J. Austral. Math. Soc. (Series A) **64** (1998), 178–194

MULTIPLICATIVE ISOGENY ESTIMATES

DAVID MASSER

(Received 26 September 1996; revised 26 September 1997)

Communicated by W. W. L. Chen

Abstract

The theory of isogeny estimates for Abelian varieties provides 'additive bounds' of the form 'd is at most B' for the degrees d of certain isogenies. We investigate whether these can be improved to 'multiplicative bounds' of the form 'd divides B'. We find that in general the answer is no (Theorem 1), but that sometimes the answer is yes (Theorem 2). Further we apply the affirmative result to the study of exceptional primes ℓ in connexion with modular Galois representations coming from elliptic curves: we prove that the additive bounds for ℓ of Masser and Wüstholz (1993) can be improved to multiplicative bounds (Theorem 3).

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 11G10 (14K02), 11G05.

1. Introduction

Let k be a number field, and let A be an Abelian variety defined over k. Since the ground-breaking work [F] of Faltings, it is known that there exists a quantity $b(k, A)$ with the following property. Suppose A^* is another Abelian variety defined over k which is isogenous over k to A. Then there is an isogeny from A^* to A, defined over k, whose degree does not exceed $b(k, A)$. In particular there are only finitely many Abelian varieties, up to isomorphism over k, which are defined over k and isogenous over k to A.

In [MW3] (see Theorem II, p. 6 and the last paragraph of p. 23) we obtained an upper bound for $b(k, A)$ of the form

$$(1.1) \qquad c(\max\{[k : \mathbb{Q}], h(A)\})^{\kappa},$$

where $h(A)$ is the logarithmic absolute semistable Faltings height of A, and the constants c, κ depend only on the dimension of A.

In [MW2] we applied this bound to obtain similar results relating to Tate's Conjecture. For example, we proved (see Corollary 2, p. 213 and the last paragraph of p. 222) that for every Abelian variety A as above, there exists M, also bounded by something like (1.1), such that whenever ℓ is a prime number not dividing M, the kernel A_ℓ of multiplication by ℓ is a semisimple module over the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$.

So in this application the ordinary upper bound or 'additive upper bound' for degrees of isogenies leads to a similar 'multiplicative upper bound' for the exceptional primes ℓ; namely ℓ divides M. It is perhaps natural to ask whether one may obtain such multiplicative upper bounds for degrees of isogenies themselves; these bounds are referred to in our title as 'multiplicative isogeny estimates'.

In general, if we have a set of quantities, each with an additive upper bound B, then we may obtain in a trivial way a multiplicative upper bound B_0. For example, we can take the product, or, slightly better, the lowest common multiple of all positive integers up to B. But both of these grow at least exponentially in B. Therefore if B has the form (1.1), the new bound B_0 will not have this form.

In the present note we shall show indeed that there do not exist multiplicative isogeny estimates of the form (1.1) for arbitrary Abelian varieties A. But on the other hand we shall show that such estimates do exist in a number of significant special cases. These have applications to Galois groups for elliptic curves, in the style of [MW1]; we shall in fact improve all the results of [MW1].

Our negative result is as follows.

THEOREM 1. *Let n be a positive integer. Then there do not exist constants c, κ, depending only on n, with the following property. For an Abelian variety A of dimension n over a number field k, there is a positive integer*

$$b_0(k, A) \leq c(\max\{[k:\mathbb{Q}], h(A)\})^\kappa$$

such that if A^* is an Abelian variety over k which is isogenous over k to A, there is an isogeny over k from A^* to A whose degree divides $b_0(k, A)$.

In other words, multiplicative isogeny estimates do not always exist, at least with the 'polynomial' bounds (1.1).

Our positive result is as follows. Let us say that the Abelian variety A is a TM-product over k (standing for Trivial Multiplication) if it is isomorphic over k to a product $A_1^{e_1} \times \cdots \times A_t^{e_t}$, where $A_1, \ldots, A_t$ are simple over k, mutually non-isogenous over k, with trivial endomorphism rings over k. Apart from the field of definition, this is the condition that appears in [MW1, p. 248, Lemma 2.2].

THEOREM 2. *Let n be a positive integer. Then there exist constants c, κ, depending only on n, with the following property. Suppose A is a* TM-*product of dimension n*

over a number field k. Then there is a positive integer

$$b_0(k, A) \leq c(\max\{[k : \mathbb{Q}], h(A)\})^{\kappa}$$

such that if A^* is an Abelian variety over k that is isogenous over k to A, there is an isogeny over k from A^* to A whose degree divides $b_0(k, A)$.

In other words, multiplicative isogeny estimates exist for TM-products, with the polynomial bounds (1.1).

This fact enables all of the additive upper bounds of [MW1] for elliptic curves to be improved to multiplicative ones of the same order of magnitude. For example, let E be an elliptic curve defined over a number field k, and for a prime number ℓ let ρ_ℓ be the standard representation of $\Gamma = \mathrm{Gal}(\bar{k}/k)$ in the general linear group $\mathrm{GL}(E_\ell)$ as in [MW1]. A fundamental result of Serre in [Se2] (see also [Se1]) says that if E has no complex multiplication then ρ_ℓ is surjective for all ℓ sufficiently large; this is more or less equivalent to the assertion that $\rho_\ell(\Gamma)$ contains the special linear group $\mathrm{SL}(E_\ell)$ for all ℓ sufficiently large.

THEOREM 3. *There exist absolute constants c, κ with the following property. Suppose E is an elliptic curve defined over a number field k, with no complex multiplication over $\bar{k}$. Then there is a positive integer*

$$M \leq c(\max\{[k : \mathbb{Q}], h(E)\})^{\kappa}$$

such that $\rho_\ell(\Gamma)$ contains $\mathrm{SL}(E_\ell)$ whenever ℓ does not divide M.

The main result of [MW1] implies this for all 'large' $\ell > M$. As pointed out in [MW2, p. 213], the multiplicative version allows us to extend this both to certain 'very small' primes ℓ (of order $\log M$) and to 'almost all' primes $\ell \leq M$ (the number of exceptions is of order $(\log M)/(\log\log M)$). But we are still far from any uniform results: for example it is asked in [Se3, p. 199] if $\ell > 37$ suffices for $k = \mathbb{Q}$ independently of the elliptic curve.

Actually one can define the representation ρ_m of Γ in $\mathrm{GL}(E_m)$ for any positive integer m. Then Theorem 3 implies (see Section 9) that

$$[\mathrm{SL}(E_m) : \mathrm{SL}(E_m) \cap \rho_m(\Gamma)] \leq M^3 \tag{1.2}$$

for all square-free m. It would be interesting to have an estimate for arbitrary m not necessarily square-free; this would quantify the most general assertion (1) of [Se2, p. 259].

The arrangement of this paper is as follows: We start with the proof of Theorem 2. This requires some additional properties of the class index introduced in [MW3], which we record in Section 2. Next in Section 3 we eliminate the second Abelian variety A^* by considering instead Galois submodules of the first Abelian variety A. This enables us to decompose everything into primary factors. Then in Section 4 we prove Theorem 2 by re-introducing A^*.

The proof of Theorem 1 is given in Section 6, using counterexamples that are essentially elliptic curves. The necessary preparations are carried out in Section 5.

The proof of Theorem 3 requires an elementary number-theoretic lemma that we give in Section 7. This is used in Section 8 to establish Theorem D, which is a uniform generalization of Theorem 2 to field extensions of bounded degree. Finally in Section 9 we give the proof of Theorem 3. We also prove multiplicative versions of all the other results of [MW1].

2. Class index

Let $\mathscr{O}$ be an order as in [MW2]. Thus $\mathscr{O}$ is a ring, containing a multiplicative identity, which is torsion-free and finitely generated as an additive group. Tensoring over $\mathbb{Z}$, we obtain an algebra $E = \mathbb{Q} \otimes \mathscr{O}$ over $\mathbb{Q}$. When E is semisimple, we define the class index $i(\mathscr{O})$ as the smallest positive integer I with the following property. If $\mathscr{M}$ is any left $\mathscr{O}$-module contained in E, also finitely generated as an Abelian group with the same rank as $\mathscr{O}$, then there is μ in $\mathscr{M}$ such that the index $[\mathscr{M} : \mathscr{O}\mu]$ of $\mathscr{O}\mu$ in $\mathscr{M}$ is at most I.

In [MW2, p. 214, Lemma 2.1] we noted that the class index behaves nicely with respect to products. Namely

$$(2.1) \qquad i(\mathscr{O}_1 \times \mathscr{O}_2) \le i(\mathscr{O}_1)i(\mathscr{O}_2)$$

for orders $\mathscr{O}_1$, $\mathscr{O}_2$ in semisimple algebras. For the present note we need an analogous result for matrix rings. Let e be a positive integer. An order $\mathscr{O}$ in an algebra E then gives rise to an order $M_e(\mathscr{O})$ in the algebra $M_e(E)$ of matrices of order e with entries in E.

LEMMA 2.1. *Suppose $\mathscr{O}$ is an order in a division algebra. Then $i(M_e(\mathscr{O})) \le (i(\mathscr{O}))^{e^2}$.*

PROOF. Write $D = \mathbb{Q} \otimes \mathscr{O}$ for the division algebra. Let $\pi_1, \dots, \pi_e$ denote the additive group homomorphisms from $M_e(D)$ to D^e obtained by taking the 1st, ..., eth rows of a matrix respectively. Let $\mathscr{M}$ be an arbitrary left $M_e(\mathscr{O})$-module contained in $M_e(D)$, finitely generated as an additive group, with the same rank as $M_e(\mathscr{O})$. Then $\pi = (\pi_1, \dots, \pi_e)$ gives an additive group monomorphism from $\mathscr{M}$ to $\pi_1(\mathscr{M}) \times \dots \times \pi_e(\mathscr{M})$. But if $u_1, \dots, u_e$ are the diagonal matrices in $M_e(\mathscr{O})$ with zero entries except for the entry 1 in the 1st, ... , eth rows respectively, we have an identity

$$(\pi_1(x_1), \ldots, \pi_e(x_e)) = \pi(u_1x_1 + \cdots + u_ex_e)$$

for $x_1, \ldots, x_e$ in $M_e(D)$. This shows that π is actually surjective, and therefore an isomorphism.

Furthermore, since row interchanges can be effected by left multiplication by elements of $M_e(\mathcal{O})$, we see that $\pi_1(\mathcal{M}) = \cdots = \pi_e(\mathcal{M}) = \mathcal{N}$, say. This $\mathcal{N}$ is a finitely generated additive subgroup of D^e, with the same rank as $\mathcal{O}^e$.

But $\mathcal{N}$ is also a left $\mathcal{O}$-module, as we see by considering the action of diagonal elements of $M_e(\mathcal{O})$ on $\mathcal{M}$. So its rank over $\mathcal{O}$ must be e.

For this situation we defined in [MW3, p. 8] the generalized class index $i_e(\mathcal{O})$. It shows that $\mathcal{N}$ contains a free $\mathcal{O}$-submodule $\mathcal{N}_0$ of index $I \leq i_e(\mathcal{O})$, which we can write as a direct sum $\mathcal{O}\mu_1 \oplus \cdots \oplus \mathcal{O}\mu_e$ for $\mu_1, \ldots, \mu_e$ in D^e.

It follows that $\mathcal{M} = \pi^{-1}(\mathcal{N}^e)$ contains $\mathcal{M}_0 = \pi^{-1}(\mathcal{N}_0^e)$ of index I^e. Further $\mathcal{M}_0 = M_e(\mathcal{O})\mu$ for $\mu = \pi^{-1}(\mu_1, \ldots, \mu_e)$.

Since $\mathcal{M}$ was arbitrary, we conclude that

$$i(M_e(\mathcal{O})) \leq (i_e(\mathcal{O}))^e$$

However, [MW3, p. 10, Lemma 2.2] implies that $i_e(\mathcal{O}) \leq (i(\mathcal{O}))^e$, and the inequality of the present lemma follows at once. This completes the proof.

3. Galois modules

Let A be an Abelian variety defined over a field k. For each positive integer m the kernel A_m of multiplication by m is a Galois module over $\mathrm{Gal}(\bar{k}/k)$.

LEMMA 3.1. *Suppose r and s are coprime positive integers. Then for every Galois submodule G of A_{rs} there are Galois submodules H of A_r and J of A_s such that $G = H \oplus J$.*

PROOF. It is clear that $A_{rs} = A_r \oplus A_s$. Let H and J be the images of the projections from G in A_{rs} to the factors A_r and A_s respectively. These are Galois modules. We get in the usual way (Goursat's Lemma) a group isomorphism between $X = H/(G \cap A_r)$ and $Y = J/(G \cap A_s)$. But X is killed by r, and Y is killed by s. Since r and s are coprime it follows that $X = Y = 0$, which leads to $G = H \oplus J$ in the usual way. This completes the proof.

Let End A denote the ring of endomorphisms of A defined over k. For φ in End A and a positive integer m write $\ker_m \varphi$ for the intersection of A_m with the kernel $\ker \varphi$ of φ. For a Galois submodule G of A_m we define

$$f_m(G) = \min\,[\ker_m \varphi : G]$$

where the minimum is taken over all φ in End A with $G \subseteq \ker_m \varphi$. This is a better version of the definition in [MW2, p. 222].

LEMMA 3.2. *Suppose r and s are coprime positive integers, and H and J are Galois submodules of A_r, A_s respectively. Then*

$$f_{rs}(H \oplus J) = f_r(H) f_s(J).$$

PROOF. There are ψ, χ in End A with

$$H \subseteq \ker_r \psi, \qquad J \subseteq \ker_s \chi$$

and

$$f_r(H) = [\ker_r \psi : H], \qquad f_s(J) = [\ker_s \chi : J].$$

Using the Chinese Remainder Theorem we can easily find φ in End$A$ such that $\varphi - \psi$, $\varphi - \chi$ are in r. End A, s. End A respectively. It follows that

$$H \subseteq \ker_r \psi = \ker_r \varphi \subseteq \ker_{rs} \varphi,$$
$$J \subseteq \ker_s \chi = \ker_s \varphi \subseteq \ker_{rs} \varphi.$$

Therefore $G = H \oplus J \subseteq \ker_{rs} \varphi$, and

$$f_{rs}(G) \leq [\ker_{rs} \varphi : G] = [\ker_r \varphi \oplus \ker_s \varphi : G] = f_r(H) f_s(J).$$

To get the opposite inequality we note that there is φ' in End A with $G \subseteq \ker_{rs} \varphi'$ and $f_{rs}(G) = [\ker_{rs} \varphi' : G]$. So

$$H \subseteq \ker_r \varphi', \qquad J \subseteq \ker_s \varphi'$$

and

$$f_r(H) \leq [\ker_r \varphi' : H], \qquad f_s(J) \leq [\ker_s \varphi' : J].$$

Therefore

$$f_{rs}(G) = [\ker_r \varphi' \oplus \ker_s \varphi' : G] = [\ker_r \varphi' : H][\ker_s \varphi' : J]$$

which is at least $f_r(H) f_s(J)$. This completes the proof.

Now assume that k is a number field, so that the quantity $b(k, A)$ of Section 1 exists.

LEMMA 3.3. *For any positive integer m and any Galois submodule G of A_m we have $f_m(G) \leq b(k, A)$.*

PROOF. This is by now very standard. Since $A^* = A/G$ is defined over k, there is an isogeny β from A/G to A, also defined over k, of degree $b \leq b(k, A)$. Composing with the canonical map from A to A/G we obtain φ in End A with $G \subseteq \ker_m \varphi$. Also $\ker \beta = (\ker \varphi)/G$, so

$$f_m(G) \leq [\ker_m \varphi : G] \leq [\ker \varphi : G] = b \leq b(k, A).$$

This completes the proof.

We can now define

$$b_0(k, A) = \max f_m(G)$$

where the maximum is over all positive integers m and all Galois submodules G of A_m. Thanks to Lemma 3.3 we have

$$b_0(k, A) \leq b(k, A). \tag{3.1}$$

The following is the crucial step from 'additive upper bounds' to 'multiplicative upper bounds'.

LEMMA 3.4. *Suppose m is a positive integer and G is a Galois submodule of A_m. Then $f_m(G)$ divides $b_0(k, A)$.*

PROOF (compare [MW2, P. 222]). Fix a prime ℓ and consider the $f_q(G_\ell)$ as q runs over all powers of ℓ and G_ℓ runs over all Galois submodules of A_q. It is clear that these are all powers of ℓ. Hence each one divides their maximum; call this maximum b_ℓ.

We now show that the infinite product $\prod b_\ell$, taken over all primes ℓ, converges to $b_0 = b_0(k, A)$. It suffices to prove

(i) Every finite product $\prod b_\ell$ is at most b_0,

(ii) Some finite product $\prod b_\ell$ is divisible by b_0.

For (i) we note that every finite product has the form $\prod f_q(G_\ell)$. But by Lemma 3.2 this has the form $f_m(G) \leq b_0$.

For (ii) we note that b_0 is some $f_m(G)$. By Lemma 3.1 we can write G as a direct sum of G_ℓ, and then once again from Lemma 3.2 we see that $f_m(G) = \prod f_q(G_\ell)$. And this latter product divides the corresponding product $\prod b_\ell$.

Therefore (i) and (ii) are true, and the infinite product $\prod b_\ell$ does indeed converge to b_0.

Finally choose any $f_m(G)$. The argument used in (ii) shows that $f_m(G)$ divides some finite product $\prod b_\ell$. This in turn divides b_0, and the proof is complete.

4. Proof of Theorem 2

Let A be an Abelian variety defined over a number field k, and let $\mathscr{O} = \operatorname{End} A$ be the ring of endomorphisms defined over k. This is an order in a semisimple algebra, and therefore has a class index $i(\mathscr{O})$ in the sense of Section 2. Let $b_0(k, A)$ be as in the previous section.

LEMMA 4.1. *Suppose $i(\mathscr{O}) = 1$. Then if A^* is an Abelian variety defined over k, which is isogenous over k to A, there is an isogeny over k from A^* to A whose degree divides $b_0(k, A)$.*

PROOF. There is an isogeny α over k from A to A^*; let m be its degree. Then $G = \ker \alpha$ is a Galois submodule of A_m. So there is φ in $\mathscr{O}$ with $G \subseteq \ker_m \varphi$ and $f_m(G) = [\ker_m \varphi : G]$.

Consider the left $\mathscr{O}$-module $\mathscr{M} = \mathscr{O}m + \mathscr{O}\varphi$. Since $i(\mathscr{O}) = 1$, there is $\tilde{\varphi}$ in $\mathscr{O}$ with $\mathscr{M} = \mathscr{O}\tilde{\varphi}$. It follows immediately that $\ker_m \varphi = \ker \tilde{\varphi}$.

We can now reverse the arguments of the proof of Lemma 3.3. We have $G \subseteq \ker \tilde{\varphi}$, and so $\tilde{\varphi}$ factorizes through the canonical quotient map from A to A/G. We get an isogeny $\tilde{\beta}$ from A/G to A with $\ker \tilde{\beta} = (\ker \tilde{\varphi})/G$. Thus $\tilde{\beta}$ has degree $[\ker \tilde{\varphi} : G] = f_m(G)$. Finally $f_m(G)$ divides $b_0(k, A)$ by Lemma 3.4, so the isogeny $\tilde{\beta}$ does what is required, since A/G and A^* are isomorphic over k. This proves the present lemma.

It is now an easy matter to deduce Theorem 2. If A is a TM-product then $\mathscr{O} = \operatorname{End} A$ is a product of matrix rings $M_e(\mathbb{Z})$. By Lemma 2.1 each of these has class index 1, so $i(\mathscr{O}) = 1$ by (2.1). And by (3.1) $b_0(k, A)$ is bounded above by an expression of the form (1.1). This completes the proof of Theorem 2.

5. Elliptic curves

Let p be a prime congruent to 1 modulo 4, let $k_0 = \mathbb{Q}(\sqrt{-p})$, and let $\mathscr{O}$ be the ring of integers of k_0. There is a complex number $\omega \neq 0$ such that the elliptic curve $E = E(p) = \mathbb{C}/\omega\mathscr{O}$ is defined over the field $\mathbb{Q}(j)$ for the value $j = j(\sqrt{-p})$ of the modular function. Then $\mathscr{O}$ is the ring of all endomorphisms $\operatorname{End}_{\mathbb{C}} E$ of E.

Let $\mathscr{M}$ be any non-zero ideal in $\mathscr{O}$, and write $E_{\mathscr{M}}$ for the finite subgroup of x in E such that $\mu x = 0$ for all μ in $\mathscr{M}$. Define the elliptic curve $E^{\mathscr{M}} = E/E_{\mathscr{M}}$; it is clearly isogenous to E.

LEMMA 5.1. *Let β be any isogeny from $E^{\mathscr{M}}$ to E. Then there is an ideal $\mathscr{M}'$ in $\mathscr{O}$, belonging to the ideal class inverse to that of $\mathscr{M}$, such that the degree of β is the norm $N(\mathscr{M}')$ of $\mathscr{M}'$.*

PROOF. The map β composes with the canonical map from E to $E^{\mathscr{M}}$ to give φ in $\mathscr{O}$. So as usual $E_{\mathscr{M}} \subseteq \ker\varphi$ and $\ker\beta = (\ker\varphi)/E_{\mathscr{M}}$. The first inclusion leads easily to $(\varphi)\mathscr{M}^{-1} \subseteq \mathscr{O}$ for the principal ideal (φ). It follows that $(\varphi) = \mathscr{M}\mathscr{M}'$ for some ideal $\mathscr{M}'$. Now the degree of β is the cardinality of $(\varphi)^{-1}/\mathscr{M}^{-1}$, or just $N(\mathscr{M}')$. This completes the proof.

For a positive integer n let $\tau(n)$ be the number of positive integer divisors of n. For any $\epsilon > 0$ it is well known (see for example [HW, p. 260, Theorem 315]) that there exists c, depending only on ϵ, such that

$$\tau(n) \leq cn^{\epsilon} \tag{5.1}$$

for all n. Henceforth we use $c_1, c_2, \ldots$ also for positive constants depending only on ϵ.

LEMMA 5.2. *For any $\epsilon > 0$ and any positive integer N there are at most $c_1 N^{\epsilon}$ ideals $\mathscr{M}$ in $\mathscr{O}$ with $N(\mathscr{M}) = N$.*

PROOF. This is also well known, but we give a short proof in order to clinch the uniformity in the quadratic field k_0. Let $N = p_1^{e_1} \cdots p_t^{e_t}$ be the prime factorization. Since every prime in $\mathbb{Z}$ has at most two prime ideal divisors in $\mathscr{O}$, it follows easily that the principal ideal (N) has at most $(e_1+1)^2 \cdots (e_t+1)^2 = (\tau(N))^2$ ideal divisors. Since $N(\mathscr{M}) = N$, the ideal $\mathscr{M}$ must be one of these, and the lemma now follows from (5.1). This completes the proof.

We now regard the elliptic curve E above as defined over the field $k = k_0(j)$.

LEMMA 5.3. *For any $\epsilon > 0$ we have $[k : \mathbb{Q}] \leq c_2 p^{1/2+\epsilon}$ and $h(E) \leq c_3 p^{1+\epsilon}$. Further the class number of $\mathscr{O}$ is at least $c_4^{-1} p^{1/2-\epsilon}$.*

PROOF. It is well known (see for example [Si2, p. 122, Theorem 4.3(b)]) that the class number is $[k : k_0]$. Siegel's Theorem (see for example [L, p. 328, Corollary]) now gives the required field estimates (with ineffective c_4).

Next j satisfies the non-trivial equation $F_p(j, j) = 0$ for the modular polynomial $F_p(X, Y)$ of degree $p + 1$. According to [C, p. 390, Corollary] this polynomial has rational integer coefficients of absolute values at most $p^{c_5 p}$. Therefore so has $F_p(X, X)$, and by standard estimates (see for example [W, p. 21, Lemme 1.1.12]) so has any irreducible factor. It follows from equally standard estimates ([W, p. 20]) that the logarithmic absolute Weil height $h(j)$ is at most $c_6 p \log p$. Finally from [Si1, p. 258, Proposition 2.1] we see that $h(E) \leq c_3 p \log p$ as well (recall that $h(E)$ is defined with reference to a field with respect to which E is semistable). This completes the proof.

Presumably we even have $h(E) \leq c_3 p^{1/2+\epsilon}$, but we do not need this.

6. Proof of Theorem 1

We start with the case $n = 1$. We shall assume Theorem 1 false and obtain a contradiction. Thus there are absolute constants c, κ with the following property. For an elliptic curve E defined over a number field k, there is a positive integer

$$b_0(k, E) \leq c(\max\{[k : \mathbb{Q}], h(E)\})^{\kappa}$$

such that if E^* is an elliptic curve over k which is isogenous over k to E, there is an isogeny over k from E^* to E whose degree divides $b_0(k, E)$.

We choose $\epsilon > 0$ sufficiently small, and again we use $c_1, c_2, \ldots$ for positive constants depending only on ϵ. To get our contradiction we take $E = E(p)$ for a large prime p as in Section 5, with field of definition $k = \mathbb{Q}(\sqrt{-p}, j(\sqrt{-p}))$. It then follows from Lemma 5.3 that

$$B = b_0(k, E) \leq c_1 p^{2\kappa}. \tag{6.1}$$

We consider $E^* = E^{\mathscr{M}}$ as $\mathscr{M}$ runs over a complete set of ideal class representatives of $\mathscr{O}$. Clearly each such $E^{\mathscr{M}}$ is isogenous to E over k, so we obtain for each such $\mathscr{M}$ an isogeny β from $E^{\mathscr{M}}$ to E whose degree divides B. By Lemma 5.1 we know that this degree has the form $N(\mathscr{M}')$ for some ideal $\mathscr{M}'$ in the inverse class. So we end up with different ideals $\mathscr{M}'_1, \ldots, \mathscr{M}'_h$, where h is the class number of $\mathscr{O}$, such that the norms

$$N(\mathscr{M}'_1), \ldots, N(\mathscr{M}'_h) \tag{6.2}$$

all divide B.

Now these norms might not be all different. But from Lemma 5.2 there are at least $h/(c_2 B^{\epsilon})$ different numbers among them. We therefore have $\tau(B) \geq h/(c_2 B^{\epsilon})$. On the other hand (5.1) gives $\tau(B) \leq c_3 B^\epsilon$, and therefore (6.1) and Lemma 5.3 lead to $p^{1/2-\epsilon} \leq c_4 p^{4\kappa\epsilon}$. For ϵ small enough and then p large enough this is impossible. Such a contradiction establishes Theorem 1, at least for $n = 1$.

These arguments may easily be extended to arbitrary $n > 1$. For example, we can find $n-1$ elliptic curves $E^{(2)}, \ldots, E^{(n)}$, defined over $\mathbb{Q}$, mutually non-isogenous over $\overline{\mathbb{Q}}$, and with trivial endomorphism rings over $\overline{\mathbb{Q}}$. We then consider the Abelian varieties $A = E \times A'$ and $A^* = E^{\mathscr{M}} \times A'$ for $A' = E^{(2)} \times \cdots \times E^{(n)}$, noting that $h(A) = h(E) + h(A')$ and that every isogeny α from A^* to A comes from an isogeny from $E^{\mathscr{M}}$ to E whose degree divides the degree of α. This completes the proof of Theorem 1.

Underlying these arguments is the following algebraic fact. Since the group-theoretic index is multiplicative, it might have seemed slightly more natural in Section 2 to define the class index as the smallest positive integer I for which all the indices $[\mathscr{M} : \mathscr{O}\mu]$ divide I. However, this 'multiplicative class index', in contrast to $i(\mathscr{O})$ itself, cannot be estimated polynomially in the discriminant of $\mathscr{O}$, as in the Class Index Lemma of [MW3, p. 8]. Indeed the orders $\mathscr{O}$ above provide counterexamples, as the argument following (6.2) easily shows.

7. Lowest common multiples

Suppose we have a set of quantities together with additive upper bounds for each member, of similar orders of magnitude. Then we may obtain a comparable 'simultaneous' bound simply by taking the maximum.

Of course this procedure fails for multiplicative upper bounds. We can rescue it in our particular circumstances by using the following elementary result.

LEMMA 7.1. *Let $B \geq 1$, $C \geq 1$ be real numbers, and let $\mathscr{B}$ be a set of positive integers. Suppose that for each integer $t \geq 1$, any t elements of $\mathscr{B}$ have lowest common multiple at most $C^t B$. Then the lowest common multiple of all elements of $\mathscr{B}$ is finite, and does not exceed $4^{eC} B^{1+\log C}$.*

PROOF. For each prime number ℓ let $B(\ell)$ be the largest power of ℓ dividing any element of $\mathscr{B}$. Taking $t = 1$ in our hypothesis, we see that $\mathscr{B}$ is a finite set and therefore $B(\ell)$ is finite. Now let $t \geq 1$ be arbitrary, and let $\ell_1, \ldots, \ell_t$ be different primes. Then $B(\ell_1), \ldots, B(\ell_t)$ all divide elements of $\mathscr{B}$, and so the lowest common multiple of these elements is at least $B(\ell_1) \cdots B(\ell_t)$. So our hypothesis implies

$$B(\ell_1) \cdots B(\ell_t) \leq C^t B. \tag{7.1}$$

Since $B(\ell) = 1$ or $B(\ell) \geq \ell$, there are only finitely many $B(\ell) > 1$; suppose there are exactly s of these, and list them in order of size as

$$1 < B_1 < B_2 < \cdots < B_s.$$

Write b for the integer part $[\log B]$. Suppose first that $s \leq b$. Then by (7.1) the lowest common multiple of all elements of $\mathscr{B}$ is

$$B_1 \cdots B_s \leq C^s B \leq B^{1+\log C}$$

and our lemma is proved.

Otherwise, suppose $s > b$. Then (7.1) gives not only

$$B_{s-b+1} \cdots B_s \leq C^b B \leq B^{1+\log C} \tag{7.2}$$

but also

$$(B_{s-b})^{b+1} \leq B_{s-b} \cdots B_s \leq C^{b+1} B.$$

Therefore

$$B_{s-b} \leq \left[C B^{1/(b+1)}\right] \leq N$$

for $N = [eC]$. Thus $B_1 \cdots B_{s-b}$ is at most the lowest common multiple of $1, \ldots, N$. This latter is well known not to exceed 4^N (see for example [RS, p. 71, Theorem 12], or the less computational [N, p. 128, Corollary]) and so from (7.2) the lowest common multiple of all elements of $\mathscr{B}$ is at most $4^N B^{1+\log C}$ as claimed. This completes the proof.

For applications it is important that the dependence on the parameter B in the conclusion of the above result should be polynomial. This does not hold under slightly weaker hypotheses. For example, if $\mathscr{B}$ is the set of positive integers up to $N = \exp(2\sqrt{\log B})$, the lowest common multiple of any t elements is at most N^t, which is itself at most $e^{t^2} B$. But the lowest common multiple of all elements grows exponentially in N, and so cannot be polynomial in B.

8. Extensions of bounded degree

Let A be an Abelian variety defined over a number field k. We define as in Section 3

$$b_0(k, A) = \max f_m(G)$$

where the maximum is over all positive integers m and all Galois submodules G of A_m. By Lemma 3.4 we know that every $f_m(G)$ actually divides $b_0(k, A)$.

Now let K be a finite extension of k. Since every $\mathrm{Gal}(\bar{k}/k)$-module is also a $\mathrm{Gal}(\bar{K}/K)$-module, it follows that

$$(8.1) \qquad b_0(k, A) \quad \text{divides} \quad b_0(K, A).$$

The following result provides a simultaneous multiplicative upper bound for the $b_0(K, A)$ as K runs over all extensions of k of bounded degree, at least if A is a TM-product in the sense of Section 1. For better comparison with Theorem 2 we state it in terms of isogenies.

THEOREM D. *Let n and D be positive integers. Then there exist constants $c(D)$, $\kappa(D)$, depending only on n and D, with the following property. Suppose A is an Abelian variety of dimension n over a number field k, and suppose also that A is a* TM-*product over every finite extension of k. Then there is a positive integer*

$$b_0(k, A; D) \leq c(D)(\max\{[k : \mathbb{Q}], h(A)\})^{\kappa(D)}$$

such that if A^* is an Abelian variety, defined over an extension K of k of relative degree at most D, that is isogenous over K to A, there is an isogeny over K from A^* to A whose degree divides $b_0(k, A; D)$.

PROOF. Let $\mathscr{B}$ be the set of $b_0(K, A)$ as K runs over all extensions of k of relative degree at most D. We are going to apply Lemma 7.1. Consider therefore any t elements $b_0(K_1, A), \dots, b_0(K_t, A)$ of $\mathscr{B}$. Then by (8.1) they all divide $b_0(L, A)$ for the compositum L of $K_1, \dots, K_t$. This latter field has degree at most $D^t d$ for $d = [k : \mathbb{Q}]$, and so Theorem 2 provides the estimate

$$b_0(L, A) \leq c(\max\{D^t d, h\})^{\kappa} \leq C^t B$$

for

$$(8.2) \qquad h = h(A), \qquad C = D^{\kappa}, \qquad B = c(\max\{d, h\})^{\kappa}$$

and constants c, κ depending only on n. Thus we can indeed apply Lemma 7.1, and we find that every element $b_0(K, A)$ of $\mathscr{B}$ divides some

$$b_0(k, A; D) \leq 4^{eC} B^{1+\log C}.$$

In view of (8.2) this completes the proof of Theorem D. Note that the dependence on the parameter D is not polynomial, although this will not matter for our applications, because D will be absolutely bounded (by 60).

9. Proof of Theorem 3

We will follow the proof in [MW1], and we will end up with the number $M = 2M_1M_2$, where

$$M_1 = b_0(k, E)b_0(k, E; 2)b_0(k, E; 60)$$

and

$$M_2 = b_0(k, E \times E)b_0(k, E \times E; 2)b_0(k, E \times E; 60).$$

More careful arguments would probably give $M = 2b_0(k, E \times E; 60)$ by itself.

To begin with, since E is a TM-product, our Theorem 2 shows that the integer b in the proof of [MW1, p. 249, Lemma 3.1] must divide $b_0(k, E)$. It follows that if the prime ℓ does not divide $b_0(k, E)$, then the group $\rho_\ell(\Gamma)$ (which in [MW1] we called $\phi_\ell(G)$) does not fix any one-dimensional subspace of E_ℓ.

Similarly since $E \times E$ is a TM-product, the integer b divides $b_0(k, E \times E)$ in the proof of [MW1, p. 249, Lemma 3.2]. It follows that if ℓ does not divide $b_0(k, E \times E)$ and $\rho_\ell(\Gamma)$ is commutative then it is contained in the multiplicative group $\mathbb{F}_\ell^*$.

As in the first paragraph of Section 4 of [MW1] we may assume that if ℓ does not divide $b_0(k, E)$ then ℓ does not divide the order of $\rho_\ell(\Gamma)$. This yields the three possibilities (i), (ii), (iii).

Case (i) is eliminated again if ℓ does not divide $b_0(k, E)$ or $b_0(k, E \times E)$. If ℓ does not divide 2 then we reduce case (ii) to case (i) over an extension K (which in [MW1] we called k_0) of k of relative degree at most 2. So this is eliminated if ℓ does not divide $b_0(k, E; 2)$ or $b_0(k, E \times E; 2)$. Finally we reduce case (iii) to case (i) over an extension field K of k of relative degree at most 60, which is eliminated if ℓ does not divide $b_0(k, E; 60)$ or $b_0(k, E \times E; 60)$.

So we see precisely the above factors of M turning up, and now Theorem 3 follows from the estimates in Theorem D. This completes the proof.

Actually, if k and E are given, there are only finitely many possibilities for the quadratic extension K of k occurring above. For by [Se2, p. 295, Lemme 2], the extension is unramified. However, this observation does not seem to be very helpful in our context; the number of possible such extensions would seem to depend on the discriminant of k and not just on its degree.

The upper bound (1.2) of Section 1 follows easily by breaking the left-hand side into factors

$$f_\ell = [\mathrm{SL}(E_\ell) : \mathrm{SL}(E_\ell) \cap \rho_\ell(\Gamma)]$$

for each prime divisor ℓ of the square-free integer m. Clearly f_ℓ is at most the cardinality $\ell(\ell^2 - 1) < \ell^3$ of $\mathrm{SL}(E_\ell)$, and by Theorem 3 we have $f_\ell = 1$ if ℓ does not divide M. So $\prod f_\ell$ is at most the product $\prod \ell^3$ over all ℓ dividing M, which is at most M^3.

In a similar way we can establish a multiplicative version of [MW1, p. 251, Proposition 1(a)]. We omit the details of the proofs, and give only the results. Denoting the number M above by $b_1(k, E)$, we find for two elliptic curves E and E' the multiplicative upper bound

$$b_2(k, E, E') = 6b_1(k, E)b_1(k, E')b_0(k, E \times E')b_0(k, E \times E'; 2)$$

(note that $E \times E'$ is a TM-product, and that the arguments of Section 5 of [MW1] require ℓ not to divide 6). Then for n elliptic curves $E^{(1)}, \dots, E^{(n)}$ we find the multiplicative bound

$$M(n) = \prod b_2\left(k, E^{(i)}, E^{(j)}\right) \tag{9.1}$$

where the product is taken over all i, j with $1 \leq i < j \leq n$. Thus the conclusion in Proposition 1(a) is valid whenever ℓ does not divide $M(n)$, and this $M(n)$ is bounded above by an expression of the form (1.1), with for example $A = E^{(1)} \times \cdots \times E^{(n)}$. Thus the new constants c, κ may depend on n, thanks to (9.1); whereas in Proposition 1(a) the analogous constants c, γ were absolute.

Finally we can establish a multiplicative version of [MW1, p. 253, Proposition 2]. If $P_1, \dots, P_s$ are linearly independent points of the group $E(k)$ of points of E defined over k, we find the bound

$$M_P = 6bb_1(k, E) \tag{9.2}$$

where $b = b(k, E; P_1, \dots, P_s)$ is the product of all primes ℓ for which $P_1, \dots, P_s$ become linearly dependent modulo $\ell.E(k)$. Thus the conclusion in Proposition 2 holds for all ℓ not dividing M_P. Of course M_P now depends also on the Néron-Tate heights $q(P_1), \dots, q(P_s)$. To estimate it efficiently we use the following result.

LEMMA 9.1. *We have* $b(k, E; P_1, \dots, P_s) \leq (s^2 Q/q_0)^{s/2}$, *where* $Q = \max\{q(P_1), \dots, q(P_s)\}$ *and* q_0 *is the smallest non-zero value of* q *on* $E(k)$.

PROOF. The same bound for the individual primes ℓ is well known (see for example the reference on [MW1, p. 254]), and a simple modification of the standard argument extends this to their product. For we can use the Chinese Remainder Theorem to combine the linear relations modulo ℓ into a single linear relation $a_1 P_1 + \cdots + a_s P_s = bP$, for integers $a_1, \dots, a_s$ and $b = b(k, E; P_1, \dots, P_s)$ with highest common factor

$$(a_1, \dots, a_s, b) = 1, \tag{9.3}$$

and some P in $E(k)$. Then the Box Principle provides in the usual way an integer t with

$$0 < t < b \tag{9.4}$$

together with integers $t_1, \ldots, t_s$ such that the

$$a'_i = ta_i - bt_i \qquad (1 \le i \le s)$$

satisfy $|a'_i| \le b^{(s-1)/s}$. Thus

$$a'_1 P_1 + \cdots + a'_s P_s = bP'$$

again for some P' in $E(k)$. Now if $b > (s^2 Q/q_0)^{s/2}$ comparison of heights forces P' to be torsion and therefore $a'_1 = \cdots = a'_s = 0$. But this latter is ruled out by (9.3) and (9.4); and so the proof is complete.

It follows easily from the discussion in [MW1, p. 254] that the quantity M_P in (9.2) satisfies $M_P \le (s^2 \tilde{M} Q)^{s/2}$, where $\tilde{M}$ is bounded above by an expression of the form (1.1) with $A = E$. Notice the extra factor s^2, which we mistakenly omitted from [MW1, Proposition 2].

References

[C] P. Cohen, 'On the coefficients of the transformation polynomials for the elliptic modular function', *Math. Proc. Cambridge Philos. Soc.* **95** (1984), 389–402.

[F] G. Faltings, 'Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern', *Invent. Math.* **73** (1983), 349–366, and *ibid.* **75** (1984), 381.

[HW] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford Univ. Press, Oxford, 1960).

[L] S. Lang, *Algebraic number theory* (Addison-Wesley, Reading, 1970).

[MW1] D. W. Masser and G. Wüstholz, 'Galois properties of division fields of elliptic curves', *Bull. London Math. Soc.* **25** (1993), 247–254.

[MW2] ———, 'Refinements of the Tate conjecture for Abelian varieties', in: *Abelian varieties* (eds. W. Barth, K. Hulek and H. Lange) (de Gruyter, Berlin, 1995) pp. 211–223.

[MW3] ———, 'Factorization estimates for Abelian varieties', *Inst. Hautes Études Sci. Publ. Math.* **81** (1995), 5–24.

[N] M. Nair, 'On Chebyshev-type inequalities for primes', *Amer. Math. Monthly* **89** (1982), 126–129.

[RS] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[Se1] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves* (Benjamin, New York, 1968).

[Se2] ———, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15** (1972), 259–331.

[Se3] ———, 'Quelques applications du théorème de densité de Chebotarev', *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201.

[Si1] J. H. Silverman, 'Heights and elliptic curves', in: *Arithmetic geometry* (eds. G. Cornell and J. H. Silverman) (Springer, Berlin, 1986) pp. 253–265.

[Si2] ———, *Advanced topics in the arithmetic of elliptic curves* (Springer, Berlin, 1994).

[W] M. Waldschmidt, 'Nombres transcendants et groupes algébriques', in: *Astérisque* 69–70 (Soc. Math. France, Paris, 1987).

Mathematisches Institut
Universität Basel
Rheinsprung 21
4051 Basel
Switzerland