ACTA ARITHMETICA
LXXXIX.1 (1999)

The number of solutions of linear equations in roots of unity

by

JAN-HENDRIK EVERTSE (Leiden)

1. Introduction. We deal with equations

$$a_1\zeta_1 + \ldots + a_n\zeta_n = 1 \quad \text{in roots of unity } \zeta_1, \ldots, \zeta_n \tag{1.1}$$

with non-zero complex coefficients. Clearly, from a solution for which one of the subsums on the left-hand side is zero, it is possible to construct infinitely many other solutions. Therefore, we restrict ourselves to solutions of (1.1) for which all subsums on the left-hand side are non-zero, i.e.,

$$\sum_{i\in I} a_i\zeta_i \neq 0 \quad \text{for each non-empty subset } I \text{ of } \{1, \ldots, n\}.$$

Such solutions of (1.1) are called *non-degenerate*.

Denote by $\nu(a_1, \ldots, a_n)$ the number of non-degenerate solutions of (1.1). First, let $a_1, \ldots, a_n$ be non-zero rational numbers. In 1965, Mann [2] showed that if $(\zeta_1, \ldots, \zeta_n)$ is a non-degenerate solution of (1.1), then $\zeta_1^d = \ldots = \zeta_n^d = 1$, where d is a product of distinct primes $\leq n+1$. From this result it can be deduced that $\nu(a_1, \ldots, a_n) \leq e^{c_1 n^2}$ for some absolute constant c_1. Later, Conway and Jones [1] showed that for every non-degenerate solution $(\zeta_1, \ldots, \zeta_n)$ of (1.1) one has $\zeta_1^d = \ldots = \zeta_n^d = 1$, where d is the product of distinct primes $p_1, \ldots, p_l$ with $\sum_{i=1}^{l}(p_i - 2) \leq n-1$. This implies that $\nu(a_1, \ldots, a_n) \leq e^{c_2 n^{3/2}(\log n)^{1/2}}$ for some absolute constant c_2. Schinzel [3] showed that if $a_1, \ldots, a_n$ are non-zero and generate an algebraic number field of degree D, then $\nu(a_1, \ldots, a_n) \leq c_2(n, D)$ for some function c_2 depending only on n and D. Later, Zannier [5] gave a different proof of this fact and computed c_2 explicitly. Finally, Schlickewei [4] succeeded in deriving an upper bound for the number of non-degenerate solutions of (1.1) depending only on n for arbitrary complex coefficients $a_1, \ldots, a_n$. His result

1991 *Mathematics Subject Classification*: 11D99, 11D05.

was

$$\nu(a_1, \ldots, a_n) \le 2^{4(n+1)!}.$$

The purpose of this paper is to derive the following improvement of Schlickewei's result:

THEOREM. *Let $n \ge 1$ and let $a_1, \ldots, a_n$ be non-zero complex numbers. Then* (1.1) *has at most $(n+1)^{3(n+1)^2}$ non-degenerate solutions.*

The constant 3 can be improved to $2 + \varepsilon$ for every $\varepsilon > 0$ and every sufficiently large n. We shall not work this out. Further, the proof of our Theorem works without modifications for equations (1.1) with coefficients $a_1, \ldots, a_n$ from any field of characteristic zero.

We mention that the proofs of Mann, Conway and Jones, Schinzel and Zannier are effective, in that they provide methods to determine all solutions of (1.1), whereas Schlickewei's proof is not. Our proof has the same defect. Further, in the case where $a_1, \ldots, a_n$ are rational numbers, our method of proof cannot be used to improve upon the estimate of Conway and Jones.

Acknowledgements. I am very grateful to Hans Peter Schlickewei for detecting an error in a previous draft of this paper, and for a suggestion with which I could improve my bound n^{cn^3} in that draft to n^{cn^2}.

2. Equations with rational coefficients. It will be more convenient to deal with a homogeneous version of equation (1.1). Thus, we consider the equation

$$a_1\zeta_1 + \ldots + a_k\zeta_k = 0 \quad \text{in roots of unity } \zeta_1, \ldots, \zeta_k, \tag{2.1}$$

where $k := n + 1 \ge 2$ and where $a_1, \ldots, a_k$ are non-zero complex numbers. Two solutions $(\zeta_1, \ldots, \zeta_k)$ and $(\zeta_1', \ldots, \zeta_k')$ of (2.1) are said to be *proportional* if there is a root of unity ϱ such that $\zeta_i' = \varrho\zeta_i$ for $i = 1, \ldots, k$. A solution $(\zeta_1, \ldots, \zeta_k)$ of (2.1) is called *non-degenerate* if $\sum_{i\in I} a_i\zeta_i \ne 0$ for each proper, non-empty subset I of $\{1, \ldots, k\}$. Thus, the Theorem is equivalent to the statement that up to proportionality, (2.1) has at most k^{3k^2} non-degenerate solutions (i.e., there is a subset of solutions of (2.1) of cardinality $\le k^{3k^2}$ such that every non-degenerate solution of (2.1) is proportional to a solution from this subset).

In the remainder of this section we assume $a_1, \ldots, a_k \in \mathbb{Q}^*$. Many of the arguments in the proof of Lemma 1 below have been borrowed from the proof of Theorem 1 of Mann [2]. This result states that every non-degenerate solution of (2.1) is proportional to a solution consisting of (not necessarily primitive) dth roots of unity, where d is the product of distinct primes $\le k$. We could have given a slightly shorter proof of our Lemma 1 by applying Mann's theorem, but we preferred to keep our paper self-contained. The *order* of a root of unity ζ is the smallest positive integer d such that $\zeta^d = 1$.

LEMMA 1. *Let* $(\zeta_1, \ldots, \zeta_k)$ *be a* (*not necessarily non-degenerate*) *solution of* (2.1). *Then there are indices* i, j *with* $1 \le i < j \le k$ *such that* ζ_i/ζ_j *is a root of unity of order* $\le k^2$.

Proof. We proceed by induction on k. If $k = 2$, then $\zeta_1/\zeta_2 = -a_2/a_1 \in \mathbb{Q}$, hence $\zeta_1/\zeta_2 = \pm 1$. Let $k \ge 3$ and suppose that the assertion holds for equations (2.1) with fewer than k unknowns. We assume that $(\zeta_1, \ldots, \zeta_k)$ is non-degenerate. This is no loss of generality since if the left-hand side of (2.1) has a proper vanishing subsum then the assertion follows by applying the induction hypothesis to that subsum. We assume also that $\zeta_1 = 1$. Again, this is no restriction, since replacing $(\zeta_1, \ldots, \zeta_k)$ by a proportional solution does not affect the quotients ζ_i/ζ_j. Lastly, we assume that $(\zeta_1, \ldots, \zeta_k) \ne (1, \ldots, 1)$.

Let d be the smallest positive integer such that $\zeta_1^d = \ldots = \zeta_k^d = 1$. Then $d > 1$. Choose any prime p dividing d and let p^m be the largest power of p dividing d. We have unique expressions

$$\zeta_i = \zeta_i^* \cdot \zeta^{\nu_i} \quad \text{for } i = 1, \ldots, k, \tag{2.2}$$

in which ζ is a primitive p^mth root of unity and for $i = 1, \ldots, k$, ζ_i^* is a root of unity with $(\zeta_i^*)^{d/p} = 1$ and $\nu_i \in \{0, \ldots, p-1\}$. Let $K = \mathbb{Q}(\zeta^*)$, where ζ^* is a primitive (d/p)th root of unity. By inserting (2.2) into (2.1) and using $a_1, \ldots, a_k \in \mathbb{Q}^*$ we get

$$\sum_{q=0}^{p-1} a(q)\zeta^q = 0 \quad \text{with} \quad a(q) = \sum_{i:\nu_i = q} a_i \zeta_i^* \in K \text{ for } q = 0, \ldots, p-1. \tag{2.3}$$

From the minimality of d it follows that at least one of the exponents $\nu_1, \ldots, \nu_k$ in (2.2) is non-zero. Recalling that $\zeta_1 = 1$ we have $\nu_1 = 0$. Hence $\{i : \nu_i = 0\}$ is a proper, non-empty subset of $\{1, \ldots, k\}$. But as $(\zeta_1, \ldots, \zeta_k)$ is non-degenerate this implies

$$a(0) = \sum_{i:\nu_i = 0} a_i \zeta_i^* \ne 0. \tag{2.4}$$

From (2.3) and (2.4) it follows that ζ has degree at most $p-1$ over K. This implies that p^2 does not divide d, since otherwise ζ would have degree p over K. Since p was an arbitrary prime divisor of d, we infer that d is square-free.

But then ζ is a primitive pth root of unity and ζ has degree $p-1$ over K and minimal polynomial $X^{p-1} + X^{p-2} + \ldots + 1$ over K. Together with (2.3) this implies $a(0) = \ldots = a(p-1)$, that is,

$$\sum_{i:\nu_i = q_1} a_i \zeta_i^* + \sum_{i:\nu_i = q_2} (-a_i) \zeta_i^* = 0 \tag{2.5}$$

for each pair $q_1, q_2 \in \{0, \ldots, p-1\}$ with $q_1 \ne q_2$.

We want to apply the induction hypothesis to (2.5). Let p be the largest prime dividing d. If $p \le 3$ then from the fact that d is square-free it follows that $d \le 6$ and hence ζ_i/ζ_j is a root of unity of order $\le 6 < k^2$ for all $i, j \in \{1, \ldots, k\}$. Suppose that $p \ge 5$. By (2.4) and $a(0) = \ldots = a(p-1)$ we have $a(q) \ne 0$ and therefore $\{i : \nu_i = q\}$ is non-empty for $q = 0, \ldots, p-1$. From this fact and $p \ge 5$ it follows that there are distinct $q_1, q_2 \in \{0, \ldots, p-1\}$ such that the set $T := \{i : \nu_i \in \{q_1, q_2\}\}$ has cardinality at most $\frac{2}{p} \cdot k < k$.

Now the induction hypothesis applied to (2.5) with these indices q_1, q_2 implies that there are different indices $h, j \in T$ such that ζ_h^*/ζ_j^* is a root of unity of order at most $(2k/p)^2$. By (2.3) we have

$$\zeta_h/\zeta_j = \zeta^a(\zeta_h^*/\zeta_j^*) \quad \text{ with } a \in \{0, q_1 - q_2, q_2 - q_1\}.$$

Recalling that ζ has order p, we infer that ζ_h/ζ_j has order at most

$$p\left(\frac{2}{p} \cdot k\right)^2 = \frac{4}{p} k^2 < k^2;$$

here we used again the fact that $p \ge 5$. This completes the proof of Lemma 1. ∎

An immediate consequence of Lemma 1 is the following:

LEMMA 2. *There is a set U of cardinality at most k^4, depending only on k, such that for every solution $(\zeta_1, \ldots, \zeta_k)$ of (2.1) there are distinct indices $i, j \in \{1, \ldots, k\}$ for which $\zeta_i/\zeta_j \in U$.*

Proof. Let U be the set of roots of unity of order $\le k^2$. This set has cardinality at most $\sum_{i=1}^{k^2} i \le k^4$. Lemma 1 implies that the assertion holds with this set U. ∎

3. Proof of the Theorem. In this section we consider equation (2.1) with arbitrary, non-zero complex coefficients $a_1, \ldots, a_k$. We first prove:

LEMMA 3. *There exists a set U_1, depending on $a_1, \ldots, a_k$ and of cardinality at most $(k!)^6$ such that for every solution $(\zeta_1, \ldots, \zeta_k)$ of (2.1) there are distinct indices $i, j \in \{1, \ldots, k\}$ with $\zeta_i/\zeta_j \in U_1$.*

Proof. Similarly to [4], our approach is to take the determinant of k solutions of (2.1), which is equal to 0, and then to expand this determinant as a sum of $k!$ terms. Thus, let $\mathbf{z}_1 = (\zeta_{11}, \ldots, \zeta_{1k}), \ldots, \mathbf{z}_k = (\zeta_{k1}, \ldots, \zeta_{kk})$ be k solutions of (2.1). Then

$$\begin{vmatrix} \zeta_{11} & \cdots & \zeta_{1k} \\ \vdots & & \vdots \\ \zeta_{k1} & \cdots & \zeta_{kk} \end{vmatrix} = 0$$

and by expanding the determinant, we get

$$\sum_{\sigma} \operatorname{sgn}(\sigma)\zeta_{1,\sigma(1)}\ldots\zeta_{k,\sigma(k)} = 0, \tag{3.1}$$

where the sum is taken over all permutations σ of $(1, \ldots, k)$ and $\operatorname{sgn}(\sigma)$ denotes the sign of σ. Note that the left-hand side of (3.1) is a sum of $k!$ roots of unity. By applying Lemma 2 to this sum, with k replaced by $k!$, we infer that there exists a set U_2 of cardinality at most $(k!)^4$ such that for every k-tuple of solutions $\mathbf{z}_1, \ldots, \mathbf{z}_k$ of (2.1), there are distinct permutations σ, τ of $(1, \ldots, k)$ with

$$\frac{\zeta_{1,\sigma(1)}}{\zeta_{1,\tau(1)}}\cdots\frac{\zeta_{k,\sigma(k)}}{\zeta_{k,\tau(k)}} \in U_2. \tag{3.2}$$

Let $m \le k$ be the smallest integer with the following property: for every m-tuple $\mathbf{z}_1 = (\zeta_{11}, \ldots, \zeta_{1k}), \ldots, \mathbf{z}_m = (\zeta_{m1}, \ldots, \zeta_{mk})$ of solutions of (2.1) there are permutations σ, τ of $(1, \ldots, k)$ with

$$\sigma \ne \tau, \quad \sigma(m+1) = \tau(m+1), \quad \ldots, \quad \sigma(k) = \tau(k) \tag{3.3}$$

such that

$$\frac{\zeta_{1,\sigma(1)}}{\zeta_{1,\tau(1)}}\cdots\frac{\zeta_{m,\sigma(m)}}{\zeta_{m,\tau(m)}} \in U_2 \tag{3.4}$$

(where the condition $\sigma(m+1) = \tau(m+1), \ldots, \sigma(k) = \tau(k)$ is understood to be empty if $m = k$). Then, clearly, $2 \le m \le k$.

First suppose that $m \ge 3$. From the minimality of m it follows that (2.1) has solutions $\mathbf{z}_1, \ldots, \mathbf{z}_{m-1}$ such that for all pairs of permutations σ, τ of $(1, \ldots, k)$ with

$$\sigma \ne \tau, \quad \sigma(m) = \tau(m), \quad \ldots, \quad \sigma(k) = \tau(k) \tag{3.5}$$

we have

$$\frac{\zeta_{1,\sigma(1)}}{\zeta_{1,\tau(1)}}\cdots\frac{\zeta_{m-1,\sigma(m-1)}}{\zeta_{m-1,\tau(m-1)}} \notin U_2. \tag{3.6}$$

We fix such solutions $\mathbf{z}_1, \ldots, \mathbf{z}_{m-1}$ and allow $\mathbf{z}_m$ to vary. Writing $\mathbf{z} = (\zeta_1, \ldots, \zeta_k)$ for $\mathbf{z}_m$, we infer from (3.3)–(3.6) that for every solution $\mathbf{z}$ of (2.1) there are permutations σ, τ of $(1, \ldots, k)$ with

$$\frac{\zeta_{1,\sigma(1)}}{\zeta_{1,\tau(1)}}\cdots\frac{\zeta_{m-1,\sigma(m-1)}}{\zeta_{m-1,\tau(m-1)}}\cdot\frac{\zeta_{\sigma(m)}}{\zeta_{\tau(m)}} \in U_2, \qquad \sigma(m) \ne \tau(m). \tag{3.7}$$

Now suppose that $m = 2$. Fix a solution $\mathbf{z}_1$ of (2.1). Then for any other solution $\mathbf{z}$ of (2.1), there are permutations σ, τ with (3.3) such that

$$\frac{\zeta_{1,\sigma(1)}}{\zeta_{1,\tau(1)}}\cdot\frac{\zeta_{\sigma(2)}}{\zeta_{\tau(2)}} \in U_2.$$

We have $\sigma(2) \neq \tau(2)$, since otherwise $\sigma(i) = \tau(i)$ for $i = 2, \ldots, k$, which contradicts $\sigma \neq \tau$. It follows that also for $m = 2$, and so for each possible value of m, one can find for every solution $\mathbf{z}$ of (2.1) permutations σ, τ with (3.7).

Writing $\sigma(m) = i$, $\tau(m) = j$ in (3.7), we infer that for every solution $\mathbf{z}$ of (2.1) there are distinct indices $i, j \in \{1, \ldots, k\}$ such that $\zeta_i/\zeta_j \in U_1$, where U_1 is the set consisting of all numbers of the form

$$\beta \cdot \frac{\zeta_{1,\tau(1)}}{\zeta_{1,\sigma(1)}} \cdots \frac{\zeta_{m-1,\tau(m-1)}}{\zeta_{m-1,\sigma(m-1)}},$$

with $\beta \in U_2$ and with σ, τ being distinct permutations of $(1, \ldots, k)$. As mentioned before, U_2 has cardinality at most $(k!)^4$. Further, the solutions $\mathbf{z}_1, \ldots, \mathbf{z}_{m-1}$ are fixed and for σ, τ we have $k!$ possibilities each. Therefore, U_1 has cardinality at most $(k!)^6$. This completes the proof of Lemma 3. We mention that the choice of the solutions $\mathbf{z}_1, \ldots, \mathbf{z}_{m-1}$ was ineffective; therefore, the set U_1 is ineffective. ■

Proof of the Theorem. We have to show that up to proportionality, (2.1) has at most k^{3k^2} non-degenerate solutions. We proceed by induction on k.

For $k = 2$, this assertion is trivial. Let $k \geq 3$ and assume that each equation (2.1) in $k-1$ variables with non-zero complex coefficients has up to proportionality at most $(k-1)^{3(k-1)^2}$ non-degenerate solutions. Let U_1 be the set from Lemma 3. Thus, for every solution $(\zeta_1, \ldots, \zeta_k)$ of (2.1) there are $\alpha \in U_1$ and distinct indices $i, j \in \{1, \ldots, k\}$ such that $\zeta_i/\zeta_j = \alpha$. The number of triples (α, i, j) with $\alpha \in U_1$, $i, j \in \{1, \ldots, k\}$ is at most

$$(k!)^6 \cdot k^2 \leq k^{6k-4}. \tag{3.8}$$

We now estimate from above the number of non-degenerate solutions $(\zeta_1, \ldots, \zeta_k)$ of (2.1) with

$$\zeta_i/\zeta_j = \alpha, \tag{3.9}$$

where (α, i, j) is a fixed triple with $\alpha \in U_1$ and $i, j \in \{1, \ldots, k\}$ with $i \neq j$. Assume for convenience that $i = k$, $j = k-1$. Then for every solution of (2.1) with (3.9) we have $a_{k-1}\zeta_{k-1} + a_k\zeta_k = a'_{k-1}\zeta_{k-1}$ with $a'_{k-1} = a_{k-1} + \alpha a_k$ and by substituting this into (2.1), we obtain

$$a_1\zeta_1 + \ldots + a_{k-2}\zeta_{k-2} + a'_{k-1}\zeta_{k-1} = 0. \tag{3.10}$$

We may assume that $a'_{k-1} \neq 0$, for otherwise for every solution of (2.1) with (3.9) we have $a_{k-1}\zeta_{k-1} + a_k\zeta_k = 0$, i.e., (2.1) does not have non-degenerate solutions with (3.9). Further, if $(\zeta_1, \ldots, \zeta_k)$ is a non-degenerate solution of (2.1) with (3.9), then $(\zeta_1, \ldots, \zeta_{k-1})$ is a non-degenerate solution of (3.10). By the induction hypothesis, (3.10) has up to proportionality at most $(k-1)^{3(k-1)^2}$ non-degenerate solutions. Since each such solution determines uniquely a solution of (2.1) with (3.9), it follows that (2.1) has up to proportionality at most $(k-1)^{3(k-1)^2}$ non-degenerate solutions with (3.9). Together with the upper bound (3.8) for the total number of triples (α, i, j), it follows that (2.1) has up to proportionality at most

$$(k-1)^{3(k-1)^2} \cdot k^{6k-4} \le k^{3k^2-6k+3+6k-4} \le k^{3k^2}$$

solutions. This completes the proof of the Theorem. ∎

References

[1] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), Acta Arith. 30 (1976), 229–240.

[2] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.

[3] A. Schinzel, *Reducibility of lacunary polynomials*, *VIII*, Acta Arith. 50 (1988), 91–106.

[4] H. P. Schlickewei, *Equations in roots of unity*, ibid. 76 (1996), 99–108.

[5] U. Zannier, *On the linear independence of roots of unity over finite extensions of* $\boldsymbol{Q}$, ibid. 52 (1989), 171–182.

Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden
The Netherlands
E-mail: evertse@wi.leidenuniv.nl

Received on 3.8.1998
and in revised form on 13.11.1998 (3434)