2-1993

When is the Number of p-Subgroups of a Group Satisfying a Property Congruent to 1 (mod p)?

Jason Fulman
Rose-Hulman Institute of Technology

Jeff Vanderkam
Rose-Hulman Institute of Technology

WHEN IS THE NUMBER OF p SUBGROUPS OF A GROUP SATSIFYING A PROPERTY CONGRUENT TO 1 MOD p?

Jason Fulman and Jeff Vanderkam

MS TR 93-01

February 1993

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198

Phone: (812) 877-8391

When Is the Number of p Subgroups of a Group Satisfying a Property Congruent to 1 mod p?

Jason Fulman and Jeff Vanderkam

February 18, 1993

Abstract

Let T be a property which holds for a group independent of whether or not this group is imbedded in a group G or in a p-Sylow of G. Using a generalization of Sylow's second theorem, we prove that if for any p group P the number of subgroups of P satisfying T is congruent to 1 mod p, then for any group G, the number of p subgroups satisfying T is also congruent to 1 mod p. As an application, we give simple proofs of several theorems, including the well-known Frobenius theorem.

Theorem 1, the main theorem of this paper, allows us to transfer certain theorems about p groups to all finite groups. In the statement of Theorem 1, T is a group property, which is true for a p group P whether or not P is viewed as a subgroup of a larger group G or as a subgroup of a p-Sylow of G. For instance all isomorphism-invariant group properties T (such as a group being a p group, or a group containing a subgroup of order 8) satisfy this condition.

Theorem 1 *Let T be a group property as above. Suppose that for any p group P, the number of subgroups of P satisfying T is congruent to* 1 *mod p. Then for any finite G, the number of p subgroups satisfying T is congruent to* 1 *mod p.*

In order to prove Theorem 1, we require Theorem 2, a known [1] generalization of Sylow's second theorem, namely that the number of p-Sylows containing a fixed p group is congruent to 1 mod p. Theorem 2 is normally proven by double coset arguments. We give a simple action based proof which makes use of the following Lemma. $N(G)$ denotes the normalizer of a group G.

Lemma 1 *A p subgroup H of G is contained in $N(P)$, where P is a p-Sylow of G, if and only if $H \subset P$.*

PROOF: If $H \subset P$, then clearly $H \subset N(P)$.

If $H \subset N(P)$, then since H is a p group it is contained in some p-Sylow of $N(P)$. However P is the unique p-Sylow of $N(P)$, since P is normal in $N(P)$ and all p-Sylows in any group, in particular $N(P)$, are conjugate. Thus $H \subset P$. □

Theorem 2 *Let H be a p-subgroup of a group G. Then the number of p-Sylows containing H is congruent to 1 mod p.*

PROOF: Let H act by conjugation on the set of all p-Sylows $P_1, \ldots, P_n$ of G. Now H fixes a p-Sylow P_i if and only if $H \subset N(P_i)$. Lemma 1 thus implies H fixes a p-Sylow P_i if and only if $H \subset P_i$. Since H is a p group, all orbits of this action have size a power of p. This implies that the number of fixed points of this action is congruent to n mod p. The result follows since $n \equiv 1$ mod p, by Sylow's second theorem. □

Now we can prove Theorem 1.

PROOF: Let G be an arbitrary group. The idea of the proof is to count (in two different ways) the number, n, of pairs (H, S) where H is a p group satisfying property T and S is a p-Sylow of G containing H (recall that each p group is contained in some p-Sylow). Intuitively, one gets two different counts by projecting onto the H and S coordinates. Note that by hypothesis we need not be concerned with whether or not H is viewed as a subgroup of S or G.

For the first count, we fix a p-Sylow S_i of G. Since S_i is a p group the number of H contained in S_i satisfying property T is congruent to 1 mod p. By Sylow's second theorem, the number of p-Sylows of G is congruent to 1 mod p. It follows that $n \equiv 1(p)$.

For the second count, we fix a p subgroup H of G with property T. By Theorem 1, the number of p-Sylows of G containing H is congruent to 1 mod p. This implies that n is equal to the number of p subgroups H of G with property T, modulo p.

The result follows by equating the two counts. □

To see the power of Theorem 1, we give a new proof of a fairly difficult result, Frobenius' theorem. A short Lemma is required (the Lemma actually holds if G is any group, but the proof [2] is harder).

Lemma 2 *Let G be an abelian p group. Then the number of subgroups of order p is congruent to 1 mod p.*

PROOF: Since G is abelian, it is a direct product of say k cyclic groups. Note that the elements of order p in G are products of elements of the form $a_1, \ldots, a_k$ where each a_i is contained in the factor i and has order 1 or p, but not all a_i have order 1. Since cyclic groups of order a power of p have precisely p elements of order 1 or p (these elements are the p elements in the unique subgroup of order p) we see that the number of elements of order p in G is $p^k - 1$. Since groups of order p are either equal or disjoint, the number of subgroups of order p of G is $(p^k - 1)/(p - 1)$ which is

$$p^{k-1} + p^{k-2} + \cdots + 1,$$

which is congruent to 1 mod p. □

Theorem 3 *(Frobenius) If p^m divides the order of G, then the number of subgroups of G of order p^m is congruent to 1 mod p.*

PROOF: The property of having order p^m is isomorphism invariant, so by Theorem 1, we can assume G is a p group. Let G act on the set of all subgroups of order p^m by conjugation. Since G is a p-group, the orbits of the action have size a power of p. The fixed points of this action are normal groups of G, so it suffices to prove that the number of normal subgroups of G of order p^m is congruent to 1 mod p. We proceed by induction on the order of G. The base case, where G is cyclic of order p is trivial.

Let n be the size of the set of pairs of the form (A, N) where A is a group of order p contained in the center Z of G, (Z is non-trivial since G is a p group), and N is a normal subgroup of order p^m of G containing A. We then count n is two different ways.

For the first count, fix N. Then the number of pairs of the form (A, N) is simply the number of groups of order p in $Z \cap N$. (Since G is a p-group, any normal subgroup H of G has non-trivial intersection with Z. This can be seen by having G act on the non-identity elements of H by conjugation, and noting that this action must have fixed points). Now since $Z \cap N$ is abelian, by Lemma 2 the number of subgroups of order p of $Z \cap N$ is congruent to 1 mod p. Thus, n is equal to the number of normal subgroups N of order p^m, modulo p.

For the second count, fix A of order p in Z. We want to count the number of normal subgroups N of order p^m containing A. Note that the homomorphism $G \to G/A$ preserves normality, so that in G/A we want the number of normal subgroups of order p^{m-1}. By the induction hypothesis, this is congruent to 1 mod p. Also, since Z is abelian, by Lemma 2 the number of A of order p in Z is congruent to 1 mod p. Thus $n \equiv 1(p)$.

The theorem now follows by equating the two counts. □

The following theorem is in fact true for all P, not just for normal P [2]. The proof for normal P, however, is in the spirit of this paper.

Theorem 4 *If p^m divides the order of G, and P is a normal subgroup of order p^k where $k \leq m$, then the number of subgroups of order p^m containing P is congruent to* 1 *mod p.*

PROOF: If P is normal in G, then it is certainly normal in the p-Sylows of G. The property of containing a fixed subgroup P satisfies the conditions of Theorem 1, so it suffices to prove this theorem for p groups G.

We prove this result by induction on k. The base case $k = 0$ is Frobenius' theorem. Assume the result for $k-1$. Now a normal subgroup of order p^k has non-trivial intersection with the center $Z(G)$. (See parenthetical comment in paragraph 3 of the previous theorem for a proof). Let A be a subgroup of order p contained in $P \cap Z$. Then the number of subgroups of G of order p^m containing P is equal to the number of subgroups of G/A of order p^{m-1} containing P/A. Note that P/A is normal and has order p^{k-1}. The result follows by the induction hypothesis. □

Acknowledgements. The authors are grateful to Gary Sherman, at whose summer program the research for this paper began. The authors are also grateful to Keith Conrad for bringing the second reference to their attention.

References

[1] Suzuki, Group Theory 1, p. 96

[2] Searcoid, A Reordering of the Sylow Theorems, American Math Monthly, Vol. 94, Number 2, Feb. 1987