J. Aust. Math. Soc. **78** (2005), 291–295

ELEMENTS OF PRIME POWER ORDER AND THEIR CONJUGACY CLASSES IN FINITE GROUPS

LÁSZLÓ HÉTHELYI and BURKHARD KÜLSHAMMER

(Received 6 May 2003; revised 17 December 2003)

Communicated by E. A. O'Brien

Abstract

We show that, for any positive integer k, there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes of elements of prime power order. This generalizes a result of E. Landau from 1903. The proof of our generalization makes use of the classification of finite simple groups.

2000 *Mathematics subject classification*: primary 20C45.

1. Introduction

Landau has proved that, for any positive integer k, there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes [3]. In this paper we prove a variant of Landau's result in which we restrict our attention to conjugacy classes of elements of prime power order only.

THEOREM 1.1. *For any positive integer k, there are only finitely many finite groups, up to isomorphism, with exactly k conjugacy classes of elements of prime power order.*

Whereas the proof of Landau's original result is elementary, our proof of Theorem 1.1 relies on the classification of finite simple groups. Theorem 1.1 is also related to a conjecture of Praeger [4, page 30]. We are grateful to L. Pyber for pointing out this reference.

In the following, we denote by $\mathrm{kpp}(G)$ the number of conjugacy classes of elements of prime power order in a finite group G. (Throughout the conjugacy class of 1 is counted as one of the conjugacy classes of elements of prime power order.)

LEMMA 1.2. *Let N be a normal subgroup of a finite group G. Then*

(i) $\operatorname{kpp}(G) \le \operatorname{kpp}(G/N) \cdot |N|$;
(ii) $\operatorname{kpp}(G/N) < \operatorname{kpp}(G)$ *unless* $N = 1$.

PROOF. Let N be arbitrary, and let C be a conjugacy class of elements of prime power order in G. Then the image $\overline{C}$ of C in $\overline{G} = G/N$ is a conjugacy class of elements of prime power order in $\overline{G}$.

Conversely, let xN be an element in G/N whose order is a power p^n of a prime p. We write $x = x_p x_{p'} = x_{p'} x_p$ where x_p is a p-element and $x_{p'}$ is a p'-element in G. Then $xN = (x_p N)(x_{p'} N) = (x_{p'} N)(x_p N)$ where $x_p N$ is a p-element and $x_{p'} N$ is a p'-element. Since xN has order p^n, we must have $x_{p'} N = 1$. Thus $xN = x_p N$, and we see that $C \mapsto \overline{C}$ is a map from the set of conjugacy classes of elements of prime power order in G *onto* the set of conjugacy classes of elements of prime power order in $\overline{G} = G/N$.

Let $N \ne 1$. Then N contains an element $x \ne 1$ of prime order. Thus the conjugacy classes of x and 1 have the same image in G/N. Hence $\operatorname{kpp}(G/N) < \operatorname{kpp}(G)$.

Now let $\overline{C}$ be a conjugacy class of elements of prime power order in $\overline{G}$. Then the pre-image of $\overline{C}$ in G consists of $|\overline{C}| \cdot |N|$ elements. These form a union of conjugacy classes $C_1, \ldots, C_r$ of G. For $i = 1, \ldots, r$, we have $\overline{C_i} = \overline{C}$ and hence $|C_i| \ge |\overline{C_i}| = |\overline{C}|$. Hence $r \le |N|$, and the result is proved. □

We are now going to prove Theorem 1.1 in a series of lemmas.

LEMMA 1.3. *There exists a function $\alpha : \mathbb{N} \to \mathbb{N}$ with the following property: Whenever k is a positive integer and G is a finite simple group with* $\operatorname{kpp}(G) = k$ *then* $|G| \le \alpha(k)$.

PROOF. Let $k \in \mathbb{N}$, and let G be a finite simple group with $\operatorname{kpp}(G) = k$. We wish to show that $|G|$ is bounded in terms of k. (Our proof will make use of the classification of finite simple groups.) Our claim is trivial if G has prime order, or if G is a sporadic simple group. If G is an alternating group A_n then $|G| = n!/2$ can have at most k different prime divisors, so $|G|$ is also bounded in this case.

Thus, in the remainder of the proof, we may assume that G is a finite simple group of Lie type. There are 16 such families of groups (see [1, page 8]). It suffices to show that there are only finitely many possibilities for G in each family.

Suppose first that $G = \operatorname{PSL}(n, q)$ for some $n > 1$ and some prime power q, so that

$$|G| = (n, q-1)^{-1} q^{\binom{n}{2}} (q^n - 1) \cdots (q - 1).$$

The Zsigmondy prime number theorem (see [2, IX.8.3]) shows that every factor $q^i - 1$ of $|G|$ with $i > 6$ contributes a new prime divisor of $|G|$ and thus a new conjugacy class of elements of prime (power) order. Hence $k = \mathrm{kpp}(G) \geq n - 6$, and we have shown that n is bounded in terms of k, in case of $G = \mathrm{PSL}(n, q)$.

We now keep n fixed and show that q is also bounded in terms of k. Let $\widehat{G} := \mathrm{SL}(n, q)$ and $\widehat{Z} := Z(\widehat{G})$, so that $|\widehat{Z}| = (n, q - 1)$. We keep $|\widehat{Z}|$ fixed. Now $\widehat{G}$ contains a maximal torus $\widehat{T}$ of order $(q - 1)^{n-1}$. We write the prime factorization of $|\widehat{T}|$ in the form $|\widehat{T}| = p_1^{a_1} \cdots p_m^{a_m}$. Then again m is bounded in terms of k. We regard m as fixed. Then $\widehat{T}$ contains $p_1^{a_1} + \cdots + p_m^{a_m} - m + 1$ elements of prime power order.

Let $\mathbf{F}$ denote the algebraic closure of the finite field $\mathbf{F}_q$ with q elements. The elements of $\widehat{T}$ can be diagonalized simultaneously in $\mathrm{GL}(n, \mathbf{F})$. Two diagonal matrices in $\mathrm{GL}(n, \mathbf{F})$ are conjugate if and only if one can be obtained from the other by permuting the diagonal entries. Hence our $p_1^{a_1} + \cdots + p_m^{a_m} - m + 1$ elements fall into at least $(n!)^{-1}(p_1^{a_1} + \cdots + p_m^{a_m} - m + 1)$ different conjugacy classes under $\mathrm{GL}(n, \mathbf{F})$. Thus

$$\mathrm{kpp}(\widehat{G}) \geq (n!)^{-1}(p_1^{a_1} + \cdots + p_m^{a_m} - m + 1),$$

and Lemma 1.2 implies that

$$k = \mathrm{kpp}(G) \geq \mathrm{kpp}(\widehat{G})/|\widehat{Z}| \geq (n, q - 1)^{-1}(n!)^{-1}(p_1^{a_1} + \cdots + p_m^{a_m} - m + 1).$$

Hence $p_1^{a_1}, \ldots, p_m^{a_m}$ are bounded in terms of k; in particular, $(q - 1)^{n-1} = p_1^{a_1} \cdots p_m^{a_m}$ is bounded in terms of k. Thus certainly q is bounded in terms of k. This finishes the proof in case $G = \mathrm{PSL}(n, q)$.

The argument is similar for the other families of finite simple groups of Lie type, and will therefore be omitted. This finishes the proof of Lemma 1.3. □

LEMMA 1.4. *There exists a function $\beta : \mathbb{N} \to \mathbb{N}$ with the following property: Whenever k is a positive integer and G is a characteristically simple finite group with* $\mathrm{kpp}(G) = k$ *then $|G| \leq \beta(k)$.*

PROOF. Let k be a positive integer, and let G be a characteristically simple finite group with $\mathrm{kpp}(G) = k$. We know that $G \cong S^r = S \times \cdots \times S$ (r factors) for a finite simple group S and a positive integer r. Now certainly $\mathrm{kpp}(G) \geq r(\mathrm{kpp}(S) - 1)$. Thus $r \leq k$ and $\mathrm{kpp}(S) \leq k$. By Lemma 1.3, we have

$$|S| \leq \max\{\alpha(1), \ldots, \alpha(k)\} =: A(k).$$

Hence $|G| \leq A(k)^k =: \beta(k)$, and the Lemma is proved. □

The following Lemma implies Theorem 1.1.

LEMMA 1.5. *There exists a function $\gamma : \mathbb{N} \to \mathbb{N}$ with the following property: Whenever k is a positive integer and G is a finite group with* $\mathrm{kpp}(G) = k$ *then $|G| \leq \gamma(k)$.*

PROOF. We define $\gamma(k)$ inductively, starting with $\gamma(1) := 1$. Then the result is certainly true for $k = 1$. So let us assume that $k > 1$, and that $\gamma(1), \ldots, \gamma(k-1)$ have been defined already. Moreover, let G be a finite group with $\mathrm{kpp}(G) = k$, and let N be a minimal normal subgroup of G. Then $\mathrm{kpp}(G/N) < k$ by Lemma 1.2 (ii) since $N \neq 1$, so that

$$|G/N| \leq \max\{\gamma(1), \ldots, \gamma(k-1)\} =: \Gamma(k-1),$$

by induction. Also, N contains at most k G-conjugacy classes of elements of prime power order. Each of these splits into at most $|G : N|$ N-conjugacy classes of elements of prime power order. Thus N contains at most $k\Gamma(k-1)$ conjugacy classes of elements of prime power order. Since N is characteristically simple we conclude that

$$|N| \leq \max\{\beta(i) : i = 1, \ldots, k\Gamma(k-1)\} =: B(k).$$

Thus $|G| \leq B(k)\Gamma(k-1) =: \gamma(k)$, and our result is proved. □

Our proof of Theorem 1.1 is now complete. At the end of this paper, we will discuss some related questions. Let π be a set of primes, and let π' denote the set of primes not contained in π. In the following, $\mathrm{k}_\pi(G)$ is defined as the number of conjugacy classes of π-elements in a finite group G, and $\mathrm{k}_{\pi'}(G)$ is defined in a similar way.

(1) Suppose that A is a π-group, that B is a π'-group, and that $G = A \times B$ is their direct product. Then $\mathrm{k}(G)$, the number of conjugacy classes of G, satisfies

$$\mathrm{k}(G) = \mathrm{k}(A)\,\mathrm{k}(B) = \mathrm{k}_\pi(G)\,\mathrm{k}_{\pi'}(G).$$

One may ask whether the inequality

$$\mathrm{k}(G) \leq \mathrm{k}_\pi(G)\,\mathrm{k}_{\pi'}(G)$$

holds for an arbitrary finite group G. This, however, is not the case: Let $\pi = \{3\}$, and let G be a dihedral group of order $6q$ where q is a prime different from 2 and 3. Then we have

$$\mathrm{k}(G) = (3q+3)/2, \quad \mathrm{k}_\pi(G) = 2, \quad \mathrm{k}_{\pi'}(G) = \mathrm{k}(G/P) = (q+3)/2,$$

with $P := O_3(G)$. Thus

$$\mathrm{k}_\pi(G)\,\mathrm{k}_{\pi'}(G) = q + 3 < (3q+3)/2 = \mathrm{k}(G).$$

(2) Now let A be a finite π'-group acting faithfully on a finite π-group B, and let G be the corresponding semidirect product. One may ask whether

$$\mathrm{k}_\pi(G)\,\mathrm{k}_{\pi'}(G) \leq |B|.$$

However, this is not true, in general. For example, let $\pi = \{p\}$ for an odd prime number p, and let $G = \mathrm{AGL}(1, p)$ be the affine general linear group of degree 1 over the field with p elements. Then G is the semidirect product of a cyclic group A of order $p - 1$ and a cyclic group B of order p. Moreover, we have $\mathrm{k}_\pi(G) = 2$ and $\mathrm{k}_{\pi'}(G) = p - 1$, but

$$|B| = p < 2(p-1) = \mathrm{k}_\pi(G)\,\mathrm{k}_{\pi'}(G).$$

Acknowledgements

The authors gratefully acknowledge financial support from the program 'Algorithmic investigations of discrete algebraic structures' sponsored by the BMBF and the TeT foundation (D-4/99). The first named author was also supported by OTKA grants T034878 and T042481. Both authors are grateful to the referee for a number of helpful suggestions.

References

[1] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups I* (Amer. Math. Soc., Providence, 1994).

[2] B. Huppert and N. Blackburn, *Finite groups II* (Springer, Berlin, 1982).

[3] E. Landau, 'Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante', *Math. Ann.* **56** (1903), 671–676.

[4] C. E. Praeger, 'Kronecker classes of fields and covering subgroups of finite groups', *J. Austral. Math. Soc. (Series A)* **57** (1994), 17–34.

Department of Algebra
Technical University of Budapest
H-1521 Budapest
Hungary
e-mail: hethelyi@math.bme.hu

Mathematical Institute
University of Jena
D-07737 Jena
Germany
e-mail: kuelshammer@uni-jena.de