Arithmetic on Abelian and Kummer varieties

Notes of a talk given for the Number Theory Seminar — Caen.
Based on an earlier talk given on April 2014 in Grenoble.

Abstract. In this talk we give an outline of the results obtained in [LR14]. The first part is a review of the algebraic theory of theta functions, and on the multiplication map. The much more elementary second part use the geometric results from the first 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!

Contents

1. Complex abelian varieties

$A = (V/\Lambda, H)$ where V is a $\mathbb{C}$-ev of dimension g, Λ 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 Ω symmetric, $\Im\Omega > 0$), Ω determines a principal polarisation $H_0 = (\Im\Omega)^{-1}$.

Definition 1.1 (Theta functions with characteristics $a, b \in \mathbb{Q}^g$)**.**

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

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

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

Date: 2014-12-17.

Theorem 1.2 (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 $\vartheta\begin{bmatrix} a/n_1 \\ b/n_2 \end{bmatrix}(n_1 z, \frac{n_1}{n_2}\Omega)$. 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 1.3 (Lefschetz)**.**

- *If* $n \geqslant 3$ *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* $A/\pm 1$*;*

2. 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 $\Phi_{\mathcal{L}} : A \to \widehat{A}_k, x \mapsto \tau_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ 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: $(y,\psi).(x,\varphi) = (x+y, \tau_x^*\psi \circ \varphi)$:

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

- The theta group fits into the exact sequence

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

- The commutator pairing $e_{\mathcal{L}}(x,y) = \widetilde{x}\widetilde{y}\widetilde{x}^{-1}\widetilde{y} \in k^*$ is non degenerate (Weil pairing), so $G(\mathcal{L})$ is an Heisenberg group. If $\psi : K(\mathcal{L})^2 \to k^*$ 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 2.1 (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, $f : A \to B = A/K$ 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 2.2. *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 $\Gamma(\mathcal{L}) \curvearrowleft G(\mathcal{L})$ is isomorphic to $V(n) \curvearrowleft G(n)$ (where $G(n)$ acts by the standard action) via $\Theta_{\mathcal{L}}$.

Explicitly if we note $Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$, $V(n) = \mathrm{Hom}(Z(\overline{n}), k)$, $(\alpha, x_1, x_2).f = y \mapsto \alpha x_2(y) f(x_1 + y)$. 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, ϑ_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.

3. Riemann relations

3.1. The Isogeny theorem.

Theorem 3.1 (Isogeny Theorem)**.** *Let $f : (A, \mathcal{L}) \to (B, \mathcal{M})$ be an isogeny between polarised abelian varieties, $\mathcal{M}$ corresponds to a section $\widetilde{K} \subset G(\mathcal{L})$ of the kernel $K = \mathrm{Ker}\, f$. $G(\mathcal{M}) = \widetilde{K}^{\perp}/\widetilde{K}$ 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 $K = K_1 \bigcap K \oplus K_2 \bigcap K$). Likewise the theta structure on $G(\mathcal{L})$ induces a compatible theta structure on $G(\mathcal{M})$. We then have for $i \in K_1(\mathcal{L}) \bigcap K^{\perp}$ (up to a constant)*

$$\vartheta^{\mathcal{M}}_{f(i)} = \sum_{j - i \in K \bigcap K_1(\mathcal{L})} \vartheta^{\mathcal{L}}_j = \sum_{j \in K_1(\mathcal{L}), f(j) = i} \vartheta^{\mathcal{L}}_j = \text{Trace of } \vartheta^{\mathcal{L}}_i \text{ under the action of } \widetilde{K}.$$

3.2. **Riemann relations.** Let $\xi : A \times A \to A \times A, (x, y) \mapsto (x + y, x - y)$ be the isogeny coming from the group law, with kernel $\mathrm{diag}\, A[2]$. 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 3.2. *For the natural product theta structure, the isogeny theorem applied to ξ yields*

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

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

$$\vartheta^{\mathcal{L}}_{i+j}(x + y)\vartheta^{\mathcal{L}}_{i-j}(x - y) = \frac{1}{2^g} \sum_{\chi \in \hat{Z}(\overline{2})} U^{\mathcal{L}^2}_{\chi,i}(x) U^{\mathcal{L}^2}_{\chi,j}(y)$$

$$U^{\mathcal{L}^2}_{\chi,i}(x) U^{\mathcal{L}^2}_{\chi,j}(y) = \sum_{t \in Z(\overline{2})} \chi(t)\vartheta^{\mathcal{L}}_{i+j+t}(x + y)\vartheta^{\mathcal{L}}_{i-j+t}(x - y)$$

Remark 3.3. In term of analytic theta functions, we have $\vartheta^{\mathcal{L}}_i(z) = \vartheta\left[\begin{smallmatrix} 0 \\ i/l \end{smallmatrix}\right](z, \frac{\Omega}{\ell})$, $\vartheta^{\mathcal{L}^2}_i(z) = \vartheta\left[\begin{smallmatrix} 0 \\ i/2l \end{smallmatrix}\right](z, \frac{\Omega}{2\ell})$, $U^{\mathcal{L}^2}_{\chi,i(z)} = \vartheta\left[\begin{smallmatrix} \chi/2 \\ i/l \end{smallmatrix}\right](2z, \frac{2\Omega}{\ell})$.

Theorem 3.4 (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 $y_1 = z - x_1$, $y_2 = z - x_2$, $y_3 = z - x_3$, $y_4 = z - y_4$. Then for all characters $\chi \in \hat{Z}(\overline{2})$ and all $i_1, i_2, i_3, i_4, m \in Z(\overline{n})$ such that $i_1 + i_2 + i_3 + i_4 = 2m$, if $j_1 = m - i_1$, $j_2 = m - j_2$, $j_3 = m - i_3$, $j_4 = m - i_4$ then*

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

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

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

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 χ, i_1 and i_2, we need to find i_3, j_4 such that

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

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

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

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

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

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

Remark 3.5 (Even and odd theta null points)**.** If $n = 2$, $U_{\chi,i}(-x) = \chi(2i)U_{\chi,i}(x)$ for $i \in Z(\overline{4})$, equivalently $\vartheta\begin{bmatrix} a/2 \\ b/2 \end{bmatrix}(-2z, \Omega) = (-1)^{{}^t a\cdot b}\vartheta(2z, \Omega)$. 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 3.6 (Mumford-Koizumi-Kempf)**.** *$\mathcal{L}_0$ is principal symmetric.*

- *$\Gamma(A, \mathcal{L}_0^n) \otimes \Gamma(A, \mathcal{L}_0^m) \to \Gamma(A, \mathcal{L}_0^{n+m})$ is surjective when $n \geqslant 2$ and $m \geqslant 3$.*
- *$\Gamma(A, \mathcal{L}_0^{2n})^+ \otimes \Gamma(A, \mathcal{L}_0^2) \to \Gamma(A, \mathcal{L}_0^{2(n+1)})^+$ is surjective when $n \geqslant 2$. 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 $\Gamma(A, \mathcal{L}_0^2) \otimes \Gamma(A, \mathcal{L}_0^2) \to \Gamma(A, \mathcal{L}_0^4)^+$ is equal to the number of non null even theta null points.*

3.4. **Normal projectivity.** A line bundle $\mathcal{L}$ on a variety X is projectively normal if $\Gamma(X, \mathcal{L}^n) \otimes \Gamma(X, \mathcal{L}) \to \Gamma(X, \mathcal{L}^{n+1})$ is surjective for all n or equivalently if $S(\Gamma(X, \mathcal{L})) \twoheadrightarrow \bigoplus \Gamma(X, \mathcal{L}^n)$. (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 3.7.

- *If $n \geqslant 3$, $(A, \mathcal{L})$ 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 3.8. 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 $g \geqslant 3$.

3.5. **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).

4. 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 κ_{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 4.1 (Compatible additions)**.** *Given $x, y, z, t \in A(\overline{k})$ 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. □

Proposition 4.2 (Multiway additions)**.** *Let $\pm P_0 \in \mathcal{K}_A(\overline{k})$ be a point not of 2-torsion. Then from $\pm P_1, \ldots, \pm P_n \in \mathcal{K}_A(\overline{k})$ and $\pm(P_0 + P_1), \ldots, \pm(P_0 + P_n) \in \mathcal{K}_A(\overline{k})$, one can compute $\pm(P_1 + \cdots + P_n)$ and $\pm(P_0 + P_1 + \cdots + P_n)$.*

Remark 4.3. A reformulation of the proposition is that the data of $P_0 + P_i \in \mathcal{K}_A(\overline{k})$ "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. □

4.1. **Multi Scalar multiplication.** To speed up the scalar multiplication $P \mapsto nP$, the GLV trick [GLV01] is to use an endomorphism α and reduces the scalar multiplication to a multi scalar multiplication $m_1P_1 + m_2P_2$ (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 4.4. Given $m_1P_1 + (m_2+1)P_2$, $(m_1+1)P_1 + m_2P_2$, we can compute $(2m_1+1)P_1 + (2m_2+1)P_2 = (m_1P_1 + (m_2+1)P_2) + (P_1) = ((m_1+1)P_1 + m_2P_2) + (P_2)$.

5. 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 $4 \to (\mathcal{K}_A, \mathcal{L}^+)$ 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 6

The theta constants of level 4 on A gives the points of 4 torsion, so we have the coordinates $U^{\mathcal{L}^2}_{\chi,i}(T)$ 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 $x + T_j = (x + T_i) + (T_i - T_j)$.

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

$$\pi(\vartheta_i(x))_{i\in Z(\overline{\ell n})} \to (\vartheta_i(x))_{i\in Z(\overline{n})}$$

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

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

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

Example 5.1. $g = 1$, $\ell = 3$, $n = 2$. $\widetilde{\pi}(x_0, \dots, x_5) = (x_0, x_3)$. $x + e_1 = (x_1, \dots, x_5, x_0)$ so $\widetilde{\pi}(x + e_1) = (x_1, x_4)$ and $\widetilde{\pi}(x + 2e_1) = (x_2, x_5)$.

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

Corollary 5.2.

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

6. 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 $\widetilde{\pi}(x), \widetilde{\pi}(x + T) = \widetilde{\pi}(x) + \widetilde{\pi}(T)$ where T is of 4-torsion.

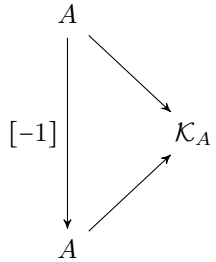
More generally, for $T \in A(\overline{k})$ such that $2T \neq 0$, we represent $x \in A(\overline{k})$ by $x \in \mathcal{K}_A(x)$, $x + T \in \mathcal{K}_A$. Addition: $(x, x + T) + (y, y + T) = (x + y = (x + T) + (y - T), x + y + T)$ (this is a three way addition and a compatible addition on the Kummer 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 6.1. 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.



7. 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 $i \in Z(\overline{2}), \chi \in \hat{Z}(\overline{2})$ and let

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

$\sum_t \chi(t) a_{i+t} a_t$ is simply the classical theta null point $\vartheta \begin{bmatrix} \chi/2 \\ i/2 \end{bmatrix} (0, \Omega)^2$. Then theorem 3.4 gives

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

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 α is such that $X_\alpha Y_0 - X_0 Y_\alpha \neq 0$). To compute κ_{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 κ_{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.yp.to/ecdh/diffchain-20060219.pdf (cit. on p. 5).

[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. 5).

[LR14] D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". June 2014. URL: http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 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. 2).

[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. 2).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
E-mail address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/