Pacific Journal of Mathematics

ON SUBGROUPS OF PRIME POWER INDEX

Langdon Frank Harris

Vol. 35, No. 1 September 1970

PACIFIC JOURNAL OF MATHEMATICS
Vol. 35, No. 1, 1970

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 $x, 2x, \cdots, mx \in S$. Let p^α 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

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

with lattice points $(x_1, x_2, \cdots, x_n)$ 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^β, $1 < p^\beta < p^\alpha$, and S is a stellar set as above, then

$$|S| \geqq p^\alpha + p \qquad \text{if } \alpha \geqq 2$$
$$|S| \geqq p + 1 \qquad \text{if } \alpha = 1 .$$

($|S|$ is the cardinal number of the set S.)
We improve this to get

THEOREM 1. *Suppose p^α is fixed, G is an abelian group without elements of order p^β, $1 < p^\beta < p^\alpha$, 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*

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

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

Let g.c.d. $(a_1, \cdots, a_k)$ denote the greatest common divisor of $a_1, \cdots, a_k$. Let V_α denote the Cartesian product of $n \geqq 1$ copies of Z_{p^α}, the residue class ring modulo p^α. Let Λ_0 denote the free abelian group of rank n. An n-tuple (in Λ_0 or in V_α) 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_α^* denote the set of those p-primitive elements of V_α whose first p-prime coefficient is 1.

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

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

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

of index p^α in Λ_0 we may identify the two. Thus we write $x \in \lambda$ to mean $\lambda \cdot x \equiv 0\,(p^\alpha)$.

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

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

C. A. Rogers [2] has proved Theorem 2 for the case $\alpha = 1$. Two n-tuples λ and μ are said to be *congruent* modulo p^γ if each component of λ is congruent modulo p^γ to the corresponding component of μ. If λ and μ are p-primitive elements of Λ_0 and $\lambda \not\equiv k\mu(p)$ for all p-prime k then

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

is a subgroup of index p^α in Λ_0, so for $\alpha \geqq 2$ there are many more subgroups of index p^α in Λ_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 Λ_0 let

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

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

THEOREM 3. *Suppose that* $\alpha \geqq \gamma \geqq 2$, $n \geqq 3$ *and* $\lambda^0 \in V_\alpha^*$ *are fixed. If for each* λ *such that* $\lambda = \lambda^0(p)$ *and* $\lambda \in V_\alpha^*$ *the congruence* $\lambda \cdot x \equiv 0\,(p^\gamma)$ *has a solution* $x \in T$ *where* T *is a stellar subset of* Λ_0 *satisfying* $T \cap p^\alpha \Lambda_0 = \varnothing$ *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*

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

or (ii) $|T| \geqq p^{\gamma-1} + \max(|T(x)|, p^{\gamma-2})$ *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 $\alpha \geqq \gamma$. Let $\mu \in V_\alpha^*$ and define

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

Then
$$A_\gamma(\mu) \cap A_{\gamma-1}(\nu) = \varnothing \quad \text{if } \mu \not\equiv \nu\,(p^{\alpha-\gamma})$$
$$A_\gamma(\mu) \supset A_{\gamma-1}(\nu) \quad \text{if } \mu \equiv \nu\,(p^{\alpha-\gamma})\,.$$

Thus

$$(*) \qquad A_\gamma(\mu) = \cup\{A_{\gamma-1}(\mu + \mu'\, p^{\alpha-\gamma}) \mid 1 \leqq \mu_i' \leqq p\}\,.$$

Since each $A_\gamma(\mu)$ is a set of $\lambda \in V_\alpha^*$ and each λ 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

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

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 $\lambda^\circ = [1, 0, \cdots, 0]$ 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

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

This implies

$$\lambda^\circ \cdot x \equiv w_1\, p^{\alpha-\gamma}\,(p^\alpha) \qquad \text{for some } w_1$$
$$w_1 + \lambda \cdot x \equiv 0\,(p^\gamma)$$
$$(1) \qquad w_1 + \sum_2^n \lambda_i\, x_i \equiv 0\,(p^\gamma)\,.$$

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

$$(2) \qquad w_1 + \sum_2^n (\mu_i' + \nu_i\, p)\, x_i \equiv 0\,(p^\gamma)$$

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

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

for some $k > 1$, without loss of generality take $k = n$, $x_n^0 = 1$ and a suitable coordinate transformation will take x^0 into $(0, \cdots, 0, 1)$ but leave $\lambda^\circ = [1, 0, \cdots, 0]$ fixed. Thus we shall work with

$$T_* = T(0, \cdots, 0, 1) = T(x^0)$$
$$\Lambda_\gamma = \Lambda_\gamma([1, 0, \cdots, 0])$$

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

$$w_1 + p \sum_2^{n-1} (\mu_i' + \nu_i p) + \mu_n' + \nu_n p \equiv 0 \ (p^\gamma) \tag{3}$$

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

$$w_1 + \mu_n' \equiv 0 \ (p) \ . \tag{4}$$

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

$$T_c = \{mx \in T_* \mid x = (cp^{\alpha-\gamma} + x_1 p^{\alpha-\gamma+1}, \ x_2 p, \cdots, x_{n-1} p, 1), \ x_i \bmod p^{\gamma-1}, \ m = 1, 2, \cdots\}$$
$$M_c = \{\Lambda(\mu') \subset \Lambda_\gamma \mid \mu_n' + c \equiv 0 \ (p)\}$$
$$Q' = \{M_c \mid B(\Lambda(\mu'), T_*) = \Lambda(\mu') \text{ for some } \Lambda(\mu') \in M_c\}$$
$$R' = \{M_c \mid M_c \notin Q'\}$$
$$Q = \cup \{\Lambda(\mu') \in M_c \mid M_c \in Q'\}$$
$$R = \cup \{\Lambda(\mu') \in M_c \mid M_c \in R'\}$$
$$P = Q \cup R = \{\Lambda(\mu') \subset \Lambda_\gamma\}$$

$T_c \subset \Lambda_0$; M_c is a collection of classes $\Lambda(\mu')$, etc.
Notice that if $\Lambda(\mu') \in R$ then $B(\Lambda(\mu'), T_*) \neq \Lambda(\mu')$, 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

$$|T_*| < p^\gamma$$

and

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

LEMMA 1. (a) *If* $\mu_n' \not\equiv -c \ (p)$ *then* $B(\Lambda(\mu'), T_c) = \varnothing$.
(b) *If* T_* *covers a* $\Lambda(\mu')$ *then*

$$|T_c| \geqq p^{\gamma-1} \ \textit{and} \ c + \mu_n' \equiv 0 \ (p) \ .$$

(c) *If the* $\Lambda(\mu')$ *covered are from* ℓ *distinct* M_c, $(0 \leqq \ell = |Q'| < p)$ *then*

$$|T_*| \geqq \ell\, p^{\gamma-1}$$
$$|Q| = \ell\, p^{n-2}$$

and

$$(5) \qquad |R| = p^{n-1} - \ell\, p^{n-2} .$$

Proof. (a) follows from (4).

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

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

Then

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

Let

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

$$|T_c| \geqq \sum_{p^\beta y \in V_c} p^\beta = \sum_{p^\beta y \in V_c} \frac{|B(\Lambda(\mu'), p^\beta y)|}{a} = \frac{1}{a} |B(\Lambda(\mu'), V_c)|$$
$$= \frac{1}{a} |B(\Lambda(\mu'), T_c)| = \frac{1}{a} |\Lambda(\mu')| = p^{\gamma-1} .$$

(c) By (a) and (b), $|T_*| \geqq \ell\, p^{\gamma-1}$. Since $|M_c| = p^{n-2}$,

$$|Q| = \ell\, p^{n-2} .$$

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

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

we have

$$|R| = p^{n-1} - \ell\, p^{n-2} .$$

This completes the proof of Lemma 1.

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

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

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

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

$$(6) \qquad |A(R, x)| = p^{n-2} - \ell\, p^{n-3}, \ell = |Q'| .$$

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

(b) follows from the fact that $x \not\equiv y\ (p)$ and Λ_γ 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 $|A(Q, x)| = \not{p}^{n-3}$. Since P is the disjoint union of Q and R, $|A(R, x)| = |A(P, x)| - |A(Q, x)| = p^{n-2} - \not{p}^{n-3}$. This completes the proof of Lemma 2.

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

$$x_1 + p\sum_2^n \lambda_i x_i \equiv 0 \ (p^2)$$

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

$$x_1 \equiv 0 \ (p), \ x_1 = pw_1 \qquad \text{for some } w_1 \ ,$$

and

$$w_1 + \sum_2^n \lambda_i x_i \equiv 0 \ (p)$$

so $(x_2, \cdots, x_n, p) = 1$ and $x * A_1$.

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

$$w_1 + \sum_2^n \lambda_i x_i \equiv 0 \ (p)$$

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

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

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

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

Then either (i) $|T| \geqq |T(y_0)| \geqq p$ *for some* $y_0 \in T$
or (ii) $|T| \geqq p + \max(|T(y)|, 1)$ *for all* $y \in T$.

Proof. If $|T(y_0)| \geqq p$ 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

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

$T \neq \varnothing$ implies $T(y_0) \neq 0$ for some $y_0 \in T$.
Some calculations show, if $y \in T \backslash T(y_0)$, then

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

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

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

$$|B(\Lambda_1, y^1) \cap B(\Lambda_1, y^2)| = \begin{cases} 0 & \text{if } y_i^1 = y_i^2 \text{ for all } i > 1 \\ p^{n-3} & \text{otherwise} . \end{cases}$$

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

$$\sum_{y \in T \backslash T(y_0)} |B(\Lambda_1, y) \backslash \{B(\Lambda_1, y) \cap B(\Lambda_1, T(y_0))\}| = \sum_{\lambda \notin B(\Lambda_1, T(y_0))} 1$$

gives

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

3. **Proof of Theorem 3.** We prove Theorem 3 by induction on γ. The case $\gamma = 2$ was settled in Lemma 3 where we noted satisfying the congruences (mod p^2) was equivalent to covering Λ_1. Similarly satisfying the congruences (mod $p^{\gamma+1}$) is equivalent to covering Λ_γ. The $\lambda \in \Lambda_1$ play a similar role to the $\Lambda_{\gamma-1}(\mu') \subset \Lambda_\gamma$; (a) and (b) in Lemma 3 play a similar role to (5) and (6) in Theorem 3.

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

Case 1. $p^\gamma > |T_*| \geqq p^{\gamma-1}$.
Recall the families Q', R', Q, R and P defined in § 2. $\Lambda(\mu') \in R$ implies

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

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

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

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

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

with (5) and (6) gives

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

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 $\Lambda(\mu') \in P$ 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

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

so that

$$|T| \geqq p^{\gamma} + p^{\gamma-1} .$$

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 $n \geqq 3$ and $\alpha \geqq 2$.

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

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

We consider two cases corresponding to those in Theorem 3.

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

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

Then

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

By Theorem 3 each $\Lambda_{\alpha-1}(\mu) \in M$ 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

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

Thus

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

Now

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

so by Theorem 3

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

and the result follows.

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

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

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

$|S|(1 + p + \cdots + p^{n-2}) \geqq (1 + p + \cdots + p^{n-1})(p^{\alpha-1} + p^{\alpha-2})$ 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

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

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 $p^{\gamma-1}$ and a T of cardinality $p^{\gamma-1} + p^{\gamma-2}$ containing no $T(x)$ of cardinality greater than $p^{\gamma-2}$. Without loss of generality, let $\lambda^{\circ} = [1, 0, \cdots, 0]$.

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

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

Finally for Lemma 1 let c be fixed and

$$T_c = \{(p^{\alpha-\gamma_c} + p^{\alpha-y+1}x, 0, \cdots, 0, 1) \mid 1 \leqq x \leqq p^{\gamma-1}\} .$$

Then

$$|T_c| = p^{\gamma-1}$$

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

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 35, No. 1 September, 1970