Rend. Istit. Mat. Univ. Trieste
Volume 51 (2019), 105–123
DOI: 10.13137/2464-8728/27068

On elliptic curves of bounded degree in a polarized Abelian variety

Lucio Guerra

Abstract. *For a polarized complex Abelian variety A we study the function $N_A(t)$ counting the number of elliptic curves in A with degree bounded by t. This extends our previous work in dimension two. We describe the collection of elliptic curves in the product $A = S \times F$ of an Abelian variety and an elliptic curve by means of an explicit parametrization, and in terms of the parametrization we express the degrees of elliptic curves relative to a split polarization. When this is applied to the self product $A = E^k$ of an elliptic curve, it turns out that an asymptotic estimate of the counting function $N_A(t)$ can be obtained from an asymptotic study of the degree form on the group of endomorphisms of the elliptic curve.*

Keywords: Elliptic curve, Abelian variety, polarization.
MS Classification 2010: 14K20, 14H52.

1. Introduction

Let A be a complex Abelian variety, of dimension $n > 1$, endowed with a polarization. With the expression 'elliptic curve in an Abelian variety' we mean a one-dimensional subtorus. Every algebraic curve in A has a degree with respect to the polarization, and the following finiteness theorem holds: for every integer $t \geq 1$ the collection of elliptic curves $E \subset A$ such that $\deg(E) \leq t$ is finite. In dimension $n = 2$ this was known to Bolza and Poincaré, and a modern account is in the paper of Kani [7]. For Jacobian varieties of arbitrary dimension the theorem was proved by Tamme and was brought to an effective form in another paper of Kani [6]. For an arbitrary Abelian variety A the theorem follows from a general result proved by Birkenhake and Lange in [1], to the effect that the collection of all Abelian subvarieties with bounded exponent in A is finite.

Denote by $N_A(t)$ the number of elliptic curves in A with degree bounded by t. In a previous paper [4], we presented an approach to the counting function $N_A(t)$ in dimension $n = 2$. In the most relevant situation, when the Abelian surface is the product $E \times E'$ of two elliptic curves, the approach was based on explicit coordinates in the Néron Severi group and an explicit Diophantine

equation for the collection of elliptic curves in the Abelian surface. We have to correct an expression given in that paper for the quantity δ that is required in the main theorem (as is explained in §3.2). This leaves the statement of the theorem formally unaltered, and the same is for its proof and its consequences.

The main aim of the present paper is to study the function $N_A(t)$ in arbitrary dimension. The problem of bounding this function is invariant under isogenies, and the most relevant case is when the Abelian variety A is the self product E^k of an elliptic curve, with a split polarization (the sum of pullback polarizations from the factors). An approach to the 3-dimensional counting function, still based on explicit Diophantine equations, was investigated in [3]. Here we present a different approach, which is based on parametrization rather than equations in coordinates.

We study the collection of elliptic curves in the product $S \times F$ of an Abelian variety and an elliptic curve. We show that the subcollection consisting of the elliptic curves which are not contained in $S \times \{0\}$ and are different from $\{0\} \times F$ is bijectively parametrized by a certain set of parameter data (Theorem 5.1) and that, with respect to a split polarization, the degrees of the corresponding elliptic curves in $S \times F$ can be expressed in terms of the parameter data (Theorem 5.2). When these results on parametrization are applied to the self product E^k of an elliptic curve, it turns out that, in this case, an estimate of the counting function $N_A(t)$ can be obtained from an asymptotic study of the degree form $f \longmapsto \deg(f)$ on the group of endomorphisms of the elliptic curve (that is provided in Proposition 4.1). The tool for this is the same result from Number Theory, concerning the number of lattice points in a bounded region in the real plane, that was used in the previous work on the 2-dimensional counting function.

Here is the fundamental information that is needed in our asymptotic estimate of the counting function. Define:

- m the minimum of the degrees of the factors of E^k, the various copies of E, with respect to the given polarization;
- d the minimum degree of an isogeny $E \to E$;
- δ when the elliptic curve has complex multiplication, the (negative) discriminant of the degree form on the endomorphism group $End(E)$.

Assume moreover that $k \geq 2$. In terms of these data, we prove (in §6) the following main result:

THEOREM 1.1. *There is an asymptotic estimate*

$$N_{E^k}(t) = C\, t^r + O(t^i),$$

where $r = k$ if the curve admits no complex multiplication, and $r = 2k - 1$ if the curve has complex multiplication, the constant C being given by

$$\frac{2^k/(k+1)}{(\sqrt{d})^{k-1}\,m^k} \quad \textit{for } r=k, \qquad \frac{(2\pi)^{k-1}/k}{(\sqrt{-\delta})^{k-1}\,m^{2k-1}} \quad \textit{for } r=2k-1,$$

the exponent i being

$$k-1 \quad \textit{for } r=k, \qquad 2k-3+2e \quad \textit{for } r=2k-1,$$

where $e = 33/104 = 0.317\ldots$.

Finally we show that the result above for the self product of an elliptic curve implies some result holding for an arbitrary polarized Abelian variety (Proposition 7.1).

2. Some preliminary material

2.1. Elliptic curves as homology classes

Let A be an Abelian variety, of dimension $n > 1$. Every curve $C \subset A$ determines a homology class $[C]$ in $H_2(A, \mathbb{Z})$. For elliptic curves (subgroups), the induced correspondence

$$\big\{\text{elliptic curves in } A\big\} \longrightarrow H_2(A, \mathbb{Z})$$

is injective and the homology classes $\gamma = [C]$ in $H_2(A, \mathbb{Z})$ corresponding to elliptic curves in A satisfy the following basic properties:

- γ is primitive (indivisible),
- $\gamma \cdot H > 0$ for some (every) ample divisor H.

These results are certainly well known (the last property is obvious), however a proof can be found in [3], §2.

In dimension $n = 2$, the homology classes of elliptic curves in the Abelian surface A belong to the Néron Severi group $NS(A) \hookrightarrow H_2(A, \mathbb{Z})$, and are characterized in that group by means of the two properties above together with the numerical condition (cf. [7], Theorem 1.1):

- $\gamma \cdot \gamma = 0$.

2.2. Degree with respect to a polarization

Let L in $NS(A)$ be an ample divisor class, representing a polarization of A. For every curve $C \subset A$ the degree with respect to the polarization is

$$\deg(C) := C \cdot L.$$

Let A be a polarized Abelian variety (we usually omit an explicit reference to the polarization). The following is a classical result: for every integer $t \geq 1$

the collection of elliptic curves $E \subset A$ such that $\deg(E) \leq t$ is finite. It is a consequence of a general result proved by Birkenhake and Lange in [1], to the effect that the collection of all Abelian subvarieties with bounded exponent in A is finite.

Let us recall some definitions. The polarization defines a natural isogeny $\phi : A \to \widehat{A}$ to the dual variety. The order of $\ker(\phi)$ is the degree of the polarization and the exponent of $\ker(\phi)$ is called the exponent of the polarization on A. Clearly the exponent is a divisor of the degree. For an Abelian subvariety E of A one has the exponent and the degree of the induced polarization. If E is an elliptic curve in A we know that the degree of the curve is equal to the degree of the induced polarization. So elliptic curves with bounded degree have bounded exponent, and the theorem follows.

We define the function

$$N_A(t)$$

counting the number of elliptic curves in A with degree bounded by t.

2.3. Product Abelian surfaces

Consider an Abelian surface of the form $E \times E'$ where E, E' are elliptic curves. There is a natural isomorphism

$$\mathbb{Z}^2 \oplus Hom(E, E') \xrightarrow{\sim} NS(E \times E')$$

$$(a, b; f) \longmapsto (b-1)[E_h] + (a - \deg(f))[E'_v] + [\Gamma_{-f}],$$

where $E_h := E \times \{0\}$ and $E'_v := \{0\} \times E'$ are the 'horizontal' and the 'vertical' factor, and Γ_{-f} is the graph of the homomorphism $-f$. The intersection form on $NS(E \times E')$ is expressed as

$$D \cdot D' \;=\; ab' + ba' - \big(\deg(f + f') - \deg(f) - \deg(f')\big)$$

if the divisors D and D' arise as above from the data $(a, b; f)$ and $(a', b'; f')$.

This is a special case of the description of correspondences between two curves in terms of homomorphisms between the associated Jacobian varieties (cf. e.g. [2], Theorem 11.5.1) and also is a special case of a result of Kani ([8], Proposition 61) for the Néron Severi group of a product Abelian variety.

2.4. Elliptic curves in a product Abelian surface

Using the description of $NS(E \times E')$ in §2.3 above and the characterization of elliptic curves in an Abelian surface in §2.1, we can now describe the collection of elements $(a, b; f)$ in the group $\mathbb{Z}^2 \oplus Hom(E, E')$ such that the corresponding divisor class $[D]$ is the class of an elliptic curve in $E \times E'$.

Besides the condition of primitivity of the element $(a, b; f)$, the numerical condition $D \cdot D = 0$ becomes

$$ab = \deg(f)$$

and the positivity condition $D \cdot H > 0$ is equivalent to

$$a + b > 0$$

(using the ample divisor $H := E_h + E'_v$).

If on $E \times E'$ we choose a split polarization $L = mE_h + nE'_v$, where m, n are positive integers, then the degree of divisors with respect to the polarization is given by the linear function

$$\deg(D) = am + bn$$

if D corresponds to $(a, b; f)$.

When E and E' are not isogenous then clearly E_h and E'_v are the only elliptic curves in $E \times E'$. When E and E' are isogenous, the graphs of homomorphisms $E \to E'$ form an infinite collection of elliptic curves in $E \times E'$.

2.5. Reducibility

We will make use of the Poincaré reducibility theorem with respect to a polarization, in the following form.

If A is a polarized Abelian variety and B is an Abelian subvariety of A, there is a unique Abelian subvariety B' of A such that the sum homomorphism $B \times B' \to A$ is an isogeny and the pullback polarization on $B \times B'$ is the sum of the pullback polarizations from B and B' (cf. [2], Theorem 5.3.5 and Corollary 5.3.6).

2.6. A result from Number Theory

The following is a classical problem in Number Theory, originating from Gauss' circle problem. Given a compact convex subset K in $\mathbb{R}^2$, estimate the number $N := \operatorname{card}(\mathbb{Z}^2 \cap K)$ of integer vectors (or lattice points) belonging to the convex set. This number is naturally approximated by the area A of the subset, and then the question is to estimate the (error or) discrepancy $N - A$. The following estimate is due to Nosarzewska [9]. If K is a compact convex region in $\mathbb{R}^2$ of area A whose boundary is a Jordan curve of length L then

$$N \leq A + \frac{1}{2}L + 1.$$

We will apply this result through the following consequence. For every scale factor $t \in \mathbb{R}_{\geq 0}$ denote by $N(t)$ the number of lattice points in the deformed region $\sqrt{t}\,K$. Then

$$N(t) \leq A\,t + \frac{L}{2}\,t^{1/2} + 1.$$

The inequality above is valid for arbitrary t. But in an asymptotic estimate

$$N(t) = A\,t + O(t^e)$$

(an implicit inequality holding for $t \gg 0$) the exponent e may be lowered, and precisely one can take

$$e = 33/104 = 0.317\ldots$$

This follows from a result of Huxley [5].

3. Summary of previous results, with correction

3.1. The homomorphism group and the degree form

For the basic theory of elliptic curves we refer to [10]. Let E, E' be elliptic curves. The homomorphism group $Hom(E, E')$ is a free abelian group of rank at most 2, and the degree map

$$Hom(E, E') \longrightarrow \mathbb{Z}$$

such that $f \longmapsto \deg(f)$ is a quadratic form.

Assume now that the elliptic curves E, E' are isogenous, i.e. that the group $Hom(E, E')$ has rank > 0. Denote by

d the minimum nonzero value of the degree form

and let $\varphi : E \longrightarrow E'$ be an isogeny of minimum degree d.

If the group $Hom(E, E')$ has rank 1, one has the isomorphism $\mathbb{Z} \xrightarrow{\sim} Hom(E, E')$ given by $x \longmapsto x\varphi$. For every $x \in \mathbb{Z}$ one has $\deg(x\varphi) = x^2 d$ and this describes the degree form.

Assume now that $Hom(E, E')$ has rank 2. This happens if and only if E has complex multiplication, and the same is for E'. In this case there is an isomorphism $\mathbb{Z}^2 \xrightarrow{\sim} Hom(E, E')$ and the degree form is expressed as a binary quadratic form. So, when the elliptic curves have complex multiplication, we denote by

δ the discriminant of the degree form.

Explicit descriptions of the homomorphism group and the degree form, in presence of complex multiplication, are given in §3.3.

Remark that both d and δ only depend on the unordered pair E, E'. This is because the isomorphism $Hom(E, E') \longleftrightarrow Hom(E', E)$, sending a homomorhism f to the dual homomorphism $\widehat{f}$, preserves the degree forms.

3.2. Estimate for the counting function

Consider a product Abelian surface $E \times E'$ endowed with a split polarization. Assume that E, E' are isogenous elliptic curves. Together with the invariants d and δ introduced in §3.1 above, we also define

m the minimum of $\deg(E)$ and $\deg(E')$, the degrees with respect to the polarization.

THEOREM 3.1. *If E, E' are isogenous, there is an asymptotic estimate*

$$N_{E\times E'}(t) = C\, t^{r-1} + O(t^i),$$

with $r = 3$ when E, E' admit no complex multiplication and $r = 4$ when E, E' have complex multiplication, the constant C being given by

$$\frac{\pi}{4\sqrt{d}\, m^2} \quad \textit{for } r = 3, \qquad \frac{\pi}{3\sqrt{-\delta}\, m^3} \quad \textit{for } r = 4,$$

the exponent i being

$$0 \quad \textit{for } r = 3, \qquad \tfrac{85}{52} = 1.634\ldots \quad \textit{for } r = 4.$$

The proof given in [4], §5.2, actually works without modification with the new definition of the quantity δ and independently of the order chosen for the factor curves. While the expression for δ given in [*ibid.*], §3.2, needs to be corrected, as is explained in the following section.

REMARK 3.2: In the statement of Theorem 3.1 the exponent which gives the order of growth of the asymptotic estimate has been written as $r - 1$ in order to remind the interpretation of r as the rank of the group $NS(E \times E')$. In higher dimensions such a purpose seems not to be meaningful any more. It must be noticed moreover that the estimate in Theorem 3.1 is slightly sharper than the estimate which is obtained from Theorem 1.1 in the special case $k = 2$ (in the earlier estimate the numerical part of the constant C is smaller and the exponent i is smaller in the case with no complex multiplication).

3.3. Computing the degree form

We use the representation of an elliptic curve E as the quotient $\mathbb{C}/\Lambda$ where $\Lambda = \langle 1, \tau\rangle$ is the lattice in $\mathbb{C}$ associated to a modulus τ for E, a complex number with positive imaginary part, that is determined up to the natural action of $SL(2, \mathbb{Z})$.

Let E and E' be elliptic curves, that we identify with $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ with $\Lambda = \langle 1, \tau\rangle$ and $\Lambda' = \langle 1, \tau'\rangle$ for suitable moduli τ and τ'. There is the natural identification

$$Hom(E, E') \longleftrightarrow \{\alpha \in \mathbb{C} \text{ s.t. } \alpha\Lambda \subseteq \Lambda'\} =: \mathcal{H}.$$

Assume that there is an isogeny $E \to E'$. In this case, according to [4], Lemma 3.1, we can choose moduli τ and τ' such that

$$\tau' = \ell\tau \quad \text{and} \quad \ell = \frac{p}{q}$$

with p, q coprime positive integers. If the homomorphism group $Hom(E, E')$ has rank 1 the situation is clear (see §3.1).

Assume now that $Hom(E, E')$ has rank 2. Then E has complex multiplication, and the same is for E'. Therefore the modulus τ is algebraic of degree 2 over $\mathbb{Q}$. So, assume that τ satisfies the equation

$$\tau^2 + \frac{u}{w}\tau + \frac{v}{w} = 0$$

with u, v, w in $\mathbb{Z}$ such that $w > 0$ and $(u, v, w) = (1)$ and moreover

$$u^2 - 4vw < 0$$

as τ is an imaginary complex number.

Remark 3.3: In the previous paper [4] in Lemma 3.4 we made a wrong assertion (the error in the proof is the claim that certain three coefficients are always coprime). Although some (slightly different) statement of the same kind is nevertheless true, it turns out to be however unnecessary for the purposes of the paper. This is because the subsequent statements, Proposition 3.5 and Proposition 3.6, and their proofs, can be slightly modified so to provide general expressions for the degree form and its discriminant. The new statements are given just below.

From the pairs w, p and v, q, dividing in each pair by the greatest common divisor, we obtain coprime pairs

$$\bar{w}, \bar{p} \quad \text{and} \quad \bar{v}, \bar{q}.$$

Moreover, since p, q are coprime, we can write

$$u = pp' + qq'$$

for suitable integers p', q'.

Proposition 3.4. *An explicit isomorphism $\mathbb{Z}^2 \xrightarrow{\sim} \mathcal{H}$ is given by*

$$(x, y) \longmapsto (xp + y\bar{p}\bar{q}q') + (y\bar{w}\bar{q})(\ell\tau).$$

Proof. The part of the proof which has to be adjusted is the analysis of the conditions for a complex number $\alpha = a + b(\ell\tau)$ to be an element of $\mathcal{H}$, namely the conditions that the rational numbers $b(p/q)(v/w)$ and $a(q/p) - b(u/w)$ be

integers. In particular, this requires that $bp(v/w)$ and $bp(u/w)$ are integers. Since u, v, w are coprime, it follows that $w \mid bp$ and hence that $\bar{w} \mid b$.

The full condition $(bp/w)(v/q) \in \mathbb{Z}$ means that $q \mid (bp/w)v$, that is $\bar{q} \mid (bp/w) = (b/\bar{w})\bar{p}$, and hence that $\bar{q} \mid (b/\bar{w})$ and $\bar{w}\bar{q} \mid b$. So the first condition above is satisfied if and only if one has $b = \bar{w}\bar{q}y$ with $y \in \mathbb{Z}$.

Then the second condition above requires that $aq - (bp/w)u$ belongs to $p\mathbb{Z}$, that is $aq - (\bar{p}\bar{q})yu \in p\mathbb{Z}$, that is $(\bar{p}\bar{q})yu = aq + a'p$ for some integer a'. Since p, q are coprime, the solutions are of the form $(a', a) = \bar{p}\bar{q}y(p', q') + x(-q, p)$ with $x \in \mathbb{Z}$. Thus $a = xp + y\bar{p}\bar{q}q'$, as in the statement. □

PROPOSITION 3.5. *The degree of the homomorphism $f : E \to E'$ corresponding to $(x, y) \in \mathbb{Z}^2$ is given by*

$$\deg(f) = x^2(pq) + xy(\bar{p}\bar{q})(qq' - pp') + y^2(\bar{p}\bar{q})(-\bar{p}\bar{q}p'q' + \bar{v}\bar{w}).$$

The discriminant of the quadratic form $f \mapsto \deg(f)$ on $Hom(E, E')$ is equal to

$$\delta = (\bar{p}\bar{q})^2\big(u^2 - 4vw\big).$$

Proof. What is only to be adjusted is the computation of $\deg(f)$ as

$$\begin{vmatrix} a & -b\ell(v/w) \\ b & (a/\ell) - b(u/w) \end{vmatrix} = \begin{vmatrix} xp + y\bar{p}\bar{q}q' & -y\bar{p}\bar{v} \\ y\bar{w}\bar{q} & xq - y\bar{p}\bar{q}p' \end{vmatrix},$$

where we used the expressions for a, b given in the previous proposition: it leads to the expression given in the statement. It is also easy to calculate the discriminant δ of this quadratic form in x, y. □

When the elliptic curves are isomorphic, the preceding formulas are simplified. In this case we have $p = q = 1$ and we can choose $p' = 0$, $q' = u$. Thus, in this particular case, the expressions given in the previous paper are indeed correct.

4. Homomorphisms with bounded degree

We present a result on the asymptotic behavior of the degree form

$$Hom(E, E') \longrightarrow \mathbb{Z}$$

that will be needed in the following. Define

$$\Phi(t)$$

to be the number of homomorphisms f having $\deg(f) \leq t$.

PROPOSITION 4.1. *Let E, E' be isogenous elliptic curves. The function $\Phi(t)$ admits the following asymptotic estimates:*

(*i*) *if E, E' are without complex multiplication then*

$$\Phi(t) = \frac{2}{\sqrt{d}} t^{1/2} + O(1)$$

where d is the minimum nonzero value of the degree form;

(*ii*) *if E, E' have complex multiplication then*

$$\Phi(t) = \frac{2\pi}{\sqrt{-\delta}} t + O(t^e)$$

where δ is the discriminant of the degree form and e is the exponent appearing in §2.6.

Proof. We have seen in §3.1 how the degree form $f \longmapsto \deg(f)$ can be expressed in terms of coordinates. (*i*) In this case there is one coordinate x and the degree form is expressed as $x \longmapsto x^2 d$; the inequality $x^2 d \leq t$ admits precisely $2 \left\lfloor \frac{1}{\sqrt{d}} t^{1/2} \right\rfloor + 1$ solutions. (*ii*) In this case, in terms of two coordinates, the degree form is expressed as a positive definite quadratic form $Q(x, y)$ with discriminant $\delta < 0$. Because of the result from Number Theory quoted in §2.6, the number of integer solutions of the inequality $Q(x, y) \leq t$ admits an estimate of the form $At + O(t^e)$ where A is the area of the ellipse $Q(x, y) \leq 1$ in $\mathbb{R}^2$, that is given by $2\pi/\sqrt{-\delta}$. □

5. Elliptic curves in a product Abelian variety

Let S be an Abelian variety, let F be an elliptic curve, and consider the product Abelian variety $A = S \times F$. We denote, for an arbitrary Abelian variety, with the symbol

$$\mathsf{EC}(A)$$

the collection of homology classes $\gamma = [C]$ in $H_2(A, \mathbb{Z})$ corresponding to elliptic curves C in A. We now describe the collection $\mathsf{EC}(A)$ for a product Abelian variety $A = S \times F$. Denote by $S_h := S \times \{0\}$ and by $F_v := \{0\} \times F$ the horizontal and the vertical factors in A.

If C is an elliptic curve in A, different from F_v, then $D = pr_1(C)$ is an elliptic curve in S, corresponding to an element $\gamma = [C]$ in the Néron Severi group $NS(D \times F)$. This group is described (see §2.3) by means of an isomorphism

$$\mathbb{Z}^2 \oplus Hom(D, F) \xrightarrow{\sim} NS(D \times F).$$

There is moreover the composite isomorphism

$$\mathbb{Z}^2 \oplus Hom(F, D) \xrightarrow{\sim} NS(F \times D) \xrightarrow{\sim} NS(D \times F)$$

where the right hand arrow is induced by the obvious isomorphism $j : F \times D \longrightarrow D \times F$, and this composite isomorphism turns out to be

$$(u, v; g) \longmapsto (u - \deg(g))[D_h] + (v - 1)[F_v] + [j_* \Gamma_{-g}].$$

In order to take into account at one time all possible elliptic curves D in S, we introduce the product $\mathbb{Z}^2 \times Hom'(F, S)$, where the superscript means nonzero homomorphisms, and the correspondence

$$C : \mathbb{Z}^2 \times Hom'(F, S) \longrightarrow H_2(S \times F, \mathbb{Z})$$

$$C(u, v; g) := (u - \deg(g))[D(g)_h] + (v - 1)[F_v] + [j_* \Gamma_{-g}]$$

where by definition $D(g) = g(F)$ and $\deg(g)$ denotes the degree of the induced isogeny $F \to g(F)$. Here j denotes the obvious isomorphism $j : F \times S \longrightarrow S \times F$.

So we define the set of "parameter data"

$$\mathsf{D}(S \times F)$$

consisting of all elements $(u, v; g)$ in $\mathbb{Z}^2 \times Hom'(F, S)$ such that

$$(u, v; g) \text{ is primitive, } uv = \deg(g) \text{ and } u + v > 0.$$

Here the word primitive clearly refers to the module $\mathbb{Z}^2 \oplus Hom(F, S)$.

THEOREM 5.1. *There is a bijective correspondence*

$$\mathsf{D}(S \times F) \longleftrightarrow \mathsf{EC}(S \times F) \setminus \Big(\mathsf{EC}(S_h) \cup \big\{[F_v]\big\}\Big)$$

induced by the correspondence C defined above.

Proof. Let C be an elliptic curve in $S \times F$ different from F_v. The projection of C into S is an elliptic curve D and the class of C in $NS(D \times F)$ is represented by a divisor of the form $(u - \deg(f))D_h + (v - 1)F_v + j_* \Gamma_{-f}$ where f is a homomorphism $F \to D$ and the conditions $(u, v; f)$ primitive and $uv = \deg(f)$ are satisfied. Note that $f = 0$ if and only if $C = D_h$ is contained in S_h (since $C \neq F_v$). Because the condition $uv = \deg(f) = 0$ admits two primitive solutions, $(1, 0; 0)$ and $(0, 1; 0)$, corresponding to the classes of D_h and F_v, respectively. If g denotes the composite homomorphism $F \to D \hookrightarrow S$ and if $f \neq 0$ then $D(g) = D$ and the class of C arises from the element $(u, v; g)$

belonging to $\mathsf{D}(S \times F)$. This shows that the correspondence in the statement is surjective.

In order to prove that the correspondence is injective, consider the homomorphism $H_2(S \times F, \mathbb{Z}) \longrightarrow H_2(S, \mathbb{Z})$ induced by the first projection map. It maps $[C(u, v; g)] \longmapsto u[D(g)]$. If $(u, v; g)$ and $(u', v'; g')$ define the same class in $H_2(S \times F, \mathbb{Z})$ then $u[D(g)] = u'[D(g')]$. Since $g, g' \neq 0$ then $u, u' \neq 0$ and therefore $[D(g)] = [D(g')]$ and $u = u'$, as the class of an elliptic curve is primitive. And then $D(g) = D(g')$ since the homology class uniquely determines the elliptic curve. Furthermore, working with the homomorphism $H_2(S \times F, \mathbb{Z}) \longrightarrow H_2(F, \mathbb{Z})$ induced by the second projection map, we also find that $v = v'$.

Let D be the elliptic curve $D(g) = D(g')$. The inclusion $D \hookrightarrow S$ induces injective homomorphisms $H_i(D, \mathbb{Z}) \longrightarrow H_i(S, \mathbb{Z})$ for $i = 1, 2$. Therefore the homomorphism $H_2(D \times F, \mathbb{Z}) \longrightarrow H_2(S \times F, \mathbb{Z})$ is injective too. Hence $(u, v; g)$ and $(u', v'; g')$ define the same class in $H_2(D \times F, \mathbb{Z})$ and it follows that $g = g'$ also holds. □

Assume now that on $A = S \times F$ we are given a split polarization

$$L = \Theta_S + n\Theta_F$$

where Θ_S and Θ_F denote the pullbacks to A of a polarization on S and the principal polarization on F, respectively, and where n is a positive integer. If the polarization on S is represented by Θ then Θ_S is represented by $\Theta \times F$; similarly, Θ_F is represented by $S \times \{0\}$.

We also consider the particular case when $S = E_1 \times \cdots \times E_k$ is a product of elliptic curves, endowed with a split polarization

$$\Theta_S = m_1\Theta_1 + \cdots + m_k\Theta_k,$$

where Θ_i denotes the pullback to A of the principal polarization on the ith factor and the coefficients m_i are positive integers. Note that in this case a homomorphism $g : F \longrightarrow S$ is given by a sequence $h_1, \ldots, h_k$ of homomorphisms $h_i : F \longrightarrow E_i$.

THEOREM 5.2. *The degree function* $\mathsf{D}(S \times F) \longrightarrow \mathbb{Z}$ *is given by*

$$\deg C(u, v; g) \;=\; u\, D(g) \cdot \Theta + n\, v.$$

In the particular case $S = E_1 \times \cdots \times E_k$*, one has the expression*

$$\deg C(u, v; g) \;=\; \frac{m_1 \deg(h_1) + \cdots + m_k \deg(h_k)}{v} + n\, v.$$

Proof. We need the following intersection numbers:

$$\begin{aligned} &D(g)_h \cdot L = D(g) \cdot \Theta, \\ &F_v \cdot L = n, \\ &j_*\Gamma_{-g} \cdot L = \deg\ g^*(\Theta) + n = \deg(g)\ D(g) \cdot \Theta + n\,. \end{aligned}$$

Therefore for the intersection number $C(u, v; g) \cdot L$ we find the expression

$$(u - \deg(g))\ D(g) \cdot \Theta + (v-1)n + \deg(g)\ D(g) \cdot \Theta + n = u\ D(g) \cdot \Theta + n\ v.$$

In the particular case, we need the following intersection number:

$$\begin{aligned} D(g) \cdot \Theta\ &=\ m_1 \# g\, h_1^{-1}(0) + \cdots + m_k \# g\, {h_k}^{-1}(0) \\ &=\ m_1 \frac{\deg(h_1)}{\deg(g)} + \cdots + m_k \frac{\deg(h_k)}{\deg(g)}. \end{aligned}$$

Hence, because of the condition $uv = \deg(g) \neq 0$, we have for $\deg C(u, v; g)$ the expression

$$\begin{aligned} u\ &\frac{m_1 \deg(h_1) + \cdots + m_k \deg(h_k)}{\deg(g)} + n\ v \\ &=\ \frac{m_1 \deg(h_1) + \cdots + m_k \deg(h_k)}{v} + n\ v. \end{aligned}$$

□

6. On the number of elliptic curves

Let $A = E^k$, with $k \geq 2$, be the kth self product of an elliptic curve E, endowed with a split polarization $L = m_1\Theta_1 + \cdots + m_k\Theta_k$, where Θ_i denotes the pullback to A of the principal polarization on the ith factor and the coefficients m_i are positive integers.

We keep the notation of §5, writing $A = E^{k-1} \times E$, and defining $(E^{k-1})_h := E^{k-1} \times \{0\}$ and $E_v := \{(0, \ldots, 0)\} \times E$. Let moreover m be the minimum among the coefficients $m_1, \ldots, m_k$.

The set $\mathsf{EC}(E^k)$ is the disjoint union of $\mathsf{EC}((E^{k-1})_h) \cup \big\{[E_v]\big\}$ and the complementary subset which, according to Proposition 5.1, is bijective to the set of parameter data $\mathsf{D}(E^k)$. It follows that the number $N_{E^k}(t)$ is, for $t \gg 0$, the sum of

$$N_{E^{k-1}}(t) + 1$$

and the number of elements of the set

$$\Big\{(u, v; g) \text{ in } \mathsf{D}(E^k) \text{ s.t. } \deg C(u, v; g) \leq t\Big\}.$$

There is the following chain of injective maps

$$\Big\{(u,v;g) \text{ prim. s.t. } u+v>0,\ uv=\deg(g)\neq 0 \text{ and } \deg C(u,v;g)\leq t\Big\}$$
$$\downarrow$$
$$\Big\{(v;h_1,\dots,h_{k-1}) \text{ s.t. } 1\leq m_k v\leq t,\quad 1\leq \frac{m_1\deg(h_1)+\cdots+m_{k-1}\deg(h_{k-1})}{v}\leq t\Big\}$$
$$\downarrow$$
$$\Big\{(v;h_1,\dots,h_{k-1}) \text{ s.t. } 1\leq v\leq \frac{t}{m},\ \ \deg(h_i)\leq v\frac{t}{m}\Big\}$$

so the number of elements of the set of parameter data in the top of the chain is bounded above by

$$\sum_{1\leq v\leq \frac{t}{m}} \Phi\left(\frac{vt}{m}\right)^{k-1}$$

where $\Phi(t)$ is the function which counts endomorphisms of E having degree bounded by t. Let us denote the bounding function above with the symbol

$$\Phi_{E^k}(t).$$

LEMMA 6.1. *There is an asymptotic estimate*

$$\Phi_{E^k}(t) = C\,t^r + O(t^i)$$

with the same constant C and the same exponents r and i which are defined in the statement of Theorem 1.1.

Proof. This is obtained applying Proposition 4.1 for the function Φ which appears in the definition of Φ_{E^k}.

If the elliptic curve E admits no complex multiplication, for the bounding function we have the expression

$$\sum_{1\leq v\leq \frac{t}{m}} \left\{\frac{2}{\sqrt{d}}\left(\frac{vt}{m}\right)^{1/2}+O(1)\right\}^{k-1}$$

where the integer d is the minimum degree of an isogeny $E\to E$. The expression above can be written as

$$\left(\frac{2}{\sqrt{dm}}\right)^{k-1}\left(t^{(k-1)/2}\sum_{1\leq v\leq \frac{t}{m}} v^{(k-1)/2}\right)+\sum_{1\leq v\leq \frac{t}{m}} O\left((vt)^{(k-2)/2}\right)\ .$$

Now, applying the estimate for a sum of powers of integers given in Remark 6.2 below, we substitute

$$\sum_{1\le v\le \frac{t}{m}} v^{(k-1)/2} = \frac{2}{k+1}\Big(\frac{t}{m}\Big)^{(k+1)/2} + O\left(t^{(k-1)/2}\right)$$

and, writing $\sum_{1\le v\le \frac{t}{m}} v^{(k-2)/2} = O\left(t^{k/2}\right)$, we substitute

$$\sum_{1\le v\le \frac{t}{m}} O\left((vt)^{(k-2)/2}\right) = O\left(t^{(k-2)/2}\sum_{1\le v\le \frac{t}{m}} v^{(k-2)/2}\right) = O\left(t^{k-1}\right)$$

and we end with the asymptotic estimate

$$\frac{2^k/(k+1)}{(\sqrt{d})^{k-1}\,m^k}\,t^k + O(t^{k-1}).$$

If the elliptic curve E has complex multiplication, the bounding function can be written as

$$\sum_{1\le v\le \frac{t}{m}} \left\{\frac{2\pi}{\sqrt{-\delta}}\left(\frac{vt}{m}\right) + O\left((vt)^e\right)\right\}^{k-1}$$

where the integer δ is the (negative) discriminant of the degree form on $End(E)$. The expression above can be written as

$$\begin{aligned} &= \sum_{1\le v\le \frac{t}{m}} \left\{\frac{(2\pi)^{k-1}}{\left(\sqrt{-\delta}\,m\right)^{k-1}}\,(vt)^{k-1} + O\left((vt)^{e+k-2}\right)\right\} \\ &= \frac{(2\pi)^{k-1}}{\left(\sqrt{-\delta}\,m\right)^{k-1}}\left(t^{k-1}\sum_{1\le v\le \frac{t}{m}} v^{k-1}\right) + \sum_{1\le v\le \frac{t}{m}} O\left((vt)^{k-2+e}\right). \end{aligned}$$

Here, using Remark 6.2 again, we substitute

$$\sum_{1\le v\le \frac{t}{m}} v^{k-1} = \frac{1}{k}\left(\frac{t}{m}\right)^k + O\left(t^{k-1}\right)$$

and, writing $\sum_{1\le v\le \frac{t}{m}} v^{k-2+e} = O\left(t^{k-1+e}\right)$, we substitute

$$\sum_{1\le v\le \frac{t}{m}} O((vt)^{k-2+e}) = O\left(t^{k-2+e}\sum_{1\le v\le \frac{t}{m}} v^{k-2+e}\right) = O\left(t^{2k-3+2e}\right)$$

and we end with the estimate

$$\frac{(2\pi)^{k-1}/k}{(\sqrt{-\delta})^{k-1}\, m^{2k-1}}\ t^{2k-1} + O\left(t^{2k-3+2e}\right). \qquad \square$$

REMARK 6.2: (Communicated by the referee.) About partial sums of increasing functions. Let $f : [0, +\infty) \to [0, +\infty)$ be an increasing function. To estimate $\sum_{n=1}^{t} f(n)$ observe that in each interval $[n, n+1]$ it satisfies $f(n) \leq f(x) \leq f(n+1)$. It follows that for each positive integer t,

$$\int_0^t f(x)dx \leq \sum_{n=1}^{t} f(n) \leq \int_1^{t+1} f(x)dx.$$

In the case $f(x) = x^p$ (p arbitrary positive real) we get

$$\frac{t^{p+1}}{p+1} \leq \sum_{n=1}^{t} n^p \leq \frac{(t+1)^{p+1}}{p+1} - \frac{1}{p+1}$$

from which it follows that

$$\sum_{n=1}^{t} n^p = \frac{t^{p+1}}{p+1} + O(t^p).$$

If t is a positive real number, an analogous estimate holds, which in the preceding proof is written in the form $\displaystyle\sum_{1\leq n\leq t} n^p = \frac{t^{p+1}}{p+1} + O(t^p)$, where n is meant to be an integer ranging in the interval $[1, t]$.

We are now in a position to prove the result in the introduction.

Proof of Theorem 1.1. Remind that the function $N_{E^k}(t)$ is bounded above by

$$N_{E^{k-1}}(t) + 1 + \Phi_{E^k}(t).$$

We argue by induction on $k \geq 2$. The initial step $k = 2$ follows immediately from the estimate of $\Phi_{E^2}(t)$ given in Lemma 6.1 above.

When $k > 2$, if the statement holds for E^{k-1} then it holds for E^k too. In both cases, either with complex multiplication or not, by the inductive assumption we have

$$N_{E^{k-1}}(t) = O(t^{r'})$$

where, in both cases,

$$r' < r \quad \text{and} \quad r' \leq i.$$

From Lemma 6.1 we know that

$$\Phi_{E^k}(t) = Ct^r + O(t^i).$$

Hence the theorem follows. $\square$

7. Arbitrary polarized Abelian varieties

7.1. Behavior under isogenies

Let A, B be polarized Abelian varieties and let $\varphi : B \to A$ be an isogeny, preserving the polarizations (the polarization on B is the pullback of the polarization on A), whose degree we call d. There is a one to one correspondence

$$\big\{\text{elliptic curves in } A\big\} \xrightarrow{\sim} \big\{\text{elliptic curves in } B\big\}.$$

Given $E \subset A$ the corresponding E^* in B is the connected component of 0 in the pre-image $\varphi^{-1}(E)$. The restricted isogeny $E^* \to E$ has degree $d_E \leq d$ (in fact a divisor of d), and the degree of E^* is given by

$$\deg(E^*) = d_E \deg(E)$$

(by the projection formula: $E^* \cdot \varphi^* L = \varphi_* E^* \cdot L = d_E\ E \cdot L$). Therefore:

$$\deg(E) \leq \deg(E^*) \leq d \deg(E).$$

It follows that the functions counting elliptic curves in A and in B are related by the following inequalities:

$$N_A(t) \leq N_B(dt) \quad \text{and} \quad N_B(t) \leq N_A(t).$$

7.2. On the counting function

Let A be a polarized Abelian variety, of dimension n. Let us say that a sequence $E_1, \ldots, E_i$ of elliptic curves in A is *independent* if the Abelian subvariety $E_1 + \cdots + E_i$ has dimension i. If A contains i independent elliptic curves then, because of the reducibility theorem (§2.5), replacing the given elliptic curves without modifying the sequence of Abelian subvarieties $E_1 + \cdots + E_j$, with $j = 1, \ldots, i$, we can even obtain that, under the sum isogeny $E_1 \times \cdots \times E_i \longrightarrow E_1 + \cdots + E_i \subseteq A$, the pullback polarization from A is a split polarization on $E_1 \times \cdots \times E_i$.

Let k be the maximum number of independent elliptic curves in A. There is, as above, a special isogeny $E_1 \times \cdots \times E_k \longrightarrow E_1 + \cdots + E_k \subseteq A$. Moreover, every elliptic curve in A is contained in $E_1 + \cdots + E_k$. Hence, without loss of generality, we may assume that $A = E_1 + \cdots + E_k$ and that, under the sum isogeny

$$E_1 \times \cdots \times E_k \longrightarrow A,$$

the pullback polarization from A is a split polarization on $E_1 \times \cdots \times E_k$. Let d be the degree of such an isogeny. From the discussion in §7.1 above, we have

$$N_A(t) \leq N_{E_1 \times \cdots \times E_k}(dt).$$

It follows that, in order to have a general estimate of the counting function $N_A(t)$, we can reduce to the particular case in which $A = E_1 \times \cdots \times E_k$ and the polarization splits.

PROPOSITION 7.1. *The function $N_A(t)$ can be given an asymptotic estimate of the form*

$$N_A(t) = Ct^r + O(t^i)$$

for some constant C and exponents r, i with $i < r$.

Proof. According to the preceding discussion, we only need to consider the case in which $A = E_1 \times \cdots \times E_k$ is a product of elliptic curves, with a split polarization.

If the factor elliptic curves are all isogenous, we can choose one elliptic curve E together with isogenies $E \to E_i$ and then construct a product isogeny $E^k \to A$, so that the pullback polarization on E^k is a split polarization again. If d is the degree of such an isogeny then, from the discussion in §7.1, we have

$$N_A(t) \leq N_{E^k}(dt)$$

and the statement follows from Theorem 1.1.

More generally, separating the collection $E_1, \ldots, E_k$ into (maximal) isogeny classes, and rearranging, we have an isomorphism

$$E_1 \times \cdots \times E_k \cong B_1 \times \cdots \times B_h,$$

each factor B_i being a maximal product of isogenous elliptic curves from the given collection. The split polarization on $E_1 \times \cdots \times E_k$ corresponds to a split polarization on $B_1 \times \cdots \times B_h$. Define $B := B_1 \times \cdots \times B_h$ and consider the isogeny $B \longrightarrow A$. Let d be the degree of such an isogeny. From the discussion in §7.1, we have

$$N_A(t) \leq N_B(dt).$$

It is easy to see that $N_B(t) = N_{B_1}(t) + \cdots + N_{B_h}(t)$. This is because an elliptic curve in B, projecting non-trivially to different factors B_r and B_s, would therefore project onto non-isogenous elliptic curves E_i and E_j, which is impossible. From the discussion above, for a product of isogenous elliptic curves, we have

$$N_{B_\ell}(t) = C_\ell\, t^{r_\ell} + O(t^{i_\ell})$$

with $i_\ell < r_\ell$. It follows that $N_B(dt) = Ct^r + O(t^i)$, where $r = \max\{r_1, \cdots, r_h\}$ and $i < r$. □

REMARK 7.2: When $A = J(C)$ is the Jacobian of a curve of genus $g > 1$, there is an effective bound for the function $N_A(t)$ due to Kani (cf. [6], Theorem 4), which is asymptotically of order $O(t^{2g^2-2})$ (*ibid.*, p. 187). The asymptotic bound in the present paper (Theorem 1.1, Proposition 7.1) is instead of order $O(t^{2g-1})$.

Acknowledgements

The author thanks the referee for the attention dedicated to the present work; in particular, for suggesting that the original treatment should be extended to arbitrary dimension, and for contributing Remark 6.2, which was a missing information needed for the generalization.

References

[1] Ch. Birkenhake and H. Lange, *The exponent of an abelian subvariety*, Math. Ann. **290** (1991), 801–814.
[2] Ch. Birkenhake and H. Lange, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften, no. 302, Springer-Verlag, Berlin, 2004.
[3] L. Guerra, *Elliptic curves of bounded degree in a polarized abelian variety*, arXiv:1306.2007 [math.AG] (2003).
[4] L. Guerra, *On elliptic curves of bounded degree in a polarized abelian surface*, Rend. Ist. Mat. Univ. Trieste **48** (2016), 495–508.
[5] M. N. Huxley, *Exponential sums and lattice points. III*, Proc. London Math. Soc. (3) **87** (2003), 591–609.
[6] E. Kani, *Bounds on the number of nonrational subfields of a function field*, Invent. Math. **85** (1986), 185–198.
[7] E. Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), 199–223.
[8] E. Kani, *The moduli space of jacobians isomorphic to a product of two elliptic curves*, Collect. Math. **67** (2016), 21–54.
[9] M. Nosarzewska, *Évaluation de la différence entre l'aire d'une région plane convexe et le nombre des points aux coordonnées entières couverts par elle*, Colloquium Math. **1** (1948), 305–311.
[10] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer-Verlag, New York, 1986.

Author's address:

Lucio Guerra
Dipartimento di Matematica e Informatica
Università di Perugia
Via Vanvitelli 1, 06123 Perugia, Italia
E-mail: lucio.guerra@unipg.it

Received January 22, 2018
Revised May 16, 2019
Accepted May 29, 2019