МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2017
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2017
Proceedings of the Forty-sixth Spring Conference
of the Union of Bulgarian Mathematicians
Borovets, April 9–13, 2017

ABOUT THE (2,3)-GENERATION OF THE SPECIAL LINEAR GROUPS OF DIMENSION 12*

Tsanko Genchev, Elenka Gencheva

We provide explicit uniform type $(2,3)$-generators for the special linear group $SL_{12}(q)$ for all q except for $q = 2$ or $q = 4$. Our considerations are easily traceable, self-contained and based only on the known list of maximal subgroups of this group

1. Introduction. $(2,3)$-generated groups are those groups which can be generated by an involution and an element of order 3 or, equivalently, the groups appearing to be homomorphic images of the famous modular group $PSL_2(\mathbb{Z})$. Now the problem concerning the $(2,3)$-generation (especially) of the special linear groups and their projective images is completely solved (see [2–7, 9–17, 20]). A short survey can be found in [11]. First attempt to treat the special linear groups with respect to this generation property was made by Tamburini in [18] where she proved the $(2,3)$-generation of $SL_n(q)$ for all $n \geq 25$ and all prime power q. The same author improved in [19] the lower bound of the dimensions n by proving the $(2,3)$-generation of $SL_n(q)$ for all $n \geq 13$ and no restrictions on q. Meanwhile, Di Martino and Vavilov proved in [3] and [4] the $(2,3)$-generation of the special linear groups of dimensions not less than 5 over all finite fields in odd characteristic and number of elements not 9. In the present paper we give our contribution to the problem by discussing the last remaining group $SL_{12}(q)$ in the light of the method used in our works [6], [15] and [7]. The $(2,3)$-generation of the same group over all finite fields has been proved in [11]. Our 3-generator is the same as in [11], but the 2-generators have an unique form. The author's (in particular permutational) approach in [11] is quite different from ours in which we make an essential use of the known list of maximal subgroups of $SL_{12}(q)$. Based on the note [8] we prove the following:

Theorem. *The group* $SL_{12}(q)$ *is* $(2,3)$*-generated for any* $q \neq 2$ *and* 4.

2. Proof of the Theorem. Let $G = SL_{12}(q)$, where $q = p^m$ and p is a prime. Set $Q = q^{11} - 1$ if $q \neq 3, 7$ and $Q = (q^{11} - 1)/2$ if $q = 3, 7$. The group G acts naturally on a twelve-dimensional vector space V over the field $F = GF(q)$. We identify V with the column vectors of F^{12}, and let $v_1, \ldots, v_{12}$ be 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.

Now, let us choose an element ω of order Q in the multiplicative group of the field $GF(q^{11})$ and set

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

$f(t) = (t-\omega)(t-\omega^{q})(t-\omega^{q^2})(t-\omega^{q^3})(t-\omega^{q^4})(t-\omega^{q^5})(t-\omega^{q^6})(t-\omega^{q^7})(t-\omega^{q^8})(t-\omega^{q^9})(t-\omega^{q^{10}}) = t^{11} - \alpha_1 t^{10} + \alpha_2 t^9 - \alpha_3 t^8 + \alpha_4 t^7 - \alpha_5 t^6 + \alpha_6 t^5 - \alpha_7 t^4 + \alpha_8 t^3 - \alpha_9 t^2 + \alpha_{10} t - \alpha_{11}$.

Then $f(t) \in F[t]$ and the polynomial $f(t)$ is irreducible over the field F. Note that $\alpha_{11} = \omega^{\frac{q^{11}-1}{q-1}}$ has order $q-1$ if $q \neq 3, 7$, $\alpha_{11} = 1$ if $q = 3$, and $\alpha_{11}^3 = 1 \neq \alpha_{11}$ if $q = 7$.

Now, the matrices

$$x = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_6\alpha_{11}^{-1} & 0 & \alpha_6 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_5\alpha_{11}^{-1} & 0 & \alpha_5 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & \alpha_4\alpha_{11}^{-1} & 0 & \alpha_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & \alpha_3\alpha_{11}^{-1} & 0 & \alpha_9 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & \alpha_8\alpha_{11}^{-1} & 0 & \alpha_8 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_7\alpha_{11}^{-1} & 0 & \alpha_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_1\alpha_{11}^{-1} & -1 & \alpha_{10} \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & \alpha_9\alpha_{11}^{-1} & 0 & \alpha_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & \alpha_2\alpha_{11}^{-1} & 0 & \alpha_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{11} \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & \alpha_{10}\alpha_{11}^{-1} & 0 & \alpha_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{11}^{-1} & 0 & 0 \end{bmatrix}$$

and

$$y = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

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

$$z = xy = \begin{bmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_6 & \alpha_6\alpha_{11}^{-1} \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_5 & \alpha_5\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & \alpha_7 & \alpha_4\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & \alpha_9 & \alpha_3\alpha_{11}^{-1} \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_8 & \alpha_8\alpha_{11}^{-1} \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_4 & \alpha_7\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & \alpha_{10} & \alpha_1\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & \alpha_3 & \alpha_9\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & \alpha_2 & \alpha_2\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{11} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & \alpha_1 & \alpha_{10}\alpha_{11}^{-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{11}^{-1} \end{bmatrix}.$$

The characteristic polynomial of z is $f_z(t) = (t - \alpha_{11}^{-1})f(t)$ and the characteristic roots α_{11}^{-1}, ω, ω^q, ω^{q^2}, ω^{q^3}, ω^{q^4}, ω^{q^5}, ω^{q^6}, ω^{q^7}, ω^{q^8}, ω^{q^9}, and $\omega^{q^{10}}$ of z are pairwise distinct. Then, in $GL_{12}(q^{11})$, z is conjugate to the matrix diag $(\alpha_{11}^{-1}$, ω, ω^q, ω^{q^2}, ω^{q^3}, ω^{q^4}, ω^{q^5}, ω^{q^6}, ω^{q^7}, ω^{q^8}, ω^{q^9}, $\omega^{q^{10}})$ and hence z is an element of $SL_{12}(q)$ of order Q.

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

Lemma 2.1. *The group H acts irreducible on the space V.*

Proof. Assume that W is an H-invariant subspace of V and $k = \dim W$, $1 \le k \le 11$.

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

$$w = \mu_1(v_1+\lambda^2 v_2+\lambda v_3)+\mu_2(v_4+\lambda^2 v_5+\lambda v_6)+\mu_3(v_7+\lambda^2 v_8+\lambda v_9)+\mu_4(v_{10}+\lambda^2 v_{11}+\lambda v_{12}),$$

where μ_1, μ_2, μ_3, and μ_4 are elements of the field F.

Now, we involve the action of x onto w: $x(w) = \nu w$ where $\nu = \pm 1$. This yields consecutively $\mu_4 \neq 0$, $\alpha_{11} = \lambda^2 \nu$, and

(1) $$\mu_3 = \lambda(\alpha_1 + \nu\alpha_{10} - \lambda\nu)\mu_4,$$

(2) $$\nu\mu_1 + \mu_2 = (\nu\alpha_4 + \alpha_7)\mu_4,$$

(3) $$\nu\mu_2 + \lambda^2\mu_3 = \lambda(\nu\alpha_3 + \alpha_9)\mu_4,$$

(4) $$(\nu + 1)(\mu_1 - \lambda\alpha_6\mu_4) = 0,$$

(5) $$(\nu + 1)(\mu_1 - \lambda^2\alpha_5\mu_4) = 0,$$

(6) $$(\nu + 1)(\mu_2 - \lambda^2\alpha_8\mu_4) = 0,$$

(7) $$(\nu + 1)(\mu_3 - \alpha_2\mu_4) = 0.$$

In particular, we have $\alpha_{11}^3 = \nu$ and $\alpha_{11}^6 = 1$. This is impossible if $q = 5$ or $q > 7$ since then α_{11} has order $q-1$. According to our assumption ($q \neq 2, 4$) only two possibilities are left: $q = 3$ (and $\alpha_{11} = 1$) or $q = 7$ (and $\alpha_{11}^3 = 1 \neq \alpha_{11}$). So $\nu = 1$, $\alpha_{11} = \lambda^2$ and (1), (2), (3), (4), (5), (6) and (7) produce $\alpha_1 = \lambda^2\alpha_2 - \alpha_{10} + \lambda$, $\alpha_6 = \lambda\alpha_5$, $\alpha_7 = \lambda^2\alpha_5 + \lambda^2\alpha_8 - \alpha_4$ and $\alpha_9 = \lambda\alpha_2 + \lambda\alpha_8 - \alpha_3$. Now $f(-1) = -(1 + \lambda + \lambda^2)(1 + \alpha_2 + \alpha_5 + \alpha_8) = 0$ both for $q = 3$ and $q = 7$, an impossibility as $f(t)$ is irreducible over the field F.

Now let $2 \le k \le 11$. Then the characteristic polynomial of $z|_W$ has degree k and has to divide $f_z(t) = (t - \alpha_{11}^{-1})f(t)$.The irreducibility of $f(t)$ over F leads immediately to the conclusion that this polynomial is $f(t)$ and $k = 11$. Now the subspace U of V which is generated by the vectors v_1, v_2, v_3, $\dots$, v_{11} is $\langle z\rangle$-invariant. If $W \neq U$ then $U \cap W$ is $\langle z\rangle$-invariant and dim $(U \cap W) = 10$. This means that the characteristic polynomial of $z|_{U\cap W}$ has degree 10 and must divide $f_z(t) = (t - \alpha_{11}^{-1})f(t)$ which is impossible. Thus $W = U$ but obviously U is not $\langle y\rangle$-invariant, a contradiction.

The lemma is proved. (Note that the above considerations fail if $q = 2$ or $q = 4$.) $\square$

Lemma 2.2. *Let M be a maximal subgroup of G having an element of order Q. Then M belongs to the class of reducible subgroups of G.*

Proof. Suppose false. The list of maximal subgroups of G is given in Tables 8.76 and 8.77 in [1]. This readily implies that one of the following holds:

1. $|M| = 12!(q-1)^{11}$ if $q > 4$.
2. $|M| = 720q^6(q-1)^{11}(q+1)^6$ if $q > 2$.
3. $|M| = 24q^{12}(q-1)^3(q^2-1)^4(q^3-1)^4$.
4. $|M| = 6q^{18}(q-1)^2(q^2-1)^3(q^3-1)^3(q^4-1)^3$.
5. $|M| = 2q^{30}(q-1)(q^2-1)^2(q^3-1)^2(q^4-1)^2(q^5-1)^2(q^6-1)^2$.
6. $|M| = 2q^{30}(q+1)(q^4-1)(q^6-1)(q^8-1)(q^{10}-1)(q^{12}-1)$.
7. $|M| = 3q^{18}(q^2+q+1)(q^6-1)(q^9-1)(q^{12}-1)$.
8. $|M| = (2, q-1)q^{16}(q^2-1)^2(q^3-1)(q^4-1)(q^5-1)(q^6-1)$ if $q > 2$.
9. $|M| = q^9(q^2-1)^2(q^3-1)^2(q^4-1)$.
10. $M \cong SL_{12}(q_0).[(12, \dfrac{q-1}{q_0-1})]$ if $q = q_0^r$ and r is a prime,
    $|M| = (12, \dfrac{q-1}{q_0-1})q_0^{66}(q_0^2-1)(q_0^3-1)(q_0^4-1)(q_0^5-1)(q_0^6-1)(q_0^7-1)(q_0^8-1)(q_0^9-1)(q_0^{10}-1)(q_0^{11}-1)(q_0^{12}-1)$.
11. $M \cong SO_{12}^+(q).[(12, q-1)]$ if q is odd,
    $|M| = (12, q-1)q^{30}(q^2-1)(q^4-1)(q^6-1)^2(q^8-1)(q^{10}-1)$.
12. $M \cong SO_{12}^-(q).[(12, q-1)]$ if q is odd,
    $|M| = (12, q-1)q^{30}(q^2-1)(q^4-1)(q^8-1)(q^{10}-1)(q^{12}-1)$.
13. $M \cong Sp_{12}(q).[(6, q-1)]$,
    $|M| = (6, q-1)q^{36}(q^2-1)(q^4-1)(q^6-1)(q^8-1)(q^{10}-1)(q^{12}-1)$.
14. $M \cong SU_{12}(q_0).[(12, q_0-1)]$ if $q = q_0^2$,
    $|M| = (12, q_0-1)q_0^{66}(q_0^2-1)(q_0^3+1)(q_0^4-1)(q_0^5+1)(q_0^6-1)(q_0^7+1)(q_0^8-1)(q_0^9+1)(q_0^{10}-1)(q_0^{11}+1)(q_0^{12}-1)$.
15. $M \cong (12, q-1) \circ 2^{\cdot}L_2(23)$ if $q = p \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \pmod{23}$ and $p \neq 2$,
    $|M|$ is a divisor of $2^5.3^2.11.23$.
16. $M \cong 12^{\cdot}L_3(4)$ if $q = 49$,
    $|M| = 2^8.3^3.5.7$.
17. $M \cong (12, q-1) \circ 6^{\cdot}Suz$ if $q = p \equiv 1 \pmod 3$,
    $|M|$ is a divisor of $2^{16}.3^9.5^2.7.11.13$.

Now, we use the well-known Zsigmondy's theorem to take a primitive prime divisor of $p^{11m}-1$, i.e., a prime r which divides $p^{11m}-1$ but does not divide p^i-1 for $0 < i < 11m$. Obviously $r \geq 23$ (as $r-1$ is a multiple of $11m$) and also r divides Q. It can be easily seen that the only orders of maximal subgroups (from the list above) divisible by r are those in cases 14, and 15 with $r = 23$. In case 14 if $Q = q_0^{22}-1$ divides the order of M, then $q_0^{11}-1$ is a divisor of $(12,q_0-1)q_0^{66}(q_0^2-1)(q_0^3+1)(q_0^4-1)(q_0^5+1)(q_0^6-1)(q_0^7+1)(q_0^8-1)(q_0^9+1)(q_0^{10}-1)(q_0^{12}-1)$, an impossibility, by the same Zsigmondy's theorem. As for the groups in case 15, we have $Q \geq \dfrac{3^{11}-1}{2} > 2^5.3^2.11.23 \geq |M|$ which is impossible.

Denote that the maximal subgroups having an element of order Q are actually the stabilizers in G of one or eleven-dimensional subspaces of V.

The lemma is proved. □

We can now complete the proof of the theorem. The group $H = \langle x, y\rangle$ has an element of order Q and H is irreducible on the space V by Lemma 2.1. Then Lemma 2.2 implies that H cannot be contained in any maximal subgroup of $G(= SL_{12}(q))$. Thus $H = G$ and $G = \langle x, y\rangle$ is a $(2,3)$-generated group.

Remark. The groups $SL_{12}(2)$ and $SL_{12}(4)$, which we do not cover in our considerations, are $(2,3)$-generated too ([11]).

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] Ts. Genchev, E. Gencheva. $(2,3)$-generation of the special linear groups of dimension 8. *Math. and Education in Math.*, **44** (2015), 167–173.

[7] E. Gencheva, Ts. Genchev, K. Tabakov. $(2,3)$-generation of the special linear groups of dimensions 9, 10 and 11. arXiv 1412.8631v5, 2016.

[8] Ts. R. Genchev. A note about the $(2,3)$-generation of $SL_{12}(q)$. arXiv 1611.09350v1, 2016.

[9] A. M. Macbeath. Generators of the linear fractional group. *Proc. Symp. Pure Math.*, **12** (1969), 14–32.

[10] P. Manolov, K. Tchakerian. $(2,3)$-generation of the groups $PSL_4(2^m)$. *Ann. Univ. Sofia, Fac. Math. Inf.*, **96** (2004), 101–104.

[11] M. A. Pellegrini. The $(2,3)$-generation of the special linear groups over finite fields. arXiv 1605.04276v2, 2016.

[12] P. Sanchini, M. C. Tamburini. Constructive $(2,3)$-generation: a permutational approach. *Rend. Sem. Mat. Fis. Milano*, **64** (1994), 141–158.

[13] K. Tabakov, K. Tchakerian. $(2,3)$-generation of the groups $PSL_6(q)$. *Serdica Math. J.*, **37**, No 4 (2011), 365–370.

[14] K. Tabakov. $(2,3)$-generation of the groups $PSL_7(q)$. *Math. and Education in Math.*, **42** (2013), 260–264.

[15] K. Tabakov, E. Gencheva, Ts. Genchev. $(2,3)$-generation of the special linear groups of dimension 11. *Math. and Education in Math.*, **45** (2016), 146–151.

[16] M. C. TAMBURINI, S. VASSALLO. (2, 3)-generazione di gruppi lineari. Scritti in onore di Giovanni Melzi. *Sci. Mat.*, **11** (1994), 391–399.

[17] 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.

[18] M. C. TAMBURINI. Generation of certain simple groups by elements of small order. *Istit. Lombardo Accad. Sci. Lett. Rend. A*, **121** (1987), 21–27.

[19] M. C. TAMBURINI. The (2, 3)-generation of matrix groups over the integers. Ischia group theory 2008, World Sci. Publ., Hackensack, NJ, 2009, 258–264.

[20] K. TCHAKERIAN. (2, 3)-generation of the groups $PSL_5(q)$. *Ann. Univ. Sofia, Fac. Math. Inf.*, **97** (2005), 105–108.

Tsanko Genchev
e-mail: genchev57@yahoo.com
Elenka Gencheva
e-mail: elenkag@abv.bg
Department of Mathematics
Technical University
Varna, Bulgaria

ОТНОСНО (2, 3)-ПОРОДЕНОСТТА НА ГРУПИТЕ $SL_{12}(q)$

Цанко Генчев, Еленка Генчева

В настоящата работа ние привеждаме в явен вид (2, 3)-пораждащи на групата $SL_{12}(q)$ над всички крайни полета $GF(q)$, с изключение на тези от тях, чийто брой на елементите е 2 или 4. Нашето доказателство е лесно проследимо и се базира само на известния списък от максимални подгрупи на $SL_{12}(q)$.