Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 346 (2008) 491–494

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Number Theory

Torsion anomalous points and families of elliptic curves

David Masser[a], Umberto Zannier[b]

[a] *Mathematisches Institut, Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland*
[b] *Scuola Normale, Piazza Cavalieri 7, 56126 Pisa, Italy*

Received 14 February 2008; accepted 25 March 2008

Available online 21 April 2008

Presented by Jean-Pierre Serre

Abstract

We prove that there are at most finitely many complex $\lambda \neq 0, 1$ such that two points on the Legendre elliptic curve $Y^2 = X(X-1)(X-\lambda)$ with coordinates $X = 2$ and $X = 3$ both have finite order. This is a very special case of some well-known conjectures on unlikely intersections with varying semiabelian varieties. ***To cite this article: D. Masser, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Points de torsion et familles de courbes elliptiques. Comme cas très spécial de certaines conjectures générales sur l'intersection d'une variété algébrique avec la réunion des sous-schémas de dimension fixée d'un schéma semi-abélien, nous montrons qu'il n'existe qu'un nombre fini de $\lambda \in \mathbf{C} \setminus \{0, 1\}$ tels que les quatre points de la courbe elliptique $Y^2 = X(X-1)(X-\lambda)$ avec $X = 2$ et $X = 3$ soient d'ordre fini. ***Pour citer cet article : D. Masser, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

Motivated by recent work on unlikely intersections, we consider here the following question. What can be said about the complex numbers $\lambda \neq 0, 1$ such that the points

$$P_\lambda = \bigl(2, \sqrt{2(2-\lambda)}\bigr), \qquad Q_\lambda = \bigl(3, \sqrt{6(3-\lambda)}\bigr) \tag{1}$$

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

It is not difficult to see that there are infinitely many λ such that P_λ alone has finite order. Reducing if necessary to Weierstrass form, we see that multiplication by n is given by sending X to $\frac{A_n(X)}{B_n(X)}$ for coprime A_n, B_n in $\mathbf{Q}[\lambda][X]$. So the order of P_λ divides n if and only if $B_n(2) = 0$. Now $B_n(2)$ is a polynomial just in λ; for example we can normalize to

$$B_2(2) = \lambda - 2, \quad B_3(2) = (\lambda^2 + 8\lambda - 16)^2, \quad B_4(2) = \lambda^2(\lambda-2)(\lambda-4)^2(3\lambda-4)^2. \tag{2}$$

E-mail addresses: David.Masser@unibas.ch (D. Masser), u.zannier@sns.it (U. Zannier).

1631-073X/$ – see front matter © 2008 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.
doi:10.1016/j.crma.2008.03.024

None of the $B_n(2)$ can vanish identically, else P_λ would have finite order for every λ, which is false, for example with $\lambda = -6$, because then $2P_\lambda = (\frac{25}{16}, -\frac{165}{64})$ which by Lutz–Nagell (see, for example, [4, p. 114]) cannot be torsion. So for each n there is λ (even algebraic) such that P_λ has order dividing n. For example with $\lambda = 4$ we get order 4. And taking n prime, we get a point of exact order n.

However, the resulting values of λ are somewhat sparse. In one sense this follows from a general result of the first author [6]; but in fact in this case a stronger conclusion can be deduced from a result of Silverman [12]. Namely, the absolute Weil height $h(\lambda)$ (see below) is bounded above.

A similar argument with $B_n(3)$ and $\lambda = -21$ with $2Q_\lambda = (\frac{25}{16}, -\frac{285}{64})$ shows that there are infinitely many λ such that Q_λ alone has finite order, with the same conclusions for the height. Thus if the two points are in some sense independent of each other, which looks plausible, then we might expect the intersection of the two sparse sets to be especially sparse and perhaps even finite. This is indeed so.

Theorem. *There are at most finitely many complex numbers $\lambda \neq 0, 1$ such that the points P_λ, Q_λ have finite order on E_λ.*

The above question did not arise from nowhere. In 1999 Bombieri and the present authors [1] studied problems on algebraic curves in powers of the multiplicative group $\mathbf{G}_m$. In 2002 Zilber [13] independently published his conjectures on intersections with tori, which turned out to be generalizations of questions formulated in [1], not only from curves to varieties but also in the context of semiabelian varieties. There the semiabelian varieties were considered fixed. In 2005 Pink [11] independently formulated even more general versions, in particular allowing the semiabelian varieties to vary. The result above is a special example in the simplest unsolved case of a curve in $E_\lambda \times E_\lambda$.

Recently Pila and the second author [10] found a new proof of some classical results of Manin–Mumford type for a fixed Abelian variety A. In order to handle the torsion points, they observe that these map to $\mathbf{Q}^s$ ($s = 2\dim A$) under some choice of the Abelian logarithm. Also, a fixed algebraic subvariety W of A maps to some fixed subvariety Z of $\mathbf{R}^s$ which is usually no longer algebraic but only analytic. Now rational points on analytic or subanalytic sets have been intensively studied in the last few years, starting with Bombieri and Pila [2] for a curve and most recently Pila and Wilkie [9] for arbitrary dimension. Their results say that the number of such points in $\frac{1}{n}\mathbf{Z}^s$ is usually of order at most n^ϵ as n tends to infinity. However there can be obstacles in the shape of semialgebraic subsets of Z.

Anyway, an upper bound for n can be found by noting that a point of order n on W, say of degree d, carries many of its conjugates with it, at least when A and W are defined over a number field. A result of the first author [5], proved using techniques from transcendence theory, states that d has order at least n^δ for some fixed $\delta > 0$ depending only on A. This leads to the appropriate restrictions on the torsion points.

Our own proof follows this general strategy, with $A = E_\lambda \times E_\lambda$ and the torsion point (P_λ, Q_λ). The fact that A is now varying makes hardly any difference to the first part of the argument, and we still end up on a subanalytic set. Now it is at worst a surface and so an earlier result of Pila [8] suffices to get the n^ϵ. Apart from the possibility that P_λ or Q_λ is generically torsion (already excluded above), it turns out that the only possible obstacle is an identity $qP_\lambda = pQ_\lambda$ for fixed non-zero integers p, q; and this too can be excluded.

To get the n^δ it suffices to have some version of [5] for varying elliptic curves. The main result of [7] is almost enough, except that there is no explicit dependence on the degree of the ground field. This was supplied by David [3], whose result is particularly sharp in several respects. Of course it involves the height of the elliptic curve, which however can be controlled with Silverman's Theorem quoted above.

Prompted by a remark of J-P. Serre, we point out that there is nothing special about our choice of X-coordinates 2 and 3. We even expect that similar arguments will allow the Theorem to be generalized to any independent points P_λ, Q_λ on E_λ defined over an algebraic closure of $\mathbf{Q}(\lambda)$. Perhaps specialization techniques will also allow $\mathbf{C}(\lambda)$ here. Note that the analogous results over a constant elliptic curve are easy consequences of Manin–Mumford itself.

2. Sketch of proof

First we record the basic result of Pila [8] that we use.

For any subset S of $\mathbf{R}^s$ we define S^{tr} as what remains of S after removing all positive-dimensional semialgebraic sets in $\mathbf{R}^s$ contained in S. Certainly S^{tr} lies inside the set S^{trans} defined in [8, p. 207].

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 disc in $\mathbf{R}^m$ and each θ is real analytic from an open neighbourhood of D to $\mathbf{R}^s$. The following result can be deduced from [8].

Lemma 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^{tr} in $\frac{1}{n}\mathbf{Z}^s$.*

We will construct our own naive-2-subanalytic subset S by means of the following functions. Let $F(\frac{1}{2}, \frac{1}{2}, 1; \lambda)$ be a hypergeometric function. We define

$$f = f(\lambda) = \pi F\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right), \qquad g = g(\lambda) = \pi \mathrm{i} F\left(\frac{1}{2}, \frac{1}{2}, 1; 1-\lambda\right);$$

these are certainly analytic in the open set Λ defined by $|\lambda| < 1,\ |1-\lambda| < 1$. They are basis elements of a period lattice of E_λ (see, for example, [4, p. 179]). Then using the standard determination of $\sqrt{\lambda - X}$ we can define

$$z = z(\lambda) = 2\int_2^\infty \frac{\mathrm{d}X}{\sqrt{X(X-1)(X-\lambda)}}, \qquad w = w(\lambda) = 2\int_3^\infty \frac{\mathrm{d}X}{\sqrt{X(X-1)(X-\lambda)}},$$

which are analytic off the real intervals $[2, \infty), [3, \infty)$ respectively, and so for example on Λ. These are elliptic logarithms of P_λ, Q_λ. It will turn out that $S^{\mathrm{tr}} = S$, and to prove this we have to know that the functions f, g, z, w are homogeneously algebraically independent on Λ. This in turn is a simple application of monodromy.

Our S will consist of the following $\theta(D)$ together with certain analytic continuations. It can be shown that there are unique real $x = x(\lambda), y = y(\lambda), u = u(\lambda), v = v(\lambda)$ with

$$z = xf + yg, \qquad w = uf + vg.$$

We can therefore define $\theta = (x, y, u, v)$ on Λ by this formula, with a small closed disc D inside Λ. As mentioned above, we have $S^{\mathrm{tr}} = S$.

We use the standard absolute Weil height

$$h(\lambda) = \frac{1}{[\mathbf{Q}(\lambda) : \mathbf{Q}]} \sum_v \log\max\{1, |\lambda|_v\}$$

of an algebraic number λ, where v runs over a suitably normalized set of valuations. The upper bound for the order of torsion follows at once from the following result, deduced from [3]:

Lemma 2. *There is an absolute constant c with the following property. Suppose for some $\lambda \neq 0, 1$ that the point P_λ or the point Q_λ has finite order n. Then λ is algebraic, and*

$$n \leqslant c[\mathbf{Q}(\lambda) : \mathbf{Q}]^2\big(1 + h(\lambda)\big).$$

In view of the next result, deduced from [12], we can eliminate the height dependence in Lemma 2.

Lemma 3. *There is an absolute constant c with the following property. Suppose for some $\lambda \neq 0, 1$ that the point P_λ or the point Q_λ has finite order. Then $h(\lambda) \leqslant c$.*

To prove our Theorem we fix any positive $\epsilon < \frac{1}{4}$. We use c, c_1, c_2, c_3 for positive absolute constants. We have to show that there are at most finitely many $\lambda \neq 0, 1$ such that P_λ and Q_λ both have finite order on E_λ. By Lemma 2 each value is algebraic, say of degree d, and thanks to Lemma 3 and the Northcott property it will suffice to prove $d \leqslant c$. We will actually argue with a single value of λ and its d conjugates.

Next, Lemma 2 together with Lemma 3 shows (by multiplying together the two orders) that there is a positive integer $n \leqslant c_1 d^4$ such that $nP_\lambda = nQ_\lambda = 0$.

Suppose that we are lucky and λ has at least $\frac{d}{2}$ conjugates μ in D. Since also $nP_\mu = nQ_\mu = 0$ on E_μ the points $\theta(\mu)$ lie in $\mathbf{Q}^4$ and even in $\frac{1}{n}\mathbf{Z}^4$.

By Lemma 1 the number of such values $\theta(\mu)$ is at most $c_2 n^{\epsilon} \leqslant c_3 d^{4\epsilon}$. We can without difficulty deduce the same estimate for the number of μ. But this is at least $\frac{d}{2}$; and $d \leqslant c$ follows.

If we are not so lucky with the conjugates, then we have to work with one of the analytic continuations of $\theta(D)$. From Lemma 3 it turns out that the number of these can be bounded by an absolute constant; and this allows the argument to proceed in the same way.

References

[1] E. Bombieri, D. Masser, U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, Int. Math. Res. Notices 20 (1999) 1119–1140.

[2] E. Bombieri, J. Pila, The number of integral points on arcs and ovals, Duke Math. J. 59 (1989) 337–357.

[3] S. David, Points de petite hauteur sur les courbes elliptiques, J. Number Theory 64 (1997) 104–129.

[4] D. Husemöller, Elliptic Curves, Springer-Verlag, 1987.

[5] D. Masser, Small values of the quadratic part of the Néron–Tate height on an abelian variety, Compositio Math. 53 (1984) 153–170.

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

[7] D. Masser, Counting points of small height on elliptic curves, Bull. Soc. Math. France 117 (1989) 247–265.

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

[9] J. Pila, A. Wilkie, The rational points of a definable set, Duke Math. J. 33 (2006) 591–616.

[10] J. Pila, U. Zannier, Rational points in periodic analytic sets and the Manin–Mumford conjecture, Rend. Lincei Mat. Appl. (RML), in press.

[11] R. Pink, A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang, manuscript dated 17th April 2005 (13 pages).

[12] J.H. Silverman, Heights and the specialization map for families of abelian varieties, J. Reine Angew. Math. 342 (1983) 197–211.

[13] B. Zilber, Exponential sums equations and the Schanuel conjecture, J. London Math. Soc. 65 (2002) 27–44.