EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 3, No. 1, 2010, 13-15
ISSN 1307-5543 – www.ejpam.com

Wreath Products, Sylow's Theorem and Fermat's Little Theorem

B.Sury

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore - 560 059, India.

Abstract. The assertion that the number of p-Sylow subgroups in a finite group is $\equiv 1 \bmod p$, begs the natural question whether one may obtain the power a^{p-1} (for any $(a,p)=1$) as the number of p-Sylow subgroups in some group naturally. Indeed, it turns out to be so as we show below. The construction involves wreath products of groups. Using wreath products, a different generalization of Euler's congruence (and, a fortiori, of Fermat's little theorem) was obtained in [1].

2000 Mathematics Subject Classifications: 20D20, 20D60

Key Words and Phrases: Wreath Product, Sylow's Theorems

---

1. Result

Given two groups A and B, recall the restricted wreath product of A by B (written $A \wr B$). This is the semidirect product group $B \propto \tilde{A}$ where $\tilde{A} = \oplus_{b \in B} A_b$ with each $A_b = A$ and B acts on the indexing set B of $\tilde{A}$ by right multiplication. We write any element of $A \wr B$ in a canonical form as $\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r)\tau(b)$ where $a_i \in A; b_i, b \in B$. Thus, two elements $\sigma_{a_1}(b_1)$ and $\sigma_{a_2}(b_2)$ commute if $b_1 \neq b_2$. Also, the product $\sigma_{a_1}(b)\sigma_{a_2}(b) = \sigma_{a_1a_2}(b)$. Finally, $\tau(b)\sigma_a(c)\tau(b)^{-1} = \sigma_a(cb)$. We prove:

Theorem 1. *Let $|B| = p$, a prime and, $(|A|,p) = 1$. Then, the number of p-Sylow subgroups in the wreath product $A \wr B$ is $|A|^{p-1}$. Thus, $|A|^{p-1} \equiv 1$ mod p.*

To prove the theorem, we shall use a lemma on the wreath product $A \wr B$ of two arbitrary finite groups. Let us denote by C the subgroup

$$C = \{\sigma_a(b_1)\cdots\sigma_a(b_n) : a \in A\}$$

where $B = \{b_1, \cdots, b_n\}$. Note that all the elements $\tau(b)$ for $b \in B$ commute element-wise with this subgroup.

Email address: `sury@isibang.ac.in` (B. Sury)

Lemma 1. *Let A, B be finite groups. Then, the normalizer of the subgroup B in $A \wr B$ equals $C \oplus B$.*

Proof. Indeed, if $\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r)\tau(b_0)$ is in the normalizer of B, we have for each $b \in B$, some $b' \in B$ so that

$$\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r)\tau(b_0)\tau(b) = \tau(b')\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r)\tau(b_0)$$
$$= \sigma_{a_1}(b_1 b')\cdots\sigma_{a_r}(b_r b')\tau(b' b_0).$$

So $b_0 b b_0^{-1} = b'$ and

$$\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r) = \sigma_{a_1}(b_1 b')\cdots\sigma_{a_r}(b_r b') = \sigma_{a_1}(b_1 b_0 b b_0^{-1})\cdots\sigma_{a_r}(b_r b_0 b b_0^{-1}).$$

As b can take any value in B, and $b_i(b_0 b_0^{-1})$; $i \leq r$ are distinct elements, we must have $B = \{b_1, \cdots, b_r\}$. Moreover, looking at a b such that $b_i(b_0 b_0^{-1}) = b_j$, we must have $a_i = a_j$. Thus, $\sigma_{a_1}(b_1)\cdots\sigma_{a_r}(b_r) \in C$. This proves the lemma.

Proof. [Theorem 1] Here, since p is the highest power of p dividing the order of $A \wr B$, the subgroup B is a p-Sylow subgroup. By lemma 1, the normalizer $N(B)$ of B has order equal to $p|A|$. Since $|A \wr B| = p|A|^p$, we have $[A \wr B : N(B)] = |A|^{p-1}$. By the second Sylow theorem, the number of p-Sylow subgroups equals the index of the normalizer. By the third Sylow theorem, this number is congruent to 1 mod p.

Lemma 2. *Let A, B be finite solvable groups of orders a, b with $(a, b) = 1$. Then, the subgroups of order b in $A \wr B$ are conjugate and, are a^{b-1} in number.*

Proof. If G is a solvable group of order mn, with $(m, n) = 1$, then it is well-known that G has subgroups of order m which are pairwise conjugate. Now $A \wr B$ has $\tilde{A}$ as a normal subgroup and the quotient is isomorphic to B. As A is solvable, so is the group $\tilde{A}$. Hence, $A \wr B$ is solvable as both $\tilde{A}$ and B are solvable. Thus, the subgroups of order b in it are pairwise conjugate and are, thus, $[A \wr B : N(B)]$ in number. This index is $a^b b/ab = a^{b-1}$.

2. Remarks

The wreath product of finite groups was considered in [1] also, where a different generalization of Euler's congruence dropped out as a byproduct. A particular case is :

Let A, B be finite abelian groups of orders a, b respectively. Then, the number of conjugacy classes in the wreath product $A \wr B$ is $\frac{1}{b}\sum_{s,t \in B} a^{[B:<s,t>]}$. In particular, when B is cyclic, this number is $\frac{1}{b}\sum_{s,t=1}^{b} a^{(b,s,t)}$.

From this, one can easily deduce Euler's congruence $a^{\phi(n)} \equiv 1$ mod n for $(a, n) = 1$. In fact, the expression in the lemma can be re-written as

$$\frac{1}{n}\sum_{s,t=1}^{n} a^{(n,s,t)} = \sum_{d|n} \phi(n/d) \frac{\sum_{l|d} a^l \phi(d/l)}{d}.$$

References

[1] I.Erovenko & B.Sury, *Commutativity degree of wreath product of finite abelian groups*, Bulletin of the Australian Math. Soc., Vol. 77 (2008) P.31-36.