LMS J. Comput. Math. 15 (2012) 308–316 © 2012 Authors
doi:10.1112/S1461157012001027

Complete addition laws on abelian varieties

Christophe Arene, David Kohel and Christophe Ritzenthaler

Abstract

We prove that under any projective embedding of an abelian variety A of dimension g, a complete set of addition laws has cardinality at least $g+1$, generalizing a result of Bosma and Lenstra for the Weierstrass model of an elliptic curve in $\mathbb{P}^2$. In contrast, we prove, moreover, that if k is any field with infinite absolute Galois group, then there exists for every abelian variety A/k a projective embedding and an addition law defined for every pair of k-rational points. For an abelian variety of dimension 1 or 2, we show that this embedding can be the classical Weierstrass model or the embedding in $\mathbb{P}^{15}$, respectively, up to a finite number of counterexamples for $|k| \leqslant 5$.

1. *Introduction*

The notion of completeness of a set of addition laws for an abelian variety A in $\mathbb{P}^r$ was introduced by Lange and Ruppert [11]. We recall that an addition law is an $(r+1)$-tuple of bihomogeneous polynomials $(p_0, \ldots, p_r)$ such that the map

$$(x, y) \longmapsto (p_0(x, y), \ldots, p_r(x, y))$$

determines the group law $\mu : A \times A \to A$ on an open subset of $A \times A$, and a set of addition laws is complete if these open sets cover $A \times A$ (see Definition 2.1). The bidegree (m, n) of an addition law is the bidegree of the polynomials p_i in x and y. Lange and Ruppert proved that the minimal bidegree of any addition law is $(2, 2)$ and determined exact dimensions for the spaces of all addition laws of a given bidegree. For an elliptic curve E in $\mathbb{P}^2$ in Weierstrass form, the space of addition laws has dimension 3, and Bosma and Lenstra [6] proved that two suffice for a complete set, determining μ on all of $E \times E$.

In 2007, Edwards introduced a new normal form for elliptic curves

$$x_1^2 + x_2^2 = a^2(1 + x_1^2 x_2^2),$$

with a particularly simple rational expression for the group law. After a coordinate scaling, Bernstein and Lange [3] transformed this model to

$$x_1^2 + x_2^2 = 1 + d x_1^2 x_2^2$$

for $d = a^4$, which admits the group law $x + y = z$ where

$$z = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_3 y_3}, \frac{y_3 - x_3}{1 - d x_3 y_3} \right)$$

with $x_3 = x_1 x_2$ and $y_3 = y_1 y_2$. In addition to giving a precise analysis of the efficiency of this group law, Bernstein and Lange observed that the addition law is k-complete over any field k in which d is a nonsquare (that is, the addition law is well-defined on all pairs of k-rational points of E). To interpret these rational expressions in terms of projective addition laws as analyzed by Lange and Ruppert, we note that $\{1, x_1, x_2, x_3\}$ forms a basis of global sections for the Riemann–Roch space of the divisor at infinity for the pair of coordinate functions (x_1, x_2),

Received 26 May 2011; revised 5 April 2012.
2000 Mathematics Subject Classification 11G20 (primary), 14K15, 11T71 (secondary).

and that this basis determines a projective embedding

$$(x_1, x_2, x_3) \longmapsto (1 : x_1 : x_2 : x_3)$$

in $\mathbb{P}^3$ which is projectively normal (see Section 2 for precise definitions). Specifically, the image curve is of the form

$$X_1^2 + X_2^2 = X_0^2 + dX_3^2, \quad X_0X_3 = X_1X_2.$$

The Edwards addition law can be interpreted as the bidegree-$(2, 2)$ addition law

$$\big((X_0Y_0 + dX_3Y_3)(X_0Y_0 - dX_3Y_3), (X_0Y_0 - dX_3Y_3)(X_1Y_2 + X_2Y_1), \\ (X_0Y_0 + dX_3Y_3)(X_0Y_3 - X_3Y_0), (X_0Y_3 - X_3Y_0)(X_1Y_2 + X_2Y_1)\big).$$

Any elliptic curve specified by an affine model has a canonical embedding associated to the complete linear system. Consequently, we refer only to such abelian varieties with projective embeddings.

In terms of degree-3 models, Bernstein, Kohel and Lange [**2**] constructed a k-complete addition law on the family of twisted Hessian curves

$$aX_0^3 + X_1^3 + X_2^3 = dX_0X_1X_2,$$

which admit the k-complete addition laws

$$(X_0X_1Y_1^2 - X_2^2Y_0Y_2,\ aX_0X_2Y_0^2 - X_1^2Y_1Y_2,\ -aX_0^2Y_0Y_1 + X_1X_2Y_2^2)$$

and

$$(X_0X_2Y_2^2 - X_1^2Y_0Y_1,\ -aX_0^2Y_0Y_2 + X_1X_2Y_1^2,\ aX_0X_1Y_0^2 - X_2^2Y_1Y_2)$$

over any field k in which a is not a cube. Any such model is equivalent to a Weierstrass model by a linear change of variables, which shows that the property of k-completeness is not special to quartic models in $\mathbb{P}^3$.

Both the Edwards and twisted Hessian models share the property that they require a level structure of rational torsion. In analogy with the quartic Edwards model, Bernstein and Lange [**4**] demonstrated by example that a general elliptic curve admits a quartic model with k-complete addition law (subject to some coefficient being a nonsquare), while resorting to a rational expression for an addition law of high bidegree. The second author of the present article gave an elementary characterization of k-completeness of addition laws of bidegree $(2, 2)$ in terms of the Galois action on an associated divisor on the curve; see [**8**, Corollary 12]. In particular, the property of k-completeness on elliptic curves is not special.

In this paper, we generalize the above results to abelian varieties. We determine new, tight bounds on the size of a complete set of addition laws under any embedding, generalizing the result of Bosma and Lenstra [**6**] for elliptic curves. Moreover, we prove that if k is any field with infinite absolute Galois group, then there exists for every abelian variety A/k a projective embedding and an addition law defined for every pair of k-rational points (see Theorem 3.1).

Our work builds on the elegant paper of Lange and Ruppert [**11**], in which the authors interpret addition laws on an abelian variety A/k in terms of sections of a certain line bundle $\mathcal{M}$ on $A \times A$. Our key idea is to observe that an addition law associated to a section s of $H^0(A \times A, \mathcal{M})$ with zero divisor $D_s := (s)_0$ is defined on $A \times A \backslash D_s$. We obtain a k-complete addition law by constructing a k-rational divisor D_s without any k-rational point. This gives an exact analogue of the elliptic curve case studied by the second author in [**8**].

In Section 2, we recall some definitions and concepts from [**11**], explain more explicitly the link between addition laws on a projective embedding of A/k and sections of $H^0(A \times A, \mathcal{M})$, and also deal with the geometric case $k = \bar{k}$. For any principally polarized abelian variety of dimension g, we give bounds on the cardinality of any complete set of addition laws; in particular, we show that its cardinality is at least $g + 1$.

In Section 3, we consider the case of a field k with infinite absolute Galois group, and prove the aforementioned result on existence of a pair consisting of a projective embedding and a k-complete addition law.

In Section 4, we specialize to elliptic curves and Jacobians of genus-two curves over a finite field k, noting that the results also extend to other fields (see Remarks 4.4 and 4.9). We prove that there exists a k-complete addition law for their classical embeddings in $\mathbb{P}^2$ and $\mathbb{P}^{15}$, respectively, as soon as $|k| \geqslant 5$ for elliptic curves and $|k| \geqslant 7$ for Jacobian surfaces. In particular, we exhibit an explicit k-complete addition law on a Weierstrass model of an elliptic curve E over k when E has no nontrivial rational 2-torsion points.

2. *Addition laws and completeness*

Let k be a field and A/k an abelian variety of dimension g. We assume that A is embedded in some projective space $\mathbb{P}^r$ over k by a very ample line bundle $\mathcal{L} = \mathcal{L}(D)$, with D being an effective divisor, and we denote by $\iota : A \hookrightarrow \mathbb{P}^r$ the corresponding morphism. We also assume in what follows that the embedding is projectively normal. Recall that A is said to be *projectively normal* in $\mathbb{P}^r$ if for every $n \geqslant 1$ the restriction map $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) \to \Gamma(A, \mathcal{L}^n)$ is surjective. This is the case in the classical settings where $\mathcal{L} = \mathcal{L}_0^a$ with $\mathcal{L}_0$ an ample line bundle and $a \geqslant 3$ (see [**5**, p. 187]).

Let I_1 and I_2 be the homogeneous defining ideals for A in $k[X_0, \ldots, X_r]$ and $k[Y_0, \ldots, Y_r]$, respectively. The *group law*

$$\mu : A \times A \to A,$$

defined by $(x, y) \mapsto x + y$, can be locally described by bihomogenous polynomials. More precisely, an *addition law* $\mathfrak{p}$ of bidegree (m, n) on $\iota(A) \subset \mathbb{P}^r$ is an $(r+1)$-tuple $(p_0, \ldots, p_r)$ of elements

$$p_i \in k[X_0, \ldots, X_r]/I_1 \otimes k[Y_0, \ldots, Y_r]/I_2$$

which are bihomogeneous of degree m and n in $X_0, \ldots, X_r$ and $Y_0, \ldots, Y_r$, respectively, and for which there exists a nonempty open subset U of $A \times A$ such that for all $(x, y) \in U(\bar{k})$,

$$\iota \circ \mu(x, y) = (p_0(\iota(x), \iota(y)) : \ldots : p_r(\iota(x), \iota(y))).$$

When A is given with a fixed embedding in $\mathbb{P}^r$, we may suppress the reference to the embedding ι and speak of addition laws on A.

Definition 2.1. A set S of addition laws is said to be *k-complete* if for any k-rational point $(x, y) \in (A \times A)(k)$ there is an addition law in S defined on an open set U containing (x, y). This set is said to be *complete* if the previous property holds over $\bar{k}$. If $S = \{\mathfrak{p}\}$ is a singleton, we say that the addition law $\mathfrak{p}$ is *k-complete* and *complete* when $k = \bar{k}$.

In [**11**, Lemma 2.1], Lange and Ruppert gave the interpretation of the possible addition laws in terms of the sections of certain line bundles.

Proposition 2.2. *Let $\pi_1, \pi_2 : A \times A \to A$ be the projection maps on the first and second factor. There is an addition law (respectively, a complete set of addition laws) of bidegree (m, n) on A with respect to the embedding in $\mathbb{P}^r$ determined by $\mathcal{L}$ if and only if*

$$H^0(A \times A, \mathcal{M}_{m,n}) \neq 0$$

(respectively, the linear system $|\mathcal{M}_{m,n}|$ is basepoint-free), where

$$\mathcal{M}_{m,n} = \mu^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n.$$

We explain how one associates an addition law to a nonzero section w in $H^0(A \times A, \mathcal{M}_{m,n})$. For $0 \leqslant j \leqslant n$, let $t_j \in H^0(A, \mathcal{L})$ be the basis given by $t_j = \iota^* X_j$ where X_j are the coordinate functions on $\mathbb{P}^r$. As shown in [**11**, p. 607], $H^0(A \times A, \mu^* \mathcal{L}) = \mu^* H^0(A, \mathcal{L})$, and so $s_j = \mu^* t_j$ is a basis of $H^0(A \times A, \mu^* \mathcal{L})$. For each j and $(x, y) \in A \times A$, we have

$$s_j(x, y) = t_j \circ \mu(x, y) = X_j(\iota \circ \mu(x, y)).$$

Now $w \otimes s_j \in H^0(A \times A, \pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n)$. As the embedding is projectively normal, we have

$$\pi_1^* \mathcal{L}^m \otimes \pi_2^* \mathcal{L}^n = (\iota \otimes \iota)^* \mathcal{O}_{\mathbb{P}^r}(m) \otimes \mathcal{O}_{\mathbb{P}^r}(n),$$

and then there exists a bihomogeneous polynomial p_j of bidegree (m, n) such that for all points $(x, y) \in A \times A$,

$$(w \otimes s_j)(x, y) = p_j(\iota(x), \iota(y)).$$

Therefore, if $U = A \times A \backslash (w)_0$, we have

$$\begin{aligned}(p_0(\iota(x), \iota(y)) : \ldots : p_r(\iota(x), \iota(y))) &= ((w \otimes s_0)(x, y) : \ldots : (w \otimes s_r)(x, y)) \\ &= (s_0(x, y) : \ldots : s_r(x, y)) \\ &= (X_0(\iota \circ \mu(x, y)) : \ldots : X_r(\iota \circ \mu(x, y))) \\ &= \iota(\mu(x, y)).\end{aligned}$$

Another natural requirement is that $\mathcal{L} = \mathcal{L}(D)$ be symmetric, that is, $[-1]^* \mathcal{L} \cong \mathcal{L}$ or, equivalently, $D \sim [-1]^* D$, as can be seen from the following lemmas.

LEMMA 2.3. *If A/k is embedded in $\mathbb{P}^r$ by a very ample symmetric line bundle $\mathcal{L}$ (projectively normal), then the inversion map $[-1]$ on A is induced by a linear automorphism of $\mathbb{P}^r$. Moreover, if* $\operatorname{char}(k) \neq 2$, *there is a choice of coordinates such that the inversion acts by ± 1 on each coordinate.*

Proof. The first statement is a direct consequence of the symmetry of $\mathcal{L}$. Now fix a basis (t_i) of $H^0(A, \mathcal{L})$ and let M be the matrix of the coordinates of $[-1]^* t_i$ in the basis (t_i). The morphism $[-1]$ is induced by an involution of $\mathbb{P}^r$, so there exists $\varepsilon \in k$ such that $M^2 - \varepsilon \operatorname{Id} = 0$.

The neutral element $O = (a_0 : \ldots : a_r)$ of $A \hookrightarrow \mathbb{P}^r$ is a fixed point for $[-1]$. Hence, the vector $(a_0, \ldots, a_r)$ is an eigenvector of the matrix M with eigenvalue $\varepsilon_0 \in k$. This implies that $\varepsilon = \varepsilon_0^2$, and if $\operatorname{char}(k) \neq 2$, then $M^2 - \varepsilon \operatorname{Id}$ factors as $(M - \varepsilon_0 \operatorname{Id})(M + \varepsilon_0 \operatorname{Id})$. This proves that M can be diagonalized over k with eigenvalues in $\{\pm \varepsilon_0\}$, and so the conclusion holds. □

Before considering non-algebraically closed fields, it is natural to examine what happens over $\bar{k}$. We start by giving an upper bound on the cardinality of a complete set of addition laws. In what follows, we define the difference map $\delta : A \times A \longrightarrow A$ by $(x, y) \mapsto x - y$, and use the product partial order on bidegree given by $(k, l) \leqslant (m, n)$ if and only if $k \leqslant m$ and $l \leqslant n$. For bidegree $(m, n) = (2, 2)$, we denote the line bundle $\mathcal{M}_{m,n}$ of Proposition 2.2 by $\mathcal{M}$. We begin by recalling a fundamental result of Lange and Ruppert; see [**11**, Propositions 2.2 and 2.3].

LEMMA 2.4. *Let $\mathcal{L}$ be an ample line bundle on A.*

(1) *If $\mathcal{L}$ is not symmetric, then $H^0(A \times A, \mathcal{M}) = 0$.*

(2) *If $\mathcal{L}$ is symmetric, then $\mathcal{M}$ is isomorphic to $\delta^* \mathcal{L}$ and is basepoint-free; consequently, $h^0(\mathcal{M}) = h^0(\mathcal{L})$.*

If $(m, n) > (2, 2)$, then $h^0(\mathcal{M}_{m,n}) = h^0(\mathcal{L})^2 (mn - m - n)^g$.

Proof. For $(m, n) > (2, 2)$, the proof follows the case of $(m, n) = (2, 3)$ treated in [**11**, Proposition 2.3]. For $(m, n) = (2, 2)$, Lange and Ruppert proved in [**11**, Proposition 2.2] that $\mathcal{M} \cong \delta^* \mathcal{L}$ and that $\mathcal{M}$ is basepoint-free. The equality $h^0(\mathcal{M}) = h^0(\mathcal{L})$ is an easy consequence

https://doi.org/10.1112/S1461157012001027 Published online by Cambridge University Press

of the fact, proved in [11], that $\mathcal{M}|_{K(\mathcal{M})_0}$ is trivial together with the fact that, as $\mathcal{L}$ is ample, its index is zero. Indeed, according to [13, Theorem 1(ii), p. 95], one then has the isomorphism $H^0(A \times A, \mathcal{M}) \cong H^0(A, \mathcal{L})$. □

The isomorphism of $\mathcal{M}$ with $\delta^*\mathcal{L}$ allows us to consider line bundles on A instead of on $A \times A$. The following well-known lemma shows that we can always find a symmetric embedding of $A/\bar{k}$.

LEMMA 2.5. *Let (A, λ) be a principally polarized abelian variety over $\bar{k}$. Then there exists a symmetric line bundle which induces the polarization λ on A.*

Proof. Suppose that $\mathcal{L}'$ is a line bundle attached to the polarization λ. We construct a symmetric line bundle $\mathcal{L}$ algebraically equivalent to $\mathcal{L}'$. Since $\mathcal{L}'$ is algebraically equivalent to $[-1]^*\mathcal{L}'$ (see [9, p. 93]), there exists $x \in A(\bar{k})$ such that the translation $\tau_x^*\mathcal{L}'$ is algebraically equivalent to $[-1]^*\mathcal{L}'$. Let y be an element of $A(\bar{k})$ such that $2y = x$, and set $\mathcal{L} = \tau_y^*\mathcal{L}'$. Then $\mathcal{L}$ is algebraically equivalent to $\mathcal{L}'$ and

$$\mathcal{L} = \tau_y^*\mathcal{L}' = \tau_{-y}^*\tau_x^*\mathcal{L}' \cong \tau_{-y}^*[-1]^*\mathcal{L}' = [-1]^*\mathcal{L},$$

so that it is symmetric. □

Suppose that $\mathcal{L}$ is a symmetric line bundle as in the preceding lemma. By Lemma 2.4, the embedding defined by $\mathcal{L}^3$ has a complete set of biquadratic addition laws of cardinality equal to $h^0\left(A, \mathcal{L}^3\right) = 3^g$. This gives an upper bound on the minimal size of a complete set of addition laws. We now determine a lower bound.

THEOREM 2.6. *Assume A is embedded in $\mathbb{P}^r$ by a symmetric line bundle. If S is a complete set of addition laws on A, then $|S| \geqslant g + 1$.*

Proof. Suppose that S is a complete set of addition laws of bidegree (m, n) on A, and let $\nabla = \ker(\mu) \subset A \times A$. By Lemma 2.3, the isomorphism

$$[\,1\,] \times [-1] : A \longrightarrow \nabla$$

is linear, and so $([\,1\,] \times [-1])^*S$ is a set of polynomial (rational) maps for $A \to \{O\} \subset A$. It follows that there exists a set I of polynomials of degree $m + n$ such that

$$([\,1\,] \times [-1])^*S = \{(a_0 q(X_0, \ldots, X_r), \ldots, a_r q(X_0, \ldots, X_r)) : q \in I\},$$

where $O = (a_0 : \cdots : a_r)$. Since S is complete, the subvariety $V(I) \cap A$ is empty. On the other hand, its dimension is at least $\dim(A) - |I| \geqslant g - |S|$, hence the cardinality of S must be at least $g + 1$. □

Although the interval $[g + 1, 3^g]$ is quite large, the lower bound shows that there is no complete addition law on any abelian variety of any dimension. For $g = 1$, these bounds show that the minimal size of a complete set of addition laws is either 2 or 3. An explicit set of cardinality 3 was already given by Lange and Ruppert in [11, Section 3] for $\mathrm{char}(k) \neq 2, 3$, and in [12] for any characteristic; furthermore, Bosma and Lenstra [6] proved that a set of minimal cardinality 2 is in fact sufficient.

3. *k-complete addition laws*

Let $\mathcal{L}$ be a very ample symmetric line bundle defined by an effective k-rational divisor D on A/k.

Since $\delta^*\mathcal{L} \cong \mathcal{M} = \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^2 \otimes \pi_2^*\mathcal{L}^2$, there exists w in $H^0(A \times A, \mathcal{M})$ such that $(w)_0 = \delta^*(D)$. As we have seen in Section 2, w defines a biquadratic addition law on the complement

https://doi.org/10.1112/S1461157012001027 Published online by Cambridge University Press

of $(w)_0 = \delta^* D$. Hence it is sufficient that D have no k-rational point for the group law to be k-complete. Note that this is also a necessary condition, since a k-rational point x on D gives the k-rational point $(x, 0)$ on $\delta^* D$.

THEOREM 3.1. *Let A/k be an abelian variety and $\iota_0 : A \hookrightarrow \mathbb{P}^{r_0}$ an embedding for some $r_0 > 1$. Assume that k has infinite absolute Galois group and let $d > r_0$ be such that there exists a separable extension K/k of degree d over k. Then there exists an embedding $\iota : A \hookrightarrow \mathbb{P}^r$ and a k-complete biquadratic addition law on $\iota(A)$, with $r = (2d)^g(r_0 + 1) - 1$.*

Proof. Let $K = k(\alpha_0)/k$ be a separable extension, and denote by $\alpha_0, \ldots, \alpha_{d-1}$ its distinct Galois conjugates in the normal closure of K/k. For $i = 0, \ldots, d - 1$, let H_i be the hyperplane in $\mathbb{P}^{r_0}$,

$$H_i : X_0 + \alpha_i X_1 + \ldots + \alpha_i^{r_0} X_{r_0} = 0.$$

Since $d > r_0$, the sets $\{1, \alpha_i, \ldots, \alpha_i^{r_0}\}$ are linearly independent over k for every i, and hence $H_i(k)$ is empty. Now $\sum H_i$ is a k-rational divisor, so let $D_0 = \iota_0^*(\sum H_i)$ and define the divisor $D = D_0 + [-1]^* D_0$. Then D is a symmetric, effective, k-rational divisor without k-rational points. Denote by $\mathcal{L}_0$ the line bundle associated to the embedding ι_0. The line bundle $\mathcal{L} = \mathcal{L}(D)$ is isomorphic to $\mathcal{L}_0^{2d}$, so $\mathcal{L}$ is very ample and provides a projectively normal embedding $A \hookrightarrow \mathbb{P}^r$ with a k-complete biquadratic addition law. By the Riemann–Roch theorem, the dimension r is equal to $(2d)^g(r_0 + 1) - 1$. □

4. *The genus-one and genus-two cases*

In the previous section, a k-complete (biquadratic) addition law was proved to exist for an embedding of the abelian variety in a projective space of high dimension. When $k = \mathbb{F}_q$ is a finite field and the abelian variety A/k has dimension 1 or 2, we will show that we can take the embedding to be the corresponding classical one. In what follows, we let σ denote the Frobenius automorphism of $\bar{k}/k$.

4.1. *Elliptic curves*

Let $A = E$ be an elliptic curve defined over $k = \mathbb{F}_q$.

LEMMA 4.1. *If $q \geqslant 5$, there exists $P_0 \in E(\bar{k})$ such that its Galois orbit is given by three distinct points whose sum is O.*

Proof. Consider the group homomorphism $N : E(\mathbb{F}_{q^3}) \to E(\mathbb{F}_q)$ given by

$$P \longmapsto P + P^\sigma + P^{\sigma^2}.$$

We are looking for a point $P_0 \in \ker(N) \backslash E(\mathbb{F}_q)$; hence we want

$$|\ker(N)| > |\ker(N) \cap E(\mathbb{F}_q)|.$$

The intersection of $\ker(N)$ with $E(\mathbb{F}_q)$ is the group of $\mathbb{F}_q$-rational 3-torsion points of E, so $|\ker(N) \cap E(\mathbb{F}_q)| \leqslant 9$. On the other hand, for all $q \geqslant 5$ we have

$$|\ker(N)| \geqslant \frac{|E(\mathbb{F}_{q^3})|}{|E(\mathbb{F}_q)|} \geqslant \frac{q^3 + 1 - 2\sqrt{q^3}}{q + 1 + 2\sqrt{q}} > 9,$$

so such a point P_0 exists in $E(\mathbb{F}_{q^3})$. □

REMARK 4.2. For each of $q = 2, 3$ and 4, there exists at least one elliptic curve over $\mathbb{F}_q$ for which $|\ker(N)| = |\ker(N) \cap E(\mathbb{F}_q)|$.

https://doi.org/10.1112/S1461157012001027 Published online by Cambridge University Press

THEOREM 4.3. *Let k be the finite field $\mathbb{F}_q$ with $q \geqslant 5$, and let E/k be an elliptic curve. There exists a k-complete biquadratic addition law on the Weierstrass model of $E \subset \mathbb{P}^2$.*

Proof. Let P_0 be a point as in Lemma 4.1, and let D be the divisor given by the sum of the Galois conjugates of P_0. It is a k-rational divisor without k-rational points. It is not a symmetric divisor, but $\mathcal{L} = \mathcal{L}(D)$ is a symmetric line bundle as $D \sim 3(O) \sim [-1]^* D$. Another consequence of the relation $D \sim 3(O)$ is that the embedding associated to $\mathcal{L}(D)$ is projectively equivalent to the Weierstrass model of E. □

REMARK 4.4. We use the fact that k is a finite field only to prove the existence of the point P_0. It is easy to see that when k is a number field, such a point always exists and so the conclusion of Theorem 4.3 still holds. Indeed, if E is defined by $y^2 + h(x)y = f(x)$, then, since k is Hilbertian (see [**10**, p. 225]), there exists $y_0 \in k$ such that $y_0^2 + h(x)y_0 - f(x)$ is irreducible. We can take $P_0 = (x_0, y_0)$ where x_0 is any root of $y_0^2 + h(x)y_0 - f(x) = 0$ in $\bar{k}$.

In particular, for $\mathrm{char}(k) \neq 2$ or 3, by means of a change of variables we may assume that E is of the form $y^2 = x^3 + ax + b$. Moreover, if E has no nontrivial k-rational 2-torsion points, then the polynomial $f(x) = x^3 + ax + b$ is irreducible over k and the sum $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ is given by the addition law $(X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)})$ of Bosma and Lenstra [**6**],

$$\begin{aligned}
&\big((X_1Y_2 + Y_1X_2)(Y_1Y_2 - 6bZ_1Z_2) - a(Y_1Z_2 + Z_1Y_2)(2X_1X_2 - aZ_1Z_2)\\
&\quad - X_1Z_2(aX_1Y_2 + 3bY_1Z_2) - Z_1X_2(aY_1X_2 + 3bZ_1Y_2),\\
&Y_1^2Y_2^2 + aX_1X_2(3X_1X_2 - 2aZ_1Z_2) - a^2(X_1Z_2 + Z_1X_2)^2\\
&\quad + 3b(X_1Z_2 + Z_1X_2)(3X_1X_2 - aZ_1Z_2) - (a^3 + 9b^2)Z_1^2Z_2^2,\\
&Y_1Y_2(Y_1Z_2 + Z_1Y_2) + (3X_1X_2 + 2aZ_1Z_2)(X_1Y_2 + Y_1X_2)\\
&\quad + (aX_1 + 3bZ_1)Y_1Z_2^2 + Z_1^2(aX_2 + 3bZ_2)Y_2\big),
\end{aligned}$$

specialized to $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, a, b)$. Under the hypothesis on the 2-torsion, the exceptional divisor $\delta^*\{Y = 0\}$ is irreducible, hence the addition law is k-complete.

4.2. *Genus-two curves*

Let C be a genus-two curve over a finite field $k = \mathbb{F}_q$, with hyperelliptic involution $P \mapsto \overline{P}$. By [**15**, Proposition 2.3.21, p. 180], there exists a (not necessarily effective) k-rational divisor P_∞ of degree 1 such that $2P_\infty$ is equivalent to the canonical divisor κ of C. The divisor Θ, defined as the image of C in $\mathrm{Jac}(C)$ under the map $P \mapsto (P) - P_\infty$, is then a k-rational, ample, symmetric divisor which defines the canonical principal polarization on $\mathrm{Jac}(C)$. For any $z \in \mathrm{Jac}(C)(\bar{k})$, we denote by Θ_z its translation $(\tau_z^*)^{-1}\Theta = \Theta + z$.

The following result can be found, for instance, in [**14**, p. 275].

PROPOSITION 4.5. *Let P and Q be points in $C(\bar{k})$, and set $z = (P) - (Q) \in \mathrm{Jac}(C)(\bar{k})$. Then we have*

$$\Theta \cap \Theta_z = \{(P) - P_\infty, (\overline{Q}) - P_\infty\}.$$

As in the previous section, we will need the existence of a Galois orbit of points for the construction of a divisor on $\mathrm{Jac}(C)$.

LEMMA 4.6. *If $q \geqslant 7$, there exists a point $P_0 \in C(\bar{k})$ such that its Galois orbit has cardinality 4 and $P_0^{\sigma^2} = \overline{P}_0$.*

Proof. Let $\phi : C \to \mathbb{P}^1$ be the quotient by the hyperelliptic involution. Note that P_0 is a point in $C(\mathbb{F}_{q^4}) \backslash C(\mathbb{F}_{q^2})$ such that $\phi(P_0)$ is in $\mathbb{P}^1(\mathbb{F}_{q^2})$. Moreover, no such point exists if and

https://doi.org/10.1112/S1461157012001027 Published online by Cambridge University Press

only if $\phi(C(\mathbb{F}_{q^2})) = \mathbb{P}^1(\mathbb{F}_{q^2})$ or, equivalently,

$$|C(\mathbb{F}_{q^2})| = 2(q^2+1) - e_2,$$

where $e_2 \leqslant 6$ is the number of ramification points of ϕ in $C(\mathbb{F}_{q^2})$. For $q \geqslant 7$, this equality contradicts the Weil bound $|C(\mathbb{F}_{q^2})| \leqslant q^2+4q+1$, and so such a point exists. □

REMARK 4.7. For each of $q = 2, 3, 4$ and 5, there exists at least one genus-two curve over $\mathbb{F}_q$ with no such point P_0. In particular, for $q = 5$ the bound is tight (for $e_2 = 6$), namely

$$|C(\mathbb{F}_{q^2})| = 2(q^2+1) - 6 = q^2 + 4q + 1 = 46,$$

and is satisfied for the curve $y^2 = x^6 + 1$ over $\mathbb{F}_5$.

THEOREM 4.8. *Let C be a genus-two curve over $\mathbb{F}_q$ with $q \geqslant 7$. There exists a k-complete biquadratic addition law for the classical embedding of* $\mathrm{Jac}(C)$ *in* $\mathbb{P}^{15}$ *determined by* $\mathcal{L}(4\Theta)$.

Proof. For the canonical divisor κ and a point P_0 as in Lemma 4.6, we define

$$\alpha_0 = (P_0) + (P_0^\sigma) - \kappa, \quad \alpha_1 = (P_0^\sigma) + (\overline{P}_0) - \kappa,$$
$$\alpha_2 = (\overline{P}_0) + (\overline{P}_0^\sigma) - \kappa, \quad \alpha_3 = (\overline{P}_0^\sigma) + (P_0) - \kappa.$$

Using Proposition 4.5, we find that

$$\Theta_{\alpha_0} \cap \Theta_{\alpha_1} = (\tau_{\alpha_0}^*)^{-1}(\Theta \cap \Theta_{(\overline{P}_0)-(P_0)}) = \{(\overline{P}_0) - P_\infty + \alpha_0\},$$
$$\Theta_{\alpha_0} \cap \Theta_{\alpha_3} = (\tau_{\alpha_0}^*)^{-1}(\Theta \cap \Theta_{(\overline{P}_0^\sigma)-(P_0^\sigma)}) = \{(\overline{P}_0^\sigma) - P_\infty + \alpha_0\}.$$

By construction, the divisor $D = \sum \Theta_{\alpha_i}$ is ample, symmetric and k-rational. Moreover, since there exists a transitive action on the components Θ_{α_i}, any k-rational point of D must be a point of the intersection

$$\Theta_{\alpha_0} \cap \Theta_{\alpha_1} \cap \Theta_{\alpha_2} \cap \Theta_{\alpha_3},$$

which is empty. Finally, we have $\sum \alpha_i = 0$ by construction, so $D \sim 4\Theta$ and D determines a k-complete addition law for the classical embedding of $\mathrm{Jac}(C)$ in $\mathbb{P}^{15}$ determined by $\mathcal{L}(4\Theta)$. □

REMARK 4.9. This construction can be generalized to other fields. For instance, following the same lines as Remark 4.4, Lemma 4.6 has an analogue over number fields k. However, a k-rational divisor P_∞ of degree 1 may no longer exist, but for the family of curves C such as $y^2 = f(x)$ with $\deg f = 5$, we can take P_∞ to be the divisor with support being the point at infinity. In this case, the analogue of Theorem 4.8 holds over a number field. Arene and Cosset have developed an algorithm to construct such an addition law [**1**].

REMARK 4.10. The construction of Theorem 4.8 uses differences of effective divisors of degree $g = 2$. In general, such degree-g divisors are necessary, since if C is a curve of genus g and we define $W_i = \mathrm{im}(\mathrm{Sym}^i\, C \to \mathrm{Jac}(C))$, then by [**7**, p. 146] the intersection

$$\bigcap \{W_{g-1} - a : a \in W_r + b\}$$

is nonempty for any $0 \leqslant r \leqslant g-1$ and any $b \in \mathrm{Jac}(C)$.

Acknowledgements. The authors thank David Gruenewald for his careful reading of and comments on a prior version of this article. They acknowledge financial support from the French ANR through grant ANR-09-BLAN-0020-01, the AXA Research Fund for the first author's PhD grant, and the Spanish MEC for grant MTM2006-11391 to the third author.

References

1. C. Arene and R. Cosset, 'Construction of a k-complete addition law on abelian surfaces', *Arithmetic, geometry, cryptography and coding theory 2011*, Contemporary Mathematics 574 (American Mathematical Society, Providence, RI, 2012).
2. D. J. Bernstein, D. Kohel and T. Lange, 'Twisted hessian curves', Preprint, 2009.
3. D. J. Bernstein and T. Lange, 'Faster addition and doubling on elliptic curves', *Advances in cryptology – ASIACRYPT 2007*, Lecture Notes in Computer Science 4833 (Springer, Berlin, 2007) 29–50.
4. D. J. Bernstein and T. Lange, 'Complete addition laws for all elliptic curves over finite fields', presentation, 2009, cr.yp.to/talks/2009.07.17/slides.pdf.
5. C. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd edn, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 302 (Springer, Berlin, 2004).
6. W. Bosma and H. W. Lenstra Jr., 'Complete systems of two addition laws for elliptic curves', *J. Number Theory* 53 (1995) 229–240.
7. H. M. Farkas and I. Kra, *Riemann surfaces*, 2nd edn, Graduate Texts in Mathematics 71 (Springer, New York, 1980).
8. D. Kohel, 'Addition law structure of elliptic curves', *J. Number Theory* 131 (2011) 894–919.
9. S. Lang, *Abelian varieties* (Springer, New York, 1983) reprint of the 1959 original.
10. S. Lang, *Fundamentals of Diophantine geometry* (Springer, New York, 1983).
11. H. Lange and W. Ruppert, 'Complete systems of addition laws on abelian varieties', *Invent. Math.* 79 (1985) 603–610.
12. H. Lange and W. Ruppert, 'Addition laws on elliptic curves in arbitrary characteristics', *J. Algebra* 107 (1987) 106–116.
13. D. Mumford, 'Varieties defined by quadratic equations', *Questions on algebraic varieties (C.I.M.E. summer school III, Ciclo, Varenna, 1969)* (Edizioni Cremonese, Rome, 1970) 29–100.
14. D. Mumford, *Curves and their Jacobians* (The University of Michigan Press, Ann Arbor, MI, 1975).
15. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications (Soviet Series) 58 (Kluwer, Dordrecht, 1991) translated from the Russian by the authors.

Christophe Arene
Institut de Mathématiques de Luminy
163 Avenue de Luminy, Case 907
13288 Marseille
France

arene.christophe@gmail.com

David Kohel
Institut de Mathématiques de Luminy
163 Avenue de Luminy, Case 907
13288 Marseille
France

kohel@iml.univ-mrs.fr

Christophe Ritzenthaler
Institut de Mathématiques de Luminy
163 Avenue de Luminy, Case 907
13288 Marseille
France

ritzenth@iml.univ-mrs.fr

https://doi.org/10.1112/S1461157012001027 Published online by Cambridge University Press