Algebra & Number Theory

Volume 6

2012

No. 6

Ideals of degree one contribute most of the height

Aaron Levin and David McKinnon

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1223

Ideals of degree one contribute most of the height

Aaron Levin and David McKinnon

Let k be a number field, $f(x) \in k[x]$ a polynomial over k with $f(0) \neq 0$, and $\mathcal{O}_{k,S}^*$ the group of S-units of k, where S is an appropriate finite set of places of k. In this note, we prove that outside of some natural exceptional set $T \subset \mathcal{O}_{k,S}^*$, the prime ideals of $\mathcal{O}_k$ dividing $f(u)$, $u \in \mathcal{O}_{k,S}^* \setminus T$, mostly have degree one over $\mathbb{Q}$; that is, the corresponding residue fields have degree one over the prime field. We also formulate a conjectural analogue of this result for rational points on an elliptic curve over a number field, and deduce our conjecture from Vojta's conjecture. We prove this conjectural analogue in certain cases when the elliptic curve has complex multiplication.

1. Introduction

If a is an algebraic integer in a number field k and $f(x) \in \mathcal{O}_k[x]$ a polynomial, then the ideals dividing $f(a)$ are simply the ideals I such that $f(a) \equiv 0 \pmod{I}$. Heuristically, the larger the cardinality of the residue ring $\mathcal{O}_k/I$, the smaller the probability that $f(a)$ and 0 are the same.

The purpose of this paper is to make this notion precise, to generalize it, and to prove it in the case described above. More specifically, in Theorem 2.1, using a result of Corvaja and Zannier, we prove a precise version of this notion for $\mathbb{G}_m$, and in Theorem 3.4, we state a conjectural analogue of Theorem 2.1 for elliptic curves over a number field, and show that it is a consequence of Vojta's conjecture [1987; 2011].

A theorem of the second author proves Vojta's conjecture in a relevant special case, and we deduce an unconditional version of Theorem 3.4 in that case. Specifically, if the elliptic curve E/k has complex multiplication, and if the algebraic point P is defined over the compositum of k with $\mathrm{End}(E) \otimes \mathbb{Q}$, then we can deduce Theorem 3.4 without the hypothesis that Vojta's conjectures are true.

MSC2010: primary 11G50; secondary 11J25.

Keywords: heights, Diophantine approximation, polynomial values, elliptic curves, Vojta's conjecture.

2. Main theorem

Let $f(x) \in k[x]$ be a polynomial over a number field k. The heuristic mentioned in the introduction suggests that a prime $\mathfrak{p}$ of k is likelier to divide $f(a)$ for $a \in k$ if the residue field $\mathcal{O}_k/\mathfrak{p}$ is small. Our main theorem will give one possible precise interpretation of this notion, where we view $\mathcal{O}_k/\mathfrak{p}$ as being small if $\mathcal{O}_k/\mathfrak{p}$ has degree one over its prime field. There is, however, an obvious way that our heuristic can fail. Suppose, for example, that f and a, and hence $f(a)$, are actually defined over a proper subfield k' of k. Then the size of $\mathcal{O}_{k'}/(\mathfrak{p} \cap \mathcal{O}_{k'})$, and not $\mathcal{O}_k/\mathfrak{p}$, is clearly the relevant quantity. In the simplest case, when $k/\mathbb{Q}$ is Galois and f is irreducible, our main theorem says, in essence, that for S-units u of k this is in fact the only way our heuristic can fail, that is, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$ unless $f(u)$ is rational, in an appropriate sense, over a proper subfield of k.

The statement of the main theorem requires a fair amount of notation. We summarize this notation as follows:

k	Extension of $\mathbb{Q}$ of degree $d \neq 1$
L	Galois closure of k over $\mathbb{Q}$
$\mathrm{Gal}(L/\mathbb{Q})$	The Galois group of L over $\mathbb{Q}$
$\mathcal{O}_k$	Ring of integers of k
$f(x)$	Nonconstant polynomial in $\mathcal{O}_k[x]$ with $f(0) \neq 0$
$f_1, \ldots, f_N$	The monic irreducible factors of f over L
S	Finite set of places of k containing the archimedean places such that if $v \in S$ and v and v' lie above the same rational prime $p \in \mathbb{Z}$ then $v' \in S$.
$\mathcal{O}_{k,S}$	Ring of S-integers of k
$\mathcal{O}_{k,S}^*$	Group of S-units of k
τ	The involution $\tau(u) = u^{-1}$ of $\mathcal{O}_{k,S}^*$.
$\mathcal{O}_{k,S}^{*\phi}$	For a homomorphism ϕ, the subgroup of $\mathcal{O}_{k,S}^*$ consisting of elements u such that $\phi(u) = u$.
$I(f(u))$	The ideal generated by $f(u)$ in the ring $\mathcal{O}_{k,S}$
$J(f(u))$	Smallest ideal dividing $I(f(u))$ such that for every prime $\mathfrak{p}$ dividing $J(f(u))$, $\mathcal{O}_{k,S}/\mathfrak{p}$ has degree greater than one over the prime field
$N(I)$	The norm of I over $\mathbb{Q}$, for any ideal I of $\mathcal{O}_k$ or $\mathcal{O}_{k,S}$
$H_k(x)$	The relative multiplicative Weil height of $x \in k$
$H(x)$	The absolute multiplicative Weil height of x, equal to $H_k(x)^{1/d}$ for $x \in k$
$h(x)$	The absolute logarithmic Weil height of x, equal to $\log H(x)$

We can now state the main theorem:

Theorem 2.1. *Let $\epsilon > 0$. Let $f(x) \in \mathbb{O}_k[x]$ satisfy $f(0) \neq 0$. Then there exists a finite set of places S' of L such that for every $u \in \mathbb{O}_{k,S}^*$ either*

(a) $$N(J(f(u))) < H(u)^\epsilon$$

or

(b) $$f_i(u)\mathbb{O}_{L,S'} = \alpha\mathbb{O}_{L,S'} \tag{1}$$

for some i and some α that lies in a proper subfield of L not containing k (in particular, if $k/\mathbb{Q}$ is Galois, α lies in a proper subfield of k).

With the exception of finitely many elements, the set of elements in $\mathbb{O}_{k,S}^*$ not satisfying (a) is contained in a finite union of cosets in $\mathbb{O}_{k,S}^*$ of the form

$$T = u_1\mathbb{O}_{k,S}^{*\sigma_1} \cup \cdots \cup u_{m'}\mathbb{O}_{k,S}^{*\sigma_{m'}} \cup u_{m'+1}\mathbb{O}_{k,S}^{*\sigma_{m'+1}\tau} \cup \cdots \cup u_m\mathbb{O}_{k,S}^{*\sigma_m\tau},$$

where $u_1, \ldots, u_m \in \mathbb{O}_{k,S}^*$ and $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k)$ (not necessarily distinct) are effectively computable.

An alternative formulation of Theorem 2.1 involving only heights is given in Corollary 2.6. We mention also that the group $\mathbb{O}_{k,S}^{*\sigma_i}$ is the same as $\mathbb{O}_{F,S_F}^*$, where F is the fixed field of σ_i and S_F is the set of places of F lying below places of S.

Note that $H(f(u)) \ll H(u)^{\deg f}$ and that

$$H_k(f(u)) = C_u N(I(f(u))) = C_u N(J(f(u)))N(I(f(u))/J(f(u))),$$

where C_u is a real number (roughly equal to the archimedean part of the height of $f(u)^{-1}$) satisfying $C_u \ll H(u)^\epsilon$ (see Lemma 2.7). Thus, Theorem 2.1 implies that for $u \in \mathbb{O}_{k,S}^* \setminus T$, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$.

Finally, let us mention some possible generalizations of Theorem 2.1. Firstly, we note that for any integer n and $u \in \mathbb{O}_{k,S}^*$, we have $J(u^n f(u)) = J(f(u))$ and $u^n f(u)\mathbb{O}_{k,S} = f(u)\mathbb{O}_{k,S}$. Thus, Theorem 2.1 immediately extends to Laurent polynomials (that is, $f(x) \in k[x, 1/x]$). However, if $f(x)$ has a zero or pole at $x = 0$, then the interpretation that for $u \in \mathbb{O}_{k,S}^* \setminus T$, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$ is no longer necessarily valid (the inequality $N(I(f(u))) \gg H_k(f(u))^{1-\epsilon}$ may not hold in the previous remark). More generally, Theorem 2.1 may be extended in a straightforward way to rational functions (appropriately using fractional ideals in place of integral ideals). In a different direction, it seems to be an interesting problem to formulate an appropriate generalization of Theorem 2.1 that is valid for S-integers (as opposed to just S-units), or to prove a multivariable analogue.

Before we begin the proof, we introduce some notation. For a number field k we denote the set of inequivalent places of k by M_k. We define the function $\log^-$ for positive real numbers x by $\log^-(x) = \min\{0, \log(x)\}$. For a place $v \in M_k$, we normalize the corresponding absolute value $|\cdot|_v$ in such a way that the product formula holds and $H(x) = \prod_{v \in M_k} \max\{1, |x|_v\}$.

Proof of Theorem 2.1. Consider the set

$$U = \{u \in \mathbb{O}_{k,S}^* \mid N(J(f(u))) \geq H(u)^\epsilon\}.$$

Let L be a Galois closure of k over $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of $\mathbb{O}_k$ of inertia degree greater than one over $\mathbb{Q}$, lying above a rational prime $p \in \mathbb{Z}$. Let $\mathfrak{q}$ be a prime of $\mathbb{O}_L$ lying above $\mathfrak{p}$. Then $\mathfrak{q}$ again has inertia degree greater than one over $\mathbb{Q}$. Let $D = D(\mathfrak{q}/p) \subset \mathrm{Gal}(L/\mathbb{Q})$ be the decomposition group of $\mathfrak{q}$ and let L^D be the decomposition field. Then $k \not\subset L^D$ since $\mathfrak{p}$ has inertia degree greater than one. It follows that there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$, $\sigma \notin \mathrm{Gal}(L/k)$.

Let S_L be the set of places of L lying above places of S. Let

$$J'(f(u)) = J(f(u))\mathbb{O}_{L,S_L}.$$

Let $\mathfrak{q}$ be a prime of $\mathbb{O}_{L,S_L}$ dividing $J'(f(u))$. From the above discussion and the definition of $J(f(u))$, there exists an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$. Let $\mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k) = \{\sigma_1, \ldots, \sigma_m\}$. For $i = 1, \ldots, m$, define the ideal $J_i'(f(u))$ to be the smallest ideal of $\mathbb{O}_{L,S_L}$ dividing $J'(f(u))$ such that $\sigma_i(J_i'(f(u))) = J_i'(f(u))$. Then $J'(f(u))$ divides $J_1'(f(u)) \cdots J_m'(f(u))$. Note also that $N(J'(f(u))) \geq N(J(f(u)))$. Let

$$U_i = \{u \in U \mid N(J_i'(f(u))) \geq H(u)^{\epsilon/m}\}.$$

Then clearly $U \subset \bigcup_{i=1}^m U_i$.

Let $r \in \{1, \ldots, m\}$, and let f^{σ_r} denote the image of f under the natural action of σ_r. By definition, $J_r'(f(u))$ divides both $f(u)\mathbb{O}_{L,S_L}$ and $f^{\sigma_r}(\sigma_r(u))\mathbb{O}_{L,S_L}$ for all u. For $u \in U_r$, we therefore obtain

$$\begin{aligned}[L:\mathbb{Q}] \sum_{v \in M_L} \log^- \max\{|f(u)|_v, |f^{\sigma_r}(\sigma_r(u))|_v\} &\leq -\log N(J_r'(f(u))) \\ &\leq -\log H(u)^{\epsilon/m} \leq -\frac{\epsilon}{m} h(u).\end{aligned}$$

Theorem 2.1 will follow essentially from the following:

Lemma 2.2 [Corvaja and Zannier 2005, Proposition 4]. *Let $f(x), g(x) \in L[x]$ be polynomials that do not vanish at $x = 0$. Then, for every $\epsilon > 0$, all but finitely many solutions $(u, u') \in (\mathbb{O}_{L,S_L}^*)^2$ to the inequality*

$$\sum_{v \in M_L} \log^- \max\{\,|f(u)|_v\,, |g(u')|_v\} < -\epsilon(\max\{h(u), h(u')\})$$

are contained in finitely many effectively computable translates of one-dimensional subgroups of $\mathbb{G}_m^2$.

Since $h(u) = h(\sigma_r(u))$ and $u, \sigma_r(u) \in \mathbb{O}^*_{L,S_L}$, taking $g = f^{\sigma_r}$ it follows immediately from Lemma 2.2 that all but finitely many elements of the set

$$V_r = \{(u, \sigma_r(u)) \mid u \in U_r\}$$

are contained in finitely many effectively computable translates of one-dimensional subgroups of $\mathbb{G}_m^2$. Let X be a translate of a one-dimensional subgroup of $\mathbb{G}_m^2$ that contains infinitely many elements of V_r. Let $(v, \sigma_r(v)) \in X \cap V_r$. Taking $u = v'/v \in \mathbb{O}^*_{k,S}$, where $(v', \sigma_r(v')) \in X \cap V_r$, we see that infinitely many elements of the form $(u, \sigma_r(u))$, $u \in \mathbb{O}^*_{k,S}$, will lie in the associated one-dimensional subgroup in $\mathbb{G}_m^2$. We now classify the possibilities for such a one-dimensional subgroup.

Suppose there exists $a, b \in \mathbb{Z}$, not both zero, such that

$$u^a \sigma_r(u)^b = 1, \tag{2}$$

for infinitely many $u \in \mathbb{O}^*_{k,S}$. We claim that $a = \pm b$. Let l be the order of σ_r. Then

$$u^{b^l} = \sigma_r^l(u)^{b^l} = \sigma_r^{l-1}(u)^{-ab^{l-1}} = \cdots = u^{(-a)^l}.$$

So $u^{b^l-(-a)^l} = 1$ for infinitely many $u \in \mathbb{O}^*_{k,S}$. This implies that $b^l = (-a)^l$, or $a = \pm b$, as claimed.

Suppose first that $a = -b$. Then for any $u \in \mathbb{O}^*_{k,S}$ satisfying (2) we have $\sigma_r(u^a) = u^a$. So $u^a \in \mathbb{O}^{*\sigma_r}_{k,S} = F \cap \mathbb{O}^*_{k,S}$, where F is the fixed field of σ_r. It follows that $\mathbb{O}^{*\sigma_r}_{k,S}$ has finite index in $\{u \in \mathbb{O}^*_{k,S} \mid u^a \sigma_r(u)^{-a} = 1\}$ and that $\{u \in \mathbb{O}^*_{k,S} \mid (u, \sigma_r(u)) \in X \cap V_r\}$ is contained in a finite number of cosets of $\mathbb{O}^{*\sigma_r}_{k,S}$ in $\mathbb{O}^*_{k,S}$.

Suppose now that $a = b$. Then for any $u \in \mathbb{O}^*_{k,S}$ satisfying (2) we have $\sigma_r(u^a) = u^{-a}$. By definition, we have $u^{-a} \in \mathbb{O}^{*\sigma_r\tau}_{k,S}$. Then, as above, we find that

$$\{u \in \mathbb{O}^*_{k,S} \mid (u, \sigma_r(u)) \in X \cap V_r\}$$

is contained in a finite number of cosets of $\mathbb{O}^{*\sigma_r\tau}_{k,S}$ in $\mathbb{O}^*_{k,S}$.

Since there are only finitely many such X and finitely many r, we conclude that there exists a set T as in the statement of the theorem such that $U \setminus T$ is finite.

We now prove that all of the elements in T satisfy (1) for some choice of S', completing the proof of the theorem. Let $f_1, \dots, f_N \in L[x]$ be the monic irreducible factors of $f(x)$ over L. First, consider cosets in $\mathbb{O}^*_{k,S}$ of the form $u_i \mathbb{O}^{*\sigma_r}_{k,S}$. From a slight modification of the first part of the proof above, we need only consider cosets $u_i \mathbb{O}^{*\sigma_r}_{k,S}$ such that for some $j \in \{1, \dots, N\}$ and $\epsilon > 0$, there are infinitely many $u \in \mathbb{O}^{*\sigma_r}_{k,S}$ such that

$$\sum_{v \in M_L} \log^- \max\{\, |f_j(u_i u)|_v\,, |f_j^{\sigma_r}(\sigma_r(u_i u))|_v\} \leq -\epsilon h(u_i u). \tag{3}$$

Note that $\sigma_r(u_iu) = \sigma_r(u_i)u$, since $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. If $f_j(u_ix)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ are relatively prime in $L[x]$, then the left-hand side of (3) is bounded from below, independent of $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. Since there are only finitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r}$ with $h(u_iu)$ bounded, this contradicts the inequality (3) for all but finitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. So $f_j(u_ix)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ have a nontrivial common factor. Since $f_j(u_ix)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ are both irreducible over L, they must then be equal up to multiplication by a constant factor. Thus,

$$\frac{f_j(u_ix)}{u_i^e} = \frac{f_j^{\sigma_r}(\sigma_r(u_i)x)}{\sigma_r(u_i)^e},$$

where $e = \deg f_j$. It follows that for all u in $\mathbb{O}_{k,S}^{*\sigma_r}$,

$$\frac{f_j(u_iu)}{u_i^e} = \sigma_r\Big(\frac{f_j(u_iu)}{u_i^e}\Big).$$

So $f_j(u_iu)/u_i^e \in k'$, the fixed field of σ_r. Then, for all $u \in \mathbb{O}_{k,S}^{*\sigma_r}$, $f_j(u_iu)/u_i^e$ lies in a proper subfield of L not containing k. So in this case (1) holds with $S' = S_L$ (and u replaced by u_iu).

Now consider a coset of the form $u_i\mathbb{O}_{k,S}^{*\sigma_r\tau}$. Again, we may assume that for some j and some $\epsilon > 0$, (3) is satisfied for infinitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$. By definition, for $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ we have $\sigma_r(u) = u^{-1}$. Let $e = \deg f_j$. Similar to before, if $f_j(u_ix)$ and $x^ef_j^{\sigma_r}(\sigma_r(u_i)/x)$ are relatively prime in $L[x]$, then it follows that

$$\sum_{v\in M_L} \log^- \max\big\{|f_j(u_iu)|_v\,,\,|f_j^{\sigma_r}(\sigma_r(u_i)/u)|_v\big\}$$

is bounded from below, independent of $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$. This again gives a contradiction with (3) and so $f_j(u_ix)$ and $x^ef_j^{\sigma_r}(\sigma_r(u_i)/x)$ must have a nontrivial common factor over L. Since f_j is irreducible over L, the two polynomials must be equal up to multiplication by a constant. Evaluating at any $x = u' \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ with $f_j(u_iu') \neq 0$, we find that we must have that

$$\frac{f_j(u_ix)}{f_j(u_iu')} = \frac{x^e f_j^{\sigma_r}(\sigma_r(u_i)/x)}{u'^e\sigma_r(f_j(u_iu'))}.$$

Since $(\mathbb{O}_{k,S}^{*\sigma_r\tau})^2$ has finite index in $\mathbb{O}_{k,S}^{*\sigma_r\tau}$, we can find a finitely many elements $u'_1, \ldots, u'_{l'} \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ with $f_j(u_iu'_l) \neq 0, l = 1, \ldots, l'$, and such that for any $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$, there exists some $l \in \{1, \ldots, l'\}$ with $u/u'_l \in (\mathbb{O}_{k,S}^{*\sigma_r\tau})^2$. Let $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ and u'_l chosen as above. Then we have the identity

$$\sigma_r\Big(\Big(\frac{u'_l}{u}\Big)^{e/2}\frac{f_j(u_iu)}{f_j(u_iu'_l)}\Big) = \Big(\frac{u'_l}{u}\Big)^{e/2}\frac{f_j(u_iu)}{f_j(u_iu'_l)}$$

and it follows that $(u_l'/u)^{e/2} f_j(u_i u)/f_j(u_i u_l') \in k'$, the fixed field of σ_r. We can enlarge S_L to a finite set of places S' of L such that $f_j(u_i u_l')$ is an S'-unit for all choices of i, j, and l. Then (1) holds for all $u \in u_i \mathbb{O}_{k,S}^{*\sigma_r \tau}$. □

In the case of a cyclic subgroup of k^* the theorem takes a particularly simple form.

Corollary 2.3. *Let $a \in k^*$. Let S be a finite set of places of k such that a is an S-unit. Assume that for all positive integers m,*

(a) *the element a^m does not lie in a proper subfield of k, and*

(b) *k is not a quadratic extension of a field k' with $N_{k'}^k(a^m) = 1$.*

Let $\epsilon > 0$ and let $f(x) \in \mathbb{O}_k[x]$ satisfy $f(0) \neq 0$. Then, for all but finitely many integers n,

$$N(J(f(a^n))) < H(a^n)^\epsilon.$$

Proof. Suppose that for infinitely many n, $N(J(f(a^n))) \geq H(a^n)^\epsilon$. Then by Theorem 2.1, there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(k/\mathbb{Q})$ and $u \in \mathbb{O}_{k,S}^*$ such that for infinitely many n, a^n lies in a coset of the form $u\mathbb{O}_{k,S}^{*\sigma}$ or $u\mathbb{O}_{k,S}^{*\sigma\tau}$. This implies that for some $m \neq 0$, $a^m \in \mathbb{O}_{k,S}^{*\sigma}$ or $a^m \in \mathbb{O}_{k,S}^{*\sigma\tau}$. In the first case, a^m lies in the proper subfield $k \cap F$ of k, where F is the fixed field of σ. Suppose that $a^m \in \mathbb{O}_{k,S}^{*\sigma\tau}$ and that a^m does not lie in a proper subfield of k. Then $k = \mathbb{Q}(a^m)$. Since $\sigma(a^m) = a^{-m}$, σ restricts to an automorphism of k over $\mathbb{Q}$. Note that $\sigma^2(a^m) = a^m$, so σ is an automorphism of k of order 2. Let k' be the fixed field of σ. Then $[k : k'] = 2$, $\mathrm{Gal}(k/k') = \{\mathrm{id}, \sigma\}$, and $N_{k'}^k(a^m) = a^m \sigma(a^m) = 1$. □

We give an example related to Fibonacci numbers to show the likely necessity of the less obvious condition (b) in Corollary 2.3.

Example 2.4. Let $k = \mathbb{Q}(\sqrt{5})$ and $a = \varphi = \frac{1+\sqrt{5}}{2} \in k^*$. Let S consist of the archimedean places of k and the prime lying above 5. Let $f(x) = x + 1$. For n odd, we have

$$\frac{\varphi^{2n}+1}{\varphi^n\sqrt{5}} = F_n,$$

where F_n is the n-th Fibonacci number. So

$$f(\varphi^{2n})\mathbb{O}_{k,S} = F_n\mathbb{O}_{k,S}.$$

A well-known naïve heuristic argument suggests that there should be infinitely many Fibonacci numbers that are prime and congruent to $\pm 2 \pmod 5$ (so that these primes are inert in k). In this case, there would be an $\epsilon > 0$ and infinitely many values of n such that $N(J(f(\varphi^n))) = N(f(\varphi^n)) > H(\varphi^n)^\epsilon$. This doesn't contradict Corollary 2.3 as $N_{\mathbb{Q}}^k(\varphi^2) = 1$.

We now give a slight reformulation of our results.

Definition 2.5. Let D be an effective divisor on $\mathbb{P}^1$ defined over k and supported on $\mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{G}_m$. Let $a \in k^*$, $a \notin \operatorname{Supp} D$, where $\operatorname{Supp} D$ is the support of D. Let h_D be the absolute logarithmic height associated to D and let $h_D = \sum_{v \in M_k} h_{D,v}$ be a decomposition of h_D into local heights (Weil functions). For a place $v \in M_k$ associated to a prime $\mathfrak{p}$ lying above a prime $p \in \mathbb{Z}$, let $f_v = f_{\mathfrak{p}} = [\mathbb{O}_k/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Set $f_v = 1$ if $v|\infty$. We define the degree-one height of a with respect to k and D by

$$h_{D,\deg_1(k)}(a) = \sum_{\substack{v \in M_k \\ f_v = 1}} h_{D,v}(a).$$

Similarly, we define

$$h_{D,\deg_{>1}(k)}(a) = \sum_{\substack{v \in M_k \\ f_v > 1}} h_{D,v}(a).$$

Note that

$$h_D(a) = h_{D,\deg_1(k)}(a) + h_{D,\deg_{>1}(k)}(a)$$

and by standard properties of heights, $h_{D,\deg_1(k)}$ and $h_{D,\deg_{>1}(k)}$ depend on the choice of h_D and the local height functions only up to $O(1)$.

Corollary 2.6. *Let D be an effective divisor on $\mathbb{P}^1$ defined over k and supported on $\mathbb{P}^1 \setminus \{0, \infty\}$. Let $f(x) \in \mathbb{O}_k[x]$ be a polynomial defining D with monic irreducible factors $f_1, \ldots, f_n$ over L. Let $\epsilon > 0$. Then there exists a finite set of places S' of L such that for every $u \in \mathbb{O}_{k,S}^*$ either*

(a) $$h_{D,\deg_{>1}(k)}(u) < \epsilon h_D(u)$$

or

(b) $$f_i(u)\mathbb{O}_{L,S'} = \alpha \mathbb{O}_{L,S'}$$

for some i and some α that lies in a proper subfield of L not containing k.

All but finitely many elements not satisfying (a) are again contained in a set T as in Theorem 2.1. There is also a similar reformulation of Corollary 2.3 in terms of $h_{D,\deg_{>1}(k)}(u)$.

Lemma 2.7. *Let D be as in Corollary 2.6. For any finite set of places $S' \subset M_k$ and any $\epsilon > 0$,*

$$\sum_{v \in S'} h_{D,v}(u) < \epsilon h(u) + O(1) \tag{4}$$

for all $u \in \mathbb{O}_{k,S}^*$.

Proof. It suffices to show this for D a point (not equal to 0 or ∞) and $S' \supset S$. Let $E = 0 + \infty$. Since u is an S'-unit, we have

$$\sum_{v \in S'} h_{E,v}(u) = 2h(u) + O(1).$$

By Roth's theorem,

$$\sum_{v\in S'} h_{D+E,v}(u) = \sum_{v\in S'} h_{D,v}(u) + 2h(u) + O(1) < (2+\epsilon)h(u) + O(1),$$

which gives (4). □

In particular, it follows from Lemma 2.7 that Corollary 2.6 remains true if we add finitely many local heights to $h_{D,\deg_{>1}(k)}$ (e.g., all the archimedean ones).

Proof of Corollary 2.6. We may take as local height functions associated to D the functions

$$h_{D,v}(a) = -\log^{-}|f(a)|_v, \quad v \in M_k.$$

Using Theorem 2.1 and Lemma 2.7, we can write, for all $u \in \mathbb{O}^*_{k,S}$,

$$\begin{aligned} h_{D,\deg_{>1}(k)}(u) &= \sum_{\substack{v\in M_k\\ f_v>1}} h_{D,v}(u) = -\sum_{\substack{v\in M_k\setminus S\\ f_v>1}} \log^{-}|f(u)|_v + \sum_{\substack{v\in S\\ f_v>1}} h_{D,v}(u) \\ &= \frac{1}{[k:\mathbb{Q}]}\log N(J(f(u))) + \sum_{\substack{v\in S\\ f_v>1}} h_{D,v}(u) \\ &< \epsilon h(u) + O(1), \end{aligned}$$

□

3. Elliptic curves

Theorem 2.1 has a conjectural analogue for elliptic curves, following from a conjectural analogue of Lemma 2.2.

Conjecture 3.1 (Vojta). *Let E be an elliptic curve defined over a number field k. Let h be an ample height function on E. Let $B \subset E(\bar{k}) \times E(\bar{k})$ be a finite set of points with B defined over k. Let $\pi : X \to E \times E$ be the morphism obtained by blowing up the points in B and let Y be the exceptional divisor of π. Let h_Y be a logarithmic height function with respect to Y. Let $\epsilon > 0$. There exists a proper Zariski closed subset $Z(\epsilon)$ of X such that for every $(P, Q) \in (E\times E)(k) - \pi(Z(\epsilon))$, we have*

$$h_Y(\pi^{-1}(P, Q)) \le \epsilon(h(P) + h(Q)) + O(1).$$

(Conjecture 3.1 is a special case of a much more general set of conjectures made by Vojta [1987; 2011].)

This enables us to deduce an analogue of Theorem 2.1 for elliptic curves. As in the previous section, it will be convenient to list the notation used:

k	Fixed number field
ℓ/k	Fixed nontrivial extension of k
L	Galois closure of ℓ over k
$\mathrm{Gal}(L/k)$	Galois group of L over k
$\mathbb{O}_k$	Ring of integers of k
S	Fixed finite set of places of L, consisting of the archimedean places of L and the places of L ramified over k
$\mathbb{O}_{L,S}$	The ring of S-integers of L
E	Fixed elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in \mathbb{O}_k$
$E(\ell)^{\nu\sigma}$	For $\nu \in \mathrm{Aut}(E)$ and $\sigma \in \mathrm{Gal}(L/k)$, the subgroup of points $x \in E(\ell)$ satisfying $\nu\sigma(x) = x$
D	Fixed effective and nontrivial ℓ-rational divisor on E
$D_1, \ldots, D_N$	The irreducible components of D over L
$I_D(P)$	Ideal associated to D and P (see Definition 3.2)
$J_D(P)$	The smallest divisor ideal of $I_D(P)$ supported on primes $\mathfrak{p}$ of $\mathbb{O}_\ell$ with $[\mathbb{O}_\ell/\mathfrak{p} : \mathbb{O}_k/(\mathbb{O}_k \cap \mathfrak{p})] > 1$
$N(I)$	Absolute norm of an ideal I of $\mathbb{O}_\ell$
$H_D(P)$	Multiplicative height function on E corresponding to D
$h_D(P)$	Logarithm of $H(P)$: $h_D(P) = \log H_D(P)$.

Definition 3.2. Let $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{O}_k$, be an elliptic curve. Let L be a number field containing k, and let P, Q be distinct elements of $E(L)$. Let $P - Q = (x_0, y_0) \in E(L)$. Define

$$I_Q(P) = \prod_{\mathfrak{p} \subset \mathbb{O}_L} \mathfrak{p}^{\max\{-\frac{1}{2}\operatorname{ord}_{\mathfrak{p}} x_0, 0\}},$$

where $\mathfrak{p}$ runs over all (finite) primes of $\mathbb{O}_L$ (this is well-defined, independent of L, if we identify ideals $\mathfrak{a} \subset \mathbb{O}_L$ and $\mathfrak{a}\mathbb{O}_{L'}$, when $L \subset L'$). If $D = \sum_{i=1}^n Q_i$, $Q_i \in E(\bar{k})$, is a nontrivial effective divisor on E, then for $P \notin \mathrm{Supp}(D)$, we define

$$I_D(P) = \prod_{i=1}^n I_{Q_i}(P).$$

Definition 3.3. Let $P \in E(\ell)$, $P \notin \mathrm{Supp}(D)$. We define the height of P with respect to degree-one primes of ℓ/k by

$$h_{D,\deg_1(\ell/k)}(P) = \sum_{v \in M_k} \sum_{\substack{w \in M_\ell \\ w \mid v \\ f_{w/v} = 1}} h_{D,w}(P),$$

where $h_{D,w}$ denotes a local Weil height with respect to D and w and $f_{w/v}$ is the inertia degree of w over v. Similarly, define

$$h_{D,\deg_{>1}(\ell/k)}(P)=\sum_{v\in M_k}\sum_{\substack{w\in M_\ell\\ w|v\\ f_{w/v}>1}} h_{D,w}(P).$$

Note that, as in the previous section, we have

$$h_{D,\deg_1(\ell/k)}(P)+h_{D,\deg_{>1}(\ell/k)}(P)=h_D(P)+O(1).$$

For $P\in E(\ell)$ and D a divisor on E defined over ℓ, the norm $N(I_D(P))$ is essentially just the nonarchimedean part of the (relative) height $H_{D,\ell}(P)=H_D(P)^{[\ell:\mathbb{Q}]}$ and $\log N(J_D(P))=[\ell:\mathbb{Q}]\,h_{D,\deg_{>1}(\ell/k)}(P)$ (up to $O(1)$). We will assume the local heights are chosen so that this last statement is an equality.

We can now state the following theorem, which in the simplest case where ℓ/k is Galois, says, roughly, that the height of P with respect to D is "mostly" supported on the degree one primes of ℓ/k, unless the ideal $I_D(P)$ is coming from a proper subfield of ℓ. Note that the fields ℓ and k here play the roles of k and $\mathbb{Q}$, respectively, from the analogous Theorem 2.1.

Theorem 3.4. *Let $\epsilon>0$. Assume that Conjecture 3.1 holds. Then, for every $P\in E(\ell)$, either*

(a) $$\frac{1}{[\ell:\mathbb{Q}]}\log N(J_D(P))=h_{D,\deg_{>1}(\ell/k)}(P)<\epsilon h_D(P),$$

or

(b) $$I_{D_i}(P)\mathcal{O}_{L,S}=\mathfrak{a}\mathcal{O}_{L,S}$$

for some i and some ideal $\mathfrak{a}\subset\mathcal{O}_{k'}$, where k' is a proper subfield of L not containing ℓ (in particular, if ℓ/k is Galois, $\mathfrak{a}$ is contained in a proper subfield of ℓ).

The set of points in $E(\ell)$ not satisfying (a) is contained in a finite union of cosets in $E(\ell)$ of the form

$$T=\bigcup_{i=1}^m P_i+E(\ell)^{\nu_i\sigma_i},$$

where $P_i\in E(\ell)$, $\sigma_i\in\mathrm{Gal}(L/k)\setminus\mathrm{Gal}(L/\ell)$, and $\nu_i\in\mathrm{Aut}(E)$ for $i=1,\dots,m$.

Proof. Let D_{red} be the reduced divisor associated to D. Then, for some positive integer c, $D<cD_{\mathrm{red}}$ and we have $h_D<ch_{D_{\mathrm{red}}}+O(1)$ and $h_{D,\deg_{>1}(\ell/k)}<ch_{D_{\mathrm{red}},\deg_{>1}(\ell/k)}+O(1)$. So without loss of generality we may assume that D is a reduced divisor. Let

$$U=\{P\in E(\ell)\mid h_{D,\deg_{>1}(\ell/k)}(P)\ge\epsilon h_D(P)\}.$$

Let L be a Galois closure of ℓ/k. Let $w' \in M_L$ lie above $w \in M_\ell$ and $v \in M_k$. As in the proof of Theorem 2.1, if $f_{w/v} > 1$, then there exists $\sigma \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$ such that $\sigma(w') = w'$. Let $\mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell) = \{\sigma_1, \ldots, \sigma_m\}$. For $i = 1, \ldots, m$, let

$$h^{(i)}_{D,\deg_{>1}(L/k)}(P) = \sum_{v \in M_k} \sum_{\substack{w \in M_L \\ w|v,\ f_{w/v}>1 \\ \sigma_i(w)=w}} h_{D,w}(P).$$

Then

$$h_{D,\deg_{>1}(\ell/k)}(P) \leq \sum_{i=1}^{m} h^{(i)}_{D,\deg_{>1}(L/k)}(P).$$

Let

$$U_i = \left\{ P \in U \;\middle|\; h^{(i)}_{D,\deg_{>1}(L/k)}(P) \geq \frac{\epsilon}{m} h_D(P) \right\}.$$

Then $U \subset \bigcup_{i=1}^{m} U_i$. Let $r \in \{1, \ldots, m\}$. If $w \in M_L$ and $\sigma_r(w) = w$, then $h_{D,w}(P) = h_{\sigma_r(D),w}(\sigma_r(P))$ and so

$$\min\{h_{D,w}(P), h_{\sigma_r(D),w}(\sigma_r(P))\} = h_{D,w}(P).$$

Let $\pi : X \to E \times E$ be the morphism obtained by blowing up the points in

$$D \times \sigma_r(D) \subset E \times E$$

and let Y be the exceptional divisor of π. By well-known properties of heights, for $(P, Q) \notin D \times \sigma_r(D)$ and $w \in M_L$, we can choose

$$h_{Y,w}(\pi^{-1}(P, Q)) = \min\{h_{D,w}(P), h_{\sigma_r(D),w}(Q)\}.$$

Let $V_r = \{(P, \sigma_r(P)) \mid P \in U_r\}$. It follows that for $(P, \sigma_r(P)) \in V_r$, we have

$$\begin{aligned} h_Y(\pi^{-1}(P, \sigma_r(P))) &\geq h^{(r)}_{D,\deg_{>1}(L/k)}(P) \geq \frac{\epsilon}{m} h_D(P) \\ &> \frac{\epsilon}{2m}(h(P) + h(\sigma_r(P)) + O(1). \end{aligned}$$

Then by Conjecture 3.1 V_r is contained in a proper Zariski closed subset of $E \times E$. If V_r is a finite set, then U_r is contained in a set T as in the theorem. Otherwise, let C be a positive-dimensional component of the Zariski closure of V_r. Then C is a curve with infinitely many rational points on it. By Faltings' theorem, C is a translate of a one-dimensional abelian subvariety E' of $E \times E$.

Any irreducible one-dimensional abelian subvariety of $E \times E$ must be an elliptic curve isogenous to E, via projection onto E. Since E' is clearly not a fiber of either of the two projection maps, there are two isogenies $\phi, \psi : E' \to E$ induced by the two projection maps, with dual isogenies $\hat{\phi}$ and $\hat{\psi}$ from E to E'. If $R = (P, Q) \in E' \subset E \times E$, then $\hat{\phi}\phi(R) = \hat{\phi}(P) = (\deg \hat{\phi})R$ and similarly $\hat{\psi}(Q) = (\deg \hat{\psi})R$.

Thus, E' is contained in the set $\{(P,Q) \in E \times E \mid (\deg \hat{\psi})\hat{\phi}(P) = (\deg \hat{\phi})\hat{\psi}(Q)\}$. Composing with an isogeny to E we find that there are nonzero endomorphisms f and g of E such that $E' \subset \{(P,Q) \in E \times E \mid f(P) = g(Q)\}$. Note that if $(P_0, \sigma_r(P_0)), (P, \sigma_r(P)) \in V_r \cap C$ then $(P - P_0, \sigma_r(P - P_0)) \in E'$. It follows that there are points of the form $(P, \sigma_r(P)) \in E'$ with $P \in E(\ell)$ such that $f(P) = g(\sigma_r(P))$.

Let $K = \mathrm{End}_L(E) \otimes \mathbb{Q}$, where $\mathrm{End}_L(E)$ is the endomorphism ring of E over L. Then σ_r is an element of a finite group acting on the finite-dimensional K-vector space $V = E(L) \otimes_{\mathrm{End}_L(E)} K$. Thus, the eigenvalues of the action of σ_r must be roots of unity. But from the above, f/g is an eigenvalue of σ_r. So we deduce that $f/g \in K$ is a root of unity. Since K is contained in a quadratic extension of $\mathbb{Q}$, this means that $f/g \in \{\pm 1, \pm i, \pm\gamma, \pm\gamma^2\}$, where γ denotes a primitive sixth root of unity. Write $g = \nu f$. Composing both sides with the dual endomorphism to f, we may assume that $f = m$, where m is a positive integer. Then, for $(P, \sigma_r(P)), (P_0, \sigma_r(P_0)) \in V_r \cap C$, we have $m(P - P_0) = \nu\sigma_r(m(P - P_0))$. This implies that U_r is contained in finitely many cosets of the form $P_i + E(\ell)^{\nu_i \sigma_r}$ in $E(\ell)$, where $P_i \in E(\ell)$ and $\nu_i \in \mathrm{Aut}(E)$. So the set of points in $E(\ell)$ not satisfying (a) is contained in a set T as in the theorem.

We now show that the set of points in the set T not satisfying condition (a) satisfies condition (b). Let $D_1, \ldots, D_N$ be the irreducible components of D over L. Consider a coset in $E(\ell)$ of the form $P_r + E(\ell)^{\nu_r \sigma_r}$, where $P_r \in E(\ell)$, $\nu_r \in \mathrm{Aut}(E)$, and $\sigma_r \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$. From the first part of the proof, we need only consider cosets such that for some i, some $\epsilon > 0$, and infinitely many elements $P \in E(\ell)^{\nu_r \sigma_r}$, we have

$$\sum_{w \in M_L} \min\{h_{D_i,w}(P + P_r), h_{\sigma_r(D_i),w}(\sigma_r(P + P_r))\} > \epsilon h(P).$$

Let $\phi : E \to E$ be the morphism $\phi(P) = \nu_r^{-1} P + \sigma_r(P_r)$. Since $\sigma_r(P + P_r) = \nu_r^{-1} P + \sigma_r(P_r)$ for $P \in E(\ell)^{\nu_r \sigma_r}$, we have (up to $O(1)$)

$$h_{\sigma_r(D_i),w}(\sigma_r(P + P_r)) = h_{\sigma_r(D_i),w}(\phi(P)) = h_{\phi^*\sigma_r(D_i),w}(P).$$

Let τ be translation by P_r. So $h_{D_i,w}(P + P_r) = h_{\tau^* D_i,w}(P) + O(1)$. So for infinitely many $P \in E(\ell)$,

$$\sum_{w \in M_L} \min\{h_{\tau^* D_i,w}(P), h_{\phi^*\sigma_r(D_i),w}(P)\} > \epsilon h(P). \tag{5}$$

If $\tau^* D_i$ and $\phi^*\sigma_r(D_i)$ have empty intersection, then as is well known,

$$\sum_{w \in M_L} \min\{h_{\tau^* D_i,w}(P), h_{\phi^*\sigma_r(D_i),w}(P)\}$$

is bounded independent of P, contradicting (5). So $\tau^* D_i \cap \phi^* \sigma_r(D_i) \neq \varnothing$. Since D_i is irreducible over L, this implies that $\tau^* D_i = \phi^* \sigma_r(D_i)$.

It follows from the definition that for any translation τ_0 and any automorphism $\nu \in \mathrm{Aut}(E)$, $I_D(\tau_0(P)) = I_{\tau_0^* D}(P)$ and $I_D(\nu P) = I_{\nu^* D}(P)$. This implies that for all $P \in E(\ell)^{\nu_r \sigma_r}$,

$$\begin{aligned}\sigma_r(I_{D_i}(P+P_r)) = I_{\sigma_r(D_i)}(\sigma_r(P)+\sigma_r(P_r)) &= I_{\sigma_r(D_i)}(\phi(P)) = I_{\phi^*\sigma_r(D_i)}(P)\\ &= I_{\tau^* D_i}(P)\\ &= I_{D_i}(P+P_r).\end{aligned}$$

So σ_r fixes the ideal $I_{D_i}(P_r + P)$, $P_r + P \in P_r + E(\ell)^{\nu_r \sigma_r}$, which implies that $I_{D_i}(P+P_r)\mathbb{O}_{L,S} = \mathfrak{a}\mathbb{O}_{L,S}$ for some ideal $\mathfrak{a}$ of $\mathbb{O}_{k'}$, where k' is the fixed field of σ_r. □

If we restrict to cyclic subgroups of $E(\ell)$, we obtain the following simpler version of Theorem 3.4.

Corollary 3.5. *Let $P \in E(\ell)$ and $\epsilon > 0$. If Conjecture 3.1 holds, then either*

$$h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$$

for all but finitely many integers n, or there exists a proper subfield $k' \subsetneq \ell$ of ℓ, a positive integer m, an elliptic curve E'/k', and an isomorphism $\phi : E \to E'$ over ℓ such that $\phi(mP)$ is a k'-rational point on E'.

Proof. Suppose that for infinitely many n, $h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$. It follows from Theorem 3.4 that for some $m > 0$, $\sigma \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$, and $\nu \in \mathrm{Aut}(E)$, we have $mP \in E(\ell)^{\nu^{-1}\sigma}$, or $\sigma(mP) = \nu mP$. From this it follows that mP is a point on a twist of E, defined over $k' \cap \ell$, where k' is the fixed field of σ. □

At the time of writing, Conjecture 3.1 is known only in the following special case. See [McKinnon 2003] for a proof, and [Silverman 2005] for a discussion of the implications of Vojta's conjecture in this context.

Theorem 3.6 [McKinnon 2003]. *Let E be an elliptic curve over a number field ℓ. Let $R = \mathrm{End}_\ell(E)$. Let M be a cyclic R-submodule of $E(\ell)$. Then Conjecture 3.1 holds for $(P, Q) \in M \times M \subset (E \times E)(\ell)$; that is, in the notation of Conjecture 3.1, there exists a proper Zariski closed subset $Z(\epsilon)$ of X such that for every $(P, Q) \in M \times M - \pi(Z(\epsilon))$, we have*

$$h_Y(\pi^{-1}(P, Q)) \leq \epsilon(h(P) + h(Q)) + O(1),$$

where h_Y is a logarithmic height function associated to the exceptional divisor on the blowup X of $E \times E$ at a finite set of points and h is any fixed ample logarithmic height on E.

Theorem 3.7. *Let E be an elliptic curve over a number field k with complex multiplication. Let ℓ be the compositum of k with the imaginary quadratic field* $\mathrm{End}_{\bar{k}}(E) \otimes \mathbb{Q}$. *Let D be a nontrivial effective divisor on E defined over ℓ. Let $P \in E(\ell)$ and $\epsilon > 0$. Then either*

$$h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$$

for all but finitely many $n > 0$, or there exists a positive integer m, an elliptic curve E'/k, and an isomorphism $\phi : E \to E'$ over ℓ such that $\phi(mP)$ is a k-rational point on E'.

Proof. If $\ell = k$ then the theorem is vacuous. So suppose that ℓ is a quadratic extension of k. Let $R = \mathrm{End}_{\bar{k}}(E)$. First, we note that $R[E(k)]$ has finite index in $E(\ell)$. Indeed, as is well-known [Silverman 1992, Exercise X-10.16], we have $\mathrm{rk}\, E(\ell) = \mathrm{rk}\, E(k) + \mathrm{rk}\, E'(k)$, where E' is a quadratic twist of E over ℓ. If $\ell = k(\sqrt{N})$, $N \in \mathbb{Z}$, then any element $n\sqrt{N} \in R$, with n a positive integer, induces an isogeny (over k) between E and a quadratic twist E' of E over ℓ. Thus, $\mathrm{rk}\, E(k) = \mathrm{rk}\, E'(k)$ and we have $\mathrm{rk}\, E(\ell) = 2\, \mathrm{rk}\, E(k) = \mathrm{rk}\, R[E(k)]$.

Next, we claim that Theorem 3.6 actually holds under the slightly weaker assumption that M contains a cyclic R-submodule M' of finite index m. Indeed, one easily reduces to considering the case where X is the blow-up of $E \times E$ at the origin $(\mathbb{O}, \mathbb{O})$ and Y is the exceptional divisor. The claim then follows by applying Theorem 3.6 to M' and from the facts

$$h_Y(\pi^{-1}(P, Q)) \le h_Y(\pi^{-1}(mP, mQ)) + O(1),$$

$(P, Q) \neq (\mathbb{O}, \mathbb{O})$, and $h(mP) = m^2 h(P) + O(1)$.

Let m be the index of $R[E(k)]$ in $E(\ell)$. Let $P \in E(\ell)$. Then we have $mP = \phi(Q)$, for some $Q \in E(k)$ and some $\phi \in R$. Let σ be the unique nonidentity element of $\mathrm{Gal}(\ell/k)$. Then $m\sigma(P) = \sigma(mP) = \sigma(\phi(Q)) = (\sigma\phi)(Q)$, so mP and $m\sigma(P)$ both belong to the cyclic R-submodule RQ of $E(\ell)$ generated by Q. So RQ has finite index in the subgroup of $E(\ell)$ generated by RQ, P, and $\sigma(P)$. Then by our earlier claim, Conjecture 3.1 holds for the points $(nP, n\sigma(P)) \in (E \times E)(\ell)$, $n \in \mathbb{Z}$. But now the same proof as in Theorem 3.4 and Corollary 3.5 works, completing the proof. □

References

[Corvaja and Zannier 2005] P. Corvaja and U. Zannier, "A lower bound for the height of a rational function at S-unit points", *Monatsh. Math.* **144**:3 (2005), 203–224. MR 2005k:11140 Zbl 1086.11035

[McKinnon 2003] D. McKinnon, "Vojta's main conjecture for blowup surfaces", *Proc. Amer. Math. Soc.* **131**:1 (2003), 1–12. MR 2003g:11071 Zbl 1022.11027

[Silverman 1992] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1992. MR 95m:11054

[Silverman 2005] J. H. Silverman, "Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups", *Monatsh. Math.* **145**:4 (2005), 333–350. MR 2006e:11087 Zbl 1197.11070

[Vojta 1987] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics **1239**, Springer, Berlin, 1987. MR 91k:11049 Zbl 0609.14011

[Vojta 2011] P. Vojta, "Diophantine approximation and Nevanlinna theory", pp. 111–224 in *Arithmetic geometry* (Cetraro, 2007), edited by P. Corvaja and C. Gasbarri, Lecture Notes in Mathematics **2009**, Springer, Berlin, 2011. MR 2012i:11076 Zbl 05882118

Communicated by Bjorn Poonen
Received 2011-06-02 Revised 2011-10-18 Accepted 2011-12-10

adlevin@math.msu.edu *Department of Mathematics, Michigan State University, East Lansing, MI 48824, United States*

dmckinnon@math.uwaterloo.ca *Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2T 2M2, Canada*

Algebra & Number Theory

msp.berkeley.edu/ant

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2012 is US $175/year for the electronic version, and $275/year (+$40 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://msp.org/
A NON-PROFIT CORPORATION
Typeset in LaTeX

Algebra & Number Theory

Volume 6 No. 6 2012