

## WELL-APPROXIMATED POINTS ON LINEAR EXTENSIONS OF ELLIPTIC CURVES

DEANNA M. CAVENY AND ROBERT TUBBS

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. We employ a result on linear forms in logarithms of algebraic points on commutative algebraic groups, a study initiated by Philippon and Waldschmidt, a so-called “local nullstellen inequality” of Brownawell, and some elementary analytic estimates to study the approximation properties of coordinates of non-generic points on a linear (algebraic) group extension of an elliptic curve.

### 1. INTRODUCTION

In this paper we examine transcendental points that lie on a one-parameter subgroup of a non-split, linear (algebraic) group extension of an elliptic curve and that have one coordinate that is well-approximated by algebraic numbers of bounded degree. We will show that there are limits as to how well a coordinate of a non-generic point on a one-parameter subgroup of such an extension can be approximated by algebraic numbers of bounded degree. To set notation, let  $E$  denote an elliptic curve defined over  $\overline{\mathbb{Q}}$ , and let  $G$  be an extension of  $E$  by either  $\mathbb{G}_a$  or  $\mathbb{G}_m$ . There is then an exact sequence of commutative algebraic groups:

$$(1.1) \quad 0 \longrightarrow L \xrightarrow{i} G \xrightarrow{\pi} E \longrightarrow 0,$$

where  $L$  is either  $\mathbb{G}_a$  or  $\mathbb{G}_m$ . In either case, let  $\overline{L}$  denote a compactification of  $L$  which we view as embedded in  $\mathbb{P}_1$ . (When  $L = \mathbb{G}_a$  (resp.  $L = \mathbb{G}_m$ ),  $\overline{L}$  is obtained by adjoining one (resp. two) points.) We then obtain the short exact sequence

$$0 \longrightarrow \mathbb{P}_1 \xrightarrow{i} \overline{G} \xrightarrow{\pi} E \longrightarrow 0.$$

J.-P. Serre, [Se], has described how to embed such extensions of elliptic curves into projective space. If we let  $0$  denote the identity element in  $E$  and  $\pi^*$  the pull-back of  $\pi$ , then the divisor  $D = (\overline{G} - G) + 3\pi^*(0)$  is very ample for  $\overline{G}$ . Moreover,  $l(D) = 6$  when  $L = \mathbb{G}_a$  and  $l(D) = 9$  when  $L = \mathbb{G}_m$ . Hence we obtain an embedding of  $\overline{G}$  into  $\mathbb{P}_5$  in the additive case and into  $\mathbb{P}_8$  in the multiplicative case, each of which can be given an explicit analytic description in terms of the Weierstrass functions  $\wp(z)$ ,  $\zeta(z)$ , and  $\sigma(z)$  associated with  $E$ . We do not recall the definitions of these functions here; however we do recall the notation that for  $\omega$

---

Received by the editors December 13, 2009.

2010 *Mathematics Subject Classification*. Primary 11J89.

The authors would like to thank the referee(s) for valuable and insightful feedback, which contributed to substantial improvements in the manuscript and its results.

©2010 American Mathematical Society  
Reverts to public domain 28 years from publication

in the lattice of periods  $\Lambda$  of  $E$ , its associated quasi-period  $\eta(\omega) \in \mathbb{C}$  satisfies the relation  $\zeta(z + \omega) = \zeta(z) + \eta(\omega)$  for all  $z \in \mathbb{C}$ .

Since the two cases  $L = \mathbb{G}_a$  and  $L = \mathbb{G}_m$  depend on different embeddings into projective space, it is not natural to consider them together. So, after describing the two embeddings and stating our main result, we will consider these two cases separately.

2. STATEMENT OF RESULTS

Before we can state our main result, we must describe the embedding of  $\overline{G}$  into projective space. To do this we first introduce two new functions: For complex numbers  $b$  and  $u_0$ , with  $u_0 \notin \Lambda$ , let

$$(2.1) \quad f_1(t, z) = t + b\zeta(z) \quad \text{and} \quad g_1(t, z) = \frac{\sigma(z - u_0)}{\sigma(z)\sigma(u_0)} e^{t+z\zeta(u_0)}.$$

Affiliated with  $f_1(t, z)$  and  $g_1(t, z)$  are additional coordinate functions of the embedding of  $G$  into projective space. In our notation, we will generally suppress the dependence of these functions on the numbers  $b$  and  $u_0$ . We define

$$(2.2) \quad f_2(t, z) = \wp(z)f_1(t, z) + \frac{b}{2}\wp'(z), \quad f_3(t, z) = \wp'(z)f_1(t, z) + 2b\wp^2(z),$$

and

$$(2.3) \quad \begin{aligned} g_2(t, z) &= g_1(-t, -z), & g_3(t, z) &= \wp(z)g_1(t, z), & g_4(t, z) &= \wp(z)g_1(-t, -z), \\ g_5(t, z) &= g_1(t, z) \frac{\wp'(z) + \wp'(u_0)}{\wp(z) - \wp(u_0)}, & g_6(t, z) &= g_1(-t, -z) \frac{\wp'(-z) + \wp'(u_0)}{\wp(-z) - \wp(u_0)}. \end{aligned}$$

With these in mind, we define two new functions by

$$(2.4) \quad \Phi_a(t, z) = \begin{cases} (1; \wp(z); \wp'(z); f_1(t, z); f_2(t, z); f_3(t, z)), & \text{for } z \notin \Lambda, \\ (0; 0; 1; 0; 0; t + b\eta(z)), & \text{for } z \in \Lambda, \end{cases}$$

and

$$(2.5) \quad \begin{aligned} &\Phi_m(t, z) \\ &= \begin{cases} (1; \wp(z); \wp'(z); g_1(t, z); g_2(t, z); g_3(t, z); g_4(t, z); g_5(t, z); g_6(t, z)), & \text{for } z \notin \Lambda \\ (0; 0; 1; 0; 0; \frac{\sigma(z-u_0)}{\sigma(u_0)} e^{t+z\zeta(u_0)}; \frac{\sigma(-z-u_0)}{\sigma(u_0)} e^{-t-z\zeta(u_0)}; 0; 0), & \text{for } z \in \Lambda. \end{cases} \end{aligned}$$

The following proposition, established in [Se], points to the importance of  $\Phi_a(t, z)$  and  $\Phi_m(t, z)$  in our study.

**Proposition 2.1.** *Assume that  $E$  is defined over  $\overline{\mathbb{Q}}$  and let  $G$ ,  $\overline{G}$ , and  $D$  be as above. Then the following hold:*

*If  $L = \mathbb{G}_a$ , there exists a non-zero algebraic number  $b$  such that  $\Phi_a(t, z)$  parametrizes a quasi-projective variety in  $\mathbb{P}_5$  which is isomorphic, as a group, to  $G$ .*

*If  $L = \mathbb{G}_m$ , there exists a non-torsion algebraic point  $u_0$  of  $\wp(z)$  such that  $\Phi_m(t, z)$  parametrizes a quasi-projective variety in  $\mathbb{P}_8$  which is isomorphic, as a group, to  $G$ .*

*Proof.* To obtain these functions one simply writes (explicitly) a basis for  $\mathcal{L}(D)$ . This is implicit in [Se] but has been made explicit in [Hi]. □

We will study points on a one-parameter subgroup of  $G(\mathbb{C})$  that have a coordinate which is well-approximated by algebraic numbers of bounded degree. To make these notions precise we begin with the following definition.

**Definition 2.2.** Let  $d_0 \in \mathbb{N}$  and  $\Delta : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ . A complex number  $\theta$  is said to be  $(d_0, \Delta)$ -approximable if there exists an infinite sequence  $\{t_k\}$  of positive real numbers, with  $\lim_{k \rightarrow \infty} t_k = \infty$ , and a corresponding sequence of algebraic numbers  $\{a_k\}$ , with  $\deg a_k \leq d_0$ ,  $\text{ht } a_k \leq t_k$ , satisfying

$$0 \neq |\theta - a_k| < e^{-\Delta(t_k)},$$

where  $\text{ht } a_k$  denotes the logarithmic height of  $a_k$ .

*Remark 2.3.* Note that if  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k} = \infty$ , then a Liouville estimate, such as Proposition 3.14 of [Wa 2000], for example, shows that  $\theta \notin \overline{\mathbb{Q}}$ .

When  $G$  is embedded into projective space as above, a one-parameter subgroup  $\phi : \mathbb{C} \rightarrow G(\mathbb{C})$  may be expressed in terms of the coordinate functions in (2.4) or (2.5). Specifically, there exist complex numbers  $\beta$  and  $\gamma$ , or  $\beta'$  and  $\gamma'$ , so that

$$(2.6) \quad \phi(z) = \Phi_a(\beta z, \gamma z) \quad (\text{or } \phi(z) = \Phi_m(\beta' z, \gamma' z)).$$

We will assume throughout this paper that the image  $\phi(\mathbb{C})$  is Zariski-dense in  $G(\mathbb{C})$ . This implies that each of  $\beta$ ,  $\gamma$ , and  $b$  is non-zero in the  $\mathbb{G}_a$  case, and each of  $\beta'$ ,  $\gamma'$ , and  $\zeta(u_0)$  is non-zero in the  $\mathbb{G}_m$  case. We lose no generality if we assume that  $\gamma = \gamma' = 1$ . In addition to assuming that  $G$  is defined over  $\overline{\mathbb{Q}}$ , we will assume that  $\phi(z)$  is as well; that is, we assume both  $\beta$  and  $\beta'$  are algebraic.

Our main result of this paper is the following.

**Theorem 2.4.** *Suppose that  $G$  is either a  $\mathbb{G}_a$  or a  $\mathbb{G}_m$  extension of an elliptic curve  $E$ , which is defined over  $\overline{\mathbb{Q}}$ , with  $G$  embedded into projective space as in Proposition 2.1. Let  $\phi(z)$  be a one-parameter subgroup of  $G$ , also defined over  $\overline{\mathbb{Q}}$ , whose image is Zariski-dense in  $G(\mathbb{C})$ .*

**a.** *Suppose  $P = \phi(u)$ , with  $u \notin \Lambda$ , is not a generic point over  $\mathbb{Q}$  for  $G$  and has a coordinate which is  $(d_0, \Delta)$ -approximable. Then for every  $\epsilon > 0$ , we have*

$$\lim_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} = 0.$$

**b.** *Equivalently, if  $P \in G(\mathbb{C})$  has a  $(d_0, \Delta)$ -approximable coordinate satisfying  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} \neq 0$  for some  $\epsilon > 0$ , then two coordinates of  $P$  are algebraically independent over  $\mathbb{Q}$ .*

We note that, in light of Remark 2.3, the power of  $t$  in the denominator of the limits in Theorem 2.4 is best possible. However, we also note that in this theorem, and so also in the following corollary, our proof will allow us to replace  $t_k^{1+\epsilon}$  by  $t_k(\log t_k)^{3+\epsilon}$ .

It is possible to glean from this theorem information concerning the algebraic independence of certain numbers. For example:

**Corollary 2.5.** *If  $\wp(u)$  is  $(d_0, \Delta)$ -approximable with  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} \neq 0$  for some  $\epsilon > 0$ , then for any non-zero algebraic number  $\beta$ , the numbers  $f_1(\beta u, u)$  and  $\wp(u)$  and the numbers  $g_1(\beta u, u)$  and  $\wp(u)$  are algebraically independent.*

*Remark 2.6.* For completeness we note that it can be deduced from Theorem 5 of [Ca-Tu] that under the hypotheses of Theorem 2.4 the other non-integral coordinates of  $P$  are well-approximated by algebraic numbers of bounded degree.

### 3. PRELIMINARY RESULTS

We begin with the following formulation of linear forms in logarithms.

**Proposition 3.1.** *Suppose  $G$  is a non-split extension of  $E$  by either  $\mathbb{G}_a$  or  $\mathbb{G}_m$ , with  $E$  defined over a number field  $K$ . Suppose  $(u_1, u_2) \in \mathbb{C}^2$  with  $\tau = \Phi_a(u_1, u_2)$  (resp.  $\tau = \Phi_m(u_1, u_2)$ ) in  $G(K)$ . Suppose all of  $\alpha, \beta, b, \zeta(u_0)$  and  $\sigma(u_0)$  also lie in  $K$ , and define  $D$  and  $H$  by*

$$D = [K : \mathbb{Q}] \quad \text{and} \quad H = \max \left\{ e, \text{ht}(\alpha), \text{ht}(\beta), \frac{\text{ht}(\tau)}{D}, \frac{\|(u_1, u_2)\|^2}{D} \right\},$$

where  $\text{ht}$  continues to denote the logarithmic height. Then there exists a constant  $C_G > 0$ , depending only on  $G$  and its embedding into projective space, so that if  $\alpha u_1 + \beta u_2 \neq 0$ , then

$$|\alpha u_1 + \beta u_2| > \exp(-C_G B(D, H)),$$

where

$$(3.1) \quad B(D, H) = D^4 (\log H + \log D) (\log \log H + \log D)^3.$$

*Proof.* See [H-K], where the result of [Ph-Wa] is improved to the above expression for  $B(D, H)$ . □

We will use the next result, concerning algebraic points on  $\phi(\mathbb{C})$ , to conclude that a certain linear form in logarithms of algebraic points is non-zero, and hence its modulus can be bounded away from zero by Proposition 3.1.

**Lemma 3.2.** *If  $\phi(z)$  is defined over  $\overline{\mathbb{Q}}$  and its image is Zariski-dense in  $G(\mathbb{C})$ , then*

$$\phi(\mathbb{C}) \cap G(\overline{\mathbb{Q}}) = \phi(0).$$

*Proof.* This result is nothing more than the Schneider-Lang Theorem. It has been codified by Waldschmidt in [Wa 1979], in the  $\mathbb{G}_a$  case as Theorem 3.2.6 and in the  $\mathbb{G}_m$  case as Theorem 3.2.10. □

### 4. ADDITIONAL PRELIMINARY RESULTS: THE $\mathbb{G}_a$ CASE

Our results provide information about the coordinate functions of  $\Phi_a$  and  $\Phi_m$  when they are evaluated at points in  $\mathbb{C}^2$  and hence depend, in part, on the behavior of these functions near the point under consideration. This information is encoded in two real numbers that we associate with each  $u \in \mathbb{C}$ . To define these, we write the equation defining an affine part of the elliptic curve in its Weierstrass form:

$$Y^2 = 4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3).$$

Then for  $u \in \mathbb{C}$ , we define two functions:

$$\kappa(u) = \min_{i=1,2,3} |\wp(u) - e_i| \quad \text{and} \quad \lambda(u) = \min_{\omega \in \Lambda} |u - \omega|.$$

Essentially,  $\kappa(u)$  measures how close  $u$  is to a zero of  $\wp'(z)$ , and  $\lambda(u)$  measures how close  $u$  is to a pole of  $\wp(z)$ .

**Lemma 4.1.** *Let  $u \in \mathbb{C}$ . Suppose that for  $a \in \mathbb{C}$ , we have  $|\wp(u) - a| < \epsilon < \kappa(u)$  for some real  $\epsilon$ . Then there exists  $u' \in \mathbb{C}$  with  $\wp(u') = a$  and  $|u - u'| < \frac{\epsilon}{2(\kappa(u) - \epsilon)^{3/2}}$ .*

*Proof.* We define  $\kappa(u)$  as above, and we let  $u$  and  $a$  be complex numbers with  $|\wp(u) - a| < \epsilon < \kappa(u)$  for some real  $\epsilon$ . Let  $L$  denote the line segment from  $a$  to  $\wp(u)$ . In our argument, it is helpful to explicitly identify the root of  $4X^3 - g_2X - g_3 = 0$  with the largest real part, and if there is more than one such root, the positive imaginary part. We call this root  $e_3$  and the other finite roots  $e_1$  and  $e_2$ .

We start with the case where  $\kappa(u)$  is  $|\wp(u) - e_1|$  or  $|\wp(u) - e_2|$ . We fix one branch cut to be the line segment from  $e_1$  to  $e_2$ , deformed if necessary, so as not to intersect  $L$ . Since  $|\wp(u) - a| < \epsilon < \kappa(u)$ , this deformation can be done so there remains an open circle around  $e_3$  which the resulting branch cut doesn't intersect. We fix our other branch cut to be from  $e_3$  to infinity. We have ensured that our path  $L$  doesn't pass through any of the roots  $e_1$ ,  $e_2$ , and  $e_3$  and doesn't cross either of the branch cuts, so there exists  $u' \in \mathbb{C}$  satisfying  $\wp(u') = a$  and

$$(4.1) \quad u - u' = \int_L \frac{dt}{\sqrt{4t^3 - g_2t - g_3}}.$$

Our remaining case is when  $\kappa(u) = |\wp(u) - e_3|$ . Here we fix one branch cut to be the line segment from  $e_1$  to  $e_2$  and the second cut to be from  $e_3$  to infinity, with this second branch cut deformed, if needed, so as not to intersect  $L$ . As above, this deformation can be accomplished without interfering with the other branch cut. Again, there exists  $u' \in \mathbb{C}$  satisfying  $\wp(u') = a$  and (4.1).

Then, in both cases,  $|u - u'| \leq |\wp(u) - \wp(u')| \max_{\xi \in \gamma} \frac{1}{|\wp'(\xi)|}$ , where  $\{\wp(\xi) : \xi \in \gamma\}$  is the path  $L$ . For  $\xi \in \gamma$ , we now have

$$|\wp'(\xi)|^2 \geq 4 \left( \min_{1 \leq i \leq 3} |\wp(\xi) - e_i| \right)^3 \geq 4(\kappa(u) - \epsilon)^3,$$

from which the lemma follows.  $\square$

Lemma 4.1 allows us to derive a simultaneous approximation measure for  $\wp(u)$  and  $f_1(\beta u, u)$  from the lower bound on a linear form in logarithms in Proposition 3.1.

**Theorem 4.2.** *Suppose that all of  $\beta, b, \zeta(u_0), \sigma(u_0), \alpha, \gamma$ , and  $\delta$  lie in  $K$ , the (algebraic) field of definition of  $E$ . Take  $D, H, B(D, H)$ , and  $C_G$  as in Proposition 3.1, where in the definition of  $H$  we replace  $\text{ht}(\tau)$  by  $\max\{\text{ht}(\alpha), \text{ht}(\gamma), \text{ht}(\delta)\}$ . For any  $u \in \mathbb{C}$ , there exists a constant  $C_a(u)$  such that if*

$$B(D, H) > \frac{1}{9C_G} \max\{8 \log 2 - \min\{0, 3 \log \kappa(u), 2 \log \lambda(u)\}, \log(|\beta| + |b|C_a(u))\},$$

then

$$(4.2) \quad |f_1(\beta u, u) - \alpha| + |\wp(u) - \delta| > \exp(-9C_G B(D, H)).$$

*Proof.* If (4.2) fails to hold, we have

$$|\wp(u) - \delta| \leq \exp(-9C_G B(D, H)).$$

Thanks to the assumed lower bound on  $B(D, H)$  in the statement of the theorem, Lemma 4.1 implies that there exists  $u' \in \mathbb{C}$  with  $\wp(u') = \delta$  and

$$|u - u'| < \exp\left(-\frac{9}{2}C_G B(D, H)\right).$$

It then follows from the definition of  $f_1$  that

$$|f_1(\beta u', u') - f_1(\beta u, u)| < \exp\left(-\frac{9}{4}C_G B(D, H)\right).$$

An application of the triangle inequality then yields

$$(4.3) \quad |f_1(\beta u', u') - \alpha| < \exp\left(-\frac{9}{8}C_G B(D, H)\right).$$

However, (4.3) can be viewed as a non-zero linear form in logarithms by recalling that  $f_1(\beta u', u') = \beta u' + b\zeta(u')$  and taking  $v' = \alpha - b\zeta(u')$ . The inequality in (4.3) then becomes  $|\beta u' - v'| < \exp\left(-\frac{9}{8}C_G B(D, H)\right)$ , where  $\Phi_a(v', u') \in G(\overline{\mathbb{Q}})$ .

In order to apply Proposition 3.1 we need to know that this linear form does not vanish. This follows from Lemma 3.2, since if it does vanish, then  $v' = \beta u'$  and consequently

$$\Phi_a(v', u') = \Phi_a(\beta u', u') = \phi(u').$$

Lemma 3.2 then implies  $u' = 0$ , which cannot hold since  $\wp(u') = \delta$ . Thus by Proposition 3.1,  $|v' - \beta u'| > \exp(-C_G B(D, H))$ , contradicting (4.3) and concluding the proof.  $\square$

Theorem 4.2 yields transcendence measures for transcendental numbers associated with algebraic points on  $E$ . For example: Suppose  $\wp(u)$  is algebraic. Then  $\beta u + b\zeta(u)$  is transcendental with the transcendence measure

$$\exp(-B(D, \log H + \log D) - 2D(\log H + D)).$$

In particular, using the expression (3.1) for  $B(D, H)$ , we get a transcendence measure for  $\beta u + b\zeta(u)$  of

$$\exp(-2D^4(\log H + \log D)(\log(\log H) + \log D)^3),$$

which is comparable with previously published estimates, for example those in [Re].

### 5. PROOF OF THEOREM 2.4: THE $\mathbb{G}_a$ CASE

Our goal is to show that for every  $\epsilon > 0$ , we have  $\lim_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} = 0$ . We are done if we can show that  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}}$  is bounded for every  $\epsilon > 0$ , because then  $\lim_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+2\epsilon}} = 0$ . We proceed by contradiction, assuming that  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} = \infty$  for some  $\epsilon > 0$ .

Since we will apply an inequality from [Br], we first fix an algebraic number  $\theta$  so that  $\mathbb{Q}(b, \zeta(u_0), g_2, g_3) = \mathbb{Q}(\theta)$ . Let  $R = \mathbb{Z}[\theta][X_1, \dots, X_5]$ .

We make explicit the polynomials which define  $G \cap V(X_0 = 1)$  in affine space:

$$\begin{aligned} P_1(X_1, X_2) &= X_2^2 - (4X_1^3 - g_2X_1 - g_3), \\ P_2(X_1, X_2, X_3, X_4) &= X_4 - (X_1X_3 + \frac{b}{2}X_2), \text{ and} \\ P_3(X_1, X_2, X_3, X_5) &= X_5 - (X_2X_3 + 2bX_1^2). \end{aligned}$$

Since  $P$  is not a generic point for  $G$ , there exists a polynomial  $Q \in R$  which vanishes at  $P$  but does not lie in the ideal defining  $G$ . Thus the ideal  $I = (P_1, P_2, P_3, Q)$  is one-dimensional.

Suppose that  $\{a_k\}$  is a sequence of algebraic numbers giving rise to our assumed approximation to one of the coordinates of  $P$ , say the  $i$ th coordinate, where we assume that we have  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} = \infty$ . For each  $k$ , let  $M_k(X_i)$  denote the minimal polynomial, over  $\mathbb{Z}$ , of the algebraic approximation  $a_k$ . We claim that for infinitely many indices  $k$ , the ideal  $I_k = (I, M_k)$  is zero-dimensional. To see this, let  $V_1, \dots, V_r$  denote the irreducible components of the algebraic set  $V = V(I)$ , and let  $p_1, \dots, p_r$  denote their associated prime ideals. If for some  $k$  and  $j$ , we have  $M_k \in p_j$ , then  $V_j \subset V(M_k)$ . Hence, every point in  $V_j$  has as its  $i$ th coordinate an algebraic number which is a conjugate of  $a_k$ . This implies that any collection of more than  $rd_0$  distinct algebraic approximations contains at least one whose minimal polynomial does not lie in any of the prime ideals  $p_j$ . It follows that there are infinitely many approximations in our original sequence  $\{a_k\}$  whose minimal polynomials do not lie in any of the prime ideals  $p_j$ . For each of these approximations and corresponding indices, the ideal  $I_k$  is zero-dimensional. We now restrict our attention to only these approximations, the collection of which we again denote by  $\{a_k\}$ , and consider the associated ideals  $I_k$ .

We first let

$$D = \max\{\deg P_1, \deg P_2, \deg P_3, \deg Q, d_0\}.$$

If we take  $k$  sufficiently large so that

$$(5.1) \quad e^{t_k} > \max\{4, |g_2|, |g_3|, 2|b|, \text{Ht}(Q)\},$$

then Theorem A' of [Br] implies that if  $\rho = \rho_k$  denotes the distance, in the sup-norm, from  $P$  to the zeros of  $I_k$ , then

$$(5.2) \quad \log \max\{|P_1(P)|, |P_2(P)|, |P_3(P)|, |Q(P)|, |M_k(P)|\} > c_a[-D^3(D + t_k) + D^4 \log \rho + D^4 \log \max\{|P|, |\theta|\}^2],$$

where the positive constant  $c_a = c_a(G, \phi, \theta)$  can be explicitly computed.

Yet for  $k$  sufficiently large,  $|M_k(P)| < \exp(-\frac{1}{2}\Delta(t_k))$ , and therefore

$$(5.3) \quad \log \max\{|P_1(P)|, |P_2(P)|, |P_3(P)|, |Q(P)|, |M_k(P)|\} < -\frac{1}{2}\Delta(t_k).$$

Combining (5.2) and (5.3), we have

$$(5.4) \quad \log \rho < \frac{D^3(D + t_k) - (D^4 \log \max\{|P|, |\theta|\}^2 + \frac{\Delta(t_k)}{2c_a})}{D^4}.$$

If  $\alpha = (\alpha_1, \dots, \alpha_5)$  is a zero of the zero-dimensional ideal  $I_k$ , then each of its coordinates is an algebraic number with

$$\deg \alpha_i \leq D^5 \quad \text{and} \quad \text{ht}(\alpha_i) \leq C'(d_0 + t_k),$$

where  $C'$  depends on the polynomials  $P_1, P_2, P_3$  and  $Q$ . If we next specify that  $\alpha$  be a zero of  $I_k$  whose distance from  $P$  is the value  $\rho$  we have estimated above, we have

$$(5.5) \quad |f_1(\beta u, u) - \alpha_4| + |\wp(u) - \alpha_2| < 2\rho.$$

The left-hand side of this inequality is precisely the expression appearing in Theorem 4.2, which offers the lower bound

$$(5.6) \quad |f_1(\beta u, u) - \alpha_4| + |\wp(u) - \alpha_2| > \exp(-9C_G D^{20}(C'(d_0 + t_k) + \log D^5)(\log(C'(d_0 + t_k)) + \log D^5)^3).$$

Combining (5.4), (5.5), and (5.6), we obtain

$$10C_G D^{20}(C'(d_0 + t_k) + \log D^5)(\log(C'(d_0 + t_k)) + \log D^5)^3 > \frac{\Delta(t_k)}{2c_a D^4},$$

which cannot hold if  $\limsup_{k \rightarrow \infty} \frac{\Delta(t_k)}{t_k^{1+\epsilon}} = \infty$ .

6. ADDITIONAL PRELIMINARY RESULTS: THE  $\mathbb{G}_m$  CASE

In order to translate Proposition 3.1 into a simultaneous approximation measure, we need the following easy result concerning the  $\sigma$ -function.

**Lemma 6.1.** *Suppose  $u_2$  is a complex number such that each of the numbers*

$$\sigma(u_2), \sigma(u_2 - u_0), \sigma(-u_2 - u_0)$$

*is non-zero. Let  $\gamma$  and  $u_1$  be complex numbers satisfying*

$$(6.1) \quad \min\{|g_1(u_1, u_2)|, |\gamma|\} > \epsilon_1 \quad \text{and} \quad |g_1(u_1, u_2) - \gamma| < \epsilon_2,$$

*for some positive real numbers  $\epsilon_1$  and  $\epsilon_2$ . Then there exists  $v'$  in  $\mathbb{C}$  such that*

$$g_1(v', u_2) = \gamma \quad \text{and} \quad |u_1 - v'| < \frac{\pi \epsilon_2}{2 \epsilon_1}.$$

*Proof.* The line  $\ell$  through  $g_1(u_1, u_2)$  and  $\gamma$  partitions the plane into an open and a closed half-plane, one of which does not contain the origin. Let  $\Gamma$  denote the semi-circle centered at  $\frac{g_1(u_1, u_2) + \gamma}{2}$  passing through both  $g_1(u_1, u_2)$  and  $\gamma$  that lies in the half-plane defined by  $\ell$  not containing the origin. Note that the radius of  $\Gamma$  is  $\frac{g_1(u_1, u_2) - \gamma}{2}$ . We then have the two estimates

$$\text{length}(\Gamma) = \pi \left| \frac{g_1(u_1, u_2) - \gamma}{2} \right| < \frac{\pi}{2} \epsilon_2$$

and

$$\max_{\xi \in \Gamma} \frac{1}{|\xi|} = \frac{1}{\min\{|g_1(u_1, u_2)|, |\gamma|\}} < \frac{1}{\epsilon_1}.$$

Therefore, if we fix a branch of the logarithm whose branch cut does not pass through  $\Gamma$ , we obtain

$$|\log g_1(u_1, u_2) - \log \gamma| = \left| \int_{\Gamma} \frac{dt}{t} \right| \leq \text{length}(\Gamma) \max_{\xi \in \Gamma} \frac{1}{|\xi|} < \frac{\pi \epsilon_2}{2 \epsilon_1}.$$

The existence of  $v'$ , satisfying the conclusion of the lemma, then follows from the observation that  $g_1(t, z) = g(z)e^t$ , where, with our choices of  $u_0$  and  $u_2$ , we know that  $g(u_2) \neq 0$ . □

This lemma allows us to deduce the  $\mathbb{G}_m$ -analogue of Theorem 4.2.

**Theorem 6.2.** *Suppose that all of  $\beta$ ,  $\zeta(u_0)$ ,  $\sigma(u_0)$ ,  $\alpha$ ,  $\gamma$ , and  $\delta$  lie in  $K$ , the (algebraic) field of definition of  $E$ . Take  $D$ ,  $H$ ,  $B(D, H)$ , and  $C_G$  as in Proposition 3.1, where in the definition  $H$  we replace  $\text{ht}(\tau)$  by  $\max\{\text{ht}(\alpha), \text{ht}(\gamma), \text{ht}(\delta)\}$ . For any  $u \in \mathbb{C}$ , there exists a constant  $C_m(u, G, \phi)$  such that if*

$$B(D, H) > \frac{1}{17C_G} \max\{8 \log 2 - \min\{0, \log \kappa(u), 3 \log \kappa(u)\}, C_m(u, G, \phi)\},$$

then

$$(6.2) \quad |g_1(\beta u, u) - \gamma| + |\wp(u) - \delta| > \exp(-17C_G B(D, H)).$$

*Proof.* The proof exactly parallels that of the proof of Theorem 4.2, so we will be brief. Assume (6.2) does not hold and apply Lemma 4.1 to find  $u'$  as above. Using the analyticity of  $g_1(\beta z, z)$  at  $z = u$ , write

$$g_1(\beta u', u') = g_1(\beta u, u) + \sum_{k=1}^{\infty} a_k (u' - u)^k.$$

Then since  $|u - u'| < \exp\left(-\frac{17}{2}C_G B(D, H)\right) < 1$ , we have

$$|g_1(\beta u', u') - \gamma| \leq |g_1(\beta u, u) - \gamma| + |u - u'| C(u, G),$$

where  $C(u, G) = \max_{|z-u|<1} \left| \sum_{k=1}^{\infty} a_k (z-u)^{k-1} \right|$ , so

$$|g_1(\beta u', u') - \gamma| < \exp\left(-\frac{17}{8}C_G B(D, H)\right).$$

We apply Lemma 6.1 with  $\epsilon_1 = \frac{1}{2}|g_1(\beta u, u)|$  and  $\epsilon_2 = \frac{\pi}{2} \exp\left(-\frac{17}{8}C_G B(D, H)\right)$  to see that there exists  $v' \in \mathbb{C}$  with  $g_1(v', u') = \gamma$  and

$$|v' - \beta u'| < \exp\left(-\frac{17}{16}C_G B(D, H)\right).$$

As in the proof of the  $\mathbb{G}_a$  case above, this last inequality can be interpreted as an upper bound for the modulus of a non-zero linear form. Viewed this way, the inequality contradicts the lower bound from Proposition 3.1.  $\square$

## 7. THE PROOF OF THEOREM 2.4: THE $\mathbb{G}_m$ CASE

The remainder of the proof parallels the proof in the  $\mathbb{G}_a$  case, beginning with the ideal generated by the polynomials:

$$Q_1(X_1, X_2) = X_2^2 - (4X_1^3 - g_2X_1 - g_3),$$

$$Q_2(X_1, X_3, X_5) = X_5 - X_1X_3,$$

$$Q_3(X_1, X_4, X_6) = X_6 - X_1X_4,$$

$$Q_4(X_1, X_2, X_3, X_7) = (X_1 - \wp(u_0))X_7 - X_3(X_2 + \wp'(u_0)),$$

$$Q_5(X_1, X_2, X_4, X_8) = (X_1 - \wp(u_0))X_8 - X_4(-X_2 + \wp'(u_0)), \text{ and}$$

$$Q_6(X_1, X_3, X_4) = X_3X_4 - (X_1 - \wp(u_0)).$$

We do not include these details.

## REFERENCES

- [Br] W. D. Brownawell, Local diophantine nullstellen inequalities, *J. of the A.M.S.* 1 (1988), No. 2, pp. 311-322. MR928261 (89h:11041)
- [Ca-Tu] D. Caveny, R. Tubbs, The arithmetic of well-approximated numbers, in *Number Theory with an Emphasis on the Markoff Spectrum*, Pollington and Moran, eds., Marcel Dekker, New York, 1993, pp. 53-60. MR1219324 (94b:11059)
- [Hi] M. Hindry, Groupes algébriques commutatifs, exemples explicites, *Sem. d'Arithmétique Saint-Etienne*, Université de Saint-Etienne, France, 1988-89, pp. 9-42.
- [H-K] N. Hirata-Kohno, Formes linéaires de logarithmes de points algébriques sur les groupes algébriques, *Invent. Math.* 104 (1991), pp. 401-433. MR1098616 (91m:11050)
- [Ph-Wa] P. Philippon, M. Waldschmidt, Formes linéaires de logarithmes sur les groupes algébriques commutatifs, *Ill. J. of Math.* 32 (1988), No. 2, pp. 281-314. MR945864 (89j:11070)
- [Re] E. Reyssat, Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle, *Bull. Soc. Math. France* 108 (1980), pp. 47-79. MR603340 (82j:10064)
- [Se] J-P. Serre, Appendix in [Wa 1979]. MR570648 (82k:10041)
- [Wa 2000] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer, New York, 2000. MR1756786 (2001c:11075)
- [Wa 1979] M. Waldschmidt, Nombres transcendants et groupes algébriques, *Astérisque*, 69-70, Société Mathématique de France, 1979. MR570648 (82k:10041)

DEPARTMENT OF MATHEMATICS, COLLEGE OF CHARLESTON, 66 GEORGE STREET, CHARLESTON, SOUTH CAROLINA 29424

*E-mail address:* `cavenyd@cofc.edu`

DEPARTMENT OF MATHEMATICS, CAMPUS BOX 395, UNIVERSITY OF COLORADO, BOULDER, COLORADO 80309

*E-mail address:* `tubbs@euclid.colorado.edu`