Proceedings of the Edinburgh Mathematical Society (1979), 22/1 17-21 ©

ON KELLER'S CONJECTURE FOR CERTAIN CYCLIC GROUPS

by A. D. SANDS
(Received 3rd June 1977)

1. Introduction

Keller (6) considered a generalisation of a problem of Minkowski (7) concerning the filling of R^n by congruent cubes. Hajós (4) reduced Minkowski's conjecture to a problem concerning the factorization of finite abelian groups and then solved this problem. In a similar manner Hajós (5) reduced Keller's conjecture to a problem in the factorization of finite abelian groups, but this problem remains unsolved, in general. It occurs also as Problem 80 in Fuchs (3). Seitz (10) has obtained a solution for cyclic groups of prime power order. In this paper we present a solution for cyclic groups whose order is the product of two prime powers.

Throughout the paper we shall be dealing with finite abelian groups using the additive notation. If $A_1, \ldots, A_k$ are subsets of such a group G and if each $g \in G$ can be expressed uniquely as $g = \Sigma a_i$, $a_i \in A_i$, then we write $G = A_1 + A_2 + \cdots + A_k$ and call this a factorization of G. We shall assume $0 \in A_i$, for each i, since the subsets $\{A_i\}$ give rise to such a factorization of G if and only if the subsets $\{g_i + A_i\}$ do so also, for any elements $g_i \in G$. We denote the order of A_i by $|A_i|$ and, to avoid trivial cases, assume $|A_i| > 1$ for each i. If A is a subset of G we define

$$A - A = \{g \in G | \exists a_1, a_2 \in A \text{ with } g = a_1 - a_2\}.$$

Note that $(A + b) - (A + b) = A - A$ for all $b \in G$. A subset A of G is called cyclic if there exists $a \in G$ and an integer n with

$$A = \{0, a, 2a, \ldots, (n-1)a\} = [a]_n.$$

Such a cyclic subset A is a subgroup if and only if the order of a is n. It is clear that $[a]_{km} = [a]_k + [ka]_m$. Thus every cyclic set is a sum of cyclic sets of prime order.

Hajós has reduced Keller's conjecture to the following. If $G = A_1 + \cdots + A_k + B$ where each A_i is cyclic, $A_i = [a_i]_{n_i}$, then there exists i such that $n_i a_i \in B - B$. In the corresponding Minkowski problem, where the centres of the cubes form a lattice, B turns out to be a subgroup of G and Hajós solved the problem by showing that in the quotient group G/B the image of one of the factors A_i is a subgroup.

2. Preliminaries

Let G be a cyclic group of order n with generator g. Let M be an irreducible representation of G. Let ρ be an nth primitive root of unity. Then $M(g) = \rho^d$ for some

integer d, $1 \leqslant d \leqslant n$. Let A be a subset of G, $A = \{m_1 g, m_2 g, \ldots, m_t g\}$. We define $M(A) = \Sigma_{a \in A} M(a) = \Sigma \rho^{dm_i}$. We define $A(x) = \Sigma x^{m_i}$. Let $n/(d, n) = m$. Then ρ^d is an mth primitive root of unity. Let $F_m(x)$ denote the mth cyclotomic polynomial. Then $M(A) = 0$ if and only if $F_m(x)$ divides $A(x)$.

If $A_1 + \cdots + A_k = G$ then $M(A_1) \ldots M(A_k) = M(G)$; $M(G) = 0$, provided M is not the identity representation. Therefore $M(A_i) = 0$ for some i.

We need a generalisation of Theorem 2 of de Bruijn (1). Let $n = km$. We define

$$G_{n,k}(x) = (x^n - 1)/(x^m - 1) = 1 + x^m + \cdots + x^{(k-1)m}$$

$$= \prod_{d|n} F_d(x) / \prod_{d|m} F_d(x) = \prod_{\substack{d|n \\ d \nmid m}} F_d(x).$$

Let p, q be distinct primes and $n = p^e q^f$.

Lemma. *Let $A(x)$ be a polynomial with non-negative integer coefficients and degree less than n. Let $F_n(x), F_{n/p}(x), \ldots, F_{n/p^{r-1}}(x)$ divide $A(x)$ where $r - 1 < e$. Then there exist polynomials $P(x)$ and $Q(x)$ with non-negative integer coefficients such that*

$$A(x) = P(x)G_{n,p^r}(x) + Q(x)G_{n,q}(x).$$

Proof. The case $r = 1$ is Theorem 2 of (1). We proceed by induction on r. Since $F_n(x), \ldots, F_{n/p^{r-2}}(x)$ divide $A(x)$ we may assume the existence of polynomials $P_1(x), Q_1(x)$ with non-negative integer coefficients such that

$$A(x) = P_1(x)G_{n,p^{r-1}}(x) + Q_1(x)G_{n,q}(x).$$

$F_{n/p^{r-1}}(x)$ divides $A(x)$. Since $F_{n/p^{r-1}}(x)$ divides $G_{n,q}(x)$ but is relatively prime to $G_{n,p^{r-1}}(x)$ we deduce that $F_{n/p^{r-1}}(x)$ divides $P_1(x)$. By Theorem 2 of (1) there exist polynomials $P(x)$ and $Q_2(x)$ with non-negative integer coefficients such that

$$P_1(x) = P(x)G_{n/p^{r-1},p}(x) + Q_2(x)G_{n/p^{r-1},q}(x).$$

Substituting for $P_1(x)$ we have

$$\begin{aligned} A(x) &= P(x)G_{n/p^{r-1},p}(x)G_{n,p^{r-1}}(x) + Q_2(x)G_{n/p^{r-1},q}(x)G_{n,p^{r-1}}(x) + Q_1(x)G_{n,q}(x) \\ &= P(x)G_{n,p^r}(x) + (Q_2(x)G_{n/q,p^{r-1}}(x) + Q_1(x))G_{n,q}(x). \end{aligned}$$

The result follows by induction.

In the case $r - 1 = e$ a simpler result holds, since $F_n(x) \cdot F_{n/p}(x) \ldots F_{n/p^e}(x) = G_{n,q}(x)$. Thus $A(x) = Q(x)G_{n,q}(x)$, and, from considerations of degree, it is clear that $Q(x)$ has non-negative integer coefficients.

3. Keller's conjecture for cyclic groups of order $p^e q^f$

Seitz (10) has proved Keller's conjecture for cyclic groups of order p^e, p a prime. Fraser and Gordon (2) gave a negative answer to Problem 82 of Fuchs (3) for finite abelian groups but obtained a positive answer for cyclic groups. From this it may be deduced that Keller's conjecture holds for 'good' cyclic groups. The only cases not covered by results in Seitz (10) are the cyclic groups of order $p^e q$. Since we are about to prove a more general result we do not include the details of this deduction.

https://doi.org/10.1017/S0013091500027747 Published online by Cambridge University Press

Theorem 1. *If G is a cyclic group of order $p^e q^f$ where p, q are distinct primes and*

$$G = A_1 + \cdots + A_k + B$$

where $A_i = [a_i]_{n_i}$ is a cyclic set, $i = 1, \ldots, k$, then there exists j such that $n_j a_j \in B - B$.

Proof. We may assume that each n_i is prime and so, since $|A_i|$ divides $|G|$, equal to either p or q. Let $n = p^e q^f$. We proceed by induction on n. Let g be a generator of G. We know that for $d|n$, $d > 1$, $F_d(x)$ divides some $A_i(x)$ or $F_d(x)$ divides $B(x)$.

Suppose first that $F_n(x)$ divides $A_j(x)$. By Theorem 2 of (**1**)

$$A_j(x) = P(x)G_{n,p}(x) + Q(x)G_{n,q}(x)$$

where $P(x)$, $Q(x)$ have non-negative integral coefficients. Substituting $x = 1$ we have

$$A_j(1) = pP(1) + qQ(1).$$

If $n_j = p$ we have $P(1) = 1$, $Q(1) = 0$; if $n_j = q$ we have $P(1) = 0$, $Q(1) = 1$. It follows that $A_j(x) = G_{n,p}(x)$ or $G_{n,q}(x)$ and so that $n_j a_j = 0 \in B - B$.

Thus we may suppose that $F_n(x)$ divides $B(x)$. Let $F_n(x), F_{n/p}(x), \ldots, F_{n/p^{r-1}}(x)$ divide $B(x)$, but $F_{n/p^r}(x)$ not divide $B(x)$ where $r \leqslant e$. Then $F_{n/p^r}(x)$ divides some $A_j(x)$. Let $A_j(x) \equiv D(x) \bmod (x^{n/p^r} - 1)$ where the degree of $D(x)$ is less than n/p^r, i.e. we form $D(x)$ from $A_j(x)$ by reducing the exponents modulo n/p^r. Since $F_{n/p^r}(x)$ divides both $A_j(x)$ and $x^{n/p^r} - 1$ it follows that $F_{n/p^r}(x)$ divides $D(x)$. As above $D(x) = G_{n/p^r,p}(x)$ or $D(x) = G_{n/p^r,q}(x)$. By the Lemma

$$B(x) = P(x)G_{n,p^r}(x) + Q(x)G_{n,q}(x),$$

where $P(x)$, $Q(x)$ have non-negative integral coefficients. Let $D(x) = G_{n/p^r,p}(x)$. Then $n_j = p$ and $a_j = (s(n/p^{r+1}) + t(n/p^r))g$. Thus $n_j a_j = u(n/p^r)g$. If $P(x) \neq 0$ it follows that $n_j a_j \in B - B$. Let $D(x) = G_{n/p^r,q}(x)$. Then $n_j = q$ and $a_j = (s(n/p^r q) + t(n/p^r))g$. Then $n_j a_j = u(n/p^r)g$ and again $n_j a_j \in B - B$ unless $P(x) = 0$. Suppose $P(x) = 0$ then $B(x) = Q(x)G_{n,q}(x)$ and $B = Q + H$ where $H = \{0, (n/q)g, \ldots, (q-1)(n/q)g\}$ is a subgroup of G. From

$$G = A_1 + \cdots + A_k + Q + H$$

we have a factorization of the quotient group

$$G/H = \bar{A}_1 + \cdots + \bar{A}_k + \bar{Q}$$

By the inductive assumption it follows that $n_j \bar{a}_j \in \bar{Q} - \bar{Q}$ for some j, i.e. that $n_j a_j \in Q - Q + H$. Since $B = Q + H$ it is clear that $n_j a_j \in B - B$.

There remains the case where $F_n(x), F_{n/p}(x), \ldots, F_{n/p^e}(x)$ divide $B(x)$. This leads again to $B(x) = Q(x)G_{n,q}(x)$ and as above, using the inductive assumption, we have $n_j a_j \in B - B$ for some j.

4. Further results on the factorization of cyclic groups

The first result here is essentially the cyclic case of the Corollary to Satz 5 of Redei (**8**).

https://doi.org/10.1017/S0013091500027747 Published online by Cambridge University Press

Theorem 2. *Let G be a finite cyclic group and α an automorphism of G. Then $G = A + B$ implies $G = \alpha(A) + B$.*

Proof. Let g be a generator of G and ρ an nth primitive root of unity where $|G| = n$. Let M be a representation of G such that $M(g) = \rho^m$. Let $\alpha(g) = g^d$. Then $(d, n) = 1$ and so ρ^m and ρ^{md} are primitive roots of unity of the same order. $M(A) = 0$ if and only if $A(\rho^m) = 0$; $A(\rho^m) = 0$ if and only if $A(\rho^{md}) = 0$; $A(\rho^{md}) = 0$ if and only if $M(\alpha(A)) = 0$. The result then follows by Hilfssatz 6 of Redei (**8**).

Theorem 3. *If G is a cyclic group then $G = A + B$ if and only if $|G| = |A||B|$ and the subsets $A - A$ and $B - B$ contain no non-zero elements of the same order.*

Proof. If $A - A$ and $B - B$ intersect only in the zero element it is clear that $|A + B| = |A||B|$. Then $|A||B| = |G|$ implies $A + B = G$.

Conversely let $A + B = G$. Then $|A||B| = |G|$. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$ be such that $a_1 - a_2$ and $b_1 - b_2$ have the same order. Since G is cyclic there exists an automorphism α of G such that $\alpha(a_1 - a_2) = b_1 - b_2$. From $\alpha(A) + B = G$ it follows that $(\alpha(A) - \alpha(A)) \cap (B - B) = 0$. Therefore $b_1 - b_2 = 0$ and so $a_1 - a_2 = 0$. Thus $A - A$ and $B - B$ contain no non-zero elements of the same order.

In (**9**) it is conjectured for finite abelian groups G that, if $G = A + B$, then A and B cannot both generate G†. This conjecture is known to be true for 'good' groups. The previous result enables us to prove it for cyclic groups of order $p^e q^f$.

Theorem 4. *If $G = A + B$ and G is a cyclic group of order $p^e q^f$, where p, q are distinct primes, then either $Gp(A) \neq G$ or $Gp(B) \neq G$.*

Proof. Let $Gp(A) = G$. Then either A contains an element a of order $p^e q^f$ or elements a_1 and a_2 of orders $p^e q^{f_1}, f_1 < f$, and $p^{e_1} q^f, e_1 < e$. In the second case $a_1 - a_2$ has order $p^e q^f$. Thus, in each case, $A - A$ contains an element of order $p^e q^f$. Similarly $Gp(B) = G$ implies that $B - B$ contains an element of order $p^e q^f$. By Theorem 3 we cannot have both $Gp(A) = G$ and $Gp(B) = G$.

C. B. Swenson has also raised this question for cyclic groups in his thesis (**11**). One sees that if $G = A + B$ and $Gp(A) = H \neq G$ then $H + g = A + (H \cap (B + g))$ for each $g \in G$. Assuming that the conjecture holds true he is able to deduce, from a knowledge of the factorizations of the proper subgroups of G, rather complicated formulae giving all factorizations of any cyclic group G.

REFERENCES

(1) N. G. DE BRUIJN, On the factorization of cyclic groups, *Indag. Math.* **15** (1953), 370–377.

(2) O. FRASER and B. GORDON, Solution to a problem of L. Fuchs, *Quart. J. Math. Oxford* (2), **25** (1974), 1–8.

†Fraser and Gordon, in a submitted paper 'Solution to a problem of A. D. Sands', have obtained a negative answer to this conjecture for certain non-cyclic groups.

(3) L. FUCHS, *Abelian Groups* (Budapest, 1958).

(4) G. HAJÓS, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Zeit.* **47** (1942), 427–467.

(5) G. HAJÓS, Sur la factorisation des groupes abéliens, *Casopis Pest. Mat. Fys.* **74** (1949), 157–162.

(6) O. H. KELLER, Über die luckenlose Einfulling des Raumes Würfeln, *J. Reine Angew. Math.* **163** (1930), 231–248.

(7) H. MINKOWSKI, *Diophantische Approximationem* (Leipzig, 1907).

(8) L. RÉDEI, Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Haupsatzes von Hajós, *Acta Math. Acad. Sci. Hungar.* **16** (1965), 329–373.

(9) A. D. SANDS, On a conjecture of G. Hajós, *Glasgow Math. J.* **15** (1974), 88–89.

(10) K. SEITZ, *Investigations in the Hajós–Redei Theory of Finite Abelian Groups* (Karl Marx University, Budapest, 1975). (MR 53 no. 655 (1977)).

(11) C. B. SWENSON, *Direct sum subset decompositions of abelian groups*, Ph.D. Thesis (Washington State University, 1972).

THE UNIVERSITY
DUNDEE
SCOTLAND