## MATEMATUKA И MATEMATUYECKO ОБРАЗОВАНИЕ, 2015 MATHEMATICS AND EDUCATION IN MATHEMATICS, 2015

Proceedings of the Forty Fourth Spring Conference of the Union of Bulgarian Mathematicians SOK "Kamchia", April 2–6, 2015

# (2, 3)-GENERATION OF THE SPECIAL LINEAR GROUPS OF DIMENSION $\mathbf{8}^*$

Ts. Genchev, E. Gencheva

We prove that the group  $PSL_8(q)$  is (2,3)-generated for any q. Actually, we find out explicit generators x and y of respective orders 2 and 3, for the group  $SL_8(q)$ .

1. Introduction. A group G is said to be (2,3)-generated if it can be generated by an involution and an element of order 3. It is well known that the famous modular group  $PSL_2(\mathbb{Z})$  is isomorphic to the free product of a cyclic group of order 2 and a cyclic group of order 3. Thus, a group (of order at least 6) appears as an epimorphic image of  $PSL_2(\mathbb{Z})$  if and only if it is a (2,3)-generated group. Many series of finite simple groups have been investigated with respect to this generation property. Almost all of them are (2,3)-generated. The most powerful (probabilistic) result in this direction is the theorem of Liebeck-Shalev and Lübeck-Malle (see Theorem 2 in [14]). This theorem states that all finite simple groups, except the symplectic groups  $PSp_4(2^k)$ ,  $PSp_4(3^k)$ , the Suzuki groups  $Sz(2^{2l+1})$  (which have no elements of order 3), and finitely many other groups, are (2,3)-generated. All these so far known exceptions, for groups of Lie type, occur in small dimensions over small fields. In more recent works ([12],[11],[10]) the authors have dealt with the classification of the finite classical simple groups of dimension up to 6 which are (2,3)-generated. They use uniform arguments to treat these groups. As far as it concerns the projective special linear groups  $PSL_n(q)$ , (2, 3)-generation has been proved in the cases  $n = 2, q \neq 9$  [8],  $n = 3, q \neq 4$  [5], [2],  $n = 4, q \neq 2$  [16], [15], [9], [12], n = 5, any q [19], [11], n = 6, any q [18], n = 7, any q [17],  $n \ge 5$ , odd  $q \ne 9$  [3], [4], and  $n \ge 13$ , any q [13]. The present paper continues the investigation of the finite simple linear groups in small dimensions. We prove the following:

**Theorem.** The group  $PSL_8(q)$  is (2,3)-generated for any q.

Thus, we have covered the missing in [4] cases q = 9 and q even which is our contribution to the problem.

To prove the theorem, we shall employ the same technique developed by Kerope Bartev Tchakerian who passed away in 2012. This technique, which has been used in [9], [19], [18] and [17], relies on the known list of maximal subgroups of  $PSL_8(q)$  and is quite different from that of the authors of [4]. Their approach is based on the classification of finite irreducible linear groups generated by root subgroups.

The paper is dedicated to the bright memory of our great teacher and friend Prof. Tchakerian.

<sup>\*2010</sup> Mathematics Subject Classification: 20F05, 20D06. Key words: (2,3)-generated group.

**2. Proof of the Theorem.** Let  $G = SL_8(q)$  and  $\overline{G} = G/Z(G) = PSL_8(q)$ , where  $q = p^m$  and p is a prime number. Set d = (8, q - 1). The group G acts naturally on the left on the eight-dimensional column vector space  $V = F^8$  over the field F = GF(q) and  $\overline{G}$  acts on the corresponding projective space P(V). We denote by  $v_1, \ldots, v_8$  the standard base of the space V, i.e.,  $v_i$  is a column which has 1 as its i-th coordinate, while all other coordinates are zeros.

We shall make use of the known list of maximal subgroups of  $\overline{G}$  given in [1]. In Aschbaher's notation any maximal subgroup of  $\overline{G}$  belongs to one of the following families  $C_1, C_2, C_3, C_4, C_5, C_6, C_8$ , and S. Roughly speaking, they are:

- $C_1$ : stabilizers of subspaces of P(V),
- $C_2$ : stabilizers of direct sum decompositions of P(V),
- $C_3$ : stabilizers of extension fields of F of prime degree,
- $C_4$ : stabilizers of tensor product decompositions of P(V),
- $C_5$ : stabilizers of subfields of F of prime index,
- $C_6$ : normalizers of extraspecial groups in absolutely irreducible representations,
- $C_8$ : classical subgroups,
- S: almost simple subgroups, absolutely irreducible on P(V), and their simple base cannot be realized over a proper subfield of F; not continued in members of  $C_8$ .

In [1] all maximal subgroups of  $\overline{G}$  are given in detail with their exact structure. For instance, the stabilizers of 1-subspaces or hyperplanes of P(V) (in the family  $C_1$  of reducible subgroups of  $\overline{G}$ ) are isomorphic to the group  $[q^7]: GL_7(q)/Z_d$  which is a homomorphic image of a split extension of a group of order  $q^7$  by the general linear group  $GL_7(q)$ . This type of maximal subgroups play a key role in our considerations. (Here we use the notation [l] as an indication for an arbitrary group of order l.)

In order to prove the theorem we have accepted the following well working (at least for linear groups of dimension  $\leq 12$ ) strategy. Firs we are looking for a maximal subgroup of  $\overline{G}$  containing an element of unique order—no one of the other types maximal subgroups of  $\overline{G}$  can contain elements of such an order. In the second step we find out two elements of respective orders 2 and 3 in  $\overline{G}$  such that their product has got this unique order. Finally, we prove that the group generated by these two elements is not contained in the corresponding type maximal subgroup of  $\overline{G}$ . In our case it is not difficult to choose such an order (with small specific correction, so that to cover almost all values of q in the final stage). Namely, let us put  $Q = q^7 - 1$  if  $q \neq 7$  and  $Q = (q^7 - 1)/2$  if q = 7. Obviously the above-mentioned stabilizers contain elements of order Q/(d,Q). Now it can be easily checked, for example using the well-known Zsigmondy's theorem, that no one of the other types of maximal subgroups of  $\overline{G}$  has order divisible by Q/(d,Q). Indeed, let us take a primitive prime divisor of  $p^{7m}-1$ , i.e., a prime r which divides  $p^{7m}-1$ but does not divide  $p^i - 1$  for 0 < i < 7m. We have  $r \ge 29$  (as r - 1 is a multiple of 7m) and hence r divides Q/(d,Q). A quick inspection of the orders of other reducible subgroups, all the groups of the remaining families  $C_2, C_3, C_4, C_5, C_6, C_8$  of irreducible geometric subgroups of  $\overline{G}$ , also in the S-family leads to the following conclusion. The only one subgroup of order divisible by r belongs to the  $C_8$ -family and it is isomorphic to  $PSU_8(q_0).[\frac{c}{d}.(8,q_0+1)]$  if m is even,  $q=q_0^2$  and  $c=q-1/[\frac{q-1}{d},q_0+1]$  (in fact,this is done in [7], Section 2.5). From the given structure of this subgroup (by simple arithmetic 168

computations) one can deduce that its order is equal to

$$q_0^{28}(q_0^2-1)(q_0^3+1)(q_0^4-1)(q_0^5+1)(q_0^6-1)(q_0^7+1)(q_0^8-1)/s$$
,

where s = 1, 2 or 4, and it is not difficult to see that this order is not divisible by Q/(d, Q). In this way we have proved the following:

**Lemma 1.** For any maximal subgroup of the group  $\overline{G}$  either it stabilizes 1-subspace or hyperplane of P(V) or it has no element of order Q/(d,Q).

Now we are ready to proceed with the next steps in our strategy.

**2.1.** We first suppose that q > 3. Let us choose an element  $\omega$  of order Q in the multiplicative group of the field  $GF(q^7)$  and let

$$f(t) = (t - \omega)(t - \omega^q)(t - \omega^{q^2})(t - \omega^{q^3})(t - \omega^{q^4})(t - \omega^{q^5})(t - \omega^{q^6})$$
  
=  $t^7 - at^6 + bt^5 - ct^4 + dt^3 - et^2 + ht - g$ .

Then  $f(t) \in F[t]$  and the polynomial f(t) is irreducible over the field F. Note that  $g = \omega^{\frac{q^7-1}{q-1}}$  has order q-1 if  $q \neq 7$ , and  $g^3 = 1 \neq g$  if q = 7.

Now let 
$$x = \begin{bmatrix} 0 & 0 & -1 & 0 & 0 & dg^{-1} & 0 & e \\ 0 & 0 & 0 & 0 & 0 & ag^{-1} & -1 & h \\ -1 & 0 & 0 & 0 & 0 & eg^{-1} & 0 & d \\ 0 & 0 & 0 & 0 & -1 & cg^{-1} & 0 & b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g \\ 0 & -1 & 0 & 0 & 0 & hg^{-1} & 0 & a \\ 0 & 0 & 0 & 0 & 0 & g^{-1} & 0 & 0 \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$
Then  $x$  and  $y$  are elements of  $G$  of orders 2 and 3, respectively. Denote

Then x and y are elements of G of orders 2 and 3, respectively. Denote

$$z = xy = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 & e & dg^{-1} \\ 0 & 0 & 0 & 0 & 0 & -1 & h & ag^{-1} \\ -1 & 0 & 0 & 0 & 0 & 0 & d & eg^{-1} \\ 0 & 0 & 0 & 0 & -1 & 0 & b & cg^{-1} \\ 0 & 0 & -1 & 0 & 0 & 0 & c & bg^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & g & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & a & hg^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g^{-1} \end{bmatrix}.$$

The characteristic polynomial of z is  $f_z(t) = (t - g^{-1})f(t)$  and the characteristic roots  $g^{-1}$ ,  $\omega$ ,  $\omega^q$ ,  $\omega^{q^2}$ ,  $\omega^{q^3}$ ,  $\omega^{q^4}$ ,  $\omega^{q^5}$ , and  $\omega^{q^6}$  of z are pairwise distinct. Then, in  $GL_8(q^7)$ , z is conjugate to the matrix diag  $(g^{-1}, \omega, \omega^q, \omega^{q^2}, \omega^{q^3}, \omega^{q^4}, \omega^{q^5}, \omega^{q^6})$  and hence z is an element of G of order Q.

Let H be the subgroup of G generated by the above elements x and y.

**Lemma 2.** The group H can not stabilize 1-subspaces or hyperplanes of the space V or equivalently H acts irreducible on V.

**Proof.** Assume that W is an H-invariant subspace of V and  $k = \dim W$ , k = 1 or 7. Let first k=1 and  $0 \neq w \in W$ . Then  $y(w)=\lambda w$ , where  $\lambda \in F$  and  $\lambda^3=1$ . This yields

$$w = \mu_1 v_1 + \mu_2 (\lambda^2 v_2 + \lambda v_3 + v_4) + \mu_3 v_5 + \mu_4 (\lambda^2 v_6 + \lambda v_7 + v_8) \quad (\mu_1, \mu_2, \mu_3, \mu_4 \in F),$$

where  $\mu_1 = \mu_3 = 0$  if  $\lambda \neq 1$ . Now  $x(w) = \nu w$ , where  $\nu = \pm 1$ . This yields consecutively  $\mu_4 \neq 0$ ,  $\lambda = \nu g^{-1}$ , and

(1) 
$$\mu_2 = \mu_4 (hg^{-1} + a\lambda - \nu\lambda^2),$$

(2) 
$$\nu \mu_1 + \lambda \mu_2 = (d\nu + e)\mu_4,$$

(3) 
$$\mu_2 + \nu \mu_3 = (b\nu + c)\mu_4.$$

In particular, we have  $g^3 = \nu$  and  $g^6 = 1$ . This is impossible if q = 5 or q > 7 since then g has order q - 1. Thus (as q > 3) q = 4 or q = 7 and, in both cases,  $g^3 = 1 \neq g$ . So  $\nu = 1$ ,  $\lambda = g^2 \neq 1$  and it follows that  $\mu_1 = \mu_3 = 0$ . Then (1), (2), (3) produce  $a = (d + e + 1)g^2 - h$  and b = (d + e)g - c. Now  $f(-1) = -(d + e + 1)(1 + g + g^2) = 0$  both for q = 4 and q = 7, a contradiction as f(t) is irreducible over the field F.

Now let k=7. The subspace U of V which is generated by the vectors  $v_1, v_2, v_3, v_4, v_5, v_6$ , and  $v_7$  is  $\langle z \rangle$ -invariant. If  $W \neq U$  then  $U \cap W$  is  $\langle z \rangle$ -invariant and dim  $(U \cap W) = 6$ . This means that the characteristic polynomial of  $z|_{U \cap W}$  has degree 6 and must divide  $f_z(t)$  which is impossible as f(t) is irreducible over F. Thus W = U but obviously U is not  $\langle y \rangle$ -invariant, a contradiction.

The lemma is proved. (Note that the statement is false for q=2 or 3.)

Now, in  $\overline{G}$ , the elements  $\overline{x}$  and  $\overline{y}$  have orders 2 and 3, respectively, and (as easily seen by the above-mentioned diagonal matrix)  $\overline{z} = \overline{x} \cdot \overline{y}$  has order Q/(d,Q). So the group  $\overline{H} = \langle \overline{x}, \overline{y} \rangle$  has an element of order Q/(d,Q) and  $\overline{H}$  is irreducible on P(V) as H is irreducible on V by Lemma 2. Then Lemma 1 implies that  $\overline{H}$  cannot be contained in any maximal subgroup of  $\overline{G}$ . Thus  $\overline{H} = \overline{G}$  and  $\overline{G} = \langle \overline{x}, \overline{y} \rangle$  is a (2,3)-generated group.

**2.2.** Lastly we suppose that q=2 or 3. We treat both cases simultaneously. Let us denote by  $x_q$  and  $y_q$  possible generators of  $SL_8(q)$  of respective orders 2 and 3. Now we shall prove that the projective images of the matrices  $x_q$  and  $y_q$  below can really generate  $PSL_8(q)$  in these cases. Let us choose the involutions  $x_2$  and  $x_3$ , also the elements  $y_2$  and  $y_3$  of order 3 to be as follows.

$$x_3 = \begin{bmatrix} 0 & -1 & -1 & 1 & -1 & 1 & 0 & 1 \\ -1 & 0 & -1 & 1 & -1 & 1 & 0 & 1 \\ 0 & -1 & -1 & 0 & -1 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 1 & 1 & -1 & -1 & 0 & -1 \\ -1 & -1 & 0 & -1 & -1 & 1 & 1 & 1 \\ 0 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \end{bmatrix}, y_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & -1 & 1 & -1 & 0 \\ 1 & 1 & 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & 1 & -1 & 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 1 & 1 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & -1 & 1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & -1 \\ 0 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 0 & -1 & -1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Now

The characteristic polynomial of  $z_q$  is  $f_{z_q}(t) = (t+1)g_q(t)$ , where  $g_2(t) = t^7 + t + 1$  and  $g_3(t) = t^7 + t^6 + t^2 + 1$ . In any case the polynomial  $g_q(t)$  is irreducible over the field GF(q) and all its roots have order  $q^7 - 1$  in  $GF(q^7)^*$  (see [6], Table C). It follows that the element  $z_q$  of  $SL_8(q)$  has order  $q^7 - 1 = Q$ .

As in the proof of Lemma 2, it can be checked that the group  $H_q=\langle x_q,y_q\rangle$  acts irreducibly on the space V. Indeed, let  $W=\langle w\rangle$  be a 1-subspace of V which is stabilized by  $H_q$ . Then  $y_q(w)=w$  yields to  $w=\mu_1v_1+\mu_2(v_2+v_3)+\mu_1(v_6+v_7)+\mu_2v_8$  (if q=2) and  $w=(-\mu_5+\mu_7)v_1+(\mu_5-\mu_6-\mu_7)v_2+(\mu_5-\mu_6+\mu_7)v_3+(\mu_5-\mu_7)v_4+\mu_5v_5+\mu_6v_6+\mu_7v_7+(\mu_5+\mu_6+\mu_7)v_8$  (if q=3), where  $\mu_1,\mu_2\in GF(2)$ , and  $\mu_5,\mu_6,\mu_7\in GF(3)$ . Now  $x_2(w)=w$  and  $x_3(w)=\nu w$  ( $\nu=\pm 1$ ) force to  $\mu_1=\mu_2=0$ , and  $\nu=-1$ ,  $\mu_5=\mu_6=\mu_7=0$ , respectively, an impossibility as  $w\neq 0$ . If W is a hyperplane of V (i.e.,  $\dim(W)=7$ ) which is invariant under the action of  $H_q$  we can obtain a contradiction (taking into account the exact form of  $z_q$ ) just as in the proof of Lemma 2.

Now, to finalize our considerations it is enough to see that, in  $PSL_8(q)$ , the elements  $\overline{x_q}$ ,  $\overline{y_q}$ , and  $\overline{z_q}$  have orders 2, 3, and Q/d, respectively. So the group  $\overline{H_q} = \langle \overline{x_q}, \overline{y_q} \rangle$  contains an element of order Q/d and acts irreducibly on P(V). According to Lemma 1 this means that  $\overline{H_q} = PSL_8(q)$  and  $PSL_8(q) = \langle \overline{x_q}, \overline{y_q} \rangle$  is a (2,3)-generated group in these cases.

The theorem is proved.  $\square$ 

**Acknowledgement.** The authors are very grateful to Prof. Marco Antonio Pellegrini who provided them with generators of the groups  $SL_8(2)$  and  $SL_8(3)$ .

#### REFERENCES

- [1] J. N. Bray, D. F. Holt, C. M. Roney-Dougal. The Maximal Subgroups of the Low-Dimensional Finite Classical Groups. London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.
- [2] J. COHEN. On non-Hurwitz groups and noncongruence of the modular group. *Glasgow Math. J.*, **22** (1981), 1–7.
- [3] L. DI MARTINO, N. A. VAVILOV. (2,3)-generation of  $SL_n(q)$ . I. Cases n = 5, 6, 7. Comm. Alg., 22, No 4 (1994), 1321–1347.
- [4] L. DI MARTINO, N. A. VAVILOV. (2,3)-generation of  $SL_n(q)$ . II. Cases  $n \geq 8$ . Comm. Alg., **24**, No 2 (1996), 487–515.
- [5] D. GARBE. Über eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe. *Math. Ann.*, **235**, No 3 (1978), 195–215.
- [6] R. Lidl, H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications vol. 20. Reading, Massachusetts etc., Addison-Wesley Company. Advanced Book Program, 1983.
- [7] M. W. LIEBECK, C. E. PRAEGER, J. SAXL. The Maximal Factorizations of the Finite Simple Groups and Their Automorphism Groups. *Mem. Amer. Math. Soc.*, 86, No 432 (1990).
- [8] A. M. MACBEATH. Generators of the linear fractional group. Proc. Symp. Pure Math., 12 (1969), 14–32.
- [9] P. MANOLOV, K. TCHAKERIAN. (2,3)-generation of the groups  $PSL_4(2^m)$ . Ann. Univ. Sofia, Fac. Math. Inf., **96** (2004), 101–104.
- [10] M. A. Pellegrini, M. Prandelli, M. C. Tamburini Bellani. The (2,3)-generation of the special unitary groups of dimension 6. arXiv: 1409.3411v2, 2015.
- [11] M. A. Pellegrini, M. C. Tamburini Bellani. The simple classical groups of dimension less than 6 which are (2, 3)-generated. arXiv: 1405.3149v2, 2015.
- [12] M. A. Pellegrini, M. C. Tamburini Bellani, M. A. Vsemirnov. Uniform (2, k)-generation of the 4-dimensional classical groups. *J. Algebra*, **369**, (2012), 322–350
- [13] P. Sanchini, M. C. Tamburini. Constructive (2,3)-generation: a permutational approach. Rend. Sem. Mat. Fis. Milano, 64 (1994), 141–158.
- [14] A. Shalev. Asymptotic group theory. *Notices Amer. Math. Soc.*, **48**, No 4 (2001), 383–389.
- [15] M. C. Tamburini, S. Vassallo. (2,3)-generazione di gruppi lineari. Scritti in onore di Giovanni Melzi. Sci. Mat., 11 (1994), 391–399.
- [16] M. C. Tamburini, S. Vassallo. (2,3)-generazione di  $SL_4(q)$  in caratteristica dispari e problemi collegati. Boll. Un. Mat. Ital. B(7), 8 (1994), 121–134.
- [17] K. TABAKOV. (2,3)-generation of the groups  $PSL_7(q)$ . Math. and Education in Math., 42 (2013), 260–264.

- [18] K. TABAKOV, K. TCHAKERIAN. (2,3)-generation of the groups  $PSL_6(q)$ . Serdica Math. J., **37**, No 4 (2011), 365–370.
- [19] K. TCHAKERIAN. (2,3)-generation of the groups  $PSL_5(q)$ . Ann. Univ. Sofia, Fac. Math. Inf., 97 (2005), 105–108.

Ts. Genchev

e-mail: genchev57@yahoo.com

E. Gencheva

e-mail: elenkag@abv.bg
Department of Mathematics
Technical University
Varna, Bulgaria

## (2,3)-ПОРОДЕНОСТ НА ГРУПИТЕ $PSL_8(q)$

### Ц. Генчев, Е. Генчева

В настоящата работа разглеждаме крайните прости линейни групи от размерност 8 и доказваме, че те са епиморфни образи на добре известната модулярна група  $PSL_2(\mathbb{Z})$ . Последното означава, че групата  $PSL_8(q)$  се поражда от един свой елемент от ред 2 (инволюция) и още един елемент от ред 3. Предложеното доказателство е в сила за произволно крайно поле GF(q), над което е дефинирана тази група. Всъщност ние посочваме в явен вид две матрици, от редове две и три съответно, които пораждат групата  $SL_8(q)$ .