МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2013
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2013
Proceedings of the Forty Second Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 2–6, 2013

(2, 3)-GENERATION OF THE GROUPS $PSL_7(q)$*

Konstantin Tabakov

In this paper we prove that the group $PSL_7(q)$ is a factor group of the modular group $PSL_2(\mathbb{Z})$ for any q, i.e., we prove that $PSL_7(q)$ is $(2,3)$-generated group for any q. In fact, we provide explicit generators x and y of orders 2 and 3, respectively, for the group $SL_7(q)$.

1. Introduction. A group G is called $(2,3)$-generated if $G = \langle x, y\rangle$ for some elements x and y, where x is an involution and y is an element of order 3. It is a well known fact that the modular group $PSL_2(\mathbb{Z})$ is isomorphic to the free product of cyclic groups of order 2 and 3. Thus a group G is $(2,3)$-generated if and only if it is a homomorphic image of the modular group $PSL_2(\mathbb{Z})$. A wide and remarkable class of the $(2,3)$-generated groups forms the so-called Hurwitz groups. A finite group G is called Hurwitz or $(2,3,7)$-generated, if it is generated by the elements of order 2 and 3, respectively and their product has order 7. In 1893 Hurwitz proved that the automorphism group of a compact Riemann surface with genus $g > 1$ always has order at most $84(g-1)$ and that this upper bound is attained precisely when the group is $(2,3,7)$-generated. It is known that the projective special linear groups of large rank are Hurwitz groups ($n \geq 287$ [7]), while for the lower ranks, fewer such groups are Hurwitz ($SL_n(q)$ is not Hurwitz for $n \leq 19$, various q [2]). For example the group $PSL_7(p^m)$ is Hurwitz, if $p \neq 7$, m is the order of $p \pmod{49}$, m is odd, and the field is algebraically closed [15].

A number of series of finite simple groups are $(2,3)$-generated. In fact the theorem of Liebeck-Shalev and Lübeck-Malle gives us a powerful result which states that all finite simple groups, except the symplectic groups $PSp_4(2^m)$, $PSp_4(3^m)$, the Suzuki groups $Sz(2^m)$ (m odd), and finitely many other groups, are $(2,3)$-generated (see [11]). Concerning the projective special linear groups $PSL_n(q)$, $(2,3)$-generation is known in the cases $n = 2, q \neq 9$ [8], $n = 3, q \neq 4$ [5], [1], $n = 4, q \neq 2$ [13], [14], [9], $n = 5$, any q [16], $n = 6$, any q [12], $n \geq 5$, odd $q \neq 9$ [3],[4], and $n \geq 13$, any q [10]. The present paper is another contribution to the problem. We prove the following

Theorem. *The group $PSL_7(q)$ is $(2,3)$-generated for any q.*

Here, we shall exploit the same technique to prove the theorem, which has been used in [16] and [12], taking into account the known list of maximal subgroups of $PSL_7(q)$. We have to note, that the approach applied by the authors in [3], when dealing with similar problems is quite different from our method, as it is based on the classification of finite irreducible linear groups generated by transvections.

*2010 Mathematics Subject Classification: 20F05, 20D06.
Key words: (2,3)-generated group.
This work is partially supported by the Scientific Research Fund of the "St. Kl. Ohridski" University of Sofia under Contract 2013.

2. Proof of the Theorem. Let $G = SL_7(q)$ and $\overline{G} = G/Z(G) = PSL_7(q)$, where $q = p^m$ and p is a prime. Set $d = (7, q-1)$ and $Q = (q^7-1)/(q-1)$. Here $d = (Q, 7)$ and $(Q, 6) = 1$.

First we choose elements x and y of G of orders 2 and 3, respectively. The goal is $z = xy$ to be an element of G of order Q.

Let

$$x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 0 & \lambda_1 \\ 1 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \\ 0 & 0 & -1 & -1 & 0 & 0 & \lambda_3 \\ 0 & 0 & 1 & 0 & 0 & 0 & \lambda_4 \\ 0 & 0 & 0 & 0 & -1 & -1 & \lambda_5 \\ 0 & 0 & 0 & 0 & 1 & 0 & \lambda_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$(x \in G,\ |x| = 2,\ y \in G,\ |y| = 3 \quad \text{for any } \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6 \in GF(q))$.

Now

$$z = xy = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & \lambda_6 \\ 0 & 0 & 0 & 0 & -1 & -1 & \lambda_5 \\ 0 & 0 & -1 & 0 & 0 & 0 & -\lambda_4 \\ 0 & 0 & -1 & -1 & 0 & 0 & \lambda_3 \\ 1 & 0 & 0 & 0 & 0 & 0 & \lambda_2 \\ -1 & -1 & 0 & 0 & 0 & 0 & \lambda_1 \end{pmatrix}.$$

The characteristic polynomial of z is $f_z(t) = t^7 - \lambda_1 t^6 + \lambda_6 t^5 + (\lambda_1 + \lambda_3 + 1)t^4 + (-\lambda_1 + \lambda_4 - \lambda_5 - \lambda_6 - 1)t^3 + (\lambda_2 + \lambda_5 + \lambda_6 + 1)t^2 - (\lambda_2 - 1)t - 1$.

Let $\omega \in GF(q^7)^*$ be of order Q and

$$f(t) = (t-\omega)(t-\omega^q)(t-\omega^{q^2})(t-\omega^{q^3})(t-\omega^{q^4})(t-\omega^{q^5})(t-\omega^{q^6}) =$$
$$= t^7 - \alpha t^6 + \beta t^5 - \gamma t^4 + \delta t^3 - \varepsilon t^2 + \zeta t - 1.$$

Then $f(t) \in GF(q)[t]$ and the polynomial $f(t)$ is irreducible over $GF(q)$. Now choose λ_1, λ_2, λ_3, λ_4, λ_5, λ_6 so that

$$\lambda_1 = \alpha,\ \lambda_6 = \beta,\ \lambda_1 + \lambda_3 + 1 = -\gamma,\ -\lambda_1 + \lambda_4 - \lambda_5 - \lambda_6 - 1 = \delta,\ \lambda_2 + \lambda_5 + \lambda_6 + 1 = -\varepsilon,$$
$$1 - \lambda_2 = \zeta,$$

i.e.

$$\lambda_1 = \alpha,\ \lambda_2 = 1 - \zeta,\ \lambda_3 = -\alpha - \gamma - 1,\ \lambda_4 = \alpha + \delta - \varepsilon + \zeta - 1,\ \lambda_5 = -\beta - \varepsilon + \zeta - 2,$$
$$\lambda_6 = \beta.$$

This implies $f_z(t) = f(t)$ and the characteristic roots ω, ω^q, ω^{q^2}, ω^{q^3}, ω^{q^4}, ω^{q^5}, ω^{q^6} of z are pairwise distinct.

Then, in $GL_7(q^7)$, z is conjugate to $\mathrm{diag}(\omega,\ \omega^q,\ \omega^{q^2},\ \omega^{q^3},\ \omega^{q^4},\ \omega^{q^5},\ \omega^{q^6})$ and hence z is an element of G of order Q.

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) $\overline{z} = \overline{x}.\overline{y}$ has order Q/d. So $\overline{H} = \langle \overline{x}, \overline{y} \rangle$ is

a subgroup of order divisible by $6Q/d$. Our goal is to prove $\overline{H} = \overline{G}$. To do this we need to know the subgroup structure of $\overline{G}$.

The maximal subgroups of $PSL_7(q)$ are classified in [6]. This implies that if $\overline{M}$ is a maximal subgroup of $\overline{G}$ then one of the following holds.

1) $|\overline{M}| = q^{21}(q-1)(q^2-1)(q^3-1)(q^4-1)(q^5-1)(q^6-1)/d$.

2) $|\overline{M}| = q^{21}(q-1)(q^2-1)^2(q^3-1)(q^4-1)(q^5-1)/d$.

3) $|\overline{M}| = q^{21}(q-1)(q^2-1)^2(q^3-1)^2(q^4-1)/d$.

4) $|\overline{M}| = 5040(q-1)^6/d$ if $q \geq 5$.

5) $\overline{M} \cong Z_{Q/d}.Z_7$;
$|\overline{M}| = 7Q/d$.

6) $\overline{M} \cong PSL_7(q_0).Z_{(d,r)}$ if $q = q_0^r$, r is a prime;
$|\overline{M}| = q_0^{21}(q_0^2-1)(q_0^3-1)(q_0^4-1)(q_0^5-1)(q_0^6-1)(q_0^7-1)(d,r)/(7,q_0-1)$.

7) $\overline{M} \cong E_{7^2}.SL_2(7)$ if $p \equiv 1,2,4 \pmod 7$, $q \equiv 1 \pmod 7, q = p$ or $q = p^3$;
$|\overline{M}| = 2^4.3.7^3$.

8) $\overline{M} \cong SO_7(q)$ if q is odd;
$|\overline{M}| = q^9(q^2-1)(q^4-1)(q^6-1)$.

9) $\overline{M} \cong PSU_7(q_0)$ if $q = q_0^2$;
$|\overline{M}| = q_0^{21}(q_0^2-1)(q_0^3+1)(q_0^4-1)(q_0^5+1)(q_0^6-1)(q_0^7+1)/(7,q_0+1)$.

10) $\overline{M} \cong PSU_3(3)$ if $5 \leq q = p \equiv 1 \pmod 4$;
$|\overline{M}| = 2^5.3^3.7$.

We shall prove that the only maximal subgroup of $\overline{G}$ whose order is a multiple of Q/d is that in case 5), of order $7Q/d$.

Suppose false, i.e. Q/d divides $|\overline{M}|$. It is not difficult to see that
$(Q, 6q(q+1)(q^2+1)(q^2+q+1)(q^2-q+1)(q^4+q^3+q^2+q+1)(q^4-q^3+q^2-q+1)) = 1$.

In cases 1), 2), 3) and 4) it follows that Q divides $(q-1)^6$, $(q-1)^6$, $(q-1)^6$, $35(q-1)^6$, respectively. So Q must divide $35(q-1)^6 = 35Q - 7.35q(q^2-q+1)^2$, i.e. Q divides 7.35, which is impossible for any $q \geq 2$.

In case 8) Q must divide $d(q-1)^3 \leq 7(q-1)^3 < Q$, an impossibility. Similarly, in case 9) the number $Q_0 = q_0^6 + q_0^5 + q_0^4 + q_0^3 + q_0^2 + q_0 + 1$ must divide $d(q_0-1)^3$, again an impossibility.

In cases 7) and 10) Q must divide $7^3 d$ and $7d$, respectively, hence Q divides 7^4, which is impossible for any $q \geq 2$.

In case 6) the simplest way to prove that Q/d does not divide $|\overline{M}|$ is to use a primitive prime divisor of $p^{7m} - 1$. For this purpose we use the following classical theorem

Theorem (Zsigmondy theorem)**.** *If $a > b > 0$ are coprime integers, then for any natural number $n > 1$ there is a prime number p (called a primitive prime divisor) that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any positive integer $k < n$, with the following exceptions*

1. $a = 2$, $b = 1$ *and* $n = 6$.

2. $a + b$ *is a power of* 2 *and* $n = 2$.

Indeed, for our aim, Zsigmondy's theorem provides a prime s which divides $p^{7m} - 1$ but does not divide $p^i - 1$ for $0 < i < 7m$. We have $s > 7$ (as $s - 1$ is a multiple of $7m$) and hence s divides Q/d. On the other hand, a glance at $|\overline{M}|$ shows that $|\overline{M}|$ is not divisible by s. So Q/d does not divide $|\overline{M}|$.

Thus we have proved that the only maximal subgroup of $\overline{G}$ whose order is a multiple of Q/d is that in case 5), of order $7Q/d$. This implies that no proper subgroup of $\overline{G}$ has order divisible by $6Q/d$. Hence $\overline{H} = \overline{G}$ and $\overline{G} = \langle \overline{x}, \overline{y} \rangle$ is a $(2, 3)$-generated group.

This completes the proof of the theorem. □

Acknowledgement. The author would like to express his gratitude posthumously to his supervisor Prof. K. Tchakerian for introducing him in the field of group theory and for the invaluable help when preparing this paper.

REFERENCES

[1] J. Cohen. On non-Hurwitz groups and noncongruence of the modular group. *Glasgow Math. J.*, **22** (1981), 1–7

[2] L. Di Martino, M. C. Tamburini, A. E. Zalesskii. On Hurwitz groups of low rank. *Comm. Alg.*, **28** (2000), 5383–5404.

[3] L. Di Martino, N. A. Vavilov. $(2, 3)$-generation of $SL(n, q)$. I. Cases $n = 5, 6, 7$. *Comm.Alg.*, **22** (1994), No 4, 1321–1347.

[4] L. Di Martino, N. A. Vavilov. $(2, 3)$-generation of $SL(n, q)$. II. Cases $n \geq 8$. *Comm. Alg.*, **24** (1996), No 2, 487–515.

[5] D. Garbe. Über eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe. *Math.Ann.*, **235** (1978), No 3, 195–215.

[6] P. Kleidman. The low-dimensional finite simple classical groups and their subgroups. Ph.D. Thesis. Cambridge, 1987.

[7] A. Lucchini, M. C. Tamburini, J. S. Wilson. Hurwitz groups of large rank. *J. London Math. Soc.*, **61** (2000), No 1, 81–92.

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

[11] A. Shalev. Asymptotic group theory. *Notices Amer. Math. Soc.*, **48** (2001), No 4, 383–389.

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

[13] M. C. Tamburini, S. Vassallo. $(2, 3)$-generazione di $SL_4(q)$ in caratteristica dispari e problemi collegati. *Boll. Unione Mat. Ital., VII. Ser.*, **B 8** (1994), No 1, 121–134.

[14] M. C. Tamburini, S. Vassallo. $(2, 3)$-generazione di gruppi lineari. Papers in honor of Giovanni Melzi. Milano (Eds Carlo Felice Manara et al.), Univ. Cattolica del Sacro Cuore. *Sci. Mat.* **11** (1994), 391–399.

[15] M. C. Tamburini, M. Vsemirnov. Irreducible $(2,3,7)$-subgroups of $PGL_n(\mathbb{F})$, $n \leq 7$. *J. Algebra*, **300** (2006), 339–362.

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

Konstantin Tabakov
Faculty of Mathematics and Informatics
"St. Kliment Ohridski" University of Sofia
5, J. Bourchier Blvd
1164 Sofia, Bulgaria
e-mail: ktabakov@fmi.uni-sofia.bg

(2, 3)-ПОРАЖДАНЕ НА ГРУПИТЕ $PSL_7(q)$

Константин Д. Табаков

В настоящата статия доказваме, че групата $PSL_7(q)$ е факторгрупа на модулярната група $PSL_2(\mathbb{Z})$, т.е. доказваме, че групата $PSL_7(q)$ е $(2,3)$-породена за всяко q. По- точно, за групата $SL_7(q)$, намираме експлицитни пораждащи x и y с редове съответно 2 и 3.