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 \( \varphi(z) \) be a Weierstrass elliptic function with algebraic invariants and complex multiplication. Suppose that \( \beta \) is cubic over the "field of multiplications" of \( \varphi(z) \) and that \( u \in \mathbb{C} \) such that \( \zeta = (\varphi(u), \varphi(\beta u), \varphi(\beta^2 u)) \) is defined. We study approximations to \( \zeta \) by points which lie on curves defined over \( \mathbb{Z} \).

In this paper we investigate how closely, in an appropriate sense, curves defined over \( \mathbb{Z} \) can come to certain points in \( \mathbb{C}^3 \) 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 \( \alpha^\beta \) and \( \alpha^{\beta^2} \) for \( \alpha, \beta \) algebraic with \( \alpha \neq 0, 1 \) and \( \beta \) cubic over \( \mathbb{Q} \), \([7]\).

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

\[
\varphi'(z)^2 = 4\varphi^3(z) - g_2\varphi(z) - g_3
\]

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

For a polynomial \( P \) over \( \mathbb{C} \), in one or several variables, let \( dP \) denote the total degree of \( P \), \( d_x P \) the partial degree of \( P \) with respect to \( x \), and \( d_x^* P = \max\{1, d_x P\} \). The height of \( P \), \( \text{ht} P \), is defined to be the maximum absolute value of the coefficients of \( P \), and \( \ell(P) = dP + \log \text{ht} P \) 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

\[
A = d_x^* P_1 (d_y P_2 + d_x^* P_2) + d_y^* P_1 (d_x P_2 + d_x^* P_2),
\]

\[
B = d_x^* P_2 (d_y^* P_1 + \log \text{ht} P_1 + \log (1 + d_x^* P_1))
+ d_y P_1 (d_y P_2 + d_x^* P_2 + \log \text{ht} P_2 + \log (1 + d_x P_2)) + d_y P_2 \log \text{ht} P_1,
\]

and define a real number \( r \) by

\[
\log r = A^2 \frac{(A + B)^2}{B} d_y^* P_1 d_x^* P_2.
\]

The main result of this paper is the following theorem.

Received by the editors June 6, 1986 and, in revised form, June 23, 1987.
Research supported in part by a grant from the National Science Foundation.

©1988 American Mathematical Society
0002-9947/88 $1.00 + $ .25 per page

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
THEOREM 1. Let \( u \) and \( \beta \) be complex numbers with \( \beta \) cubic over \( K_T \), such that all of \( \varphi(u), \varphi(\beta u), \varphi(\beta^2 u) \) are defined. There exists a constant \( C^* > 0 \) such that for all \( C_1 > C^* \) there exists an effectively computable constant \( C = C(C_1, \varphi, \beta, u) \) with the following property. If \( P_1(x, y) \) and \( P_2(x, y, z) \) are coprime polynomials which satisfy

\[
\log \max_{i=1,2} \{|P_i(\varphi(u), \varphi(\beta u), \varphi(\beta^2 u))|\} < -r^C
\]

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

\[
dU + \log \text{ht}U < r^{C/C_1}, \quad \log |U(\varphi(u))| < -r^{C/4}.
\]

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

\[
t(V) < r^{C/C_1}, \quad \log |V(\varphi(\beta u))| < -r^{C/4}.
\]

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

**Lemma 0.** Suppose that \( \varphi(z) \) has complex multiplication and algebraic invariants. Let \( u \) and \( \beta \) be complex numbers with \( \beta \) algebraic, \( \beta \notin K_T \), such that \( \varphi(u) \) and \( \varphi(\beta u) \) 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

\[
\log \max\{|P(\varphi(u))|, |Q(\varphi(\beta u))|\} > -t^{C_0}.
\]

**Proof.** See [2].

Along these lines we will deduce the following theorem.

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

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

where \( r = (dP_1)^2(dP_2)^2(dP_1 \cdot t(P_2) + dP_2 \cdot t(P_1)) d_x^*P_2. \)

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

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

\[
P(x) = p_0(x - a_1) \cdots (x - a_n) \quad (p_0 \neq 0),
Q(x) = q_0(x - b_1) \cdots (x - b_m) \quad (q_0 \neq 0)
\]

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

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

where the product is over all pairs \( (i, j) \) for which \( a_i \neq b_j \).
Lemma 1. Let $p_0, \ldots, p_n$ and $q_0, \ldots, q_m$ denote the coefficients of $P(X)$ and $Q(X)$, respectively. The semi-resultant $r[P, Q]$ is an integral polynomial in $p_0, \ldots, p_n$ of degree $m$, in $q_0, \ldots, q_m$ 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 $\theta \in \mathbb{C}$

$$|r[P, Q]| \leq 2^{5mn} \text{ht}(P)^m \text{ht}(Q)^n \max\{|P_1(\theta)|, |Q_1(\theta)|\}.$$

Proof. See [4].

Remark. To emphasize those eliminations which require the semi-resultant we use the ordinary resultant of two polynomials, 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 $\mathbb{C}^3$ near $(\varphi(u), \varphi(\beta u), \varphi(\beta^2 u))$, in an appropriate sense.

Lemma 2. Assume that (1) holds but that no nonzero integral polynomial satisfies (2). Then there exist complex numbers $\theta_2$ and $\theta_3$ which satisfy:

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

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

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

provided $C$ is sufficiently large.

Proof. If $P_1(\varphi(u), \varphi(\beta u)) = 0$ take $\theta_2 = \beta u$ and proceed to the choice of $\theta_3$ below. Otherwise, note that $d_y P_1 \neq 0$, else $P_1$ satisfies estimates (2), contrary to our hypothesis. Factor $P_1(\varphi(u), y)$ in the algebraic closure of $Q(\varphi(u))$ in $\mathbb{C}$ as

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

$d \leq d_y P_1$. Since $t(g) \leq 2(d_x P_1 + \log \text{ht} P_1) < \log r < r^{C/C'}$ (for $C$ sufficiently large) our denial that (2) holds implies $\log |g(\varphi(u))| \geq -r^{C/4}$. Therefore

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

Choose $\theta_2'$ such that $\zeta_j = \varphi(\theta_2')$ gives this minimum.

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

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

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

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

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

For $i = 3$, if $P_2(\varphi(u), \varphi(\theta_2), \varphi(\beta^2 u)) = 0$ take $\theta_3 = \beta^2 u$. Otherwise we observe that if $d_x P_2 = 0$, then $U(x) = \text{Res}_y[P_1, P_2]$ 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 $x = \varphi(u)$; 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 $x = \varphi(u)$, $y = \varphi(\theta_2)$. Then $R'_2(\varphi(u), \varphi(\theta_2), z) \neq 0$ and we may consider the factorization

$$R'_2(\varphi(u), \varphi(\theta_2), z) = h(\varphi(u), \varphi(\theta_2)) \prod_{j=1}^{d_z R'_2} (z - \zeta_j),$$

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

If

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

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

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

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

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

Moreover, $Q(\varphi(u), y)$ and $P_1(\varphi(u), y)$ 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

$$\log \min_{1 \leq j \leq d_z R'_2} |\varphi(\beta^2 u) - \zeta_j| < -r^{9C/10}.$$

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 $\theta_2$ and $\theta_3$ the remainder of this section is devoted to proving Proposition 1 below, from which we deduce Theorem 1. Henceforth we use the notation

$$g = d_y^* P_1 d_x^* P_2 / B, \quad S_0 = \lceil r^{C/4} \rceil, \quad S_1 = \lceil r^{C/11} \rceil$$

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

$$D = \lceil Sg^{1/4} \log^{1/4} S \rceil, \quad L = \lceil \kappa S^3 g^{-3/4} \log^{-3/4} S \rceil$$

where $\kappa$ 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

$$d_z Q_S \leq c_1(d_x P_2 + d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$

$$d_y Q_S \leq c_2(d_y P_2 + d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$

$$\log \text{ht} Q_S \leq c_3(d_z P_2 + \log \text{ht} P_2 + \log(1 + d_P 2) + g^{-1} d_z P_2) S^3 g^{1/4} \log^{1/4} S,$$

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

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

¹The numbered constants $c_1, \ldots, c_{58}$ in this paper are effective and depend at most on $u, \beta$, and $\varphi(x)$.
Before embarking on the proof of this proposition we introduce a bit more notation. Let \( \sigma(z) \) denote the Weierstrass sigma function and put

\[
p(z) = (p_1(z), p_2(z), p_3(z)) = (\sigma^3(z), \sigma^3(z)\varphi(z), \sigma^3(z)\varphi'(z));
\]

\( p : \mathbb{C} \rightarrow E \) parametrizes the complex points on the elliptic curve \( E \) which is associated with \( \varphi(z) \). Also, let \( \mathcal{O} \) denote the ring \( \mathbb{Z} + \rho\mathbb{Z} \) where \( \rho = nr \) for a denominator \( n \) of \( r \). We put

\[
V = \mathcal{O} + \mathcal{O} \cdot \beta + \mathcal{O} \cdot \beta^2
\]

and for \( N \in \mathbb{N} \)

\[
V(N) = \mathcal{O}(N) + \mathcal{O}(N)\beta + \mathcal{O}(N)\beta^2
\]

where \( \mathcal{O}(N) = \{ s_1 + s_2\rho : |s| < N \} \). We will encounter polynomials with coefficients in \( \mathcal{R} = \mathcal{O}[g_2/4, g_3/4] \), so we define the size of an element \( \alpha \in \mathcal{R} \) 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 \( A_{i,j}^{(v)}(X, Y, Z) \) (\( 1 \leq i \leq 3, 1 \leq j \leq 3 \)), in the triples of variables \( X, Y, Z \) of multidegree at most \( (c_5 N^2, c_5 N^2, c_5 N^2) \) and with coefficients in \( \mathcal{R} \) of size at most \( c_6(N^2 + 1) \) such that for each \( i \),

\[
(A_{i,1}^{(v)}(p(u), p(\beta u), p(\beta^2 u)), \ldots, A_{i,3}^{(v)}(p(u), p(\beta u), p(\beta^2 u)))
\]

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 \( i \),

\[
\max_{1 \leq i \leq 3} |A_{i,j}^{(v)}(p(u), p(\beta u), p(\beta^2 u))| < \exp(-c_7 S^6 \log S),
\]

then the inequality remains valid with \( \theta_2 \) replacing \( \beta u \) and \( \theta_3 \) replacing \( \beta^2 u \), with possibly a different constant, due to Lemma 2. Moreover,

\[
(A_{i,1}^{(v)}(p(u), p(\theta_2), p(\theta_3)), \ldots, A_{i,3}^{(v)}(p(u), p(\theta_2), p(\theta_3)))
\]

are projective coordinates for the point \( p(\beta^{i-1}uv) \) following the substitution of \( \theta_k \) for \( \beta^{i-1}u \) (\( k = 2, 3 \)) 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 \( |p_k(\theta_k)| \geq c_8 \), for \( C \) sufficiently large, and

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

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

\[
\left| \frac{P_{i,1}^{(v)}}{P_{i,2}^{(v)}} (\varphi(u), \ldots, \varphi'(\theta_3)) \right| \leq \exp(-c_{11} S^6 \log S),
\]

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

\[
|P_{i,j}^{(v)} (\varphi(u), \ldots, \varphi'(\theta_3))| \leq \exp(-c_{12} S^6 \log S).
\]

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

\[
|P_{i,2}^{(v)} (\varphi(u), \ldots, \varphi'(\theta_3))| \leq \exp(c_{13} (\eta S)^2)
\]

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

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

If \( d_x P' = 0 \) put \( Q_S(x, y) = P'(x, y) \); otherwise, let

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

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

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

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

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

\[
F(v) = 0 \quad \text{for all } v \in V(S).
\]

**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 \( A_{l,j}^{(v)} \) introduced above and for each \( v \in V(S) \) and for each \( i, 1 \leq i \leq 3, \) let \( A_{i,j}^{(v)} \) denote one of these polynomials for which

\[
\log |A_{i,j}^{(v)} (p(u), p(\beta u), p(\beta^2 u))| > -c_7 S^6 \log S.
\]

We introduce the notation

\[
p(x, y, z) = (1, \varphi(x), \varphi'(x), 1, \varphi(y), \varphi'(y), 1, \varphi(z), \varphi'(z))
\]
and use the multihomogeneity of $P$ to write
\[
F(v) = \prod_{i=1}^{3} \left[ \left( \frac{p_{i}(v)(\beta^{i-1}uv)}{A_{i,j}(v)(p(u),p(\beta u),p(\beta^{2}u))} \right)^{D} \cdot (\sigma(\beta^{i-1}u))^{c_{5}DS^{2}} \right] \\
\times \sum_{l=0}^{L} \sum_{v \in I} a_{l,v}v^{l}m_{\nu,v}(p(u,\beta u,\beta^{2}u));
\]

where each monomial $m_{\nu,v}(X, Y, Z)$ 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 $\varphi(z)$), and has coefficients in $\mathcal{R}$ of size at most $c_{20}DS^{2}$.

For concreteness write
\[
m_{\nu,v}(p(u,\beta u,\beta^{2}u)) = c_{\nu,v} \prod_{k=1}^{3} \varphi(\beta^{k-1}u)^{d_{\nu,k}} \prod_{k=1}^{3} \varphi'(\beta^{k-1}u)^{e_{\nu,k}}
\]

with $c_{\nu,v} \in \mathcal{R}$ 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
\[
\sum_{l=0}^{L} \sum_{v \in I} a_{l,v}v^{l}m_{\nu,v}(p(u,\beta u,\beta^{2}u)) = 0, \quad v \in V(S),
\]

may be rewritten as
\[
\sum_{e \in T} \left( \sum_{l=0}^{L} \sum_{v \in I \atop e_{\nu} = e} a_{l,v}v^{l}c_{\nu,v} \prod_{k=1}^{3} \varphi(\beta^{k-1}u)^{d_{\nu,k}} \prod_{k=1}^{3} \varphi'(\beta^{k-1}u)^{e_{\nu,k}} \right) = 0
\]

for $v \in V(S)$.

We may then solve the system of equations
\[
\sum_{l=0}^{L} \sum_{v \in I \atop e_{\nu} = e} a_{l,v}(x, y, z)v^{l}c_{\nu,v}x^{d_{\nu,1}}y^{d_{\nu,2}}z^{d_{\nu,3}} = 0
\]

for $e \in T, v \in V(S)$, formally provided we take $\kappa$ 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 $a_{l,v}(x, y, z)$ by themselves divided by their greatest common factors gives the lemma.

**Step 2 (altering the auxiliary function).** For each $l, \nu$ with $0 \leq l \leq L$ and $\nu \in I$ let
\[
\alpha_{l,\nu}(z) = a_{l,\nu}(p(u), p(\theta_{2}), z).
\]

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
\[
t(b_{k}) \leq \max_{l,\nu} a_{l,\nu} \leq c_{17}DS^{2} + c_{18}L \log L.
\]
Moreover, if all $\alpha_l, \nu(z) = 0$, then $b_k(\varphi(u), \varphi(\theta_2)) = 0$ for $k = 1, 2$, hence both of
$\varphi(u)$ and $\varphi(\theta_2)$ are algebraic, and (2) holds trivially.

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

$$\alpha_l, \nu(z) = m^\sigma(z) r_l, \nu(\varphi(u), \varphi(\theta_2), z).$$

Define

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

By our choice of $\sigma$, $\phi(z) \neq 0$.

For $v \in V(S)$, $\phi(v)$ equals the expression on the right side of equation (8) with $r_l, \nu(\varphi(u), \varphi(\theta_2), \varphi(\theta_3))$ replacing $\alpha_l, \nu(\varphi(u), \varphi(\theta_2), \varphi(\theta_3))$. Since the system of
equations (9) was solved formally, we know that for each $v \in V(S)$

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

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

We next show that

$$(10) \prod_{i=1}^{3} \left[ \frac{p_j(v)(\beta^{i-1}uv)}{A_{i,j}(v)(p(u), p(\beta u), p(\beta^2 u))} \right]^D (\sigma(\beta^{i-1}u)) c_3 DS^2$$

remains defined and is nonzero following the substitution of $\theta_k$ 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 $\theta_k$ for $\beta^{k-1}u$ ($k = 2, 3$) we will obtain

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

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

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

Additionally, once $\theta_k$ ($k = 2, 3$) 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 $|\sigma(\theta_k)| < c_4$ establishes the above bound for $M_{v, \theta}$.

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

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

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

\( N_{v,\theta} \) is divisible by \( |\varphi(\beta u) - \varphi(\theta_2)| \) 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
\[ \log |F(z)| < -c_{28}S^6 \log S, \quad \text{for all } z \text{ with } |z| < c_{29}S^2. \]

Moreover by applying the Hermite interpolation formula we conclude that
\[ \log |\phi(v)| < -c_{30}S^6 \log S, \quad \text{for all } v \in V(\eta S), \quad \eta < c_{31}S. \]

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

Step 3 (arithmetic estimates). For simplicity assume that \( \beta \) is integral over \( \mathcal{O} \) with \( \beta^3 = a\beta^2 + b\beta + c, \ a, b, c, \in \mathcal{O} \). Let
\[ h_1 = (1, u, \theta_2, \theta_3), \]
\[ h_2 = (\beta, \theta_2, \theta_3, cu + b\theta_2 + a\theta_3), \]
\[ h_3 = (\beta^2, \theta_2, \theta_3, cu + b\theta_2 + a\theta_3, acu + (ab + c)\theta_2 + (a^2 + b)\theta_3) \]

and let
\[ V^* = \mathcal{O} h_1 + \mathcal{O} h_2 + \mathcal{O} h_3 \subseteq \mathcal{T}_G(\mathbb{C}), \]

where \( \mathcal{T}_G(\mathbb{C}) \) denotes the tangent space of \( G = G_a \times E^3 \) at its identity element.
The exponential map \( \exp_G : \mathcal{T}_G(\mathbb{C}) \rightarrow G(\mathbb{C}) \) 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 \( P(1, w, X, Y, Z) \) 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
\[ d = \max\{l, d_1, d_2, d_3\} < \exp(r^{6C/10}), \]
for \( r \) as defined above, then for any \( k \) with
\[ k^6 > C_G \max\{d^3, ld^3\} \]
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 \( P \in \mathbb{C}[X_1, \ldots, X_n] \) 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 \( \mathcal{O} \)-module \( W \subseteq \mathbb{C}^n \)
with \( P(p(w_1), \ldots, p(w_n)) = 0 \) for all \((w_1, \ldots, w_n) \in W\). Then there exists a constant \( C_4 \), depending on \( E_n \), and \( t_1, \ldots, t_n \in \mathcal{C}(C_4 d^{1/2}) \), not all zero, such that \( t_1 w_1 + \cdots + t_n w_n \in \mathcal{C} \cdot \omega_1 \) for all \((w_1, \ldots, w_n) \in W\).

**PROOF.** Let \( W = g_1 \mathcal{C} + \cdots + g_r \mathcal{C} \) with \( g_i = (g_{i1}, \ldots, g_{in}) \), \( 1 \leq i \leq r \). Define linear forms by

\[
M_i(u) = g_{i1} u_1 + \cdots + g_{in} u_n, \quad u \in \mathbb{C}^n,
\]

\[
L_j(x) = g_{j1} x_1 + \cdots + g_{jn} x_n, \quad x \in \mathbb{C}^r,
\]

for \( 1 \leq i \leq r \), \( 1 \leq j \leq n \). Then for \((x_1, \ldots, x_r) \in \mathcal{C}^r\)

\[
P(p(L_1(x)), \ldots, p(L_n(x))) = 0
\]

by hypothesis.

Let

\[
P_1(1, \varphi(z_1), \varphi'(z_1), \ldots, 1, \varphi(z_n), \varphi'(z_n)) = \prod_{i=1}^{n} [\sigma(z_i)]^{-d z_i} P(p(z_1), \ldots, p(z_n))
\]

and take the relative norm from \( C(\varphi(z_i), \varphi'(z_i))_{i=1, \ldots, n} \) to \( C(\varphi(z_i))_{i=1, \ldots, n} \), to obtain a polynomial \( P_2(x_1, \ldots, x_n) \) with \( P_2(\varphi(L_1(x)), \ldots, \varphi(L_n(x))) = 0 \) for all \( x \in \mathcal{C}^r \) for which no \( L_j(x) \) lies in \( \mathcal{C} \). \( P \neq 0 \) implies that \( P_2 \neq 0 \).

Choose arbitrary \( \zeta_1, \ldots, \zeta_n \in \mathbb{C} \) such that \(|\varphi(\zeta_1)| + \cdots + |\varphi(\zeta_n)| \leq 1 \). We recall that for \( z \in \mathbb{C} \), \(|z|\) denotes the distance from \( z \) to the nearest point of \( \mathcal{L} \). If for every choice of \( \zeta_1, \ldots, \zeta_n \) there exists \( x \in \mathcal{C}^r \) such that \( \max_{1 \leq j \leq n} ||L_j(x) - \zeta_j|| < c_{32} d^{-1/2} \), then by the argument of [8, pp. 75, 76] \( \max_{1 \leq j \leq n} ||\varphi(L_j(x)) - \varphi(\zeta_j)|| < c_{33} d^{-1/2} \). 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 \( \zeta_1, \ldots, \zeta_n \) chosen as above,

\[
(17) \quad \max_{1 \leq j \leq n} ||L_j(x) - \zeta_j|| > \frac{1}{2} c_{32} d^{-1/2}
\]

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

\[
||L_j(x) - \zeta_j|| = ||\zeta_j|| > c_{34} = c_{34}(\varphi)
\]

by the choice of \( \zeta_j \). Hence (17) holds for all \( x \in \mathcal{C}^r \), with possibly a different constant.

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

\[
\max_{1 \leq j \leq n} \left\| \frac{L_j(x)}{\omega_1} - \frac{\zeta_j}{\omega_1} \right\|' > \frac{1}{2} c_{35} d^{-1/2}
\]

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

We also need the following information regarding linear forms in \( u, \theta_2, \theta_3 \) with coefficients in \( \mathcal{O} \).

---

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
LEMMA 5. Suppose for some integer \( N \geq 0 \) there exist \( a_1, a_2, a_3 \in \mathcal{O}(N) \), not all zero, such that \( a_1u + a_2\theta_2 + a_3\theta_3 = 0 \). 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 \( u, \theta_2, \theta_3 \) 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 \( \Gamma(N) = \{ \exp_G(v) : v \in V^*(N) \} \), 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 \( \text{cod}_G G' = r_1 + r_2 \), i.e., \( G/G' = G_1 \times G_2' \) where \( \dim G_2' = r_2 \), such that
\[
(18) \quad \text{card}((\Gamma(k) + G')/G') \leq C_G l^{r_1} d^{r_2},
\]
where \( C_G \) depends only on \( G \). Moreover, there is a multihomogeneous polynomial, \( P_{G'} \), of multidegree at most \( (c_{39}, c_{39} d_1, c_{39} d_2, c_{39} d_3) \) which vanishes on \( G' \).

For any connected algebraic subgroup \( G' \) of \( G \) let \( t(G', k) \) denote the maximal number of \( \mathcal{E} \)-linearly independent elements in \( \Gamma(k) \cap G' \). Then
\[
(19) \quad \text{card}((\Gamma(k) + G')/G') \geq k^{6-2t(G', k)}.
\]
Let \( \pi_1 : G \to G_1 \) and \( \pi_2 : G \to E^3 \) denote the projection mappings. If \( \Gamma \cap G' \) is not trivial, then the \( \mathcal{E} \)-linear independence of 1, \( \beta \), and \( \beta^2 \) implies that \( \pi_1(G') \neq 0 \). Since \( G_1 \) and \( E^3 \) are disjoint in the sense of [9], \( G' = G_1 \times G'' \) 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 \( P_{G''}(X, Y, Z) \) 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 \( \mathcal{E} \)-linearly independent elements \( g_1 \) and \( g_2 \) in \( \Gamma(k) \) such that \( P_{G''} \) vanishes on \( \pi_2 \circ \exp_G(\mathcal{E} g_1 + \mathcal{E} g_2) \). By Lemma 4 there exist \( (t_1, t_2, t_3) \in \mathcal{E}(C_4 d^{1/2}) \), \( d = \max\{d_1, d_2, d_3\} \), such that if \( g_i = (g_{i1}, g_{i2}, g_{i3}) \), then \( t_1 g_{i1} + t_2 g_{i2} + t_3 g_{i3} \in \mathcal{E} \omega_i \) \((i = 1, 2)\). If we express each of these forms as an expression in \( u, \theta_2, \theta_3 \), then the \( \mathcal{E} \)-linear independence of \( g_2 \) and \( g_3 \) allows us to eliminate the common occurrence of \( \omega_i \) and obtain \( a_1u + a_2\theta_2 + a_3\theta_3 = 0 \), with \( a_1, a_2, a_3 \in \mathcal{E}(c_{40} k^2 d) \). 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 \( \text{cod}_G G' < 3 \). 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), \( \Gamma(k) \subseteq \Gamma(k) \). 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 \( s_1, s_2, s_3 \in \mathcal{O}(k_0) \) are such that \( \exp_G(s_1h_1 + s_2h_2 + s_3h_3) \in \Gamma \cap G' \); here \( h_1, h_2, h_3 \) are the elements of \( \mathcal{F}_G(C) \) introduced at the beginning of Step 3. If we let \( H \) denote the \( 3 \times 3 \) matrix whose \( i \)th 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 \( \sigma_i \in \mathcal{O}(c_{42}k_0) \). Since \( \det H = \text{Norm}_{K_\gamma, \beta}/K_{\gamma}(\beta) \neq 0 \) we conclude that there exist \( a_1, a_2, a_3 \in \mathcal{O}(c_{43}k_0^2) \) with \( a_1u + a_2\theta_2 + a_3\theta_3 = 0 \); 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

\[
\text{card}(\langle \Gamma(k_0) + G' \rangle / G') \geq k_0^5,
\]

and assuming (18) holds:

\[
C_G \max\{d^3, 4d^3 \} \geq k_6;
\]

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

**Step 4 (deducing the result).** Put

\[
P_v^*(w, X, Y, Z) = \sum_{l=0}^{L} \sum_{\nu \in I} \tau_{l, \nu}(\varphi(u), \psi(\theta_2), \varphi(\theta_3))w^lm_{\nu, v}(X, Y, Z).
\]

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 \( P_v^*|_{\exp_G(v_0)} \neq 0 \). This is clearly equivalent to \( \phi(v_0)^* \neq 0 \) (where \( * \) indicates that \( \theta_k \) 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

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

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

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

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 \( z \), \( b_{l, \nu, 0}(\varphi(u), \varphi(\theta_2)) \), satisfies

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
otherwise Proposition 1 is established. Let
\[ Q'_S = r_2\left[ P_2(x, y, z), m^g(x)H(x, y, z) \right]. \]
Then multiply by a denominator \( \delta \) for \( g_2/4 \) and \( g_3/4 \) to the appropriate power \( \varepsilon \) and let
\[ Q_S(x, y) = N_{Q(\rho, \beta, g_2, g_3) / Q(\delta^6 Q'(x, y))}. \]
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 \( S, S_0 \leq S \leq S_1 \), there exists a nonzero polynomial \( R_S(x) \in \mathbb{Z}[x] \) with
\[
\deg R_S \leq c_{50}(S^3 g^{1/4} \log^{1/4} S) A, \\
\log ht R_S \leq c_{50}(S^3 g^{1/4} \log^{1/4} S)(B + g^{-1} d_y P_1 d_z P_2); \\
such that \log |R_S(\varphi(u))| < -c_{51} S^6 \log S.
\]

**PROOF.** Let \( q_0(\varphi(u)) \) denote the leading coefficient of \( Q_S(\varphi(u), y) \), viewed as a polynomial in \( y \). If
\[
\log |q_0(\varphi(u))| < -\frac{1}{2} c_{4} S^6 \log S
\]
let \( R_S(x) = q_0(x) \). Otherwise
\[
\left| \frac{Q_S(\varphi(u), \varphi(\theta_2))}{q_0(\varphi(u))} \right| < -c_{52} S^6 \log S.
\]
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 \( S, S_0 \leq S \leq S_1 \), 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., \( T_S(x) = U_S^{g_S}(x) \); and, satisfies the estimates
\[
\deg T_S \leq \deg R_S, \quad \log ht(T_S) \leq 2(\deg R_S + \log ht(R_S))
\]
with \( \log |T_S(\varphi(u))| < -c_{53} S^6 \log S. \)
For \( S_0 \leq S < S_1 \) put \( n_S = \text{Res}(T_S, T_{S+1}) \). Then \( n_S \) is an integer with
\[
\log |n_S| \leq -c_{54} S^6 \log S; \text{ hence } n_S = 0 \text{ and } U_S(x) = U_{S+1}(x). \]
Denote this irreducible polynomial by \( U(x) \).
Since \( U(x) = U_{S_0}(x) \) we have
\[
\deg U \leq c_{55} \frac{1}{e_{S_0}}(S_0^3 g^{1/4} \log^{1/4} S_0) A, \\
\log ht U \leq c_{56} \frac{1}{e_{S_0}}(S_0^3 g^{1/4} \log^{1/4} S_0)(A + B + g^{-1} d_y P_1 d_z P_2).
\]
However \( e_{S_0} \geq 1 \) and therefore for \( C \) sufficiently large
\[
\deg U + \log ht U \leq r^{C/C_1}.
\]
Also, \( U(x) = U_{S_1}(x) \) and therefore
\[
\log |U(\varphi(u))| < -c_{57} \frac{1}{e_{S_1}} S_1^6 \log S_1,
\]
which together with \( e_{S_1} \leq \deg R_{S_1} \) yields
\[
\log |U(p(u))| < -c_{58}(S_1^3 g^{-1/4} \log^{3/4} S_1) A^{-1}.
\]
For \( C \) large enough \( \log |U(p(u))| < -r^{C/4} \). 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