

INTERSECTING CURVES AND ALGEBRAIC SUBGROUPS: CONJECTURES AND MORE RESULTS

E. BOMBIERI, D. MASSER, AND U. ZANNIER

ABSTRACT. This paper solves in the affirmative, up to dimension $n = 5$, a question raised in an earlier paper by the authors. The equivalence of the problem with a conjecture of Shou-Wu Zhang is proved in the Appendix.

1. INTRODUCTION

In this note we answer in the affirmative a special case of a question raised in our previous paper [BMZ]. For $n \geq 2$ let \mathcal{C} be an algebraic curve, defined over the field $\overline{\mathbf{Q}}$ of algebraic numbers and lying in affine n -space. It will be convenient to assume that \mathcal{C} is absolutely irreducible and to think of it as a quasi-affine subset of the group variety \mathbf{G}_m^n defined by the non-vanishing of the coordinates x_1, \dots, x_n . We consider the intersections of \mathcal{C} with varying algebraic subgroups; recall that these subgroups are defined by finitely many monomial equations $x_1^{a_1} \cdots x_n^{a_n} = 1$. In Theorem 2 of [BMZ, p. 1121] we proved the following result.

Theorem A ([BMZ]). *Suppose that \mathcal{C} is not contained in any translate of an algebraic subgroup of dimension at most $n - 1$, and let \mathcal{H} denote the union of all algebraic subgroups of dimension at most $n - 2$. Then $\mathcal{C} \cap \mathcal{H}$ is a finite set.*

The question raised in [BMZ, second Remark, p. 1121] concerns the minimal hypothesis on \mathcal{C} which suffices for the same finiteness conclusion. It is easy to see that some hypothesis is needed. In fact, suppose that \mathcal{C} is contained in a translate by a torsion point of an algebraic subgroup H of dimension at most $n - 1$. We can assume that H is irreducible, of dimension exactly $n - 1$. Then, after an algebraic group automorphism, we can identify H with \mathbf{G}_m^{n-1} in \mathbf{G}_m^n , defined by taking the last coordinate $x_n = 1$. There is thus a curve \mathcal{C}' in \mathbf{G}_m^{n-1} together with a torsion point Q_0 in \mathbf{G}_m such that $\mathcal{C} = \mathcal{C}' \times Q_0$ in $\mathbf{G}_m^{n-1} \times \mathbf{G}_m = \mathbf{G}_m^n$. If \mathcal{H}' denotes the union of all algebraic subgroups of \mathbf{G}_m^{n-1} of dimension at most $n - 2$, it is not difficult to see that $\mathcal{C}' \cap \mathcal{H}'$ is infinite; for example, if x_{n-1} is not constant on \mathcal{C}' , then it takes all but finitely many root of unity values. It follows that $\mathcal{C} \cap \mathcal{H}$ is also infinite.

We believe that this situation provides the only obstacle to finiteness. For the sake of brevity, we refer to a translate of an algebraic subgroup of \mathbf{G}_m^n as a coset, and if the translation is done by a torsion point, then we speak of a torsion coset. If the dimension is at most $n - 1$, then we say that the coset is proper. Thus we would like to state the following conjecture.

Received by the editors February 2, 2004 and, in revised form, July 14, 2004.
2000 *Mathematics Subject Classification*. Primary 11J95; Secondary 11G30, 11G50.

Conjecture A. *Suppose that \mathcal{C} is not contained in a proper torsion coset. Then $\mathcal{C} \cap \mathcal{H}$ is a finite set.*

In a somewhat different form, and also in the context of abelian varieties, the same conjecture has been independently stated by Shou-Wu Zhang. With his kind permission, we discuss this further in the Appendix. Actually when \mathcal{C} lies in a power E^n of an elliptic curve with complex multiplication, the analogue of Conjecture A was recently proved by Gaël Rémond and Evelina Viada [RV, Théorème 1.7, p. 1917].

Already in [BMZ] some easier cases of this conjecture were disposed of. In view of Theorem A we may assume that \mathcal{C} is contained in a coset of dimension $d \leq n-1$. We noted in [BMZ, pp. 1121-1122] that the cases $d = 1$ and $d = 2$ follow from a well-known result of Liardet (so we may take $n \geq 4$). The object of the present note is to settle the next case $d = 3$. In other words:

Theorem. *For $n \geq 4$ let \mathcal{C} be an absolutely irreducible curve in \mathbf{G}_m^n defined over $\overline{\mathbf{Q}}$. Suppose that \mathcal{C} is not contained in a proper torsion coset, but also that \mathcal{C} is contained in a coset of dimension at most 3. Then $\mathcal{C} \cap \mathcal{H}$ is a finite set.*

Corollary. *Conjecture A holds for \mathcal{C} in \mathbf{G}_m^5 .*

All these results can of course be formulated in more elementary terms of multiplicative dependence. As noted in [BMZ], a very special case of our Theorem is the following: *there are only finitely many algebraic $\tau \neq 0, 1, -1$ for which there are two independent multiplicative dependence relations between the numbers $2, 3, \tau, 1 - \tau, 1 + \tau$.* Possibly, there are quite a few such τ ; we found 56 rational τ , and Cohen and Zannier found 34 irrational τ in [CZ].

The proof of our Theorem may be conveniently illustrated with the above example. Let

$$(1) \quad 2^a 3^b \tau^c (1 - \tau)^d (1 + \tau)^e = 1$$

be one of the dependence relations, and let σ be an element of the absolute Galois group $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Applying σ to (1) and eliminating 2 and 3 leads to a relation

$$(2) \quad x^c y^d z^e = 1$$

for

$$(3) \quad x = \tau/\omega, \quad y = (1 - \tau)/(1 - \omega), \quad z = (1 + \tau)/(1 + \omega)$$

and the conjugate $\omega := \sigma(\tau)$. Now (3) can be regarded as parametrizing a surface \mathcal{X} in \mathbf{G}_m^3 ; the equation happens to be

$$(4) \quad xy + xz - 2yz - 2x + y + z = 0.$$

Then (2) is a dependence relation on \mathcal{X} . But in fact we have two independent relations (1), and these lead to two independent relations (2). This means that we are intersecting \mathcal{X} with the union \mathcal{H}_1 of all algebraic subgroups of dimension at most 1.

Such intersections $\mathcal{X} \cap \mathcal{H}_1$, for varieties \mathcal{X} of arbitrary dimension in \mathbf{G}_m^n , were investigated by Bombieri and Zannier [Zan]. Their work, involving a certain open subset \mathcal{X}° of \mathcal{X} , implies in our situation that the point (3) either lies in a fixed finite union of one-dimensional cosets, or it has bounded absolute height.

If the first possibility holds for all choices of σ , then this situation can be reduced by Galois theory to Liardet's Theorem as above. The second possibility for a single

σ essentially implies that the original point $(2, 3, \tau, 1 - \tau, 1 + \tau)$ on our curve \mathcal{C} also has bounded height. This would also be the conclusion of Theorem 1 of [BMZ, p. 1120] if it applied (which it does not). But we can now imitate the arguments of [BMZ, pp. 1132-1139] which deduced the finiteness of $\mathcal{C} \cap \mathcal{H}$ from this boundedness of height. Here the recent work of Amoroso and Zannier [AZ] allows an alternative presentation.

The reader will appreciate that the key to establishing the full Conjecture A for curves \mathcal{C} is almost certainly the further study of surfaces \mathcal{X} . More precisely, if \mathcal{X} is in \mathbf{G}_m^n , then one should intersect \mathcal{X} with subgroups of dimension not 1 but $n - 2$. It is likely that this too leads to sets of bounded height. Indeed some precise results of this sort can be proved, but at the moment they do not seem enough to deduce the full Conjecture A. We will return to this surface aspect in later work.

Our present paper is organized as follows. In section 2 we collect together some preliminary observations about curves and surfaces. These then allow the Theorem and Corollary to be established in section 3. Finally, in the Appendix we state Zhang's form of our Conjecture A and we prove its equivalence with this conjecture.

In order to avoid excessive length, we have not tried to make this paper completely self-contained; in particular the reader is advised to have [BMZ] at hand when reading section 2.

2. PRELIMINARIES

We record here what we need on curves from [BMZ] and on surfaces from [Zan], together with the construction of surfaces from curves exemplified by (3).

The first result involves the absolute logarithmic height function $h(P) = h(x_1) + \dots + h(x_n)$ used in [BMZ], for $P = (x_1, \dots, x_n)$ in $\mathbf{G}_m^n(\overline{\mathbf{Q}})$. It may be thought of as a conditional version of our conjecture.

Lemma 1. *Suppose that $n \geq 3$ and that \mathcal{C} is not contained in a proper torsion coset. Then for any $B > 0$ there are only finitely many points P in $\mathcal{C} \cap \mathcal{H}$ with $h(P) \leq B$.*

Proof. We follow the arguments in [BMZ, §4], with Γ as the group generated by the coordinates of P . If the rank r of Γ is zero, then the desired result follows from Liardet's Theorem in the form explicitly involving torsion cosets, given in [La2, Theorem 6.4, p. 203] or more generally [Li, Théorème 4, p. 205].

Otherwise $1 \leq r \leq n - 2$ and we have a factorization as in (4.1) of [BMZ]. Now we can deduce (4.2) of [BMZ], not using Theorem 1 of [BMZ] but simply using our present hypothesis $h(P) \leq B$ in the form $h(P) \ll 1$. Thus the constants implied by this notation depend only on n , \mathcal{C} , and B . If $r \leq n - 3$, then we can conclude with a single application of [AD] as in (4.6) of [BMZ]. Namely, the degree d of $\mathbf{Q}(P)$ satisfies $d \ll 1$. We now deduce the desired result from Northcott's Theorem.

If $r = n - 2$, then we could similarly use the arguments of Lemmas 4, 5 and 6 of [BMZ]. But we wish to point out an alternative method. The equation (4.6) now yields $d \ll N^{1/(1-\epsilon)}$ and so $\mathbf{Q}(P)$ contains a cyclotomic field $\mathbf{Q}(\zeta)$ of degree $\phi(N) \gg d^{1-2\epsilon}$ which is almost as big as d itself. The Amoroso-Zannier Theorem on the relative abelian situation (see [AZ, Theorem 1.1, p. 712]) implies that $h(g) \gg d^{-3\epsilon}$ for any g in $\mathbf{Q}(P)$ not a root of unity. This holds for each generator g_i ($1 \leq i \leq r$) of Γ and therefore $h(g_1) \cdots h(g_r) \gg d^{-3r\epsilon}$. The displayed equation before (4.5) of [BMZ] now implies $\Pi \ll d^{3r\epsilon}$. And then (4.4) gives $d \ll (N\Pi)^{1/2}$.

Finally, $N \ll \phi(N)^{1+\epsilon} \leq d^{1+\epsilon}$, and so choosing ϵ small enough leads to $d \ll 1$. We conclude as above using Northcott's Theorem.

The second result of this section refers to the union \mathcal{H}_1 of all algebraic subgroups of \mathbf{G}_m^n of dimension at most 1.

Theorem B ([Zan]). *Let \mathcal{X} be a variety in \mathbf{G}_m^n defined over $\overline{\mathbf{Q}}$, and let \mathcal{X}° denote the complement in \mathcal{X} of the union of all positive dimensional cosets entirely contained in \mathcal{X} . Then*

(a) $\mathcal{X} \setminus \mathcal{X}^\circ$ is a finite union of sets of the form $\alpha^{-1}(\mathbf{G}_m^k \times \mathcal{Y})$, where α is an automorphism of \mathbf{G}_m^n , k is a positive integer, and \mathcal{Y} is a variety in \mathbf{G}_m^{n-k} defined over $\overline{\mathbf{Q}}$.

(b) The points of $\mathcal{X}^\circ \cap \mathcal{H}_1$ have bounded height.

Proof. Part (a) follows easily from the earlier work of Bombieri and Zannier [BZ]; see in particular the displayed equation at p. 343. Part (b) is essentially Theorem 1 (p. 524) of [Zan]; it is not difficult to see using $(\mathcal{X}_1 \cup \mathcal{X}_2)^\circ \subset \mathcal{X}_1^\circ \cup \mathcal{X}_2^\circ$ that the irreducibility of \mathcal{X} there is irrelevant.

Finally, to construct surfaces from curves we use the quotient map $\varphi : \mathbf{G}_m^n \times \mathbf{G}_m^n \rightarrow \mathbf{G}_m^n$ taking $(x_1, \dots, x_n) \times (y_1, \dots, y_n)$ to $(x_1/y_1, \dots, x_n/y_n)$. We use the same symbol \ll as above, but now the implied constants depend only on n and \mathcal{C} .

Lemma 2. *Suppose that \mathcal{C} is not contained in any proper coset. Then*

(a) $\mathcal{X} = \varphi(\mathcal{C} \times \mathcal{C})$ is a surface.

(b) There is a finite set $Z \subset \mathcal{X}(\overline{\mathbf{Q}})$ such that

$$h(P) + h(Q) \ll h(\varphi(P, Q)) + 1$$

for any P, Q in $\mathcal{C}(\overline{\mathbf{Q}})$ with $\varphi(P, Q) \notin Z$.

Proof. Part (a) is relatively easy: if \mathcal{X} were a curve, then $\mathcal{X} = \varphi(\mathcal{C}, Q) = \varphi(\mathcal{C}, P)$ for any P, Q in \mathcal{C} . This implies that \mathcal{X} is in the stabilizer H of \mathcal{C} , and so \mathcal{C} lies in a translate of H . But this is ruled out by hypothesis, because H is a proper algebraic subgroup.

For part (b) we have to work a bit harder; the result is easy to prove with an exceptional set Z that is a curve, but we need a finite set. Incidentally, the situation $P = Q$ shows that this finite set can never be avoided.

We begin by noting that \mathcal{X} is quasi-affine, and so by Noether normalization there is an everywhere finite morphism $\pi : \mathcal{X} \rightarrow \mathbf{A}^2$ to the affine plane. We can even take the affine coordinates x, y to lie in the coordinate ring $\overline{\mathbf{Q}}[\mathcal{X}]$ of \mathcal{X} (and even as linear forms); see for example [La1, pp. 22-23]. Hence setting $\psi := \pi \circ \varphi$ we obtain a morphism $\psi : \mathcal{C} \times \mathcal{C} \rightarrow \mathbf{A}^2$, generically of finite degree. In particular, the function field $\overline{\mathbf{Q}}(\mathcal{C} \times \mathcal{C})$ is a finite extension of the rational function field $\overline{\mathbf{Q}}(x, y)$. It follows that if ζ is any coordinate function on $\mathcal{C} \times \mathcal{C}$ (or indeed anything in $\overline{\mathbf{Q}}(\mathcal{C} \times \mathcal{C})$), then there is a non-trivial equation $f(x, y, \zeta) = 0$ for some absolutely irreducible polynomial f over $\overline{\mathbf{Q}}$. Let S_ζ be the set of points $(x, y) \in \mathbf{A}^2$ at which f becomes identically zero in the third variable. Then S_ζ is finite, otherwise f would have a non-trivial polynomial factor in $\overline{\mathbf{Q}}[x, y]$. It is now immediate that if $\psi(P, Q) \notin S_\zeta$, then we have $h(\zeta(P, Q)) \ll h(\psi(P, Q)) + 1$, for any P and Q in $\mathcal{C}(\overline{\mathbf{Q}})$. In fact, if a non-zero polynomial f_0 over $\overline{\mathbf{Q}}$ in a single variable has degree d , then any zero z of f_0 has height $h(z) \leq h(f_0) + \log d$, where $h(f_0)$ is the homogeneous height of the coefficient vector of f_0 . Further, because x, y are in $\overline{\mathbf{Q}}[\mathcal{X}]$ we have

$h(\pi(R)) \ll h(R)+1$ for any R in $\mathcal{X}(\overline{\mathbf{Q}})$. It follows that $h(\psi(P, Q)) \ll h(\varphi(P, Q))+1$. Since π is everywhere finite, the present lemma follows on taking $Z = \bigcup \pi^{-1}(S_\zeta)$, with ζ running over a set of coordinate functions on $\mathcal{C} \times \mathcal{C}$.

3. PROOF OF THE THEOREM AND COROLLARY

Suppose that our irreducible curve \mathcal{C} lies in a translate of an algebraic subgroup H_0 , without loss of generality itself irreducible. If H_0 has dimension 1 or 2, we already noted that the required result was proved in [BMZ]. Hence we need only consider the case in which H_0 has dimension 3 and \mathcal{C} is not contained in a coset of dimension 2.

After an automorphism of \mathbf{G}_m^n we may identify H_0 with the subgroup defined by $x_4 = \dots = x_n = 1$. The curve \mathcal{C} now becomes $\mathcal{C} = \mathcal{C}' \times Q_0$ in $\mathbf{G}_m^3 \times \mathbf{G}_m^{n-3} = \mathbf{G}_m^n$, where $\mathcal{C}' \subset \mathbf{G}_m^3$ and $Q_0 = (g_4, \dots, g_n) \in \mathbf{G}_m^{n-3}(\overline{\mathbf{Q}})$.

The irreducible curve \mathcal{C}' is not contained in a proper coset of \mathbf{G}_m^3 because by hypothesis \mathcal{C} is not contained in a coset of dimension 2. Note also that the algebraic numbers g_4, \dots, g_n are multiplicatively independent, otherwise \mathcal{C} would be contained in a proper subgroup. Let Γ be the subgroup of $\overline{\mathbf{Q}}^*$ generated by g_4, \dots, g_n .

We will require one preparatory observation. Recall (for example [Zan, p. 520]) that there is a one-to-one correspondence between algebraic subgroups H of \mathbf{G}_m^n and subgroups L of \mathbf{Z}^n . Namely, any H is defined by a finite system of monomial equations each of the form

$$(5) \quad x_1^{a_1} \dots x_n^{a_n} = 1$$

and L is generated by the exponent vectors $\mathbf{a} = (a_1, \dots, a_n)$ in \mathbf{Z}^n . More significant for us is the associated vector space $W = L \otimes \mathbf{Q}$ of \mathbf{Q}^n , which we denote by $W(H)$ to indicate its dependence on H . Its dimension is the codimension of H in \mathbf{G}_m^n .

Lemma 3. *Let $\mathcal{C}, \mathcal{C}'$ be as above.*

(a) *If H in \mathbf{G}_m^n is an algebraic subgroup of dimension $n-2$ with $\mathcal{C} \cap H$ non-empty, then $H' := H \cap \mathbf{G}_m^3$ is an algebraic subgroup of \mathbf{G}_m^3 of dimension 1.*

(b) *Given a vector subspace W_0 of \mathbf{Q}^3 of dimension 2, denote by $\mathcal{H}(W_0)$ the union of all algebraic subgroups H of \mathbf{G}_m^n of dimension $n-2$ with $W(H \cap \mathbf{G}_m^3) = W_0$. Then $\mathcal{C} \cap \mathcal{H}(W_0)$ is a finite set.*

Proof. For part (a), let L be the subgroup of \mathbf{Z}^n of rank 2 corresponding to H . The projection L' in \mathbf{Z}^3 of L obtained by taking the first three coordinates still has rank 2. Otherwise, L would contain a non-zero vector $(0, 0, 0, a_4, \dots, a_n)$. Since $\mathcal{C} \cap H$ is non-empty, this would imply $g_4^{a_4} \dots g_n^{a_n} = 1$, a contradiction. So L' indeed has rank 2 and it therefore corresponds to a subgroup $H' = H \cap \mathbf{G}_m^3$ of dimension 1, as required.

For part (b), we can pick basis elements $(p_1, p_2, p_3), (q_1, q_2, q_3)$ of W_0 in \mathbf{Z}^3 . Now,

$$(6) \quad \mu(x_1, x_2, x_3) = (x_1^{p_1} x_2^{p_2} x_3^{p_3}, x_1^{q_1} x_2^{q_2} x_3^{q_3})$$

defines a morphism $\mu : \mathbf{G}_m^3 \rightarrow \mathbf{G}_m^2$. Since \mathcal{C}' is not contained in a proper coset, this induces a morphism $\mu : \mathcal{C}' \rightarrow \mathcal{C}''$ onto a curve $\mathcal{C}'' \subset \mathbf{G}_m^2$ defined over $\overline{\mathbf{Q}}$; furthermore \mathcal{C}'' is not contained in a proper coset.

In proving the finiteness of $\mathcal{C} \cap \mathcal{H}(W_0)$ we may restrict our attention to those H in $\mathcal{H}(W_0)$ for which $\mathcal{C} \cap H$ is non-empty. If \mathbf{a} as in (5) lies in the corresponding subgroup L in \mathbf{Z}^n , and $\mathbf{a}' = (a_1, a_2, a_3)$ in L' is the projection to \mathbf{Z}^3 , then (5) for $P = (x_1, x_2, x_3, g_4, \dots, g_n) = P' \times Q_0$ in $\mathcal{C} = \mathcal{C}' \times Q_0$ implies that $x_1^{a_1} x_2^{a_2} x_3^{a_3}$ lies in

Γ . Since every vector of $W_0 = W(H \cap \mathbf{G}_m^3)$ has a multiple of type \mathbf{a}' , we see that the components of $\mu(P')$ in (6) lie in the division group $\sqrt{\Gamma}$ of Γ .

We can now apply Liardet's Theorem in the slightly stronger form given in [La2, Theorem 7.3, p. 207] or [Li, Théorème 1, p. 187]. As \mathcal{C}'' is not contained in a proper coset, it follows that $\mu(P')$ lies in a finite set independent of P' . Since μ is a quasi-finite morphism, we conclude that the points $P = P' \times Q_0$ lie in a finite set independent of P' (or H), thereby proving what we want.

We are now in a position to follow through the proof of our Theorem. Let K be a number field of definition for \mathcal{C} . In establishing the finiteness of the set of points P of $\mathcal{C} \cap \mathcal{H}$ we may restrict attention to those P lying in some H of dimension exactly $n - 2$. It follows from Lemma 3(a) that $H' = H \cap \mathbf{G}_m^3$ is a subgroup of dimension 1.

As $\mathcal{C}' \subset \mathbf{G}_m^3$ is not contained in a proper coset, Lemma 2(a) shows that $\mathcal{X} = \varphi(\mathcal{C}' \times \mathcal{C}')$ is a surface, clearly irreducible, for the quotient map φ associated with \mathbf{G}_m^3 .

Write $P = P' \times Q_0$ on $\mathcal{C} = \mathcal{C}' \times Q_0$, and let σ be any element of the Galois group $\text{Gal}(\overline{K}/K)$. Writing down equations (5) for P as in (1), applying σ and eliminating the offending translate $Q_0 = \sigma(Q_0)$, we find that the point

$$(7) \quad P_\sigma = \varphi(\sigma(P'), P')$$

as in (3) lies in H' , as in (2). Because $\sigma(P')$ is also in \mathcal{C}' , it follows that P_σ lies in $\mathcal{X} \cap \mathcal{H}_1$, in the notation of Theorem B(b).

There are now two cases to distinguish. The first and easiest is when there is σ such that P_σ lies in \mathcal{X}° but not in the finite set Z of Lemma 2(b). Then Theorem B(b) implies that the height of P_σ is bounded independently of P and σ , and Lemma 2(b) implies that the same is true of the height of P' . Thus the same holds for $P = P' \times Q_0$ on $\mathcal{C} \cap H$ and now our Theorem follows from an application of Lemma 1.

The second case is when P_σ lies in $\mathcal{X} \setminus \mathcal{X}^\circ$ or Z for every σ . Theorem B(a) tells us that $\mathcal{X} \setminus \mathcal{X}^\circ$ is a finite union of $\alpha^{-1}(\mathbf{G}_m^k \times \mathcal{Y})$, for automorphisms α of \mathbf{G}_m^3 , positive integers k , and varieties \mathcal{Y} in \mathbf{G}_m^{3-k} . As \mathcal{X} is a surface, each $k = 1$ or 2 .

If $k = 1$, then the corresponding \mathcal{Y} must in fact be a finite set. Otherwise \mathcal{Y} is a curve in \mathbf{G}_m^2 and $\alpha(\mathcal{X}) = \mathbf{G}_m \times \mathcal{Y}$. Now the projection \mathcal{C}'' of $\alpha(\mathcal{C}')$ to \mathbf{G}_m^2 would satisfy $\varphi(\mathcal{C}'' \times \mathcal{C}'') = \mathcal{Y}$ for the quotient map associated with \mathbf{G}_m^2 . Then Lemma 2(a) would imply that \mathcal{C}'' is contained in a proper coset. So $\alpha(\mathcal{C}')$, and therefore also \mathcal{C}' , would be contained in a proper coset, which we have ruled out near the beginning of this section.

Similarly, the possibility $k = 2$ can be entirely eliminated, for then $\alpha(\mathcal{X}) = \mathbf{G}_m^2 \times \mathcal{Y}$ for a single point \mathcal{Y} in \mathbf{G}_m and we could argue as above with the projection of $\alpha(\mathcal{C}')$ to \mathbf{G}_m .

Thus if P_σ lies in $\mathcal{X} \setminus \mathcal{X}^\circ$, then it lies in a fixed union of cosets $y_1 H_1, \dots, y_s H_s$, defined over $\overline{\mathbf{Q}}$, with irreducible H_1, \dots, H_s of dimension 1. Also if P_σ lies in Z , this situation can be included simply by increasing s . So from now on we can assume that P_σ lies in the union of $y_1 H_1, \dots, y_s H_s$, for all σ in $\text{Gal}(\overline{K}/K)$. This property is preserved if we replace K by a finite extension over which $y_1 H_1, \dots, y_s H_s$ are defined. Now y_1, \dots, y_s lie in $\mathbf{G}_m^3(K)$.

Let us first dispose of the possibility that our original $H' = H \cap \mathbf{G}_m^3$ has some $y_i H_i$ ($1 \leq i \leq s$) as an irreducible component. Then H lies in the set $\mathcal{H}(W_i)$ defined

in Lemma 3(b) for $W_i = W(H_i)$. Therefore P in $\mathcal{C} \cap H$ lies in the finite set $\mathcal{C} \cap \mathcal{H}(W_i)$ independent of P . This means that in continuing the proof of our Theorem we may further assume that $y_1 H_1, \dots, y_s H_s$ are not irreducible components of H' .

We next claim the existence of a positive integer M , possibly depending on P , such that P'^M lies in $\mathbf{G}_m^3(K)$.

To start with, P_σ lies in some zero-dimensional $H' \cap y_i H_i$, which we can write as $z_i(H' \cap H_i)$ for some z_i . So $H' \cap H_i$ is a finite subgroup of \mathbf{G}_m^3 , of order say m_i . The finite set $z_i(H' \cap H_i)$ is defined over K . Considering m_i -th powers we deduce that $z_i^{m_i} \in \mathbf{G}_m^3(K)$. It follows that $P_\sigma^{m_i} \in \mathbf{G}_m^3(K)$ and so $P_\sigma^m \in \mathbf{G}_m^3(K)$ for $m = m_1 \cdots m_s$.

This holds for all σ in $\text{Gal}(\overline{K}/K)$; let us therefore consider P_σ^m for fixed P as a function $\chi(\sigma)$ of σ . For any τ in $\text{Gal}(\overline{K}/K)$ we calculate from (7): $\chi(\tau\sigma) = \chi(\tau)(\tau(\chi(\sigma))) = \chi(\tau)\chi(\sigma)$. Thus χ is a homomorphism from $\text{Gal}(\overline{K}/K)$ to $\mathbf{G}_m^3(K)$. As P' is defined over some number field, the image of χ is a finite group, say of order l . Thus $P_\sigma^M = 1$ for $M = ml$ and all σ . We conclude that P'^M lies in $\mathbf{G}_m^3(K)$, as desired.

The final stage of the proof is expressed in terms of valuations. Recall that $P' = (x_1, x_2, x_3)$ was a point on the curve \mathcal{C}' in \mathbf{G}_m^3 defined over K . Select non-zero polynomials f_1, f_2, f_3 over K vanishing on the various projections of \mathcal{C}' to \mathbf{G}_m^2 . Let V be the set of non-archimedean valuations on K which are trivial on the group Γ (generated by g_1, \dots, g_n) and on the non-zero coefficients of f_1, f_2, f_3 . The complementary set S of all other valuations on K is finite. For each $v \in V$ we fix once and for all an extension, again denoted by v , to \overline{K} .

Let $v \in V$ and consider the equation $f_3(x_1, x_2) = 0$. Since v is non-archimedean there must appear two monomials with the same value, and since v is trivial on the coefficients of f_3 we get an additive relation $b_1 v(x_1) + b_2 v(x_2) = 0$, where $(b_1, b_2) \in \mathbf{Z}^2$ is non-zero taken from a finite set independent of P' or v . The same argument applies to any pair $v(x_i), v(x_j)$ with $1 \leq i < j \leq 3$.

Therefore the point $v(P') = (v(x_1), v(x_2), v(x_3))$ lies in a finite set of \mathbf{Q} -vector spaces of dimension at most 1, also independent of P' or v .

Suppose first that $v(P') = 0$ for every v in V . Then each x_i^M belongs to the finitely generated group Γ_S of S -units of K . So x_i is in the division group $\sqrt{\Gamma_S}$, and we can apply Liardet's Theorem to finish the proof of our Theorem in this case.

Suppose then instead that there is v in V with $v(P') \neq 0$, so that $v(P')$ lies in a finite set of \mathbf{Q} -vector spaces U of dimension 1. Writing down the equations (5) for $P = P' \times Q_0$ in H , applying v and using that v is trivial on Γ , we deduce that $a_1 v(x_1) + a_2 v(x_2) + a_3 v(x_3) = 0$ for all $\mathbf{a}' = (a_1, a_2, a_3)$ in the equations defining $H' = H \cap \mathbf{G}_m^3$. So this holds for all \mathbf{a}' in $W(H')$, and hence the latter two-dimensional space is determined by its orthogonality to some U . We can therefore apply Lemma 3(b) once more, and this completes the proof of our Theorem.

To deduce the Corollary we may split into three cases. Let \mathcal{C} be a curve in \mathbf{G}_m^5 not contained in a proper torsion coset.

First, if \mathcal{C} is not contained in any proper coset, then the result follows from Theorem A above.

Second, if \mathcal{C} is contained in a coset of dimension 3, then it follows from the Theorem above.

Finally, if \mathcal{C} is contained in a coset of dimension 4, then after an automorphism we can suppose that $\mathcal{C} = \mathcal{C}' \times Q_0$ with \mathcal{C}' in \mathbf{G}_m^4 and Q_0 in \mathbf{G}_m . If $P = P' \times Q_0$

is in $\mathcal{C} \cap \mathcal{H}$ (“two relations”), then P' in \mathcal{C}' lies in a proper algebraic subgroup of \mathbf{G}_m^4 (“one relation”). Should \mathcal{C}' lie in a coset of dimension 3, then so does \mathcal{C} and we are back in the second case. Otherwise we can apply Theorem 1 of [BMZ] to \mathcal{C}' and we deduce that P' has bounded height. Thus $P = P' \times Q_0$ also has bounded height. We conclude using Lemma 1 above.

APPENDIX: A CONJECTURE OF SHOU-WU ZHANG

We shall now briefly discuss the conjecture of Zhang alluded to above. Although Zhang formulated the conjecture for commutative algebraic groups more general than \mathbf{G}_m^h and varieties other than curves, here we shall limit ourselves to the cases relevant to this paper.

We start with a modified definition of multiplicative dependence of morphisms, due to Zhang. Then let \mathcal{C} be a quasi-projective irreducible curve over \mathbf{Q} and let $f_1, \dots, f_N : \mathcal{C} \rightarrow \mathbf{G}_m^h$ be morphisms over \mathbf{Q} .

Definition. We say that f_1, \dots, f_N are *Zhang-independent* if for any integers a_1, \dots, a_N , not all zero, the Zariski closure of $f_1^{a_1} \cdots f_N^{a_N}(\mathcal{C})$ is not a torsion coset in \mathbf{G}_m^h .

We do not insist here that the alluded torsion coset is proper. Observe that if the f_i are multiplicatively dependent, then some non-trivial combination $f_1^{a_1} \cdots f_N^{a_N}(\mathcal{C})$ is the identity of \mathbf{G}_m^h , whence the f_i are *a fortiori* Zhang-dependent. In other words, this notion of independence is stronger than the usual one. With this definition we have:

Conjecture Z. *Let f_1, \dots, f_N be morphisms from \mathcal{C} to \mathbf{G}_m^h which are Zhang-independent. Then for all but finitely many points $P \in \mathcal{C}(\overline{\mathbf{Q}})$ the values $f_1(P), \dots, f_N(P)$ are multiplicatively independent.*

We shall show the equivalence of Conjecture Z with Conjecture A stated in §1 above.

Part (i): Conjecture Z \Rightarrow Conjecture A. Let $\mathcal{C} \subset \mathbf{G}_m^n$ ($n \geq 2$) be a curve not contained in any proper torsion coset, so the coordinates x_1, \dots, x_n on \mathcal{C} are multiplicatively independent rational functions. By applying Conjecture Z to suitable data, we proceed to show that $\mathcal{C} \cap \mathcal{H}$ is finite.

We choose $N := (n-1)^2$ morphisms $f_i : \mathcal{C} \rightarrow \mathbf{G}_m^n$ by taking $f_i := (\mathbf{x}^{\mathbf{v}_{i1}}, \dots, \mathbf{x}^{\mathbf{v}_{in}})$, for “generic” (in a sense to be explained) integral vectors $\mathbf{v}_{ij} \in \mathbf{Z}^n$, $i = 1, \dots, N$, $j = 1, \dots, n$.¹ Then we have

$$(8) \quad f_1^{a_1} \cdots f_N^{a_N} = (\mathbf{x}^{a_1 \mathbf{v}_{11} + \cdots + a_N \mathbf{v}_{N1}}, \dots, \mathbf{x}^{a_1 \mathbf{v}_{1n} + \cdots + a_N \mathbf{v}_{Nn}}).$$

This expression shows that for the f_i to be Zhang-independent it is necessary and sufficient that the rank of the n vectors $a_1 \mathbf{v}_{1j} + \cdots + a_N \mathbf{v}_{Nj}$, $j = 1, \dots, n$, is ≥ 2 for any choice of the integers² a_i , not all zero. We prove in a short lemma that the integral vectors \mathbf{v}_{ij} may be chosen with such property.

Lemma A. *For any integer $n \geq 2$, there exist integral vectors $\mathbf{v}_{ij} \in \mathbf{Z}^n$, $i = 1, \dots, N = (n-1)^2$, $j = 1, \dots, n$, such that for any complex numbers a_1, \dots, a_N the rank of the n vectors $a_1 \mathbf{v}_{1j} + \cdots + a_N \mathbf{v}_{Nj}$ is ≤ 1 if and only if $a_1 = \cdots = a_N = 0$.*

¹Here we adopt the usual notation $\mathbf{x}^{\mathbf{v}} := x_1^{v_1} \cdots x_n^{v_n}$ for $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{v} = (v_1, \dots, v_n)$.

²This integrality will not matter in what follows; introducing it would lead to a notion of *virtual* Zhang-dependence which we do not pursue here.

Proof of lemma. A little inspection shows that we have to prove the existence of an $n \times n$ integer matrix $\mathbf{M} = \mathbf{M}(\mathbf{a})$, whose entries are linear forms in the $N = (n - 1)^2$ numbers a_1, \dots, a_N , with the property that

$$\text{rank } \mathbf{M}(\mathbf{a}) \leq 1 \quad \Rightarrow \quad \mathbf{a} := (a_1, \dots, a_N) = 0.$$

Now, it is not difficult to see that $2n - 1$ generic bilinear forms in $\mathbf{u} = (u_1, \dots, u_n)$, $\mathbf{w} = (w_1, \dots, w_n)$ have no common zero in $\mathbf{P}_{n-1} \times \mathbf{P}_{n-1}$ (either by an inductive process, or using Segre coordinates in \mathbf{P}_{n^2-1} , or by the theory of mixed resultants as for example in [GKZ, p. 438]). Consider the $2n - 1$ terms $u_i w_j$ involving u_n or w_n ; these may be indexed by (i, j) in $K_n := \{1, \dots, n\}^2 \setminus \{1, \dots, n - 1\}^2$. The corresponding coefficient vectors in the bilinear forms are independent. Therefore, by taking suitable linear combinations we can assume that the above bilinear forms have the shape

$$B_{ij} = u_i w_j - C_{ij} \quad ((i, j) \in K_n),$$

with C_{ij} bilinear in $u_1, \dots, u_{n-1}, w_1, \dots, w_{n-1}$. By specialization we can further assume that the coefficients of C_{ij} are in \mathbf{Z} . Introduce the N variables $y_{rs} = u_r w_s$ (for $(r, s) \in \{1, \dots, n - 1\}^2$) and express C_{ij} as a linear form $L_{ij}(\mathbf{y})$ in the y_{rs} , for $(i, j) \in K_n$. Also, define $L_{ij} = y_{ij}$ for the remaining $(i, j) \in \{1, \dots, n - 1\}^2$. These linear forms now define the required matrix \mathbf{M} , after we identify a_1, \dots, a_N with some ordering of the y_{rs} .

Why is this? Suppose that for some complex value \mathbf{y} the rank of $\mathbf{M}(\mathbf{y})$ is at most 1. Then there are complex \mathbf{u}, \mathbf{w} with $u_i w_j = L_{ij}(\mathbf{y})$, for $(i, j) \in \{1, \dots, n\}^2$. In particular, $u_r w_s = y_{rs}$ for $(r, s) \in \{1, \dots, n - 1\}^2$ and now the other equations

$$u_i w_j = L_{ij}(\mathbf{y}) = C_{ij}(u_1, \dots, u_{n-1}, w_1, \dots, w_{n-1}), \quad (i, j) \in K_n,$$

imply that $\mathbf{u} = 0$ or $\mathbf{w} = 0$; in either case we get the required $\mathbf{y} = 0$, finally proving the lemma.

Coming back to the morphisms f_i , recall using (8) that the lemma proves that they may be chosen to be Zhang-independent, as we shall assume.

We now apply the Conjecture Z to our curve \mathcal{C} and morphisms f_i . We conclude that for all $P \in \mathcal{C}(\overline{\mathbf{Q}})$ outside a certain finite set Σ the values $f_i(P)$, $i = 1, \dots, N$, are multiplicatively independent.

Now let $P \in \mathcal{C}(\overline{\mathbf{Q}})$ lie in $\mathcal{C} \cap \mathcal{H}$, i.e. in some algebraic subgroup of codimension ≥ 2 . Then the multiplicative rank of the group G generated by the coordinates of P is $\leq n - 2$. Thus the vectors $f_1(P), \dots, f_N(P)$ lie in the Cartesian product G^n , whose rank is at most $n(n - 2)$. As $N = (n - 1)^2 > n(n - 2)$ these vectors must be multiplicatively dependent. In view of the above, we conclude that P lies in the finite set Σ , proving the conclusion of Conjecture A for the curve \mathcal{C} , and proving therefore the implication in question.

Part (ii): Conjecture A \Rightarrow Conjecture Z. Now let f_1, \dots, f_N be Zhang-independent morphisms from \mathcal{C} to \mathbf{G}_m^h . We start by disposing of an easy case: if f_1, \dots, f_N are all constant, then the conclusion of Conjecture Z holds unconditionally. This is because the dependence of any values $f_1(P), \dots, f_N(P)$ would immediately imply the Zhang-dependence of the morphisms f_1, \dots, f_N .

Therefore we can assume that f_1, \dots, f_N are not all constant. Each morphism has h coordinates which are morphisms from \mathcal{C} to \mathbf{G}_m , and so the complete set of

Nh coordinates generate a group of multiplicative rank $n \geq 1$. Choose a basis $\varphi = (\varphi_1, \dots, \varphi_n)$ of representatives modulo torsion. Then for any integers a_1, \dots, a_N we have

$$(9) \quad f_1^{a_1} \cdots f_N^{a_N} = (\zeta_1 \varphi^{a_1 \mathbf{v}_{11} + \cdots + a_N \mathbf{v}_{N1}}, \dots, \zeta_h \varphi^{a_1 \mathbf{v}_{1h} + \cdots + a_N \mathbf{v}_{Nh}})$$

for roots of unity ζ_1, \dots, ζ_h depending on a_1, \dots, a_N and integral vectors $\mathbf{v}_{ij} \in \mathbf{Z}^n$ ($1 \leq i \leq N, 1 \leq j \leq h$) not depending on a_1, \dots, a_N .

We now contend that the following version of the property in Lemma A holds: for any integers a_1, \dots, a_N , either $f_1^{a_1} \cdots f_N^{a_N}$ is a constant morphism or the rank of the vectors $a_1 \mathbf{v}_{1j} + \cdots + a_N \mathbf{v}_{Nj}$ ($1 \leq j \leq h$) is at least 2. In fact, if the latter rank is at most 1, then by (9) $f_1^{a_1} \cdots f_N^{a_N}(\mathcal{C})$ is contained in a one-dimensional torsion coset in \mathbf{G}_m^h . So its Zariski-closure must be either a single point or the whole of this coset. The second possibility is excluded by Zhang-independence, and the above contention follows.

Assume now that $P \in \mathcal{C}$ is an algebraic point such that the values $f_1(P), \dots, f_N(P)$ are dependent, so that a relation $(f_1(P))^{a_1} \cdots (f_N(P))^{a_N} = (1, \dots, 1)$ in \mathbf{G}_m^h holds for some integers a_1, \dots, a_N not all zero. Now $f_1^{a_1} \cdots f_N^{a_N}$ cannot be a constant, or else this constant would be $(1, \dots, 1)$, contradicting the Zhang-independence. So, in view of the above contention, the rank of the $a_1 \mathbf{v}_{1j} + \cdots + a_N \mathbf{v}_{Nj}$ ($1 \leq j \leq h$) in \mathbf{Z}^n is at least 2. In particular $n \geq 2$ and (9) shows that $\varphi(P)$ lies in an algebraic subgroup of \mathbf{G}_m^n of dimension at most $n - 2$.

The conclusion of Conjecture A for the curve $\varphi(\mathcal{C})$ in \mathbf{G}_m^n then says that $\varphi(P)$ lies in a finite set independent of P .

Now φ is not constant because we assumed that f_1, \dots, f_N are not all constant. Thus the point P also lies in a finite set, proving the conclusion of Conjecture Z and the second half of the equivalence.

ACKNOWLEDGEMENT

We are grateful to the Institute for Advanced Study (Princeton), the Mathematisches Institut (University of Basel) and the Istituto Universitario di Architettura (Venice) for hospitality and support during the preparation of this paper, and we reiterate our thanks to Shou-Wu Zhang for permission to mention his conjecture.

REFERENCES

- [AD] F. Amoroso, S. David, Le problème de Lehmer en dimension supérieure, *J. Reine Angew. Math.* **513** (1999), 145-179. MR1713323 (2001a:11116)
- [AZ] F. Amoroso, U. Zannier, A relative Dobrowolski lower bound over abelian extensions, *Ann. Scuola Norm. Sup. Pisa* **29** (2000), 711-727. MR1817715 (2003a:11078)
- [BMZ] E. Bombieri, D. Masser and U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, *International Math. Research Notices* **20** (1999), 1119-1140. MR1728021 (2001c:11081)
- [BZ] E. Bombieri, U. Zannier, Algebraic points on subvarieties of \mathbf{G}_m^n , *International Math. Research Notices* **7** (1995), 333-347. MR1350686 (96h:11061)
- [CZ] P.B. Cohen, U. Zannier, Multiplicative independence and bounded height, an example, *Proc. Algebraic Number Theory and Dioph. Approx. Conference, Graz, 1998* (Walter de Gruyter, 2000), 93-101. MR1770456 (2001f:11103)
- [GKZ] I.M. Gelfand, M.M. Kapranov, A.V. Zelevinski, *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, 1993. MR1264417 (95e:14045)
- [La1] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley, 1973. MR0344244 (49:8983)
- [La2] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983. MR0715605 (85j:11005)

- [Li] P. Liardet, Sur une conjecture de Serge Lang, *Astérisque* **24-25** (1975), 187-210. MR0376688 (51:12863)
- [RV] G. Rémond, E. Viada, Problème de Mordell-Lang modulo certaines sous-variétés abéliennes, *International Math. Research Notices* **35** (2003), 1915-1931. MR1995142 (2004h:11054)
- [S] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopaedia of Mathematics and its Applications, vol. **77**, Cambridge, 2000. MR1770638 (2001h:11135)
- [Zag] D. Zagier, Algebraic numbers close to both 0 and 1, *Math. Comp.* **61** (1993), 485-491. MR1197513 (94c:11104)
- [Zan] U. Zannier, *Proof of Conjecture 1*, Appendix to [S]. MR1770638 (2001h:11135)
- [Zh] S. Zhang, Positive line bundles on arithmetic surfaces, *Annals of Math.* **136** (1992), 569-587. MR1189866 (93j:14024)

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540
E-mail address: `eb@math.ias.edu`

MATHEMATISCHES INSTITUT, UNIVERSITÄT BASEL, RHEINSPRUNG 21, CH-4051 BASEL, SWITZERLAND
E-mail address: `masser@math.unibas.ch`

SCUOLA NORMALE SUPERIORE, PIAZZA DEI CAVALIERI, 56100 PISA, ITALY
E-mail address: `u.zannier@sns.it`