Arch. Math. 105 (2015), 529–538

0003-889X/15/060529-10
published online October 31, 2015
DOI 10.1007/s00013-015-0835-5

Archiv der Mathematik

On the number of elements that are not kth powers in a group

W. Cocke, I. M. Isaacs, and D. Skabelund

Abstract. Let k be a positive integer, and suppose that the number of elements of a group G that are not kth powers in G is nonzero but finite. If G is finite, we obtain an upper bound on $|G|$, and we present some conditions sufficient to guarantee that G actually is finite.

Mathematics Subject Classification. 20F99.

Keywords. Non-kth-power, Nilpotent, Residually finite.

1. Introduction. Let G be a possibly infinite group, and fix an integer $k > 0$. In this paper, we consider the set of elements in G that are not kth powers. In other words, we are interested in the complement in G of the set

$$G^k = \{x^k \mid x \in G\}.$$

We write $\mathcal{N}_k(G) = G - G^k$ and $n_k(G) = |\mathcal{N}_k(G)|$, so $\mathcal{N}_k(G)$ is the set of non-kth-powers in G and $n_k(G)$ is the number of such elements. Our goal is to obtain information about $|G|$ under the assumption that $0 < n_k(G) < \infty$.

We begin with an easy observation.

Lemma A. *Suppose that $0 < n_k(G) < \infty$, where G is a group. If G^k is a subgroup, then $|G| \le 2n_k(G)$, and in particular, G is finite.*

Proof. Since $n_k(G) > 0$, we can choose a non-kth-power $x \in G$. The coset xG^k is disjoint from G^k, and thus $xG^k \subseteq \mathcal{N}_k(G)$. Then $|G^k| = |xG^k| \le n_k(G)$, and since $|G| = |G^k| + n_k(G)$, we conclude that $|G| \le 2n_k(G)$. ☐

Although G^k is certainly not a subgroup in general, it is a subgroup if G is abelian, and thus Lemma A applies in this case, and thus $|G| \le 2n_k(G)$ for abelian groups. (The situation where G^k is a subgroup has been well studied, and we mention in particular the paper [4] by Liebeck and Shalev.)

The research of the first author was supported under NSF Grant DGE-1256259.

Our goal is to prove something like the conclusion of Lemma A in general, where G^k is not necessarily a subgroup. If G is a finite group, we obtain a quadratic upper bound on $|G|$, which, as we shall see, is attained infinitely often. Unfortunately, we have only partial results for groups that are not assumed to be finite.

The finite-group case of this problem has been studied previously. For example, in [1], Bannai et al. used the classification of finite simple groups to show that if k divides $|G|$, then $n_k(G) \geq \left[\sqrt{|G|}\,\right]$. A classification-free proof of this inequality was given by Lévai and Pyber in [2], and more recently, in [3], Lucido and Pournaki gave another proof for the case $k = 2$.

For finite groups, we prove a somewhat sharper inequality with an even more elementary proof.

Theorem B. *Assume that G is finite, and write $n = n_k(G)$. If $n > 0$, then $|G| \leq n(n+1)$, and in fact $|G| \leq n^2$ except in the case where G is a Frobenius group with kernel of order $n+1$ and complement of order n, and in that case, $\mathcal{N}_k(G)$ is exactly the set of nonidentity elements of the Frobenius kernel.*

Observe that in the exceptional case of the theorem, where $|G| > n^2$, we have $|G| = n(n+1)$, and in this situation, the nonidentity elements of the Frobenius kernel are conjugate in G, and thus they all have the same prime order p. It follows that the Frobenius kernel is an elementary abelian p-group, and we conclude that $n + 1$ must be a prime power.

Conversely, given an arbitrary prime power p^e, there exist Frobenius groups with elementary abelian kernels of order p^e and complements of order $p^e - 1$. In such a group, all of the elements outside of the kernel have order not divisible by p, and so all of those elements are pth powers. It is easy to see that in this case, none of the nonidentity elements of the kernel is a pth power, and thus, taking $k = p$, we have $n = n_p(G) = p^e - 1$ and $|G| = n(n+1)$. It follows that our upper bound $n(n+1)$ for $|G|$ is attained infinitely often: whenever $k = p$ is prime and $n_k(G)$ has the form $p^e - 1$.

Without some additional conditions on a group G, we have been unable to prove that if the number of non-kth-powers in G is nonzero but finite, then $|G|$ must be finite. We can prove the following, however.

Theorem C. *Let G be a group, and assume that $0 < n_k(G) < \infty$. Suppose also that one of the following holds.*

(1) *G satisfies the maximal condition on cyclic subgroups.*
(2) *G has a finite-index nilpotent subgroup.*
(3) *G is residually finite.*

Then G is finite.

In particular, a group in which all elements have bounded finite order satisfies condition (1) of Theorem C, and thus such a group must be finite if its set of non-kth-powers is nonempty and finite.

A key step in our proof of Theorem C is the following, which may be of some independent interest.

Lemma D. *Suppose that* $0 < n_p(G) < \infty$*, where* p *is prime. Then there exists a finite-index subgroup* $H \subseteq G$ *such that* $\mathcal{N}_p(H) \subseteq \mathbf{Z}(H)$ *and* $0 < n_p(H) \leq n_p(G)$*.*

2. Finite groups. We work first to prove Theorem B in the case where k is a prime number; the general case will then follow fairly easily. Given a prime p, we will say that an element of a possibly infinite group is p-regular if it has finite order not divisible by p.

We begin with an elementary general observation.

Lemma 2.1. *Let* $x \in G$*, and let* p *be prime. Then* $x \in \mathcal{N}_p(G)$ *if and only if* x *is not* p*-regular and the cyclic group* $\langle x \rangle$ *does not have index* p *in any cyclic subgroup of* G*.*

Proof. First, suppose $x \in \mathcal{N}_p(G)$. If x has finite order m, where m is not divisible by p, write $ap + bm = 1$ for integers a and b. Then $x^m = 1$, so $x = x^{ap}x^{bm} = (x^a)^p$, and this is a contradiction since x is a non-pth-power. Also, if $\langle x \rangle$ has index p in a cyclic group B, then $x \in \langle x \rangle = B^p$, which is also a contradiction.

We must show now that if $x \notin \mathcal{N}_p(G)$, then either x is p-regular, or else $\langle x \rangle$ has index p in some cyclic subgroup. Let $y \in G$ with $y^p = x$. Then $\langle x \rangle \subseteq \langle y \rangle$ and $|\langle y \rangle : \langle x \rangle|$ is the order of y modulo $\langle x \rangle$, and this order divides p. If $|\langle y \rangle : \langle x \rangle| \neq p$, therefore, we have $\langle y \rangle = \langle x \rangle$, and thus y is a power of x. Writing $y = x^e$, we have $x = y^p = x^{pe}$, and thus x has finite order dividing $pe - 1$, and so x is p-regular. □

Lemma 2.2. *Let* $H \subseteq G$*, where* G *is finite, and let* p *be prime. Then* $n_p(H) \leq n_p(G)$*.*

In fact, Lemma 2.2 remains true if the assumption that $|G|$ is finite is relaxed, and we assume only that the index $|G : H|$ is finite. We will prove that more general result later, but we have decided to provide a separate elementary proof for the finite case.

Proof of Lemma 2.2 For elements $x \in G^p$, write $\theta(x) = \{y \in G \mid y^p = x\}$, and observe that the sets $\theta(x)$ are nonempty and disjoint, and their union is the whole group G. It follows that

$$n_p(G) = |G| - |G^p| = \sum_{x \in G^p} |\theta(x)| - |G^p| = \sum_{x \in G^p} (|\theta(x)| - 1).$$

Similarly, if $x \in H^p$, we write $\varphi(x) = \{y \in H \mid y^p = x\}$. Then

$$n_p(H) = \sum_{x \in H^p} (|\varphi(x)| - 1).$$

Now $H^p \subseteq G^p$, and for elements $x \in H^p$, we have $\varphi(x) = H \cap \theta(x)$, so $|\varphi(x)| \leq |\theta(x)|$. Also, each term in the sum for $n_p(G)$ is nonnegative, so a comparison of the two sums shows that $n_p(H) \leq n_p(G)$, as required. □

Lemma 2.3. *Let* G *be finite, and suppose that* p *divides* $|\mathbf{Z}(G)|$*, where* p *is prime. Then* $|G| \leq 2n_p(G)$*.*

Proof. Let $Z \subseteq \mathbf{Z}(G)$ with $|Z| = p$. Since all elements in each coset of Z in G have the same pth power, it follows that $|G^p|$ is at most the number of cosets, which is $|G|/p$. Then

$$n_p(G) = |G| - |G^p| \geq |G| - \frac{|G|}{p} = \frac{p-1}{p}|G| \geq \frac{|G|}{2},$$

and the result follows. □

Next, we state the case of Theorem B where k is prime.

Theorem 2.4. *Let $|G|$ be finite, and assume that $n_p(G) > 0$, where p is prime. Then writing $n = n_p(G)$, we have $|G| \leq n(n+1)$. In fact, $|G| \leq n^2$ unless G is a Frobenius group with kernel of order $n+1$ and complement of order n, and in this case, $\mathcal{N}_p(G)$ is exactly the set of nonidentity elements of the Frobenius kernel.*

Before we begin the proof, we recall that if a group G contains a nonidentity proper normal subgroup C such that $\mathbf{C}_G(x) \subseteq C$ for all nonidentity elements $x \in C$, then G is a Frobenius group with Frobenius kernel C. To see this, observe first that C must contain a full Sylow q-subgroup of G for each prime divisor q of $|C|$. It follows that C is a Hall subgroup of G, and hence by the Schur–Zassenhaus theorem, C has a complement H in G. Since no nonidentity element of C commutes with any nonidentity element of H, it follows that G is a Frobenius group with kernel C and complement H.

Proof of Theorem 2.4 The set $\mathcal{N}_p(G)$ is a union of conjugacy classes of G, and we suppose first that it is not a single conjugacy class, so some class contained in $\mathcal{N}_p(G)$ has size at most $n/2$. Let x be a member of this class, and write $C = \mathbf{C}_G(x)$, so $|G : C| \leq n/2$.

Since $x \in \mathcal{N}_p(G)$, it follows from Lemma 2.1 that the order of x is divisible by p. Then p divides $|\mathbf{Z}(C)|$, so we can apply Lemma 2.3 to conclude that $|C| \leq 2n_p(C)$, and we have

$$|G| = |C||G : C| \leq (2n_p(C))(n/2) \leq (2n)(n/2) = n^2,$$

as required, where the second inequality follows since $n_p(C) \leq n_p(G) = n$ by Lemma 2.2.

Now assume that $\mathcal{N}_p(G)$ is a single conjugacy class, so all members of $\mathcal{N}_p(G)$ have the same order, and by Lemma 2.1, this order must be divisible by p. Then p divides $|G|$, and we let A be a cyclic p-subgroup of G having the largest possible order. Then A is nontrivial, so each generator of A has prime-power order equal to $|A| > 1$. Since A does not have index p in a larger cyclic subgroup, it follows by Lemma 2.1 that every generator of A lies in $\mathcal{N}_p(G)$. The common order of the elements of $\mathcal{N}_p(G)$, therefore, is $|A|$.

Suppose $|A| > p$. Then the pth powers of the elements of $\mathcal{N}_p(G)$ form a conjugacy class K, with elements having order divisible by p. Also, the map $x \mapsto x^p$ is not injective on the set of generators of A, so it is not injective on $\mathcal{N}_p(G)$, and thus $|K| < n$. Let $x \in \mathcal{N}_p(G)$, and write $C = \mathbf{C}_G(x^p)$. Then $|G : C| = |K| < n$, and since $\mathbf{C}_G(x) \subseteq C$, it follows that $|G : C|$ divides $|G : \mathbf{C}_G(x)| = n$, and thus $|G : C| \leq n/2$. Now $x^p \in \mathbf{Z}(C)$ and x^p has order divisible by p, so we can apply Lemmas 2.2 and 2.3 to deduce that $|C| \leq 2n_p(C) \leq 2n_p(G) = 2n$, and thus $|G| = |C||G : C| \leq n^2$.

We can assume now that all elements of $\mathcal{N}_p(G)$ have order p. Let y be an arbitrary element of G having order divisible by p, and let B be maximal among cyclic subgroups of G containing y. Then B does not have index p in a larger cyclic subgroup, and p divides $|B|$. By Lemma 2.1, therefore, each generator of B lies in $\mathcal{N}_p(G)$, so $|B| = p$, and thus y generates B. It follows that $y \in \mathcal{N}_p(G)$, and we see that $\mathcal{N}_p(G)$ is the set of elements of G with order divisible by p. In particular, every element with order divisible by p has order p, exactly.

Now let $a \in \mathcal{N}_p(G)$, and let $C = \mathbf{C}_G(a)$, so $|G : C| = n_p(G) = n$. If $c \in C$ has order m not divisible by p, then ac has order mp, which is divisible by p, and thus ac has order p and $m = 1$. Each nonidentity element of C, therefore, has order divisible by p, and hence has order p and lies in $\mathcal{N}_p(G)$, and we conclude that $|C| \leq n+1$. If this inequality is strict, we get $|G| = |G : C||C| \leq n^2$, as wanted.

We can assume now that $|C| = n + 1$, so $|G| = |C||G : C| = n(n + 1)$. In this case, $C = \{1\} \cup \mathcal{N}_p(G)$, so $C \lhd G$, and thus $C = \mathbf{C}_G(u)$ for every member u of the conjugacy class $\mathcal{N}_p(G)$. In particular, this holds for all nonidentity elements $u \in C$, and it follows that G is a Frobenius group with kernel C. Since $|G : C| = n$, the Frobenius complement has order n, and this completes the proof. □

The following lemma will enable us to deduce Theorem B from Theorem 2.4.

Lemma 2.5. *Let G be a group, and suppose that $0 < n_k(G) < \infty$. Then there exists a prime p dividing k such that $0 < n_p(G) \leq n_k(G)$.*

Proof. We proceed by induction on k. Since $n_k(G) > 0$, some element of G is not a kth power, and thus $k > 1$. If k is prime, there is nothing to prove, so assume that $k = ab$, where $a > 1$ and $b > 1$, and thus $a < k$ and $b < k$. Now every kth power in G is both an ath power and a bth power, so the numbers of non-ath-powers and non-bth-powers in G are at most $n_k(G)$. If the number of non-ath-powers or the number of non-bth-powers in G is nonzero, the result follows by the inductive hypothesis, with a or b in place of k. We can thus assume that every element of G is both an ath power and a bth power. Now let $x \in G$ be arbitrary, and write $x = u^a$ and $u = v^b$ for elements $u, v \in G$. Then $x = v^{ab} = v^k$, and thus every element of G is a kth power, and this is a contradiction. □

Proof of Theorem B By Lemma 2.5, we can choose a prime divisor p of k such that $0 < n_p(G) \leq n$, where we recall that $n = n_k(G)$. By Theorem 2.4, we have $|G| \leq n_p(G)(n_p(G) + 1)$, so if $n_p(G) < n$, it follows that $|G| < n^2$, and there is nothing further to prove.

We can assume now that $n_p(G) = n = n_k(G)$. Since p divides k, we see that $\mathcal{N}_p(G) \subseteq \mathcal{N}_k(G)$, and thus $\mathcal{N}_p(G) = \mathcal{N}_k(G)$. By Theorem 2.4, we have $|G| \leq n(n + 1)$, and in fact $|G| \leq n^2$ unless $|G| = n(n + 1)$, and in that case, G is a Frobenius group and $\mathcal{N}_p(G) = \mathcal{N}_k(G)$ is exactly the set of nonidentity elements in the Frobenius kernel of order $n+1$. Also, the Frobenius complement has order n, and the proof is complete. □

3. Possibly infinite groups. We begin with a result that includes the promised stronger form of Lemma 2.2.

Lemma 3.1. *Suppose $H \subseteq G$ has finite index, and let p be prime.*

(a) *If $y \in \mathcal{N}_p(H)$, then $y = x^t$ for some element $x \in \mathcal{N}_p(G)$, where t is a power of p.*
(b) *There exists an injective map $f : \mathcal{N}_p(H) \to \mathcal{N}_p(G)$ such that y is a power of $f(y)$ for all $y \in \mathcal{N}_p(H)$. Also $f(y) = y$ if $y \in H \cap \mathcal{N}_p(G)$.*
(c) *$n_p(H) \leq n_p(G)$.*

Proof. Given $y \in H$, let $\mathcal{P}(y)$ be the set of pairs (x, t), where $x \in G$ and t is a power of p such that $x^t = y$. Note that $\mathcal{P}(y)$ is nonempty since $(y, 1) \in \mathcal{P}(y)$. Suppose now that $y \in \mathcal{N}_p(H)$ and $(x, t) \in \mathcal{P}(y)$. Note that if $s < t$, where s is a power of p, then $x^s \notin H$ since otherwise, $x^{t/p}$ is a pth root of y in H, and this contradicts the assumption that $y \in \mathcal{N}_p(H)$.

We argue now that $t \leq |G : H|$. Let $B = \langle x \rangle$, and note that $|B : B \cap H| < \infty$ since $x^t \in B \cap H$. Writing $m = |B : B \cap H|$, we see that m is the order of the image of x in $B/(B \cap H)$. It follows that m divides t, and in particular, m is a power of p. Since $x^m \in H$, we cannot have $m < t$, so $m = t$, and thus $t = m = |B : B \cap H| \leq |G : H|$, as claimed.

Now given $y \in \mathcal{N}_p(H)$, choose $(x, t) \in \mathcal{P}(y)$ with t as large as possible. (There is a maximum for t because, as we have seen, $t \leq |G : H|$.) The maximality of t guarantees that $x \in \mathcal{N}_p(G)$, and (a) follows.

For (b), let f be the (not necessarily uniquely determined) function $\mathcal{N}_p(H) \to \mathcal{N}_p(G)$ defined as follows. Given $y \in \mathcal{N}_p(H)$, we set $f(y) = x$, where as above, $x \in \mathcal{N}_p(G)$ and $x^t = y$, where t is some power of p. Also, we have seen that t must be the smallest power of p such that $x^t \in H$, and thus x determines t. It follows that x determines $y = x^t$, and we conclude that the map f is injective. Also, if it happens that $y \in \mathcal{N}_p(G)$, we must have $t = 1$, and thus $f(y) = x = x^t = y$.

Finally, (c) follows because there is an injective map $f : \mathcal{N}_p(H) \to \mathcal{N}_p(G)$. □

Proof of Lemma D For this proof, we write $m(G)$ to denote the number of elements of $\mathcal{N}_p(G)$ that are not central in a group G. We are given that $0 < n_p(G) < \infty$, and we show by induction on $m(G)$ that there exists a finite-index subgroup $H \subseteq G$ such that $0 < n_p(H) \leq n_p(G)$ and $\mathcal{N}_p(H) \subseteq \mathbf{Z}(H)$.

If $m(G) = 0$, then every element of $\mathcal{N}_p(G)$ is central in G, so we can take $H = G$, and there is nothing further to prove. We can assume, therefore, that there exists some element $a \in \mathcal{N}_p(G)$ such that $\mathbf{C}_G(a) < G$, and we write $C = \mathbf{C}_G(a)$. All conjugates of a in G lie in $\mathcal{N}_p(G)$, and thus $|G : C| \leq n_p(G) < \infty$. Also, $a \in C \cap \mathcal{N}_p(G) \subseteq \mathcal{N}_p(C)$, so $n_p(C) > 0$, and by Lemma 3.1, we have $n_p(C) < \infty$.

We wish to apply the inductive hypothesis to the group C, and to do this, we must establish that $m(C) < m(G)$. Let $f : \mathcal{N}_p(C) \to \mathcal{N}_p(G)$ be the injective map of Lemma 3.1. If $y \in \mathcal{N}_p(C)$ and y is not central in C, then since y is a power of $f(y)$, we see that $f(y)$ does not centralize C, and thus $f(y)$ is some noncentral element in $\mathcal{N}_p(G)$, and also, $f(y) \neq a$. It follows that f defines an injective map from the set of elements of $\mathcal{N}_p(C)$ that are not central in C into the set of elements of $\mathcal{N}_p(G)$ that are not central in G. Also, since the image of this map excludes a, the image is a proper subset of the set of elements of $\mathcal{N}_p(G)$ that are not central in G, and thus $m(C) < m(G)$. The inductive hypothesis now yields the result. □

Next, we prove the first part of Theorem C.

Theorem 3.2. *Suppose that the set of cyclic subgroups of the group G satisfies the maximal condition, and assume that $0 < n_k(G) < \infty$. Then G is finite.*

Proof. By Lemma 2.5, we can assume that k is a prime number, and we write $k = p$. Lemma D guarantees that there is a finite-index subgroup $H \subseteq G$ such that $0 < n_p(H) < \infty$ and $\mathcal{N}_p(H) \subseteq \mathbf{Z}(H)$. Since the maximal condition on cyclic subgroups is inherited by subgroups of G, we can replace G by H, and thus we can assume that $\mathcal{N}_p(G) \subseteq \mathbf{Z}(G)$.

We claim now that $\mathbf{Z}(G)$ contains every element of G that is not p-regular. If x is such an element, we can apply the maximal condition to choose a maximal cyclic subgroup B containing x. Since x is not p-regular, a generator b for B is not p-regular, so by Lemma 2.1, we have $b \in \mathcal{N}_p(G) \subseteq \mathbf{Z}(G)$, and thus $x \in \mathbf{Z}(G)$, as wanted.

Now let $z \in \mathcal{N}_p(G)$ and suppose that $y \in G$ is p-regular, so $y^r = 1$, for some integer r not divisible by p. We argue that zy is not p-regular. Otherwise, $(zy)^s = 1$ for some integer s not divisible by p, and thus $1 = (zy)^{rs} = z^{rs}y^{rs} = z^{rs}$, and hence z is p-regular. By Lemma 2.1, however, this is a contradiction because $z \in \mathcal{N}_p(G)$. By the result of the previous paragraph, $zy \in \mathbf{Z}(G)$, and thus $y \in \mathbf{Z}(G)$.

We have now shown that $\mathbf{Z}(G)$ contains all non-p-regular elements of G as well as all p-regular elements of G, and thus $\mathbf{Z}(G) = G$. Then G is abelian, so G^p is a subgroup, and thus $|G| \leq 2n_p(G) < \infty$, by Lemma A. □

The following is the second part of Theorem C.

Theorem 3.3. *Suppose that G has a nilpotent subgroup of finite index, and assume that $0 < n_k(G) < \infty$. Then G is finite.*

Before we proceed with the proof, we recall that in a possibly infinite nilpotent group G, the upper central series is the subgroup chain

$$1 = Z_0 < Z_1 < \cdots < Z_c = G,$$

where c is a nonnegative integer and Z_i is defined by the formula $Z_i/Z_{i-1} = \mathbf{Z}(G/Z_{i-1})$ for $0 < i \leq c$. The integer c is the nilpotence class of G, and we observe that $c = 0$ precisely when G is trivial.

Proof of Theorem 3.3 By Lemma 2.5, we can assume that $k = p$ is prime. By Lemma D, there is a finite-index subgroup $H \subseteq G$ such that $0 < n_p(H) < \infty$ and $\mathcal{N}_p(H) \leq \mathbf{Z}(H)$. The assumption that G has a finite-index nilpotent subgroup is inherited by subgroups of G, so there exists a finite-index nilpotent subgroup $K \subseteq H$. Now $K\mathbf{Z}(H)$ is nilpotent, so we can assume that $\mathbf{Z}(H) \subseteq K$, and thus $\mathcal{N}_p(H) \subseteq K$, and we have $\mathcal{N}_p(H) \subseteq \mathcal{N}_p(K)$. Also, $n_p(K) \leq n_p(H)$ by Lemma 3.1, and it follows that $\mathcal{N}_p(K) = \mathcal{N}_p(H) \subseteq \mathbf{Z}(H)$, and thus $\mathcal{N}_p(K) \subseteq \mathbf{Z}(K)$. Also, $n_p(K) = n_p(H)$, so $0 < n_p(K) < \infty$.

Now K has finite index in G, so it suffices to show that $|K| < \infty$, and thus we can replace G with K. We can assume, therefore, that G is nilpotent and that $\mathcal{N}_p(G) \subseteq \mathbf{Z}(G)$. In this situation, we show by induction on the nilpotence class c of G that $|G|$ is finite.

If $c \leq 1$ then G is abelian, so G^p is a subgroup, and the result follows by Lemma A. We can assume, therefore, that $c \geq 2$. Let $Z = \mathbf{Z}(G)$ and write $Y/Z = \mathbf{Z}(G/Z)$, so G/Y has nilpotence class $c - 2$.

Now Z^p is a normal subgroup of G, and we argue that Y/Z^p is central in G/Z^p. It suffices to show that $[y, g] \in Z^p$ for all elements $y \in Y$ and $g \in G$. If $g \in \mathcal{N}_p(G)$, then g is central, and thus $[y, g] = 1 \in Z^p$, as required. Otherwise, g is a pth power in G, and we can write $g = u^p$ for some element $u \in G$. Since $Y/Z = \mathbf{Z}(G/Z)$, it follows that $[y, u] \in Z$, and thus $[y, g] = [y, u^p] = [y, u]^p \in Z^p$, and this shows that Y/Z^p is central in G/Z^p, as claimed. Also, since G/Y has nilpotence class $c - 2$, it follows that the class of G/Z^p is at most $c - 1$.

Now write $\overline{G} = G/Z^p$, and let the overbar denote the canonical homomorphism from G onto $\overline{G}$. We wish to apply the inductive hypothesis to the group $\overline{G}$, so we must verify that $0 < n_p(\overline{G}) < \infty$ and $\mathcal{N}_p(\overline{G}) \subseteq \mathbf{Z}(\overline{G})$.

It suffices to show that $\mathcal{N}_p(\overline{G}) = \overline{\mathcal{N}_p(G)}$, or equivalently, that an element $x \in G$ is a pth power if and only if $\overline{x}$ is a pth power in $\overline{G}$. One direction of this is trivial: if $x = u^p$, then $\overline{x} = \overline{u^p} = (\overline{u})^p$. Conversely, suppose that $\overline{x} = (\overline{u})^p$ for some element $u \in G$. Then $\overline{x} = \overline{u^p}$, and thus x lies in the coset $u^p Z^p$. It follows that $x = u^p z^p = (uz)^p$ for some element $z \in Z$, and thus x is a pth power, as wanted.

By the inductive hypothesis, $|\overline{G}| < \infty$, so $|G : Z| \leq |G : Z^p| < \infty$, and thus by Lemma 3.1, we have $n_p(Z) \leq n_p(G) < \infty$. Also, $\mathcal{N}_p(G) \subseteq Z$, so $\mathcal{N}_p(G) \subseteq \mathcal{N}_p(Z)$, and thus $0 < n_p(Z)$. It follows by Lemma A that $|Z| < \infty$, and thus $|G| = |G : Z||Z| < \infty$. □

To prove the third part of Theorem C, we need two easy preliminary results.

Lemma 3.4. *Let $Z = \mathbf{Z}(G)$, and suppose $0 < n_p(G) < \infty$, where p is prime. Then*

(a) $|Z^p| \leq n_p(G)$.
(b) *Every element of Z has finite order at most $pn_p(G)$.*
(c) *If $x \in \mathcal{N}_p(G)$, then x has finite order at most $pn_p(G)$.*

Proof. Let $x \in \mathcal{N}_p(G)$. If $z \in Z$, we argue that $xz^p \in \mathcal{N}_p(G)$. Otherwise, $xz^p = u^p$ for some element $u \in G$, and thus $x = u^p z^{-p} = (uz^{-1})^p$, and this is a contradiction. We thus have $xZ^p \subseteq \mathcal{N}_p(G)$, and thus $|Z^p| = |xZ^p| \leq n_p(G)$, as required for (a).

For (b), let $z \in Z$. Then $\langle z^p \rangle \subseteq Z^p$, so $|\langle z^p \rangle| \leq n_p(G)$ by (a). Now (b) follows since $|\langle z \rangle| \leq p|\langle z^p \rangle|$.

To prove (c), let $C = \mathbf{C}_G(x)$. Then $|G : C| \le n_p(G) < \infty$ since all conjugates of x in G lie in $\mathcal{N}_p(G)$. By Lemma 3.1, therefore, we have $n_p(C) \le n_p(G)$. Also $x \in \mathcal{N}_p(C)$, so $0 < n_p(C)$, and since $x \in \mathbf{Z}(C)$, it follows by (b) that x has finite order at most $pn_p(C) \le pn_p(G)$, as required. □

Lemma 3.5. *Let $H \subseteq G$ have finite index divisible by a prime number p. If $n_p(G) < \infty$, then G is finite.*

Proof. We can replace H by the intersection of its G-conjugates, and hence it is no loss to assume that $H \lhd G$. Now G/H is a finite group with order divisible by p, so it contains an element of order p, and thus the pth-power map on G/H is not injective. It follows that this map is not surjective, and hence $\mathcal{N}_p(G/H)$ is nonempty. Let $X \in \mathcal{N}_p(G/H)$, where X is some coset of H. Now $X \subseteq \mathcal{N}_p(G)$, since otherwise, there exists an element $v \in G$ such that $v^p \in X$, and thus $X = Hv^p = (Hv)^p$, and this is a contradiction since X is a non-pth-power in G/H. It follows that $|H| = |X| \le n_p(G) < \infty$, and since $|G : H| < \infty$ by assumption, we conclude that $|G| < \infty$, as required. □

Recall now that a group G is said to be residually finite if the intersection of the finite-index normal subgroups of G is trivial. The following is the third part of Theorem C.

Theorem 3.6. *Assume that G is residually finite and that $0 < n_k(G) < \infty$. Then G is finite.*

Proof. As usual, we can assume that $k = p$ is prime, and we let $x \in \mathcal{N}_p(G)$. Then x has finite order by Lemma 3.4, and this order is divisible by p by Lemma 2.1. Some power y of x is thus a nonidentity element having p-power order, and since G is residually finite, there exists a finite-index subgroup $H \lhd G$ such that $y \notin H$. Then $Hy \in G/H$ is a nonidentity element with p-power order, and thus p divides $|G/H|$. It follows by Lemma 3.5 that $|G|$ is finite. □

References

[1] E. Bannai et al. On the number of elements which are not nth powers in finite groups, Comm. Algebra **17** (1989) 2865–2870

[2] L. Lévai and L. Pyber, “Profinite groups with many commuting pairs or involutions”, Arch. Math. **75** (2000) 1–7

[3] M. S. Lucido and M. R. Pournaki, Probability that an element of a finite group has a square root, Colloq. Math., **112** (2008) 147–155

[4] M. W. Liebeck and A. Shalev, Powers in finite groups and a criterion for solubility, Proc. Amer. Math. Soc. **141** (2013) 4179–4189

W. Cocke and I. M. Isaacs
Mathematics Department,
University of Wisconsin,
480 Lincoln Dr.,
Madison,
WI 53706, USA
e-mail: isaacs@math.wisc.edu

W. Cocke
e-mail: cocke@math.wisc.edu

D. Skabelund
Mathematics Department,
University of Illinois,
1409 W. Green St.,
Urbana,
IL 61801, USA
e-mail: skabelu2@illinois.edu

Received: 15 June 2015