$  (which specify the condition  $Q = \iota P$ ) are already members of the Gröbner basis. The fresh variables  $q_x, q_y$  force the denominators  $\delta_{ix}$  and  $\delta_{iy}$  to be invertible. Here the equations  $\nu_{iy} = \nu_{ix} - \delta_{ix} = 0$  specify the sum  $(1, 0) = (\nu_{ix}/\delta_{ix}, \nu_{iy}/\delta_{iy})$  of  $Q$  and  $P$ . □

**Lemma 8 (covering).** *The rule (13) defining  $\oplus$  assigns at least one value for every pair of points in  $E$ .*

*Proof.* If  $Q = \tau\rho^k\iota P$ , then  $\tau Q$  does not have the form  $\tau\rho^k\iota P$  because the action of  $G$  is fixed-point free. By dichotomy,

$$[P, i] \oplus [Q, j] = [P \oplus_{\ell} \tau Q, i + j + 1] \tag{16}$$

works for some  $\ell$ . Otherwise, by dichotomy  $P \oplus_{\ell} Q$  is defined for some  $\ell$ . □

**Lemma 9 (well-defined).** *Addition  $\oplus$  given by (13) on  $E$  is well-defined.*

*Proof.* The right-hand side of (13) is well-defined by coherence (11), provided we show well-definedness across gluings (12). We use dichotomy. If  $Q = \tau\rho^k\iota P$ , then by an easy simplification of polynomials,

$$\delta_0(z, \tau\rho^k\iota z) = \delta_1(z, \tau\rho^k\iota z) = 0.$$

so that only one rule (16) for  $\oplus$  applies (up to coherence (11) and inversion (8)), making it necessarily well-defined. Otherwise, coherence (11), inversion (8), and (7) give when  $[Q, j] = [\tau Q, j + 1]$ :

$$[P \oplus_k \tau Q, i + j + 1] = [\tau(P \oplus_k \tau Q), i + j] = [P \oplus_{k+1} Q, i + j] = [P \oplus_\ell Q, i + j].$$

□

### 5.4 Group Law

**Theorem 2.** *E is an abelian group.*

*Proof.* We have already shown the existence of an identity and inverse.

We prove associativity. Both sides of the associativity identity are clearly invariant under shifts  $[P, i] \mapsto [P, i + j]$  of the indices. Thus, it is enough to show

$$[P, 0] \oplus ([Q, 0] \oplus [R, 0]) = ([P, 0] \oplus [Q, 0]) \oplus [R, 0].$$

By polynomial division, we have the following associativity identities

$$(z_1 \oplus_k z_2) \oplus_\ell z_3 \equiv z_1 \oplus_i (z_2 \oplus_j z_3) \pmod{\{e_1, e_2, e_3\}} \tag{17}$$

in the appropriate localizations, for  $i, j, k, \ell \in \mathbb{F}_2$ .

Note that  $(g[P_1, i] \oplus [P_2, j]) = g([P_1, i] \oplus [P_2, j])$  for  $g \in G$ , as can easily be checked on generators  $g = \tau, \rho$  of  $G$ , using dichotomy, (13), and (9). We use this to cancel group elements  $g$  from both sides of equations without further comment.

We claim that

$$([P, 0] \oplus [Q, 0]) \oplus [\iota Q, 0] = [P, 0]. \tag{18}$$

The special case  $Q = \tau\rho^k\iota(P)$  is easy. We reduce the claim to the case where  $P \oplus_\ell Q \neq \tau\rho^k Q$ , by applying  $\tau$  to both sides of (18) and replacing  $P$  with  $\tau P$  if necessary. Then by dichotomy, the left-hand side simplifies by affine associativity 17 to give the claim.

Finally, we have general associativity by repeated use of dichotomy, which reduces in each case to (17) or (18). □

### 5.5 Formalization in Isabelle/HOL of Projective Edwards Curves

Following the change of variables performed in Sect. 5.1, it is assumed that  $c = 1$  and  $d = t^2$  where  $t \neq -1, 0, 1$ . The resulting formalization is more challenging. In the following, some key insights are emphasized.

**Gröbner Basis.** The proof of Lemma 7 (dichotomy) requires solving particular instances of the ideal membership problem. Formalization caught and corrected some ideal membership errors in [Hal16], which resulted from an incorrect interpretation of computer algebra calculations. For instance, a goal

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

(derived from [Hal16]) had to be corrected to

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

to prove (15). In another subcase, it was necessary to strengthen the hypothesis  $\delta_+ = 0$  to  $\delta_- \neq 0$ . Eventually, after some reworking, *algebra* solved the required ideal membership problems.

**Definition of the Group Addition.** We defined the addition in three stages. This is convenient for some lemmas like covering (Lemma 8). First, we define the addition on projective points (Fig. 3). Then, we add two classes of points by applying the basic addition to any pair of points coming from each class. Finally, we apply the gluing relation and obtain as a result a set of classes with a unique element, which is then defined as the resulting class (Fig. 4).

The definitions use Isabelle’s ability to encode partial functions. However, it is possible to obtain an equivalent definition more suitable for execution. In

```

type_synonym ('b) ppoint = (('b × 'b) × bit)

p_add :: 'a ppoint ⇒ 'a ppoint ⇒ 'a ppoint where
  p_add ((x1, y1), l) ((x2, y2), j) = (add (x1, y1) (x2, y2), l+j)
  if delta x1 y1 x2 y2 ≠ 0 ∧ (x1, y1) ∈ e'_aff ∧ (x2, y2) ∈ e'_aff
| p_add ((x1, y1), l) ((x2, y2), j) = (ext_add (x1, y1) (x2, y2), l+j)
  if delta' x1 y1 x2 y2 ≠ 0 ∧ (x1, y1) ∈ e'_aff ∧ (x2, y2) ∈ e'_aff

```

Fig. 3. Definition of  $\oplus$  on points

```

type_synonym ('b) pclass = ('b) ppoint set

proj_add_class :: ('a) pclass ⇒ ('a) pclass ⇒ ('a) pclass set
  proj_add_class c1 c2 =
    (p_add ' {((x1, y1), i), ((x2, y2), j)}.
      ((x1, y1), i), ((x2, y2), j)) ∈ c1 × c2 ∧
      ((x1, y1), (x2, y2)) ∈ e'_aff_0 ∪ e'_aff_1} // gluing
  if c1 ∈ e_proj and c2 ∈ e_proj

proj_addition c1 c2 = the_elem (proj_add_class c1 c2)

```

Fig. 4. Definition of  $\oplus$  on classes

particular, it is easy to compute the gluing relation (see lemmas `e_proj_elim_1`, `e_proj_elim_2` and `e_proj_aff` in the formalization scripts).

Finally, since projective addition works with classes, we had to show that its definition does not depend on the representative used.

**Table 1.** List of  $\delta$  relations

|  |  |  |
|--|--|--|
| $\delta \tau P_1 \tau P_2 \neq 0$                  | $\implies$   | $\delta P_1 P_2 \neq 0$                                |
| $\delta' \tau P_1 \tau P_2 \neq 0$                 | $\implies$   | $\delta' P_1 P_2 \neq 0$                               |
| $\delta P_1 P_2 \neq 0,$                           | $\delta P_1 \tau P_2 \neq 0$                       | $\implies \delta' P_1 P_2 \neq 0$                      |
| $\delta' P_1 P_2 \neq 0,$                          | $\delta' P_1 \tau P_2 \neq 0$                      | $\implies \delta P_1 P_2 \neq 0$                       |
| $\delta' (P_1 \oplus_1 P_2) \tau \iota P_2 \neq 0$ | $\implies$   | $\delta (P_1 \oplus_1 P_2) \iota P_2 \neq 0$           |
| $\delta P_1 P_2 \neq 0,$                           | $\delta (P_1 \oplus_0 P_2) \tau \iota P_2 \neq 0$  | $\implies \delta' (P_1 \oplus_0 P_2) \iota P_2 \neq 0$ |
| $\delta P_1 P_2 \neq 0,$                           | $\delta' (P_0 \oplus_0 P_1) \tau \iota P_2 \neq 0$ | $\implies \delta (P_0 \oplus_0 P_1) \iota P_2 \neq 0$  |
| $\delta' P_1 P_2 \neq 0,$                          | $\delta (P_0 \oplus_1 P_1) \tau \iota P_2 \neq 0$  | $\implies \delta' (P_0 \oplus_1 P_1) \iota P_2 \neq 0$ |

**Proof of Associativity.** During formalization, we found several relations between  $\delta$  expressions (see Table 1). While they were proven in order to show associativity, the upper group can rather be used to establish the independence of class representative and the lower group is crucial to establish the associativity law.

In particular, the lower part of the table is fundamental to the formal proof of Eq. (18). In more detail, the formal proof development showed that it was necessary to perform a dichotomy (Lemma 7) three times. The first dichotomy is performed on  $P, Q$ . The non-summable case was easy. Therefore, we set  $R = P \oplus Q$ . On each of the resulting branches, a dichotomy on  $R, \iota Q$  is performed. This time the summable cases were easy, but the non-summable case required a third dichotomy on  $R, \tau \iota Q$ . The non-summable case was solved using the no-fixed-point theorem but for the summable subcases the following expression is obtained:

$$([P, 0] \oplus [Q, 0]) \oplus [\tau \iota Q, 0] = [(P \oplus Q) \oplus \tau \iota Q, 0]$$

Here we cannot invoke associativity because  $Q, \tau \iota Q$  are non-summable (lemma `not_add_self`). Instead, we use the equations from the lower part of the table and the hypothesis of the second dichotomy to get a contradiction.

## 6 Conclusion

We have shown that Isabelle can encompass the process of defining, computing and certifying intensive algebraic calculations. The encoding in a proof-assistant allows a better comprehension of the methods used and helps to clarify its structure.

## References

- [ALNR11] Arene, C., Lange, T., Naehrig, M., Ritzenthaler, C.: Faster computation of the Tate pairing. *J. Number Theory* **131**(5), 842–857 (2011)
- [BBJ+08] Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) *AFRICACRYPT 2008*. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008). [https://doi.org/10.1007/978-3-540-68164-9\\_26](https://doi.org/10.1007/978-3-540-68164-9_26)
- [BJ02] Brier, É., Joye, M.: Weierstraß elliptic curves and side-channel attacks. In: Naccache, D., Paillier, P. (eds.) *PKC 2002*. LNCS, vol. 2274, pp. 335–345. Springer, Heidelberg (2002). [https://doi.org/10.1007/3-540-45664-3\\_24](https://doi.org/10.1007/3-540-45664-3_24)
- [BL07] Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) *ASIACRYPT 2007*. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-76900-2\\_3](https://doi.org/10.1007/978-3-540-76900-2_3)
- [BLS12] Bernstein, D.J., Lange, T., Schwabe, P.: The security impact of a new cryptographic library. In: Hevia, A., Neven, G. (eds.) *LATINCRYPT 2012*. LNCS, vol. 7533, pp. 159–176. Springer, Heidelberg (2012). [https://doi.org/10.1007/978-3-642-33481-8\\_9](https://doi.org/10.1007/978-3-642-33481-8_9)
- [BS14] Bartzia, E.-I., Strub, P.-Y.: A formal library for elliptic curves in the Coq proof assistant. In: Klein, G., Gamboa, R. (eds.) *ITP 2014*. LNCS, vol. 8558, pp. 77–92. Springer, Cham (2014). [https://doi.org/10.1007/978-3-319-08970-6\\_6](https://doi.org/10.1007/978-3-319-08970-6_6)
- [Cha08] Chaieb, A.: Automated methods for formal proofs in simple arithmetics and algebra. Ph.D. thesis, Technische Universität München (2008)
- [CLO92] Cox, D., Little, J., O’Shea, D.: *Ideals, Varieties, and Algorithms*, vol. 3. Springer, New York (1992). <https://doi.org/10.1007/978-1-4757-2181-2>
- [CW07] Chaieb, A., Wenzel, M.: Context aware calculation and deduction. In: Kauers, M., Kerber, M., Miner, R., Windsteiger, W. (eds.) *Calculemus/MKM -2007*. LNCS (LNAI), vol. 4573, pp. 27–39. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-73086-6\\_3](https://doi.org/10.1007/978-3-540-73086-6_3)
- [Edw07] Edwards, H.: A normal form for elliptic curves. *Bull. Am. Math. Soc.* **44**(3), 393–422 (2007)
- [EPG+17] Erbsen, A., Philipoom, J., Gross, J., Sloan, R., Chlipala, A.: Systematic generation of fast elliptic curve cryptography implementations. Technical report, MIT, Cambridge, MA, USA (2017)
- [Erb17] Erbsen, A.: Crafting certified elliptic curve cryptography implementations in Coq. Ph.D. thesis, Massachusetts Institute of Technology (2017)
- [Fri98] Friedl, S.: An elementary proof of the group law for elliptic curves. *The Group Law on Elliptic Curves* (1998)
- [Fri17] Friedl, S.: An elementary proof of the group law for elliptic curves. *Groups Complex. Cryptol.* **9**(2), 117–123 (2017)
- [Hal16] Hales, T.: The group law for Edwards curves. arXiv preprint [arXiv:1610.05278](https://arxiv.org/abs/1610.05278) (2016)
- [Har07] Harrison, J.: Automating elementary number-theoretic proofs using Gröbner bases. In: Pfenning, F. (ed.) *CADE 2007*. LNCS (LNAI), vol. 4603, pp. 51–66. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-73595-3\\_5](https://doi.org/10.1007/978-3-540-73595-3_5)
- [NT14] Noschinski, L., Traut, C.: Pattern-based subterm selection in Isabelle. In: *Proceedings of Isabelle Workshop* (2014)

- [Rus17] Russinoff, D.M.: A computationally surveyable proof of the group properties of an elliptic curve. arXiv preprint [arXiv:1705.01226](https://arxiv.org/abs/1705.01226) (2017)
- [The07] Théry, L., Hanrot, G.: Primality proving with elliptic curves. In: Schneider, K., Brandt, J. (eds.) TPHOLS 2007. LNCS, vol. 4732, pp. 319–333. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-74591-4\\_24](https://doi.org/10.1007/978-3-540-74591-4_24)
- [Wen19] Wenzel, M.: The Isabelle/Isar reference manual (2019)