A New Proof of the Generalized Wilson's Theorem
Author(s): G. A. Miller
Published by: Annals of Mathematics
Stable URL: http://www.jstor.org/stable/1967333
Accessed: 27/02/2011 02:20

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/action/showPublisher?publisherCode=annals.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.
A NEW PROOF OF THE GENERALIZED WILSON'S THEOREM

By G. A. Miller

By employing several elementary theorems of substitution groups it is possible to give a very simple proof of Wilson's theorem in the theory of numbers. This proof makes no use of the theory in regard to the number of roots of a congruence. In fact, the idea of congruence is not employed at all except in so far as this concept is involved in that of periodicity. We proceed to develop the theorems of substitution groups which will be employed.

1. Statement of the Theorem. Product of All the Operators in an Abelian Group. Wilson's theorem relates to the \( \phi(g) \) numbers prime to an integer \( g \) and less than \( g \), and asserts that their product is congruent, modulo \( g \), to \(-1\) in three cases, viz. when \( g = p^a \), \( 2p^a \), or \( 4 \), and in all other cases the product is congruent to \(+1\). (Here \( p \) denotes an odd prime, and \( a \) any positive integer). Now these \( \phi(g) \) numbers combined by multiplication and the products taken modulo \( g \) form a group of a certain special kind, the group of isomorphisms of a cyclic group with itself. The order of the cyclic group is \( g \), and the group of isomorphisms is necessarily abelian. Further details have been explained in a recent number of the Annals (Second Series, Vol. 2, p. 77). We shall expect, therefore, to come upon the equivalent in Group theory of Wilson's theorem in numbers if we examine abelian groups, particularly such as can be groups of isomorphisms of cyclic groups.

All the operators whose orders exceed two in any group may be so arranged that their continued product is the identity. This may be done, for instance, by associating each operator with its inverse. As in an abelian group \( (A) \) any product is independent of the order of the factors, it follows that the continued product of all the operators whose orders exceed two in \( A \) is the identity.

If the group \( A \) contains no operator of order two, then the product of all its operators is the identity. It remains to examine separately the operators of order two when any such are contained in the group.

All the operators of order two in \( A \) generate a group \( (A_1) \) of order \( 2^a \), which has \( a \) independent generators of order 2. If \( s_i \) denotes any one of these, then \( A_1 \) is the direct product of the group \( (1, s_1) \) and the subgroup of order
THE GENERALIZED WILSON'S THEOREM

2^{a-1}$ generated by the remaining independent generators. It follows that $s_1$ is a factor of one-half of the operators of $A_1$ and hence does not appear in the continued product of all the operators of $A_1$ whenever $a > 1$. Since any operator of order 2 could have been taken for $s_1$, we have the theorem: If an abelian group contains more than one operator of order two, the continued product of all its operators is the identity; if it contains only one such operator, this operator is the continued product of all its operators.

2. Order of a Cyclic Group whose Group of Isomorphisms Contains only One Operator of Order Two. We proceed to prove that the order of such a cyclic group is of one of the three forms, $p^a$, $2p^a$, or 4.

Let $M$ represent any metacyclic substitution group of order $p(p-1)$ and of degree $p$. The subgroup $(M_1)$ which is composed of all the substitutions of $M$ which omit a given letter is regular and of degree $p - 1$, since each one of its substitutions transforms each substitution of order $p$ in $M$ into a power of itself. As $M_1$ is a group of isomorphisms of a cyclic group, it is abelian.* If it contained more than one substitution of order 2, $M$ would contain more than $p$ such substitutions, since no two conjugates under $M$ can occur in $M_1$ and each substitution of order 2 in $M$ has $p$ conjugates under $M$.

Suppose, then, that $M$ could contain more than $p$ substitutions of order 2. Each of these would involve $(p-1)/2$ transpositions, and, as there are only $p(p-1)/2$ distinct transpositions of $p$ letters, two substitutions of order two would have a common transposition. Their product would, therefore, be of a lower degree than $p-1$. As this is contrary to the fact that $M_1$ is regular and of degree $p-1$, it follows that the group of isomorphisms of a cyclic group of order $p$ contains only one operator of order 2.

The group of isomorphisms of the cyclic group of order $p^a$, $a > 1$, is the direct product of the cyclic group of order $p^{a-1}$ and of the group of isomorphisms of the group of order $p$.† From this it follows that the group of isomorphisms of the cyclic group of order $p^a$ (and hence also of the cyclic group of order $2p^a$) contains only one operator of order 2. It has been proved without the use of the theory of congruences† that the group of isomorphisms of the cyclic group of order $2^a$ contains just three operators of order 2 whenever $a > 2$; when $a = 2$ this group of isomorphisms is evidently of order 2. That is,

---

* Transactions of the American Mathematical Society, vol. 1 (1900), p. 397. From the theory of primitive roots it follows directly that $M_1$ is the cyclic group of order $p - 1$, but the present proof is independent of this theory.

if the group of isomorphisms of a cyclic group of order \(2^a\) contains only one operator of order 2, then \(a\) must be 2.

Since the group of isomorphisms \((G_1)\) of the cyclic group \((G)\) of order \(g = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}\) is the direct product\(^*\) of the groups of isomorphisms of the cyclic groups of orders \(2^{a_0}, p_1^{a_1}, p_2^{a_2}, \cdots p_m^{a_m}\), and since each of these groups of isomorphisms is of even order (except that of order \(2^{a_0}\) when \(a_0 = 1\)) it follows that \(G_1\) must involve more than one operator of order 2 with the exception of the three cases when its order is \(p^a, 2p^a,\) or 4 where \(p\) is any odd prime. That is, if the group of isomorphisms of a cyclic group contains only one operator of order 2, the order of the cyclic group must be one of the three numbers 4, \(p^a, 2p^a\), where \(p\) is any odd prime.

3. Conclusion. As stated in the introduction, the group \(G_1\) of the preceding paragraphs is representable by the \(\phi(g)\) numbers less than \(g\) and prime to \(g\), when they are combined by multiplication, the products being replaced by their least residues modulo \(g\). To complete now the proof of the generalized Wilson’s theorem it is only necessary to notice that in the three exceptional cases specified in §1 the one operator of order two corresponds to the numbers \(p^a - 1, 2p^a - 1,\) and 3 respectively,—numbers congruent in their respective systems to \(-1\), while the identity corresponds to \(+1\). With these facts in mind it is evident that the theorems demonstrated in §§1, 2 constitute precisely a statement, in the language of group theory, of Wilson’s theorem.

Stanford University, December, 1902.

\*Transactions of the American Mathematical Society, vol. 1, 1900, p. 396, Theorem II.