GREATEST COMMON DIVISORS AND PLANE CURVES

TAKEHIKO YASUDA

Abstract. We study relation between greatest common divisors of integer pairs satisfying an algebraic equation and plane curve singularities.

This short manuscript is a modification of Appendix of the preprint [Yas16]. The main body of the preprint has been published as [Yas18] after some modification.

Bugeaud, Corvaja and Zannier [BCZ03, CZ05] obtained an upper bound for $\gcd(a-1, b-1)$ for certain families of integer pairs (a, b). To explain their result in relation to Vojta's conjecture, Silverman [Sil05] observed that the greatest common divisor is essentially a height function associated to a subscheme of codimension ≥ 2, although he uses the blowup along the subscheme and a height function associated to the exceptional divisor instead (see also [Yas12, Yas11]). He then formulated a conjectural generalization of the result of Bugeaud, Corvaja and Zannier.

As an application of Silverman's observation, we relate estimation of $\gcd(a, b)$ for integer pairs (a, b) satisfying an algebraic equation with the multiplicity of the corresponding plane curve at the origin.

1. Weill functions and heights

Let k be a number field and let M_k be the set of its places. To a projective variety X over k and a closed subscheme $Z \subset X$, we associate a *Weil function*

$$\lambda_Z \colon X(\bar{k}) \times M_k \to [0, +\infty],$$

following [Sil87], which is unique up to addition of M_k-bounded functions. We write

$$\lambda_{\mathfrak{a},v}(x) := \lambda_{\mathfrak{a}}(x, v).$$

The *height function* h_Z associated to Z on the k-point set $X(k)$ is defined as

$$h_Z(x) := \sum_{v \in M_k} \lambda_{Z,v}(x).$$

We recall a few basic properties of Weil functions and height functions.

Proposition 1.1 ([Sil87, Th. 2.1]). (1) *For a morphism $f \colon Y \to X$ of varieties and a closed subscheme $Z \subset X$, we have*

$$\lambda_Z \circ f = \lambda_{f^{-1}Z}.$$

(2) *For $Z \subset Z' \subset X$,*

$$\lambda_Z \leq \lambda_{Z'}.$$

2010 *Mathematics Subject Classification.* 11D75,11G50,14F18,14E30,14J17.

(3) *For closed subvarieties* $Z, Z' \subset X$,

$$\lambda_{Z+Z'} = \lambda_Z + \lambda_{Z'}.$$

Here, if Z *and* Z' *are defined by ideal sheaves* $\mathfrak{a}$ *and* $\mathfrak{a}'$ *respectively, then* $Z + Z'$ *is the closed subscheme defined by the product* $\mathfrak{a}\mathfrak{a}'$.

(4) *For closed subvarieties* $Z, Z' \subset X$,

$$\lambda_{Z\cap Z'} = \min\{\lambda_Z + \lambda_{Z'}\}.$$

Here, if Z *and* Z' *are defined by ideal sheaves* $\mathfrak{a}$ *and* $\mathfrak{a}'$ *respectively, then* $Z \cap Z'$ *is the closed subscheme defined by the sum* $\mathfrak{a} + \mathfrak{a}'$.

Let $X = \mathbb{P}^n_k$ *be a projective space of dimension* n *with homogeneous coordinates* $x_0, \dots, x_n$ *and* D *the Cartier divisor defined by a homogeneous polynomial* $f \in k[x_0, \dots, x_n]$ *of degree* d. *Then the function*

$$\lambda_{D_i}((x_0 : \cdots : x_n), v) := -\log \frac{\|f(x_0, \dots, x_n)\|_v}{\max\{\|x_0\|_v, \dots, \|x_n\|_v\}^d}$$

is a Weil function with respect to D.

Lemma 1.2. *Let* X *be a projective variety and* $C, D \subset X$ *proper closed subschemes with* $C \cap D = \emptyset$. *Let* $h_D \colon X(k) \to \mathbb{R} \cup \{\infty\}$ *be a height function of* D. *Then its restriction* $h_D|_{C(k)}$ *is a bounded function.*

Proof. From the functoriality of the Weil function, $h_D|_{C(k)}$ is a height function of $D \cap C$ as a closed subscheme of C. In our situation, it is empty and any height function of it is bounded. □

2. Greatest common divisors

Lemma 2.1. *Let* $Z \subset \mathbb{P}^n_{\mathbb{Q}}$ *be the closed subscheme defined by the ideal* $\langle f_1, \dots, f_l\rangle \subset \mathbb{Q}[x_0, \dots, x_n]$ *generated by homogenous polynomials* $f_1, \dots, f_l \in \mathbb{Z}[x_0, \dots, x_n]$. *For a point* $x \in \mathbb{P}^n_{\mathbb{Q}}(\mathbb{Q})$, *we write* $x = (x_0 : x_1 : \cdots : x_n)$ *in terms of integers* x_i *with* $\gcd(x_0, x_1, \dots, x_n) = 1$ *and define* $f_i(x) := f_i(x_0, \dots, x_n) \in \mathbb{Z}$. *Then*

$$N_Z(x) := \log \gcd(f_1(x), \dots, f_l(x))$$

is a counting function of Z *with respect to* $S = \{\infty\}$, *and*

$$h_Z(x) := \log \gcd(f_1(x), \dots, f_l(x)) - \max_{1\le i\le l} \log \frac{|f_i(x)|_\infty}{\max\{|x_0|_\infty, \dots, |x_n|_\infty\}^{\deg f_i}}$$

is a height function of Z.

Proof. We first note that for integers a_i,

$$\log \gcd(a_1, \dots, a_l) = -\sum_{p\in M_{\mathbb{Q}};\, p\neq\infty} \max_i |a_i|_p.$$

From Propositions 1.1 and 1.1,

$$\lambda_{Z,p}(x) := \min_{1\le i\le l} \left\{-\log \frac{|f_i(x)|_p}{\max\{|x_0|_p, \dots, |x_n|_p\}^{\deg f_i}}\right\} \quad (p \in M_{\mathbb{Q}})$$

is a Weil function of Z. For $p \neq \infty$, since $\gcd(x_0, \dots, x_n) = 1$, we have

$$\max\{|x_0|_p, \dots, |x_n|_p\} = 1$$

and

$$\lambda_{Z,p}(x) = -\log \max_i |f_i(x)|_p.$$

We conclude that

$$\begin{aligned} N_Z(x) :&= \sum_{p \in M_{\mathbb{Q}};\, p \neq \infty} \lambda_{Z,p}(x) \\ &= -\sum_{p \in M_{\mathbb{Q}};\, p \neq \infty} \log \max_i |f_i(x)|_p \\ &= \log \gcd(f_1(x), \dots, f_l(x)) \end{aligned}$$

is a counting function of Z and

$$\begin{aligned} h_Z(x) &:= N_Z(x) + \lambda_{Z,\infty}(x) \\ &= \log \gcd(f_1(x), \dots, f_l(x)) - \max_{1 \le i \le l} \log \frac{|f_i(x)|_\infty}{\max\{|x_0|_\infty, \dots, |x_n|_\infty\}^{\deg f_i}} \end{aligned}$$

is a height function of Z. □

Example 2.2. For $l < n$, let Z be the linear subspace defined by

$$x_0 = x_1 = \cdots = x_l = 0.$$

Then

$$N_Z(x) = \log \gcd(x_0, \dots, x_l)$$

is a counting function of Z. Since

$$\begin{aligned} &\max_{0 \le i \le l} \frac{|x_i|_\infty}{\max\{|x_0|_\infty, \dots, |x_n|_\infty\}} \\ &= \frac{\max\{|x_0|_\infty, \dots, |x_l|_\infty\}}{\max\{|x_0|_\infty, \dots, |x_n|_\infty\}} \\ &= \min\left\{1, \frac{\max\{|x_0|_\infty, \dots, |x_l|_\infty\}}{\max\{|x_{l+1}|_\infty, \dots, |x_n|_\infty\}}\right\}, \end{aligned}$$

the function

$$h_Z(x) = \log \gcd(x_0, \dots, x_l) - \log \min\left\{1, \frac{\max\{|x_0|_\infty, \dots, |x_l|_\infty\}}{\max\{|x_{l+1}|_\infty, \dots, |x_n|_\infty\}}\right\}$$

is a height function of Z.

Lemma 2.3. *Let X be an irreducible projective variety of dimension one over a number field k and $\pi\colon \tilde{X} \to X$ the normalization. Let $Z \subset X$ be a proper closed subscheme and $l \in \mathbb{Z}$ the degree of the scheme-theoretic pull-back $\pi^{-1}Z$ naturally regarded as a divisor. Let D be a divisor of X of degree l supported in the smooth locus of X. Then, for every $\epsilon > 0$, their exist constants $C_1, C_2 > 0$ such that for all $x \in (X \setminus Z)(\bar{k})$,*

$$(1-\epsilon)h_D(x) - C_1 \le h_Z(x) \le (1+\epsilon)h_D(x) + C_2. \tag{2.1}$$

Moreover, if X is rational (that is, birational to $\mathbb{P}^1_k$), then

$$h_Z(x) = h_D(x) + O(1).$$

Proof. Let $\tilde{Z} := \pi^{-1}Z$ and $\tilde{D} := \pi^*D$. Since they are divisors of equal degree, height functions $h_{\tilde{Z}}$ and $h_{\tilde{D}}$ are quasi-equivalent (see [Lan83, Cor. 3.5, Ch. 4]), hence so are h_D and h_Z; it exactly means (2.1). If X is rational, then $\tilde{Z}$ and $\tilde{D}$ are linearly equivalent. Therefore $h_{\tilde{Z}}$ and $h_{\tilde{D}}$ differs only by a bounded function, and the same holds for h_Z and h_D. □

Theorem 2.4. *Let $X \subset \mathbb{P}^2_k$ be an integral plane curve of degree d and let $O := (0:0:1) \in \mathbb{P}^2_k(k)$. Suppose that X has multiplicity m at O, that is, m is the largest integer n such that $\mathcal{I}_{X,O} \subset \mathfrak{m}_O^n$, where $\mathcal{I}_X \subset \mathcal{O}_{\mathbb{P}^2_k}$ is the defining ideal sheaf of X, $\mathcal{I}_{X,O}$ is its stalk at O and $\mathfrak{m}_O$ is the maximal ideal of the local ring $\mathcal{O}_{\mathbb{P}^2_k,O}$. Let h be the standard logarithmic height on $\mathbb{P}^2_k$ given by*

$$h((x:y:z)) = \sum_{w \in M_L} \log \max\{\|x\|_w, \|y\|_w, \|z\|_w\}$$

for so large finite extention L/k that $x, y, z \in L$. Then, for every $\epsilon > 0$, their exist constants $C_1, C_2 > 0$ such that for all $x \in (X \setminus \{O\})(\bar{k})$,

$$\left(\frac{m}{d} - \epsilon\right) h(x) - C_1 \le h_O(x) \le \left(\frac{m}{d} + \epsilon\right) h(x) + C_2.$$

Moreover, if X is rational, then

$$h_O(x) = \frac{m}{d} h(x) + O(1).$$

Proof. The standard height h is a height function of a line in $\mathbb{P}^2_k$. Take a general line L which does not meet any singularity of X. We regard the closed point O as a reduced scheme and apply Lemma 2.3 to $Z = O$ and $D = L \cap X$. To see the assertion, we need to show that m is equal to l as in Lemma 2.3. Since these numbers are stable under extension of the base field, we consider a plane curve germ $\hat{X} = \operatorname{Spec} \bar{k}[[x,y]]/\langle f \rangle$ defined over $\bar{k}$. The multiplicity is then equal to the order of f. If $\hat{X}_i$, $i = 1, \dots, r$, are the irreducible components of $\hat{X}$ and if m_i and l_i are the numbers similarly defined for $\hat{X}_i$, then

$$m = \sum_{i=1}^r m_i \text{ and } l = \sum_{i=1}^r l_i.$$

Therefore, we may assume that $\hat{X}$ is irreducible. Then $\hat{X} \cong \operatorname{Spec} \bar{k}[[g,h]]$, where $g, h \in \bar{k}[[t]]$ are power series of distinct orders such that $\operatorname{Spec} \bar{k}[[t]] \to \hat{X}$ is birational. Now it is easy to see that

$$m = \min\{\operatorname{ord}(g), \operatorname{ord}(f)\} = l.$$

We have completed the proof. □

Note that the theorem is valid even if $O \notin X$; then $m = 0$ and h_O is bounded (Lemma 1.2). The theorem asserts that a singular point has more rational points around it more than a smooth point does and that its extent is determined by the multiplicity, the most fundamental invariant of plane curve singularities.

Remark 2.5. Theorem 2.4 is non-trivial only when X has infinitely many k-points; it means from Faltings' theorem that X has a geometric irreducible component birational to $\mathbb{P}^1$ or an elliptic curve. If X is smooth, then this is possible only when $d \leq 3$. However, if we allow singularities, then there exist plane curves of arbitrary degree having infinitely many k-points.

Specializing the theorem to the case $k = \mathbb{Q}$ and to $\mathbb{Q}$-rational points, we obtain:

Corollary 2.6. *Let $f(x, y) \in \mathbb{Q}[x, y]$ be an irreducible polynomial and let d and m be the degree and the order of f respectively. Then, for every $\epsilon > 0$, their exist positive constants C_1, C_2 such that for all triplets $(x, y, z) \neq (0, 0, 0)$, $(0, 0, 1)$ of integers satisfying* $\gcd(x, y, z) = 1$ *and $f(x, y, z) = 0$, we have*

$$\left(\frac{m}{d} - \epsilon\right) \log \max\{|x|, |y|, |z|\} - C_1 \leq \log \gcd(x, y) - \log \min\left\{1, \frac{\max\{|x|, |y|\}}{|z|}\right\} \leq \left(\frac{m}{d} + \epsilon\right) \log \max\{|x|, |y|, |z|\} + C_2. \tag{2.2}$$

Moreover, if X is rational, then

$$\log \gcd(x, y) - \log \min\left\{1, \frac{\max\{|x|, |y|\}}{|z|}\right\} = \frac{m}{d} \log \max\{|x|, |y|, |z|\} + O(1).$$

Furthermore, excluding points close to the origin relative to the Euclidean topology, we obtain the following simpler estimation.

Corollary 2.7. *With the same notation as above, for every $\epsilon, \delta > 0$, their exist positive constants C_1', C_2' such that for all triplets $(x, y, z) \neq (0, 0, 0)$, $(0, 0, 1)$ of integers satisfying* $\gcd(x, y, z) = 1$, *$f(x, y, z) = 0$ and* $\max\{|x/z|, |y/z|\} \geq \delta$, *we have*

$$C_1' \max\{|x|, |y|\}^{m/d-\epsilon} \leq \gcd(x, y) \leq C_2' \max\{|x|, |y|\}^{m/d+\epsilon}.$$

Moreover, if X is rational, then we can replace ϵ with zero.

Proof. From the condition $\max\{|x/z|, |y/z|\} \geq \delta$, the term

$$-\log \min\left\{1, \frac{\max\{|x|, |y|\}}{|z|}\right\}$$

in (2.2) is bounded and hence can be eliminated. If $\delta \geq 1$, then the condition $\max\{|x/z|, |y/z|\} \geq \delta$ implies

$$\log \max\{|x|, |y|, |z|\} - \log \max\{|x|, |y|\} = 0.$$

If $\delta < 1$, then

$$\begin{aligned} 0 &\leq \log \max\{|x|, |y|, |z|\} - \log \max\{|x|, |y|\} \\ &\leq -\log \max\{|x/z|, |y/z|\} \leq -\log \delta. \end{aligned}$$

Therefore $\log \max\{|x|, |y|, |z|\}$ in (2.2) can be replaced with $\log \max\{|x|, |y|\}$. Writing the resulting inequalities mutliplicatively, we obtain the corollary. □

Note that the condition imposed in the last corollary on triplets (x, y, z) are satisfied by $(x, y, 1)$ for integer pairs (x, y) with $f(x, y) = 0$.

Example 2.8. Let $X \subset \mathbb{A}^2_{\mathbb{Q}}$ be the affine plane curve defined by $x^d = y^m$ for coprime positive integers d, m with $d > m$. This curve is rational and has degree d and multiplicity m at O. An integral point p of X is of the form (a^m, a^d) for an integer a. With $O = (0, 0)$, we have

$$\gcd(a^m, a^d) = |a^m| = \max\{|a^m|, |a^d|\}^{m/d}.$$

Next consider the affine plane curve Y defined by $(x+1)^d = (y+1)^m$ for the same d, m as above. This is a translation of X. Note that Y contains O as a smooth point, namely Y has multiplicity one at O. An integral point p of Y is of the form $(a^m - 1, a^d - 1)$ for an integer a. We claim that for $|a| > 1$,

$$\gcd(a^m - 1, a^d - 1) = |a - 1|.$$

To show this, we need to show that

$$\gcd(a^{m-1} + a^{m-1} + \cdots + 1, a^{d-1} + a^{d-1} + \cdots + 1) = 1,$$

which can be proved by induction and using the fact that

$$\begin{aligned}&\gcd(a^{m-1} + a^{m-1} + \cdots + 1, a^{d-1} + a^{d-1} + \cdots + 1)\\ &= \gcd(a^{m-1} + a^{m-1} + \cdots + 1, a^{(d-m)-1} + a^{(d-m)-1} + \cdots + 1).\end{aligned}$$

From the claim,

$$\gcd(a^m - 1, a^d - 1) \sim \max\{|a^m - 1|, |a^d - 1|\}^{1/d} \quad (|a| \to \infty).$$

Finally consider the curve Z defined by $x^d = (y + 1)^m$. This curve does not pass through the origin, equivalently it has multiplicity $m = 0$ at O. An integral point p of Z is of the form $(a^m, a^d - 1)$ for an integer a. Clearly

$$\gcd(a^m, a^d - 1) = 1 = \max\{|a^m|, |a^d - 1|\}^{0/d}.$$

References

[BCZ03] Yann Bugeaud, Pietro Corvaja, and Umberto Zannier. An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.*, 243(1):79–84, 2003.

[CZ05] Pietro Corvaja and Umberto Zannier. A lower bound for the height of a rational function at S-unit points. *Monatsh. Math.*, 144(3):203–224, 2005.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Sil87] Joseph H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. *Math. Ann.*, 279(2):193–216, 1987.

[Sil05] Joseph H. Silverman. Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. *Monatsh. Math.*, 145(4):333–350, 2005.

[Yas11] Yu Yasufuku. Vojta's conjecture on blowups of $\mathbb{P}^n$, greatest common divisors, and the *abc* conjecture. *Monatsh. Math.*, 163(2):237–247, 2011.

[Yas12] Yu Yasufuku. Integral points and Vojta's conjecture on rational surfaces. *Trans. Amer. Math. Soc.*, 364(2):767–784, 2012.

[Yas16] Takehiko Yasuda. Vojta's conjecture for singular varieties. arXiv:1610.03593v1, 2016.

[Yas18] Takehiko Yasuda. Vojta's conjecture, singularities and multiplier-type ideals. *Kodai Math. J.*, 41(3):566–578, 2018.

Department of Mathematics, Graduate School of Science, Osaka University, Toyonaka, Osaka 560-0043, Japan, tel:+81-6-6850-5326, fax:+81-6-6850-5327

Email address: takehikoyasuda@math.sci.osaka-u.ac.jp