TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 362, Number 4, April 2010, Pages 2115–2123
S 0002-9947(09)05012-0
Article electronically published on November 18, 2009

THE DIOPHANTINE EQUATION $\alpha_1^{x_1} \cdots \alpha_n^{x_n} = f(x_1, \ldots, x_n)$. II

P. CORVAJA, W. M. SCHMIDT, AND U. ZANNIER

Abstract. We will deal with the equation of the title where $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent complex numbers and f is a polynomial. We will give a bound for the number of solutions which depends only on n and the degree of f. Two further results which play a rôle in the proof are of independent interest.

1. Introduction

Throughout, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ will be in $(\mathbb{C}^\times)^n$ with multiplicatively independent components, and for $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ set

$$\boldsymbol{\alpha}^{\mathbf{x}} = \alpha_1^{x_1} \cdots \alpha_n^{x_n}.$$

f will be a polynominal in n variables of total degree $\delta > 0$ with complex coefficients. By a special case of a theorem of Laurent [3], [4], the equation of the title, i.e.,

$$\boldsymbol{\alpha}^{\mathbf{x}} = f(\mathbf{x}), \tag{1.1}$$

has only finitely many solutions $\mathbf{x} \in \mathbb{Z}^n$.

Set

$$\Delta = \binom{n+\delta}{n}, \qquad B = \Delta + 1. \tag{1.2}$$

Again as a special case of a more general theorem, it had been proved in [6] that when

$$K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \tag{1.3}$$

is a number field of degree d, then there are at most

$$d^{6B^2} 2^{35B^3} \tag{1.4}$$

solutions. Here we will establish a bound which depends only on n and δ:

Theorem 1. *The equation* (1.1) *has not more than*

$$\exp(B^{9B}) \tag{1.5}$$

solutions.

Remarks. (i) In the first paper [8] under the present title the bound (1.5) was derived under the hypothesis that K contains no roots of unity, but ± 1.

(ii) The constant 9 in (1.5) is of no significance and could easily be reduced.

Received by the editors May 13, 2008.
2000 *Mathematics Subject Classification.* Primary 11D61, 11D45; Secondary 11R18.

(iii) It is not hard to see that the conclusion of Theorem 1 remains valid for solutions $\mathbf{x} \in \mathbb{Q}^n$, provided that for such $\mathbf{x}$ we set $\alpha_i^{x_i} = e^{a_i x_i}$ $(i = 1, \dots, n)$, where $a_1, \dots, a_n$ are fixed logarithms of $\alpha_1, \dots, \alpha_n$, i.e., are any complex numbers which are linearly independent over $\mathbb{Q}$.

(iv) It would be desirable to generalize our result so as to provide a bound for the more general theorem of Laurent on polynomial–exponential equations, which depends only on the number n of variables and the number and the degrees of the polynomials occurring in the equation, i.e., to give a variation on the estimate in [6] which is independent of a field K containing the data. Such a result is known [7] when $n = 1$.

When ζ is a root of unity of order q, then $\mathbb{Q}(\zeta)$ is of degree $\phi(q)$. More generally, when a field k is contained in $\mathbb{Q}(\zeta)$, then $[k(\zeta) : k] = \phi(q)/\deg k$. On the other hand we have

Theorem 2. *Let k be a number field, and $\alpha^q \in k^\times$, where q is the least positive integer with this property. Then*

$$[k(\alpha) : k] \geqq \phi(q)/D_A, \tag{1.6}$$

where D_A is the degree of the largest abelian subfield of k.

We also have

Theorem 3. *Let k be a number field of degree D. Let $\mathcal{G} \subset \overline{\mathbb{Q}}^\times$ be a multiplicative group generated by n elements, set $\mathcal{H} = \mathcal{G} \cap k^\times$, and suppose $\mathcal{G}/\mathcal{H}$ to be finite. Then any k-vector space $V \subset \overline{\mathbb{Q}}$ of dimension r intersects at most $(g(r, D))^n$ cosets of $\mathcal{H}$ in $\mathcal{G}$.*

We may take $g = g_1$ or $g = g_2$, where

$$g_1(r, D) = 2g_3(r)D^4 \tag{1.7}$$

with

$$g_3(r) = (r + 1)^{12(r+1)^2},$$

and

$$g_2(r, D) = cg_3(r)D^{1+1/\log^+ \log^+ D}, \tag{1.8}$$

where c is an absolute constant and $\log^+ x = \max(1, \log x)$.

Remarks. (i) The estimate with g_2 is stronger but involves the constant c, which however could be estimated with a little extra effort. The simpler estimate with g_1 will suffice to deduce Theorem 1.

(ii) Suppose $\alpha^q \in k^\times$, and q is the least natural number with this property. If $\mathcal{G}$ is generated by α, then $\mathcal{H} = \mathcal{G} \cap k^\times$ is generated by α^q, and the cosets of $\mathcal{H}$ are represented by α^j with $0 \leqq j < q$. By Theorem 3 the number of integers j, $0 \leqq j < q$, with α^j in a given k-vector space of dimension r is bounded by $g(r, D)$.

(iii) On the other hand in [5] it was shown that the number of such integers j is at most

$$g_4(k, \alpha)r(\log r + 2)$$

with an explicit function $g_4(k, \alpha)$. The question thus arises as to whether $g_3(r)$ can be replaced by a slower growing function.

We will first prove Theorem 2, then Theorem 3, and finally deduce Theorem 1 from Theorem 3 and results of [8].

2. Proof of Theorem 2

Let ζ be a primitive q-th root of 1, and set $K = k(\zeta, u)$. Then K is a Galois extension of k, and we set $G = \mathrm{Gal}(K/k)$. The subgroups

$$Z = \mathrm{Gal}(K/k(\zeta)), \qquad X = \mathrm{Gal}(K/k(u))$$

have cardinalities $|Z|, |X|$ with

$$|Z|[k(\zeta) : k] = [K : k(\zeta)][k(\zeta) : k] = [K : k],$$
$$|X|[k(u) : k] = [K : k(u)][k(u) : k] = [K : k],$$

and therefore

$$[k(u) : k] = \frac{|Z|}{|X|}[k(\zeta) : k]. \tag{2.1}$$

Our proof of Theorem 2 will essentially consist of three steps. In the first step we will find that

$$|Z| = q/m \tag{2.2}$$

for a certain divisor m of q. Write $q = m^* q^*$, where m^* is composed of primes dividing m, and $\gcd(q^*, m) = 1$. In the second and hardest step we will show that

$$|X| \leqq \phi(q^*)m^*/m, \tag{2.3}$$

and in the third step we will establish

$$[k(\zeta) : k] \geqq \phi(q)/D_A. \tag{2.4}$$

Substitution of (2.2), (2.3), and (2.4) into (2.1) yields

$$[k(u) : k] \geqq \frac{1}{D_A} \frac{q\phi(q)}{\phi(q^*)m^*} = \frac{q\phi(m^*)\phi(q^*)}{D_A\phi(q^*)m^*} = \frac{q}{D_A} \cdot \frac{\phi(m^*)}{m^*}.$$

Here $m^* \mid q$, and among divisors m^* of q, the quotient $\phi(m^*)/m^*$ is least when $m^* = q$, so that $[k(u) : k] \geqq (q/D_A)(\phi(q)/q) = \phi(q)/D_A$, and Theorem 2 will follow.

Each $g \in G$ is determined by its action on ζ and u. We have

$$g(\zeta) = \zeta^{a_g} \quad \text{with} \quad a_g \in (Z/(q))^\times,$$
$$g(u) = \zeta^{b_g} u \quad \text{with} \quad b_g \in \mathbb{Z}/(q).$$

The b_g ($g \in G$) are relatively prime in $\mathbb{Z}/(q)$, i.e., there is no divisor $\ell > 1$ of q which divides all of them. For otherwise $g(u^{q/\ell}) = \zeta^{(q/\ell)b_g} u^{q/\ell} = u^{q/\ell}$ for each $g \in G$, and therefore $u^{q/\ell} \in k$, contradicting the minimality of q.

For g, h in G,

$$gh(\zeta) = g(\zeta^{a_h}) = \zeta^{a_g a_h}, \quad gh(u) = g(\zeta^{b_h} u) = \zeta^{b_h a_g + b_g} u,$$

hence

$$a_{gh} = a_g a_h, \qquad b_{gh} = b_g + a_g b_h. \tag{2.5}$$

The map $\alpha : G \to (\mathbb{Z}/(q))^\times$ with $\alpha(g) = a_g$ is a homomorphism. Its image, being a subgroup of $(Z/(q))^\times$, is commutative. Its kernel consists of elements g with $a_g = 1$, i.e., with $g(\zeta) = \zeta$, and hence equals Z. We therefore may identify G/Z with a subgroup of $(\mathbb{Z}/(q))^\times$ so that G/Z is commutative, and we may interpret α as a surjective homomorphism into G/Z. Let $\alpha \mid X$ be the restriction of α to X.

Its kernel consists of $X \cap Z = \{id\}$. Thus the image $\alpha(X) \subset G/Z$ has cardinality $|\alpha(X)| = |X|$.

The map $\beta : G \to \mathbb{Z}/(q)$ with $\beta(g) = b_g$ is not a homomorphism.[1] Its "kernel" consists of g with $b_g = 0$, i.e., $g(u) = u$, and hence equals X. For g, h in Z

$$b_{gh} = b_g + a_g b_h = b_g + b_h.$$

Hence the restriction of β to Z, denoted by $\beta \mid Z$, is a homomorphism. Its kernel consists of elements $g \in Z$ lying in X, and hence equals $Z \cap X = \{id\}$. Therefore $\beta \mid Z$ is an injection. Its image in $\mathbb{Z}/(q)$ consists of elements $a \equiv 0 (\mathrm{mod}\ m)$ where m is a divisor of q, and (2.2) follows. This completes step one.

Let $\bar{x}$ be the reduction mod m of an element $x \in Z/(q)$. We have

$$\bar{a}_z = 1, \qquad \bar{b}_z = 0 \qquad \text{for} \quad z \in Z.$$

Since $\gcd(a_g, q) = 1$ for each $g \in G$, then also $\gcd(\bar{a}_g, m) = 1$. Since the b_g with $g \in G$ are coprime in $\mathbb{Z}/(q)$, the $\bar{b}_g$ are coprime in $\mathbb{Z}/(m)$. By (2.5), for $g \in G$, $z \in Z$,

$$\begin{aligned} &\bar{a}_{gz} = \bar{a}_{zg} = \bar{a}_z \bar{a}_g = \bar{a}_g, \\ &\bar{b}_{gz} = \bar{b}_g + \bar{a}_g \bar{b}_z = \bar{b}_g, \quad \bar{b}_{zg} = \bar{b}_z + \bar{a}_z \bar{b}_g = \bar{b}_g. \end{aligned} \tag{2.6}$$

Therefore $\bar{a}_g, \bar{b}_g$ depend only on the coset of Z to which g belongs, hence only on the image of g in G/Z. As a consequence, $\bar{a}_\tau, \bar{b}_\tau$ can be defined for $\tau \in G/Z$ in a natural way. Since G/Z is commutative, (2.6) yields

$$\bar{b}_{\sigma\tau} = \bar{b}_\sigma + \bar{a}_\sigma \bar{b}_\tau, \qquad \bar{b}_{\sigma\tau} = \bar{b}_{\tau\sigma} = \bar{b}_\tau + \bar{a}_\tau \bar{b}_\sigma$$

for σ, τ in G/Z, and hence

$$\bar{b}_\sigma (\bar{a}_\tau - 1) = \bar{b}_\tau (\bar{a}_\sigma - 1).$$

Let $T \subset G/Z$ consist of elements τ with $\bar{b}_\tau = 0$. Then $\bar{b}_\sigma (\bar{a}_\tau - 1) = 0$ for $\tau \in T$, $\sigma \in G/Z$. But the $\bar{b}_\sigma$ with $\sigma \in G/Z$ are coprime in $Z/(m)$, so that

$$\bar{a}_\tau = 1 \quad \text{for} \quad \tau \in T. \tag{2.7}$$

When $g \in X$, then $b_g = 0$, $\bar{b}_g = 0$, and hence $\bar{b}_\tau = 0$ when $\tau \in \alpha(X) \subset G/Z$. We may infer that $\alpha(X) \subset T$, so that

$$|X| = |\alpha(X)| \leqq |T|. \tag{2.8}$$

To finish step 2 we need to estimate $|T|$. Since G/Z may be identified with a subgroup of $(\mathbb{Z}/(q))^\times$, and by (2.7), the cardinality $|T|$ is bounded by the number of residue classes mod q which are prime to q and are $\equiv 1 (\mathrm{mod}\ m)$. Recall the notation $q = m^* q^*$ and observe that $m \mid m^*$. By the Chinese Remainder Theorem, the number of residue classes in question is the product of (i) the number of residue classes mod m^* which are $\equiv 1 (\mathrm{mod}\ m)$, which equals m^*/m, and (ii) the number of residue classes mod q^*, which are coprime to q^*, which is $\phi(q^*)$. Therefore

$$|T| \leqq \phi(q^*) m^*/m,$$

and this together with (2.8) gives (2.3).

[1] It is a 1-cocycle.

$\mathbb{Q}(\zeta)$ is normal over $k \cap \mathbb{Q}(\zeta)$, so that by a well known theorem of Galois theory also $k(\zeta)$ is normal over k, and $[k(\zeta) : k] = [\mathbb{Q}(\zeta) : (\mathbb{Q}(\zeta) \cap k)]$. Hence

$$[k(\zeta) : k] = \deg \mathbb{Q}(\zeta) / \deg(\mathbb{Q}(\zeta) \cap k) \geqq \phi(q)/D_A,$$

since $\mathbb{Q}(\zeta) \cap k$, being abelian, is contained in the maximal abelian subfield of k.

This completes step 3, hence the proof of Theorem 2.

3. Proof of Theorem 3

Let k be a subfield of $\mathbb{C}$. An element $\xi \in \mathbb{C}$ will be called a *radical* of k if $\xi^m \in k^\times$ for some natural m. Given $(\xi_1 : \cdots : \xi_s)$ in projective space over $\mathbb{C}$, we will write $k(\xi_1 : \cdots : \xi_s)$ for the field generated over k by the quotients ξ_i/ξ_j with $1 \leqq i, j \leqq s$, $\xi_j \neq 1$. When

$$\sum_{i=1}^{s} \lambda_i \xi_i = 0 \tag{3.1}$$

is an equation with nonzero coefficients $\lambda_1, \ldots, \lambda_s$ in unknowns $\xi_1, \ldots, \xi_s$, a solution will be called *nondegenerate* if no nontrivial subsum of the sum in (3.1) vanishes.

Lemma. *Suppose $s \geqq 2$, suppose $\lambda_i \in k^\times$ for $1 \leqq i \leqq s$, and suppose $(\xi_1, \ldots, \xi_s)$ is a nondegenerate solution of (3.1) where each ξ_i is a radical of k. Then*

$$[k(\xi_1 : \cdots : \xi_s) : k] \leqq g_5(s), \tag{3.2}$$

where $g_5(s) = s^{3s^2}$.

Moreover, when k is a number field of degree D, then there is a positive integer $q < Q = Q(s, D)$ with

$$(\xi_i/\xi_j)^q \in k^\times (1 \leqq i, j \leqq s). \tag{3.3}$$

We may set $Q = Q_1$ or $Q = Q_2$, where

$$Q_1(s, D) = g_5(s)^2 D^2, \quad Q_2(s, D) = c g_5(s)^2 D \log^+ \log^+ D. \tag{3.4}$$

The letter c, here and below, will denote absolute positive constants, not all the same, so that for instance $x \leqq c^2$ or $x \leqq e^c$ will imply $x \leqq c$.

Proof of the Lemma. Let σ be an embedding of $k(\xi_1 : \cdots : \xi_s)$ over k into $\mathbb{C}$. When $\xi^m \in k^\times$ for some natural m, then $(\sigma(\xi))^m = \sigma(\xi^m) = \xi^m$, so that $\sigma(\xi) = \xi\zeta$ where ζ is a root of unity. Applying σ to (3.1) where each ξ_i is a radical of k, we obtain

$$\sum_{i=1}^{s} \lambda_i \xi_i \zeta_{\sigma i} = 0, \tag{3.5}$$

where $\zeta_{\sigma i}$ $(i = 1, \ldots, s)$ is a root of unity. We will interpret (3.5) as an equation in $\zeta_{\sigma 1}, \ldots, \zeta_{\sigma s}$. When $(\xi_1, \ldots, \xi_s)$ is a nondegenerate solution of (3.1), $(\zeta_{\sigma 1}, \ldots, \zeta_{\sigma s})$ is a nondegenerate solution of (3.5). According to J.-H. Evertse [1] there are up to a factor of proportionality at most $g_5(s)$ such solutions in roots of unity. Since $\sigma(\xi_i/\xi_j) = (\zeta_{\sigma i}/\zeta_{\sigma j})(\xi_i/\xi_j)$ for $1 \leqq i, j \leqq s$, there are at most $g_5(s)$ distinct embeddings of $k(\xi_1 : \cdots : \xi_s)$ over k into $\mathbb{C}$, and (3.2) follows.

Let $\mathcal{A}$ be the multiplicative group generated by the quotients ξ_i/ξ_j $(1 \leqq i, j \leqq s)$, and set $\mathcal{B} = \mathcal{A} \cap k^\times$. Then $\mathcal{A}$ as well as $\mathcal{B}$ is finitely generated, and each element of $\mathcal{A}/\mathcal{B}$ is of finite order, so that $\mathcal{A}/\mathcal{B}$ is finite. By the Fundamental Theorem of finite abelian groups there is an element $\bar{\eta} \in \mathcal{A}/\mathcal{B}$ of some order q such that every element of $\mathcal{A}/\mathcal{B}$ has order dividing q. Every $\theta \in \mathcal{A}$ has image $\bar{\theta} \in \mathcal{A}/\mathcal{B}$ of order

dividing q, so that $\bar{\theta}^q = 1$ and $\theta^q \in k^\times$. In particular, the quotients ξ_i/ξ_j will have (3.3).

Here $\bar{\eta}$ is the image of some $\eta \in \mathcal{A}$ with $\eta^q \in \mathcal{B} \subset k^\times$, where q is the least natural number with this property. Since $\eta \in k(\xi_1 : \cdots : \xi_s)$, (3.2) yields $[k(\eta) : k] \leqq g_5(s)$. On the other hand Theorem 2 gives $[k(\eta) : k] \geqq \phi(q)/D$, so that

$$\phi(q) \leqq g_5(s)D.$$

We may suppose $q \geqq 3$, so that, as is easily seen, $\phi(q) > q^{1/2}$; hence $q < \phi(q)^2 \leqq g_5(s)^2 D^2 = Q_1(s, D)$. On the other hand $\phi(q) > cq/\log^+\log^+ q$ (see, e.g., [2], Theorem 328), so that

$$q < c\phi(q)\log^+\log^+\phi(q) < cg_5(s)D\log^+\log^+(g_5(s)D).$$

Since $\log^+\log^+ xy < c(\log^+\log^+ x)(\log^+\log^+ y)$, we obtain

$$q < cg_5(s)(\log^+\log^+ g_5(s))D\log^+\log^+ D;$$

therefore $q < Q_2(s, D)$. □

Proof of Theorem 3. Let $\xi_1, \ldots, \xi_n$ be a set of generators of $\mathcal{G}$, and for $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$ write

$$\boldsymbol{\xi}^{\mathbf{m}} = \xi_1^{m_1} \cdots \xi_n^{m_n}. \tag{3.6}$$

The elements of $\mathcal{G}$ may be written as $\boldsymbol{\xi}^{\mathbf{m}}$ with $\mathbf{m} \in \mathbb{Z}^n$, but not necessarily uniquely. Since $\mathcal{G}/\mathcal{H}$ is finite, the n-tuples $\mathbf{m}$ with $\boldsymbol{\xi}^{\mathbf{m}} \in \mathcal{H}$ form a lattice $\Lambda \subset \mathbb{Z}^n$. When $\mathcal{P} \subset \mathbb{Z}^n$ is a set of representatives of the cosets of Λ, then the cosets of $\mathcal{H}$ are uniquely represented by the elements (3.6) with $\mathbf{m} \in \mathcal{P}$.

Whether $\boldsymbol{\xi}^{\mathbf{m}}$ lies in V depends only on the coset of $\mathcal{H}$ to which $\mathbf{m}$ belongs. We therefore have to estimate the cardinality of the set $\mathcal{M}$ of elements $\mathbf{m} \in \mathcal{P}$ with $\boldsymbol{\xi}^{\mathbf{m}} \in V$. The case $r = 1$ of Theorem 3 holds since $g(1, D) \geqq 1$, and since when $\mathbf{u}, \mathbf{v}$ are in $\mathcal{M}$ with $\boldsymbol{\xi}^{\mathbf{u}}, \boldsymbol{\xi}^{\mathbf{v}}$ linearly dependent over k, then $\boldsymbol{\xi}^{\mathbf{u}-\mathbf{v}}$ lies in $k^\times$, and hence in $\mathcal{H}$, so that $\mathbf{u} - \mathbf{v} \in \Lambda$. Therefore $\mathbf{u} = \mathbf{v}$ in view of $\mathbf{u}, \mathbf{v} \in \mathcal{P}$. In the induction step from $r-1$ to r we may suppose that the elements $\boldsymbol{\xi}^{\mathbf{m}}$ with $\mathbf{m} \in \mathcal{M}$ generate V, for otherwise V may be replaced by a space of dimension less than r. For $h > 0$ and $\mathbf{a}_1, \ldots, \mathbf{a}_h$ in $\mathcal{M}$, let $q(\mathbf{a}_1, \ldots, a_h)$ be the least positive integer q with

$$\boldsymbol{\xi}^{q(\mathbf{a}_i - \mathbf{a}_j)} \in k^\times \qquad (1 \leqq i, j \leqq h).$$

Such q certainly exists; in fact there is a $q > 0$ with $q\mathbb{Z}^n \subset \Lambda$. Also,

$$q(\mathbf{a}_i, \mathbf{a}_j) \mid q(\mathbf{a}_1, \ldots, \mathbf{a}_h) \qquad (1 \leqq i, j \leqq h). \tag{3.7}$$

Let R be the maximum of $q(\mathbf{u}, \mathbf{v})$ over $\mathbf{u}, \mathbf{v}$ in $\mathcal{M}$, and pick $\mathbf{a}_1, \mathbf{a}_2$ in $\mathcal{M}$ with

$$q(\mathbf{a}_1, \mathbf{a}_2) = R.$$

Since $q(\mathbf{u}, \mathbf{u}) = 1$ and $q(\mathbf{u}, \mathbf{v}) > 1$ for $\mathbf{u} \neq \mathbf{v}$ in $\mathcal{M}$, we will have $\mathbf{a}_1 \neq \mathbf{a}_2$ provided $|\mathcal{M}| > 1$, which we certainly may suppose. Then $\boldsymbol{\xi}^{a_1}, \boldsymbol{\xi}^{\mathbf{a}_2}$ are linearly independent over k.

When $r > 2$ pick $\mathbf{a}_3, \ldots, \mathbf{a}_r$ in $\mathcal{M}$ such that $\boldsymbol{\xi}^{\mathbf{a}_1}, \boldsymbol{\xi}^{\mathbf{a}_2}, \ldots, \boldsymbol{\xi}^{\mathbf{a}_r}$ are a basis of V. Each $\boldsymbol{\xi}^{\mathbf{m}}$ with $\mathbf{m} \in \mathcal{M}$ has a unique representation

$$\boldsymbol{\xi}^{\mathbf{m}} = \lambda_1 \boldsymbol{\xi}^{\mathbf{a}_1} + \lambda_2 \boldsymbol{\xi}^{\mathbf{a}_2} + \cdots + \lambda_r \boldsymbol{\xi}^{\mathbf{a}_r} \tag{3.8}$$

with coefficients $\lambda_i \in k$. The elements $\boldsymbol{\xi}^{\mathbf{m}}$ having $\lambda_i = 0$ for given i lie in a space of dimension $r-1$. By induction, and since $rg_3(r-1) < \frac{1}{2}g_3(r)$, the number of $\mathbf{m} \in \mathcal{M}$ with some $\lambda_i = 0$ is less than

$$\frac{1}{2}\min((g_1(r,D))^n, (g_2(r,D))^n). \tag{3.9}$$

Let $\mathcal{M}'$ be the set of $\mathbf{m} \in \mathcal{M}$ where no λ_i $(1 \leqq i \leqq r)$ in (3.8) vanishes, and for $\mathbf{m} \in \mathcal{M}'$ write

$$p(\mathbf{m}) = q(\mathbf{m}, \mathbf{a}_1, \dots, \mathbf{a}_r).$$

Since $\boldsymbol{\xi}^{\mathbf{a}_1}, \dots, \mathbf{a}^{\mathbf{a}_r}$ are linearly independent over k, so that no subsum of the sum in (3.8) vanishes, we may apply the Lemma with $s = r+1$ to see that

$$p(\mathbf{m}) < Q(r+1, D) = S, \tag{3.10}$$

say. Therefore $\ell := p(\mathbf{m})/q(\mathbf{a}_1, \mathbf{a}_2) < S/R$, and ℓ is an integer by (3.7). There are fewer than S/R choices for ℓ, and hence fewer than S/R choices for $p(\mathbf{m})$.

Let $h(x)$ for $x \geqq 1$ be an upper bound for the number of divisors of positive integers not exceeding x. Since $q(\mathbf{m}, \mathbf{a}_1)$ is a divisor of $p(\mathbf{m})$ by (3.7), we see that when the latter is given, there are at most $h(p(\mathbf{m})) \leqq h(S)$ choices for $q(m, \mathbf{a}_1)$. Altogether there are at most

$$h(S)S/R \tag{3.11}$$

possibilities for $q(\mathbf{m}, \mathbf{a}_1)$.

Let us count n-tuples $\mathbf{m} \in \mathcal{M}'$ with given $q(\mathbf{m}, a_1)$, say $q(\mathbf{m}, \mathbf{a}_1) = t$, where $t \leqq R$ by definition of R. Such $\mathbf{m}$ will have $t(\mathbf{m} - \mathbf{a}_1) \in \Lambda$, and hence

$$t\mathbf{m} \equiv \mathbf{a}_1 (\text{mod } \Lambda). \tag{3.12}$$

The map $\overline{\mathbf{m}} \mapsto t\overline{\mathbf{m}}$ from Z^n/Λ into itself has kernel of cardinality at most t^n, since $\mathbb{Z}^n/\Lambda$ is a product of at most n cyclic groups, and a map $x \mapsto tx$ in an additive cyclic group has kernel of cardinality $\leqq t$. Since $\mathcal{P}$ is a set of representatives of Z^n/Λ, there are at most $t^n \leqq R^n$ elements $\mathbf{m} \in \mathcal{P}$ with (3.12), hence at most R^n choices for $\mathbf{m}$ when $q(\mathbf{m}, \mathbf{a}_1)$ is given. Multiplying this by the quantity in (3.11) we obtain

$$|\mathcal{M}'| \leqq h(S)SR^{n-1} \leqq h(S)S^n$$

since $R = q(\mathbf{a}_1, \mathbf{a}_2) \leqq q(\mathbf{m}, \mathbf{a}_1, \dots, \mathbf{a}_r) = p(\mathbf{m}) < S$.

Here $S = Q(r+1, D) \leqq Q_1(r+1, D) = (g_5(r+1))^2D^2$, and since $h(S) \leqq S$,

$$|\mathcal{M}'| < S^{n+1} \leqq S^{2n} \leqq ((g_5(r+1))^4D^4)^n = (g_3(r)D^4)^n \leqq \frac{1}{2}(g_1(r,D))^n,$$

which in conjunction with the bound (3.9) yields $|\mathcal{M}| < (g_1(r,D))^n$.

On the other hand $S \leqq Q_2(r+1, D) = c(g_5(r+1))^2 D \log^+\log^+ D$. Moreover,

$$h(x) < cx^{(3/4)/\log^+\log^+ x},$$

e.g., by Theorem 317 in [2]. Thus

$$h(D\log^+\log^+ D) < c(D\log^+\log^+ D)^{(3/4)/\log^+\log^+ D} < cD_0^{3/4}$$

with $D_0 = D^{1/\log^+\log^+ D}$. Since $h(xy) < ch(x)h(y) \leqq Cxh(y)$,

$$h(S) < c(g_5(r+1))^2 D_0^{3/4},$$

and

$$|\mathcal{M}'| < S^n h(S) < c^n (g_5(r+1))^{2n+2} (D \log^+ \log^+ D)^n D_0^{3/4}$$
$$< (c(g_5(r+1))^4 D D_0)^n = (c g_3(r) D D_0)^n < \frac{1}{2}(g_2(r,D))^n,$$

which together with the estimate (3.9) yields $|\mathcal{M}| < (g_2(r,D))^n$.

4. Deduction of Theorem 1

We will follow the approach of [8]. We will show by induction on n that the number of solutions of (1.1) is less than

$$\exp(2n^2 B^{8B}). \tag{4.1}$$

Since $B > n$, $B \geqq 3$, the theorem will follow. Let $r_{\mathbb{Q}}$ be the dimension of the vector space $V_{\mathbb{Q}}$ over $\mathbb{Q}$ spanned by the coefficients of f, so that $r_{\mathbb{Q}} \leqq \Delta$, where Δ is given by (1.2). Let $\mathcal{G}$ be the multiplicative group generated by $\alpha_1, \dots, \alpha_n$. As in [8] we will first reduce to the case when there is a field $L \subset K$ of degree $D \leqq r_{\mathbb{Q}}$ such that $\mathcal{H} := \mathcal{G} \cap L^\times$ is of finite index in $\mathcal{G}$.

For an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and $1 \leqq k \leqq r_{\mathbb{Q}}$, let $G(\sigma,k)$[2] be the group defined in [8]. When there is a σ with rank $G(\sigma,k) < n$ for each k, $1 \leqq k \leqq r_{\mathbb{Q}}$, the solutions fall into fewer than

$$\exp((6B)^{3B}(n+1) + B) \tag{4.2}$$

classes as defined in [8]. (In [8] the summand B in the exponent was missing. It stems from the fact that there are $2^r < e^B$ sets $\mathcal{K}$.) Solutions in each class come from equations such as (1.1) in $n-1$ variables. When $n = 1$ there is at most one solution in each class, and in fact for any n there are by induction fewer than

$$\exp(2(n-1)^2 B^{8B}) \tag{4.3}$$

solutions in each class. Since $B \geqq 3$ we have

$$(6B)^{3B}(n+1) + B + 2(n-1)^2 B^{8B} < 2n^2 B^{8B},$$

and the product of the quantities in (4.2) and (4.3) is less than the one in (4.1).

When for each σ there is a k, $1 \leqq k \leqq r_{\mathbb{Q}}$, with rank $G(\sigma,k) = n$, then one concludes as in [8] that $\mathcal{G}^m \subset L^\times$ for some $m \in \mathbb{N}$ and some field $L \subset K$ of degree $D \leqq r_{\mathbb{Q}} < B$. Here $\mathcal{G}^m$, which had been defined to consist of powers α^m with $\alpha \in \mathcal{G}$, is of finite index in $\mathcal{G}$, and since $\mathcal{G}^m \subset \mathcal{H}$, $\mathcal{H}$ is also of finite index.

Equation (1.1) implies that $\boldsymbol{\alpha}^{\mathbf{x}}$ lies in the L-vector space V spanned by the coefficients of f. By Theorem 3 (with L in place of k), $\boldsymbol{\alpha}^{\mathbf{x}}$ will lie in the union of not more than $(g_1(r,D))^n$ cosets of $\mathcal{H}$ where $r = \dim V \leqq \Delta = B - 1$, so that

$$g_1(r,D) < g_1(B-1,B) = 2g_3(B-1)B^4 = 2B^{12B^2} \cdot B^4 < 2^{13B^3}. \tag{4.4}$$

Here $\mathcal{H}$ will be a free group of rank $\ell \leqq n$ generated by elements $\beta_i = \boldsymbol{\alpha}^{\mathbf{g}_i}$ with $\mathbf{g}_i \in Z^n$ $(i = 1, \dots, \ell)$. Thus $\boldsymbol{\alpha}^{\mathbf{x}}$ is in $\mathcal{H}$ when $\mathbf{x} = y_1\mathbf{g}_1 + \cdots + y_\ell \mathbf{g}_\ell$ with

[2]Let $\mathcal{S}$ consist of the embeddings $\sigma : K \hookrightarrow \mathbb{C}$, and for $\boldsymbol{\alpha} \in K^n$ and $\sigma \in \mathcal{S}$ define $\sigma(\boldsymbol{\alpha})$ component-wise. Let $b_1, \dots, b_{r_{\mathbb{Q}}}$ be a basis of $V_{\mathbb{Q}}$. There are elements $\sigma_1, \dots, \sigma_{r_{\mathbb{Q}}}$ of $\mathcal{S}$ such that $\det(\sigma_i(b_j))_{1 \leqq i,j \leqq r_Q}$ is nonzero. The group $G(\sigma,k)$ for $\sigma \in \mathcal{S}$ and $1 \leqq k \leqq r_{\mathbb{Q}}$ consists of points $\mathbf{y} \in Z^n$ with

$$\sigma(\boldsymbol{\alpha})^{\mathbf{y}} = \sigma_k(\boldsymbol{\alpha})^{\mathbf{y}}.$$

The arguments in [8] depend on earlier work by several authors on linear equations in variables which lie in a multiplicative group.

$y = (y_1, \ldots, y_\ell) \in \mathbb{Z}^\ell$, and is in a fixed coset of $\mathcal{H}$ when $\mathbf{x} = \mathbf{z} + y_1\mathbf{g}_1 + \cdots + y_\ell\mathbf{g}_\ell$ with fixed $\mathbf{z}$. Substitution into (1.1) and division by $\boldsymbol{\alpha}^{\mathbf{z}}$ yields

$$\beta_1^{y_1} \cdots \beta_\ell^{y_\ell} = \boldsymbol{\alpha}^{-\mathbf{z}} f(\mathbf{z} + y_1\mathbf{g}_1 + \cdots + y_\ell\mathbf{g}_\ell) = f_{\mathbf{z}}(y_1, \ldots, y_\ell), \tag{4.5}$$

say. This is of the same type as equation (1.1). But we have gained, for the β_i lie in the field L of degree $D < B$. Therefore by the estimate (1.4) the number of solutions $\mathbf{y} \in \mathbb{Z}^\ell$ of (4.5) is less than

$$B^{6B^2} \cdot 2^{35B^3} < 2^{41B^3}.$$

Multiplication by the number of cosets, which is at most $(g_1(r, D))^n < 2^{13B^3 n}$, gives less than 2^{54nB^3}, which in turn is much less than the claimed bound (4.1). □

References

1. J.-H. Evertse. *The number of solutions of linear equations in roots of unity.* Acta Arith. **89** (1999), 45–51. MR1692199 (2000e:11033)
2. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* 3rd ed. Clarendon Press, Oxford (1954). MR0067125 (16:673c)
3. M. Laurent. *Équations exponentielles polynômes et suites récurrentes linéaires.* Astérisque **147–148** (1987), 343–344.
4. M. Laurent. *Équations exponentielles polynômes et suites récurrentes linéaires*, II. J. Number Theory **31** (1989), 24–53. MR978098 (90b:11023)
5. A. Schinzel and W. M. Schmidt. *Powers of Roots in Linear Spaces.* Journal of Number Theory (to appear).
6. H. P. Schlickewei and W. M. Schmidt. *The Number of Solutions of Polynomial–Exponential Equations.* Compositio Math. **120** (2000), 193–225. MR1739179 (2001b:11022)
7. W. M. Schmidt. *The zero multiplicity of linear recurrence sequences.* Acta Math. **182** (1999), 243–282. MR1710183 (2000j:11043)
8. W. M. Schmidt. *The Diophantine Equation* $\alpha_1^{x_1} \cdots \alpha_n^{x_n} = f(x_1, \ldots, x_n)$. Analytic Number Theory. Essays in Honour of Klaus Roth, 414–420. Cambridge University Press (2009). MR2508660

Department of Mathematics and Informatics, University of Udine, Via delle Scienze 206, 33100 Udine, Italy

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395

Department of Mathematics, Scuola Normale Superiore, Piazza de Cavalier, 56100 Pisa, Italy