# ELLIPTIC CURVES WITH LONG ARITHMETIC PROGRESSIONS HAVE LARGE RANK

NATALIA GARCIA-FRITZ AND HECTOR PASTEN

Abstract. For any family of elliptic curves over the rational numbers with fixed $j$-invariant, we prove that the existence of a long sequence of rational points whose $x$-coordinates form a non-trivial arithmetic progression implies that the Mordell-Weil rank is large, and similarly for $y$-coordinates. We give applications related to uniform boundedness of ranks, conjectures by Bremner and Mohanty, and arithmetic statistics on elliptic curves. Our approach involves Nevanlinna theory as well as Rémond's quantitative extension of results of Faltings.

## 1. Introduction

It is an open problem whether the ranks of elliptic curves over $\mathbb{Q}$ are uniformly bounded. Various heuristics have been developed in support of uniform boundedness [1, 27, 31, 32, 37, 46]. Also, the second author has shown [28] that a conjecture of Lang in diophantine approximation implies uniform boundedness of ranks for families of elliptic curves with a fixed $j$-invariant. In the direction of unboundedness, it is known that elliptic curves over a global function field such as $\mathbb{F}_p(t)$ can have arbitrarily large rank even if one considers quadratic twists families [38, 43] and examples over $\mathbb{Q}$ with remarkably large rank are known [8]. It is natural to look for a mechanism forcing the rank of elliptic curves over $\mathbb{Q}$ to be large, and certain patterns on rational points seem to achieve this.

Given an elliptic curve $E$ over $\mathbb{Q}$, an *$x$-arithmetic progression* is a sequence $P_1, ..., P_N$ of $\mathbb{Q}$-rational points on $E$ having their $x$-coordinates in arithmetic progression for some choice of Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ for $E$. A *$y$-arithmetic progression* on $E$ is defined similarly. Such sequences are said to be *non-trivial* if the resulting arithmetic progression in $x$ or $y$ coordinates is non-constant. These definitions are in fact independent of the choice of Weierstrass equation.

Bremner [5] has conjectured that rational points of an $x$-arithmetic progression on an elliptic curve $E$ over $\mathbb{Q}$ tend to be linearly independent in the Mordell-Weil group. The conjecture is motivated by numerous examples, as well as theoretical evidence such as [6] where it is shown that for a quadratic twist family over $\mathbb{Q}$, the elliptic curves of rank 1 have $x$-arithmetic progressions of uniformly bounded length. See also [7, 14, 26, 41, 42] and the references therein for further examples supporting Bremner's conjecture.

In this work we prove Bremner's conjecture for families of elliptic curves with fixed $j$-invariant, in particular, for quadratic twist families. Given an elliptic curve $E$ over $\mathbb{Q}$, we let $\beta_x(E)$ be the maximal length of a non-trivial $x$-arithmetic progression of rational points in $E$, and $\beta_y(E)$ is defined similarly for $y$-arithmetic progressions. We prove

**Theorem 1.1.** *Let $j_0 \in \mathbb{Q}$. There is an effectively computable constant $c(j_0) > 0$ that only depends on $j_0$, such that for every elliptic curve $E$ over $\mathbb{Q}$ with $j$-invariant equal to $j_0$ we have*

$$1 + \operatorname{rank} E(\mathbb{Q}) \geq c(j_0) \cdot \log \max\{\beta_x(E), \beta_y(E)\}.$$

*Date*: February 28, 2020.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 30D35, 11B25.

*Key words and phrases.* Ranks, arithmetic progression, elliptic curve, Nevanlinna theory, abelian varieties.

N. G.-F. was supported by the FONDECYT Iniciación en Investigación grant 11170192 and the CONICYT PAI grant 79170039. H.P. was supported by FONDECYT Regular grant 1190442.

In this work, by "effectively computable" we always mean that an explicit closed formula can be obtained after some calculation. For instance, in Theorem 1.1 we can take

$$c(j_0) = \frac{1}{80^{46}\,(209 + \max\{\log(1+\log H(j_0)), 255 + \log\,(2+\log(1+\log H(j_0)))\})} \tag{1.1}$$

where $H(j_0)$ is the naive height, namely $H(a/b) = \max\{|a|, |b|\}$ for coprime integers $a, b$ with $b \neq 0$. Although it should be clear from the formula that we did not try to numerically optimize this estimate, let us remark that this value for $c(j_0)$ is satisfactory in the aspect that it is of the order of magnitude of $1/(\log\log H(j_0))$, so, it tends to 0 extremely slowly.

We prove that (1.1) is admissible for Theorem 1.1 in Section 6.5 using (among other tools) a comparison between the Theta height and the Faltings height of abelian varieties [30].

It turns out that arithmetic progressions on elliptic curves not only relate to the rank. We also prove that the (algebraic) torsion points do not have arbitrarily long patterns of this type.

**Theorem 1.2.** *Let $E$ be an elliptic curve over $\mathbb{Q}^{alg}$ with a given Weierstrass equation. The set of $x$-coordinates of the torsion points of $E(\mathbb{Q}^{alg})$ does not contain arbitrarily long non-trivial arithmetic progressions. The same holds for $y$-coordinates. A bound for the length of such progressions can be effectively computed from the $j$-invariant of $E$.*

Heuristically, these results are consistent with the fact that the group structure on elliptic curves is incompatible with the additive structure of the affine line via the $x$ or $y$-coordinate maps.

Theorems 1.1 and 1.2 (cf. Section 6.4) are special cases of Theorem 6.1 which concerns elliptic curves over number fields and more general patterns on algebraic points, not just arithmetic progressions on $x$ or $y$-coordinates of rational points. Our proof of Theorem 6.1 heavily uses Nevanlinna's value distribution theory for complex holomorphic maps in order to compute the Kawamata locus of certain sub-varieties of abelian varieties. This will allow us to apply Rémond's quantitative version of Faltings' theorem on rational points of sub-varieties of abelian varieties (cf. [10, 11, 34]), which will be our main tool to control $x$ and $y$-arithmetic progressions on elliptic curves.

Let us now discuss some applications of Theorem 1.1. Given an elliptic curve $E$ over $\mathbb{Q}$ and a squarefree integer $D$, we let $E^{(D)}$ be the quadratic twist of $E$ by $D$. The number of distinct prime factors of $D$ is denoted by $\omega(D)$. From Theorem 1.1 and standard rank bounds we deduce

**Corollary 1.3** (cf. Sec. 7.1)**.** *Given an elliptic curve $E$ over $\mathbb{Q}$, there is an effectively computable constant $C(E) > 0$ such that for every squarefree integer $D$ we have*

$$\max\{\beta_x(E^{(D)}), \beta_y(E^{(D)})\} \leq C(E)^{\omega(D)+1}.$$

In connection with conjectures on uniform boundedness of ranks, Theorem 1.1 directly gives

**Corollary 1.4.** *Let $j_0 \in \mathbb{Q}$. Suppose that the elliptic curves over $\mathbb{Q}$ of $j$-invariant equal to $j_0$ have uniformly bounded Mordell-Weil rank. Then there is a number $N(j_0)$ only depending on $j_0$ with the following property: For each elliptic curve $E$ over $\mathbb{Q}$ with $j$-invariant equal to $j_0$ we have*

$$\max\{\beta_x(E), \beta_y(E)\} \leq N(j_0).$$

We remark that, in view of [28], the assumption that elliptic curves over $\mathbb{Q}$ with a fixed $j$-invariant have uniformly bounded Mordell-Weil rank, is implied by a conjecture of Lang on the error terms in Diophantine approximation.

Mohanty [24, 25] conjectured that there is a uniform bound for the length of $x$ and $y$-arithmetic progressions on Mordell elliptic curves $A_n : y^2 = x^3 + n$ with $n \in \mathbb{Z}$ sixth-power free. Mohanty in fact made the stronger conjecture that $\beta_x(A_n)$ and $\beta_y(A_n)$ are at most 4, but this was disproved for $y$-arithmetic progressions by Lee and Velez [20]. Several constructions as well as extensive numerical searches have been carried out looking for long $x$ or $y$-arithmetic progressions on Mordell elliptic

curves (cf. [42] and the references therein), but the record continues to be $x$-arithmetic progressions of length 4 and $y$-arithmetic progressions of length 6 as found by Lee and Velez [20].

Mohanty's conjecture on uniform boundedness of $x$ and $y$ arithmetic progressions on Mordell elliptic curves remains open. In support of this conjecture besides the search for examples, the first author used extensions of methods by Bogomolov and Vojta to show that the case of $y$-arithmetic progressions follows from the Bombieri-Lang conjecture for surfaces of general type [13]. In addition, let us remark that Corollary 1.4 with $j_0 = 0$ gives

**Corollary 1.5.** *The uniform boundedness conjecture for ranks of elliptic curves over $\mathbb{Q}$ with $j$-invariant equal to 0 implies Mohanty's conjecture for both $x$ and $y$-arithmetic progressions.*

Theorem 1.1 also allows us to prove *unconditionally* that Mohanty's conjecture holds on average, in the sense that the average $\tau$-moments of $\beta_x(A_n)$ and $\beta_y(A_n)$ are finite for certain $\tau > 0$.

**Theorem 1.6** (cf. Sec. 7.2)**.** *For $x > 0$ let $S(x)$ be the set of sixth-power free integers $n$ with $|n| \leq x$. There are absolute constants $\tau, M > 0$ such that for all $x > 1$ we have*

$$\frac{1}{\#S(x)} \sum_{n \in S(x)} \max\{\beta_x(A_n), \beta_y(A_n)\}^\tau < M.$$

The proof of Theorem 1.6 combines Theorem 1.1 with results of Fouvry [12] on upper bounds for the average size of 3-isogeny Selmer groups for Mordell elliptic curves, which in turn relies on the Davenport-Heilbronn theorem on 3-torsion of class groups of quadratic fields. See [2] for the exact computation of the average size of the 3-isogeny Selmer groups of Mordell elliptic curves.

More generally, Theorem 1.1 allows us to study arithmetic statistic questions related to $\beta_x(E)$ and $\beta_y(E)$ provided that we have good control on Selmer groups. Indeed, given a positive integer $m$ and an elliptic curve $E$ over $\mathbb{Q}$ we have the exact sequence

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to S_m(E) \to Ш(E)[m] \to 0 \tag{1.2}$$

where $S_m(E)$ is the $m$-Selmer group and $Ш(E)[m]$ is the $m$-torsion of the Shafarevich-Tate group. The classical proof of the Mordell-Weil theorem shows that $S_m(E)$ is finite, and from (1.2) we have

$$m^{\operatorname{rank} E(\mathbb{Q})} \leq \#\left(E(\mathbb{Q})/mE(\mathbb{Q})\right) \leq \#S_m(E).$$

Therefore, estimates for the size of $m$-Selmer groups give bounds for *exponential* functions of the rank, and we remark that there are several strong results in the literature for the arithmetic statistics for the size of $m$-Selmer group of elliptic curves. This is well-suited for our applications, as Theorem 1.1 (and, more generally, Theorem 6.1) bounds the maximal length of an arithmetic progression in terms of an exponential function of the rank. For applications along these lines, it is crucial that our lower bound for the rank in Theorem 1.1 is logarithmic; see Section 7 for details.

As the literature on arithmetic statistics of $m$-Selmer groups of elliptic curves is abundant and growing, we will only focus on the particularly convenient case of the elliptic curves $B_n$ defined by $y^2 = x^3 - n^2x$. These elliptic curves are associated to the classical "congruent number problem". Here, results of Heath-Brown [17] allow us to control *all* the average moments of $\beta_x(B_n)$ and $\beta_y(B_n)$.

**Theorem 1.7** (cf. Sec. 7.3)**.** *Let $Q(x)$ be the set of odd squarefree integers $n$ with $1 \leq n \leq x$. Let $k > 0$. There is a constant $M(k) > 0$ depending only on $k$ such that for all $x > 1$ we have*

$$\frac{1}{\#Q(x)} \sum_{n \in Q(x)} \max\{\beta_x(B_n), \beta_y(B_n)\}^k < M(k).$$

Let us mention that $x$-arithmetic progressions on the elliptic curves $B_n$ are studied in detail in [6] *under the assumption* $\operatorname{rank} B_n(\mathbb{Q}) \leq 1$ and in [41] for a specific sub-family arising from an elliptic surface of rank 3. The study in [6] is motivated by a connection with the problem of existence of a $3 \times 3$ magic square formed by different integer squares [36].

## 2. Review of Nevanlinna theory

In this section we set up the notation regarding Nevanlinna theory for holomorphic maps into complex projective varieties. Specially, we introduce the counting, proximity and height functions. We also recall the fundamental properties of these functions, including the First and Second Main Theorems. All the results in this section are standard and we include them for later reference. See for instance [45] for proofs and more general versions of the results in this section.

2.1. **Definitions.** Let $X$ be a smooth projective variety over $\mathbb{C}$ (we will identify the algebraic variety $X$ with the complex manifold $X(\mathbb{C})$ if no confusion can arise). Let $D$ be a divisor on $X$ and for each point $x \in X$ we let $\phi_{D,x}$ be a local equation for $D$. The support of $D$ is $\operatorname{supp} D$. Given a complex holomorphic map $f : \mathbb{C} \to X$ with image not contained in $\operatorname{supp} D$, we define for $r \geq 0$

$$n_X(f, D, r) = \sum_{|z| \leq r} \operatorname{ord}_z(f^* \phi_{D,f(z)}).$$

For each $r$ the sum is finite. The *counting function* is

$$\begin{aligned} N_X(f, D, r) &= \int_0^r (n_X(f, D, t) - n_X(f, D, 0)) \frac{dt}{t} + n_X(f, D, 0) \log r \\ &= \sum_{0 < |z| \leq r} \operatorname{ord}_z(f^* \phi_{D,f(z)}) \log \frac{r}{|z|} + \operatorname{ord}_0(f^* \phi_{D,f(z)}) \log r. \end{aligned}$$

If $f(0) \notin \operatorname{supp} D$, then the counting function takes the simpler form

$$N_X(f, D, r) = \int_0^r n_X(f, D, t) \frac{dt}{t}.$$

A *Weil function for* $D$ is a function $\lambda_{X,D} : X - \operatorname{supp} D \to \mathbb{R}$ satisfying that for each $x \in X$ there is a complex neighborhood $U_x \subseteq X$ of $x$ and a continuous function $\alpha_x : U_x \to \mathbb{R}$ such that $\lambda_{X,D}(y) = -\log |\phi_{D,x}(y)| + \alpha_x(y)$ for all $y \in U_x - \operatorname{supp} D$. It is a standard result that Weil functions for $D$ exist, and they are unique up to a bounded continuous function on $X - \operatorname{supp} D$.

With $f : \mathbb{C} \to X$ and $D$ as before and a choice of Weil function $\lambda_{X,D}$, the *proximity function* is

$$m_X(f, D, r) = \int_0^{2\pi} \lambda_{X,D} \left( f(r \cdot \exp(i\theta)) \right) \frac{d\theta}{2\pi}.$$

The function $m_X(f, D, -) : \mathbb{R}_{\geq 0} \to \mathbb{R}$ is well-defined up to adding a bounded function.

The *Nevanlinna height* of $f$ with respect to $D$ is the function $T_X(f, D, -) : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by

$$T_X(f, D, r) = N_X(f, D, r) + m_X(f, D, r).$$

Due to the choice of Weil function in $m_X(f, D, -)$, we have that $T_X(f, D, -)$ is well defined up to a bounded function of $r$.

2.2. **Basic properties.** Let us briefly recall some of the fundamental properties of the counting, proximity, and height functions. We use Landau's notation $u(x) = O(v(x))$ for functions $u, v : \mathbb{R}_{\geq 0} \to \mathbb{C}$ with $v$ positive valued, to indicate that there is a constant $M$ independent of $x$ such that for all $x > 0$ we have $|u(x)| \leq M \cdot v(x)$.

**Lemma 2.1.** *Let $X$ be a smooth complex projective variety and $f : \mathbb{C} \to X$ a holomorphic map.*

- *(Additivity) Let $D_1, D_2$ be divisors on $X$ such that the image of $f$ is not contained in $\operatorname{supp} D_1 \cup \operatorname{supp} D_2$. Let $a, b \in \mathbb{Z}$. Then for all $r > 0$ we have*

$$\begin{aligned} N_X(f, aD_1 + bD_2, r) &= aN_X(f, D_1, r) + bN_X(f, D_2, r) \\ m_X(f, aD_1 + bD_2, r) &= am_X(f, D_1, r) + bm_X(f, D_2, r) + O(1) \\ T_X(f, aD_1 + bD_2, r) &= aT_X(f, D_1, r) + bT_X(f, D_2, r) + O(1) \end{aligned}$$

*where the error terms are independent of $r$.*

- *(Effectivity) Let $D$ be an effective divisor on $X$ such that the image of $f$ is not contained in* $\operatorname{supp} D$. *Then for all $r \geq 1$ we have*

$$N_X(f, D, r) \geq 0, \quad m_X(f, D, r) \geq O(1), \quad T_X(f, D, r) \geq O(1)$$

*where the error terms are independent of $r$.*

- *(Functoriality) Let $Y$ be a smooth complex projective variety, $D$ a divisor on $Y$ and let $\gamma : X \to Y$ be a morphism. If the image of $\gamma \circ f$ is not contained in* $\operatorname{supp} D$, *then*

$$\begin{aligned} N_X(f, \gamma^* D, r) &= N_Y(\gamma \circ f, D, r) \\ m_X(f, \gamma^* D, r) &= m_Y(\gamma \circ f, D, r) + O(1) \\ T_X(f, \gamma^* D, r) &= T_Y(\gamma \circ f, D, r) + O(1) \end{aligned}$$

*where the error terms are independent of $r$.*

**Lemma 2.2** (Ample height property)**.** *Let $X$ be a smooth complex projective variety. Let $f : \mathbb{C} \to X$ be a holomorphic map. Let $D$ be an ample divisor on $X$ such that the image of $f$ is not contained in* $\operatorname{supp} D$. *If $f$ is non-constant, then $T_X(f, D, r)$ grows to infinity.*

**Lemma 2.3** (First Main Theorem)**.** *Let $X$ be a smooth complex projective variety and let $f : \mathbb{C} \to X$ be a holomorphic map. Let $D_1, D_2$ be linearly equivalent divisors on $X$ such that the image of $f$ is not contained in* $\operatorname{supp} D_1 \cup \operatorname{supp} D_2$. *Then $T_X(f, D_1, r) = T_X(f, D_2, r) + O(1)$.*

2.3. **Truncated counting functions.** When $D$ is an effective reduced divisor on $X$ and the image of $f : \mathbb{C} \to X$ is not contained in $\operatorname{supp} D$, we define

$$n_X^{(1)}(f, D, r) = \#\{z \in \mathbb{C} : |z| \leq r \text{ and } f(z) \in \operatorname{supp} D\}$$

and the *truncated counting function*

$$N_X^{(1)}(f, D, r) = \int_0^r \left( n_X^{(1)}(f, D, t) - n_X^{(1)}(f, D, 0) \right) \frac{dt}{t} + n_X^{(1)}(f, D, 0) \log r.$$

We note that $N_X^{(1)}(f, D, r) \geq 0$ for $r \geq 1$. In general, the truncated counting function does not respect additivity. It is useful to observe that for an effective reduced divisor $D$ on $X$ and a holomorphic map $f : \mathbb{C} \to X$ whose image is not contained in $\operatorname{supp} D$, for all $r \geq 1$ we have

$$0 \leq N_X^{(1)}(f, D, r) \leq N_X(f, D, r) \leq T_X(f, D, r) + O(1) \tag{2.1}$$

where the last estimate is due to the effectivity property of $m_X(f, D, r)$.

2.4. **Second Main Theorem.** Let us state the Second Main Theorem of Nevanlinna theory in the case of holomorphic maps to a curve $X$. For functions $u, v : \mathbb{R}_{\geq 0} \to \mathbb{R}$, the notation $u(r) \leq_{exc} v(r)$ means that $u(r) \leq v(r)$ holds for $r$ outside a subset of $\mathbb{R}_{\geq 0}$ of finite Lebesgue measure. Similarly for $u(r) =_{exc} v(r)$. In addition, for $v$ positive valued we use Landau's notation $u(x) = o(v(x))$ to indicate that $\lim_{x \to \infty} u(x)/v(x) = 0$.

**Theorem 2.4** (Second Main Theorem, see Theorem 23.2 [45])**.** *Let $X$ be a smooth projective curve. Let $K$ be a canonical divisor on $X$ and let $A$ be an ample divisor on $X$. Let $\alpha_1, ..., \alpha_q \in X$ be different points. Let $f : \mathbb{C} \to X$ be a holomorphic map different from the constant function $\alpha_j$ for each $j$, with image not contained in the support of $K$ and $A$. We have*

$$T_X(f, K, r) + \sum_{j=1}^{q} T_X(f, \alpha_j, r) \leq_{exc} \sum_{j=1}^{q} N_X^{(1)}(f, \alpha_j, r) + O\left(\log \max\{1, T_X(f, A, r)\}\right) + o(\log r).$$

When $f$ is constant, the result is trivial. If $f$ is non-constant, then the statement takes a simpler form, as the image of $f$ is not contained in the support of any divisor.

Due to Picard's theorem, the theorem is non-trivial only when $X$ has genus 0 or 1. We remark that a general second main theorem for algebraic varieties is still conjectural and pertains to the general setting of Vojta's conjectures, but we will only need the case of curves in this work.

2.5. **Meromorphic functions on $\mathbb{C}$.** The case of $X = \mathbb{P}^1$ will be particularly relevant for us. Here we identify the Riemann sphere $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ with $\mathbb{P}^1$ so that $\mathbb{C}$ corresponds to the affine chart $\{[1 : \alpha] : \alpha \in \mathbb{C}\} \subseteq \mathbb{P}^1$ and $\infty$ corresponds to $[0 : 1] \in \mathbb{P}^1$.

Let $\mathscr{M}$ be the field of complex meromorphic functions on $\mathbb{C}$. Under the previous identifications, a function $h \in \mathscr{M}$ can be seen as a holomorphic map $h : \mathbb{C} \to \mathbb{P}^1$. In this way, given $h \in \mathscr{M}$ and a point $\alpha \in \mathbb{C}_\infty$ we can define $N(h, \alpha, r)$, $m(h, \alpha, r)$, $T(h, \alpha, r)$, and $N^{(1)}(h, \alpha, r)$ in the obvious way using the corresponding holomorphic map $h : \mathbb{C} \to \mathbb{P}^1$ (the subscript $\mathbb{P}^1$ is omitted as in this context it is clear). Furthermore, we define

$$T(h, r) = T(h, \infty, r)$$

and we observe that for any choice of $\alpha \in \mathbb{C}$, the First Main Theorem gives

$$T(h, r) = T(h, \alpha, r) + O(1)$$

as functions of $r > 0$, provided that $h$ is not the constant function $\alpha$. Also, since $-2\infty$ is a canonical divisor on $\mathbb{P}^1$, the Second Main Theorem takes the form

$$(q - 2 + o(1))T(h, r) \leq_{exc} \sum_{j=1}^{q} N^{(1)}(h, \alpha_j, r) \tag{2.2}$$

where $\alpha_1, ..., \alpha_q \in \mathbb{P}^1$ are different points and $h \in \mathscr{M}$ a meromorphic function different from the constant function $\alpha_j$ for each $j$ (the error term can be made more precise if necessary).

## 3. Preliminary lemmas on holomorphic maps

3.1. **Comparison of counting functions.** The next lemma will allow us to compare counting functions of various sorts.

**Lemma 3.1.** *Let $n_1(r), n_2(r) : \mathbb{R}_{r\geq 0} \to \mathbb{Z}_{\geq 0}$ be functions whose points of discontinuity form a discrete set. Define*

$$N_i(r) = \int_0^r (n_i(t) - n_i(0))t^{-1}dt + n_i(0) \log r$$

*for $i = 1, 2$. If $n_1(r) \leq n_2(r)$ for all $r \geq 0$, then $N_1(r) \leq N_2(r) + O(1)$.*

*Proof.* By linearity, we may assume that $n_1(r) = 0$ for all $r$, and we need to show that $N_2(r)$ is bounded from below by a constant. It suffices to consider $r \geq 1$, in which case we have

$$N_2(r) = \int_0^r (n_2(t) - n_2(0))\frac{dt}{t} + n_2(0) \log r \geq \int_0^1 (n_2(t) - n_2(0))\frac{dt}{t}.$$

The last quantity is a constant. □

3.2. **Holomorphic maps to elliptic curves.**

**Lemma 3.2.** *Let $E$ be a complex elliptic curve and let $\alpha \in E$. Let $f : \mathbb{C} \to E$ be a non-constant holomorphic map. Then*

$$T_E(f, \alpha, r) =_{exc} (1 + o(1))N_E(f, \alpha, r) =_{exc} (1 + o(1))N_E^{(1)}(f, \alpha, r).$$

*Furthermore, for every effective non-zero divisor $D$ we have*

$$T_E(f, D, r) =_{exc} (1 + o(1))N_E(f, D, r).$$

*Proof.* A canonical divisor for $E$ is $D = 0$, and the divisor $\alpha$ is ample. By the Second Main Theorem

$$T_E(f, \alpha, r) \leq_{exc} N_E^{(1)}(f, \alpha, r) + O(\log \max\{1, T_E(f, \alpha, r)\}) + o(\log r).$$

As $f$ is transcendental, the error term is $o(T_E(f, \alpha, r))$. The first part follows from (2.1). The second part is deduced by additivity and the fact that positive degree divisors on curves are ample. □

3.3. **Meromorphic functions arising from elliptic curves.** We will be considering meromorphic functions $h \in \mathscr{M}$ that can be written in the form $h = g \circ \phi$ with $E$ an elliptic curve over $\mathbb{C}$, $\phi : \mathbb{C} \to E$ holomorphic, and $g : E \to \mathbb{P}^1$ a rational function. Meromorphic functions $h$ of this type have better value distribution properties than general meromorphic functions.

**Lemma 3.3.** *Let $E$ be a complex elliptic curve, $g : E \to \mathbb{P}^1$ a non-constant morphism of degree $d$, and $\phi : \mathbb{C} \to E$ a non-constant holomorphic map. Let $h = g \circ \phi \in \mathscr{M}$ and let $\alpha \in \mathbb{P}^1$. We have*

$$N(h, \alpha, r) =_{exc} (1 + o(1))T(h, r) \tag{3.1}$$

*and*

$$N^{(1)}(h, \alpha, r) =_{exc} \left(\frac{\#g^{-1}(\alpha)}{d} + o(1)\right) T(h, r). \tag{3.2}$$

*Proof.* By functoriality of the counting function we have

$$N(h, \alpha, r) = N(g \circ \phi, \alpha, r) = N_E(\phi, g^*\alpha, r).$$

By Lemma 3.2 and functoriality of the height

$$N_E(\phi, g^*\alpha, r) =_{exc} (1 + o(1))T_E(\phi, g^*\alpha, r) = (1 + o(1))T(h, \alpha, r).$$

which proves (3.1).

For $z_0 \in \mathbb{C}$ we have $\phi(z_0) \in g^{-1}(\alpha)$ if and only if $h(z_0) = \alpha$. Together with Lemma 3.2, this gives

$$N^{(1)}(h, \alpha, r) = \sum_{\beta \in g^{-1}(\alpha)} N_E^{(1)}(\phi, \beta, r) =_{exc} (1 + o(1)) \sum_{\beta \in g^{-1}(\alpha)} T_E(\phi, \beta, r).$$

The divisor $g^*(\infty)$ on $E$ is ample of degree $d$, hence, it is numerically equivalent to the divisor $d \cdot \beta$ for any given point $\beta \in E$. Lemma 3.2 in [22] allows us to compare the height for two effective, ample, numerically equivalent divisors, and we get

$$d \cdot T_E(\phi, \beta, r) = T_E(\phi, d \cdot \beta, r) + O(1) = (1 + o(1))T_E(\phi, g^*(\infty), r)$$

from which we deduce

$$\begin{aligned}\sum_{\beta \in g^{-1}(\alpha)} T_E(\phi, \beta, r) &= \frac{1}{d} \sum_{\beta \in g^{-1}(\alpha)} d \cdot T_E(\phi, \beta, r) = \frac{1}{d} \sum_{\beta \in g^{-1}(\alpha)} (1 + o(1))T_E(\phi, g^*(\infty), r) \\ &= \left(\frac{\#g^{-1}(\alpha)}{d} + o(1)\right) T_E(\phi, g^*(\infty), r) = \left(\frac{\#g^{-1}(\alpha)}{d} + o(1)\right) T(h, r).\end{aligned}$$

This proves (3.2). □

3.4. **GCD counting functions.** Given non-constant meromorphic functions $h_1, h_2 \in \mathscr{M}$ we define

$$n_{GCD}(h_1, h_2, r) = \sum_{|z| \leq r} \min\{\mathrm{ord}_z^+(h_1), \mathrm{ord}_z^+(h_2)\}.$$

The *GCD counting function* is

$$N_{GCD}(h_1, h_2, r) = \int_0^r (n_{GCD}(h_1, h_2, t) - n_{GCD}(h_1, h_2, 0)) \frac{dt}{t} + n_{GCD}(h_1, h_2, 0) \log r.$$

From Lemma 3.1 and the effectivity for proximity functions we deduce the *trivial GCD bound*

$$N_{GCD}(h_1, h_2, r) \leq N(h_j, 0, r) \leq T(h_j, 0, r) + O(1) = T(h_j, r) + O(1), \quad \text{for } j = 1, 2.$$

There are several works in the literature on the problem of improving this trivial bound for the GCD counting function under various assumptions, see for instance [29, 23, 21]. For our purposes, the following will suffice.

**Lemma 3.4.** *Let $\alpha_1, ..., \alpha_q \in \mathbb{C}$ be distinct and let $h_1, h_2 \in \mathscr{M}$ be different non-constant meromorphic functions. We have*

$$\sum_{j=1}^{q} N_{GCD}(h_1 - \alpha_j, h_2 - \alpha_j, r) \leq T(h_1, r) + T(h_2, r) - N_{GCD}(1/h_1, 1/h_2, r) + O(1).$$

*Proof.* For $z \in \mathbb{C}$ and each $j$ we have

$$\min\{\mathrm{ord}_z^+(h_1 - \alpha_j), \mathrm{ord}_z^+(h_2 - \alpha_j)\} \leq \mathrm{ord}_z^+(h_1 - h_2)$$

and

$$\min\{\mathrm{ord}_z^+(1/h_1), \mathrm{ord}_z^+(1/h_2)\} \leq \mathrm{ord}^+\left(\frac{1}{h_1} - \frac{1}{h_2}\right).$$

Let $H = (h_1, h_2) : \mathbb{C} \to \mathbb{P}^1 \times \mathbb{P}^1$ and let $\Delta \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ be the diagonal. From the previous order estimates and the definition of the various counting functions involved, it follows that

$$N_{GCD}(1/h_1, 1/h_2, r) + \sum_{j=1}^{q} N_{GCD}(h_1 - \alpha_j, h_2 - \alpha_j, r) \leq N_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \Delta, r).$$

Let $\pi_1, \pi_2 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ be the projections onto the two factors respectively. On $\mathbb{P}^1 \times \mathbb{P}^1$ we have the linear equivalence $\Delta \sim \pi_1^*\infty + \pi_2^*\infty$, and we get

$$\begin{aligned}
N_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \Delta, r) &\leq T_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \Delta, r) + O(1) && \text{effectivity} \\
&= T_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \pi_1^*\infty + \pi_2^*\infty, r) + O(1) && \text{First Main Theorem} \\
&= T_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \pi_1^*\infty, r) + T_{\mathbb{P}^1 \times \mathbb{P}^1}(H, \pi_2^*\infty, r) + O(1) && \text{additivity} \\
&= T(h_1, r) + T(h_2, r) + O(1) && \text{functoriality.}
\end{aligned}$$

□

## 4. Arithmetic progressions of holomorphic maps

### 4.1. **Bound for arithmetic progressions.**

In this section we prove

**Theorem 4.1.** *Let $E$ be an elliptic curve over $\mathbb{C}$ and let $g : E \to \mathbb{P}^1$ be a non-constant morphism of degree $d$. Let $M \geq 2$ be an integer and for $j = 1, 2, ..., M$ let $\phi_j : \mathbb{C} \to E$ be non-constant holomorphic maps. Define the meromorphic functions $f_j = g \circ \phi_j \in \mathscr{M}$. Suppose that there are $F_1, F_2 \in \mathscr{M}$ with $F_2$ not the zero function, and pairwise distinct complex numbers $a_1, ..., a_M \in \mathbb{C}$ such that $f_j = F_1 + a_j F_2$ for each $j$. Then $M \leq 10d^2 - 4d$.*

The result will be applied in Section 6 in a case where the functions $f_1, ..., f_j$ are distinct (not necessarily consecutive) terms of an arithmetic progression in $\mathscr{M}$.

4.2. **Pole computation.**

**Lemma 4.2.** *Let us keep the notation and assumptions of Theorem 4.1. Let $\epsilon > 0$. There are indices $i_1 \neq i_2$ in $\{1, 2, ..., M\}$ and a Borel set $U \subseteq \mathbb{R}_{\geq 0}$ of infinite Lebesgue measure such that for all $r \in U$ we have $T(f_{i_2}, r) \leq T(f_{i_1}, r)$ and*

$$\left(1 - \frac{2}{M} - \epsilon\right) \max_{1 \leq j \leq M} T(f_j, r) \leq N_{GCD}(1/f_{i_1}, 1/f_{i_2}, r) \leq T(f_{i_1}, r) + O(1).$$

*Proof.* Given $z_0 \in \mathbb{C}$, we note that if some of the $f_j = F_1 + a_j F_2$ has a pole at $z_0$, then $F_1$ or $F_2$ has a pole at $z_0$. As the complex numbers $a_j$ are different, for all $1 \leq j \leq M$ with at most one exception we get that

$$\mathrm{ord}_{z_0}(f_j) = \min\{\mathrm{ord}_{z_0} F_1, \mathrm{ord}_{z_0} F_2\} = \min_{1 \leq i \leq M} \mathrm{ord}_{z_0} f_i < 0.$$

Therefore,

$$\begin{aligned} \sum_{i<j} n_{GCD}(1/f_i, 1/f_j, r) &= \sum_{|z| \leq r} \sum_{i<j} \min\{\mathrm{ord}_z^+(1/f_i), \mathrm{ord}_z^+(1/f_j)\} \\ &\geq \sum_{|z| \leq r} \binom{M-1}{2} \max_{1 \leq i \leq M} \mathrm{ord}_z^+(1/f_i). \end{aligned}$$

It follows that for each $1 \leq i_0 \leq M$ we have

$$\sum_{i<j} n_{GCD}(1/f_i, 1/f_j, r) \geq \binom{M-1}{2} n(f_{i_0}, \infty, r).$$

By Lemma 3.1 and Lemma 3.3, for any given $\epsilon > 0$ we get

$$\sum_{i<j} N_{GCD}(1/f_i, 1/f_j, r) \geq \binom{M-1}{2} N(f_{i_0}, \infty, r) \geq_{exc} \binom{M-1}{2} (1-\epsilon) T(f_{i_0}, r).$$

Since $i_0$ is arbitrary, we get

$$\sum_{i<j} N_{GCD}(1/f_i, 1/f_j, r) \geq_{exc} \binom{M-1}{2} (1-\epsilon) \max_{1 \leq i \leq M} T(f_i, r).$$

The first sum has $\binom{M}{2}$ terms. A contradiction argument shows that there are indices $i_1 \neq i_2$ in $\{1, 2, ..., M\}$ and a Borel set $V \subseteq \mathbb{R}_{\geq 0}$ of infinite Lebesgue measure such that for all $r \in V$ we have

$$N_{GCD}(1/f_{i_1}, 1/f_{i_2}, r) \geq \frac{\binom{M-1}{2}}{\binom{M}{2}} (1-\epsilon) \max_{1 \leq i \leq M} T(f_i, r) = \left(1 - \frac{2}{M}\right)(1-\epsilon) \max_{1 \leq i \leq M} T(f_i, r).$$

After switching $i_1$, $i_2$ if necessary and replacing $V$ by an infinite measure subset $U$, for all $r \in U$ we also have $T(f_{i_2}, r) \leq T(f_{i_1}, r)$. Finally, the trivial GCD bound gives

$$N_{GCD}(1/f_{i_1}, 1/f_{i_2}, r) \leq N(1/f_{i_1}, 0, r) = N(f_{i_1}, \infty, r) \leq T(f_{i_1}, r) + O(1).$$

We get the result adjusting $\epsilon$. □

4.3. **Two numerical lemmas.**

**Lemma 4.3.** *For $x \in \mathbb{R}$, let us write $x^+ = \max\{0, x\}$. For every $A, B \in \mathbb{R}$ we have*

$$(A - B)^+ \geq A^+ - \min\{A^+, B^+\}.$$

*Proof.* This is readily checked by considering the following cases: $A \leq B$; $0 \geq A > B$; $A > 0 \geq B$; $A > B > 0$. The details are left to the reader. □

**Lemma 4.4.** *Let $E$ be a complex elliptic curve and let $g : E \to \mathbb{P}^1$ be a non-constant morphism of degree $d$. Let $\alpha_1, ..., \alpha_k \in \mathbb{C}$ be the set of affine branch points (after identifying $\mathbb{P}^1 = \mathbb{C}_\infty$). We have*

$$1 \leq k \leq 2d \qquad \text{and} \qquad \sum_{j=1}^{k} \frac{\#g^{-1}(\alpha_j)}{d} \leq k - 1 - \frac{1}{d}.$$

*Proof.* The total number of branch points of a ramified morphism to $\mathbb{P}^1$ is always at least 2, so $k \geq 1$. The Riemann-Hurwitz formula gives $(2 \cdot 1 - 2) = d \cdot (2 \cdot 0 - 2) + \sum_{\alpha \in \mathbb{P}^1} \left(d - \#g^{-1}(\alpha)\right)$, thus

$$2d = \sum_{\alpha \in \mathbb{P}^1} \left(d - \#g^{-1}(\alpha)\right) \geq \sum_{\substack{\alpha \in \mathbb{P}^1 \\ \alpha \text{ branch}}} 1 \geq k.$$

This proves the bounds for $k$. Finally, there is at most one branch points other than the $\alpha_j$, so the Riemann-Hurwitz formula gives

$$2d = \sum_{\alpha \in \mathbb{P}^1} \left(d - \#g^{-1}(\alpha)\right) \leq (d-1) + \sum_{j=1}^{k} (d - \#g^{-1}(\alpha_j)) = (k+1)d - 1 - \sum_{j=1}^{k} \#g^{-1}(\alpha_j)$$

and the result follows. □

4.4. **Proof of Theorem 4.1.** Let us keep the notation and assumptions of Theorem 4.1. Furthermore, we may assume $M \geq 4$, so that the expressions $M-1$, $M-2$, and $M-3$ are positive (this is relevant as we will eventually divide by them in some computations).

Let $\epsilon > 0$. Up to relabeling the functions $f_j$ if necessary, Lemma 4.2 shows that there is a Borel set $U \subseteq \mathbb{R}_{\geq 0}$ of infinite Lebesgue measure such that for all $r \in U$ we have

$$T(f_2, r) \leq T(f_1, r) \tag{4.1}$$

and

$$\left(1 - \frac{2}{M} - \epsilon\right) \max_{1 \leq j \leq M} T(f_j, r) \leq N_{GCD}(1/f_1, 1/f_2, r) \leq T(f_1, r) + O(1). \tag{4.2}$$

For each $1 \leq j \leq M$ define the complex numbers

$$\lambda_j = \frac{a_2 - a_j}{a_2 - a_1}, \quad \mu_j = \frac{a_1 - a_j}{a_1 - a_2} \quad \gamma_j = \frac{a_j - a_2}{a_j - a_1}$$

and observe that

- All the numbers $\lambda_j, \mu_j, \gamma_j$ are non-zero.
- The numbers $\lambda_j$ are pairwise different. Similarly for the numbers $\mu_j$ and the numbers $\gamma_j$.
- $\lambda_j + \mu_j = 1$.
- $\lambda_j a_1 + \mu_j a_2 = a_j$.
- $\gamma_j = -\lambda_j / \mu_j$.

Let $\alpha \in \mathbb{C}$. We note that

$$\lambda_j(f_1 - \alpha) + \mu_j(f_2 - \alpha) = (\lambda_j + \mu_j)F_1 + (\lambda_j a_1 + \mu_j a_2)F_2 - (\lambda_j + \mu_j)\alpha = f_j - \alpha.$$

hence

$$\frac{f_2 - \alpha}{f_1 - \alpha} - \gamma_j = \mu_j^{-1} \cdot \frac{f_j - \alpha}{f_1 - \alpha}. \tag{4.3}$$

From this equation we observe that the meromorphic function $(f_2 - \alpha)/(f_1 - \alpha) \in \mathscr{M}$ is not the constant function $\gamma_j$ for any $j$, since $f_j$ is not the constant function $\alpha$ ($f_j$ is non-constant).

Also from (4.3) we see that given any complex number $\alpha \in \mathbb{C}$, for all $r \geq 0$ we have

$$N^{(1)}\left(\frac{f_2 - \alpha}{f_1 - \alpha}, \gamma_j, r\right) = N^{(1)}\left(\frac{f_j - \alpha}{f_1 - \alpha}, 0, r\right). \tag{4.4}$$

Given $\alpha \in \mathbb{C}$, let us give an upper bound for the average (for $2 \leq j \leq M$) of the right hand side of the previous expression. Let $B[r] = \{z \in \mathbb{C} : |z| \leq r\}$. First we observe

$$\sum_{j=2}^{M} n^{(1)}\left(\frac{f_j-\alpha}{f_1-\alpha}, 0, r\right) \leq \sum_{j=2}^{M} n^{(1)}\left(f_j-\alpha, 0, r\right) + \sum_{j=2}^{M} \#\left\{z \in B[r] : \mathrm{ord}_z(f_1-\alpha) < \mathrm{ord}_z(f_j-\alpha) \leq 0\right\}.$$

Since $f_j = F_1 + a_j F_2$, we see that if $f_1$ has a pole at some $z_0$, then all the $f_j$ have a pole of the same order at $z_0$ with at most one possible exception for $j$. Thus, given $z_0 \in \mathbb{C}$, the condition $\mathrm{ord}_{z_0}(f_1-\alpha) < \mathrm{ord}_{z_0}(f_j-\alpha) \leq 0$ holds for at most one $j$, in which case $f_1$ has a pole. We get

$$\sum_{j=2}^{M} \#\left\{z \in B[r] : \mathrm{ord}_z(f_1-\alpha) < \mathrm{ord}_z(f_j-\alpha) \leq 0\right\} \leq n^{(1)}(f_1, \infty, r),$$

from which we deduce

$$\sum_{j=2}^{M} n^{(1)}\left(\frac{f_j-\alpha}{f_1-\alpha}, 0, r\right) \leq n^{(1)}(f_1, \infty, r) + \sum_{j=2}^{M} n^{(1)}\left(f_j-\alpha, 0, r\right).$$

Therefore, Lemma 3.1 gives

$$\sum_{j=2}^{M} N^{(1)}\left(\frac{f_j-\alpha}{f_1-\alpha}, 0, r\right) \leq N^{(1)}(f_1, \infty, r) + \sum_{j=2}^{M} N^{(1)}\left(f_j-\alpha, 0, r\right) + O(1). \tag{4.5}$$

Let us write

$$T(r) = \max_{1 \leq j \leq M} T(f_j, r).$$

Using (4.5), (4.4), the fact that $N^{(1)}\left(f_j-\alpha, 0, r\right) = N^{(1)}\left(f_j, \alpha, r\right)$, and Lemma 3.3, we deduce that for any given $\alpha \in \mathbb{C}$

$$\begin{aligned} \sum_{j=2}^{M} N^{(1)}\left(\frac{f_2-\alpha}{f_1-\alpha}, \gamma_j, r\right) &\leq N^{(1)}(f_1, \infty, r) + \sum_{j=2}^{M} N^{(1)}\left(f_j, \alpha, r\right) + O(1) \\ &=_{exc} N^{(1)}(f_1, \infty, r) + \left(\frac{\#g^{-1}(\alpha)}{d} + o(1)\right) \sum_{j=2}^{M} T(f_j, r) \\ &\leq T(f_1, r) + \left(\frac{\#g^{-1}(\alpha)}{d} + o(1)\right)(M-1)T(r). \end{aligned} \tag{4.6}$$

As explained after (4.3), the meromorphic function $(f_2-\alpha)/(f_1-\alpha) \in \mathscr{M}$ is not equal to the constant function $\gamma_j$ for any $j$. The Second Main Theorem (2.2) with the targets $\gamma_2, ..., \gamma_M$ (here, $q = M-1$) gives that for any fixed $\alpha \in \mathbb{C}$

$$(M-3+o(1))T\left(\frac{f_2-\alpha}{f_1-\alpha}, r\right) \leq_{exc} \sum_{j=2}^{M} N^{(1)}\left(\frac{f_2-\alpha}{f_1-\alpha}, \gamma_j, r\right). \tag{4.7}$$

Let us give a lower bound for the expression on the left hand side of (4.7). By Lemma 4.3 we have

$$\begin{aligned} n\left(\frac{f_2-\alpha}{f_1-\alpha},\infty,r\right) &= \sum_{|z|\le r}\max\{0,\mathrm{ord}_z(f_1-\alpha)-\mathrm{ord}_z(f_2-\alpha)\} \\ &\ge \sum_{|z|\le r}\mathrm{ord}_z^+(f_1-\alpha)-\sum_{|z|\le r}\min\{\mathrm{ord}_z^+(f_1-\alpha),\mathrm{ord}_z^+(f_2-\alpha)\} \\ &= n(f_1,\alpha,r)-n_{GCD}(f_1-\alpha,f_2-\alpha,r). \end{aligned}$$

Lemma 3.1 gives the desired lower bound for the left hand side of (4.7):

$$N(f_1,\alpha,r)-N_{GCD}(f_1-\alpha,f_2-\alpha,r)\le N\left(\frac{f_2-\alpha}{f_1-\alpha},\infty,r\right)+O(1)\le T\left(\frac{f_2-\alpha}{f_1-\alpha},r\right)+O(1). \tag{4.8}$$

We conclude that for any given $\alpha\in\mathbb{C}$ the following holds:

$$\begin{aligned} &(M-3+o(1))\left((1+o(1))T(f_1,r)-N_{GCD}(f_1-\alpha,f_2-\alpha,r)\right) \\ &\quad =_{exc}(M-3+o(1))\left(N(f_1,\alpha,r)-N_{GCD}(f_1-\alpha,f_2-\alpha,r)\right) && \text{by Lemma 3.3} \\ &\quad \le_{exc}\sum_{j=2}^{M}N^{(1)}\left(\frac{f_2-\alpha}{f_1-\alpha},\gamma_j,r\right) && \text{by (4.8) and (4.7)} \\ &\quad \le_{exc}T(f_1,r)+\left(\frac{\#g^{-1}(\alpha)}{d}+o(1)\right)(M-1)T(r) && \text{by (4.6).} \end{aligned}$$

Rearranging and collecting the error terms, we conclude

$$(M-4)T(f_1,r)\le_{exc}\left(\frac{\#g^{-1}(\alpha)}{d}+o(1)\right)(M-1)T(r)+(M-3)N_{GCD}(f_1-\alpha,f_2-\alpha,r). \tag{4.9}$$

Let $k$ be the number of affine branch points in $\mathbb{C}_\infty=\mathbb{P}^1$ of $g:\mathbb{E}\to\mathbb{P}^1$ and let $\alpha_1,...,\alpha_k\in\mathbb{C}$ be these branch points. Lemma 3.4 gives

$$\sum_{i=1}^{k}N_{GCD}(f_1-\alpha_i,f_2-\alpha_i,r)\le T(f_1,r)+T(f_2,r)-N_{GCD}(1/f_1,1/f_2,r)+O(1).$$

Using (4.1) and (4.2) we get for all $r$ in the infinite measure set $U$

$$\sum_{i=1}^{k}N_{GCD}(f_1-\alpha_i,f_2-\alpha_i,r)\le 2T(f_1,r)-\left(1-\frac{2}{M}-\epsilon\right)T(r)+O(1).$$

Removing a finite measure subset from $U$ we get an infinite measure set $U'\subseteq U\subseteq\mathbb{R}_{\ge 0}$ such that for all $r\in U'$ the previous estimate holds as well as (4.9) for $\alpha=\alpha_j$ with $1\le j\le k$. This gives that for all $r\in U'$ we have

$$\begin{aligned} k(M-4)T(f_1,r)\le &\left(\sum_{j=1}^{k}\frac{\#g^{-1}(\alpha_j)}{d}+o(1)\right)(M-1)T(r) \\ &+2(M-3)T(f_1,r)-(M-3)\left(1-\frac{2}{M}-\epsilon\right)T(r). \end{aligned}$$

Let us write

$$S=\sum_{j=1}^{k}\frac{\#g^{-1}(\alpha_j)}{d}.$$

Rearranging we get

$$\left(\frac{M-4}{M-3}\cdot k-2\right)T(f_1,r)\leq\left(\frac{M-1}{M-3}\cdot S+o(1)-1+\frac{2}{M}+\epsilon\right)T(r).$$

Using (4.2) (which is valid for $r\in U'$) we get

$$\left(\frac{M-4}{M-3}\cdot k-2\right)\left(1-\frac{2}{M}-\epsilon\right)T(r)\leq\left(\frac{M-1}{M-3}\cdot S+o(1)-1+\frac{2}{M}+\epsilon\right)T(r).$$

Since $U'\subseteq\mathbb{R}_{\geq 0}$ has infinite measure, we can let $r\to+\infty$ over a sequence in $U'$. As the functions $f_j$ are non-constant, we get $T(r)\to+\infty$ over this sequence, and we deduce

$$\left(\frac{M-4}{M-3}\cdot k-2\right)\left(1-\frac{2}{M}-\epsilon\right)\leq\frac{M-1}{M-3}\cdot S-1+\frac{2}{M}+\epsilon.$$

Since $\epsilon>0$ is arbitrary and $S\leq k-1-1/d$ (cf. Lemma 4.4) we obtain

$$\left(\frac{M-4}{M-3}\cdot k-2\right)\left(1-\frac{2}{M}\right)\leq\frac{M-1}{M-3}\left(k-1-\frac{1}{d}\right)-1+\frac{2}{M}.$$

If $M$ were very large, this would approximately give $k-2\leq k-1-1/d-1=k-2-1/d$ which is not possible. So, it is clear that this expression constrains the size of $M$. Let us work out the precise details in order to get the desired bound: Rearranging we obtain

$$\frac{(M-1)M}{d}+2(2M-3)-(5M-8)\cdot k\leq 0. \tag{4.10}$$

The quadratic function

$$u(t)=t(t-1)/d+2(2t-3)-(5t-8)k$$

is increasing for $t\geq t_0=(1+(5k-4)d)/2$ and satisfies $u((5k-4)d)=3k-2\geq 1$. Since $(5k-4)d\geq t_0$ we deduce that $u(t)\geq 1$ for $t\geq(5k-4)d$. Therefore, (4.10) with Lemma 4.4 shows that

$$M\leq(5k-4)d\leq 10d^2-4d.$$

This concludes the proof of Theorem 4.1. □

## 5. Some geometric constructions

5.1. **Notation and first constructions.** Let $k$ be an algebraically closed field of characteristic 0, let $E$ be an elliptic curve over $k$ and let $n$ be a positive integer. Let $g\in k(E)$ be a non-constant rational function of degree $d$. We identify $\mathbb{A}^1_k$ with the affine chart $\{[x_0:x_1]\in\mathbb{P}^1_k : x_0\neq 0\}$ of $\mathbb{P}^1_k$. In particular, $g$ can be identified with a morphism $g:E\to\mathbb{P}^1_k$ of degree $d$ defined over $k$. We consider the abelian variety $A=E^n$ of dimension $n$. Let $G_n:A\to(\mathbb{P}^1)^n$ be the morphism obtained from $n$ copies of $g$.

**Lemma 5.1.** *The morphism $G_n$ is finite of degree $d^n$ and flat.*

*Proof.* The map $g:E\to\mathbb{P}^1_k$ is surjective and finite of degree $d$. Hence, $G_n:E^n\to(\mathbb{P}^1_k)^n$ is surjective and finite of degree $d^n$. On the other hand, the map $g$ is flat by [16] III Prop. 9.7. Hence, repeated applications of [16] III Prop. 9.2 give that $G_n$ is flat. □

5.2. **The surfaces $U_n$ and $H_n$.** Let us assume that $n \geq 3$. Let $u_1, ..., u_n$ be the coordinates on $\mathbb{A}^n_k$ and let us define the affine variety

$$U_n : \begin{cases} u_3 - 2u_2 + u_1 = 0 \\ \vdots \\ u_n - 2u_{n-1} + u_{n-2} = 0 \end{cases} \subseteq \mathbb{A}^n_k. \tag{5.1}$$

Under the previously chosen inclusion $\mathbb{A}^1_k \subseteq \mathbb{P}^1_k$, we have $\mathbb{A}^n_k \subseteq (\mathbb{P}^1_k)^n$. Let $H_n$ be the Zariski closure of $U_n$ in $(\mathbb{P}^1_k)^n$. Let $p_j : (\mathbb{P}^1_k)^n \to \mathbb{P}^1_k$ be the $j$-th coordinate projection.

**Lemma 5.2.** *We have that $U_n$ is a linear surface in $\mathbb{A}^n_k$ and $H_n$ is an irreducible projective surface. Furthermore, for every $j$ we have that $p_j$ restricts to a surjective map $H_n \to \mathbb{P}^1_k$.*

*Proof.* $U_n$ is a linear surface because the $n-2$ linear equations defining it are linearly independent. The other claims follow. □

**Lemma 5.3.** *Let $1 \leq i < j \leq n$. The projection $p_{ij} : (\mathbb{P}^1_k)^n \to (\mathbb{P}^1_k)^2$ onto the coordinates $i$ and $j$ restricts to a map $H_n \to (\mathbb{P}^1_k)^2$ which is finite of degree 1 above $\mathbb{A}^2_k$.*

*Proof.* From the equations of $U_n$, we note that if a point $(\alpha_1, ..., \alpha_n) \in H_n$ has some coordinate $\alpha_j = \infty \in \mathbb{P}^1_k$, then all other coordinates with at most one exception are also equal to $\infty$. Thus, the preimage of $\mathbb{A}^2_k$ under $p_{ij}|_{H_n} : H_n \to (\mathbb{P}^1_k)^2$ is precisely $U_n$. Finally, since $k$ has characteristic 0, fixing $u_i$ and $u_j$ in $k$ (with $i \neq j$) determines a unique point in $U_n$, namely

$$u_\ell = \frac{\ell - j}{i - j} \cdot u_i + \frac{\ell - i}{j - i} \cdot u_j, \quad 1 \leq \ell \leq n.$$

□

5.3. **The surfaces $V_n$ and $X_n$.** Let us define

$$X_n = G_n^{-1}(H_n) \subseteq A \quad \text{and} \quad V_n = G_n^{-1}(U_n) \subseteq X_n.$$

**Lemma 5.4.** *We have that $X_n$ is a projective surface and $V_n$ is a dense open subset in $X_n$. Moreover, the morphism $G_n : E^n \to (\mathbb{P}^1_k)^n$ restricts to a morphism $G'_n : X_n \to H_n$ which is surjective, finite of degree $d^n$, and flat.*

*Proof.* Since $G_n$ is flat (cf. Lemma 5.1), it is open by [16] III Exer. 9.1. It follows that $G_n^{-1}(cl(S)) = cl(G_n^{-1}(S))$ for every set $S \subseteq (\mathbb{P}^1_k)^n$, where $cl(-)$ denotes Zariski closure. As $cl(U_n) = H_n$, we get that $X_n$ is the Zariski closure of $V_n$.

The branch divisor of $G_n$ is $\sum_{j=1}^n p_j^* B_g$ where $B_g \subseteq \mathbb{P}^1_k$ is the branch divisor of $g$. From Lemma 5.2 we deduce that $H_n$ is not contained in the branch locus of $G_n$. It follows that $G_n$ restricts to a finite surjective map $G'_n : X_n \to H_n$ of degree $d^n$. We note that $V_n = G_n^{-1}(U_n) = (G')_n^{-1}(U_n)$ and $U_n$ is open in $H_n$, thus $V_n$ is open.

Finally, note that $G'_n$ is the base change of $G_n$ by the closed immersion $H_n \to (\mathbb{P}^1_k)^n$, hence $G'_n$ is flat (cf. [16] III Prop. 9.2). As $G_n$ has pure relative dimension 0, we obtain from Lemma 5.2 and [16] III Coro. 9.6 that $\dim X_n = \dim H_n = 2$. □

5.4. **A line sheaf on $E^n$.** Let $\pi_j : E^n \to E$ be the $j$-th coordinate projection. Let $e_E$ be the neutral point of $E$ and consider the following line sheaf on $E^n$:

$$\mathscr{L}_n = \mathscr{O}\left(\sum_{j=1}^n \pi_j^* e_E\right).$$

**Lemma 5.5.** *The line sheaf $\mathscr{L}_n$ on the abelian variety $E^n$ is ample and symmetric.*

*Proof.* For $m \in \mathbb{Z}$ and $B$ an abelian variety, we write $[m]_B$ for the endomorphism of multiplication by $m$ on $B$. Let $A = E^n$ as before. We have $[-1]_E^* e_E = e_E$, hence

$$\begin{aligned}[-1]_A^* \sum_{j=1}^n \pi_j^* e_E &= \sum_{j=1}^n [-1]_A^* \pi_j^* e_E = \sum_{j=1}^n (\pi_j [-1]_A)^* e_E \\ &= \sum_{j=1}^n ([-1]_E \pi_j)^* e_E = \sum_{j=1}^n \pi_j^* [-1]_E^* e_E = \sum_{j=1}^n \pi_j^* e_E.\end{aligned}$$

It follows that $\mathscr{L}_n$ is symmetric on $E^n$. Since $\mathscr{L}_n \simeq \bigotimes_{j=1}^n \pi_j^* \mathscr{O}(e_E)$ and $\mathscr{O}(e_E)$ is ample on $E$ (it has degree 1), we get that $\mathscr{L}_n$ is ample on $E^n$. □

5.5. **Degree estimates.** Given a line sheaf $\mathscr{F}$ on a smooth projective variety $Y$ and a closed set $Z \subseteq Y$, we define $\deg_{\mathscr{F}} Z$ as $\deg([\mathscr{F}]^{\dim Z} \cdot [Z])$ if $Z$ is irreducible, and we extend this definition linearly for general $Z$. Here, the intersection product occurs in the Chow ring $Ch(Y) = \oplus_j Ch^j(Y)$ of $Y$ (graded by codimension) and $\deg : Ch_0(Y) \to \mathbb{Z}$ is the usual degree map on 0-cycles —we use the standard convention that $Ch^j$ denotes codimension $j$ cycles, while $Ch_j$ denotes cycles of dimension $j$. For instance, see Appendix A in [16] for a survey of intersection theory.

**Lemma 5.6.** *We have* $\deg_{\mathscr{L}_n} X_n \leq (n^2 - n) d^{2n-2}$.

*Proof.* For the following computations, let us recall that if $f : Y \to Z$ is a morphism of smooth projective varieties over $k$, then the pull-back $f^* : Ch(Z) \to Ch(Y)$ is a graded ring morphism, while the push-forward $f_* : Ch(Y) \to Ch(Z)$ respects addition and shifts the grading.

As $X_n$ is a surface, we have $\deg_{\mathscr{L}_n} X_n = \deg([\mathscr{L}_n]^2 \cdot [X_n])$. We expand the intersection product

$$\begin{aligned}[\mathscr{L}_n]^2 \cdot [X_n] &= \sum_{i=1}^n \sum_{j=1}^n [\pi_i^* e_E] \cdot [\pi_j^* e_E] \cdot [X_n] \\ &= \sum_{i=1}^n [\pi_i^* e_E]^2 \cdot [X_n] + 2 \sum_{1 \leq i < j \leq n} [\pi_i^* e_E] \cdot [\pi_j^* e_E] \cdot [X_n]\end{aligned}$$

Moving $e_E$ on $E$, we see that $[\pi_i^* e_E]^2 = 0 \in Ch^2(A)$. On the other hand, $[X_n] = G_n^*[H_n] \in Ch_2(A)$ by Lemma 5.4. Hence, the projection formula gives the following identities in $Ch_0((\mathbb{P}^1_k)^n)$

$$\begin{aligned}(G_n)_* \left( [\mathscr{L}_n]^2 \cdot [X_n] \right) &= 2 \sum_{1 \leq i < j \leq n} (G_n)_* \left( [\pi_i^* e_E] \cdot [\pi_j^* e_E] \cdot G_n^* [H_n] \right) \\ &= 2 \sum_{1 \leq i < j \leq n} (G_n)_* ([\pi_i^* e_E] \cdot [\pi_j^* e_E]) \cdot [H_n] \\ &= 2 \sum_{1 \leq i < j \leq n} (G_n)_* ([\pi_{ij}^* ((e_E, e_E))]) \cdot [H_n]\end{aligned}$$

where $\pi_{ij} : E^n \to E^2$ is the projection onto the $i$ and $j$ coordinates.

Note that $\pi_{ij}^*((e_E, e_E))$ is obtained from $E^n$ by replacing the copies of $E$ in the coordinates $i$ and $j$ by $\{e_E\}$. Let $p_{ij} : (\mathbb{P}^1_k)^n \to (\mathbb{P}^1_k)^2$ be the projection onto the coordinates $i$ and $j$. We deduce that the map $\pi_{ij}^*((e_E, e_E)) \to p_{ij}^*((g(e_E), g(e_E)))$ induced by $G_n$ is (up to the obvious isomorphisms) the same as $G_{n-2} : E^{n-2} \to (\mathbb{P}^1_k)^{n-2}$, which has degree $d^{n-2}$ by Lemma 5.1. This gives

$$(G_n)_* ([\pi_{ij}^* ((e_E, e_E))]) = d^{n-2} [p_{ij}^* ((g(e_E), g(e_E))] \in Ch^2((\mathbb{P}^1_k)^n).$$

Choose a $k$-rational point $x \in \mathbb{A}^1_k \subseteq \mathbb{P}^1_k$. For $i < j$, Lemma 5.3 gives the following on $(\mathbb{P}^1_k)^n$

$$\deg \left( [p_{ij}^* ((g(e_E), g(e_E))] \cdot [H_n] \right) = \deg \left( [p_{ij}^* ((x, x))] \cdot [H_n] \right) = 1.$$

From here we deduce

$$\deg\left((G_n)_*\left([\mathscr{L}_n]^2\cdot[X_n]\right)\right)=(n^2-n)d^{n-2}.$$

As $G_n : A\to(\mathbb{P}^1_k)^n$ is finite of degree $d^n$ (cf. Lemma 5.1), we get the desired bound. □

## 6. Arithmetic progressions for finite rank groups

6.1. **Main arithmetic result.** Let $L$ be a field. An *arithmetic progression* in $L$ is a sequence $u_1,...,u_n$ of elements of $L$ such that for some $a,b\in L$ we have $u_j=a+jb$ for each $j=1,...,n$. We say that the arithmetic progression $u_1,...,u_n$ is *trivial* if al the terms $u_j$ are equal, i.e. $b=0$. Otherwise, the arithmetic progression is said to be *non-trivial*.

The rank of an abelian group $\Gamma$ is defined as

$$\operatorname{rank}\Gamma=\dim_{\mathbb{Q}}(\Gamma\otimes_{\mathbb{Z}}\mathbb{Q}).$$

In particular, if $\Gamma$ is a torsion abelian group, then $\operatorname{rank}\Gamma=0$.

**Theorem 6.1.** *Let $j_0\in\mathbb{Q}^{alg}$ and let $d\geq 2$ be an integer. There is an effectively computable constant $\kappa(j_0,d)$ depending only on $j_0$ and $d$ such that the following holds:*

*Let $E$ be an elliptic curve over $\mathbb{Q}^{alg}$ with $j$-invariant equal to $j_0$. Let $g\in k(E)$ be a non-constant rational function on $E$ of degree $d$ defined over $\mathbb{Q}^{alg}$. Let $\Gamma\subseteq E(\mathbb{Q}^{alg})$ be a subgroup of finite rank. Suppose that for a positive integer $N$ there is a sequence $P_1,...,P_N$ of points in $\Gamma$ such that no $P_j$ is a pole of $g$, and the sequence $g(P_1),...,g(P_N)\in\mathbb{Q}^{alg}$ is a non-trivial arithmetic progression. Then*

$$1+\operatorname{rank}\Gamma>\kappa(j_0,d)\cdot\log N.$$

We remark that if $L$ is a field of positive characteristic $p>0$, then a non-trivial arithmetic progression in $L$ can have repeated terms. However, if $L$ has characteristic 0, then an arithmetic progression is non-trivial (i.e. not all terms are the same) if and only if all its terms are different. For our purposes, we will work in characteristic zero.

We will need the following characterization of arithmetic progressions.

**Lemma 6.2.** *Let $n\geq 3$ be an integer, let $L$ be a field, and let $u_1,...,u_n\in L$. The sequence $u_1,...,u_n$ is an arithmetic progression if and only if $u_j-2u_{j-1}+u_{j-2}=0$ for each $3\leq j\leq n$.*

*Proof.* Arithmetic progressions satisfy the required equations since one directly checks

$$(a+jb)-2(a+(j-1)b)+(a+(j-2)b)=0.$$

Conversely, if the sequence $u_1,...,u_n$ satisfies $u_j-2u_{j-1}+u_{j-2}=0$ for each $3\leq j\leq n$, then inductively one proves that $u_j=a+jb$ with $a=2u_1-u_2$ and $b=u_2-u_1$. □

6.2. **Lang's conjecture after Vojta, Faltings, and Rémond.** In [10, 11] Faltings proved Lang's conjecture on rational points in sub-varieties of abelian varieties. Namely, if $L$ is a number field, $A$ is an abelian variety over $L$ and $X\subseteq A$ is a sub-variety defined over $L$, then all but finitely many $L$-rational points of $X$ are contained in the Kawamata locus of $X$; i.e., the union of translates of positive dimensional abelian sub-varieties of $A$ contained in $X$. (We recall that the Kawamata locus is Zariski closed by a theorem of Kawamata [18].) This proof extended ideas of Vojta's proof [44] of Faltings' theorem for curves [9]. See also Bombieri's simplification [3] of Vojta's argument.

Faltings' theorem on sub-varieties of abelian varieties has been extended in several directions. We need a quantitative generalization due to Rémond [34, 35], which also extends Raynaud's theorem on torsion points [33] (i.e. the Manin-Mumford conjecture).

**Theorem 6.3** (Rémond)**.** *Let $A$ be an abelian variety of dimension $n$ defined over $\mathbb{Q}^{alg}$, and let $\mathscr{L}$ be a symmetric ample invertible sheaf on $A$. There is an effectively computable number $c(A,\mathscr{L})>0$ such that the following holds:*

*Let $X$ be a closed subvariety of $A$ of dimension $m$, and let $\Lambda$ be a subgroup of $A(\mathbb{Q}^{alg})$ such that its rank $r = \dim_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$ is finite. There is a non-negative integer*

$$R \leq (c(A, \mathscr{L}) \deg_{\mathscr{L}} X)^{(r+1)n^{5(m+1)^2}}$$

*and there exist points $x_1, \ldots, x_R$ in $X(\mathbb{Q}^{alg}) \cap \Lambda$ and abelian subvarieties $T_1, \ldots, T_R$ of $A$ satisfying that $x_i + T_i \subseteq X$ for each $1 \leq i \leq R$, and*

$$X(\mathbb{Q}^{alg}) \cap \Lambda = \bigcup_{i=1}^{R} (x_i + T_i)(\mathbb{Q}^{alg}) \cap \Lambda.$$

This formulation is the same as Théorème 1.2 in [34], with the additional remark that the number $c(A, \mathscr{L})$ can be effectively computed. In fact, this point is explained in *loc. cit.* after the statement of Théorème 1.2, and the precise details are given in Théorème 2.1 and the paragraph after it.

Moreover, a simple closed formula for $c(A, \mathscr{L})$ is given in Théorème 1.3 of [35] using the notion of *theta height* of $A$, under the assumption that $\mathscr{L}$ induces a principal polarization. See Section 6.5 for details on how to use these explicit effective estimates in our context.

6.3. **Proof of Theorem 6.1.** Let us keep the notation and assumptions of Theorem 6.1. Let us consider constructions from Section 5 with $k = \mathbb{Q}^{alg}$, $n = 10d^2 - 4d + 2$, and the choice of $E$ and $g$ given in Theorem 6.1. Especially, we obtain the morphism $G_n : E^n \to (\mathbb{P}^1_k)^n$, the projective surfaces $H_n \subseteq (\mathbb{P}^1_k)^n$ and $X_n \subseteq E^n$, the open sets $U_n \subseteq H_n$ and $V_n \subseteq X_n$, and the line sheaf $\mathscr{L}_n$ on $E^n$.

Let $\Delta_n = \{u_1 = u_2 = ... = u_n\} \subseteq \mathbb{A}^n_k$ be the diagonal line. We observe that $\Delta_n$ is a Zariski closed set in $U_n$. Let us define

$$U_n^0 = U_n - \Delta_n \quad \text{and} \quad V_n^0 = G_n^{-1}(U_n^0) \subseteq V_n.$$

**Lemma 6.4.** *Let $L/k$ be a field extension. Let $\alpha_1, ..., \alpha_n \in L$. We have that the sequence is an arithmetic progression in $L$ if and only if $(\alpha_1, ..., \alpha_n) \in U_n(L)$. In this case, the arithmetic progression is non-trivial if and only if $(\alpha_1, ..., \alpha_n) \in U_n^0(L)$.*

*Furthermore, let $P_1, ..., P_n$ be a sequence of points in $E(L)$. We have that $g(P_1), ..., g(P_n)$ is an arithmetic progression in $L = \mathbb{A}^1_k(L)$ if and only if $(P_1, ..., P_n) \in V_n(L)$. In this case, the arithmetic progression is non-trivial if and only if $(P_1, ..., P_n) \in V_n^0(L)$.*

*Proof.* The sequence $\alpha_1, ..., \alpha_n$ is an arithmetic progression if and only if it has second differences equal to 0 (cf. Lemma 6.2). This is equivalent to the condition that $(\alpha_1, ..., \alpha_n) \in U_n(L)$. The sequence is trivial if and only if all terms are equal, which is equivalent to $(\alpha_1, ..., \alpha_n) \in \Delta_n(L)$.

The second part follows from the first part, using $V_n = G_n^{-1}(U_n)$ and $V_n^0 = G_n^{-1}(U_n^0)$. □

Note that $V_n^0$ is a non-empty open set of $V_n$, thus, of $X_n$. Let $Z_n = X_n - V_n^0$; this is a proper Zariski closed subset of $X_n$. We now show that the Kawamata locus of $X_n$ is contained in $Z_n$.

**Lemma 6.5.** *Let $T \subseteq E^n$ be an abelian sub-variety of strictly positive dimension, and suppose that $x \in X_n(k)$ satisfies $x + T \subseteq X_n$. Then $x + T \subseteq Z_n$.*

*Proof.* Let $T' = x + T$. Since $T'(\mathbb{C})$ is a positive dimensional complex torus, there is a non-constant holomorphic map $\phi : \mathbb{C} \to X_n$ whose image is Zariski dense in $T'$; this can be seen by considering $T' \simeq \mathbb{C}^g/\Lambda$ for a lattice $\Lambda \subseteq \mathbb{C}^g$. Let us write $\phi_j = \pi_j \circ \phi : \mathbb{C} \to E$, so that $\phi = (\phi_1, ..., \phi_n)$.

By contradiction, suppose that $T'$ is not contained in $Z_n$. Then the image of $\phi$ meets $V_n^0$. Thus, the image of $G_n \circ \phi$ meets $U_n^0$. In particular, all the compositions $f_j = g \circ \phi_j$ are complex meromorphic functions (i.e. $\phi_j$ is not identically a pole of $g$, for each $j$).

The image of $G_n \circ \phi = (f_1, ..., f_n)$ is contained in the projective surface $H_n$ and meets the Zariski open subset $U_n^0 \subseteq H_n$. It follows that for all but countably many $z_0 \in \mathbb{C}$ we have

$(f_1(z_0),...,f_n(z_0)) \in U_n^0$. In fact, composing $G_n \circ \phi$ with local equations for the Zariski closed set $H_n - U_n^0 \subseteq H_n$, the claim follows from the fact that the zero set of a non-constant complex meromorphic function in one variable is at most countable.

By the identity principle, we get that $(f_1,...,f_n) \in \mathscr{M}^n$ satisfies the equations defining $U_n$ but not the equations defining $\Delta_n$. This means that $(f_1,...,f_n) \in U_n^0(\mathscr{M})$ as an $\mathscr{M}$-rational point. By Lemma 6.4 with $L = \mathscr{M}$, we get that $f_1,...,f_n$ is a non-trivial arithmetic progression in $\mathscr{M}$. Hence, there are $F_1, F_2 \in \mathscr{M}$ such that $F_2$ is not the zero function and $f_j = F_1 + jF_2$ for each $1 \leq j \leq n$.

As $\phi$ is non-constant and $g$ is finite, at least one of the $f_j$ is non-constant. Thus, at least one of $F_1$ or $F_2$ is non-constant, and it follows that at most one of the $f_1,...,f_n$ can be constant. Relabeling if necessary and deleting one term, we apply Theorem 4.1 with $M = n-1$ to conclude that $M \leq 10d^2 - 4d$. Since $n = 10d^2 - 4d + 2$ we get $10d^2 - 4d + 1 \leq 10d^2 - 4d$, a contradiction. $\square$

Finally, we proceed to conclude the proof of Theorem 6.1.

We apply Theorem 6.3 with $A = E^n$ and $\mathscr{L} = \mathscr{L}_n$; this choice of sheaf is allowed by Lemma 5.5. We obtain the effectively computable constant $c(E^n, \mathscr{L}_n) > 0$ provided by Theorem 6.3. This constant only depends on the isomorphism class over $k = \mathbb{Q}^{alg}$ of the pair $(E^n, \mathscr{L}_n)$. By construction (see Section 5.4), this data is uniquely determined by the isomorphism class of $E$ over $k$ and the integer $n = 10d^2 - 4d + 2$. Therefore, $c(E^n, \mathscr{L}_n)$ only depends on $d$ and $j_0$, the $j$-invariant of $E$, and this dependence is effective. Let us write $c(j_0, d)$ instead of $c(E^n, \mathscr{L}_n)$ to make explicit that this quantity only depends on $j_0$ and $d$. (See Section 6.5 for a concrete example.)

We take $X = X_n$, which has dimension $m = 2$ (cf. Lemma 5.4). Let us consider the group $\Lambda = \Gamma \times \cdots \times \Gamma \subseteq E^n(k)$ with $\Gamma$ as in Theorem 6.1 and observe that $\Lambda$ has finite rank

$$r = \operatorname{rank} \Lambda = n \cdot \operatorname{rank} \Gamma.$$

By Lemma 5.6, the number $R$ provided by Theorem 6.3 satisfies

$$R \leq (c(j_0,d) \deg_{\mathscr{L}_n} X_n)^{n^{45}(r+1)} \leq R_0 := \left(c(j_0,d) \cdot (n^2-n) d^{2n-2}\right)^{n^{45}(1+n \cdot \operatorname{rank} \Gamma)}. \tag{6.1}$$

In addition, there are points $x_1,...,x_R \in X_n(k)$ and abelian sub-varieties $T_1,...,T_R \subseteq E^n$ such that

$$V_n^0(k) \cap \Lambda \subseteq X_n(k) \cap \Lambda \subseteq \bigcup_{i=1}^{R} (x_i + T_i)(k).$$

By Lemma 6.5, all the $T_i$ with $\dim T_i \geq 1$ satisfy $x_i + T_i \subseteq Z_n$. Thus, writing

$$I = \{1 \leq i \leq R : T_i = \{e_A\}\}$$

we get

$$V_n^0(k) \cap \Lambda \subseteq \bigcup_{i \in I} (x_i + T_i)(k) = \{x_i : i \in I\}.$$

In particular,

$$\# \left(V_n^0(k) \cap \Lambda\right) \leq R. \tag{6.2}$$

Let us define

$$C(j_0,d) = \left(c(j_0,d) \cdot (n^2-n) d^{2n-2}\right)^{n^{46}} \quad \text{with} \quad n = 10d^2 - 4d + 2. \tag{6.3}$$

By (6.1) and (6.2), we see that

$$C(j_0,d)^{1+\operatorname{rank}\Gamma} = R_0 \left(c(j_0,d) \cdot (n^2-n) d^{2n-2}\right)^{n^{46}-n^{45}} > 2R_0 > n + R_0 \geq n + \# \left(V_n^0(k) \cap \Lambda\right). \tag{6.4}$$

Let $P_1,...,P_N \in \Gamma$ be as in the statement of Theorem 6.1, i.e, $g(P_1),...,g(P_N)$ is a non-trivial arithmetic progression in $k$. We note that for each $j = 1,...,N-n$ the sequence $g(P_j), g(P_{j+1}),..., g(P_{j+n-1})$ is a non-trivial arithmetic progression in $k$ of length $n$, and all these $N-n$ sequences are different. From Lemma 6.4 we deduce that $(P_j,...,P_{j+n-1}) \in V_n^0(k)$ for each $j = 1,...,N-n$ and these are

different points as their images under $G_n$ are different. Furthermore, by assumption $P_i \in \Gamma$ for each $i$, so we get $(P_j, ..., P_{j+n-1}) \in V_n^0(k) \cap \Lambda$. This proves $\#\left(V_n^0(k) \cap \Lambda\right) \geq N - n$.

Together with (6.4) we finally get

$$C(j_0, d)^{1+\operatorname{rank}\Gamma} > N.$$

This proves Theorem 6.1 with

$$\kappa(j_0, d) = 1/\log C(j_0, d). \tag{6.5}$$

Since $c(j_0, d)$ is effectively computable, so are $C(j_0, d)$ and $\kappa(j_0, d)$. □

6.4. **Consequences.** Let us formulate here two direct consequences of Theorem 6.1 that relate arithmetic progressions of rational points to two different aspects of the arithmetic of elliptic curves: the *rank*, and on the other hand, the *torsion* part.

**Corollary 6.6.** *Let $j_0 \in \mathbb{Q}^{alg}$ and let $d$ be a positive integer. There is an effectively computable constant $\kappa(j_0, d) > 0$ depending only on $j_0$ and $d$ such that the following holds:*

*Let $L \subseteq \mathbb{Q}^{alg}$ be a number field containing $j_0$ and let $E$ be an elliptic curve over $L$ with $j$-invariant equal to $j_0$. Let $g$ be a non-constant rational function on $E$ defined over $L$ of degree $d$. If for some $N$ there is a sequence of points $P_1, ..., P_N \in E(L)$ such that $g(P_1), ..., g(P_N)$ is a non-trivial arithmetic progression in $L$, then*

$$1 + \operatorname{rank} E(L) > \kappa(j_0, d) \cdot \log N$$

*Proof.* All elliptic curves over number fields with $j$-invariant equal to $j_0$ are isomorphic to each other after base change to $\mathbb{Q}^{alg}$. Thus, the result is immediate from Theorem 6.1 applied to $E' = E \otimes_L \mathbb{Q}^{alg}$ choosing the group $\Gamma = E(L)$, which is a group of finite rank by the Mordell-Weil theorem. Here, we use the inclusion $\Gamma \subseteq E(\mathbb{Q}^{alg}) \simeq E'(\mathbb{Q}^{alg})$. □

**Corollary 6.7.** *Let $E$ be an elliptic curve over $\mathbb{Q}^{alg}$ and let $d$ be a positive integer. There is an effectively computable constant $N(E, d)$ depending only on $E$ and $d$ such that the following holds:*

*Let $g$ be a non-constant rational function on $E$ defined over $\mathbb{Q}^{alg}$ of degree $d$. Let $S_g \subseteq E(\mathbb{Q}^{alg})$ be the set of poles of $g$ and let $E(\mathbb{Q}^{alg})_{tor}$ be the group of all torsion points of $E$. The set*

$$g\left(E(\mathbb{Q}^{alg})_{tor} - S_g\right) \subseteq \mathbb{Q}^{alg}$$

*does not contain non-trivial arithmetic progressions of length greater than $N(E, d)$.*

*Proof.* The group $\Gamma = E(\mathbb{Q}^{alg})_{tor}$ has rank 0 and the isomorphism class of $E$ over $\mathbb{Q}^{alg}$ is determined by the $j$-invariant. Thus, the result is a direct consequence of Theorem 6.1. □

As a special case, we obtain two of the main results stated in the Introduction.

*Proof of Theorem 1.1.* The result follows from Corollary 6.6 with $d = 2$ for $x$-coordinates, $d = 3$ for $y$-coordinates, and choosing $L = \mathbb{Q}$. □

*Proof of Theorem 1.2.* The result follows from Corollary 6.7 with $d = 2$ for $x$-coordinates and $d = 3$ for $y$-coordinates. □

6.5. **Effectivity.** Here we prove that (1.1) gives an admissible value for $c(j_0)$ in Theorem 1.1. Although we restrict ourselves to the setting of Theorem 1.1 for the sake of simplicity, it will be clear from the argument that a similar (although lengthier) computation gives an explicit value for the effective constants in Theorem 6.1 and its consequences.

Let $j_0 \in \mathbb{Q}$. From the proof of Theorem 1.1 (cf. Section 6.4) we note that $c(j_0)$ can be chosen as any value smaller than

$$\min\{\kappa(j_0, 2), \kappa(j_0, 3)\} = \frac{1}{\log \max\{C(j_0, 2), C(j_0, 3)\}} = \frac{1}{\log C(j_0, 3)}$$

with $\kappa(j_0, d)$ and $C(j_0, d)$ as defined in (6.3) and (6.5). Here we used that for $j_0$ fixed, one can check that the quantity $C(j_0, d)$ is increasing on $d$. We compute

$$\log C(j_0, 3) = 80^{46} \left(\log(c(j_0, 3)) + \log(6320) + 158 \log(3)\right) < 80^{46} \left(\log(c(j_0, 3)) + 183\right) \tag{6.6}$$

where $c(j_0, 3)$ is as in Section 6.3. Namely, $c(j_0, 3) = c(E^n, \mathscr{L}_n)$ where $n = 10 \cdot 3^2 - 4 \cdot 3 + 2 = 80$, $E$ is an elliptic curve over $\mathbb{Q}^{alg}$ with $j$-invariant equal to $j_0$, and $c(A, \mathscr{L})$ is the constant appearing in Theorem 6.3.

An admissible value for $c(A, \mathscr{L})$ is given in Théorème 1.3 of [35] under the additional assumption that $\mathscr{L}$ induces a principal polarization. In our case, $\mathscr{L} = \mathscr{L}_n \simeq \bigotimes_{j=1}^{n} \pi_j^* \mathscr{O}(e_E)$ induces a principal polarization on $E^n$, see [19]. Therefore, the formula from [35] directly applies. In our case, the abelian variety $A = E^n$ and the sheaf $\mathscr{L}_n$ can be defined over $\mathbb{Q}$ because $j_0 \in \mathbb{Q}$. Therefore, Théorème 1.3 of [35] allows us to take

$$c(j_0, 3) = c(E^n, \mathscr{L}_n) = 2^{34} \cdot \max\{1, h_\Theta(E^n)\}, \quad n = 80 \tag{6.7}$$

where $h_\Theta$ denotes the *Theta height* associated to the line sheaf $\mathscr{L}^{\otimes 16}$. Let us estimate the Theta height. First we compare it to the semi-stable Faltings' height $h_F$ using results by Pazuki, namely Corollary 1.3(2) in [30]. Here we use the normalization of $h_F$ used in *loc. cit.* As we are using the Theta height associated to $\mathscr{L}^{\otimes 16}$, we must choose $r = 4$ in [30] Corollary 1.3(2), which gives

$$\begin{aligned} h_\Theta(E^n) &\leq \frac{1}{2} \max\{1, h_F(E^n)\} + C_2(80, 4) \log\left(2 + \max\{1, h_F(E^n)\}\right) \\ &< \frac{1}{2} \max\{1, h_F(E^n)\} + e^{256} \log(2 + \max\{1, h_F(E^n)\}). \end{aligned}$$

Since the Faltings height satisfies $h_F(A_1 \times A_2) = h_F(A_1) + h_F(A_2)$ (cf. equation (2.7) in [4] for instance) and we chose $n = 80$, we find

$$h_\Theta(E^n) < \frac{1}{2} \max\{1, 80 h_F(E)\} + e^{256} \log(2 + \max\{1, 80 h_F(E)\}).$$

Lemme 7.9 in [15] (see also [39]) gives $h_F(E) \leq h(j_0)/12 - 0.72 < h(j_0)$ where $h(x) = \log H(x)$ for $x \in \mathbb{Q}$ (note that the normalization of the Faltings height in [15] and [30] is the same), from which we get

$$\begin{aligned} h_\Theta(E^n) &< \frac{1}{2} \max\left\{1, \frac{20}{3} h(j_0)\right\} + e^{256} \log\left(2 + \max\left\{1, \frac{20}{3} h(j_0)\right\}\right) \\ &\leq \frac{10}{3}(1 + h(j_0)) + e^{256} \log\left(\frac{20}{3}(1 + h(j_0))\right) \\ &\leq \max\left\{\frac{20}{3}(1 + h(j_0)), e^{257} \log\left(\frac{20}{3}(1 + h(j_0))\right)\right\}. \end{aligned}$$

From (6.7) we get

$$\begin{aligned} \log c(j_0, 3) &< 34 \log 2 + \max\left\{\log \frac{20}{3} + \log(1 + h(j_0)), 257 + \log\left(\log \frac{20}{3} + \log(1 + h(j_0))\right)\right\} \\ &< 24 + \max\{2 + \log(1 + h(j_0)), 257 + \log\left(2 + \log(1 + h(j_0))\right)\} \\ &= 26 + \max\{\log(1 + h(j_0)), 255 + \log\left(2 + \log(1 + h(j_0))\right)\}. \end{aligned}$$

Finally (6.6) gives

$$\log C(j_0, 3) < 80^{46} \left(209 + \max\{\log(1 + h(j_0)), 255 + \log\left(2 + \log(1 + h(j_0))\right)\}\right)$$

which proves (1.1). □

## 7. Bounding the rank and applications

7.1. **Pointwise rank bounds.** Let us recall the following bound for the rank of the quadratic twist of an elliptic curve. A similar result holds over number fields, although to simplify the notation we only state the case of $\mathbb{Q}$. Here we recall that $\omega(D)$ is the number of distinct prime divisors of $D$.

**Lemma 7.1.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. There is an effectively computable constant $c(E)$ depending only on $E$ such that for all squarefree integers $D$ we have*

$$\operatorname{rank} E^{(D)}(\mathbb{Q}) \leq 12 \cdot \omega(D) + c(E).$$

*Proof.* This follows from [40] Ch. VIII, Exercise 8.1 with $m = 2$. In particular, $c(E)$ is bounded by a multiple of the number of places of bad reduction of $E$ plus the 2-rank of the class group of $K = \mathbb{Q}(E[2]) = \mathbb{Q}(E^{(D)}[2])$. □

From this we get

**Corollary 7.2.** *Let $E$ be an elliptic curve over $\mathbb{Q}$ and let $d$ be a positive integer. There is an effectively computable constant $C(E, d)$ depending only on $E$ and $d$ such that the following holds:*

*Let $D$ be a squarefree integer. Let $g$ be a rational function on $E^{(D)}$ defined over $\mathbb{Q}$ of degree $d$. If for some $N$ there is a sequence of rational points $P_1, ..., P_N \in E^{(D)}(\mathbb{Q})$ satisfying that $g(P_1), ..., g(P_N)$ is a non-trivial arithmetic progression in $\mathbb{Q}$, then $N < C(E, d)^{\omega(D)+1}$.*

*Proof.* The result is obtained from Corollary 6.6 with $L = \mathbb{Q}$, using the fact that taking quadratic twists does not change the $j$-invariant, and using Lemma 7.1 to bound $\operatorname{rank} E^{(D)}(\mathbb{Q})$. □

We note that Corollary 1.3 is a special case of Corollary 7.2.

7.2. **Average bounds for Mordell curves.** As in the introduction, for $x > 0$ we let $S(x)$ be the set of sixth-power free integers $n$ with $|n| \leq x$. It is an elementary result in Analytic Number Theory that the number of $k$-power free positive integers up to $x$ is asymptotic to $x/\zeta(k)$ where $\zeta(s)$ is the Riemann zeta function. In particular we have

**Lemma 7.3.** *As $x \to \infty$ we have the asymptotic estimate*

$$\#S(x) \sim \frac{2}{\zeta(6)} \cdot x = \frac{1890}{\pi^6} \cdot x.$$

For $n$ a sixth-power free integer, we consider the Mordell elliptic curve $A_n$ defined by the equation $y^2 = x^3 + n$. The following theorem is a special case of a result due to Fouvry, cf. [12] Théorème 1 (using the bounds $R^+(\sqrt{3}) \leq 115$ and $R^-(\sqrt{3}) \leq 100$ given there).

**Theorem 7.4.** *The following estimate holds for all large enough $x$:*

$$\sum_{n \in S(x)} 3^{(\operatorname{rank} A_n(\mathbb{Q}))/2} < 216 \cdot x.$$

With these results, we can proceed to the proof of Theorem 1.6.

*Proof of Theorem 1.6.* By Theorem 1.1 with $j_0 = 0$ we have

$$\max\{\beta_x(A_n), \beta_y(A_n)\} \leq \exp\left((1 + \operatorname{rank} A_n(\mathbb{Q}))/c\right)$$

where $c = c(0) > 0$ is an absolute constant. Let us take $\tau = (c \cdot \log 3)/2 > 0$ and note that

$$\max\{\beta_x(A_n), \beta_y(A_n)\}^\tau \leq \sqrt{3} \cdot 3^{(\operatorname{rank} A_n(\mathbb{Q}))/2}.$$

Theorem 7.4 gives that for all large enough $x$ we have

$$\sum_{n \in S(x)} \max\{\beta_x(A_n), \beta_y(A_n)\}^\tau \leq 216\sqrt{3} \cdot x.$$

Since $216\sqrt{3}\cdot 1890/\pi^6 < 735.5$, Lemma 7.3 gives that for all large enough $x$ we have

$$\sum_{n\in S(x)} \max\{\beta_x(A_n),\beta_y(A_n)\}^\tau < 800\cdot \#S(x).$$

The result follows □

We remark that we can use Corollary 6.6 instead of Theorem 1.1 to obtain a version of Theorem 1.6 for more general rational functions, not just $x$ and $y$-coordinates.

As explained in the introduction, a crucial aspect in the proof of Theorem 1.6 is that our lower bounds for the rank are logarithmic on the maximal length of an arithmetic progression (cf. Theorems 1.1 and 6.1), and not worse than logarithmic. Briefly, the reason why Fouvry's theorem can control averages of an exponential function of the rank that the core of [12] is an average estimate for the size of certain 3-isogeny Selmer groups, which is then used as an upper bound for $\#\left(A_n(\mathbb{Q})/3A_n(\mathbb{Q})\right) \geq 3^{\operatorname{rank} A_n(\mathbb{Q})}$.

7.3. **Average bounds for congruent number curves.** For $x>0$, let $Q(x)$ be the set of odd squarefree positive integers $n\leq x$. We remark that it is an elementary exercise in sieve theory to check that $\#Q(x)\sim (3/\pi^2)\cdot x$ as $x\to\infty$.

Given a squarefree integer $n$, we consider the elliptic curve $B_n$ defined by $y^2=x^3-n^2x$. These elliptic curves are associated to the classical congruent number problem. The following theorem is a direct consequence of Theorem 1 in [17] by Heath-Brown.

**Theorem 7.5.** *Let $\ell$ be a positive integer. As $x\to\infty$ we have the asymptotic estimate*

$$\sum_{n\in Q(x)} \left(\#S_2(B_n)\right)^\ell \sim 4^{\ell+1}\prod_{j=1}^{\ell}\left(1+2^j\right)\cdot \#Q(x).$$

*In particular, there is a positive constant $\gamma(\ell)$ depending only on $m$ such that for all $x>1$ we have*

$$\sum_{n\in Q(x)} \left(\#S_2(B_n)\right)^\ell < \gamma(\ell)\cdot \#Q(x).$$

The previous bound for the moments of $\#S_2(B_n)$ allows us to prove Theorem 1.7.

*Proof.* All the elliptic curves $B_n$ have $j$-invariant equal to 1728. For each squarefree positive integer $n$, Theorem 1.1 with $j_0=1728$ gives

$$\max\{\beta_x(B_n),\beta_y(B_n)\}\leq \exp\left((1+\operatorname{rank} B_n(\mathbb{Q}))/c\right)$$

where $c=c(1728)>0$ is an absolute constant. Given $k>0$ we choose the positive integer

$$\ell=\ell(k)=\left\lceil \frac{k}{c\log 2}\right\rceil$$

where $\lceil t\rceil$ is the smallest integer bigger than or equal to $t$. Thus, $\ell\log 2\geq k/c$ and we deduce

$$\max\{\beta_x(B_n),\beta_y(B_n)\}^k \leq 2^{(1+\operatorname{rank} B_n(\mathbb{Q}))\cdot\ell} < \#\left(B_n(\mathbb{Q})/2B_n(\mathbb{Q})\right)^\ell$$

for each squarefree positive integer $n$. Here we used the classical fact that the rational torsion of $B_n$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, so that $\#\left(B_n(\mathbb{Q})/2B_n(\mathbb{Q})\right)=2^{2+\operatorname{rank} B_n(\mathbb{Q})}$.

The fundamental injective map $B_n(\mathbb{Q})/2B_n(\mathbb{Q})\to S_2(B_n(\mathbb{Q}))$ (cf. the exact sequence (1.2)) together with Theorem 7.5 finally give that for all $x>1$

$$\sum_{n\in S(x)} \max\{\beta_x(B_n),\beta_y(B_n)\}^k < \gamma\left(\left\lceil\frac{k}{c\log 2}\right\rceil\right)\cdot \#Q(x)$$

□

Finally, we remark that using Corollary 6.6 instead of Theorem 1.1, the same argument gives a version of Theorem 1.7 for any non-constant rational function on $B_n$, not just $x$ and $y$ coordinates.


## Funding

This work was supported by FONDECYT [Iniciación en Investigación 11170192 to N.G.-F., Regular 1190442 to H.P.]; and CONICYT [PAI79170039 to N. G.-F.].

## Acknowledgements

We thank Dino Lorenzini and Eduardo Friedman for encouraging us to extend our methods beyond the case of arithmetic progressions in $x$ and $y$-coordinates. Also, we are indebted to Éric Gaudron for valuable suggestions regarding effectivity. Finally, we thank the anonymous referee for carefully reading this manuscript and for several useful comments.


## References


[1] M. Bhargava, D. Kane, H. Lenstra, B. Poonen, E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves.* Camb. J. Math. 3 (2015), no. 3, 275-321.

[2] M. Bhargava, N. Elkies, A. Shnidman, *The average size of the* 3*-isogeny Selmer groups of elliptic curves* $y^2 = x^3+k$. J. Lond. Math. Soc. (2) (2019). DOI: 10.1112/jlms.12271

[3] E. Bombieri, *The Mordell conjecture revisited.* Ann. Sc. Norm. Super. Pisa Cl. Sci. (5), 1990, vol. 17, no 4, 615-640.

[4] J.-B. Bost, *Périodes et isogénies des variétés abéliennes sur les corps de nombres.* Astérisque, tome 237 (1996), Séminaire Bourbaki, exp. no 795, 115-161.

[5] A. Bremner, *On arithmetic progressions on elliptic curves.* Exp. Math., 1999, vol. 8, no 4, 409-413.

[6] A. Bremner, J. Silverman, N. Tzanakis, *Integral points in arithmetic progression on* $y^2 = x(x^2 - n^2)$. J. Number Theory, (2000) 80(2), 187-208.

[7] G. Campbell, *A note on arithmetic progressions on elliptic curves.* J. Integer Seq. 6 (2003), no. 03.1.3.

[8] N. Elkies, $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.* Listserv. 3 Apr. 2006. NmbrThry.

[9] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349-366.

[10] G. Faltings, *Diophantine approximation on abelian varieties.* Ann. of Math. (2), 133 (1991), 549-576.

[11] G. Faltings, *The general case of S. Lang's conjecture.* Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991). Perspect. Math. 15. Academic Press. San Diego. (1994) 175-182.

[12] E. Fouvry, *Sur le comportement en moyenne du rang des courbes* $y^2 = x^3 + k$. Séminaire de Théorie des Nombres, Paris, 1990-91, Progr. Math. (1993), 61-84.

[13] N. Garcia-Fritz, *Quadratic sequences of powers and Mohanty's conjecture.* Int. J. Number Theory 14.02 (2018), 479-507.

[14] I. Garcia-Selfa, J. Tornero. *Searching for simultaneous arithmetic progressions on elliptic curves.* Bull. Aust. Math. Soc. 71, no. 3 (2005), 417-424.

[15] É. Gaudron, G. Rémond, *Théorème des périodes et degrés minimaux d'isogénies.* Comment. Math. Helv. 89 (2014), no. 2, 343-403.

[16] R. Hartshorne, *Algebraic geometry.* Grad. Texts in Math., No. 52. Springer- Verlag, New York-Heidelberg (1977).

[17] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem, II.* Invent. Math., (1994) vol. 118, no 1, 331-370.

[18] Y. Kawamata. *On Bloch's conjecture.* Invent. Math. 57 (1980), 97-100.

[19] H. Lange, *Principal polarizations on products of elliptic curves.* (English summary) The geometry of Riemann surfaces and abelian varieties, 153-162, Contemp. Math., 397, Amer. Math. Soc., Providence, RI, 2006.

[20] J. Lee, W. Vélez, *Integral solutions in arithmetic progression for* $y^2 = x^3 + k$. Period. Math. Hungar. 25, no. 1 (1992), 31-49.

[21] A. Levin, J. Wang, *Greatest common divisors of analytic functions and Nevanlinna theory on algebraic tori.* arXiv preprint arXiv:1903.03876 (2019).

[22] H. Liao, M. Ru, A note on the second main theorem for holomorphic curves into algebraic varieties. Bull. Inst. Math. Acad. Sin. (N.S.) Vol. 9 (2014), No. 4, 671-684.

[23] X. Liu, G. Yu, *Upper Bounds of GCD Counting Function for Holomorphic Maps.* The J. Geom. Anal. (2019) 29, 1032-1042.

[24] S. P. Mohanty, *On consecutive integer solutions for* $y^2 - k = x^3$. Proc. Amer. Math. Soc. 48 (1975), 281-285.

[25] S. P. Mohanty, *Integer solutions in arithmetic progression for* $y^2 - k = x^3$. Acta Math. Hungar., (1980) 36, 261-265.
[26] D. Moody, A. Zargar, *On the rank of elliptic curves with long arithmetic progressions*. In Colloq. Math. (Vol. 148, 47-68). Inst. Math., Polish Acad. Sci. (2017).
[27] J. Park, B. Poonen, J. Voight, M. Wood. *A heuristic for boundedness of ranks of elliptic curves*. J. Eur. Math. Soc. (JEMS) (2019). DOI: 10.4171/JEMS/893
[28] H. Pasten, *Bounded ranks and Diophantine error terms*. Math. Res. Lett., 26 (2019), no. 5, 1559-1570.
[29] H. Pasten, J. Wang, *GCD Bounds for Analytic Functions*. Int. Math. Res. Not. IMRN (2017), no. 1, 47-95.
[30] F. Pazuki, *Theta height and Faltigs height*. Bull. Soc. Math. France 140 (1), (2012), 19-49.
[31] B. Poonen, *Heuristics for the arithmetic of elliptic curves*. Preprint (2017). arXiv: 1711.10112
[32] B. Poonen, E. Rains, *Random maximal isotropic subspaces and Selmer groups*. J. Amer. Math. Soc. 25 (2012), no. 1, 245-269.
[33] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 327-352. Birkhäuser Boston, Boston, MA, 1983.
[34] G. Rémond, *Décompte dans une conjecture de Lang*. Invent. Math., (2000) 142 (3), 513-545.
[35] G. Rémond, *Sur les sous-variétés des tores*. Compos. Math. 134.3 (2002), 337-366.
[36] J. Robertson, *Magic Squares of Squares*. Math. Mag., Vol. 69, No. 4 (1996), 289-293.
[37] K. Rubin, A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*. Exp. Math. 9 (2000), no. 4, 583-590.
[38] I. Shafarevitch, J. Tate, *The rank of elliptic curves*. Dokl. Akad. Nauk 175 (1967), 770-773.
[39] J. Silverman, *Heights and elliptic curves*. Arithmetic geometry (Storrs, Conn., 1984), 253-265, Springer, New York, (1986).
[40] J. Silverman, *The arithmetic of elliptic curves*. Second edition. Grad. Texts in Math., 106. Springer, Dordrecht, (2009).
[41] B. Spearman, *Arithmetic progressions on congruent number elliptic curves*. The Rocky Mountain J. Math., Vol. 41, No. 6 (2011), 2033-2044.
[42] M. Ulas, *Rational Points in Arithmetic Progressions on* $y^2 = x^n + k$. Canad. Math. Bull. 55, no. 1 (2012), 193-207.
[43] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) 155 (2002), no. 1, 295-315.
[44] P. Vojta, *Siegel's theorem in the compact case*. Ann. of Math. (2), 1991, 509-548.
[45] P. Vojta, *Diophantine approximation and Nevanlinna theory*. Arithmetic geometry, 111-224, Lecture Notes in Math. 2009, Springer, Berlin (2011).
[46] M. Watkins, S. Donnelly, N. Elkies, T. Fisher, A. Granville, N. Rogers, *Ranks of quadratic twists of elliptic curves*, Publ. Math. de Besançon 2014/2 (2014), 63-98.

Departamento de Matemáticas
Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna
Macul, RM, Chile
*E-mail address*, N. Garcia-Fritz: natalia.garcia@mat.uc.cl

Departamento de Matemáticas
Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna
Macul, RM, Chile
*E-mail address*, H. Pasten: hector.pasten@mat.uc.cl