The geometry of efficient arithmetic on elliptic curves

David Kohel
Institut de Mathématiques de Marseille

University of Oxford – Cryptography Seminar
26 octobre 2016

Elliptic curve cryptography

In 1985, Miller and Koblitz introduced the use of elliptic curves in cryptography. This replaced $\mathbb{F}_p^* = \mathbb{G}_m(\mathbb{F}_p)$ (in the protocols of Diffie and Hellman or ElGamal) with the group $E(\mathbb{F}_p)$ of rational points on an elliptic curve $E/\mathbb{F}_p$.

This was made possible by the introduction of a polynomial-time algorithm of Schoof for computing the cardinality $|E(\mathbb{F}_p)|$ in the same year.

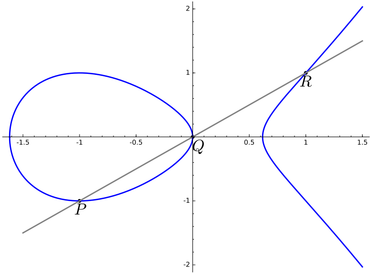
The default model for computing in $E(\mathbb{F}_p)$ involved embedding E as a Weierstrass model $Y^2Z = X^3 + aXZ^2 + bZ^3$ in $\mathbb{P}^2$, with identity $O = (0 : 1 : 0)$. We focus on the role of the choice of model on the algorithms for elliptic curve arithmetic.

Addition morphism

On a Weierstrass model E, the addition morphism is defined by the rule "three points on a line L sum to O". This interprets the relation

$$L.E = (P) + (Q) + (R) \sim 3(O) = L_\infty.E,$$

where $L_\infty = V(Z)$ is the line at infinity, in the Picard group of E.



Rational addition law on Weierstrass model

This rule determines the addition morphism $\mu : E \times E \to E$ on all affine points

$$P_1 = (x_1, y_1) = (x_1 : y_1 : 1) \text{ and } P_2 = (x_2, y_2) = (x_2 : y_2 : 1)$$

with $x_1 \neq x_2$, by setting

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}, \quad \nu = \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}.$$

Then $P_1 + P_2 = P_3 = (x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu)$.

N.B. This defines μ outside of the *diagonal* Δ, the *antidiagonal* ∇, the *horizontal* $H = E \times \{O\}$ and *vertical* $V = \{O\} \times E$ divisors.

A projective addition law on Weierstrass model

Projectively, in (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2), we have

$$\lambda = \frac{Y_1 Z_2 - Z_1 Y_2}{X_1 Z_2 - Z_1 X_2}, \quad \nu = \frac{X_1 Y_2 - Y_1 X_2}{X_1 Z_2 - Z_1 X_2},$$

and then

$$x_3 = \left(\frac{Y_1 Z_2 - Z_1 Y_2}{X_1 Z_2 - Z_1 X_2}\right)^2 - \frac{X_1 Z_2 + Z_1 X_2}{Z_1 Z_2},$$

$$y_3 = -\left(\frac{Y_1 Z_2 - Z_1 Y_2}{X_1 Z_2 - Z_1 X_2}\right) x_3 - \frac{X_1 Y_2 - Y_1 X_2}{X_1 Z_2 - Z_1 X_2}.$$

Clearing denominators we obtain bihomogeneous polynomial expressions (X_3, Y_3, Z_3) of bidegree $(4, 4)$ in the input points, or $(3, 3)$ after exploiting a cancellation of $Z_1 Z_2$ in x_3.

Projective addition laws on Weierstrass models

It was well-known (after Lange & Ruppert) that there exists a finite dimensional space of bidegree $(2,2)$ *addition laws* (homogeneous polynomial maps for μ), and that any nonzero addition law fails to be defined on some divisor on $E \times E$, its *exceptional divisor*.

Bosma & Lenstra computed explicit bidegree $(2,2)$ addition laws for a Weierstrass model E, which span a 3-dimensional space, and showed that two addition laws suffice to define μ globally.

However, compared to the bidegree $(4,4)$ addition law defined by

$$(X_3(X_1Z_2 - Z_1X_2),\ Y_3,\ (X_1Z_2 - Z_1X_2)^3 Z_1Z_2),$$

where

$$\begin{aligned} X_3 &= (Y_1Z_2 - Z_1Y_2)^2 Z_1Z_2 - (X_1Z_2 + Z_1X_2)(X_1Z_2 - Z_1X_2)^2, \\ Y_3 &= -(Y_1Z_2 - Z_1Y_2)X_3 - (X_1Y_2 - Y_1X_2)(X_1Z_2 - Z_1X_2)^2 Z_1Z_2, \end{aligned}$$

the bidegree $(2,2)$ polynomials are too cumbersome to be practical.

Scalar multiplication

The principal operation in elliptic curve cryptography is scalar multiplication. To carry out $[n] : E \to E$, the doubling morphism $[2]$ plays an important role. If $n_r \ldots n_0$ is the binary representation of n, then

$$[n]P = \sum_{i=0}^{r} n_i [2^i]P,$$

and we can determine $[n]P (= Q_r)$ by calculating in parallel the sequences (P_i) and (Q_i) with $P_0 = P$, $Q_0 = n_0 P$,

$$P_i = [2^i]P = [2]P_{i-1}, \text{ and } Q_i = Q_{i-1} + n_i P_i.$$

Using windowing methods, the number of calls to $[2]$ exceeds additions, and it becomes important to have efficient doubling.

Arithmetic on Weierstrass models

If E has a rational 2-torsion point, then a speed-up can be obtained by an isogeny decomposition

$$[2] = \varphi \circ \hat{\varphi}.$$

Optimally the isogenies φ and $\hat{\varphi}$ are given by quadratic polynomails.

Unfortunately for Weierstrass models, no quadratic polynomials defining a 2-isogeny of Weierstrass models can exist.

Worse, any polynomial map (necessarily of degree ≥ 3) must fail on some subset of points.

In contrast, quartic models in $\mathbb{P}^3$ admit 2-isogenies defined by quadratic polynomials.

Edwards model of elliptic curves

In 2007, Edwards introduced a model of elliptic curve with remarkable properties. Bernstein, Lange, et al. carried out a descent of the base field and twist , we obtain the *twisted Edwards model*

$$E : ax^2 + y^2 = 1 + dz^2, \; z = xy,$$

with identity $O = (0, 1, 0)$. This embeds via $(1 : x : y : z)$ as the project model in $\mathbb{P}^3$

$$aX_1^2 + X_2^2 = X_0^2 + dX_3^3, \; X_0X_3 = X_1X_2.$$

This model combines features of efficient doubling and addition laws, combined with arithmetic completeness — if d and d/a are nonsquares in k^*, then a single addition law is valid for all points over k.

Edwards addition law

The interest in Edwards model is the simple rational addition law:

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_3, y_3, z_3),$$

given by

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d z_1 z_2} \text{ and } y_3 = \frac{-a x_1 x_2 + y_1 y_2}{1 - d z_1 z_2} \text{ with } z_3 = x_3 y_3.$$

In terms of the projective model in $\mathbb{P}^3$, this gives

$$P + Q = (U_0 V_0 : U_0 V_1 : U_1 V_0 : U_1 V_1)$$

where each U_i, V_j are bilinear in the coordinates of P and Q:

$$(U_0, U_1) \in \left\{ \begin{array}{c} (X_2 Y_1 - X_1 Y_2,\ X_0 Y_3 - X_3 Y_0), \\ (X_0 Y_0 - d X_3 Y_3, X_2 Y_2 - a X_1 Y_1) \end{array} \right\}$$

$$(V_0, V_1) \in \left\{ \begin{array}{c} (a X_1 Y_1 + X_2 Y_2, X_0 Y_3 + X_3 Y_0), \\ (X_0 Y_0 + d X_3 Y_3,\ X_2 Y_1 + X_1 Y_2) \end{array} \right\}$$

Edwards arithmetic

In comparison to the multipage formulas for bidegree $(2, 2)$ addition laws on the Weierstrass model, these addition laws on Edwards' model is strikingly elegant and efficient.

Moreover, specializing to $X_i = Y_i$, we find simple expressions for doubling as well, which also are everywhere defined.

These results spawned a minor industry of optimization of the pair of elliptic curve model and algorithms for evaluating their addition and doubling laws.

Elliptic curve models

The previous discussion motivates the study of elliptic curves with given *projective model*, by which we mean E/k with given embedding $\iota : E \to \mathbb{P}^r$.

The addition and doubling laws are polynomial expressions in terms of the coordinate functions $X_0, \ldots, X_r$, which play an intrinsic role in their definition.

To understand elliptic curve arithmetic, rather than classifying curves up to arbitrary isomorphism, we will be interested in elliptic curves up to *projective linear isomorphism*.

Such a classification determines the complexity of arithmetic on elliptic curves, up to additions and multiplications by constants.

Embeddings by complete linear systems

The classification is simplified by the imposed condition that the curve model is given by a complete linear system with respect to an effective divisor $D = (P_0) + \cdots + (P_r)$.

If the Riemann-Roch space has basis $(1, x_1, \ldots, x_r)$, the map

$$P \longmapsto (1 : x_1(P) : \cdots : x_r(P)).$$

gives an embedding in $E \to \mathbb{P}^r$ ($r = \deg(D) - 1$) such that the line $X_0 = 0$ then cuts out D.

The question of projective linear isomorphism between two models for E is reduced to whether the two divisors are linearly equivalent.

This equivalence class, in turn, is uniquely determined by the degree $d = r + 1$ and the point $P = P_0 + \cdots + P_r \in E(k)$.

Elliptic curve models

The fastest arithmetic is observed for elliptic curve models with a high degree of symmetry. Such symmetries come from $[-1]$ and translation by points in a finite subgroup $G \subset E[d]$.

This suggests the study of elliptic curve models $E \to \mathbb{P}^r$, embedding with respect to a divisor D such that:

1. $[-1]$ is a projective linear transformation.
2. Translation by $P \in G$ acts by projective linear transformation.

Moreover by choose the basis of coordinate functions, so that d-torsion points act by a combination of coordinate permutation and scalar multiplication by roots of unity, the resulting addition laws take a particularly simple form.

Hessian normal form

For cubic models, it is natural to investigate models with 3-torsion level structure, which acts linearly. The Hessian normal form is an embedded cubic curve $H \subset \mathbb{P}^2$ given by

$$X^3 + Y^3 + Z^3 = dXYZ,$$

and with identity $(0 : 1 : -1)$. The 3-torsion subgroup decomposes $H[3] \cong \boldsymbol{\mu}_3 \times \mathbb{Z}/3\mathbb{Z}$, such that $P = (1 : \zeta_3 : \zeta_3^2) \in \boldsymbol{\mu}_3$ acts by

$$(X : Y : Z) \mapsto (X : \zeta_3 Y : \zeta_3^2 Z),$$

$Q = (1 : -1 : 0) \in \mathbb{Z}/3ZZ$ acts by $(X : Y : Z) \mapsto (Y : Z : X)$, and

$$[-1](X : Y : Z) = (X : Z : Y).$$

The line $X_0 = 0$ cuts out a subgroup

$$\{(0, 1, -1), (0, \zeta_3, -\zeta_3^2), (0, \zeta_3^2, -\zeta_3)\}$$

isomorphic to $\boldsymbol{\mu}_3 = \{1, \zeta_3, \zeta_3^2\}$.

Split μ_4-normal form

The split $\boldsymbol{\mu}_4$-normal form $C \subset \mathbb{P}^3$ is the elliptic curve model

$$X_0^2 - X_2^2 = c^2\,X_1X_3,\;\; X_1^2 - X_3^2 = c^2\,X_0X_2,$$

with identity $O = (c:1:0:1)$. A subgroup isomorphic to $\boldsymbol{\mu}_4 = \{1, i, -1, -i\}$ is cut out by $X_2 = 0$:

$$\{(c:1:0:1),(c:i:0:i),(c:-1:0:-1),(c:-i:0:-i)\}.$$

We note that this model is isomorphic to the -1-twist of an Edwards curves, which admits addition laws with the most efficient known evaluation algorithm, but has good reduction at 2.

The split $\boldsymbol{\mu}_4$-normal form is analogous to the above Hessian normal form in that it parametrizes a full level-4 structure.

Explicit addition laws

We recall that, by a theorem of Lange and Ruppert, the minimal bidegree of any addition law is $(2, 2)$, and for an elliptic curve model of degree d, the laws of this minimal bidegree span a space of dimension d.

We give the form of these addition laws, and the resulting complexity for the above models.

Addition laws: Hessian model

Theorem

The space of addition laws of bidegree $(2, 2)$ *on* H *is spanned by:*

$$
\begin{aligned}
&(\,X_1^2Y_2Z_2 - Y_1Z_1X_2^2,\ Z_1^2X_2Y_2 - X_1Y_1Z_2^2,\ \ Y_1^2X_2Z_2 - X_1Z_1Y_2^2\,),\\
&(\,X_1Y_1Y_2^2 - Z_1^2X_2Z_2,\ X_1Z_1X_2^2 - Y_1^2Y_2Z_2,\ \ Y_1Z_1Z_2^2 - X_1^2X_2Y_2\,),\\
&(\,X_1Z_1Z_2^2 - Y_1^2X_2Y_2,\ Y_1Z_1Y_2^2 - X_1^2X_2Z_2,\ \ X_1Y_1X_2^2 - Z_1^2Y_2Z_2\,).
\end{aligned}
$$

As a consequence, the doubling map sends (X, Y, Z) to

$$(X(Y^3 - Z^3), (X^3 - Y^3)Z, Y(Z^3 - X^3)).$$

The best known algorithms for evaluating these maps gives a complexity of $12\mathbf{M}$ for addition and $7\mathbf{M} + 1\mathbf{S}$ for doubling.

Addition laws: split μ_4-normal form

Theorem

The space of addition laws of bidegree $(2,2)$ for C is spanned by :

$$
\begin{aligned}
&(X_{13}^2 - X_{31}^2,\ c(X_{13}X_{20} - X_{31}X_{02}),\ X_{20}^2 - X_{02}^2,\ c(X_{20}X_{31} - X_{13}X_{02})),\\
&(c(X_{03}X_{10} + X_{21}X_{32}),\ X_{10}^2 - X_{32}^2,\ c(X_{03}X_{32} + X_{10}X_{21}),\ X_{03}^2 - X_{21}^2),\\
&(X_{00}^2 - X_{22}^2,\ c(X_{00}X_{11} - X_{22}X_{33}),\ X_{11}^2 - X_{33}^2,\ c(X_{00}X_{33} - X_{11}X_{22})),\\
&(c(X_{01}X_{30} + X_{12}X_{23}),\ X_{01}^2 - X_{23}^2,\ c(X_{01}X_{12} + X_{23}X_{30}),\ X_{30}^2 - X_{12}^2),
\end{aligned}
$$

where $X_{ij} = X_i Y_j$.

and the doubling map sends (X_0, X_1, X_2, X_3) to

$$(X_0^4 - X_2^4, cX_0^2X_1^2 - cX_2^2X_3^2, X_1^4 - X_3^4, -cX_1^2X_2^2 + cX_0^2X_3^2).$$

We deduce the best known complexity for their evaluation: $8\mathbf{M}$ for addition ($7\mathbf{M} + 2\mathbf{S}$ in char. 2) and $4\mathbf{M} + 3\mathbf{S}$ ($2\mathbf{M} + 5\mathbf{S}$ in char. 2).

A split μ_4 addition eigenform

Let $T = (c : i : 0 : -i) \in \boldsymbol{\mu}_4 \subset C[4]$, set τ to be the translation by T map (given by $\tau((x_0 : x_1 : x_2 : x_3)) = (x_0 : ix_1 : -x_2 : -ix_3))$. Similarly let $S = (0 : -1 : c : 1) \in C[2]$ and let σ be the translation by S map (given by $\sigma((x_0 : x_1 : x_2 : x_3)) = (x_2 : x_3 : -x_0 : -x_1))$. Then both $\tau \times \tau^{-1}$ and $\sigma \times \sigma^{-1}$ (lift to) act on the space of addition laws of a given degree, and the addition law (f_0, f_1, f_2, f_3) where

$$\begin{aligned} f_0 &= X_0^2 Y_0^2 - X_2^2 Y_2^2, & f_1 &= c(X_0 X_1 Y_0 Y_1 - X_2 X_3 Y_2 Y_3),\\ f_2 &= X_1^2 Y_1^2 - X_3^2 Y_3^2, & f_3 &= c\,(X_0 X_3 Y_0 Y_3 - X_1 X_2 Y_1 Y_2) \end{aligned}$$

is a common eigenform of $\tau \times \tau^{-1}$ and $\varsigma \times \varsigma^{-1}$.

We note moreover that the exceptional divisor for this addition law is $\Delta_S + \Delta_R + \Delta_{S+T} + \Delta_{S-T}$, where $R = S + 2T \in C[2]$.

Evaluating a split μ_4 addition eigenform

Let $V_X = \langle X_0, X_1, X_2, X_3\rangle$ and $V_Y = \langle Y_0, Y_1, Y_2, Y_3\rangle$, and set

$$V = V_X \otimes V_Y \supset V_0 = V^{\tau\times\tau^{-1}} = \langle X_0 Y_0, X_1 Y_1, X_2 Y_2, X_3 Y_3\rangle.$$

We further decompose $V_0 = V^+ \oplus V^{-1}$ into eigenspaces with respect to the action of $\varsigma \times \varsigma^{-1}$, where

$$\begin{aligned} V^+ &= \langle X_0 Y_0 + X_2 Y_2, X_1 Y_1 + X_3 Y_3\rangle, \text{ and} \\ V^- &= \langle X_0 Y_0 - X_2 Y_2, X_1 Y_1 - X_3 Y_3\rangle. \end{aligned}$$

Clearly

$$\begin{aligned} f_0 &= (X_0 Y_0 + X_2 Y_2)(X_0 Y_0 - X_2 Y_2), \text{ and} \\ f_2 &= (X_1 Y_1 + X_3 Y_3)(X_1 Y_1 - X_3 Y_3). \end{aligned}$$

are both in $V^+ \otimes V^-$.

Evaluating a split μ_4-normal form eigenform

In addition, so are f_1 and f_3, since

$$\begin{aligned} c^{-1}(f_1 + f_3) &= (X_1 Y_1 + X_3 Y_3)(X_0 Y_0 - X_2 Y_2), \text{ and} \\ c^{-1}(f_1 - f_3) &= (X_0 Y_0 + X_2 Y_2)(X_1 Y_1 - X_3 Y_3). \end{aligned}$$

Consequently, $V^+ \otimes V^{-1} = \langle f_0, f_1, f_2, f_3 \rangle$, and computing V^+ and V^- each with $2\mathbf{M}$, followed by $4\mathbf{M}$ to compute

$$V^+ \otimes V^{-1} \subset \mathrm{Sym}^2(V_X) \otimes \mathrm{Sym}^2(V_Y).$$

This gives a complexity of $8\mathbf{M}$ to compute the addition law (plus two multiplications by the constant c, denoted $2\mathbf{m}$).

Explaining the complexity for split μ_4-normal form

As noted above the exceptional divisor for the eigenform (f_0, f_1, f_2, f_3) is

$$\Delta_S + \Delta_R + \Delta_{S+T} + \Delta_{S-T},$$

and we note that the divisors cut out by

$$\begin{aligned} V^+ &= \langle X_0 Y_0 + X_2 Y_2, X_1 Y_1 + X_3 Y_3 \rangle \text{ and} \\ V^- &= \langle X_0 Y_0 - X_2 Y_2, X_1 Y_1 - X_3 Y_3 \rangle, \end{aligned}$$

are precisely

$$\Delta_{S+T} + \Delta_{S-T} \text{ and } \Delta_S + \Delta_R,$$

respectively. The product space $V_X \otimes V_Y$ then cuts out exactly the exceptional divisor of (f_0, f_1, f_2, f_3) which explains the equality

$$V^+ \otimes V^{-1} = \langle f_0, f_1, f_2, f_3 \rangle.$$

Nonoptimal complexity of Hessian addition eigenform

Since the number of coordinate functions $(= 3)$ and the dimension of the target vector space $(= 3)$ of an addition law on a cubic model are smaller than for a quartic model. As a result, one might expect a better complexity for evaluation of an addition eigenform on the Hessian model.

However this is not the case, since we fail to have an analogous "factorization" of the form

$$\langle f_0, f_1, f_2 \rangle = V^+ \otimes V^{-1}.$$

in particular the dimension of $\langle f_0, f_1, f_2 \rangle$ is prime. Moreover, the exceptional divisor of (f_0, f_1, f_2) is of the form

$$\Delta_{T_1} + \Delta_{T_2} + \Delta_{T_3} \sim 3\Delta,$$

which does not decompose into two summands of the same degree.

Evaluating a Hessian addition eigenform

Let $T = (0 : \zeta_3 : -\zeta_3^2) \in H[3]$ and set τ to be the translation by T map (given by $\tau((x_0 : x_1 : x_2)) = (x_0 : \zeta_3 x_1 : \zeta_3^2 x_2))$. We consider the following addition eigenform:

$$(f_0, f_1, f_2) = \left(X_0^2 Y_1 Y_2 - X_1 X_2 Y_0^2, X_2^2 Y_0 Y_1 - X_0 X_1 Y_2^2, X_1^2 Y_0 Y_2 - X_0 X_2 Y_1^2\right)$$

for the action of $\tau \times \tau^{-1}$. As above, we set

$$V_X = \langle X_0, X_1, X_2 \rangle \text{ and } V_Y = \langle Y_0, Y_1, Y_2 \rangle.$$

Computing the addition eigenform requires the computation of the 3-dimensional subspace

$$\langle f_0, f_1, f_2 \rangle \subset \mathrm{Sym}^2(V_X) \otimes \mathrm{Sym}^2(V_Y)$$

inside a 36-dimensional space.

Evaluating a Hessian addition eigenform

In order to compute a subspace of $\mathrm{Sym}^2(V_X) \otimes \mathrm{Sym}^2(V_Y)$, we can pass via subspaces of $\mathrm{Sym}^2(V_X)$ and $\mathrm{Sym}^2(V_Y)$ or of $V_X \otimes V_Y$. We have eigenspace decompositions of the spaces

$$\begin{aligned}\mathrm{Sym}^2(V_X) &= \langle X_0^2, X_1X_2\rangle \oplus \langle X_0X_1, X_2^2\rangle \oplus \langle X_0X_2, X_1^2\rangle,\\ \mathrm{Sym}^2(V_Y) &= \langle Y_0^2, Y_1Y_2\rangle \oplus \langle Y_0Y_1, Y_2^2\rangle \oplus \langle Y_0Y_2, Y_1^2\rangle,\end{aligned}$$

and similarly $V_X \otimes V_Y = V_0 \otimes V_1 \otimes V_2$, where

$$\begin{aligned}V_0 &= \langle X_0Y_0,\ X_1Y_1,\ X_2Y_2\rangle,\\ V_1 &= \langle X_1Y_0,\ X_2Y_1,\ X_0Y_2\rangle,\\ V_2 &= \langle X_0Y_1,\ X_1Y_2,\ X_2Y_0\rangle.\end{aligned}$$

The computation of each of V_0, V_1 and V_2 require $3\mathbf{M}$. We note that $\langle f_0, f_1, f_2\rangle \subset V_1 \otimes V_2$.

Evaluating a Hessian addition eigenform

The space $V_1 \otimes V_2$ requires 9**M**, but $\langle f_0, f_1, f_2 \rangle$ is contained in the six dimensional space

$$\left\langle \begin{array}{ll} X_0Y_1 \cdot X_0Y_2, & X_1Y_0 \cdot X_2Y_0, \\ X_2Y_2 \cdot X_2Y_1, & X_0Y_2 \cdot X_1Y_2, \\ X_1Y_0 \cdot X_1Y_2, & X_0Y_1 \cdot X_2Y_1 \end{array} \right\rangle,$$

which we construct using 6**M**. Together with the 3**M** for each of V_1 and V_2, this gives a complexity of 12**M**.

What went wrong? The exceptional divisor of (f_0, f_1, f_2) is 3Δ. If we consider the subspace stable under $(P, Q) \mapsto (Q, P)$,

$$\langle X_0Y_1 - X_1Y_0, X_0Y_2 - X_2Y_0, X_0Y_3 - X_3Y_0 \rangle$$

of $V_1 \oplus V_2$ cutting out Δ (as a divisor). Unlike in the above case, without taking differences of products, we can only expect to cut out the divisor 2Δ.