Monatsh. Math. 145, 333–350 (2005)
DOI 10.1007/s00605-005-0299-y

Monatshefte für
Mathematik
Printed in Austria

Generalized Greatest Common Divisors, Divisibility Sequences, and Vojta's Conjecture for Blowups

By

Joseph H. Silverman

Brown University, Providence, RI, USA

Communicated by W. M. Schmidt

Received February 2, 2004; accepted in revised form November 17, 2004
Published online April 6, 2005

Abstract. We apply Vojta's conjecture to blowups and deduce a number of deep statements regarding (generalized) greatest common divisors on varieties, in particular on projective space and on abelian varieties. Special cases of these statements generalize earlier results and conjectures. We also discuss the relationship between generalized greatest common divisors and the divisibility sequences attached to algebraic groups, and we apply Vojta's conjecture to obtain a strong bound on the divisibility sequences attached to abelian varieties of dimension at least two.

2000 Mathematics Subject Classification: 11G35; 11D75, 11J25, 14G25, 14J20
Key words: Greatest common divisor, divisibility sequence, algebraic group, Vojta conjecture

Introduction

Bugeaud, Corvaja, and Zannier [3] recently proved that if a and b are multiplicatively independent integers, then for every $\epsilon > 0$ there is a constant $N = N(a, b, \epsilon)$ so that

$$\gcd(a^n - 1, b^n - 1) \leqslant 2^{\epsilon n} \quad \text{for all } n \geqslant N. \tag{1}$$

The proof of this beautiful, but innocuous looking, inequality requires an ingenious application of Schmidt's Subspace Theorem [15]. Corvaja and Zannier [5, Proposition 4] generalize (1) by replacing a^n and b^n with arbitrary elements from a fixed finitely generated subgroup of $\bar{\mathbb{Q}}^*$. For ease of exposition, we state their result over $\mathbb{Q}$.

Theorem 1 (Corvaja and Zannier [5]). *Let S be a finite set of rational primes and let $\epsilon > 0$. There is a finite set $Z = Z(S, \epsilon) \subset \mathbb{Z}^2$ so that all $\alpha, \beta \in \mathbb{Z}_S^* \cap \mathbb{Z}$ satisfy one of the following three conditions*:

(1) $(\alpha, \beta) \in Z$.
(2) $\alpha^m = \beta^n$ *for some* (m, n) *satisfying* $1 \leqslant \max\{m, n\} \leqslant \epsilon^{-1}$.
(3) $\gcd(\alpha - 1, \beta - 1) \leqslant \max(|\alpha|, |\beta|)^{\epsilon}$.

The author's research supported by NSA grant H98230-04-1-0064.

In other words, if $\alpha, \beta \in \mathbb{Z}$ are S-units, then

$$\gcd(\alpha - 1, \beta - 1) \leqslant \max(|\alpha|, |\beta|)^{\epsilon}$$

except for some obvious families of exceptions together with a finite number of additional exceptions. Analogous statements for elliptic curves and/or over function fields have been studied by a number of authors [1, 14, 20, 21].

The purpose of this note is to explain how Vojta's Conjecture [25, Conjecture 3.4.3] applied to varieties blown up along smooth subvarieties leads to a very general statement about greatest common divisors that encompasses many known results and previous conjectures. Thus although we do not prove unconditional results in this paper, we hope that the application of Vojta's conjecture will help to put the problem of gcd bounds into a general context, while at the same time suggesting precise statements whose proofs may be possible using current techniques from Diophantine approximation and arithmetic geometry. (See also McKinnon's paper [14] for a discussion of Vojta's conjecture applied to certain blowups.)

We begin in the Section 1 by describing three special cases of our main theorem. These serve to motivate our general result and to justify the notation that is needed later. We next in Section 2 set notation and explain how a generalized concept of greatest common divisor is naturally formulated in terms of the height of points on blowup varieties with respect to the exceptional divisor of the blowup. Section 3 states Vojta's conjecture, followed in Section 4 by our main result (Theorem 6) in which we apply Vojta's conjecture to a blowup variety, making use of the well-known relation between the canonical bundle on a variety and on its blowup. In Section 5 we apply our main theorem to prove the three special cases from Section 1, including some additional arguments to pin down the exceptional sets more precisely. Section 6 takes up the question of divisibility sequences, which are sequences $(a_n)_{n \geqslant 1}$ satisfying $m|n \Rightarrow a_m|a_n$. We are especially interested in divisibility sequences associated to algebraic groups, or more precisely, to group schemes over $\mathbb{Z}$. We show that these geometric divisibility sequences are closely related to generalized greatest common divisors and apply Vojta's conjecture to the divisibility sequences attached to abelian varieties of dimension at least 2. Finally, in Section 7, we make a few final remarks and pose some questions.

1. Three Special Cases Over $\mathbb{Q}$

In this section we describe three special cases of our main theorem. These generalize earlier results and conjectures appearing in the literature. In order to avoid excessive notation, we restrict ourselves to working over $\mathbb{Q}$. All results are conditional on the validity of Vojta's conjecture. We refer the reader to Section 3 (Conjecture 5) or to Vojta's original monograph [25, Conjecture 3.4.3] for the statement of Vojta's conjecture. In order to state our first result, we need one piece of notation.

Definition 1. Let S be a finite set of rational primes. For any nonzero integer $x \in \mathbb{Z}$, we write $|x|'_S$ for the largest divisor of x that is not divisible by any of the primes in S, i.e.

$$|x|'_S = |x| \prod_{p \in S} |x|_p.$$

Informally, we call $|x|'_S$ the "prime-to-S" part of x. In particular, x is an S-unit if and only if $|x|'_S = 1$.

Our first result deals with $\mathbb{P}^n$ blown up along a smooth subvariety.

Theorem 2. *Fix a finite set of rational primes S. Let $f_1, f_2, \ldots, f_t \in \mathbb{Z}[X_0, \ldots, X_n]$ be homogeneous polynomials so that the set of zeros*

$$V = \{f_1 = f_2 = \cdots = f_t = 0\} \subset \mathbb{P}^n$$

is a smooth variety, and assume further that V has transversal intersection with the union of the coordinate hyperplanes $\bigcup_{i=0}^n \{X_i = 0\}$. Let $r = n - \dim(V)$ denote the codimension of V in $\mathbb{P}^n$.

Assume that $r \geqslant 2$ and that Vojta's conjecture is true (for $\mathbb{P}^n$ blown up along V). Fix $\epsilon > 0$. Then there is a homogeneous polynomial $0 \neq g \in \mathbb{Z}[X_0, \ldots, X_n]$, depending on $f_1, \ldots, f_t$ and ϵ, and a constant $\delta > 0$, depending on $f_1, \ldots, f_t$, so that every

$$\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} \quad \textit{with } \gcd(x_0, \ldots, x_n) = 1$$

satisfies either

(1) $g(\mathbf{x}) = 0$, *or*
(2) $\gcd(f_1(\mathbf{x}), \ldots, f_t(\mathbf{x})) \leqslant \max\{|x_0|, \ldots, |x_n|\}^{\epsilon} \cdot \left(|x_0 x_1 \cdots x_n|'_S\right)^{1/(r-1+\delta\epsilon)}$.

Example 1. We apply Theorem 2 to $\mathbb{P}^2$ with $f_1 = X_1 - X_0$ and $f_2 = X_2 - X_0$. Then V is a single point and $r = 2$, so the theorem says that off of a one dimensional exceptional set we have

$$\gcd(x_1 - x_0, x_2 - x_0) \leqslant \max\{|x_0|, |x_1|, |x_2|\}^{\epsilon} \cdot \left(|x_0 x_1 x_2|'_S\right)^{1/(1+\delta\epsilon)}. \tag{2}$$

In particular, suppose that we take $x_0 = 1$ and restrict x_1 and x_2 to be S-units, as in Theorem 1. Then $|x_0 x_1 x_2|'_S = 1$, so (2) becomes

$$\gcd(x_1 - 1, x_2 - 1) \leqslant \max\{|x_1|, |x_2|\}^{\epsilon}$$

and we recover Theorem 1, albeit conditional on Vojta's conjecture.[1] Thus Vojta's conjecture implies a natural generalization of Theorem 1 in which we remove the restriction that α and β be S-units and replace condition (3) of Theorem 1 with the inequality

$$\gcd(\alpha - 1, \beta - 1) \leqslant \max\{|\alpha|, |\beta|\}^{\epsilon} \cdot \left(|\alpha\beta|'_S\right)^{1/(1+\delta\epsilon)}. \tag{3}$$

It would be quite interesting to give an unconditional proof of this generalization. We also remark that a closer analysis of this special case of Theorem 2 shows that (3) should be valid for any $\delta < 1$.

[1] Theorem 1 also includes a description of the exceptional set, but once one knows that the exceptional set is a union of curves, it is not hard to recover the full result.

Our second example deals with elliptic curves and has applications to the theory of elliptic divisibility sequences.

Theorem 3. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation, and for any nonzero point $P=(x_P,y_P)\in E(\mathbb{Q})$, write $x_P=A_P/D_P^2$ as a fraction in lowest terms with $D_P>0$. Also let $H(P)=H(x_P)=\max\{|A_P|,|D_P^2|\}$ be the usual Weil height on E.*

Assume that Vojta's conjecture is true (for E^2 blown up at (O,O)). Then for every $\epsilon>0$ there is a proper closed subvariety $Z=Z_\epsilon(E)\subset E^2$ so that

$$\gcd(D_P,D_Q)\leqslant (H(P)\cdot H(Q))^\epsilon \quad \textit{for all } (P,Q)\in E^2(\mathbb{Q})\setminus Z.$$

The exceptional set Z consists of a finite number of translates of proper algebraic subgroups of E^2. If E does not have CM, then we can say more precisely that Z is a finite union of translates of the subgroups

$$\{(mT,nT)\in E^2 : T\in E\} \quad \textit{with } (m,n)\in\mathbb{Z}^2 \textit{ satisfying } m^2+n^2\leqslant \frac{1}{2\epsilon}.$$

(A similar statement holds if E has CM, with m and n replaced by more general isogenies.)

Example 2. Let $E/\mathbb{Q}$ be an elliptic curve and $P\in E(\mathbb{Q})$ a point of infinite order. With notation as in Theorem 3, the *elliptic divisibility sequence* (EDS) associated to P is the sequence of integers $(D_{nP})_{n\geqslant 1}$. (For further information about elliptic divisibility sequences, including a not-quite-equivalent alternative definition, see [6–8, 14, 17, 21–24, 26, 27].) These sequences have the property that if $m|n$, then $D_{mP}|D_{nP}$, whence their name. Now let P and Q be independent points in $E(\mathbb{Q})$. Then Theorem 3 implies that there is a constant $C=C_\epsilon(E,P,Q)$ so that

$$\gcd(D_{mP},D_{nQ})\leqslant C\max\{D_{mP},D_{nQ}\}^\epsilon \quad \text{for all } m,n\geqslant 1.$$

Note that since P and Q are independent, there are only finitely many multiples (mP,nQ) that lie on any fixed curve in E^2. We are also using Siegel's theorem [18, IX.3.3], which says that $2\log D_{nP}\sim h(nP)$ as $n\to\infty$.

Our final example is the amusing observation that Vojta's conjecture allows us to mix greatest common divisors on a multiplicative group with those on an elliptic curve. The following result, although far from the most general, gives a flavor of what can be proven. Again, an unconditional proof would be quite interesting.

Theorem 4. *Let $E/\mathbb{Q}$ be an elliptic curve and let S be a finite set of rational primes. Assume that Vojta's conjecture is true for $E\times\mathbb{P}^1$ blown up at $(O,1)$. Then for every $\epsilon>0$ there is a constant $C=C(E,S,\epsilon)$ so that*

$$\gcd(D_Q,b-1)\leqslant C\cdot\max\{D_Q,H(b)\}^\epsilon \quad \textit{for all } Q\in E(\mathbb{Q}) \textit{ and } b\in\mathbb{Z}_S^*.$$

(By convention, we define the greatest common divisor of two rational numbers to be the greatest common divisor of their numerators.) In particular, if $P\in E(\mathbb{Q})$ is a point of infinite order and if $a\geqslant 2$ is an integer, then

$$\gcd(D_{nP},a^m-1)\leqslant \max\{D_{nP},a^m\}^\epsilon$$

provided that $\max\{m,n\}$ *is sufficiently large.*

2. Generalized GCD's and Blowups

We set the following notation, which will remain fixed throughout this paper. For definitions and normalizations related to absolute values and heights, see [12, Part B] or [13, Chapters 2, 3].

- k a number field.
- M_k a complete set of absolute values on k. For $v \in M_k$, we define $v^+(\alpha) = \max\{v(\alpha), 0\}$, and we assume that the absolute values are normalized so that $h(\alpha) = \sum_{v \in M_k} v^+(\alpha)$ is the absolute logarithmic Weil height of α. We denote by M_k^0, respectively by M_k^∞, the set of nonarchimedean, respectively archimedean, places in M_k.
- S a finite set of places of k, including all of the archimedean places.
- X/k a smooth projective variety defined over k.
- $h_{X,D}$ an absolute logarithmic Weil height on X with respect to the divisor D.
- $\lambda_{X,D}$ an absolute logarithmic local height on X with respect to the divisor D.

Let $a, b \in \mathbb{Z}$. The greatest common divisor of a and b is given by the formula

$$\begin{aligned} \log \gcd(a,b) &= \sum_{p \text{ prime}} \min\{\operatorname{ord}_p(a), \operatorname{ord}_p(b)\} \log p \\ &= \sum_{v \in M_{\mathbb{Q}}^0} \min\{v(\alpha), v(\beta)\}. \end{aligned}$$

If a and b are rational numbers, rather than integers, then we can compute the gcd of their numerators by using v^+ in place of v, and having done this, there is no reason to restrict ourselves to the nonarchimedean places. Moving from $\mathbb{Q}$ to the number field k, we follow [5] and define the *generalized* (*logarithmic*) *greatest common divisor* of $\alpha, \beta \in k$ to be the quantity

$$h_{\mathrm{gcd}}(\alpha, \beta) = \sum_{v \in M_k} \min\{v^+(\alpha), v^+(\beta)\}.$$

In particular, if $\alpha, \beta \in \mathbb{Z}$, then $h_{\mathrm{gcd}}(\alpha, \beta) = \log \gcd(\alpha, \beta)$.

A fancier way to view the function

$$v^+ : k \longrightarrow [0, \infty]$$

is as the local height function on $\mathbb{P}^1(k)$ with respect to the divisor (0), where we identify $k \cup \{\infty\}$ with $\mathbb{P}^1(k)$ and set $v^+(\infty) = 0$. We would like to find a similar height theoretic interpretation for the function

$$G : \mathbb{P}^1(k) \times \mathbb{P}^1(k) \longrightarrow [0, \infty], \qquad (\alpha, \beta) \longmapsto \min\{v^+(\alpha), v^+(\beta)\},$$

that appears in the definition of the generalized greatest common divisor. Intuitively, $G(\alpha, \beta)$ is large if and only if the point (α, β) is v-adically close to the point $(0, 0)$. This resembles the intuitive characterization of a local height function,

$$\lambda_{X,D}(P, v) = -\log\,(v - \text{adic distance from } P \text{ to } D),$$

except that $(0, 0)$ is not a divisor on $(\mathbb{P}^1)^2$. However, there is a general theory that associates a local height function $\lambda_{X,Y}(P, v)$ to any subvariety Y of X, or more generally to any closed subscheme Y, see [19] or [25, §5]. For our purposes, it is convenient to use an equivalent formulation in terms of blowups.

Continuing with our example, let $X=(\mathbb{P}^1)^2$, let $\pi:\tilde{X}\to X$ be the blowup of X at the point $(0,0)$, and let $E=\pi^{-1}(0,0)$ be the exceptional divisor of the blowup. Then it is an easy exercise using explicit equations (or see [25, Lemma 2.5.2]) to verify that a local height function on $\tilde{X}$ for the divisor E is given by the formula

$$\lambda_{\tilde{X},E}(\pi^{-1}(\alpha,\beta),v)=\min\{v^+(\alpha),v^+(\beta)\}\quad\text{for all } (\alpha,\beta)\in X(k)\backslash(0,0).$$

Adding these local heights gives the global formula

$$h_{\mathrm{gcd}}(\alpha,\beta)=\sum_{v\in M_k}\lambda_{\tilde{X},E}(\pi^{-1}(\alpha,\beta),v)=h_{\tilde{X},E}(\pi^{-1}(\alpha,\beta)).$$

In other words, the (generalized) logarithmic gcd of α and β is equal to the Weil height of (α,β) on a blowup of $(\mathbb{P}^1)^2$ with respect to the exceptional divisor of the blowup. This identification allows us to bring the machinery of heights to bear on problems concerning greatest common divisors, and in particular allows us to apply Vojta's conjecture to such problems.

Having identified $h_{\mathrm{gcd}}(\alpha,\beta)$ with the Weil height on a particular blowup, it is natural to generalize the notion of greatest common divisor to arbitrary varieties blown up along arbitrary subvarieties.

Definition 2. Let X/k be a smooth variety and let $Y/k\subset X/k$ be a subvariety of codimension $r\geqslant 2$. Let $\pi:\tilde{X}\to X$ be the blowup of X along Y, and let $\tilde{Y}=\pi^{-1}(Y)$ be the exceptional divisor of the blowup. For $P\in X\backslash Y$, we let $\tilde{P}=\pi^{-1}(P)\in\tilde{X}$.

The *generalized* (*logarithmic*) *greatest common divisor of the point* $P\in(X\backslash Y)(k)$ *with respect to* Y *is the quantity*

$$h_{\mathrm{gcd}}(P;Y)=h_{\tilde{X},\tilde{Y}}(\tilde{P}).$$

Example 3. Let $X=\mathbb{P}^n$ and let $Y=[1,0,0,\dots,0]$. For $\mathbf{x}\in\mathbb{P}^n(\mathbb{Q})$, choose homogeneous coordinates $\mathbf{x}=[x_0,x_1,\dots,x_n]$ with $x_i\in\mathbb{Z}$ and $\gcd(x_0,\dots,x_n)=1$. Then

$$h_{\mathrm{gcd}}(\mathbf{x};Y)=\log\gcd(x_1,x_2,\dots,x_n)+O(1).$$

Example 4. Again let $X=\mathbb{P}^n$ and let Y be a subvariety of codimension $r\geqslant 2$ defined by the vanishing of a collection of homogeneous polynomials $f_1,f_2,\dots,f_t\in\mathbb{Z}[X_0,\dots,X_n]$. Then for all points $\mathbf{x}=[x_0,x_1,\dots,x_n]\in\mathbb{P}^n(\mathbb{Q})$ written with normalized homogeneous coordinates as in Example 3, we have

$$h_{\mathrm{gcd}}(\mathbf{x};Y)=\log\gcd(f_1(\mathbf{x}),\dots,f_t(\mathbf{x}))+O(1).$$

Compare the righthand side of this formula with the lefthand side of condition (2) in Theorem 2. This identification allows us to reformulate Theorem 2 in terms of heights on blown up varieties and thence to apply Vojta's conjecture.

Example 5. Let $E/\mathbb{Q}$ be an elliptic curve given by a (minimal) Weierstrass equation, let $X = E^2$, let $Y = \{(O,O)\}$, and let $\pi_1, \pi_2 : X \to E$ denote the two projections. The square of the ideal sheaf $\mathscr{I}_Y$ of Y is generated locally by the two functions $\pi_1^*(x^{-1})$ and $\pi_2^*(x^{-1})$,

$$\mathscr{I}_Y^2 = \pi_1^*(x^{-1})\mathscr{O}_{X,Y} + \pi_2^*(x^{-1})\mathscr{O}_{X,Y}.$$

Hence the greatest common divisor of a point $(P,Q) \in X(\mathbb{Q})$ with respect to $Y = \{(O,O)\}$ is given by

$$\begin{aligned} h_{\mathrm{gcd}}((P,Q);Y) &= \sum_{v \in M_{\mathbb{Q}}} \frac{1}{2} \min\{v^+(x_P^{-1}), v^+(x_Q^{-1})\} \\ &= \log \gcd(D_P, D_Q), \end{aligned} \tag{4}$$

where recall (cf. Theorem 3) that for $P \in E(\mathbb{Q})$, we write $x_P = A_P/D_P^2$.

3. Vojta's Conjecture

We recall the statement of Vojta's conjecture [25, Conjecture 3.4.3].

Conjecture 5 (Vojta [25]). *Set the following notation*:

k	*a number field.*
S	*a finite set of places of k.*
X/k	*a smooth projective variety.*
A	*an ample divisor on X.*
D	*a normal crossings divisor on X.*
K_X	*a canonical divisor on X.*

Then for every $\epsilon > 0$ there exists a proper Zariski-closed subset $Z = Z(\epsilon, X, A, D, k, S)$ of X and a constant $C_\epsilon = C_\epsilon(X, A, D, k, S)$ so that

$$\sum_{v \in S} \lambda_{X,D}(P,v) + h_{X,K_X}(P) \leqslant \epsilon h_{X,A}(P) + C_\epsilon \quad \textit{for all } P \in X(k) \backslash Z. \tag{5}$$

Remark 1. We remind the reader that D is a *normal crossings divisor* if at every point in the support of D there are local coordinates $(z_1, \ldots, z_n)$ so that D is given locally by an equation of the form $z_1 z_2 \cdots z_i = 0$.

Remark 2. Vojta's conjecture contains the additional statement that aside from a set of dimension zero, the set Z may be chosen independently of the field k and the set of places S. In other words, there is a set $Z_0 = Z_0(\epsilon, X, A, D)$ so that for any finite extension k'/k and any finite set of places S' of k', there is a finite set of *points* $Z_1 = Z_1(\epsilon, X, A, D, k', S')$ so that (5) holds for all $P \in X(k')$ with $P \notin Z = Z_0 \cup Z_1$. We will be working over a single number field, so we will not need this stronger version.

Remark 3. In Vojta's conjecture and throughout this paper, when we say that a constant depends on a divisor D on a variety X, we assume that both global and local heights $h_{X,D}$ and $\lambda_{X,D}$ have been chosen and that the constant in question may depend on this choice.

Definition 3. With notation as in the statement of Conjecture 5, we let

$$h_{X,D,S}(P)=\sum_{v\in S}\lambda_{X,D}(P,v)\quad\text{and}\quad h'_{X,D,S}(P)=\sum_{v\notin S}\lambda_{X,D}(P,v).$$

This corresponds to Vojta's notation [25] via $m_S(D,P)=h_{X,D,S}(P)$ and $N_S(D,P)=h'_{X,D,S}(P)$. Making an analogy with Nevanlinna theory, Vojta calls $m_S(D,P)$ the "proximity function" and $N_S(D,P)$ the "counting function." Then Vojta's fundamental inequality (5) becomes the succinct statement

$$h_{X,D,S}(P)+h_{X,K_X}(P)\leqslant \epsilon h_{X,A}(P)+C_\epsilon\quad\text{for all } P\in X(k)\backslash Z. \tag{6}$$

4. Applying Vojta's Conjecture to Blowups

Let X/k be a smooth variety and let $Y/k\subset X/k$ be a smooth subvariety of codimension $r\geqslant 2$. Let $\pi:\tilde{X}\to X$ be the blowup of X along Y, and let $\tilde{Y}=\pi^{-1}(Y)$ be the exceptional divisor of the blowup. For $P\in X\backslash Y$, we let $\tilde{P}=\pi^{-1}(P)\in\tilde{X}$. A nice property of blowups of smooth varieties along smooth subvarieties is that it is easy to describe a canonical divisor on the blowup [11, Exercise II.8.5],

$$K_{\tilde{X}}\sim\pi^*K_X+(r-1)\tilde{Y}.$$

(Here $\sim$ denotes linear equivalence.) We also observe that if A is an ample divisor on X, then there exists an integer N so that $-\tilde{Y}+N\pi^*A$ is ample on $\tilde{X}$. This follows from the Nakai-Moishezon Criterion [11, Theorem A.5.1]. We choose such an N and let

$$\tilde{A}=-\frac{1}{N}\tilde{Y}+\pi^*A\in\operatorname{Div}(\tilde{X})\otimes\mathbb{Q},$$

so $\tilde{A}$ is in the ample cone of $\tilde{X}$.

We make the following assumptions:[2]

$$\begin{bmatrix}\bullet & \text{The anticanonical divisor } -K_X \text{ is a normal}\\ & \text{crossings divisor.}\\ \bullet & Y \text{ intersects the support of } K_X \text{ transversally.}\end{bmatrix} \tag{7}$$

We recall that two closed algebraic subsets W_1 and W_2 of a nonsingular variety V are transversal at a point $P\in W_1\cap W_2$ if the intersection of their tangent spaces at P has codimension equal to the sum of the codimensions of W_1 and W_2. In particular, W_1 and W_2 are nonsingular at P. (See [16, II §2.1] for details.) The transversality assumption (7) implies that the pullback $\pi^*(-K_X)$ is isomorphic to $-K_X$, so in particular $\pi^*(-K_X)$ is again a normal crossings divisor, but now on the blownup variety $\tilde{X}$. This allows us to apply Vojta's conjecture to the variety $\tilde{X}$ and the divisor $D=-\pi^*K_X$ to obtain the inequality

$$h_{\tilde{X},-\pi^*K_X,S}(\tilde{P})+h_{\tilde{X}},K_{\tilde{X}}(\tilde{P})\leqslant\epsilon h_{\tilde{X},\tilde{A}}(\tilde{P})+C_\epsilon\quad\text{for all } \tilde{P}\in\tilde{X}(k)\backslash\tilde{Z}.$$

[2] It actually suffices to assume that some multiple of $-K_X$ is a normal crossings divisor. The case $K_X=0$ is also permitted.

Substituting

$$K_{\tilde{X}} = \pi^* K_X + (r-1)\tilde{Y} \quad \text{and} \quad \tilde{A} = -\frac{1}{N}\tilde{Y} + \pi^* A$$

and using functorial properties of height functions, we obtain

$$\begin{aligned} &- h_{X,K_X,S}(P) + h_{X,K_X}(P) + (r-1)h_{\tilde{X},\tilde{Y}}(\tilde{P}) \\ &\qquad \leqslant \epsilon h_{X,A}(P) - \frac{\epsilon}{N} h_{\tilde{X},\tilde{Y}}(\tilde{P}) + C_\epsilon \quad \text{for all } P \in X(k) \setminus Z, \end{aligned}$$

where we have written $Z = \pi(\tilde{Z})$. The two leftmost terms may be combined using $h_{X,D,S} + h'_{X,D,S} = h_{X,D}$, which yields

$$h'_{X,K_X,S}(P) + \Bigl(r - 1 + \frac{\epsilon}{N}\Bigr) h_{\tilde{X},\tilde{Y}}(\tilde{P}) \leqslant \epsilon h_{X,A}(P) + C_\epsilon \quad \text{for all } P \in X(k) \setminus Z.$$

Finally, a small amount of algebra, the definition $h_{\mathrm{gcd}}(P;Y) = h_{\tilde{X},\tilde{Y}}(\tilde{P})$, and setting $\delta = \epsilon/N$ gives the following result, where for the convenience of the reader we restate all of our assumptions.

Theorem 6. *Let X/k be a smooth variety, let A be an ample divisor on X, let K_X be a canonical divisor on X, and let $Y/k \subset X/k$ be a smooth subvariety of codimension $r \geqslant 2$. Assume that the following conditions are valid*:

(a) *$-K_X$ is a normal crossings divisor.*
(b) *Y intersects the support of $-K_X$ transversally.*
(c) *Vojta's conjecture is true.*[3]

Then for every finite set of places S and every $0 < \epsilon < r-1$ there is a proper closed subvariety $Z = Z(\epsilon, X, Y, A, k, S) \subsetneq X$, a constant $C_\epsilon = C_\epsilon(X, Y, A, k, S)$, and a constant $\delta = \delta(X, Y, A) > 0$ so that

$$h_{\mathrm{gcd}}(P;Y) \leqslant \epsilon h_{X,A}(P) + \frac{1}{r-1+\delta\epsilon} h'_{X,-K_X,S}(P) + C_\epsilon \quad \textit{for all } P \in X(k) \setminus Z. \tag{8}$$

5. Proofs of Theorems 2, 3, and 4

In this section we show how our main result (Theorem 6) can be used to prove the three special cases stated in Section 1.

Proof of Theorem 2. We apply Theorem 6 to the following data:

$$\begin{aligned} X &= \mathbb{P}^n, \\ Y &= \{f_1 = f_2 = \cdots = f_t = 0\} \subset \mathbb{P}^n, \\ K_X &= -\sum_{i=0}^{n} H_i, \quad \text{where } H_i = \{X_i = 0\} \in \mathrm{Div}(\mathbb{P}^n), \\ A &= H_0. \end{aligned}$$

[3] More precisely, it suffices to assume that Vojta's conjecture is true for the blowup $\pi : \tilde{X} \to X$ of X along Y and for the divisor $D = -\pi^* K_X$.

Notice that $-K_X$ is a normal crossings divisor and that Y intersects the support of $-K_X$ transversally by assumption. For $P \in \mathbb{P}^n(\mathbb{Q})$, let $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ with $\gcd(x_i) = 1$ be normalized homogeneous coordinates for P. Then by definition of the Weil height we have

$$h_{X,A} = \log\max\{|x_0|, \ldots, |x_n|\}, \tag{9}$$

and Example 4 says that

$$h_{\gcd}(P;Y) = \log\gcd(f_1(\mathbf{x}), \ldots, f_t(\mathbf{x})). \tag{10}$$

(All height equalities up to $O(1)$.) Further, by definition of the S-part of the height, we have

$$h'_{X,H_i,S}(P) = \sum_{v \notin S} v^+(x_i) = \log|x_i|'_S,$$

so

$$h'_{X,-K_X,S}(P) = \sum_{i=0}^{n} h'_{X,H_i,S}(P) = \log|x_0x_1\cdots x_n|'_S. \tag{11}$$

We now substitute (9), (10) and (11) into the inequality (8) of Theorem 6 to obtain

$$\begin{aligned} &\log\gcd(f_1(\mathbf{x}), \ldots, f_t(\mathbf{x})) \\ &\quad\leqslant \epsilon\log\max\{|x_0|, \ldots, |x_n|\} + \frac{1}{r-1+\delta\epsilon}\log|x_0x_1\cdots x_n|'_S + C_\epsilon \\ &\qquad\qquad\qquad\qquad\text{for all } P = [\mathbf{x}] \in \mathbb{P}^n(\mathbb{Q})\setminus Z. \end{aligned}$$

Exponentiating this inequality completes the proof of Theorem 2, once we observe that the exceptional set Z is contained in some hypersurface, so may be replaced by the zero set of a single nonzero polynomial. □

Proof of Theorem 3. Let $\pi_1, \pi_2 : E \times E \to E$ be the two projections. We apply Theorem 6 to the following data:

$$X = E \times E, \qquad Y = \{(O,O)\}, \qquad K_X = 0, \qquad A = \pi_1^*(O) + \pi_2^*(O).$$

We compute

$$\begin{aligned} h_{X,A}(P,Q) &= h_{E\times E,\pi_1^*(O)+\pi_2^*(O)}(P,Q) && \text{definition of } X \text{ and } A, \\ &= h_{E,O}(P) + h_{E,O}(Q) + O(1) && \text{functoriality of heights.} \end{aligned} \tag{12}$$

Next we recall from (4) in Example 5 that the generalized greatest common divisor of (P,Q) with respect to (O,O) is given by

$$h_{\gcd}((P,Q);(O,O)) = \log\gcd(D_P, D_Q). \tag{13}$$

Substituting (12) and (13) into inequality (8) of Theorem 6 yields (note $K_X = 0$, so the $h'_{X,-K_X,S}$ term disappears)

$$\log\gcd(D_P, D_Q) \leqslant \epsilon(h_{E,O}(P) + h_{E,O}(Q)) + C_\epsilon \quad \text{for all } (P,Q) \in E^2(\mathbb{Q})\setminus Z.$$

Exponentiating gives the first part of Theorem 3.

It remains to describe the exceptional set Z. Let $\Gamma \subset Z$ be an irreducible component of Z such that

$$\log \gcd(D_P, D_Q) \geqslant \epsilon(h(P) + h(Q)) + C_\epsilon \quad \text{for infinitely many } (P,Q) \in \Gamma(\mathbb{Q}), \tag{14}$$

where to ease notation we let $h(P) = h_{E,O}(P)$. Faltings' theorem [10] tells us that Γ is a translate of an abelian subvariety of E^2, i.e. Γ is a translate of an elliptic curve. If E does not have CM, then the abelian subvarieties of E^2 are precisely the curves

$$\Gamma_{n_1,n_2} = \{(n_1T, n_2T) : T \in E\} \quad \text{for } n_1, n_2 \geqslant 0 \text{ with } \gcd(n_1,n_2) = 1.$$

Thus the assumption that Γ contains infinitely many points satisfying (14) implies that there is a fixed pair of integers (n_1, n_2) as above and a fixed pair of points $(R_1, R_2) \in E^2(\mathbb{Q})$ so that

$$\Gamma = \Gamma_{n_1,n_2} + (R_1, R_2) = \{(n_1T + R_1, n_2T + R_2) : T \in E\}.$$

Hence

$$\begin{aligned} \log \gcd(D_{n_1T+R_1}, D_{n_2T+R_2}) &\geqslant \epsilon(h(n_1T + R_1) + h(n_2T + R_2)) + O(1) \\ &= \epsilon(n_1^2 + n_2^2)h(T) + O\left(\sqrt{h(T)}\right) \\ &\qquad \text{for infinitely many } T \in E(\mathbb{Q}). \end{aligned} \tag{15}$$

Here the big-O constant may depend on (R_1, R_2) and on (n_1, n_2), as long as it is independent of T. We have also used the positivity and quadratic nature of the height ([18, VIII §9]) in the form

$$h(nT + R) = n^2 h(T) + O_{E,R}\left(\sqrt{h(T)}\right).$$

It remains to bound $\gcd(D_{n_1T+R_1}, D_{n_2T+R_2})$. Since $\gcd(n_1, n_2) = 1$ by assumption, we can choose integers (u_1, u_2) with $u_1n_1 + u_2n_2 = 1$ and set $R_3 = u_1R_1 + u_2R_2$. Note that R_3 is independent of T. Let p be a prime. Working in $E(\mathbb{Q}_p)$, we have

$$\begin{aligned} &p^e \mid \gcd(D_{n_1T+R_1}, D_{n_2T+R_2}) \\ &\quad\Longleftrightarrow n_1T + R_1 \equiv O \pmod{p^e} \quad \text{and} \quad n_2T + R_2 \equiv O \pmod{p^e} \\ &\quad\Longrightarrow T + R_3 = u_1(n_1T + R_1) + u_2(n_2T + R_2) \equiv O \pmod{p^e} \\ &\quad\Longrightarrow p^e \mid D_{T+R_3}. \end{aligned}$$

Thus $\gcd(D_{n_1T+R_1}, D_{n_2T+R_2})$ divides D_{T+R_3}, so

$$\begin{aligned} \log \gcd(D_{n_1T+R_1}, D_{n_2T+R_2}) &\leqslant \log D_{T+R_3} \\ &\leqslant h(T + R_3) \\ &\leqslant h(T) + O\left(\sqrt{h(T)}\right). \end{aligned} \tag{16}$$

Combining (15) and (16) yields

$$h(T) \geqslant \epsilon(n_1^2 + n_2^2)h(T) + O\left(\sqrt{h(T)}\right) \quad \text{for infinitely many } T \in E(\mathbb{Q}).$$

Letting $h(T) \to \infty$, we conclude that

$$1 \geqslant \epsilon(n_1^2 + n_2^2). \tag{17}$$

This completes the proof of Theorem 3 once we observe that the height function $H(P)$ used in the statement of Theorem 3 satisfies $\log H(P) = 2h_{E,O}(P)$. $\square$

Proof of Theorem 4. This time we apply Theorem 6 with

$$\begin{aligned} X &= E \times \mathbb{P}^1, \\ A &= \pi_1^*(O) + \pi_2^*(\infty), \\ K_X &= -\pi_2^*(0) - \pi_2^*(\infty), \\ Y &= \{(O,1)\}, \end{aligned}$$

where $\pi_1 : X \to E$ and $\pi_2 : X \to \mathbb{P}^1$ are the projections. Then for any $(Q,b) \in E(\mathbb{Q}) \times \mathbb{Q}$ we have

$$\begin{aligned} h_{X,A}(Q,b) &= h_{E,O}(Q) + h(b) \\ h_{\mathrm{gcd}}((Q,b);(0,1)) &= \log \gcd(D_Q, b-1). \end{aligned}$$

Further, if $b \in \mathbb{Z}_S^*$, then

$$h'_{X,-K_X,S}(Q,b) = h'_{\mathbb{P}^1,(0),S}(b) + h'_{\mathbb{P}^1,(\infty),S}(b) = 0.$$

Thus Theorem 6 yields

$$\log \gcd(D_Q, b-1) \leqslant \epsilon(h_{E,O}(Q) + h(b)) + O(1)$$
$$\text{for } (Q,b) \in E(\mathbb{Q}) \times \mathbb{Z}_S^* \text{ with } (Q,b) \notin Z.$$

Siegel's theorem [18, IX.3.3] says that $h_{E,O}(Q) \sim \log D_Q$ as $h_{E,O}(Q) \to \infty$, so exponentiating and adjusting ϵ gives

$$\gcd(D_Q, b-1) \leqslant C \cdot \max(D_Q, H(b))^{\epsilon}$$
$$\text{for } (Q,b) \in E(\mathbb{Q}) \times \mathbb{Z}_S^* \text{ with } (Q,b) \notin Z.$$

It remains to deal with the exceptional set Z. It suffices to consider an irreducible component $\Gamma \subset Z$ of dimension 1 with

$$\log \gcd(D_Q, b-1) \geqslant \epsilon(h_{E,O}(Q) + h(b)) + O(1)$$
$$\text{for infinitely many } (Q,b) \in (E(\mathbb{Q}) \times \mathbb{Z}_S^*) \cap \Gamma. \tag{18}$$

In particular, $\#\Gamma(\mathbb{Q}) = \infty$, so Faltings' theorem [9] reduces us to the case that Γ has genus 0 or 1. If either $\pi_1(\Gamma)$ or $\pi_2(\Gamma)$ consists of a single point, it suffices to adjust the constant, so we assume that $\pi_1(\Gamma) = E$ and $\pi_2(\Gamma) = \mathbb{P}^1$. In particular, the fact that $\pi_1(\Gamma) = E$ implies that Γ cannot have genus 0, so we are reduced to the case that Γ has genus 1.

The fact that Γ satisfies (18) implies that $\pi_2(\Gamma) \cap \mathbb{Z}_S^*$ is infinite. In other words, the map

$$\pi_2 : \Gamma(\mathbb{Q}) \longrightarrow \mathbb{Q} \cup \{\infty\}$$

takes on infinitely many S-unit values. But $\Gamma(\mathbb{Q})$ is the Mordell-Weil group of an elliptic curve, so Siegel's theorem [18, IX.3.2.2] says that this is not possible (indeed, it is not even possible to take on infinitely many S-integral values). This completes the proof that the exceptional set may be taken to be a finite set of points, and hence may be eliminated entirely by adjusting the constants. □

6. Divisibility Sequences and Algebraic Groups

A *divisibility sequence* is a sequence of integers $(a_n)_{n \geqslant 1}$ with the property that

$$m|n \Longrightarrow a_m|a_n.$$

We have already briefly discussed the divisibility sequences (D_{nP}) associated to a point of infinite order P on an elliptic curve $E(\mathbb{Q})$. Other familiar divisibility sequences include sequences of the form $(a^n - b^n)$ and the Fibonacci sequence (F_n). There are many natural ways to generalize the notion of divisibility sequence, for example by replacing divisibility of positive integers with divisibility of ideals in a ring. In the most abstract formulation, one might define a divisibility sequence as simply an order-preserving map between two partially ordered sets (posets). In this section we restrict our attention to classical divisibility sequences of rational integers, but the reader should be aware that virtually everything that we say can be easily generalized (albeit at the cost of some notational inconvenience) to the partially ordered set of integral ideals in number fields, and in some cases to other Dedekind domains or even more general rings.

The divisibility sequence $(a^n - b^n)_{n \geqslant 1}$ is naturally associated to the rank one subgroup of $\mathbb{G}_m(\mathbb{Q})$ generated by a/b, just as the divisibility sequence $(D_{nP})_{n \geqslant 1}$ comes from the rank one subgroup of $E(\mathbb{Q})$ generated by P. This suggests creating divisibility sequences from other algebraic groups G defined over $\mathbb{Q}$. In order to make this precise, we need to choose a model over $\mathbb{Z}$, although a different choice of model only changes the sequence at finitely many primes.

Definition 4. Let $\mathscr{G}/\mathbb{Z}$ be a group scheme over $\mathbb{Z}$, let $\mathscr{O} \subset \mathscr{G}(\mathbb{Z})$ be the identity element of $\mathscr{G}$, and let $\mathscr{P} \in \mathscr{G}(\mathbb{Z})$ be a nonzero section. We associate to $\mathscr{P}$ a positive integer $D_{\mathscr{P}}$ by the condition

$$\operatorname{ord}_p(D_{\mathscr{P}}) = (\mathscr{P} \cdot \mathscr{O})_p \quad \text{for all primes } p,$$

where in general $(\mathscr{P}_1 \cdot \mathscr{P}_2)_p$ denotes the arithmetic intersection index of the sections $\mathscr{P}_1$ and $\mathscr{P}_2$ on the fiber over p.

Equivalently, let $\mathscr{I}_{\mathscr{O}}$ be the ideal sheaf of $\mathscr{O} \subset \mathscr{G}$, where we identify the section $\mathscr{O}$ with its image $\mathscr{O}(\mathbb{Z})$, taken with the induced reduced subscheme structure. Then $\mathscr{P}^*(\mathscr{I}_{\mathscr{O}})$ is an ideal sheaf on $\operatorname{Spec}(\mathbb{Z})$, i.e. it is an ideal of $\mathbb{Z}$. Then $D_{\mathscr{P}}$ is determined by the condition that it generates this ideal,

$$D_{\mathscr{P}} \cdot \mathbb{Z} = (\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}).$$

These $D_{\mathscr{P}}$ values are closely associated to certain generalized greatest common divisors.

Proposition 7. *Let $\mathscr{G}/\mathbb{Z}$ be a group scheme, let $G = \mathscr{G} \times_{\mathbb{Z}} \mathbb{Q}$ be the associated algebraic group over $\mathbb{Q}$, let $\rho : \mathscr{G}(\mathbb{Z}) \to G(\mathbb{Q})$ denote restriction to the generic fiber, and let $O = \rho(\mathscr{O}) \in G(\mathbb{Q})$ be the identity element of G. Then*

$$\log D_{\mathscr{P}} \leqslant h_{\mathrm{gcd}}(\rho(\mathscr{P}); O) + O(1) \quad \textit{for all } \mathscr{P} \in \mathscr{G}(\mathbb{Z}).$$

(*In principle, the height function might depend on the choice of a completion and projective embedding of G. However, these only affect* $h_{\text{gcd}}(\,\cdot\,;O)$ *up to* $O(1)$.)

Proof. This is just a matter of unsorting the definitions and decomposing h_{gcd} into a sum of local heights. With the obvious notation, we find that

$$\lambda_{\text{gcd}}(\rho(\mathscr{P});O;v) = \lambda_{\tilde{G},\tilde{O}}(\rho(\mathscr{P}),v) = v(D_{\mathscr{P}}) \quad \text{for all nonarchimedean places } v.$$

This gives the stated result, with the contributions from the (nonnegative) archimedean local heights giving an inequality, rather than an equality. □

We next show that a sequence of the form $(D_{n\mathscr{P}})_{n\geqslant 1}$ is a divisibility sequence.

Proposition 8. *Let* $\mathscr{G}/\mathbb{Z}$ *be a group scheme and let* $\mathscr{P}\in\mathscr{G}(\mathbb{Z})$ *be a point (section) of infinite order. Then the sequence* $(D_{n\mathscr{P}})_{n\geqslant 1}$ *is a divisibility sequence. We call it the divisibility sequence associated to* $\mathscr{P}$ *(and* $\mathscr{G}$*).*

Proof. For each integer $n \geqslant 1$, let $\mu_n : \mathscr{G} \to \mathscr{G}$ be the n^{th}-power morphism. The section $n\mathscr{P}\in\mathscr{G}(\mathbb{Z})$ is the composition

$$\text{Spec}(\mathbb{Z}) \xrightarrow{\mathscr{P}} \mathscr{G} \xrightarrow{\mu_n} \mathscr{G}.$$

Now let $m|n$, say $n = mr$. Then

$$\begin{aligned}
D_{n\mathscr{P}}\cdot\mathbb{Z} &= (n\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}) && \text{by definition of } D_{n\mathscr{P}},\\
&= (\mu_n\circ\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}) && \text{since } n\mathscr{P} = \mu_n\circ\mathscr{P} \text{ as maps},\\
&= (\mu_r\circ\mu_m\circ\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}) && \text{since } \mu_n = \mu_{rm} = \mu_r\circ\mu_m,\\
&= (\mu_m\circ\mathscr{P})^*\circ\mu_r^*(\mathscr{I}_{\mathscr{O}}) &&\\
&\subseteq (\mu_m\circ\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}) && \text{since } \mu_r^*(\mathscr{I}_{\mathscr{O}}) \subseteq \mathscr{I}_{\mathscr{O}},\\
&= (m\mathscr{P})^*(\mathscr{I}_{\mathscr{O}}) = D_{m\mathscr{P}}\cdot\mathbb{Z} && \text{by definition of } D_{m\mathscr{P}}.
\end{aligned}$$

The one point that possibly requires further explanation is the inclusion $\mu_r^*(\mathscr{I}_{\mathscr{O}}) \subseteq \mathscr{I}_{\mathscr{O}}$ of ideal sheaves on $\mathscr{G}$. The validity of this inclusion follows from the following two facts:

- The sheaf $\mathscr{I}_{\mathscr{O}}$ is the ideal sheaf of the image $\mathscr{O}(\mathbb{Z})$ of the identity section with its induced-reduced subscheme structure.
- The zero section satisfies $r\mathscr{O} = \mathscr{O}$, so $\mu_r(\mathscr{O}(\mathbb{Z})) = (r\mathscr{O})(\mathbb{Z}) = \mathscr{O}(\mathbb{Z})$ as subsets of $\mathscr{G}$.

This proves that $D_{n\mathscr{P}}\cdot\mathbb{Z} \subseteq D_{m\mathscr{P}}\cdot\mathbb{Z}$, which is equivalent to $D_{m\mathscr{P}}|D_{n\mathscr{P}}$. □

Definition 5. A *geometric divisibility sequence* is the divisibility sequence $(D_{n\mathscr{P}})_{n\geqslant 1}$ associated to a point (section) $\mathscr{P}$ of infinite order in a group scheme $\mathscr{G}/\mathbb{Z}$ as in Proposition 8.

Some algebraic groups have particularly nice models over $\mathbb{Z}$. In particular, if $A/\mathbb{Q}$ is an abelian variety, then the Néron model of $A/\mathbb{Q}$ is a group scheme $\mathscr{A}/\mathbb{Z}$ characterized, up to canonical isomorphism, by a certain universal mapping property and by the fact that its generic fiber is $A/\mathbb{Q}$ [2]. Note that the fiber of $\mathscr{A} \to \mathrm{Spec}(\mathbb{Z})$ over a closed point (p) is a smooth group variety over $\mathbb{F}_p$, but it need not be complete, i.e. finitely many fibers may be extensions of abelian varieties by tori and unipotent groups. The existence of the Néron model prompts the following definition.

Definition 6. Let $A/\mathbb{Q}$ be an abelian variety and let $P \in A(\mathbb{Q})$ be a point of infinite order. The *abelian divisibility sequence* associated to P is the divisibility sequence associated to the lift $\mathscr{P}$ of P to a section of the Néron model $\mathscr{A}/\mathbb{Z}$ of $A/\mathbb{Q}$. By abuse of notation, we denote this sequence by $(D_{nP})_{n \geqslant 1}$.

We next show that Vojta's conjecture implies a strong upper bound for abelian divisibility sequences on abelian varieties of dimension at least 2. This result generalizes Theorem 3 (take $A = E \times E$).

Proposition 9. *Let $A/\mathbb{Q}$ be an abelian variety of dimension at least 2, and assume that Vojta's conjecture is true for A blown up at O. Fix a Weil height*

$$h : A(\mathbb{Q}) \to \mathbb{R} \tag{19}$$

on A with respect to an ample symmetric divisor.

(a) *For every $\epsilon > 0$ there is a constant $C = C(A, \epsilon)$ and a proper algebraic subvariety $Z \subsetneq A$ so that*

$$h_{\mathrm{gcd}}(P; O) \leqslant \epsilon h(P) + C \quad \textit{for all } P \in A(\mathbb{Q}) \setminus Z.$$

The exceptional set Z consists of a finite union of translates of nontrivial abelian subvarieties of A, so in particular, if A is simple, then we may take $Z = \emptyset$.

(b) *Let $(D_{nP})_{n \geqslant 1}$ be the abelian divisibility sequence associated to a point of infinite order $P \in A(\mathbb{Q})$, and assume further that the group $\mathbb{Z}P$ generated by P is Zariski dense in A. Then for every $\epsilon > 0$ there is a constant $C = C(A, P, \epsilon)$ so that*

$$\log D_{nP} \leqslant \epsilon n^2 + C \quad \textit{for all } n \geqslant 1.$$

Remark 4. We observe that Proposition 9 is false if A is an elliptic curve, since then we have $h_{\mathrm{gcd}}(P; O) = h_{E,O}(P)$ and $\log D_{nP} \sim n^2 \hat{h}(P)$. The reason that our proof of Proposition 9 fails when $\dim(A) = 1$ is the requirement in Theorem 6 that the subvariety Y have codimension at least 2 in X.

Proof of Proposition 9. (a) We apply Theorem 6 to the variety A, the subvariety consisting of the single point O, and the ample divisor used to define the height (19). The canonical divisor on A is trivial, so Theorem 6 says that there is a subvariety $Z \subsetneq A$ such that

$$h_{\mathrm{gcd}}(P; O) \leqslant \epsilon h(P) + O(1) \quad \text{for all } P \in A(\mathbb{Q}) \setminus Z.$$

This proves (a), other than the characterization of Z. Let $Z' \subset Z$ be any irreducible subvariety of Z. If $Z'(\mathbb{Q})$ is finite, then we may discard it and adjust the $O(1)$

accordingly. And if $Z'(\mathbb{Q})$ is infinite, then Faltings' theorem [10] says that Z' is a translate of an abelian subvariety of A.

(b) We compute

$$\begin{aligned} \log D_{nP} &\leqslant h_{\mathrm{gcd}}(nP;O) + O(1) && \text{from Proposition 7,} \\ &\leqslant \epsilon h(nP) + O(1) && \text{from (a), assuming } nP \notin Z, \\ &\leqslant \epsilon n^2 \hat{h}(P) + O(1) && \text{canonical height property [12, B.5.1]} \end{aligned}$$

The fact that P has infinite order implies that $\hat{h}(P) > 0$, so after replacing ϵ with $\epsilon/\hat{h}(P)$, this completes the proof of (b) provided $nP \notin Z$.

Suppose that $Z \neq \emptyset$, and let Z_1 be an irreducible component of Z that contains infinitely many multiples of P. From (a), we know that $Z_1 = A_1 + R_1$ for an abelian subvariety $A_1 \subsetneq A$ and a point $R_1 \in A(\mathbb{Q})$. Choose $n_2 > n_1$ with $n_1 P \in Z_1$ and $n_2 P \in Z_1$. Then $(n_2 - n_1)P \in A_1$. Letting $N = n_2 - n_1$, it follows that $P \in A_1 + A[N]$, and hence that $nP \in A_1 + A[N]$ for all $n \geqslant 1$. This contradicts the assumption that $\mathbb{Z}P$ is Zariski dense in A, and hence there is no exceptional set. □

7. Final Remarks and Questions

We have proven a number of strong bounds for generalized greatest common divisors and divisibility sequences, all conditional on the validity of Vojta's beautiful, but deep, conjecture applied to an appropriate blowup variety. It would be of great interest to find unconditional proofs of some of these results.

In addition to height bounds, there are many other natural questions that one might ask about abelian, or more generally geometric, divisibility sequences. For example, which such sequences contain infinitely many prime numbers (cf. [8]). This is, of course, a notoriously difficult question, even for the simplest divisibility sequence $2^n - 1$. There is some evidence [6] that elliptic divisibility sequences $(D_{nP})_{n \geqslant 1}$ do not contain infinitely many primes, although more general elliptic divisibility "sequences" $(D_{nP+mQ})_{m,n \geqslant 1}$ may well contain infinitely many primes.

One might ask if a geometric divisibility sequence necessarily grows, or if it often returns to small values. For example, Ailon and Rudnick [1] conjecture that if $a, b \in \mathbb{Z}$ are multiplicatively independent, then

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1) \quad \text{for infinitely many } n \geqslant 1.$$

They prove a strong version of this with $\mathbb{Z}$ replaced by the polynomial ring $\mathbb{C}[T]$. (See also [20] and [21] for analogs over $\mathbb{F}_q[T]$ and for elliptic curves.) We certainly suspect that the same is true for semiabelian varieties.

Conjecture 10. *Let $\mathcal{G}/\mathbb{Z}$ be a group scheme, let $\mathcal{P} \in \mathcal{G}(\mathbb{Z})$ be a $\mathbb{Z}$-valued point, and assume that the following are true*:

(1) *The generic fiber $G = \mathcal{G} \times_{\mathbb{Z}} \mathbb{Q}$ is an irreducible commutative algebraic group of dimension at least 2 with no unipotent part.*

(2) *The restriction $P \in G(\mathbb{Q})$ of $\mathcal{P}$ to the generic fiber has the property that the subgroup $\mathbb{Z}P$ generated by P is Zariski dense in G.*

Then the geometric divisibility sequence $(D_{n\mathscr{P}})_{n \geqslant 1}$ *corresponding to* $\mathscr{P}$ *satisfies*

$$D_{n\mathscr{P}} = D_{\mathscr{P}} \quad \textit{for infinitely many } n \geqslant 1.$$

It is tempting to guess that something similar is true for geometric divisibility sequences associated to any irreducible algebraic group of dimension at least 2, regardless of whether or not it is commutative. (Note that the Zariski density condition is vital.) But with no significant evidence for even Conjecture 10, we will be content to leave the general case as a question.

Acknowledgements. I would like to thank Y. Bugeaud, P. Corvaja, D. McKinnon, Z. Rudnick, G. Walsh, U. Zannier, and the referee for their helpful suggestions and correspondence, D. Abramovich, P. Corvaja, and U. Zannier for bringing to my attention some inaccuracies in the initial draft, and D. McKinnon for pointing out that the nonintersection condition in Theorem 6 could be relaxed to a transversality condition.

References

[1] Ailon N, Rudnick Z (2005) Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. Acta Arith, to appear (ArXiv math.NT/0202102)
[2] Artin M (1986) Néron models. Cornell G, Silverman JH (eds) In: Arithmetic Geometry, pp 213–230. New York: Springer
[3] Bugeaud Y, Corvaja P, Zannier U (2003) An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. Math Z **243**: 79–84
[4] Corvaja P, Zannier U (2002) On the greatest prime factor of $(ab + 1)(ac + 1)$. Proc Amer Math Soc **131**: 1705–1709
[5] Corvaja P (2005) A lower bound for the height of a rational function at S-unit points. Monatsh Math, to appear (ArXiv math.NT/0311030)
[6] Einsiedler M, Everest G, Ward T (2001) Primes in elliptic divisibility sequences. LMS J Comput Math **4**: 1–13 (electronic)
[7] Everest G, van der Poorten A, Shparlinski I, Ward T (2003) Recurrence Sequences. Providence, RI: Amer Math Soc
[8] Everest G, Ward T (2001) Primes in divisibility sequences. Cubo Mat Educ **3**: 245–259
[9] Faltings G (1983) Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent Math **73**: 349–366
[10] Faltings G (1991) Diophantine approximation on abelian varieties. Ann Math **133**: 549–576
[11] Hartshorne R (1977) Algebraic Geometry. New York: Springer
[12] Hindry M, Silverman JH (2000) Diophantine Geometry: An Introduction. New York: Springer
[13] Lang S (1983) Fundamentals of Diophantine Geometry. New York: Springer
[14] McKinnon D (2003) Vojta's main conjecture for blowup surfaces. Proc Amer Math Soc **131**: 1–12 (electronic)
[15] Schmidt W (1980) Diophantine Approximation. Lect Notes Math **785**. Berlin Heidelberg New York: Springer
[16] Shafarevich IR (1977) Basic Algebraic Geometry. (Translated from the Russian by K A Hirsch). Berlin: Springer (revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974)
[17] Shipsey R (2000) Elliptic divisibility sequences. PhD Thesis, Goldsmith's College, University of London
[18] Silverman JH (1986) The Arithmetic of Elliptic Curves. New York: Springer
[19] Silverman JH (1987) Arithmetic distance functions and height functions in Diophantine geometry. Math Ann **279**: 193–216
[20] Silverman JH (2004) Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. New York J Math (electronic) **10**: 37–43 (ArXiv math.NT/0401356)
[21] Silverman JH (2005) Common divisors of elliptic divisibility sequences over function fields. Manuscripta Math, to appear (ArXiv math.NT/0402016)
[22] Silverman JH (2005) p-adic properties of division polynomials and elliptic divisibility sequences. Math Ann, to appear (ArXiv math.NT/0404412)
[23] Silverman JH, Stephens N (2004) The sign of an elliptic divisibility sequence. Preprint (ArXiv:mathNT/0402415)

[24] Swart CS (2003) Elliptic divisibility sequences. PhD Thesis, Royal Holloway, University of London
[25] Vojta P (1987) Diophantine Approximations and Value Distribution Theory. Lect Notes Math **1239**. Berlin Heidelberg New York: Springer
[26] Ward M (1948) Memoir on elliptic divisibility sequences. Amer J Math **70**: 31–74
[27] Ward M (1948) The law of repetition of primes in an elliptic divisibility sequence. Duke Math J **15**: 941–946

Author's address: Mathematics Department, Box 1917, Brown University, Providence, RI 02912, USA, e-mail: jhs@math.brown.edu