SOME "ANZAHL" THEOREMS FOR GROUPS OF PRIME-POWER ORDERS

BY LOO-KENG HUA (華羅庚) AND HSIO-FU TUAN (段學復).

In the theory of p-groups, or groups whose orders are powers of a prime p, there are a number of the so-called "Anzahl" theorems which relate to the number of sub-groups with a certain property. We shall define a group $\mathfrak{G}$ of order p^n as of rank δ, if the highest order of the elements of $\mathfrak{G}$ is equal to $p^{n-\delta}$. By means of this notion the "Anzahl" theorem due to Miller can be restated as follows:

If $\mathfrak{G}$ is a group of order $p^n (p \geq 3, n \geq 3)$ of rank ≥ 1, then the number of sub-groups of order $p^m (1 < m < n)$ of rank 0 is congruent to zero, mod p.

The main object of the present paper is to establish the following theorem:

If $\mathfrak{G}$ is a group of order $p^n (p \geq 3, n \geq 5)$ of rank ≥ 2, then the number of sub-groups of order $p^m (2 < m < n-1)$ of rank 0 is congruent to zero, mod p^2, and the number of sub-groups of order $p^m (3 < m < n)$ of rank 1 is congruent to zero, mod p.

In the proof of this theorem we employ mathematical induction over n in two ways, according to whether $\mathfrak{G}$ does not contain or actually contains a sub-group of index p of rank 1. In the first case, we establish the theorem by a direct application of the enumeration principle due to P. Hall.(1) In the second case, we shall make use of the following theorem which seems to have some interests in itself.

---

(1) *Proc. London Math. Soc.* (2) **36** (1933), 29-95.

If $\mathfrak{G}$ is a group of order $p^n (p \geq 3, n \geq 5)$ of rank 2, then $\mathfrak{G}$ has one and only one sub-group of index p of rank 2.(2)

In the following pages, we shall always denote by p an odd prime number.

§1. Throughout this section, $\mathfrak{G}$ always denotes a group of rank 2. It contains a (normal) sub-group $\mathfrak{M}_1$ of index p of rank 1. It is known that $\mathfrak{M}_1$ is of the form(3)

(1) $$\mathfrak{M}_1 = \{ A_1, A_2 \}, \quad A_1^{p^{n-2}} = 1, \quad A_2^{p} = 1, \quad (A_1 A_2) = A_1^{p^{n-3+\delta}}$$

where $\delta = 1$ or 0, for $n \geq 4$. Evidently

$$(A_1^{a_1} A_2^{a_2})^p = A_1^{a_1 p}.$$

Let B be any element of $\mathfrak{G}$ but not in $\mathfrak{M}_1$, then $\mathfrak{G} = \{\mathfrak{M}_1, B\}$. Since B^p belongs to $\mathfrak{M}_1$ and the p-th power of each element of $\mathfrak{M}_1$ belongs to the central of $\mathfrak{M}_1$, we have then

$$A_1^p B^p = B^p A_1^p.$$

Let

$$B^{-1} A_1 B = A_1^{a_1} A_2^{a_2}.$$

Then

$$B^{-1} A_1^p B = A_1^{a_1 p}$$

and

$$A_1^p = B^{-p} A_1^p B^p = A_1^{a_1^p p}.$$

Therefore

(2) The proofs of Miller's and Kulakoff's "Anzahl" theorems as given by Hall (loc. cit.) by the application of his enumeration principle both depend essentially on an analogous result, namelf, If $\mathfrak{G}$ is a group of order $p^n (p \geq 3, n \geq 3)$ of rank 1, then $\mathfrak{G}$ has one and only one sub-group of index p of rank 1.

(3) See, for example, H. Zassenhaus, *Lehrbuch der Gruppentheorie* I (1937), 114.

$$a_1^p \equiv 1 \pmod{p^{n-3}}.$$

Consequently, for $n \geq 5$,

$$a_1 \equiv 1 \pmod{p^{n-4}}.$$

Thus the commutator (A_1, B) of order $\leq p^2$, and can be written as

(2) $$(A_1, B) = A_1^{\lambda p^{n-4}} A_2^{\mu}.$$

Consequently we have

(3) $$(A_1^p, B) = A_1^{\lambda p^{n-3}}$$

and

(4) $$(A_1^{p^2}, B) = 1.$$

Since B^p belongs to $\mathfrak{M}_1$, by (1) and (4), we have, for $n \geq 5$

(5) $$(A_2, B) = A_1^{p^{n-3} \nu}.$$

Using mathematical induction, we can easily obtain

$$(B A_1)^e = B^e A_1^e A_1^{p^{n-4} \lambda c(e)} A_2^{d(e)} \quad (\text{for } e > 0),$$

where

$$c(e) \equiv \tfrac{1}{2} e(e-1) \pmod{p}$$

and $d(e)$ is a certain integer depending on e, since

$$(A_1, B^e) = A_1^{\lambda e_1 p^{n-4}} A_2^{e_2} \quad e_1 \equiv e \pmod{p}.$$

In particular, for $p = e$, we have

$$(B A_1)^p = B^p A_1^p A_1^{p^{n-3} a} A_2^b$$

The right hand side belongs to $\mathfrak{M}_1$, and therefore

(6) $$(B A_1)^{p^2} = B^{p^2} A_1^{p^2}.$$

Further

$$(B A_2)^p = B^p A_2^p (A_2, B)^{\frac{1}{2} p (p-1)} = B^p.$$

Since B is any element which belongs to $\mathfrak{G}$, but not to $\mathfrak{M}_1$, we can easily obtain that

$$(B A_1^s A_2^t)^{p^2} = B^{p^2} A_1^{s p^2} \tag{7}$$

LEMMA. *For $p \geq 3$ and $n \geq 5$, in a group $\mathfrak{G}$ of order p^n of rank 2:*

(i) ~~*There is one and only one sub-group of index p of rank 2;*~~

(ii) *There is no sub-group of index p of rank ≥ 3;*

(iii) *The number of sub-groups of index p of rank 1 is congruent to zero,* mod p; *and*

(iv) *The number of cyclic sub-groups of order $p^m (3 \leq m \leq n-2)$ is p^2.*

Proof. There exists an element B of $\mathfrak{G}$, not in $\mathfrak{M}_1$, of order $\leq p^2$. In fact, if B is an element of order $p^m (2 < m \leq n-2)$ belonging to $\mathfrak{G}$, but not to $\mathfrak{M}_1$, then

$$B'^{p} = A_1^{p^{n-m-1} a} A_2^b \text{ and } B'^{p^2} = A_1^{p^{n-m} a}.$$

Let $B = B' A_1^{-p^{n-m-2} a}$. Thus, by (6)

$$B^{p^2} = B'^{p^2} A_1^{-p^{n-m} a} = 1.$$

We have $\mathfrak{G} = \{ \mathfrak{M}_1, B \} = \{ A_1, A_2, B \}$. More precisely,

$$B^\mu A_1^{\nu_1} A_2^{\nu_2}, \quad 0 \leq \mu < p, \quad 0 \leq \nu_1 < p^{n-2}, \quad 0 \leq \nu_2 < p,$$

give p^n different elements of $\mathfrak{G}$. We shall prove that

$$B^\mu A_1^{p \nu_1'} A_2^{\nu_2}, \quad 0 \leq \mu < p, \quad 0 \leq \nu_1' < p^{n-3}, \quad 0 \leq \nu_2 < p, \tag{8}$$

form a group $\mathfrak{M}_1'$, of index p of rank 2. By (1), (3) and (5), (8) evidently form a group which contains an element A_1^p of order p^{n-3}.

Further, by (7), no element of (8) is of order p^{n-2}. Since (8) contains all elements of order $\leq p^{n-3}$ of $\mathfrak{G}$, the uniqueness in (i) and the result in (ii) follow immediately.

It is known that the number of sub-groups of index p of $\mathfrak{G}$ is congruent to 1 (mod p). We have shown that one of them is of rank 2 and none of them is of rank o and ≥ 3. Therefore the number of sub-groups of index p of rank 1 is congruent to zero, mod p.

The elements of order p^m $(m \geq 3)$ are of the form

$$B^{\mu} A_1^{p^{n-2-m}\lambda_1} A_2^{\lambda_2}, \qquad p \nmid \lambda_1$$

Thus there are $p^2\varphi(p^m)$ such elements and therefore the group $\mathfrak{G}$ has p^2 cyclic sub-groups of order p^m.

§2. **Enumeration Principle**[4]. Let $\mathfrak{G}$ be any p-group and let $\mathfrak{D}$ be its principal sub-group of index p^d. Let $\mathfrak{M}_\alpha$ denote a typical major sub-group of index p^α of $\mathfrak{G}$ with $o \leq \alpha \leq d$ (naturally $\mathfrak{M}_d = \mathfrak{D}$ and $\mathfrak{M}_o = \mathfrak{G}$) Let $\mathfrak{N}$ be any set of sub-groups of $\mathfrak{G}$. Let $n(\mathfrak{M}_\alpha)$ denote the number of members of $\mathfrak{N}$ which belong to $\mathfrak{M}_\alpha$. Then

$$n(\mathfrak{M}_0) - \sum_{(\mathfrak{M}_1)} n(\mathfrak{M}_1) + p \sum_{(\mathfrak{M}_2)} n(\mathfrak{M}_2) - p^3 \sum_{(\mathfrak{M}_3)} n(\mathfrak{M}_3) + \cdots$$
$$+ (-1)^d p^{\frac{1}{2}d(d-1)} n(\mathfrak{M}_d) = 0,$$

where the sum $\sum_{(\mathfrak{M}_\alpha)}$ being taken over the $\Phi_{d,\alpha}$ sub-groups $\mathfrak{M}_\alpha$ of $\mathfrak{G}$ and

$$\Phi_{d,\alpha} = \frac{(p^d - 1) \cdots (p^d - p^{\alpha-1})}{(p^\alpha - 1) \cdots (p^\alpha - p^{\alpha-1})}.$$

THEOREM 1. *If $\mathfrak{G}$ is a group of prime-power order $p^n (p \geq 3, n \geq 5)$ of rank ≥ 2, then the number of sub-groups of order $p^m (4 \leq m \leq n-1)$ of rank 1 is congruent to zero,* mod p.

Proof. For $m = n - 1$, there are two cases to distinguish, according to whether $\mathfrak{G}$ does not contain or actually contains a maximal sub-group of rank 1. The first case is trivial. In the second case, it is an immediate consequence of the lemma (iii). Therefore the theorem is true for $m = n - 1$. The theorem is thus true for $n = 5$.

(4) loc. cit.

Now we can assume that $m < n-1$. Take $\mathfrak{N}$ to be the set of all sub-groups of order $p^m(m \geq 4)$ of rank 1. By enumeration principle, we have

$$n(\mathfrak{M}_0) \equiv \sum_{(\mathfrak{M}_1)} n(\mathfrak{M}_1) \pmod p.$$

First, let $\mathfrak{G}$ have no maximal sub-group of rank 1, then since $m < n-1$, we have, by the hypothesis of induction, that

$$n(\mathfrak{M}_1) \equiv 0 \pmod p$$

for each $\mathfrak{M}_1$, and hence

$$n(\mathfrak{M}_0) \equiv 0 \pmod p.$$

Secondly, let $\mathfrak{G}$ have a maximal sub-group of rank 1, then $\mathfrak{G}$ is of rank 2. By the lemma, $\mathfrak{G}$ has one maximal sub-group of rank 2, and others, $\varphi_{d,1} - 1$ in number $(\varphi_{d,1} - 1 \equiv 0 \pmod p)$, are all of rank 1. The induction is completed by the hypothesis of induction and the fact that every group of rank 1 contains a unique sub-group of order p^m of rank 1(5).

THEOREM 2. *Let $\mathfrak{G}$ be a group of order p^n $(p \geq 3, n \geq 5)$ of rank ≥ 2, then the number of cyclic sub-groups of order $p^m(3 \leq m \leq n-2)$ of $\mathfrak{G}$ is congruent to zero,* mod p^2.

Proof. For $m = n-2$, there are two cases to distinguish, according to whether $\mathfrak{G}$ does not contain or actually contains a maximal sub-group of rank 1. For the first case, the truth is evident. For the second case, $\mathfrak{G}$ is of rank 2, the lemma (iv) tells the truth. The theorem is thus true for $n = 5$.

Now we can assume that $m < n-2$. Take $\mathfrak{N}$ to be the set of all cyclic sub-groups of order $p^m(m \geq 3)$. By enumeration principle, we have

$$n(\mathfrak{M}_0) \equiv \sum_{(\mathfrak{M}_1)} n(\mathfrak{M}_1) - p \sum_{(\mathfrak{M}_2)} n(\mathfrak{M}_2) \pmod{p^2}.$$

First, let $\mathfrak{G}$ have no maximal sub-group of rank 1, then, since $m < n-2$, we have, by the hypothesis of induction, that

(5) See footnote (2).

$$n(\mathfrak{M}_1) \equiv 0 \pmod{p^2} \quad \text{for each } \mathfrak{M}_1$$

Further $\mathfrak{M}_2$ cannot be cyclic, hence, by Miller's theorem,

$$n(\mathfrak{M}_2) \equiv 0 \pmod{p} \quad \text{for each } \mathfrak{M}_2.$$

Thus $n(\mathfrak{M}_0) \equiv 0 \pmod{p^2}$.

Secondly, let $\mathfrak{G}$ have a maximal sub-group of rank 1, then $\mathfrak{G}$ is of rank 2, and the theorem follows from lemma (iv)

§3. For $p = 2$, the theorems are false. In fact, we have the following "Gegenbeispiel". The group

$$A^{2^{n-2}} = 1, \quad B^4 = 1, \quad B^{-1}AB = A^{-1}, \quad n \geq 5$$

of order 2^n has only one cyclic sub-group (A) of order 2^{n-2}, since $(A^{\lambda}B)^4 = B^4 = 1$, and has only one sub-group (A, B^2) of order 2^{n-1} of rank 1.

The restriction on m and n in the theorems also can not be improved as is shown by the following "Gegenbeispiel":

$$A_1^{p^{n-2}} = A_2^{p^2} = 1, \quad (A_1, A_2) = 1.$$

(Received 5, May, 1939)

Added 1, June, 1939. It is very easy to deduce from the lemma that the number of solutions of

$$x^{p^m} = 1 \qquad , m \geq 3$$

for x belonging to a group of rank 2, is divisible by p^{m+2}. Basing on this fact we can generalize a result due to Kulakoff, to the following form

THEOREM 3. *If* $\mathfrak{G}$ *is a group of order* p^n $(n \geq 5)$ *and rank* ≥ 2, *then the number of solutions of* $x^{p^m} = 1$ $(1 < m < n-1)$ *is divisible by* p^{m+2}.

Department of Mathematics
National Tsing Hua University