

# ON SUBGROUPS OF PRIME POWER INDEX

L. F. HARRIS

Let  $G$  be an abelian group. A set  $S \subset G$  is a stellar set if  $mx \in S$  implies  $x, 2x, \dots, mx \in S$ . Let  $p^\alpha$  be a fixed prime power. It is shown that if  $S \cap p^\alpha G = \emptyset$ ,  $G$  satisfies a mild condition, and  $S$  intersects all the subgroups  $K$  of index  $G:K = p^\alpha$ , then the cardinality of  $S$  is bounded below by  $p^\alpha + p^{\alpha-1}$ . This bound is the best possible. The problem is reduced to solving a number of congruence relations

$$\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n \equiv 0 (p^\alpha)$$

with lattice points  $(x_1, x_2, \dots, x_n)$  in a stellar set  $S$  in Euclidean  $n$ -space. This in turn leads to an interesting result on congruence classes of subgroups and points which tells something about the solution in integers of the above congruence relation.

G. K. White [3] has shown that if  $G$  is an abelian group without elements of order  $p^\beta$ ,  $1 < p^\beta < p^\alpha$ , and  $S$  is a stellar set as above, then

$$\begin{aligned} |S| &\geq p^\alpha + p && \text{if } \alpha \geq 2 \\ |S| &\geq p + 1 && \text{if } \alpha = 1. \end{aligned}$$

( $|S|$  is the cardinal number of the set  $S$ .)

We improve this to get

**THEOREM 1.** *Suppose  $p^\alpha$  is fixed,  $G$  is an abelian group without elements of order  $p^\beta$ ,  $1 < p^\beta < p^\alpha$ , and  $S$  is a stellar set satisfying  $S \cap p^\alpha G = \emptyset$  which intersects all the subgroups  $K$  of index  $G:K = p^\alpha$ . Then*

$$|S| \geq p^\alpha + p^{\alpha-1}.$$

J. W. S. Cassels [1] has shown that if a stellar set  $S$  intersects all the subgroups of index  $\leq m$  in an abelian group without elements of finite order than  $|S| \geq m$ . Our result is an improvement for  $m = p^\alpha$ .

Let g.c.d.  $(a_1, \dots, a_k)$  denote the greatest common divisor of  $a_1, \dots, a_k$ . Let  $V_\alpha$  denote the Cartesian product of  $n \geq 1$  copies of  $Z_{p^\alpha}$ , the residue class ring modulo  $p^\alpha$ . Let  $A_0$  denote the free abelian group of rank  $n$ . An  $n$ -tuple (in  $A_0$  or in  $V_\alpha$ ) is said to be  $p$ -primitive if  $p$  does not divide at least one coefficient of the  $n$ -tuple. An integer  $x$  is said to be  $p$ -prime if g.c.d.  $(p, x) = 1$ . Let  $V_\alpha^*$  denote the set

of those  $p$ -primitive elements of  $V_\alpha$  whose first  $p$ -prime coefficient is 1.

If  $x = (x_1, \dots, x_n) \in \Lambda_0$  and  $\lambda = [\lambda_1, \dots, \lambda_n] \in V_\alpha^*$

the dot product is  $\lambda \cdot x = \lambda_1 x_1 + \dots + \lambda_n x_n$ . Because of the one-to-one correspondence between  $\lambda \in V_\alpha^*$  and the subgroup

$$\{x \mid x \in \Lambda_0 \text{ and } \lambda \cdot x \equiv 0 \pmod{p^\alpha}\}$$

of index  $p^\alpha$  in  $\Lambda_0$  we may identify the two. Thus we write  $x \in \lambda$  to mean  $\lambda \cdot x \equiv 0 \pmod{p^\alpha}$ .

By the same reasoning as in [3], Theorem 1 follows from

**THEOREM 2.** *Suppose that for fixed  $p^\alpha, n \geq 2$  every congruence  $\lambda \cdot x \equiv 0 \pmod{p^\alpha}, \lambda \in V_\alpha^*$ , has a solution  $x$  in a stellar set  $S$  satisfying  $S \cap p^\alpha \Lambda_0 = \emptyset$ . Then  $|S| \geq p^\alpha + p^{\alpha-1}$ .*

C. A. Rogers [2] has proved Theorem 2 for the case  $\alpha = 1$ . Two  $n$ -tuples  $\lambda$  and  $\mu$  are said to be *congruent modulo  $p^r$*  if each component of  $\lambda$  is congruent modulo  $p^r$  to the corresponding component of  $\mu$ . If  $\lambda$  and  $\mu$  are  $p$ -primitive elements of  $\Lambda_0$  and  $\lambda \not\equiv k\mu \pmod{p}$  for all  $p$ -prime  $k$  then

$$\{x \mid x \in \Lambda_0 \text{ and } \lambda \cdot x \equiv 0 \pmod{p^{\alpha-1}} \text{ and } \mu \cdot x \equiv 0 \pmod{p}\}$$

is a subgroup of index  $p^\alpha$  in  $\Lambda_0$ , so for  $\alpha \geq 2$  there are many more subgroups of index  $p^\alpha$  in  $\Lambda_0$  than those we are considering in Theorem 2. In order to prove Theorem 2 we need a result on congruence classes of subgroups and points which has some interest in its own right. If  $y$  is a  $p$ -primitive element in a stellar set  $T$  in  $\Lambda_0$  let

$$T(y) = \{mx \in T \mid x \equiv y \pmod{p} \text{ and } m = 1, 2, 3, \dots\}.$$

Then  $T(y)$  is also stellar and we say  $T(y)$  is a  $p$ -class of points of  $T$ .

**THEOREM 3.** *Suppose that  $\alpha \geq \gamma \geq 2, n \geq 3$  and  $\lambda^0 \in V_\alpha^*$  are fixed. If for each  $\lambda$  such that  $\lambda = \lambda^0 \pmod{p}$  and  $\lambda \in V_\alpha^*$  the congruence  $\lambda \cdot x \equiv 0 \pmod{p^\gamma}$  has a solution  $x \in T$  where  $T$  is a stellar subset of  $\Lambda_0$  satisfying  $T \cap p^\alpha \Lambda_0 = \emptyset$  then either (i) all the congruences have a solution in a  $p$ -class  $T(x^0)$  of points of  $T$  for some  $x^0 \in T$  and*

$$|T| \geq |T(x^0)| \geq p^{\gamma-1}$$

or (ii)  $|T| \geq p^{\gamma-1} + \max(|T(x)|, p^{\gamma-2})$  for all  $x \in T$ .

**2. Lemmas.** Theorem 3 is proved by induction. We need two

lemmas for the inductive step and one for the case  $\gamma = 2$ . Assume  $\alpha \geq \gamma$ . Let  $\mu \in V_\alpha^*$  and define

$$A_\gamma(\mu) = \{\lambda \mid \lambda \equiv \mu(p^{\alpha-\gamma})\} = \{\mu + \lambda p^{\alpha-\gamma} \mid 1 \leq \lambda_i \leq p^r\} \subset V_\alpha^*.$$

$$\begin{aligned} \text{Then} \quad A_\gamma(\mu) \cap A_{\gamma-1}(\nu) &= \emptyset & \text{if } \mu \not\equiv \nu(p^{\alpha-\gamma}) \\ A_\gamma(\mu) \supset A_{\gamma-1}(\nu) && \text{if } \mu \equiv \nu(p^{\alpha-\gamma}). \end{aligned}$$

Thus

$$(*) \quad A_\gamma(\mu) = \cup \{A_{\gamma-1}(\mu + \mu' p^{\alpha-\gamma}) \mid 1 \leq \mu'_i \leq p\}.$$

Since each  $A_\gamma(\mu)$  is a set of  $\lambda \in V_\alpha^*$  and each  $\lambda$  can be regarded as a set of  $x \in A_0$ , the  $x$  are in some sense "second level" elements of  $A_\gamma(\mu)$ . We write  $x * A_\gamma(\mu)$  if  $x \in \lambda$  for some  $\lambda \in A_\gamma(\mu)$ .

Suppose  $C$  is a family of  $A_\gamma(\mu)$ . We define ordered pairs

$$\begin{aligned} A(C, x) &= \{A_\gamma(\mu) \mid A_\gamma(\mu) \in C \text{ and } x * A_\gamma(\mu)\} \\ B(A_\gamma(\mu), x) &= \{\lambda \mid \lambda \in A_\gamma(\mu) \text{ and } x \in \lambda\} \\ B(A_\gamma(\mu), T) &= \bigcup_{x \in T} B(A_\gamma(\mu), x). \end{aligned}$$

We say  $T$  covers  $A_\gamma(\mu)$  if and only if  $B(A_\gamma(\mu), T) = A_\gamma(\mu)$ .

We wish to cover  $A_\gamma(\lambda^\circ)$ . Without loss generality take  $\lambda^\circ = [1, 0, \dots, 0]$  and let  $A_\gamma = A_\gamma(\lambda^\circ)$ . Now  $x * A_\gamma$  if and only if

$$\lambda \cdot x = (\lambda^\circ + p^{\alpha-\gamma}\lambda) \cdot x \equiv 0(p^\alpha)$$

for some

$$\lambda^\circ + p^{\alpha-\gamma}\lambda = [1, \lambda_2 p^{\alpha-\gamma}, \dots, \lambda_n p^{\alpha-\gamma}] \in A_\gamma.$$

This implies

$$\begin{aligned} \lambda^\circ \cdot x &\equiv w_1 p^{\alpha-\gamma} (p^\alpha) & \text{for some } w_1 \\ w_1 + \lambda \cdot x &\equiv 0(p^r) \\ (1) \quad w_1 + \sum_2^n \lambda_i x_i &\equiv 0(p^r). \end{aligned}$$

Thus  $T$  covers  $A_\gamma$  if and only if the congruence (1) is satisfied for all  $[1, \lambda_2, \dots, \lambda_n]$  by points  $(p^{\alpha-\gamma} w_1, x_2, \dots, x_n) \in T$ . By (\*) we may write (1) as

$$(2) \quad w_1 + \sum_2^n (\mu'_i + \nu_i p) x_i \equiv 0(p^r)$$

and  $T$  covers  $A_{\gamma-1}(\lambda^\circ + \mu' p^{\alpha-\gamma})$  if and only if (2) is satisfied for all  $\nu_i$ . To simplify notation let  $A(\mu') = A_{\gamma-1}(\lambda^\circ + \mu' p^{\alpha-\gamma})$ .

Since  $\lambda^\circ = [1, 0, \dots, 0]$  implies  $x_1^\circ \equiv 0(p)$ ,  $(x_k^\circ, p) = 1$

for some  $k > 1$ , without loss of generality take  $k = n$ ,  $x_n^\circ = 1$  and

a suitable coordinate transformation will take  $x^0$  into  $(0, \dots, 0, 1)$  but leave  $\lambda^0 = [1, 0, \dots, 0]$  fixed. Thus we shall work with

$$\begin{aligned} T_* &= T(0, \dots, 0, 1) = T(x^0) \\ A_\gamma &= A_\gamma([1, 0, \dots, 0]) \end{aligned}$$

but our results hold for all  $T(x)$  and  $A_\gamma(\mu)$ . Now  $x \in T_*$  and  $x * A_\gamma$  implies

$$(3) \quad w_1 + p \sum_{i=2}^{n-1} (\mu'_i + \nu_i p) + \mu'_n + \nu_n p \equiv 0 \pmod{p^r}$$

so  $x \in T_*$  and  $x * A(\mu')$  if and only if

$$(4) \quad w_1 + \mu'_n \equiv 0 \pmod{p}.$$

Because of (4) we can define subsets  $T_c$  of  $T_*$  which are in  $A(\mu')$ . At the same time we define families of congruence classes  $A(\mu') \subset A_\gamma$  which we shall need for the lemmas. In the following  $c = 1, \dots, p$ .

$$T_c = \{mx \in T_* \mid x = (cp^{\alpha-\gamma} + x_1 p^{\alpha-\gamma+1}, x_2 p, \dots, x_{n-1} p, 1), \\ x_i \bmod p^{r-1}, m = 1, 2, \dots\}$$

$$M_c = \{A(\mu') \subset A_\gamma \mid \mu'_n + c \equiv 0 \pmod{p}\}$$

$$Q' = \{M_c \mid B(A(\mu'), T_*) = A(\mu') \text{ for some } A(\mu') \in M_c\}$$

$$R' = \{M_c \mid M_c \notin Q'\}$$

$$Q = \cup \{A(\mu') \in M_c \mid M_c \in Q'\}$$

$$R = \cup \{A(\mu') \in M_c \mid M_c \in R'\}$$

$$P = Q \cup R = \{A(\mu') \subset A_\gamma\}$$

$T_c \subset A_0$ ;  $M_c$  is a collection of classes  $A(\mu')$ , etc.

Notice that if  $A(\mu') \in R$  then  $B(A(\mu'), T_*) \neq A(\mu')$ , but the converse is not necessarily true. Also  $T_*$  is the disjoint union

$$T_* = \bigcup_{c=1}^p T_c$$

and  $P$  is the disjoint union of  $Q$  and  $R$ . Hereafter suppose

$$|T_*| < p^r$$

and

$$(0, 0, \dots, 0) \notin T_*.$$

**LEMMA 1.** (a) If  $\mu'_n \equiv -c \pmod{p}$  then  $B(A(\mu'), T_c) = \emptyset$ .

(b) If  $T_*$  covers a  $A(\mu')$  then

$$|T_c| \geq p^{r-1} \text{ and } c + \mu'_n \equiv 0 \pmod{p}.$$

(c) If the  $A(\mu')$  covered are from  $\ell$  distinct  $M_c$ , ( $0 \leq \ell = |Q'| < p$ ) then

$$\begin{aligned} |T_*| &\geq \not\prec p^{\gamma-1} \\ |Q| &= \not\prec p^{n-2} \end{aligned}$$

and

$$(5) \quad |R| = p^{n-1} - \not\prec p^{n-2}.$$

*Proof.* (a) follows from (4).

(b) Define a set  $V_c$ , *not stellar*, by

$$V_c = \{p^\beta y \in T_c \mid \text{if } p^b y \in T_c \text{ then } b \leq \beta, y \text{ } p\text{-primitive}\}.$$

Then

$$|T_c| \geq \sum_{p^\beta y \in V_c} p^\beta \text{ and } B(A(\mu'), T_c) = B(A(\mu'), V_c).$$

Let

$$a = p^{(\gamma-1)(n-2)} = |B(A(\mu'), x)| \text{ for any } p\text{-primitive } x * A(\mu').$$

$$\begin{aligned} |T_c| &\geq \sum_{p^\beta y \in V_c} p^\beta = \sum_{p^\beta y \in V_c} \frac{|B(A(\mu'), p^\beta y)|}{a} = \frac{1}{a} |B(A(\mu'), V_c)| \\ &= \frac{1}{a} |B(A(\mu'), T_c)| = \frac{1}{a} |A(\mu')| = p^{\gamma-1}. \end{aligned}$$

(c) By (a) and (b),  $|T_*| \geq \not\prec p^{\gamma-1}$ . Since  $|M_c| = p^{n-2}$ ,

$$|Q| = \not\prec p^{n-2}.$$

Because  $P$  is the disjoint union of  $Q$  and  $R$ , and

$$|P| = p^{n-1}$$

we have

$$|R| = p^{n-1} - \not\prec p^{n-2}.$$

This completes the proof of Lemma 1.

Of course  $T \setminus T_*$  denotes  $\{x \in T \mid x \notin T_*\}$ .

**LEMMA 2.** (a)  $|A(P, x)| = p^{n-2}$  for any  $x \in T$ . If  $x \in T \setminus T_*$ ,  $y \in T_*$  then

(b)  $|A(P, x) \cap A(P, y)| = p^{n-3}$  and

(c) the number of  $A(\mu') \in R$  with  $x * A(\mu')$  is

$$(6) \quad |A(R, x)| = p^{n-2} - \not\prec p^{n-3}, \not\prec = |Q'|.$$

*Proof.* (a) If  $x \in T$  and  $x * A_\gamma$  then  $(x_2, \dots, x_n, p) = 1$  implies there are  $p^{n-2}$  choices for  $\mu'_2, \dots, \mu'_n$ .

(b) follows from the fact that  $x \not\equiv y \pmod{p}$  and  $A_\gamma$  is fixed.

(c) If  $y \in T_*$  then  $y \in T_c$  for a unique  $c$ . By Lemma 1(a)  $A(P, y) = A(M_c, y) \subset M_c$  and counting shows  $A(P, y) = M_c$ . Now it is easy to

see that  $|A(Q, x)| = \not\prec p^{n-3}$ . Since  $P$  is the disjoint union of  $Q$  and  $R$ ,  $|A(R, x)| = |A(P, x)| - |A(Q, x)| = p^{n-2} - \not\prec p^{n-3}$ . This completes the proof of Lemma 2.

In Theorem 3 if  $\gamma = 2$ ,  $\lambda^\circ = [1, 0, \dots, 0]$ , then  $x \in T$  must satisfy the congruence

$$x_1 + p \sum_2^n \lambda_i x_i \equiv 0 \pmod{p^2}$$

for some  $\lambda_2, \dots, \lambda_n$ . Thus

$$x_1 \equiv 0 \pmod{p}, \quad x_1 = pw_1 \quad \text{for some } w_1,$$

and

$$w_1 + \sum_2^n \lambda_i x_i \equiv 0 \pmod{p}$$

so  $(x_2, \dots, x_n, p) = 1$  and  $x \in A_1$ .

**LEMMA 3.** Suppose  $n \geq 3$  and for each  $\lambda = [1, \lambda_2, \dots, \lambda_n]$  the congruence

$$w_1 + \sum_2^n \lambda_i x_i \equiv 0 \pmod{p}$$

has a solution  $x \in T$ , where  $T$  is a stellar set of points, such that if  $x \in T$  and for some integer  $m$

$$x = m(w_1, x_2, \dots, x_n) \text{ then g.c.d. } (x_2, \dots, x_n, p) = 1.$$

Denote  $\tilde{x} = (x_2, \dots, x_n)$ .

Let

$$T(y_0) = \{my \in T \mid \tilde{y} \equiv \tilde{y}_0(p), \quad m = 1, 2, 3, \dots\} \text{ for some } p\text{-primitive } y_0.$$

Then either (i)  $|T| \geq |T(y_0)| \geq p$  for some  $y_0 \in T$

or (ii)  $|T| \geq p + \max(|T(y)|, 1)$  for all  $y \in T$ .

*Proof.* If  $|T(y_0)| \geq p$  for some  $y_0 \in T$  we are done. Assume  $|T(y)| < p$  for all  $y \in T$ . Then  $T$  is a  $p$ -primitive set since  $p^\beta y \in T$  implies

$$y, 2y, \dots, p^\beta y \in T(y).$$

$T \neq \emptyset$  implies  $T(y_0) \neq \emptyset$  for some  $y_0 \in T$ .

Some calculations show, if  $y \in T \setminus T(y_0)$ , then

$$(a) \quad |A_1 \setminus B(A_1, T(y_0))| = p^{n-1} - |T(y_0)| p^{n-2},$$

$$(b) \quad |B(A_1, y) \setminus \{B(A_1, y) \cap B(A_1, T(y_0))\}| = p^{n-2} - |T(y_0)| p^{n-3}.$$

If  $y^j = (y_1^j, \dots, y_n^j)$ ,  $j = 1, 2$  are two distinct points in  $T \setminus T(y_0)$  then

$$|B(A_1, y^1) \cap B(A_1, y^2)| = \begin{cases} 0 & \text{if } y_i^1 = y_i^2 \text{ for all } i > 1 \\ p^{n-s} & \text{otherwise.} \end{cases}$$

Substituting the above, together with (a) and (b), in

$$\sum_{y \in T \setminus T(y_0)} |B(A_1, y) \setminus \{B(A_1, y) \cap B(A_1, T(y_0))\}| = \sum_{\lambda \in B(\Delta_1, T(y_0))} 1$$

gives

$$|T| - |T(y_0)| \geq p.$$

**3. Proof of Theorem 3.** We prove Theorem 3 by induction on  $\gamma$ . The case  $\gamma = 2$  was settled in Lemma 3 where we noted satisfying the congruences  $(\text{mod } p^2)$  was equivalent to covering  $A_1$ . Similarly satisfying the congruences  $(\text{mod } p^{\gamma+1})$  is equivalent to covering  $A_\gamma$ . The  $\lambda \in A_1$  play a similar role to the  $A_{\gamma-1}(\mu') \subset A_\gamma$ ; (a) and (b) in Lemma 3 play a similar role to (5) and (6) in Theorem 3.

We assume Theorem 3 true for some  $\gamma \geq 2$  and will show it holds for  $\gamma + 1$ . Thus we will be concerned with covering  $A_\gamma$ , and shall consider it in terms of the  $A_{\gamma-1}(\mu') \subset A_\gamma$ . We must distinguish two cases:

*Case 1.*  $p^\gamma > |T_*| \geq p^{\gamma-1}$ .

Recall the families  $Q', R', Q, R$  and  $P$  defined in § 2.  $A(\mu') \in R$  implies

$$B(A(\mu'), T_*) \neq A(\mu')$$

and the induction implies the number of points of  $T$  in  $A(\mu')$  is

$$|T| \geq p^{\gamma-1} + \max(|T_*|, p^{\gamma-2}) \text{ for each } A(\mu') \in T.$$

In other words, at least  $p^{\gamma-1}$  points of  $T \setminus T_*$  are in each  $A(\mu') \in R$ . Combining

$$\sum_{x \in T \setminus T_*} |A(R, x)| = \sum_{A(\mu') \in R} |\{x \in T \setminus T_* \mid x * A(\mu')\}|$$

with (5) and (6) gives

$$|T| - |T_*| \geq p^\gamma.$$

*Case 2.* For all  $x \in T$ ,  $p^{\gamma-1} > |T(x)|$ .

By induction, the cardinality of the subset of points of  $T$  that covers  $A(\mu') \in P$  is greater than or equal to  $p^{\gamma-1} + p^{\gamma-2}$ .

Notice that  $|P| = p^{n-1}$ .

Lemma 2 (a) gives  $|A(P, x)| = p^{n-2}$ .

We have

$$\sum_{x \in T} |A(P, x)| = \sum_{\Delta(\mu') \in P} |\{x \in T \mid x * A(\mu')\}|$$

so that

$$|T| \geq p^r + p^{r-1}.$$

**4. Proof of Theorems 1 and 2.** As remarked earlier, it is sufficient to prove Theorem 2 in order to conclude Theorem 1. Thus we shall prove only Theorem 2. By [2] and [3] we may assume  $n \geq 3$  and  $\alpha \geq 2$ .

We apply Theorem 3 with  $\alpha = \gamma \geq 2$ . Thus we have a result about covering the  $A_{\alpha-1}(\mu) \subset V_\alpha^*$ .

Let  $N = \{A_{\alpha-1}(\mu) \mid A_{\alpha-1}(\mu) \subset V_\alpha^*\}$ . The number of  $A_{\alpha-1}(\mu) \subset V_\alpha^*$  is  $|N| = 1 + p + \dots + p^{n-1}$  and  $|A(N, x)| = 1 + p + \dots + p^{n-2}$  for any  $x \in S$ .

We consider two cases corresponding to those in Theorem 3.

*Case 1.*  $|T_*| \geq p^{\alpha-1}$ .

Let  $M = \{A_{\alpha-1}(\mu) \in N \mid B(A_{\alpha-1}(\mu), T_*) = \emptyset\}$ .

Then

$$|M| = |N| - |A(N, T_*)| = p^{n-1}.$$

By Theorem 3 each  $A_{\alpha-1}(\mu) \in M$  will need at least  $p^{\alpha-1}$  points of  $S \setminus T_*$  to be covered by  $S$ .

If  $x \in S \setminus T_*$ ,  $y \in T_*$  then

$$|A(N, x) \cap A(N, y)| = 1 + p + \dots + p^{n-3}.$$

Thus

$$|A(M, x)| = |A(N, x)| - |A(N, x) \cap A(N, y)| = p^{n-2}.$$

Now

$$\sum_{x \in S \setminus T_*} |A(M, x)| = \sum_{\Delta_{\alpha-1}(\mu) \in M} |\{x \in S \setminus T_* \mid x * A_{\alpha-1}(\mu)\}|$$

so by Theorem 3

$$(|S| - |T_*|)p^{n-2} \geq p^{n-1}p^{\alpha-1}$$

and the result follows.

*Case 2.* For all  $x \in S$ ,  $p^{\alpha-1} > |T(x)|$ .

By Theorem 3, to cover each  $A_{\alpha-1}(\mu) \in N$  will require at least  $p^{\alpha-1} + p^{\alpha-2}$  points of  $S$ . We have

$$\sum_{x \in S} |A(N, x)| = \sum_{\Delta_{\alpha-1}(\mu) \in N} |\{x \in S \mid x * A_{\alpha-1}(\mu)\}|.$$



$|S|(1 + p + \cdots + p^{n-2}) \geq (1 + p + \cdots + p^{n-1})(p^{\alpha-1} + p^{\alpha-2})$  and the theorem follows.

**5. Bounds.** Our bounds in Theorem 2, 3 and Lemma 1 are the best possible in the sense that we can exhibit sets of minimum cardinality which satisfy the conditions. For Theorem 2 let

$$S = \{(x, 1, 0, \dots, 0) \mid 1 \leq x \leq p^\alpha\} \cup \{(1, px, 0, \dots, 0) \mid 1 \leq x \leq p^{\alpha-1}\}.$$

Then

$$|S| = p^\alpha + p^{\alpha-1}$$

and  $S$  satisfies all the congruences. Notice that  $S$  is composed of  $p + 1$  disjoint sets  $T(x)$ , each of cardinality  $p^{\alpha-1}$ . We expect this because of the strict inequality in Case 2 of the proof of Theorem 2, as compared with the inequality in Case 1.

For Theorem 3 we exhibit a  $T(x^\circ)$  of cardinality  $p^{r-1}$  and a  $T$  of cardinality  $p^{r-1} + p^{r-2}$  containing no  $T(x)$  of cardinality greater than  $p^{r-2}$ . Without loss of generality, let  $\lambda^\circ = [1, 0, \dots, 0]$ .

$$\begin{aligned} T(x^\circ) &= \{(xp, 0, \dots, 0, 1) \mid 1 \leq x \leq p^{r-1}\} \\ T &= \{(0, \dots, 0, xp + c, 1) \mid 1 \leq x \leq p^{r-2}, 1 \leq c \leq p\} \cup \\ &\quad \{(0, \dots, 0, 1, xp) \mid 1 \leq x \leq p^{r-2}\}. \end{aligned}$$

All the congruences of Theorem 3 are clearly satisfied by each of these sets.

Finally for Lemma 1 let  $c$  be fixed and

$$T_c = \{(p^{\alpha-r_c} + p^{\alpha-y+1}x, 0, \dots, 0, 1) \mid 1 \leq x \leq p^{r-1}\}.$$

Then

$$|T_c| = p^{r-1}$$

and

$$B(\Lambda(\mu'), T_c) = \Lambda(\mu') \text{ for all } \Lambda(\mu') \in M_c.$$

The author wishes to thank Dr. G. K. White for his advice and encouragement in the preparation of this paper.

#### BIBLIOGRAPHY

1. J. W. S. Cassels, *On the subgroups of infinite abelian groups*, J. London, Math. Soc. **33** (1958), 281-4.
2. C. A. Rogers, *The number of lattice points in a star body*, J. London, Math. Soc. **26** (1951) 307-310.

3. G. K. White, *On subgroups of fixed index*, Pacific J. Math. **28** (1969), 225-232.

Received June 16, 1969.

UNIVERSITY OF BRITISH COLUMBIA  
VANCOUVER