ISRAEL JOURNAL OF MATHEMATICS **132** (2002), 265–275

THE ORDERS OF NONSINGULAR DERIVATIONS OF MODULAR LIE ALGEBRAS

BY

S. MATTAREI*

Dipartimento di Matematica, Università degli Studi di Trento
via Sommarive 14, I-38050 Povo (Trento), Italy
e-mail: mattarei@science.unitn.it

ABSTRACT

We extend the results of Shalev [Sh] on the orders of nonsingular derivations of finite-dimensional non-nilpotent modular Lie algebras.

1. Introduction

Aner Shalev addressed the following problem in [Sh].

PROBLEM 1: *Which are the possible orders n of nonsingular derivations of finite-dimensional non-nilpotent Lie algebras of prime characteristic p?*

The significance of Problem 1 is well illustrated in the Introduction of Shalev's paper [Sh], to which we refer for a broader discussion. Here we will just mention a couple of relevant facts. On the one hand, the fact that $n = p - 1$ is not a solution for Problem 1 plays a crucial role in the effective proof given by Shalev in [Sh1] of the strongest of the coclass conjectures of Leedham-Green and Newman for pro-p groups [LGN]. On the other hand, the fact that Problem 1 does have solutions has implications for the coclass theory of Lie algebras. In fact, for all $k \geq 2$ there exist finite-dimensional simple Lie algebras of characteristic p which have nonsingular derivations of order $p^k - 1$, namely certain algebras discovered

* The author is grateful to Ministero dell'Università e della Ricerca Scientifica, Italy, for financial support to the project "Graded Lie algebras and pro-p-groups of finite width".
Received June 11, 2001

by Albert and Frank [AF] (nowadays also known as Hamiltonian of type ω_2, see for example [BKK]); these were employed in [Sh2] to construct the first examples of non-soluble modular graded Lie algebras of maximal class, thus disproving the analogues of Conjectures C and D of [LGN] for modular graded Lie algebras.

By means of an application of Engel's theorem, Shalev showed that Problem 1 is closely related to the following number-theoretic problem in finite fields.

PROBLEM 2: *For which numbers n is there an element $\alpha \in \bar{\mathbb{F}}_p$ (the algebraic closure of the field of p elements $\mathbb{F}_p$) such that $(\alpha + \lambda)^n = 1$ for all $\lambda \in \mathbb{F}_p$?*

More precisely, Shalev proved that if a number n satisfies the condition in Problem 1, then it also satisfies the condition in Problem 2. (This was stated only for n prime to p, since both problems are easily reduced to this case, but is true in general, because if n satisfies either condition, then any multiple of n also does.) Shalev also remarked that "it is unlikely that the converse also holds". However, we show in Section 2 of this note that the converse actually holds. Therefore, the two problems are fully equivalent.

From the above discussion it is clear that the admissible numbers n for Problem 1 or, equivalently, for Problem 2, include those of the form $p^k - 1$ for all $k \geq 2$, and all their multiples. However, these numbers do not exhaust all possibilities: for example, $(p^p - 1)/(p - 1)$ is admissible, and is not a multiple of any $p^k - 1$ for $k \geq 2$, if p is odd (see [Sh, Example 2.6]). But also for $p = 2$ there are more possibilities, the smallest being $n = 73$, mentioned in [Sh, Example 2.5]. In fact, a computer calculation shows that the only admissible numbers for $p = 2$ which are less than 10^4, are not proper multiples of other admissible numbers, and are not of the form $2^k - 1$, are 73, 85, 3133 and 4369. The paper [Bar] is also relevant to the case $p = 2$.

Although the determination of all numbers n which satisfy the condition in Problem 2 appears to be difficult, in [Sh] Shalev offered one step in that direction by proving that no number less than $p^2 - 1$ satisfies the condition. We offer one further step by proving, in Section 3, that the only numbers less than $p^3 - 1$ (for $p > 3$) which satisfy the condition are multiples of $p^2 - 1$.

In the final section of this paper we briefly discuss to what extent these results may admit generalization.

ACKNOWLEDGEMENT: I am grateful to the referee for his useful comments.

2. Nonsingular derivations of non-nilpotent Lie algebras

All Lie algebras in this paper are finite-dimensional of prime characteristic.

THEOREM 2.1: *Let $\alpha, \beta \in \bar{\mathbb{F}}_p$ with $\alpha\beta^{-1} \notin \mathbb{F}_p$ and let n be the least common multiple of the (multiplicative) orders of β and $\alpha + \lambda\beta$ when λ ranges over $\mathbb{F}_p$. Then there exists a (soluble) non-nilpotent Lie algebra over $\bar{\mathbb{F}}_p$ with a nonsingular derivation of order n.*

Proof: We slightly modify a classical example of a soluble but not triangulable matrix Lie algebra (see for example [Jac, pp. 52–53], or [Sel, p. 96]). Our example also appeared in [Win, p. 142].

Let M be a p-dimensional vector space over $\bar{\mathbb{F}}_p$ with base $e_1, \ldots, e_p$, and let E, F be the linear transformations of M defined by $e_iE = e_{i+1}$ (indices modulo p), and $e_iF = (\alpha + i\beta)e_i$. The transformations E and F span a two-dimensional soluble Lie algebra, which has M as a right module. Let L be the semidirect sum of M and $\langle E \rangle$ with respect to this action. Then F acts on L as a derivation, with eigenvalues β on $\langle E \rangle$, and $\alpha + \lambda\beta$ for $\lambda \in \mathbb{F}_p$ on M. The assertion about the order of the derivation follows. ∎

Remark 2.2: In [Sh, Lemma 2.2] Shalev shows, by using Engel's theorem, that if a non-nilpotent Lie algebra has a nonsingular derivation D of order prime to p, then the set S of its eigenvalues must contain a whole affine $\mathbb{F}_p$-line $\{\alpha + \lambda\beta\colon \lambda \in \mathbb{F}_p\}$. In our example, in addition to the line S contains one further element (namely the difference of two points of the line, say β). A closer look at the the proof of [Sh, Lemma 2.2] shows that this is indeed necessary. The nilpotency of a Lie algebra with a nonsingular derivation whose set of (generalized) eigenvalues is contained in an affine $\mathbb{F}_p$-line also follows from the following more general fact. If there is a maximal $\mathbb{F}_p$-subspace in $\bar{\mathbb{F}}_p$ which contains no eigenvalue of D, the cosets of that subspace give rise to a grading of L on the additive group of $\mathbb{F}_p$, where the component of degree zero is trivial. This implies that L is nilpotent, according to Higman's proof of his theorem on Lie rings with a fixed-point-free automorphism of prime order [Hig].

COROLLARY 2.3: *Let p be a prime number and let n be a positive integer, prime to p. The following statements are equivalent:*

1. *there exists a non-nilpotent Lie algebra of characteristic p with a nonsingular derivation of order n;*
2. *there exists an element $\alpha \in \bar{\mathbb{F}}_p$ such that $(\alpha + \lambda)^n = 1$ for all $\lambda \in \mathbb{F}_p$;*

3. *there exists an element* $c \in \bar{\mathbb{F}}_p^*$ *such that* $x^p - x - c$ *divides* $x^n - 1$ *as elements of the polynomial ring* $\bar{\mathbb{F}}_p[x]$.

Proof: It is proved in [Sh, Lemma 2.2] that the first statement implies the second.

If the second statement is true, Theorem 2.1 asserts the existence of a non-nilpotent Lie algebra L with a nonsingular derivation D of order m, the least common multiple of the orders of $\alpha + \lambda$ for $\lambda \in \mathbb{F}_p$. Since n is a multiple of m, it is easy to construct a Lie algebra with a nonsingular derivation of order n, for example, as suggested in [Sh], the tensor product $L \otimes_{\mathbb{F}} F[x]/(x^n - 1)$ with the derivation $D \otimes x$ (acting on the second factor as multiplication by x). An alternative construction, which may increase less the dimension, is forming the direct sum of L with an abelian Lie algebra, on which the derivation acts as a (nonsingular) linear map of order n.

The equivalence of the second and third statements is easy. In fact, the third statement follows from the second one by taking $c = \alpha^p - \alpha$. In the other direction, suppose that the third statement holds, and let $\alpha \in \bar{\mathbb{F}}_p$ be a root of the polynomial $x^p - x - c$. Then $\prod_{\lambda=0}^{p-1}(x - \alpha - \lambda) = (x - \alpha)^p - (x - \alpha) = x^p - x - c$ divides $x^n - 1 = \prod_{\rho \in R}(x - \rho)$, where R is the set of nth roots of unity in $\bar{\mathbb{F}}_p$, and the conclusion follows. ∎

In particular, Corollary 2.3 gives an affirmative answer to the final question of Shalev's paper, namely, there exists a finite-dimensional (soluble) non-nilpotent Lie algebra of characteristic p with a nonsingular derivation of order $(p^p - 1)/(p - 1)$ if p is odd, and of order 73 if $p = 2$.

3. The orders smaller than p^3

According to the result of the previous section, the possible orders of nonsingular derivations of non-nilpotent Lie algebras of characteristic p are those positive integers n such that $x^{n'} - 1$, where n' denotes the p'-part of n, is divisible by some polynomial of the form $x^p - x - c$. Let $\mathcal{N}_p$ denote the set of such possible orders.

We will determine all elements of $\mathcal{N}_p$ which are smaller than p^3; more precisely, we will show that they are the multiples of $p^2 - 1$, and $p^3 - 1$, for $p > 3$. (When $p = 3$ one has to include $(3^3 - 1)/2$, since $(p^p - 1)/(p - 1) \in \mathcal{N}_p$ always, as shown in [Sh, Example 2.6].)

It is shown in [Sh] that $\mathcal{N}_p$ contains no element smaller than $p^2 - 1$. Shalev's proof consists of reducing the polynomial x^n modulo $x^p - x - c$ and showing that

the result cannot be 1 if $n < p^2 - 1$. In one of two cases this is done by performing a binomial expansion and showing that a certain binomial coefficient is nonzero. This part of the proof appears to be hard to generalize to larger values of n. We offer here a variation of Shalev's proof which does not require any binomial expansion and illustrates our technique: rather than just using the congruence $x^n \equiv 1 \pmod{x^p - x - c}$ as in [Sh], we will make full use of the congruences $x^{m+n} \equiv x^m \pmod{x^p - x - c}$.

LEMMA 3.1: *Suppose $n \in \mathcal{N}_p$ satisfies $n < p^2$. Then $n = p^2 - 1$.*

Proof: Let $c \in \bar{\mathbb{F}}_p$ be such that $x^n \equiv 1 \pmod{x^p - x - c}$. All congruences in the present proof should be understood modulo $x^p - x - c$.

Note that powers x^m with m a power of p are easy to reduce modulo $x^p - x - c$. In fact, $x^{p^2} \equiv (x + c)^p = x^p + c^p \equiv x + c + c^p$ and, more generally, $x^{p^i} \equiv x + c + \cdots + c^{p^{i-1}}$.

Write $n = a_1 p + a_0$, with $0 \leq a_0, a_1 < p$. Suppose first that $a_0 + a_1 < p$. After replacing x^p with $x + c$, the congruence $x^n = (x^p)^{a_1} x^{a_0} \equiv 1$ becomes

$$(x + c)^{a_1} x^{a_0} \equiv 1.$$

Since both members are polynomials of degree less than p, we obtain $a_0 = a_1 = 0$, contradicting the fact that n is a positive integer.

Now suppose that $a_0 + a_1 \geq p$. Then the congruence $x^{p^2} \equiv x^{p^2 - n}$ becomes

$$x + c + c^p \equiv (x + c)^{p-1-a_1} x^{p-a_0},$$

because the p-adic expansion of $p^2 - n$ is $p^2 - n = (p - 1 - a_1)p + (p - a_0)$. Both members are polynomials of degree less than p, because $(p-1-a_1)+(p-a_0) < p$. Therefore, the congruence must be an equality. Since $x + c + c^p$ and $x + c$ are coprime (as c is nonzero), we conclude that $a_0 = a_1 = p - 1$, as desired. ∎

Now we use the same method of proof of Lemma 3.1 to determine all elements of $\mathcal{N}_p$ which are smaller than p^3. We will actually give a slightly stronger formulation. We recall that the order of a polynomial $f(x) \in \bar{\mathbb{F}}_p[x]$ with nonzero constant term is the smallest positive integer n such that $f(x)$ divides $x^n - 1$ in $\bar{\mathbb{F}}_p[x]$. When we talk about the order of a polynomial we shall implicitly assume that its constant term is nonzero. If $f(x)$ has no multiple roots, the order of $f(x)$ coincides with the order of the subgroup of $\bar{\mathbb{F}}_p^*$ generated by the roots of $f(x)$ and, in particular, is prime to p. Since $x^p - x - c$ has no multiple roots, it follows from Corollary 2.3 that the numbers in $\mathcal{N}_p$ are exactly all multiples of

the possible orders of polynomials of the form $x^p - x - c$. Furthermore, since the roots of $x^p - x - c$ form an affine $\mathbb{F}_p$-line with direction 1 in $\bar{\mathbb{F}}_p^*$ (see the last part of the proof of Corollary 2.3), the set $\mathcal{N}_p$ has also the following geometric interpretation: the numbers in $\mathcal{N}_p$ are the orders of subgroups of $\bar{\mathbb{F}}_p^*$ generated by a single affine $\mathbb{F}_p$-line with direction 1, and their multiples.

LEMMA 3.2: *Let p be a prime greater than 3, and suppose that the polynomial $x^p - x - c \in \bar{\mathbb{F}}_p$ has order $n < p^3$. Then $n = p^2 - 1$, or $n = p^3 - 1$.*

Proof: All congruences in the present proof should be understood modulo $x^p - x - c$.

Write n in its p-adic expansion $n = a_2p^2 + a_1p + a_0$, with $0 \leq a_0, a_1, a_2 < p$. It will be convenient to shorten this as $n = (a_2, a_1, a_0)$.

(1) If $a_0 + a_1 + a_2 < p$, we simply reduce modulo $x^p - x - c$ the congruence $x^n \equiv 1$, thus obtaining

$$(x + c + c^p)^{a_2}(x + c)^{a_1}x^{a_0} \equiv 1.$$

Since both members are polynomials of degree less than p, we obtain $a_0 = a_1 = a_2 = 0$, which is impossible.

(2) Another easy case is when $a_0 + a_1 + a_2 > 2p - 2$. Then we reduce modulo $x^p - x - c$ the congruence $x^{p^3} \equiv x^{p^3-n}$. Noting that $p^3 - n = (p - 1 - a_2, p - 1 - a_1, p - a_0)$, we obtain

$$x + c + c^p + c^{p^2} \equiv (x + c + c^p)^{p-1-a_2}(x + c)^{p-1-a_1}x^{p-a_0}.$$

Since the second member has degree less than p, it must have degree 1 like the first member, and we conclude that $a_0 = a_1 = a_2 = p - 1$, that is, $n = p^3 - 1$.

To proceed further, we will need to use the congruence $x^{m+n} \equiv x^m$ in all possible ways. If $m = (\ldots, b_2, b_1, b_0)$ is the p-adic expansion of m, then the expansion of the sum $m + n$ is $(\ldots, c_2, c_1, c_0)$, where the digits c_i are determined inductively by the rule

$$c_i = \begin{cases} a_i + b_i & \text{if } a_i + b_i < p \text{ and } c_{i-1} \geq a_{i-1} + b_{i-1}, \\ a_i + b_i - p & \text{if } a_i + b_i \geq p \text{ and } c_{i-1} \geq a_{i-1} + b_{i-1}, \\ a_i + b_i + 1 & \text{if } a_i + b_i < p - 1 \text{ and } c_{i-1} < a_{i-1} + b_{i-1}, \\ a_i + b_i - p + 1 & \text{if } a_i + b_i \geq p - 1 \text{ and } c_{i-1} < a_{i-1} + b_{i-1}, \end{cases}$$

where a_{-1}, b_{-1}, c_{-1} are assumed to be zero. In fact, $c_i < a_i + b_i$ occurs exactly if a *carry* has been produced by adding up a_i and b_i, possibly together with a

previous carry. Note, however, that this is also equivalent to the fact that $c_i < b_i$ together with $a_i < p-1$.

In the most general situation, reduction modulo $x^p - x - c$ of the congruence $x^{m+n} \equiv x^m$ yields

$$x^{c_0}(x+c)^{c_1}(x+c+c^p)^{c_2}\cdots \equiv x^{b_0}(x+c)^{b_1}(x+c+c^p)^{b_2}\cdots.$$

Since all factors appearing here are coprime to $x^p - x - c$ (for example, because $x+c+c^p+\cdots+c^{p^{i-1}} = x+\alpha^{p^i}-\alpha$, where α is any root of x^p-x-c), any factors appearing on both sides of the congruence can be cancelled. It follows that we may assume that at least one digit of each pair b_i, c_i vanishes. Also, a moment's thought shows that it does not pay to have any carries left of c_3 (say, for example, trying to use the congruence $x^{p^4} \equiv x^{p^4-n}$ in case (2) above), for the right member of the congruence would then always have degree at least p. So the congruences at our disposal are essentially 8 (two of which we have already seen above), each of them being determined by which digit additions produce a carry. To save on words, we will identify each of them by writing the matrix $\begin{bmatrix} \cdots & b_1 & b_0 \\ \cdots & c_1 & c_0 \end{bmatrix}$ of the digits of the two exponents in the congruence $x^{m+n} \equiv x^m$ that we are using, its reduction modulo $x^p - x - c$, and the consequences which we can draw for a_0, a_1, a_2 (possibly a contradiction) when both members have degree less than p. We will omit the actual argument, which will be the same in each case: when both members have degree less than p, they must be equal as polynomials, and unique factorization together with the fact that $x \neq x+c \neq x+c+c^p \neq x+c+c^p+c^{p^2}$ yields the desired conclusion. We have already seen the cases of $\begin{bmatrix} & & 0 \\ a_2 & a_1 & a_0 \end{bmatrix}$ and $\begin{bmatrix} p-1-a_2 & p-1-a_1 & p-a_0 \\ 1 \quad 0 & 0 & 0 \end{bmatrix}$.

(3) The exponents $\begin{bmatrix} & p-a_1 & 0 \\ a_2+1 & 0 & a_0 \end{bmatrix}$ give the congruence

$$(x+c+c^p)^{a_2+1}x^{a_0} \equiv (x+c)^{p-a_1}.$$

If $a_0 + a_2 < p-1$ and $a_1 > 0$ we obtain a contradiction.

(4) The exponents $\begin{bmatrix} p-a_2 & 0 & p-a_0 \\ 1 \quad 0 & a_1+1 & 0 \end{bmatrix}$ give the congruence

$$(x+c+c^p+c^{p^2})(x+c)^{a_1+1} \equiv (x+c+c^p)^{p-a_2}x^{p-a_0}.$$

If $a_0 + a_2 > p$ and $a_1 < p-2$ we obtain a contradiction.

(5) The exponents $\begin{bmatrix} p-a_2 & 0 & 0 \\ 1 \quad 0 & a_1 & a_0 \end{bmatrix}$ give the congruence

$$(x+c+c^p+c^{p^2})(x+c)^{a_1}x^{a_0} \equiv (x+c+c^p)^{p-a_2}.$$

If $a_0 + a_1 < p-1$ and $a_2 > 0$ we obtain a contradiction.

(6) The exponents $\begin{bmatrix} & p-1-a_1 & p-a_0 \\ a_2+1 & 0 & 0 \end{bmatrix}$ give the congruence

$$(x+c+c^p)^{a_2+1} \equiv (x+c)^{p-1-a_1} x^{p-a_0}.$$

If $a_0+a_1 > p-1$ and $a_2 < p-1$ we obtain a contradiction unless $c^p+c=0$, $a_0+a_2 = p-1$ and $a_1 = p-1$, in which case $n = (a_2+1)(p^2-1)$. However, from $x^{p^2} \equiv x+c+c^p = x$ we conclude that $n = p^2-1$.

(7) The exponents $\begin{bmatrix} & & p-a_0 \\ a_2 & a_1+1 & 0 \end{bmatrix}$ give the congruence

$$(x+c+c^p)^{a_2}(x+c)^{a_1+1} \equiv x^{p-a_0}.$$

If $a_1 + a_2 < p-1$ and $a_0 > 0$ we obtain a contradiction.

(8) The exponents $\begin{bmatrix} & p-1-a_2 & p-a_1 & 0 \\ 1 & 0 & 0 & a_0 \end{bmatrix}$ give the congruence

$$(x+c+c^p+c^{p^2})x^{a_0} \equiv (x+c+c^p)^{p-1-a_2}(x+c)^{p-a_1}.$$

If $a_1 + a_2 > p-1$ and $a_0 < p-1$ we deduce that $a_0 + a_2 = p-1$ and $a_1 = p-1$. Just as in case (6), we conclude that $n = p^2-1$.

It is now easy to see that all possibilities for (a_2, a_1, a_0) are covered by the above cases (and none of the cases is superfluous), except $a_0 = a_1 = a_2 = (p-1)/2$. In fact, apart from this exception, at least one of the numbers a_0+a_1, a_0+a_2, a_1+a_2 will be either less than or more than $p-1$, and we fall into (at least) one of the cases above (the slight deviation of case (4) from the apparently general pattern is not a problem, since if both a_0+a_1 and a_1+a_2 equal $p-1$, then a_0+a_2 will be even, and hence never equal to p).

To deal with the unfortunate exception of $a_0 = a_1 = a_2 = (p-1)/2$ we are forced to perform one further reduction modulo $x^p - x - c$. We have

$$\begin{aligned} x^n \equiv & (x+c+c^p)^{(p-1)/2}(x+c)^{(p-1)/2}x^{(p-1)/2} \\ = & x^{(p-1)/2}\sum_i \binom{(p-1)/2}{i} x^i c^{(p-1)/2-i} \cdot \\ & \cdot \sum_j \binom{(p-1)/2}{j} x^j (c+c^p)^{(p-1)/2-j}. \end{aligned}$$

This is a polynomial in x of degree $3(p-1)/2$, with no terms of degree less than $(p-1)/2$. Therefore, only its two terms of highest degree, namely

$$x^{(3p-3)/2} + \left(-c + \frac{p-1}{2}c^p\right)x^{(3p-5)/2},$$

will affect the term of degree $(p-3)/2$ of its reduction modulo $x^p - x - c$, which will thus be

$$cx^{(p-3)/2} + \Big(-c + \frac{p-1}{2}c^p \Big) x^{(p-3)/2} = \frac{p-1}{2} c^p x^{(p-3)/2}.$$

Since $c \neq 0$ and $p > 3$, the reduced polynomial cannot be 1, and we reach a contradiction. ∎

Remark 3.3: Note that a variation of the above proof, which would have perhaps simplified the discussion slightly, would be expanding n into a p-adic form with digits of both signs and absolute value less than $p/2$. Our approach has the advantage of showing that the congruence $x^{m+n} \equiv x^m$ has been used in all possible ways.

COROLLARY 3.4: *Let $p > 3$ and suppose that $n \in \mathcal{N}_p$ satisfies $n < p^3$. Then n is either $p^3 - 1$, or a multiple of $p^2 - 1$.*

In the situation of Lemma 3.2 but for $p = 3$, besides the cases $n = 3^2 - 1$ and $n = 3^3 - 1$ we must allow for the possibility that $n = (3^3 - 1)/2 = 13$. When $n = 13$, the final argument in the proof of Lemma 3.2 also yields that $c = 1$. However, this is just one case of an easily proved general fact: for any prime p, there is exactly one polynomial of the form $x^p - x - c \in \bar{\mathbb{F}}_p[x]$ whose order divides $(p^p - 1)/(p - 1)$, namely $x^p - x - 1$. Incidentally, it is also easy to prove that the order of $x^p - x - c$ cannot divide any number of the form $(p^k - 1)/(p - 1)$ for p odd and $k < p$.

4. Final remarks

We will point out to what extent and in which directions Lemma 3.2 and Corollary 3.4 could be generalized.

For some time we mistakenly believed in the following statement: the elements of $\mathcal{N}_p$ which are smaller than p^p are either multiples of $p^i - 1$ for some $1 < i < p$, or multiples of $(p^p - 1)/(p - 1)$. In fact, this is certainly true for $p = 3$ because of Corollary 3.4, and can be shown to be true also for $p = 5$, with the help of a computer. However, such a strong statement already fails for $p = 7$, as the following example shows.

Example 4.1: We have $(7^5 - 1)/2 \in \mathcal{N}_7$. In fact, a computer calculation shows that the order of $x^7 - x - c$ in characteristic 7 divides $(7^5 - 1)/2$ if and only if c is a root of the polynomial

$$\begin{aligned} &c^{15} + 2c^{12} + 6c^9 + 6c^6 + 3c^3 + 6 \\ &\quad = (c^5 + c^3 + 3c^2 + 5c + 5)(c^5 + 2c^3 + 3c^2 + 6c + 3)(c^5 + 4c^3 + 3c^2 + 3c + 6). \end{aligned}$$

Actually, for such values of c the order of $x^7 - x - c$ is exactly $(7^5 - 1)/2$, since one can check that no other proper divisor of $7^5 - 1$ can be the order of a trinomial of that form.

Similarly, one can compute that the order of $x^{11} - x - c$ in characteristic 11 is $(11^5 - 1)/2$ if and only if c is a root of $c^5 + 7$ (and such order cannot be any other proper divisor of $11^5 - 1$). Hence $(11^5 - 1)/2$ belongs to $\mathcal{N}_{11}$. However, one can also check that $(13^5 - 1)/2 \notin \mathcal{N}_{13}$.

Example 4.1 also shows that a direct extension of Lemma 3.2, showing that the only possible values $n < p^5$ for the order of the polynomial $x^p - x - c \in \bar{\mathbb{F}}_p$ are numbers of the form $n = p^i - 1$, would require at least $p > 11$ as an assumption. We have reasons to believe that a similar assertion describing the possible orders $n < p^4$ should be true for all $p > 3$, though our method of proof of Lemma 3.2 appears insufficient to deal with that case.

More generally, we propose the following question.

QUESTION 4.2: *Given an integer $r > 1$, is it true for all sufficiently large primes p that all possible values $n < p^r$ for the order of the polynomial $x^p - x - c \in \bar{\mathbb{F}}_p$ have the form $n = p^i - 1$?*

It is perhaps worth noting that this is true if we restrict our attention to those n which divide $p^r - 1$ (instead of all $n < p^r$). This is an immediate consequence of the following result of H. Davenport [Dav, Theorem 1]: given $k > 1$, if the prime p is sufficiently large (depending only on k) and $\mathbb{F}_{p^k} = \mathbb{F}_p(\alpha)$, then there exists $\lambda \in \mathbb{F}_p$ such that $\alpha + \lambda$ is a primitive element of $\mathbb{F}_{p^k}$ (that is, a generator of $\mathbb{F}_{p^k}^*$). In fact, if $x^p - x - c$ has order a divisor n of $p^r - 1$ and α is one of its roots, then $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^k}$ for some divisor k of r, and $\mathbb{F}_{p^k}$ contains all the roots of that polynomial; Davenport's theorem applied to all subfields $\mathbb{F}_{p^k}$ of $\mathbb{F}_{p^r}$ (whose number is independent of p) implies that at least one of the roots is primitive, and so $n = p^k - 1$, provided p is larger than a bound which depends only on r.

Of course, Question 4.2 is much stronger than this. In case it turns out to be false in general, it would nevertheless be interesting to determine the highest r for which its statement is true.

References

[AF] A. A. Albert and M. S. Frank, *Simple Lie algebras of characteristic p*, Rendiconti del Seminario Matematico Università e Politecnico di Torino **14** (1954–55), 117–139.

[Bar] L. Bartholdy, *Lamps, Factorizations, and Finite Fields*, The American Mathematical Monthly **107** (2000), 429–436.

[BKK] G. Benkart, A. I. Kostrikin and M. I. Kuznetsov, *Finite-dimensional simple Lie algebras with a nonsingular derivation*, Journal of Algebra **171** (1995), 894–916.

[Dav] H. Davenport, *On primitive roots in finite fields*, Quarterly Journal of Mathematics **8** (1937), 308–312.

[Hig] G. Higman, *Groups and rings which have automorphisms without nontrivial fixed elements*, Journal of the London Mathematical Society **32** (1957), 321–334.

[Jac] N. Jacobson, *Lie Algebras*, Wiley-Interscience, New York, 1962.

[LGN] C. R. Leedham-Green and M. F. Newman, *Space groups and groups of prime power order I*, Archiv der Mathematik **35** (1980), 193–202.

[Sel] G. B. Seligman, *Modular Lie algebras*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40, Springer-Verlag, New York, 1967.

[Sh] A. Shalev, *The orders of nonsingular derivations*, Journal of the Australian Mathematical Society (Series A) **67** (1999), 254–260.

[Sh1] A. Shalev, *The structure of finite p-groups: effective proof of the coclass conjectures*, Inventiones Mathematicae **115** (1994), 315–345.

[Sh2] A. Shalev, *Simple Lie algebras and Lie algebras of maximal class*, Archiv der Mathematik **63** (1994), 297–301.

[Win] D. J. Winter, *On groups of automorphisms of Lie algebras*, Journal of Algebra **8** (1968), 131–142.