

# Arithmetic on Abelian and Kummer varieties

*Notes of a talk given for the LFANT Algorithmic Number Theory Seminar — Bordeaux.  
Based on earlier talks given in Grenoble and Caen.*

ABSTRACT. In this talk we give an outline of the results obtained in [LR14]. The first part is a review of the arithmetic on elliptic curves and Jacobians of hyperelliptic curves. The second part is more sophisticated and review the algebraic theory of theta functions, and the multiplication map. The much more elementary third part use the geometric results from the second one to improve the arithmetic on Abelian and Kummer varieties. **Warning:** These notes are in a very rough state, and probably contain a lot of errors, refer to the article for more details! Also the cost of the arithmetic mentioned for the different models do not always count the same thing, sometime we forget multiplication by small constants and sometime look at the addition with a normalized projective point, so be careful before comparing them!

## CONTENTS

1. Arithmetic on Elliptic Curves	1
2. Jacobian of hyperelliptic curves	3
3. Complex abelian varieties	3
4. Heisenberg group	4
5. Riemann relations	5
5.1. The Isogeny theorem	5
5.2. Riemann relations	6
5.3. Multiplication map	7
5.4. Normal projectivity	7
5.5. Addition, Differential addition	8
6. Arithmetic on Kummer varieties	8
6.1. Multi Scalar multiplication	8
7. Changing level	9
7.1. Compressing coordinates	9
8. Arithmetic on abelian varieties	9
9. Formulae	10
References	11

## 1. ARITHMETIC ON ELLIPTIC CURVES

**Elliptic curve in short Weierstrass form** over a field  $k$   $E : y^2 = x^3 + ax + b$  (always such a model when  $\text{char } k > 3$ ).

- Distinct points  $P$  and  $Q$ :

$$P + Q = -R = (x_R, -y_R)$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = y_P + \lambda(x_R - x_P)$$

(If  $x_P = x_Q$  then  $P = -Q$  and  $P + Q = 0_E$ ).

- If  $P = Q$ , then  $\lambda$  comes from the tangent at  $P$ :

$$\begin{aligned}\lambda &= \frac{3x_P^2 + b}{2y_P} \\ x_R &= \lambda^2 - 2x_P \\ y_R &= y_P + \lambda(x_R - x_P)\end{aligned}$$

One can avoid divisions by working with projective coordinates  $(X : Y : Z)$ :

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Cost for an addition: 11M+7S in Extended Jacobian coordinates (not counting multiplication by small constants).

The scalar multiplication  $P \mapsto n.P$  is computed via the standard double and add algorithm, on average  $\log n$  doubling and  $1/2 \log n$  additions. Standard tricks to speed-up include NAF form, windowing... The multiscalar multiplication  $(P, Q) \mapsto n.P + m.Q$  can also be computed via doubling and the addition of  $P$ ,  $Q$  or  $P + Q$  according to the bits of  $n$  and  $m$ , on average  $\log N$  doubling and  $3/4 \log N$  additions where  $N = \max(n, m)$ . GLV idea: if there exists an efficiently computable endomorphism  $\alpha$  such that  $\alpha(P) = u.P$  where  $u \approx \sqrt{n}$ , then replace the scalar multiplication  $n.P$  by the multiscalar multiplication  $n_1P + n_2\alpha(P)$ . One can expect  $n_1$  and  $n_2$  to be half the size of  $n \Rightarrow$  from  $\log n$  doubling and  $1/2 \log n$  additions to  $1/2 \log n$  doubling and  $3/8 \log n$  additions.

**Edwards curves:**  $E : x^2 + y^2 = 1 + dx^2y^2$ ,  $d \neq 0, -1$ ,  $\text{char } k > 2$ . Addition of  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$ :

$$P + Q = \left( \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Neutral element:  $(0, 1)$ ;  $-(x, y) = (x, y)$ ;  $T = (1, 0)$  has order 4,  $2T = (0, 1)$ . (Conversely every elliptic curve with a point of 4-torsion has an Edwards curve model). When  $d = 0$  we get a circle (a curve of genus 0) and we find back the addition law on the circle coming from the sine and cosine laws. If  $d$  is not a square in  $K$ , then there are no exceptional points: the denominators are always nonzero (for rational points in  $K$ ) so we have a complete addition law (very useful to prevent some Side Channel Attacks). Cost for an addition: 10M+1S (Projective coordinates), 9M+1S (Inverted coordinates).

**Twisted Edwards curves:**  $E : ax^2 + y^2 = 1 + dx^2y^2$ . Addition of  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$ :

$$P + Q = \left( \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Neutral element:  $(0, 1)$ ;  $-(x, y) = (x, y)$ ;  $T = (0, -1)$  has order 2 (conversely if all points of 2-torsion of an elliptic curve  $E$  are rational then  $E$  is 2-isogenous to a twisted Edwards curve). Extensively studied by Bernstein and Lange, still complete addition if  $a$  is a square and  $d$  not a square. Cost for an addition: 10M+1S (Projective coordinates), 9M (Extended coordinates), 8M (Extended coordinates with  $a = -1$ ).

**Montgomery curves:**  $E : By^2 = x^3 + Ax^2 + x$  (birationally equivalent to twisted Edwards curves). The map  $E \rightarrow \mathbb{A}^1$ ,  $(x, y) \mapsto (x)$  maps  $E$  to the Kummer line  $K_E = E/\pm 1$ . We represent a point  $\pm P \in K_E$  by the projective coordinates  $(X : Z)$  where  $x = X/Z$ . Differential addition: Given  $\pm P_1 = (X_1 : Z_1)$ ,  $\pm P_2 = (X_2 : Z_2)$  and  $\pm(P_1 - P_2) = (X_3 : Z_3)$ ; then one can compute  $\pm(P_1 + P_2) = (X_4 : Z_4)$  by

$$\begin{aligned}X_4 &= Z_3 ((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2))^2 \\ Z_4 &= X_3 ((X_1 - Z_1)(X_2 + Z_2) - (X_1 + Z_1)(X_2 - Z_2))^2\end{aligned}$$

Cost: 2M+2S for a doubling and 4M+2S for a differential addition.

**Montgomery's scalar multiplication:** The scalar multiplication  $\pm P \mapsto \pm n \cdot P$  can be computed through differential additions if we can construct a differential chain. If  $\pm[n]P = (X_n - Z_n)$ , then

$$\begin{aligned} X_{m+n} &= Z_{m-n} ((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2 \\ Z_{m+n} &= X_{m-n} ((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n))^2 \end{aligned}$$

Montgomery's ladder use the chain  $nP, (n+1)P$ : from  $nP, (n+1)P$  the next iteration computes  $2nP, (2n+1)P$  or  $(2n+1)P, (2n+2)P$  via one doubling and one differential addition.

## 2. JACOBIAN OF HYPERELLIPTIC CURVES

$H : y^2 = f(x)$ ,  $\deg f = 2g + 1$ : hyperelliptic curve of genus  $g$  with a rational point at infinity. Every divisor  $D$  can be represented by a reduced divisor

$$\tilde{D} = \sum_{i=1}^r (P_i) - r(\infty)$$

where  $r \leq g$  and  $P_i \neq -P_j$  for  $i \neq j$ . The divisor  $D$  is represented by its Mumford coordinates  $(u, v)$  where if  $P_i = (x_i, y_i)$ :

$$\begin{aligned} u(x) &= \prod (x - x_i) \\ v(x_i) &= y_i \\ \deg v &< \deg u \leq g \\ u(x) &| v(x)^2 - f(x); \end{aligned}$$

The last condition encodes that  $y - v(x)$  has multiplicity  $m_i = v_{P_i}(D)$  at  $P_i$ . From  $(u, v)$ ,  $D$  is recovered by  $D = \text{div}(u(x)) \wedge \text{div}(v(x) - y)$ .

**Algorithm 2.1** (Cantor's algorithm). **Input:**  $D_1 = (u_1, v_1), D_2 = (u_2, v_2)$ ;

**Output:**  $D = (u, v)$  such that  $D \sim D_1 + D_2$ ;

(1) **Semireduce:** Compute the extended gcd of  $u_1, u_2, v_1 + v_2$

$$\begin{aligned} d &= s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2) \\ u &= \frac{u_1 u_2}{d^2} \\ v &= \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \text{ modulo } u \end{aligned}$$

(2) **Reduce:**

$$\begin{aligned} u &= \frac{f - v^2}{u} \quad (\text{Use the function } f - v^2 \text{ to reduce the current divisor}) \\ v &= -v \text{ modulo } u \end{aligned}$$

until  $\deg u \leq g$ .

Cost in genus 2: 32M + 7S for a doubling and 36M + 5S for an addition in weighted coordinates [Lan05]; 21M + 12S for a doubling and 29M + 7S for an addition in Jacobian coordinates [HC14].

## 3. COMPLEX ABELIAN VARIETIES

$A = (V/\Lambda, H)$  where  $V$  is a  $\mathbb{C}$ -ev of dimension  $g$ ,  $\Lambda$  is a lattice of rank  $2g$  and  $E = \Im H$  is symplectic,  $E(ix, iy) = E(x, y)$  and  $E(\Lambda, \Lambda) \subset \mathbb{Z}$ . If  $\Lambda = \mathbb{Z}^g + \Omega \mathbb{Z}^g$  where  $\Omega \in \mathfrak{H}_g$  (ie  $\Omega$  symmetric,  $\Im \Omega > 0$ ),  $\Omega$  determines a principal polarisation  $H_0 = (\Im \Omega)^{-1}$ .

**Definition 3.1** (Theta functions with characteristics  $a, b \in \mathbb{Q}^g$ ).

$$\vartheta \left[ \begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i {}^t(n+a) \cdot \Omega \cdot (n+a) + 2\pi i {}^t(n+a) \cdot (z+b)}.$$

	Montgomery	Level 2	Twisted Edwards (Inverted)	Jacobians coordinates
Doubling				
Mixed Addition	$5M + 4S + 1m_0$	$3M + 6S + 3m_0$	$3M + 4S + 1m_0$ $8M + 1S + 2m_0$	$3M + 5S$ $7M + 6S + 1m_0$
	Mumford (Jacobian coordinates)		Level 2	Level 4
Doubling				
Mixed Addition		$21M + 12S + 2m_0$ $29M + 7S$	$7M + 12S + 9m_0$	$49M + 36S + 27m_0$

TABLE 1. Multiplication cost in dimension 1 and 2 (one step).

To get coordinates, we need a projective embedding, which corresponds to an (ample) line bundle  $\mathcal{L}$ . The sections of  $\mathcal{L}$  correspond to functions  $f$  such that

$$f(z + \lambda) = a_{\mathcal{L}}(z, \lambda)f(z)$$

where  $a_{\mathcal{L}}$  is the automorphic factor associated to  $\mathcal{L}$ , satisfying the cocycle condition

$$a_{\mathcal{L}}(z, \lambda_1 + \lambda_2) = a_{\mathcal{L}}(z, \lambda_1)a_{\mathcal{L}}(z + \lambda_1, \lambda_2).$$

**Theorem 3.2** (Appell-Humbert).

$$a_{\mathcal{L}}(z, \lambda) = \chi(\lambda)e^{\pi H(z, \lambda) + \frac{\pi}{2}H(\lambda, \lambda)}$$

where  $\chi(\lambda) = \pm 1$  (when  $\mathcal{L}$  is symmetric).

If  $\mathcal{L} = \mathcal{L}_0^n$  ie if the polarisation  $H$  is  $nH_0$ , the sections are called theta functions of level  $n$ . If  $n = n_1n_2$  a basis is given by  $\vartheta \left[ \begin{smallmatrix} a/n_1 \\ b/n_2 \end{smallmatrix} \right] (n_1z, \frac{n_1}{n_2}\Omega)$ . A choice of basis is uniquely determined (up to a constant) by a representation of the action by translation by points of  $n$ -torsions.

**Proposition 3.3** (Lefschetz).

- If  $n \geq 3$  we get an embedding of  $A$  into projective space;
- If  $n = 2$  and  $\mathcal{L}_0$  is indecomposable, we get an embedding of the Kummer variety  $A/\pm 1$ ;

**Example 3.4.** Let  $E_1$  and  $E_2$  be two elliptic curves,  $\mathcal{L}_1$  and  $\mathcal{L}_2$  be the corresponding canonical polarisation coming from  $0_{E_i}$  and Let  $\mathcal{L}_0 = \mathcal{L}_1 \star \mathcal{L}_2$  be the product polarisation on  $E_1 \times E_2$ . Then the embedding given by the sections of  $\mathcal{L} = \mathcal{L}_0^2$  give a projective embedding of  $E_1/\pm 1 \times E_2/\pm 1$  which is a quotient of the Kummer variety  $((E_1 \times E_2)/\pm 1)$ . (Note: some terminology call the Kummer variety the quotient of  $A$  by all the automorphisms; here we only quotient by  $\pm 1$ . Generically this give the same definitions but not always as the example of product varieties show).

#### 4. HEISENBERG GROUP

$(A, \mathcal{L})/k$  polarised abelian variety over an algebraically closed field  $k$ . Assume for simplicity that  $\mathcal{L}$  is ample, and  $\mathcal{L} = \mathcal{L}_0^n$  where  $\mathcal{L}_0$  is principal and  $n$  is prime to the characteristic of  $k$ .

We note  $\Phi_{\mathcal{L}} : A \rightarrow \widehat{A}_k, x \mapsto \tau_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$  the corresponding polarisation. The kernel  $K(\mathcal{L})$  of  $\Phi_{\mathcal{L}}$  is then  $A[n]$ .

**Theta group:**

- $G(\mathcal{L}) := \{(x, \varphi) \mid x \in K(\mathcal{L}), \varphi : \mathcal{L} \xrightarrow{\sim} \tau_x^* \mathcal{L}\}$ .
- Group law:  $(y, \psi) \cdot (x, \varphi) = (x + y, \tau_x^* \psi \circ \varphi)$ :

$$\mathcal{L} \xrightarrow{\varphi} \tau_x^* \mathcal{L} \xrightarrow{\tau_x^* \psi} \tau_y^* \tau_x^* \mathcal{L}.$$

- The theta group fits into the exact sequence

$$0 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0.$$

- The commutator pairing  $e_{\mathcal{L}}(x, y) = \widetilde{xy}\widetilde{x}^{-1}\widetilde{y} \in k^*$  is non degenerate (Weil pairing), so  $G(\mathcal{L})$  is an Heisenberg group. If  $\psi : K(\mathcal{L})^2 \rightarrow k^*$  is the 2-cocycle corresponding to the central extension  $G(\mathcal{L})$ , then  $e_{\mathcal{L}}(x, y) = \frac{\psi(x, y)}{\psi(y, x)}$ .
- Action of  $G(\mathcal{L})$  on  $\Gamma(\mathcal{L})$ :

$$(x, \varphi).f = \tau_{-x}^*(\varphi(f)).$$

**Standard Heisenberg group:**  $K(n) := (\mathbb{Z}/n\mathbb{Z})^g \oplus \widehat{(\mathbb{Z}/n\mathbb{Z})^g}$ . The Heisenberg group  $G(n)$  is the central extension

$$0 \longrightarrow k^* \longrightarrow G(n) \longrightarrow K(n) \longrightarrow 0$$

given by the 2-cocycle  $\psi(x, y) = x_2(y_1)$ . Concretely  $(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha\beta x_2(y_1), x_1 + y_1, x_2 + y_2)$ . The symplectic isomorphism  $(K(n), e_n) \simeq (K(\mathcal{L}), e_{\mathcal{L}})$  extends (not uniquely in general) to an isomorphism  $\Theta_{\mathcal{L}} : G(n) \xrightarrow{\sim} G(\mathcal{L})$  (Theta structure of level  $n$ ).

**Theorem 4.1** (Mackey).  $G(n)$  has a unique irreducible representation  $V(n)$  of weight 1 (ie  $k^*$  acts by the natural character). If  $V$  is a representation of weight 1, then  $V = V(n)^r$  where  $r = \dim_k V^{\widetilde{K}}$  and  $K$  is a maximal isotropic subgroup of  $K(n)$ . Moreover the action of  $\widetilde{K}$  on  $V(n)$  is the standard adjoint representation, so  $V(n)$  has dimension  $n^g$ .

*Proof.* See [Mum66; Mum91]. □

**Descent:** If  $K \subset K(\mathcal{L})$  is isotropic,  $f : A \rightarrow B = A/K$  then level subgroup  $\widetilde{K} \subset G(\mathcal{L})$  (ie a section of  $K$ )  $\Leftrightarrow$  descent data of  $\mathcal{L} \Leftrightarrow \mathcal{M}$  ample bundle on  $B$  such that  $f^*M = \mathcal{L}$ .

**Theorem 4.2.** The action of  $G(\mathcal{L})$  on  $\Gamma(\mathcal{L})$  is irreducible.

*Proof.* If  $\widetilde{K}$  is maximal, by descent theory  $\mathcal{L}$  descends to a principal line bundle  $\mathcal{M}$  on  $A/K$ .  $\Gamma(\mathcal{L})^{\widetilde{K}} = \Gamma(\mathcal{M})$  is then of dimension 1. □

In particular  $\Gamma(\mathcal{L}) \curvearrowright G(\mathcal{L})$  is isomorphic to  $V(n) \curvearrowright G(n)$  (where  $G(n)$  acts by the standard action) via  $\Theta_{\mathcal{L}}$ .

Explicitly if we note  $Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$ ,  $V(n) = \text{Hom}(Z(\overline{n}), k)$ ,  $(\alpha, x_1, x_2).f = y \mapsto \alpha x_2(y)f(x_1 + y)$ . So there exists a unique basis  $(\vartheta_i)_{i \in K_1(\mathcal{L})}$  of  $\Gamma(\mathcal{L})$  such that the action of  $G(\mathcal{L})$  is given by

$$(\alpha, x_1, x_2).\vartheta_i = \alpha x_2(i)\vartheta_{i-x_1}.$$

(Abuse of notation: we see  $G(\mathcal{L}) = k^* \times K_1(\mathcal{L}) \times K_2(\mathcal{L})$  as a set, where  $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$  is the decomposition into maximal isotropic subgroups coming from  $\Theta_{\mathcal{L}}$ , and  $x_2(i)$  is the action coming from the 2-cocycle.)

Concretely,  $\vartheta_0$  is a non trivial section in  $\Gamma(\mathcal{L})^{\widetilde{K}_2(\mathcal{L})}$  and if  $i \in K_1(\mathcal{L})$ ,  $\vartheta_i = s(i).\vartheta_0$  where  $s$  is the canonical section coming from the theta structure and  $\widetilde{K}_2 = s(K_2)$  is the level subgroup above  $K_2$ .

## 5. RIEMANN RELATIONS

### 5.1. The Isogeny theorem.

**Theorem 5.1** (Isogeny Theorem). Let  $f : (A, \mathcal{L}) \rightarrow (B, \mathcal{M})$  be an isogeny between polarised abelian varieties,  $\mathcal{M}$  corresponds to a section  $\widetilde{K} \subset G(\mathcal{L})$  of the kernel  $K = \text{Ker } f$ .  $G(\mathcal{M}) = \widetilde{K}^\perp / \widetilde{K}$  and the decomposition  $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$  induces via  $f$  a decomposition  $K(\mathcal{M}) = K_1(\mathcal{M}) \oplus K_2(\mathcal{M})$  (if we assume that  $K = K_1 \cap K \oplus K_2 \cap K$ ). Likewise the theta structure on  $G(\mathcal{L})$  induces a compatible theta structure on  $G(\mathcal{M})$ . We then have for  $i \in K_1(\mathcal{L}) \cap K^\perp$  (up to a constant)

$$\vartheta_{f(i)}^{\mathcal{M}} = \sum_{j-i \in K \cap K_1(\mathcal{L})} \vartheta_j^{\mathcal{L}} = \sum_{j \in K_1(\mathcal{L}), f(j)=i} \vartheta_j^{\mathcal{L}} = \text{Trace of } \vartheta_i^{\mathcal{L}} \text{ under the action of } \widetilde{K}.$$

**5.2. Riemann relations.** Let  $\xi : A \times A \rightarrow A \times A, (x, y) \mapsto (x + y, x - y)$  be the isogeny coming from the group law, with kernel  $\text{diag } A[2]$ . We now assume that  $\mathcal{L}$  is totally symmetric, ie  $\mathcal{L} = \mathcal{L}_0^n$  with  $\mathcal{L}_0$  symmetric and  $2 \mid n$ . We have  $\xi^*(\mathcal{L} \star \mathcal{L}) = \mathcal{L}^2 \star \mathcal{L}^2$  where  $\mathcal{L} \star \mathcal{M} := p_1^* \mathcal{L} \otimes p_2^* \mathcal{M}$ .

**Proposition 5.2.** *For the natural product theta structure, the isogeny theorem applied to  $\xi$  yields*

$$\vartheta_{i+j}^{\mathcal{L}}(x+y)\vartheta_{i-j}^{\mathcal{L}}(x-y) = \sum_{t \in K_1(\mathcal{L})[2]} \vartheta_{i+t}^{\mathcal{L}^2} \vartheta_{j+t}^{\mathcal{L}^2}.$$

*This formula is easily invertible if we do a Fourier transform: for  $\chi \in \hat{Z}(\bar{2})$  and  $i \in Z(2n)$ , let  $U_{\chi,i}^{\mathcal{L}} = \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i+t}^{\mathcal{L}^2}$ . Then we obtain the duplication formulae*

$$\begin{aligned} \vartheta_{i+j}^{\mathcal{L}}(x+y)\vartheta_{i-j}^{\mathcal{L}}(x-y) &= \frac{1}{2g} \sum_{\chi \in \hat{Z}(\bar{2})} U_{\chi,i}^{\mathcal{L}^2}(x) U_{\chi,j}^{\mathcal{L}^2}(y) \\ U_{\chi,i}^{\mathcal{L}^2}(x) U_{\chi,j}^{\mathcal{L}^2}(y) &= \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i+j+t}^{\mathcal{L}}(x+y) \vartheta_{i-j+t}^{\mathcal{L}}(x-y) \end{aligned}$$

**Remark 5.3.** In term of analytic theta functions, we have  $\vartheta_i^{\mathcal{L}}(z) = \vartheta \left[ \begin{smallmatrix} 0 \\ i/l \end{smallmatrix} \right] (z, \frac{\Omega}{\ell})$ ,  $\vartheta_i^{\mathcal{L}^2}(z) = \vartheta \left[ \begin{smallmatrix} 0 \\ i/2l \end{smallmatrix} \right] (z, \frac{\Omega}{2\ell})$ ,  $U_{\chi,i}^{\mathcal{L}^2}(z) = \vartheta \left[ \begin{smallmatrix} \chi/2 \\ i/l \end{smallmatrix} \right] (2z, \frac{2\Omega}{\ell})$ .

**Theorem 5.4** (Riemann relations). *Let  $x_1, x_2, x_3, x_4, z \in \mathbb{C}^g$ , such that  $2z = x_1 + x_2 + x_3 + x_4$  and let  $y_1 = z - x_1, y_2 = z - x_2, y_3 = z - x_3, y_4 = z - x_4$ . Then for all characters  $\chi \in \hat{Z}(\bar{2})$  and all  $i_1, i_2, i_3, i_4, m \in Z(\bar{n})$  such that  $i_1 + i_2 + i_3 + i_4 = 2m$ , if  $j_1 = m - i_1, j_2 = m - i_2, j_3 = m - i_3, j_4 = m - i_4$  then*

$$(1) \quad \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i_1+t}(x_1) \vartheta_{i_2+t}(x_2) \right) \cdot \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i_3+t}(x_3) \vartheta_{i_4+t}(x_4) \right) = \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{j_1+t}(y_1) \vartheta_{j_2+t}(y_2) \right) \cdot \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{j_3+t}(y_3) \vartheta_{j_4+t}(y_4) \right).$$

*In particular, we have the addition formulae for  $z_1, z_2 \in \mathbb{C}^g$  (with  $\chi, i_1, i_2, i_3, i_4$  like before):*

$$(2) \quad \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i_1+t}(z_1 + z_2) \vartheta_{i_2+t}(z_1 - z_2) \right) \cdot \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i_3+t}(0) \vartheta_{i_4+t}(0) \right) = \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{j_1+t}(z_2) \vartheta_{j_2+t}(z_2) \right) \cdot \left( \sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{j_3+t}(z_1) \vartheta_{j_4+t}(z_1) \right).$$

*Proof.* Using the duplication formulae the left term of eq. (1) is equal to  $U_{\chi,m_1}(z_1)U_{\chi,m_2}(z_2)U_{\chi,m_3}(z_3)U_{\chi,m_4}(z_4)$  while the right term is equal to  $U_{\chi,m_1}(z_1)U_{\chi,m_4}(z_4)U_{\chi,m_3}(z_3)U_{\chi,m_2}(z_2)$  where  $z_1 = \frac{x_1+x_2}{2}, z_2 = \frac{x_1-x_2}{2}, z_3 = \frac{x_3+x_4}{2}, z_4 = \frac{x_3-x_4}{2}$  and  $m_1 = \frac{i_1+i_2}{2}, m_2 = \frac{i_1-i_2}{2}, m_3 = \frac{i_3+i_4}{2}, m_4 = \frac{i_3-i_4}{2}$ .

The differential addition comes by plugging

$$z_1 + z_2, z_1 - z_2, 0, 0 \mid -z_2, z_2, z_1, z_1$$

another useful application is the three way affine addition with

$$z_1 + z_2 + z_3, z_1, z_2, z_3 \mid 0, z_2 + z_3, z_1 + z_3, z_1 + z_2.$$

□

**Question:** For  $\chi, i_1$  and  $i_2$ , we need to find  $i_3, i_4$  such that

$$\sum \chi(t) \vartheta_{i_3+t}^{\mathcal{L}}(0) \vartheta_{i_4+t}^{\mathcal{L}}(0) = U_{\chi, \frac{i_3+i_4}{2}}^{\mathcal{L}^2}(0) U_{\chi, \frac{i_3-i_4}{2}}^{\mathcal{L}^2}(0)$$

is not null. Then by eq. (2) we can recover all  $\sum_{t \in Z(\bar{2})} \chi(t) \vartheta_{i_1+t}^{\mathcal{L}}(z_1 + z_2) \vartheta_{i_2+t}^{\mathcal{L}}(z_1 - z_2)$  and by doing appropriate sums of characters we recover all products  $\vartheta_{i_1}^{\mathcal{L}}(z_1 + z_2) \vartheta_{i_2}^{\mathcal{L}}(z_1 - z_2)$ . This is needed for

projective addition or affine differential additions. Remark: we can translate  $m_3 = \frac{i_3+i_4}{2}$  and  $m_4 = \frac{i_3-i_4}{2}$  by  $t_1, t_2$  in  $2Z(2n)$ .

**Example 5.5.** Using  $n = 2$  and analytic theta functions for visibility, the duplication formulae above are given by

$$\begin{aligned} \vartheta \begin{bmatrix} 0 \\ i/2 \end{bmatrix} (z_1 + z_2, \Omega/2) \vartheta \begin{bmatrix} 0 \\ j/2 \end{bmatrix} (z_1 - z_2, \Omega/2) &= \sum_{t \in \frac{1}{2}\mathbb{Z}^g / \mathbb{Z}^g} \vartheta \begin{bmatrix} \frac{t}{2} \\ \frac{i+j}{n} \end{bmatrix} (2z_1, \Omega) \vartheta \begin{bmatrix} \frac{t}{2} \\ \frac{i-j}{n} \end{bmatrix} (2z_2, \Omega) \\ \vartheta \begin{bmatrix} \chi/2 \\ i/2 \end{bmatrix} (2z_1, \Omega) \vartheta \begin{bmatrix} \chi/2 \\ j/2 \end{bmatrix} (2z_2, \Omega) &= \\ \frac{1}{2^g} \sum_{t \in \frac{1}{2}\mathbb{Z}^g / \mathbb{Z}^g} e^{-2i\pi t \chi \cdot t} \vartheta \begin{bmatrix} 2\chi \\ \frac{i+j}{4} + t \end{bmatrix} (z_1 + z_2, \Omega/2) \vartheta \begin{bmatrix} 0 \\ \frac{i-j}{4} + t \end{bmatrix} (z_1 - z_2, \Omega/2). \end{aligned}$$

To compute the addition law, given  $\chi, i_1, i_2$  we need to find  $i_3, i_4$  such that

$$\vartheta \begin{bmatrix} \frac{\chi}{2} \\ \frac{i_3+i_4}{2} \end{bmatrix} (0, \Omega) \vartheta \begin{bmatrix} \frac{\chi}{2} \\ \frac{i_3-i_4}{2} \end{bmatrix} (0, \Omega) \neq 0.$$

**5.3. Multiplication map.** Let  $m : A \rightarrow A \times A, x \mapsto (x, x)$  which induces the multiplication map  $m^* : \Gamma(A, \mathcal{L}) \otimes \Gamma(A, \mathcal{L}) \rightarrow \Gamma(A, \mathcal{L}^2)$ .

The following diagram show that  $m^* = S^* \xi^*$ .

$$\begin{array}{ccc} (X, \mathcal{L}^2) & & \\ S \downarrow & \searrow m & \\ (X \times X, \mathcal{L}^2 \star \mathcal{L}^2) & \xrightarrow{\xi} & (X \times X, \mathcal{L} \star \mathcal{L}). \end{array}$$

By the duplication formulae,  $m^*$  is then given by  $\vartheta_i^{\mathcal{L}} \otimes \vartheta_j^{\mathcal{L}} \mapsto \sum_{\chi \in \hat{Z}(\bar{2})} U_{\chi, u}^{\mathcal{L}^2} U_{\chi, v}^{\mathcal{L}^2}(0)$  for any  $u, v \in Z(2n)$  such that  $i = u+v, j = u-v$ , or via a change of variable  $\sum_t \chi(t) \vartheta_{u+v+t}^{\mathcal{L}}(x) \otimes \vartheta_{u-v+t}^{\mathcal{L}}(x) \mapsto U_{\chi, i}^{\mathcal{L}^2}(x) U_{\chi, j}^{\mathcal{L}^2}(0)$ . So the rank of the multiplication map is closely linked to the non annulation of the theta null points.

**Remark 5.6** (Even and odd theta null points). If  $n = 2$ ,  $U_{\chi, i}(-x) = \chi(2i) U_{\chi, i}(x)$  for  $i \in Z(\bar{4})$ , equivalently  $\vartheta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (-2z, \Omega) = (-1)^{a \cdot b} \vartheta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (2z, \Omega)$ . There is  $2^{g-1}(2^g + 1)$  even theta null points vs  $2^{g-1}(2^g - 1)$  odd theta null points. Ex:  $g = 1, 3$  vs  $1$ ;  $g = 2, 10$  vs  $6$ ;  $g = 3, 36$  vs  $28$ .

**Theorem 5.7** (Mumford-Koizumi-Kempf).  $\mathcal{L}_0$  is principal symmetric.

- $\Gamma(A, \mathcal{L}_0^n) \otimes \Gamma(A, \mathcal{L}_0^m) \rightarrow \Gamma(A, \mathcal{L}_0^{n+m})$  is surjective when  $n \geq 2$  and  $m \geq 3$ .
- $\Gamma(A, \mathcal{L}_0^{2n})^+ \otimes \Gamma(A, \mathcal{L}_0^2) \rightarrow \Gamma(A, \mathcal{L}_0^{2(n+1)})^+$  is surjective when  $n \geq 2$ . Here  $\Gamma(A, \mathcal{L}_0^{2n})^+$  denotes the even sections of  $\Gamma(A, \mathcal{L}_0^{2n})$ . Equivalently, since  $\mathcal{L}_0^{2n}$  is totally symmetric, it descends to an ample line bundle  $\mathcal{M}^+$  on the Kummer variety  $\mathcal{K}_A = A/\pm 1$ , and  $\Gamma(A, \mathcal{L}_0^{2n})^+ = \Gamma(\mathcal{K}_A, \mathcal{M}^+)$ .
- The rank of  $\Gamma(A, \mathcal{L}_0^2) \otimes \Gamma(A, \mathcal{L}_0^2) \rightarrow \Gamma(A, \mathcal{L}_0^4)^+$  is equal to the number of non null even theta null points.

**5.4. Normal projectivity.** A line bundle  $\mathcal{L}$  on a variety  $X$  is projectively normal if  $\Gamma(X, \mathcal{L}^n) \otimes \Gamma(X, \mathcal{L}) \rightarrow \Gamma(X, \mathcal{L}^{n+1})$  is surjective for all  $n$  or equivalently if  $S(\Gamma(X, \mathcal{L})) \rightarrow \bigoplus_{n>0} \Gamma(X, \mathcal{L}^n)$ . (And so if  $X$  is normal, its projective homogeneous ring in the embedding given by  $\mathcal{L}$  is normal). Remark:  $\mathcal{L}$  is very ample iff the map above is surjective for  $n \gg 0$ .

**Corollary 5.8.**

- If  $n \geq 3$ ,  $(A, \mathcal{L})$  is projectively normal, and we have a projective embedding of  $A$ ;
- If  $n = 2$ , the projective embedding of  $\mathcal{K}_A$  is projectively normal iff the even theta null points are not null. **We now assume that this is the case whenever  $n = 2$ .**

**Example 5.9.** The product of the even theta null points is null whenever  $A$  is not absolutely simple or when it is the Jacobian of an hyperelliptic curve of genus  $g \geq 3$ .

5.5. **Addition, Differential addition.** Given  $\vartheta_i(x), \vartheta_i(y)$  we can recover ( $n$  even)

- $\vartheta_i(x+y)\vartheta_j(x-y)$  when  $n > 2$  ( $\Rightarrow$  projective addition, affine differential addition)
- $\kappa_{ij} := \vartheta_i(x+y)\vartheta_j(x-y) + \vartheta_j(x+y)\vartheta_i(x-y)$  if  $n = 2$ , the “symmetric sum” ( $\Rightarrow$  differential projective or affine addition).

**Algorithm 5.10.** Differential addition with  $g = 1, n = 2$ .

**Input:**  $z_P = (x_0, x_1), z_Q = (y_0, y_1)$  and  $z_{P-Q} = (z_0, z_1)$  with  $z_0 z_1 \neq 0$ ;  $z_0 = (a, b)$  and  $A = 2(a^2 + b^2), B = 2(a^2 - b^2)$ .

**Output:**  $z_{P+Q} = (t_0, t_1)$ .

- (1)  $t'_0 = (x_0^2 + x_1^2)(y_0^2 + y_1^2)/A$
- (2)  $t'_1 = (x_0^2 - x_1^2)(y_0^2 - y_1^2)/B$
- (3)  $t_0 = (t'_0 + t'_1)/z_0$
- (4)  $t_1 = (t'_0 - t'_1)/z_1$

Return  $(t_0, t_1)$

Cost:  $3M+6S+3m_0$  for a step of the scalar ladder, compared to  $5M+4S+1m_0$  for the Montgomery model. In genus 2 the cost of one step is  $7M+12S+9m_0$ .

## 6. ARITHMETIC ON KUMMER VARIETIES

We assume here that  $n = 2$  and that the even theta null points are non zero.

The polynomial  $P_{i\alpha} := X^2 - 2\frac{\kappa_{i\alpha}}{\kappa_{\alpha\alpha}}X + \frac{\kappa_{ii}}{\kappa_{\alpha\alpha}}$  has for roots  $\{\frac{\vartheta_i(x+y)}{\vartheta_\alpha(x+y)}, \frac{\vartheta_i(x-y)}{\vartheta_\alpha(x-y)}\}$ . Once a root is chosen, some two by two linear equations involving the  $\kappa_{ij}$  and the roots allows to recover the theta coordinates of  $x+y$ . This gives equations for the degree two scheme  $\{x+y, x-y\}$ .

**Lemma 6.1** (Compatible additions). *Given  $x, y, z, t \in A(\bar{k})$  such that  $x+y = z+t$  but  $x-y \neq \pm z-t$  then one can compute  $x+y (= z+t)$  on the Kummer (from the points on the Kummer).*

*Proof.* This is just the intersection of the two schemes of degree two defining  $\{x \pm y\}$  and  $\{z \pm t\}$ ; in practice this is just a gcd of two degree two polynomials.  $\square$

**Proposition 6.2** (Multiway additions). *Let  $\pm P_0 \in \mathcal{K}_A(\bar{k})$  be a point not of 2-torsion. Then from  $\pm P_1, \dots, \pm P_n \in \mathcal{K}_A(\bar{k})$  and  $\pm(P_0 + P_1), \dots, \pm(P_0 + P_n) \in \mathcal{K}_A(\bar{k})$ , one can compute  $\pm(P_1 + \dots + P_n)$  and  $\pm(P_0 + P_1 + \dots + P_n)$ .*

**Remark 6.3.** A reformulation of the proposition is that the data of  $P_0 + P_i \in \mathcal{K}_A(\bar{k})$  “fixes” the sign of  $P_i$  relatively to the one of  $P_0$ , and so we can compute the additions since we have “compatible” signs.

*Proof.* This reduces to the case  $n = 2$ , which uses (in the generic case)  $(P_1) + (P_2) = (P_1 - P_0) + (P_2 + P_0)$  and  $(P_0 + P_1) + P_2 = P_1 + (P_0 + P_2)$ . And a verification shows that in the non generic case a direct computation is possible.  $\square$

**6.1. Multi Scalar multiplication.** To speed up the scalar multiplication  $P \mapsto nP$ , the GLV trick [GLV01] is to use an endomorphism  $\alpha$  and reduces the scalar multiplication to a multi scalar multiplication  $m_1 P_1 + m_2 P_2$  (for instance if  $\alpha P = tP$ , fix  $P_1 = P, P_2 = \alpha(P)$ , and  $n = m_1 + tm_2$ ). The doubling and add method works again, with the addition being either  $P_1, P_2$  or  $P_1 + P_2$  according to the bits of  $(m_1, m_2)$ .

On the Kummer variety a Montgomery ladder  $mP, (m+1)P \mapsto 2mP, (2m+1)P$  or  $(2m+1)P, (2m+2)P$  computes the scalar multiplication. The two dimensional scalar multiplication uses a square  $\pm(mP + nQ), \pm((m+1)P + nQ), \pm(mP + (n+1)Q), \pm((m+1)P + (n+1)Q)$  and depending whether the current bits of  $(m_1, m_2)$  is  $(0, 0), (1, 0), (0, 1)$  or  $(1, 1)$ , adds  $\pm(mP + nQ), \pm((m+1)P + nQ), \pm(mP + (n+1)Q)$  or  $\pm((m+1)P + (n+1)Q)$  to the four points. But this is not interesting, we expect to halve the length of the chain by two, but each steps is twice as costly. A better approach from [Ber06] uses a triangle.

But via the compatible additions, we just need to keep two points!

**Example 6.4.** Given  $m_1 P_1 + (m_2 + 1)P_2, (m_1 + 1)P_1 + m_2 P_2$ , we can compute  $(2m_1 + 1)P_1 + (2m_2 + 1)P_2 = (m_1 P_1 + (m_2 + 1)P_2) + (P_1) = ((m_1 + 1)P_1 + m_2 P_2) + (P_2)$ .



## 7. CHANGING LEVEL

For an elliptic curve  $y^2 = f(x)$ , the map  $(x, y) \mapsto x$  maps the elliptic curve to the Kummer line. Going back to the elliptic curve involve a square root. For abelian variety, a similar map to the Kummer is  $(A, \mathcal{L}^2)$  level 4  $\rightarrow (\mathcal{K}_A, \mathcal{L}^+)$  level 2 via the duplication formula. We want to go back from level 2 to level 4, using only one square root. We would also like to be able to describe a point on  $A$  using just the point on  $\mathcal{K}_A$  and an extra coordinate to encode the sign, like is possible on elliptic curve (going back to the full level 4 adds a lot of coordinates). This will be described in section 8

The theta constants of level 4 on  $A$  gives the points of 4 torsion, so we have the coordinates  $U_{\chi,i}^{\mathcal{L}^2}(T)$  for  $T$  a point of four torsion. The duplication formulae gives  $U_{\chi,i}(x)U_{\chi,i}(0) = \sum \chi(t)\vartheta_{2i+t}(x)\vartheta_t(x)$ , but  $U_{\chi,i}(0) = 0$  for odd coordinates, so we don't recover all level 4 coordinates given the level 2 ones. But  $0 \neq U_{\chi,0}(0) = U_{\chi,i}(T_i)$  for an (explicit) point of four torsion  $T$ . So we can use  $U_{\chi,i}(x)U_{\chi,i}(T_i) = \sum \chi(t)\vartheta_{2i+t}(x+T_i)\vartheta_t(x-T_i)$ .

We thus need to compute  $x + T_i$  via a square roots, then we can recover all the other ones via  $x + T_j = (x + T_i) + (T_i - T_j)$ .

**7.1. Compressing coordinates.** Another way to descend level is via the isogeny theorem:

$$\pi(\vartheta_i(x))_{i \in Z(\ell n)} \rightarrow (\vartheta_i(x))_{i \in Z(\bar{n})}$$

is the isogeny of kernel  $K_2(\mathcal{L})[\ell]$ .

*Proof.* The isogeny sends  $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) \rightarrow \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{\ell}\mathbb{Z}^g)$ . Looking at the level  $\ell n$  and  $n$  theta functions we indeed have for  $b \in Z(\bar{n})$   $\vartheta \left[ \begin{smallmatrix} 0 \\ b/\ell n \end{smallmatrix} \right] \left( z, \frac{\Omega}{\ell n} \right) = \vartheta \left[ \begin{smallmatrix} 0 \\ b/n \end{smallmatrix} \right] \left( z, \frac{\Omega/\ell}{n} \right)$ .  $\square$

Let  $e_1, \dots, e_g$  be a basis of  $K_1(\mathcal{L})$ . Then from  $\tilde{\pi}(x + \sum \lambda_i e_i)$ , where  $\lambda_i \in \{0, \dots, \ell - 1\}$  we can recover  $x$  (here  $\tilde{\pi}$  is the affine lift of  $\pi$ ).

**Example 7.1.**  $g = 1, \ell = 3, n = 2$ .  $\tilde{\pi}(x_0, \dots, x_5) = (x_0, x_3)$ .  $x + e_1 = (x_1, \dots, x_5, x_0)$  so  $\tilde{\pi}(x + e_1) = (x_1, x_4)$  and  $\tilde{\pi}(x + 2e_1) = (x_2, x_5)$ .

But  $\tilde{\pi}(x + \sum \lambda_i e_i) = \tilde{\pi}(x) + \sum \lambda_i \tilde{\pi}(e_i)$  so we can recover everything using multiway affine additions (which are just a composition of differential and three way affine additions).

**Corollary 7.2.**

- 0 is uniquely determined by  $\tilde{\pi}(0)$ ,  $\tilde{\pi}(e_i)$  and  $\tilde{\pi}(e_i + e_j)$   $((1 + g + g(g + 1)/2)n^g$  coordinates).
- $x$  is uniquely determined by  $\tilde{\pi}(x)$ ,  $\tilde{\pi}(x + e_i)$   $((1 + g)n^g$  coordinates).

## 8. ARITHMETIC ON ABELIAN VARIETIES

**Level (2, 4):** this gives an embedding of  $A$  (if  $A$  is absolutely simple), and the compression of coordinates from above show that we can use the coordinates  $\tilde{\pi}(x)$ ,  $\tilde{\pi}(x + T) = \tilde{\pi}(x) + \tilde{\pi}(T)$  where  $T$  is of 4-torsion.

More generally, for  $T \in A(\bar{k})$  such that  $2T \neq 0$ , we represent  $x \in A(\bar{k})$  by  $x \in \mathcal{K}_A(x)$ ,  $x + T \in \mathcal{K}_A$ . Addition:  $(x, x + T) + (y, y + T) = (x + y = (x + T) + (y - T), x + y + T)$  (this is a three way addition and a compatible addition on the Kummer so this is quite costly). Doubling is just a doubling and a differential addition on the Kummer so this is a lot less costly.

The standard scalar multiplication costs too much because of the additions. One can instead do a Montgomery scalar multiplication with  $(nx, (n + 1)x, (n + 1)x + T)$  which uses a doubling and two differential additions on the Kummer at each step.

Even better, just do a Montgomery scalar multiplication  $(nx, (n + 1)x)$  on the Kummer and at the last step compute  $(n + 1)x + T = nx + (x + T)$ . This also works for multi-exponentiation.

Finally this representation is very compact,  $x + T$  is simply represented by a root of the polynomial  $P_{i\alpha}$ . So we have a representation that only needs one extra coordinate compared to the Kummer one, and has a scalar multiplication (almost) as efficient, but we can still compute additions.

**Remark 8.1.** Changing representation:  $(x, x + T_1) \mapsto (x, x + T_2)$  via  $x + T_2 = (x + T_1) + (T_2 - T_1)$ . This needs a choice of  $T_1 + T_2$  in  $\{\pm T_1 \pm T_2\}$ , but this choice is necessary since  $[-1]$  is an automorphism.

$$\begin{array}{ccc}
& A & \\
& \searrow & \\
[-1] \downarrow & & \mathcal{K}_A \\
& \nearrow & \\
& A &
\end{array}$$

## 9. FORMULAE

Let  $(a_i)_{i \in Z(\bar{2})}$  be the level two theta null point representing a Kummer variety  $\mathcal{K}_A$  of dimension 2. Let  $x = (x_i)_{i \in Z(\bar{2})}$  and  $y = (y_i)_{i \in Z(\bar{2})}$ , we let  $X = x + y$  and  $Y = x - y$ . We will give formulae for the coordinates  $2\kappa_{ij} = X_i Y_j + X_j Y_i$ .

Let  $i \in Z(\bar{2}), \chi \in \hat{Z}(\bar{2})$  and let

$$z_i^\chi = \left( \sum_{t \in Z(\bar{2})} \chi(t) x_{i+t} x_t \right) \left( \sum_{t \in Z(\bar{2})} \chi(t) y_{i+t} y_t \right) / \left( \sum_{t \in Z(\bar{2})} \chi(t) a_{i+t} a_t \right).$$

$\sum_t \chi(t) a_{i+t} a_t$  is simply the classical theta null point  $\vartheta \left[ \begin{smallmatrix} \chi/2 \\ i/2 \end{smallmatrix} \right] (0, \Omega)^2$ . Then theorem 5.4 gives

$$\begin{aligned}
4X_{00}Y_{00} &= z_{00}^{00} + z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\
4X_{01}Y_{01} &= z_{00}^{00} - z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\
4X_{10}Y_{10} &= z_{00}^{00} + z_{00}^{01} - z_{00}^{10} - z_{00}^{11}; \\
4X_{11}Y_{11} &= z_{00}^{00} - z_{00}^{01} - z_{00}^{10} + z_{00}^{11};
\end{aligned}$$

$$\begin{aligned}
2(X_{10}Y_{00} + X_{00}Y_{10}) &= z_{10}^{00} + z_{10}^{01}; \\
2(X_{11}Y_{01} + X_{01}Y_{11}) &= z_{10}^{00} - z_{10}^{01}; \\
2(X_{01}Y_{00} + X_{00}Y_{01}) &= z_{01}^{00} + z_{01}^{10}; \\
2(X_{11}Y_{10} + X_{10}Y_{11}) &= z_{01}^{00} - z_{01}^{10}; \\
2(X_{11}Y_{00} + X_{00}Y_{11}) &= z_{11}^{00} + z_{11}^{11}; \\
2(X_{01}Y_{10} + X_{10}Y_{01}) &= z_{11}^{00} - z_{11}^{11};
\end{aligned}$$

We describe the degree two scheme  $\{X, Y\}$  by the polynomial  $\mathfrak{P}_\alpha(Z) = Z^2 - 2\frac{\kappa_{\alpha 0}}{\kappa_{00}}Z + \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}$  whose roots are  $\{\frac{X_\alpha}{X_0}, \frac{Y_\alpha}{Y_0}\}$  (where  $\alpha$  is such that  $X_\alpha Y_0 - X_0 Y_\alpha \neq 0$ ). To compute  $\kappa_{00}$  and  $\kappa_{\alpha\alpha}$  we need  $4M + 8S + 3M_0$ , and to compute  $\kappa_{\alpha 0}$  we need  $2M + 4S + 2M_0$ ; so in total to compute  $\mathfrak{P}_\alpha$ , we need  $6M + 12S + 5M_0 + 2I$ .

Once we have a root  $Z$ , if we let  $Z' = 2\frac{\kappa_{\alpha 0}}{\kappa_{00}} - Z$  be the conjugate root (corresponding to  $\frac{Y_\alpha}{Y_0}$ ), we can recover the coordinates  $X_i, Y_i$  by solving the equation

$$\begin{pmatrix} 1 & 1 \\ Z & Z' \end{pmatrix} \begin{pmatrix} Y_i/Y_0 \\ X_i/X_0 \end{pmatrix} = \begin{pmatrix} 2\kappa_{0i}/\kappa_{00} \\ 2\kappa_{\alpha i}/\kappa_{00} \end{pmatrix};$$

We find  $X_i = \frac{2(Z\kappa_{0i} - \kappa_{\alpha i})}{\kappa_{00}(Z - Z')} = \frac{Z\kappa_{0i} - \kappa_{\alpha i}}{Z\kappa_{00} - \kappa_{\alpha 0}}$  for  $i \neq 0, \alpha$  (here we have  $X_0 = 1, X_\alpha = Z$ ). But usually we will express  $Z = (X_0 : X_\alpha) \in \mathbb{P}^1$  as a point in the projective line, and we find that

$$X_i = \frac{X_\alpha \kappa_{0i} - X_0 \kappa_{\alpha i}}{X_\alpha \kappa_{00} - X_0 \kappa_{\alpha 0}}.$$

Recovering the projective coordinates of  $X$  then costs  $8M$  (given the  $\kappa_{ij}$ ). To sum up, given  $Z = (X_0 : X_\alpha)$  recovering  $X$  costs in total  $(10M + 20S + 9M_0) + 8M = 18M + 20S + 9M_0$ .

For a compatible addition, where  $x + y = z + t$ , we can find  $Z$  as the common root between  $\mathfrak{P}_\alpha$  and the similar polynomial  $\mathfrak{P}'_\alpha(Z) = Z^2 - 2\frac{\kappa'_{\alpha 0}}{\kappa'_{00}}Z + \frac{\kappa'_{\alpha\alpha}}{\kappa'_{00}}$  coming from the symmetric coordinates  $z_i t_j + t_i z_j$ . Computing the coefficients needed for  $\mathfrak{P}'_\alpha$  costs  $6M + 12S + 5M_0$ . The common root is

$$Z = \frac{\frac{\kappa'_{\alpha\alpha}}{\kappa'_{00}} - \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}}{-2\frac{\kappa_{\alpha 0}}{\kappa_{00}} + 2\frac{\kappa'_{\alpha 0}}{\kappa'_{00}}} = \frac{\kappa'_{\alpha\alpha}\kappa_{00} - \kappa_{\alpha\alpha}\kappa'_{00}}{2(\kappa'_{\alpha 0}\kappa_{00} - \kappa_{\alpha 0}\kappa'_{00})}.$$

Computing  $Z$  projectively costs  $4M$ . In the end, a compatible addition costs  $(18M + 20S + 9M_0) + (6M + 12S + 5M_0) + 4M = 28M + 32S + 14M_0$ .

## REFERENCES

- [Ber06] D. J. Bernstein. “Differential addition chains”. 2006. URL: <http://cr.yyp.to/ecdh/diffchain-20060219.pdf> (cit. on p. 8).
- [BL07] D. Bernstein and T. Lange. *Explicit-formulas database*. 2007. URL: <http://hyperelliptic.org/EFD>.
- [GLV01] R. P. Gallant, R. J. Lambert, and S. A. Vanstone. “Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms”. In: *CRYPTO*. Ed. by J. Kilian. Vol. 2139. Lecture Notes in Computer Science. Springer, 2001, pp. 190–200. ISBN: 3-540-42456-3 (cit. on p. 8).
- [HC14] H. Hisil and C. Costello. “Jacobian Coordinates on Genus 2 Curves”. 2014. eprint: [2014/385](https://arxiv.org/abs/2014/385) (cit. on p. 3).
- [Lan05] T. Lange. “Formulae for arithmetic on genus 2 hyperelliptic curves”. In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328 (cit. on p. 3).
- [LR14] D. Lubicz and D. Robert. “Arithmetic on Abelian and Kummer Varieties”. June 2014. URL: <http://www.normalesup.org/~robert/pro/publications/articles/arithmetric.pdf>. HAL: [hal-01057467](https://hal.archives-ouvertes.fr/hal-01057467), eprint: [2014/493](https://arxiv.org/abs/2014/493). (Cit. on p. 1).
- [Mum66] D. Mumford. “On the equations defining abelian varieties. I”. In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on p. 5).
- [Mum91] D. Mumford. *Tata lectures on theta III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA: Birkhäuser Boston Inc., 1991, pp. viii+202. ISBN: 0-8176-3440-1 (cit. on p. 5).

INRIA BORDEAUX-SUD-OUEST, 200 AVENUE DE LA VIEILLE TOUR, 33405 TALENCE CEDEX FRANCE  
 E-mail address: [damien.robert@inria.fr](mailto:damien.robert@inria.fr)  
 URL: <http://www.normalesup.org/~robert/>