ACTA ARITHMETICA
XXX (1976)

Trigonometric diophantine equations (On vanishing sums of roots of unity)

by

J. H. Conway (Cambridge) and A. J. Jones (London)

1. Introduction. The equation

$$R(x_1, \ldots, x_l, \operatorname{trig}_1 \pi\theta_1(x_1, \ldots, x_l), \ldots, \operatorname{trig}_n \pi\theta_n(x_1, \ldots, x_l)) = 0$$

s called a *trigonometric diophantine equation* if

(i) $R, \theta_1, \ldots, \theta_l$ are rational functions of their arguments, with rational number coefficients.

(ii) $\operatorname{trig}_1, \ldots, \operatorname{trig}_n$ are functions chosen from the set {sin, cos, tan, cot, sec, cosec}.

(iii) It is to be solved in integers for some of the x_i, and rational numbers for the others.

The equation is called an *ordinary diophantine equation* if $n = 0$. In this paper we shall give an effective procedure which given any trigonometric diophantine equation in variables $x_1, \ldots, x_l$ produces an 'equivalent' ordinary diophantine equation in variables $x_1, \ldots, x_m$ $(m > l)$. To be precise, $r_1, \ldots, r_l$ is a solution of the first equation if and only if there are numbers $r_{l+1}, \ldots, r_m$ such that $r_1, \ldots, r_m$ is a solution of the second. If we neglect the new variables (and they usually enter only in a rather trivial way) then we can say that our process produces an ordinary diophantine equation which has the same solutions as any given trigonometric diophantine equation. Thus no problems arise in solving equations such as

$$x\cos\pi\left(\frac{y}{x^2+2}\right) + (y^2+3x)\tan\pi\left(\frac{3xy}{5y^2-7x}\right) = 1$$

which do not already arise in the solution of ordinary diophantine equations. Of course it follows from the work of Matijasevič [8] that this reduction is not necessarily helpful since arbitrarily hard problems can still arise! Nevertheless we show in the second part of this paper that a detailed consideration of vanishing sums of roots of unity yields a method which is quite practicable in simple cases.

We are grateful to the referee for drawing our attention to several obscurities and for providing the reference to the important paper of Rédei [9].

2. Preliminary reductions. Our problem as stated has a certain artificiality, and is not very well defined, since we have neglected the problems concerned with infinite arguments or values of the trigonometric functions. We proceed at once to strip it of its spurious generality. It is plain that we can suppose all the trigonometric functions to be cosines, since for example we can replace $\tan\pi\theta$ by $\cos\pi(\frac{1}{2}-\theta)/\cos\pi\theta$, and it is reasonable to interpret 'zero of R' as 'zero of the numerator of R', so that we can suppose R to be a polynomial. (Other, perhaps more reasonable, interpretations of this phrase can be accomodated almost as readily — we choose this one to simplify the exposition). If we now replace $2\cos 2\pi\theta$ by $e(\theta)+e(-\theta)$, where $e(x)$ denotes $e^{2\pi i x}$, and use the identity $e(x)\,e(y) = e(x+y)$ we get an equation of the form

$$X_1 e(\Theta_1)+\ldots+X_N e(\Theta_N) = 0 \tag{1}$$

in which X_i, Θ_i are given rational functions of $x_1, \ldots, x_l$ and N is fixed. But we shall prove in Theorem 3 that the solutions in rationals of the equation

$$x_1 e(\theta_1)+\ldots+x_N e(\theta_N) = 0 \tag{2}$$

in which $x_1, \ldots, x_N, \theta_1, \ldots, \theta_N$ are *variables*, fall into a finite number of parametric families of the form

$$x_i = L_i(p_1, \ldots, p_k),$$
$$\theta_i = M_i(p_1, \ldots, p_k)$$

in which the L_i and M_i are linear functions and some of the parameters p_j range through the integers, the others through the rationals.

For each such parametric solution of (2) we consider the equation in variables $x_1, \ldots, x_l, p_1, \ldots, p_k$

$$\sum_{i=1}^{N}\{(X_i-L_i(p_1, \ldots, p_k))^2+(\Theta_i-M_i(p_1, \ldots, p_k))^2\} = 0. \tag{3}$$

Then it is obvious that the solutions of this equation restrict, when we ignore the variables p_j, to solutions of (1), and that we obtain all the solutions of (1) by considering a finite number of equations (3), one for each parametric family, say the equations $\Gamma_1 = 0, \ldots, \Gamma_K = 0$. In other words, the solutions of (1) are precisely those values of $x_1, \ldots, x_l$ which are obtained from solutions of the equation

$$\Gamma_1\Gamma_2\ldots\Gamma_K = 0.$$

The reader now appreciates just how artificial our problem was. However several trigonometric diophantine equations have been used in the literature, for example Coxeter [1], and provided with *ad hoc* solutions, Gordan [5] and Crosby [2] (these applications are briefly discussed in our concluding section), so it is quite valuable to realise that (2) is essentially the *only* such equation, and that for any given value of N it can be solved completely in a quite effective way. We shall illustrate these remarks later by finding all rational linear combinations of four cosines of rational angles (i.e. rational multiples of π).

3. The ring of formal sums of roots of unity. A number of the form $e(\theta)$ with rational θ is a complex number of finite multiplicative order, or in other words a root of unity. From now on we shall call a complex number satisfying $x^n = 1$ an *n-th root*, or just a *root* when n is immaterial. We call it a *primitive* nth root if n is its exact order. The least common order of a set of roots is the least n for which they all satisfy $x^n = 1$. Our problem has been reduced to that of finding all linear dependences among roots of unity, and it seems natural to attack it with the following terminology.

Take an infinite dimensional vector space over the rationals, with one basis vector $\boldsymbol{\alpha}$ for each root α, and convert it into a ring by writing $\boldsymbol{\alpha\beta} = \boldsymbol{\gamma}$ whenever $\alpha\beta = \gamma$. The elements of this ring we call *formal sums of roots of unity*, or just *formal sums*. The formal sum S *involves* the root α when the expression for S in terms of the above basis has non-zero coefficient of $\boldsymbol{\alpha}$. The *length* $l(S)$ of S is the number of roots involved in S, and its *exponent* $e(S)$ is their least common order. The sum S is called *similar* to $k\cdot\boldsymbol{\alpha}S$ for any root α and any non-zero rational number k, and the *reduced exponent* $r(S)$ of S is the least exponent of any sum similar to S. If S involves 1 we call it *monic*; its exponent then coincides with its reduced exponent. The *value* $v(S)$ of $S = \sum c_\alpha \boldsymbol{\alpha}$ is of course the complex number $\sum c_\alpha \alpha$, and we call S a *vanishing sum* when $v(S) = 0$.

We call roots α, β *equivalent* if α/β has squarefree order, noting that equivalence *is* an equivalent relation. If $n = ab$, where a and b are coprime, then any nth root ω factorises as a product of ath and bth roots α and β in a unique way. We write $\alpha = \omega[a]$, $\beta = \omega[b]$. Finally we call a vanishing sum *minimal* if no proper subsum vanishes.

THEOREM 1. *Any vanishing sum also vanishes when restricted to any equivalence class* (*i.e. the partial sum of just those terms of S from the given equivalence class vanishes*).

Proof. The roots involved in S are all powers of a single root ω, say, of order $n = e(S)$. Let a be the greatest squarefree divisor of n, and let $n = ab$, $\Omega = \omega^a$. Then $a+1$ and n are coprime, and so there is an automorphism of the field $Q(\omega)$ replacing ω by $\omega^{a+1} = \omega\Omega$. It is easy to see that this automorphism multiplies two powers of ω by the same power of Ω if and only if they are equivalent, and so S transforms to the new vanishing sum

$$S_0+\Omega S_1+\Omega^2 S_2+\ldots+\Omega^{b-1}S_{b-1},$$

where the S_i are the sums obtained by restricting S to equivalence classes.

Repeatedly applying this automorphism we obtain a number of such sums which on adding and using $1+\Omega+\ldots+\Omega^{b-1}=0$ yield bS_0, and so S_0 (and similarly the other S_i), must vanish.

In view of Theorem 1 we now restrict our attention to sums involving only roots of squarefree order. Our next theorem gives an exact criterion for such a sum to vanish.

THEOREM 2. *Consider $S=\sum c_\alpha \alpha$, where α ranges over all n-th roots and n is squarefree, then S vanishes if and only if we have*

(4) $$\sum_{d|n}\mu(d)c_{\omega[d]}=0$$

for every primitive n-th root ω, μ being the Möbius function.

Remark. This theorem appears in Rédei ([9], Satz 3).

Proof. Let α be an imprimitive nth root, so that the order of α is not divisible by some prime factor p of n, and let Ω be a primitive pth root. Then the equation

$$\alpha+\alpha\Omega+\alpha\Omega^2+\ldots+\alpha\Omega^{p-1}=0$$

enables us to express α as a linear combination of nth roots whose orders are strictly larger than that of α, and repeating the process, if necessary, we ultimately express α as a linear combination of primitive nth roots.

But the above equation, considered as an equation of the type $\sum c_\omega \omega=0$ (with many zero coefficients) satisfies the criterion (4), because if $\alpha=\omega[e]$ for some primitive root ω, then $\omega[pe]$ has the form $\alpha\Omega^i$ and only for $d=e$ or pe is $c_{\omega[d]}\neq 0$.

It therefore follows that our criterion for the vanishing of S holds in general if and only if it holds for sums S with $c_\alpha=0$ for all imprimitive α. But for such S the criterion merely demands that $c_\alpha=0$ for all the remaining α, so that our theorem holds if and only if the primitive nth roots are linearly independent over the rationals. However we have just shown that the $\varphi(n)$ primitive nth roots span the field they generate, and since this field has degree $\varphi(n)$ they must form a basis for it as a vector space over the rationals, and the result follows.

We could also have completed the proof along the same lines as our proof of Theorem 1, using the following lemma.

LEMMA 1. *If $S_0+\omega S_1+\ldots+\omega^{p-1}S_{p-1}$ is a vanishing sum, ω being a primitive p-th root, and the S_i having exponents prime to p, then the S_i all have the same value.*

Proof. Let K be the smallest extension of the rationals containing all the roots of unity involved. Then there is an automorphism of K fixing each root whose order is coprime to p but replacing ω by any other primitive pth root. Applying these automorphisms to S and adding the resulting equations we obtain

$$v\big((p-1)S_0-S_1-\ldots-S_{p-1}\big)=0,$$

so that S_0 has value

$$\frac{1}{p}v(S_0+S_1+\ldots+S_{p-1})$$

and similarly we see that the other S_i also have this value.

THEOREM 3. *Let r be the product of all primes $p\leqslant N$. Then to each pair of functions*

$$f\colon\{1,2,\ldots,N\}\to\{1,2,\ldots,N\},\qquad g\colon\{1,2,\ldots,N\}\to\{0,1,\ldots,r-1\}$$

there is a parametric solution of

(5) $$x_1e(\theta_1)+\ldots+x_Ne(\theta_N)=0$$

of the form

(6) $$\theta_i=p_i+q_{f(i)}+g(i)/r,$$

(7) $$x_i=L_i(r_1,\ldots,r_N),$$

where the $p_1,\ldots,p_N$ are arbitrary integer parameters, $q_1,\ldots,q_N$, $r_1,\ldots,r_N$ are arbitrary rational parameters, and the linear functions $L_1,\ldots,L_N$ depend only on the pair f, g. Every solution of (5) *is a case of one of these parametric solutions.*

Proof. Given any solution of (5), we first produce from it the parameters which satisfy (6).

After Theorem 1, the sum of the terms of (5) in each equivalence class vanishes, so by Lemma 1, any prime dividing the reduced exponent of one of these sums is at most N. Thus two $e(\theta_i)$ in (5) belong to the same equivalence class if and only if the corresponding θ_i differ by an integral multiple of $1/r$. Hence there exist rational numbers $s_1,\ldots,s_N$, with s_i depending only on the equivalence class of $e(\theta_i)$ in (5) such that θ_i-s_i is an integral multiple of $1/r$, say

$$\theta_i-s_i=p_i+g(i)/r,$$

where p_i is integral and $g(i)\in\{0,1,\dots,r-1\}$. If we number the equivalence classes by numbers from $1,2,\dots,N$ (at most), and let $f(i)$ be the number of the class containing $e(\theta_i)$, then we can write $s_i = q_{f(i)}$, obtaining (6).

Now for each pair f, g we must find the conditions the x_i must satisfy to give a solution of (5). For each rth root ω, define $e_\omega(k)$ as the sum of all the x_i for which $f(i)=k$ and $e\big(g(i)/r\big)=\omega$. Then Theorem 2 shows that the required conditions are simply that

$$\sum_{d|r}\mu(d)\,e_{\omega[d]}(k) = 0$$

for each primitive rth root ω and each $k\in\{1,\dots,N\}$. Since these are linear conditions on the x_i we can express their general solution in the form (7), thereby proving the theorem.

This also completes the proof of our assertion that trigonometric diophantine equations reduce to ordinary ones. To make this into a practicable method for solving trigonometric equations we must erect a theory of vanishing sums.

4. Vanishing sums. In Theorem 6 we shall in fact find all vanishing sums of length $\leqslant 9$. These might suggest that any vanishing sum can be obtained from a shorter one by adding a sum similar to $\mathbf{1}+\omega+\dots+\omega^{p-1}$ for some pth root ω. That this is not generally the case is shown by the vanishing sum

$$S = \left|\begin{array}{ccc} \mathbf{1} & \alpha & \alpha^2 \\ \mathbf{1} & \beta+\beta^2 & \beta^3+\beta^4 \\ \mathbf{1}+\gamma & \gamma^2+\gamma^3 & \gamma^4+\gamma^5+\gamma^6 \end{array}\right|$$

in which α, β, γ are roots of order 3, 5, 7 respectively. Here we have $l(S) = 23$, but it can be shown that whenever $S = S'+S''$ with S' similar to $\mathbf{1}+\omega+\dots+\omega^{p-1}$ then $l(S'')>23$. However the following theorem gives a valid way of obtaining vanishing sums from shorter ones.

THEOREM 4. *Let S be a vanishing sum. Then either S is similar to $\mathbf{1}+\omega+\dots+\omega^{r-1}$ for some prime r and primitive r-th root ω, or $S = S'+S''$, where S', S'' are vanishing sums satisfying*

$$l(S')\leqslant l(S),\quad r(S')<r(S),\quad l(S'')<l(S),\quad r(S'')\leqslant r(S).$$

Proof. We suppose S monic, so that $r(S)=e(S)=r$, say, and after Theorem 1 we can suppose r squarefree. If r is prime Lemma 1 proves that S is similar to $\mathbf{1}+\omega+\dots+\omega^{p-1}$, ω a primitive rth root, so that we suppose r composite. If now every rth root is involved in S, we can take S' as $a\mathbf{1}+a\omega+\dots+a\omega^{p-1}$ and S'' as $S-S'$, where ω is a primitive pth root for some $p|r$, and a is the coefficient of $\mathbf{1}$ in S. Then

$$l(S') = r(S') = p < r = r(S) = l(S)$$

while plainly $r(S'')\leqslant r$, and $l(S'')<r$ since S'' does not involve 1.

If, on the other hand, some rth root is not involved, we have $l(S)<r$, so that some prime p divides r but not $l(S)$. If we write S in the form

$$\mathbf{1}S_0+\omega S_1+\dots+\omega^{p-1}S_{p-1},$$

in which the exponent of each S_i divides r/p and ω is a primitive pth root, then Lemma 1 shows that the value of the S_i are all equal. But since $p\nmid l(S)$ their lengths cannot all be equal. We let S_i have the minimal length, and suppose $l(S_i)<l(S_j)$. Then we can take S' as $(S_j-S_i)\omega^j$, when S'' will be the sum obtained from S by replacing S_j by S_i. We then have

$$l(S')\leqslant l(S_i)+l(S_j)\leqslant l(S)$$

(with strict inequality unless $p=2$), and also

$$r(S')\leqslant r/p<r=r(S),$$

while plainly $r(S'')\leqslant r(S)$, and

$$l(S'') = l(S)-l(S_j)+l(S_i)<l(S).$$

A more detailed argument yields the following relation between $l(S)$ and $r(S)$. Recall that a vanishing sum is *minimal* if no proper subsum vanishes. We have

THEOREM 5. *If a minimal vanishing sum has length l and reduced exponent r, then*

$$l\geqslant \sum_{p|r}(p-2)+2 = f(r),\ \textit{say}.$$

This is an immediate corollary of the following lemma.

LEMMA 2. *Let S be a vanishing sum of the form $\sum S_\alpha\alpha$, where α ranges over all the r-th roots, and the S_α are sums with exponents coprime to r. Then either there is a divisor d of r with $d>1$ such that for each d-th root ω the sum vanishes when restricted to the α with $\alpha[d]=\omega$ (when we call it d-splitting) or the number of non-vanishing S_α is at least $f(r)$.*

Remark. For $d=1$ d-splitting means that the sum S is a vanishing sum, and r-splitting means that each term of the sum is zero.

Proof. We suppose S is not d-splitting for any $d<r$. It does not affect the lemma to suppose also that any two S_α which have the same value are identical. For any divisor d of r we can express S in the form

$$S_0+\omega S_1+\dots+\omega^{d^*-1}S_{d^*-1}$$

where $dd^* = r$, each S_i has exponent coprime to d^*, and ω is a primitive d^*th root. The number of non-vanishing sums S_i is, by induction, at least $f(d^*)$, and the lemma will be proved if we show that for some d there are terms S_i and S_j $(i \neq j)$ which together contain at least $f(d)$ non-vanishing terms of S, for then the total number of non-vanishing terms in S will be at least $f(d^*)-2+f(d) = f(r)$. It will suffice to prove that for some d there are terms S_i and S_j for which $S_i - S_j$ is not D-splitting for any proper divisor D of d, for then the sum $S_i - S_j$ has at least $f(d)$ terms by induction.

Now there exist values of d for which two of the sums S_i have the same value but are not equal, since it is easy to see that if the S_i are all equal for $d = r/p$, p prime, then S is d-splitting. Consider then the smallest such d, noting that $d > 1$, and let S_i, S_j be unequal terms with the same value. If $S_i - S_j$ is D-splitting for some $D|d$, $D < d$, $DD^* = d$, then expressing S_i and S_j in the forms

$$S_i = S_i^0 + S_i^1\Omega + \ldots + S_i^{D-1}\Omega^{D-1},$$
$$S_j = S_j^0 + S_j^1\Omega + \ldots + S_j^{D-1}\Omega^{D-1},$$

wherein the S_i^k and S_j^k have exponents coprime to D and Ω is a primitive Dth root, we see that $v(S_i^k - S_j^k) = 0$ for each k, but since S_i and S_j are unequal there must be some k for which S_i^k and S_j^k are unequal, and this therefore contradicts the minimality of d. Thus $S_i - S_j$ is not D-splitting for any $D|d$, whence by induction it has at least $f(d)$ terms as required.

Since a minimal sum obviously cannot be d-splitting the theorem follows. The result is best possible, as can be seen by considering a vanishing sum of the form

$$S_1 + S_2 + \ldots + S_k$$

where

$$S_i = \varepsilon_i(\mathbf{1} + \omega_i + \ldots + \omega_i^{p_i-1}),$$

where ω_i is a primitive p_ith root, ε_1 is an arbitrary root and ε_{i+1} is chosen so that one of the terms of S_{i+1} is the negative of some term in $S_1 + \ldots + S_i$. It is an interesting exercise to show (by considering when equality holds in the proof of the theorem) that this is in fact the most general example for which the bound is exactly attained.

Our Theorem 5 improves a similar result of Mann ([7], Theorem 1). We can also readily deduce the following

Corollary. *A minimal vanishing sum of length l and reduced exponent r has*

$$r = O\{\exp\big(C(l\log l)^{1/2}\big)\}$$

for every $C > 1$.

The proof is routine and we suppress it, but the corollary is worth mentioning because it is an improvement, essentially best possible, of a result of Schinzel ([10], Theorem 1, Cor. 3). (A similar corollary could be deduced from Mann's theorem.)

Professor Schinzel remarked, upon seeing an earlier draft of this paper, that an immediate consequence is that, for squarefree n, the number of non-vanishing coefficients in the nth cyclotomic polynomial is $\geqslant (\log n)^2/\log\log n$. An interesting problem in its own right would be to substantially improve this estimate.

5. Vanishing sums of small length. According to our previous definitions formal sums such as $\mathbf{1}+\boldsymbol{a}+\boldsymbol{a}^2$ and $\mathbf{1}-(-\boldsymbol{a})+\boldsymbol{a}^2$ are unequal, but from now on we intend to regard them as identical. This is equivalent to replacing our original ring of formal sums of roots of unity by a new one obtained by adding relations $-(-\boldsymbol{\omega}) = \boldsymbol{\omega}$ for all roots ω.

Theorem 6. *Let S be a non-empty*(1) *vanishing sum of length at most* 9. *Then either S involves θ, $\alpha\theta$, $\alpha^2\theta$ for some root θ, or S is similar to one of*

$$\mathbf{1}+\boldsymbol{\beta}+\boldsymbol{\beta}^2+\boldsymbol{\beta}^3+\boldsymbol{\beta}^4, \qquad -\boldsymbol{\alpha}-\boldsymbol{\alpha}^2+\boldsymbol{\beta}+\boldsymbol{\beta}^2+\boldsymbol{\beta}^3+\boldsymbol{\beta}^4,$$
$$\mathbf{1}+\boldsymbol{\gamma}+\boldsymbol{\gamma}^2+\boldsymbol{\gamma}^3+\boldsymbol{\gamma}^4+\boldsymbol{\gamma}^5+\boldsymbol{\gamma}^6, \qquad \mathbf{1}+\boldsymbol{\beta}+\boldsymbol{\beta}^4-(\boldsymbol{\alpha}+\boldsymbol{\alpha}^2)(\boldsymbol{\beta}^2+\boldsymbol{\beta}^3),$$
$$-\boldsymbol{\alpha}-\boldsymbol{\alpha}^2+\boldsymbol{\gamma}+\boldsymbol{\gamma}^2+\boldsymbol{\gamma}^3+\boldsymbol{\gamma}^4+\boldsymbol{\gamma}^5+\boldsymbol{\gamma}^6, \qquad \boldsymbol{\beta}+\boldsymbol{\beta}^4-(\boldsymbol{\alpha}+\boldsymbol{\alpha}^2)(\mathbf{1}+\boldsymbol{\beta}^2+\boldsymbol{\beta}^3),$$
$$\mathbf{1}+\boldsymbol{\gamma}^2+\boldsymbol{\gamma}^3+\boldsymbol{\gamma}^4+\boldsymbol{\gamma}^5-(\boldsymbol{\alpha}+\boldsymbol{\alpha}^2)(\boldsymbol{\gamma}+\boldsymbol{\gamma}^6), \qquad \mathbf{1}-(\boldsymbol{\alpha}+\boldsymbol{\alpha}^2)(\boldsymbol{\beta}+\boldsymbol{\beta}^2+\boldsymbol{\beta}^3+\boldsymbol{\beta}^4),$$

where α, β, γ are primitive roots of orders 3, 5, 7 *respectively.*

Proof. Suppose that S is minimal. In this case we can further suppose its exponent is squarefree and, using the remark before the theorem, also odd. Let p be the largest prime divisor of $e(S)$ so that by Theorem 5 $p \leqslant 7$. Express S as

$$S_0 + \omega S_1 + \ldots + \omega^{p-1}S_{p-1},$$

where ω is a primitive pth root and the S_i have exponents prime to p. If $p = 3$, then S can involve only 1, α, α^2, and so must be $\mathbf{1}+\boldsymbol{a}+\boldsymbol{a}^2$. If $p \geqslant 5$ however, some S_i has at most one term (otherwise $l(S) \geqslant 2p \geqslant 10$). Since the S_i have the same value, by Lemma 1, no S_i has value zero, and we can suppose without loss of generality that $S_0 = \mathbf{1}$. All the S_i have therefore the value 1.

Now if some $S_i \neq \mathbf{1}$, $\mathbf{1} - S_i$ is a vanishing sum of exponent prime to p, and this exponent must be 3, for otherwise we should obtain $35|e(S)$, contradicting Theorem 5. It follows that $\mathbf{1} - S_i = k\delta(\mathbf{1}+\boldsymbol{a}+\boldsymbol{a}^2)$ for some rational k and root δ. Now if $k\delta \neq 1$, S involves $\delta\omega^i$, $a\delta\omega^i$, $a^2\delta\omega^i$, and if $k\delta = 1$ then $S_i = -\boldsymbol{a}-\boldsymbol{a}^2$. But any case in which S_i is either $\mathbf{1}$ or

(1) Under the new rules sums such as $\mathbf{1}+\boldsymbol{i}^2 = \mathbf{1}-\mathbf{1} = 0$ are the empty sum.

$-\alpha-\alpha^2$ and $l(S) \leqslant 9$ is readily seen to be similar to one from the displayed list.

Finally, if S is not minimal, any minimal subsum of S has already been shown to satisfy the theorem. However one such subsum has at most 4 terms, hence it, and *a fortiori* S itself, must involve, θ, $\alpha\theta$, $\alpha^2\theta$ for some root θ.

6. Rational sums of cosines of rational angles. We can now use Theorem 6 to find the complete solution of the equation

$$A\cos 2\pi a + B\cos 2\pi b + C\cos 2\pi c + D\cos 2\pi d = E \tag{8}$$

in which all the variables are rational.

THEOREM 7. *Suppose we have at most four distinct rational multiples of π lying strictly between 0 and $\pi/2$ for which some rational linear combination of their cosines is rational but no proper subset has this property. Then the appropriate linear combination is proportional to one from the following list:*

$$\cos\pi/3 = \tfrac{1}{2},$$
$$-\cos\varphi + \cos(\pi/3-\varphi) + \cos(\pi/3+\varphi) = 0 \quad (0 < \varphi < \pi/6),$$
$$\cos\pi/5 - \cos 2\pi/5 = \tfrac{1}{2},$$
$$\cos\pi/7 - \cos 2\pi/7 + \cos 3\pi/7 = \tfrac{1}{2},$$
$$\cos\pi/5 - \cos\pi/15 + \cos 4\pi/15 = \tfrac{1}{2},$$
$$-\cos 2\pi/5 + \cos 2\pi/15 - \cos 7\pi/15 = \tfrac{1}{2},$$
$$\cos\pi/7 + \cos 3\pi/7 - \cos\pi/21 + \cos 8\pi/21 = \tfrac{1}{2},$$
$$\cos\pi/7 - \cos 2\pi/7 + \cos 2\pi/21 - \cos 5\pi/21 = \tfrac{1}{2},$$
$$-\cos 2\pi/7 + \cos 3\pi/7 + \cos 4\pi/21 + \cos 10\pi/21 = \tfrac{1}{2},$$
$$-\cos\pi/15 + \cos 2\pi/15 + \cos 4\pi/15 - \cos 7\pi/15 = \tfrac{1}{2}.$$

This generalizes the result of Włodarski [11].

Proof. On replacing $2\cos 2\pi x$ by $e(x)+e(-x)$ we obtain a non-empty vanishing sum S of roots of unity with at most 9 terms. Conversely from such a vanishing sum in which each root appears with the same coefficient as its complex conjugate we obtain a rational linear combination of at most four cosines in which we can normalize the angles to the range $[0, \pi/2)$.

We now apply Theorem 6. If θ, $\alpha\theta$, $\alpha^2\theta$ are all involved we have two cases. Firstly if $e^{i\pi x}$ and $e^{-i\pi x}$ are two of the corresponding three terms, or if one of them is the constant term, we obtain a equation which normalizes to $\cos\pi/3 = \frac{1}{2}$. In the second case θ, $\alpha\theta$, $\alpha^2\theta$ correspond to terms from three distinct cosines for which the normalized angles satisfy the second equation on our list.

Otherwise the sum is similar to one of those displayed in Theorem 6 and, since each root appears as often as its complex conjugate, we may suppose it is exactly one of these listed. Taking all possibilities for the primitive roots involved, and normalizing the resulting angles, we obtain the results quoted, together with a few cases in which partial sums are linearly dependent on some of the above list.

7. Conclusion. Particular trigonometric diophantine equations arise in many geometric situations. Gordan's equation

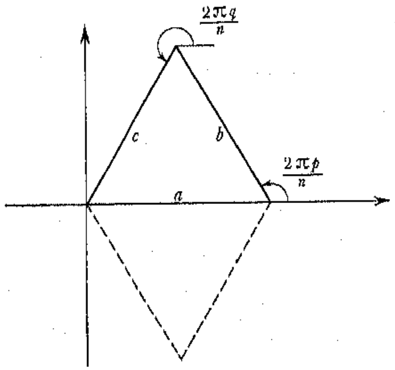
$$\cos 2\pi a + \cos 2\pi b + \cos 2\pi c = -1 \qquad (0 \leqslant a, b, c \leqslant \tfrac{1}{2})$$

arises in the enumeration of finite linear groups [5] and in the related problem of enumerating the regular star polyhedra ([1], § 6.7). Crosby's equation [2]

$$\cos 2\pi a + \cos 2\pi b + \cos 2\pi c = 0 \qquad (0 \leqslant a, b, c \leqslant \tfrac{1}{2})$$

can be used in the corresponding enumeration of 4-dimensional regular star polytopes ([1], § 14.5).

Both these equations are covered by Theorem 7, and make assertions about the dihedral angles of certain classes of tetrahedra. It seems quite probable that the general tetrahedron all of whose dihedral angles are rational can be found by our techniques. A rather harder problem is to enumerate all rectifiable tetrahedra, that is tetrahedra which can be dissected into polyhedral pieces which can be reassembled to form a cube. Many such tetrahedra are known (Goldberg [4]), and our main theorem, together with Dehn's solution [3] to Hilbert's third problem, shows that their complete enumeration reduces in principle to an ordinary diophantine equation.



Mann [7] uses vanishing sums to find polygons with rational sides and angles that are rational multiples of π. Using the geometry of the complex plane we see that Theorem 7 enables us to find all such polygons with at most 9 sides. Another geometrical problem in which roots of unity are involved is treated by Kárteszi [6].

Such geometrical problems can often be solved by applying our methods *in situ*, without translating into algebraic form. We give as an example a simple proof that a triangle whose edges are all rational and whose angles are all rational multiples of π is necessarily equilateral.

Placing the triangle in the complex plane as shown in the Figure on page 239, we obtain the equation

$$a+b\omega^p+c\omega^q = 0,$$

where ω is a primitive nth root of unity and p and q are chosen so that n is minimal. If k is coprime to n, ω^k is also a primitive root of unity, and we obtain

$$a+b\omega^{kp}+c\omega^{kq} = 0,$$

which corresponds to another triangle with the same edge lengths a, b, c, the edge of length a being shared. The only other possible position is the reflected one shown, corresponding to $k = -1$, so we must have $(k, n) = 1$ implies $k \equiv \pm 1 \pmod n$. But this implies $n = 1, 2, 3, 4, 6$ so that either all angles are multiples of right angles or all angles are multiples of $\pi/3$. Thus the only possibility for a proper triangle is equilateral.

References

[1] H. S. M. Coxeter, *Regular polytopes*, Methuen 1948.

[2] W. J. R. Crosby, *Solution to problem* 4136, Amer. Math. Monthly 53 (1946), pp. 103–107.

[3] M. Dehn, *Über den Rauminhalt*, Math. Ann. 55 (1902), pp. 465–478; Gottingen Nachr. Math. Phys. 1900, pp. 345–354.

[4] M. Goldberg, *Two more tetrahedra equivalent to cubes by dissection*, Elemente der Math. 24 (1969), pp. 130–132; 25 (1970), p. 48.

[5] P. Gordan, *Ueber endliche Gruppen linearer Transformationen einer Veränderlichen*, Math. Ann. 12 (1877), pp. 23–46.

[6] F. Kárteszi, *Intorno a punti allineati di certi reticoli circolari*, Rend. Sem. Matem. Messina 11 (1964–65), pp. 1–12.

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

[8] Ju. V. Matijasevič, *The Diophantineness of enumerable sets* (Russian), Dokl. Akad. Nauk SSSR 191 (1970), pp. 279–282; in English: Sov. Math. Dokl. 11 (1970), pp. 354–358.

[9] L. Rédei, *Natürliche Basen des Kreisteilungskörpers*, Teil I, Abh. Math. Sem. Hamburg 23 (1959), pp. 180–200.

[10] A. Schinzel, *On sums of roots of unity*, Acta Arith. 11 (1966), pp. 419–432.

[11] L. Włodarski, *On the equation* $\cos a_1+\cos a_2+\cos a_3+\cos a_4 = 0$, Ann. Univ. Budapestiniensis 12 (1969), pp. 147–155.

D. P. M. M. S.
Cambridge, England
ROYAL HOLLOWAY COLLEGE
Egham, Surrey, England

Received on 22. 8. 1974
and in revised form on 4. 3. 1975 (612)

ACTA ARITHMETICA
XXX (1976)

A stopping time problem on the positive integers

by

RIHO TERRAS (Del Mar, Calif.)

Define a function X on the natural numbers $\boldsymbol{N} = \{0, 1, 2, \ldots\}$ by setting $X(n) = 1$ when n is odd and $X(n) = 0$ when n is even. Now define a function T mapping $\boldsymbol{N}$ into itself by setting

$$Tn = \big(3^{X(n)}n+X(n)\big)/2.$$

Note that if n is odd then $Tn = (3n+1)/2$ else $Tn = n/2$. Given an $n \in \boldsymbol{N}$ the number Tn is to be regarded as a successor to n. We shall be interested in analyzing the successor function T when it is applied iteratively to n.

Before describing the principal result it will be convenient to introduce some additional notation. Set T^0 to be the identity function on $\boldsymbol{N}$. If T^k has been defined then define T^{k+1} by setting $T^{k+1}n = T(T^kn)$.

DEFINITION 0.1. Set $\chi(n) = k$ if k is the smallest positive integer such that $T^kn < n$. If no such integer exists set $\chi(n) = \infty$. The number $\chi(n)$ will be called the *stopping time* of n.

Observe that $\chi(0) = \chi(1) = \infty$. The conjecture concerning χ is that $\chi(n)$ is finite for all $n \geqslant 2$. It is easy to see that this conjecture is true if and only if for every integer $n \geqslant 2$ there exists a positive integer k such that $T^kn = 1$. In this guise the problem has fascinated computer scientists [3] and has also circulated in popular mathematics circles [1]. In mathematical circles this problem is frequently referred to as the Collatz–Kakutani problem.

The principal result of this paper touching on this problem is the demonstration that χ possesses a well defined distribution function

$$F(k) = \lim_{m\to\infty}(1/m)\mu\{n \leqslant m \mid \chi(n) \geqslant k\} \tag{0}$$

where μ denotes the counting function. The distribution F will be derived theoretically and it shall be demonstrated that $\lim_{k\to\infty} F(k) = 0$.

Perhaps the most useful technique to evolve from the machinery developed is an extremely simple technique for computing actual values