TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 309, Number 1, September 1988

A DIOPHANTINE PROBLEM ON ELLIPTIC CURVES

ROBERT TUBBS

ABSTRACT. This paper examines simultaneous diophantine approximations to coordinates of certain points on a product of elliptic curves. Specifically, let $\wp(z)$ be a Weierstrass elliptic function with algebraic invariants and complex multiplication. Suppose that β is cubic over the "field of multiplications" of $\wp(z)$ and that $u \in \mathbf{C}$ such that $\varsigma = (\wp(u), \wp(\beta u), \wp(\beta^2 u))$ is defined. We study approximations to ς by points which lie on curves defined over $\mathbf{Z}$.

In this paper we investigate how closely, in an appropriate sense, curves defined over $\mathbf{Z}$ can come to certain points in $\mathbf{C}^3$ whose coordinates are given as values of elliptic functions. We show that integral polynomials which define the curve locally cannot both have moduli at the point, which are small in terms of the degree and height of the polynomials. This study was motivated by a desire to provide an elliptic analogue to W. D. Brownawell's generalization [**3**] of A. O. Gelfond and N. I. Feldman's measure for the algebraic independence of α^β and α^{β^2} for α, β algebraic with $\alpha \neq 0, 1$ and β cubic over $\mathbf{Q}$, [**7**].

Let $\wp(z)$ be a Weierstrass elliptic function satisfying the Weierstrass equation

$$\wp'(z)^2 = 4\wp^3(z) - g_2\wp(z) - g_3$$

and with lattice of periods $\mathscr{L} = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}$. We assume throughout this paper that g_2 and g_3 (the invariants of $\wp(z)$) are algebraic. Additionally, we assume that $\wp(z)$ has complex multiplication, in which case $\tau = \omega_2/\omega_1$ is a quadratic irrationality and $K_\tau = \mathbf{Q}(\tau)$ is called the field of multiplications for $\wp(z)$.

For a polynomial P over $\mathbf{C}$, in one or several variables, let dP denote the total degree of P, d_xP the partial degree of P with respect to x, and $d_x^*P = \max\{1, d_xP\}$. The height of P, ht P, is defined to be the maximum absolute value of the coefficients of P, and $t(P) = dP + \log \operatorname{ht} P$ is called the size of P. Moreover, for a pair of polynomials $P_1(x,y)$ and $P_2(x,y,z)$ we define several quantities which appear below. Namely, let

$$\begin{aligned} A &= d_x^*P_1(d_yP_2 + d_z^*P_2) + d_y^*P_1(d_xP_2 + d_z^*P_2), \\ B &= d_z^*P_2(d_y^*P_1 + \log \operatorname{ht} P_1 + \log(1 + d_x^*P_1)) \\ &\quad + d_yP_1(d_yP_2 + d_z^*P_2 + \log \operatorname{ht} P_2 + \log(1 + dP_2)) + d_yP_2 \log \operatorname{ht} P_1, \end{aligned}$$

and define a real number r by

$$\log r = A^2 \frac{(A+B)^2}{B} d_y^*P_1\, d_z^*P_2.$$

The main result of this paper is the following theorem.

Received by the editors June 6, 1986 and, in revised form, June 23, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11J89; Secondary 11G99.
Research supported in part by a grant from the National Science Foundation.

THEOREM 1. *Let u and β be complex numbers with β cubic over K_τ, such that all of $\wp(u), \wp(\beta u), \wp(\beta^2 u)$ are defined. There exists a constant $C^* > 0$ such that for all $C_1 > C^*$ there exists an effectively computable constant $C = C(C_1, \wp, \beta, u)$ with the following property. If $P_1(x, y)$ and $P_2(x, y, z)$ are coprime polynomials which satisfy*

$$\log \max_{i=1,2}\{|P_i(\wp(u), \wp(\beta u), \wp(\beta^2 u))|\} < -r^C \tag{1}$$

then there exists a nonzero polynomial $U(x) \in \mathbb{Z}[x]$ with

$$dU + \log \operatorname{ht} U < r^{C/C_1}, \qquad \log |U(\wp(u))| < -r^{C/4}. \tag{2}$$

This theorem provides an elliptic analogue to the theorem of [**3**], which was alluded to in the introductory paragraph above. Note that if (1) holds with the roles of x and y reversed in the definitions of A and B the conclusion of the theorem would then be that there exists a nonzero polynomial $V(y) \in \mathbb{Z}[y]$ with

$$t(V) < r^{C/C_1}, \qquad \log |V(\wp(\beta u))| < -r^{C/4}. \tag{3}$$

Not both (2) and (3) can hold, as the following result of A. Bijlsma shows:

LEMMA 0. *Suppose that $\wp(z)$ has complex multiplication and algebraic invariants. Let u and β be complex numbers with β algebraic, $\beta \notin K_\tau$, such that $\wp(u)$ and $\wp(\beta u)$ are defined. There are positive constants C_0 and t_0 such that for any nonzero polynomials $P(x)$ and $Q(x)$ in $\mathbb{Z}[x]$ with $t(P) + t(Q) = t > t_0$, one has*

$$\log \max\{|P(\wp(u))|,\ |Q(\wp(\beta u))|\} > -t^{C_0}.$$

PROOF. See [**2**].

Along these lines we will deduce the following theorem.

THEOREM 2. *Let u and β be complex numbers with β cubic over K_τ, such that all of $\wp(u), \wp(\beta u)$, and $\wp(\beta^2 u)$ are defined. There exists an effectively computable constant $C_2 = C_2(C_0, \wp, \beta, u) > 0$ such that for all coprime integral polynomials P_1, P_2*

$$\log \max_{i=1,2}\{|P_i(\wp(u), \wp(\beta u), \wp(\beta^2 u))|\} > -r^{C_2},$$

where $\log r = (dP_1)^2 (dP_2)^2 (dP_1 \cdot t(P_2) + dP_2 \cdot t(P_1))\, d_z^* P_2$.

In particular, Theorem 2 implies a generalization of the main theorem of [**11**] wherein u was assumed to be a nontorsion algebraic point for $\wp(z)$.

I. The deduction of Theorem 1 depends on elementary elimination theory; we will use the semi-resultant to perform these eliminations. For the convenience of the reader we recall that for polynomials

$$\begin{aligned} P(x) &= p_0(x - a_1) \cdots (x - a_n) \qquad (p_0 \neq 0), \\ Q(x) &= q_0(x - b_1) \cdots (x - b_m) \qquad (q_0 \neq 0) \end{aligned}$$

with complex coefficients, the semi-resultant $r[P, Q]$ is defined by

$$r[P, Q] = p_0^m q_0^n \prod (a_i - b_j)$$

where the product is over all pairs (i, j) for which $a_i \neq b_j$.

LEMMA 1. *Let $p_0, \dots, p_n$ and $q_0, \dots, q_m$ denote the coefficients of $P(X)$ and $Q(X)$, respectively. The semi-resultant $r[P,Q]$ is an integral polynomial in $p_0, \dots,$ p_n of degree m, in $q_0, \dots, q_m$ of degree n, and has coefficients of absolute values at most 5^{mn}. Furthermore, if $P_1(x)$ and $Q_1(x)$ are monic coprime factors of $P(x)$ and $Q(x)$ respectively, then for any $\theta \in \mathbf{C}$*

$$|r[P,Q]| \leq 2^{8mn} \operatorname{ht}(P)^m \operatorname{ht}(Q)^n \max\{|P_1(\theta)|,\ |Q_1(\theta)|\}.$$

PROOF. See [4].

REMARK. To emphasize those eliminations which require the semi-resultant we use the ordinary resultant of two polynomials, $\operatorname{Res}[P,Q]$, whenever it suffices.

We begin with a common zero of P_1 and P_2 which has some additional approximation properties. Roughly speaking, the idea behind this lemma is that if (1) holds but Theorem 1 does not, then P_1 and P_2 must have a common zero in $\mathbf{C}^3$ near $(\wp(u), \wp(\beta u), \wp(\beta^2 u))$, in an appropriate sense.

LEMMA 2. *Assume that* (1) *holds but that no nonzero integral polynomial satisfies* (2). *Then there exist complex numbers θ_2 and θ_3 which satisfy:*

(a) $P_1(\wp(u), \wp(\theta_2)) = P_2(\wp(u), \wp(\theta_2), \wp(\theta_3)) = 0$,

(b) $\log \max_{i=2,3}\{|\wp(\beta^{i-1}u) - \wp(\theta_i)|,\ |\wp'(\beta^{i-1}u) - \wp'(\theta_i)|\} < -r^{7C/10}$,

(c) $\log \max_{i=2,3}\{|\beta^{i-1}u - \theta_i|\} < -r^{7C/10}$,

provided C is sufficiently large.

PROOF. If $P_1(\wp(u), \wp(\beta u)) = 0$ take $\theta_2 = \beta u$ and proceed to the choice of θ_3 below. Otherwise, note that $d_y P_1 \neq 0$, else P_1 satisfies estimates (2), contrary to our hypothesis. Factor $P_1(\wp(u), y)$ in the algebraic closure of $\mathbf{Q}(\wp(u))$ in $\mathbf{C}$ as

$$P_1(\wp(u), y) = g(\wp(u)) \prod_{j=1}^{d} (y - \varsigma_j),$$

$d \leq d_y P_1$. Since $t(g) \leq 2(d_x P_1 + \log \operatorname{ht} P_1) < \log r < r^{C/C_1}$ (for C sufficiently large) our denial that (2) holds implies $\log |g(\wp(u))| \geq -r^{C/4}$. Therefore

$$\min_{1 \leq j \leq d} \log |\wp(\beta u) - \varsigma_j| < -r^{9C/10}.$$

Choose θ_2'' such that $\varsigma_j = \wp(\theta_2'')$ gives this minimum.

Let $\|z\|$ denote the distance from z to the nearest point of the lattice $\mathscr{L}$. The sigma expansion of $\wp(\beta u) - \wp(\theta_2'')$ together with the product representation for the sigma function yields

$$\log \min\{\|\beta u - \theta_2''\|,\ \|\beta u + \theta_2''\|\} < -r^{8C/10}.$$

Let θ_2' denote whichever of θ_2'' or $-\theta_2''$ gives this minimum. Then for some $\omega_0 \in \mathscr{L}$

$$\|\beta u - \theta_2'\| = |\beta u - (\theta_2' + \omega_0)|.$$

So put $\theta_2 = \theta_2' + \omega_0$. Then $P_1(\wp(u), \wp(\theta_2)) = 0$ and the inequalities of (b) and (c) hold for $i = 2$.

For $i = 3$, if $P_2(\wp(u), \wp(\theta_2), \wp(\beta^2 u)) = 0$ take $\theta_3 = \beta^2 u$. Otherwise we observe that if $d_z P_2 = 0$, then $U(x) = \operatorname{Res}_y[P_1, P_2]$ satisfies (2), violating our hypothesis. Write $P_2 = V_2 + R_2$ where V_2 is the sum of all monomials in y and z of P_2 whose coefficients vanish at $x = \wp(u)$; and $R_2 = V_2' + R_2'$ where V_2' is the sum of all monomials in z of R_2 whose coefficients vanish at $x = \wp(u)$, $y = \wp(\theta_2)$. Then $R_2'(\wp(u), \wp(\theta_2), z) \neq 0$ and we may consider the factorization

$$R_2'(\wp(u), \wp(\theta_2), z) = h(\wp(u), \wp(\theta_2)) \prod_{j=1}^{d_z R_2'} (z - \varsigma_j),$$

with $t(h) \leq 2(d_x P_2 + d_y P_2 + \log \operatorname{ht} P_2) < \log r$.

If

$$\log |h(\wp(u), \wp(\theta_2))| < -2r^{C/4}$$

let $h_0(x)$ denote the leading coefficient of $h(x, y)$ considered as a polynomial in y. Then $h_0(\wp(u)) \neq 0$, by our definition of $R_2(x, y, z)$ above. If $\log |h_0(\wp(u))| < -r^{C/4}$ then $U(x) = h_0(x)$ satisfies (2), contrary to our hypothesis. Therefore

$$\log \left| \frac{h(\wp(u), \wp(\theta_2))}{h_0(\wp(u))} \right| < -r^{C/4}$$

and hence the quotient of $h(x, y)$ by $h_0(x)$ has a monic factor $Q(x, y) \in \mathbb{Z}[x, y]$ with $t(Q) < 2t(h) < 4 \log r$, and

$$\log |Q(\wp(u), \wp(\theta_2))| < -r^{C/4}.$$

Moreover, $Q(\wp(u), y)$ and $P_1(\wp(u), y)$ are coprime since P_1 and P_2 are. Put $U(x) = r_y[P_1(x, y), h(x, y)]$; then $U(x)$ satisfies (2), contrary to our hypothesis.

Therefore we may conclude that $d_z R_2' > 0$ and

$$\log \min_{1 \leq j \leq d_z R_2'} |\wp(\beta^2 u) - \varsigma_j| < -r^{9C/10}.$$

Employing the arguments above with $i = 2$, this leads to $\theta_3 \in \mathbb{C}$ satisfying (a), (b) and (c). This completes the proof of the lemma.

With these choices of θ_2 and θ_3 the remainder of this section is devoted to proving Proposition 1 below, from which we deduce Theorem 1. Henceforth we use the notation

$$g = d_y^* P_1 \, d_z^* P_2 / B, \quad S_0 = [r^{C/4C_1}], \quad S_1 = [r^{C/11}]$$

and for each integer S, $S_0 \leq S \leq S_1$,

$$D = [S g^{1/4} \log^{1/4} S], \qquad L = [\kappa S^3 g^{-3/4} \log^{-3/4} S]$$

where κ is a large constant.[1]

PROPOSITION 1. *If* (1) *holds but* (2) *does not, then for each* S, $S_0 \leq S \leq S_1$, *there exists a nonzero polynomial* $Q_S(x, y) \in \mathbb{Z}[x, y]$ *with*

$$d_x Q_S \leq c_1 (d_x P_2 + d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$
$$d_y Q_S \leq c_2 (d_y P_2 + d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$
$$\log \operatorname{ht} Q_S \leq c_3 (d_z P_2 + \log \operatorname{ht} P_2 + \log(1 + dP_2) + g^{-1} d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$

such that $Q_S(\wp(u), \wp(\theta_2)) \neq 0$ *and*

$$\log |Q_S(\wp(u), \wp(\theta_2))| < -c_4 S^6 \log S.$$

[1] The numbered constants $c_1, \ldots, c_{58}$ in this paper are effective and depend at most on u, β, and $\wp(z)$.

Before embarking on the proof of this proposition we introduce a bit more notation. Let $\sigma(z)$ denote the Weierstrass sigma function and put

$$p(z) = (p_1(z), p_2(z), p_3(z)) = (\sigma^3(z), \sigma^3(z)\wp(z), \sigma^3(z)\wp'(z));$$

$p\colon \mathbb{C} \to E$ parametrizes the complex points on the elliptic curve E which is associated with $\wp(z)$. Also, let $\mathscr{O}$ denote the ring $\mathbb{Z} + \rho\mathbb{Z}$ where $\rho = n\tau$ for a denominator n of τ. We put

$$V = \mathscr{O} + \mathscr{O} \cdot \beta + \mathscr{O} \cdot \beta^2$$

and for $N \in \mathbb{N}$

$$V(N) = \mathscr{O}(N) + \mathscr{O}(N)\beta + \mathscr{O}(N)\beta^2$$

where $\mathscr{O}(N) = \{s_1 + s_2\rho \colon |s| < N\}$. We will encounter polynomials with coefficients in $\mathscr{R} = \mathscr{O}[g_2/4, g_3/4]$, so we define the size of an element $\alpha \in \mathscr{R}$ to be the least real number t for which there exists a polynomial $p_\alpha(x, y, z) \in \mathbb{Z}[x, y, z]$ of size t such that $\alpha = p_\alpha(\rho, g_2/4, g_3/4)$.

For each $v \in V(N)$ there exist multihomogeneous polynomials $A_{i,j}^{(v)}(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ $(1 \le i \le 3, 1 \le j \le 3)$, in the triples of variables $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ of multidegree at most (c_5N^2, c_5N^2, c_5N^2) and with coefficients in $\mathscr{R}$ of size at most $c_6(N^2+1)$ such that for each i,

$$(A_{i,1}^{(v)}(p(u), p(\beta u), p(\beta^2 u)), \dots, A_{i,3}^{(v)}(p(u), p(\beta u), p(\beta^2 u)))$$

are projective coordinates of $p(\beta^{i-1}uv)$ (for example, see [**1**]).

If there exists $v \in V(\eta S)$, for some $\eta < S$, such that for some i,

$$\max_{1 \le j \le 3} |A_{i,j}^{(v)}(p(u), p(\beta u), p(\beta^2 u))| < \exp(-c_7 S^6 \log S), \tag{4}$$

then the inequality remains valid with θ_2 replacing βu and θ_3 replacing $\beta^2 u$, with possibly a different constant, due to Lemma 2. Moreover,

$$(A_{i,1}^{(v)}(p(u), p(\theta_2), p(\theta_3)), \dots, A_{i,3}^{(v)}(p(u), p(\theta_2), p(\theta_3)))$$

are projective coordinates for the point $p(\beta^{i-1}uv)$ following the substitution of θ_k for $\beta^{k-1}u$ $(k = 2, 3)$ in each argument. Let $A_i^{(v)}$ denote one of the polynomials $A_{i,j}^{(v)}$ which does not vanish at $(p(u), p(\theta_2), p(\theta_3))$.

For each k let $p_{(k)}(z)$ denote the function among $p_1(z), p_2(z), p_3(z)$ for which $|p_j(\theta_k)|$ is maximal, where we have taken $\theta_1 = u$. Then $|p_{(k)}(\theta_k)| \ge c_8$, for C sufficiently large, and

$$\left[\prod_{k=1}^{3} p_{(k)}(\theta_k)\right]^{-\deg A_i^{(v)}} A_i^{(v)}(p(u), p(\theta_2), p(\theta_3)) = \frac{P_{i,1}^{(v)}}{P_{i,2}^{(v)}}(\wp(u), \wp'(u), \wp(\theta_2), \wp'(\theta_2), \wp(\theta_3), \wp'(\theta_3))$$

with $P_{i,j}^{(v)} \in \mathscr{R}[x_1, x_2, y_1, y_2, z_1, z_2]$ of degree at most $c_9(\eta S)^2$ and with coefficients of size at most $c_{10}(\eta S)^2$. From (4), with θ_k replacing $\beta^{k-1}u$, and our choice of

$p_{(k)}(z)$ we deduce that

$$\left|\frac{P_{i,1}^{(v)}}{P_{i,2}^{(v)}}(\wp(u),\dots,\wp'(\theta_3))\right| \leq \exp(-c_{11}S^6\log S), \tag{5}$$

and therefore one of $P_{i,j}^{(v)}$ $(j=1,2)$ satisfies

$$|P_{i,j}^{(v)}(\wp(u),\dots,\wp'(\theta_3))| \leq \exp(-c_{12}S^6\log S). \tag{6}$$

(If $P_{i,2}^{(v)}$ satisfies (6) we are done, otherwise the simple estimate

$$|P_{i,2}^{(v)}(\wp(u),\dots,\wp'(\theta_3))| \leq \exp(c_{13}(\eta S)^2)$$

combined with (5) implies that (6) holds with $j=1$).

Standard elimination techniques (e.g., [11]) then yield a nonzero polynomial $P'(x,y,z) \in \mathbb{Z}[x,y,z]$ with $t(P') \leq c_{14}(\eta S)^2$ and

$$0 \neq |P'(\wp(u),\wp(\theta_2),\wp(\theta_3))| \leq \exp(-c_{15}S^6\log S).$$

If $d_zP' = 0$ put $Q_S(x,y) = P'(x,y)$; otherwise, let

$$Q_S(x,y) = \mathrm{Res}_z[P_2(x,y,z),P'(x,y,z)].$$

One can verify that the estimates of Proposition 1 hold.

Therefore we need to establish the proposition when (4) does not hold. This we do in a sequence of steps.

Step 1 (*the auxiliary function*). Let $M = \{m_\nu\colon \nu \in I\}$, for some indexing set I, be a maximal collection of multihomogeneous monomials in the triples of variables $\mathbf{X},\mathbf{Y},\mathbf{Z}$ of multidegree (D,D,D) which are linear independent modulo the ideal which defines E^3: $\mathrm{Card}(M) \geq c_{16}D^3$.

LEMMA 3. *For all pairs* (l,ν), $0 \leq l \leq L$, $\nu \in I$, *there exists a polynomial* $a_{l,\nu} \in \mathbb{Z}[x,y,z]$ *with* $\deg a_{l,\nu} \leq c_{17}DS^2, \log\mathrm{ht}\, a_{l,\nu} \leq c_{18}L\log L$, *where the* $a_{l,\nu}$*'s do not have a common factor, such that for the polynomial*

$$P(w,\mathbf{X},\mathbf{Y},\mathbf{Z}) = \sum_{l=0}^{L}\sum_{\nu\in I} a_{l,\nu}(\wp(u),\wp(\beta u),\wp(\beta^2u))w^l m_\nu(\mathbf{X},\mathbf{Y},\mathbf{Z})$$

the function $F(z) = P(z,p(uz),p(\beta uz),p(\beta^2uz))$ *satisfies*

$$F(v) = 0 \quad \textit{for all } v \in V(S). \tag{7}$$

PROOF. We treat the coefficients $a_{l,\nu}$ as unknowns and apply the box-principle to solve the system of equations (7). To obtain the correct setup we recall the polynomials $A_{i,j}^{(v)}$ introduced above and for each $v \in V(S)$ and for each i, $1 \leq i \leq 3$, let $A_{i,j(v)}^{(v)}$ denote one of these polynomials for which

$$\log|A_{i,j(v)}^{(v)}(p(u),p(\beta u),p(\beta^2u))| > -c_7S^6\log S.$$

We introduce the notation

$$p(x,y,z) = (1,\wp(x),\wp'(x),1,\wp(y),\wp'(y),1,\wp(z),\wp'(z))$$

and use the multihomogeneity of P to write

$$F(v) = \prod_{i=1}^{3} \left[\left(\frac{p_{j(v)}(\beta^{i-1}uv)}{A^{(v)}_{i,j(v)}(p(u), p(\beta u), p(\beta^2 u))} \right)^D \cdot (\sigma(\beta^{i-1}u))^{c_5 DS^2} \right] \tag{8}$$
$$\times \sum_{l=0}^{L} \sum_{\nu \in I} a_{l,\nu} v^l m_{\nu,v}(p(u, \beta u, \beta^2 u));$$

where each monomial $m_{\nu,v}(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ has degree at most $c_{19}DS^2$, is at most linear in each of X_3, Y_3, Z_3 (due to the differential equation for $\wp(z)$), and has coefficients in $\mathscr{R}$ of size at most $c_{20}DS^2$.

For concreteness write

$$m_{\nu,v}(p(u, \beta u, \beta^2 u)) = c_{\nu,v} \prod_{k=1}^{3} \wp(\beta^{k-1}u)^{d_{\nu,k}} \prod_{k=1}^{3} \wp'(\beta^{k-1}u)^{e_{\nu,k}}$$

with $c_{\nu,v} \in \mathscr{R}$ of size at most $c_{20}DS^2$ and all $e_{\nu,k} \in \{0,1\}$. Put $e_\nu = (e_{\nu,1}, e_{\nu,2}, e_{\nu,3})$ and $T = \{0,1\} \times \{0,1\} \times \{0,1\}$. Then the system of equations

$$\sum_{l=0}^{L} \sum_{\nu \in I} a_{l,\nu} v^l m_{\nu,v}(p(u, \beta u, \beta^2 u)) = 0, \qquad v \in V(S), \tag{9}$$

may be rewritten as

$$\sum_{e \in T} \left(\sum_{l=0}^{L} \sum_{\substack{\nu \in I \\ e_\nu = e}} a_{l,\nu} v^l c_{\nu,v} \prod_{k=1}^{3} \wp(\beta^{k-1}u)^{d_{\nu,k}} \right) \prod_{k=1}^{3} \wp'(\beta^{k-1}u)^{e_{\nu,k}} = 0$$

for $v \in V(S)$.

We may then solve the system of equations

$$\sum_{l=0}^{L} \sum_{\substack{\nu \in I \\ e_\nu = e}} a_{l,\nu}(x, y, z) v^l c_{\nu,v} x^{d_{\nu,1}} y^{d_{\nu,2}} z^{d_{\nu,3}} = 0$$

for $e \in T$, $v \in V(S)$, *formally* provided we take κ sufficiently large. (This is done by extending Lemma 1 of [**3**] to the case where the polynomials, which are the coefficients of the system of equations, have coefficients in the ring of integers of some algebraic number field.) Replacing the polynomials $a_{l,\nu}(x, y, z)$ by themselves divided by their greatest common factors gives the lemma.

Step 2 (*altering the auxiliary function*). For each l, ν with $0 \le l \le L$ and $\nu \in I$ let

$$\alpha_{l,\nu}(z) = a_{l,\nu}(\wp(u), \wp(\theta_2), z).$$

Since we have taken the polynomials $a_{l,\nu}$ without a common factor, then not all of $\alpha_{l,\nu}(z) = 0$. To see this, let J denote the ideal in $\mathbb{Z}[x, y]$ generated by all of the coefficients of the polynomials $a_{l,\nu}(x, y, z)$ viewed as polynomials in z. J is a zero dimensional ideal, hence there exist relatively prime polynomials $b_1(x, y), b_2(x, y)$ in J with

$$t(b_k) \le \max_{l,\nu} a_{l,\nu} \le c_{17}DS^2 + c_{18}L \log L.$$

Moreover, if all $\alpha_{l,\nu}(z) = 0$, then $b_k(\wp(u), \wp(\theta_2)) = 0$ for $k = 1,2$, hence both of $\wp(u)$ and $\wp(\theta_2)$ are algebraic, and (2) holds trivially.

Let $m(z)$ denote the minimal monic polynomial of $\wp(\theta_3)$ over $\mathbb{Q}(\wp(u), \wp(\theta_2))$ and take $\sigma > 0$ maximal such that for all l, ν

$$\alpha_{l,\nu}(z) = m^{\sigma}(z) r_{l,\nu}(\wp(u), \wp(\theta_2), z).$$

Define

$$\phi(z) = \sum_{l=0}^{L} \sum_{\nu \in I} r_{l,\nu}(\wp(u), \wp(\theta_2), \wp(\theta_3)) z^l m_\nu(p(uz), p(\beta uz), p(\beta^2 uz)).$$

By our choice of σ, $\phi(z) \neq 0$.

For $v \in V(S)$, $\phi(v)$ equals the expression on the right side of equation (8) with $r_{l,\nu}(\wp(u), \wp(\theta_2), \wp(\theta_3))$ replacing $a_{l,\nu}(\wp(u), \wp(\beta u), \wp(\beta^2 u))$. Since the system of equations (9) was solved formally, we know that for each $v \in V(S)$

$$0 = \sum_{l=0}^{L} \sum_{\nu \in I} r_{l,\nu}(\wp(u), \wp(\theta_2), \wp(\theta_3)) v^l m_{\nu,v}(p(u, \theta_2, \theta_3))$$

(recall the notation $p(x, y, z)$ from above).

We next show that

$$\prod_{i=1}^{3} \left[\left(\frac{p_{j(v)}(\beta^{i-1}uv)}{A^{(v)}_{i,j(v)}(p(u), p(\beta u), p(\beta^2 u))} \right)^{D} (\sigma(\beta^{i-1}u))^{c_5 D S^2} \right] \tag{10}$$

remains defined and is nonzero following the substitution of θ_k for $\beta^{k-1}u$ $(k = 2,3)$. Moreover, if we let $M_{v,\theta}$ denote the maximum of the modulus of (10) and of (10) following the substitution of θ_k for $\beta^{k-1}u$ $(k = 2,3)$ we will obtain

$$\log M_{v,\theta} < c_{22} D S^6 \log S.$$

To verify this estimate we recall our choice of θ_k and deduce from our choice of $j(v)$ that

$$\log |A^{(v)}_{i,j(v)}(p(u), p(\theta_2), p(\theta_3))| > -c_7 S^6 \log S. \tag{11}$$

Additionally, once θ_k $(k = 2,3)$ has been substituted into $p_{j(v)}(\beta^{i-1}uv)$ the modulus of the new value is at most $\exp(c_{23} S^2)$. Combining these estimates with $|\sigma(\theta_k)| < c_{24}$ establishes the above bound for $M_{v,\theta}$.

For $v \in V(S)$ let $\phi(v)^*$ denote $\phi(v)$ following the substitution of θ_k for $\beta^{k-1}u$ $(k = 2,3)$. Then the above argument shows that $\phi(v)^* = 0$. Moreover, this implies that

$$|\phi(v)| < \exp(-c_{25} r^{7C/10}) \tag{12}$$

for all $v \in V(S)$. If $\theta_k = \beta^{k-1}u$ for $k = 2,3$ this is trivial since $\phi(v) = \phi(v)^* = 0$. Otherwise, suppose, for example, that $\theta_2 \neq \beta u$. Then

$$|\phi(v)| = |\phi(v) - \phi(v)^*| \leq M_{v,\theta} \times N_{v,\theta}$$

where

$$N_{v,\theta} = \left| \sum_{l=0}^{L} \sum_{\nu \in I} r_{l,\nu}(\wp(u), \wp(\theta_2), \wp(\theta_3)) v^l (m_{\nu,v}(p(u, \beta u, \beta^2 u)) - m_{\nu,v}(p(u, \theta_2, \theta_3))) \right| .$$

$N_{v,\theta}$ is divisible by $|\wp(\beta u) - \wp(\theta_2)|$ and therefore

$$\log|\phi(v)| < \log(M_{v,\theta}) - r^{7C/10} + c_{26}(DS^2 + L\log L) < -c_{25} r^{7C/10}.$$

The maximum modulus principle applied on circles of radii $c_{27}S^{13/6}$ and $c_{27}S^{14/6}$ yields

$$\log|F(z)| < -c_{28}S^6 \log S, \quad \text{for all } z \text{ with } |z| < c_{29}S^2. \tag{13}$$

Moreover by applying the Hermite interpolation formula we conclude that

$$\log|\phi(v)| < -c_{30}S^6 \log S, \quad \text{for all } v \in V(\eta S),\ \eta < c_{31}S.$$

(For details in an analogous situation, see [**3**].)

Step 3 (*arithmetic estimates*). For simplicity assume that β is integral over $\mathscr{O}$ with $\beta^3 = a\beta^2 + b\beta + c$, $a, b, c, \in \mathscr{O}$. Let

$$\begin{aligned} h_1 &= (1, u, \theta_2, \theta_3), \\ h_2 &= (\beta, \theta_2, \theta_3, cu + b\theta_2 + a\theta_3), \\ h_3 &= (\beta^2, \theta_3, cu + b\theta_2 + a\theta_3, acu + (ab + c)\theta_2 + (a^2 + b)\theta_3) \end{aligned}$$

and let

$$V^* = \mathscr{O}h_1 + \mathscr{O}h_2 + \mathscr{O}h_3 \subseteq \mathscr{T}_G(\mathbb{C}), \tag{14}$$

where $\mathscr{T}_G(\mathbb{C})$ denotes the tangent space of $G = \mathbf{G}_a \times E^3$ at its identity element. The exponential map $\exp_G \colon \mathscr{T}_G(\mathbb{C}) \to G(\mathbb{C})$ may be expressed as $\exp_G(z_1, \ldots, z_4) = (z_1, p(z_2), p(z_3), p(z_4))$.

PROPOSITION 2. *Let $P(1, w, \mathbf{X}, \mathbf{Y}, \mathbf{Z})$ be a multihomogeneous polynomial of multidegree (l, d_1, d_2, d_3) which does not vanish identically on G. There exist constants $C_3 = C_3(u, \beta, G)$ and C_G such that if $C > C_3$ and*

$$d = \max\{1, d_1, d_2, d_3\} < \exp(r^{6C/10}), \tag{15}$$

for r as defined above, then for any k with

$$k^6 > C_G \max\{d^3, ld^3\} \tag{16}$$

there exists $v_0 \in V^*(k)$ such that $P|_{\exp_G(v_0)} \neq 0$.

To prove Proposition 2 we begin with the following result which was suggested to the author by D. W. Masser.

LEMMA 4. *Suppose that $P \in \mathbb{C}[\mathbf{X}_1, \ldots, \mathbf{X}_n]$ is a multihomogeneous polynomial of maximum multidegree at most d, which does not vanish identically on E^n. Suppose further that there exists a finitely generated $\mathscr{O}$-module $W \subseteq \mathbb{C}^n$*

with $P(p(w_1),\dots,p(w_n)) = 0$ for all $(w_1,\dots,w_n) \in W$. Then there exists a constant C_4, depending on E^n, and $t_1,\dots,t_n \in \mathscr{O}(C_4 d^{1/2})$, not all zero, such that $t_1w_1 + \cdots + t_nw_n \in \mathscr{O}\cdot\omega_1$ for all $(w_1,\dots,w_n) \in W$.

PROOF. Let $W = g_1\mathscr{O} + \cdots + g_r\mathscr{O}$ with $g_i = (g_{i1},\dots,g_{in})$, $1 \le i \le r$. Define linear forms by

$$\begin{aligned} M_i(u) &= g_{i1}u_1 + \cdots + g_{in}u_n, \qquad && u \in \mathbb{C}^n,\\ L_j(x) &= g_{1j}x_1 + \cdots + g_{rj}x_r, && x \in \mathbb{C}^r, \end{aligned}$$

for $1 \le i \le r$, $1 \le j \le n$. Then for $(x_1,\dots,x_r) \in \mathscr{O}^r$

$$P(p(L_1(x)),\dots,p(L_n(x))) = 0$$

by hypothesis.

Let

$$P_1(1,\wp(z_1),\wp'(z_1),\dots,1,\wp(z_n),\wp'(z_n)) = \prod_{i=1}^{n}[\sigma^3(z_i)]^{-d_{x_i}P}P(p(z_1),\dots,p(z_n))$$

and take the relative norm from $\mathbb{C}(\wp(z_i),\wp'(z_i))_{i=1,\dots,n}$ to $\mathbb{C}(\wp(z_i))_{i=1,\dots,n}$, to obtain a polynomial $P_2(x_1,\dots,x_n)$ with $P_2(\wp(L_1(x)),\dots,\wp(L_n(x))) = 0$ for all $x \in \mathscr{O}^r$ for which no $L_j(x)$ lies in $\mathscr{L}$. $P \ne 0$ implies that $P_2 \ne 0$.

Choose arbitrary $\varsigma_1,\dots,\varsigma_n \in \mathbb{C}$ such that $|\wp(\varsigma_1)|+\cdots+|\wp(\varsigma_n)| \le 1$. We recall that for $z \in \mathbb{C}$, $\|z\|$ denotes the distance from z to the nearest point of $\mathscr{L}$. If for every choice of $\varsigma_1,\dots,\varsigma_n$ there exists $x \in \mathscr{O}^r$ such that $\max_{1\le j\le n}\|L_j(x)-\varsigma_j\| < c_{32}\,d^{-1/2}$, then by the argument of [**8**, pp. 75, 76] $\max_{1\le j\le n}|\wp(L_j(x)) - \wp(\varsigma_j)| < c_{33}\,d^{-1/2}$. If c_{32}, and therefore c_{33}, is sufficiently small, then Theorem A3 of [**8**] implies that $P_2 = 0$, contrary to our hypothesis.

Therefore there exists a constant $c_{32} > 0$ such that for some $\varsigma_1,\dots,\varsigma_n$ chosen as above,

$$\max_{1\le j\le n}\|L_j(x) - \varsigma_j\| > \tfrac{1}{2}c_{32}\,d^{-1/2} \tag{17}$$

for all $x \in \mathscr{O}^r$ for which none of $L_j(x)$ lies in $\mathscr{L}$. However, if $L_j(x) \in \mathscr{L}$ then

$$\|L_j(x) - \varsigma_j\| = \|\varsigma_j\| > c_{34} = c_{34}(\wp)$$

by the choice of ς_j. Hence (17) holds for all $x \in \mathscr{O}^r$, with possibly a different constant.

Let $\|x\|'$ denote the distance to the nearest element of $\mathscr{O}$. Recalling that $\mathscr{O}\cdot\omega_1 \subseteq \mathscr{L}$ we deduce from (17) that

$$\max_{1\le j\le n}\left\|\frac{L_j(x)}{\omega_1} - \frac{\varsigma_j}{\omega_1}\right\|' > \frac{1}{2}c_{35}\,d^{-1/2}$$

for all $x \in \mathscr{O}^r$. By the $\mathscr{O}$-analogue of Theorem XVII of [**5**] we may conclude that there exists $t \in \mathscr{O}^n(C_4 d^{1/2}), t \ne 0$, such that $\|M_i(t)/\omega_1\|' = 0$ for $1 \le i \le r$. This completes the proof of Lemma 3.

We also need the following information regarding linear forms in u, θ_2, θ_3 with coefficients in $\mathscr{O}$.

LEMMA 5. *Suppose for some integer $N \geq 0$ there exist $a_1, a_2, a_3 \in \mathscr{O}(N)$, not all zero, such that $a_1 u + a_2\theta_2 + a_3\theta_3 = 0$. Then there exists a constant $c_{36} > 0$ such that $N \geq \exp(c_{36} r^{7C/10})$.*

PROOF. By elementary estimates $|a_1 + a_2\beta + a_3\beta^2| > c_{37}N^{-5}$ and therefore if the form involving u, θ_2, θ_3 vanishes,

$$c_{37}N^{-5}|u| \leq 2 \max_{k=2,3} |a_k| \cdot |\theta_k - \beta^{k-1}u| \leq 2N \exp(-r^{7C/10}).$$

The lemma is immediate.

We are now in a position to give the proof of Proposition 2. For $N \geq 1$ let $\Gamma(N) = \{\exp_G(v) \colon v \in V^*(N)\}$, with V^* defined as in (14). If $P|_{\exp_G(v)} = 0$ for all $v \in V^*(k)$, for some $k \geq 1$, then Théorème 2.1 of [**10**] implies that there exists a connected algebraic subgroup G' of G, with $\operatorname{cod}_G G' = r_1 + r_2$, i.e., $G/G' = \mathbf{G}_a^{r_1} \times G_2'$ where $\dim G_2' = r_2$, such that

$$\operatorname{card}((\Gamma(k) + G')/G') \leq C_G l^{r_1} d^{r_2}, \tag{18}$$

where C_G depends only on G. Moreover, there is a multihomogeneous polynomial, $P_{G'}$, of multidegree at most $(c_{38}l, c_{39}\, d_1, c_{39}\, d_2, c_{39}\, d_3)$ which vanishes on G'.

For any connected algebraic subgroup G' of G let $t(G', k)$ denote the maximal number of $\mathscr{O}$-linearly independent elements in $\Gamma(k) \cap G'$. Then

$$\operatorname{card}((\Gamma(k) + G')/G') \geq k^{6-2t(G',k)}. \tag{19}$$

Let $\pi_1 \colon G \to \mathbf{G}_a$ and $\pi_2 \colon G \to E^3$ denote the projection mappings. If $\Gamma \cap G'$ is not trivial, then the $\mathscr{O}$-linear independence of $1, \beta$, and β^2 implies that $\pi_1(G') \neq 0$. Since $\mathbf{G}_a$ and E^3 are disjoint in the sense of [**9**], $G' = \mathbf{G}_a \times G''$ where G'' is a connected algebraic subgroup of E^3 of codimension r_2, and $r_1 = 0$. From the existence of the polynomial $P_{G'}$ above, it follows that there exists a polynomial $P_{G''}(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ of multidegree at most $(c_{39}\, d_1, c_{39}\, d_2, c_{39}\, d_3)$ which vanishes on G''. We now estimate each of the parameters $t(G', k)$.

Suppose $1 \leq r_2 < 3$ and that for some $k > 1$, $t(G', k) \geq 2$, then there exist $\mathscr{O}$-linearly independent elements g_1 and g_2 in $\Gamma(k)$ such that $P_{G''}$ vanishes on $\pi_2 \circ \exp_G(\mathscr{O}g_1 + \mathscr{O}g_2)$. By Lemma 4 there exist $(t_1, t_2, t_3) \in \mathscr{O}^3(C_4\, d^{1/2})$, $d = \max\{d_1, d_2, d_3\}$, such that if $g_i = (g_{i1}, g_{i2}, g_{i3})$, then $t_1 g_{i1} + t_2 g_{i2} + t_3 g_{i3} \in \mathscr{O}\omega_1$ $(i = 1, 2)$. If we express each of these forms as an expression in u, θ_2, θ_3, then the $\mathscr{O}$-linear independence of g_2 and g_3 allows us to eliminate the common occurrence of ω_1 and obtain $a_1 u + a_2\theta_2 + a_3\theta_3 = 0$, with $a_1, a_2, a_3 \in \mathscr{O}(c_{40}k^2\, d)$. From Lemma 5, $c_{40}k^2\, d \geq \exp(c_{36}r^{7C/10})$; and combining (19) and (18) yields

$$C_G\, d^{r_2} \geq k^2 \geq c_{41}\, d^{-1} \exp(c_{36} r^{7C/10}),$$

contrary to (15) for C_3 sufficiently large.

Therefore $t(G', k) \leq 1$ for all $k > 1$, whenever $\operatorname{cod}_G G' < 3$. If (18) holds for some G' of codimension $0 + r_2$, then from (19) $C_G\, d^{r_2} \geq k^4$, which cannot hold provided k satisfies (16).

We now treat the cases when $r_2 = 3$ or when $\Gamma \cap G'$ is trivial, together. To do this choose k_0 with $k_0^6 = [C_G \max\{d^3, l\, d^3\}] + 1$, and note that for any k satisfying (16), $\Gamma(k_0) \subseteq \Gamma(k)$. We also note that in each of the cases under consideration, $\Gamma(k_0) \cap G'$ consists only of the identity element of G. This is clear when $\Gamma \cap G'$ is trivial, so we only need to substantiate this when $r_2 = 3$.

When $r_2 = 3$, $\pi_2(G')$ is a zero dimensional connected algebraic subgroup of E^3, and therefore consists only of the identity element of E^3. Suppose that $s_1, s_2, s_3 \in \mathscr{O}(k_0)$ are such that $\exp_G(s_1 h_1 + s_2 h_2 + s_3 h_3) \in \Gamma \cap G'$; here h_1, h_2, h_3 are the elements of $\mathscr{T}_G(\mathbb{C})$ introduced at the beginning of Step 3. If we let H denote the 3×3 matrix whose ith column consists of the last three coordinates of h_i, then

$$H = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} \omega_1$$

for $\sigma_i \in \mathscr{O}(c_{42} k_0)$. Since $\det H = \operatorname{Norm}_{K_\tau(\beta)/K_\tau}(\beta) \neq 0$ we conclude that there exist $a_1, a_2, a_3 \in \mathscr{O}(c_{43} k_0^2)$ with $a_1 u + a_2 \theta_2 + a_3 \theta_3 = 0$; and all $a_i = 0$ if and only if all $s_i = 0$, $i = 1, 2, 3$.

Then by Lemma 5, if not all $a_i = 0$, then $c_{43} k_0^2 > \exp(c_{36} r^{7C/10})$, which is contrary to our choice of k_0 above combined with (15), provided we take C_3 sufficiently large. Therefore $a_1 = a_2 = a_3 = 0$, and $\Gamma(k_0) \cap G'$ is trivial.

We can now conclude the proof of the proposition. When $\Gamma(k_0) \cap G'$ is trivial, (19) yields

$$\operatorname{card}((\Gamma(k_0) + G')/G') \geq k_0^6,$$

and assuming (18) holds:

$$C_G \max\{d^3, ld^3\} \geq k^6;$$

this last inequality is contrary to (16) and establishes the proposition in every case.

Step 4 (*deducing the result*). Put

$$P_v^*(w, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \sum_{l=0}^{L} \sum_{\nu \in I} r_{l,\nu}(\wp(u), \wp(\theta_2), \wp(\theta_3)) w^l m_{\nu,v}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}).$$

We recall the set V^* defined by (14). With the choice of parameters L, D, and S we note that for c_{44} sufficiently large there exists $v_0 \in V^*(c_{44} S)$ such that $P_{v_0}^*|_{\exp_G(v_0)} \neq 0$. This is clearly equivalent to $\phi(v_0)^* \neq 0$ (where $*$ indicates that θ_k has been substituted for $\beta^{k-1} u$, $k = 2, 3$ in each argument of the function).

Through a procedure similar to the one used to estimate $|\phi(v)|$ above, we conclude that

$$\log |\phi(v_0)^*| < -c_{45} S^6 \log S;$$

and from (8) and (11) that

$$\log |P_{v_0}^*(s_1 + s_2 \beta + s_3 \beta^2, p(u, \theta_2, \theta_3))| < -c_{46} S^6 \log S.$$

Taking the relative norm from $\mathbb{Q}(\beta, \wp(u), \wp'(u), \wp(\theta_2), \wp'(\theta_2), \wp(\theta_3), \wp'(\theta_3))$ to $\mathbb{Q}(\wp(u), \wp(\theta_2), \wp(\theta_3))$ we obtain a polynomial expression $H(\wp(u), \wp(\theta_2), \wp(\theta_3))$, which is nonzero, where $H(x, y, z)$ is equal to $P_{v_0}^*$ with each monomial $w^l m_{\nu, v_0}(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ replaced by a polynomial $p_{\nu, v_0}(x, y, z)$. Each polynomial p_{ν, v_0} has coefficients in $\mathscr{R}$ of size at most $c_{47}(DS^2 + L \log S)$ and has degree at most $c_{47} DS^2$. Moreover

$$\log |H(\wp(u), \wp(\theta_1), \wp(\theta_2))| < -c_{48} S^6 \log S.$$

We return briefly to the functions $\alpha_{l,\nu}(z)$ from Step 2. For those $\alpha_{l,\nu}(z)$ which are not zero we may assume that the leading coefficient of z, $b_{l,\nu,0}(\wp(u), \wp(\theta_2))$, satisfies

$$\log |b_{l,\nu,0}(\wp(u), \wp(\theta_2))| > -c_{49} S^6 \log S,$$

otherwise Proposition 1 is established. Let

$$Q'_S = r_z[P_2(x,y,z), m^\sigma(x)H(x,y,z)].$$

Then multiply by a denominator δ for $g_2/4$ and $g_3/4$ to the appropriate power ε and let

$$Q_S(x,y) = N_{Q(\rho,\beta,g_2,g_3)/Q}(\delta^\varepsilon Q'_S(x,y)).$$

The techniques of [**3**] show that $Q_S(x,y)$ satisfies the conclusion of Proposition 1.

II. We now deduce Theorem 1 from Proposition 1. We do this by first establishing the following corollary of Proposition 1.

COROLLARY 1. *For each S, $S_0 \le S \le S_1$, there exists a nonzero polynomial $R_S(x) \in \mathbb{Z}[x]$ with*

$$\deg R_S \le c_{50}(S^3 g^{1/4} \log^{1/4} S)A,$$
$$\log \operatorname{ht} R_S \le c_{50}(S^3 g^{1/4} \log^{1/4} S)(B + g^{-1}\, d_y P_1\, d_z P_2);$$

such that $\log|R_S(\wp(u))| < -c_{51} S^6 \log S$.

PROOF. Let $q_0(\wp(u))$ denote the leading coefficient of $Q_S(\wp(u), y)$, viewed as a polynomial in y. If

$$\log|q_0(\wp(u))| < -\tfrac{1}{2} c_4 S^6 \log S$$

let $R_S(x) = q_0(x)$. Otherwise

$$\left|\frac{Q_S(\wp(u), \wp(\theta_2))}{q_0(\wp(u))}\right| < -c_{52} S^6 \log S.$$

Put $R_S(x) = r_y[P_1(x,y), Q_S(x,y)]$. Using the estimates of Lemma 1 and recalling the definitions of A, B, and g, we deduce that $R_S(x)$ satisfies the corollary.

For each S, $S_0 \le S \le S_1$, Lemma VI of [**6**] implies that there is a factor $T_S(x)$ of $R_S(x)$ which is the power of an irreducible polynomial $U_S(x)$, i.e., $T_S(x) = U_S^{e_S}(x)$; and, satisfies the estimates

$$\deg T_S \le \deg R_S, \qquad \log \operatorname{ht}(T_S) \le 2(\deg R_S + \log \operatorname{ht}(R_S))$$

with $\log|T_S(\wp(u))| < -c_{53} S^6 \log S$.

For $S_0 \le S < S_1$ put $n_S = \operatorname{Res}(T_S, T_{S+1})$. Then n_S is an integer with $\log|n_S| \le -c_{54} S^6 \log S$; hence $n_S = 0$ and $U_S(x) = U_{S+1}(x)$. Denote this irreducible polynomial by $U(x)$.

Since $U(x) = U_{S_0}(x)$ we have

$$\deg U \le c_{55} \frac{1}{e_{S_0}} (S_0^3 g^{1/4} \log^{1/4} S_0) A,$$

$$\log \operatorname{ht} U \le c_{56} \frac{1}{e_{S_0}} (S_0^3 g^{1/4} \log^{1/4} S_0)(A + B + g^{-1}\, d_y P_1\, d_z P_2).$$

However $e_{S_0} \ge 1$ and therefore for C sufficiently large

$$\deg U + \log \operatorname{ht} U \le r^{C/C_1}.$$

Also, $U(x) = U_{S_1}(x)$ and therefore

$$\log|U(\wp(u))| < -c_{57} \frac{1}{e_{S_1}} S_1^6 \log S_1,$$

which together with $e_{S_1} \leq \deg R_{S_1}$ yields

$$\log|U(\wp(u))| < -c_{58}(S_1^3 g^{-1/4} \log^{3/4} S_1)A^{-1}.$$

For C large enough $\log|U(\wp(u))| < -r^{C/4}$. This proves Theorem 1.

REMARK. To deduce Theorem 2 from Theorem 1 we must consider cases which are determined by the variables which appear in the polynomials P_1 and P_2 satisfying the hypotheses of the theorem. The easiest case is where we assume that $P_1 = P_1(x,y)$ and $P_2 = P_2(x,y,z)$ do not satisfy the conclusion of Theorem 2. Then we apply Theorem 1 and obtain $U(x)$ and $V(x)$, as above, which violates the conclusion of Lemma 0.

In general, we lose no generality if we assume that $d_x P_1 > 0$. Then there are several cases to consider. However by taking resultants, if necessary, each of these may be either reduced to the situation of Theorem 1 or to two polynomials each in one unknown, which is the situation examined in Lemma 0. We omit these details.

REFERENCES

1. D. Bertrand, *Problèmes locaux, Appendice* I, Nombres Transcendants et Groupes Algébriques, Asterisque, pp. 69–70, M. Waldschmidt.
2. A. Bijlsma, *An elliptic analogue of the Franklin-Schneider theorem*, Ann. Fac. Sci. Toulouse Math. **2** (1980), 101-116.
3. W. D. Brownawell, *On the Gelfond-Feldman measure of algebraic independence*, Composito Math. **38** (1979), 355–368.
4. ——, *Some remarks on semi-resultants*, Transcendence Theory: Advances and Applications (A. Baker and D. W. Masser, eds.), Academic Press, London, 1977.
5. J. W. S. Cassels, *An introduction to diophantine approximation*, Cambridge Univ. Press, Cambridge, 1957.
6. A. O. Gelfond, *Transcendental and algebraic numbers*, Dover, New York, 1960; Russian ed., 1951.
7. A. O. Gelfond and N. I. Feldman, *On the measure of the relative transcendence of certain numbers*, Izv. Akad. Nauk SSSR Ser. Mat. **14** (1950), 493–500.
8. D. W. Masser, *Elliptic functions and transcendence*, Lecture Notes in Math., vol. 437, Springer-Verlag, New York, 1975.
9. D. W. Masser and G. Wüstholz, *Zero estimates on group varieties.* II, Invent. Math. **80** (1985), 233-267.
10. P. Philippon, *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), 355–383.
11. R. Tubbs,*On the measure of algebraic independence of certain values of elliptic functions*, J. Number Theory **23** (1986), 60–79.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO
80309-0426