JOURNAL de Théorie des Nombres de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

David MASSER et Umberto ZANNIER

**Bicyclotomic polynomials and impossible intersections**

Tome 25, n° 3 (2013), p. 635-659.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_3_635_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **25** (2013), 635–659

# Bicyclotomic polynomials and impossible intersections

par David MASSER et Umberto ZANNIER

Résumé. Nous avons déjà démontré qu'il n'existe qu'un nombre fini de nombres complexes $t \neq 0, 1$ tels que les points $(2, \sqrt{2(2-t)})$ et $(3, \sqrt{6(3-t)})$ soient d'ordre fini sur la courbe elliptique de Legendre définie par $y^2 = x(x-1)(x-t)$. Nous avons généralisé ensuite ce résultat aux couples de points algébriques quelconques sur $\mathbf{C}(t)$. Nous revenons ici aux points $(u, \sqrt{u(u-1)(u-t)})$ et $(v, \sqrt{v(v-1)(v-t)})$ avec des nombres complexes $u$ et $v$ quelconques.

Abstract. In a recent paper we proved that there are at most finitely many complex numbers $t \neq 0, 1$ such that the points $(2, \sqrt{2(2-t)})$ and $(3, \sqrt{6(3-t)})$ are both torsion on the Legendre elliptic curve defined by $y^2 = x(x-1)(x-t)$. In a sequel we gave a generalization to any two points with coordinates algebraic over the field $\mathbf{Q}(t)$ and even over $\mathbf{C}(t)$. Here we reconsider the special case $(u, \sqrt{u(u-1)(u-t)})$ and $(v, \sqrt{v(v-1)(v-t)})$ with complex numbers $u$ and $v$.

## 1. Introduction

Motivated by recent work on unlikely intersections, we proved in [6] (see also [5] for a short version) the finiteness of the set of complex numbers $t \neq 0, 1$ such that the points

$$(2, \sqrt{2(2-t)}),\ (3, \sqrt{6(3-t)}) \tag{1.1}$$

both have finite order on the elliptic curve $E_t$ defined by $y^2 = x(x-1)(x-t)$.

The presenter (J-P. Serre) of [5] wondered what happens when the abscissas $2, 3$ are replaced by any two distinct complex numbers $u, v$. In fact we had already noted that our method is capable of some extension, and in [7] we generalized the result to any abscissas defined over an algebraic closure of $\mathbf{C}(t)$; of course then the ordinates are also defined over this closure. See also the discussion in section III.4 of [14].

Manuscrit reçu le 1er septembre 2011.
*Classification math.* 11G05, 14H52.

In this note we return to the question of the presenter; thus we take complex numbers $u, v$ and we investigate the set $\mathcal{T} = \mathcal{T}(u, v)$ of all complex $t \neq 0, 1$ such that the points

$$P = (u, \sqrt{u(u-1)(u-t)}),\ Q = (v, \sqrt{v(v-1)(v-t)}) \tag{1.2}$$

both have finite order.

In fact the presenter's question was much more detailed. He considered the transcendence degree $\delta = \delta(u, v)$ of $\mathbf{Q}(u, v)$ over $\mathbf{Q}$ and asked separately about the cases $\delta = 0, 1, 2$. We consider each case in turn.

In general the results of [7] imply that $\mathcal{T}(u, v)$ is at most finite except when there is a relation

$$qP = pQ \tag{1.3}$$

holding identically in $t$, where $p, q$ are integers not both zero. Actually (1.3) is a considerable restriction. We can note that $P$ is defined over an extension of $\mathbf{Q}(t)$ ramified at $t = u$, and similarly $Q$ at $t = v$. So as soon as $u \neq v$ we conclude $2qP = 2pQ = 0$ also identically. But as soon as $u \neq 0, 1$ we note as well that $P$ is defined over an extension ramified outside $t = 0, 1$ and so cannot be torsion. Thus $q = 0$; and a similar argument for $Q$ shows that $p = 0$ as soon as $v \neq 0, 1$. Thus (1.3) can hold only if $u = 0, 1$ or $v = 0, 1$ or $u = v$. In fact these cases were already excluded by our presenter.

So if we too exclude these cases from now on, by means of

$$uv(u-1)(v-1)(u-v) \neq 0, \tag{1.4}$$

then $\mathcal{T}(u, v)$ is at most finite.

The case $\delta = 0$ means that $u, v$ are both algebraic. But then the proof of finiteness relies on certain estimates of Pila [8] whose effectivity is not clear (see however his recent work [9]), and so we still cannot effectively compute $\mathcal{T}$, even in the original case (1.1).

The case $\delta = 2$ means that $u, v$ are algebraically independent. Then, as suspected by the presenter, things are very much easier. Indeed a simple argument shows that $\mathcal{T}(u, v)$ is empty. For it is well-known that multiplication by a positive integer $n$ is given by sending $(x, y)$ to

$$\left( \frac{A_n(x,t)}{B_n(x,t)},\ y_n \right), \tag{1.5}$$

where $A_n(X, T), B_n(X, T)$ are polynomials in $\mathbf{Q}[X, T]$ depending only on $n$. Further we can normalize to

$$A_n(X, T) = X^{n^2} + \cdots, \quad B_n(X, T) = n^2 X^{n^2-1} + \cdots \tag{1.6}$$

where the remaining terms have smaller degree in $X$.

It follows that if $P$ in (1.2) is torsion then $B_n(u,t)=0$ so $u$ is algebraic over $\mathbf{Q}(t)$; and similarly with $Q$ that $v$ is algebraic over $\mathbf{Q}(t)$. But then $u,v$ cannot be algebraically independent over $\mathbf{Q}$.

It is the halfway case $\delta=1$ which we will study in this note. In fact no fewer than five different techniques can be used.

Firstly this case can be quickly deduced fron Raynaud's Theorem [10] applied to a curve in $E_T\times E_T$ over the function field $\mathbf{Q}(T)$.

Secondly we can specialize $t$ as Raynaud did, even ending up on a curve in $E_\tau\times E_\tau$ for a fixed algebraic $\tau$; our situation is of course considerably simpler than his.

Thirdly we can specialize rather $u$ and $v$ to algebraic numbers thus reaching the case $\delta=0$. However the details are not so straightforward and new ideas are needed to avoid collapsing in the specialization procedure. Similar problems were solved in [1] using *abc* techniques. Here we have to use some stability properties of Néron-Tate heights on an elliptic threefold together with some upper bounds for values of points on a elliptic surface.

In fact the effectivity of the above three techniques is not quite clear, and so we give a fourth alternative which shows not only that $\mathcal{T}(u,v)$ is usually empty, but also that when it is not empty then it can be effectively found in terms of the unique polynomial relation connecting $u$ and $v$. Here is a more precise statement.

**Theorem 1.** *For each positive integer $d$ there is an effectively computable finite set $\mathcal{F}_d$ of polynomials in $\mathbf{Q}[U,V]$, irreducible over $\mathbf{Q}$ and of degree $d$, with the following property. Suppose $u,v$ in* (1.4) *are complex numbers, not both algebraic over $\mathbf{Q}$, and algebraically dependent over $\mathbf{Q}$ through a polynomial over $\mathbf{Q}$ irreducible over $\mathbf{Q}$ of degree $d$. Then the set $\mathcal{T}(u,v)$ is effectively computable. If further $F(u,v)\neq 0$ for every $F$ in $\mathcal{F}_d$, then the set $\mathcal{T}(u,v)$ is empty.*

For example, the cardinality of $\mathcal{T}(u,v)$ is at most $6(12d)^{32}$ and that of $\mathcal{F}_d$ is at most $200(12d)^{33}$. The proof will make the rest of the effectivity clear.

A variant of the method enables us to strengthen the result by replacing $\mathbf{Q}$ throughout by its algebraic closure $\overline{\mathbf{Q}}$. We postpone the statement and its proof to an Appendix.

When $d=1$ in Theorem 1 we go further by proving that $\mathcal{F}_1$ can be taken to consist of just $U+V$ and $U+V-2$. This implies the following.

**Theorem 2.** *Suppose $u, v$ in (1.4) are complex numbers, not both algebraic over $\mathbf{Q}$, with $1, u, v$ linearly dependent over $\mathbf{Q}$ but $u + v \neq 0,\ u + v \neq 2$. Then the set $\mathcal{T}(u, v)$ is empty.*

For example there are no complex numbers $t \neq 0, 1$ such that

$$(2\pi, \sqrt{2\pi(2\pi - 1)(2\pi - t)}),\ (3\pi, \sqrt{3\pi(3\pi - 1)(3\pi - t)})$$

have finite order on $E_t$. Already in [7] we showed that there are at most $10^{40}$.

We may note that $u + v = 0, 2$ are genuine exceptions, coming from $4P = 4Q = 0$ on the elliptic curve $E_t$ for $t = u^2, 2u - u^2$. They reflect the fact that the points with abscissas $\pm\sqrt{T}, 1 \pm \sqrt{1 - T}$ have order 4 on $E_T$.

More non-empty $\mathcal{F}_d$ can be found by taking $rP = sQ = 0$ for various integers $r, s$.

For example $(r, s) = (2, 4)$ and the above points of order 4 as well as that with abscissa $T \pm \sqrt{T^2 - T}$ lead to the following relations

$$v^2 - u = 0,\ v^2 - 2v + u = 0,\ v^2 - 2uv + u = 0\ (t = u)$$

corresponding to elements of $\mathcal{F}_2$. Or $(r, s) = (4, 4)$ also to

$$u^2 + v^2 - 2v = 0\ (t = u^2)$$

also of $\mathcal{F}_2$, as well as

$$2u^2v - u^2 - v^2 = 0\ (t = u^2),$$

$$2u^2v - u^2 - 4uv + v^2 + 2u = 0\ (t = 2u - u^2)$$

of $\mathcal{F}_3$. Or $(r, s) = (2, 3)$ gives

$$4uv^3 - 3v^4 - 6uv^2 + 4v^3 + u^2 = 0\ (t = u)$$

of $\mathcal{F}_4$. Or $(r, s) = (2, 6)$ gives three relations

$$v^4 + 4u^2v - 6uv^2 - 3u^2 + 4uv = 0,\ v^4 - 4u^2v + 6uv^2 - 4v^3 + u^2 = 0,$$

$$v^4 - 4uv^3 + 6uv^2 + u^2 - 4uv = 0$$

with $t = u$ also of $\mathcal{F}_4$. Or $(r, s) = (4, 3)$ gives two relations

$$4u^2v^3 + u^4 - 6u^2v^2 - 3v^4 + 4v^3 = 0\ (t = u^2)$$

$$4u^2v^3 - u^4 - 6u^2v^2 - 8uv^3 + 3v^4 + 4u^3 + 12uv^2 - 4v^3 - 4u^2 = 0\ (t = 2u - u^2)$$

of $\mathcal{F}_5$ and finally

$$8u^3v^3 - 12u^2v^4 - 12u^3v^2 + 12u^2v^3 + 12uv^4 + u^4 + 6u^2v^2 - 16uv^3 - 3v^4 + 4v^3 = 0$$

$(t = \frac{u^2}{2u-1})$ of $\mathcal{F}_6$. But perhaps $\mathcal{F}_7$ may be empty.

We will prove Theorem 1 by extending the arguments of sections 10, 11, 12, 13 of [7] about the generic Galois groups of the fields generated

by torsion points. But for the proof of Theorem 2 we need to identify the actual minimal polynomials of the abscissas of these points. These are essentially the irreducible factors of the $B_n(X,T)$ in (1.6), which may be considered as elliptic analogues of the cyclotomic factors of $X^n-1$. We take the liberty of calling these bicyclotomic polynomials; the adjective can refer not only to the variables $X,T$ instead of $X$, but also to the underlying groups $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/n\mathbf{Z}$ instead of $\mathbf{Z}/n\mathbf{Z}$. We also need to know the next two terms in (1.6) as well as those also for the irreducible factors. All this will be carried out in section 2, and we prove Theorem 2 in section 3. It is convenient then to give the proof of Theorem 1 in section 4.

We then present the simple deduction from Raynaud's Theorem in section 5, together with the specialization argument for $t$. However we postpone until a later work the more difficult argument for $u,v$, which will actually be carried out in the more general context of the product of two different elliptic curves; for the moment we content ourselves with a sketch.

Then in section 6 we give a list of the bicyclotomic polynomials of low degree, and in section 7 we make a couple of remarks on the $(A,B)$ model defined by $y^2=x^3+Ax+B$.

Finally in an Appendix we state and prove the stronger form of Theorem 1.

We heartily thank Professor J-P. Serre for his care in presenting [5], which led to the results of the present paper.

## 2. Bicyclotomic polynomials

The cyclotomic polynomials are of course the irreducible factors of $X^n-1$ over $\mathbf{Q}$. Here we consider the Legendre elliptic analogues to be those of $B_n=B_n(X,T)$; thus the curve $y^2=x(x-1)(x-T)$ provides an additional variable. It will turn out that they are irreducible even over $\mathbf{C}$.

It is known that $B_n(X,T)/n^2$ for $n\geq 2$ is the product of $X-x$ taken over the abscissas $x$ of all non-zero points of order dividing $n$.

There are at least two reasons why $B_n$ is not irreducible. One is simply because a point and its inverse have the same abscissa, so $B_n$ is essentially a perfect square. The other is due to the points of each fixed order $d$ dividing $n$. This leads to the following first attempt at describing the irreducible factors.

For $n\geq 2$ we define $B_n^*=B_n^*(X,T)$ as the product of $X-x$ taken over all distinct abscissas $x$ of points of order exactly $n$ multiplied further by a leading coefficient. For $n\geq 3$ this is $e^{\Lambda(n)}$, where $\Lambda$ is the von Mangoldt

function, but for $n = 2$ it is 4. For example $B_2^*(X,T) = 4X(X-1)(X-T)$; and it suits us to define also $B_1^*(X,T) = 1$. For $n \geq 3$ the degree with respect to $X$ is $\frac{1}{2}\phi_2(n)$, where

$$\phi_2(n) \;=\; n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) \;=\; n^2 \sum_{d|n} \frac{\mu(d)}{d^2}.$$

Thus we have for $n$ odd

$$B_n(X,T) \;=\; \prod_{d|n} B_d^*(X,T)^2, \tag{2.1}$$

and we will soon see that the factors $B_d^*(X,T)$ $(d \neq 1)$ here are all irreducible. And for $n$ even

$$B_n(X,T) \;=\; B_2^*(X,T) \prod_{2 \neq d|n} B_d^*(X,T)^2;$$

however the irreducibility here is not such a simple matter, as the example $B_2^*(X,T)$ shows. But we will see that the $B_d^*(X,T)$ here are irreducible for all odd $d \neq 1$.

Now Möbius Inversion of (2.1) and the subsequent formula gives

$$B_n^*(X,T)^2 \;=\; \prod_{d|n} B_d(X,T)^{\mu(n/d)} \tag{2.2}$$

for all $n \geq 3$, whether odd or even.

Now for even $n$ there is a more subtle reason why $B_n^*$ is not irreducible. Namely if $P$ has order $n = 2m$ then $mP$ is one of the three points

$$Q^{(0)} = (0,0),\; Q^{(1)} = (1,0),\; Q^{(\infty)} = (T,0)$$

of order 2; and these are of course all rational over $\mathbf{Q}(T)$. Thus for even $n = 2m$ we define $B_n^{(0)}(X,T), B_n^{(1)}(X,T), B_n^{(\infty)}(X,T)$ as the products of $X - x$ taken over all distinct abscissas $x$ of points $P$ of order exactly $n$ with $mP = Q^{(0)}, Q^{(1)}, Q^{(\infty)}$ respectively. Here it is natural to take monic polynomials. Their degrees are $\frac{1}{6}\phi_2(n)$ if $n \neq 2$; and of course

$$B_2^{(0)}(X,T) = X,\; B_2^{(1)}(X,T) = X - 1,\; B_2^{(\infty)}(X,T) = X - T.$$

Thus for even $n \neq 2$ we have

$$B_n^*(X,T) \;=\; e^{\Lambda(n)} B_n^{(0)}(X,T) B_n^{(1)}(X,T) B_n^{(\infty)}(X,T),$$

and we will next see that all the factors here are irreducible. This will mean that

$$4X(X-1)(X-T)\prod_{2\neq d|n,\ d\ \text{odd}} B_d^*(X,T)^2 \prod_{2\neq d|n,\ d\ \text{even}} B_d^{(0)}(X,T)^2 B_d^{(1)}(X,T)^2 B_d^{(\infty)}(X,T)^2$$

gives the irreducible factorization of $B_n(X,T)$ for even $n$.

Here follows the irreducibility result for these bicyclotomic polynomials.

**Lemma 2.1.** *The polynomials*

$$B_n^*(X,T) \quad (\textit{odd } n \neq 1)$$

*and*

$$B_n^{(0)}(X,T), B_n^{(1)}(X,T), B_n^{(\infty)}(X,T) \quad (\textit{even } n)$$

*are irreducible over* $\mathbf{Q}$.

*Proof.* Suppose first that $n$ is odd, and let $x$ be the abscissa of a point of order exactly $n$ on $E_T$. We will show that $x$ has degree $\frac{1}{2}\phi_2(n)$ over $\mathbf{Q}(T)$. As $B_n^*(x,T)=0$ gives an equation of this degree, the irreducibility over $\mathbf{Q}$ follows.

We need a model over $\mathbf{Q}(j)$ with as usual

$$j \;=\; 256\frac{(T^2-T+1)^3}{T^2(1-T)^2},$$

which as in [7] we take as $\check{E}_j$ defined by

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

with

$$\check{x} = \chi^2(x - \frac{1}{3}(T+1)),\ \check{y} = 2\chi^3 y \tag{2.3}$$

where $\chi$ is anything with

$$\chi^2 \;=\; 9\frac{T^2-T+1}{(T-2)(T+1)(2T-1)}.$$

As $\chi^2$ is in $\mathbf{Q}(T)$, it suffices to show that $\check{x}$ has degree $\frac{1}{2}\phi_2(n)$ over $\mathbf{Q}(T)$.

Write $K_N$ for the field generated over $K=\mathbf{Q}(j)$ by the set $\check{E}_j[N]$ of points of order dividing $N$ on $\check{E}_j$, so that $K_2=\mathbf{Q}(T)$. We know from Lemma 10.1 of [7] that $K_{2n}/K$ has group $GL_2(\mathbf{Z}/2n\mathbf{Z})$. So the group of $K_{2n}/K_2$ is the subgroup of elements congruent to the identity mod 2. This subgroup injects into $GL_2(\mathbf{Z}/n\mathbf{Z})$ via reduction mod $n$, because 2 and $n$

are coprime. The injection is surjective; so the group of $K_{2n}/K_2$ may be identified with $GL_2(\mathbf{Z}/n\mathbf{Z})$. Now a point $(\check{x},\check{y})$ of order $n$ in $\check{E}_j[2n]$ has stabilizer of size $n\phi_1(n) = n^2\prod_{p|n}(1-\frac{1}{p})$. So the number of conjugates over $K_2$ is this size divided into the size $n\phi_1(n)\phi_2(n)$ of $GL_2(\mathbf{Z}/n\mathbf{Z})$. Hence we get precisely $\phi_2(n)$ different conjugates of $(\check{x},\check{y})$. Each comes with its inverse (distinct as $n \neq 2$), and so we get $\frac{1}{2}\phi_2(n)$ conjugates of $\check{x}$ as needed.

Next suppose that $n$ is even. There is then no need for $K_{2n}$, and similar arguments show that the group of $K_n/K_2$ is the kernel of the reduction of $GL_2(\mathbf{Z}/n\mathbf{Z})$ mod 2. Now this has size $\frac{1}{6}n\phi_1(n)\phi_2(n)$. And now a point of order $n$ has stabilizer of size $\frac{1}{2}n\phi_1(n)$; for example we get the set of all $\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}$ with $b$ congruent to 0 mod 2 and $d$ congruent to 1 mod 2. The latter is automatically implied by $(d,n)=1$, and the former gives $\frac{1}{2}n$ values. So we get $\frac{1}{3}\phi_2(n)$ conjugates for $(\check{x},\check{y})$, leading as before to $\frac{1}{6}\phi_2(n)$ conjugates for $\check{x}$ provided $n \neq 2$. As this is the common degree of $B_n^{(0)}, B_n^{(1)}, B_n^{(\infty)}$ the proof is complete. □

The irreducibility over $\mathbf{C}$ (which we do not need in this paper) may be proved in a similar way using instead Corollary 2 of [3] (p.69) which involves $SL_2$. Then all the above sizes get divided by $\phi_1(n)$. See also the Appendix below.

Next we calculate some terms of these bicyclotomic polynomials.

We start with a few more terms in (1.6). We could not find these in the classical literature, either for the Weierstrass model $y^2 = 4x^3 - g_2x - g_3$ or the model $y^2 = x^3 + Ax + B$ used in [12] (pp. 105, 202).

**Lemma 2.2.** *We have*

$$A_n(X,T) = X^{n^2} - \frac{1}{6}n^2(n^2-1)TX^{n^2-2} + \frac{1}{45}n^2(n^2-1)(n^2-4)(T^2+T)X^{n^2-3} + \cdots$$

*(so no term in $X^{n^2-1}$),*

$$B_n(X,T) = n^2X^{n^2-1} - \frac{1}{3}n^2(n^2-1)(T+1)X^{n^2-2} + \frac{1}{90}n^2(n^2-1)\left(a_nT^2+b_nT+a_n\right)X^{n^2-3} + \cdots,$$

*where $a_n = 4n^2-16$, $b_n = 11n^2-14$ and the remaining terms have smaller degree in $X$. Further the term in $A_n(X,T)$ of smallest degree in $X$ is $n^2T^{(n^2-1)/2}X$ ($n$ odd) and $T^{n^2/2}$ ($n$ even).*

*Finally*

$$\begin{aligned} A_n(1-X,1-T) &= (-1)^n(A_n(X,T)-B_n(X,T)),\\ B_n(1-X,1-T) &= -(-1)^nB_n(X,T),\\ T^{n^2}A_n(T^{-1}X,T^{-1}) &= A_n(X,T),\\ T^{n^2-1}B_n(T^{-1}X,T^{-1}) &= B_n(X,T). \end{aligned}$$

*Proof.* It is natural to define also $A_0(X,T)=1, B_0(X,T)=0$. Using the addition law to evaluate $n(X,Y)\pm(X,Y)$ as in [12] (p.216) we get the recurrence relations

$$A_{n-1}A_{n+1}=(XA_n-TB_n)^2,\ B_{n-1}B_{n+1}=(A_n-XB_n)^2 \tag{2.4}$$

for $A_n=A_n(X,T),\ B_n=B_n(X,T)$.

Already the first of these shows with a simple induction that $A_n$ has no term in $X^{n^2-1}$ (alternatively the analogous assertion for the Weierstrass model is a consequence of the fact that there is no non-zero modular form of weight 2, and then (2.3) - see also section 7 - implies it for Legendre).

Writing therefore

$$A_n=X^{n^2}+\alpha'_nX^{n^2-2}+\alpha''_nX^{n^2-3}+\cdots,$$

$$B_n=n^2(X^{n^2-1}+\beta'_nX^{n^2-2}+\beta''_nX^{n^2-3}+\cdots)$$

with $\alpha'_n,\alpha''_n,\beta'_n,\beta''_n$ in $\mathbf{Q}[T]$ we deduce from (2.4)

$$\alpha'_{n-1}+\alpha'_{n+1}=2(\alpha'_n-n^2T),\ \alpha''_{n-1}+\alpha''_{n+1}=2(\alpha''_n-n^2\beta'_nT),$$

$$(n^2-1)(\beta'_{n-1}+\beta'_{n+1})=2n^2\beta'_n,$$

$$(n^2-1)^2(\beta''_{n-1}+\beta''_{n+1}+\beta'_{n-1}\beta'_{n+1})=n^4\beta'^2_n-2(n^2-1)(\alpha'_n-n^2\beta''_n);$$

all for $n=1,2,3,\ldots$. These make it clear that $\alpha'_{n+1},\alpha''_{n+1},\beta'_{n+1},\beta''_{n+1}$ are determined by $\alpha'_{n-1},\alpha''_{n-1},\beta'_{n-1},\beta''_{n-1}$ and $\alpha'_n,\alpha''_n,\beta'_n,\beta''_n$, and the expansions now follow with a somewhat tedious induction.

We use a similar procedure to find the last terms of $A_n$, except that we must load the induction with the last terms of $B_n$, which are $T^{(n^2-1)/2}$ ($n$ odd) and $n^2T^{(n^2-2)/2}X$ ($n$ even).

Finally the last four identities.

We note that the equation $Y^2=X(X-1)(X-T)$ is the same as $\tilde{Y}^2=\tilde{X}(\tilde{X}-1)(\tilde{X}-\tilde{T})$ with $\tilde{X}=1-X,\tilde{Y}=iY$ and $\tilde{T}=1-T$. This yields a map $\varphi$ from $E_T$ to $E_{1-T}$ which is necessarily a group homomorphism; and now $\varphi(n(X,Y))=n\varphi(X,Y)$ means that $1-\frac{A_n(X,T)}{B_n(X,T)}=\frac{A_n(\tilde{X},\tilde{T})}{B_n(\tilde{X},\tilde{T})}$. Looking at the highest power of $X$ gives the first two identities.

A similar argument with $\tilde{X} = T^{-1}X,\ \tilde{Y} = T^{-3/2}Y$ and $\tilde{T} = T^{-1}$ from $E_T$ to $E_{1/T}$ completes the proof of the present lemma. We may remark that the last of the identities shows that $B_n(X,T)$ has degree at most $n^2-1$ in $T$. □

We may also note that

$$A_{n-1}B_{n+1}+A_{n+1}B_{n-1} \ = \ 2XA_n^2+(2X^2+2T-4TX-4X)A_nB_n+2TXB_n^2.$$

This can be combined with (2.4) to show that all $A_n(X,T), B_n(X,T)$ actually lie in $\mathbf{Z}[X,T]$, a fact not obvious from the model $y^2 = x^3 + Ax + B$ used in [12] because the transition between the two models involves a denominator 3 as in (2.3) above. We will not need this fact here.

We will now obtain the analogues of (2.2) for $B_n^{(0)}, B_n^{(1)}, B_n^{(\infty)}$ for even $n = 2m$. We write $n = 2^\nu n_1$ with $n_1$ odd and $\nu \geq 1$. Then

$$A_m(X,T) \ = \ \prod_{d_1|n_1} B^{(0)}_{nd_1/n_1}(X,T)^2 \quad (n \neq 2). \tag{2.5}$$

This is because the zeroes of the left-hand side are the abscissas of the $P$ with $mP = Q^{(0)}$. So the order of $P$ divides $2m = n = 2^\nu n_1$; however the order must be divisible by $2^\nu$ otherwise we would have $mP = 0$. So the possible orders are $2^\nu d_1 = nd_1/n_1$ as in (2.5). Now Inversion gives

$$B_n^{(0)}(X,T)^2 \ = \ \prod_{d_1|n_1} A_{md_1/n_1}(X,T)^{\mu(n_1/d_1)} \ (n \neq 2). \tag{2.6}$$

Similarly we get

$$A_m(X,T) - B_m(X,T) \ = \ \prod_{d_1|n_1} B^{(1)}_{nd_1/n_1}(X,T)^2 \ (n \neq 2)$$

with inverse

$$B_n^{(1)}(X,T)^2 = \prod_{d_1|n_1} \Big(A_{md_1/n_1}(X,T) - B_{md_1/n_1}(X,T)\Big)^{\mu(n_1/d_1)} \quad (n \neq 2), \tag{2.7}$$

and

$$A_m(X,T) - TB_m(X,T) \ = \ \prod_{d_1|n_1} B^{(\infty)}_{nd_1/n_1}(X,T)^2 \ (n \neq 2)$$

with inverse

$$B_n^{(\infty)}(X,T)^2 = \prod_{d_1|n_1} \Big(A_{md_1/n_1}(X,T) - TB_{md_1/n_1}(X,T)\Big)^{\mu(n_1/d_1)} \quad (n \neq 2). \tag{2.8}$$

We write

$$\phi_4(n) = n^4 \prod_{p|n} \left(1 - \frac{1}{p^4}\right) = n^4 \sum_{d|n} \frac{\mu(d)}{d^4},$$

$$\phi_6(n) = n^6 \prod_{p|n} \left(1 - \frac{1}{p^6}\right) = n^6 \sum_{d|n} \frac{\mu(d)}{d^6}$$

for yet more analogues of Euler's phi function. We also define

$$\psi(n) = -2\phi_4(n) + 5\phi_2(n)^2 - 20\phi_2(n),\ \chi(n) = 2\phi_4(n) + 10\phi_2(n)^2 - 10\phi_2(n),$$
$$\omega(n) = \phi_6(n) - 21\phi_4(n) + 84\phi_2(n),\ \theta(n) = 2\phi_4(n) - 10\phi_2(n).$$

**Lemma 2.3.** *For odd $n \neq 1$ we have*

$$e^{-\Lambda(n)} B_n^*(X,T) = X^{\phi_2(n)/2} - \frac{1}{6}\phi_2(n)(T+1)X^{\phi_2(n)/2-1} + \frac{1}{360}(\psi(n)T^2 + \chi(n)T + \psi(n))X^{\phi_2(n)/2-2} + \cdots$$

*For even $n \neq 2$ we have*

$$B_n^{(0)}(X,T) = X^{\phi_2(n)/6} - \frac{1}{360}\theta(n)TX^{\phi_2(n)/6-2} + \frac{1}{5670}\omega(n)(T^2+T)X^{\phi_2(n)/6-3} + \cdots$$

*(so no term in $X^{\phi_2(n)/6-1}$), and*

$$B_n^{(1)}(X,T) = X^{\phi_2(n)/6} - \frac{1}{6}\phi_2(n)X^{\phi_2(n)/6-1} + \frac{1}{360}(\theta(n)T + \psi(n))X^{\phi_2(n)/6-2} + \cdots,$$

$$B_n^{(\infty)}(X,T) = X^{\phi_2(n)/6} - \frac{1}{6}\phi_2(n)TX^{\phi_2(n)/6-1} + \frac{1}{360}(\psi(n)T^2 + \theta(n)T)X^{\phi_2(n)/6-2} + \cdots,$$

*and the remaining terms have smaller degree in $X$. Further the term in $B_n^{(0)}(X,T)$ of smallest degree in $X$ is $\pm e^{\Lambda(m)}T^{\phi_2(n)/12}$ ($m$ odd) and $\pm T^{\phi_2(n)/12}$ ($m$ even). Finally*

$$B_n^{(0)}(1-X, 1-T) \ = \ B_n^{(1)}(X,T). \tag{2.9}$$

*Proof.* To get at $B_n^{(0)}(X,T)$ we take (2.6) and we substitute the expansions in Lemma 2.2 for the various $A_n$ after taking out the highest power of $X$ as a factor. We evaluate the products using a formal Laurent series identity

$$\prod_{d \in \mathcal{D}} \left(1 + \frac{u_d}{X^2} + \frac{v_d}{X^3} + \cdots\right)^{m_d} \ = \ 1 + \frac{U}{X^2} + \frac{V}{X^3} + \cdots$$

with

$$U = \sum_{d\in\mathcal{D}} m_d u_d,\ V = \sum_{d\in\mathcal{D}} m_d v_d$$

and a finite set $\mathcal{D}$. This in turn is checked for example by taking logarithms and then exponentiating. The terms of smallest degree in $B_n^{(0)}(X,T)$ are much easier to handle.

To prove (2.9), at least up to sign, we compare (2.6), (2.7) using Lemma 2.2. The sign follows from the fact that $\frac{1}{6}\phi_2(n)$ is even.

This enables us to deduce the expansion of $B_n^{(1)}$ from that of $B_n^{(0)}$. And similarly comparing (2.7), (2.8) gives

$$T^{\phi_2(n)/6} B_n^{(1)}(T^{-1}X, T^{-1}) \ = \ B_n^{(\infty)}(X,T)$$

which leads to the expansion of $B_n^{(\infty)}$.

For $B_n^*(X,T)$ we argue similarly with (2.2) but with slightly more tedious calculations based on

$$\prod_{d\in\mathcal{D}} \left(1 + \frac{u_d}{X} + \frac{v_d}{X^2} + \cdots\right)^{m_d} \ = \ 1 + \frac{U}{X} + \frac{2V + U^2 - W}{2X^2} + \cdots$$

with $U, V$ as above and $W = \sum_{d\in\mathcal{D}} m_d u_d^2$. This completes the proof.

We may also note that the $B_n^*(X,T), B_n^{(0)}(X,T), B_n^{(1)}(X,T), B_n^{(\infty)}(X,T)$ also lie in $\mathbf{Z}[X,T]$; but again we will not need this fact here.

## 3. Proof of Theorem 2

We start with a preliminary result.

**Proposition 3.1.** *Suppose that $a \neq 0, b, c \neq 0$ are rational numbers with $(a,b) \neq (1,0)$, and let $r \neq 1, s \neq 1$ be positive integers such that*

$$cB_r^?(X,T) \ = \ B_s^{??}(aX+b,T) \tag{3.1}$$

*where the symbols $?, ??$ represent superscripts $*, (0), (1), (\infty)$ restricted as in Lemma 2.1. Then the only possibilities are*

$$\begin{aligned}
aB_2^{(0)}(X,T) \ &= \ B_2^{(1)}(aX+1,T),\\
aB_2^{(0)}(X,T) \ &= \ B_2^{(0)}(aX,T),\\
B_4^{(0)}(X,T) \ &= \ B_4^{(0)}(-X,T),\\
aB_2^{(1)}(X,T) \ &= \ B_2^{(1)}(aX+1-a,T),\\
B_4^{(1)}(X,T) \ &= \ B_4^{(1)}(-X+2,T).
\end{aligned}$$

*Proof.* By symmetry there are ten cases for the ordered pair $(?, ??)$. We take these in increasing level of difficulty and we beg forgiveness for further tediousness. At any rate the first six are relatively easy.

1. $(*, *)$. Now in (3.1) it suffices to take

$$B_r^*(X,T) \;=\; e^{\Lambda(r)}(X^R - \frac{1}{3}R(T+1)X^{R-1} + \cdots) \tag{3.2}$$

$$B_s^*(X,T) \;=\; e^{\Lambda(s)}(X^S - \frac{1}{3}S(T+1)X^{S-1} + \cdots)$$

with $R = \phi_2(r)/2,\ S = \phi_2(s)/2$. We find first $R = S = N$ (say). However the resulting equation $\phi_2(r) = \phi_2(s)$ seems too reminiscent of Carmichael's Conjecture to be useful. But also

$$ce^{\Lambda(r)} = a^N e^{\Lambda(s)},$$

$$-\frac{1}{3}ce^{\Lambda(r)}N(T+1) \;=\; e^{\Lambda(s)}(Na^{N-1}b - \frac{1}{3}Na^{N-1}(T+1)).$$

Eliminating $ce^{\Lambda(r)-\Lambda(s)}$ and then equating coefficients of powers of $T$ leads quickly to the excluded case $a = 1, b = 0$.

2. $(*, (0))$. The case $s = 2$ is easily settled. Otherwise we take (3.2) together with

$$B_s^{(0)}(X,T) \;=\; X^S + 0.X^{S-1} + \cdots \tag{3.3}$$

this time with $S = \phi_2(s)/6$; and a similar procedure gives at once the contradiction $a = 0$.

3. $(*, (1))$. Again we can take (3.2) with

$$B_s^{(1)}(X,T) \;=\; X^S - SX^{S-1} + \cdots \tag{3.4}$$

and $S = \phi_2(s)/6$; and a similar procedure gives again the contradiction $a = 0$.

4. $((0), (\infty))$. The cases $r = 2$ or $s = 2$ are easily settled. Otherwise the analogue of (3.3) for $B_r^{(0)}$ with

$$B_s^{(\infty)}(X,T) \;=\; X^S - STX^{S-1} + \cdots \tag{3.5}$$

again leads to $a = 0$.

5. $((1), (\infty))$. A similar procedure with (3.4) and (3.5) leads to a more blatant contradiction.

6. $((\infty), (\infty))$. Now (3.5) leads again to the excluded $a = 1, b = 0$.

7. $(*,(\infty))$. The case $s=2$ is easily settled. Otherwise a similar use of (3.2) and (3.5) with $R=\phi_2(r)/2, S=\phi_2(s)/6$ leads to $a=3, b=-1$, so far no contradiction. Also $R=S=N$ and $c=3^N e^{-\Lambda(r)}$. Thus (3.1) becomes

$$3^N e^{-\Lambda(r)} B_r^*(X,T) \;=\; B_s^{(\infty)}(3X-1,T).$$

Now we use all the terms in Lemma 2.3 for $B_r^*$ and $B_s^{(\infty)}$. We equate coefficients of $X^{N-2}$ and then coefficients of $T^2$ and $T^0$. We get a double appearance of $\frac{1}{40}\psi(r)$, the first time being $\frac{1}{360}\psi(s)$ and the second time being $\frac{1}{2}N(N-1)$. Eliminating $\psi(r)$ gives after a short calculation and a slightly surprising cancellation the equation $\phi_4(s)=5\phi_2(s)$. This is quickly solved; clearly

$$\frac{90}{\pi^4}s^4 = \frac{1}{\zeta(4)}s^4 < \phi_4(s) = 5\phi_2(s) < 5s^2$$

a contradiction for $s\neq 2$.

8. $((0),(1))$. The case $r=2$ or $s=2$ leads quickly to the first displayed possibility. Otherwise from (3.3) and (3.4) we get $b=1$, also no contradiction. But using two terms of $B_r^{(0)}$ and three terms of $B_s^{(1)}$ in Lemma 2.3 and equating coefficients of $T^0$ leads to the same $\phi_4(s)=5\phi_2(s)$.

9. $((0),(0))$. The case $r=2$ or $s=2$ leads to the second displayed possibility. Otherwise from (3.3) we get $R=S=N,\ c=a^N$, and $b=0$. To find $a$ we look at the terms of smallest degree in $X$.

If $r/2, s/2$ are both even, we get $c=\pm 1$ and so $a=\pm 1$. And if $r/2, s/2$ are both odd we get $c=\pm e^{\Lambda(s/2)}/e^{\Lambda(r/2)}$. If $a\neq\pm 1$ then the height of $c=a^N$ is at least $2^N$; but $\pm e^{\Lambda(s/2)}/e^{\Lambda(r/2)}$ has height at most $\max\{r/2, s/2\}$. If for example $r\leq s$ then we get $2^S\leq s/2$ which leads easily back to $r=s=2$; and similarly if $r\geq s$. So $a=\pm 1$ here too; and the same conclusion follows with the other parities of $r/2, s/2$.

As $b=0$ in fact $a=-1$ and $c=(-1)^N$. Finally considering just the signs of the coefficients of $X^{N-3}$ in $cB_r^{(0)}(X,T)=B_s^{(0)}(-X,T)$ gives the contradictory $c=-(-1)^N$ provided $\omega(r)>0$ and $\omega(s)>0$. In fact $\omega(n)>0$ for all even $n\neq 2$ apart from $\omega(4)=0$; this leads to the third displayed possibility.

10. $((1),(1))$. Now $cB_r^{(1)}(X,T)=B_s^{(1)}(aX+b,T)$ can be written using Lemma 2.3 as $cB_r^{(0)}(\tilde X,\tilde T)=B_s^{(0)}(\tilde a\tilde X+\tilde b,\tilde T)$ for

$$\tilde X = 1-X,\ \tilde T = 1-T,\ \tilde a = a,\ \tilde b = 1-a-b$$

with $(\tilde a,\tilde b)\neq(1,0)$. Then the previous case leads to the fourth and fifth displayed possibilities.

We can now prove Theorem 2. But first we remark that in the general case $\delta = 1$ both $u$ and $v$ must be transcendental over $\mathbf{Q}$ if $\mathcal{T}(u, v)$ is non-empty. For example if $u$ is algebraic over $\mathbf{Q}$ then $P$ being torsion would imply that $t$ is algebraic over $\mathbf{Q}$ otherwise $P$ would be identically torsion contradicting the ramification $(u \neq 0, 1)$. But then $Q$ being torsion would imply that $v$ too is algebraic over $\mathbf{Q}$.

Thus our linear relation takes the form $v = au + b$ for rational $a \neq 0, b$. Suppose $P = (u, \sqrt{u(u-1)(u-t)})$ has exact order $r \neq 1$ and $Q = (v, \sqrt{v(v-1)(v-t)})$ has exact order $s \neq 1$. Then we have

$$0 = B_r^?(u, t),\ 0 = B_s^{??}(v, t) = B_s^{??}(au + b, t)$$

where $?, ??$ are taken from the set $\{*, (0), (1), (\infty)\}$. Now the equations

$$B_r^?(X, T) \ = \ B_s^{??}(aX + b, T) \ = \ 0$$

must define a variety with at least one curve component, else $u$ would be algebraic over $\mathbf{Q}$. This implies by the irreducibility in Lemma 2.1 an identity (3.1) for rational $c \neq 0$.

Now $(a, b) \neq (1, 0)$ otherwise $u = v$ which is forbidden by (1.4). So Proposition 3.1 implies that $r = s = 2$ or $r = s = 4$. In the first case $u = 0, 1, t$ and $v = 0, 1, t$; however these too are forbidden by (1.4). In the second case we find $u + v = 0$ or $u + v = 2$. This proves Theorem 2.

## 4. Proof of Theorem 1

There is a non-zero polynomial $F_0(U, V)$ in $\mathbf{Q}[U, V]$, irreducible over $\mathbf{Q}$ of degree $d$, such that

$$F_0(u, v) = 0. \tag{4.1}$$

We are in the situation of the Proposition of [7] section 2, with the curve $C$ parametrized in affine $\mathbf{A}^5$ by

$$(u, \sqrt{u(u-1)(u-t)}, v, \sqrt{v(v-1)(v-t)}, t)$$

as $t$ varies. So $C$ is defined over $\mathcal{K} = \mathbf{Q}(u, v)$. In [7] section 13 we took $W_{\mathcal{K}}$ in $\mathbf{A}^7$ parametrized by

$$(u, \sqrt{u(u-1)(u-t)}, v, \sqrt{v(v-1)(v-t)}, t, u, v)$$

as $t, u, v$ vary subject only to (4.1). This is a surface defined over $\mathbf{Q}$. We took $W_0$ as the projection to $\mathbf{A}^3$ parametrized by $(u, v, t)$. This is also a surface, of degree at most $D_0 = d$. Now go back to the original complex numbers $u, v, t$ with $P, Q$ torsion on $E_t$. The arguments of [7], in particular

equation (13.2) there, yield integers $p, q$, possibly depending on $t$, with (1.3) and

$$0 < \max\{|p|, |q|\} < (12D_0)^8 = (12d)^8 = M.$$

By (1.5) this leads to an equation

$$C_{pq}(u, v, t) = 0$$

with

$$C_{pq}(U, V, T) \;=\; A_q(U, T)B_p(V, T) - A_p(V, T)B_q(U, T)$$

and $A_n, B_n$ suitably defined for $n \leq 0$ as in [7] section 14.

Now the polynomial $C_{pq}(u, v, T)$ cannot be identically zero in $T$, otherwise (1.3) would hold identically, which we have excluded with (1.4). This leads at once to the estimate for the cardinality of $\mathcal{T}(u, v)$. Namely $C_{pq}(u, v, T)$ has degree at most $p^2 + q^2 - 1 \leq 2M^2$ in $T$, so for such $(p, q)$ there are at most $2M^2$ values of $t$. This would give at most $2M^2(2M+1)^2 < 6(12d)^{32}$ in all, as was to be proved.

But how do we extract the set $\mathcal{F}_d$?

We already remarked in the preceding section that both of $u$ and $v$ must be transcendental over $\mathbf{Q}$. This means that $F_0(U, V)$ must involve both $U$ and $V$. A similar argument (without ramification) shows that $t$ must be transcendental over $\mathbf{Q}$.

We claim that in fact $P$ has order $r < \pi(12d)^{17/2}$.

Suppose first that $C_{pq}(U, V, T)$ does not involve $V$. Then we get an equation $C(u, t) = 0$, which must involve $u$ because $t$ is transcendental over $\mathbf{Q}$. It follows that $[\mathbf{Q}(u, t) : \mathbf{Q}(t)] \leq 2M^2$. But also $B_r^?(u, t) = 0$ where the symbol ? represents superscripts $*, (0), (1), (\infty)$ restricted as in Lemma 2.1, and it follows that $2M^2 \geq \frac{1}{6}\phi_2(r) > \frac{1}{6}\frac{1}{\zeta(2)}r^2 = \frac{1}{\pi^2}r^2$. This leads to $r < \pi\sqrt{2M^2} = \pi\sqrt{2}(12d)^8$ better than we claimed.

If $C_{pq}(U, V, T)$ does involve $V$, then the resultant $G(U, T)$ of $F_0(U, V)$ and $C_{pq}(U, V, T)$ with respect to $V$ is defined.

If this resultant were identically zero, then the two polynomials would have a non-trivial common factor $D(U, V, T)$ in $\mathbf{Q}[U, V, T]$. As this divides $F_0(U, V)$ it must be independent of $T$ and in fact identical with $F_0(U, V)$ up to constants. So $F_0(U, V)$ would divide $C_{pq}(U, V, T)$. However as $p, q$ vary, these $C_{pq}(U, V, T)$ have up to constants at most finitely many divisors of degree $d$ (and probably none independent of $T$), and so it suffices to include those irreducible ones (independent of $T$) among the set $\mathcal{F}_d$.

Thus we can assume that $G(U,T)$ is not identically zero. Now the equation $G(u,t)=0$ shows as above that $P$ has order at most $\pi\sqrt{N}$, where $N$ is the degree of $G$. Clearly $N \leq 4dM^2 < (12d)^{17}$ and so our claim follows.

Of course the same argument applies to $Q$. There are thus positive integers $r$ and $s$, both at most $\pi(12d)^{17/2}$, such that

$$B_r(u,t) = B_s(v,t) = 0.$$

Both $B_r(U,T)$ and $B_s(V,T)$ must involve $T$ (again ramification), so their resultant $H(U,V)$ with respect to $T$ is defined. Again it is non-zero, this time because a common factor would have to be independent of both $V$ and $U$ and so in $\mathbf{Q}[T]$; however this is absurd because there can be no algebraic (or even complex) number $t_0$ with $B_r(U,t_0) = B_s(V,t_0) = 0$ from (1.6).

And now $H(u,v) = 0$ shows that it suffices also to include in $\mathcal{F}_d$ all irreducible factors of $H(U,V)$ of degree $d$ up to constants. Using the remark immediately following the proof of Lemma 2.2 we find that the degree of $H$ is at most $2r^2s^2 \leq 2\pi^4(12d)^{34}$, so it can have at most $2\pi^4(12d)^{33} < 200(12d)^{33}$ such factors.

Finally it is now clear how to compute everything effectively.

## 5. Specialization

It is easy to deduce the case $\delta = 1$ from Raynaud's work. Suppose the complex number $t \neq 0, 1$ is such that $P$ and $Q$ in (1.2) are both torsion. Then $t$ is transcendental over $\mathbf{Q}$ otherwise $u$ and $v$ would both be in $\overline{\mathbf{Q}}$. So there is an isomorphism $\sigma$ from $\mathbf{Q}(t)$ to some field $\mathcal{F}$ independent of $t$. We can extend to a bigger field containing also the coordinates of $P$ and $Q$. Then $\sigma(P)$ and $\sigma(Q)$ are torsion on $E_{\sigma(t)}$ and $(\sigma(P), \sigma(Q))$ lies on a fixed curve, even defined over $\mathbf{Q}$, on $A = E_{\sigma(t)} \times E_{\sigma(t)}$ defined over $\mathcal{F}$. We are therefore in the situation of Manin-Mumford over the fixed field $\mathcal{F}$.

Now $\sigma$ applied to (1.4) and the discussion around (1.3) shows that $q\sigma(P) \neq p\sigma(Q)$ for any integers $p$ and $q$ not both zero. It follows from Raynaud's Theorem 1 (p. 207 but also p.226) of [10] that the number of $(\sigma(P), \sigma(Q))$ is at most finite. So $\sigma(P)$ and $\sigma(Q)$ have orders bounded above independently of $t$. So also $P$ and $Q$, which leads to the desired finiteness of the set of complex numbers $t$.

Using our bicyclotomic polynomials (which imply standard properties of good reduction) we can specialize $t$ to some algebraic $\tau$ and thus reduce to Manin-Mumford over $\overline{\mathbf{Q}}$.

Namely as in section 4 there is a non-zero polynomial $F_0$ over $\mathbf{Q}$, irreducible over $\mathbf{Q}$, such that $F_0(u,v) = 0$. We start by finding an algebraic

(and even rational) $\tau$ such that the curve $F_0 = 0$ relating the abscissas on $E_\tau \times E_\tau$ does not have any one-dimensional torsion translate as a component.

For such a torsion translate is defined by an equation $q\tilde{P} - p\tilde{Q} = R$ with a torsion point $R$. By considering geometric degrees we can easily bound $|q|, |p|$ and then assume them fixed. Now we can choose algebraic $u_0, v_0$ with $F_0(u_0, v_0) = 0$ but

$$u_0 v_0 (u_0 - 1)(v_0 - 1)(u_0 - v_0) \neq 0$$

as in (1.4). Then

$$R(t) = q(u_0, \sqrt{u_0(u_0 - 1)(u_0 - t)}) - p(v_0, \sqrt{v_0(v_0 - 1)(v_0 - t)})$$

cannot be identically torsion, say of order $n$, on $E_t$ by (1.4) and the discussion around (1.3) after multiplying by $n$. It now suffices to find $\tau$ such that $R(\tau)$ is not torsion on $E_\tau$. This can be done for example by appealing to Silverman's Theorem to the effect that an inadmissible $\tau$ has bounded height; or we could also use the results of [4] implying that such $\tau$ are sparse.

Having found $\tau$, suppose now the complex number $t \neq 0, 1$ is such that $P$ has exact order $r \neq 1$ and $Q$ has exact order $s \neq 1$. Then we have

$$B_r^?(u, t) = B_s^{??}(v, t) = 0 \tag{5.1}$$

as in section 3. Consider the variety with coordinates $(U, W, V, Z, T)$ in $\mathbf{A}^5$ subject to

$$F_0(U, V) = B_r^?(U, T) = B_s^{??}(V, T) = 0$$

and of course

$$W^2 = U(U - 1)(U - T), \; Z^2 = V(V - 1)(V - T).$$

It is clearly of dimension at most 1 defined over $\mathbf{Q}$ containing the point $\Pi = (u, w, v, z, t)$, where $w = \sqrt{u(u-1)(u-t)}$, $z = \sqrt{v(v-1)(v-t)}$; and the transcendence of $t$ noted above shows that it has at least one curve component $\mathcal{C}_{rs}$ also containing $\Pi$. We are going to specialize $\Pi$ over $\overline{\mathbf{Q}}$ in the sense of [13] (p.26). This requires a little care, as it lies on the variety $\mathcal{C}_{rs}$ depending on the unknown $r, s$.

But we can certainly start by specializing $t$ to $\tau$.

Next by (5.1) $u, v$ and so $w, z$ are integral over $\mathbf{Q}[t]$. So by Proposition 22 of [13] (p. 41) we can indeed specialize $(u, w, v, z, t)$ to some $(u_{rs}, w_{rs}, v_{rs}, z_{rs}, \tau)$. In particular on $E_\tau$ the point $(u_{rs}, w_{rs})$ still has order $r$ and the point $(v_{rs}, z_{rs})$ still has order $s$. Further $F_0(u_{rs}, v_{rs}) = 0$. From the choice of $\tau$ we conclude that $r$ and $s$ are bounded and this implies the finiteness of the original set of $t$ as desired.

We finish this section with a brief sketch of how to specialize $u$ and $v$ rather than $t$.

We follow the preceding argument until the curve $\mathcal{C}_{rs}$. From the irreducibility of $B_r^?, B_s^{??}$ it can be seen that the degree $\Delta_{rs}$ of $\mathcal{C}_{rs}$ is at least $\delta(r^2+s^2)-c$; here and elsewhere $\delta, c$ denote positive absolute constants.

We intersect $\mathcal{C}_{rs}$ with a hyperplane $H_\lambda$ defined by $U=\lambda T$. For generic $\lambda$ there will be $\Delta_{rs}$ different intersection points. However we wish to choose non-generic $\lambda$ and indeed some fixed $\lambda$ independent of $r$ and $s$. But then there could be fewer intersection points.

We can resolve this by noting that $B_r(U,T)=0$ on $\mathcal{C}_{rs}$ and so $B_r(\lambda T,T)=0$ on the intersection. For generic $\lambda$ this latter polynomial has degree $\Delta_r \geq \delta r^2 - c$. Now an argument based on the stability (or uniformity) of values of the functional Néron-Tate height on a family of elliptic surfaces shows that the degree of $B_r(\lambda T,T)$ is at least $\Delta_r - c$ for all $\lambda$ outside a finite set independent of $r$. It follows that for such $\lambda$ the set $\mathcal{C}_{rs}\cap H_\lambda$ has at least $\Delta_{rs}-c$ points counted with multiplicity. We fix such a $\lambda$.

Another argument based on Wang's proof of the effective Roth theorem for function fields shows that the multiplicities of zeroes of $B_r(\lambda T,T)$ are at most $\epsilon r^2 + C$, where $C$ depends only on the arbitrary $\epsilon > 0$.

It follows that for any $N$ the set $\mathcal{C}_{rs}\cap H_\lambda$ has at least $N$ different points provided $r$ and $s$ are sufficiently large with respect to $N$. These take the form $\Pi_t=(\lambda t, w_t, v_t, z_t, t)$ with fixed algebraic functions $w_t, v_t, z_t$ of $t$. So we have found many $t$ with the points $(\lambda t, w_t), (v_t, z_t)$ both torsion on $E_t$. But this can be made to contradict the finiteness result of [7].

A variation on this argument is to note that if our result for transcendence degree 1 is false, then there exist infinitely many pairs $(r,s)$ above. Now for each such $(r,s)$ we can find at least one $\Pi_t$ ($t=t_{rs}\neq 0,1$) on $\mathcal{C}_{rs}\cap H_\lambda$ (for this we still need the effective Roth argument). Clearly for different $(r,s)$ the $t_{rs}$ are different, and we conclude as above.

Yet another variation enables us to reduce directly to the case $\delta=0$. One can show as in the proof of Lemma 2.3 that the degree of $B_n^*(X,T)$ in $T$ is $\frac{1}{4}\phi_2(n)$ for odd $n\neq 1$, and that the degrees of $B_n^{(0)}(X,T), B_n^{(1)}(X,T)$, $B_n^{(\infty)}(X,T)$ in $T$ are $\frac{1}{12}\phi_2(n)$ for even $n\neq 2$. We now intersect with $U=\lambda$ in a similar way, leading to many $t$ with $(\lambda, \sqrt{\lambda(\lambda-1)(\lambda-t)})$, $(\mu, \sqrt{\mu(\mu-1)(\mu-t)})$ both torsion, where $F_0(\lambda,\mu)=0$.

## 6. Examples

Here, for the possible amusement of the reader, we exhibit here some of the shorter polynomials.

First, the $B_n = B_n(X,T)$ (usually reducible), for convenience together with the $A_n = A_n(X,T)$ for $n = 1, 2, 3$.

Of course $A_1 = X, B_1 = 1$. Then

$$A_2 = X^4 - 2TX^2 + T^2,\ B_2 = 4X^3 - (4T+4)X^2 + 4TX,$$

$$A_3 = X^9 - 12TX^7 + (8T^2+8T)X^6 + 30T^2X^5 - (48T^2+48T^3)X^4 + (16T^4+68T^3+16T^2)X^3 - (24T^4+24T^3)X^2 + 9T^4X,$$

$$B_3 = 9X^8 - (24T+24)X^7 + (16T^2+68T+16)X^6 - (48T^2+48T)X^5 + 30T^2X^4 + (8T^3+8T^2)X^3 - 12T^3X^2 + T^4.$$

Then the irreducible $B_n^* = B_n^*(X,T)$ for $n = 1, 3, 5$.

Again $B_1^* = 1$. Then

$$B_3^* = 3X^4 - 4(T+1)X^3 + 6TX^2 - T^2,$$

$$B_5^* = 5X^{12} - (20T+20)X^{11} + (16T^2+94T+16)X^{10} - (80T^2+80T)X^9 - 105T^2X^8 + (360T^3+360T^2)X^7 - (240T^4+780T^3+240T^2)X^6 + (64T^5+560T^4+560T^3+64T^2)X^5 - (160T^5+445T^4+160T^3)X^4 + (140T^5+140T^4)X^3 - 50T^5X^2 + T^6.$$

Finally the irreducible $B_n^{(0)} = B_n^{(0)}(X,T),\ B_n^{(1)} = B_n^{(1)}(X,T),\ B_n^{(\infty)} = B_n^{(\infty)}(X,T),$ for $n = 2, 4, 6, 8, 10$.

Now $B_2^{(0)} = X, B_2^{(1)} = X - 1, B_2^{(\infty)} = X - T$. Then

$$B_4^{(0)} = X^2 - T,\ B_4^{(1)} = X^2 - 2X + T,\ B_4^{(\infty)} = X^2 - 2TX + T,$$

$$B_6^{(0)} = X^4 - 6TX^2 + (4T^2+4T)X - 3T^2,$$

$$B_6^{(1)} = X^4 - 4X^3 + 6TX^2 - 4T^2X + T^2,$$

$$B_6^{(\infty)} = X^4 - 4TX^3 + 6TX^2 - 4TX + T^2,$$

$$B_8^{(0)} = X^8 - 20TX^6 + (32T^2+32T)X^5 - (16T^3+58T^2+16T)X^4 + (32T^3+32T^2)X^3 - 20T^3X^2 + T^4,$$

$$B_8^{(1)} = X^8 - 8X^7 + (20T+8)X^6 - (32T^2+24T)X^5 + (16T^3+54T^2)X^4 - (32T^3+24T^2)X^3 + (20T^3+8T^2)X^2 - 8T^3X + T^4,$$

$$B_8^{(\infty)} = X^8 - 8TX^7 + (8T^2+20T)X^6 - (24T^2+32T)X^5 + (54T^2+16T)X^4 - (24T^3+32T^2)X^3 + (8T^4+20T^3)X^2 - 8T^4X + T^4,$$

$B_{10}^{(0)} = X^{12} - 50TX^{10} + (140T^2 + 140T)X^9 - (160T^3 + 445T^2 + 160T)X^8 + (64T^4 + 560T^3 + 560T^2 + 64T)X^7 - (240T^4 + 780T^3 + 240T^2)X^6 + (360T^4 + 360T^3)X^5 - 105T^4X^4 - (80T^5 + 80T^4)X^3 + (16T^6 + 94T^5 + 16T^4)X^2 - (20T^6 + 20T^5)X + 5T^6,$

$B_{10}^{(1)} = X^{12} - 12X^{11} + (50T + 16)X^{10} - (140T^2 + 80T)X^9 + (160T^3 + 335T^2)X^8 - (64T^4 + 464T^3 + 264T^2)X^7 + (208T^4 + 508T^3 + 208T^2)X^6 - (264T^4 + 464T^3 + 64T^2)X^5 + (335T^4 + 160T^3)X^4 - (80T^5 + 140T^4)X^3 + (16T^6 + 50T^5)X^2 - 12T^6X + T^6,$

$B_{10}^{(\infty)} = X^{12} - 12TX^{11} + (16T^2 + 50T)X^{10} - (80T^2 + 140T)X^9 + (335T^2 + 160T)X^8 - (264T^3 + 464T^2 + 64T)X^7 + (208T^4 + 508T^3 + 208T^2)X^6 - (64T^5 + 464T^4 + 264T^3)X^5 + (160T^5 + 335T^4)X^4 - (140T^5 + 80T^4)X^3 + (50T^5 + 16T^4)X^2 - 12T^5X + T^6.$

## 7. The $(A, B)$ model

Here, for the possible convenience of the reader, we exhibit the first few terms of the multiplication polynomials for the model $y^2 = x^3 + Ax + B$. They can be calculated by using weight arguments to see the general forms

$$x^{n^2} + \lambda_n A x^{n^2-2} + \mu_n B x^{n^2-3} + \cdots \tag{7.1}$$

for the numerator and

$$n^2 x^{n^2-1} + \nu_n A x^{n^2-3} + \cdots \tag{7.2}$$

for the denominator, where $\lambda_n, \mu_n, \nu_n$ depend only on $n$. We convert from Legendre $Y^2 = X(X-1)(X-T)$ using

$$x = X - \frac{1}{3}(T+1) \tag{7.3}$$

and we find

$$A = -\frac{1}{3}(T^2 - T + 1),\ B = -\frac{1}{27}(T+1)(T-2)(2T-1). \tag{7.4}$$

We substitute (7.3) and (7.4) into (7.1) and (7.2), compare with the first part of Lemma 2.2, not forgetting to translate back with an extra $\frac{1}{3}(T+1)$, and equate some coefficients to find the values of $\lambda_n, \mu_n, \nu_n$. We find

$$\lambda_n = -\frac{1}{6}n^2(n^2-1),\ \mu_n = -\frac{2}{15}n^2(n^4-1),\ \nu_n = \frac{1}{30}n^2(n^2-1)(n^2+6).$$

## 8. Appendix

Here we strengthen Theorem 1 as follows.

**Theorem** $\overline{1}$. *For each positive integer $d$ there is an effectively computable finite set $\overline{\mathcal{F}}_d$ of polynomials in $\overline{\mathbf{Q}}[U,V]$, irreducible over $\overline{\mathbf{Q}}$ and of degree $d$, with the following property. Suppose $u, v$ in* (1.4) *are complex numbers, not both algebraic over $\overline{\mathbf{Q}}$, and algebraically dependent over $\overline{\mathbf{Q}}$ through a polynomial over $\overline{\mathbf{Q}}$ irreducible over $\overline{\mathbf{Q}}$ of degree $d$. Then the set $\mathcal{T}(u,v)$ is effectively computable. If further $F(u,v) \neq 0$ for every $F$ in $\overline{\mathcal{F}}_d$, then the set $\mathcal{T}(u,v)$ is empty.*

*Proof.* This will also show, as for Theorem 1, that the cardinality of $\mathcal{T}(u,v)$ is bounded effectively in terms of $d$. However here we adopt instead a Galois strategy, similar to that for Lang's original problem of curves in $\mathbf{G}_{\mathrm{m}}^2$. This will lead to better estimates.

There is an irreducible relation $F_0(u,v) = 0$, where $F_0$ in $\overline{\mathbf{Q}}[U,V]$ has degree $d$. Let us consider the set $\mathcal{T} = \mathcal{T}(u,v)$ and pick a $t$ in $\mathcal{T}$, letting $r, s$ denote the exact orders of the corresponding points $P, Q$ on $E_t$ with abscissas $u, v$ respectively.

As noted in section 4 above, $t$ is transcendental, like $u, v$; hence as in section 5 we may regard $t$ as an independent variable, with the proviso that then $u, v$ are viewed as certain algebraic functions of $t$, that is, the abscissas of the torsion points $P, Q$ in $E_t(\overline{\mathbf{Q}(t)})$, still of the same orders. We want to prove a bound depending only on $d$ for these orders.

The curve $E_t$ is isomorphic (over $\mathbf{Q}(t)$) to a curve $\check{E}_j$ defined over $\mathbf{Q}(j)$ by a Weierstrass equation as in section 3, with transcendental invariant $j = j(E_t) = 256\frac{(t^2-t+1)^3}{t^2(1-t)^2}$.

Now $\mathbf{Q}(t)$ becomes the field generated over $\mathbf{Q}(j)$ (or even $\mathbf{Q}$) by the 2-torsion on $\check{E}_j$. After this isomorphism, we get torsion points $\check{P}, \check{Q}$ in $\check{E}_j$. The abscissas $\check{u}, \check{v}$ of $\check{P}, \check{Q}$ are also easily expressed as certain linear functions of $u, v$ with coefficients in $\mathbf{Q}(t)$.

These abscissas together with the corresponding ordinates generate over $\mathbf{Q}(j)$ fields contained in modular function fields of levels $r, s$, as explained for example in [3]. As such, these fields are subfields of the corresponding field whose level is the lowest common multiple $k$ of $2, r, s$, denoted here $K_k$; that is, $K_k = \mathbf{Q}(j, \check{E}_j[k])$ is the field generated over $\mathbf{Q}(j)$ by the coordinates of all torsion points on $\check{E}_j$ of order dividing $k$. Now the Galois structure of $K_k/\mathbf{Q}(j)$ is well known to be the maximal possible one. Namely, viewing the $k$-torsion on $\check{E}_j$ as a finite group isomorphic to

$\mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/k\mathbf{Z}$, and viewing the Galois action through its natural representation as a subgroup of $GL_2(\mathbf{Z}/k\mathbf{Z})$, we know that the Galois image is in fact the whole group $GL_2(\mathbf{Z}/k\mathbf{Z})$ (see also Lemma 10.1 of [7]). Moreover, by Corollary 1(ii),(iii) of [3] (p.68), the Galois group of $\overline{\mathbf{Q}}(j, \check{E}_j[k])$ over $\overline{\mathbf{Q}}(j)$ corresponds to $SL_2(\mathbf{Z}/k\mathbf{Z})$.

The original equation $F_0(u, v) = 0$ relating the abscissas of the points on $E_t$ yields a similar equation $\check{F}_0(\check{u}, \check{v}, t) = 0$, where $\check{F}_0(U, V, t)$ in $\overline{\mathbf{Q}}(t)[U, V]$ again has degree $d$ in $U, V$. This equation yields a curve $C$ in $\check{E}_j \times \check{E}_j$, defined over $\overline{\mathbf{Q}}(t)$. Note that this curve $C$ is possibly reducible, but since $\check{F}_0$ defines an irreducible (over $\overline{\mathbf{Q}}$) curve in the $(U, V)$-plane, it gives rise to at most four components in $\check{E}_j \times \check{E}_j$: in fact, $C$ is the inverse image of the plane curve $\check{F}_0 = 0$, through the $\check{x} \times \check{x}$-map, of degree 4, from $\check{E}_j \times \check{E}_j$ to projective $\mathbf{P}_1 \times \mathbf{P}_1$. Also, if $Z$ is an irreducible component of $C$, then every other component is obtained as the image of $Z$ by some automorphism $[\pm 1] \times [\pm 1]$ of $\check{E}_j \times \check{E}_j$, where $[n]$ denotes multiplication by $n$.

Let us now use the Galois group over $\mathbf{Q}(t)$ of the modular function field $K_k$ of level $k$; this Galois group is represented as the subgroup $\Gamma$ of $GL_2(\mathbf{Z}/k\mathbf{Z})$ of index 6 consisting of the matrices congruent to the identity (mod 2), and so it contains all $[\ell]$ with $\ell$ prime to $k$.

And the Galois group $Gal(\overline{\mathbf{Q}}(j, \check{E}_j[k])/\overline{\mathbf{Q}}(t))$ is $\Omega = \Gamma \cap SL_2(\mathbf{Z}/k\mathbf{Z})$, also of index 6 in $SL_2(\mathbf{Z}/k\mathbf{Z})$. Hence if $g$ is in $\Omega$, then $g$ fixes a field of definition for $C$, so $C^g = C$.

Take now $\ell > 1$ be prime to $k$ and let us extend $[\ell]$ to an automorphism of $\overline{\mathbf{Q}(t)}$ over $\mathbf{Q}(t)$. If $L$ is a (Galois) number field such that $F_0, \check{F}_0, C$ are defined over $L(t)$, suppose that this automorphism acts on $L$ as $\sigma$ in $Gal(L/\mathbf{Q})$. (It may happen that this $\sigma$ is not uniquely determined by $\ell$.)

Then for all $g$ in $\Omega$ we have

$$(\check{P}^g, \check{Q}^g) \in C, \qquad (\ell\check{P}^g, \ell\check{Q}^g) \in C^\sigma. \tag{8.1}$$

We note that the stabilizer in $SL_2(\mathbf{Z}/n\mathbf{Z})$ of a point of order $n$ has size $n$. This follows as in the proof of Lemma 10.1 of [7]; the Euler function $\phi_1$ there drops out. Thus the orbit of the point under $SL_2(\mathbf{Z}/n\mathbf{Z})$ has size $\phi_2(n) = n^2 \prod_{p|n}(1 - \frac{1}{p^2}) > \frac{6}{\pi^2} n^2$, just as in Lemma 10.1; this is behind the irreducibility of the polynomials $B_n^?(X, T)$ in Lemma 2.1 over $\overline{\mathbf{Q}}$ or $\mathbf{C}$.

We need here the orbit of $(\check{P}, \check{Q})$ under $\Omega$, but this can be found as follows. We work first in $SL_2(\mathbf{Z}/k\mathbf{Z})$, and by the Chinese Remainder Theorem it suffices to work in $SL_2(\mathbf{Z}/p^e\mathbf{Z})$ for each prime power $p^e$ dividing $k$. If $p \neq 2$ then at least one of $\check{P}, \check{Q}$, considered in $(\mathbf{Z}/p^e\mathbf{Z})^2$, has order

$p^e$, and so its stabilizer has size $p^e$. So that of $(\check{P}, \check{Q})$ has size at most $p^e$. If $p = 2$ then at least one of $\check{P}, \check{Q}$, considered in $(\mathbf{Z}/2^e\mathbf{Z})^2$, has order either $2^e$ or $2^{e-1}$. If the former, then the stabilizer in $SL_2(\mathbf{Z}/2^e\mathbf{Z})$ has size $2^e$ as before. But if the latter, then we get $2^{e-1}$ multiplied by the index $[SL_2(\mathbf{Z}/2^e\mathbf{Z}) : SL_2(\mathbf{Z}/2^{e-1}\mathbf{Z})] = 8$, that is $4.2^e$. Multiplying over all primes $p$, we see that the stabilizer of $(\check{P}, \check{Q})$ in $SL_2(\mathbf{Z}/k\mathbf{Z})$ has size at most $4k$. So also in the subgroup $\Omega$; and so the orbit under $\Omega$ has size at least $\frac{k\phi_2(k)/6}{4k} > \frac{k^2}{4\pi^2}$.

Now only two cases can occur.

*I: There is no component common to both $C^\sigma$ and $[\ell]C$.*

Then by Bezout's theorem applied to the projection of these curves to $\mathbf{P}_1 \times \mathbf{P}_1$ (this is a bit simpler than working in $\check{E}_j \times \check{E}_j$) we find that the cardinality of $C^\sigma \cap [\ell]C$ is at most $4d^2\ell^2$, whence, by (8.1) and the above orbit calculations, $k \le 4\pi d\ell$.

If for some real $\lambda \ge 41$ we cannot take $\ell \le \lambda$ then all primes $p \le \lambda$ divide $k$. In particular $\vartheta(\lambda) \le \log k$ in the standard notation of prime number theory. However by the Corollary 3.16 (p.70) of [11] we have $\vartheta(\lambda) > \lambda(1 - \frac{1}{\log \lambda}) > \frac{1}{2}\lambda$. So choosing $\lambda = 41 + 2\log k$ we deduce $\ell \le \lambda$.

It follows that

$$k \;\le\; 4\pi d(41 + 2\log k) \tag{8.2}$$

which is at most $4\pi d(41+4\sqrt{k}) \le 180\pi d\sqrt{k}$. This gives $\log k \le 2\log(180\pi d)$ and then from (8.2)

$$k \;\le\; 4\pi d(41 + 4\log(180\pi d)) \;\le\; 180\pi d \log(180\pi d).$$

In this case the order of torsion is likewise bounded for both points. Each double relation $rP = sQ = 0$ yields, on eliminating $t$ as in section 4, a relation between $u, v$ (nontrivial because the $B_n(X, T)$ are essentially monic in $X$), which possibly gives an element of $\overline{\mathcal{F}}_d$. Clearly only finitely many elements can arise in this way, and they can be computed.

*II: There is a component common to both $C^\sigma$ and $[\ell]C$.*

Let $[\ell]Z$ be such a component, where $Z$ is a component of $C$. We have already noted that every other component is obtained as the image of one of them by some $\mu = [\pm 1] \times [\pm 1]$ on $\check{E}_j \times \check{E}_j$. Then we have $\mu Z^\sigma = [\ell]Z$ for some such $\mu$. Iterating shows that $[\ell^m]Z = Z$ for some $m \ge 1$. But then by general theory $Z$ is a translate by a torsion point of an irreducible algebraic subgroup.

However this would say that the original relation $F_0(u, v) = 0$ defines a union of at most four torsion translates of an algebraic subgroup. In turn, the original points $P, Q$ on $E_t$ with abscissas $u, v$ respectively would be linearly dependent on $E_t$, which we can exclude, for instance by ramification, as in section 1.

This completes the proof. □

**Remark.** It is probably possible to obtain quantitatively better estimates by transposing to this elliptic context the cyclotomic arguments of Beukers and Smyth [2].

## References


[1] E. Bombieri, D. Masser and U. Zannier, *Finiteness results for multiplicatively dependent points on complex curves*, Michigan Math. J. **51** (2003), 451–466.

[2] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number theory for the millennium I (Urbana 2000), A.K. Peters Ltd. (2002), 67–85.

[3] S. Lang, *Elliptic functions*, Addison-Wesley (1973).

[4] D. Masser, *Specializations of finitely generated subgroups of abelian varieties*, Trans. Amer. Math. Soc. **311** (1989), 413–424.

[5] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*. C. R. Acad. Sci. Paris, Ser. I **346** (2008), 491–494.

[6] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), 1677–1691.

[7] D. Masser and U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Annalen **352** (2012), 453–484.

[8] J. Pila, *Integer points on the dilation of a subanalytic surface*, Quart. J. Math. **55** (2004), 207–223.

[9] J. Pila, *Counting rational points on a certain exponential-algebraic surface*, Annales Institut Fourier **60** (2010), 489–514.

[10] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Inventiones Math. **71** (1983), 207–233.

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

[12] J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag (1986).

[13] A. Weil, *Foundations of algebraic geometry*, American Math. Soc. Colloquium Pub. **XXIX** (1946).

[14] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Math. Studies, **181**, Princeton (2012).



David Masser
Mathematisches Institut
Universität Basel, Rheinsprung 21
4051 Basel, Switzerland
*E-mail*: David.Masser@unibas.ch

Umberto Zannier
Scuola Normale, Piazza Cavalieri 7
56126 Pisa, Italy
*E-mail*: u.zannier@sns.it