PDMI PREPRINT - 17/2004

GROUPS $\mathbf{G_2(p)}$ AS QUOTIENTS OF $(\mathbf{2, 3, 7; 2p})$

MAXIM VSEMIRNOV

Steklov Institute of Mathmatics,
Fontanka 27, St.Petersburg, 191023, Russia
and
Sidney Sussex College,
Sidney Street, Cambridge, CB2 3HU, United Kingdom
(E-mail: mv254@dpmms.cam.ac.uk, vsemir@pdmi.ras.ru)

ABSTRACT

We prove that for any prime $p \geq 5$ the group $G_2(p)$ is a quotient of $(2, 3, 7; 2p) = \langle X, Y : X^2 = Y^2 = (XY)^7 = [X, Y]^{2p} = 1\rangle$.

1 Introduction

During last decades non-trivial finite quotients of the abstract group

$$T(2,3,7) = \langle X, Y : X^2 = Y^2 = (XY)^7 = 1 \rangle$$

attracted a reasonable interest; see [3], [4], [6], [14], [15], [17], [18], [21], [22]. These quotients are also known as *Hurwitz groups*, while the corresponding generators, i.e., the images of X and Y, are called *Hurwitz generators* or *Hurwitz pairs*. The reader may find extensive lists of further references in the surveys [4] and [22].

A special attention was paid to the problem of describing finite simple or almost simple Hurwitz groups. Although the complete answer is still unknown, there are significant achievements in this direction [14], [15], [17], [18]. [24]. Among other examples we especially mention a real masterpiece of computation showing that Monster is Hurwitz [24].

There are two kinds of positive results in this area: constructive, e.g., [14], [15], where Hurwitz generators are given explicitly, and non-constructive, e.g., [17], [18], [24], where only existence theorems were known.

For example, G. Malle [17] proved that the groups $G_2(q)$ are Hurwitz provided $q > 4$. However, his method produced no explicit generators. Recently, the author [25] found a family of Hurwitz generators for $G_2(3^m)$, $m \geq 2$. Using completely different ideas, the author and M.C. Tamburini parameterized up to conjugation all Hurwitz pairs of matrices in $\mathrm{GL}_7(F)$ for an arbitrary field F. Looking at these pairs one can in principle determine groups generated by them. In particular, this might include a constructive version of Malle's result. However, the complete analysis is rather lengthy and this project is now in progress.

Another problem is to search for Hurwitz generators that satisfy further relations. For instance, one can impose certain conditions on their commutator. The following abstract group appears naturally in this context:

$$(2,3,7;n) = \langle X, Y : X^2 = Y^2 = (XY)^7 = [X,Y]^n = 1 \rangle$$

One can ask whether these groups are finite or infinite. Leech [12], [13] and Sims [19] were among the first who addressed this problem. It was solved by joint efforts of Holt, Plesken, and Souvigner [8], [9], and independently by Howie and Thomas, [10]. The last remaining case was settled in [9], and also in [7]. Now we know that $(2,3,7;n)$ is infinite if and only if $n \geq 9$. However, there was no systematic study of finite quotients of these groups. We can only mention the conjecture of Holt and Plesken [8] asserting that for any sufficiently large n there is at least one prime power q such that $(2,3,7;n)$ projects onto $\mathrm{PSL}_2(q)$.

The aim of this paper is to detect groups $G_2(p)$ among the quotients of $(2,3,7;2p)$, $p \geq 5$. Here and in what follows p is an odd prime number, $\mathbb{F}_p$ is a finite field with p elements and $\bar{\mathbb{F}}_p$ is its algebraic closure.

Theorem 1. *For any prime $p \geq 5$, the group $G_2(p)$ is a quotient of $(2,3,7;2p)$. In other words, $G_2(p)$ can be generated by two elements, say x and y, such that*

$$x^2 = y^3 = (xy)^7 = [x,y]^{2p} = 1.$$

One may regard this theorem as a strengthened analogue of Malle's result. Moreover we construct the required generators explicitly. For details, see Theorem 2 in Section 2.

The proof of Theorem 1 uses the knowledge of the maximal subgroups of $G_2(p)$ [11], [1]. Therefore, it is based on the classification of finite simple groups.

The main result of this paper was inspired by the joint research started in [23], which allowed to find the required generators x and y. However the proof of Theorem 1 is completely independent of [23]. The author is extremely grateful to M.C. Tamburini for her kind permission to use the results of [23] prior to their publication.

2 Generators of $G_2(p)$, $p \geq 5$

Let us consider the following two matrices:

$$x = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 1 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}. \tag{1}$$

This is a particular case of a two-parametric family of matrices studied in [23]. It corresponds to the following choice of parameters in [23]: $r_3 = -2$, $r_7 = 0$. It is straightforward to verify that

$$x^2 = y^3 = (xy)^7 = 1.$$

Moreover,

$$[x, y] = x^{-1}y^{-1}xy = c^{-1} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} c,$$

where

$$c = \begin{pmatrix} -6 & 2 & 8 & 6 & -2 & -8 & -4 \\ -20 & 10 & 24 & 22 & -4 & -32 & -12 \\ -23 & 17 & 26 & 29 & 1 & -50 & -10 \\ 0 & 1 & -1 & -1 & 0 & 1 & 0 \\ -1 & 1 & 0 & -1 & 1 & 0 & -2 \\ 4 & -3 & 0 & 3 & -4 & 0 & 6 \\ -3 & 2 & 0 & -1 & 4 & 2 & -4 \end{pmatrix}.$$

Since $\det c = 2048 = 2^{11}$, the matrix c^{-1} is well defined for any odd prime p. Now it is clear that in $\mathrm{GL}_7(\mathbb{F}_p)$ we have

$$[x, y]^{2p} = 1, \tag{2}$$

and moreover the order of $[x, y]$ is exactly $2p$. Thus we proved the following lemma.

Lemma 1. *Let p be an odd prime and let x, $y \in \mathrm{GL}_7(p)$ be defined by (1). Then the group $\langle x, y\rangle$ is a quotient of $(2, 3, 7; 2p)$.*

Table 1: Multiplication table for the algebra $\mathcal{O}$.

	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_5$	$\mathbf{e}_4$	$-\mathbf{e}_7$	$-\mathbf{e}_6$
$\mathbf{e}_2$	$\mathbf{e}_2$	$-\mathbf{e}_3$	$4\mathbf{e}_0$	$-4\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$	$4\mathbf{e}_4$	$4\mathbf{e}_5$
$\mathbf{e}_3$	$\mathbf{e}_3$	$-\mathbf{e}_2$	$4\mathbf{e}_1$	$-4\mathbf{e}_0$	$\mathbf{e}_7$	$\mathbf{e}_6$	$-4\mathbf{e}_5$	$-4\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$-\mathbf{e}_5$	$-\mathbf{e}_6$	$-\mathbf{e}_7$	$24\mathbf{e}_0$	$-24\mathbf{e}_1$	$-24\mathbf{e}_2$	$-24\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$-\mathbf{e}_4$	$-\mathbf{e}_7$	$-\mathbf{e}_6$	$24\mathbf{e}_1$	$-24\mathbf{e}_0$	$24\mathbf{e}_3$	$24\mathbf{e}_2$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\mathbf{e}_7$	$-4\mathbf{e}_4$	$4\mathbf{e}_5$	$24\mathbf{e}_2$	$-24\mathbf{e}_3$	$-96\mathbf{e}_0$	$-96\mathbf{e}_1$
$\mathbf{e}_7$	$\mathbf{e}_7$	$\mathbf{e}_6$	$-4\mathbf{e}_5$	$4\mathbf{e}_4$	$24\mathbf{e}_3$	$-24\mathbf{e}_2$	$96\mathbf{e}_1$	$96\mathbf{e}_0$

For $p = 3$, we have $x^2 = y^3 = (xy)^7 = [x, y]^6 = 1$, which is a well known presentation of $\mathrm{PSL}_2(13)$; see [5]. Theorem 1 will follow from the following statement, which describes the groups $\langle x, y\rangle$ for $p \geq 5$.

Theorem 2. *For $p \geq 5$, the group $\langle x, y\rangle$ is isomorphic to $G_2(p)$.*

First, we establish some auxiliary facts about the groups under consideration.

Lemma 2. *For any prime $p \geq 5$, the group $\langle x, y\rangle$ is conjugate to a subgroup of $G_2(p)$.*

Proof. Using the well known characterization of groups of type G_2, e.g., see [20, Chapter 2], it is enough to show that $\langle x, y\rangle$ is isomorphic to a subgroup of the automorphism group of an octonion algebra over $\mathbb{F}_p$. To keep the structure constants of this algebra as nice as possible it is more convenient to work with a conjugate group instead of $\langle x, y\rangle$ itself.

Let $\mathcal{O}$ be generated as a vector space by $\mathbf{e}_0$, $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$, $\mathbf{e}_4$, $\mathbf{e}_5$, $\mathbf{e}_6$ and $\mathbf{e}_7$. We define the multiplicative structure of $\mathcal{O}$ by Table 1. It is straightforward to verify that $\mathcal{O}$ is an alternative algebra. Set

$$g = \begin{pmatrix} 1 & 1 & 3 & 1 & 1 & -10 & -2 \\ 0 & 1 & 1 & 0 & -8 & -12 & -20 \\ 0 & 0 & 1 & 0 & -10 & -15 & -19 \\ 1 & 1 & 3 & -1 & -1 & 10 & 2 \\ 0 & 1 & 1 & 0 & -8 & 0 & -8 \\ 0 & 0 & 1 & 0 & -6 & 3 & -9 \\ 0 & 0 & 0 & 0 & -8 & -6 & -14 \end{pmatrix},$$

and let us consider two 8×8 matrices:

$$x_8 = \begin{pmatrix} 1 & 0 \\ 0 & g^{-1}xg \end{pmatrix}, \qquad y_8 = \begin{pmatrix} 1 & 0 \\ 0 & g^{-1}yg \end{pmatrix}.$$

Since $p \geq 5$ and $\det g = -2304 = -2^8 \cdot 3^2$, both x_8 and y_8 are well defined. A direct calculation shows that

$$(x_8 u)(x_8 v) = x_8(uv), \qquad (y_8 u)(y_8 v) = y_8(uv),$$

for any u, $v \in \mathcal{O}$. In other words, x_8 and y_8 are automorphisms of the algebra $\mathcal{O}$. This proves Lemma 2. □

Lemma 3. *Let $\bar{\chi}, \bar{\upsilon} \in \mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ be a Hurwitz pair and let d be the order of $[\bar{\chi}, \bar{\upsilon}]$. Then $d \geq 4$. Suppose further that $p \neq 13$. Then d is relatively prime to p.*

Proof. Since the groups $(2, 3, 7; n)$ with $n = 1, 2, 3$ are trivial, we have $d \geq 4$. Let χ, υ be linear preimages of $\bar{\chi}$ and $\bar{\upsilon}$, respectively. Multiplying υ by ± 1 if necessary, me may assume that $(\chi\upsilon)^7 = 1$. It follows from the proof of Theorem 1 in [6] that up to conjugation

$$\chi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \upsilon = \begin{pmatrix} 0 & \epsilon^{-1} \\ -\epsilon & \pm 1 \end{pmatrix},$$

where ϵ is a primitive 7th root of unity if $p \neq 7$ and $\epsilon = 1$ if $p = 7$. We have that

$$[\chi, \upsilon] = \chi^{-1}\upsilon^{-1}\chi\upsilon = \begin{pmatrix} \epsilon^2 & \mp\epsilon \\ \mp\epsilon & 1 + \epsilon^{-2} \end{pmatrix},$$

where both signs in $\mp$ are the same. Both eigenvalues of $[\chi, \upsilon]$ are zeros of

$$f(t) = t^2 - (\epsilon^2 + 1 + \epsilon^{-2}) + 1.$$

The polynomial f has one double zero iff

$$(\epsilon^4 + \epsilon^2 + 1)^2 - 4\epsilon^4 = 0. \tag{3}$$

Recall that

$$\epsilon^6 + \epsilon^5 + \epsilon^4 + \epsilon^3 + \epsilon^2 + \epsilon + 1 = 0. \tag{4}$$

Eliminating ϵ from (3) and (4) we see that these equations may have a common root only if $p = 13$. Therefore, for $p \neq 13$ the eigenvalues of $[\chi, \upsilon]$ are distinct. In particular, $[\chi, \upsilon]$ is semisimple, hence its order is relatively prime to p. □

Lemma 4. *For any odd prime p, the group $\langle x, y \rangle$ is an absolutely irreducible subgroup of $\mathrm{GL}_7(\mathbb{F}_p)$.*

Proof. Any reducible subgroup of $\mathrm{GL}_7(\mathbb{F}_p)$ is $\mathrm{GL}_7(\bar{\mathbb{F}}_p)$-conjugate to a group of upper block-triangular matrices, where restrictions to diagonal blocks are irreducible. Let us denote the size of these diagonal blocks (starting from the upper left corner) by $n_1, \ldots, n_k$.

Clearly, there is no irreducible two-dimensional *linear* representation of $T(2, 3, 7)$ since the only involution in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ is central. Thus, $n_i \neq 2$, $i = 1, \ldots, k$.

The only one dimensional representation of $T(2, 3, 7)$ is trivial. On the other hand, one can verify directly that for any $p \geq 5$

- 1 is an eigenvalue of x and y of multiplicity 3;

- the only common eigenvector of x and y is the zero vector;
- the only common eigenvector of x^t and y^t is the zero vector (here x^t and y^t are the transposes of x and y, respectively).

Thus, neither n_1 nor n_k is 1. In particular, this gives us only the following possibilities:

$$n_1 = 3,\ n_2 = 1,\ n_3 = 3,\ \text{or } n_1 = 3,\ n_2 = 4,\ \text{or } n_1 = 4,\ n_2 = 3. \tag{5}$$

By a result of Cohen [2], any irreducible Hurwitz subgroup of $\mathrm{SL}_3(\bar{\mathbb{F}}_p)$ is isomorphic to either $\mathrm{PSL}_2(7)$ or $\mathrm{PSL}_2(q)$, where $q = p$ for $p \equiv \pm 1 \pmod 7$, $q = p^3$ for $p \equiv \pm 2, \pm 3 \pmod 7$. It is also well known that any pair χ, υ of Hurwitz generators for $\mathrm{PSL}_2(7)$ satisfies $[\chi, \upsilon]^4 = 1$. Now, Lemma 3 together with (2) shows that $n_i \neq 3$ if $p \neq 13$. This already proves irreducibility of $\langle x, y\rangle$ for $p \neq 13$.

Now let $p = 13$. This case requires a bit more efforts. By Theorem 4.15 in [22], irreducible Hurwitz subgroups of $\mathrm{PSL}_4(\bar{\mathbb{F}}_{13})$ can be isomorphic only to $\mathrm{PSL}_2(13) \times \mathrm{PSL}_2(13)$, or $\mathrm{PSL}_2(13)$, or $\mathrm{PSL}_2(7)$. A linear preimage (in $\mathrm{SL}_4(\bar{\mathbb{F}}_{13})$) of any of these groups is at most 4 times larger. Combining this with Cohen's result cited above, we conclude that in each case listed in (5) the order of a possible block-triangle group is $2^{a_2} \cdot 3^{a_3} \cdot 7^{a_7} \cdot 13^{a_{13}}$ for some a_2, a_3 ,a_7, and a_{13}. On the other hand, for $p = 13$ the group $\langle x, y\rangle$ contains an element of order 61; for instance one can choose $([x, y]^3 y)^3$. Thus, $\langle x, y\rangle$ cannot be reducible in this case, too. $\square$

Proof of Theorems 1 and 2. We prove that $\langle x, y\rangle$ is not conjugate to any proper subgroup of $G_2(p)$. The list of all maximal subgroups of $G_2(p^m)$ (up to conjugation) was given in [11, Theorem A] and also in [1]. We keep the notation of [11].

The groups P_a, P_b, $C_{H_0}(S_2)$ (involution centralizer), K_+, and K_- are reducible, so these groups and their subgroups are excluded by Lemma 4.

By Macbeath's theorem [16], Hurwitz subgroups of $\mathrm{PGL}_2(p)$ are $\mathrm{PSL}_2(p)$ for $p \equiv 0, \pm 1 \pmod 7$. When $p \neq 13$ these groups are excluded by (2) and Lemma 3. The group $\mathrm{PSL}_2(13)$ will be discussed later.

The remaining possible maximal subgroups of $G_2(p)$ are

$$I = 2^3 \cdot \mathrm{PSL}_3(2), \quad \mathrm{PSL}_2(8), \quad G_2(2), \quad J_1, \quad \text{and} \quad \mathrm{PSL}_2(13). \tag{6}$$

Recall that $\mathrm{PSL}_2(13)$ also appeared above as a subgroup of $\mathrm{PGL}_2(13)$. For any group in (6), prime factors of its order are in the set

$$S = \{2, 3, 5, 7, 11, 13, 19\}.$$

Recall that the order of $[x, y]$ is $2p$. Therefore, if $p \notin S$, the group $\langle x, y\rangle$ and its conjugates are not contained in any of the groups listed in (6).

If $p \in S$ and $p \geq 5$, then we find an element in $\langle x, y\rangle$ such that its order is divisible by a prime not in S; see Table 2. Therefore, also in this case $\langle x, y\rangle$ and its conjugates are not contained in any of the groups listed in (6).

This proves Theorem 2. Theorem 1 immediately follows from Theorem 2. $\square$

Table 2:

p	element of $\langle x,y\rangle$	order
5	$[[x,y]^5,(xy)^3]$	31
7	$[[x,y]^6,y]$	43
11	$[[x,y]^5,y]$	$3\cdot 37$
13	$[x,y]^3y$	$3\cdot 61$
19	$[x,y]^5y$	$3\cdot 127$

3 Concluding remarks

It would be very interesting to find a presentation of the group $G_2(p)$, $p\geq 5$, giving a minimal complete set of relations which are satisfied by the above generators x and y. Analyzing elements of $\langle x,y\rangle$ one can find other nice relations in addition to those inherited from $(2,3,7;2p)$. We give several examples.

Example 1. Let $g=((xy)^2xy^2)^2(xyxy^2)^2$. For $p=5$, we have $g^5=1$, while for $p>5$ the matrix g is conjugate to

$$\begin{pmatrix} 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&-1&7&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&-1&7 \end{pmatrix}.$$

The roots of $t^2-7t+1=0$ are

$$\frac{7\pm 3\sqrt{5}}{2}=\left(\frac{1\pm\sqrt{5}}{2}\right)^4.$$

where $\sqrt{5}$ is any solution of $a^2=5$ in $\bar{\mathbb{F}}_p$. If $\left(\frac{5}{p}\right)=1$, then

$$\left(\frac{1\pm\sqrt{5}}{2}\right)^{p-1}=1.$$

If $\left(\frac{5}{p}\right)=-1$, then

$$\left(\frac{1-\sqrt{5}}{2}\right)=\left(\frac{1+\sqrt{5}}{2}\right)^p \text{ and } \left(\frac{1+\sqrt{5}}{2}\right)^{p+1}=-1.$$

Therefore $g^{e(p)}=1$, where

$$e(p)=\begin{cases} (p-1)/4 & \text{if } p\equiv 1,9 \pmod{20};\\ (p-1)/2 & \text{if } p\equiv 11,19 \pmod{20};\\ (p+1)/2 & \text{if } p\equiv 3,7,13,17 \pmod{20}. \end{cases}$$

For a fixed p, let $o(g,p)$ be the order of g. It may happen that the actual order $o(g,p)$ is a proper divisor of $e(p)$. For instance, $o(g,47)=8=e(47)/3$, $o(g,89)=11=e(89)/2$, $o(g,139)=23=e(139)/3$.

Example 2. Let $g=(xy^2)(xy)^2(xy^2)^2xy(xy^2)(xy)^2$. The order of g is 44 if $p=11$. Now assume that $p\geq 5$, $p\neq 11$. Then the matrix g is conjugate to

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & -1 & 0 & -46 & 0 \end{pmatrix}.$$

Now we study how the polynomial $f(t)=t^4+46t^2+1$ factorizes over $\mathbb{F}_p$. There are three types of factors:

(i) $(t^2-at+1)(t^2+at+1)$, which occurs iff $a^2=-44$;

(ii) $(t^2-bt-1)(t^2+bt-1)$, which occurs iff $b^2=-48$;

(iii) $(t^2+c)(t^2+1/c)$, which occurs iff $c+c^{-1}=46$ or, in equivalent way, 33 is a square in $\mathbb{F}_p$;

Since $p\neq 2,3,11$, we have $a,b\neq 0$, i.e., these three factorizations are distinct. Since $\left(\frac{-44}{p}\right)\left(\frac{-48}{p}\right)\left(\frac{33}{p}\right)=1$, at least one of these possibilities always happens. In other words, f is always reducible over $\mathbb{F}_p$. Let τ be any zero of f.

If $\left(\frac{-11}{p}\right)=\left(\frac{-3}{p}\right)=1$, then all factorizations (i)–(iii) exist, i.e., $\tau\in\mathbb{F}_p$ and f is a product of four linear polynomials. In particular, $\tau^{p-1}=1$.

If $\left(\frac{-11}{p}\right)=1$ and $\left(\frac{-3}{p}\right)=-1$, then only case (i) happens. Then $\tau=\pm a/2\pm 2\sqrt{-3}$ and $\mathbb{F}_p[\tau]=\mathbb{F}_{p^2}$. Therefore, $a/2-2\sqrt{-3}=(a/2+2\sqrt{-3})^p$ and $-a/2-2\sqrt{-3}=(-a/2+2\sqrt{-3})^p$. In particular, $\tau^{p+1}=1$.

If $\left(\frac{-11}{p}\right)=-1$ and $\left(\frac{-3}{p}\right)=1$, then only case (ii) happens. Then $\tau=\pm b/2\pm\sqrt{-11}$ and $\mathbb{F}_p[\tau]=\mathbb{F}_{p^2}$. Therefore, $b/2-\sqrt{-11}=(b/2+\sqrt{-11})^p$, $-b/2-\sqrt{-11}=(-b/2+\sqrt{-11})^p$. In particular, $\tau^{p+1}=-1$.

Finally, if $\left(\frac{-11}{p}\right)=\left(\frac{-3}{p}\right)=-1$, then only case (iii) happens. Then $\tau^{2(p-1)}=(-c)^{\pm(p-1)}=1$.

Using quadratic reciprocity we find that conditions $\left(\frac{-11}{p}\right)=\pm 1$, $\left(\frac{-3}{p}\right)=\pm 1$ depend only on the residue of p modulo 33. Thus, we deduce that $g^{e(p)}=1$, where

$$e(p)=\begin{cases} p-1 & \text{if } p\equiv 1,4,16,25,31 \pmod{33};\\ p+1 & \text{if } p\equiv 5,14,20,23,26 \pmod{33};\\ 2(p+1) & \text{if } p\equiv 7,10,13,19,28 \pmod{33};\\ 2(p-1) & \text{if } p\equiv 2,8,17,29,32 \pmod{33} \text{ and } p\neq 2. \end{cases}$$

Again, it may happen that the actual order $o(g,p)$ is a proper divisor of $e(p)$. For instance, $o(g,157)=78=e(157)/2$, $o(g,23)=8=e(23)/3$, $o(g,139)=56=e(139)/5$, and $o(g,239)=68=e(239)/7$.

References

[1] M. Aschbacher, *Chevalley groups of type G_2 as the group of a trilinear form.* J. Algebra **109** (1987), no. 1, 193–259.

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

[3] M. D. E. Conder, *Generators for alternating and symmetric groups*, J. London Math. Soc. (2) **22** (1980), 75–86.

[4] M. D. E. Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. **23** (1990), 359–370.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups.* Oxford University Press, 1985.

[6] L. Di Martino, M. C. Tamburini and A. E. Zalesski, *On Hurwitz groups of low rank* Comm. Algebra, **28** (2000) no. 11, 5383–5404.

[7] M. Edjvet, *An example of an infinite group.* In: Discrete groups and geometry (Birmingham, 1991), London Math. Soc. Lecture Note Ser., **173**, Cambridge Univ. Press, Cambridge (1992), 66–74.

[8] D. F. Holt and W. Plesken, *A cohomological criterion for a finitely presented group to be infinite.* J. Lond. Math. Soc., II. Ser. **45** (1992), No.3, 469–480.

[9] D. F. Holt, W. Plesken, and B. Souvignier, *Constructing a representation of the group* $(2, 3, 7; 11)$. J. Symbolic Comput. **24** (1997), no. 3-4, 489–492.

[10] J. Howie and R. M. Thomas, *The groups $(2, 3, p; q)$; asphericity and a conjecture of Coxeter.* J. Algebra **154** (1993), no. 2, 289–309.

[11] P. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups.* J. Algebra **117** (1988), no. 1, 30–71.

[12] J. Leech, *Generators for certain normal subgroups of* (2, 3, 7). Proc. Cambridge Philos. Soc. **61** (1965) 321–332.

[13] J. Leech, *Note on the abstract group* (2, 3, 7; 9). Proc. Cambridge Philos. Soc. **62** (1966), 7–10.

[14] A. Lucchini and M. C. Tamburini, *Classical groups of large rank as Hurwitz groups*, J. Algebra **219** (1999), 531–546.

[15] A. Lucchini, M. C. Tamburini and J. S. Wilson, *Hurwitz groups of large rank*, J. London Math. Soc. (2) **61** (2000), 81-92.

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

[17] G. Malle, *Hurwitz groups and $G_2(q)$*, Canad. Math. Bull. **33** (1990), 349–357.

[18] G. Malle, *Small rank exceptional Hurwitz groups*, Groups of Lie type and their geometries, London Math. Soc. Lecture Notes, **207** (1995), 173–183. Cambridge University Press,

[19] C. C. Sims, *On the group* $(2, 3, 7; 9)$. Notices Amer. Math. Soc. **11** (1964), 687–688.

[20] T. A. springer and F. D. Veldkamp. *Octonions, Jordan Algebras and Exceprional Groups*. Springer-Verlag, 2000.

[21] M. C. Tamburini and A. Zalesskii, *Classical groups in dimension* 5 *which are Hurwitz*, to appear.

[22] M. C. Tamburini and M. Vsemirnov, *Hurwitz groups and Hurwitz generation,* to appear as an invited chapter in *Handbook of Algebra,* vol. 4.

[23] M. C. Tamburini and M. Vsemirnov, *Hurwitz groups in dimensions less than 8,* in preparation.

[24] R. A. Wilson, *The Monster is a Hurwitz group*, J. Group Theory **4** (2001), no. 4, 367–374.

[25] M. Vsemirnov, *Exact Hurwitz generators is small dimensions. I.* Preprint PDMI no. 18/2004, 20pp. Submitted to J. Algebra.