MULTIPLICATIVE AND LINEAR DEPENDENCE IN FINITE FIELDS AND ON ELLIPTIC CURVES MODULO PRIMES

FABRIZIO BARROERO, LAURA CAPUANO, LÁSZLÓ MÉRAI, ALINA OSTAFE, AND MIN SHA

Abstract. For positive integers K and L, we introduce and study the notion of K-multiplicative dependence over the algebraic closure $\overline{\mathbb{F}}_p$ of a finite prime field $\mathbb{F}_p$, as well as L-linear dependence of points on elliptic curves in reduction modulo primes. One of our main results shows that, given non-zero rational functions $\varphi_1, \ldots, \varphi_m, \varrho_1, \ldots, \varrho_n \in \mathbb{Q}(X)$ and an elliptic curve E defined over the integers $\mathbb{Z}$, for any sufficiently large prime p, for all but finitely many $\alpha \in \overline{\mathbb{F}}_p$, at most one of the following two can happen: $\varphi_1(\alpha), \ldots, \varphi_m(\alpha)$ are K-multiplicatively dependent or the points $(\varrho_1(\alpha), \cdot), \ldots, (\varrho_n(\alpha), \cdot)$ are L-linearly dependent on the reduction of E modulo p. As one of our main tools, we prove a general statement about the intersection of an irreducible curve in the split semiabelian variety $\mathbb{G}_{\mathrm{m}}^m \times E^n$ with the algebraic subgroups of codimension at least 2.

As an application of our results, we improve a result of M. C. Chang and extend a result of J. F. Voloch about elements of large order in finite fields in some special cases.

Contents

2010 *Mathematics Subject Classification.* 11T30, 11G05, 11G20, 11U09.

Key words and phrases. Multiplicative dependence, linear dependence, rational function, elliptic curve, finite field, unlikely intersection, o-minimality.

1. Introduction

We say that n non-zero complex numbers $\alpha_1, \dots, \alpha_n$ are *multiplicatively dependent* if there exists a non-zero integer vector $(k_1, \dots, k_n) \in \mathbb{Z}^n$ such that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1. \tag{1.1}$$

Consequently, a point in the complex space $\mathbb{C}^n$ is called *multiplicatively dependent* if its coordinates are all non-zero and are multiplicatively dependent. The same definition of multiplicative dependence applies to rational functions as well.

Moreover, we say that non-zero rational functions $f_1, \dots, f_n \in \mathbb{C}(X)$ are *multiplicatively independent modulo constants* if there is no non-zero integer vector $(k_1, \dots, k_n)$ such that

$$f_1^{k_1} \cdots f_n^{k_n} \in \mathbb{C}^*.$$

Multiplicative dependence of algebraic numbers and of rational functions has been studied extensively in recent years from various aspects; see, for instance, [6, 7, 9, 16, 31, 32, 33, 39]. In particular, a result of Bombieri, Masser and Zannier [9] in the context of unlikely intersections over tori says that given n non-zero multiplicatively independent modulo constants rational functions $f_1, \dots, f_n \in \overline{\mathbb{Q}}(X)$, there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that $f_1(\alpha), \dots, f_n(\alpha)$ satisfy two independent multiplicative relations. This result has been later extended over $\mathbb{C}$ in [10] (and in fact over the algebraic closure of any field of characteristic zero), and also relaxed by Maurin [27] over $\overline{\mathbb{Q}}$ and by Bombieri, Masser and Zannier [11] over $\mathbb{C}$ showing it holds for rational functions which are multiplicatively independent only.

The analogous problem of linear dependence of points on elliptic curves was considered not long after [9], for instance in [41]. The finiteness result corresponding to Maurin's Theorem was proved by Viada in [42] under some conjecture that was later showed by Galateau in [18].

In this paper, we are interested in studying the multiplicative dependence of elements in the algebraic closure of a finite prime field and the linear dependence of points on elliptic curves modulo primes.

For a prime p, let $\overline{\mathbb{F}}_p$ denote the algebraic closure of the field $\mathbb{F}_p$ of p elements. Note that any element of $\overline{\mathbb{F}}_p^*$ has finite order, so Maurin's finiteness result in characteristic 0 does not hold in full generality in positive characteristic. In this context, Masser proposed some conjecture in positive characteristic putting more restrictive hypothesis on the rational functions in order to recover Maurin's finiteness result [27], and proved it for $n = 3$ [28, Theorem 1.1]. For other results on unlikely intersections in positive characteristic, see also [20, 36, 37].

In this paper we refine the notion of multiplicative dependence over $\overline{\mathbb{F}}_p$ defined by (1.1), and we introduce the following concept.

Definition 1.1 (*K-multiplicative dependence*)**.** Let K be a positive integer. We say that elements $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_p^*$ are *K-multiplicatively dependent* if there exists a non-zero integer vector $(k_1, \ldots, k_n)$ such that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1 \quad \text{and} \quad \max_{i=1,\ldots,n} |k_i| \le K.$$

We use $\mathrm{ord}_p(\alpha)$ to denote the multiplicative order of $\alpha \in \overline{\mathbb{F}}_p^*$ (that is, the size of the multiplicative group generated by α).

Let E be an elliptic curve defined by a Weierstrass equation over the rational integers $\mathbb{Z}$:

$$Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{Z}, \quad 4a^3 + 27b^2 \neq 0. \tag{1.2}$$

If the reduction of E modulo p, denoted by E_p, is also an elliptic curve (that is, $p > 2$ and $4a^3 + 27b^2 \not\equiv 0 \pmod p$), then for any $\alpha \in \overline{\mathbb{F}}_p$, we define $\mathrm{ord}_E(\alpha)$ to be the order of the point (α, β) on the elliptic curve E_p for some $\beta \in \overline{\mathbb{F}}_p$. We always denote by O the point at infinity of an elliptic curve.

Definition 1.2 (*L-linear dependence*)**.** Let L be a positive integer. We say that the points $P_1, \ldots, P_n$ on the reduction E_p of the elliptic curve E modulo p (assuming E_p is also an elliptic curve) are *L-linearly dependent* if there exists a non-zero integer vector $(k_1, \ldots, k_n)$ such that

$$k_1 P_1 + \cdots + k_n P_n = O \quad \text{and} \quad \max_{i=1,\ldots,n} |k_i| \le L. \tag{1.3}$$

Moreover, for any $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{F}}_p$, we say that the points

$$(\alpha_1, \cdot), \ldots, (\alpha_n, \cdot) \tag{1.4}$$

are *L-linearly dependent* if the points $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)$ are L-linearly dependent for some $\beta_1, \ldots, \beta_n \in \overline{\mathbb{F}}_p$ such that $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n) \in E_p$.

We remark that for each $\alpha_i \in \overline{\mathbb{F}}_p$ there is some $\beta_i \in \overline{\mathbb{F}}_p$ such that $(\alpha_i, \beta_i) \in E_p$. As the curve E is defined by the Weierstrass equation (1.2), the value β_i is unique up to sign and moreover $-(\alpha_i, \beta_i) = (\alpha_i, -\beta_i)$ on E_p. Thus, by changing the sign of the coefficients k_i in (1.3) if necessary, we see that the notion of L-linearly dependence of (1.4) does not depend on the choices of β_i. Here and there we also say that $(\alpha_i, \cdot)$ is a point (by fixing the second coordinate as β_i or $-\beta_i$). Moreover, these notions also apply to elliptic curves defined over an arbitrary field.

2. Main results

In this section we present the main results of this paper, together with some consequences. The proofs will be given in Section 5.

Here and in the rest of the paper, for $\alpha \in \overline{\mathbb{F}}_p$ and $f \in \mathbb{Q}(X)$, the expression $f(\alpha)$ indicates the element of $\overline{\mathbb{F}}_p$ that is obtained by substituting α in the reduction modulo p of the rational function f, when this is possible. We implicitly exclude the primes p such that the reductions of the rational functions we are considering are not defined.

Let E be an elliptic curve defined as in (1.2). Let K, L be two positive integers, and let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ whose components are all non-zero rational functions in $\mathbb{Q}(X)$. Informally, three of our main results can be summarised as follows: under some natural conditions on the involved functions and the curve, for any sufficiently large prime p, one has:

- the number of elements $\alpha \in \overline{\mathbb{F}}_p$, for which $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ satisfy two independent multiplicative relations with exponents bounded above by K, L in absolute value, respectively, can be upper bounded independently of p, K, L;
- the number of elements $\alpha \in \overline{\mathbb{F}}_p$, for which $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ are K-multiplicatively dependent and the points
$$(\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot)$$
are L-linearly dependent on E_p, can be upper bounded independently of p, K, L;
- the number of elements $\alpha \in \overline{\mathbb{F}}_p$, for which $(\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot)$ satisfy two independent linear relations over $\mathbb{Z}$ with coefficients bounded above by K, L in absolute value, respectively, can be upper bounded independently of p, K, L.

In the sequel, we state the above three results precisely and present their consequences.

2.1. Multiplicative dependence with two independent relations.

Given $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m) \in \mathbb{Q}(X)^m$ a vector of non-zero rational functions, consider the set

$$\mathcal{S}_1 = \Big\{\alpha \in \overline{\mathbb{Q}} : \prod_{i=1}^{m} \varphi_i(\alpha)^{k_i} = \prod_{i=1}^{m} \varphi_i(\alpha)^{\ell_i} = 1 \text{ for some linearly independent } (k_1, \dots, k_m), (\ell_1, \dots, \ell_m) \in \mathbb{Z}^m \Big\}.$$

As noted in the introduction, by [27], if $\varphi_1, \dots, \varphi_m$ are multiplicatively independent, this set is finite and its cardinality is effectively computable, see Lemma 3.9 below.

For positive integers $K, L \geq 1$ and prime p, define the set

(2.1)
$$\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L) = \Big\{\alpha \in \overline{\mathbb{F}}_p : \prod_{i=1}^{m} \varphi_i(\alpha)^{k_i} = \prod_{i=1}^{m} \varphi_i(\alpha)^{\ell_i} = 1 \text{ for some linearly independent } (k_1, \dots, k_m), (\ell_1, \dots, \ell_m) \in \mathbb{Z}^m, \max_{i=1,\dots,m} |k_i| \leq K, \max_{i=1,\dots,m} |\ell_i| \leq L \Big\}.$$

Our first main result is the following:

Theorem 2.1. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m) \in \mathbb{Q}(X)^m$ whose components are non-zero multiplicatively independent rational functions. Then, there exists an effectively computable constant c_1 depending only on $\boldsymbol{\varphi}$ such that for arbitrary integers $K, L \geq 1$, and any prime $p > \exp(c_1 KL)$, for the set (2.1) we have*

$$\#\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L) \leq \#\mathcal{S}_1,$$

where $\#\mathcal{S}_1$ is effectively computable, and the elements of $\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$ come from the reduction modulo p of elements of $\mathcal{S}_1$.

We remark that recently Kerr, Mello and Shparlinski [25, Theorem 2.2], using similar ideas, established, for almost all primes p, a lower bound of the form $p^{1/(2m+2)+o(1)}$ for the order of all but finitely many vectors $(\varphi_1(\alpha), \dots, \varphi_m(\alpha))$, $\alpha \in \overline{\mathbb{F}}_p$, which satisfy two independent multiplicative relations as in the set $\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$. One can compare this with Corollary 2.5 below.

We have the following straightforward consequence. For this, we define

(2.2)
$$\mathcal{D}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p, K, L) = \{\alpha \in \overline{\mathbb{F}}_p : \ \varphi_1(\alpha), \dots, \varphi_m(\alpha) \text{ are } K\text{-multiplicatively dependent and } \varrho_1(\alpha), \dots, \varrho_n(\alpha) \text{ are } L\text{-multiplicatively dependent}\}.$$

Corollary 2.2. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ whose components are all non-zero rational functions in $\mathbb{Q}(X)$ such that $\varphi_1, \dots, \varphi_m, \varrho_1, \dots, \varrho_n$ are mulitplicatively independent. Then, there are two effectively computable constants c_1 and c_2, depending only on $\boldsymbol{\varphi}$ and $\boldsymbol{\varrho}$ such that for arbitrary integers $K, L \geq 1$, and any prime $p > \exp(c_1 KL)$, for the set (2.2) we have*

$$\#\mathcal{D}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p, K, L) \leq c_2.$$

Taking $m = n = 1$ and $K = L = \lceil c_3 (\log p)^{1/2} \rceil$ for some effectively computable constant c_3 depending only on $\varphi = \varphi_1$ and $\varrho = \varrho_1$ in Corollary 2.2, we directly obtain:

Corollary 2.3. *Let $\varphi, \varrho \in \mathbb{Q}(X)$ be non-zero rational functions such that φ, ϱ are multiplicatively independent. Then, there are three effectively computable constants c_1, c_2, c_3 depending only on φ, ϱ such that for any prime $p > c_1$, for all but c_2 elements $\alpha \in \overline{\mathbb{F}}_p$ we have*

$$\max\{\mathrm{ord}_p(\varphi(\alpha)), \mathrm{ord}_p(\varrho(\alpha))\} \geq c_3 (\log p)^{1/2}.$$

Corollary 2.3, applied to the curve $Y = \varphi(X)$, improves a result of Chang [13, Theorem 1.1] in this special case which is of the shape

$$\max\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\varphi(\alpha))\} \gg \left(\frac{\log p}{\log\log p}\right)^{1/2}.$$

The improvement of the same shape has been pointed out in [14, Section 5]. See [43] for an earlier work of Voloch.

One can also obtain a trade-off between the number of possible exceptional values α and the parameters K, L. Here, $v_p(u)$ denotes the p-adic valuation of a non-zero integer u (that is, the highest exponent v such that p^v divides u), and we define $v_p(0) = \infty$.

Theorem 2.4. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m) \in \mathbb{Q}(X)^m$ be defined as in Theorem 2.1. Then, there are two effectively computable constants c_1, c_2 depending only on $\boldsymbol{\varphi}$ such that for arbitrary integers $K, L \geq 1$, there is a positive integer T with*

$$\log T \leq c_1 (KL)^{m+1}$$

such that for any prime p and for the set (2.1) we have

$$\#\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L) \leq v_p(T) + c_2.$$

As a consequence, we obtain:

Corollary 2.5. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m) \in \mathbb{Q}(X)^m$ be defined as in Theorem 2.1. Then, there are two effectively computable constants c_1, c_2 depending only on $\boldsymbol{\varphi}$ such that as $N \to \infty$, for all but $c_1 N (\log N)^{-2}$ primes $p \leq N$ and for all but at most c_2 elements $\alpha \in \overline{\mathbb{F}}_p$, at least $m-1$ elements of $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ are of order at least $(N/\log N)^{1/(2m+2)}$.*

Similarly to Theorem 2.4, we have:

Theorem 2.6. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ be defined as in Corollary 2.2. Then, there are two effectively computable constants c_1, c_2 depending only on $\boldsymbol{\varphi}$ and $\boldsymbol{\varrho}$ such that for arbitrary integers $K, L \geq 1$, there is a positive integer T with*

$$\log T \leq c_1 K^{m+1} L^{n+1}$$

such that for any prime p and for the set (2.2) we have

$$\#\mathcal{D}_{\boldsymbol{\varphi},\boldsymbol{\varrho}}(p, K, L) \leq v_p(T) + c_2.$$

Using Theorem 2.6, we obtain the following corollary.

Corollary 2.7. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ be defined as in Corollary 2.2. Then, there are two effectively computable constants c_1, c_2 depending only on $\boldsymbol{\varphi}$ and $\boldsymbol{\varrho}$ such that as $N \to \infty$, for all but $c_1 N (\log N)^{-2}$ primes $p \leq N$ and for all but at most c_2 elements $\alpha \in \overline{\mathbb{F}}_p$, at least one of the two finitely generated subgroups of $\overline{\mathbb{F}}_p^*$*

$$\langle \varphi_1(\alpha), \dots, \varphi_m(\alpha) \rangle \qquad \text{and} \qquad \langle \varrho_1(\alpha), \dots, \varrho_n(\alpha) \rangle$$

is of order at least $N^{mn/(2mn+m+n)} (\log N)^{-1/2}$.

With $m = n = 1, \varrho_1 = X$ and $Y = \varphi_1(X)$, Corollary 2.7 recovers the result of Chang [13, Theorem 1.2] in this special case (see [14] for a generalisation to algebraic varieties).

2.2. **Multiplicative dependence and linear dependence.** We fix an elliptic curve E defined by (1.2). Given $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m) \in \mathbb{Q}(X)^m$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n) \in \mathbb{Q}(X)^n$ two vectors of non-zero rational functions, we define

$$\mathcal{S}_2 = \big\{ \alpha \in \overline{\mathbb{Q}} : \varphi_1(\alpha), \dots, \varphi_m(\alpha) \text{ are multiplicatively dependent and } (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \text{ are linearly dependent} \big\}.$$

Under the conditions of Theorem 2.8 below on $\boldsymbol{\varphi}$ and $\boldsymbol{\varrho}$, the set $\mathcal{S}_2$ is finite, as proved in Lemma 3.11.

For positive integers $K, L \geq 1$ and prime p, define the set

(2.3)
$$\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L) = \big\{\alpha \in \overline{\mathbb{F}}_p : \ \varphi_1(\alpha),\dots,\varphi_m(\alpha) \text{ are } K\text{-multiplicatively dependent and } (\varrho_1(\alpha),\cdot),\dots,(\varrho_n(\alpha),\cdot) \text{ are } L\text{-linearly dependent}\big\}.$$

For the cardinality $\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L)$, we have:

Theorem 2.8. *Let E be an elliptic curve defined by (1.2), and let $\boldsymbol{\varphi} = (\varphi_1,\dots,\varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1,\dots,\varrho_n)$ whose components are all non-zero rational functions in $\mathbb{Q}(X)$ such that $\varphi_1,\dots,\varphi_m$ are multiplicatively independent and the points $(\varrho_1(X),\cdot),\dots,(\varrho_n(X),\cdot)$ in $E(\overline{\mathbb{Q}(X)})$ are linearly independent over $\mathbb{Z}$. Suppose moreover that at least one of the following conditions holds:*

1. *$\varphi_1,\dots,\varphi_m$ are multiplicatively independent modulo constants;*
2. *the points $(\varrho_1(X),\cdot),\dots,(\varrho_n(X),\cdot)$ are linearly independent over the endomorphism ring $\mathrm{End}(E)$ modulo points in $E(\overline{\mathbb{Q}})$.*

Then, there exist an effectively computable constant c_1 depending only on $\boldsymbol{\varphi},\boldsymbol{\varrho},E$ such that for any $p > \exp(c_1KL^2)$, for the set (2.3) we have

$$\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L) \leq \#\mathcal{S}_2,$$

and the elements of $\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L)$ come from the reduction modulo p of elements of $\mathcal{S}_2$.

Taking $m = n = 1$ and $K = L = \lceil c_3(\log p)^{1/3}\rceil$ for some effectively computable constant c_3 depending only on $E, \varphi = \varphi_1$ and $\varrho = \varrho_1$ in Theorem 2.8, we get:

Corollary 2.9. *Let $\varphi, \varrho \in \mathbb{Q}(X)$ be non-constant rational functions. Then, there exist two effectively computable constants c_1, c_3 and a constant c_2 depending only on φ, ϱ, E such that for any prime $p > c_1$ and for all but c_2 elements $\alpha \in \overline{\mathbb{F}}_p$ we have*

$$\max\{\mathrm{ord}_p(\varphi(\alpha)), \mathrm{ord}_E(\varrho(\alpha))\} \geq c_3(\log p)^{1/3}.$$

A result of Voloch [44, Theorem 4.1] roughly states that for a point P on a fixed elliptic curve over a finite field, under some conditions about the order of P and the degree of the field generated by P, the order of the y-coordinate of P is large. So, Corollary 2.9 is somehow an extension of Voloch's result in large characteristic.

One can also obtain a trade-off between the number of possible exceptional values α and the parameters K, L.

Theorem 2.10. *Let $E, \boldsymbol{\varphi} = (\varphi_1,\dots,\varphi_m), \boldsymbol{\varrho} = (\varrho_1,\dots,\varrho_n)$ be defined as in Theorem 2.8. Then, there exist an effectively computable constant c_1 and a constant c_2 both depending only on $\boldsymbol{\varphi},\boldsymbol{\varrho},E$ such that for arbitrary integers $K, L \geq 1$, there is a positive integer T with*

$$\log T \leq c_1K^{m+1}L^{n+2}$$

such that for any prime p for which the reduction E_p of E is also an elliptic curve and for the set (2.3) we have

$$\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L) \leq v_p(T) + c_2.$$

Moreover, when $n = 1$, the constant c_2 is also effectively computable.

Using Theorem 2.10, we obtain the following corollary.

Corollary 2.11. *Let $E, \boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m), \boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ be defined as in Theorem 2.8. Then, there exist an effectively computable constant c_1 and a constant c_2 both depending only on $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ such that as $N \to \infty$, for all but $c_1 N (\log N)^{-2}$ primes $p \le N$ and for all but at most c_2 elements $\alpha \in \overline{\mathbb{F}}_p$, either the order of the subgroup $\langle \varphi_1(\alpha), \dots, \varphi_m(\alpha) \rangle$ in $\overline{\mathbb{F}}_p^*$ or the order of the subgroup $\langle (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \rangle$ in $E(\overline{\mathbb{F}}_p)$ is at least*

$$N^{mn/(2mn+2m+n)} (\log N)^{-1/2}.$$

Moreover, when $n = 1$, the constant c_2 is also effectively computable.

2.3. **Linear dependence with two independent relations.** Given $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n) \in \mathbb{Q}(X)^n$ a vector of non-zero rational functions, define the set

$$\mathcal{S}_3 = \Big\{ \alpha \in \overline{\mathbb{Q}} : \sum_{i=1}^{n} k_i(\varrho_i(\alpha), \cdot) = \sum_{i=1}^{n} \ell_i(\varrho_i(\alpha), \cdot) = O \text{ for some linearly independent } (k_1, \dots, k_n), (\ell_1, \dots, \ell_n) \in \mathbb{Z}^n \Big\}.$$

As mentioned in the introduction, under the conditions of Theorem 2.12 below on $\boldsymbol{\varrho}$, the set $\mathcal{S}_3$ was proved to be finite by Viada [42] and Galateau [18], see Lemma 3.10.

For positive integers $K, L \ge 1$ and prime p, define the set:

(2.4)

$$\mathcal{C}_{\boldsymbol{\varrho},E}(p, K, L) = \Big\{ \alpha \in \overline{\mathbb{F}}_p : \sum_{i=1}^{n} k_i(\varrho_i(\alpha), \cdot) = \sum_{i=1}^{n} \ell_i(\varrho_i(\alpha), \cdot) = O \text{ for some linearly independent } (k_1, \dots, k_n), (\ell_1, \dots, \ell_n) \in \mathbb{Z}^n, \max_{i=1,\dots,n} |k_i| \le K, \max_{i=1,\dots,n} |\ell_i| \le L \Big\}.$$

For the cardinality $\#\mathcal{C}_{\boldsymbol{\varrho},E}(p, K, L)$, we have:

Theorem 2.12. *Let $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n) \in \mathbb{Q}(X)^n$ be a vector of non-zero rational functions such that the points $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ in $E(\overline{\mathbb{Q}(X)})$ are linearly independent over $\mathrm{End}(E)$. Then, there exist an effectively computable constant c_1 depending only on $\boldsymbol{\varrho}, E$ such that for arbitrary integers $K, L \ge 1$, and any prime $p > \exp(c_1 K^2 L^2)$, for the set (2.4) we have*

$$\#\mathcal{C}_{\boldsymbol{\varrho},E}(p, K, L) \le \#\mathcal{S}_3,$$

and the elements of $\mathcal{C}_{\boldsymbol{\varrho},E}(p, K, L)$ come from the reduction modulo p of elements of $\mathcal{S}_3$.

We have the following straightforward consequence about the set:

$$\mathcal{E}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) = \big\{ \alpha \in \overline{\mathbb{F}}_p : (\varphi_1(\alpha), \cdot), \dots, (\varphi_m(\alpha), \cdot) \text{ are } K\text{-linearly dependent and } (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \text{ are } L\text{-linearly dependent} \big\} \tag{2.5}$$

Corollary 2.13. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ whose components are all non-zero rational functions in $\mathbb{Q}(X)$ such that the points $(\varphi_1(X), \cdot), \dots, (\varphi_m(X), \cdot)$, $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ in $E(\overline{\mathbb{Q}(X)})$ are linearly independent over $\mathrm{End}(E)$. Then, there exist an effectively computable constant c_1 and a constant c_2 both depending only*

on $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ *such that for arbitrary integers* $K, L \geq 1$*, and any prime* $p > \exp(c_1 K^2 L^2)$*, for the set* (2.2) *we have*

$$\#\mathcal{E}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) \leq c_2.$$

Taking $m = n = 1$ and $K = L = \lceil c_3(\log p)^{1/4} \rceil$ for some effectively computable constant c_3 depending only on $E, \varphi = \varphi_1$ and $\varrho = \varrho_1$ in Corollary 2.13, we directly have:

Corollary 2.14. *Let* $\varphi, \varrho \in \mathbb{Q}(X)$ *be non-zero rational functions such that the two points* $(\varphi(X), \cdot), (\varrho(X), \cdot)$ *in* $E(\overline{\mathbb{Q}(X)})$ *are linearly independent over* $\mathrm{End}(E)$*. Then, there exist two effectively computable constants* c_1, c_3 *and a constant* c_2 *all depending only on* φ, ϱ, E *such that for any prime* $p > c_1$*, for all but* c_2 *elements* $\alpha \in \overline{\mathbb{F}}_p$ *we have*

$$\max\{\mathrm{ord}_E(\varphi(\alpha)), \mathrm{ord}_E(\varrho(\alpha))\} \geq c_3(\log p)^{1/4}.$$

One can also obtain a trade-off between the number of possible exceptional values α and the parameters K, L.

Theorem 2.15. *Let* $\boldsymbol{\varrho} = (\varrho_1, \ldots, \varrho_n) \in \mathbb{Q}(X)^n$ *be defined as in Theorem 2.12. Then, there exist an effectively computable constant* c_1 *and a constant* c_2 *both depending only on* $\boldsymbol{\varrho}, E$ *such that for arbitrary integers* $K, L \geq 1$*, there is a positive integer* T *with*

$$\log T \leq c_1(KL)^{n+2}$$

such that for any prime p *for which the reduction* E_p *of* E *is also an elliptic curve and for the set* (2.4) *we have*

$$\#\mathcal{C}_{\boldsymbol{\varrho},E}(p, K, L) \leq v_p(T) + c_2.$$

As a consequence, we obtain:

Corollary 2.16. *Let* $\boldsymbol{\varrho} = (\varrho_1, \ldots, \varrho_n) \in \mathbb{Q}(X)^n$ *be defined as in Theorem 2.12. Then, there exist an effectively computable constant* c_1 *and a constant* c_2 *both depending only on* $\boldsymbol{\varrho}, E$ *such that as* $N \to \infty$*, for all but* $c_1 N(\log N)^{-2}$ *primes* $p \leq N$ *and for all but at most* c_2 *elements* $\alpha \in \overline{\mathbb{F}}_p$*, at least* $n - 1$ *points of* $(\varrho_1(\alpha), \cdot), \ldots, (\varrho_n(\alpha), \cdot)$ *are of order at least* $(N/\log N)^{1/(2n+4)}$*.*

Similarly to Theorem 2.15, we have:

Theorem 2.17. *Let* $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_m)$ *and* $\boldsymbol{\varrho} = (\varrho_1, \ldots, \varrho_n)$ *be defined as in Corollary 2.13. Then, there exist an effectively computable constant* c_1 *and a constant* c_2 *both depending only on* $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ *such that for arbitrary integers* $K, L \geq 1$*, there is a positive integer* T *with*

$$\log T \leq c_1 K^{m+2} L^{n+2}$$

such that for any prime p *for which the reduction* E_p *of* E *is also an elliptic curve and for the set* (2.5) *we have*

$$\#\mathcal{E}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) \leq v_p(T) + c_2.$$

Using Theorem 2.17, we obtain the following corollary.

Corollary 2.18. *Let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ be defined as in Corollary 2.13. Then, there exist an effectively computable constant c_1 and a constant c_2 both depending only on $\boldsymbol{\varphi}, \boldsymbol{\varrho}, E$ such that as $N \to \infty$, for all but $c_1 N(\log N)^{-2}$ primes $p \le N$ and for all but at most c_2 elements $\alpha \in \overline{\mathbb{F}}_p$, at least one of the two finitely generated groups*

$$\langle (\varphi_1(\alpha), \cdot), \dots, (\varphi_m(\alpha), \cdot) \rangle \qquad \text{and} \qquad \langle (\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot) \rangle$$

is of order at least $N^{mn/(2mn+2m+2n)}(\log N)^{-1/2}$.

3. Preliminaries

Throughout the paper, we use the Landau symbol O and the Vinogradov symbol $\ll$. Recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \le cV$ with some absolute constant $c > 0$. To emphasise the dependence of the implied constant c on some parameter (or a list of parameters) β, we write $U = O_\beta(V)$ or $U \ll_\beta V$.

3.1. **Heights of polynomials and rational functions.** For any non-zero polynomial $f \in \mathbb{C}[X]$, we define the height of f, denoted by $H(f)$, to be the maximum of the absolute values of its coefficients, and we also define

$$\mathrm{h}(f) = \max\{0, \log H(f)\}.$$

If $f(X) = a_d \prod_{i=1}^{d}(X - \alpha_i)$ with $a_d \neq 0$, then the Mahler measure of f is defined to be

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{|\alpha_i|, 1\}.$$

It is well-known that (see, for instance, [45, Equation (3.12)])

$$2^{-d} H(f) \le M(f) \le \sqrt{d+1}\, H(f). \tag{3.1}$$

The following bound on the height of a product of several polynomials is well-known and holds in much broader generality; see, for example, [26, Lemma 1.2 (1.b)].

Lemma 3.1. *Let $f_1, \dots, f_n \in \mathbb{C}[X]$ be non-zero polynomials. Then*

$$\mathrm{h}\left(\prod_{i=1}^{n} f_i\right) \le \sum_{i=1}^{n} \left(\mathrm{h}(f_i) + \deg f_i\right).$$

Clearly, the notion of height naturally extends to multivariate polynomials, namely for non-zero polynomial $f \in \mathbb{C}[X_1, \dots, X_n]$ we let $H(f)$ be the maximum of the absolute values of its coefficients and $\mathrm{h}(f) = \max\{0, \log H(f)\}$.

Moreover, for a rational function $R = f/g$, where $f, g \in \mathbb{Z}[X_1, \dots, X_n]$ are coprime, we define $\deg R = \max\{\deg f, \deg g\}$,

$$H(R) = \max\{H(f), H(g)\} \qquad \text{and} \qquad \mathrm{h}(R) = \max\{\mathrm{h}(f), \mathrm{h}(g)\}.$$

We need the following estimate on the height of composition of rational functions, which is a special case of [15, Lemma 3.3].

Lemma 3.2. *Let $R \in \mathbb{Q}[X_1, \dots, X_n]$ and $f_1, \dots, f_n \in \mathbb{Q}(X)$. Set $d = \max_{i=1,\dots,n} \deg f_i$ and $h = \max_{i=1,\dots,n} \mathrm{h}(f_i)$. Then*

$$\deg R(f_1, \dots, f_n) \le dn \deg R,$$
$$\mathrm{h}(R(f_1, \dots, f_n)) \le \mathrm{h}(R) + h \deg R + (3dn+1)\log(n+1)\deg R.$$

3.2. **The size and divisibility of resultants.** We start with the following simple estimate on the absolute value of the resultant of two polynomials; see [19, Theorem 6.23]. Its proof relies on applying Hadamard's inequality to the Sylvester matrix of f and g.

Lemma 3.3. *Let $f, g \in \mathbb{C}[X]$ be non-zero polynomials. Then, their resultant $\mathrm{Res}(f,g)$ satisfies*

$$|\mathrm{Res}(f,g)| \le \left(\sqrt{\deg f + 1}\, H(f)\right)^{\deg g} \left(\sqrt{\deg g + 1}\, H(g)\right)^{\deg f}.$$

Now, given two non-zero polynomials $f, g \in \mathbb{Z}[X]$, it is well-known that if their reductions modulo a prime p have a common factor, then their resultant $\mathrm{Res}(f,g)$ is divisible by p. The following result of Gómez-Pérez, Gutiérrez, Ibeas and Sevilla [21] refines this property for polynomials with several common roots modulo p.

Lemma 3.4. *Let $f, g \in \mathbb{Z}[X]$ be two non-zero polynomials whose reductions modulo p do not vanish identically and have m common roots in $\overline{\mathbb{F}}_p$, counted with multiplicities. Then,*

$$m \le v_p\left(\mathrm{Res}(f,g)\right).$$

3.3. **Division polynomials and their heights.** Let E be an elliptic curve defined as in (1.2). For any integer $n \ge 1$, let ψ_n be the n-th division polynomial of E; see [40, Exercise 3.7] or [46, Section 3.2] for their definition and properties. That is,

$$\psi_0 = 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2Y,$$
$$\psi_3 = 3X^4 + 6aX^2 + 12bX - a^2,$$
$$\psi_4 = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \ge 2,$$
$$\psi_{2m} = (2Y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \ge 3.$$

We remark, that the polynomials ψ_n are reduced by the curve equation (1.2), in particular $\psi_n \in \mathbb{Z}[X]$ if n is odd, $\psi_n \in Y\mathbb{Z}[X]$ if n is even, and $\psi_n^2 \in \mathbb{Z}[X]$ for any $n \ge 0$. Moreover (see, for instance, [46, Lemma 3.3] and the proof of [46, Lemma 3.5]), we have

$$\begin{aligned} &\psi_n = nX^{(n^2-1)/2} + (\text{lower degree terms}) \in \mathbb{Z}[X] \quad \text{for odd } n, \\ &\psi_n/Y = nX^{(n^2-4)/2} + (\text{lower degree terms}) \in \mathbb{Z}[X] \quad \text{for even } n. \end{aligned} \tag{3.2}$$

For any integer $n \ge 1$, let $\Psi_n \in \mathbb{Z}[X]$ be defined by

$$\Psi_n = \begin{cases} \psi_n & \text{if } n \text{ is odd,} \\ \psi_n/Y & \text{if } n \text{ is even.} \end{cases} \tag{3.3}$$

By convention, put $\Psi_0 = 0$.

We also define

$$\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1} \qquad n \geq 1,$$

where as before, ϕ_n is reduced by the curve equation (1.2), in particular, $\phi_n \in \mathbb{Z}[X]$. By convention, put $\phi_0 = 0$.

We note that an affine point $P = (x, y)$ on E is n-torsion if $\Psi_n(x) = 0$ for $n \geq 3$ and 2-torsion if $y = 0$. On the other hand, if $P = (x, y)$ is not an n-torsion point, then by [46, Theorem 3.6], the first coordinate of the point nP is

$$\frac{\phi_n(x)}{\psi_n^2(x)}. \tag{3.4}$$

The following lemma follows directly from [30, Corollary 1] (note that the polynomials Ψ_n here are exactly the division polynomials f_n defined in [30]).

Lemma 3.5. *There exists an effectively computable constant c depending only on E such that for any integer $n \geq 1$ we have*

$$\mathrm{h}(\Psi_n) \leq cn^2.$$

We conclude this section by giving a bound on the height of the polynomials ϕ_n.

Lemma 3.6. *There exists an effectively computable constant c depending only on E such that for any integer $n \geq 1$ we have*

$$\mathrm{h}(\phi_n) \leq cn^2.$$

Proof. If n is odd, then we have

$$\phi_n = X\Psi_n^2 - (X^3 + aX + b)\Psi_{n+1}\Psi_{n-1},$$

and so, using Lemma 3.1 and noticing $H(\Psi_n) \geq n$ by (3.2) we obtain

$$\begin{aligned}\mathrm{h}(\phi_n) &\leq \mathrm{h}(\Psi_n^2) + \mathrm{h}((X^3 + aX + b)\Psi_{n+1}\Psi_{n-1}) \\ &\leq 2(\mathrm{h}(\Psi_n) + \deg \Psi_n) + \mathrm{h}(\Psi_{n+1}) + \mathrm{h}(\Psi_{n-1}) \\ &\quad + \mathrm{h}(X^3 + aX + b) + \deg \Psi_{n+1} + \deg \Psi_{n-1} + 3.\end{aligned}$$

In addition, if n is even, then since

$$\phi_n = X(X^3 + aX + b)\Psi_n^2 - \Psi_{n+1}\Psi_{n-1},$$

as the above we obtain

$$\begin{aligned}\mathrm{h}(\phi_n) &\leq \mathrm{h}((X^3 + aX + b)\Psi_n^2) + \mathrm{h}(\Psi_{n+1}\Psi_{n-1}) \\ &\leq 2(\mathrm{h}(\Psi_n) + \deg \Psi_n) + \mathrm{h}(X^3 + aX + b) + 3 \\ &\quad + \mathrm{h}(\Psi_{n+1}) + \mathrm{h}(\Psi_{n-1}) + \deg \Psi_{n+1} + \deg \Psi_{n-1}.\end{aligned}$$

Now, the desired result follows from (3.2) and Lemma 3.5. □

3.4. **Summation polynomials.** In this section we recall *summation polynomials* of elliptic curves introduced by Semaev [38], and bound the height of such polynomials.

Lemma 3.7. *Let E be an elliptic curve of the form (1.2) defined over a field $\mathbb{K}$ of characteristic different from 2 and 3. For any integer $n \geq 2$, there exists a polynomial $\sigma_n \in \mathbb{Z}[X_1, \ldots, X_n, a, b]$ (called the n-th summation polynomial) with the following property: for any $x_1, \ldots, x_n \in \overline{\mathbb{K}}$, we have $\sigma_n(x_1, \ldots, x_n) = 0$ if and only if there are $y_1, \ldots, y_n \in \overline{\mathbb{K}}$ such that $(x_i, y_i) \in E, 1 \leq i \leq n$, and $(x_1, y_1) + \cdots + (x_n, y_n) = O$ on the curve. Moreover, the polynomials σ_n can be defined by*

$$\begin{aligned} \sigma_2(X_1, X_2) &= X_1 - X_2, \\ \sigma_3(X_1, X_2, X_3) &= (X_1 - X_2)^2 X_3^2 - 2\left((X_1 + X_2)(X_1X_2 + a) + 2b\right) X_3 \\ &\quad + (X_1X_2 - a)^2 - 4b(X_1 + X_2), \\ \sigma_n(X_1, \ldots, X_n) &= \mathrm{Res}_X\left(\sigma_{n-k}(X_1, \ldots, X_{n-k-1}, X), \sigma_{k+2}(X_{n-k}, \ldots, X_n, X)\right) \end{aligned} \tag{3.5}$$

for any $n \geq 4$ and $1 \leq k \leq n-3$, where Res_X denotes the resultant with respect to the variable X.

For any $n \geq 3$, σ_n is an irreducible symmetric polynomial which has degree 2^{n-2} in each variable.

We now bound the height of summation polynomials.

Lemma 3.8. *Let E and $\sigma_n \in \mathbb{Z}[X_1, \ldots, X_n, a, b]$, $n \geq 2$, be defined as in Lemma 3.7, $\mathbb{K} = \mathbb{C}$ and σ_n of the form (3.5). Then*

$$\mathrm{h}(\sigma_n) = \exp\big(O(n)\big),$$

where the implied constant is effectively computable depending only on the curve E.

Proof. We proceed by induction. Assume that $n \geq 4$ and

$$\mathrm{h}(\sigma_j) \leq \exp(cj), \quad 2 \leq j < n, \tag{3.6}$$

for some constant c. Write σ_n in the form (3.5) with $k = \lfloor (n-1)/2 \rfloor$.

Put

$$\begin{aligned} d &= \deg_X \sigma_{n-k}(X_1, \ldots, X_{n-k-1}, X), \\ m &= \deg_X \sigma_{k+2}(X_{n-k}, \ldots, X_n, X). \end{aligned}$$

By definition, σ_n is the determinant of the Sylvester matrix of the polynomials $\sigma_{n-k}(X_1, \ldots, X_{n-k-1}, X)$ and $\sigma_{k+2}(X_{n-k}, \ldots, X_n, X)$ with respect to X. By expanding this determinant, we know that σ_n is the sum of at most (because by Lemma 3.7, $d = 2^{n-k-2}$ and $m = 2^k$)

$$(d+1)^m (m+1)^d = \exp(\exp(O(n))) \tag{3.7}$$

summands of the form

$$f_1 \ldots f_m g_1 \ldots g_d, \tag{3.8}$$

where $f_i \in \mathbb{Z}[X_1, ..., X_{n-k-1}]$ and $g_j \in \mathbb{Z}[X_{n-k}, ..., X_n]$ are coefficients of σ_{n-k} and σ_{k+2} respectively considered as polynomials with respect to the variable X. Clearly, for each i and each j,

$$\mathrm{h}(f_i) \le \mathrm{h}(\sigma_{n-k}) \qquad \text{and} \qquad \mathrm{h}(g_j) \le \mathrm{h}(\sigma_{k+2}). \tag{3.9}$$

In addition, by Lemma 3.7 the degree of f_i and g_j in each variable is at most 2^{n-k-2} and 2^k, respectively, thus f_i and g_j have at most $(2^{n-k-2}+1)^{n-k-1}$ and $(2^k+1)^{k+1}$ nonzero terms. Then, expanding all the products in (3.8), the maximal number of common monomials is at most

$$(2^{n-k-2}+1)^{m(n-k-1)} \cdot (2^k+1)^{d(k+1)} = \exp(\exp(O(n))). \tag{3.10}$$

Hence, it follows from (3.6), (3.7), (3.8), (3.9) and (3.10) that

$$\begin{aligned} \mathrm{h}(\sigma_n) &\le \exp(O(n)) + \exp(O(n)) + m \cdot \mathrm{h}(\sigma_{n-k}) + d \cdot \mathrm{h}(\sigma_{k+2}) \\ &\le \exp(O(n)) + 2^{(n-1)/2} \exp(c(n-k)) + 2^{(n-1)/2} \exp(c(k+2)) \\ &\le \exp(O(n)) + 2^{(n+1)/2} \exp(c(n/2+3/2)), \end{aligned}$$

and the desired result follows by choosing the constant c large enough. Moreover, since the implied constants in both (3.7) and (3.10) are effectively computable, the constant c is also effectively computable. □

3.5. **Unlikely Intersections results.** In this section, we list a series of results about multiplicative dependence of rational functions in $\overline{\mathbb{Q}}(X)$ and linear dependence on elliptic curves for points defined over $\overline{\mathbb{Q}}$. Namely, in order to prove Theorems 2.1, 2.8 and 2.12, one needs first to consider the analogous problems in $\overline{\mathbb{Q}}$ (rather than $\overline{\mathbb{F}}_p$), and to show finiteness results. These problems fit in the more general framework of problems of unlikely intersections, which have been deeply studied in the last decades (see, for instance, [47]).

More specifically, the following lemma is an effective version of a result of Maurin [27, Théorème 1.2] concerning multiplicative dependence of values of rational functions in $\mathbb{Q}(X)$, which in fact was initially proved by Bombieri, Masser and Zannier [9] under a more restrictive condition of multiplicative independence of the involved functions modulo constants.

Lemma 3.9. *Let $\mathbb{K}$ be a number field and let $f_1, \dots, f_m \in \mathbb{K}(X)$ be non-zero multiplicatively independent rational functions defined over $\mathbb{K}$. Then, the cardinality of the set of $\alpha \in \overline{\mathbb{Q}}$ for which there exist linearly independent vectors $(k_1, \dots, k_m)$ and $(\ell_1, \dots, \ell_m) \in \mathbb{Z}^m$ such that*

$$f_1(\alpha)^{k_1} \cdots f_m(\alpha)^{k_m} = f_1(\alpha)^{\ell_1} \cdots f_m(\alpha)^{\ell_m} = 1$$

is bounded by an effectively computable constant C depending only on $\mathbb{K}$ and $f_1, \dots, f_m$.

Proof. The ineffective version of this result is proved by Maurin in [27, Théorème 1.2]. In [8], Bombieri, Habegger, Masser and Zannier give a different argument to prove [27, Théorème 1.2], showing that effectivity would follow from an effective version of Habegger's theorem [22]. This has finally been proved by Habegger himself in [23]. □

The following lemma is a special case of [18, Théorème H]. The latter was a conditional result due to Viada [42] and made unconditional by Galateau [18].

Lemma 3.10. *Let E be an elliptic curve defined over a number field $\mathbb{K}$ by a Weierstrass equation, and let $n \geq 1$ be an integer. Let $\mathcal{C}$ be an irreducible curve in E^n, also defined over $\mathbb{K}$, with coordinates $(X_1, Y_1, \dots, X_n, Y_n)$ such that the points (X_j, Y_j) are linearly independent over $\mathrm{End}(E)$. Then, there are at most finitely many points $c \in \mathcal{C}(\mathbb{C})$ such that $(X_j(c), Y_j(c))$, $j = 1, \dots, n$, satisfy two independent linear relations over $\mathrm{End}(E)$.*

The following result is a special case of Corollary 4.5 in Section 4. It will be used in the proof of Theorem 2.8.

Lemma 3.11. *Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation, and let $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_m)$ and $\boldsymbol{\varrho} = (\varrho_1, \dots, \varrho_n)$ be vectors of non-zero rational functions in $\mathbb{Q}(X)$ such that $\varphi_1, \dots, \varphi_m$ are multiplicatively independent and the points $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ in $E(\overline{\mathbb{Q}(X)})$ are linearly independent over $\mathbb{Z}$. Suppose moreover that at least one of the following conditions holds:*

(1) *$\varphi_1, \dots, \varphi_m$ are multiplicatively independent modulo constants;*
(2) *the points $(\varrho_1(X), \cdot), \dots, (\varrho_n(X), \cdot)$ are linearly independent over $\mathrm{End}(E)$ modulo points in $E(\overline{\mathbb{Q}})$.*

Then, there are at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ are multiplicatively dependent and the points $(\varrho_1(\alpha), \cdot), \dots, (\varrho_n(\alpha), \cdot)$ in $E(\overline{\mathbb{Q}})$ are linearly dependent over $\mathbb{Z}$.

In full generality, the proof of this result is in principle not effective, and this makes the constant c_2 in the statement of Theorem 2.8 ineffective. If $n = 1$, the condition of linear dependence of the point $(\varrho_1(\alpha), \cdot)$ means that it is a torsion point, and in this case, it is possible to give an effective version of Lemma 3.11, which is the content of the following lemma.

Lemma 3.12. *In Lemma 3.11 when $n = 1$, the order of the torsion point $(\varrho_1(\alpha), \cdot)$ can be effectively upper bounded uniformly, and in particular, the cardinality of the set of $\alpha \in \overline{\mathbb{Q}}$ such that $\varphi_1(\alpha), \dots, \varphi_m(\alpha)$ are multiplicatively dependent and $(\varrho_1(\alpha), \cdot)$ has finite order can be effectively bounded.*

Proof. By [6, Theorem 1.4], there exists an effectively computable bound B for the order of $(\varrho_1(\alpha), \cdot)$ depending on $E, \boldsymbol{\varphi}, \rho_1$ and a lower bound ϵ for the height of elements of $\mathbb{Q}(E_{\mathrm{tor}})^* \setminus \mu_\infty$. Such an effective lower bound is provided by Frey [17, Theorem 1.2] and, in case E has complex multiplication, by Amoroso and Zannier [1]. □

4. Unlikely intersections in $\mathbb{G}_{\mathrm{m}}^m \times E^n$

To prove Theorem 2.8, we will need a finiteness result for multiplicative relations for rational functions in $\overline{\mathbb{Q}}(X)$ and linear dependence on elliptic curves. This will follow from a general statement about the intersection of an irreducible curve in the split semiabelian variety $\mathbb{G}_{\mathrm{m}}^m \times E^n$ with the algebraic subgroups of codimension at least 2, which we prove in this section. This result fits in the more general framework of unlikely intersections, and it is a particular case of the well known Zilber-Pink conjecture (for an account on these problems, see [47]).

Theorem 4.1. *Let E be an elliptic curve defined over a number field $\mathbb{K}$ by a Weierstrass equation, and let $m, n \geq 1$ be integers. Let $\mathcal{C}$ be an irreducible curve in $\mathbb{G}_{\mathrm{m}}^m \times E^n$, also defined over $\mathbb{K}$, with coordinates $(Z_1, \dots, Z_m, X_1, Y_1, \dots, X_n, Y_n)$ such that $Z_1, \dots, Z_m$ are multiplicatively independent and the points (X_i, Y_i) are linearly independent over* $\mathrm{End}(E)$. *Suppose moreover that at least one of the following conditions holds:*

(1) *$Z_1, \dots, Z_m$ are multiplicatively independent modulo constants;*
(2) *the points (X_i, Y_i) are linearly independent over* $\mathrm{End}(E)$ *modulo points in $E(\overline{\mathbb{Q}})$.*

Then, there are at most finitely many points $c \in \mathcal{C}(\mathbb{C})$ such that $Z_i(c)$, $i = 1, \dots, m$, are multiplicatively dependent and $(X_j(c), Y_j(c))$, $j = 1, \dots, n$, are linearly dependent over $\mathrm{End}(E)$.

The proof of Theorem 4.1 can be obtained by adapting the proof of [5, Theorem 1.2] to this setting. In particular, one follows the general strategy introduced by Pila and Zannier in [35] using the theory of o-minimal structures to give an alternative proof of the Manin-Mumford conjecture for abelian varieties. The strategy is based on the combination of various results coming from o-minimality, Diophantine geometry and transcendence results.

An important ingredient of the proof is the well-known Pila-Wilkie Theorem [34] which provides an estimate for the number of rational points on a "sufficiently transcendental" real subanalytic variety. Using abelian logarithms, these rational points correspond to torsion points. For more details about the general strategy and how it has been applied to other problems we refer to [47].

On the other hand, if one wants to deal with points lying in proper algebraic subgroups like in Theorem 4.1, a more refined result is needed. For instance, first in [4] and then in [5], the authors adapted ideas introduced in [12] to deal with linear relations rather than just with torsion points.

Let $\mathfrak{h}$ denote the absolute logarithmic Weil heights on $\mathbb{G}_{\mathrm{m}}(\overline{\mathbb{Q}})$ and on $E(\overline{\mathbb{Q}})$, and let us define a height $\tilde{\mathfrak{h}}$ on $\mathcal{C}(\overline{\mathbb{Q}})$ by

$$\tilde{\mathfrak{h}}(c) := \mathfrak{h}(Z_1(c)) + \cdots + \mathfrak{h}(Z_m(c)) + \mathfrak{h}(X_1(c), Y_1(c)) + \cdots + \mathfrak{h}(X_n(c), Y_n(c)).$$

We call $\mathcal{C}_0$ the set of such points of $\mathcal{C}(\mathbb{C})$ that we want to prove to be finite in Theorem 4.1. First, we note that the points in $\mathcal{C}_0$ must be algebraic. Moreover, as at least one of the conditions (1) and (2) in Theorem 4.1 holds, $\mathcal{C}_0$ is a set of bounded height respectively by

(1) [9, Theorem 1];
(2) [41, Theorem 1].

We then just have to exhibit a bound on their degree over the number field $\mathbb{K}$.

Lemma 4.2. *There exists a compact (in the complex topology) subset $\mathcal{C}^*$ of $\mathcal{C}$, such that for all $c \in \mathcal{C}_0$ of degree large enough, at least half of the Galois conjugates of c over $\mathbb{K}$ lie in $\mathcal{C}^*$*

Proof. See [29, Lemma 8.2]. □

Note that, if $c \in \mathcal{C}_0$, then all its Galois conjugates over $\mathbb{K}$ satisfy again some dependence relations, hence they must also lie in $\mathcal{C}_0$.

We now cover the set $\mathcal{C}^*$ appearing in Lemma 4.2 with finitely many discs $D_1, \dots, D_{\gamma_1}$. Let D be one of these discs. We set $R = \mathrm{End}(E)$ and $P_j = (X_j, Y_j)$. For $\mathbf{a} = (a_1, \dots, a_m) \in \mathbb{Z}^m \setminus \{0\}$ and $\mathbf{b} = (b_1, \dots, b_n) \in R^n \setminus \{0\}$ we set

$$D(\mathbf{a}, \mathbf{b}) := \left\{ c \in D : \prod_{i=1}^{m} Z_i(c)^{a_i} = 1 \text{ and } \sum_{j=1}^{n} b_j P_j(c) = O \right\}.$$

For the rest of the section the implied constants will depend on $\mathcal{C}$ and D. Any further dependence will be expressed by an index.

Lemma 4.3. *If $c \in D \cap \mathcal{C}_0$, there are $\mathbf{a} \in \mathbb{Z}^m \setminus \{0\}$ and $\mathbf{b} \in R^n \setminus \{0\}$ such that $c \in D(\mathbf{a}, \mathbf{b})$ and*

$$\max\{|\mathbf{a}|, |\mathbf{b}|\} \ll [\mathbb{K}(c) : \mathbb{K}]^{\gamma_2}, \tag{4.1}$$

for some constant $\gamma_2 > 0$ depending on the curve $\mathcal{C}$ and the disc D, where $|\mathbf{a}| = \max\{|a_1|, \dots, |a_m|\}$ and $|\mathbf{b}| = \max\{|b_1|, \dots, |b_n|\}$.

Proof. See [5, Lemmas 5.1 and 5.2] and (if E has CM) [3, Lemma 6.1]. □

We denote by $u_1, \dots, u_m$ the principal determinations of the standard logarithms of $Z_1, \dots, Z_m$ and by $w_1, \dots, w_n$ the elliptic logarithms of $P_1, \dots, P_n$ seen as analytic functions on (an open neighbourhood of) D. These functions satisfy the equations

$$u_i = p_i + 2\pi\sqrt{-1}q_i, \quad w_j = r_j + s_j\tau, \quad \text{for } i = 1, \dots, m \text{ and } j = 1, \dots, n,$$

where $(1, \tau)$ is a basis of the period lattice of E and p_i, q_i, r_j, s_j are real-valued functions defined on D. If we view the compact disc D as subset of $\mathbb{R}^2$, we can define

$$\begin{aligned} \theta : \ D \subset \mathbb{R}^2 &\to \mathbb{R}^{2m+2n} \\ c &\mapsto (p_1(c), q_1(c), \dots, p_m(c), q_m(c), r_1(c), s_1(c), \dots, r_n(c), s_n(c)). \end{aligned}$$

The image $\theta(D)$ is a subanalytic surface of $\mathbb{R}^{2m+2n}$ which we denote by S. Note that θ is injective. Moreover, as D is compact, we have that the functions q_i, r_j and s_j take bounded values. The $p_1, q_1, \dots, p_m, q_m, r_1, s_1, \dots, r_n, s_n$ are sometimes called Betti-coordinates and θ the Betti-map.

For any $b \in R$ and any point $P \in E(\overline{\mathbb{Q}})$, given $\rho + \sigma\tau$ an elliptic logarithm of P, a logarithm of bP is given by $\rho' + \sigma'\tau$, where

$$\begin{pmatrix} \rho' \\ \sigma' \end{pmatrix} = A(b) \begin{pmatrix} \rho \\ \sigma \end{pmatrix},$$

for some $A(b) \in M_2(\mathbb{Z})$, where $M_2(\mathbb{Z})$ is the ring of 2×2 matrices over $\mathbb{Z}$.

For $l \in \mathbb{Z}$, clearly

$$A(l) = \begin{pmatrix} l & 0 \\ 0 & l \end{pmatrix}.$$

If $R = \mathbb{Z}[\alpha]$ for some imaginary quadratic α, we have that

$$A(l_1 + \alpha l_2) = \begin{pmatrix} l_1 & 0 \\ 0 & l_1 \end{pmatrix} + A(\alpha) \begin{pmatrix} l_2 & 0 \\ 0 & l_2 \end{pmatrix}.$$

Note that, as the entries of $A(\alpha)$ are fixed and depend only on E, if $|A|$ is the maximum of the absolute values of the entries of a matrix $A \in M_2(\mathbb{Z})$, then we have $|A(b)| \ll |b|$ for all $b \in R$.

Using the function θ defined before, the points of $\mathcal{C}_0$ that satisfy two relations will correspond to points of S lying on linear varieties defined by equations of some special form with integer coefficients. In particular, if $c \in D(\mathbf{a}, \mathbf{b})$, there are integers e, f, g such that

$$\begin{cases} \sum_{i=1}^m a_i u_i = 2\pi\sqrt{-1}e, \\ \sum_{j=1}^n b_j w_j = f + g\tau, \end{cases}$$

which translates to

$$\begin{cases} \sum_{i=1}^m a_i p_i = 0, \\ \sum_{i=1}^m a_i q_i = e, \\ \sum_{j=1}^n A(b_j)(r_j, s_j)^{\mathrm{t}} = (f, g)^{\mathrm{t}}, \end{cases}$$

holding for $\theta(c)$ (here $\cdot^{\mathrm{t}}$ denotes the transposition).

We define

$$W = \Bigg\{ (\alpha_1, \dots, \alpha_m, B_1, \dots, B_n, \sigma_1, \sigma_2, \sigma_3, p_1, q_1, \dots, p_m, q_m, r_1, s_1, \dots, r_n, s_n) \in$$
$$\mathbb{R}^m \times M_2(\mathbb{R})^n \times \mathbb{R}^3 \times S : \sum_{i=1}^m \alpha_i p_i = 0, \sum_{i=1}^m \alpha_i q_i = \sigma_1, \sum_{j=1}^n B_j (r_j, s_j)^{\mathrm{t}} = (\sigma_2, \sigma_3)^{\mathrm{t}} \Bigg\},$$

and, for $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_m) \in \mathbb{R}^m$ and $\mathbf{B} = (B_1, \dots, B_n) \in M_2(\mathbb{R})^n$, the fiber

$$W_{\boldsymbol{\alpha}, \mathbf{B}} = \{ (\sigma_1, \sigma_2, \sigma_3, p_1, q_1, \dots, p_m, q_m, r_1, s_1, \dots, r_n, s_n) \in \mathbb{R}^3 \times S : (\alpha_1, \dots, \alpha_m, B_1, \dots, B_n, \sigma_1, \sigma_2, \sigma_3, p_1, \dots, s_n) \in W \}.$$

We let π_1 be the projection from $\mathbb{R}^3 \times S \subseteq \mathbb{R}^3 \times \mathbb{R}^{2m+2n}$ to $\mathbb{R}^3$, while π_2 indicates the projection to S. We also define, for $T \geq 0$,

$$W^{\sim}_{\boldsymbol{\alpha}, \mathbf{B}}(\mathbb{Q}, T) = \{ (\sigma_1, \sigma_2, \sigma_3, p_1, q_1, \dots, p_m, q_m, r_1, s_1, \dots, r_n, s_n) \in W_{\boldsymbol{\alpha}, \mathbf{B}} : (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{Q}^3 \text{ and } H(\sigma_1, \sigma_2, \sigma_3) \leq T \},$$

where $H(\sigma_1, \sigma_2, \sigma_3)$ is the maximum of the absolute values of the numerators and denominators of the σ_j when they are written in lowest terms.

Fix now $\mathbf{a} \in \mathbb{Z}^m$ and $\mathbf{b} \in R^n$. Note that, if $c \in D(\mathbf{a}, \mathbf{b})$, then by the above discussion there are integers e, f, g such that $(e, f, g, \theta(c)) \in W_{\mathbf{a}, A(\mathbf{b})}$, where $A(\mathbf{b}) = (A(b_1), \dots, A(b_n))$. Since $q_1, \dots, q_m, r_1, s_1, \dots, r_n, s_n$ take bounded values as D is a compact disc, we can suppose that

$$\max\{|e|, |f|, |g|, |\mathbf{a}|, |A(\mathbf{b})|\} \leq T_0,$$

for some T_0 with $T_0 \ll \max\{|\mathbf{a}|, |A(\mathbf{b})|\} \ll \max\{|\mathbf{a}|, |\mathbf{b}|\}$. Therefore, if we let

$$\Sigma_{\mathbf{a}, \mathbf{b}} := \pi_2^{-1}(\theta(D(\mathbf{a}, \mathbf{b}))) \cap W_{\mathbf{a}, A(\mathbf{b})},$$

then we have $\Sigma_{\mathbf{a}, \mathbf{b}} \subseteq W^{\sim}_{\mathbf{a}, A(\mathbf{b})}(\mathbb{Q}, T_0)$. Note that $\theta(D(\mathbf{a}, \mathbf{b})) \subseteq \pi_2(W_{\mathbf{a}, A(\mathbf{b})})$.

We claim that, for every $\epsilon > 0$, we have an upper bound for the cardinality of $D(\mathbf{a}, \mathbf{b})$ of the form

$$|D(\mathbf{a}, \mathbf{b})| \ll_\epsilon (\max\{|\mathbf{a}|, |A(\mathbf{b})|\})^\epsilon. \tag{4.2}$$

If not, by the previous considerations the following lemma would be contradicted.

Lemma 4.4. *For every $\epsilon > 0$ we have $|\pi_2(\Sigma_{\mathbf{a},\mathbf{b}})| \ll_\epsilon T_0^\epsilon$.*

Proof. Suppose there is a positive constant $\gamma_3 = \gamma_3(W, \epsilon)$ such that $|\pi_2(\Sigma_{\mathbf{a},\mathbf{b}})| \geq \gamma_3 T_0^\epsilon$. Then, by [24, Corollary 7.2], there exists a definable function $\delta : [0,1] \to W_{\mathbf{a},A(\mathbf{b})}$ such that

(1) the map $\delta_1 := \pi_1 \circ \delta : [0,1] \to \mathbb{R}^3$ is semi-algebraic and its restriction to $(0,1)$ is real analytic;
(2) the composition $\delta_2 := \pi_2 \circ \delta : [0,1] \to S$ is non-constant;
(3) we have $\pi_2(\delta(0)) \in \pi_2(\Sigma_{\mathbf{a},\mathbf{b}})$.

By rescaling and restricting the domain we can suppose that the path δ_1 is contained in a real algebraic curve. Moreover, by (3) above, there exists $c_0 \in D(\mathbf{a}, \mathbf{b})$ with $\theta(c_0) = \delta_2(0)$.

We now consider the map

$$\begin{array}{rccc} \phi: & \mathbb{G}_{\mathrm{m}}^m \times E^n & \to & \mathbb{G}_{\mathrm{m}} \times E \\ & (Z_1, \dots, Z_m, P_1, \dots, P_n) & \mapsto & (\prod_{i=1}^m Z_i^{a_i}, \prod_{j=1}^n b_j P_j) \end{array}$$

and its differential

$$\begin{array}{rccc} d\phi: & \mathbb{C}^m \times \mathbb{C}^n & \to & \mathbb{C} \times \mathbb{C} \\ & (u_1, \dots, u_m, w_1, \dots, w_n) & \mapsto & (\sum_{i=1}^m a_i u_i, \sum_{j=1}^n b_j w_j) =: (u', w'). \end{array}$$

Note that $\phi(\mathcal{C})$ cannot be constant, otherwise both conditions (1) and (2) in the hypotheses of Theorem 4.1 would be false. Therefore $\phi(\mathcal{C})$ is a curve.

We can see $\sigma_1, \sigma_2, \sigma_3, p_1, q_1, \dots, p_m, q_m, r_1, s_1, \dots, r_n, s_n$, and consequently $u_1, \dots, u_m$, $w_1, \dots, w_n, u', w'$, as coordinate functions on $[0,1]$. We have that the transcendence degree $\operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(\sigma_1, \sigma_2, \sigma_3) \leq 1$ and recall that, by the definition of W, the two relations $u' = 2\pi\sqrt{-1}\sigma_1$ and $w' = \sigma_2 + \sigma_3\tau$ must hold. We deduce that

$$\operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(\sigma_1, \sigma_2, \sigma_3, u', w') \leq 1.$$

This gives a map

$$\delta' := (u', w') : [0,1] \to \mathbb{C} \times \mathbb{C}$$

that is real semi-algebraic, continuous and with $\delta'|_{(0,1)}$ real analytic. By Ax's Theorem [2] (see [24, Theorem 5.4]), the Zariski closure in $\mathbb{G}_{\mathrm{m}} \times E$ of the image of $\exp \circ \delta'$, which is contained in $\phi(\mathcal{C})$, is a coset, that must actually be a torsion coset, because $\phi(c_0)$ is the neutral element of $\mathbb{G}_{\mathrm{m}} \times E$. If this torsion coset is a curve, then it coincides with $\phi(\mathcal{C})$ and this contradicts the hypotheses of Theorem 4.1. If the coset is a point, then $u' = \sum_{i=1}^m a_i u_i$ and $w' = \sum_{j=1}^n b_j w_j$ are both constant and equal to $d\phi(c_0)$ on $[0,1]$. This again contradicts the hypotheses of Theorem 4.1. □

Now we are ready to prove Theorem 4.1.

Proof of Theorem 4.1. Fix a $c_0 \in \mathcal{C}_0$ of large degree over $\mathbb{K}$. By Lemma 4.2 we have that one of the discs $D_1, \dots, D_{\gamma_1}$, say D_1, contains at least $[\mathbb{K}(c_0) : \mathbb{K}]/(2\gamma_1)$ conjugates of c_0. Moreover, if $c_0 \in D_1(\mathbf{a}, \mathbf{b})$ for some $\mathbf{a} \in \mathbb{Z}^m$ and $\mathbf{b} \in R^n$, all of these conjugates belong to $D_1(\mathbf{a}, \mathbf{b})$. Therefore, combining this with (4.1) and (4.2), we get

$$[\mathbb{K}(c_0) : \mathbb{K}] \ll |D_1(\mathbf{a}, \mathbf{b})| \ll_\epsilon (\max\{|\mathbf{a}|, |\mathbf{b}|\})^\epsilon \ll_\epsilon [\mathbb{K}(c_0) : \mathbb{K}]^{\gamma_2 \epsilon},$$

which, after choosing $\epsilon < 1/(2\gamma_2)$, leads to a contradiction if $[\mathbb{K}(c_0) : \mathbb{K}]$ is too large. This completes the proof of Theorem 4.1. □

We now formulate and prove a corollary of Theorem 4.1. Notice that Lemma 3.11 is a special case of it.

The point of the corollary is that, if one only needs to consider relations over $\mathbb{Z}$ among the $P_j(c)$, one can relax the hypotheses and assume that the P_j are linearly independent over $\mathbb{Z}$ and not over $\mathrm{End}(E)$. Note that the analogous fact does not hold in the setting of Lemma 3.10. Indeed, two points that are generically dependent over $\mathrm{End}(E)$ but not over $\mathbb{Z}$ can specialize infinitely many times to two torsion points.

Corollary 4.5. *Let E be an elliptic curve defined over a number field $\mathbb{K}$ by a Weierstrass equation, and let $m, n \geq 1$ be integers. Let $\mathcal{C}$ be an irreducible curve in $\mathbb{G}_{\mathrm{m}}^m \times E^n$, also defined over $\mathbb{K}$, with coordinates $(Z_1, \dots, Z_m, X_1, Y_1, \dots, X_n, Y_n)$ such that $Z_1, \dots, Z_m$ are multiplicatively independent and the points $P_j := (X_j, Y_j)$ are linearly independent over $\mathbb{Z}$. Suppose moreover that at least one of the following conditions holds:*

1. *$Z_1, \dots, Z_m$ are multiplicatively independent modulo constants;*
2. *the points P_j are linearly independent over $\mathrm{End}(E)$ modulo points in $E(\overline{\mathbb{Q}})$.*

Then, there are at most finitely many points $c \in \mathcal{C}(\mathbb{C})$ such that the $Z_i(c)$ are multiplicatively dependent and the $P_j(c)$ are linearly dependent over $\mathbb{Z}$.

Proof. It is clear that our claim follows directly from Theorem 4.1 in case the points $P_1, \dots, P_n$ are linearly independent over $\mathrm{End}(E)$. We only need to consider the case in which $R := \mathrm{End}(E) \neq \mathbb{Z}$ and the points $P_1, \dots, P_n$ satisfy a linear dependence relation over $\mathrm{End}(E)$, but none over $\mathbb{Z}$.

Set

$$\Lambda = \left\{ (\rho_1, \dots, \rho_n) \in R^n : \sum_{j=1}^n \rho_j P_j = O \right\}.$$

Our hypothesis on the P_j implies that $\Lambda \cap \mathbb{Z}^n = \{0\}$. This is a finitely generated R-submodule of R^n of some rank n', $1 \leq n' < n$. It is a well known fact (see, e.g., Lemma 2.3 of [5]) that the set

$$\mathcal{L}(\Lambda) = \left\{ (Q_1, \dots, Q_n) \in E^n : \sum_{j=1}^n \rho_j Q_j = O \text{ for all } (\rho_1, \dots, \rho_n) \in \Lambda \right\}$$

defines an algebraic subgroup of E^n of dimension $n - n'$. Moreover, there is a surjective and finite homomorphism of algebraic groups

$$\phi : \mathcal{L}(\Lambda) \to E^{n-n'}.$$

Then, our hypotheses imply that $\phi(P_1, \dots, P_n)$ gives an irreducible curve that does not lie in a proper algebraic subgroup of $E^{n-n'}$.

Suppose there are infinitely many points $c \in \mathcal{C}(\mathbb{C})$ such that $Z_1(c), \dots, Z_m(c)$ are multiplicatively dependent and $P_1(c), \dots, P_n(c)$ are linearly dependent over $\mathbb{Z}$. Then, every $(P_1(c), \dots, P_n(c))$ lies in a proper algebraic subgroup of $\mathcal{L}(\Lambda)$ and its image via ϕ in a proper algebraic subgroup of $E^{n-n'}$. A contradiction arises by applying Theorem 4.1 to the curve in $\mathbb{G}_{\mathrm{m}}^m \times E^{n-n'}$ given by $(Z_1, \dots, Z_m, \phi(P_1, \dots, P_n))$, concluding the proof. □

5. Proofs of main results

5.1. **Proof of Theorem 2.1.** For any non-zero integer vector $\boldsymbol{k} = (k_1, \dots, k_m) \in \mathbb{Z}^m$, we define the rational function

$$\Omega_{\boldsymbol{k}}(X) = \varphi_1(X)^{k_1} \cdots \varphi_m(X)^{k_m}.$$

We write $\varphi_i = f_i/g_i$ with relatively prime polynomials $f_i, g_i \in \mathbb{Z}[X]$, $i = 1, \dots, m$, and thus we have $\Omega_{\boldsymbol{k}}(X) = F_{\boldsymbol{k}}(X)/G_{\boldsymbol{k}}(X)$ with polynomials $F_{\boldsymbol{k}}(X), G_{\boldsymbol{k}}(X) \in \mathbb{Z}[X]$ that are defined by

$$\begin{aligned} F_{\boldsymbol{k}}(X) &= \prod_{\substack{1 \le i \le m \\ k_i > 0}} f_i(X)^{k_i} \prod_{\substack{1 \le i \le m \\ k_i < 0}} g_i(X)^{-k_i}, \\ G_{\boldsymbol{k}}(X) &= \prod_{\substack{1 \le i \le m \\ k_i < 0}} f_i(X)^{-k_i} \prod_{\substack{1 \le i \le m \\ k_i > 0}} g_i(X)^{k_i}. \end{aligned} \tag{5.1}$$

Recall that $\mathcal{S}_1 \subset \mathbb{C}$ is the set of all the elements $\alpha \in \mathbb{C}$ which are solutions to the system of equations

$$\Omega_{\boldsymbol{k}}(X) - 1 = \Omega_{\boldsymbol{\ell}}(X) - 1 = 0 \tag{5.2}$$

for some linearly independent vectors $\boldsymbol{k}, \boldsymbol{\ell} \in \mathbb{Z}^m$. Clearly, if $\alpha \in \mathcal{S}_1$, then every Galois conjugate of α over $\mathbb{Q}$ is also in $\mathcal{S}_1$.

By Lemma 3.9 the set $\mathcal{S}_1$ is finite and we have

$$\#\mathcal{S}_1 \ll_{\boldsymbol{\varphi}} 1, \tag{5.3}$$

where the implied constant is effectively computable.

Let $W_{\mathcal{S}_1} \in \mathbb{Z}[X]$ be the product of all the irreducible polynomials (without multiplicity) having some $\alpha \in \mathcal{S}_1$ as a root. Clearly, we have

$$\deg W_{\mathcal{S}_1} = \#\mathcal{S}_1.$$

Define

$$P_{\boldsymbol{\ell}} = \frac{F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}}}{\gcd(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}}, (F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}})')} \qquad \text{and} \qquad \tilde{P}_{\boldsymbol{\ell}} = \frac{P_{\boldsymbol{\ell}}}{\gcd(P_{\boldsymbol{\ell}}, W_{\mathcal{S}_1})} \in \mathbb{Z}[X].$$

Note that since the polynomial $P_{\boldsymbol{\ell}}$ has only simple roots, we have $\gcd(\tilde{P}_{\boldsymbol{\ell}}, W_{\mathcal{S}_1}) = 1$.

Then, the system of equations

$$F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X) = \tilde{P}_{\boldsymbol{\ell}}(X) = 0 \tag{5.4}$$

has no solution over $\mathbb{C}$. We denote

$$R_{\boldsymbol{k},\boldsymbol{\ell}} = \mathrm{Res}(F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X), \tilde{P}_{\boldsymbol{\ell}}(X)),$$

which is non-zero.

Thus, if $p > |R_{\boldsymbol{k},\boldsymbol{\ell}}|$, then $p \nmid R_{\boldsymbol{k},\boldsymbol{\ell}}$, and therefore the system of equations (5.4) has no solution over $\overline{\mathbb{F}}_p$. It is easy to see that the desired result follows when

$$p > \max_{\boldsymbol{k}\in\{0,\pm1,\dots,\pm K\}^m\setminus\{\mathbf{0}\}} \max_{\boldsymbol{\ell}\in\{0,\pm1,\dots,\pm L\}^m\setminus\{\mathbf{0}\}} |R_{\boldsymbol{k},\boldsymbol{\ell}}|. \tag{5.5}$$

Hence, it remains to estimate $R_{\boldsymbol{k},\boldsymbol{\ell}}$, for the parameters $\boldsymbol{k}$ and $\boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.5).

We note that considering $F_{\boldsymbol{k}}$ and $G_{\boldsymbol{k}}$, defined by (5.1), as products of at most $|k_1| + \ldots + |k_m|$ polynomials, we have

$$\deg(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}) \ll_{\boldsymbol{\varphi}} K,$$

and by Lemma 3.1 we obtain

$$\begin{aligned}\mathrm{h}\left(F_{\boldsymbol{k}}\right), \mathrm{h}\left(G_{\boldsymbol{k}}\right) &\le \sum_{i=1}^{m} \left(|k_i| \max\{\mathrm{h}(f_i) + \deg f_i, \mathrm{h}(g_i) + \deg g_i\}\right)\\ &\ll_{\boldsymbol{\varphi}} K,\end{aligned}$$

which implies

$$\mathrm{h}\left(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}\right) \ll_{\boldsymbol{\varphi}} K.$$

For the polynomial $\tilde{P}_{\boldsymbol{\ell}}$, we clearly have

$$\deg(\tilde{P}_{\boldsymbol{\ell}}) \le \deg(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}}) \ll_{\boldsymbol{\varphi}} L,$$

and it follows from (3.1) that

$$\begin{aligned}H(\tilde{P}_{\boldsymbol{\ell}}) &\le 2^{\deg \tilde{P}_{\boldsymbol{\ell}}} M(\tilde{P}_{\boldsymbol{\ell}}) \le 2^{\deg(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}})} M(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}})\\ &\le 2^{\deg(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}})} \sqrt{\deg(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}}) + 1} H(F_{\boldsymbol{\ell}} - G_{\boldsymbol{\ell}}).\end{aligned}$$

Thus, we conclude that

$$\mathrm{h}(\tilde{P}_{\boldsymbol{\ell}}) \ll_{\boldsymbol{\varphi}} L.$$

Therefore, for the parameters $\boldsymbol{k}$ and $\boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.5), by Lemma 3.3 we obtain

$$\log |R_{\boldsymbol{k},\boldsymbol{\ell}}| \ll_{\boldsymbol{\varphi}} KL, \tag{5.6}$$

which together with (5.5) gives the desired lower bound $\exp(c_1 KL)$ for p. Since all the implied constants in the above estimates are effectively computable, the constant c_1 is also effectively computable.

Finally, by the above discussions, when $p > \exp(c_1 KL)$, the system of equations (5.4) has no solution over $\overline{\mathbb{F}}_p$ for any linearly independent vectors $\boldsymbol{k}, \boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.5). In addition, if α is a solution of (5.2) but not a solution of (5.4) over $\overline{\mathbb{F}}_p$, then α must be a root of $W_{\mathcal{S}_1}$ over $\overline{\mathbb{F}}_p$. Hence, for the set $\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$ we have

$$\#\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L) \le \deg W_{\mathcal{S}_1} = \#\mathcal{S}_1.$$

This completes the proof by noticing (5.3).

5.2. **Proof of Corollary 2.2.** This follows directly from Theorem 2.1 applied to the rational functions $\varphi_1, \ldots, \varphi_m, \varrho_1, \ldots, \varrho_n$ instead of $\varphi_1, \ldots, \varphi_m$.

5.3. **Proof of Theorem 2.4.** We proceed as in the proof of Theorem 2.1. However, now invoking Lemma 3.4 to estimate the number $s(\boldsymbol{k}, \boldsymbol{\ell})$ of solutions to the system of equations (5.4) over $\overline{\mathbb{F}}_p$ for the parameters $\boldsymbol{k}$ and $\boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.5), we obtain

$$\sum_{\substack{\boldsymbol{k}\in\{0,\pm1,\ldots,\pm K\}^m\setminus\{\mathbf{0}\}\\ \boldsymbol{\ell}\in\{0,\pm1,\ldots,\pm L\}^m\setminus\{\mathbf{0}\}}} s(\boldsymbol{k}, \boldsymbol{\ell}) \le v_p(T),$$

where

$$T = \prod_{\boldsymbol{k}\in\{0,\pm1,\ldots,\pm K\}^m\setminus\{\mathbf{0}\}} \prod_{\boldsymbol{\ell}\in\{0,\pm1,\ldots,\pm L\}^m\setminus\{\mathbf{0}\}} |R_{\boldsymbol{k},\boldsymbol{\ell}}|.$$

Using the bound (5.6), we get the desired upper bound for $\log T$. Hence, we have

$$\#\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L) \le v_p(T) + \deg W_{\mathcal{S}_1} = v_p(T) + \#\mathcal{S}_1,$$

which completes the proof by noticing (5.3).

5.4. **Proof of Corollary 2.5.** Assuming that N is large enough, we take

$$K = L = \left\lceil (N/\log N)^{1/(2m+2)} \right\rceil$$

in Theorem 2.4. Since T has at most $c \log T/\log\log T$ distinct prime divisors for some absolute constant c, using the bound in Theorem 2.4, we derive that $v_p(T) = 0$ for all but

$$c \log T/\log\log T \ll_{\boldsymbol{\varphi}} (KL)^{m+1}/\log((KL)^{m+1}) \ll N(\log N)^{-2}$$

primes p (even without the restriction $p \le N$) when N is large enough.

If $v_p(T) = 0$, then by Theorem 2.4 we have that the cardinality $\#\mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$ is at most c_2 which is a constant depending on $\boldsymbol{\varphi}$. Note that if $\alpha \notin \mathcal{A}_{\boldsymbol{\varphi}}(p, K, L)$, then the elements $\varphi_1(\alpha), \ldots, \varphi_m(\alpha)$ do not satisfy two independent multiplicative relations with exponents bounded above by K in absolute value. Hence, at least $m - 1$ elements of $\varphi_1(\alpha), \ldots, \varphi_m(\alpha)$ are of order at least K. This completes the proof.

5.5. **Proof of Theorem 2.6.** It suffices to follow the same arguments as in the proof of Theorem 2.4 by noticing that in this case we need to consider vectors $\boldsymbol{k} \in \{0, \pm1, \ldots, \pm K\}^m \setminus \{\mathbf{0}\}$ and $\boldsymbol{\ell} \in \{0, \pm1, \ldots, \pm L\}^n \setminus \{\mathbf{0}\}$, and thus the contribution of those $\boldsymbol{\ell}$ is L^{n+1} in the bound of $\log T$ instead of L^{m+1}. This completes the proof.

5.6. **Proof of Corollary 2.7.** For N large enough, we take

$$K = \left\lceil N^{n/(2mn+m+n)}/(\log N)^{1/(2m)} \right\rceil \qquad \text{and} \qquad L = \left\lceil N^{m/(2mn+m+n)}/(\log N)^{1/(2n)} \right\rceil$$

in Theorem 2.6. Since T has at most $c \log T/\log\log T$ distinct prime divisors for some absolute constant c, using the bound in Theorem 2.6, we obtain that $v_p(T) = 0$ for all but

$$c \log T/\log\log T \ll_{\boldsymbol{\varphi},\boldsymbol{\varrho}} K^{m+1}L^{n+1}/\log(K^{m+1}L^{n+1}) \ll N(\log N)^{-2}$$

primes p when N is large enough.

Note that any K-multiplicatively independent elements $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{F}}_p^*$ generate a subgroup of $\overline{\mathbb{F}}_p^*$ of order at least $K^m \geq N^{mn/(2mn+m+n)}(\log N)^{-1/2}$. In addition, we have $L^n \geq N^{mn/(2mn+m+n)}(\log N)^{-1/2}$. The desired result now follows.

5.7. **Proof of Theorem 2.8.** For any m-tuple $\boldsymbol{k} = (k_1, \ldots, k_m) \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ define

$$\Omega_{\boldsymbol{k}} = \varphi_1^{k_1} \ldots \varphi_m^{k_m} \in \mathbb{Q}(X),$$

and for any n-tuple $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ let $\Theta_{\boldsymbol{\ell}} \in \mathbb{Q}(X)$ be defined by

$$\Theta_{\boldsymbol{\ell}} = \begin{cases} \Psi_{\ell_1} \circ \varrho_1 & \text{if } n = 1, \\ \sigma_n\left(\frac{\phi_{\ell_1}}{\psi_{\ell_1}^2} \circ \varrho_1, \ldots, \frac{\phi_{\ell_n}}{\psi_{\ell_n}^2} \circ \varrho_n\right) & \text{if } n \geq 2, \end{cases}$$

where $\psi_{\ell_1}, \Psi_{\ell_1}, \phi_{\ell_1}$ have been defined in Section 3.3 and σ_n is the n-th summation polynomial associated to the curve E defined in Lemma 3.7.

We remark that for any $\alpha \in \mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L)$, if $(\varrho_i(\alpha), \cdot)$ is a torsion point for some $1 \leq i \leq n$, then this situation is essentially reduced to the case when $n = 1$.

So, from now on, when $n \geq 2$, we do not consider those $\alpha \in \mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L)$ such that $(\varrho_i(\alpha), \cdot)$ is a torsion point for some $1 \leq i \leq n$.

The proof follows similar lines as in the proof of Theorem 2.1. Indeed, recall that $\mathcal{S}_2 \subset \mathbb{C}$ is the set of all the elements $\alpha \in \mathbb{C}$ which are solutions to the system of equations

$$\Omega_{\boldsymbol{k}}(X) - 1 = \Theta_{\boldsymbol{\ell}}(X) = 0 \quad \text{for some } \boldsymbol{k} \in \mathbb{Z}^m \setminus \{\mathbf{0}\} \text{ and } \boldsymbol{\ell} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}.$$

By Lemma 3.11 (for $n = 1$ it suffices to apply Lemma 3.12) and noticing (3.4) and the definition of summation polynomials, the set $\mathcal{S}_2$ is finite and we have

$$\#\mathcal{S}_2 \ll_{\boldsymbol{\varphi},\boldsymbol{\varrho},E} 1,$$

where the implied constant is effectively computable when $n = 1$ by Lemma 3.12.

Write

$$\Omega_{\boldsymbol{k}} = \frac{F_{\boldsymbol{k}}}{G_{\boldsymbol{k}}}, \quad \gcd(F_{\boldsymbol{k}}, G_{\boldsymbol{k}}) = 1, \qquad \text{and} \qquad \Theta_{\boldsymbol{\ell}} = \frac{U_{\boldsymbol{\ell}}}{V_{\boldsymbol{\ell}}}, \quad \gcd(U_{\boldsymbol{\ell}}, V_{\boldsymbol{\ell}}) = 1,$$

with polynomials $F_{\boldsymbol{k}}, G_{\boldsymbol{k}}, U_{\boldsymbol{\ell}}, V_{\boldsymbol{\ell}} \in \mathbb{Z}[X]$.

Let $W_{\mathcal{S}_2} \in \mathbb{Z}[X]$ be the product of all the irreducible polynomials (without multiplicity) having some $\alpha \in \mathcal{S}_2$ as a root. Define

$$\overline{U}_{\boldsymbol{\ell}} = \frac{U_{\boldsymbol{\ell}}}{\gcd(U_{\boldsymbol{\ell}}, U'_{\boldsymbol{\ell}})} \qquad \text{and} \qquad \tilde{U}_{\boldsymbol{\ell}} = \frac{\overline{U}_{\boldsymbol{\ell}}}{\gcd(\overline{U}_{\boldsymbol{\ell}}, W_{\mathcal{S}_2})} \in \mathbb{Z}[X].$$

Note that since the polynomial $\overline{U}_{\boldsymbol{\ell}}$ has only simple roots, we have $\gcd(\tilde{U}_{\boldsymbol{\ell}}, W_{\mathcal{S}_2}) = 1$.

Then, the system of equations

$$F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X) = \tilde{U}_{\boldsymbol{\ell}}(X) = 0 \tag{5.7}$$

has no solution over $\mathbb{C}$. We denote

$$R_{\boldsymbol{k},\boldsymbol{\ell}} = \operatorname{Res}(F_{\boldsymbol{k}}(X) - G_{\boldsymbol{k}}(X), \tilde{U}_{\boldsymbol{\ell}}(X)),$$

which is non-zero.

Thus, if $p > |R_{\boldsymbol{k},\boldsymbol{\ell}}|$, then $p \nmid R_{\boldsymbol{k},\boldsymbol{\ell}}$, and therefore the system of equations (5.7) has no solution over $\overline{\mathbb{F}}_p$. It is easy to see that the desired result follows when

$$p > \max_{\boldsymbol{k}\in\{0,\pm1,\ldots,\pm K\}^m\setminus\{\boldsymbol{0}\}} \max_{\boldsymbol{\ell}\in\{0,\pm1,\ldots,\pm L\}^n\setminus\{\boldsymbol{0}\}} |R_{\boldsymbol{k},\boldsymbol{\ell}}|. \tag{5.8}$$

Hence, it remains to estimate $R_{\boldsymbol{k},\boldsymbol{\ell}}$, for the parameters $\boldsymbol{k}$ and $\boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.8).

From the proof of Theorem 2.1, for any $\boldsymbol{k} \in \{0, \pm1, \ldots, \pm K\}^m \setminus \{\boldsymbol{0}\}$ we have

$$\deg(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}) \ll_{\boldsymbol{\varphi}} K, \qquad \mathrm{h}(F_{\boldsymbol{k}} - G_{\boldsymbol{k}}) \ll_{\boldsymbol{\varphi}} K. \tag{5.9}$$

If $n = 1$ (that is, $\boldsymbol{\ell} = \ell_1$), then directly by Lemmas 3.2 and 3.5 and by (3.2), for $\ell_1 \le L$, we have

$$\deg \Theta_{\ell_1} \ll_{\varrho_1} L^2 \qquad \text{and} \qquad \mathrm{h}\left(\Theta_{\ell_1}\right) \ll_{\varrho_1,E} L^2. \tag{5.10}$$

Now, we assume that $n \ge 2$. In this case, it follows from (3.1) that

$$\begin{aligned} H(\tilde{U}_{\boldsymbol{\ell}}) &\le 2^{\deg \tilde{U}_{\boldsymbol{\ell}}} M(\tilde{U}_{\boldsymbol{\ell}}) \le 2^{\deg U_{\boldsymbol{\ell}}} M(U_{\boldsymbol{\ell}}) \\ &\le 2^{\deg U_{\boldsymbol{\ell}}} \sqrt{\deg U_{\boldsymbol{\ell}} + 1} H(U_{\boldsymbol{\ell}}). \end{aligned} \tag{5.11}$$

By Lemmas 3.2, 3.5 and 3.6 we have

$$\begin{aligned} \deg(\phi_{\ell_i} \circ \varrho_i) &\ll_{\varrho_i} \ell_i^2 \qquad \text{and} \qquad \deg(\psi_{\ell_i}^2 \circ \varrho_i) \ll_{\varrho_i} \ell_i^2, \\ \mathrm{h}(\phi_{\ell_i} \circ \varrho_i) &\ll_{\varrho_i,E} \ell_i^2 \qquad \text{and} \qquad \mathrm{h}(\psi_{\ell_i}^2 \circ \varrho_i) \ll_{\varrho_i,E} \ell_i^2. \end{aligned} \tag{5.12}$$

Applying again Lemma 3.2 (with $R = \sigma_n$ and $f_i = \frac{\phi_{\ell_i}}{\psi_{\ell_i}^2} \circ \varrho_i$, $i = 1, \ldots, n$), Lemmas 3.7 and 3.8 and the estimates (5.12), for $\boldsymbol{\ell} \in \{0, \pm1, \ldots, \pm L\}^n \setminus \{\boldsymbol{0}\}$ we obtain

$$\deg \Theta_{\boldsymbol{\ell}} \ll_{\boldsymbol{\varrho}} L^2, \qquad \mathrm{h}\left(\Theta_{\boldsymbol{\ell}}\right) \ll_{\boldsymbol{\varrho},E} L^2. \tag{5.13}$$

Now, since by definitions of degree and height of a rational function we have

$$\deg \tilde{U}_{\boldsymbol{\ell}} \le \deg U_{\boldsymbol{\ell}} \le \deg \Theta_{\boldsymbol{\ell}}, \qquad \mathrm{h}(U_{\boldsymbol{\ell}}) \le \mathrm{h}(\Theta_{\boldsymbol{\ell}}),$$

from (5.10), (5.11) and (5.13) for both cases we conclude that

$$\deg \tilde{U}_{\boldsymbol{\ell}} \ll_{\boldsymbol{\varrho}} L^2, \qquad h(\tilde{U}_{\boldsymbol{\ell}}) \ll_{\boldsymbol{\varrho},E} L^2. \tag{5.14}$$

Therefore, for the parameters $\boldsymbol{k}$ and $\boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.8), by Lemma 3.3 and using (5.9) and (5.14), we obtain

$$\log |R_{\boldsymbol{k},\boldsymbol{\ell}}| \ll_{\boldsymbol{\varphi},\boldsymbol{\varrho},E} KL^2, \tag{5.15}$$

which together with (5.8) gives the desired lower bound $\exp(c_1 KL^2)$ for p. Since the implied constants in (5.9), (5.10), (5.12), (5.13) and (5.14) are all effectively computable, the constant c_1 is also effectively computable.

Finally, by the above discussions, when $p > \exp(c_1 KL^2)$, the system of equations (5.7) has no solution over $\overline{\mathbb{F}}_p$ for any $\boldsymbol{k}, \boldsymbol{\ell}$ in the same ranges as on the right hand side of (5.8). Hence, as before, we obtain

$$\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p, K, L) \le \#\mathcal{S}_2.$$

This completes the proof.

5.8. **Proof of Theorem 2.10.** We proceed as in the proof of Theorem 2.8 and follow the approach in proving Theorem 2.4. However, this time we use the bound (5.15) instead of (5.6). So, the cardinality $\#\mathcal{B}_{\boldsymbol{\varphi},\boldsymbol{\varrho},E}(p,K,L)$ is at most $v_p(T)+\#\mathcal{S}_2$. The desired result then follows.

5.9. **Proof of Corollary 2.11.** We follow the approach in proving Corollary 2.7. Assuming that N is large enough and taking

$$K=\left\lceil N^{n/(2mn+2m+n)}/(\log N)^{1/(2m)}\right\rceil \qquad \text{and} \qquad L=\left\lceil N^{m/(2mn+2m+n)}/(\log N)^{1/(2n)}\right\rceil$$

in Theorem 2.10, we obtain the desired result.

5.10. **Proof of Theorem 2.12.** For any n-tuples $\boldsymbol{k}=(k_1,\dots,k_n)\in\mathbb{Z}^n\setminus\{\mathbf{0}\}$, as before we define

$$\Theta_{\boldsymbol{k}}=\begin{cases}\Psi_{k_1}\circ\varrho_1 & \text{if } n=1,\\ \sigma_n\left(\frac{\phi_{k_1}}{\psi_{k_1}^2}\circ\varrho_1,\dots,\frac{\phi_{k_n}}{\psi_{k_n}^2}\circ\varrho_n\right) & \text{if } n\ge 2.\end{cases}$$

Recall that $\mathcal{S}_3\subset\mathbb{C}$ is the set of all the elements $\alpha\in\mathbb{C}$ which are solutions to the system of equations

$$\Theta_{\boldsymbol{k}}(X)=\Theta_{\boldsymbol{\ell}}(X)=0$$

for some linearly independent vectors $\boldsymbol{k},\boldsymbol{\ell}\in\mathbb{Z}^n$. Note that $\boldsymbol{k},\boldsymbol{\ell}$ are also linearly independent over $\mathrm{End}(E)$. Then, by Lemma 3.10 the set $\mathcal{S}_3$ is finite and we have

$$\#\mathcal{S}_3\ll_{\boldsymbol{\varrho},E}1.$$

Now, applying similar lines as in the proof of Theorem 2.8, (5.15) becomes

$$\log|R_{\boldsymbol{k},\boldsymbol{\ell}}|\ll_{\boldsymbol{\varrho},E}K^2L^2,$$

where $\boldsymbol{k},\boldsymbol{\ell}$ are two linearly independent vectors in $\mathbb{Z}^n$ satisfying

$$\boldsymbol{k}\in\{0,\pm1,\dots,\pm K\}^m,\quad \boldsymbol{\ell}\in\{0,\pm1,\dots,\pm L\}^n.$$

Then, we obtain that there exist an effectively computable constant c_1 and a constant c_2 both depending only on $\boldsymbol{\varrho},E$ such that for any prime $p>\exp(c_1K^2L^2)$, for the set (2.4) we have

$$\#\mathcal{C}_{\boldsymbol{\varrho},E}(p,K,L)\le\#\mathcal{S}_3.$$

Here we omit the details.

5.11. **Proof of Theorems 2.15 and 2.17.** Both results can be proved by proceeding as in the proof of Theorem 2.12 and following the same approach as in proving Theorem 2.4.

5.12. **Proof of Corollary 2.16.** One can prove the desired result by following the approach used in proving Corollary 2.5 with

$$K=L=\left\lceil(N/\log N)^{1/(2n+4)}\right\rceil$$

in Theorem 2.15.

5.13. **Proof of Corollary 2.18.** We obtain the desired result by following the approach in proving Corollary 2.7 with

$$K = \left\lceil N^{n/(2mn+2m+2n)}/(\log N)^{1/(2m)} \right\rceil \qquad \text{and} \qquad L = \left\lceil N^{m/(2mn+2m+2n)}/(\log N)^{1/(2n)} \right\rceil$$

in Theorem 2.17.

Acknowledgement

The authors are grateful to Igor Shparlinski and Umberto Zannier for helpful discussions, and to the authors of [25] for sending them a preliminary version of their work. For this research, L.M. was supported by the Austrian Science Fund (FWF): Project P31762, A.O. was supported by the Australian Research Council Grants DP180100201 and DP200100355, and M.S. was supported by the Australian Research Council Grant DE190100888. A.O. also gratefully acknowledges the generosity and hospitality of the Max Planck Institute for Mathematics where parts of her work on this project were developed.

References

[1] F. Amoroso and U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*, B. Lond. Math. Soc. **42** (2010), 489–498.15

[2] J. Ax, *Some topics in differential algebraic geometry. I. Analytic subgroups of algebraic groups*, Amer. J. Math. **94** (1972), 1195–1204.19

[3] F. Barroero, *CM relations in fibered powers of elliptic families*, J. Inst. Math. Jussieu, **18** (2019), 941–956.17

[4] F. Barroero and L. Capuano, *Linear relations in families of powers of elliptic curves*, Algebra & Number Theory **10** (2016), 195–214.16

[5] F. Barroero and L. Capuano, *Unlikely intersections in products of families of elliptic curves and the multiplicative group*, Q. J. Math. **68** (2017), 1117–1138. 16, 17, 20

[6] F. Barroero and M. Sha, *Torsion points with multiplicatively dependent coordinates on elliptic curves*, B. Lond. Math. Soc., https://doi.org/10.1112/blms.12363. 2, 15

[7] A. Bérczes, A. Ostafe, I. E. Shparlinski and J. H. Silverman, *Multiplicative dependence among iterated values of rational functions modulo finitely generated groups*, Int. Math. Res. Notices, https://doi.org/10.1093/imrn/rnz091. 2

[8] E. Bombieri, P. Habegger, D. Masser and U. Zannier, *A note on Maurin's theorem*, Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **21** (2010), 251–260.14

[9] E. Bombieri, D. Masser and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Notices **20** (1999), 1119–1140. 2, 14, 16

[10] E. Bombieri, D. Masser and U. Zannier,*Finiteness results for multiplicatively dependent points on complex curves*, Michigan Math. J. **51** (2003), 451–466. 2

[11] E. Bombieri, D. Masser and U. Zannier, *On unlikely intersections of complex varieties with tori*, Acta Arith. **133** (2008), 309–323. 2

[12] L. Capuano, D. Masser, J. Pila, and U. Zannier, *Rational points on Grassmannians and unlikely intersections in tori*, B. Lond. Math. Soc. **48** (2016), 141–154.16

[13] M.-C. Chang, *Elements of large order in prime finite fields*, B. Aust. Math. Soc. **88** (2013), 169–176. 5, 6

[14] M.-C. Chang, B. Kerr, I. E. Shparlinski and U. Zannier, *Elements of large orders on varieties over prime finite fields*, J. Theor. Nombres Bordeaux **26** (2014), 579–593. 5, 6

[15] C. D'Andrea, A. Ostafe, M. Sombra and I. Shparlinski, *Reductions modulo primes of systems of polynomial equations and algebraic dynamical systems*, Trans. Amer. Math. Soc. **371** (2019), 1169–1198. 10

[16] A. Dubickas and M. Sha, *Multiplicative dependence of the translations of algebraic numbers*, Rev. Mat. Iberoam. **34** (2018), 1789–1808. 2

[17] L. Frey, *Explicit small heights in infinite non-abelian extensions*, Preprint, 2019, available at https://arxiv.org/abs/1712.04214. 15

[18] A. Galateau, *Une minoration du minimum essentiel sur les variétés abéliennes*, Comment. Math. Helv. **85** (2010), 775–812. 2, 8, 15

[19] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 3rd edition, Cambridge Univ. Press, Cambridge, 2013. 11

[20] D. Ghioca and R. Moosa, *Division points on subvarieties of isotrivial semi-abelian varieties*, Int. Math. Res. Notices **2006** (2006), 1–23. 3

[21] D. Gómez-Pérez, J. Gutierrez, A. Ibeas and D. Sevilla, *Common factors of resultants modulo p*, B. Aust. Math. Soc. **79** (2009), 299–302. 11

[22] P. Habegger, *On the Bounded Height Conjecture*, Int. Math. Res. Notices **2009** (2009), 860–886. 14

[23] P. Habegger, *Effective height upper bounds on algebraic tori*, Around the Zilber-Pink conjecture, Panor. Synthèses, 52, Soc. Math. France, Paris, 2017, 167–242. 14

[24] P. Habegger and J. Pila, *O-minimality and certain atypical intersections*, Ann. Sci. Éc. Norm. Supér. **49** (2016), 813–858. 19

[25] B. Kerr, J. Mello and I. E. Shparlinski, *On elements of large order of elliptic curves and multiplicative dependent images of rational functions over finite fields*, Preprint, 2020. 5, 27

[26] T. Krick, L. M. Pardo and M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J. **109** (2001), 521–598. 10

[27] G. Maurin, *Courbes algébriques et équations multiplicatives*, Math. Ann. **341** (2008), 789–824. 2, 3, 4, 14

[28] D. Masser, *Unlikely intersections for curves in the multiplicative groups over positive characteristic*, Q. J. Math. **65** (2014), 505-515. 3

[29] D. Masser and U. Zannier, *Torsion points on families of products of elliptic curves*, Adv. Math. **259** (2014), 116–133. 16

[30] J. McKee, *Computing division polynomials*, Math. Comp. **63** (1994), 767–771. 12

[31] A. Ostafe, M. Sha, I. E. Shparlinski and U. Zannier, *On abelian multiplicatively dependent points on a curve in a torus*, Q. J. Math. **69** (2018), 391–401. 2

[32] A. Ostafe, M. Sha, I. E. Shparlinski and U. Zannier, *On multiplicative dependence of values of rational functions and a generalisation of the Northcott theorem*, Michigan Math. J. **68** (2019), 385–407. 2

[33] F. Pappalardi, M. Sha, I. E. Shparlinski and C. Stewart, *On multiplicatively dependent vectors of algebraic numbers*, Trans. Amer. Math. Soc. **370** (2018), 6221–6244. 2

[34] J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), 591–616. 16

[35] J. Pila and U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Rend. Lincei Mat. Appl. **19** (2008), 149–162. 16

[36] R. Pink and D. Rössler, *On the Manin-Mumford and Mordell-Lang conjectures in positive characteristic*, Algebra & Number Theory **7** (2013), 2039–2057. 3

[37] T. Scanlon, *Positive characteristic ManinMumford theorem*, Compos. Math. **141** (2005), 1351-1364. 3

[38] I. A. Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Preprint, 2004, available at https://eprint.iacr.org/2004/031. 13

[39] M. Sha, I. E. Shparlinski and C. Stewart, *On the distribution of multiplicatively dependent vectors*, Preprint, 2019, available at https://arxiv.org/abs/1903.09796. 2

[40] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, Dordrecht, 2009. 11

[41] E. Viada, *The intersection of a curve with algebraic subgroups in a product of elliptic curves*, Ann. Sc. Norm. Super. Pisa Cl. Sci. **2** (2003), 47–75. 2, 16

[42] E. Viada, *The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve*, Algebra & Number Theory **2** (2008), 249–298. 2, 8, 15
[43] J. F. Voloch, *On the order of points on curves over finite fields*, Integers **7** (2007), A49. 5
[44] J. F. Voloch, *Elements of high order on finite fields from elliptic curves*, B. Aust. Math. Soc. **81** (2010), 425–429. 7
[45] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren Math. Wiss. 326, Springer, Berlin, 2000. 10
[46] L. C. Washington, *Elliptic curves: number theory and cryptography*, 2nd ed., Chapman & Hall/CRC, Boca Raton, 2008. 11, 12
[47] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, 2012, With appendixes by David Masser. 14, 15, 16

Dipartimento di Matematica e Fisica, Università di Roma Tre, Largo San Murialdo 1, 00146 Roma, Italy
E-mail address: fbarroero@gmail.com

DISMA "Luigi Lagrange", Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy
E-mail address: laura.capuano@polito.it

Johann Radon Institute for Computational and Applied Mathematics, Altenberger Strasse 69, 4040 Linz, Austria
E-mail address: laszlo.merai@oeaw.ac.at

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: alina.ostafe@unsw.edu.au

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: shamin2010@gmail.com