Rend. Istit. Mat. Univ. Trieste
Volume 48 (2016), 495–508
DOI: 10.13137/2464-8728/13169

On elliptic curves of bounded degree in a polarized Abelian surface

Lucio Guerra

Abstract. *For a polarized complex Abelian surface A we study the function $N_A(t)$ counting the number of elliptic curves in A with degree bounded by t. We describe elliptic curves as solutions of an explicit Diophantine equation, and we show that computing the number of solutions is reduced to the classical problem in Number Theory of counting lattice points lying on an explicit bounded subset of Euclidean space. We obtain in this way some asymptotic estimate for the counting function.*

Keywords: Elliptic curve, Abelian surface, polarization, lattice points.
MS Classification 2010: 14K20, 11D45.

1. Introduction

Let A be a complex Abelian surface. With the expression 'elliptic curve in an Abelian surface' we mean a one-dimensional subtorus. The collection of all elliptic curves in A is (at most) countable (and possibly empty). Assume that A is endowed with a polarization. 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. This was known to Bolza and Poincaré, and a modern account is in the paper of Kani [4].

Denote by $N_A(t)$ the number of elliptic curves in A with degree bounded by t. The aim in the present paper is to present an approach to the counting function $N_A(t)$. The problem of bounding this function is invariant under isogenies, and the most relevant case is when A is the product $E \times E'$ of two elliptic curves, with a split polarization (the sum of two pullback polarizations from the factors). When we consider $E \times E'$ as a polarized Abelian surface we always assume that it is endowed with such a split polarization.

We show (see §4) that computing elliptic curves in $E \times E'$ is reduced to solving some explicit Diophantine equation, in terms of coordinates in the Néron Severi group $NS(E \times E')$. It turns out that computing $N_{E\times E'}(t)$ is reduced to counting points of the lattice $\mathbb{Z}^r$ lying on an explicit bounded subset of $\mathbb{R}^r$, where r is the rank of the Néron Severi group. This is a classical topic in Number Theory, originating from Gauss' circle problem and still a field of active research. So we are lead to apply some result from that field, and in this way we obtain an asymptotic estimate for the counting function.

Clearly when $r = 2$ then $N_{E\times E'}(t) = 2$. So assume that $r \geq 3$. Denote by m the minimum of $\deg(E)$ and $\deg(E')$, the degrees with respect to the polarization, and assume that $m = \deg(E')$. When $r = 3$ then E and E' are isogenous, so let d be the degree of a primitive isogeny $E \to E'$. When $r = 4$, E and E' are isogenous elliptic curves with complex multiplication; we denote by δ the discriminant of the relevant imaginary quadratic field (see §3.2). In terms of these properties, we prove (in §5.2) the following main result.

THEOREM 1.1. *Assume that $r \geq 3$. There is an asymptotic estimate*

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

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 e being

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

Finally we show that the result for a product Abelian surface implies some result holding for an arbitrary polarized Abelian surface (Proposition 6.1), and we observe that the estimates for $N_A(t)$ obtained in this way are, at least asymptotically, sharper than an existing upper bound (Remark 6.2).

2. Some preliminary material

2.1. Elliptic curves as divisor classes

Let A be an Abelian surface. Every curve $C \subset A$ determines a divisor class $[C]$ in the Néron Severi group $NS(A)$. For elliptic curves (subgroups), the induced correspondence

$$\big\{\text{elliptic curves in } A\big\} \longrightarrow NS(A)$$

is injective and the divisor classes in $NS(A)$ corresponding to elliptic curves in A are characterized by the following properties (cf. [4], Theorem 1.1):

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

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 surface (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* (cf. [4], Corollary 1.3). We define the function

$$N_A(t)$$

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

An important special case is when $A = J(C)$ is the Jacobian variety of a curve of genus 2, with the canonical polarization. Elliptic curves $E \subset J(C)$ correspond bijectively to isomorphism classes of non-constant morphisms $f : C \to E$ to an elliptic curve E, which do not factor as $C \to E' \to E$ where $E' \to E$ is a non-isomorphic isogeny, and the degree $\deg(E)$ in $J(C)$ coincides with the degree $\deg(f)$ of the corresponding morphism. As a corollary of the theorem above, it follows that: for every integer $t \geq 1$ the collection of isomorphism classes of morphisms $f : C \to E$ which do not factor through a non-trivial isogeny of E and have $\deg(f) \leq t$ is finite.

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

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

induced by the homomorphism

$$D : \mathbb{Z}^2 \oplus Hom(E, E') \longrightarrow Div(E \times E')$$

that is defined by

$$D(a, b, f) \ := \ (b-1)E_h + (a - \deg f)E'_v + \Gamma_{-f}$$

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

$$D(a, b, f) \cdot D(a', b', f') \ = \ ab' + ba' - \big(\deg(f + f') - \deg(f) - \deg(f')\big).$$

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. [1], Theorem 11.5.1) and also is a special case of a result of Kani ([5], Proposition 61) for the Néron Severi group of a product Abelian variety.

2.4. 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. [1], Theorem 5.3.5 and Corollary 5.3.6).

3. The homomorphism group

Let E and E' be elliptic curves, that we identify with E_τ and $E_{\tau'}$ for suitable moduli τ and τ', and denote by $\Lambda := \langle 1, \tau \rangle$ and $\Lambda' := \langle 1, \tau' \rangle$ the corresponding lattices in $\mathbb{C}$. There is the natural identification

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

3.1. In presence of an isogeny

Assume that there is an isogeny $E \to E'$.

Lemma 3.1. *In this case, we can choose τ such that $\Lambda = \langle 1, \tau \rangle$ and such that for some $\ell \in \mathbb{Q}_{>0}$ the complex number $\ell\tau$ is the modulus of an elliptic curve E'' isomorphic to E'.*

Proof. Assume that $\alpha \in \mathbb{C}$ represents an isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. In the present setting the lattice Λ is of the form $\langle 1, \tau \rangle$. Hence $\alpha \in \Lambda'$. Write $\alpha = p\beta$ with $\beta \in \Lambda'$ primitive and $p \in \mathbb{Z}_{>0}$.

In $\Lambda'/\langle \alpha \rangle$ the torsion submodule is $\langle \beta \rangle / \langle \alpha \rangle \cong \mathbb{Z}_p$. Since $\Lambda'/\langle \beta \rangle$ is torsion free of rank 1, one can find $\omega' \in \Lambda'$ such that

$$\Lambda' = \langle \beta, \omega' \rangle.$$

The module $\alpha\Lambda/\langle \alpha \rangle$ is a free module of rank 1 (isomorphic to $\Lambda/\mathbb{Z}$). Therefore the induced homomorphism

$$\alpha\Lambda/\langle \alpha \rangle \longrightarrow \Lambda'/\langle \beta \rangle$$

is injective. It follows that there is some multiple $q\omega'$ with $q \in \mathbb{Z}_{>0}$ such that $q\omega' \in \alpha\Lambda$, thus $q\omega' = \alpha\omega$ with $\omega \in \Lambda$, and moreover

$$\alpha\Lambda = \langle \alpha, q\omega' \rangle,$$

whence it follows that

$$\Lambda = \langle 1, \omega \rangle.$$

Note that $\Lambda'/\alpha\Lambda \cong \mathbb{Z}_p \times \mathbb{Z}_q$, so the degree of the given isogeny is pq.

We can choose ω' with $\mathrm{im}(\omega') > 0$ and, replacing α with $-\alpha$ if necessary, we obtain that $\mathrm{im}(\omega) > 0$. We can replace the initial τ with this ω. Then define $\omega'' := \omega'/\beta = (p/q)\omega$ and define $\Lambda'' := \langle 1, \omega'' \rangle$. Clearly β represents an isomorphism $\mathbb{C}/\Lambda'' \to \mathbb{C}/\Lambda'$ and the modulus ω'' for $\mathbb{C}/\Lambda''$ is as in the statement. (Note, by the way, that p represents an isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda''$ that, followed by the isomorphism β, gives the initial isogeny α.) □

Remark 3.2. In the setting of the proof above, we see that α defines a primitive isogeny if and only if it defines a cyclic isogeny, and both conditions are equivalent to p, q being coprime integers.

It is enough to observe that: if t is an integer, then $(1/t)\alpha$ sends $\Lambda = \langle 1, \omega \rangle$ into $\Lambda' = \langle \beta, \omega' \rangle$ if and only if t is a common divisor of p, q; on the other hand, the quotient $\Lambda'/\alpha\Lambda \cong \mathbb{Z}_p \times \mathbb{Z}_q$ is a cyclic group if and only if p, q are coprime.

It is well known that an isogeny of minimum degree between two given elliptic curves is a cyclic isogeny (cf. [6], Lemma 6.2).

Assume now that E and E' are isogenous elliptic curves, and assume that they have moduli τ and τ' as in the Lemma, with

$$\tau' = \ell\tau$$

and $\ell = p/q$ with p, q coprime positive integers. Then clearly $\mathcal{H}$ contains the integer p (corresponding to some primitive isogeny of degree pq) and also the subset $p\mathbb{Z}$.

Remark 3.3. If f is the homomorphism corresponding to $x \in \mathbb{Z}$, then

$$\deg(f) = x^2(pq).$$

Because f is just multiplication by x in E followed by the given isogeny $E \to E'$, of degree pq.

3.2. In presence of complex multiplication

Let us continue with the same setting (E and E' isogenous, $\Lambda = \langle 1, \tau \rangle$ and $\Lambda' = \langle 1, \tau' \rangle$, with $\tau' = \ell\tau$). We may assume that the given isogeny is primitive.

Assume now that the homomorphism group $Hom(E, E')$ has rank > 1. Then E has complex multiplication, and the same is for E'. Therefore the modulus τ is algebraic of degree 2 over $\mathbb{Q}$ (cf. e.g. [9], Chapter VI, Theorem 5.5). 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

$$\delta := u^2 - 4vw < 0$$

as τ is an imaginary complex number. Note that $\delta \equiv 0, 1 \pmod 4$.

Lemma 3.4. *In the equation above we also have that $p \mid w$ and $q \mid v$.*

Proof. The quadratic equation for τ is related to the quadratic equation for $\ell\tau$ over $\mathbb{Q}$, that we write as $\left(\frac{p}{q}\tau\right)^2 + \frac{u'}{w'}\left(\frac{p}{q}\tau\right) + \frac{v'}{w'} = 0$, where u', v', w' are coprime integers with w' positive. Divide both w', q by their greatest common divisor and denote by $\tilde{w}, \tilde{q}$ the resulting coprime pair, and similarly define a coprime pair $\tilde{v}, \tilde{p}$ obtained from v', p. So we have

$$\tau^2 + \frac{u'\tilde{p}\tilde{q}}{\tilde{w}\tilde{p}p}\tau + \frac{\tilde{v}\tilde{q}q}{\tilde{w}\tilde{p}p} = 0,$$

and it is easily seen that $u = u'\tilde{p}\tilde{q}$, $v = \tilde{v}\tilde{q}q$, $w = \tilde{w}\tilde{p}p$ have no common divisor: because $\tilde{v}\tilde{q}q, p$ and $\tilde{w}\tilde{p}p, q$ are coprime pairs, and because u', v', w' have no common divisor. □

Thus we define

$$\bar{w} := w/p \quad \text{and} \quad \bar{v} := v/q.$$

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

$$u = pp' + qq'$$

for suitable integers p', q'.

Proposition 3.5. *In the present setting, an explicit isomorphism $\mathbb{Z}^2 \to \mathcal{H}$ is given by*

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

Proof. Let $\alpha \in \mathbb{C}$ represent an homomorphism $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, i.e. both α and $\alpha\tau$ belong to Λ'. Write $\alpha = a + b(\ell\tau)$ with a, b integers. Then

$$\alpha\tau = -(b\ell v/w) + ((a/\ell) - (bu/w))(\ell\tau).$$

Hence $\alpha\tau \in \Lambda'$ if and only if

$$b\ell(v/w),\ a/\ell - b(u/w)\ \in \mathbb{Z}.$$

So the set $\mathcal{H}$ consists of the complex numbers $\alpha \in \Lambda'$ which satisfy the two conditions above.

The map $\mathbb{Z}^2 \to \mathbb{C}$ defined in the statement restricts to $\mathbb{Z}^2 \to \mathcal{H}$, as is easily checked using the conditions above. It is clearly an injective homomorphism and we have to show that it is surjective.

Let α be an element of $\mathcal{H}$. In the representation given above we have that $b(\bar{v}/\bar{w}) \in \mathbb{Z}$ and $aq - b(u/\bar{w}) \in p\mathbb{Z}$, and in particular $b(\bar{v}/\bar{w})$ and $b(u/\bar{w})$ are integers. Since u, v, w are coprime, it follows that $\bar{w} \mid b$, and the first condition above is satisfied. So write

$$b = y\bar{w}$$

with $y \in \mathbb{Z}$. Then the second condition above requires that $yu = aq + a'p$ for some integer a'. Since p, q are coprime, the solutions are of the form $(a', a) = y(p', q') + x(-q, p)$ with $x \in \mathbb{Z}$. Thus

$$a = xp + yq'.$$

This proves that α belongs to the image of the map in the statement. □

Proposition 3.6. *The degree of the homomorphism $f : E \to E'$ corresponding to $(x, y) \in \mathbb{Z}^2$ is given by*

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

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

Proof. With the notation of the preceding proof, the degree is given by the absolute value of the determinant of the submodule $\alpha\Lambda$ in Λ', that is

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

where we used the expressions for a, b given in the preceding proof. It is then easy to calculate that the determinant is equal to the expression given in the statement. It is also easy to check that the discriminant of this quadratic form in x, y is given by $u^2 - 4(pq)(\bar{v}\bar{w}) = u^2 - 4vw = \delta$. □

4. Elliptic curves in a product Abelian surface

Consider an Abelian surface of the form $E \times E'$ where E, E' are elliptic curves. Let r be the rank of the Néron Severi group $NS(E \times E')$. We have (see §2.3) a natural isomorphism

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

and we can describe (see §2.1) the collection of elements (a, b, f) in the group $\mathbb{Z}^2 \oplus Hom(E, E')$ such that the corresponding divisor class $[D(a, b, f)]$ 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 $L = mE_h + nE'_v = D(n, m, 0)$, where m, n are positive integers, then the degree $\deg(D) = D \cdot L$ with respect to the polarization is given by the linear function

$$am + bn.$$

Furthermore, we have (see §3) a description of the group of homomorphisms between two elliptic curves, i.e. an explicit isomorphism

$$Hom(E, E') \longleftrightarrow \mathbb{Z}^h$$

where h is the rank of the homomorphism group. So we have an explicit isomorphism

$$NS(E \times E') \longleftrightarrow \mathbb{Z}^r$$

where $r = h + 2$ is the rank of the Néron Severi group, and in terms of coordinates in $\mathbb{Z}^r$ the description of elliptic curves in $E \times E'$ can be written as a Diophantine equation, with some limitation. We will study the equation according to the values of the rank r.

The case $r = 2$, i.e. $h = 0$, is when E and E' are not isogenous. Clearly E_h and E'_v are the only elliptic curves in $E \times E'$. When E and E' are isogenous, i.e. $r \geq 3$ and $h \geq 1$, there are infinitely many elliptic curves in $E \times E'$, the graphs of homomorphisms $E \to E'$. Then (see §3) we have $r = 4$ if and only if both E and E' have complex multiplication.

For small values of the degree $am + bn$, it is sometimes possible to compute all solutions of the Diophantine equation.

Example 4.1. Elliptic curves of degree at most 2. The maximum number is attained only if on $E \times E'$ is given the principal split polarization ($m = n = 1$). So assume this is the case. The only elliptic curves of degree 1 are E_h and E'_v. An elliptic curve of degree 2 must be the graph of an isomorphism $E \xrightarrow{\sim} E'$ (follows from $ab = \deg(f)$). Hence, without loss of generality, we may assume that $E = E'$ (and $\ell = 1$). In the self product E^2 the diagonal and the anti-diagonal are elliptic curves of degree 2. If E has no complex multiplication, these are the only ones. *If E has complex multiplication, the* *maximum number of elliptic curves of degree* 2 *in* E^2 *is equal to* 6*, and is attained if and only if* $\delta = -3$. The degree form is written as $x^2 - uxy + vwy^2$, equal to $\big((2x-uy)^2 - \delta t^2\big)/4$, and we only have to compute the solutions of $(2x-uy)^2 - \delta t^2 = 4$ (where $\delta \equiv 0, 1 \pmod 4$). Two solutions are $(\pm 1, 0)$ for every δ, that give the diagonal and the anti-diagonal; for more solutions we must have $-\delta = 3, 4$; if $-\delta = 4$ two more are $\pm(u/2, 1)$, if $-\delta = 3$ four more are $\pm((u \pm 1)/2, 1)$.

Remark 4.2. The following result is found in a recent paper by Rosen and Schnidman ([8], Lemma 2.10): in a polarized Abelian surface with polarization degree ≥ 5 there is at most one elliptic curve of degree 2.

5. On the number of elliptic curves

5.1. 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 [7]. 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 [2].

5.2. Estimate for the counting function

Let $E \times E'$ be a product Abelian surface, endowed with a split polarization. Let r be the rank of the Néron Severi group $NS(E \times E')$ and assume that

$r \geq 3$. Here we prove the result in the introduction, asserting that there is an asymptotic estimate $N_{E\times E'}(t) = Ct^{r-1} + O(t^e)$, with the constant C and the exponent e as given in the statement.

Proof of Theorem 1.1. We work in terms of coordinates, as explained in §4. The degree with respect to the polarization is given by the linear function $am + bn$. We assume that $m \leq n$, so that $m = \deg(E'_v)$ is the minimum degree occurring in the statement. Define $t' := [t/m]$, and assume that $t' \geq 1$ since otherwise the inequality $am + bn \leq t$ has no nonzero solution.

We have to estimate the collection of primitive vectors (a, b, f) in $\mathbb{Z}^2 \times Hom(E, E')$ such that $ab = \deg(f)$ and $a + b > 0$ and $am + bn \leq t$. Note that $a + b > 0$ may be replaced with $a, b \geq 0$. There are at most two such vectors with $ab = 0$, since then $f = 0$. The subcollection with $ab \neq 0$ is mapped, forgetting b, to the collection

$$\big\{(a, f) \;\text{ s.t. }\; f \neq 0,\;\; 0 < a < t',\;\; \deg(f) \leq a(t' - a)\big\}$$

and the map is injective. Therefore we have

$$N_{E\times E'}(t) \leq 2 + \sum_{a=0}^{t'} R(a, t)$$

where $R(a, t)$ is the number of nonzero f such that $\deg(f) \leq a(t' - a)$. The function $R(a, t)$ can be estimated, according to the values of the rank $r = h+2$, using the description of the quadratic form $\deg(f)$ given in §3.

When $r = 3$ then $R(a, t)$ is the number of nonzero $x \in \mathbb{Z}$ such that $x^2 d \leq a(t' - a)$, where d is the degree of a primitive isogeny $E \to E'$, by Remark 3.3, and hence $R(a, t) \leq \frac{2}{\sqrt{d}} \big(a(t' - a)\big)^{1/2}$. We will show in Remark 5.1 below that

$$\sum_{a=0}^{t'} \big(a(t' - a)\big)^{1/2} = \frac{\pi}{8}\, t'^2 + O(1).$$

Therefore, since $t' \leq t/m$, in this case we have the asymptotic estimate

$$N_{E\times E'}(t) = \frac{\pi}{4\sqrt{d}\, m^2}\, t^2 + O(1).$$

When $r = 4$ then $R(a, t)$ is the number of nonzero vectors $(x, y) \in \mathbb{Z}^2$ such that $Q(x, y) \leq a(t' - a)$, where $Q(x, y)$ is the coordinate expression for the quadratic form $\deg(f)$, given in Proposition 3.6, whose determinant is equal to $-\delta$. Applying the result in §5.1 we have

$$R(a, t) = A\, a(t' - a) + O((a(t' - a))^e)$$

with $e = 33/104$, where $A = 2\pi/\sqrt{-\delta}$ is the area of the region $Q(x, y) \leq 1$ in $\mathbb{R}^2$. Remark here that for every a the discrepancy above arises from a single discrepancy function $N(t) - At$. It follows that

$$\sum_{a=0}^{t'} R(a,t) = A\left(\sum_{a=0}^{t'} a(t'-a)\right) + O\left(\sum_{a=0}^{t'} \big(a(t'-a)\big)^e\right).$$

We have to estimate the summations occurring in this formula. For one summation we have an exact formula

$$\sum_{a=0}^{t'} a(t'-a) = \frac{1}{6}t'(t'+1)(t'-1).$$

For the other summation, using a basic approximation method as explained in Remark 5.1 below, we find the asymptotic estimate

$$\sum_{a=0}^{t'} \big(a(t'-a)\big)^e = O({t'}^{2e+1}).$$

Summing up, we obtain for the function $N_{E\times E'}(t)$ an estimate that is a function of t' and then, using $t' \leq t/m$, we obtain one that is a function of t. Explicitely, we find the asymptotic estimate

$$N_{E\times E'}(t) = \frac{A}{6}\left(\frac{t^3}{m^3} - \frac{t}{m}\right) + O(t^{2e+1}) = \left(\frac{2\pi}{6\sqrt{-\delta}\, m^3}\right) t^3 + O(t^{2e+1}),$$

with $e = 33/104$, as in the statement. □

Remark 5.1. In the interval $[0, t]$, with t a positive integer, for the function $f(x) := \big(x(t-x)\big)^e$ with $0 < e < 1$, applying the approximation method known as the 'trapezoidal rule', in the interval $[1, t-1]$ and for $t \geq 2$, we have that

$$\int_1^{t-1} f(x)dx - \sum_{n=1}^{t-1} f(n) = -\frac{t-2}{12} f''(\xi)$$

for some ξ in $[1, t-1]$; since for f'' the maximum value is $f''(t/2) = -c/t^{2-2e}$ where $c = (e/2)4^{2-e}$, and since

$$\int_0^t f(x)dx = H\, t^{2e+1}$$

where $H = \displaystyle\int_0^1 (y(1-y))^e dy$, it follows that

$$\sum_{n=0}^{t} f(n) \leq H\, t^{2e+1} - \frac{c}{12}\,\frac{t-2}{t^{2-2e}}\,.$$

For $e = 1/2$ the special value $H = \pi/8$ is used in the proof above.

6. Arbitrary polarized Abelian surfaces

6.1. Behavior under isogenies

Let A, B be polarized Abelian surfaces 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

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

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:

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

6.2. On the counting function

Let A be a polarized Abelian surface. Let r be the rank of the Néron Severi group $NS(A)$. We may assume that A is a non-simple Abelian surface, so it contains an elliptic curve E. It follows from the reducibility theorem (see §2.4) that A also contains a complementary elliptic curve E' and there is an isogeny $E \times E' \to A$, where the pullback polarization on $E \times E'$ is a split polarization. Let d be the minimum degree of such an isogeny. Choose an isogeny $E \times E' \to A$ as above of degree d.

The rank of the Néron Severi group $NS(E \times E')$ is also equal to r, and there is a bijective correspondence

$$\bigl\{\text{elliptic curves in } A\bigr\} \xrightarrow{\sim} \bigl\{\text{elliptic curves in } E \times E'\bigr\}$$

described in the previous subsection. Clearly, as A is non-simple, then $r \geq 2$ and if $r = 2$ then $N_A(t) = 2$. Note that: when $r \geq 3$ there are in A infinitely many elliptic curves, as is in $E \times E'$.

Proposition 6.1. *Assume that $r \geq 3$. The function $N_A(t)$ can be given an asymptotic estimate of the form*

$$N_A(t) = C\, t^{r-1} + O(t^e),$$

for some constant C and exponent $e < r - 2$.

Proof. If A is non-simple, and $E \times E' \to A$ is an isogeny of degree d, as in the description above, then

$$N_A(t) \leq N_{E \times E'}(d\, t)$$

(see §6.1); the estimate for the function $N_{E \times E'}(t)$ is given in Theorem 1.1, and so the statement follows. □

Remark 6.2. 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. [3], Theorem 4), which is of order $O(t^{2g^2-2})$, in particular for $g = 2$ of order $O(t^6)$. As the order found in the present paper is smaller, we are encouraged to believe that our approach may lead to some sharper asymptotic estimate for arbitrary g.

Acknowledgements

The author acknowledges his debt to the referee for several substantial contributions, especially for pointing out an error in the previous version of Lemma 3.1, and also for suggesting how to improve the setting and the presentation of the paper.

References

[1] Ch. Birkenhake and H. Lange, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften, no. 302, Springer-Verlag, Berlin, 2004.

[2] M. N. Huxley, *Exponential sums and lattice points. III*, Proc. London Math. Soc. (3) **87** (2003), 591–609.

[3] E. Kani, *Bounds on the number of nonrational subfields of a function field*, Invent. Math. **85** (1986), 185–198.

[4] E. Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), 199–223.

[5] E. Kani, *The moduli space of Jacobians isomorphic to a product of two elliptic curves*, Preprint (2013), `http://www.mast.queensu.ca/∼kani`.

[6] D. W. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves*, Invent. Math. **100** (1990), 1–24.

[7] 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.

[8] J. Rosen and A. Shnidman, *Néron-Severi groups of product abelian surfaces*, `arXiv:1402.2233 [math.AG]`.

[9] 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 April 27, 2015
Revised December 21, 2015
Accepted February 8, 2016