Journal of Algebra 478 (2017) 153–173

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Generation of finite simple groups by an involution and an element of prime order

Carlisle S.H. King

Imperial College London, SW7 2AZ, United Kingdom

ARTICLE INFO

Article history:
Received 15 March 2016
Available online 16 January 2017
Communicated by Gunter Malle

Keywords:
Finite group theory
Generation of finite groups
Classical groups

ABSTRACT

We prove that every non-abelian finite simple group is generated by an involution and an element of prime order.

1. Introduction

Given a finite simple group G, it is natural to ask which elements generate G. Results of Miller [26], Steinberg [36], Aschbacher and Guralnick [2] prove that every finite simple group is generated by a pair of elements. A natural refinement is then to ask whether the orders of the generating elements may be restricted: given a finite simple group G and a pair of positive integers (a, b), does there exist a pair of elements $x, y \in G$ with x of order a and y of order b such that $G = \langle x, y \rangle$? If such a pair exists, we say G is (a, b)-generated.

As two involutions generate a dihedral group, the smallest pair of interest is $(2, 3)$. The question of which finite simple groups are $(2, 3)$-generated has been studied extensively. All alternating groups A_n except for $n = 3, 6, 7, 8$ are $(2, 3)$-generated by [26].

E-mail address: carlisle.king10@ic.ac.uk.

http://dx.doi.org/10.1016/j.jalgebra.2016.12.031
0021-8693/

All but finitely many simple classical groups not equal to $PSp_4(2^a), PSp_4(3^a)$ are $(2,3)$-generated by [21]. In fact, recent work by Pellegrini [29] completes the classification of the $(2,3)$-generated finite simple projective special linear groups, which shows that $PSL_n(q)$ is $(2,3)$-generated for $(n,q) \neq (2,9),(3,4),(4,2)$. There is also literature on the $(2,3)$-generation of many other simple classical groups $Cl_n(q)$, showing a positive result for large n explicitly listed (for example, see [33]). All simple exceptional groups except for ${}^2B_2(2^{2m+1})$ (which contain no elements of order 3) are $(2,3)$-generated by [22]. And all sporadic simple groups except for M_{11}, M_{22}, M_{23} and McL are $(2,3)$-generated by [42].

Nevertheless, the problem of determining exactly which finite simple groups are $(2,3)$-generated, or more generally $(2,p)$-generated for some prime p, remains open. In this paper, we prove:

Theorem 1. *Every non-abelian finite simple group G is generated by an involution and an element of prime order.*

By [26], for $n \geq 5$ and $n \neq 6,7,8$, the alternating groups A_n are $(2,3)$-generated, and by [27] these exceptions are $(2,5)$-generated. By [22] the exceptional groups not equal to ${}^2B_2(2^{2m+1})$ are $(2,3)$-generated, and by [9] the Suzuki groups are $(2,5)$-generated. By [42] the sporadic groups not equal to $M_{11}, M_{22}, M_{23}, McL$, are $(2,3)$-generated, and by [41] these exceptions are $(2,p)$-generated for $p = 11,5,23,5$ respectively (in fact, all of these exceptions are $(2,5)$-generated, which can be seen using GAP). By Lemma 2.4 below, the 4-dimensional symplectic groups $PSp_4(2^a)$ $(a > 1)$, $PSp_4(3^a)$ are $(2,5)$-generated, and when combined with Lemmas 2.1 and 2.2, this shows that all finite simple classical groups with natural module of dimension $n \leq 7$ (and $P\Omega_8^+(2)$) are $(2,p)$-generated for some $p \in \{3,5,7\}$.

By Zsigmondy's theorem [43], for $q, e > 1$ with $(q,e) \neq (2^a-1,2),(2,6)$, there exists a prime divisor $r = r_{q,e}$ of $q^e - 1$ such that r does not divide $q^i - 1$ for $i < e$. We call r a primitive prime divisor of $q^e - 1$. Notice that, in general, $r_{q,e}$ is not uniquely determined by (q,e). In the group $(\mathbb{F}_r)^\times$, q has order e, and so $r \equiv 1 \bmod e$. In view of the above discussion, Theorem 1 follows from the following result.

Theorem 2. *Let G be a finite simple classical group with natural module of dimension n over $\mathbb{F}_{q^\delta}$, where $\delta = 2$ if G is unitary and $\delta = 1$ otherwise. Assume $n \geq 8$ and $G \neq P\Omega_8^+(2)$. Let r be a primitive prime divisor of $q^e - 1$, where e is listed in Table 1. Then G is $(2,r)$-generated.*

We note that r is well-defined for the groups described in Theorem 2.

There is a large literature on other aspects of the generation of finite simple groups, and we note just a few results. In [24], it is shown that every non-abelian finite simple group other than $PSU_3(3)$ is generated by three involutions. In [11], and proved independently in [35], it is shown that, given a finite simple group G, there exists a conjugacy