Math. Ann. (2012) 352:453–484
DOI 10.1007/s00208-011-0645-4

Mathematische Annalen

Torsion points on families of squares of elliptic curves

D. Masser · U. Zannier

Received: 25 July 2010 / Revised: 9 January 2011 / Published online: 15 February 2011

Abstract In a recent paper we proved that there are at most finitely many complex numbers $\lambda \neq 0, 1$ such that the points $(2, \sqrt{2(2-\lambda)})$ and $(3, \sqrt{6(3-\lambda)})$ are both torsion on the elliptic curve defined by $Y^2 = X(X-1)(X-\lambda)$. Here we give a generalization to any two points with coordinates algebraic over the field $\mathbf{Q}(\lambda)$ and even over $\mathbf{C}(\lambda)$. This implies a special case of a variant of Pink's Conjecture for a variety inside a semiabelian scheme: namely for any curve inside any scheme isogenous to a fibred product of two isogenous elliptic schemes.

Mathematics Subject Classification (2000) 11G05 · 11G50 · 14K05 · 14J20

1 Introduction

Motivated by recent work on unlikely intersections, we consider here the following conjecture to be found in our recent article [17].

Conjecture *Let $\mathcal{S}$ be a semiabelian scheme over a variety defined over $\mathbf{C}$, and denote by $\mathcal{S}^{[c]}$ the union of its semiabelian subschemes of codimension at least c. Let $\mathcal{V}$ be an irreducible closed subvariety of $\mathcal{S}$. Then $\mathcal{V} \cap \mathcal{S}^{[1+\dim \mathcal{V}]}$ is contained in a finite union of semiabelian subschemes of $\mathcal{S}$ of positive codimension.*

This is a variant of that stated by Pink [21] in 2005, which generalized the Zilber Conjectures [26] to schemes.

D. Masser (✉)
Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland
e-mail: David.Masser@unibas.ch

U. Zannier
Scuola Normale, Piazza Cavalieri 7, 56126 Pisa, Italy
e-mail: u.zannier@sns.it

In [17] (see also [16] for a short version) we verified this conjecture in a special case where $\mathcal{S}$ is the fibred square of the standard Legendre elliptic family, with coordinates (X_1, Y_1), (X_2, Y_2), and $\mathcal{V}$ is the curve defined by $X_1 = 2$, $X_2 = 3$. This amounted to the finiteness of the set of complex numbers $\lambda \neq 0, 1$ such that the points

$$\left(2, \sqrt{2(2-\lambda)}\right), \quad \left(3, \sqrt{6(3-\lambda)}\right) \tag{1.1}$$

both have finite order on the elliptic curve E_λ defined by $Y^2 = X(X-1)(X-\lambda)$.

A referee for [16] asked what happens when the X-coordinates 2,3 are replaced by any two distinct complex numbers κ, κ'. In fact we had already noted that our method is capable of some extension, and here we generalize the result to any X-coordinates defined over an algebraic closure of $\mathbf{C}(\lambda)$; of course then the Y-coordinates are also defined over this closure. It turns out that this is equivalent to the Conjecture above with $\mathcal{S}$ isogenous to the product of two isogenous elliptic schemes and $\mathcal{V}$ a curve. Thus we shall prove the following result.

Theorem *Let $\mathcal{A}$ be an abelian surface scheme over a variety defined over $\mathbf{C}$, and suppose that $\mathcal{A}$ is isogenous to the fibred product of two isogenous elliptic schemes. Let $\mathcal{V}$ be an irreducible closed curve in $\mathcal{A}$. Then $\mathcal{V} \cap \mathcal{A}^{[2]}$ is contained in a finite union of abelian subschemes of $\mathcal{A}$ of positive codimension.*

We will soon see that the base variety can be assumed to be irreducible of dimension at most one. In case it is a point, then $\mathcal{A}$ is constant and we see the classical result of Manin–Mumford type in the special situation under consideration. In fact we will appeal to the classical result to eliminate this case.

We give some simple examples of our theorem for base curves.

Thus we get the finiteness of the set of complex numbers $\tau \neq 0, \pm\frac{3\sqrt{3}}{8}$ such that the points (τ, τ) and $(-\tau, \tau)$ have finite order on the Weierstrass elliptic curve defined by $Y^2 = 4X^3 - 4\tau^2 X + \tau^2$. Or that of the set of complex numbers $\lambda \neq 0, 1$ such that the points

$$\left(2\lambda, \lambda\sqrt{2(2\lambda-1)}\right), \quad \left(3\lambda, \lambda\sqrt{6(3\lambda-1)}\right) \tag{1.2}$$

have finite order on E_λ (compare with (1.1)). Or the complex numbers τ with $64\tau^6 \neq 27\pi^4$ such that (τ, π) and $(-\tau, \pi)$ have finite order on $Y^2 = 4X^3 - 4\tau^2 X + \pi^2$. Or the complex numbers $\lambda \neq 0, 1$ such that

$$\left(2\pi, \sqrt{2\pi(2\pi-1)(2\pi-\lambda)}\right), \quad \left(3\pi, \sqrt{3\pi(3\pi-1)(3\pi-\lambda)}\right) \tag{1.3}$$

have finite order on E_λ (compare with (1.2)).

In all these examples $\mathcal{A}$ is a scheme over a curve parametrized by τ or λ. It can be checked that $\mathcal{V}$ does not lie in $\mathcal{A}^{[1]}$; thus it has zero-dimensional intersection with any subscheme of positive codimension, leading to finiteness statements. To do this checking we note that because there is no complex multiplication, we can find p, q in $\mathbf{Z}$ not both zero such that $qP = pQ$ on such a subscheme, at least for all values of the curve

parameter with at most finitely many exceptions. However $\mathcal{V}$ projects down to the full curve and so it suffices to disprove $qP = pQ$ identically on $\mathcal{V}$. For this there are several methods available such as specialization of the parameter or using it to calculate functional Néron-Tate height pairings and check that the regulator is non-zero.

In the scheme-theoretical context, the natural limit of our method seems at the moment to be the situation of a curve inside a semiabelian scheme of relative dimension 2. In future papers we will consider schemes of non-simple abelian surfaces, which by the above Theorem amounts to $\mathcal{A}$ being isogenous to the product of two non-isogenous elliptic schemes, and then schemes of simple abelian surfaces. One could also consider extensions of an elliptic scheme by $\mathbf{G}_m$.

When $\mathcal{A}$ and $\mathcal{V}$ are defined over the field $\overline{\mathbf{Q}}$ of all algebraic numbers, our proof follows the general strategy of [16,17] and [20]. In the context of Legendre elliptic curves, this amounts to the study of equations

$$z = xf + yg, \quad w = uf + vg \tag{1.4}$$

where z, w are elliptic logarithms of points P_λ, Q_λ like (1.1) or (1.2), and f, g are basis elements of the period lattice of E_λ. Our coefficients x, y, u, v are real and their locus S in $\mathbf{R}^4$ is subanalytic, of dimension at most 2 because a complex curve has real dimension 2. When P_λ, Q_λ are both torsion for some specific λ, say of orders dividing some n, then we get a rational point in $\frac{1}{n}\mathbf{Z}^4$ on S. The work of Pila [19] provides for any $\epsilon > 0$ an upper bound for their number of order at most n^ϵ as n tends to infinity, provided we avoid connected semialgebraic curves inside S.

Now if it happens that $qP_\lambda = pQ_\lambda$ for generic λ and integers p, q not both zero, then we get the analogue of an abelian subscheme as in the Theorem.

Otherwise we are able to show that there are no such semialgebraic curves. This follows from the homogeneous algebraic independence of the functions f, g, z, w in (1.4). In [17] the analogous independence was proved with relatively simple arguments involving monodromy on f and g so essentially $SL_2(\mathbf{Z})$. Extending these arguments to the present paper involves monodromy on all of f, g, z, w and is a rather more complicated matter. But Bertrand wondered if the algebraic independence of z, w over $\mathbf{C}(f, g)$ would suffice, because this he had already proved in 1990 using some D-module theory applied to the Picard–Fuchs differential operator. And indeed it turns out that this alternative independence does suffice (in fact it even implies the homogeneous independence in view of the much easier linear independence of f and g).

Nevertheless we think it of definite interest to present in Appendix A a self-contained proof of the algebraic independence, even not necessarily homogeneous, of f, g, z, w. No D-modules are used, and the exponential map plays a role similar to that of the Picard–Fuchs operator to kill the periods. The monodromy on f, g, z, w leads to an arithmetic subgroup E of $SL_4(\mathbf{Z})$. This could be handled in the same style as in [17] provided we exploit the many hyperbolic elements of $SL_2(\mathbf{Z})$ to obtain infinitely many different real quadratic fields for the eigenvalues. But here we have taken a different approach using the Zariski closure of E in $SL_4(\mathbf{C})$ which turns out to be much more amenable, thanks to some elementary cohomology. In fact we can determine this closure precisely (see Lemma A.5). However both approaches seem to need some extra considerations involving logarithmic singularities. For completeness

we include in this Appendix also a short self-contained derivation of the monodromy on f and g; our reference in [17] for this may have been not quite satisfactory.

We conclude the proof over $\overline{\mathbf{Q}}$ as in [17] by combining Silverman's Specialization Theorem [24] with David's result [7] on counting conjugates of torsion points to show by contrast that the number of rational points is of order at least n^{δ} for some $\delta > 0$. Comparison of this lower bound with the above upper bound leads to an estimate for n which suffices to prove the Theorem.

When $\mathcal{A}$ and $\mathcal{V}$ are not defined over $\overline{\mathbf{Q}}$ as in (1.3), we may suppose that λ is transcendental over $\mathbf{Q}$. Now there arises the possibility of using a specialization argument like those of [3] or [4]. However the classical theory of Fricke and Weber provides so much Galois information on torsion points that we no longer need the work of [19]. This leads to effective and even explicit results. For example if κ, κ' are distinct transcendental numbers with $\frac{\kappa'}{\kappa}$ rational, then there are at most 10^{40} complex values of $\lambda \neq 0, 1$ such that the points

$$\left(\kappa, \sqrt{\kappa(\kappa-1)(\kappa-\lambda)}\right), \quad \left(\kappa', \sqrt{\kappa'(\kappa'-1)(\kappa'-\lambda)}\right) \tag{1.5}$$

both have finite order on E_λ. Further in any specific case (like (1.3)) it will be clear how to find effectively all these λ (probably none). Actually in a subsequent note we will use additional ideas to show for example that there really are no λ even in a situation slightly more general than (1.5).

Here is a brief section-by-section account of this paper.

In Sect. 2 we show how to reduce to a Proposition involving the special case $\mathcal{A} = E_\lambda^2$, and in Sect. 3 we recall the main result of [19] on subanalytic sets. Our own set is constructed from elliptic logarithms defined in Sect. 4. The relevant algebraic independence result is then proved in Sect. 5 (or Appendix A). This then leads in Sect. 6 to the non-existence of Pila's semialgebraic curves in our set. Then in Sects. 7 and 8 we record the consequences of the work of David and Silverman for our purposes, and the proof of the Proposition over $\overline{\mathbf{Q}}$ is completed in Sect. 9.

When things are not over $\overline{\mathbf{Q}}$, we begin in Sect. 10 with a statement of the Galois-theoretical situation. There follow in Sect. 11 two results about a fixed relation between the X-coordinates of points like (1.3). These are developed further in Sect. 12 with the help of Tate curves; and in Appendix B we present an alternative argument using instead diophantine approximation ideas present in Liardet's proof of his theorem on torsion points in $\mathbf{G}_m \times \mathbf{G}_m$. We finish the proof of our Proposition in Sect. 13, and we check our examples in Sect. 14.

We heartily thank Daniel Bertrand for his interest in these matters and his intervention in the algebraic independence proof. This idea promises to be especially valuable in the extensions to other schemes.

2 Reduction to a Legendre curve

We start by noting that the above Conjecture is isogeny invariant in the following sense. Let $\mathcal{S}$, $\mathcal{S}'$ be semiabelian schemes defined over varieties over $\mathbf{C}$ and suppose that there is an isogeny σ from $\mathcal{S}$ to $\mathcal{S}'$. Then the Conjecture for $\mathcal{S}'$ implies the Conjecture for $\mathcal{S}$.

For let $\mathcal{V}$ be a subvariety of $\mathcal{S}$, say of dimension d. Then $\mathcal{V}' = \sigma(\mathcal{V})$ is a subvariety of $\sigma(\mathcal{S}) = \mathcal{S}'$ of the same dimension. A point t of $\mathcal{V} \cap \mathcal{S}^{[1+d]}$ maps to $t' = \sigma(t)$ in $\mathcal{V}' \cap \sigma(\mathcal{S}^{[1+d]})$. Now if $\mathcal{T}$ is a semiabelian subscheme of $\mathcal{S}$ of codimension at least $1+d$, then $\sigma(\mathcal{T})$ is a semiabelian subscheme of $\mathcal{S}'$ of the same codimension. It follows that t' lies in $\mathcal{V}' \cap \mathcal{S}'^{[1+d]}$. The Conjecture for $\mathcal{S}'$ shows that $t' = \sigma(t)$ lies in a finite union of semiabelian subschemes of $\mathcal{S}'$ of positive codimension; and this gives at once the corresponding assertion for t in $\mathcal{V} \cap \mathcal{S}^{[1+d]}$.

Next, as mentioned in the Introduction, if $\mathcal{V}$ is a curve then we can assume that the base variety is irreducible of dimension at most one. For if π is the projection to the original base, we merely have to restrict $\mathcal{S}$ to the fibres over $\pi(\mathcal{V})$.

Now we have an isogeny from the $\mathcal{S} = A$ of our Theorem to the fibred square $\mathcal{E}^2$ of an elliptic scheme. Under the above assumption about the base variety for the latter, the reduction of $\mathcal{E}$ to Legendre form provides σ as above, with $\mathcal{S}' = E_\lambda^2$ having coordinates now (X, Y) and say (U, V). Let $\mathcal{V}$ be a curve in $\mathcal{S}$. Then $\sigma(\mathcal{V})$ in E_λ^2 is a curve C in the affine space $\mathbf{A}^5$ with coordinates X, Y, U, V, λ. We will regard it as being parametrized by $(\xi, \eta, \mu, \nu, \lambda)$ with $\xi, \eta, \mu, \nu, \lambda$ functions in $\mathbf{C}(C)$.

If the points $P = (\xi, \eta)$, $Q = (\mu, \nu)$ satisfy $qP = pQ$ for some integers p, q not both zero, then the whole of $\sigma(\mathcal{V})$ lies in the corresponding one-dimensional abelian subscheme, so the Theorem is trivial for $\mathcal{S}'$. Thus we are entitled to assume $qP \neq pQ$ for all such integers.

If λ is constant on C, then the base variety can be considered as a point and the Theorem for $\mathcal{S}'$ follows from Manin–Mumford as mentioned in the Introduction.

From all these considerations, we see that our Theorem for $\mathcal{A}$ is implied by the following statement.

Proposition *Let C in $\mathbf{A}^5$ be a curve defined over $\mathbf{C}$ and parametrized by $(\xi, \eta, \mu, \nu, \lambda)$, with λ non-constant. Suppose that the points*

$$P = (\xi, \eta), \quad Q = (\mu, \nu)$$

lie on the Legendre elliptic curve E_λ and satisfy there

$$qP \neq pQ \tag{2.1}$$

for all integers p, q not both zero. Then there are at most finitely many points $\mathbf{c}$ in $C(\mathbf{C})$ such that

$$P(\mathbf{c}) = (\xi(\mathbf{c}), \eta(\mathbf{c})), \quad Q(\mathbf{c}) = (\mu(\mathbf{c}), \nu(\mathbf{c}))$$

are both of finite order on $E_{\lambda(\mathbf{c})}$.

We shall prove this Proposition when C is defined over $\overline{\mathbf{Q}}$ in $\mathbf{C}$, which we refer to as the algebraic case, in the following Sects. 3 to 9. Due to the use of Pila's result (not to mention the work of David using transcendence techniques) this can be considered the deepest case. Then in Sects. 10 to 13 we do the same when C is not defined over $\overline{\mathbf{Q}}$, which we refer to as the transcendental case. This is by comparison less deep.

Of course one could equally well regard P, Q above as sections of a special non-isotrivial pencil of elliptic curves, and then the isogeny invariance shows that the statement continues to hold for any such pencil.

3 Rational points

In this section we record the basic result of Pila [19] that we shall use in the algebraic case. Recall that a semialgebraic set in $\mathbf{R}^s$ is one defined by a finite number of polynomial inequalities $A \geq 0$ or $A > 0$. There are several other similar-looking and equivalent definitions (e.g. [23, p. 51]). It has a dimension (e.g. [2, p. 14]).

For any subset S of $\mathbf{R}^s$ we define S^{trans} as what remains of S after removing all positive-dimensional connected semialgebraic sets in $\mathbf{R}^s$ contained in S. This coincides with the definition in [19, p. 207], because a semialgebraic set is certainly semianalytic (see [23, p. vii] or [2, p. 10] for definitions) and so by [23, p. 40] it is subanalytic.

The result of [19] concerns compact subanalytic sets. In order to avoid the technicalities of their definition, we replace the notion by something simpler, as in [17]. Let m be a positive integer. We define a naive-m-subanalytic subset of $\mathbf{R}^s$ as a finite union of $\theta(D)$, where each D is a closed ball in $\mathbf{R}^m$ and each θ is real analytic from an open neighbourhood of D to $\mathbf{R}^s$.

Lemma 3.1 *Suppose S is a naive-2-subanalytic subset of $\mathbf{R}^s$. Then for any $\epsilon > 0$ there is a $c = c(S, \epsilon)$ with the following property. For each positive integer n there are at most cn^{ϵ} rational points of S^{trans} in $\frac{1}{n}\mathbf{Z}^s$.*

Proof See Lemma 2.1 of [17].

4 Functions

In the algebraic case we will construct our naive-2-subanalytic subset S by means of the following functions. Let

$$F(t) = F\left(\frac{1}{2}, \frac{1}{2}, 1; t\right) = \sum_{m=0}^{\infty} \frac{(2m)!^2}{2^{4m} m!^4} t^m$$

be a hypergeometric function. With λ in $\mathbf{C}(C)$ as in the Proposition, we write

$$f = \pi F(\lambda), \quad g = \pi i F(1 - \lambda). \tag{4.1}$$

As in [17] we use the open set Λ defined in $\mathbf{C}$ by

$$|t| < 1, \ |1 - t| < 1. \tag{4.2}$$

Then f and g are well-defined at all $\mathbf{c}$ in $\lambda^{-1}(\Lambda)$ in $C(\mathbf{C})$. They are analytic in $\lambda = \lambda(\mathbf{c})$. It is well-known that they are basis elements of a period lattice of E_λ with

respect to $\frac{dX}{2Y}$ (see for example [8, p. 179]). In particular, if we write $\exp_t$ for the associated exponential function from $\mathbf{C}$ to $E_t(\mathbf{C})$, we have

$$\exp_\lambda(f) = \exp_\lambda(g) = O \tag{4.3}$$

for the origin O of E_λ.

Next let $P = (\xi, \eta)$, $Q = (\mu, \nu)$ be as in the Proposition with ξ, η, μ, ν in $\mathbf{C}(C)$. We note that $\xi \neq 0, 1, \lambda$ identically, otherwise $2P = O$ contradicting (2.1). Similarly $\mu \neq 0, 1, \lambda$ identically. We would like to define

$$z = \int_P^O \frac{dX}{2Y}, \quad w = \int_Q^O \frac{dX}{2Y} \tag{4.4}$$

as elliptic logarithms of P, Q which are analytic in a suitable sense. This is now possible everywhere locally apart from finitely many exceptional points.

In what follows we write $\hat{C}$ for the set of points $\mathbf{c}$ of $C(\mathbf{C})$ with $\lambda(\mathbf{c}), \xi(\mathbf{c}), \mu(\mathbf{c}) \neq 0, 1, \infty$ and $\lambda(\mathbf{c}) \neq \xi(\mathbf{c}), \lambda(\mathbf{c}) \neq \mu(\mathbf{c})$.

Fix $\mathbf{c}_*$ in $\hat{C}$. Choose a path in the X-plane from $\xi(\mathbf{c}_*)$ to ∞ not passing through $0, 1, \lambda(\mathbf{c}_*)$. Via the fixed determination of $Y = \sqrt{X(X-1)(X-\lambda(\mathbf{c}_*))}$ equal to $\eta(\mathbf{c}_*)$ at $X = \xi(\mathbf{c}_*)$ this path extends to a path on $E_{\lambda(\mathbf{c}_*)}$ from $P(\mathbf{c}_*)$ to O ready for integration as in (4.4), so the integral

$$z(\mathbf{c}_*) = \int_{\xi(\mathbf{c}_*)}^{\infty} \frac{dX}{2\sqrt{X(X-1)(X-\lambda(\mathbf{c}_*))}}$$

makes sense. This can be extended to $\mathbf{c}$ near $\mathbf{c}_*$ by writing

$$\int_{\xi(\mathbf{c})}^{\infty} = \int_{\xi(\mathbf{c}_*)}^{\infty} + \int_{\xi(\mathbf{c})}^{\xi(\mathbf{c}_*)}$$

and integrating $\frac{dX}{2\sqrt{X(X-1)(X-\lambda(\mathbf{c}))}}$. In the first term on the right the path is fixed and the integrand is determined by continuity from Y above; it is a power series in $\lambda(\mathbf{c}) - \lambda(\mathbf{c}_*)$ with coefficients algebraic over $\mathbf{C}(X)$. So this term ends up as a function analytic in $\lambda(\mathbf{c})$ like f and g above.

In the second term we take for example any local path; and it is now more suitable to expand the integrand as a double power series in $\lambda(\mathbf{c}) - \lambda(\mathbf{c}_*)$ and $X - \xi(\mathbf{c}_*)$ with coefficients in $\mathbf{C}$. So this time we end up with a double power series in $\lambda(\mathbf{c}) - \lambda(\mathbf{c}_*)$ and $\xi(\mathbf{c}) - \xi(\mathbf{c}_*)$.

Similarly for w we get a double power series in $\lambda(\mathbf{c}) - \lambda(\mathbf{c}_*)$ and $\mu(\mathbf{c}) - \mu(\mathbf{c}_*)$.

At any rate we have

$$\exp_\lambda(z) = P, \quad \exp_\lambda(w) = Q \tag{4.5}$$

(in (3.9) of [17] we expressed this in terms of Weierstrass functions).

5 Algebraic independence

Thus, fixing any point $\mathbf{c}_*$ of $\lambda^{-1}(\Lambda)$ also in $\hat{C}$, we see that f, g, z, w are well-defined on a small neighbourhood N_* of $\mathbf{c}_*$. In order to prove $S^{\text{trans}} = S$ we will need the following result.

Lemma 5.1 *The functions z, w are algebraically independent over $\mathbf{C}(f, g)$ on N_*.*

Proof This is an immediate consequence of Théorème 5 of [1, p. 136] with $r = 2$; one can choose the parameter $x = \lambda$ there (recall that λ is not constant) as long as $\xi(\mathbf{c})$ and $\mu(\mathbf{c})$ are analytic in $\lambda(\mathbf{c})$, which will certainly be the case on a non-empty open subset of N_*. And one can simply ignore the first derivatives in the statement of this theorem.

6 A naive-2-subanalytic set

We describe here our naive-2-subanalytic subset S. First we construct local functions from C to $\mathbf{R}^4$. Recall that $\hat{C}$ is obtained from $C(\mathbf{C})$ by the removal of a finite set of points. Fix $\mathbf{c}_*$ in $\lambda^{-1}(\Lambda)$, choose $\mathbf{c}$ in $\hat{C}$ and then a path from $\mathbf{c}_*$ to $\mathbf{c}$ lying in $\hat{C}$. We can easily continue f, g along the path using (4.1).

The continuation of the functions z, w is a bit more troublesome. It is convenient to remove a few more points from $\hat{C}$; these are the singular points together with the points at which the differential of λ vanishes. Let C_0 be the finite subset which we have removed so far, and write $\widehat{C}$ for what remains. We can now speak of functions analytic on $\widehat{C}$.

To continue z from $\mathbf{c}_*$ to $\mathbf{c}$ in $\widehat{C}$ it suffices to verify that if N_1, N_2 are small open subsets in $\widehat{C}$, with $N_1 \cap N_2$ connected, such that z has an analytic definition z_1 on N_1 and an analytic definition z_2 on N_2, then it has an analytic definition on $N_1 \cup N_2$. But from (4.5) we deduce $\exp_\lambda(z_1) = \exp_\lambda(z_2)$ on $N_1 \cap N_2$. Thus there are rational integers x, y with $z_2 = xf + yg + z_1$ on this intersection, and they must be constant there. So all we have to do is for example to change z_2 to $z_2 - (xf + yg)$ on N_2. Similarly for w. Using the same path it is easy to see that we can continue the function (f, g, z, w) from a small neighbourhood of $\mathbf{c}_*$ to a small neighbourhood $N_\mathbf{c}$ of $\mathbf{c}$ in $\widehat{C}$. The end result is a function $(f_\mathbf{c}, g_\mathbf{c}, z_\mathbf{c}, w_\mathbf{c})$ analytic on $N_\mathbf{c}$. Write Ω_t for the period lattice of the curve E_t with respect to $\frac{\mathrm{d}X}{2Y}$.

Lemma 6.1 *The functions $z_\mathbf{c}, w_\mathbf{c}$ are algebraically independent over $\mathbf{C}(f_\mathbf{c}, g_\mathbf{c})$ on $N_\mathbf{c}$. Further we have $\Omega_\lambda = \mathbf{Z} f_\mathbf{c} + \mathbf{Z} g_\mathbf{c}$ on $N_\mathbf{c}$.*

Proof We could continue an algebraic dependence relation backwards to get the same relation between f, g, z, w on a neighbourhood of $\mathbf{c}_*$; however this would contradict Lemma 5.1. The assertion about Ω_λ follows from the analogous assertion in Lemma 4.1 of [17].

Introducing now complex conjugate functions, we deduce that the function

$$\Delta_\mathbf{c} \;=\; f_\mathbf{c}\overline{g_\mathbf{c}} - \overline{f_\mathbf{c}} g_\mathbf{c} \;=\; 2ig_\mathbf{c}\overline{g_\mathbf{c}}\,\Im\left(\frac{f_\mathbf{c}}{g_\mathbf{c}}\right) \tag{6.1}$$

is non-zero on $N_{\mathbf{c}}$. We can therefore define $x_{\mathbf{c}}, y_{\mathbf{c}}, u_{\mathbf{c}}, v_{\mathbf{c}}$ on $N_{\mathbf{c}}$ by

$$x_{\mathbf{c}} = \frac{z_{\mathbf{c}}\overline{g_{\mathbf{c}}} - \overline{z_{\mathbf{c}}}g_{\mathbf{c}}}{\Delta_{\mathbf{c}}}, \quad y_{\mathbf{c}} = -\frac{z_{\mathbf{c}}\overline{f_{\mathbf{c}}} - \overline{z_{\mathbf{c}}}f_{\mathbf{c}}}{\Delta_{\mathbf{c}}},$$
$$u_{\mathbf{c}} = \frac{w_{\mathbf{c}}\overline{g_{\mathbf{c}}} - \overline{w_{\mathbf{c}}}g_{\mathbf{c}}}{\Delta_{\mathbf{c}}}, \quad v_{\mathbf{c}} = -\frac{w_{\mathbf{c}}\overline{f_{\mathbf{c}}} - \overline{w_{\mathbf{c}}}f_{\mathbf{c}}}{\Delta_{\mathbf{c}}}.$$

We check that these are real-valued with

$$z_{\mathbf{c}} = x_{\mathbf{c}}f_{\mathbf{c}} + y_{\mathbf{c}}g_{\mathbf{c}}, \quad w_{\mathbf{c}} = u_{\mathbf{c}}f_{\mathbf{c}} + v_{\mathbf{c}}g_{\mathbf{c}}. \tag{6.2}$$

Now we can define S. For small $\delta > 0$ (later to be specified) we define Λ_δ as the set of complex t satisfying $|t| \leq \frac{1}{\delta}$ and

$$|t - \lambda(\mathbf{c})| \;\geq\; \delta \tag{6.3}$$

for all $\mathbf{c}$ in C_0 with $\lambda(\mathbf{c}) \neq \infty$.

Fix t in Λ_δ; there are then only finitely many $\mathbf{c}$ in C with $\lambda(\mathbf{c}) = t$, and these all lie in $\widehat{C}$. Fix one of these $\mathbf{c}$. Then there is a small neighbourhood $N_{\mathbf{c}}$ of $\mathbf{c}$ such that λ gives an analytic isomorphism from $N_{\mathbf{c}}$ to $\lambda(N_{\mathbf{c}})$. Write λ^{-1} for the local inverse on $\lambda(N_{\mathbf{c}})$. Choose a closed disc $D_{\mathbf{c}}$ inside $\lambda(N_{\mathbf{c}})$ centred at t, and define

$$\theta_{\mathbf{c}} \;=\; (x_{\mathbf{c}}, y_{\mathbf{c}}, u_{\mathbf{c}}, v_{\mathbf{c}}) \circ \lambda^{-1}$$

from $D_{\mathbf{c}}$ to $\mathbf{R}^4$. By compactness there is a finite set Π of $\mathbf{c}$ such that the $D_{\mathbf{c}}$ cover Λ_δ. Then our naive-2-subanalytic subset $S = S_\delta$ in $\mathbf{R}^4$ is defined as the union of $\theta_{\mathbf{c}}(D_{\mathbf{c}})$ over Π.

Lemma 6.2 *We have* $S^{\text{trans}} = S$.

Proof Because every semialgebraic surface contains semialgebraic curves, it will suffice to deduce a contradiction from the existence of a semialgebraic curve B_s lying in S. Now B_s is Zariski-dense in its Zariski-closure B, a real algebraic curve. Thus we could find a subset $\hat{B}$ of B, also Zariski-dense in B, contained in some $\theta_{\mathbf{c}}(D_{\mathbf{c}})$. It will suffice to know that $\hat{B}$ is infinite. Then $\hat{B} = \theta_{\mathbf{c}}(E)$ for some infinite subset E of $D_{\mathbf{c}}$.

Now (6.2) shows that $z_{\mathbf{c}}, w_{\mathbf{c}}$ lie in $\Phi = \mathbf{C}(x_{\mathbf{c}}, y_{\mathbf{c}}, u_{\mathbf{c}}, v_{\mathbf{c}}, f_{\mathbf{c}}, g_{\mathbf{c}})$. But if we restrict to $\lambda^{-1}(E)$, then Φ has transcendence degree at most 1 over $\mathbf{C}(f_{\mathbf{c}}, g_{\mathbf{c}})$. It follows that $z_{\mathbf{c}}, w_{\mathbf{c}}$ are algebraically dependent over $\mathbf{C}(f_{\mathbf{c}}, g_{\mathbf{c}})$ on $\lambda^{-1}(E)$. More precisely, with independent variables T_f, T_g, T_z, T_w, there exists a polynomial A in $\mathbf{C}[T_f, T_g, T_z, T_w]$ such that the relation $A(f_{\mathbf{c}}, g_{\mathbf{c}}, z_{\mathbf{c}}, w_{\mathbf{c}}) = 0$ holds on $\lambda^{-1}(E)$ and $A(f_{\mathbf{c}}, g_{\mathbf{c}}, T_z, T_w)$ is not identically zero in $\mathbf{C}(f_{\mathbf{c}}, g_{\mathbf{c}})[T_z, T_w]$. By a standard principle for analytic functions ("Identity Theorem" or [10, p. 85]) this relation persists on all of $N_{\mathbf{c}}$. And now this contradicts Lemma 6.1. Thus the present lemma is proved.

We are all set up for an efficient application of Lemma 3.1. It will turn out that every $\mathbf{c}$ in our Proposition leads to many rational points on S, and of course we have to estimate their denominator. This we do in the next short section.

7 Orders of torsion

We use the standard absolute Weil height

$$h(\alpha) \;=\; \frac{1}{[\mathbf{Q}(\alpha):\mathbf{Q}]}\sum_{v}\log\max\{1,|\alpha|_v\}$$

of an algebraic number α, where v runs over a suitably normalized set of valuations; and also the standard extension to vectors. See for example [25, p. 208].

Lemma 7.1 *There is a constant $c = c(E, P, Q)$ with the following property. Suppose for some $\mathbf{c}$ in $\hat{C}$ that the point $P(\mathbf{c})$ or the point $Q(\mathbf{c})$ has finite order n. Then $\alpha = \lambda(\mathbf{c})$ is algebraic, and*

$$n \;\le\; c[\mathbf{Q}(\alpha):\mathbf{Q}]^2(1+h(\alpha)).$$

Proof Suppose $P(\mathbf{c})$ has order n. As C is defined over $\overline{\mathbf{Q}}$, it is clear that $\alpha = \lambda(\mathbf{c})$ is algebraic, otherwise $q = n, p = 0$ would contradict (2.1). Then the points $P(\mathbf{c}), \ldots, nP(\mathbf{c})$ are distinct with zero Néron-Tate heights. We use Théorème 1.2(i) of [7, p. 106] with any archimedean v, noting that by his definition $h_v(E) \ge \frac{\sqrt{3}}{2}$. We get $n \le c_1(d^*h + d^*\log d^*)$ with $d^* = [\mathbf{Q}(\xi(\mathbf{c}), \eta(\mathbf{c})) : \mathbf{Q}]$ and $h = \max\{1, h(j)\}$ for the modular invariant $j = j(E)$, with c_1 absolute. Clearly $d^* \le c_2[\mathbf{Q}(\alpha) : \mathbf{Q}]$ with c_2 independent of $\mathbf{c}$. As $j = 256\frac{(\alpha^2-\alpha+1)^3}{\alpha^2(1-\alpha)^2}$ (see for example [8, p. 83] or [25, p. 54]) the result for $P(\mathbf{c})$ follows at once, with a similar argument for $Q(\mathbf{c})$.

8 Heights

In view of the following result we can eliminate the height dependence in Lemma 7.1.

Lemma 8.1 *There is a constant $c = c(E, P, Q)$ with the following property. Suppose for some $\mathbf{c}$ in $\hat{C}$ that the point $P(\mathbf{c})$ or the point $Q(\mathbf{c})$ has finite order. Then $h(\alpha) \le c$ for $\alpha = \lambda(\mathbf{c})$.*

Proof This is a consequence of Silverman's Specialization Theorem [24, p. 197], because we have seen that neither P nor Q is identically of finite order. In fact the direct proof of the corresponding Lemma 6.1 in [17] can be generalized to the present situation.

Another advantage of bounded height is the following easy remark concerning the sets C_0 and Λ_δ in Sect. 6. Write B for the set of points $\lambda(\mathbf{c})$ in (6.3). As C is defined over $\overline{\mathbf{Q}}$, these points are algebraic.

Lemma 8.2 *Given a number field K containing B in $\mathbf{C}$ and a constant a, there is a positive constant $\delta = \delta(K, a, C)$ depending only on K, a and C with the following property. Suppose α is algebraic not in B with $h(\alpha) \le a$. Then there are at least $\frac{1}{2}[K(\alpha) : K]$ different K-embeddings σ of $K(\alpha)$ in $\mathbf{C}$ such that $\sigma(\alpha)$ lies in Λ_δ.*

Proof Suppose that there are $l-1$ inequalities (6.3) defining Λ_δ. A typical one is $|t-\beta| \geq \delta$ with β in B. Let Σ be the set of K-embeddings σ of $K(\alpha)$ in $\mathbf{C}$ and let k be the number of these such that $t = \sigma(\alpha)$ fails to satisfy this inequality. Now the height $h(\alpha-\beta) \leq a + h(\beta) + \log 2$ and this height is also

$$\frac{1}{d^*}\sum_v \log\max\left\{1, \left|\frac{1}{\alpha-\beta}\right|_v\right\} \geq \frac{1}{d^*}\sum_{\sigma\in\Sigma}\log\max\left\{1, \left|\frac{1}{\sigma(\alpha)-\beta}\right|\right\}$$
$$> \frac{k}{d^*}\log\left(\frac{1}{\delta}\right),$$

where $d^* = [K(\alpha):\mathbf{Q}]$. Choosing δ small enough in terms of K, a, τ we find that

$$k \leq \frac{d^*}{2l[K:\mathbf{Q}]} = \frac{1}{2l}[K(\alpha):K].$$

With suitable δ the same inequality holds regarding the remaining inequality $|t| \leq \frac{1}{\delta}$ defining Λ_δ, and the result follows.

9 Proof of Proposition in the algebraic case

We will need an asymmetric version of the rudimentary zero estimate of [17].

Lemma 9.1 *Suppose $f_0, f_1, \ldots, f_s$ are analytic in an open neighbourhood N of a compact set $\mathcal{K}$ in $\mathbf{C}$ and f_0 is linearly independent of $f_1, \ldots, f_s$ over $\mathbf{C}$. Then there is $c = c(f_0, f_1, \ldots, f_s)$ with the following property. For any complex numbers $a_1, \ldots, a_s$ the function $F = f_0 + a_1 f_1 + \cdots + a_s f_s$ has at most c different zeroes on $\mathcal{K}$.*

Proof Of course $f_0 \neq 0$. So if $f_1 = \cdots = f_s = 0$ the result is clear. Otherwise, by replacing $f_1, \ldots, f_s$ by a maximal linearly independent subset, we can assume that they are themselves independent; and now the result follows from Lemma 7.1 of [17] with $s+1$ functions.

To prove our Proposition we fix any positive $\epsilon < \frac{1}{4}$. We use $c, c_1, c_2, \ldots,$ for positive constants depending only on E, P, Q. We have to show that there are at most finitely many $\mathbf{c}$ such that $P(\mathbf{c})$ and $Q(\mathbf{c})$ both have finite order on E. By Lemma 7.1 each such value $\alpha = \lambda(\mathbf{c})$ is algebraic, say of degree $d = [\mathbf{Q}(\alpha):\mathbf{Q}]$, and thanks to Lemma 8.1 and the Northcott property it will suffice to prove that $d \leq c$. We will actually argue with a single value of α, which we can take outside the set B of Sect. 8.

Next, Lemma 7.1 together with Lemma 8.1 shows (by multiplying together the two orders) that there is a positive integer

$$n \leq c_1 d^4 \tag{9.1}$$

such that

$$nP(\mathbf{c}) = nQ(\mathbf{c}) = 0. \tag{9.2}$$

Fix a number field K containing B and a field of definition for the curve C such that E is defined over $K(C)$ and λ lies in $K(C)$. By Lemma 8.1 and Lemma 8.2 the algebraic number α has at least $\frac{1}{2}[K(\alpha) : K]$ conjugates over K in some Λ_δ; here $\delta = c_2$. Now Λ_δ is the union of at most c_3 closed discs $D_{\mathbf{c}}$, and so there is $\mathbf{c}$ such that $D_{\mathbf{c}}$ contains at least $\frac{1}{2c_3}[K(\alpha) : K] \geq \frac{1}{c_4}d$ conjugates $t = \sigma(\alpha)$. For each such t there is $\mathbf{c}_\sigma$ in $N_{\mathbf{c}}$ with $t = \lambda(\mathbf{c}_\sigma)$. And the corresponding conjugate points $P_\sigma(\mathbf{c})$, $Q_\sigma(\mathbf{c})$ also satisfy $nP_\sigma(\mathbf{c}) = nQ_\sigma(\mathbf{c}) = 0$.

We claim that each point $\Theta = \theta_{\mathbf{c}}(t)$ lies in $\mathbf{Q}^4$ and even that $n\Theta$ lies in $\mathbf{Z}^4$.

Now the function $\theta_{\mathbf{c}}$ arises from continuations $f_{\mathbf{c}}, g_{\mathbf{c}}, z_{\mathbf{c}}, w_{\mathbf{c}}$ of the functions in Sect. 6 evaluated at $\mathbf{c}_\sigma$. We deduce from (4.5) that

$$\exp_\lambda(z_{\mathbf{c}}) = P(\mathbf{c}), \quad \exp_\lambda(w_{\mathbf{c}}) = Q(\mathbf{c}) \tag{9.3}$$

on $N_{\mathbf{c}}$. At $\mathbf{c}_\sigma$ this implies

$$\exp_t(nz_{\mathbf{c}}(\mathbf{c}_\sigma)) = \exp_t(nw_{\mathbf{c}}(\mathbf{c}_\sigma)) = O. \tag{9.4}$$

It follows that $nz_{\mathbf{c}}(\mathbf{c}_\sigma), nw_{\mathbf{c}}(\mathbf{c}_\sigma)$ lie in the period lattice Ω_t, which by Lemma 6.1 is just $\mathbf{Z}f_{\mathbf{c}}(\mathbf{c}_\sigma) + \mathbf{Z}g_{\mathbf{c}}(\mathbf{c}_\sigma)$. Thus (6.2) shows that

$$nx_{\mathbf{c}}(\mathbf{c}_\sigma),\ ny_{\mathbf{c}}(\mathbf{c}_\sigma),\ nu_{\mathbf{c}}(\mathbf{c}_\sigma),\ nv_{\mathbf{c}}(\mathbf{c}_\sigma)$$

lie in $\mathbf{Z}$. Thus indeed $n\Theta$ lies in $\mathbf{Z}^4$ as claimed.

So now each $\theta_{\mathbf{c}}(t)$ in the set S of Sect. 6 has common denominator dividing n. By Lemma 3.1 and Lemma 6.2, the number of such values $\theta_{\mathbf{c}}(t)$ is at most $c_5 n^\epsilon$. By (9.1) this is at most $c_6 d^{4\epsilon}$. Let $\Theta = (x, y, u, v)$ be one of these values. For any $t = \lambda(\mathbf{c}_\sigma)$ with $\theta_{\mathbf{c}}(t) = \Theta$ we have

$$z_{\mathbf{c}}(\mathbf{c}_\sigma) \ = \ x_{\mathbf{c}}(\mathbf{c}_\sigma) f_{\mathbf{c}}(\mathbf{c}_\sigma) + y_{\mathbf{c}}(\mathbf{c}_\sigma) g_{\mathbf{c}}(\mathbf{c}_\sigma) \ = \ x f_{\mathbf{c}}(\mathbf{c}_\sigma) + y g_{\mathbf{c}}(\mathbf{c}_\sigma).$$

Lemma 6.1 implies that $z_{\mathbf{c}}$ is linearly independent of $f_{\mathbf{c}}$ and $g_{\mathbf{c}}$. So Lemma 9.1 shows that the number of $\mathbf{c}_\sigma$ for each Θ is at most c_7.

Thus the total number of $\mathbf{c}_\sigma$ is at most $c_8 d^{4\epsilon}$. Now this contradicts the lower bound $\frac{1}{c_4}d$ noted just after (9.2), provided d is sufficiently large. As observed near the beginning of this section, that suffices to prove our Proposition in the algebraic case.

10 Galois groups

The following observation is crucial for the proof of the Proposition in the transcendental case.

Lemma 10.1 *Let j be a complex number transcendental over $\mathbf{Q}$, and let $\check{E}$ be a Weierstrass elliptic curve defined over $\mathbf{Q}(j)$ with invariant j. Then for any integer $n > 1$ the field generated over $\mathbf{Q}(j)$ by the coordinates of all points on $\check{E}$ of order dividing n is a Galois extension of $\mathbf{Q}(j)$ whose group is isomorphic to $GL_2(\mathbf{Z}/n\mathbf{Z})$. If $\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ is the period lattice with respect to the standard exponential map* exp,

then γ *in* $GL_2(\mathbf{Z}/n\mathbf{Z})$ *sends* $\exp\left(\frac{m_1\omega_1+m_2\omega_2}{n}\right)$ *to* $\exp\left(\frac{m_1^\gamma\omega_1+m_2^\gamma\omega_2}{n}\right)$ *where* $\gamma\begin{pmatrix}m_1\\m_2\end{pmatrix}=\begin{pmatrix}m_1^\gamma\\m_2^\gamma\end{pmatrix}$. *In particular for any divisor* $r>1$ *of* n *the group* $GL_2(\mathbf{Z}/n\mathbf{Z})$ *acts transitively on points of order exactly* r, *and any such point has exactly* $\phi_2(r)=r^2\prod_{p|r}(1-p^{-2})$ *different conjugates.*

Proof This is all classical; see for example Corollary 1 of [9, p. 68] for the Galois group and its action, where however the words "order N" must be replaced throughout by "order dividing N". The transitivity on points of order exactly n is clear from $\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}a\\c\end{pmatrix}$ because the highest common factor $\mathrm{hcf}\{a,c,n\}=1$. Taking $\begin{pmatrix}a\\c\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$ shows that the stabilizer has order $n\phi_1(n)$ with Euler's ϕ_1; however $GL_2(\mathbf{Z}/n\mathbf{Z})$ has order $n\phi_1(n)\phi_2(n)$, and so a point of exact order n indeed has $\phi_2(n)$ conjugates. The corresponding statements for the divisor r follow at once from the surjectivity of the natural homomorphism from $GL_2(\mathbf{Z}/n\mathbf{Z})$ to $GL_2(\mathbf{Z}/r\mathbf{Z})$ (this latter may be seen for example by using the Chinese Remainder Theorem to reduce to the prime-power case). This proves the lemma.

11 Relations

The following is the first of a sequence of three results about the elliptic curve $\check{E}_j$ defined by

$$\check{Y}^2 \;=\; 4\check{X}^3-\frac{27j}{j-1728}\check{X}-\frac{27j}{j-1728}$$

for a complex number j transcendental over $\mathbf{Q}$. The first two results are in the present section and the third, whose proof uses slightly different techniques, is in the next section.

Lemma 11.1 *Suppose* $\check{P}=(\check{\xi},\check{\eta})$, $\check{Q}=(\check{\mu},\check{\nu})$ *are points of orders* n_P, n_Q *respectively on* $\check{E}_j$ *satisfying a relation*

$$\check{F}(\check{\xi},\check{\mu})=0 \tag{11.1}$$

with non-zero $\check{F}$ *of degree at most* $\check{D}$ *with coefficients in* $\mathbf{Q}(j)$. *Then either*

$$\max\{n_P,n_Q\} \;\le\; (2\check{D})^2n' \tag{11.2}$$

for $n'=\mathrm{hcf}\{n_P,n_Q\}$; *or there are integers* p,q, *not both zero, such that*

$$q\check{P}=p\check{Q} \tag{11.3}$$

and

$$\max\{|p|, |q|\} < (2\check{D})^8. \tag{11.4}$$

Proof We really want to prove just the single alternative (11.3), (11.4). But for the moment we have to put up with (11.2) as well, which says that n_P, n_Q have essentially the same prime factorization.

We first dispose of the possibility that $\check{F}$ in (11.1) does not involve one of $\check{\xi}, \check{\mu}$. Say it does not involve $\check{\mu}$. Then $\check{\xi}$ is algebraic of degree at most $\check{D}$ over $\mathbf{Q}(j)$. So $\check{P} = (\check{\xi}, \check{\eta})$ is algebraic of degree at most $2\check{D}$ over $\mathbf{Q}(j)$. However Lemma 10.1 says that the degree is exactly $\phi_2(n_P)$. We conclude

$$\frac{6}{\pi^2} n_P^2 \;=\; n_P^2 \prod_p (1 - p^{-2}) \;<\; \phi_2(n_P) \;\leq\; 2\check{D}.$$

Now $n_P P = 0Q$ is the required (11.3), and (11.4) is certainly satisfied.

We can use the same argument if $\check{F}(\check{\xi}, T)$ is identically zero in T.

Similarly if $\check{F}$ does not involve $\check{\xi}$ or $\check{F}(T, \check{\mu})$ is identically zero in T, using the order n_Q of Q.

So henceforth we may assume that $\check{F}$ involves both $\check{\xi}, \check{\mu}$ and $\check{F}(\check{\xi}, T)$, $\check{F}(T, \check{\mu})$ are not identically zero. We now prove (11.2).

To this end we introduce a period lattice and write

$$\check{P} = \exp\left(\frac{p_1\omega_1 + p_2\omega_2}{n_P}\right), \quad \check{Q} = \exp\left(\frac{q_1\omega_1 + q_2\omega_2}{n_Q}\right)$$

with $\mathrm{hcf}\{p_1, p_2, n_P\} = \mathrm{hcf}\{q_1, q_2, n_Q\} = 1$ and we use $GL_2(\mathbf{Z}/n\mathbf{Z})$ for $n = n_P n_Q$. By Lemma 10.1 with $r = n_Q$ there is α in this group with $\alpha \begin{pmatrix} n_Q \\ 0 \end{pmatrix} = \begin{pmatrix} n_Q p_1 \\ n_Q p_2 \end{pmatrix}$. We consider the Galois element σ corresponding to $\alpha \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \alpha^{-1}$. Since $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} n_Q \\ 0 \end{pmatrix} = \begin{pmatrix} n_Q \\ 0 \end{pmatrix}$ it fixes $\check{P}$ and therefore also $\check{\xi}$. Thus by (11.1) we get $\check{F}(\check{\xi}, \check{\mu}^\sigma) = 0$. As $\check{F}(\check{\xi}, T)$ is not identically zero there are at most $\check{D}$ possibilities for $\check{\mu}^\sigma$ as σ varies. So at most $2\check{D}$ possibilities for $\check{Q}^\sigma = (\check{\mu}^\sigma, \check{\nu}^\sigma)$ as σ varies.

On the other hand the action on $\check{Q}$ is given by $\alpha \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$ for $\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \alpha^{-1} \begin{pmatrix} n_P q_1 \\ n_P q_2 \end{pmatrix}$, and so there are at most $2\check{D}$ possibilities for $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$ as σ varies. Thus taking $b = 0, 1, \ldots, 2\check{D}$ we get a positive integer $b_0 \leq 2\check{D}$ with $b_0 s_2 = 0$ in $\mathbf{Z}/n\mathbf{Z}$. Writing $\alpha^{-1} = \begin{pmatrix} k_1 & k_2 \\ l_1 & l_2 \end{pmatrix}$ we get $b_0 n_P (l_1 q_1 + l_2 q_2) = 0$ in $\mathbf{Z}/n\mathbf{Z}$. Thus

$$n_Q \mid b_0(l_1 q_1 + l_2 q_2). \tag{11.5}$$

Next consider the σ corresponding to $\alpha \begin{pmatrix} 1 & 0 \\ c^* n_P & 1 \end{pmatrix} \alpha^{-1}$. Since $\begin{pmatrix} 1 & 0 \\ c^* n_P & 1 \end{pmatrix} \begin{pmatrix} n_Q \\ 0 \end{pmatrix} = \begin{pmatrix} n_Q \\ 0 \end{pmatrix}$ this also fixes $\check{P}$. So the same arguments give a positive integer $c_0^* \leq 2\check{D}$, now with $c_0^* n_P s_1 = 0$ in $\mathbf{Z}/n\mathbf{Z}$. Thus $n_Q | c_0^* n_P (k_1 q_1 + k_2 q_2)$. With (11.5) this implies that $b_0 c_0^* n_P \begin{pmatrix} k_1 & k_2 \\ l_1 & l_2 \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = 0$ in $GL_2(\mathbf{Z}/n_Q\mathbf{Z})$. But as $\mathrm{hcf}\{q_1, q_2, n_Q\} = 1$ and $\begin{pmatrix} k_1 & k_2 \\ l_1 & l_2 \end{pmatrix}$ is in $GL_2(\mathbf{Z}/n_Q\mathbf{Z})$ this means that $n_Q | d_0 n_P$ for $d_0 = b_0 c_0^* \leq (2\check{D})^2$. Thus the lowest common multiple $\frac{n_P n_Q}{n'}$ of n_P and n_Q divides $d_0 n_P$, and so

$$n_Q \leq d_0 n' \leq (2\check{D})^2 n'. \tag{11.6}$$

We now repeat the whole Galois argument fixing $\check{Q}$ instead of $\check{P}$. We find that

$$n_P \leq (2\check{D})^2 n'; \tag{11.7}$$

and the combination of this with (11.6) gives (11.2).

Lemma 11.2 *Suppose $\check{P} = (\check{\xi}, \check{\eta})$, $\check{Q} = (\check{\mu}, \check{\nu})$ are points of orders n_P, n_Q respectively on $\check{E}_j$ satisfying a relation*

$$\check{F}(\check{\xi}, \check{\mu}) = 0$$

with non-zero $\check{F}$ of degree at most $\check{D}$ with coefficients in $\mathbf{Q}(j)$. Then either there are integers p', q' such that

$$q'\check{P} = p'\check{Q} \tag{11.8}$$

for some integer q' with

$$1 \leq q' \leq (2\check{D})^7; \tag{11.9}$$

or there are integers p, q, not both zero, such that

$$q\check{P} = p\check{Q}$$

and

$$\max\{|p|, |q|\} < (2\check{D})^8.$$

Proof Again we get (11.3), (11.4) but this time with the alternative (11.8), (11.9), which says that $\check{P}$ essentially lies in the group generated by $\check{Q}$. So we can assume

that (11.2) holds. With n' as in the previous lemma we note that the points $\check{P}' = \frac{n_P}{n'}\check{P}$, $\check{Q}' = \frac{n_Q}{n'}\check{Q}$ with

$$\check{P}' = \exp\left(\frac{p_1\omega_1 + p_2\omega_2}{n'}\right), \quad \check{Q}' = \exp\left(\frac{q_1\omega_1 + q_2\omega_2}{n'}\right)$$

have orders exactly n'. This enables us to repeat the argument of the previous lemma now using $GL_2(\mathbf{Z}/n'\mathbf{Z})$. By Lemma 10.1 with $r = n'$ there is α in this group with $\alpha\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}p_1\\p_2\end{pmatrix}$. We consider the Galois element σ corresponding to $\alpha\begin{pmatrix}1 & b\\0 & 1\end{pmatrix}\alpha^{-1}$. Since $\begin{pmatrix}1 & b\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$ it fixes $\check{P}'$. Now we have no handy analogue of (11.1) for $\check{P}'$, $\check{Q}'$, so we re-use (11.1) itself by arguing as follows. By (11.7) and $\check{P}' = \frac{n_P}{n'}\check{P}$ we get at most $(\frac{n_P}{n'})^2 \le (2\check{D})^4$ possibilities for $\check{P}^\sigma$ as σ varies, and therefore also for $\check{\xi}^\sigma$. Now by (11.1) we get $\check{F}(\check{\xi}^\sigma, \check{\mu}^\sigma) = 0$. As before we can assume that $\check{F}(\check{\xi}^\sigma, T)$ is not identically zero, and so there are at most $\check{D}(2\check{D})^4$ possibilities for $\check{\mu}^\sigma$. So at most $(2\check{D})^5$ possibilities for $\check{Q}^\sigma = (\check{\mu}^\sigma, \check{\nu}^\sigma)$. And finally at most $(2\check{D})^5$ possibilities for $\check{Q}'^\sigma = \frac{n_Q}{n'}\check{Q}^\sigma$.

On the other hand the action on $\check{Q}'$ is now given by $\alpha\begin{pmatrix}1 & b\\0 & 1\end{pmatrix}\begin{pmatrix}s_1\\s_2\end{pmatrix}$ for $\begin{pmatrix}s_1\\s_2\end{pmatrix} = \alpha^{-1}\begin{pmatrix}q_1\\q_2\end{pmatrix}$, and so there are at most $(2\check{D})^5$ possibilities for $\begin{pmatrix}1 & b\\0 & 1\end{pmatrix}\begin{pmatrix}s_1\\s_2\end{pmatrix}$. Thus taking $0 \le b \le (2\check{D})^5$ we get a positive integer $b_0 \le (2\check{D})^5$ with $b_0 s_2 = 0$ in $\mathbf{Z}/n'\mathbf{Z}$. Writing $\alpha^{-1} = \begin{pmatrix}k_1 & k_2\\l_1 & l_2\end{pmatrix}$ we get $b_0(l_1q_1 + l_2q_2) = 0$ in $\mathbf{Z}/n'\mathbf{Z}$. Thus

$$n' \mid b_0(l_1q_1 + l_2q_2). \tag{11.10}$$

Now the definition of α implies $n' | l_1p_1 + l_2p_2$. Eliminating l_1, l_2 between this and (11.10) using $\mathrm{hcf}\{l_1, l_2, n'\} = 1$ gives $n' | b_0(p_1q_2 - p_2q_1)$. Thus

$$b_0q_1\check{P}' = b_0p_1\check{Q}', \quad b_0q_2\check{P}' = b_0p_2\check{Q}'.$$

As also $\mathrm{hcf}\{q_1, q_2, n'\} = 1$ this gives $b_0\check{P}' = b_0h\check{Q}'$ with some integer h. This in turn gives (11.8), and certainly

$$1 \le q' = b_0\frac{n_P}{n'} \le (2\check{D})^7$$

is bounded as in (11.9). This proves the present lemma.

However $|p'| = b_0|h|\frac{n_Q}{n'}$ in (11.8) is probably not bounded and so we have not yet reached (11.4).

To try to reach this we could use an elliptic analogue of the original argument of Liardet for $\mathbf{G}_m \times \mathbf{G}_m$ (see for example [11, pp. 203–205]); note however that our elliptic curve is not defined over a number field. Sadly we reach only the weaker bound

$$\max\{|p|, |q|\} < 72\pi^2(2\check{D})^{14} \tag{11.11}$$

(this suffices of course to prove the Proposition). Still, the details may be of independent interest, and so we present them separately in Appendix B.

12 Tate curves

Finally we make it down to (11.3) and (11.4) alone.

Lemma 12.1 *Suppose* $\check{P} = (\check{\xi}, \check{\eta})$, $\check{Q} = (\check{\mu}, \check{\nu})$ *are points of orders* n_P, n_Q *respectively on* $\check{E}_j$ *satisfying a relation*

$$\check{F}(\check{\xi}, \check{\mu}) = 0$$

with non-zero $\check{F}$ *of degree at most* $\check{D}$ *with coefficients in* $\mathbf{Q}(j)$. *Then there are integers* p, q, *not both zero, such that*

$$q\check{P} = p\check{Q}$$

and

$$\max\{|p|, |q|\} < (2\check{D})^8.$$

Proof We may now assume (11.8), (11.9). To reach (11.4) we exploit (11.1) and (11.9) through a kind of Puiseux expansion. More specifically, it will be convenient to use yet a third model, the Tate curve. Thus we argue $\frac{1}{j}$-adically.

Since j is transcendental over $\mathbf{Q}$, we can equip the field $\mathbf{Q}(j)$ with a non-archimedean valuation with $|j| > 1$. Equivalently we embed $\mathbf{Q}(j)$ in the quotient field k of the ring $\mathbf{Q}[[1/j]]$ of power series in $1/j$. As in [9, p. 201] we can define u with $|u| < 1$ in k via the functional inverse of the standard expansion $j = j(u) = u^{-1} + 744 + 196884u + \cdots$ (we already used the classical q too often). We do not need refinements to take care of characteristic 2 and 3, and so we can use the equally standard expansions

$$\frac{1}{12}\left(1 + 240\sum_{n=1}^{\infty}\frac{n^3u^n}{1-u^n}\right), \quad \frac{1}{216}\left(-1 + 504\sum_{n=1}^{\infty}\frac{n^5u^n}{1-u^n}\right) \tag{12.1}$$

in [9, p. 197]. They converge and give the analogues of g_2, g_3 for an elliptic curve. We can reach $\check{E}_j$ by adjusting the coordinates by any χ with $\chi^2 = \frac{g_2}{g_3}$; and we end up with the parametrizations $\exp(w) = (\check{X}(w), \check{Y}(w))$ on the multiplicative group k^*, where

$$\chi^{-2}\check{X}(w) - \frac{1}{12} = \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty}\left(\frac{u^n w}{(1-u^n w)^2} + \frac{u^n w^{-1}}{(1-u^n w^{-1})^2} - 2\frac{u^n}{(1-u^n)^2}\right) \tag{12.2}$$

as in [9, pp. 197–198].

Now the relation (11.1) says that the $\check{X}$-coordinates of $\check{P}$ of order n_P and $\check{Q}$ of order n_Q on the archimedean $\check{E}_j(\overline{\mathbf{Q}(j)})$ are related by an equation over $\mathbf{Q}(j)$ of degree at most $\check{D}$. And (11.9) says $q'\check{P} = p'\check{Q}$. These equations persist for certain points $\check{P}_k = (\check{\xi}_k, \check{\eta}_k)$ still of order n_P and $\check{Q}_k = (\check{\mu}_k, \check{\nu}_k)$ still of order n_Q on the non-archimedean $\check{E}_j(\bar{k})$; indeed the properties are independent of any metric. In particular

$$\check{F}_k(\check{\xi}_k, \check{\mu}_k) = 0 \tag{12.3}$$

for non-zero $\check{F}_k$ over $\mathbf{Q}(j)$ of degree at most $\check{D}$, as well as

$$q'\check{P}_k = p'\check{Q}_k \tag{12.4}$$

(and we could even take $\check{F}_k = \check{F}$).

The Galois transitivity on points of order n_Q also persists, and so we can assume

$$\check{Q}_k = \exp(u^{1/n_Q}), \quad \check{\mu}_k = \check{X}(u^{1/n_Q}). \tag{12.5}$$

As for P_k, let us write $N = q'n_Q$, so by (12.4) it is a point of order dividing N. Thus we have

$$\check{P}_k = \exp(\zeta u^{l/N}), \quad \check{\xi}_k = \check{X}(\zeta u^{l/N}) \tag{12.6}$$

where ζ is a root of unity and l is an integer with $0 \le l < N$. Replacing if necessary $\check{P}_k$ by $-\check{P}_k$ and q' by $-q'$, we can even suppose that $0 \le l \le \frac{N}{2}$.

Next from Theorem 1 in [9, p. 199], the relation (12.4) yields $(\zeta u^{l/N})^{q'} = (u^{1/n_Q})^{p'}$ up to a factor in $u^{\mathbf{Z}}$, and in particular we deduce

$$l \equiv p' \bmod n_Q. \tag{12.7}$$

To get more information about l, q' we look at valuations in (12.3), which we rewrite as

$$\sum f_{a,b} X_T(\zeta u^{l/N})^a X_T(u^{1/n_Q})^b = 0, \tag{12.8}$$

summed over all non-negative integers a, b with $a + b \le \check{D}$, where $X_T(w)$ is the right-hand side of (12.2); now the $f_{a,b}$ lie in $\mathbf{Q}(j, \chi^2)$ and so in k, because of (12.1) and $\chi^2 = \frac{g_2}{g_3}$.

This (12.2) shows that if $|w| \ge |u|^{1/2}$, then the term of biggest absolute value in $X_T(w)$ is w. The value may appear a second time if $|w| = |u|^{1/2}$, namely from uw^{-1}. This cannot occur at $w = u^{1/n_Q}$ unless $n_Q = 2$, in which case we have a tiny (11.3) anyway. Neglecting this trivial case, we deduce from (12.5) that $|X_T(u^{1/n_Q})| = |u|^{1/n_Q}$.

For $|X_T(\zeta u^{l/N})|$ we argue similarly. This time for $w = \zeta u^{l/N}$ we can have two terms of equal biggest value only if $l = \frac{N}{2}$, in which case they are $w = \zeta u^{1/2}$ and

$uw^{-1} = \zeta^{-1}u^{1/2}$. These cancel out only if $\zeta^2 = -1$; but this would mean $n_P = 4$ which is similarly negligible. We conclude from (12.6) that $|X_T(\zeta u^{l/N})| = |u|^{l/N}$.

Now, since the valuation on k is discrete, there must exist in equation (12.8) two terms of equal absolute value. The absolute value of a typical term is, up to a factor in $|u|^{\mathbf{Z}}$, of the shape $|u|^{\frac{al}{N}+\frac{b}{n_Q}}$. Equating two of these with different (a, b), we get $a_0 l \equiv b_0 q' \bmod N$ for integers a_0, b_0 bounded in absolute value by $\check{D}$, and not both zero. From (12.7) we conclude $a_0 q' \check{P} = b_0 q' \check{Q}$ which in view of (11.10) gives at last the required (11.3), (11.4).

13 Proof of Proposition in the transcendental case

Now our curve C is not defined over $\overline{\mathbf{Q}}$. Let $\mathbf{c}$ be as in the Proposition. If $\lambda(\mathbf{c})$ is algebraic over $\mathbf{Q}$, then $P(\mathbf{c})$, $Q(\mathbf{c})$ are torsion points on an elliptic curve defined over $\overline{\mathbf{Q}}$ and so $\xi(\mathbf{c})$, $\eta(\mathbf{c})$, $\mu(\mathbf{c})$, $\nu(\mathbf{c})$ are also in $\overline{\mathbf{Q}}$. Thus we get a point of $C(\overline{\mathbf{Q}})$. But as C is not defined over $\overline{\mathbf{Q}}$, at most finitely many points turn up in this way (see for example Lemma 3 of [4, p. 313]).

So we can henceforth suppose that $\lambda = \lambda(\mathbf{c})$ is transcendental over $\mathbf{Q}$. We will now find bounded integers p, q, not both zero, such that

$$q P(\mathbf{c}) = p Q(\mathbf{c}). \tag{13.1}$$

This leads to the finiteness of the $\mathbf{c}$, as by hypothesis $qP \neq pQ$ identically. In fact our bounds on p, q will be explicit.

To express our bounds, we may suppose that C is defined over a field $\mathcal{K}$ finitely generated over $\mathbf{Q}$. So there are $\kappa_1, \ldots, \kappa_t$ algebraically independent over $\mathbf{Q}$ such that $\mathcal{K}$ is a finite extension of $\mathbf{Q}(\kappa_1, \ldots, \kappa_t)$, say $\mathcal{K} = \mathbf{Q}(\kappa_0, \kappa_1, \ldots, \kappa_t)$. We can regard C, much as in [3, p. 463] or [4, p. 316], as a variety $W_{\mathcal{K}}$ in $\mathbf{A}^{t+6}$ parametrized by $(\xi, \eta, \mu, \nu, \lambda, \kappa_0, \kappa_1, \ldots, \kappa_t)$ and defined over $\mathbf{Q}$; as such it has dimension $t + 1$.

If $t = 1$ we define $\mathcal{K}_0 = \mathbf{Q}$. If $t > 1$ we note that $\mathbf{Q}(\lambda, \kappa_1, \ldots, \kappa_t)$ has transcendence degree at least $t - 1$ over $\mathbf{Q}(\lambda)$. Thus we may suppose that $\kappa_1, \ldots, \kappa_{t-1}$ are algebraically independent over $\mathbf{Q}(\lambda)$. In this case we define $\mathcal{K}_0 = \mathbf{Q}(\kappa_1, \ldots, \kappa_{t-1})$.

If $t = 1$ we write W_0 for the projection of $W_{\mathcal{K}}$ to the coordinates (ξ, μ, λ). If $t > 1$ we write W_0 for the projection of $W_{\mathcal{K}}$ to the coordinates $(\xi, \mu, \lambda, \kappa_1, \ldots, \kappa_{t-1})$. Finally we write D_0 for the degree of W_0 as a variety in $\mathbf{A}^{t+2}$. Our bounds for p, q in (13.1) are then

$$\max\{|p|, |q|\} < (12D_0)^8. \tag{13.2}$$

We start by finding a bounded non-trivial relation between $\xi = \xi(\mathbf{c})$ and $\mu = \mu(\mathbf{c})$.

The variety W_0 has dimension at most $t + 1$. If it is $t + 1$, then W_0 is defined by the vanishing of a single non-zero polynomial in $\xi, \mu, \lambda, \kappa_1, \ldots, \kappa_{t-1}$; and by the algebraic independence of $\lambda, \kappa_1, \ldots, \kappa_{t-1}$ this provides a relation

$$F(\xi, \mu) = 0 \tag{13.3}$$

where F has degree at most D_0 and coefficients in $\mathcal{K}_0(\lambda)$.

If however W_0 has dimension less than $t+1$, then again by the algebraic independence of $\lambda, \kappa_1, \ldots, \kappa_{t-1}$ it must be t. Now project down to W_1 in $\mathbf{A}^{t+1}$ with coordinates $(\xi, \lambda, \kappa_1, \ldots, \kappa_{t-1})$. This has dimension at most t but also at least t so exactly t. Also its degree is at most that of W_0; see for example the Proposition of [6, p. 254] unless W_0 is a cone over the centre $(0, \ldots, 0)$ of projection (in which case we have equality). It too is defined by the vanishing of a single polynomial; and this too leads to (13.3) (now without μ).

Thus (13.3) is our promised bounded non-trivial relation between ξ and μ. But these coordinates refer to the Legendre model, whereas Sects. 11 and 12 refer to a Weierstrass model. That is no big problem (note however that Lemma 10.1 would be false for the Legendre model because for example all points of order 2 are rational). In [17] we used

$$\tilde{Y}^2 = 4\tilde{X}^3 - g_2\tilde{X} - g_3$$

with

$$g_2 = \frac{4}{3}(\lambda^2 - \lambda + 1), \quad g_3 = \frac{4}{27}(\lambda - 2)(\lambda + 1)(2\lambda - 1);$$

this could now be denoted by $\tilde{E}_\lambda$ (recall here $\lambda = \lambda(\mathbf{c})$). The isomorphism from E_λ to $\tilde{E}_\lambda$ is given by sending (X, Y) to $(\tilde{X}, \tilde{Y})$ with

$$\tilde{X} = X - \frac{1}{3}(\lambda + 1), \quad \tilde{Y} = 2Y.$$

Correspondingly

$$\tilde{\xi} = \xi - \frac{1}{3}(\lambda + 1), \quad \tilde{\mu} = \mu - \frac{1}{3}(\lambda + 1)$$

satisfy from (13.3) an equation

$$\tilde{F}(\tilde{\xi}, \tilde{\mu}) = 0 \tag{13.4}$$

also with non-zero $\tilde{F}$ of degree at most D_0 and coefficients in $\mathcal{K}_0(\lambda)$.

We observe that $\tilde{E}_\lambda$ is defined over $\mathbf{Q}(\lambda)$ but not necessarily over $\mathbf{Q}(j)$; in fact

$$j = 256\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1 - \lambda)^2} \tag{13.5}$$

(and of course the 2-torsion is still rational). We could deal with this problem using Weber coordinates but we may as well proceed straight to $\check{E}_j$; note from (13.5) that j is transcendental over $\mathbf{Q}$. The isomorphism from $\tilde{E}_\lambda$ to $\check{E}_j$ is given by sending $(\tilde{X}, \tilde{Y})$ to $(\check{X}, \check{Y})$ with

$$\check{X} = \chi^2\tilde{X}, \quad \check{Y} = \chi^3\tilde{Y},$$

where χ is anything with

$$\chi^2 = \frac{g_2}{g_3} = \frac{9(\lambda^2-\lambda+1)}{(\lambda-2)(\lambda+1)(2\lambda-1)}.$$

Correspondingly

$$\check{\xi} = \chi^2\tilde{\xi}, \quad \check{\mu} = \chi^2\tilde{\mu}$$

are also related by a non-trivial polynomial equation like (13.4) of degree at most D_0 and coefficients in $\mathcal{K}_0(\lambda)$.

And then taking norms using (13.5) provides a similar relation, but now of degree at most $6D_0$ and with coefficients now in $\mathcal{K}_0(j)$.

Next $\mathcal{K}_0(j)$ and $\overline{\mathbf{Q}(j)}$ are linearly disjoint over $\mathbf{Q}(j)$. This is trivial if $t = 1$, and if $t > 1$ we could apply for example Proposition 3.3 of [12, p. 363], with L there as $\overline{\mathbf{Q}(j)}$, k there as $\mathbf{Q}(j)$, and $u_1, \dots, u_r$ there as $\kappa_1, \dots, \kappa_{t-1}$. As $\check{\xi}, \check{\mu}$ are coordinates of torsion points on the elliptic curve $\check{E}_j$ defined over $\mathbf{Q}(j)$, they are in $\overline{\mathbf{Q}(j)}$, and we end up with a new relation

$$\check{F}(\check{\xi}, \check{\mu}) = 0$$

with non-zero $\check{F}$ still of degree at most $6D_0$ but with coefficients now in $\mathbf{Q}(j)$.

Now Lemma 12.1 with $D = 6D_0$ gives at once (13.2) for (13.1), thereby completing the proof of the Proposition in the transcendental case.

As indicated in the Introduction, there is a good possibility that the Proposition in this case could be proved by a specialization argument from the algebraic case like those of [3] or [4].

14 Examples

We start with the verification of (2.1) in the first two examples mentioned in the Introduction. For $P = (\tau, \tau)$ and $Q = (-\tau, \tau)$ on $Y^2 = 4X^3 - 4\tau^2X + \tau^2$ we note that $P + Q = R = (0, \tau)$, and it is proved in [5] (see p. 28) that R and P form a basis for the set of points over $\mathbf{C}(\tau)$. The example $P = (2\lambda, \lambda\sqrt{2(2\lambda-1)})$, $Q = (3\lambda, \lambda\sqrt{6(3\lambda-1)})$ in (1.2) is much easier, because the Y-coordinates of qP and pQ are multiples of $\sqrt{2\lambda-1}$ and $\sqrt{3\lambda-1}$ respectively by elements of $\mathbf{C}(\lambda)$, and so from equality would follow $2qP = 2pQ = 0$. But the fact that P and Q are not separately torsion is also clear because they are ramified outside $0, 1, \infty$.

Next we check (2.1) for the points $P = (\tau, \pi)$ and $Q = (-\tau, \pi)$ on $\tilde{Y}^2 = 4\tilde{X}^3 - 4\tau^2\tilde{X} + \pi^2$. In fact a relation $qP = pQ$ identically in τ would lead via the transcendence of π to the same relation with π replaced throughout by any parameter independent of τ (for example by using the multiplication formulae), and then we could specialize this parameter to τ to bring us back to the example just before (1.2).

We may take such considerations further in order to check the bound 10^{40} regarding the points, call them P, Q respectively, in (1.5). We note that the curve C is

parametrized by

$$(\xi, \eta, \mu, \nu, \lambda) = (\kappa, \sqrt{\kappa(\kappa-1)(\kappa-\lambda)}, \kappa', \sqrt{\kappa'(\kappa'-1)(\kappa'-\lambda)}, \lambda)$$

and is therefore defined over $\mathcal{K} = \mathbf{Q}(\kappa, \kappa')$, which by our assumption that κ is transcendental over $\mathbf{Q}$ and $\frac{\kappa'}{\kappa} = \rho$ is rational is $\mathbf{Q}(\kappa)$ with transcendence degree $t = 1$. So the surface W_0 over $\mathbf{Q}$ is parametrized by $(\kappa, \rho\kappa, \lambda)$ and of degree $D_0 = 1$, the relation (13.3) being simply $\rho\xi = \mu$. We deduce from (13.2) that $qP = pQ$ for some p, q, possibly depending on the value of λ, with

$$0 < \max\{|p|, |q|\} \le M = 12^8. \tag{14.1}$$

To finish we use the multiplication formula $\frac{A_n(X,\lambda)}{B_n(X,\lambda)}$ $(n = 1, 2, 3, \ldots)$ from [17] whose leading terms in X can be normalized to

$$A_n(X, \lambda) = X^{n^2} + \cdots, \quad B_n(X, \lambda) = n^2 X^{n^2-1} + \cdots. \tag{14.2}$$

In fact the degrees in λ are at most also n^2 and $n^2 - 1$ respectively. This can be seen for example from the analogous formula for the Weierstrass model, in which both numerator and denominator are isobaric of these weights when $\tilde{X}, g_2, g_3$ are assigned the weights 1,2,3 respectively. It is natural also to define $A_{-n}(X, \lambda) = A_n(X, \lambda)$, $B_{-n}(X, \lambda) = B_n(X, \lambda)$ and $A_0(X, \lambda) = 1$, $B_0(X, \lambda) = 0$.

We then find the relation $C_{pq}(\kappa, \lambda) = 0$ for the polynomial

$$C_{pq}(X, T) = A_q(X, T)B_p(\rho X, T) - A_p(\rho X, T)B_q(X, T).$$

For any pair (p, q) out of the $(2M + 1)^2 - 1$ in (14.1), we will show in a moment that $C_{pq}(\kappa, T)$ is not identically zero in the variable T. Its degree is at most $p^2 + q^2 - 1 \le 2M^2$, so for such (p, q) there are at most $2M^2$ values of λ. This would give at most $2M^2(2M + 1)^2 < 10^{40}$ in all, as was to be proved.

What if some $C_{pq}(\kappa, T)$ were identically zero in T? This would mean $qP = pQ$ identically in λ. But P is defined over an extension of $\mathbf{Q}(\lambda)$ ramified at $\lambda = \kappa$, and similarly Q at κ'. As $\kappa \ne \kappa'$ we conclude as above $2qP = 2pQ = 0$ also identically. But $\kappa, \kappa' \ne 0, 1$ and so as above we see that P, Q are not torsion.

Finally in a specific example like (1.3) one sees at once how to actually find all the values of λ: one just has to solve the finitely many equations $C_{pq}(2\pi, \lambda) = 0$ (with $\rho = \frac{3}{2}$) and check if the points (1.3) are both torsion, for example by calculating the Néron-Tate height when π is regarded as a variable. As mentioned in the Introduction, in a subsequent note we will show for example that there are no λ at all, even in a situation slightly more general than (1.5).

Appendix A

We present here a self-contained proof that the functions f, g, z, w of Lemma 5.1 are algebraically independent on N_*. As explained in the Introduction, just the

homogeneous independence suffices for the proof of the Proposition in the algebraic case. It is convenient now to replace C by a complete non-singular model of itself, and there will be no confusion in denoting this too by C. Of course $\lambda, \xi, \eta, \mu, \nu$ remain functions on the new C. Again we define $\hat{C}$ as in Sect. 4.

We will have to define principal values of f, g, z, w locally on $\hat{C}$. We do this by modifying the discussion in Sect. 4 to use straight line paths in the X-plane in order to control the winding numbers.

Choose a half-line $\mathcal{H}(\mathbf{c})$ from $\xi(\mathbf{c})$ to ∞ not passing through $0, 1, \lambda(\mathbf{c})$. Via the fixed determination of $Y = \sqrt{X(X-1)(X-\lambda(\mathbf{c}))}$ equal to $\eta(\mathbf{c})$ at $X = \xi(\mathbf{c})$ this half-line extends to a path on $E_{\lambda(\mathbf{c})}$ from P to O ready for integration as in (4.4). The resulting $z(\mathbf{c})$, $w(\mathbf{c})$ we could call principal values. And in a small neighbourhood of $\mathbf{c}$ we can repeat the same with for example a half-line parallel to $\mathcal{H}(\mathbf{c})$. This defines $z(\mathbf{c})$ locally at any point of $\hat{C}$; and similarly for $w(\mathbf{c})$. However it would be a "forlorn hope" that z and w are defined globally on $\hat{C}$.

We can also define principal values $f(\mathbf{c}), g(\mathbf{c})$ using such integrals and thereby avoid the explicit hypergeometric series $F(t)$ above. But for this we have to make a few more choices.

For f we use the distinguished point 1. First choose $s = s(\mathbf{c}) \neq 0, 1, \lambda(\mathbf{c})$. But also s has to avoid four half-lines. Two start from 1 and go in the direction precisely opposite to 0 and $\lambda(\mathbf{c})$, and the other two start from 0 and $\lambda(\mathbf{c})$ and go in the direction precisely opposite to 1. This enables us to choose a thin closed sector centred at s, not containing 0 and $\lambda(\mathbf{c})$, whose interior contains 1. Its boundary consists of two half-lines $\mathcal{H}^1, \mathcal{H}^2$ from s to ∞. On choosing a value s' of $\sqrt{s(s-1)(s-\lambda(\mathbf{c}))}$, we see that each extends to a path on $E_{\lambda(\mathbf{c})}$ from (s, s') to O. We thus obtain a loop from O to itself, and we accordingly define $f = \int_O^O \frac{\mathrm{d}X}{2Y}$ as in (4.4), described in such a way that the corresponding X-loop is in the clockwise sense. Thus $f(\mathbf{c})$ is defined locally at any point of $\hat{C}$. We define $g(\mathbf{c})$ in a similar way with distinguished point 0 instead of 1. Thus the two half-lines start from 0 and go in the direction precisely opposite to 1 and $\lambda(\mathbf{c})$, and two start from 1 and $\lambda(\mathbf{c})$ and go in the direction precisely opposite to 0; and the sector contains 0 but not 1 or $\lambda(\mathbf{c})$. But now there is hardly any hope at all that these are defined globally on $\hat{C}$. At any rate

$$\exp_\lambda(f) = O, \quad \exp_\lambda(g) = O.$$

Why do these agree with (4.1)? Well, for $\lambda(\mathbf{c})$ near $\frac{1}{2}$ we can take for example $s = \frac{3}{4}$ with s' near $i\frac{\sqrt{3}}{8}$, and it is easily checked using Cauchy's Theorem that

$$f(\mathbf{c}) = \int_1^\infty \frac{\mathrm{d}X}{\sqrt{X(X-1)(X-\lambda(\mathbf{c}))}}$$

as in [8, p. 179]. By Theorem 6.1 there, this is just $\pi F(\lambda(\mathbf{c}))$ as in (4.1). Similarly for $g(\mathbf{c})$ with $\lambda(\mathbf{c})$ near $\frac{1}{2}$, $s = \frac{1}{4}$, s' near $\frac{\sqrt{3}}{8}$ and $g(\mathbf{c}) = \int_{-\infty}^0 \frac{\mathrm{d}X}{\sqrt{X(X-1)(X-\lambda(\mathbf{c}))}} = \pi i F(1-\lambda(\mathbf{c}))$.

For complex numbers $t \neq 0, 1$ and $s \neq 0, 1, t$ and a half-line $\mathcal{H}$ from s to ∞ not passing through $0, 1, t$ we define

$$I(\mathcal{H}, t) \;=\; \int\limits_{\mathcal{H}} \frac{|\mathrm{d}X|}{\sqrt{|X(X-1)(X-t)|}}.$$

The following result will be used to establish at worst logarithmic singularities near $t = 0, 1$ and even zeroes near $t = \infty$.

Lemma A.1 *There is an absolute constant c such that*

$$I(\mathcal{H}, t) \;\leq\; c\, \frac{\max\{|\log|t||, |\log|1-t||\}}{\sqrt{1+|t|}}.$$

Proof Consider first the case

$$|t| \leq 1, \quad \mathrm{Re}\, t \leq \frac{1}{2}, \tag{A.1}$$

so that $|1 - t| \geq \frac{1}{2}$; and then the subcase $|t| \geq \frac{1}{4}$. Now $0, 1, t$ are well-separated from each other, and so a point X of $\mathcal{H}$ gets very close to at most one of $0, 1, t$. In the subsequent estimates it is convenient to use $\ll, \gg$ instead of positive absolute constants.

If X gets close to 0, then we have $|X - 1| \gg 1 + |X|$ and $|X - t| \gg 1 + |X|$. Now this part of the integral is $\ll \int_0^\infty \frac{\mathrm{d}x}{(1+x)\sqrt{x}} = \pi$. If X gets close to 1, then we can argue similarly. And if X gets close to t, then we get a contribution $\ll \int_0^\infty \frac{\mathrm{d}x}{(1+x)\sqrt{|x-\theta|}}$ for $\theta = |t|$, which is easily seen to be bounded above independently of θ.

And if X stays away from all three, then the corresponding integral $I(\mathcal{H}, t) \ll \int_0^\infty \frac{\mathrm{d}x}{(1+x)\sqrt{1+x}} = 2$.

This implies the lemma in the present subcase.

Staying with (A.1), consider now the remaining subcase $0 < |t| \leq \frac{1}{4}$. Then we get $I(\mathcal{H}, t) \leq \int_0^\infty \frac{\mathrm{d}x}{\sqrt{|x(x-1)(x-\theta)|}}$. The part from 0 to θ is $\ll \int_0^\theta \frac{\mathrm{d}x}{\sqrt{x(\theta-x)}} = \pi$. The part from θ to $\frac{1}{2}$ is

$$\ll \int\limits_{\theta}^{1+\theta} \frac{\mathrm{d}x}{\sqrt{x(x-\theta)}} \;=\; -\log\theta + \log(\theta + 2 + 2\sqrt{1+\theta}) \;\ll\; |\log\theta| + 1; \tag{A.2}$$

it is this that causes the first logarithm in the inequality of the lemma. Finally the part from $\frac{1}{2}$ to ∞ is $\ll \int_{1/2}^\infty \frac{\mathrm{d}x}{x\sqrt{|x-1|}}$.

This settles the case (A.1).

To finish off, we check easily by replacing X by tX and $1 - X$ that

$$I(\mathcal{H}, t) \;=\; \frac{1}{\sqrt{|t|}}\, I\left(t\mathcal{H}, \frac{1}{t}\right), \quad I(\mathcal{H}, t) \;=\; I(1-\mathcal{H}, 1-t)$$

in an obvious notation for half-lines (compare [8, p. 82]). Using the first shows that we can assume the first inequality in (A.1); and using the second shows that we can also assume the second inequality.

Lemma A.2 *There is an absolute constant c such that for $\mathbf{c}$ in $\hat{C}$ we have for the principal values*

$$\max\{|f(\mathbf{c})|, |g(\mathbf{c})|, |z(\mathbf{c})|, |w(\mathbf{c})|\} \ \le \ c\,\frac{\max\{|\log|t||, |\log|1-t||\}}{\sqrt{1+|t|}}$$

for $t = \lambda(\mathbf{c})$.

Proof It is clear that $|z(\mathbf{c})| \le \frac{1}{2}I(\mathcal{H}, t)$, where $\mathcal{H} = \mathcal{H}(\mathbf{c})$ is our half-line from $\xi(\mathbf{c})$ not through $0, 1, t$. Now we appeal to Lemma A.1; and similarly for w. And $|f(\mathbf{c})| \le \frac{1}{2}I(\mathcal{H}^1, t) + \frac{1}{2}I(\mathcal{H}^2, t)$, and similarly for g.

We next consider the monodromy.

For f and g this is quickly deduced from [17]. Let t be any point of the set $\hat{\mathbf{C}}$ of all complex $t \neq 0, 1$, and let us traverse a loop $\mathcal{L}$ pointed at t; that is, from t to itself, lying in $\hat{\mathbf{C}}$. If $\mathcal{L}$ encircles 0 once in the anticlockwise sense and does not encircle 1, then after the traverse $F = F(t)$ stays fixed and $G = F(1-t)$ becomes $-2iF + G$ (compare (3.5) of [17]). Incidentally this can also be seen directly using (A.2); we sketch the proof because the reference given in [17] may have been not quite satisfactory. Namely from (4.1) and the period property (4.3) it is clear that G must become $aiF + bG$ for certain integers a, b. But for small $t > 0$ we have (see for example [8, p. 179])

$$\pi G(t) \ = \ \int_1^\infty \frac{dX}{\sqrt{X(X-1)(X-1+t)}}$$

for the non-negative real square root. This is $J_0(t) + J_1(t)$ for

$$J_0(t) = \int_1^2 \left(\frac{1}{\sqrt{X(X-1)}} - \frac{1}{\sqrt{X-1}}\right)\frac{dX}{\sqrt{X-1+t}} + \int_2^\infty \frac{dX}{\sqrt{X(X-1)(X-1+t)}},$$

$$J_1(t) = \int_1^2 \frac{dX}{\sqrt{(X-1)(X-1+t)}}.$$

We can easily check that $J_0(t)$ is up to a constant $o(1)$ as $t \to 0$; the point is that the bracketed part of the first integral is zero at $X = 1$. And with $x = X-1+t = X-1+\theta$ we find that $J_1(t)$ is precisely the integral in (A.2). Thus $\pi G(t) + \log t$ is up to a constant $o(1)$. So if the loop is small then it hardly changes. On the other hand since

$F(0) = 1$ it becomes

$$\pi\ (aiF(t) + bG(t)) + (\log t + 2\pi i)$$
$$= (\pi G(t) + \log t) + \pi i(a+2) - (b-1)\log t + o(1).$$

It follows that $a = -2$ and $b = 1$ as claimed.

Similarly if $\mathcal{L}$ encircles 1 once in the anticlockwise sense and does not encircle 0, then G stays fixed and F becomes $F - 2iG$ (compare (3.4) of [17]). These correspond to the elements $\gamma_0 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\gamma_1 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ respectively of $\Gamma = SL_2(\mathbf{Z})$ acting on (the right of) the vector $(\pi F, \pi iG)$. These two matrices generate a subgroup of Γ called $\Gamma^*(2)$ (in fact of index 12).

Next consider a general pointed loop in $\hat{C}$. Its image under λ is a loop like $\mathcal{L}$ above. Thus traversing the loop in $\hat{C}$ leads to an element of $\Gamma^*(2)$ acting on (f, g), and the set of all such loops in $\hat{C}$ yields a subgroup Γ_λ of $\Gamma^*(2)$. We write $\iota = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for the identity matrix.

Lemma A.3 *There are non-zero integers n_0, n_1 with $\gamma_0^{n_0}, \gamma_1^{n_1}$ in Γ_λ, and there is γ in Γ_λ with invertible $\gamma - \iota$.*

Proof Fix any point $\mathbf{c}_0$ of C in $\lambda^{-1}(0)$, and fix a path $\mathcal{P}$ from $\mathbf{c}_*$ to $\mathbf{c}_0$ inside $\hat{C}$ (apart from $\mathbf{c}_0$). We can make from this a loop $\mathcal{P}_0$ from $\mathbf{c}_*$ to itself by traversing the path up to just before $\mathbf{c}_0$, then going around $\mathbf{c}_0$ once, and then returning to $\mathbf{c}_*$. Then $\mathcal{L} = \lambda(\mathcal{P}_0)$ is a loop from $t_* = \lambda(\mathbf{c}_*)$ to itself. The number of times it encircles 0 in the positive sense is some $n_0 \neq 0$, and it does not encircle 1 because $\lambda(\mathcal{P})$ stays away from 1. The effect of $\mathcal{P}_0$ on (f, g) is therefore $\gamma_0^{n_0}$. Similarly we can find a loop $\mathcal{P}_1$ from $\mathbf{c}_*$ to itself whose effect on (f, g) is $\gamma_1^{n_1}$ for some $n_1 \neq 0$. So our Γ_λ contains $\gamma_0^{n_0}$ and $\gamma_1^{n_1}$ as claimed. Finally we calculate that $\gamma = \gamma_0^{n_0}\gamma_1^{n_1}$ has trace $m = 2 - 4n_0n_1 \neq 2$, and it follows that $\det(\gamma - \iota) = 2 - m \neq 0$. This proves the lemma.

As for the monodromy of z and w, the argument of Sect. 6 on the continuation shows also that traversing z around any loop in $\hat{C}$ will change it to $z + pf + qg$ for rational integers p, q. Similarly w becomes $w + rf + sg$ for rational integers r, s.

Thus going around a pointed loop in $\hat{C}$ has the effect of multiplying the vector (f, g, z, w) on the right by a matrix $\varepsilon = \begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}$, where γ is in Γ_λ and $\delta = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$ is in the ring $M_2(\mathbf{Z})$ of all integral matrices. We get a monodromy group $E(\mathbf{Z})$ in $SL_4(\mathbf{Z})$ by restricting to loops pointed at say $\mathbf{c}_*$.

For later use we record the following remark.

Main Lemma *Suppose that h is a linear combination of f, g, z, w with rational coefficients which has no monodromy; that is, h is invariant under $E(\mathbf{Z})$. Then $h = 0$.*

Proof We can suppose that the coefficients are in $\mathbf{Z}$. It follows from the theory of analytic continuation that h is globally analytic on $\hat{C}$, in spite of the previous "forlorn hope". But we can even extend it to the remaining finite set $C_?$ of points of C in the following way.

Fix $\mathbf{c}_?$ in $C_?$. Fix an analytic isomorphism from some open set of $\mathbf{C}$ containing the interval $[0, 1]$ to an open neighbourhood of $\mathbf{c}_?$ not containing any other point of $C_?$ and taking 1 to $\mathbf{c}_?$. By restriction it gives an analytic path (see [10, p. 290]) from some $\mathbf{c}_{**}$ in $\hat{C}$ to $\mathbf{c}_?$. We claim that we can define z analytically along the image of $[0, 1)$ of this path.

From the discussion in Sect. 4 of the straight line $\mathcal{H}(\mathbf{c})$ from $\xi(\mathbf{c})$ to ∞ we see that it is a question of choosing this line continuously while making sure that it does not pass through $0, 1, \lambda(\mathbf{c})$. Thus there are at most three forbidden directions determined by the arguments of the non-zero numbers $\xi(\mathbf{c}), \xi(\mathbf{c}) - 1, \xi(\mathbf{c}) - \lambda(\mathbf{c})$. As $\mathbf{c}$ approaches $\mathbf{c}_?$ along our analytic path these arguments, even if the numbers themselves go to 0 or ∞, all have limits. This can be seen from considering the real and imaginary parts, which are real analytic functions on $[0, 1]$; for example, it is impossible for $\xi(\mathbf{c})$ to approach 0 along a spiral with infinite winding number. Therefore it suffices to fix a direction for $\mathbf{s}(\mathbf{c})$ different from these three limits; and this will work provided $\mathbf{c}_{**}$ was close enough to $\mathbf{c}_?$. We obtain an analytic definition $z_?(\mathbf{c})$ of $z(\mathbf{c})$, for $\mathbf{c}$ in some open set whose closure contains $\mathbf{c}_?$, satisfying the estimates of Lemma A.2.

We obtain similarly $w_?(\mathbf{c})$. And also $f_?(\mathbf{c})$; here it suffices to choose $s = s(\mathbf{c})$ with say $|s - 1| = \frac{1}{2}$ and make sure that the argument of $1 - s$ avoids the arguments of $\pm(1 - \lambda(\mathbf{c}))$ and ± 1. Similarly for $g_?(\mathbf{c})$.

Thus also for $h_?(\mathbf{c})$. Since the coefficients in h are in $\mathbf{Z}$, exponentiation shows that there are integers $m_?, n_?$ with $h_?(\mathbf{c}) = h(\mathbf{c}) + m_? f_?(\mathbf{c}) + n_? g_?(\mathbf{c})$. By continuity these integers must be constants.

Finally $h(\mathbf{c}) = h_?(\mathbf{c}) - (m_? f_?(\mathbf{c}) + n_? g_?(\mathbf{c}))$ satisfies the estimates of Lemma A.2. This implies that it has at most bounded growth as $\lambda(\mathbf{c})$ approaches any limit $\lambda_? \neq 0, 1, \infty$, and at most logarithmic growth as $\lambda(\mathbf{c})$ approaches $0, 1, \infty$. Thus h must be analytic on all on C.

As C was complete non-singular this means that h is constant on C. However we can choose $\mathbf{c}_?$ with $\lambda(\mathbf{c}_?) = \infty$, and then Lemma A.2 shows that the constant must be zero. This completes the proof.

Fortunately we are able to avoid any arithmetical complications later with $E(\mathbf{Z})$ by working with its Zariski closure in $SL_4(\mathbf{C})$. This closure is also much easier to describe; with possible slight abuse of notation we call it $E(\mathbf{C})$ (there is no implication that $E(\mathbf{Z})$ is the set of its integral points). We start with the following observation about the first cohomology H^1.

Lemma A.4 *Let V be a complex vector space and left $SL_2(\mathbf{C})$-module, and let ψ be a cocycle from $SL_2(\mathbf{C})$ to V, so that $\psi(\gamma\gamma') = \gamma\psi(\gamma') + \psi(\gamma)$. Then ψ is a coboundary, so that there exists δ_0 in V with $\psi(\gamma) = (\gamma - \iota)\delta_0$.*

Proof This can be easily derived from the standard restriction-inflation sequence using the group $\{\iota, -\iota\}$, or from Sah's Lemma in [12, p. 303] with G there as $SL_2(\mathbf{C})$ and E there as V. We take τ there as $-\iota$; then the map taking δ to $\tau\delta - \delta = -2\delta$ is an automorphism of E, and so $H^1(G, E) = 0$.

Lemma A.5 *The group $E(\mathbf{C})$ is the set of $\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}$ for all γ in $SL_2(\mathbf{C})$ and all δ in $M_2(\mathbf{C})$.*

Proof Clearly the elements of $E(\mathbf{C})$ have the shape $\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}$ for γ in $SL_2(\mathbf{C})$ and δ in $M_2(\mathbf{C})$. The identity

$$\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix} \begin{pmatrix} \gamma' & \delta' \\ 0 & \iota \end{pmatrix} = \begin{pmatrix} \gamma\gamma' & \gamma\delta' + \delta \\ 0 & \iota \end{pmatrix} \tag{A.3}$$

shows that the map taking $\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}$ to γ defines a homomorphism φ from $E(\mathbf{C})$ to $SL_2(\mathbf{C})$. And since

$$\begin{pmatrix} \iota & \delta \\ 0 & \iota \end{pmatrix} \begin{pmatrix} \iota & \delta' \\ 0 & \iota \end{pmatrix} = \begin{pmatrix} \iota & \delta + \delta' \\ 0 & \iota \end{pmatrix}$$

the kernel of φ may be identified with an additive algebraic subgroup K of $M_2(\mathbf{C})$, which is just a $\mathbf{C}$-vector subspace of $\mathbf{C}^4$.

Now Lemma A.3 shows that $\varphi(E(\mathbf{Z}))$ contains $\gamma_0^{n_0} = \begin{pmatrix} 1 & 2n_0 \\ 0 & 1 \end{pmatrix}$ and $\gamma_1^{n_1} = \begin{pmatrix} 1 & 0 \\ -2n_1 & 1 \end{pmatrix}$. We have an identity

$$\begin{pmatrix} 1 & t_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & t_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 + t_1 t_2 & * \\ t_2 & 1 + t_2 t_3 \end{pmatrix}.$$

The functions t_2, $1 + t_1 t_2$, $1 + t_2 t_3$ here are easily seen to be algebraically independent. Taking t_1 and t_3 as arbitrary integer multiples of $2n_1$ and t_2 as an arbitrary integer multiple of $2n_0$, we deduce that the Zariski closure Z of $\varphi(E(\mathbf{Z}))$ has dimension at least 3. From general principles $\varphi(E(\mathbf{C}))$ is closed and so contains Z. As $\varphi(E(\mathbf{C}))$ lies in the irreducible $SL_2(\mathbf{C})$ we conclude that $\varphi(E(\mathbf{C})) = SL_2(\mathbf{C})$.

Also $\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}^{-1} = \begin{pmatrix} \gamma^{-1} & -\gamma^{-1}\delta \\ 0 & \iota \end{pmatrix}$ and so

$$\begin{pmatrix} \gamma & \delta' \\ 0 & \iota \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}^{-1} = \begin{pmatrix} \iota & \delta' - \delta \\ 0 & \iota \end{pmatrix}.$$

This shows that for any γ in $SL_2(\mathbf{C})$ the inverse image $\varphi^{-1}(\gamma)$ consists of the $\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}$ for all δ in a certain coset K_γ of K. Also

$$\begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix} \begin{pmatrix} \iota & \delta_0 \\ 0 & \iota \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ 0 & \iota \end{pmatrix}^{-1} = \begin{pmatrix} \iota & \gamma\delta_0 \\ 0 & \iota \end{pmatrix}.$$

This shows that K is stable under left multiplication by $\varphi(E(\mathbf{C})) = SL_2(\mathbf{C})$. Since K is also an additive group, it is similarly stable by the additive group generated by $SL_2(\mathbf{C})$, which is $M_2(\mathbf{C})$.

Now we have three cases.

(i) K contains some non-singular β. Then K contains $M_2(\mathbf{C})\beta = M_2(\mathbf{C})$ so $K = M_2(\mathbf{C})$. Thus every $K_\gamma = K$ and we are finished.

(ii) Every element of K is singular but $K \neq 0$. Pick any $\beta \neq 0$ in K. Then K contains $K_? = M_2(\mathbf{C})\beta$, which now has dimension 2. In fact $K = K_?$, as the following argument shows.

If not, then pick some β' in K not in $K_?$. Then K would contain $K'_? = M_2(\mathbf{C})\beta'$ and so also $K_? + K'_?$. The latter has dimension at least 3; if it had dimension 4 then it would be $M_2(\mathbf{C})$ and we would be in case (i). Thus $K_? + K'_?$ has dimension 3 and $K_?$, $K'_?$ must meet non-trivially, say in $\zeta \neq 0$. However β has some vector $v \neq 0$ in its kernel, and β' some $v' \neq 0$, and by choice of β' these two vectors must be independent. But then $\zeta v = \zeta v' = 0$ is a contradiction.

Thus indeed $K = K_?$. Now each γ in $SL_2(\mathbf{C})$ determines a unique coset K_γ as above, so we get a map ψ from $SL_2(\mathbf{C})$ to $V = M_2(\mathbf{C})/K$. The identity (A.3) shows that $\psi(\gamma\gamma') = \gamma\psi(\gamma') + \psi(\gamma)$, so that ψ is a cocycle. By Lemma A.4 it is a coboundary, so that there exists α in $M_2(\mathbf{C})$ such that $\psi(\gamma) = (\gamma - \iota)(\alpha + K)$.

Next pick $v \neq 0$ in $\mathbf{C}^2$ with $\beta v = 0$. The effect of monodromy is to multiply $\mathbf{t} = (f, g, z, w)$ by some $\varepsilon = \begin{pmatrix} \gamma & (\gamma - \iota)\alpha + \delta \\ 0 & \iota \end{pmatrix}$ in $E(\mathbf{Z})$, where δ is in K. We check that $\varepsilon \begin{pmatrix} -\alpha v \\ v \end{pmatrix} = \begin{pmatrix} -\alpha v + \delta v \\ v \end{pmatrix} = \begin{pmatrix} -\alpha v \\ v \end{pmatrix}$. Thus the function

$$h \;=\; (z, w)v - (f, g)\alpha v \;=\; (f, g, z, w)\begin{pmatrix} -\alpha v \\ v \end{pmatrix}$$

has no monodromy.

Now we cannot have $\delta = 0$ on $E(\mathbf{Z})$, otherwise $\delta = 0$ on $E(\mathbf{C})$ and then $K = 0$ contrary to our assumption in (ii). So there is some $\delta \neq 0$ on $E(\mathbf{Z})$, and now $\delta v = 0$ implies that we can take v above in $\mathbf{Q}^2$. By Lemma A.3 we can find γ in Γ_λ with $\gamma - \iota$ invertible, and now $\alpha = (\gamma - \iota)^{-1}((\gamma - \iota)\alpha + \delta) - (\gamma - \iota)^{-1}\delta$ lies in $M_2(\mathbf{Q})$. So αv is also in $\mathbf{Q}^2$. Then the Main Lemma implies $h = 0$ identically.

We can even multiply by denominators to get $v, \alpha v$ in $\mathbf{Z}^2$. But then exponentiating $h = 0$ via (4.5) would contradict (2.1).

(iii) $K = 0$. This is formally the same as case (ii) with $\beta = 0$; now $K = K_?$ (= 0) automatically. Now we consider the two functions $z^\#$, $w^\#$ defined by

$$(z^\#, w^\#) \;=\; (z, w) - (f, g)\alpha \;=\; (f, g, z, w)\begin{pmatrix} -\alpha \\ \iota \end{pmatrix}$$

As in case (ii) above we consider the effect of monodromy, now with $\varepsilon = \begin{pmatrix} \gamma & (\gamma - \iota)\alpha \\ 0 & \iota \end{pmatrix}$. Here we get $\varepsilon \begin{pmatrix} -\alpha \\ \iota \end{pmatrix} = \begin{pmatrix} -\alpha \\ \iota \end{pmatrix}$. So now there is no monodromy for both $z^\#$ and $w^\#$. Again we can find γ in Γ_λ with $\gamma - \iota$ invertible, and it follows that α lies in $M_2(\mathbf{Q})$. Thus the Main Lemma implies $z^\# = w^\# = 0$ identically.

Now multiplying $(z, w) = (f, g)\alpha$ by a denominator before exponentiating, we find this time that both P and Q in (2.1) are torsion, a worse contradiction than before. The proof is complete.

Finally we can prove that the functions f, g, z, w are algebraically independent over $\mathbf{C}$ on N_*.

Let A be any complex polynomial such that $A(\mathbf{t}) = 0$ on N_*, where $\mathbf{t} = (f, g, z, w)$. Then the monodromy using any ε in $E(\mathbf{Z})$ yields also $A(\mathbf{t}\varepsilon) = 0$. Let us specialize to some point on N_* where f, g, z, w take non-zero values f_0, g_0, z_0, w_0. We obtain $A(\mathbf{t}_0\varepsilon) = 0$ for $\mathbf{t}_0 = (f_0, g_0, z_0, w_0)$ and all ε in $E(\mathbf{Z})$. This therefore holds also for all ε in the Zariski closure $E(\mathbf{C})$. However it is easy to see from Lemma A.5 that the resulting $\mathbf{t}_0\varepsilon$ are Zariski dense in $\mathbf{C}^4$. Thus $A = 0$ and the result follows.

Appendix B

We prove here (11.11) for (11.3); along the way we are entitled to assume (11.2), (11.8) and (11.9).

If $n' \le (2\check{D})^7$ then we immediately get (11.3) with the better bounds

$$q = n_P = \frac{n_P}{n'} n' \le (2\check{D})^9, \quad p = n_Q = \frac{n_Q}{n'} n' \le (2\check{D})^9.$$

Otherwise, if $n' > (2\check{D})^7$ then $L = (2\check{D})^{-7/2}\sqrt{n'} > 1$ and we can find integers k, l with

$$1 \le l \le L, \quad \left| \frac{p'}{n'} - \frac{k}{l} \right| \le \frac{1}{lL}.$$

Writing

$$m = p'l - n'k, \quad p'' = \frac{n_Q}{n'} m, \quad q'' = lq' \frac{n_Q}{n'}$$

we find that

$$q''\check{P} = lq' \frac{n_Q}{n'} \check{P} = lp' \frac{n_Q}{n'} \check{Q} = (lp' - kn') \frac{n_Q}{n'} \check{Q} = p''\check{Q}$$

is yet another relation (11.3). But now it is unlikely that either of

$$|q''| \le (2\check{D})^{11/2}\sqrt{n'}, \quad |p''| \le (2\check{D})^{11/2}\sqrt{n'}$$

are bounded; however they are both small relative to n'.

We see anyway that the point $R = (\check{P}, \check{Q})$ on $\check{E}_j \times \check{E}_j$ lies in the one-dimensional algebraic subgroup $G = G(q'', p'')$ defined by $q''\check{P} = p''\check{Q}$. Thanks to (11.1) it also lies on a subvariety Z_1, also one-dimensional, defined by $\check{F} = 0$. Both G and Z_1 are

defined over $\mathbf{Q}(j)$. Replacing Z_1 by some component containing R, we may assume that Z_1 is irreducible over $\mathbf{Q}(j)$.

First assume that Z_1 is not a component of G over $\mathbf{Q}(j)$. Then $Z_0 = G \cap Z_1$ is a finite set of cardinality at most $\deg G \deg Z_1$, where the degree is taken with respect to the Segre embedding of $\mathbf{P}_2 \times \mathbf{P}_2$ in $\mathbf{P}_8$. It is well-known that

$$\deg G \;=\; 3(q''^2 + p''^2) \;\le\; 6(2\check{D})^{11}n'.$$

The identity here must be classical, but it is also a special case of Theorem B.1 of the Ph.D. Thesis [13, pp. 70–71] of Liebendörfer; see also Theorem 5.1 of her paper [14, p. 561] with Rémond for the most general results in this direction. Further Z_1 is a component of a variety defined by the polynomial $\check{F}$ which still has degree at most $\check{D}$ in $\mathbf{P}_8$, together with the quadratic Plücker equations of $\mathbf{P}_2 \times \mathbf{P}_2$ in $\mathbf{P}_8$ and the two cubic equations defining $\check{E}_j \times \check{E}_j$ in $\mathbf{P}_2 \times \mathbf{P}_2$. It follows from some form of Bezout that

$$\deg Z_1 \;\le\; 3^2 2^4 \check{D} \;=\; 72(2\check{D})$$

(see for example Theorem II of [15, p. 419] with $r = 0, n = 8, D = 1, s = 7$). So there are at most $432(2\check{D})^{12}n'$ points in Z_0.

On the other hand Z_0 contains all conjugates R^σ of R over $\mathbf{Q}(j)$. There are at least $\phi_2(n_P)$ different R^σ; hence

$$\frac{6}{\pi^2}n'^2 \;\le\; \frac{6}{\pi^2}n_P^2 \;<\; \phi_2(n_P) \;\le\; 432(2\check{D})^{12}n'.$$

So $n' < 72\pi^2(2\check{D})^{12}$. And now we get (11.3) with

$$q = n_P = \frac{n_P}{n'}n' < 72\pi^2(2\check{D})^{14}, \quad p = n_Q = \frac{n_Q}{n'}n' < 72\pi^2(2\check{D})^{14}$$

as desired in (11.11)

What if Z_1 is a component of G over $\mathbf{Q}(j)$? The components over $\mathbf{C}$ are well-known to be translations of the neutral component G_0 over $\mathbf{C}$ by torsion points. And G_0 is defined by $q_0\check{P} = p_0\check{Q}$ with $q_0 = \frac{q''}{n''}$, $p_0 = \frac{p''}{n''}$ and $n'' = \mathrm{hcf}\{q'', p''\}$. Thus each component G_S of G over $\mathbf{C}$ is defined by $q_0\check{P} - p_0\check{Q} = S$ for torsion S in $\check{E}_j$. So Z_1 is a finite union of G_S. Let s be the largest order of any S here appearing. Then for every σ in $GL_2(\mathbf{Z}/s\mathbf{Z})$ the G_{S^σ} is a component over $\mathbf{C}$ of Z_1. Again there are exactly $\phi_2(s)$ different G_{S^σ} for fixed S. And the degrees of these G_{S^σ} are reasonably well-known to be the same and equal to the degree $3(q_0^2 + p_0^2)$ of G_0. See for example Lemme 2 of Moreau's paper [18, p. 192] and Proposition 2.3 of Roy's article [22, p. 172]. This time it follows that

$$\frac{18}{\pi^2}((q_0 s)^2 + (p_0 s)^2) \;<\; 3(q_0^2 + p_0^2)\phi_2(s) \;\le\; 6\deg Z_1 \;\le\; 432(2\check{D}).$$

And finally R lies in some $G_{S'}$ with S' of order $s' \leq s$, and so we get (11.3), even with

$$|q| = |q_0|_{s'} < 5\pi(2\check{D})^{1/2}, \quad |p| = |p_0|_{s'} < 5\pi(2\check{D})^{1/2}.$$

This completes the proof of (11.11).

References

1. Bertrand, D.: Extensions de D-modules et groupes de Galois différentiels. In: Springer Lecture Notes, vol. 1454, pp. 125–141 (1990)
2. Bierstone, E., Milman, P.: Semianalytic and subanalytic sets. Pub. Math. I.H.E.S. **67**, 5–42 (1988)
3. Bombieri, E., Masser, D., Zannier, U.: Finiteness results for multiplicatively dependent points on complex curves. Mich. Math. J. **51**, 451–466 (2003)
4. Bombieri, E., Masser, D., Zannier, U.: On unlikely intersections of complex varieties with tori. Acta Arith. **133**, 309–323 (2008)
5. Cox, A., Zucker, S.: Intersection numbers of sections of elliptic surfaces. Invent. Math. **53**, 1–44 (1979)
6. Danilov, V.I.: Algebraic varieties and schemes. In: Shafarevich, I.R. Algebraic Geometry I. Encyclopaedia of Mathematical Sciences, vol. 23, Springer-Verlag, New York (1994)
7. David, S.: Points de petite hauteur sur les courbes elliptiques. J. Number Theory **64**, 104–129 (1997)
8. Husemöller, D.: Elliptic Curves. Springer-Verlag, New York (1987)
9. Lang, S.: Elliptic Functions. Addison-Wesley, Reading (1973)
10. Lang, S.: Complex Analysis. Addison-Wesley, Reading (1977)
11. Lang, S.: Fundamentals of Diophantine Geometry. Springer-Verlag, New York (1983)
12. Lang, S.: Algebra. Addison-Wesley, New York (1993)
13. Liebendörfer, C.: Linear equations and heights over division algebras. Ph.D. thesis, Basel (2002)
14. Liebendörfer, C., Rémond, G.: Hauteurs de sous-espaces sur les corps non commutatifs. Math. Z. **255**, 549–577 (2007)
15. Masser, D., Wüstholz, G.: Fields of large transcendence degree generated by values of elliptic functions. Invent. Math. **72**, 407–464 (1983)
16. Masser, D., Zannier, U.: Torsion anomalous points and families of elliptic curves. C. R. Acad. Sci. Paris, Ser. I **346**, 491–494 (2008)
17. Masser, D., Zannier, U.: Torsion anomalous points and families of elliptic curves. Am. J. Math. 132, 1677–1691 (2010)
18. Moreau, J.-C.: Démonstrations géometriques de lemmes de zéros II. In: Bertrand, D., Waldschmidt, M. Approximations diophantiennes et nombres transcendants, Progress in Math 31., pp. 191–197. Birkhäuser, Basel (1983)
19. Pila, J.: Integer points on the dilation of a subanalytic surface. Q. J. Math. **55**, 207–223 (2004)
20. Pila, J., Zannier, U.: Rational points in periodic analytic sets and the Manin-Mumford conjecture. Rendiconti Lincei Mat. Appl. **19**, 149–162 (2008)
21. Pink, R.: A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang. Manuscript dated 17th April 2005
22. Roy, D.: Zero estimates on commutative algebraic groups. In: Nesterenko, Y., Philippon, P. (eds.) Introduction to Algebraic Independence Theory. Lecture Notes, vol. 1752, pp. 167–185. Springer, New York (2001)
23. Shiota, M.: Geometry of subanalytic and semialgebraic sets. In: Progress in Mathematics, vol. 150. Birkhäuser, Basel (1997)
24. Silverman, J.H.: Heights and the specialization map for families of abelian varieties. J. Reine Angew. Math. **342**, 197–211 (1983)
25. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer-Verlag, New York (1986)
26. Zilber, B.: Exponential sums equations and the Schanuel conjecture. J. Lond. Math. Soc. **65**, 27–44 (2002)