BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 25, Number 2, October 1991

ON A CONJECTURE OF FROBENIUS

NOBUO IIYORI AND HIROYOSHI YAMAKI

ABSTRACT. Let G be a finite group and e be a positive integer dividing the order of G. Frobenius conjectured that if the number of elements whose orders divide e equals e, then G has a subgroup of order e. We announce that the Frobenius conjecture has been proved via the classification of finite simple groups.

Let G be a finite group and e be a positive integer dividing $|G|$, the order of G. Let $L_e(G) = \{x \in G | x^e = 1\}$. In 1895 Frobenius [4] proved the following result:

$$|L_e(G)| = ke \quad \text{for an integer} \quad k \geq 1$$

and he made the following conjecture.

Frobenius conjecture. *If $k = 1$, then the e elements of $L_e(G)$ form a characteristic subgroup of G, that is, a subgroup of G that is invariant under the automorphism group of G.*

If the e elements of $L_e(G)$ form a subgroup, then $L_e(G)$ is necessarily a characteristic subgroup by the definition of $L_e(G)$. If e is a power of a prime, the conjecture is true by Sylow's theorem. M. Hall [6] gives a proof of the conjecture when G is solvable. It is proved by Zemlin [16] that the minimal counterexample to the conjecture is a nonabelian simple group. The purpose of this note is to announce the following

Theorem. *The conjecture of Frobenius is always true.*

Because of the classification of finite simple groups we may assume that G is isomorphic with

(1) A_n $(n \geq 5)$, the alternating group on n letters,
(2) a simple group of Lie type, or
(3) one of the twenty-six sporadic simple groups.

Received by the editors January 29, 1991 and, in revised form, March 29, 1991.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20D05, 20D06, 20D08; Secondary 20B05.
The second author was partially supported by Grant-in-Aid for Scientific Research, Ministry of Education, Science, and Culture.

We refer to [11] for the alternating groups, [7, 8, 11, 15] for the simple groups of Lie type and [14] for the sporadic simple groups. In order to verify the conjecture two lemmas play crucial role.

Lemma 1 [10, 11, 16]. *Let G be a finite group and e be a positive integer dividing $|G|$. Assume that $e = |L_e(G)|$. If p is a prime divisor of e and $|G|/e$, then Sylow p-subgroups of G are cyclic, generalized quaternion, dihedral, or quasidihedral.*

Lemma 2 [11, 15]. *Let G be a finite simple group and S be a nilpotent Hall π-subgroup of G. Suppose that S is disjoint from its distinct conjugates and $C_G(x)$ is contained in $SC_G(S)$ for all x in $S^\sharp$. If e is minimal such that $e = |L_e(G)|$ divides $|G|$ and $e > 1$, then $|S|$ divides either e or $|G|/e$.*

Remark. *We apply this lemma only when S is abelian.*

Basic idea of the proof can be found in [15]. Let e be minimal such that $e = |L_e(G)|$ divides $|G|$ and $1 < e < |G|$. Since G is simple we have to prove that there exists no such e.

Suppose that there exists a prime p that divides both e and $|G|/e$. Let P be a Sylow p-subgroup of G. If $p = 2$, then P is dihedral or quasidihedral by Lemma 1 and G is isomorphic with A_7, M_{11}, $L_2(q)$, $q \equiv 1(2)$, $q > 3$; $L_3(q)$, $q \equiv -1(4)$; or $U_3(q)$, $q \equiv 1(4)$ (see [5]). By [7, 11, 14, 15] the conjecture holds for these simple groups. If p is an odd prime, then P is cyclic by Lemma 1. Blau [1] yields that P is disjoint from its distinct conjugates since G is simple. Let x be a nontrivial element of P. Then $C_G(x)$ is p-closed and every p'-element acts trivially on $\Omega_1(P)$. It follows that $C_G(x) = C_G(P)$. However Lemma 2 implies that $|P|$ divides either e or $|G|/e$, which is a contradiction by the choice of p. It follows that e is a Hall divisor of $|G|$, that is, $(e, |G|/e) = 1$. In order to illustrate briefly our proof we consider the cases that $G = E_7(q)$, the simple Chevalley group of type E_7 and $G = P\Omega_{2m}(-1, q)$, the orthogonal simple group with nonmaximal Witt index (see [7, 8]).

Let G be a simple Chevalley group $E_7(q)$. By [2] G contains Hall abelian subgroups H in a maximal torus $T(E_7)$ and K in a maximal torus $T(E_6(a_1))$ such that $|H| = (q^6-q^3+1)(3, q+1)^{-1}$, $|K| = (q^6 + q^3 + 1)(3, q - 1)^{-1}$, $(N_G(H) : C_G(H)) = (N_G(K) : C_G(K)) = 18$, $|C_G(h)| = (q^6 - q^3 + 1)(q + 1)$, $h \in H^\sharp$ and

$|C_G(k)| = (q^6 + q^3 + 1)(q - 1)$, $k \in K^\sharp$ (see also [9, 13]). H and K satisfy the condition of Lemma 2. It follows that either $L_e(G)$ contains all conjugates of H or not and either $L_e(G)$ contains all conjugates of K or not. Now we have four possibilities: (i) $e \equiv 0(|H||K|)$, (ii) $e \equiv 0(|H|)$ and $(e, |K|) = 1$, (iii) $e \equiv 0(|K|)$ and $(e, |H|) = 1$, (iv) $(e, |H||K|) = 1$. Case (ii) (*resp.* case (iii)) yields that $e = |L_e(G)| > |G|/19(q+1)$ (*resp.* $e > |G|/19(q-1)$), a contradiction. Case (iv) cannot happen since G contains $(|G|_q)^2 = q^{126}$ unipotent elements by [12]. In case (i) let $\pi = (q - 1, |G|/e)$ and $\rho = (q + 1, |G|/e)$. If $\pi = 1$ or $\rho = 1$, then $e > |G|/20$. This is impossible since e is a Hall divisor of $|G|$. If $\pi \neq 1 \neq \rho$, the counting arguments, which are slightly more complicated than those of [15], yield that $e = |L_e(G)| > |G|/15 \operatorname{Max}\{\pi, \rho\}$. Now we can prove $e > |G|/11$. This is a contradiction since e is a Hall divisor of $|G|$. This implies that $e = 1$ or $e = |G|$.

Let G be the orthogonal simple group $P\Omega_{2m}(-1, q)$. If $q = 2$ and $m = 4$ or 5, then the conjecture holds by [3]. Thus we assume that $G \neq P\Omega_8(-1, 2)$, $P\Omega_{10}(-1, 2)$. By [2] G contains a torus $T(C_{m-i})$ $(0 \leq i \leq [m/2])$ of order $(q^m + 1)(q^m + 1, 4)^{-1}$ or $(q^{m-i} + 1)$ (see also [9, 13]). Let $g_j(q) = (q^j + 1, \prod_{k|j}(q^k + 1)^N)$ for a sufficiently large integer N. Let $h_j(q) = (q^j + 1)/g_j(q)$. $T(C_{m-i})$ contains a Hall subgroup H_{m-i} $(0 \leq i \leq [m/2])$ in G with $h_{m-i}(q) = |H_{m-i}|$ and $C_G(H_{m-i}) \supseteq T(C_{m-i})$. H_{m-i} satisfies the condition of Lemma 2. It follows that either $L_e(G)$ contains all conjugates of H_{m-i} or not. We note that $(N_G(H_m) : C_G(H_m))$ divides $2m$. The counting arguments for $E_7(q)$ can be piled up using H_{m-i}. If $h_m(q)$ divides e, then $e = |L_e(G)| > (|H_m| - 1)|K|(G : N_G(H_m))/\nu$ where $C_G(H_m) = H_m \times K$ and $\nu = (|K|, |G|/e)$. We can easily get a contradiction, which yields that $h_m(q)$ divides $|G|/e$. We can successfully prove that e is a power of 2 if q is odd and $e = 1$ if q is even by the similar counting arguments. This contradiction shows that $e = 1$ or $e = |G|$.

Acknowledgment

Both authors would like to thank the anonymous referees for suggestions that helped make the paper clearer and more readable.

References

1. H. I. Blau, *On trivial intersection of cyclic Sylow subgroups*, Proc. Amer. Math. Soc. **94** (1985), 572–576.
2. R. W. Carter, *Conjugacy classes in the Weyl group*, Compositio Math. **25** (1972), 1–59.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
4. G. Frobenius, *Verallgemeinerung des Sylowschen Satze*, Berliner Sitz. (1895), pp. 981–993.
5. D. Gorenstein, *The Classification of Finite Simple Groups*, Vol.1, Plenum Press, New York, 1983.
6. M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.
7. N. Iiyori, *A conjecture of Frobenius and the simple groups of Lie type*, IV, J. Algebra (to appear).
8. N. Iiyori and H. Yamaki, *A conjecture of Frobenius and the simple groups of Lie type*, III, J. Algebra (to appear).
9. N. Iiyori and H. Yamaki, *Prime graph components of the simple groups of Lie type over the field of even characteristic*, Proc. Japan Acad. **67** (1991), 82–83.
10. M. Murai, *On a conjecture of Frobenius*, Sugaku **35** (1983), 82–84. (Japanese)
11. J. Rust, *On a conjecture of Frobenius*, Ph.D. Thesis, Univ. of Chicago, 1966.
12. R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. **80** (1968).
13. J. S. Williams, *Prime graph components of finite groups*, J. Algebra **69** (1981), 487–513.
14. H. Yamaki, *A conjecture of Frobenius and the sporadic simple groups*, I, Comm. Algebra **11** (1983), 2513–2518; II, Math. Comp. **46** (1986), 609–611; *Supplement*, Math. Comp. **46** (1986), S43–S46.
15. H. Yamaki, *A conjecture of Frobenius and the simple groups of Lie type*, I, Arch. Math. **42** (1984), 344–347; II, J. Algebra **96** (1985), 391–396.
16. R. Zemlin, *On a conjecture arising from a theorem of Frobenius*, Ph.D. Thesis, Ohio State Univ., 1954.

Institute of Mathematics, University of Tsukuba, Ibaraki, 305 Japan