COUNTING \( p \)-SUBGROUPS

ERNST SNAPPER

Abstract. There are many theorems which state that the number of \( p \)-subgroups of a finite group, where these \( p \)-subgroups satisfy varying conditions, is congruent 1 modulo \( p \). We derive here a simple theorem which has all these special theorems as corollaries.

1. Introduction. \( G \) stands for a finite group of order \( g \) and \( p \) for a prime number dividing \( g \). The theorem, mentioned in the abstract, is:

**Theorem.** Let \( K \) be a subgroup of \( G \) of order \( p^m \). If \( m \leq n \) and \( p^n \) divides \( g \), the number of subgroups of \( G \) of order \( p^n \) which contain \( K \) is congruent 1 modulo \( p \).

Several special cases of the theorem occur in the literature. For example, if \( m = 0 \), one obtains that the number of subgroups of \( G \) of order \( p^n \) is congruent 1 modulo \( p \); or, if \( n \) is chosen as large as possible, one obtains that the number of Sylow \( p \)-subgroups of \( G \) which contain \( K \) is congruent 1 modulo \( p \) [1, p. 152].

2. The proof of the theorem. The theorem is trivial when \( n = m \).

Case 1. \( n = m + 1 \). Suppose that \( K \) is contained in \( t \) subgroups \( H_1, \ldots, H_t \) of \( G \) of order \( p^{m+1} \). Since \( p^n \) divides \( g \), \( t \geq 1 \), and it is well known that \( K \) is normal in each \( H_i \). Consequently, the groups \( H_i \) are subgroups of the normalizer \( N \) of \( K \) in \( G \), whence \( t \) is the number of subgroups of order \( p \) of \( N/K \). Clearly, \( p^{[N:K]} \) and there are of course several elementary ways of showing that the number of subgroups of order \( p \) of a group whose order is divisible by \( p \) is congruent 1 modulo \( p \).

Case 2. \( n = m + 1 + s \), where \( s \geq 1 \). We make the induction hypothesis that the theorem has been proved for \( n = m, m + 1, \ldots, m + s \). Let \( L_1, \ldots, L_t \) be the subgroups of \( G \) of order \( p^{m+s} \) which contain \( K \), and \( H_1, \ldots, H_u \) the subgroups of order \( p^{m+s+1} \) containing \( K \). Since \( p^n \mid g \), \( t \) and \( u \) are positive, and we consider the \( t \times u \) matrix \( (a_{ij}) \) where \( a_{ij} = 1 \) if \( L_i \subseteq H_j \) and 0 otherwise. The row sum \( \sum_{j=1}^u a_{ij} \) of the matrix is denoted...
by \( r_i \), and the column sum \( \sum_{i=1}^t a_{ij} \) by \( c_j \), which gives the following tableau

\[
\begin{array}{ccc|c}
H_1 & \cdots & H_u & r_1 \\
L_1 & & a_{ij} & \\
& & & \\
& & & \\
L_t & c_1 & \cdots & c_u \\
\end{array}
\]

By the induction hypothesis, \( t \equiv 1 \pmod{p} \) and we must show that \( u \equiv 1 \pmod{p} \). Since \( r_1 + \cdots + r_t = c_1 + \cdots + c_u \), it is sufficient to show that each \( r_i \equiv 1 \pmod{p} \) and each \( c_j \equiv 1 \pmod{p} \). However, \( r_i \) is the number of subgroups of order \( p^{m+s+1} \) of \( G \) which contain \( L_i \), whence \( r_i \equiv 1 \pmod{p} \) by Case 1. Furthermore, \( c_j \) is the number of subgroups of order \( p^{m+s} \) of \( H_j \) which contain \( K \), whence \( c_j \equiv 1 \pmod{p} \) by the induction hypothesis. Done.

3. Normal \( p \)-subgroups. The theorem also enables one to obtain the standard statements which refer to normal \( p \)-subgroups. The proof of the following corollary shows how this works.

**Corollary.** Let everything be as in the theorem, but assume furthermore that \( G \) is a \( p \)-group and \( K \) is normal in \( G \). Then, the number of normal subgroups of \( G \) of order \( p^n \) which contain \( K \) is congruent 1 modulo \( p \) \([1, p. 129]\).

**Proof.** Let \( \{ H_1, \cdots, H_t \} \) be the set of subgroups of \( G \) of order \( p^n \) which contain \( K \). Since \( K \) is normal in \( G \), \( G \) acts on this set of groups by inner automorphisms. Since \( G \) is a \( p \)-group, the number of fixed points of \( G \) in the permutation representation \((G, \{ H_1, \cdots, H_t \})\) is congruent \( t \pmod{p} \). However, \( G \) leaves \( H_i \) fixed if and only if \( H_i \) is normal in \( G \), and \( t \equiv 1 \pmod{p} \) by the theorem.

**Reference**


Department of Mathematics, Dartmouth College, Hanover, New Hampshire 03755