Groups in which the Bounded Nilpotency of Two-generator Subgroups is a Transitive Relation

Costantino Delizia  Primož Moravec *  Chiara Nicotera

1,3 Dipartimento di Matematica e Informatica, Università di Salerno
Via Ponte don Melillo, 84084 - Fisciano (SA), Italy
1 e-mail: cdelizia@unisa.it  3 e-mail: cnicotera@unisa.it

2 Fakulteta za Matematiko in Fiziko, Univerza v Ljubljani
Jadranska 19, 1000 Ljubljana, Slovenia
e-mail: primoz.moravec@fmf.uni-lj.si

Abstract. In this paper we describe the structure of locally finite groups in which the bounded nilpotency of two-generator subgroups is a transitive relation. We also introduce the notion of (nilpotent of class \(c\))-transitive kernel. Our results generalize several known results related to the groups in which commutativity is a transitive relation.

MSC 2000: 20E15, 20D25

Keywords: nilpotent-transitive groups, (nilpotent of class \(c\))-transitive kernel, locally finite groups, Frobenius groups

1. Introduction

Let \(c\) be a positive integer and let \(\mathfrak{N}_c\) denote the class of all groups which are nilpotent of class \(\leq c\). A group \(G\) is said to be an \(\mathfrak{N}_cT\)-group if for all \(x, y, z \in G\setminus\{1\}\) the relations \(\langle x, y \rangle \in \mathfrak{N}_c\) and \(\langle y, z \rangle \in \mathfrak{N}_c\) imply \(\langle x, z \rangle \in \mathfrak{N}_c\). In the case \(c = 1\) these groups are known as commutative-transitive groups (also \(CT\)-groups)

*The second author was partially supported by G.N.S.A.G.A. He also wishes to thank the Department of Mathematics and Informatics at the University of Salerno for its excellent hospitality
or CA-groups) and have been studied by several authors [2, 3, 4, 8, 11, 14, 15]. It is not difficult to see that CT-groups are precisely the groups in which centralizers of non-identity elements are abelian. The study of these groups was initiated by Weisner [14] in 1925, but there are some fallacies in his proofs. Nevertheless, it turns out that finite CT-groups are either soluble or simple. Finite nonabelian simple CT-groups have been classified by Suzuki [11]. He proved that every finite nonabelian simple CT-group is isomorphic to some $\text{PSL}(2, 2^f)$, where $f > 1$. The complete description of finite soluble CT-groups has been given by Wu [15] (see also a paper of Lescot [8]), who has also obtained information on locally finite CT-groups and polycyclic CT-groups. At roughly the same time Fine et al. [4] introduced the notion of the commutative-transitive kernel of a group. This topic has been further explored by the first and the third author; see [2] and [3].

Passing to finite $\mathfrak{N}_c T$-groups with $c > 1$ we first note that in these groups centralizers of non-identity elements are nilpotent. The converse is not true, however, as the example of $\text{PSL}(2, 9)$ shows (see Proposition 4.5). Compared to the CT-case, this may seem to be a certain disadvantage at first glance, but nevertheless we obtain satisfactory information on the structure of locally finite $\mathfrak{N}_c T$-groups. We show that soluble locally finite $\mathfrak{N}_c T$-groups are either Frobenius groups or belong to the class of groups in which every two-generator subgroup is nilpotent of class $\leq c$. Furthermore, we prove that finite $\mathfrak{N}_c T$-groups are either soluble or simple. This provides a generalization of results in [15]. Additionally, we show that the groups $\text{PSL}(2, 2^f)$, where $f > 1$, and Suzuki groups $\text{Sz}(q)$, with $q = 2^{2n+1} > 2$, are the only finite nonabelian simple $\mathfrak{N}_c T$-groups for $c > 1$. This result is probably the strongest evidence showing the gap between CT-groups and $\mathfrak{N}_c T$-groups with $c > 1$. We also show that locally finite $\mathfrak{N}_c T$-groups are either locally soluble or simple. In the latter case we give a classification of these groups.

Another notion closely related to CT-groups is the commutative-transitive kernel of a group. Given a group $G$, we can construct a characteristic subgroup $T(G)$ as the union of a chain $1 = T_0(G) \leq T_1(G) \leq \cdots$ in such way that $G/T(G)$ is a CT-group [4]. In [2] it is proved that if $G$ is locally finite, then $T(G) = T_1(G)$. Similar results have also been obtained in [3] for other classes of groups, such as supersoluble groups. In analogy with this we introduce the notion of the $\mathfrak{N}_c$-transitive kernel of a group and prove that it has similar properties like the commutative-transitive kernel.

In the final section we present some examples of $\mathfrak{N}_c(T)$-groups. In particular, we present Frobenius $\mathfrak{N}_c(T)$-groups with nonabelian kernel and Frobenius $\mathfrak{N}_c(T)$-groups with noncyclic complement. We also show that some finite linear groups with nilpotent centralizers are in a certain sense far from being $\mathfrak{N}_c T$-groups.

2. $\mathfrak{N}_c T$-groups

In this section we investigate the structure of locally finite $\mathfrak{N}_c T$-groups. In the beginning we exhibit some basic properties of these groups. For positive integers $r > 1$ and $n$ denote by $\mathfrak{N}(r, n)$ the class of all groups in which every $r$-generator subgroup is nilpotent of class $\leq n$. Every finite $\mathfrak{N}(r, n)$-group is nilpotent by Zorn’s...
theorem (see Theorem 12.3.4 in [10]). It is now clear that every locally nilpotent \( \mathfrak{N}_T \)-group is also an \( \mathfrak{N}(2, c) \)-group. In fact, every \( \mathfrak{N}_T \)-group with nontrivial center is an \( \mathfrak{N}(2, c) \)-group. On the other hand, the property \( \mathfrak{N}_T \) behaves badly under taking quotients and forming direct products. For, it is known that every free (soluble) group is a CT-group [15]. Moreover if \( G \) and \( H \) are \( \mathfrak{N}_T \)-groups and there exist \( x, y \in G \) such that \( \langle x, y \rangle \) is not nilpotent, then it is easy to see that \( G \times H \) is not an \( \mathfrak{N}_d \)-group for any \( d \in \mathbb{N} \).

Our first result shows that the classes of \( \mathfrak{N}_T \)-groups form a chain.

**Proposition 2.1.** Let \( c \) and \( d \) be integers, \( c \geq d \geq 1 \). Then every \( \mathfrak{N}_d \)-group is also an \( \mathfrak{N}_c \)-group.

**Proof.** Let \( G \) be an \( \mathfrak{N}_d \)-group. Let \( x, y, z \in G \setminus \{1\} \) and suppose that the groups \( \langle x, y \rangle \) and \( \langle y, z \rangle \) are nilpotent of class \( \leq c \). By the above remarks \( \langle x, y \rangle \) and \( \langle y, z \rangle \) are nilpotent of class \( \leq d \). As \( G \) is an \( \mathfrak{N}_d \)-group, it follows that \( \langle x, z \rangle \) is nilpotent of class \( \leq d \), hence it is nilpotent of class \( \leq c \). \( \square \)

The following lemma is crucial for the description of soluble locally finite \( \mathfrak{N}_T \)-groups.

**Lemma 2.2.** Let \( G \) be a locally finite \( \mathfrak{N}_T \)-group with nontrivial Hirsch-Plotkin radical \( H \). Then the factor group \( G/H \) acts fixed-point-freely on \( H \) by conjugation.

**Proof.** As the Hirsch-Plotkin radical \( H \) is a locally nilpotent \( \mathfrak{N}_c \)-group, it is also an \( \mathfrak{N}(2, c) \)-group. Let \( y \) be a nontrivial element in \( H \). Suppose there exists \( a \in C_G(y) \setminus H \). Since the group \( \langle a, y \rangle \) is abelian and \( H \) is an \( \mathfrak{N}(2, c) \)-group, we conclude that the group \( \langle a, h \rangle \) is nilpotent of class \( \leq c \) for every \( h \in H \), since \( G \) is an \( \mathfrak{N}_T \)-group. By conjugation we get that \( \langle a^g, h \rangle \) is also nilpotent of class \( \leq c \) for all \( g \in G \) and \( h \in H \). As \( G \) is an \( \mathfrak{N}_T \)-group, this implies that the group \( \langle a, a^g \rangle \) is nilpotent of class \( \leq c \) for every \( g \in G \). In particular, we have \( 1 = [a^g, a] = [a, g, a] \) for all \( g \in G \), hence \( a \) is a left \((c+1)\)-Engel element of \( G \). As \( G \) is locally finite, this implies that \( a \in H \) (see, for instance, Exercise 12.3.2 of [10]), which is a contradiction. \( \square \)

**Theorem 2.3.** Every locally finite soluble \( \mathfrak{N}_T \)-group is either an \( \mathfrak{N}(2, c) \)-group or a Frobenius group whose kernel and complement are both \( \mathfrak{N}(2, c) \)-groups. Conversely, every locally finite Frobenius group in which kernel and complement are both \( \mathfrak{N}(2, c) \)-groups is an \( \mathfrak{N}_T \)-group.

**Proof.** Let \( G \) be a locally finite soluble \( \mathfrak{N}_T \)-group and suppose \( G \) is not in \( \mathfrak{N}(2, c) \). Let \( N \) be its Hirsch-Plotkin radical. As \( N \) is also an \( \mathfrak{N}_T \)-group, it is an \( \mathfrak{N}(2, c) \)-group. By Lemma 2.2 \( G/N \) acts fixed-point-freely on \( N \), hence \( G \) is a Frobenius group with the kernel \( N \) and a complement \( H \); see, for instance, Proposition 1.1.3 in [7]. Since \( H \) has a nontrivial center [7, Theorem 1.1.2], we have that \( H \in \mathfrak{N}(2, c) \). Besides, \( N \) is nilpotent by the same result from [7].

Conversely, let \( G \) be a locally finite Frobenius group with the kernel \( N \) and a complement \( H \) and suppose that both \( N \) and \( H \) are \( \mathfrak{N}(2, c) \)-groups. Let \( x, y, z \in G \setminus \{1\} \) and let the groups \( \langle x, y \rangle \) and \( \langle y, z \rangle \) be nilpotent of class \( \leq c \). Suppose
\( x \in N \) and \( y \notin N \). Then the equation \([x, c y] = 1\) implies \([x, c^{-1} y] = 1\), since \( H \) acts fixed-point-freely on \( N \). By the same argument we get \( x = 1 \), which is not possible. This shows that if \( x \in N \) then \( y \in N \) and similarly also \( z \in N \). But in this case \( \langle x, z \rangle \) is clearly nilpotent of class \( \leq c \), since \( N \) is an \( \mathfrak{N}(2, c) \)-group. Thus we may assume that \( x, y, z \notin N \). Let \( x \in H^g \) and \( y \in H^k \) for some \( g, k \in G \) and suppose \( H^g \neq H^k \). We clearly have \( C_G(x) \leq H^g \) and \( C_G(y) \leq H^k \). Let \( \alpha \) be any simple commutator of weight \( c \) with entries in \( \{x, y\} \). As \( \langle x, y \rangle \) is nilpotent of class \( \leq c \), we have \( \alpha \in C_G(x) \cap C_G(y) = 1 \). This implies that \( \langle x, y \rangle \) is nilpotent of class \( \leq c - 1 \). Continuing with this process, we end at \( x = y = 1 \) which is impossible. Hence we conclude that \( \langle x, y \rangle \leq H^g \) and similarly also \( \langle y, z \rangle \leq H^g \). Therefore we have \( \langle x, z \rangle \leq H^g \). But \( H^g \) is an \( \mathfrak{N}(2, c) \)-group, hence the group \( \langle x, z \rangle \) is nilpotent of class \( \leq c \). This concludes the proof. \( \square \)

Theorem 2.3 can be further refined when we restrict ourselves to finite groups.

**Theorem 2.4.** Let \( G \) be a finite group. Then \( G \) is a soluble \( \mathfrak{N}_c T \)-group if and only if it is either an \( \mathfrak{N}(2, c) \)-group or a Frobenius group with the kernel which is an \( \mathfrak{N}(2, c) \)-group and a complement which is nilpotent of class \( \leq c \).

**Proof.** By Theorem 2.3 we only need to show that if \( G \) is a finite soluble \( \mathfrak{N}_c T \)-group which is not an \( \mathfrak{N}(2, c) \)-group, then every complement \( H \) of the Frobenius kernel \( N \) of \( G \) is nilpotent of class \( \leq c \). Suppose \( N \) is not abelian. Then the order of \( H \) is odd, hence all Sylow subgroups of \( H \) are cyclic. This implies that \( H \) is cyclic. Assume now that \( N \) is abelian. Then all the Sylow \( p \)-subgroups of \( H \) are cyclic for \( p \neq 2 \), whereas the Sylow 2-subgroup is either cyclic or a generalized quaternion group \( Q_{2^n} [5] \). Moreover, since \( H \in \mathfrak{N}(2, c) \), we obtain \( n \leq c + 1 \). As \( H \) is nilpotent and all its Sylow subgroups are nilpotent of class \( \leq c \), the nilpotency class of \( H \) does not exceed \( c \). \( \square \)

Let \( G \) be a finite \( \mathfrak{N}_c T \)-group and suppose \( G \notin \mathfrak{N}(2, c) \). If the Fitting subgroup of \( G \) is nontrivial, then Lemma 2.2 together with Theorem 2.4 shows that \( G \) is soluble and so its structure is completely determined by Theorem 2.4. The complete classification of finite insoluble \( \mathfrak{N}_c T \)-groups is described in our next result. Note that it has been shown in [11] that the groups \( \text{PSL}(2, 2^f) \), where \( f > 1 \), are the only finite insoluble \( \mathfrak{N}_1 T \)-groups. Passing to finite \( \mathfrak{N}_c T \)-groups with \( c > 1 \), we obtain an additional family of simple groups.

**Theorem 2.5.** Let \( G \) be a finite \( \mathfrak{N}_c T \)-group with \( c > 1 \). Then \( G \) is either soluble or simple. Moreover, \( G \) is a nonabelian simple \( \mathfrak{N}_c T \)-group if and only if it is isomorphic either to \( \text{PSL}(2, 2^f) \), where \( f > 1 \), or to \( \text{Sz}(q) \), the Suzuki group with parameter \( q = 2^{2^{n+1}} > 2 \).

**Proof.** It is easy to see that in every finite \( \mathfrak{N}_c T \)-group \( G \) the centralizers of nontrivial elements are nilpotent, i.e., \( G \) is a \( CN \)-group. Suppose that \( G \) is not soluble. By a result of Suzuki [12, Part I, Theorem 4], \( G \) is a \( CIT \)-group, i.e., the centralizer of any involution in \( G \) is a 2-group. Let \( P \) and \( Q \) be any Sylow \( p \)-subgroups of \( G \) and suppose that \( P \cap Q \neq 1 \). Since \( P \) and \( Q \) are \( \mathfrak{N}(2, c) \)-groups and \( G \) is
an $\mathfrak{N}_cT$-group, we conclude that $\langle P, Q \rangle$ is an $\mathfrak{N}(2, c)$-group, hence it is nilpotent. This shows that $\langle P, Q \rangle$ is a $p$-group, which implies $P = Q$. Therefore Sylow subgroups of $G$ are independent. Combining Theorem 1 in Part I and Theorem 3 in Part II of [12], we conclude that $G$ has to be simple. Additionally, we also obtain that $G$ is a $ZT$-group, that is, $G$ is faithfully represented as a doubly transitive permutation group of odd degree in which the identity is the only element fixing three distinct letters. The structure of these groups is described in [13]. It turns out that $G$ is isomorphic either to $\text{PSL}(2, 2^f)$, where $f > 1$, or to $\text{Sz}(q)$ with $q = 2^{2n+1} > 2$.

It remains to prove that $\text{PSL}(2, 2^f)$ and $\text{Sz}(q)$ are $\mathfrak{N}_cT$-groups. For projective special linear groups this has been done in [11]. Now, let $G = \text{Sz}(q)$ where $q = 2^{2n+1} > 2$. By Theorem 3.10 c) in [6] $G$ has a nontrivial partition $(G_i)_{i \in I}$, where for every $i \in I$ the group $G_i$ is either cyclic or nilpotent of class $\leq 2$. Moreover, the proof of result 3.11 in [6] implies that for all $g \in G \setminus \{1\}$ the relation $g \in G_i$ implies that $C_G(g) \leq G_i$. Let $x, y, z \in G \setminus \{1\}$ and suppose that the groups $\langle x, y \rangle$ and $\langle y, z \rangle$ are nilpotent of class $\leq 2$. Let $a$ and $b$ be nontrivial elements in $Z(\langle x, y \rangle)$ and $Z(\langle y, z \rangle)$, respectively, and suppose that $a \in G_i$ and $b \in G_j$ for some $i, j \in I$. Then $y \in C_G(a) \cap C_G(b) \leq G_i \cap G_j$, hence $i = j$. But now we get $x, z \in G_i$ and since $G_i$ is nilpotent of class $\leq 2$, the same is true for the group $\langle x, z \rangle$. Hence $G$ is an $\mathfrak{N}_2T$-group. By Proposition 2.1 $G$ is an $\mathfrak{N}_cT$-group for every $c > 1$.

It is proved in [15] that every locally finite insoluble $CT$-group is isomorphic to $\text{PSL}(2, F)$ for some locally finite field $F$. For $\mathfrak{N}_cT$-groups, where $c > 1$, we have the following result.

**Theorem 2.6.** Let $c > 1$ and let $G$ be a locally finite $\mathfrak{N}_cT$-group which is not locally soluble. Then there exists a locally finite field $F$ such that $G$ is isomorphic either to $\text{PSL}(2, F)$ or to $\text{Sz}(F)$.

**Proof.** Let $G$ be a locally finite $\mathfrak{N}_cT$-group and suppose that $G$ is not locally soluble. Then $G$ contains a finite insoluble subgroup, hence every finite subgroup of $G$ is contained in some finite insoluble subgroup of $G$. Using Theorem 2.5, we conclude that every finitely generated subgroup of $G$ has a faithful representation of degree 4 over some field of even characteristic. By Mal’cev’s representation theorem [7, Theorem 1.6], $G$ has a faithful representation of the same degree over a field which is an ultraproduct of some finite fields. Hence $G$ is a linear periodic group. It is not difficult to see that $G$ has to be simple. Namely, the set of all finite nonabelian simple subgroups of $G$ is a local system of $G$. By a theorem of Winter [7] the group $G$ is countable. Thus we obtain a chain $(G_i)_{i \in \mathbb{N}}$ of nonabelian finite simple subgroups in $G$ such that $G$ is the union of this chain. By Theorem 2.5 we have either $G_i \cong \text{PSL}(2, F_i)$ or $G_i \cong \text{Sz}(F_i)$ for suitable finite fields $F_i$, $i \in \mathbb{N}$. On the other hand, $\text{PSL}(2, F)$ does not contain any Suzuki group as a subgroup and vice versa (this follows from [13] and Dickson’s theorem in [5]). Therefore we either have $G_i \cong \text{PSL}(2, F_i)$ for all $i \in \mathbb{N}$ or $G_i \cong \text{Sz}(F_i)$ for all $i \in \mathbb{N}$. By a theorem of Kegel [7, Theorem 4.18] there exists a locally finite field $F$ such that either $G \cong \text{PSL}(2, F)$ or $G \cong \text{Sz}(F)$. 

Let the group $G$ be locally finite and locally soluble. If $G$ is an $\mathfrak{N}_2$-group, then Theorem 2.5 implies that every finitely generated subgroup of $G$ is either a 2-Engel group or a Frobenius group with the kernel which is a 2-Engel group and a complement which is nilpotent of class $\leq 2$. As every 2-Engel group is nilpotent of class $\leq 3$ (see [9, p. 45]), the derived length of finitely generated subgroups of $G$ is bounded, so $G$ is actually soluble. Therefore we have:

**Corollary 2.7.** Let $G$ be a locally finite $\mathfrak{N}_2$-group. Then $G$ is either soluble or simple.

The structure of locally finite $\mathfrak{N}_c$-groups, where $c > 2$, is more complicated. Namely, Bachmuth and Mochizuki [1] constructed an insoluble $\mathfrak{N}(2,3)$-group of exponent 5. This is a locally finite $\mathfrak{N}_3$-group in which all finite subgroups are nilpotent. Therefore the result of Corollary 2.7 is no longer true for $\mathfrak{N}_c$-groups with $c > 2$.

### 3. $\mathfrak{N}_c$-transitive kernel

Let $G$ be a group and let $c$ be a positive integer. Put $T^{(c)}_0(G) = 1$ and let $T^{(c)}_1(G)$ be the group generated by all commutators $[x_1, x_2, \ldots, x_{c+1}]$ for $x_i \in \{a, b\}$, where $a$ and $b$ are nontrivial elements of $G$ such that there exist $t \in \mathbb{N}_0$ and $y_1, \ldots, y_t \in G \setminus \{1\}$ with $\langle a, y_1 \rangle \in \mathfrak{N}_c, \langle y_1, y_2 \rangle \in \mathfrak{N}_c, \ldots, \langle y_t, b \rangle \in \mathfrak{N}_c$. It is clear that $T^{(c)}_1(G)$ is a characteristic subgroup of $G$. For $n > 1$ we define $T^{(c)}_n(G)$ inductively by $T^{(c)}_n(G)/T^{(c)}_{n-1}(G) = T^{(c)}_1(G)/T^{(c)}_{n-1}(G))$. So we get a chain $1 = T^{(c)}_0(G) \leq T^{(c)}_1(G) \leq \cdots \leq T^{(c)}_n(G) \leq \cdots$ of characteristic subgroups of the group $G$. We define

$$T^{(c)}(G) = \bigcup_{n \in \mathbb{N}_0} T^{(c)}_n(G)$$

to be the \textit{(nilpotent of class $c$)-transitive kernel} or, shorter, $\mathfrak{N}_c$-transitive kernel of the group $G$. In the case $c = 1$ this definition coincides with the usual definition of the commutative-transitive kernel given in [4]. From the definition it also follows that $T^{(c)}(G)$ is a characteristic subgroup of $G$ and that $T^{(c)}(G) = 1$ if and only if $G$ is an $\mathfrak{N}_T$-group. Moreover, $G/T^{(c)}(G)$ is an $\mathfrak{N}_T$-group for every group $G$. Additionally, notice that $T^{(c)}(G) = T^{(c)}_n(G)$ for some $n \in \mathbb{N}_0$ if and only if $G/T^{(c)}_n(G)$ is an $\mathfrak{N}_T$-group. We use the notation $\Gamma_t(G) = \langle \gamma_t(\langle a, b \rangle) \mid a, b \in G \rangle$.

It is easy to see that $T^{(c)}(G) \leq \Gamma_{c+1}(G)$.

In [2] it is proved that if $G$ is a locally finite group, then $T^{(1)}(G) = T^{(1)}_1(G)$. In this section we shall show that we have an analogous result for the $\mathfrak{N}_c$-transitive kernel.

**Proposition 3.1.** Let $G$ be a group and $H$ a subgroup of $G$. Let $c$ be a positive integer and suppose that the set $S = \{h \in H \mid \langle h, k \rangle \in \mathfrak{N}_c \text{ for all } k \in H \}$ contains a nontrivial element. Then the group $HT^{(c)}_1(G)/T^{(c)}_1(G)$ is an $\mathfrak{N}(2, c)$-group.
Proof. Let \( z \in S \setminus \{1\} \). For all \( a, b \in H \setminus \{1\} \) we have \( \gamma_{c+1}((a, b)) \leq T_1^{(c)}(H) \), since the groups \( \langle a, z \rangle \) and \( \langle z, b \rangle \) are nilpotent of class \( \leq c \). This implies that \( \Gamma_{c+1}(H) = T_1^{(c)}(H) \leq T_1^{(c)}(G) \), so \( HT_1^{(c)}(G)/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group.

Note that Proposition 3.1 implies that if \( G \) is a finite group, then every Sylow subgroup of \( G/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group. In particular, if \( G \) is finite then the Fitting subgroup of \( G/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group.

**Proposition 3.2.** The class of finite \( \mathfrak{N}_c \)-groups is closed under taking quotients.

**Proof.** By Theorem 2.5 it suffices to consider finite soluble \( \mathfrak{N}_c \)-groups. So suppose that \( G \) is a finite soluble \( \mathfrak{N}_c \)-group. If \( G \in \mathfrak{N}(2, c) \), then we are done. Otherwise, \( G \) is a Frobenius group with the kernel \( F = \text{Fitt}(G) \) which is an \( \mathfrak{N}(2, c) \)-group and a complement \( H \) which is nilpotent of class \( \leq c \) by Theorem 2.4. If \( N \) is a normal subgroup of \( G \), then we have either \( N \leq F \) or \( F \leq N \). If \( F \leq N \), then \( G/N \) is nilpotent of class \( \leq c \), hence it is an \( \mathfrak{N}_c \)-group. Assume now that \( N \) is a proper subgroup of \( F \). Then \( G/N = F/N \rtimes H \), where the action of \( H \) on \( F/N \) is induced by the conjugation on \( F \) with elements of \( H \). Since the subgroup \( N \) is invariant under the action of \( H \), we conclude that \( H \) acts fixed-point-freely on \( F/N \) by Satz 8.10 in [5]. Therefore \( G/N \) is an \( \mathfrak{N}_c \)-group by Theorem 2.4.

The following result is a generalization of Theorem 3 in [2]:

**Theorem 3.3.** Let \( G \) be a finite group. Then \( T^{(c)}(G) = T_1^{(c)}(G) \) for every positive integer \( c \).

**Proof.** If \( T_1^{(c)}(G) = 1 \) or \( T_1^{(c)}(G) = \Gamma_{c+1}(G) \), then we have nothing to prove. So we may assume that \( 1 \neq T_1^{(c)}(G) < \Gamma_{c+1}(G) \). Additionally, we may suppose that \( T^{(c)}(H) = T_1^{(c)}(H) \) for every proper subgroup \( H \) of \( G \). Let \( \mathcal{F} = \{ 1 \neq H < G \mid \Gamma_{c+1}(H) \leq T_1^{(c)}(G) \} \). Then this set is not empty since \( T_1^{(c)}(G) \notin \mathcal{F} \). So \( \mathcal{F} \) has a maximal element \( N \). First of all, it is clear that \( N 
= G \), since \( T_1^{(c)}(G) \neq \Gamma_{c+1}(G) \). Furthermore, since \( NT_1^{(c)}(G)/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group, the group \( NT_1^{(c)}(G) \) also belongs to \( \mathcal{F} \), so we have \( T_1^{(c)}(G) \leq N \) by the maximality of \( N \). Let \( F/T_1^{(c)}(G) \) be the Fitting subgroup of \( G/T_1^{(c)}(G) \). Since \( N/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group, it is nilpotent, hence \( N/T_1^{(c)}(G) \leq F/T_1^{(c)}(G) \). On the other hand, since \( F/T_1^{(c)}(G) \) is an \( \mathfrak{N}(2, c) \)-group, we have that \( \Gamma_{c+1}(F) \leq T_1^{(c)}(G) \). Thus \( F \in \mathcal{F} \), hence \( F = N \) by the maximality of \( N \) in \( \mathcal{F} \). Consider now the set \( S = \{ h \in N \mid \langle h, k \rangle \in \mathfrak{N}_c \text{ for all } k \in N \} \). Here we have to consider the following two cases.

**Case 1.** Suppose that \( S \neq \{1\} \) and let \( h \) be a nontrivial element of \( S \). Let \( y \in N \setminus \{1\} \) and let \( a \in C_G(y) \). For every \( b \in N \) we have \( \gamma_{c+1}((a, b)) \leq T_1^{(c)}(G) \), since \( \langle a, y \rangle \), \( \langle y, h \rangle \) and \( \langle h, b \rangle \) are in \( \mathfrak{N}_c \). Additionally we have that \( \langle a^g, y^h \rangle \), \( \langle y^g, h \rangle \), \( \langle h, y^k \rangle \) and \( \langle y^g, a^k \rangle \) are in \( \mathfrak{N}_c \) for all \( g, k \in G \). Hence \( \gamma_{c+1}((a^g, a^k)) \leq T_1^{(c)}(G) \) for all \( g, k \in G \). In particular, this implies that \( aT_1^{(c)}(G) \) is a left \((c + 1)\)-Engel
element of the group $G/T_1^{(c)}(G)$, hence it is contained in the Fitting subgroup of $G/T_1^{(c)}(G)$ by Theorem 12.3.7 in [10]. This gives that $a \in N$. By Satz 8.5 in [5] $G$ is a Frobenius group and $N$ is its kernel. Let $A$ be a complement of $N$ in $G$. Since $T_1^{(c)}(A) \leq A \cap T_1^{(c)}(G) \leq A \cap N = 1$, it follows that $A$ is an $\mathfrak{N}_c T$-group. Moreover the center of $A$ is nontrivial by [5, Satz 8.18], so $A$ is an $\mathfrak{N}(2, c)$-group. Therefore $G$ is soluble. If the nilpotency class of $N$ does not exceed $c$, then $G$ is an $\mathfrak{N}_c T$-group by Theorem 2.3 and $T_1^{(c)}(G) = 1$, which is a contradiction. Hence we may suppose that the nilpotency class of $N$ is greater than $c$. Consider the group $G/T_1^{(c)}(G) = N/T_1^{(c)}(G) \rtimes AT_1^{(c)}(G)/T_1^{(c)}(G)$. This is a Frobenius group with the kernel $N/T_1^{(c)}(G) \in \mathfrak{N}(2, c)$ and complement $AT_1^{(c)}(G)/T_1^{(c)}(G)$ which is also an $\mathfrak{N}(2, c)$-group. By Theorem 2.3 the group $G/T_1^{(c)}(G)$ is an $\mathfrak{N}_c T$-group, hence $T_1^{(c)}(G) = T_1^{(c)}(G)$ in this case.

Case 2. Suppose now that $S = \{1\}$. Let $\Phi(G)$ be the Frattini subgroup of $G$. If $T_1^{(c)}(G) \leq \Phi(G)$, then the nilpotency of the group $N/T_1^{(c)}(G)$ implies that $N$ is nilpotent, which is a contradiction. Hence $T_1^{(c)}(G) \not\leq \Phi(G)$, so there exists a maximal subgroup $M$ of $G$ such that $T_1^{(c)}(G) \not\leq M$. Then $G = MT_1^{(c)}(G)$ and $T_1^{(c)}(M) = T_1^{(c)}(G)$ since $M < G$. From $T_1^{(c)}(M) \leq T_1^{(c)}(G) \cap M$ we now obtain that $G/T_1^{(c)}(G)$ is an $\mathfrak{N}_c T$-group, since it is a homomorphic image of the $\mathfrak{N}_c T$-group $M/T_1^{(c)}(M)$. So $T_1^{(c)}(G) = T_1^{(c)}(G)$, as required.

\begin{corollary}
Let $G$ be a locally finite group. Then $T_1^{(c)}(G) = T_1^{(c)}(G)$ for every positive integer $c$.
\end{corollary}

\begin{proof}
It suffices to show that if $G$ is locally finite, then $G/T_1^{(c)}(G)$ is an $\mathfrak{N}_c T$-group. Let $x, y, z \in G \setminus T_1^{(c)}(G)$ and suppose that the groups $\langle x, y \rangle T_1^{(c)}(G) / T_1^{(c)}(G)$ and $\langle y, z \rangle T_1^{(c)}(G) / T_1^{(c)}(G)$ are nilpotent of class $\leq c$. This means that $\gamma_{c+1}(\langle x, y \rangle) \leq T_1^{(c)}(G)$ and $\gamma_{c+1}(\langle y, z \rangle) \leq T_1^{(c)}(G)$. Let $\{\alpha_1, \ldots, \alpha_r\}$ and $\{\bar{\alpha}_1, \ldots, \bar{\alpha}_r\}$ be the sets of all simple commutators of weight $c+1$ with entries from $\{x, y\}$ and $\{y, z\}$, respectively. For every $i = 1, \ldots, r$ we have

$$
\alpha_i = \prod_{t=1}^{n_i} [x_{i,t,1}, \ldots, x_{i,t,c+1}]^{e_{i,t}},
$$

where $e_{i,t} = \pm 1$, $x_{i,t,j} \in \{a_{i,t}, b_{i,t}\}$ for some $a_{i,t}, b_{i,t} \in G$ for which there exist $y_{i,t,1}, \ldots, y_{i,t,s_i,1}$ in $G$ such that $\langle a_{i,t}, y_{i,t,1} \rangle, \langle y_{i,t,1}, y_{i,t,2} \rangle, \ldots, \langle y_{i,t,s_i,1}, b_{i,t} \rangle$ are nilpotent of class $\leq c$, for all $i = 1, \ldots, r$, $j = 1, \ldots, c+1$ and $t = 1, \ldots, n_i$. Similarly,

$$
\bar{\alpha}_i = \prod_{t=1}^{m_i} [\bar{x}_{i',t',1}, \ldots, \bar{x}_{i',t',c+1}]^{f_{i',t'}},
$$

where $f_{i',t'} = \pm 1$, $\bar{x}_{i',t',j} \in \{\bar{a}_{i',t'}, \bar{b}_{i',t'}\}$ for some $\bar{a}_{i',t'}, \bar{b}_{i',t'} \in G$ for which there exist $\bar{y}_{i',t',1}, \ldots, \bar{y}_{i',t',s_i',1}$ in $G$ such that $\langle \bar{a}_{i',t'}, \bar{y}_{i',t',1} \rangle, \langle \bar{y}_{i',t',1}, \bar{y}_{i',t',2} \rangle, \ldots, \langle \bar{y}_{i',t',s_i',1}, \bar{b}_{i',t'} \rangle$ are nilpotent of class $\leq c$, for all $i' = 1, \ldots, r'$, $j = 1, \ldots, c+1$ and $t' = 1, \ldots, m_i$. Let $H$ be the subgroup of $G$ generated by all $x, y, z, x_{i,t,j}, y_{i,t,j}, a_{i,t}, \bar{a}_{i',t'}, y_{i',t,k}, \bar{y}_{i',t',k}$.
where \( i = 1, \ldots, r, k = 1, \ldots, n_i, k' = 1, \ldots, s_{i,k'} \). Then \( \gamma_{c+1}(\langle x, y \rangle) \leq T_1^{(c)}(H) \) and \( \gamma_{c+1}(\langle y, z \rangle) \leq T_1^{(c)}(H) \). Since \( H/T_1^{(c)}(H) \) is an \( \mathfrak{N}_cT \)-group by Theorem 3.3, we have \( \gamma_{c+1}(\langle y, z \rangle) \leq T_1^{(c)}(H) \leq T_1^{(c)}(G) \). This concludes the proof.

\[ \square \]

**Remark 3.5.** Let \( G \) be a locally nilpotent group, and let \( c \geq 1 \) be any positive integer. It easily follows from Proposition 3.1 that \( T_1^{(c)}(G) = T^{(c)}(G) = \Gamma_{c+1}(G) \).

**Remark 3.6.** Let \( G \) be a supersoluble group. It is proved in [3] that \( T^{(1)}(G) = T_1^{(1)}(G) \). It is to be expected that the same holds true for \( \mathfrak{N}_cT \)-transitive kernel where \( c > 1 \), and that the proofs require only suitable modifications of those in [3].

4. Examples and non-examples

Theorem 2.4 completely describes the structure of finite soluble \( \mathfrak{N}_cT \)-groups. At least in the case \( c \leq 2 \) we are able to obtain more detailed information about these groups, using the descriptions of fixed-point-free actions on finite abelian groups obtained by Zassenhaus [16].

**Example 4.1.** Let \( G \) be a finite soluble \( \mathfrak{N}_1T \)-group (or \( CT \)-group) which is not abelian. Then \( G = F \times \langle x \rangle \) where \( F \) is abelian and \( \langle x \rangle \) acts fixed-point-freely on \( F \) (see Theorem 2.4 or Theorem 10 of [15]). Suppose \( F = \bigoplus_{i=1}^m F_i \) where \( F_i \cong \mathbb{Z}^{n_i}_{p_i} \) and \( \epsilon_i \neq \epsilon_j \) if \( p_i = p_j \). Let \( k \) be the order of \( \langle x \rangle \). Then it follows from [16] that \( x = (x_1, \ldots, x_m) \) where \( \langle x_i \rangle \) is a fixed-point-free automorphism group of order \( k \) on \( G_i \) for all \( i = 1, \ldots, m \). Conversely, for every \( x \) with this property the group \( \langle x \rangle \) acts fixed-point-freely on \( F \). Note also that a necessary and sufficient condition for the existence of a fixed-point-free automorphism on \( F \) is given in Theorem 2 of [15].

As the class of \( \mathfrak{N}(2, 2) \)-groups coincides with the variety of 2-Engel groups, Theorem 2.4 implies that a finite soluble \( \mathfrak{N}_2T \)-group is either 2-Engel or it is a Frobenius group with the kernel \( F \) which is 2-Engel and a complement \( H \) which is nilpotent of class \( \leq 2 \). Thus it follows from Levi’s theorem (see [9, p. 45]) that \( F \) is nilpotent of class \( \leq 3 \). Moreover, if \( |H| \) is even, then \( F \) is abelian. In this case, \( H \) is either a cyclic group or the quaternion group \( Q_8 \) of order 8 or \( C_m \times Q_8 \) where \( m \) is odd. Our next example shows that there is essentially only one possibility of having a Frobenius \( \mathfrak{N}_2T \)-group with the prescribed kernel and a complement isomorphic to \( Q_8 \).

**Example 4.2.** Let \( F \) be a finite abelian group and \( F = \bigoplus_{i=1}^m F_i \) where \( F_i \cong \mathbb{Z}^{n_i}_{p_i} \) and \( \epsilon_i \neq \epsilon_j \) if \( p_i = p_j \). Then it follows from [16] that \( F \) admits a quaternion fixed-point-free automorphism group \( H \) of order 8 if and only if \( 2 \nmid p_i \) and \( 2 \nmid n_i \).
for all \( i = 1, \ldots, m \). In this case, \( H \) is conjugated to the group \( \langle x, y \rangle \) where the restrictions of \( x \) and \( y \) on \( F_i \) can be presented by matrices

\[
A_i = \bigoplus_{j=1}^{n_i/2} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B_i = \bigoplus_{j=1}^{n_i/2} \begin{pmatrix} \alpha_i & \beta_i \\ \beta_i & -\alpha_i \end{pmatrix},
\]

where \( i = 1, \ldots, m \) and \( \alpha_i^2 + \beta_i^2 \equiv -1 \mod p_i^\alpha \) for all \( i = 1, \ldots, m \).

In the following example we present a Frobenius group \( G \) with abelian kernel \( F \) and a complement \( H \) which is isomorphic to \( C_p \times Q_8 \), where \( p \) is an arbitrary odd prime. Of course, in this case \( G \) is an \( \mathfrak{F}_2T \)-group.

**Example 4.3.** Let \( q \) be a prime such that \( p | (q - 1) \) and let \( F = C_q^2 \). Let \( a, b \in \mathbb{Z}_q \) be such that \( a^2 + b^2 + 1 \equiv 0 \mod q \). Consider the automorphisms of \( C_q^2 \) represented by the following matrices over \( \mathbb{Z}_q \):

\[
A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad X = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}.
\]

Here \( \zeta \) is a primitive \( p \)-th root modulo \( q \). Then we have \( \langle A, B, X \rangle \cong C_p \times Q_8 \) and it can be verified that \( H = \langle A, B, X \rangle \) acts fixed-point-freely on \( F \). The corresponding Frobenius group \( F \rtimes H \) is an \( \mathfrak{F}_2T \)-group, but it is not an \( \mathfrak{F}_1T \)-group.

On the other hand, if the order of \( H \) is odd, then \( H \) is cyclic and the group \( F \) may be nonabelian. In the next example we show that this is indeed so.

**Example 4.4.** Let \( D = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \) be an elementary group of order 16. Put \( D_1 = D \rtimes \langle a \rangle \), where \( a \) is an element of order 2 acting on \( D \) in the following way: \( [x_1, a] = x_3 x_4 \), \( [x_2, a] = x_4 \), \( [x_3, a] = [x_4, a] = 1 \). We make another split extension \( F = D_1 \rtimes \langle b \rangle \), where \( b \) induces an automorphism of order 2 on \( D_1 \) in the following way: \( [x_1, b] = x_3 \), \( [x_2, b] = x_3 x_4 \) and \( [x_3, b] = [x_4, b] = [a, b] = 1 \). The group \( F \) is nilpotent of class 2 and \( |F| = 64 \). Consider the following map on \( F \):

\[
x_1^a = x_2, \quad x_2^a = x_1 x_2, \quad x_3^a = x_4, \quad x_4^a = x_3 x_4, \quad a^a = ab, \quad b^a = a.
\]

It can be verified that \( \alpha \) is an automorphism of order 3 on \( F \). Moreover, \( \alpha \) acts fixed-point-freely on \( F \). The corresponding split extension \( G = F \rtimes \langle \alpha \rangle \) is an \( \mathfrak{F}_2T \)-group of order 192 with the kernel \( F \). One can verify that this is the smallest example of a non-nilpotent soluble \( \mathfrak{F}_2T \)-group having the nonabelian Frobenius kernel.

Finite simple groups with nilpotent centralizers are classified in [12] and [13]. It turns out that every finite nonabelian simple \( CN \)-group is of one of the following types:

(i) \( \text{PSL}(2, 2^f) \), where \( f > 1 \);

(ii) \( \text{Sz}(q) \), the Suzuki group with parameter \( q = 2^{2n+1} > 2 \);
(iii) PSL(2, p), where p is either a Fermat prime or a Mersenne prime;
(iv) PSL(2, 9);
(v) PSL(3, 4).

By Theorem 2.5 only groups listed under (i) and (ii) are \( N_c T \)-groups for \( c > 1 \). Our aim is to show that in groups (iii)-(v) we can always find such nontrivial elements \( x, y \) and \( z \) that the groups \( \langle x, y \rangle \) and \( \langle y, z \rangle \) are nilpotent of class \( \leq 2 \), yet the group \( \langle x, z \rangle \) is not even nilpotent. We call such a triple of elements a **bad triple**.

**Proposition 4.5.** In the groups PSL(2, 9) and PSL(3, 4) there exist bad triples of elements.

**Proof.** First we want to show that our proposition holds true for PSL(3, 4). To this end, consider the matrices

\[
A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\]

over the Galois field GF(4). It is easy to see that \( A, B \) and \( C \) belong to SL(3, 4). Besides, these matrices are not in the center of SL(3, 4) and a straightforward calculation shows that \([A, B] = [B, C, C] = [C, B, B] = 1\). Let \( \overline{A}, \overline{B} \) and \( \overline{C} \) be the homomorphic images of \( A, B \) and \( C \), respectively, under the canonical homomorphism SL(3, 4) \( \rightarrow \) PSL(3, 4). Then the group \( \langle \overline{A}, \overline{B} \rangle \) is abelian and \( \langle \overline{B}, \overline{C} \rangle \) is nilpotent of class 2. On the other hand, \( \langle \overline{A}, \overline{C} \rangle \) is not nilpotent, since \([A, C], [A, C, C] \notin Z(SL(3, 4)) \text{ and } [A, C, C, C] = [A, C, C] \).

A similar argument also works for the group PSL(2, 9). In this case, we have to consider the following matrices in SL(2, 9):

\[
A = \begin{pmatrix} \zeta^3 & 0 \\ 0 & \zeta^5 \end{pmatrix}, \quad B = \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta^6 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 1 & \zeta^4 \\ \zeta^4 & \zeta^4 \end{pmatrix}.
\]

Here \( \zeta \) is a generator of the multiplicative group of GF(9). If \( \overline{A}, \overline{B} \) and \( \overline{C} \) are the corresponding elements of PSL(2, 9), then it is a routine to verify that the group \( \langle \overline{A}, \overline{B} \rangle \) is abelian and \( \langle \overline{B}, \overline{C} \rangle \) is nilpotent of class 2, but \( \langle \overline{A}, \overline{C} \rangle \) is not nilpotent.

Finally we consider the groups PSL(2, p) where \( p \) is a Fermat prime or a Mersenne prime. If \( p = 5 \), then PSL(2, 5) \( \cong \) PSL(2, 4) is an \( N_1 T \)-group by [11]. For \( p > 5 \) the situation is completely different.

**Proposition 4.6.** If \( p \) is a Fermat prime or a Mersenne prime and \( p \neq 5 \), then PSL(2, p) contains a bad triple of elements.

**Proof.** First we cover the case of Fermat primes. For this we need the following number-theoretical result:

**Claim 1.** If \( p \) is a Fermat prime, then there exists \( x \in \mathbb{Z}_p \) such that \( 2x^2 \equiv -1 \mod p \).
Proof of Claim 1. Let $p = 2^n + 1$ for some $n > 1$. It is enough to show that $2^{2n-1}$ is a quadratic residue modulo $p$. Let $P$ be the set of all integers $a \in \{0, \ldots, p-1\}$ which are primitive roots modulo $p$ and let $Q$ be the set of all $a \in \{0, \ldots, p-1\}$ which are not quadratic residues modulo $p$. We shall show that $P = Q$. First, if $a \notin Q$, then there exists an integer $t$ such that $t^2 \equiv a \pmod{p}$. By Euler's theorem, $a^{\phi(p)/2} \equiv t^{\phi(p)} \equiv 1 \pmod{p}$, hence $a$ is not a primitive root modulo $p$ (here $\phi$ is the Euler function). This shows that $P \subseteq Q$. To prove the converse inclusion, note that $p$ has exactly $\phi(\phi(p))$ incongruent primitive roots and exactly $(p-1)/2$ quadratic non-residues. Hence

$$|P| = \phi(\phi(p)) = \phi(p-1) = \phi(2^{2n}) = 2^{2n-1} = \frac{p-1}{2} = |Q|$$

and therefore $P = Q$. Since $2^{2n-1} \notin P = Q$, we have that $2^{2n-1} \equiv x^2 \pmod{p}$ for some $x \in \mathbb{Z}_p$, hence $2x^2 \equiv -1 \pmod{p}$, as desired.

Now we are ready to finish the proof. Let $c, x \in \mathbb{Z}_p$ be such that $c^2 \equiv -1 \pmod{p}$, $c \not\equiv -c \pmod{p}$ and $2x^2 \equiv -1 \pmod{p}$ (such $x$ exists by Claim 1). Let

$$A = \begin{pmatrix} 2x & 0 \\ 0 & -x \end{pmatrix}, \quad B = \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} x & x \\ x & -x \end{pmatrix}$$

be matrices in $\text{SL}(2, \mathbb{Z}) \setminus \mathbb{Z}(\text{SL}(2, \mathbb{Z}))$. It is clear that $A$ and $B$ commute, and a short calculation shows that $[B, C, C]$ and $[C, B, B]$ belong to $\mathbb{Z}(\text{SL}(2, \mathbb{Z}))$. To prove that $\text{PSL}(2, p)$ is not an $\mathfrak{M}$-group for any $c > 1$ it suffices to show that $[C, nA] \notin \mathbb{Z}(\text{SL}(2, \mathbb{Z}))$ for any $n \in \mathbb{N}$. More precisely, we shall prove that

$$[C, nA] = x^{3 \cdot 2^{n-2}} \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix},$$

where $a_n, b_n, c_n, d_n \in \mathbb{Z}_p$ are such that at least one of $b_n, c_n$ and at least one of $a_n, d_n$ are not zero. First note that this is true for $n = 1$, hence we may assume that $n > 1$. Then

$$[C, n+1A] = x^{3 \cdot 2^{n+1-2}} \begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix},$$

where $a_{n+1} = -2a_n d_n - 4b_n c_n$, $b_{n+1} = 3b_n d_n$, $c_{n+1} = 2a_n c_n$ and $d_{n+1} = b_n c_n - 2a_n d_n$. If both $b_{n+1}$ and $c_{n+1}$ are zero, then $a_n = d_n = 0$ which is not possible by the induction assumption. Similarly, if $a_{n+1} = d_{n+1} = 0$, then $a_n d_n = -2b_n c_n$ and $b_n c_n = 2a_n d_n$, hence $5b_n c_n = 0$, a contradiction since $p > 5$. This concludes the proof for Fermat primes.

Assume now that $p$ is a Mersenne prime. In this case we need the following auxiliary result:

Claim 2. If $p$ is a Mersenne prime, then there exist $x, y \in \mathbb{Z}_p$ such that $x^2 - x + 1 \equiv 0 \pmod{p}$ and $xy^4 \equiv 2y^2 + 1 \pmod{p}$.

Proof of Claim 2. First note that since $p$ is a Mersenne prime, $p - 1$ is divisible by 6. The congruence equation $x^2 \equiv -1 \pmod{p}$ is clearly solvable, hence it has $\text{gcd}(3, p-1) = 3$ incongruent solutions. This shows that the equation $x^2 - x + 1 = 0$ is solvable in $\mathbb{Z}_p$. Let $x_1$ and $x_2$ be its solutions. Then $x_2 = x_1^{-1} = 1 - x_1$. We claim
that at least one of $1 + x_1, 1 + x_2$ is a quadratic residue modulo $p$. For this note that since $(p - 1)/2$ is odd, Euler’s criterion implies that for every $a \in \mathbb{Z}_p \setminus \{0\}$ we have that precisely one of $a$ and $-a$ is a quadratic residue modulo $p$. Furthermore, since $\gcd(2^k, p - 1) = \gcd(2, p - 1)$, every quadratic residue modulo $p$ is also a $2^k$-power residue modulo $p$. Suppose $1 + x_1$ is not a square residue modulo $p$. Then $-1 - x_1$ is a quadratic residue modulo $p$ and $1 + x_2 = 2 - x_1 = 1 - x_1^2 = x_1^2(-1 - x_1)$ is a square residue modulo $p$. So from now on we assume $x$ is such that $1 - x + x^2 \equiv 0 \mod p$ and $1 + x$ is a square residue modulo $p$. Then the equation $xt^2 - 2t - 1 = 0$ has two solutions in $\mathbb{Z}_p$, namely $t_{1,2} = x^{-1}(1 \pm c) = x^2(-1 \mp c)$, where $c^2 = 1 + x$ in $\mathbb{Z}_p$. In order to ensure the existence of $y$ it suffices to prove that $-1 \mp c$ are square residues modulo $p$. Since $(-1 + c)(-1 - c) = -x = x^4$, we have that $-1 + c$ and $-1 - c$ are either both squares or both non-squares in $\mathbb{Z}_p$. Assume that they are not squares. Then $1 + c$ and $1 - c$ are squares in $\mathbb{Z}_p$. For every square $q$ in $\mathbb{Z}_p$ denote by $\sqrt{q}$ the square in $\mathbb{Z}_p$ for which $(\sqrt{q})^2 = q$. Let $u = \sqrt{1 - c}$ and $v = \sqrt{1 + c}$. Then $(u + v)^2 = u^2 + v^2 + 2uv = 2(1 + \sqrt{1 - c^2}) = 2(1 + \sqrt{-x}) = 2(1 + x^2)$. Since $p \equiv -1 \mod 8$, 2 is a square residue modulo $p$, hence $1 + x^2$ is a square in $\mathbb{Z}_p$. On the other hand, $-1 - x^2 = -x = x^4$ is also a square in $\mathbb{Z}_p$. This leads to a contradiction, hence our claim is proved.

Let $x$ and $y$ be as above and let

$$A = \begin{pmatrix} 0 & x^2 \\ x & 0 \end{pmatrix}, \quad B = \begin{pmatrix} x & x \\ -1 & -x \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 0 & y \\ -y^{-1} & 0 \end{pmatrix}$$

be matrices in $\text{SL}(2, p) \setminus Z(\text{SL}(2, p))$. It is not difficult to check that $[A, B] = -1$, hence $[A, B] \in Z(\text{SL}(2, p))$. Beside that, we have $[B, C, C] = (a_{ij})_{i,j}$, and a straightforward calculation shows that $a_{11} - a_{22} = x - x^2y^4 - 2x^4y^2 = 0$ by Claim 2. Similarly, we obtain $a_{21} = a_{12} = 0$, hence $[B, C, C]$ belongs to $Z(\text{SL}(2, p))$. Furthermore, it can be checked that the same holds true for $[C, B, B]$. On the other hand, an induction argument shows that

$$[A, nC] = \begin{pmatrix} y^{(-2)^n}x^{2^{n+1}} & 0 \\ 0 & y^{(-2)^n}x^{2^n} \end{pmatrix}$$

for every $n \in \mathbb{N}$. If $[A, nC] \in Z(\text{SL}(2, p))$ for some $n \in \mathbb{N}$, then $y^{(-2)^m}x^{2^{m+1}} = y^{(-2)^m}x^{2^m} = 1$ in $\mathbb{Z}_p$ for every $m > n$. Besides we have that $x^k$ is either $x - 1$ or $-x$, depending on whether $k$ is odd or even, respectively. Suppose $m > n$ and let $m$ be even. Then $[A, mC] = 1$ implies $y^{2m}(x - 1) = 1$ and $y^{-2m}x = -1$. Similarly, from $[A, m+1C] = 1$ we obtain $y^{-2m+1}x = -1$ and $y^{2m+1}(x - 1) = 1$. This implies $y^{2m} = 1$ and hence $x = -1$, which contradicts the choice of $x$. □

References


Received July 7, 2005