INTERSECTING THE TORSION OF ELLIPTIC CURVES

NATALIA GARCIA-FRITZ[⊠] and HECTOR PASTEN

Abstract

Bogomolov and Tschinkel ['Algebraic varieties over small fields', *Diophantine Geometry*, U. Zannier (ed.), CRM Series, 4 (Scuola Normale Superiore di Pisa, Pisa, 2007), 73–91] proved that, given two complex elliptic curves E_1 and E_2 along with even degree-2 maps $\pi_j \colon E_j \to \mathbb{P}^1$ having different branch loci, the intersection of the image of the torsion points of E_1 and E_2 under their respective π_j is finite. They conjectured (also in works with Fu) that the cardinality of this intersection is uniformly bounded independently of the elliptic curves. The recent proof of the uniform Manin–Mumford conjecture implies a full solution of the Bogomolov–Fu–Tschinkel conjecture. In this paper, we prove a generalisation of the Bogomolov–Fu–Tschinkel conjecture whereby, instead of even degree-2 maps, one can use any rational functions of bounded degree on the elliptic curves as long as they have different branch loci. Our approach combines Nevanlinna theory with the uniform Manin–Mumford conjecture. With similar techniques, we also prove a result on lower bounds for ranks of elliptic curves over number fields.

2020 *Mathematics subject classification*: primary 11G05; secondary 14G25, 14H52.

Keywords and phrases: elliptic curve, torsion, rank, Mordell–Lang, Manin–Mumford, uniformity.

1. Introduction

For an elliptic curve E over $\mathbb{C}$, we let $E[\infty]$ be the set of all its torsion points. A morphism $f \colon E \to \mathbb{P}^1$ is said to be *even* if $f(-P) = f(P)$ for all P in E. In 2007, Bogomolov and Tschinkel [3] used Raynaud's theorem (the Manin–Mumford conjecture) to prove the following result.

THEOREM 1.1 (Bogomolov–Tschinkel). *Let E_1 and E_2 be complex elliptic curves. For each $i = 1, 2$, let $\pi_j \colon E_j \to \mathbb{P}^1$ be a degree-2 morphism that is even, and suppose that the branch loci of π_1 and π_2 in $\mathbb{P}^1$ are different. Then $\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])$ is finite.*

We remark that if E is a complex elliptic curve and $\pi \colon E \to \mathbb{P}^1$ is an even degree-2 map, then its branch locus is precisely $\pi(E[2]) \subseteq \mathbb{P}^1$. The previous theorem motivated the following conjecture, which seems to have first appeared explicitly in joint works of Bogomolov, Fu and Tschinkel [1–3].

CONJECTURE 1.2 (Bogomolov–Fu–Tschinkel). *There is a constant c with the following property.*

For any complex elliptic curves E_1 and E_2, and for even degree-2 maps $\pi_j \colon E_j \to \mathbb{P}^1$ whose branch loci in $\mathbb{P}^1$ are different, $\#(\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])) < c$.

A first breakthrough was obtained in 2020 by DeMarco *et al.* [4] when they proved the conjectured uniform bound in the case where E_1 and E_2 are given in Legendre form $y^2 = x(x-1)(x-\lambda)$ and π_j are the corresponding projections onto the x-coordinate. As noted in [7], the Bogomolov–Fu–Tschinkel conjecture is now completely solved thanks to the recent proof of the uniform Manin–Mumford conjecture [6, 8, 10, 11, 14]. See also [5, 12] for alternative proofs of the Bogomolov–Fu–Tschinkel conjecture. In this work, we prove the following generalisation.

THEOREM 1.3 (Main Theorem for torsion). *Let d be a positive integer. There is a constant $c_0(d)$, depending only on d, which has the following property.*

For any complex elliptic curves E_1 and E_2 and nonconstant morphisms $g_j \colon E_j \to \mathbb{P}^1$ of degree $\deg(g_j) \le d$ whose branch loci in $\mathbb{P}^1$ are different,

$$\#(g_1(E_1[\infty]) \cap g_2(E_2[\infty])) < c_0(d).$$

In a similar vein, if, instead of torsion points, we consider the Mordell–Weil group of elliptic curves over number fields, we obtain the following result.

THEOREM 1.4 (Main Theorem for ranks). *Let d be a positive integer. There is a constant $\kappa(d) > 0$, depending only on d, with the following property.*

Let k be a number field and let E_1 and E_2 be elliptic curves over k. Let $g_j \colon E_j \to \mathbb{P}^1$ be nonconstant morphisms defined over k of degree $\deg(g_j) \le d$ with different branch loci. Then

$$1 + \operatorname{rank} E_1(k) + \operatorname{rank} E_2(k) \ge \kappa(d) \cdot \log \max\{1, \#(g_1(E_1(k)) \cap g_2(E_2(k)))\}.$$

Thus, if two elliptic curves over a number field k have large intersection of the image of their k-rational points under rational maps to $\mathbb{P}^1$ of fixed degree and different branch loci, then at least one of the two elliptic curves has large rank over k. Thus, Theorem 1.4 is connected to the question of boundedness of ranks of elliptic curves over number fields.

To conclude this introduction, let us briefly describe our methods. The proof of the Bogomolov–Fu–Tschinkel conjecture applies the uniform Manin–Mumford conjecture to the curve $X \subseteq E_1 \times E_2$, which is defined by the equation $\pi_1(P_1) = \pi_2(P_2)$ for $(P_1, P_2) \in E_1 \times E_2$. For this, one checks that X is an irreducible curve of geometric genus at least 2.

In the more general setting of Theorem 1.3, there is no reason for $g_1(P_1) = g_2(P_2)$ to define an irreducible curve in $E_1 \times E_2$ and one needs to ensure that all the irreducible components of the resulting algebraic set are curves of geometric genus at least 2. This is achieved in an indirect way using Nevanlinna theory, for which we review the

necessary background in Section 2. This approach originates in the authors' proof of Bremner's conjecture [9]. In this way, we first obtain a purely geometric result in Section 3 (Theorem 3.3) from which Theorem 1.3 is deduced in Section 5 using the uniform Manin–Mumford conjecture (now a theorem). Finally, Theorem 1.4 is also proved in Section 5 by combining our geometric result with the uniform Mordell–Lang conjecture [6, 8, 10, 14] (see Section 4) instead of the uniform Manin–Mumford conjecture.

2. Nevanlinna theory

We use Landau's notation o. Thus, $o(1)$ represents a function that tends to 0. In addition, the subscript '*exc*' in inequalities and equalities between functions of a variable $r \in \mathbb{R}_{\geq 0}$ means that the claimed relationship holds for r outside a set of finite measure in $\mathbb{R}_{\geq 0}$.

In the first half of the 1920s, Nevanlinna developed a very successful theory to study value distribution of complex meromorphic functions. In this section, we recall some basic results of this theory; we refer the reader to [13] for a general reference.

Let $\mathcal{M}$ be the field of (possibly transcendental) complex meromorphic functions on $\mathbb{C}$. Given a nonconstant $h \in \mathcal{M}$, a point $\alpha \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ and a real number $r \geq 0$, we define

$$n_h^{(1)}(\alpha, r) = \#\{z_0 \in \mathbb{C} : |z_0| \leq r \text{ and } h(z_0) = \alpha\},$$

where the case $h(z_0) = \infty$ is understood as the condition that h has a pole at z_0. The *truncated counting function* $N_h^{(1)}(\alpha, r)$ is then defined as the logarithmic average

$$N_h^{(1)}(\alpha, r) = \int_0^r (n_h^{(1)}(\alpha, t) - n_h^{(1)}(\alpha, 0)) \frac{dt}{t} + n_h^{(1)}(\alpha, 0) \log r.$$

Associated to every $h \in \mathcal{M}$, there is the *Nevanlinna height* (or *characteristic*) function

$$T_h \colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},$$

which has the basic property that it is bounded if h is constant; otherwise $T_f(r)$ grows to infinity as $r \to \infty$. We recall that the function $T_h(r)$ is only defined up to adding a bounded function. Intuitively, $T_h(r)$ measures the complexity of h restricted to the disk $\{z \in \mathbb{C} : |z| \leq r\}$ as r grows. For our purposes, we do not need to recall the precise definition of $T_h(r)$ (which can be found, for example, in [13]), but instead we simply need its relationship to the truncated counting function, which is provided by the *Second Main Theorem* of Nevanlinna theory.

THEOREM 2.1 (Second Main Theorem). *Let $h \in \mathcal{M}$ be nonconstant and let $\alpha_1, \ldots, \alpha_q$ be different points in $\mathbb{P}^1(\mathbb{C})$. Then*

$$\sum_{j=1}^q N_h^{(1)}(\alpha_j, r) \geq_{exc} (q - 2 + o(1)) T_h(r).$$

In addition to the previous general result, we need another relationship between the Nevanlinna height and the truncated counting function in a special case.

LEMMA 2.2 ([9, Lemma 3.3]). *Let E be a complex elliptic curve and let $g \colon E \to \mathbb{P}^1$ be a nonconstant morphism of degree d. Let $\phi \colon \mathbb{C} \to E$ be a nonconstant holomorphic map and let $\alpha \in \mathbb{P}^1(\mathbb{C})$. Consider the nonconstant meromorphic function $h = g \circ \phi \in \mathcal{M}$. Then*

$$N_h^{(1)}(\alpha, r) =_{exc} \left(\frac{\# g^{-1}(\alpha)}{d} + o(1) \right) T_h(r).$$

We remark that our proof of the previous lemma in [9] uses the Second Main Theorem for holomorphic maps to elliptic curves rather than the case of meromorphic functions cited above.

3. Geometric preliminaries

Let us fix some notation and assumptions for this section. Let E_1 and E_2 be complex elliptic curves. For $j = 1, 2$, let $g_j \colon E_j \to \mathbb{P}^1$ be a nonconstant morphism of degree d_j. Suppose that g_1 and g_2 have different branch loci in $\mathbb{P}^1$. Let $X \subseteq E_1 \times E_2$ be the one-dimensional algebraic set defined by the equation $g_1(P_1) = g_2(P_2)$ on $(P_1, P_2) \in E_1 \times E_2$: that is, X is the pre-image of the diagonal $\Delta \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ via the map $G = (g_1, g_2) \colon E_1 \times E_2 \to \mathbb{P}^1 \times \mathbb{P}^1$.

If $Z \subseteq E_1 \times E_2$ is a one-dimensional algebraic set, we define its degree $\deg(Z)$ as the intersection number $Z.(V_1 + V_2)$, where Z is seen as a reduced divisor, and we define $V_1 = \{0\} \times E_2$ and $V_2 = E_1 \times \{0\}$, where 0 is the neutral point of the corresponding elliptic curve. Here, we remark that the divisor $V_1 + V_2$ on $E_1 \times E_2$ is ample.

LEMMA 3.1. *We have $\deg(X) \le (d_1 + d_2) d_1 d_2$.*

PROOF. Let $\Delta \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ be the diagonal and let $L_1 = \{p_1\} \times \mathbb{P}^1$ and $L_1 = \mathbb{P}^1 \times \{p_2\}$ for a fixed choice of points $p_1, p_2 \in \mathbb{P}^1$. Then Δ is linearly equivalent to $L_1 + L_2$.

Note that $X = G^{-1}\Delta \le G^*\Delta$ as divisors, and by the projection formula,

$$
\begin{aligned}
\deg(X) &\le \deg(G^*\Delta) \\
&= (G^*(L_1 + L_2)) \cdot (V_1 + V_2) \\
&\le G^* G_*(G^*(L_1 + L_2) \cdot (V_1 + V_2)) \\
&= G^*((L_1 + L_2) \cdot G_*(V_1 + V_2)) \\
&= d_1 d_2 (L_1 + L_2) \cdot (d_2 \cdot \{g_1(0)\} \times \mathbb{P}^1 + d_1 \cdot \mathbb{P}^1 \times \{g_2(0)\}) \\
&= d_1 d_2 (d_1 + d_2). \qquad \square
\end{aligned}
$$

Before we give the main result of this section, we recall the Riemann–Hurwitz formula, which is useful in our argument.

LEMMA 3.2 (Riemann–Hurwitz formula). *Let Y_1 and Y_2 be smooth projective (complex) curves of genus $\mathfrak{g}_1$ and $\mathfrak{g}_2$, respectively, and let $g\colon Y_1 \to Y_2$ be a nonconstant morphism of degree d. Let $\alpha_1, \ldots, \alpha_m \in Y_2$ be all the branch values of g. Then*

$$2(\mathfrak{g}_1 - 1) = 2d(\mathfrak{g}_2 - 1) + \sum_{j=1}^{m}(d - \#g^{-1}(\alpha_j)).$$

With this at hand, we can prove our geometric result.

THEOREM 3.3. *Every irreducible component of X is a curve of geometric genus at least 2.*

PROOF. Let $C \subseteq X$ be an irreducible component and, for the sake of contradiction, suppose that C has geometric genus 0 or 1. As $C \subseteq E_1 \times E_2$, we see that, necessarily, C has geometric genus 1, because the projection to at least one component E_i is nonconstant. Since elliptic curves can be uniformised by holomorphic functions from $\mathbb{C}$, we obtain a nonconstant holomorphic map $\phi = (\phi_1, \phi_2)\colon \mathbb{C} \to C \subseteq E_1 \times E_2$, where at least one of $\phi_j\colon \mathbb{C} \to E_j$ is nonconstant. By the definition of X, we see that $g_1 \circ \phi_1 = g_2 \circ \phi_2$, and we conclude that both ϕ_j are nonconstant.

Let $h = g_1 \circ \phi_1 = g_2 \circ \phi_2 \in \mathcal{M}$. Since g_1 and g_2 have different branch loci, we may assume, without loss of generality, that there is $\beta \in \mathbb{P}^1$ that is a branch value of g_2 but not of g_1. Let $\alpha_1, \ldots, \alpha_m \in \mathbb{P}^1$ be the different branch values of g_1.

By the Second Main Theorem 2.1 with $q = m + 1$,

$$N_h^{(1)}(\beta, r) + \sum_{j=1}^{m} N_h^{(1)}(\alpha_j, r) \geq_{exc} (m - 1 + o(1))T_h(r).$$

On the other hand, Lemma 2.2 gives

$$N_h^{(1)}(\beta, r) =_{exc} \left(\frac{\#g_2^{-1}(\beta)}{d_2} + o(1)\right)T_h(r)$$

and, for each $1 \leq j \leq m$, we similarly obtain

$$N_h^{(1)}(\alpha_j, r) =_{exc} \left(\frac{\#g_1^{-1}(\alpha_j)}{d_1} + o(1)\right)T_h(r).$$

Putting all of this together, we find that

$$\left(\frac{\#g_2^{-1}(\beta)}{d_2} + \sum_{j=1}^{m} \frac{\#g_1^{-1}(\alpha_j)}{d_1} + o(1)\right)T_h(r) \geq_{exc} (m - 1 + o(1))T_h(r).$$

Letting $r \to \infty$, since h is nonconstant, we deduce that

$$m - 1 \leq \frac{\#g_2^{-1}(\beta)}{d_2} + \sum_{j=1}^{m} \frac{\#g_1^{-1}(\alpha_j)}{d_1}.$$

Since β is a branch value of g_2, we have $\# g_2^{-1}(\beta) < d_2$, and hence

$$m - 1 < 1 + \frac{1}{d_1} \sum_{j=1}^{m} \# g_1^{-1}(\alpha_j). \tag{3.1}$$

On the other hand, the Riemann–Hurwitz formula (in the form of Lemma 3.2) applied to $g_1 \colon E_1 \to \mathbb{P}^1$ gives

$$0 = -2d_1 + \sum_{j=1}^{m} (d_1 - \# g_1^{-1}(\alpha_j))$$

from which

$$\frac{1}{d_1} \sum_{j=1}^{m} \# g_1^{-1}(\alpha_j) = m - 2.$$

This contradicts the bound (3.1). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

4. Uniform Mordell–Lang and Manin–Mumford

The rank of an abelian group Γ, denoted by $\operatorname{rank} \Gamma$, is defined as the dimension over $\mathbb{Q}$ of the vector space $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$.

After the recent works [6, 8, 10, 14], the uniform Mordell–Lang conjecture is proved. Here, we recall the version obtained in [8] in the case of (possibly singular) curves contained in abelian varieties.

THEOREM 4.1 (Uniform Mordell–Lang for curves). *Let $n, D \geq 1$ be integers. There is a constant $c(n, D)$, depending only on n and D, with the following property.*

Let A be an abelian variety over $\mathbb{C}$ of dimension n, let $\mathscr{L}$ be an ample line sheaf on A and let $X \subseteq A$ be a one-dimensional Zariski closed subset with $\deg_{\mathscr{L}}(X) \leq D$. Let $\Gamma \leq A(\mathbb{C})$ be a subgroup of finite rank and let $r = \operatorname{rank} \Gamma$. If all irreducible components of X have geometric genus at least 2, then

$$\#(\Gamma \cap X) \leq c(n, D)^{1+r}.$$

As usual, $\deg_{\mathscr{L}}(X)$ is defined as the intersection number of $\mathscr{L}$ with X. Theorem 4.1 follows from Theorem 1.1 in [8]; note that here we do not require that X is irreducible, but this case also follows from the same theorem because $\deg_{\mathscr{L}}(X)$ is additive on X and it is a strictly positive integer as $\mathscr{L}$ is ample.

In the special case where Γ is the full torsion subgroup of A, one has $r = 0$ and the previous result specialises to the uniform Manin–Mumford conjecture.

THEOREM 4.2 (Uniform Manin–Mumford for curves). *Let $n, D \geq 1$ be integers. There is a constant $c(n, D)$, depending only on n and D, with the following property.*

Let A be an abelian variety over $\mathbb{C}$ of dimension n, let $\mathscr{L}$ be an ample line sheaf on A and let $X \subseteq A$ be a one-dimensional Zariski closed subset with $\deg_{\mathscr{L}}(X) \leq D$.

Let $A[\infty]$ be the subgroup of all torsion points of $A(\mathbb{C})$. If all irreducible components of X have geometric genus at least 2, then

$$\#(A[\infty] \cap X) \leq c(n, D).$$

We point out that we use these results only when the abelian variety A is the product of two elliptic curves, so one may refer to [11].

5. Torsion and ranks

In this section, we prove Theorems 1.3 and 1.4. For this, let us fix some common notation. Let k be $\mathbb{C}$ in the case of Theorem 1.3 or a number field in the case of Theorem 1.4. Let E_1 and E_2 be elliptic curves and let $g_j \colon E_j \to \mathbb{P}^1$ be morphisms of degrees $d_j \leq d$ for $j = 1, 2$, all defined over k. We assume that the branch loci of g_1 and g_2 in $\mathbb{P}^1$ are different.

Let $G = (g_1, g_2) \colon E_1 \times E_2 \to \mathbb{P}^1 \times \mathbb{P}^1$, let $\Delta \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ be the diagonal and let $X = G^{-1}\Delta \subseteq E_1 \times E_2$. We note that X is the locus of geometric points (P_1, P_2) in $E_1 \times E_2$ satisfying $g_1(P_1) = g_2(P_2)$.

By Lemma 3.1, $\deg(X) \leq d_1 d_2 (d_1 + d_2) \leq 2d^3$, where $\deg(X)$ is the degree with respect to the ample divisor $V_1 + V_2$, as defined in Section 3. Furthermore, by Theorem 3.3, the (geometric) irreducible components of X have geometric genus at least 2.

PROOF OF THEOREM 1.3. Let $\Gamma = E_1[\infty] \times E_2[\infty]$; this is the group of torsion points of the abelian surface $E_1 \times E_2$. By Theorem 4.2,

$$\#(\Gamma \cap X) \leq c(2, 2d^3)$$

with $c(n, D)$ as in Theorem 4.2. We note that

$$g_1(E_1[\infty]) \cap g_2(E_2[\infty]) = G(\Gamma) \cap \Delta = G(\Gamma \cap X)$$

and we obtain the result with $c_0(d) = c(2, 2d^3)$. □

PROOF OF THEOREM 1.4. The proof is very similar. Let $\Gamma = E_1(k) \times E_2(k)$; by the Mordell–Weil theorem, this group is finitely generated and its rank is $r = \operatorname{rank} E_1(k) + \operatorname{rank} E_2(k)$. By Theorem 4.1,

$$\#(\Gamma \cap X) \leq c(2, 2d^3)^{1+r}$$

with $c(n, D)$ as in Theorem 4.1. We note that

$$g_1(E_1(k)) \cap g_2(E_2(k)) = G(\Gamma) \cap \Delta = G(\Gamma \cap X)$$

and we obtain the result with $\kappa(d) = 1/\log c(2, 2d^3)$. □

Acknowledgements

References

[1]   F. Bogomolov and H. Fu, 'Division polynomials and intersection of projective torsion points', *Eur. J. Math.* **2**(3) (2016), 644–660.

[2]   F. Bogomolov, H. Fu and Y. Tschinkel, 'Torsion of elliptic curves and unlikely intersections', in: *Geometry and Physics*, Vol. I (eds. J. E. Andersen, A. Dancer and O. García-Prada) (Oxford University Press, Oxford, 2018), 19–37.

[3]   F. Bogomolov and Y. Tschinkel, 'Algebraic varieties over small fields', in: *Diophantine Geometry*, CRM Series, 4 (ed. U. Zannier) (Scuola Normale Superiore di Pisa, Pisa, 2007), 73–91.

[4]   L. DeMarco, H. Krieger and H. Ye, 'Uniform Manin–Mumford for a family of genus 2 curves', *Ann. of Math. (2)* **191**(3) (2020), 949–1001.

[5]   L. DeMarco and N. Mavraki, 'Dynamics on $\mathbb{P}^1$: preperiodic points and pairwise stability', *Compos. Math.*, to appear.

[6]   V. Dimitrov, Z. Gao and P. Habegger, 'Uniformity in Mordell–Lang for curves', *Ann. of Math. (2)* **194**(1) (2021), 237–298.

[7]   H. Fu and M. Stoll, 'Elliptic curves with common torsion x-coordinates and hyperelliptic torsion packets', *Proc. Amer. Math. Soc.* **150**(12) (2022), 5137–5149.

[8]   Z. Gao, T. Ge and L. Kühne, 'The uniform Mordell–Lang conjecture', Preprint, 2021, arXiv:2105.15085.

[9]   N. Garcia-Fritz and H. Pasten, 'Elliptic curves with long arithmetic progressions have large rank', *Int. Math. Res. Not. IMRN* **2021**(10) (2021), 7394–7432.

[10] L. Kühne, 'Equidistribution in families of abelian varieties and uniformity', Preprint, 2021, arXiv:2101.10272.

[11] L. Kühne, 'The relative Bogomolov conjecture for fibered products of elliptic curves', *J. reine angew. Math.* **795** (2023), 243–270.

[12] J. Poineau, 'Dynamique analytique sur **Z**. II: Écart uniforme entre Lattès et conjecture de Bogomolov–Fu–Tschinkel', Preprint, 2023, arXiv:2207.01574.

[13] P. Vojta, 'Diophantine approximation and Nevanlinna theory', in: *Arithmetic Geometry*, Lecture Notes in Mathematics, 2009 (eds. J.-L. Colliot-Thélène, P. Swinnerton-Dyer and P. Vojta) (Springer, Berlin, 2011), 111–224.

[14] X. Yuan, 'Arithmetic bigness and a uniform Bogomolov-type result', Preprint, 2023, arXiv:2108.05625.

NATALIA GARCIA-FRITZ, Departamento de Matemáticas,
Pontificia Universidad Católica de Chile,
Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
e-mail: natalia.garcia@uc.cl

HECTOR PASTEN, Departamento de Matemáticas,
Pontificia Universidad Católica de Chile,
Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
e-mail: hector.pasten@uc.cl