Invent. math. 100, 1–24 (1990)

Inventiones mathematicae

Estimating isogenies on elliptic curves

D.W. Masser[1] and G. Wüstholz[2]

[1] Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109-1003, USA
[2] Departement für Mathematik, ETH-Zentrum, CH-8092 Zürich, Switzerland

1. Introduction

The object of this paper is to prove a new type of estimate for isogenies between elliptic curves. This has several diophantine applications (effective versions of Serre's Galois irreducibility theorem and Shafarevich's theorem, for example) which are presented in another paper [MW3]. Later articles will deal with the corresponding problems for abelian varieties of arbitrary dimension.

Right at the beginning we emphasize that we are identifying elliptic curves E with Weierstrass equations

$$y^2 = 4x^3 - g_2 x - g_3 .$$

Thus, for example, to say that E is defined over a field k means that its invariants g_2 and g_3 lie in k.

We will be dealing with isogenies φ between E and a second elliptic curve also defined over k. For the purpose of this paper it is not usually convenient to specify the field of definition of φ. However, we may note that φ is necessarily defined over a finite extension of k (see Lemma 6.1 below).

Suppose E is defined over a number field k. We shall measure E somewhat crudely by the quantity

$$w(E) = \max\{1, h(g_2), h(g_3)\},$$

where h denotes the absolute logarithmic Weil height (see for example [Wa] p. 19). We can now state our main result.

Theorem. *Given a positive integer d, there exists a constant c, depending effectively on d, with the following property. Let k be a number field of degree at most d, and let E be an elliptic curve defined over k. Suppose E is isogenous to a second elliptic curve that is also defined over k. Then there is an isogeny between the two elliptic curves whose degree is at most $c(w(E))^4$.*

The proof will be by transcendence techniques. These were already used by D. and G. Chudnovsky [CC] (see also [La]) to obtain some results of the

above type. Their Corollary 2.2 (p. 2214) implies that when k is the rational field $\mathbb{Q}$ there is an effective bound for the degree of the isogeny. In Proposition 2.3 (p. 2214), stated without proof, they announce an explicit bound, still for $k=\mathbb{Q}$. However, it is exponential in $w(E)$ and it depends also on the second elliptic curve.

More significantly, their Theorem 4 (p. 2215) implies that when k is real there is an effective bound for the degree of the isogeny depending only on k and E. The idea of the proof can be sketched as follows. Suppose φ is an isogeny from the second elliptic curve E^* to E. Then φ corresponds to multiplication on the tangent spaces by some algebraic number α satisfying

$$\alpha \Omega^* \subseteq \Omega \tag{1.1}$$

for the associated period lattices Ω^*, Ω. Thus for any ω^* in Ω^* there is ω in Ω such that

$$\alpha \omega^* = \omega. \tag{1.2}$$

Now the assumption that k is real enables us to choose ω and ω^* in (1.2) independently of the isogeny φ. Then transcendence techniques can be advantageously applied to the vanishing linear form $\alpha\omega^* - \omega$. More specifically we can use Gelfond's method with two elliptic functions to obtain a new isogeny, generally of much smaller degree, between E and E^*.

If k is not real, the inclusion (1.1) has to be expressed in the form

$$\alpha \omega_1^* = m_{11}\omega_1 + m_{12}\omega_2, \quad \alpha \omega_2^* = m_{21}\omega_1 + m_{22}\omega_2 \tag{1.3}$$

for fixed basis elements ω_1, ω_2 of Ω and ω_1^*, ω_2^* of Ω^*. Thus it is now Baker's method that we should use, as in Baker's own paper [Ba] or Wüstholz's generalization [Wü2]; and moreover the version for simultaneous linear forms (see for example [Lo]). In particular we need multiplicity estimates in the style of [Wü1] or [P].

The plan of this paper is as follows. In Sect. 2 we prove an effective version of a theorem of Kolchin for products of elliptic curves. This will be required to supplement the information provided by multiplicity estimates.

Then in Sect. 3 we prepare for the transcendence argument by recording a number of analytic and algebraic estimates, mostly of a familiar kind, for a single elliptic curve.

Next, in Sects. 4 and 5 we state and prove a Proposition essentially of the same depth as the Theorem. The proof, by transcendence techniques, is divided as usual into two parts: in Sect. 4 we do the "construction", and in Sect. 5 we do the "deconstruction". The Proposition actually applies only to isogenies that are normalized in the sense that $\alpha = 1$ in (1.1), and in Sect. 6 we show how this restriction can be eliminated.

Finally in Sect. 7 we complete the proof of the Theorem. We also make some additional remarks about the proof of the Proposition in the case of complex multiplication. This is not quite covered by the arguments of the earlier

sections. We end the paper by showing that our estimates of Sect. 2 are essentially best possible.

Acknowledgements. This research was begun at the 1986 Durham Conference on Transcendence, and we would like to thank the organizers, Professor A. Baker and Dr. R.C. Mason, for providing such a stimulating yet relaxed environment. The first author was supported in part by the National Science Foundation.

2. Isogenies and subgroups

Throughout this section, all varieties will be assumed without further reference to be defined over the field $\mathbb{C}$ of complex numbers.

Let E_1 and E_2 be elliptic curves, and for positive integers n_1 and n_2 write G for the algebraic group $E_1^{n_1} \times E_2^{n_2}$. We say that a connected algebraic subgroup H of G is split if it has the form $H = H_1 \times H_2$ for algebraic subgroups H_1 of $E_1^{n_1}$ and H_2 of $E_2^{n_2}$; and otherwise we say that H is non-split.

Suppose G has a non-split connected algebraic subgroup. Then it follows easily from a result of Kolchin [K] (see also Lemma 7 (p. 262) of [MW2]) that E_1 and E_2 must be isogenous. In this section we will prove a quantitative version of this observation (the Isogeny Lemma below).

We start with two lemmas on degrees in projective space. For a closed irreducible projective variety X and a non-negative integer t let $\mathscr{H}(X; t)$ denote the usual Hilbert counting function. Recall that as $t \to \infty$ we have

$$\mathscr{H}(X; t)/t^d \to (\deg X)/d!,$$

where d is the dimension of X and $\deg X$ denotes its degree.

For positive integers n and m let $k+1 = (n+1)(m+1)$, and identify the product $\mathbb{P}_n \times \mathbb{P}_m$ of projective spaces as a subset of $\mathbb{P}_k$ by means of the Segre embedding. Let π be the projection from $\mathbb{P}_n \times \mathbb{P}_m$ to $\mathbb{P}_n$. By the fundamental theorem of elimination theory, this is a closed map.

Lemma 2.1. *Suppose X in $\mathbb{P}_n \times \mathbb{P}_m$ is irreducible, and that X and $\pi(X)$ have the same dimension. Then* $\deg \pi(X) \leqq \deg X$.

Proof. Fix a large positive integer t, let

$$h = \mathscr{H}(\pi(X); t), \tag{2.1}$$

and denote by $M_1(x), \ldots, M_h(x)$ the corresponding monomials in $x = (x_0, \ldots, x_n)$ that are linearly independent modulo the prime ideal $I(\pi(X))$ of $\pi(X)$. Let $y = (y_0, \ldots, y_m)$ be variables on $\mathbb{P}_m$, so that each $M_i(x)\, y_j^t (1 \leqq i \leqq h,\ 0 \leqq j \leqq m)$ can be written as a monomial of degree t in the variables of $\mathbb{P}_k$. Call these monomials $M_{ij} (1 \leqq i \leqq h,\ 0 \leqq j \leqq m)$. We claim that there exists j with $0 \leqq j \leqq m$ such that $M_{1j}, \ldots, M_{hj}$ are linearly independent modulo the prime ideal $I(X)$ of X.

If not, then we have a collection of relations

$$\sum_{i=1}^{h} \mu_{ij} M_{ij} \equiv 0 \,(\mathrm{mod}\, I(X)) \qquad (0 \leqq j \leqq m) \tag{2.2}$$

with $\mu_{1j}, \ldots, \mu_{hj}$ not all zero $(0 \leqq j \leqq m)$. Let H_j be the hypersurface of $\mathbb{P}_n$ defined by the vanishing of $\sum_{i=1}^{h} \mu_{ij} M_i(x) (0 \leqq j \leqq m)$. Pick any ξ in $\pi(X)$. Then (ξ, η) is in X for some η in $\mathbb{P}_m$, and there exists j with $0 \leqq j \leqq m$ such that the jth projective coordinate η_j of η is non-zero. Since $M_{ij}(\xi, \eta) = M_i(\xi) \eta_j^t$ we deduce from (2.2) that ξ lies in H_j. Since ξ was arbitrary, this shows that $\pi(X)$ is contained in the union of $H_0, \ldots, H_m$. But because $\pi(X)$ is irreducible, we conclude that $\pi(X)$ must be contained in H_j for some j with $0 \leqq j \leqq m$. However, this contradicts the linear independence of $M_1, \ldots, M_h$ modulo $I(\pi(X))$.

Thus the above claim is established, and we deduce that

$$\mathscr{H}(X; t) \geqq h = \mathscr{H}(\pi(X); t).$$

Since X and $\pi(X)$ have the same dimension, the present lemma follows on making $t \to \infty$.

Lemma 2.2. *Suppose X is an irreducible variety, and $H_1, \ldots, H_m$ are hypersurfaces in projective space of degrees at most $D \geqq 1$. Then $Y = X \cap H_1 \cap \ldots \cap H_m$ satisfies*

$$D^e \deg Y \leqq D^d \deg X,$$

where d and e are the dimensions of X and Y respectively.

Proof. This kind of estimate is implicit in [MW2] (pp. 249, 250), but we will deduce it from Proposition 3.3 (p. 365) of Philippon's paper [P]. In the notation there, take $p = 1$ and $P_1, \ldots, P_m$ as the defining polynomials of $H_1, \ldots, H_m$, with $I_0 = I(X)$ the prime ideal of X. Then $SH(\sqrt{I}; D) \geqq D^e \deg Y$ while $SH(\sqrt{I_0}; D) = D^d \deg X$; so the present lemma is immediate.

From now on, we shall assume that E_1 and E_2 are elliptic curves embedded in $\mathbb{P}_2$ by means of Weierstrass equations, and that any product $G = E_1^{n_1} \times E_2^{n_2}$ is embedded in $\mathbb{P}_k$ using the Segre map. Here $k + 1 = 3^{n_1 + n_2}$. Thus any subvariety H of G has a well-defined degree.

Lemma 2.3. *Suppose n_1 and n_2 are positive integers with $n_1 + n_2 > 2$, and let H be a non-split connected algebraic subgroup of $E_1^{n_1} \times E_2^{n_2}$ of dimension d. Then there exist positive integers n_1' and n_2' with $n_1' + n_2' < n_1 + n_2$, and a non-split connected algebraic subgroup H' of $E_1^{n_1'} \times E_2^{n_2'}$ of dimension d', such that*

$$3^{d'} \deg H' \leqq 3^d \deg H.$$

Proof. Let E be any of the simple factors of $G = E_1^{n_1} \times E_2^{n_2}$, let G' be the natural complementary factor, so that $G = E \times G'$, and let π be the projection from G to G'. Suppose the dimension of $\pi(H)$ is strictly less than the dimension of H. Then the kernel of π restricted to H has positive dimension, and it follows

that $H = E \times \pi(H)$. From this we can deduce two things. Firstly, since $H \neq G$ there must exist E such that H and $\pi(H)$ have the same dimension, and without loss of generality we can suppose $E = E_1$. Second, since H is non-split we must have $n_1 \geqq 2$.

Thus π is the projection from $G = E_1^{n_1} \times E_1 \times E_2^{n_2}$ to $E_1^{n_1-1} \times E_2^{n_2}$. Since H and $\pi(H)$ have the same dimension, they are isogenous and so there exists an isogeny $\hat{\pi}$ from $\pi(H)$ to H which is an inverse of π up to multiplication by some non-zero rational integer.

We can now identify the group H' of the present lemma. Let O be the zero of $E_1^{n_1-1}$. We claim that either

(a) $K = \pi(H)$ is non-split in $E_1^{n_1-1} \times E_2^{n_2}$, or

(b) L is non-split in $E_1 \times E_2^{n_2}$, where $O \times L$ is the maximal connected subgroup of the intersection of H with $O \times E_1 \times E_2^{n_2}$.

Let us assume on the contrary that (a) and (b) are both false. Then

$$K = K_1 \times K_2, \qquad L = L_1 \times L_2$$

for $K_1 \subseteq E_1^{n_1-1}$, $L_1 \subseteq E_1$ and K_2, $L_2 \subseteq E_2^{n_2}$. Write $J = \hat{\pi}(O \times K_2)$. Since $\pi(J) = O \times K_2$, it follows that $J \subseteq O \times E_1 \times E_2^{n_2}$. Because J is a connected subgroup of H, we even have $J \subseteq O \times L$. Applying π again, we get $O \times K_2 \subseteq O \times L_2$ and so $K_2 \subseteq L_2$. Since H already contains $O \times L_1 \times L_2$, it therefore contains $O \times O_1 \times K_2$ (where O_1 is the zero of E_1). But because K_2 is the projection to $E_2^{n_2}$ of H, it follows easily that H is split in $E_1^{n_1} \times E_2^{n_2}$. This contradicts one of our hypotheses, and thereby establishes the validity of either (a) or (b).

Finally, if (a) is true, then the present lemma holds with $n_1' = n_1 - 1$, $n_2' = n_2$ and $H' = K$ using Lemma 2.1. And if (b) is true, then the present lemma holds with $n_1' = 1$, $n_2' = n_2$ and $H' = L$. For since $Z = O \times E_1 \times E_2^{n_2}$ is defined in G by equations of degrees at most 3, we see from Lemma 2.2 that

$$3^{d'} \deg(Z \cap H) \leqq 3^d \deg H.$$

Also $\deg(O \times L) \leqq \deg(Z \cap H)$, and since $O \times L$ projects down to L in the sense of Lemma 2.1, we have $\deg L \leqq \deg(O \times L)$. These inequalities combine to give the desired estimates for $\deg H'$ in case (b), and this completes the proof of the present lemma.

We can now prove the main result of this section.

Isogeny Lemma. *For positive integers n_1 and n_2 suppose $E_1^{n_1} \times E_2^{n_2}$ has a non-split connected algebraic subgroup of dimension d and degree Δ. Then there is an isogeny between E_1 and E_2 of degree at most $3^{2d}\Delta^2$.*

Proof. Actually we shall need this result only for $n_1 = n_2 = 2$, but it is no harder to establish it in general. We start with the case $n_1 = n_2 = 1$.

Let H be a non-split connected algebraic subgroup of $E_1 \times E_2$ of degree Δ in $\mathbb{P}_8$. Then H has codimension 1 in $E_1 \times E_2$. Let O_1 and O_2 be the zeros of E_1 and E_2, and define algebraic subgroups H_1 of E_1 and H_2 of E_2 by

$$H_1 \times O_2 = H \cap (E_1 \times O_2), \qquad O_1 \times H_2 = H \cap (O_1 \times E_2).$$

Since $E_1 \times O_2$ and $O_1 \times E_2$ are defined in $\mathbb{P}_8$ by equations of degree at most 3, we find from Lemma 2.2 that

$$\deg(H_1 \times O_2) \leqq 3\Delta, \quad \deg(O_1 \times H_2) \leqq 3\Delta.$$

Because $H_1 \times O_2$ and $O_1 \times H_2$ project down to H_1 and H_2 in the sense of Lemma 2.1, we deduce that

$$\deg H_1 \leqq 3\Delta, \quad \deg H_2 \leqq 3\Delta.$$

But since H is non-split it is easy to see that H_1 and H_2 are finite. Therefore their cardinalities h_1 and h_2 satisfy

$$h_1 \leqq 3\Delta, \quad h_2 \leqq 3\Delta. \tag{2.3}$$

We can now define an isogeny φ from E_1 to E_2 by $\varphi(x_1) = h_2 x_2$, where x_2 is any element of E_2 with

$$(x_1, x_2) \text{ in } H. \tag{2.4}$$

The degree N of φ is the cardinality of the kernel Φ of φ. To estimate this, note that each x_1 in Φ gives rise via (2.4) to an element x_2 of the kernel F_2 of multiplication by h_2 in E_2. But for each x_2 in E_2 the set of x_1 in E_1 satisfying (2.4) is a coset $C(x_2)$ of H_1. Also if $x_2' \equiv x_2'' \pmod{H_2}$ then $(x_1, x_2') \equiv (x_1, x_2'') \pmod{H}$, so that $C(x_2') = C(x_2'')$. Hence as x_2 runs over F_2 the number of different cosets arising in this way is the index $[F_2 : H_2]$ of H_2 in F_2, which is $h_2^2/h_2 = h_2$. Each coset has cardinality h_1, so we get $N \leqq h_1 h_2$, which by (2.3) is at most $9\Delta^2$. This proves the Isogeny Lemma for $n_1 = n_2 = 1$.

The general case can be reduced to this case by repeated applications of Lemma 2.3. Eventually we must end up with a non-split connected algebraic subgroup $\tilde{H}$ of $E_1 \times E_2$, of dimension 1, satisfying $3 \deg \tilde{H} \leqq 3^d \Delta$. By what has just been established, this yields an isogeny between E_1 and E_2 of degree at most $9(\deg \tilde{H})^2 \leqq 3^{2d} \Delta^2$. The proof of the Isogeny Lemma is therefore complete.

We shall see in Sect. 7 that the exponent 2 of Δ^2 in this result cannot be improved, whatever the values of n_1, n_2 and d.

3. Preliminary estimates

Let Ω be a lattice in the complex plane. We can choose basis elements ω_1, ω_2 of Ω in such a way that the ratio $\tau = \omega_2/\omega_1$ lies in the standard fundamental region for the modular group. Thus we have $|\tau| \geqq 1$ and $\tau = x + iy$ for real x, y satisfying

$$|x| \leqq \tfrac{1}{2}, \quad y \geqq \tfrac{1}{2}\sqrt{3}. \tag{3.1}$$

Also the determinant A of Ω is given by $A = y|\omega_1|^2$.

Let g_2 and g_3 be the invariants of Ω, and let $\wp(z)$ be the corresponding Weierstrass function. Write

$$\gamma = \max\{|\tfrac{1}{4} g_2|^{1/2}, |\tfrac{1}{4} g_3|^{1/3}\}. \tag{3.2}$$

Lemma 3.1. *There exists an absolute constant c_1 and a function $\vartheta_0(z)$, such that $\vartheta(z) = \gamma\, \vartheta_0(z)$ and $\mathfrak{F}(z) = \wp(z)\, \vartheta_0(z)$ are entire functions, with no common zeroes, that satisfy*

$$|\log \max\{|\vartheta(z)|, |\mathfrak{F}(z)|\} - \pi |z|^2/A| \leqq c_1 y$$

for all complex z.

Proof. This is just Lemma 3.1 of [M].

We shall also need the following estimate for $\wp(z)$ itself, which is not a direct consequence of the preceding result. Let $\|z\|$ denote the distance from z to the nearest element of Ω.

Lemma 3.2. *There exists an absolute constant c_2 such that*

$$|\wp(z) - \wp(\tfrac{1}{2}\omega_2)| \leqq c_2 \|z\|^{-2}$$

for all complex z not in Ω.

Proof. Let $q = e^{2\pi i \tau}$, $w = \pi z/\omega_1$, $Q = e^{iw}$ and

$$F(v) = (1 - q^v Q^2)^2 (1 - q^v Q^{-2})^2 (1 - q^v)^{-4} \qquad (v \neq 0).$$

The identity

$$\wp(z) - \wp(\tfrac{1}{2}\omega_2) = z^{-2} (w^{-1} \sin w)^{-2} \prod_{n=1}^{\infty} \{F(n - \tfrac{1}{2})/F(n)\} \tag{3.3}$$

is most easily verified by comparison of poles and zeroes.

By periodicity it is enough to prove the lemma when $z = t_1 \omega_1 + t_2 \omega_2$ for real t_1, t_2 with $|t_1| \leqq \frac{1}{2}$, $|t_2| \leqq \frac{1}{2}$. Then $|Q| = e^{-\pi t_2 y}$, $|q| = e^{-2\pi y}$. So for $v \geqq \frac{1}{2}$ we have

$$|1 - q^v Q^{\pm 2}| \leqq 1 + |q|^{v - \frac{1}{2}}, \qquad |1 - q^v| \geqq 1 - |q|^v.$$

Since $|q| \leqq e^{-\pi\sqrt{3}} < 1$ it follows without difficulty that $\prod_{n=1}^{\infty} |F(n - \frac{1}{2})|$ is bounded above by an absolute constant. Similarly for $v \geqq 1$ we have

$$|1 - q^v Q^{\pm 2}| \geqq 1 - |q|^{v - \frac{1}{2}}, \qquad |1 - q^v| \leqq 1 + |q|^v,$$

and it follows that $\prod_{n=1}^{\infty} |F(n)|$ is bounded below by a positive absolute constant.

Finally for $w = \pi z/\omega_1$ we have $z \neq 0$ and

$$|\operatorname{Re} w| = \pi(t_1 + x t_2) \leqq 3\pi/4.$$

Since $|z|^{-2} \leqq \|z\|^{-2}$ in (3.3), it suffices now to verify that $|w^{-1} \sin w|$ is bounded below by a positive absolute constant whenever $|\operatorname{Re} w| \leqq 3\pi/4$. For this we may suppose $t = \operatorname{Im} w \geqq 0$. If $t \leqq 3\pi/4$ the assertion is true by compactness. If $t > 3\pi/4$ then $|w| < t\sqrt{2}$ so

$$|\sin w| \geqq \tfrac{1}{2}(e^t - e^{-t}) > t > |w|/\sqrt{2}.$$

This completes the proof of the lemma.

It is perhaps interesting to note that an application of Cauchy's Integral Formula to Lemma 3.2 yields the inequality

$$|\wp'(z)| \leqq c\,\|z\|^{-3}$$

for an absolute constant c.

For the rest of this section we let d be a positive integer and we let k be a number field of degree at most d. We assume that the invariants g_2 and g_3 of Ω lie in k, and we use the notation

$$w = \max\{1, h(g_2), h(g_3)\}$$

as in Sect. 1. Recall that h is the absolute logarithmic height.

Lemma 3.3. *There is a constant $c_3 > 1$, depending only on d, such that*

(i) $c_3^{-w} \leqq \gamma \leqq c_3^{w}$,
(ii) $\tfrac{1}{2}\sqrt{3} \leqq y \leqq c_3 w$,
(iii) $A \geqq c_3^{-w}$,
(iv) $|\omega_i| \geqq c_3^{-w}$ $(i = 1, 2)$,
(v) $A^{-1}|\omega_i|^2 \leqq c_3 w$ $(i = 1, 2)$.

Proof. The first of these is immediate from the Definition (3.2) together with elementary properties of heights. The second follows in a similar way after using the estimate (see [FP] p. 187)

$$y \leqq (2\pi)^{-1} \log(|j| + 1193),$$

where

$$j = j(\tau) = 1728\, g_2^3/(g_2^3 - 27\, g_3^2).$$

The third was proved in Lemma 4.3 of [M]; and the fourth is then clear using (ii) and the fact that $|\omega_1|^2 = y^{-1} A$. Finally the fifth inequality is a consequence of the equation

$$A^{-1}|\omega_2|^2 = y^{-1}(x^2 + y^2)$$

together with (ii) and (3.1).

Lemma 3.4. *There is a constant c_4, depending only on d, and a positive integer $b \leqq c_4^{w}$, with the following properties. Suppose n is a positive integer, ζ is an element of Ω/n not in Ω, and write $\xi = \wp(\zeta)$. Then*

(i) *ξ is an algebraic number of degree at most $c_4 n^2$ with $h(\xi) \leqq c_4 w$,*
(ii) *$b n^2 \xi$ is an algebraic integer, and $|\xi| \leqq c_4^{w} n^2$.*

Proof. Here c_5, c_6, ... will denote positive constants depending only on d. We assume first that $\frac{1}{4}g_2$ and $\frac{1}{4}g_3$ are algebraic integers. The classical multiplication formulae (see [S] p. 105 or [Ba] p. 158) show that there is a polynomial $B_n(x, y_2, y_3)$, with rational integer coefficients, and leading term $n^2 x^{n^2-1}$ as a polynomial in x, such that $B_n(\xi, \frac{1}{4}g_2, \frac{1}{4}g_3)=0$. Thus ξ clearly has degree at most $d(n^2-1)\leqq c_5 n^2$, and $n^2\xi$ is an algebraic integer.

To estimate $h(\xi)$ we observe that the Néron-Tate height $q(P)$ of the corresponding point P in $\mathbb{P}_2$ with projective coordinates 1, $\wp(\zeta)$, $\wp'(\zeta)$ satisfies $q(P)=0$. Then from Lemma 4.1 of [M] we deduce that the absolute logarithmic height $h(P)$ satisfies $h(P)\leqq c_6 w$. But $h(\xi)\leqq h(P)$.

Finally from Lemma 3.2 we have

$$|\xi|\leqq|\wp(\tfrac{1}{2}\omega_2)|+c_7\,\|\zeta\|^{-2}. \tag{3.4}$$

Now $\wp(\frac{1}{2}\omega_2)$ is one of the zeroes of $4x^3-g_2x-g_3$; so clearly $|\wp(\frac{1}{2}\omega_2)|\leqq c_8^w$. And since τ is in the fundamental domain of the modular group we know that every non-zero period ω of Ω satisfies $|\omega|\geqq|\omega_1|$. It follows that $\|\zeta\|\geqq|\omega_1|/n$. This together with (3.4) and (iv) of Lemma 3.3 show that $|\xi|\leqq c_9^w n^2$ as desired.

This proves the present lemma when $\frac{1}{4}g_2$ and $\frac{1}{4}g_3$ are algebraic integers. The general case follows on noting that we can find a positive integer $b_0\leqq c_{10}^w$ such that $\frac{1}{4}b_0^4 g_2$ and $\frac{1}{4}b_0^6 g_3$ are algebraic integers. These correspond to the lattice $\Omega_0=\Omega/b_0$ with Weierstrass function $\wp_0(z)=b_0^2\,\wp(b_0 z)$. Thus all the statements of the lemma hold for $\xi_0=\wp_0(\zeta/b_0)$ with

$$w_0=\max\{1, h(b_0^4 g_2), h(b_0^6 g_3)\}.$$

But since $\xi_0=b_0^2\xi$ and

$$w_0\leqq w+6\log b_0\leqq c_{11}\,w$$

we deduce everything at once for ξ as well. This completes the proof.

4. The Proposition: construction

Let E and E^* be elliptic curves defined over $\mathbb{C}$. As emphasized in the introduction, we are identifying these with their Weierstrass equations, and consequently we have associated period lattices Ω and Ω^*.

Let φ be an isogeny from E^* to E. There is a unique complex number α such that φ corresponds to multiplication by α on the tangent spaces; thus $\alpha\Omega^*\subseteq\Omega$ and the relative index $[\Omega:\alpha\Omega^*]$ is the degree of φ. We shall say that φ is normalized if $\alpha=1$. We also say that φ is cyclic if its kernel is a cyclic group; that is, the quotient $\Omega/\alpha\Omega^*$ is cyclic.

Of course any given isogeny can be normalized by a suitable change of scale. But this changes the invariants. In Sect. 6 we will show how to keep track of such a change. Meanwhile the present section and the next section are devoted to a proof of the following result.

Proposition. *Given a positive integer d, there exists an effective constant c, depending only on d, with the following property. Suppose E and E^* are elliptic curves defined over a number field k of degree at most d, and that there is a normalized cyclic isogeny from E^* to E of degree N. Then there is an isogeny between E and E^* of degree at most $c\{w(E)+w(E^*)+\log N\}^4$.*

We embark straightaway on the proof of this Proposition, with φ as the normalized cyclic isogeny. Then $\Omega^* \subseteq \Omega$ and $[\Omega : \Omega^*] = N$. Introduce basis elements ω_1, ω_2 of Ω and ω_1^*, ω_2^* of Ω^* as in Sect. 3, so that the numbers $\tau = \omega_2/\omega_1$ and $\tau^* = \omega_2^*/\omega_1^*$ lie in the usual fundamental region. Then there are rational integers m_{ij} $(i, j = 1, 2)$ such that

$$\omega_1^* = m_{11}\omega_1 + m_{12}\omega_2, \quad \omega_2^* = m_{21}\omega_1 + m_{22}\omega_2 \tag{4.1}$$

and also

$$m_{11}m_{22} - m_{12}m_{21} = \pm N. \tag{4.2}$$

We shall apply transcendence techniques to the simultaneous linear forms (4.1). Write

$$h = w(E) + w(E^*) \geqq 2,$$

and let $c_1, c_2, \ldots$ be positive constants depending only on d.

Lemma 4.1. *We have*

$$|m_{ij}| \leqq c_1 N^{\frac{1}{2}} h \quad (i, j = 1, 2).$$

Proof. The equations (4.1) yield the relation

$$\tau^* = (m_{22}\tau + m_{21})/(m_{12}\tau + m_{11}), \tag{4.3}$$

and by taking imaginary parts we deduce

$$y^* = (m_{11}m_{22} - m_{12}m_{21})\, y\, |m_{12}\tau + m_{11}|^{-2}, \tag{4.4}$$

where $y = \operatorname{Im}\tau$ and $y^* = \operatorname{Im}\tau^*$. This shows incidentally that the right-hand side of (4.2) should be $+N$. Now with $x = \operatorname{Re}\tau$ we get

$$(m_{12}x + m_{11})^2 + (m_{12}y)^2 = |m_{12}\tau + m_{11}|^2 = N\, y/y^*. \tag{4.5}$$

In particular

$$|m_{12}| \leqq c_2\{N/(y\, y^*)\}^{\frac{1}{2}}. \tag{4.6}$$

Also (4.5) leads to

$$|m_{11}| \leqq |m_{12}x| + \{|m_{12}y|^2 + (N\, y/y^*)\}^{\frac{1}{2}}$$

which by (4.6) gives

$$|m_{11}| \leqq c_3(N\, y/y^*)^{\frac{1}{2}} \tag{4.7}$$

using $|x| \leqq \frac{1}{2}$, $y \geqq \frac{1}{2}\sqrt{3}$.

Next from (4.3) we get

$$|m_{22}\tau+m_{21}|^2=|\tau^*|^2\,|m_{12}\tau+m_{11}|^2.$$

Since $y^*\geqq\frac{1}{2}\sqrt{3}$ and $|\mathrm{Re}\,\tau^*|\leqq\frac{1}{2}$, we see that $|\tau^*|\leqq c_4 y^*$, and thus by (4.5)

$$(m_{22}x+m_{21})^2+(m_{22}y)^2=|m_{22}\tau+m_{21}|^2\leqq c_5 N y y^*.$$

Therefore

$$|m_{22}|\leqq c_6(N y^*/y)^{\frac{1}{2}}. \tag{4.8}$$

and

$$|m_{21}|\leqq|m_{22}x|+\{|m_{22}y|^2+c_5 N y y^*\}^{\frac{1}{2}}\leqq c_7(N y y^*)^{\frac{1}{2}}. \tag{4.9}$$

The present lemma, in slightly sharpened form, now follows from the inequalities (4.6), (4.7), (4.8) and (4.9) together with the bounds $y\leqq c_8 h$ and $y^*\leqq c_8 h$ arising from (ii) of Lemma 3.3.

We now let C be a sufficiently large constant depending only on d, and we put

$$L=h+\log N\geqq 2.$$

We define positive integers D and T by

$$D=[C^{20}L^2],\qquad T=[C^{39}L^4].$$

Let $\wp(z)$ and $\wp^*(z)$ be the Weierstrass functions corresponding to Ω and Ω^* respectively. For $t>0$ and independent variables z_1, z_2 left $\mathscr{D}(t)$ denote the set of differential operators of the form

$$\partial=(\partial/\partial z_1)^{t_1}(\partial/\partial z_2)^{t_2}(t_1\geqq 0,\ t_2\geqq 0,\ t_1+t_2<t).$$

Lemma 4.2. *There is a non-zero polynomial $P(X_1, X_2, X_1^*, X_2^*)$, of degree at most D in each variable, whose coefficients are rational integers of absolute values at most $\exp(c_9 TL)$, such that the function*

$$f(z_1, z_2)=P(\wp(z_1), \wp(z_2), \wp^*(m_{11}z_1+m_{12}z_2), \wp^*(m_{21}z_1+m_{22}z_2))$$

satisfies

$$\partial f(\tfrac{1}{2}\omega_1, \tfrac{1}{2}\omega_2)=0$$

for all ∂ in $\mathscr{D}(8T)$.

Proof. This runs along standard lines. Let M denote any monomial of degree at most D in each of the four functions appearing in f, and let ∂ be any operator of $\mathscr{D}(8T)$. Then ∂M can be written as a polynomial in the four numbers m_{ij} $(i, j=1, 2)$ as well as the twelve functions obtained from the above four by replacing the Weierstrass functions by their first and second derivatives. From Lemma 3 (p. 157) of [Ba] it is easily seen that this polynomial has total degree at most $c_{10}(D+T)$ and that its coefficients are rational integers of absolute values at most $T^{8T}c_{11}^{D+T}$.

Now by Lemma 4.1 we have $\log|m_{ij}| \leqq c_{12} L$ for each non-zero m_{ij} $(i, j = 1, 2)$. Also from (4.1) the twelve functions at $(z_1, z_2) = (\frac{1}{2}\omega_1, \frac{1}{2}\omega_2)$ take the values

$$\wp^{(t)}(\tfrac{1}{2}\omega_j),\ \wp^{*(t)}(\tfrac{1}{2}\omega_j^*) \qquad (t = 0, 1, 2;\ j = 1, 2).$$

Since the invariants g_2, g_3, g_2^*, g_3^* have heights at most $h \leqq L$, it follows easily that these values also have heights at most $c_{13} L$. They lie in an extension k' of k of relative degree at most 3^4.

Finally the conditions of Lemma 4.2 amount to $R \leqq (8T)^2$ homogeneous linear equations in $S = (D+1)^4$ unknowns with coefficients in the field k' of degree at most $81d$. Since $S \geqq CR$ these can be solved in rational integers using some form of Siegel's Lemma (see for example [AM] p. 26). We find the upper bound $T^{8T} c_{14}^{L(D+T)}$ for the solution, and since $D \leqq T$ this completes the proof of the present lemma.

Let now $\vartheta_0(z)$ and $\vartheta_0^*(z)$ denote the functions in Lemma 3.1 corresponding to $\wp(z)$ and $\wp^*(z)$ respectively. Thus the function

$$\Theta(z_1, z_2) = \{\vartheta_0(z_1)\, \vartheta_0(z_2)\, \vartheta_0^*(m_{11} z_1 + m_{12} z_2)\, \vartheta_0^*(m_{21} z_1 + m_{22} z_2)\}^D$$

is entire. We also define

$$F(z_1, z_2) = \Theta(z_1, z_2) f(z_1, z_2).$$

Lemma 4.3. *The function $F(z_1, z_2)$ is entire. Further, for any complex number z and any operator ∂ in $\mathscr{D}(4T+1)$ we have*

$$|\partial F(\omega_1 z, \omega_2 z)| \leqq \exp\{c_{15} L(T + D|z|^2)\}.$$

Proof. Let γ, γ^*, ϑ, ϑ^*, $\tilde{\vartheta}$, $\tilde{\vartheta}^*$ be as in Sect. 3 corresponding to $\wp$, $\wp^*$. Then $F(z_1, z_2)$ can be expressed as a polynomial in the eight functions

$$\gamma^{-1}\vartheta(z_i),\ \tilde{\vartheta}(z_i),\ \gamma^{*-1}\vartheta^*(m_{i1} z_1 + m_{i2} z_2),\ \tilde{\vartheta}^*(m_{i1} z_1 + m_{i2} z_2) \qquad (i = 1, 2), \tag{4.10}$$

and it is therefore entire. Note that the polynomial appearing here is just the quadrihomogenized version of the polynomial P constructed in Lemma 4.2.

Now write

$$M = \max_{i,j=1,2} |m_{ij}|$$

and

$$\Delta = \min(A, A^*)$$

for the determinants A and A^* of the lattices Ω and Ω^* respectively. Define $\delta = M^{-1} \Delta^{\frac{1}{2}}$. For any complex number z let z_1 and z_2 be complex numbers satisfying

$$|z_i - \omega_i z| = \delta \qquad (i = 1, 2). \tag{4.11}$$

We claim that

$$|F(z_1, z_2)| \leqq \exp\{c_{16} L(T + D|z|^2)\}. \tag{4.12}$$

For we have $|z_i| \leqq \delta + |\omega_i z|$, and so Lemma 3.1 leads to

$$\log \max\{|\vartheta(z_i)|, |\vartheta'(z_i)|\} \leqq c_{17}\{y + A^{-1}\delta^2 + A^{-1}|\omega_i|^2 |z|^2\} \quad (i=1, 2).$$

Now $A^{-1}\delta^2 \leqq M^{-2} \leqq 1$, and from the estimates (i), (ii) and (v) of Lemma 3.3 we find that the first two expressions in (4.10) have absolute values at most

$$\exp\{c_{18} L(1+|z|^2)\}. \tag{4.13}$$

The last two expressions are estimated in a similar way. The numbers $z_i^* = m_{i1} z_1 + m_{i2} z_2$ satisfy

$$|z_i^* - \omega_i^* z| \leqq 2M\delta \quad (i=1, 2)$$

from (4.1) and (4.11). Thus we obtain this time

$$\log \max\{|\vartheta^*(z_i^*)|, |\vartheta'^*(z_i^*)|\} \leqq c_{17}\{y^* + 4M^2 A^{*-1}\delta^2 + A^{*-1}|\omega_i^*|^2 |z|^2\} \quad (i=1, 2).$$

But $4M^2 A^{*-1}\delta^2 \leqq 4$, and so, using Lemma 3.3 for E^*, we end up with the upper bound (4.13) for the absolute values of all the expressions in (4.10).

The inequality (4.12) now follows immediately from the estimates for the polynomial P given in Lemma 4.2.

Finally the Cauchy Integral Formula expresses

$$(2\pi i)^2 (t_1! t_2!)^{-1} \partial F(\omega_1 z, \omega_2 z)$$

as the integral of

$$(z_1 - \omega_1 z)^{-t_1-1} (z_2 - \omega_2 z)^{-t_2-1} F(z_1, z_2)$$

around the circles defined by (4.11). So using (4.12) we find that

$$|\partial F(\omega_1 z, \omega_2 z)| \leqq t_1! t_2! \delta^{-(t_1+t_2)} E,$$

where E is the expression on the right-hand side of (4.12). By Lemma 4.1 and (iii) of Lemma 3.3, we have $\delta \geqq c_{19}^{-h} \geqq c_{19}^{-L}$, and the inequality of the present lemma follows immediately. This concludes the proof.

Next we denote by Q the unique integral power of 2 that satisfies

$$C^{17/8} < Q \leqq 2C^{17/8}.$$

Lemma 4.4. *For any odd integer q and $\zeta = q/Q$, we have*

$$|\Theta(\omega_1 \zeta, \omega_2 \zeta)| \geqq \exp(-c_{20} DLQ^2).$$

Further, for any ∂ in $\mathscr{D}(4T+1)$ such that $\partial f(\omega_1 \zeta, \omega_2 \zeta) \neq 0$, we have

$$|\partial f(\omega_1 \zeta, \omega_2 \zeta)| \geqq \exp(-c_{20} TLQ^8).$$

Proof. We start by noting that for $z_1=\omega_1\zeta$, $z_2=\omega_2\zeta$ the functions appearing in f take the values

$$\wp(\omega_1\zeta),\ \wp(\omega_2\zeta),\ \wp^*(\omega_1^*\zeta),\ \wp^*(\omega_2^*\zeta). \tag{4.14}$$

By (i) of Lemma 3.4, these are algebraic numbers of degrees at most $c_{21}Q^2$ with heights at most $c_{21}h$. In particular

$$\max\{\gamma, |\wp(\omega_i\zeta)|\} \leqq c_{22}^{hQ^2} \quad (i=1, 2).$$

It follows from Lemmas 3.1 and 3.3 that

$$|\vartheta_0(\omega_i\zeta)| \geqq c_{23}^{-hQ^2-y} \geqq c_{24}^{-hQ^2} \quad (i=1, 2);$$

and a similar bound holds for $|\vartheta_0^*(\omega_i^*\zeta)|$ $(i=1, 2)$. These together imply the first inequality of the present lemma.

The second inequality follows rather as in the proof of Lemma 4.2. We write $\alpha=\partial f(\omega_1\zeta, \omega_2\zeta)$ as a polynomial in the m_{ij} $(i, j=1, 2)$ and the twelve numbers obtained by replacing the Weierstrass functions in (4.14) by their first and second derivatives. We find without difficulty, again using (i) of Lemma 3.4, that α has degree at most $c_{25}Q^8$ and height at most $c_{25}TL$. If $\alpha\neq 0$ the required lower bound for $|\alpha|$ follows at once. This completes the proof.

Lemma 4.5. *For any odd integer q and any ∂ in $\mathscr{D}(4T+1)$ we have*

$$\partial f(q\omega_1/Q, q\omega_2/Q)=0. \tag{4.15}$$

Proof. Assume that this is not so. Then there exists an odd integer q and an operator ∂ in $\mathscr{D}(4T+1)$ such that

$$\alpha=\partial f(\omega_1\zeta, \omega_2\zeta)\neq 0$$

for $\zeta=q/Q$. Since $f(\omega_1 z, \omega_2 z)$ has period 1 we may suppose that $0<\zeta<1$, and by choosing ∂ of minimal order we can also suppose that

$$\alpha\Theta(\omega_1\zeta, \omega_2\zeta)=G(\zeta), \tag{4.16}$$

where

$$G(z)=\partial F(\omega_1 z, \omega_2 z).$$

We shall estimate $G(\zeta)$ by the usual Schwarz Lemma.

Now any derivative $G^{(t)}(z)$ can be written as a linear combination of the $\partial' f(\omega_1 z, \omega_2 z)$ for ∂' in $\mathscr{D}(t+1+4T)$. Consequently by Lemma 4.2 and periodicity we have

$$G^{(t)}(s+\tfrac{1}{2})=0 \tag{4.17}$$

for any integer t with $0 \leqq t < 4T$ and any integer s. We apply the Schwarz Lemma to (4.17) for $0 \leqq s < S$, where

$$S = [C^{18} L].$$

We find that

$$|G(\zeta)| \leqq 2^{-4TS} M,$$

where M is the supremum of $|G(z)|$ for $|z| \leqq 5S$. From Lemma 4.3 we get

$$M \leqq \exp\{c_{26} L(T + DS^2)\} \leqq \exp(c_{27} LDS^2).$$

It follows that $|G(\zeta)| \leqq 2^{-2TS}$. Finally using (4.16) and Lemma 4.4 we see that

$$|\alpha| \leqq 2^{-2TS} \exp(c_{20} DLQ^2) \leqq 2^{-TS}.$$

But also from Lemma 4.4 we have the lower bound

$$|\alpha| \geqq \exp(-c_{20} TLQ^8).$$

These contradict each other; and so the present lemma is proved.

This completes the constructive part of the proof of the Proposition.

5. The Proposition: deconstruction

We next interpret the equations (4.15) on the algebraic group $G = E^2 \times E^{*2}$ embedded in projective space as in Sect. 2. At one place in this section (Lemma 5.2) it will be necessary to assume that neither E nor E^* has complex multiplication. In Sect. 7 we indicate how to eliminate this assumption.

Let ε be the usual exponential map from $\mathbb{C}^4$ to G obtained from the functions $\wp(z_1)$, $\wp(z_2)$, $\wp^*(z_1^*)$, $\wp^*(z_2^*)$ (and their derivatives) for independent complex variables z_1, z_2, z_1^*, z_2^*. Define a subspace Z of $\mathbb{C}^4$ by the equations

$$z_1^* = m_{11} z_1 + m_{12} z_2, \quad z_2^* = m_{21} z_1 + m_{22} z_2 \tag{5.1}$$

corresponding to (4.1). Write O, O^* and O_G for the zeros of E^2, E^{*2} and G respectively.

Lemma 5.1. *The intersection of $\varepsilon(Z)$ with $O \times E^{*2}$ is a finite group of cardinality at least N.*

Proof. Let J be this intersection. Since $N\Omega \subseteq \Omega^*$, it follows easily that $NJ = O_G$, so J must be finite. Now recall that the isogeny φ is cyclic. This means that we can find ω in Ω generating Ω over Ω^*. Consider the homomorphism ψ from $\mathbb{Z}^2$ to J defined for integers a_1, a_2 by

$$\psi(a_1, a_2) = \varepsilon\{a_1 \omega, a_2 \omega, (m_{11} a_1 + m_{12} a_2)\omega, (m_{21} a_1 + m_{22} a_2)\omega\}.$$

Its kernel Ψ may be identified in the usual terminology of the geometry of numbers (see [Ca] pp. 23, 24) with the polar lattice of $N^{-1}M$, where M is the lattice generated in $\mathbb{Z}^2$ by (m_{11}, m_{12}) and (m_{21}, m_{22}). Since M has determinant

N, we see that Ψ has determinant $N^2 N^{-1} = N$ as well. Hence the cardinality of J is at least as large as that of $\psi(\mathbb{Z}^2)$, which is N. This proves the lemma (actually it can be shown that J has cardinality exactly N).

Next let Σ be the set of even multiples of the point

$$\sigma = \varepsilon(\omega_1/Q, \omega_2/Q, \omega_1^*/Q, \omega_2^*/Q)$$

in G. This has cardinality $\frac{1}{2}Q$.

Lemma 5.2. *Suppose $H \neq G$ is a split connected algebraic subgroup of G. Then the points of Σ are distinct modulo H.*

Proof. It suffices to show that if $2r\sigma$ lies in H for some integer r, then $\frac{1}{2}Q$ divides r. Write $H = K \times K^*$ for K in E^2 and K^* in E^{*2}. Then either $K \neq E^2$ or $K^* \neq E^{*2}$. Suppose first that $K \neq E^2$. Since we are assuming that E has no complex multiplication, it follows by Kolchin's Theorem [K] that there is a non-zero linear form $k_1\pi_1 + k_2\pi_2$ vanishing identically on K. Here π_1 and π_2 denote the projections of E^2 onto its factors, and k_1 and k_2 are rational integers. Since K is connected, we can even suppose that k_1 and k_2 are relatively prime (see for example Lemma 3 (p. 430) of [MW 1]). Thus if $2r\sigma$ lies in H, we see that $2r(k_1\omega_1 + k_2\omega_2)/Q$ lies in Ω. Hence Q divides both $2rk_1$ and $2rk_2$, and so Q divides $2r$; which is what we wanted to prove.

If instead we have $K^* \neq E^{*2}$ then the argument is exactly parallel. This completes the proof of the present lemma.

For the rest of this section $c_1, c_2, \ldots$ will denote positive absolute constants. Recall that any connected algebraic subgroup H of G has the form $\varepsilon(W)$ for some subspace W of $\mathbb{C}^4$.

Lemma 5.3. *There is a connected algebraic subgroup $H = \varepsilon(W) \neq G$ of G such that*

$$T^{\rho} R \Delta \leqq c_1 D^r, \tag{5.2}$$

where r is the codimension of H in G, Δ is the degree of H, R is the number of points in Σ distinct modulo H, and ρ is the codimension of $Z \cap W$ in Z.

Proof. Let Σ_0 denote the set of odd multiples of the point σ in G. In the usual terminology of multiplicity estimates, the equations (4.15) imply that there is a polynomial, homogeneous of degree D, that vanishes to order at least $4T+1$ along $\varepsilon(Z)$ at all points of Σ_0, but does not vanish identically on G. This is almost the situation (with $p=1$, $n=4$) of Théorème 2.1 (p. 358) of Philippon's paper [P]. In the notation of [P], our Σ_0 is not $\Sigma(4)$ but its translate $\sigma + \Sigma(4)$. This makes no difference to the proof in [P], and the conclusion is unchanged. The inequality (5.2) follows at once, provided we note that translations on a single elliptic curve may be described by homogeneous polynomials of degree 2 (see for example Lemma 1 (p. 427) of [MW 1]).

We now proceed to derive the new isogeny required in the Proposition, taking each possible value of ρ in (5.2) in turn.

The case $\rho = 2$ is ruled out at once. For then (5.2) gives

$$R \leqq c_2 C^2 D^{r-4}. \tag{5.3}$$

Hence $r=4$, or $H=O_G$. So $R=\frac{1}{2}Q$; but now (5.3) contradicts the definition of Q.

Next consider the case $\rho=1$. Then $Z\cap W$ has dimension 1, so that $r\leqq 3$. If H is non-split, the Isogeny Lemma provides an isogeny of degree at most $c_3\Delta^2$. But (5.2) now implies $\Delta\leqq c_4 C^{21} L^2$. Thus we get our desired conclusion. So we may assume that $H=K\times K^*$ is split.

First suppose $r=3$. Then $Z\cap W$ and W both have dimension 1, so

$$W\subseteq Z. \tag{5.4}$$

But also we must have $K=O$ or $K^*=O^*$. If $K=O$, then (5.4) leads immediately to $K^*=O^*$ using (5.1), which is impossible. If $K^*=O^*$, we get similarly $K=O$, since the determinant in (4.2) is non-zero. So we cannot have $r=3$.

Next suppose $r\leqq 2$ (and still $\rho=1$). From Lemma 5.2 we have $R=\frac{1}{2}Q$; but (5.2) now implies $R\leqq c_5 C$, again contradicting the definition of Q.

This finishes the case $\rho=1$. It remains to consider the case $\rho=0$. Now

$$Z\subseteq W \tag{5.5}$$

and so $r\leqq 2$.

First suppose $r=2$. Then $Z=W$, so that by Lemma 5.1 the intersection J of H with $O\times E^{*2}$ is a finite set of cardinality at least N. Therefore $\deg J\geqq N$. On the other hand, since $O\times E^{*2}$ is defined by equations of degree at most 3, we find using Lemma 2.2 that $\deg J\leqq 9\Delta$. Thus $N\leqq 9\Delta$. But (5.2) now implies $\Delta\leqq c_1 D^2$. So $N\leqq 9c_1 D^2\leqq c_6 C^{40} L^4$, and we see that the degree of the original isogeny φ satisfies the required estimate.

Next suppose $r=1$. Then by (5.1) and (5.5) we see that W is defined by a single equation of the form

$$\lambda_1(m_{11}z_1+m_{12}z_2-z_1^*)+\lambda_2(m_{21}z_1+m_{22}z_2-z_2^*)=0 \tag{5.6}$$

for complex numbers λ_1, λ_2 not both zero. The left-hand side of (5.6) clearly must involve either z_1^* or z_2^*; and since the determinant in (4.2) is non-zero the same holds for z_1 and z_2. It follows easily that $H=\varepsilon(W)$ is non-split. Now (5.2) implies $\Delta\leqq c_1 D$, and therefore the Isogeny Lemma gives us our desired isogeny of degree at most $c_3\Delta^2\leqq c_7 C^{40} L^4$.

This finishes the case $\rho=0$, and thereby completes the proof of the Proposition, at least when there is no complex multiplication.

6. Normalizing the isogeny

In order to apply our Proposition, we have to show how our isogenies can be assumed to be both cyclic and normalized. The arguments of this section will hold even in the case of complex multiplication. Let K be a subfield of $\mathbb{C}$.

Lemma 6.1. *Suppose E_1 and E_2 are elliptic curves defined over K and φ is an isogeny between them. Then φ is defined over an extension of K of relative degree at most* 12.

Proof. Suppose φ corresponds to multiplication by α on the tangent spaces. Let σ be any automorphism of $\mathbb{C}$ fixing K. Then $\sigma\varphi$ is also an isogeny between E_1 and E_2, and it corresponds to multiplication by $\sigma\alpha$. Composing $\sigma\varphi$ with the dual of φ, we must end up with an endomorphism of one of the elliptic curves. It follows that $(\sigma\alpha)/\alpha$ lies in some complex quadratic extension F of $\mathbb{Q}$ not depending on σ. In particular, as σ varies we obtain at most countably many $\sigma\alpha$, and so α must be algebraic over K.

The minimal equation for α over K may be written in the form

$$x^e + a_1 x^{e-e_1} + \ldots + a_m = 0 \tag{6.1}$$

for non-zero $a_1, \ldots, a_m$ in K and integers $e, e_1, \ldots, e_m$ with $1 \leqq e_1 < \ldots < e_m = e$. Then the roots of (6.1) are the different $\sigma\alpha$. Since $(\sigma\alpha)/\alpha$ lies in F, it follows that for each i with $1 \leqq i \leqq m$ the e_i-th symmetric function $\pm a_i$ of these roots is a multiple of α^{e_i} by an element of F. Thus each α^{e_i} lies in the compositum KF of K and F. Consequently $\beta = \alpha^h$ also lies in KF, where h is the highest common factor of $e_1, \ldots, e_m$.

However, the left-hand side of (6.1) can be written as a polynomial in x^h, and therefore $e^{2\pi i/h}\alpha$ is also a root of (6.1). Thus $e^{2\pi i/h}$ lies in F. As F is complex quadratic, this implies $h \leqq 6$. It follows that $\alpha = \beta^{1/h}$ is of degree at most 6 over KF, and therefore of degree at most 12 over K. So there are at most 12 possible values of $\sigma\alpha$. Hence there are at most 12 possible conjugate isogenies $\sigma\varphi$; which means that φ must be defined over an extension of K of relative degree at most 12. This completes the proof (actually it can be shown that the number 12 here is sharp).

Lemma 6.2. *Suppose E_1 and E_2 are elliptic curves defined over K and φ is an isogeny between them also defined over K, of minimal degree among such isogenies. Then φ is cyclic.*

Proof. This is just group theory. Suppose to the contrary that φ maps E_1 to E_2 and that its kernel Φ is of order N but is not cyclic. Writing Φ as a product of cyclic groups of prime-power order, we see that there must be at least two factors of orders p^a and p^b for some prime p and some positive integers a and b. In particular Φ contains a product of two cyclic groups of order p, and it therefore contains the kernel of multiplication $[p]$ by p on E_1. Since $[p]$ is defined over K, we deduce from Corollary 4.11 (p. 77) of [S] that φ factorizes through $[p]$ to give an isogeny from E_1 to E_2, still defined over K, of degree N/p^2. This contradicts minimality and thereby proves the lemma.

Lemma 6.3. *Let Ω and Ω^* be lattices with Weierstrass functions $\wp(z)$ and $\wp^*(z)$ respectively, and suppose Ω is a sublattice of Ω^* of index N. Then*

(i) $\wp^*(z) = \wp(z) + \sum\{\wp(z+\omega^*) - \wp(\omega^*)\}$

where the sum is over representatives ω^* of non-zero elements of Ω^*/Ω,

(ii) *$\wp^*(z)$ is a rational function of $\wp(z)$ of degree N.*

Proof. The difference between the two sides in (i) is readily seen to be an entire function periodic with respect to Ω^*; and it vanishes at $z=0$. This gives (i). And (ii) follows easily from standard arguments; for example the denominator of the required rational function can be taken as the product $\Pi\{\wp(z)-\wp(\omega^*)\}$ over all ω^* as in (i). This completes the proof.

Lemma 6.4. *For $B\geqq 1$, $S\geqq 1$ let α be an algebraic number such that*
(i) *there is a positive integer $b\leqq B$ such that $b\alpha$ is an algebraic integer,*
(ii) *all conjugates of α have absolute values at most S.*
Then $h(\alpha)\leqq\log(BS)$.

Proof. Let F be any number field, of degree m say, that contains α. Then

$$m\,h(\alpha)=\sum\log\max(1,|\alpha|_v)$$

where the sum is over all suitably normalized valuations v on F. For non-archimedean v we have

$$|\alpha|_v=|b^{-1}|_v\,|b\alpha|_v\leqq|b^{-1}|_v$$

and so this part of the sum contributes at most $m\log b\leqq m\log B$. For archimedean v we have $|\alpha|_v\leqq S$, and so this part contributes at most $m\log S$. The lemma follows at once.

We can now effectively normalize our given isogeny.

Normalizing Lemma. *Given a positive integer d, there exists a constant c, depending only on d, with the following property. Let k be a number field of degree at most d, let E and E_1^* be elliptic curves defined over k, and let φ be an isogeny from E to E_1^* of degree N. Suppose k' is the smallest extension field of k over which φ is defined. Then k' has relative degree at most 12 over k, and we can find an elliptic curve E^*, defined over k' and isomorphic over k' to E_1^*, such that the induced isogeny from E to E^* is normalized. Further we have*

$$w(E^*)\leqq c\,w(E)+13\log N.$$

Proof. By Lemma 6.1 we have $[k':k]\leqq 12$. Let Ω be the period lattice of E and let Ω^* be the kernel of φ composed with the exponential map on E. Thus Ω is a sublattice of Ω^* of index N. By Lemma 6.3, the Weierstrass function corresponding to Ω^* is given by

$$\wp^*(z)=\wp(z)+\sum\{\wp(z+\omega^*)-\wp(\omega^*)\},\tag{6.2}$$

where the sum is over all representatives ω^* of non-zero elements of Ω^*/Ω.

Now recall that if g_2 and g_3 are the invariants of Ω we have the Laurent expansion

$$\wp(z)=z^{-2}+(g_2/20)\,z^2+(g_3/28)\,z^4+\ldots,$$

with a similar expression for $\wp^*(z)$ involving the invariants g_2^* and g_3^* of Ω^*. Multiply (6.2) by z^2, differentiate four times and then six times, and put $z=0$. We find that

$$g_2^* = g_2 + 10\sum \wp''(\omega^*), \qquad g_3^* = g_3 + (7/6)\sum \wp^{(\mathrm{iv})}(\omega^*). \tag{6.3}$$

The differential equation for $\wp(z)$ gives also

$$\wp''(z) = 6(\wp(z))^2 - \tfrac{1}{2} g_2, \qquad \wp^{(\mathrm{iv})}(z) = 120(\wp(z))^3 - 18\, g_2\, \wp(z) - 12\, g_3. \tag{6.4}$$

Now let $c_1, c_2, \ldots$ be positive constants depending only on d, and write $w = w(E)$. Since $N\Omega^* \subseteq \Omega$, we see that each ω^* lies in Ω/N but not in Ω. Thus from (ii) of Lemma 3.4 we obtain a positive integer $b_1 \leqq c_1^w$ such that each $b_1 N^2\, \wp(\omega^*)$ is an algebraic integer. We may also suppose that $b_1 g_2$ and $b_1 g_3$ are algebraic integers. It follows from (6.3) and (6.4) that $b g_2^*$ and $b g_3^*$ are algebraic integers for some positive integer $b \leqq B \leqq c_2^w N^6$. We also have the estimate $|\wp(\omega^*)| \leqq c_3^w N^2$, and we deduce similarly that $|g_2^*| \leqq S$, $|g_3^*| \leqq S$ for some $S \leqq c_4^w N^7$.

Next we claim that the same estimate holds for the absolute values of all the conjugates of g_2^* and g_3^*. For these are given by expressions like (6.3) involving the conjugates of g_2 and g_3 and the corresponding conjugate Weierstrass functions; and since conjugate fields have the same degree, Lemma 3.4 applies to these conjugates as well (compare [Ba] p. 159).

Now let E^* be the elliptic curve with invariants g_2^* and g_3^*. The required estimate for $w(E^*)$ follows at once from Lemma 6.4 and the above bounds for B and S. Since φ is defined over k' the coordinates $\wp(\omega^*)$ of the non-zero points of its kernel Φ form complete sets of conjugates over k', and it follows from (6.3) that g_2^* and g_3^* lie in k'. Finally E^* can be identified with $\mathbb{C}/\Omega^* = (\mathbb{C}/\Omega)/(\Omega^*/\Omega)$ and so with E/Φ; also the map φ factorizes through an isomorphism from E/Φ to E_1^* that is clearly defined over k'. And since $\Omega \subseteq \Omega^*$ and $[\Omega^* : \Omega] = N$ the induced isogeny from E to E^* is normalized. This completes the proof of the lemma.

No particular significance attaches to the number 13 appearing in this result; it merely reflects our comparatively crude choice of measure $w(E)$ for the elliptic curve E.

7. Proof of Theorem

Let $c_1, c_2, \ldots$ denote positive constants depending only on d. Suppose E is isogenous to some elliptic curve E_1^* also defined over k. Let N be the smallest degree of any isogeny between E and E_1^*. By Lemma 6.2 there is a cyclic isogeny from E to E_1^* of degree N. We now use the Normalizing Lemma to construct an extension k' of k with $[k' : k] \leqq 12$, and an elliptic curve E^* defined over k' and isomorphic to E_1^*, such that the induced isogeny φ from E to E^* is normalized, and we have

$$w(E^*) \leqq c_1(w(E) + \log N).$$

Since φ is cyclic, we deduce from the Proposition that there is an isogeny between E and E^* whose degree N_1 satisfies

$$N_1 \leqq c_2(w(E)+w(E^*)+\log N)^4 \leqq c_3(w(E)+\log N)^4.$$

So there is also an isogeny of degree N_1 between E and E_1^*, and the minimality of N implies that

$$N \leqq N_1 \leqq c_3(w(E)+\log N)^4.$$

Therefore $N \leqq c_4(w(E))^4$, and this completes the proof of the Theorem, at least when there is no complex multiplication.

We next show how to proceed when at least one of E and E^* has complex multiplication. Of course in this case both curves must have complex multiplication, and even over the same quadratic field F. Since the arguments of Sect. 6 hold in general, it suffices to prove the Proposition in this case.

All we need for this is a single relation from (4.1). Write this as $\omega_1^* = \mu_1 \omega_1$ where $\mu_1 = m_{11} + m_{12}\tau$. We can then construct an auxiliary polynomial involving just the functions $\wp(z)$ and $\wp^*(\mu_1 z)$ evaluated at rational multiples of $z = \omega_1$ (it turns out that there is no gain in considering multiples by irrational numbers in F).

The only problem with this approach is to estimate the height of μ_1 in terms of N and the parameter $h = w(E)+w(E^*)$. In view of Lemma 4.1, it is enough to estimate the height of τ. This can be done using a result of A. Faisant and G. Philibert [FP] as follows. By (i) of Lemma 3 (p. 187) of [FP], there is a positive integer $b \leqq (0.191)\log|j(\tau)|$ such that $b\tau$ is an algebraic integer; at least provided $\tau \neq e^{2\pi i/3}$. From this it follows easily from Lemma 6.4 that the (non-logarithmic) absolute height of τ is at most $c h^2$ for some c depending only on d (see also p. 192 of [FP] for the slightly sharper estimate $c h^{3/2}$). This comfortably suffices for our purposes (in fact our proof would operate even with an exponential estimate c^h).

The constructive part of the proof of the Proposition now presents no difficulties; indeed we no longer have to use Baker's method or division values. The deconstructive part also simplifies considerably; we can show directly using the elementary results of [BM] that the auxiliary function must vanish identically. Then a simple argument leads to the desired new isogeny. Because the proofs are much closer to the classical style, we excuse ourselves from giving any further details.

Actually these considerations lead to a little more information. The new isogeny φ_1 constructed in this way clearly corresponds to multiplication on the tangent spaces by some rational multiple of μ_1. But we could equally well have argued with the second relation $\omega_2^* = \mu_2 \omega_1$ from (4.1), where $\mu_2 = m_{21} + m_{22}\tau$. This yields a new isogeny φ_2 corresponding to multiplication on the tangent spaces by some rational multiple of μ_2. Since $\mu_1/\mu_2 = \omega_1^*/\omega_2^*$ is irrational, the isogenies φ_1, φ_2 must be linearly independent over the rational integers.

It follows without difficulty that by suitably adapting the arguments of Sect. 7 we can prove that if E has complex multiplication and is isogenous to a second elliptic curve defined over k, then there are two linearly independent isogenies

between them of degrees at most $c(w(E))^4$. It is amusing to note further, in the style of successive minima, that thanks to the use of the smaller periods ω_1 and ω_1^*, the estimate for the degree of one of these isogenies can be improved to $c(w(E))^2$. In particular, our Theorem for a single isogeny holds with $c(w(E))^2$ in place of $c(w(E))^4$ in the case of complex multiplication.

It is perhaps also worth remarking that in the case of complex multiplication it is easy to construct explicitly a complex number $\beta \neq 0$ such that $\beta(\mathbb{Z}+\mathbb{Z}\tau) \subseteq \mathbb{Z}+\mathbb{Z}\tau^*$. This corresponds to an isogeny from E to E^*, and by using the estimates of [FP] for τ^* as well as τ, we find that its degree is at most $c h^6$ for c depending only on d. So we obtain an estimate slightly weaker than that of the Proposition, but on the other hand it is independent of N.

Finally, as promised, we show that the estimate of the Isogeny Lemma in Sect. 2 cannot be improved, except possibly for the constants. We need first a result about isogenies considered as projective morphisms.

Lemma 7.1. *Let E_1 and E_2 be elliptic curves in $\mathbb{P}_2$ and let φ be an isogeny from E_1 to E_2 of degree N. Then, as a morphism, φ can be described by homogeneous polynomials of degrees $8N$.*

Proof. By a change of scale we can suppose that φ is normalized in the sense of the preceding sections. It follows from Lemma 6.3 that the Weierstrass function $\wp_2(z)$ is a rational function of degree N in $\wp_1(z)$. Differentiation then gives $\wp_2'(z)/\wp_1'(z)$ as a rational function of degree at most $2N$ in $\wp_1(z)$. The resulting expressions show that, at least on some non-empty open subset of E_1, the map φ can be described by homogeneous polynomials of degree $2N$.

Now, as remarked in Sect. 5, any translation T_a by a on E_1 can be described as a morphism by homogeneous polynomials of degree 2. The present lemma follows easily by writing

$$\varphi(x_1) = T_b(\varphi(T_a(x_1))) \qquad (b = -\varphi(a))$$

for all a in E_1. Actually it is not too difficult to reduce the degree $8N$ to N, by using the explicit formulae in [V] (p. 239) together with the considerations of [MW 1] (p. 448).

Now let $N = n^2$ be any perfect square, and let E_1 and E_2 be the elliptic curves with period lattices

$$\Omega_1 = \mathbb{Z} + iN\mathbb{Z}, \qquad \Omega_2 = \mathbb{Z} + i\mathbb{Z}.$$

The inclusion $\Omega_1 \subseteq \Omega_2$ gives rise to a (normalized) cyclic isogeny φ from E_1 to E_2 of degree N, and it is easy to see that there is no isogeny of smaller degree. As usual embed $G = E_1 \times E_2$ in $\mathbb{P}_8$. We proceed to construct a non-split connected algebraic subgroup H of G with degree

$$\Delta \leqq 2^4 \cdot 3^6 N^{\frac{1}{2}}.$$

This shows that for $n_1 = n_2 = 1$ the exponent 2 in the Isogeny Lemma cannot be improved, and even that the constant 3^2 cannot be replaced by anything smaller than $2^{-8} \cdot 3^{-12}$.

Consider first the algebraic subgroup H' of G defined as the set of (x_1, x_2) in G for which $\varphi(x_1)=n x_2$. Lemma 7.1 shows that φ is described by homogeneous polynomials of degree $8N$. Also Serre proves ([Wa] p. 195 – see also [MW1] p. 447) that multiplication by n can be described by homogeneous polynomials of degree $n^2=N$. It follows that H' is defined in G by homogeneous polynomials of degree $8N$. Since already G is defined in $\mathbb{P}_8$ by homogeneous polynomials of degree 3, we deduce from two applications of Lemma 2.2 that

$$\deg H' \leqq 2^3 \cdot 3^6 N.$$

Now H' is generally not connected. Indeed let $\hat{\varphi}$ be the isogeny dual to φ, and define a function f from $E_1 \times E_2$ to E_1 by

$$f(x_1, x_2)=n x_1 - \hat{\varphi}(x_2).$$

On H' we have

$$\varphi(f(x_1, x_2))=n\varphi(x_1)-N x_2=n(\varphi(x_1)-n x_2)=0.$$

Therefore $f(H')$ is finite. Let x_1 be any element of the kernel Φ of φ. Since $\varphi(x_1)=0$ and $f(x_1, 0)=n x_1$, we see that $n x_1$ is in $f(H')$. Since Φ is cyclic of order n^2, we get exactly n different points $n x_1$ in this way. Thus the cardinality of $f(H')$ is at least n.

It follows that H' has at least n connected components. If Δ is the degree of the maximal connected subgroup, these components all have degrees at least $\frac{1}{2}\Delta$ (see [MW2] p. 243 or [P] p. 376). Thus, as promised,

$$\Delta \leqq 2n^{-1} \deg H' \leqq 2^4 \cdot 3^6 n = 2^4 \cdot 3^6 N^{\frac{1}{2}}.$$

This example for $n_1=n_2=1$ can readily be extended to arbitrary n_1 and n_2, and even to arbitrary values of the dimension d of H. We simply take any product of factors of $E_1^{n_1-1} \times E_2^{n_2-1}$ and we multiply this by the above subgroup H of $E_1 \times E_2$.

References

[AM] Anderson, M., Masser, D.W.: Lower bounds for heights on elliptic curves. Math. Z. **174**, 23–34 (1980)

[Ba] Baker, A.: On the periods of the Weierstrass $\wp$-function. Symposia Math. Vol. IV, INDAM Rome 1968, Academic Press, London 1970, pp. 155–174

[BM] Brownawell, W.D., Masser, D.W.: Multiplicity estimates for analytic functions I. J. Reine Angew. Math. **314**, 200–216 (1979)

[Ca] Cassels, J.W.S.: An introduction to the geometry of numbers. Berlin Göttingen Heidelberg: Springer 1959

[CC] Chudnovsky, D.V., Chudnovsky, G.V.: Padé approximations and algebraic geometry. Proc. Natl. Acad. Sci. USA **82**, 2212–2216 (1985)

[FP] Faisant, A., Philibert, G.: Quelques résultats de transcendance liés à l'invariant modulaire j. J. Number Theory **25**, 184–200 (1987)

[K] Kolchin, E.R.: Algebraic groups and algebraic dependence. Am. J. Math. **90**, 1151–1164 (1968)

[La] Laurent, M.: Une nouvelle démonstration du théorème d'isogénie, d'après D.V. et G.V.

Choodnovsky, Séminaire de Théorie de Nombres de Paris 1985–6, Boston Basel Stuttgart, Birkhäuser, 1987, pp. 119–131

[Lo] Loxton, J.H.: Some problems involving powers of integers. Acta Arith. **46**, 113–123 (1986)

[M] Masser, D.W.: Counting points of small height on elliptic curves. Bull. Soc. Math. Fr. (to appear)

[MW1] Masser, D.W., Wüstholz, G.: Fields of large transcendence degree generated by values of elliptic functions. Invent. Math. **72**, 407–464 (1983)

[MW2] Masser, D.W., Wüstholz, G.: Zero estimates on group varieties II. Invent. Math. **80**, 233–267 (1985)

[MW3] Masser, D.W., Wüstholz, G.: Some effective estimates for elliptic curves, to appear in the Proceedings of the 1988 Erlangen Workshop on Arithmetic Complex Manifolds. (Lect. Notes Math., Berlin Heidelberg New York: Springer, to appear)

[P] Philippon, P.: Lemmes de zéros dans les groupes algébriques. Bull. Soc. Math. Fr. **114**, 355–383 (1986)

[S] Silverman, J.H.: The arithmetic of elliptic curves. New York Berlin Heidelberg: Springer 1986

[V] Vélu, J.: Isogénies entre courbes elliptiques. C.R. Acad. Sci. Paris A **273**, 238–241 (1973)

[Wa] Waldschmidt, M.: Nombres transcendants et groupes algébriques. Astérisque **69–70** (1979)

[Wü1] Wüstholz, G.: Multiplicity estimates on group varieties. Ann. Math. **129**, 471–500 (1989)

[Wü2] Wüstholz, G.: Zum Periodenproblem. Invent. Math. **78**, 381–391 (1984)

Oblatum 17-I-1989 & 17-VII-1989