J. Austral. Math. Soc. (Series A) 35 (1983), 405–420

THE SIMULTANEOUS REPRESENTATION OF INTEGERS BY PRODUCTS OF CERTAIN RATIONAL FUNCTIONS

P. D. T. A. ELLIOTT

(Received 21 October 1982)

Communicated by J. H. Loxton

Abstract

It is proved that an arbitrary pair of positive integers can be simultaneously represented by products of the values at integer points of certain rational functions. Linear recurrences in $\mathbb{Z}$-modules and elliptic power sums are applied.

1980 *Mathematics subject classification (Amer. Math. Soc.)*: 10 H 25, 10 K 20, 10 L 10, 10 M 05.

Let

$$P(x) = \prod_{i=0}^{h} (x + a_i)^{b_i}$$

be a rational function with non-negative integers $a_0 < a_1 < \cdots < a_h$, and integral exponents b_i which may be positive or negative but whose highest common factor is 1.

THEOREM. *Let m_1, m_2 and t be positive integers. Then there is a (simultaneous) representation*

$$m_1 = \prod_{j=1}^{r} P(n_j)^{\varepsilon_j}, \qquad m_2 = \prod_{j=1}^{r} P(n_j + t)^{\varepsilon_j},$$

with positive integers n_j and each $\varepsilon_j = \pm 1$.

The method of proof shows that there are in fact infinitely many such representations. A bound for the n_j in terms of m_1, m_2 and t could be found at the expense of complication of detail.

The existence of a one-dimensional representation involving only m_1 was established algebraically in the author's paper Elliott (1983). The present proof applies new ideas. In particular, studies are made of linear recurrences defined over **Z**-modules; and of the asymptotic behaviour of elliptic power-sums.

Let Q_1 be the abelian group of positive rational fractions with multiplication as the rule of combination, and let Q_2 be the direct sum of two copies of Q_1.

Let Γ be the subgroup of Q_2 generated by the (direct) summands $P(n) \oplus P(n+t)$, $n = 1, 2, \ldots$.

I shall establish the theorem by proving, in three steps, that the quotient group $G = Q_2/\Gamma$ is trivial.

Step one: G is finitely generated

Let H be a **Z**-module, with the operation of **Z** on H written on the left. We shall study the solution-sequences $(\alpha_1, \alpha_2, \ldots)$ in H^ω of the recurrence

$$\sum_{j=0}^{k} c_j \alpha_{n+j} = 0, \tag{1}$$

where the c_j are integers with highest common factor 1.

Without loss of generality $c = c_k \neq 0$ and $k \geqslant 2$ will be assumed.

Lemma 1. *Let M be an integer so that $M\alpha_n = 0$ for $n = 1, \ldots, k$. Then*

$$Mc^n \alpha_n = 0$$

for all $n \geqslant 1$.

Proof. By induction on n. In fact

$$Mc\alpha_{k+1} = -\sum_{j=0}^{k-1} c_j M\alpha_{j+1} = 0,$$

and so on, to give $Mc^{n-k}\alpha_n = 0$ for $n \geqslant k+1$, from which the desired result follows.

Under the conditions of this lemma, each element $-\alpha_n$ which appears in a solution sequence of (1) has finite order. From now on we shall assume that every element of the module H has finite order.

Let p be a (positive) rational prime.

For each positive integer n let $|n|_p = p^{-r}$, where p^r is the exact power of the prime p which appears in the canonical factorisation of n in the rational integers.

With this definition one begins the derivation of the well-known p-adic metric on the rational numbers. We shall do our best to construct a valuation on the $\mathbf{Z}$-module H.

If α is a non-zero element of H which has order m, and if p^s is the exact power of p which divides m, $s = 0$ being permissible, we define $v(\alpha) = p^s$.

We set $v(0) = 1$.

The appropriate properties of this *pre-valuation* are embodied in

LEMMA 2. (i) $v(\alpha) \geqslant 1$ *always*,
(ii) $v(n\alpha) = v(\alpha)$ *if* $(n, p) = 1$,
(iii) $v(n\alpha) \leqslant \max(|n|_p v(\alpha), 1)$,
(iv) $v(\alpha + \beta) \leqslant \max(v(\alpha), v(\beta))$.

PROOF. Assertions (i) and (ii) follow directly from the definition of the pre-valuation.

If α and β have orders u and v respectively, then the least common multiple $[u, v]$ will annihilate $\alpha + \beta$:

$$[u, v](\alpha + \beta) = 0.$$

Thus

$$v(\alpha + \beta) \leqslant |[u, v]|_p^{-1} = \max\left(|u|_p^{-1}, |v|_p^{-1}\right) = \max(v(\alpha), v(\beta)),$$

giving (iv).

Let α be a non-zero element of order m. Let m and n be exactly divisible by p^s and p^r respectively. If $r \geqslant s$ then $|n|_p v(\alpha) = p^{-r+s} \leqslant 1$, giving the inequality of (iii). Otherwise $(p^{-r}m)n\alpha = 0$ and $v(n\alpha) \leqslant p^{s-r} = |n|_p v(\alpha)$, from which the inequality of (iii) is again obtained.

Returning to the recurrence (1) we note that not every coefficient c_j is divisible by our (arbitrary) prime p.

LEMMA 3. *Let* $(\alpha_1, \alpha_2, \ldots)$ *be a solution to the equation* (1). *Then for every* $n \geqslant k + 1$ *with* $v(\alpha_n) > 1$

either: *there is an integer* j, $1 \leqslant j \leqslant k$, *so that*

(i) $$v(\alpha_n) \leqslant v(\alpha_{n-j}),$$

or: *there is an infinite sequence*

$$v(\alpha_n) \leqslant p^{-1} v(\alpha_{n+r_1}) \leqslant p^{-2} v(\alpha_{n+r_1+r_2}) \leqslant \cdots$$

where each r_i *satisfies* $1 \leqslant r_i \leqslant k$.

PROOF. Let $\mu = c_h$ be the coefficient c_j, with the maximum j for which $(p, c_j) = 1$. Then for (each) $n \geqslant k + 1$

$$\mu\alpha_n = \sum_{j=1}^{k-h} d_j\alpha_{n+j} + \sum_{j=1}^{h} e_j\alpha_{n-j}$$

where the integers d_j are divisible by p. As usual, empty sums are deemed to be 0.

In view of Lemma 2

$$v(\alpha_n) = v(\mu\alpha_n) \leqslant \max\left\{ \max_{1 \leqslant j \leqslant k-h} v(d_j\alpha_{n+j}),\ \max_{1 \leqslant j \leqslant h} v(e_j\alpha_{n-j})\right\}.$$

Suppose first that this upper bound is $v(e_j\alpha_{n-j})$ for some j in the range $1 \leqslant j \leqslant h$. Then since $|e_j|_p \leqslant 1$,

$$v(\alpha_n) \leqslant \max\big(v(\alpha_{n-j}), 1\big).$$

By hypothesis $v(\alpha_n) > 1$, giving $v(\alpha_n) \leqslant v(\alpha_{n-j})$, the first possibility in the lemma.

Otherwise

$$v(\alpha_n) \leqslant v(d_j\alpha_{n+j}) \leqslant \max\big(|d_j|_p v(\alpha_{n+j}), 1\big)$$

for some j in the range $1 \leqslant j \leqslant k - h \leqslant k$. Once again $v(\alpha_n) > 1$, giving now

$$v(\alpha_n) \leqslant p^{-1}v(\alpha_{n+r_1}) \tag{2}$$

for some r_1 in the interval $1 \leqslant r_1 \leqslant k$.

We suppose r_1 to be the minimal integer for which this inequality is valid, and repeat the above argument with $n + r_1$ in place of n. Note that $v(\alpha_{n+r_1}) > 1$.

If in this manner we arrive at an inequality

$$v(\alpha_{n+r_1}) \leqslant v(\alpha_{n+r_1-j})$$

with $1 \leqslant j \leqslant h$, let $m = n + r_1 - j$.

For $m < n$ we get again an inequality of the form (i) in the statement of the lemma.

With $m = n$ we would have

$$v(\alpha_n) \leqslant p^{-1}v(\alpha_{n+r_1}) \leqslant p^{-1}v(\alpha_m) = p^{-1}v(\alpha_n),$$

which is impossible.

For $n < m < n + r_1$ we would get

$$v(\alpha_n) \leqslant p^{-1}v(\alpha_{n+(m-n)}),$$

contradicting the minimality of r_1.

Otherwise we shall obtain an analogue of the inequality (2):

$$v(\alpha_{n+r_1}) \leqslant p^{-1}v(\alpha_{n+r_1+r_2})$$

for some (minimal) r_2 in the interval $1 \leqslant r_2 \leqslant k$.

The proof now proceeds by induction.

REMARKS. This lemma shows that in some sense the order of α_n either remains bounded, or grows exponentially. In particular the results of Lemma 1 is not unreasonable.

We come now to our applications to the theorem. We shall apply the following result from the author's paper Elliott (1983).

Let Δ be a subgroup of Q_2.

LEMMA 4. *In order that the quotient group Q_2/Δ be trivial, it is necessary and sufficient that every homomorphism of it into the additive $\mathbf{Z}$-module $Q/\mathbf{Z}$ be trivial.*

REMARK. $Q/\mathbf{Z}$ is the well-known additive group of the rationals (mod 1), and it is not a field.

Any homomorphism of a group Q_2/Δ into $\mathbf{Q}/\mathbf{Z}$ will have the form

$$y \oplus z \mapsto f_1(y) + f_2(z)$$

where the $f_i(\ )$ are, in the usual notation of analytic number theory, *completely additive arithmetic functions* with values in $Q/\mathbf{Z}$.

In our present circumstances we take for Δ the group generated by Γ (see earlier) and a finite collection

$$l \oplus 1, \qquad 1 \oplus l, \qquad 1 \leqslant l \leqslant T,$$

and show that for a suitably chosen T, Q_2/Δ is trivial. It will suffice to establish

LEMMA 5. *With a suitably chosen (finite) T, any pair (f_1, f_2) of additive functions which take values in $Q/\mathbf{Z}$ and satisfies*

$$f_1(P(n)) + f_2(P(n+t)) = 0 \tag{3}$$

for all $n \geqslant 1$, together with

$$f_i(l) = 0, \qquad i = 1, 2, , 1 \leqslant l \leqslant T, \tag{4}$$

is necessarily trivial.

During the proof of this lemma we shall apply (perhaps surprisingly) the following sieve result.

https://doi.org/10.1017/S1446788700027099 Published online by Cambridge University Press

LEMMA 6. *Let d be a positive integer. Then there is a constant g so that the number of integers m in the interval $n < m < n + y$ which have no prime factor q in the range $d < q < \sqrt{y}$ is at most*

$$\frac{gy}{\log y}$$

uniformly for all integers $n \geqslant 1$ and real $y \geqslant 2$.

PROOF. See Chapter 2 of the author's book Elliott (1979b) or the account of sieve theory given by Halberstam and Richert (1974).

PROOF OF LEMMA 5. In view of the additive nature of the f_i

$$f_i(P(n)) = \sum_{j=0}^{h} b_j f_i(n + a_j).$$

The hypothesis (3) of Lemma 5 may thus be expressed in the form $\sum_{j=0}^{k} c_j \alpha_{n+j} = 0$ for all $n \geqslant 1$, where $k = a_h$, $\alpha_n = f_1(n) + f_2(n + t)$, and the integers c_j, not all zero, have highest common factor 1.

We aim to prove that $f_i(n) = 0$, $i = 1, 2$, and so $\alpha_n = 0$, for all n. By hypothesis this assertion is valid for $1 \leqslant n \leqslant T - t$.

Let $c = c_k$, which is without loss of generality positive. If $T \geqslant k + t$ then $\alpha_n = 0$ for $1 \leqslant n \leqslant k$, and by Lemma 1, $c^n \alpha_n = 0$ for all positive integers n.

If $c = 1$ then $\alpha_n = 0$ for all n, and this already leads to the complete result. Indeed, replacing n by nt we obtain

$$\begin{aligned} 0 = \alpha_{nt} &= f_1(nt) + f_2(t\{n + 1\}) \\ &= f_1(n) + f_2(n + 1) \end{aligned}$$

since $T \geqslant t$ and $f_1(t) = 0 = f_2(t)$.

Writing β_n for $f_1(n) + f_2(n + 1)$ we see that for $s \geqslant 2$

$$\begin{aligned} f_2(s) &= \beta_{s-1} - f_1(s - 1), \\ f_1(s) &= f_1(s/2) \quad \textit{if s is even}, \\ f_1(s/2) &= \beta_s - f_2((s + 1)/2) \quad \textit{if s is odd}, \end{aligned} \tag{5}$$

since $T \geqslant 2$ and $f_1(2) = 0 = f_2(2)$.

Together with $\beta_s = 0$ for $s \geqslant 1$ these relations clearly demonstrate (inductively) the triviality of the functions f_i.

Suppose now that $c > 1$. Choose a prime divisor p of c and define a pre-valuation $v(\ )$ on $Q/\mathbf{Z}$ in terms of p. We shall prove that if T is fixed at a large enough value, *independent of the definition of the f_i*, then $v(\alpha_n) = 1$ holds for all n.

We argue by contradiction, noting that $v(\alpha_n) = 1$ for $1 \leqslant n \leqslant T - t$. Assume that there is an integer $n \geqslant k + 1$ with $v(\alpha_n) > 1$. We apply Lemma 3 with the least such n. This rules out the possibility (i) given by that lemma, and we must have an infinite chain of inequalities

$$(6) \qquad v(\alpha_n) \leqslant p^{-1}v(\alpha_{n+r_1}) \leqslant p^{-2}v(\alpha_{n+r_1+r_2}) \leqslant \cdots$$

with $1 \leqslant r_i \leqslant k$.

There must be an integer J, bounded only in terms of k and t, so that each of the integers

$$n + \sum_{i=1}^{J} r_i, \qquad \left(n + \sum_{i=1}^{J} r_i\right) + t$$

has a prime factor q in the range $2t \leqslant q \leqslant n/(2t)$. For otherwise the integers

$$n + \sum_{i=1}^{w} r_i + \begin{Bmatrix} 0 \\ t \end{Bmatrix}$$

for $w = 1, 2, \ldots, z$, will between them generate at least $z/4$ numbers m which have no such factors, and which lie in the interval $n < m < n + kz + t$. According to Lemma 6, either $n \leqslant 2t(kz + t)^{1/2}$ or

$$z/4 \leqslant g(kz + t)/\log(kz + t).$$

We choose for z a value large enough that this last inequality fails, and then restrict T to exceed $2t(kz + t)^{1/2} + t$. Since $v(\alpha_n) > 1$ this will not allow the penultimate inequality.

Hence, writing δ for the sum $r_1 + \cdots + r_J$, we have

$$n + \delta = m_1 m_2, \qquad n + \delta + t = m_3 m_4$$

where $2t < m_i \leqslant (n + \delta + t)/(2t)$ for $i = 1, \ldots, 4$. Therefore

$$\alpha_{n+\delta} = \sum_{i=1}^{2} f_1(m_i) + \sum_{j=3}^{4} f_2(m_j)$$

where for all large enough values of n

$$\max_{1 \leqslant i \leqslant 4} m_i \leqslant (n + Jk + t)/(2t) < (n - 1)/t.$$

According to our temporary hypothesis, $v(\alpha_u) = 1$ for $1 \leqslant u \leqslant n - 1$, so that $v(\beta_s) = 1$ for $1 \leqslant s \leqslant (n - 1)/t$. The relations (5) then allow us to assert that

$$v(f_i(s)) = 1$$

for $i = 1, 2$ and all s not exceeding $(n - 1)/t$. In particular we may conclude that $v(\alpha_{n+\delta}) = 1$. Our chain of inequalities (6) now gives the impossible $v(\alpha_n) \leqslant 1$.

We may carry out this argument using each of the prime divisors of c, and since the primes which divide the order of α_n also divide c, obtain that $\alpha_n = 0$ for every positive n.

Lemma 5 is now immediate, and with its proof we have completed step one.

Step two: G is finite

In this section I apply quite different ideas.

Elliptic power-sums.

LEMMA 7. *Let z_j, $j = 1, \ldots, k$, be complex numbers which satisfy $|z_j| = 1$. Let ρ_j, $j = 1, \ldots, k$ be further complex numbers, and assume that the function*

$$H(n) = \sum_{j=1}^{k} \rho_j z_j^{n^2}$$

is not zero for all positive integers n. Then

$$\limsup_{n\to\infty} |H(n)| > 0.$$

PROOF. We argue by induction on k. The case $k = 1$ is trivial.

Let $k \geqslant 2$. Without loss of generality $\rho_1 \neq 0$.

Suppose first that no z_j/z_1 is a root of unity. Then

$$H(n) = z_1^{n^2}\left(\rho_1 + \sum_{j=2}^{k} \rho_j \left(z_j z_1^{-1}\right)^{n^2}\right)$$

where for $j \geqslant 2$, $z_j z_1^{-1} = \exp(2\pi i \theta_j)$ for some irrational real number θ_j. Hence

$$\lim_{x\to\infty} x^{-1} \sum_{n\leqslant x} z_1^{-n^2} H(n) = \rho_1 + \sum_{j=2}^{k} \rho_j \lim_{x\to\infty} x^{-1} \sum_{n\leqslant x} e^{2\pi i n^2 \theta_j} = \rho_1,$$

each right-hand limit being zero by a result of Hermann Weyl. For an account of the appropriate estimates for exponential sums see Cassels (1957) Chapter IV. Sharper bounds may be obtained by using a transcendence measure for the sum of two logarithms of algebraic integers, and then applying this to the Weyl-sum inequality given in Vaughan (1981) Lemma (2.4). In this case we deduce that

$$\limsup_{n\to\infty} |H(n)| \geqslant |\rho_1| > 0.$$

Otherwise we can write

$$z_j = \lambda_j z_1, \qquad j = 2, \ldots, m,$$

where z_j/z_1 is not a root of unity for $m < j \leqslant k$. We write $H(n)$ in the form

$$z_1^{n^2}\left(\sum_{j=1}^{m} \rho_j \lambda_j^{n^2} + \sum_{j=m+1}^{k} \rho_j \left(z_j z_1^{-1}\right)^{n^2}\right) = z_1^{n^2}\left(H_1(n) + H_2(n)\right)$$

say. If $H_1(n) = 0$ for all n, then $H_2(n)$ is non-zero for at least one integer n, and we may apply our induction hypothesis to obtain the desired result. If $H_1(n) \neq 0$

https://doi.org/10.1017/S1446788700027099 Published online by Cambridge University Press

for some n, then the function

$$J(n) = \sum_{j=1}^{m} \rho_j \lambda_j^{n^2}$$

is periodic, or period q say, and there is an integer t so that $J(t) \neq 0$. Thus for all positive integers r

$$z_1^{-(t+rq)^2} H(t + rq) = J(t) + H_2(t + rq).$$

Once again $z_j/z_1 = \exp(2\pi i \theta_j)$ where θ_j is irrational for $j > m$, and by another appeal to a Weyl-sum inequality

$$\frac{1}{y} \sum_{r \leq y} e^{2\pi i (r^2 q^2 + 2rtq)\theta_j} \to 0 \quad \text{as } y \to \infty.$$

Hence $\lim_{r\to\infty} 1/y \Sigma_{r \leq y} H_2(t + rq) = 0$, and arguing as earlier

$$\limsup_{n\to\infty} |H(n)| \geq \limsup_{r\to\infty} |H(t + rq)| \geq |J(t)| > 0.$$

This completes the proof of Lemma 7.

REMARK. The above proof shows that if $H(n)$ vanishes for all $n \geq 1$ then either every $\rho_j = 0$, or some ratio z_i/z_j with $i \neq j$ is a root of unity.

The analogue of Lemma 4 which is relevant to this part of the proof of the theorem is the following

LEMMA 8. *In order that every element of Q_2/Γ should have a finite order, it is necessary and sufficient that there should be no non-trivial homomorphisms of Q_2/Γ into the additive group of real numbers.*

PROOF. A proof of this result may be found in the author's paper Elliott (1983), where an account is given of earlier related results.

In order to apply Lemma 8 we show that any pair (f_1, f_2) of real-valued additive arithmetic functions which satisfies

$$f_1(P(n)) + f_2(P(n + t)) = 0$$

for all $n \geq 1$ must be trivial. As in *step one*, with $\alpha_n = f_1(n) + f_2(n + t)$ we have $\Sigma_{j=0}^{k} c_j \alpha_{n+j} = 0$. Since the real numbers form a field this linear recurrence has a solution of the form

$$f_1(n) + f_2(n + t) = \alpha_n = \sum_{j=1}^{w} F_j(n) \delta_j^n, \qquad n = 1, 2, \ldots,$$

where the δ_j lie in some algebraic extension of the rational field Q, and the $F_j(x)$ may be taken to be polynomials defined over this same extension field.

Replacing n by tn and appealing to the additive nature of the f_i,

$$f_1(n) + f_2(n+1) = \sum_{j=2}^{w} F_j(tn)\delta_j^{tn} - \sum_{i=1}^{2} f_i(t).$$

This holds for all positive integers n, including even integers:

$$f_1(2n) + f_2(2n+1) = \sum_{j=1}^{w} F_j(2tn)\delta_j^{2tn} - \sum_{i=1}^{2} f_i(t).$$

By subtraction, writing f for f_2, we see that $f(2n+1) - f(n+1)$ and so $f(2n-1) - f(n)$ have representations of the same type:

$$f(2n-1) - f(n) = \sum_{j=1}^{s} R_j(n)\lambda_j^n.$$

Suppose now that the ratio $\lambda_1\lambda_2^{-1}$ is a root of unity, say $\lambda_1^d = \lambda_2^d$. If in this representation we replace n by dn then

$$f(2dn-1) - f(n) = \sum_{j=1}^{s} R_j(dn)\lambda_j^{dn} + f(d),$$

where the terms $R_1(dn)\lambda_1^{dn} + R_2(dn)\lambda_2^{dn}$ may be coalesced into a single term of the same form.

Continuing in this manner we reach a representation

$$f(D^2n-1) - f(n) = \sum_{j=1}^{r} S_j(n)\omega_j^n + \text{constant}, \tag{7}$$

with D a positive integer, and where no ratio $\omega_i\omega_j^{-1}$ with $i \neq j$ is a root of unity.

We shall prove that a representation of this type is only available to trivial additive functions f. To this end we need

LEMMA 9. *Let A ($\geqslant 2$) be a positive integer. If a completely real-valued function f has $f(An-1) - f(n)$ bounded for all $n \geqslant 1$, then it must be of the form $B \log n$ for all positive n.*

PROOF. A (somewhat) complicated proof of a similar result may be found in the author's paper Elliott (1979a). In order to obtain the present result by the same method only minor adjustments are necessary, together with a proof that if $f(An-1) - f(n)$ is bounded, then so for $n \geqslant 2$ is $f(n)/\log n$. This last we shall now supply.

Suppose that $|f(Am-1)-f(m)| \leqslant C$ for all $m \geqslant 1$. If an integer n is divisible by a prime divisor q of A, then there is an integer $n_1 = n/q < (1-(2A)^{-1})n$ so that

$$|f(n)| \leqslant |f(n_1)| + |f(q)|.$$

Otherwise n will have the form $Am + l$, where $1 \leqslant l \leqslant A$, $(l, A) = 1$. In this case let z be the unique integer in the interval $1 \leqslant z \leqslant A$ which satisfies $zl \equiv -1 \pmod{A}$, say with $zl = Au - 1$. Note that $A \geqslant 2$ and therefore $z \leqslant A - 1$ must hold. Then

$$\begin{aligned} f(n) &= f(zn) - f(z) \\ &= f(A\{am + u\} - 1) - f(z) \end{aligned}$$

so that writing $n_1 = zm + u$ and appealing to our hypothesis

$$|f(n)| \leqslant |f(n_1)| + C + |f(z)|.$$

Here the integer n_1 does not exceed $(1 - A^{-1})n + 1$.

Defining $U(x) = \max_{n \leqslant x} |f(n)|$ we have

(8) $$U(x) \leqslant U((1 - 1/2A)x) + \text{constant}$$

for all sufficiently large (in terms of A only) values of x.

An easy induction proof now completes the argument.

Without loss of generality we may assume that

$$\omega = |\omega_1| = |\omega_2| = \cdots = |\omega_h| > |\omega_{h+1}| \geqslant \cdots \geqslant |\omega_r|.$$

Moreover, we may also assume that

$$d = \text{degree}\, S_1(x) \geqslant \text{degree}\, S_2(x) \geqslant \cdots \geqslant \text{degree}\, S_h(x).$$

Of course the polynomials $S_j(x)$ with $j > h$ (if there are any) may have degrees greater than d.

LEMMA 10. *If $d \geqslant 1$ or $|\omega| > 1$ then there is a constant E so that*

$$|f(n)| \leqslant En^d \max(\omega, 1)^n$$

for all positive integers n.

PROOF. It follows from the representation (7) that

$$|f(D^2n - 1) - f(n)| \leqslant Ln^d \max(\omega, 1)^n$$

for some constant L and all $n \geqslant 1$.

The argument given in the above account of Lemma 9 may be applied here also. In the same notation as before (save that $A = D^2$) we obtain

$$U(x) \leqslant U((1 - 1/2A)x) + Mx^d \max(\omega, 1)^x$$

as an analogue of (8).

An inductive proof of Lemma 10 is now readily arranged.

If in the representation (7) we replace n by n^2, the term $D^2n^2 - 1$ factorises into $(Dn - 1)(Dn + 1)$ and we obtain

$$\sum_{j=1}^{r} S_j(n^2)\omega_j^{n^2} = f(Dn + 1) + f(Dn - 1) - 2f(n) + N$$

for some constant N. Under the conditions of Lemma 10 this right-hand side does not exceed a constant multiple of $n^d \max(\omega, 1)^{nD}$ in size.

Suppose now that $\omega > 1$. Dividing both sides of the above equation by $n^{2d}\omega^{n^2}$ we obtain an asymptotic relation

$$\sum_{j=1}^{h} \rho_j z_j^{n^2} \to 0, \qquad n \to \infty,$$

since no matter what the values of d or D,

$$n^{-d}\max(\omega, 1)^{nD}\omega^{-n^2} \to 0$$

as n becomes unbounded. Here we have written z_j for $\omega_j\omega^{-1}$, and ρ_j is the coefficient of x^d in the polynomial $S_j(x)$.

In view of Lemma 7, the elliptic power-sum $\sum_{j=1}^{h}\rho_j z_j^{n^2}$ must be zero for all $n \geqslant 1$. But since not all the $\rho_j = 0$, and we have arranged that no ratio z_i/z_j with $i \neq j$ is a root of unity, this cannot be the case.

Thus $\omega \leqslant 1$, and every $|\omega_j| \leqslant 1$.

Suppose now, without loss of generality, that $\omega = 1$ but that $d \geqslant 1$. Then Lemma 10 yields the bound $|f(n)| \leqslant En^d$. The argument given above will once again lead to a contradiction.

We can therefore write

$$f(D^2n - 1) - f(n) = \sum_{j=1}^{h} \rho_j\omega_j^n + Y + O(c^{-n})$$

where Y and $c > 1$ are constants, and every $|\omega_j| = 1$. In particular $f(D^2n - 1) - f(n)$ is bounded for all n.

Applying Lemma 9 with $A = D^2$ we conclude that $f(n)$ has the form $B\log n$ for all positive n.

Since $\log(D^2n - 1) - \log n = 2\log D - (D^2n)^{-1} + O(n^{-2})$ we can define

$$\rho_0 = Y - 2\log D, \qquad \omega_0 = 1,$$

and write

$$\sum_{j=0}^{h} \rho_j\omega_j^n = -\frac{B}{D^2n} + O\left(\frac{1}{n^2}\right).$$

https://doi.org/10.1017/S1446788700027099 Published online by Cambridge University Press

Suppose for the moment that B is non-zero. Replacing n by n^2 gives

$$V(n) = \sum_{j=0}^{h} \rho_j \omega_j^{n^2} = -\frac{B}{(Dn)^2} + O\left(\frac{1}{n^4}\right).$$

Here the expression on the right hand side (and so also $V(n)$) does not vanish for all large n.

Another application of Lemma 7 gives $\limsup_{n\to\infty} |V(n)| > 0$, which is not compatible with the bound $V(n) = O(n^{-2})$. Hence $B = 0$, and we have proved that $f_2(n) = f(n) = 0$ for all positive integers n.

Returning to our first representation for α_n we now have the simpler

$$(9) \qquad f_1(n) = \sum_{j=1}^{w} F_j(n)\delta_j^n$$

valid for $n = 1, 2, \ldots$.

There are several ways to deduce that f_1 is trivial. For example, since $f_1(n)$ satisfies the linear recurrence

$$(10) \qquad \sum_{j=0}^{h} b_j f_1(n + a_j) = 0$$

we may appeal to Theorem 1 of the author's paper Elliott (1980) to deduce that $f_1(n)$ has the form $C \log n$ for some constant C. Substituting into (10) gives

$$C \sum_{j=0}^{h} b_j \log(n + a_j) = 0.$$

If $C \neq 0$ then as $n \to \infty$ there is for positive t an asymptotic estimate

$$\sum_{j=0}^{h} b_j \left(\log n + \sum_{r=1}^{t} (-1)^{r+1} \left(\frac{a_j}{n}\right)^r \right) = O(n^{-t+1}).$$

From these we deduce that $\sum_{j=0}^{h} b_j a_j^r = 0$, $r = 0, 1, \ldots$. Hence

$$\sum_{j=0}^{h} b_j \log(x + a_j)$$

vanishes as a function of complex x, first for $|x| < 1$ and then, by analytic continuation, over the half-plane $\mathrm{Re}(x) > 0$.

Thus the rational function

$$P(x) = \prod_{j=0}^{h} (x + a_j)^{b_j}$$

is identically one; a nonsense.

Alternatively, we may treat the representation (9) as we did that of (7), after arranging that the ratios δ_i/δ_j, $i \neq j$ are not roots of unity. In this way $f_1(n)$ is seen to be bounded, and a (uniformly) bounded completely additive (real-valued) function is identically zero.

We have now proved that every element of the group $G = Q_2/\Gamma$ has finite order, and since we established in part one that G is finitely distributed, it must in fact be finite.

This completes step two.

Step three: G is trivial

Once again the argument takes a different turn. The argument hinges upon the following analogue of Lemma 8, a proof of which may be found in the author's paper Elliott (1983).

Let p be a prime number.

LEMMA 11. *In order that every element of the group Q_2/Γ be a pth-power, it is necessary and sufficient that there be no non-trivial homomorphism of it into the additive group of a finite field F_p of p elements.*

Let (f_1, f_2) be a pair of additive functions which take values in F_p. If

$$f_1(P(n)) + f_2(P(n+t)) = 0$$

for all positive integers n, then as in *Step two* $\alpha_n = f_1(n) + f_2(n+t)$ satisfies a linear recurrence $\sum_{j=0}^{k} c_j \alpha_{n+j} = 0$. Here the c_j are interpreted in F_p according to the map

$$c_j \to c_j \pmod{p} \quad \text{in } \mathbf{Z}/p\mathbf{Z},$$

and since $(c_0, \ldots, c_k) = 1$, not all the c_j vanish (mod p).

We obtain formally the same representation

$$f_1(n) + f_2(n+t) = \sum_{j=1}^{w} F_j(n)\delta_j^n$$

as in *step two*, and with f denoting f_2, reach

$$f(2n-1) - f(n) = \sum_{j=1}^{r} R_j(n)\lambda_j^n \tag{11}$$

where the λ_j and the coefficients in the polynomials R_j all belong to a finite algebraic extension of F_p, say F_q.

https://doi.org/10.1017/S1446788700027099 Published online by Cambridge University Press

In particular each λ_j^n is periodic in n, of period $q - 1$. The $R_j(n)$ are periodic in n, of period p, so that the whole of the expression on the right-hand side of the above equation is periodic, with a period $p(q - 1)$.

The function $f(2n - 1) - f(n)$ is therefore periodic, of period $d = p(q - 1)$. This may not be its minimal period, but that will not matter in what follows.

Replacing n by $2n^2$ we see that the function

$$f(2n - 1) + f(2n + 1) - 2f(n) = f(4n^2 - 1) - f(2n^2) + f(2)$$

is also periodic, with the same period; and by subtraction the difference

$$f(2n + 1) - f(2n - 1). \tag{12}$$

We shall denote their difference by $g(n)$.

Let $T = \sum_{n=1}^{d} g(n)$ be a sum over a period (mod d). Then for any positive integer s

$$\sum_{n=1}^{pds} \{f(2n + 1) - f(2n - 1)\} = sp\,T = 0.$$

But the sum telescopes to give $f(2pds + 1) = 0$ for all $s \geqslant 1$.

An additive function, with values in F_p, which satisfies

$$f(Dn + 1) = 0$$

for some positive integer D and all $n \geqslant 1$, need not be identically zero on the integers prime to D. It will, however, be given by

$$\exp(2\pi i f(n)/p) = \chi(n)$$

for some (fixed) Dirichlet character χ (mod D).

We shall not need this last result. In fact (12) shows that $g(2pds)$ has a period 1 in s; it is constant for all $s \geqslant 1$. With what we have already established, the replacement of n in (12) by $2pds$ shows that

$$f(2pds - 1) = f(2pd - 1) = \text{constant}$$

for all positive s.

Equation (11) with $2pds$ in place of n allows us to assert that if $\lambda_0 = 1$ and $R_0(x)$ is a suitable constant (polynomial), then there is a representation

$$f(s) = -\sum_{j=0}^{r} R_j(2pds)\lambda_j^{2pds}$$

valid for all $s \geqslant 1$. The expression on the right-hand side of this equation has period 1, so that $f(n)$ is a constant, μ say.

Since

$$-\mu = f(1^2) - 2f(1) = 0,$$

we have proved that the additive function $f_2 = f$ vanishes identically.

https://doi.org/10.1017/S1446788700027099 Published online by Cambridge University Press

In particular

$$f_1(n) = \sum_{j=1}^{w} F_j(n)\delta_j^n$$

for all $n \geqslant 1$. It is easy to obtain from this representation that $f_1(n)$ is periodic and then a constant, and so zero.

In view of Lemma 11 we see that whatever the choice of prime p, each element of the group G is a pth-power. This forces G to be trivial. For example let G have order r, so that each element g of G satisfies $g^r = 1$. If p is a prime divisor of r then there is a further element γ of G so that $g = \gamma^p$. Hence

$$g^{rp^{-1}} = \gamma^r = 1.$$

Proceeding inductively we obtain $g = 1$, and the triviality of G.

The theorem is proved.

References

J. W. S. Cassels (1957), *An introduction to diophantine approximation* (Cambridge University Tracts No. 45).

P. D. T. A. Elliott (1979a), 'Sums and differences of additive arithmetic functions in mean square,' *J. Reine Angew. Math.* **309**, 21–54.

P. D. T. A. Elliott (1979b), *Probabilistic number theory*, I (Grundlehren Math. Wiss. No. 239, Springer, Berlin and New York).

P. D. T. A. Elliott (1980), 'On sums of additive arithmetic functions with shifted arguments,' *J. London Math. Soc.* (2) **22**, 25–38.

P. D. T. A. Elliott (1983), 'On representing integers as products of integers of a prescribed type,' *J. Austral. Math. Soc. Ser A* **35**, 143–161.

H. Halberstam and H.-E. Richert (1974), *Sieve methods* (Academic Press, London).

R. C. Vaughan (1981), *The Hardy-Littlewood method* (Cambridge University Tracts No. 80).

University of Colorado
Boulder, Colorado 80309
U.S.A.