Two-variable identities in groups and Lie algebras [*]

Fritz Grunewald
Math. Institut, Heinrich Heine Universität,
40225 Düsseldorf, GERMANY
e-mail: grunewald@math.uni-duesseldorf.de

Boris Kunyavskiĭ[†]
Dept of Math. and Computer Science, Bar-Ilan University,
52900 Ramat Gan, ISRAEL
e-mail: kunyav@macs.biu.ac.il

Daniela Nikolova
Insitute of Math., Bulgarian Academy of Sciences,
Sofia, BULGARIA
e-mail: daniela@moi.math.bas.bg

Eugene Plotkin[†]
Dept of Math. and Computer Science, Bar-Ilan University,
52900 Ramat Gan, ISRAEL
e-mail: plotkin@macs.biu.ac.il

Abstract

We study two-variable Engel-like relations and identities characterizing finite dimensional solvable Lie algebras and, conjecturally, finite solvable groups, and introduce some invariants of finite groups associated to such relations.

[*] This research was supported by the Israel Science Foundation founded by the Israel Academy of Sciences and Humanities — Center of Excellence Program.

[†] Partially supported by the Ministry of Absorption (Israel) and the Minerva Foundation through the Emmy Noether Research Institute of Mathematics.

1 Motivation

Our primary interest in problems discussed in the present paper came from a paper by Segev [25] where the Margulis–Platonov conjecture had been related to some properties of the commuting graph of a finite simple group. (Given a finite group F, its commuting graph $\Gamma(F)$ has vertices indexed by the elements of F different from 1; $x, y \in F$ are joined by an edge if and only if they commute.) In a more recent paper [26] the expected properties of this graph have been proved.

In its simplest form, the Margulis–Platonov conjecture asserts that if G is any (absolutely almost) simple linear algebraic group defined over a number field k then the group of rational points $G(k)$ contains no non-central normal subgroups if and only if the same is true for all groups $G(k_v)$ where v runs over all places of k and k_v stands for the completion of k at v (see [22, 9.1]). The most difficult case of this conjecture is that of anisotropic groups of type A_n. In the case of the inner forms, Potapchik and Rapinchuk [24] reduced the conjecture to a purely algebraic statement that the multiplicative group of any finite dimensional division k-algebra has no non-abelian finite simple quotients. For this purpose, Segev proved [25] that if D is a finite dimensional division algebra over an arbitrary field and F is a finite simple non-abelian group whose commuting graph $\Gamma(F)$ is either balanced (see [25] for the definition), or is of diameter greater than 4, then F cannot be a quotient of D^*. In [26], it is proved that the commuting graph of any finite non-abelian simple group is either balanced, or of diameter greater than 4. This completes the proof.

All above shows that $\Gamma(F)$ is a powerful invariant of F. After Segev's lecture on this topic, B. Plotkin suggested two natural generalizations of the commuting graph of a group. Namely, it is natural to consider graphs of nilpotency and solvability of an arbitrary group G. To define them, we need to formulate conditions of nilpotency and solvability as two-variable relations between the elements of G. This is done in Section 2. In Section 3 we consider Lie-algebraic analogues of these conditions. In Section 4 we focus on the case of linear algebraic groups and groups of their rational points. In Section 5 we return to the case of finite groups which was the main motivation for this paper.

Notation. If G is a group, $x, y \in G$, let $[x, y] = x^{-1}y^{-1}xy$. If L is a Lie algebra, $x, y \in L$, we use the same symbol $[x, y]$ for the Lie product.

Acknowledgements. This work was done while D. Nikolova was visiting Bar-Ilan University and Ben-Gurion University of the Negev, Israel, and the National University of Ireland, Galway. The paper was finished while B. Kunyavskiĭ and E. Plotkin were visiting SFB 343 “Diskrete Strukturen in der Mathematik” (University of Bielefeld). The authors gratefully appreciate hospitality and support of these institutions. We thank M. Borovoi, R. Farnsteiner, A. Premet, and N. Vavilov for very useful discussions and correspondence. Our special thanks go to B. Plotkin whose ideas and encouragement were indispensable, and to A. Feldman and R. Shklyar for their help in computer experiments.

2 New invariants of finite groups

Our primary goal is to introduce some new invariants of a group G associated to two-variable relations between elements of G.

Definition 2.1 *Let G be an arbitrary group, and let ρ be a binary relation on G. We define a (directed) graph $\Gamma^+ = \Gamma^+_\rho(G)$ (ρ-graph of G) as follows: the vertices of Γ^+ are indexed by the elements of G different from 1, and vertices g, h form an edge directed from g to h if and only if $g \neq h$ and $g\rho h$. We denote by Γ the non-directed graph obtained from Γ^+ by forgetting orientation and deleting multiple edges.*

Remark. If ρ is symmetric, we only consider the non-directed graph $\Gamma_\rho(G)$.
Example. If ρ is the commuting relation (i.e. $g\rho h$ if and only if $gh = hg$), we get the commuting graph of G studied in [25].

First we consider "nilpotency relations". Denote Engel words by $v_1 = v_1(x, y) = [x, y]$, $v_2 = [v_1, y], \dots, v_n = [v_{n-1}, y], \dots$.

Definition 2.2 *Let G be an arbitrary group. We say that elements $g, h \in G$ are in n-Engel relation ν_n if $v_n(g, h) = 1$. Elements g, h are said to be in nilpotency relation ν if they are in n-Engel relation for some n.*

Recall that a finite group G is nilpotent if and only if the identity $v_n(x, y) \equiv 1$ holds in G for some n, or, in terms of the above definition, if and only if $g\nu h$ for all $g, h \in G$. Note that $v_k \equiv 1$ implies $v_l \equiv 1$ for all $l > k$.

Definition 2.3 *The graph $\Gamma_\nu(G)$ (resp. $\Gamma^+_\nu(G)$) is called the nilpotency graph (resp. directed nilpotency graph) of G. The diameters of these graphs are denoted by $d_\nu(G)$ and $d^+_\nu(G)$, respectively. (If there are vertices g, h with no path from g to h, the diameter is defined to be infinite.)*

Problem 2.4 *To investigate nilpotency graphs of finite simple groups and to estimate their diameters.*

We turn now to "solvability relations". Here we immediately encounter the following

Problem 2.5 *Find a sequence of words $\{e_n(x, y)\}_{n=1}^\infty$ in two variables x, y such that a finite group G is solvable if and only if for some n the identity $e_n \equiv 1$ holds in G.*

Remark. Similarly to the nilpotency case, we require that the identity $e_k \equiv 1$ would imply $e_l \equiv 1$ for all $l > k$.

With such a sequence at our disposal, we could define the solvability relation in G and the corresponding graphs repeating, word by word, Definitions 2.2–2.3.

There is strong evidence that Problem 2.5 has a positive solution, and finite solvable groups can be characterized by two-variable identities.

Theorem 2.6 [28], [8] *Let G be a finite group in which every two elements generate a solvable subgroup. Then G is solvable.*

However, Theorem 2.6 does not provide any explicit two-variable laws for finite solvable groups. We present several candidates for such e_n's.

Definition 2.7 *Let $\{e_n(x,y)\}_{n=1}^{\infty}$ be defined by one of the following three formulae:*

$$\begin{array}{lllllll} e_1 & = & [x,y], & & & & \\ e_1' & = & [e_1,x], & e_1'' = [e_1,y], & e_2 & = & [e_1',e_1''], \quad \ldots \\ e_n' & = & [e_n,x], & e_n'' = [e_n,y], & e_{n+1} & = & [e_n',e_n''], \quad \ldots \end{array} \tag{1}$$

$$e_1=[x,y], e_2=[xe_1x^{-1},ye_1y^{-1}],\ldots,e_{n+1}=[xe_nx^{-1},ye_ny^{-1}],\ldots \tag{2}$$

$$\begin{array}{l} e_1'=x, e_1''=y, e_1=[e_1',e_1''],\ldots \\ e_{n+1}'=[[e_n',e_n''],e_n'], e_{n+1}''=[[e_n'',e_n'],e_n''], e_{n+1}=[e_{n+1}',e_{n+1}''],\ldots \end{array} \tag{3}$$

We call sequences (1)–(3) *reasonable.*

Note that for all reasonable sequences, $e_k \equiv 1$ implies $e_l \equiv 1$ for all $l > k$.

Remark. There is a natural way to produce reasonable sequences generalizing (2). Namely, let w be a word in x, y, x^{-1}, y^{-1}. Define

$$e_1^w = w, e_{n+1}^w = [xe_n^w x^{-1}, ye_n^w y^{-1}],\ldots.$$

A clever choice of w might lead to a sequence with good properties. We shall discuss the matter in detail in our forthcoming paper.

Definition 2.8 *Fix a reasonable sequence $\{e_i\}$. Let G be an arbitrary group. We say that elements $g,h \in G$ are in relation σ_n (with respect to $\{e_i\}$) if $e_n(g,h)=1$. Elements g,h are said to be in solvability relation σ if and only if they are in relation σ_n for some n. We call σ-graph $\Gamma_\sigma(G)$ (resp. $\Gamma_\sigma^+(G)$) the solvability graph (resp. the directed solvability graph) of G.*

To justify the above definition, one has to prove the following analogue of the Engel property.

Conjecture 2.9 (B. Plotkin) *Let $\{e_i\}$ be a reasonable sequence. A finite group G is solvable if and only if for some n the identity $e_n \equiv 1$ holds in G.*

Clearly, if G is solvable of derived length n, then $e_n \equiv 1$ holds in G.

Remark. There is another way to define nilpotency and solvability relations: $g,h \in G$ are in relation ν (resp. σ) if and only if the subgroup of G generated by g and h is nilpotent (resp. solvable). Such relations have an advantage to be symmetric and disadvantage to be less constructive. We do not consider them in the present paper. We refer the reader to [23] for yet another definition of the solvability graph and relationship with abstract algebraic geometry over groups.

There are several results concerning characterization of solvable groups in terms of two-variable identities [19], [20], [5]. Namely, it was proved in [19], [20] that if a finite group G satisfies for some n the identity $v_2 \equiv v_n$, where $\{v_i\}$ is the sequence of Engel words, then G is solvable. However, it is easy to find a solvable group satisfying no identity of the form $v_2 \equiv v_n$. For example, take G a finite nilpotent group of class 3 such that the identity $v_2 \equiv 1$ does not hold in G. Since $v_3 \equiv 1$, the group G cannot satisfy any identity of the form $v_2 \equiv v_m$. However, G is solvable.

In [5] it was proved that the identity $v_3 \equiv v_n$ can hold in certain finite simple groups such as $\mathrm{PSL}(2,4)$, $\mathrm{PSL}(2,8)$, etc. Let us also mention a pioneer result of N. Gupta [10]: any finite group satisfying the identity $v_1 \equiv v_n$ is abelian.

At this point, let us introduce some more new invariants of finite groups. Our first remark is that given any infinite sequence of distinct words in m variables $\{w_i(x_1,\dots,x_m)\}_{i=1}^{\infty}$, any finite group G satisfies a law of the type

$$w_k(x_1,\dots,x_m) \equiv w_l(x_1,\dots,x_m).$$

for some k and l. (Indeed, the set of values of the w_i's is finite.)

The next definition goes back to [11]. It generalizes the notion of Engel depth (cf. [4], [5]).

Definition 2.10 *The pair (k,l) for which the identity $v_k(x,y) \equiv v_l(x,y)$ holds, with minimal $k+l$, is called the Engel invariant of G.*

Remark. To justify the above definition, one has to check that the pair (k,l) with the required properties is unique. Indeed, suppose that we have two Engel identities in G: $e_k \equiv e_l$ and $e_m \equiv e_n$ with $k < m < n < l$ and $k+l = m+n$ minimal with this property.

We have $e_m(x,y) = e_n(x,y)$ for all x,y. Plug $e_{l-n}(x,y)$ instead of x. We get $e_{l-n+m}(x,y) = e_l(x,y)$ for all x,y. Hence $e_k(x,y) = e_{l-n+m}(x,y)$ for all x,y. Therefore, because of minimality of $k+l$, we have $k+(l-n+m) \geq k+l$, i.e. $m-n \geq 0$, contradiction. The Engel invariant is thus well defined.

This remark also shows that the number k in Definition 2.10 coincides with the Engel depth of G as defined in [4], [5]. However, the second parameter l is also important as the following beautiful result shows [11, Th. 4.3]: with the notation of Definition 2.10, if $k+l$ is odd then G is solvable.

Problem 2.11 *To compute Engel invariants for particular classes of finite groups.*

In [18], Engel invariants have been computed in some groups, classes of groups and varieties of groups such as some groups of small order; the class of dihedral groups D_p where p is an odd prime; the solvable locally finite varieties of groups A_kA_l for k and l powers of one and the same prime number p, and for k and l coprime integers; the infinite series of simple groups (the alternating groups A_n for $n > 5$ and the special projective groups $\mathrm{PSL}(2,q)$ for some of the first groups in the series).

One can consider the analogues of Definition 2.10 and Problem 2.11 with the Engel sequence replaced by one of reasonable (in the sense of Definition 2.7) sequences.

Definition 2.12 *Let $\{e_i\}$ be a reasonable sequence. The pair (k, l) for which the identity $e_k(x, y) \equiv e_l(x, y)$ holds, with minimal $k + l$, is called σ-invariant of G. If there are several such pairs, we choose among them the pair with minimal k and define it to be $\sigma(G)$.*

Problem 2.13 *To compute σ-invariants for particular classes of finite groups.*

3 Lie-algebraic analogues

On replacing commutators by Lie products (and 1 by 0), we get sequences similar to (1)–(3) for Lie algebras. We also call them reasonable. Here the situation is much more clear (at least, in finite dimensional case). We restrict ourselves by considering the Lie analogue of sequence (1).

Theorem 3.1 *Let L be a finite dimensional Lie algebra over an infinite field k of characteristic $p > 5$. Let $\{e_i\}$ be defined by formulae (1). Then L is solvable if and only if for some n the identity $e_n \equiv 0$ holds in L.*

Proof. Obviously, if L is solvable then it satisfies an identity of the form $e_n(x, y) \equiv 0$ since for any $X, Y \in L$ the value $e_n(X, Y)$ belongs to the corresponding term of the derived series. Conversely, let L satisfy the identity $e_n \equiv 0$. First suppose that k is algebraically closed. If L is not solvable then $L^{\mathrm{ss}} = L/\mathrm{rad}(L)$ is semisimple and non-zero (here $\mathrm{rad}(L)$ denotes the solvable radical of L, i.e. its maximal solvable ideal). If $\mathrm{char}(F) = 0$, let us denote by $\{E_\alpha, H_\alpha, E_{-\alpha}\}$ the standard basis of sl_2. Then $[E_\alpha, E_{-\alpha}] = H_\alpha$, $[H_\alpha, E_\alpha] = 2E_\alpha$, $[H_\alpha, E_{-\alpha}] = -2E_{-\alpha}$. Set $x = E_\alpha$, $y = E_{-\alpha}$. Then

$$\begin{array}{rclrclrcl} e_1 & = & H_\alpha, & e_1' & = & 2E_\alpha, & e_1'' & = & -2E_{-\alpha}, \\ e_2 & = & -4H_\alpha, & \ldots, \end{array}$$

i.e. $e_n = mH_\alpha$ with $m \neq 0$. Thus for any n we have $e_n(E_\alpha, E_{-\alpha}) \neq 0$.

Let now $\mathrm{char}(k) = p > 5$. First assume that L is restricted (see [27, 2.1] for the definition; we refer to the same book for all background material in modular Lie algebras). Then we can use the classification theorem of [2] in order to mimic the proof in characteristic zero. To be more precise, [2] says that all simple restricted Lie algebras are given by the list predicted by the Kostrikin–Shafarevich conjecture. One can then verify that each of such algebras contains sl_2. For the algebras of classical type this is obvious. As to the algebras of Cartan type, one has to consider them as graded Lie algebras (see [27, Ch. 4]) and notice that the zero component L_0 contains sl_2. Indeed, $S(n; \mathbf{1})_0 \cong sl_n$ ([27, Prop. 3.3.4]), $H(2r; \mathbf{1})_0 \cong sp_{2r}$ ([27, Prop. 4.4.4]), $K(2r+1; \mathbf{1})_0$ contains sp_{2r} ([27, Ex. 4.5.3]), and $W(n; \mathbf{1})_0 \cong gl_n$ ([27, Prop. 2.2.4]). In this last case for $n = 1$ one has to consider the algebra $L_{-1} \oplus L_0 \oplus L_1$; one can show that it is isomorphic to sl_2.

If L is not restricted, one needs more subtle arguments.

Lemma 3.2 *Every simple Lie algebra L defined over a field of characteristic $p > 5$ contains a subalgebra S with quotient isomorphic to sl_2.* [1]

Proof. Assume the contrary. Let L denote a counter-example of minimal dimension to the assertion of the lemma. Let L° denote a maximal subalgebra of L. We wish to show that L° is solvable. If not, then $L^{\mathrm{ss}} = L^\circ/\mathrm{rad}(L^\circ)$ is a non-zero semisimple Lie algebra. By [1, Th. 9.3], L^{ss} contains a simple algebra S. Let $S_1 = \pi^{-1}(S)$ be the preimage of S with respect to the natural projection $\pi\colon L^\circ \to L^{\mathrm{ss}}$, we have $S_1/\ker\pi \cong S$. Since $\dim S < \dim L$, there is a subalgebra $T \subseteq S$ and an ideal J in T such that $T/J \cong sl_2$. Denote $T_1 = \pi^{-1}(T)$, $J_1 = \pi^{-1}(J)$. We have $T_1/J_1 \cong sl_2$, contradiction. We thus proved that L° is solvable. By [29, Cor. 1.4], L must be isomorphic either to sl_2, or to the Zassenhaus algebra $W(1;m)$. In the first case we are done. In the second case L is graded, and we set $S = L_{-1} \oplus L_0 \oplus L_1$. Each of the three components is one-dimensional, and a straightforward computation using the table of structure constants shows that $S \cong sl_2$. The lemma is proved. □

Let us continue the proof of the theorem. We have a Lie algebra L satisfying the identity $e_n(x,y) \equiv 0$. We wish to prove that L is solvable. Assume the contrary. Then, arguing as in the proof of Lemma 3.2 (i.e. considering $L/\mathrm{rad}(L)$ and using [1, Th. 9.3]), we conclude that L has a simple subalgebra S. From Lemma 3.2 it follows that S (and hence L) has a subfactor isomorphic to sl_2. Since identities remain true in sub- and factor-algebras, $e_n \equiv 0$ must hold in sl_2, contradiction. We thus proved the "if" part of the theorem in the case where k is algebraically closed.

Let now k be an arbitrary infinite field, and suppose that L is a Lie algebra over k satisfying an identity $w(x,y) \equiv 0$, where w stands for one of the e_n's. We wish to prove that the identity $w(x,y) \equiv 0$ also holds in the Lie algebra $\overline{L} = L \otimes_k \bar{k}$ defined over an algebraic closure $\bar{k}$ of k. Indeed, let $\{E_1, \dots, E_d\}$ denote a k-basis of L. On writing arbitrary $x, y \in L$ with respect to this basis: $x = \sum \alpha_i E_i$, $y = \sum \beta_i E_i$, we translate the identity $w(x,y) \equiv 0$ into identities of the form

$$P_i(\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d) = 0, \qquad i = 1, \dots, d,$$

where P_i are polynomials. Since all the values of each P_i are zero and k is infinite, we conclude that the P_i's are zero polynomials (see, for example, [15, Ch. IV, §1, Cor. 1.7]). Let now $\bar{x}, \bar{y} \in \overline{L}$ are arbitrary elements. On writing them with respect to the same basis $\{E_i\}$ (with coefficients from $\bar{k}$) and plugging into the expression for $w(\bar{x}, \bar{y})$, we obtain the same polynomials P_i as coefficients at E_i. But we have already proved that they are zero. Hence $w(\bar{x}, \bar{y}) = 0$.

The theorem is proved. □

Note one more result in the same spirit (cf. [10], [11], [19], [20], [5] for the group case). Recall that $\{v_i\}$ is the Engel sequence, $v_i(x,y) = [[[x,y],y]\dots y]$ (for brevity we denote this expression by $[x, y_i]$).

Proposition 3.3 *Let L be a finite dimensional Lie algebra over a field of characteristic different from 2 such that the identity $v_k \equiv v_l$ holds in L. Then L is solvable. Moreover, if L satisfies $v_1 \equiv v_l$ then L is abelian.*

[1] A. Premet informed us that one can modify the proof to be valid for all $p > 2$.

Proof. As in the preceding theorem, we can reduce to the case where the ground field is algebraically closed. First consider the characteristic zero case. Again, if L is not solvable then $L^{\mathrm{ss}} = L/\mathrm{rad}(L)$ is non-zero and contains sl_2. Set $x = H_\alpha$, $y = E_\alpha$. We have $v_1 = 2E_\alpha$, $v_2 = 4E_\alpha, \dots$, thus $v_k \equiv v_l$ leads to $2^k E_\alpha = 2^l E_\alpha$, contradiction. In the positive characteristic, we just reproduce the arguments from Theorem 3.1.

Let now $v_1 \equiv v_l$. We proceed by induction on $\dim L$. If $\dim L = 1$ then L is abelian. Suppose that all subalgebras of dimension less than $n = \dim L$ are abelian. By the first part of the proposition, L is solvable. Hence $L' = [L, L]$ is of dimension less than n and therefore is abelian. We have to prove that $L' = 0$. Take any $[x, z] \in L'$. By assumption, $[x, z] = [x, z_l]$. Let $z = [x, y]$. Then $[x, [x, y]] = [x, [x, y]_l] = 0$ since L' is abelian. Therefore $[[x, y], x] = 0$ and hence $[[y, x], x] = 0$ and $[y, x_l] = 0$. Applying our assumption once again we get $[y, x] = 0$, so that $L' = 0$ and thus L is abelian. □

Remark. As in the case of finite groups, one can note that the identity $v_2 \equiv v_l$ gives only a sufficient condition for a finite dimensional Lie algebra to be solvable.

4 Identities in linear groups

One of the most promising approaches to the proof of Conjecture 2.9 is related to the study of identities in finite linear groups. To be more precise, the following question seems to be critical: let $\{e_i\}$ denote one of the reasonable sequences (see formulae (1)–(3)), and let $G = \mathrm{PSL}(2, p)$, $p > 3$; is it true that neither of the formulae e_n is an identity in G? (See the next section for more details.) It is known [21], [17, Cor. 52.12] that any finite group G has a finite basis of identities but for $\mathrm{PSL}(2, p)$ the explicit bases are known only for $p \leq 13$ (see [6] and references therein). Clearly the identities of $\mathrm{PSL}(2, p)$ heavily depend on p because $\mathrm{PSL}(2, \mathbb{Z})$ has no identities at all. Thus looking at $\mathcal{G} = \mathcal{PSL}(2, \cdot)$ as at a group scheme, one can say that different values of $\mathcal{G}$ have different identities. On the other hand, if an affine group scheme $\mathcal{G}$ is assumed to be either abelian, or nilpotent, or solvable, then all its values inherit the corresponding identities. Therefore, given a linear group $G \subset \mathrm{GL}(n, k)$ isomorphic to the group $\mathcal{G}(k)$ of k-rational points of an affine group scheme $\mathcal{G}$, it is important to distinguish its "structural" identities (i.e. coming from $\mathcal{G}$) from those arising from the special choice of k.

We now make all above considerations more precise. First introduce some notation. Given an affine group scheme $\mathcal{G}$, we denote

- $\mu\colon \mathcal{G} \times \mathcal{G} \to \mathcal{G}$, multiplication,
- $i\colon \mathcal{G} \to \mathcal{G}$, inversion,
- $e\colon \mathcal{E} \to \mathcal{G}$, unit (where $\mathcal{E} = \{e\}$ is the final object in the category of affine group schemes),
- $c\colon \mathcal{G} \to \mathcal{G}$, constant morphism, $c(g) = e$, (i.e. $c\colon \mathcal{G} \to \mathcal{E} \xrightarrow{e} \mathcal{G}$, where $\mathcal{G} \to \mathcal{E}$ is the unique morphism from $\mathcal{G}$ to $\mathcal{E}$),
- $\mathrm{id}\colon \mathcal{G} \to \mathcal{G}$, identity,

- $t\colon \mathcal{G}\times\mathcal{G}\to\mathcal{G}\times\mathcal{G}$, transposition, i.e. $t=(\mathrm{pr}_2,\mathrm{pr}_1)$.

We wish to define the commutator $u\colon \mathcal{G}\times\mathcal{G}\to\mathcal{G}$. Let $\tilde{\mu}\colon \mathcal{G}\times\mathcal{G}\times\mathcal{G}\times\mathcal{G}\to\mathcal{G}$ be the composition $(\mathcal{G}\times\mathcal{G})\times(\mathcal{G}\times\mathcal{G})\xrightarrow{\mu\times\mu}\mathcal{G}\times\mathcal{G}\xrightarrow{\mu}\mathcal{G}$. We then define u as the composite morphism $u\colon \mathcal{G}\times\mathcal{G}\xrightarrow{(i\times i,\mathrm{id}\times\mathrm{id})}\mathcal{G}\times\mathcal{G}\times\mathcal{G}\times\mathcal{G}\xrightarrow{\tilde{\mu}}\mathcal{G}$.

Observation. A group scheme $\mathcal{G}$ is commutative if and only if $u=c$.

Remark. Of course, one can express the commutativity condition without using commutators, just saying that $\mu\circ t=\mu$.

We now want to generalize the above construction. We define, by unduction,

$$\begin{array}{lcll} e_1 & = & u=[x,y]=x^{-1}y^{-1}xy, & \dots \\ e_{n+1} & = & [[e_n,x],[e_n,y]], & \dots \end{array} \tag{4}$$

More formally, we first define $e'_n=[e_n,x]$ and $e''_n=[e_n,y]$ as follows:

$$\begin{array}{lcllll} e'_n & : & \mathcal{G}\times\mathcal{G} & \xrightarrow{(e_n,\mathrm{pr}_1)} & \mathcal{G}\times\mathcal{G} & \xrightarrow{u} & \mathcal{G}, \\ e''_n & : & \mathcal{G}\times\mathcal{G} & \xrightarrow{(e_n,\mathrm{pr}_2)} & \mathcal{G}\times\mathcal{G} & \xrightarrow{u} & \mathcal{G}. \end{array} \tag{5}$$

Then e_{n+1} is defined as the composite morphism

$$e_{n+1}\colon \mathcal{G}\times\mathcal{G}\xrightarrow{(e'_n,e''_n)}\mathcal{G}\times\mathcal{G}\xrightarrow{u}\mathcal{G}.$$

The two other reasonable sequences (see formulae (2)–(3)) can be defined in a similar way.

Proposition 4.1 *Let $\mathcal{G}$ be a connected affine algebraic group over a field k. Then $\mathcal{G}$ is solvable if and only if $e_n=c$ for some $n\geq 1$.*

Proof. Necessity. We prove by induction that the image of e_n lies in the n-th derived subgroup $D^n\mathcal{G}$ of $\mathcal{G}$. For $n=1$ this is obvious. Since $D^n\mathcal{G}$ is a normal subgroup in $\mathcal{G}$, by induction hypothesis e'_n and e''_n each map $\mathcal{G}\times\mathcal{G}$ into $D^n\mathcal{G}$. Hence e_{n+1} maps $\mathcal{G}\times\mathcal{G}$ into $D^{n+1}\mathcal{G}$.

Sufficiency. First note that the condition $e_n=c$ is equivalent to the fact that all groups $\mathcal{G}(A)$, where A is any k-algebra, satisfy the identity $e_n(x,y)\equiv 1$. This property is thus hereditary with respect to sub- and factor-groups. Suppose that $\mathcal{G}$ satisfies $e_n=c$ but is not solvable. In view of the above remark, the quotient $\mathcal{G}^{\mathrm{red}}=\mathcal{G}/\mathcal{G}^{\mathrm{u}}$, where $\mathcal{G}^{\mathrm{u}}$ stands for the unipotent radical of $\mathcal{G}$, is a non-trivial reductive group satisfying $e_n=c$. Furthermore, its derived group $\mathcal{G}^{\mathrm{ss}}=[\mathcal{G}^{\mathrm{red}},\mathcal{G}^{\mathrm{red}}]$ is a non-trivial semisimple group satisfying the same property. Hence the k-group $\mathcal{SL}_2$ being a subgroup of $\mathcal{G}^{\mathrm{ss}}$ must satisfy the same law. Its quotient $\mathcal{PSL}_2$ thus also satisfies $e_n=c$. Therefore, the identity $e_n(x,y)\equiv 1$ must hold in all groups $\mathrm{PSL}_2(A)$ where A is a k-algebra, that is impossible [14]. □

We now go over to a "structural" analogue of the Engel law. Define $v_1=u$ and, by induction,

$$v_{n+1}\colon \mathcal{G}\times\mathcal{G}\xrightarrow{(v_n,\mathrm{pr}_2)}\mathcal{G}\times\mathcal{G}\xrightarrow{u}\mathcal{G}.$$

Proposition 4.2 *Let $\mathcal{G}$ be a connected affine algebraic group over a field k. Then $\mathcal{G}$ is nilpotent if and only if $v_n = c$ for some $n \geq 1$.*

Proof. Let $C^n\mathcal{G}$ denote the n-th term of the lower central series. Then v_n maps $\mathcal{G} \times \mathcal{G}$ into $C^n\mathcal{G}$. This proves the "only if" part. Let now $v_n = c$. Then, as in the proof of Proposition 4.1, we conclude that $\mathcal{G}$ is solvable. Hence $\overline{G} = \mathcal{G}(\bar{k})$ is solvable (here $\bar{k}$ stands for a (fixed) algebraic closure of k). According to [7, IV, 4.1.5], we only need to prove that $\overline{G}$ is nilpotent. Since $\overline{G}$ is solvable and connected, it is isomorphic to a semi-direct product $T \ltimes U$ where T is a torus and U is nilpotent. If $T = \{e\}$ or $U = \{e\}$ then $\overline{G}$ is nilpotent. Hence we may assume that $\dim T \geq 1$ and $\dim U \geq 1$. If T is central in $\overline{G}$ then $\overline{G}$ is nilpotent [3, 10.6(3)]. If not, U contains a one-dimensional subgroup U_1 that does not commute with T. Since $\bar{k}$ is algebraically closed, U_1 is isomorphic to the additive group $\mathbf{G}_{\mathrm{a}}$. Hence T acts on U_1 as follows: $t^{-1}ut = \lambda(t)u$ where $u \in U_1$, $t \in T$, $\lambda \colon T \to \mathbf{G}_{\mathrm{m}}$ is a character of T (cf. [3, 10.10]). Thus $t^{-1}u^{-1}t = \lambda^{-1}u^{-1}$ and $t^{-1}u^{-1}tu = \lambda^{-1}$, so $[u, t] = \lambda(t) \neq 1$ for $u \neq 1$, $t \neq 1$. By induction, we obtain $v_n(u, t) = \lambda \neq 1$ for any n, which is a contradiction. □

5 Main conjecture

In this section we return to Conjecture 2.9. Our first observation is that by standard arguments one can reduce to considering only a finite number of series of finite simple groups. To be more precise, one can easily derive Conjecture 2.9 from the following

Conjecture 5.1 *Let G be one of the following groups:*

1. $\mathrm{PSL}(2, p)$ $(p = 5 \text{ or } p \equiv \pm 2 \pmod 5, p \neq 3)$,
2. $\mathrm{PSL}(2, 2^p)$,
3. $\mathrm{PSL}(2, 3^p)$ $(p \text{ odd})$,
4. $\mathrm{Sz}(2^p)$ $(p \text{ odd})$,
5. $\mathrm{PSL}(3, 3)$.

Let $\{e_i\}$ be one of sequences (1)–(3). Then neither of identities $e_n \equiv 1$ holds in G.

Indeed, according to [28], the list of Conjecture 5.1 is exactly the list of minimal finite non-solvable groups (that is, the groups whose every subgroup is solvable). On our way to proving Conjecture 5.1, we proceed by case-by-case computer investigation. In order to prove that $e_n \equiv 1$ is not a law in G, it is enough to show that for some $k < l$ the equation $e_k(x, y) = e_l(x, y)$ has a non-trivial solution $(x_0, y_0) \in G \times G$ (non-trivial means that $e_k(x_0, y_0) = e_l(x_0, y_0) \neq 1$; by the construction of the sequences, it suffices to check that the right-hand side does not equal 1).

The case $G = \mathrm{PSL}(3,3)$ is the easiest one. Say, if the e_n's are taken from sequence (1), the matrices

$$x_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}, \qquad y_0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

give a solution to the equation $e_{17} = e_{21}$, and thus $e_n \equiv 1$ is not a law in $\mathrm{PSL}(3,3)$.

For $G = \mathrm{PSL}(2,p)$, computer search gives a solution to $e_2 = e_4$ (where the e_i's are taken from sequence (2)) for all $p < 1000$ except for $p = 293$ (as in chess, $e2 - e4$ usually wins!). The equation $e_3 = e_5$ has a solution in $\mathrm{PSL}(2,p)$ for all $p < 1000$, and this result remains true for all $p < 1500$ except, possibly, for $p = 1163$ for which calculations take too much time.

See Appendix for more details concerning numerical experiments.

To conclude, we present the following model case that can be viewed as a testing ground for proving Conjecture 5.1.

Proposition 5.2 *Let the sequence $\{e_i\}$ be given by formulae (1). If the identity $e_2 \equiv 1$ holds in a finite group G then G is solvable.*

Proof. As above, it is enough to prove that the identity $e_2 \equiv 1$ does not hold in the minimal non-solvable groups. For $G = \mathrm{PSL}(3,3)$ it is proved above. Let now $G = \mathrm{PSL}(2,q)$. Take

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

with $t \neq 0$. Then $e_2(x,y) = A(t)$ can be viewed as a polynomial matrix in indeterminate t. Its entry $A_{1,2}$ equals $-2t^3(t+1)f(t)$, where $f(t) = t^8 + t^7 - t^6 - 4t^5 - 8t^4 - 5t^3 + t^2 + 4t + 2$. Since $A_{1,2}(t)$ can only vanish at $t = 0$, $t = -1$, and at the roots of $f(t)$, we conclude that for odd $q \geq 11$ the identity $e_2 \equiv 1$ cannot hold in $\mathrm{PSL}(2,q)$. For $q = 5$ and $q = 7$ we have $A_{1,2}(1) \neq 0$. Thus we proved the proposition for $G = \mathrm{PSL}(2,p)$ and $G = \mathrm{PSL}(2,3^p)$.

Next consider the case $G = \mathrm{PSL}(2,2^p)$. Take

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} t & 1 \\ 1 & 0 \end{pmatrix}.$$

As above, we have $e_2(x,y) = B(t)$, a polynomial matrix in one variable t running over the finite field $\mathbb{F}_q$, $q = 2^p$, with $B_{1,2} = t(t^8+1)$. One can easily see that $B_{1,2}(t)$ cannot vanish at all $t \in \mathbb{F}_q$.

It only remains to consider the case of Suzuki groups $G = \mathrm{Sz}(q)$. We recall (see, for example, [13, Ch. XI, §3]) that as a subgroup of $\mathrm{GL}(4,q)$ the group G is generated by the following matrices:

$$S(\alpha,\beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha^z & 1 & 0 & 0 \\ \beta & \alpha & 1 & 0 \\ \alpha^{2z+1} + \alpha^z\beta + \beta^{2z} & \alpha^{1+z} + \beta & \alpha^z & 1 \end{pmatrix}, \qquad \alpha, \beta \in \mathbb{F}_q,$$

$$M(\zeta) = \begin{pmatrix} \zeta^z & 0 & 0 & 0 \\ 0 & \zeta^{1-z} & 0 & 0 \\ 0 & 0 & \zeta^{z-1} & 0 \\ 0 & 0 & 0 & \zeta^{-z} \end{pmatrix}, \qquad \zeta \in \mathbb{F}_q^*, \qquad \text{and } J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Here $z = 2^{\frac{p-1}{2}}$. We now take $x = J$, $y = S(1,t)$. As above, a straightforward computation (using MAPLE) gives $e_2(x,y)$ as a polynomial matrix $C(t)$. Its entry $C_{4,1}(t)$ equals $t^{2z}(t^z + 1)$. The number of roots of $t^z + 1$ in $\mathbb{F}_q$ does not exceed z which is strictly smaller than $q - 1$, and thus $C_{4,1}(t)$ cannot vanish at all $t \in \mathbb{F}_q$. □

Remark. Probably one can characterize neither finite nilpotent groups of a fixed class, nor finite solvable groups of a fixed derived length by means of two-variable identities. For example, there exists a non-metabelian solvable group G such that all its 2-generator subgroups are metabelian [16], [9].

Appendix

We present here some results of computer experiments. In Table 1 for each $p < 200$ we exhibit one solution (x, y) to the equation $e_2(x, y) = e_4(x, y)$ where the e_i's are taken from sequence (2). In the next two tables for $p < 80$ we present the number of solutions to the above equation for sequences (1), (2), respectively. Finally, we include the C++ code for the programs computing the number of solutions.

p	x	y	p	x	y
5	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-2 & -1\\ 1 & 0\end{pmatrix}$	7	$\begin{pmatrix}0 & -1\\ 1 & 3\end{pmatrix}$	$\begin{pmatrix}-3 & 2\\ -2 & 1\end{pmatrix}$
11	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-5 & -5\\ 0 & 2\end{pmatrix}$	13	$\begin{pmatrix}0 & -1\\ 1 & 6\end{pmatrix}$	$\begin{pmatrix}-5 & -5\\ -6 & -1\end{pmatrix}$
17	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-8 & -5\\ 3 & 6\end{pmatrix}$	19	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-9 & -8\\ 1 & 5\end{pmatrix}$
23	$\begin{pmatrix}0 & -1\\ 1 & 11\end{pmatrix}$	$\begin{pmatrix}-11 & -11\\ -10 & -8\end{pmatrix}$	29	$\begin{pmatrix}0 & -1\\ 1 & 5\end{pmatrix}$	$\begin{pmatrix}-14 & -13\\ -6 & 13\end{pmatrix}$
31	$\begin{pmatrix}0 & -1\\ 1 & 5\end{pmatrix}$	$\begin{pmatrix}-15 & -15\\ -2 & 0\end{pmatrix}$	37	$\begin{pmatrix}0 & -1\\ 1 & 3\end{pmatrix}$	$\begin{pmatrix}-18 & -12\\ 11 & -3\end{pmatrix}$
41	$\begin{pmatrix}0 & -1\\ 1 & 12\end{pmatrix}$	$\begin{pmatrix}-20 & -14\\ -3 & 4\end{pmatrix}$	43	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-21 & -20\\ 1 & 5\end{pmatrix}$
47	$\begin{pmatrix}0 & -1\\ 1 & 16\end{pmatrix}$	$\begin{pmatrix}-23 & -21\\ -20 & 4\end{pmatrix}$	53	$\begin{pmatrix}0 & -1\\ 1 & 19\end{pmatrix}$	$\begin{pmatrix}-26 & -24\\ -18 & 18\end{pmatrix}$
59	$\begin{pmatrix}0 & -1\\ 1 & 24\end{pmatrix}$	$\begin{pmatrix}-29 & -24\\ 23 & 19\end{pmatrix}$	61	$\begin{pmatrix}0 & -1\\ 1 & 29\end{pmatrix}$	$\begin{pmatrix}-30 & -28\\ -12 & 3\end{pmatrix}$
67	$\begin{pmatrix}0 & -1\\ 1 & 2\end{pmatrix}$	$\begin{pmatrix}-33 & -28\\ 17 & -12\end{pmatrix}$	71	$\begin{pmatrix}0 & -1\\ 1 & 34\end{pmatrix}$	$\begin{pmatrix}-35 & -32\\ -26 & 33\end{pmatrix}$
73	$\begin{pmatrix}0 & -1\\ 1 & 22\end{pmatrix}$	$\begin{pmatrix}-36 & -36\\ 12 & 14\end{pmatrix}$	79	$\begin{pmatrix}0 & -1\\ 1 & 29\end{pmatrix}$	$\begin{pmatrix}-39 & -39\\ 36 & 38\end{pmatrix}$
83	$\begin{pmatrix}0 & -1\\ 1 & 34\end{pmatrix}$	$\begin{pmatrix}-41 & -35\\ -40 & -20\end{pmatrix}$	89	$\begin{pmatrix}0 & -1\\ 1 & 39\end{pmatrix}$	$\begin{pmatrix}-44 & -44\\ 38 & 40\end{pmatrix}$
97	$\begin{pmatrix}0 & -1\\ 1 & 13\end{pmatrix}$	$\begin{pmatrix}-48 & -45\\ -3 & -19\end{pmatrix}$	101	$\begin{pmatrix}0 & -1\\ 1 & 45\end{pmatrix}$	$\begin{pmatrix}-50 & -45\\ -17 & 17\end{pmatrix}$
103	$\begin{pmatrix}0 & -1\\ 1 & 19\end{pmatrix}$	$\begin{pmatrix}-51 & -44\\ 8 & 19\end{pmatrix}$	107	$\begin{pmatrix}0 & -1\\ 1 & 47\end{pmatrix}$	$\begin{pmatrix}-53 & -31\\ -1 & -43\end{pmatrix}$
109	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-54 & -49\\ 5 & -52\end{pmatrix}$	113	$\begin{pmatrix}0 & -1\\ 1 & 47\end{pmatrix}$	$\begin{pmatrix}-56 & -56\\ -11 & -9\end{pmatrix}$
127	$\begin{pmatrix}0 & -1\\ 1 & 8\end{pmatrix}$	$\begin{pmatrix}-63 & -55\\ -11 & -58\end{pmatrix}$	131	$\begin{pmatrix}0 & -1\\ 1 & 11\end{pmatrix}$	$\begin{pmatrix}-65 & -58\\ 13 & -65\end{pmatrix}$
137	$\begin{pmatrix}0 & -1\\ 1 & 11\end{pmatrix}$	$\begin{pmatrix}-68 & -54\\ -59 & -65\end{pmatrix}$	139	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-69 & -68\\ 1 & 5\end{pmatrix}$
149	$\begin{pmatrix}0 & -1\\ 1 & 40\end{pmatrix}$	$\begin{pmatrix}-74 & -69\\ 20 & 73\end{pmatrix}$	151	$\begin{pmatrix}0 & -1\\ 1 & 64\end{pmatrix}$	$\begin{pmatrix}-75 & -73\\ -21 & 48\end{pmatrix}$
157	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-78 & -68\\ 10 & 55\end{pmatrix}$	163	$\begin{pmatrix}0 & -1\\ 1 & 58\end{pmatrix}$	$\begin{pmatrix}-81 & -30\\ -59 & -44\end{pmatrix}$
167	$\begin{pmatrix}0 & -1\\ 1 & 14\end{pmatrix}$	$\begin{pmatrix}-83 & -76\\ -83 & -74\end{pmatrix}$	173	$\begin{pmatrix}0 & -1\\ 1 & 37\end{pmatrix}$	$\begin{pmatrix}-86 & -63\\ -23 & -41\end{pmatrix}$
179	$\begin{pmatrix}0 & -1\\ 1 & 53\end{pmatrix}$	$\begin{pmatrix}-89 & -88\\ -59 & 4\end{pmatrix}$	181	$\begin{pmatrix}0 & -1\\ 1 & 49\end{pmatrix}$	$\begin{pmatrix}-90 & -86\\ -20 & 3\end{pmatrix}$
191	$\begin{pmatrix}0 & -1\\ 1 & 88\end{pmatrix}$	$\begin{pmatrix}-95 & -85\\ -41 & -95\end{pmatrix}$	193	$\begin{pmatrix}0 & -1\\ 1 & 84\end{pmatrix}$	$\begin{pmatrix}-96 & -94\\ -62 & 78\end{pmatrix}$
197	$\begin{pmatrix}0 & -1\\ 1 & 24\end{pmatrix}$	$\begin{pmatrix}-98 & -86\\ -20 & 93\end{pmatrix}$	199	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}-99 & -95\\ 4 & 38\end{pmatrix}$

TABLE 1: Solutions to $e_2 = e_4$ (formulae (1))

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
N_1	0	84	96	300	668	80	88	360	760	440	664	848	1312	428	712	480	1616	1432	1168	1904

TABLE 2: Numbers of solutions to $e_2 = e_4$ (formulae (1))

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
N_2	22	16	134	28	36	304	136	526	670	296	990	590	760	428	1064	728	402	1136	584	2050

TABLE 3: Numbers of solutions to $e_2 = e_4$ (formulae (2))

```
//#==============================================================#
//#                                                              #
//#       The sequence U1 = [X,Y]; Un+1 = [[Un,X],[Un,Y]]        #
//#                                                              #
//#                X = ||0 -1||  Y = ||a b||                     #
//#                    ||1  t||      ||c d||                     #
//#                                                              #
//#==============================================================#

//#==============================================================#
//#                                                              #
//# The program computes the number of the solutions for U2= U4  #
//#                                                   or U2=-U4  #
//#               for given prime p                              #
//#                                                              #
//#==============================================================#


#include <stdio.h>
#include <math.h>
#include <stdlib.h>

//***************************************************
void display(long data[][2]);
void multiply(long X[2][2],long Y[2][2],int p);
void inv_X(long X[2][2]);
void inv_Y(long Y[2][2]);
void U_2(long X[2][2],long Y[2][2],int p);
void U_3(long X[2][2],long Y[2][2],int p);
void U_4(long X[2][2],long Y[2][2],int p);
void minus_U_4();
void Commutator(long X[2][2],long Y[2][2],int p);
int find_number_of_solutions(int p);
bool equal(long X[2][2],long Y[2][2],int p);


//*****************************************************
//Global variables
static long C[2][2];
static long U2[2][2];
static long U4[2][2];
static long minus_U4[2][2];
static long U3[2][2];
static long M[2][2];
static long InvX[2][2];
static long InvY[2][2];
static long tmp1[2][2];
static long tmp2[2][2];
static long tmp[2][2];
static long temp1[2][2];
static long temp2[2][2];
FILE *output;
//*****************************************************

int main(void)   {
int p ;

output = fopen("numbers.txt", "a+");
fclose(output);
printf("Enter the prime number P: ");
scanf("%d",&p);
printf("\n");
output = fopen("numbers.txt", "a+");
fprintf(output, "======");
fprintf(output, "P = ");
fprintf(output, "%d", p," ");
fprintf(output,"\n ");
fprintf(output, "The number of solutions is: ");
fprintf(output, "%d", find_number_of_solutions(p)," ");
fprintf(output, "======");
fprintf(output,"\n ");
```

```
fclose(output);
 return(0);
}
//******************************************************************************
void display(long data[2][2]) {
output = fopen("numbers.txt", "a+");
   fprintf(output, " \n*********************************\n");
   for (int i = 0; i < 2; i++) {
        for (int j = 0; j < 2; j++)
        {
             fprintf(output, "%d", data[i][j]);
             fprintf(output, " ");
          }
             fprintf(output, " \n");

       }
       fprintf(output, " \n*********************************\n");
       fclose(output);
   }
//*******************************************************************************

void multiply(long X[2][2],long Y[2][2],int p)
{
 M[0][0] = (X[0][0]*Y[0][0]+X[0][1]*Y[1][0])%p;
 M[0][1] = (X[0][0]*Y[0][1]+X[0][1]*Y[1][1])%p;
 M[1][0] = (X[1][0]*Y[0][0]+X[1][1]*Y[1][0])%p;
 M[1][1] = (X[1][0]*Y[0][1]+X[1][1]*Y[1][1])%p;

}
//***************************************************

 void inv_X(long X[2][2])
 {
  InvX[0][0] =  X[1][1];
  InvX[0][1] = -X[0][1];
  InvX[1][0] = -X[1][0];
  InvX[1][1] =  X[0][0];
  }

  void inv_Y(long Y[2][2])
 {
  InvY[0][0] =  Y[1][1];
  InvY[0][1] = -Y[0][1];
  InvY[1][0] = -Y[1][0];
  InvY[1][1] =  Y[0][0];
  }
//******************************************************************************
  void Commutator(long X[2][2],long Y[2][2],int p)
  {
   inv_X(X);
   inv_Y(Y);
   multiply(InvX,InvY,p);
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
       temp1[i][j]=M[i][j];
   multiply(temp1,X,p);
   for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
       temp2[i][j]=M[i][j];
   multiply(temp2,Y,p);
   for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
     {
      C[i][j]=M[i][j];
      M[i][j]=0;
     }
   }

//*****************************************************************************
  void U_2(long X[2][2],long Y[2][2],int p)
  {
   Commutator(X,Y,p);
    for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp[i][j]=C[i][j];
   Commutator(tmp,X,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp1[i][j]=C[i][j];
   Commutator(tmp,Y,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp2[i][j]=C[i][j];
     Commutator(tmp1,tmp2,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
```

```
      U2[i][j]=C[i][j];
    }

  void U_3(long X[2][2],long Y[2][2],int p)
  {
   Commutator(U2,X,p);
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp1[i][j]=C[i][j];
   Commutator(U2,Y,p);
   for(i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp2[i][j]=C[i][j];

   Commutator(tmp1,tmp2,p);
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      U3[i][j]=C[i][j];
 }

void U_4(long X[2][2],long Y[2][2],int p)
  {
   Commutator(U3,X,p);
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp1[i][j]=C[i][j];
   Commutator(U3,Y,p);
   for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp2[i][j]=C[i][j];

   Commutator(tmp1,tmp2,p);
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      U4[i][j]=C[i][j];
 }

void minus_U_4()
{
 for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      minus_U4[i][j]=-U4[i][j];
}
```

```
//******************************************************************************
bool equal(long X[2][2],long Y[2][2],int p)
{
 if((((X[0][0]-Y[0][0])%p)==0)&&
    (((X[0][1]-Y[0][1])%p)==0)&&
    (((X[1][0]-Y[1][0])%p)==0)&&
    (((X[1][1]-Y[1][1])%p)==0))
    return(true);
  else
    return(false);
}

//******************************************************************************

int find_number_of_solutions(int p)
{
 static long E[2][2];
 E[0][0]=1;
 E[0][1]=0;
 E[1][0]=0;
 E[1][1]=1;
 static long X[2][2];
 static long Y[2][2];
 int counter =0;

 for(int i=(1-p)/2;i<=(p-1)/2;i++)
    for(int j=(1-p)/2;j<=(p-1)/2;j++)
for(int m=(1-p)/2;m<=(p-1)/2;m++)
for(int n=(1-p)/2;n<=(p-1)/2;n++)
for(int k=(1-p)/2;k<=(p-1)/2;k++)
            {
if (((i*n-j*m-1)%p)==0)
               {
                X[0][0]=0;
                X[0][1]=-1;
                X[1][0]=1;
                X[1][1]=k;

                Y[0][0]=i;
                Y[0][1]=j;
                Y[1][0]=m;
                Y[1][1]=n;
                U_2(X,Y,p);
                U_3(X,Y,p);
                U_4(X,Y,p);
        minus_U_4();


  if((!equal(U3,E,p))&&
  ((equal(U2,U4,p))||
                           (equal(U2,minus_U4,p))))
{
                        counter=counter+1;

                    }
                   }
                }
return(counter);
}
```

Figure 1: Program for computing the number of solutions to $e_2 = e_4$ (formulae (1))

```
//#===============================================================#
//#                                                               #
//#    The sequence U1 = [X,Y]; Un+1 = [ X^-1*Un*X,Y^-1*Un*Y ]    #
//#                                                               #
//#                X = ||0 -1||  Y = ||a b||                      #
//#                    ||1  t||      ||c d||                      #
//#                                                               #
//#===============================================================#


//#===============================================================#
//#                                                               #
//# The program computes the number of the solutions for U2= U4   #
//#                                                   or U2=-U4   #
//#               for given prime p                               #
//#                                                               #
//#===============================================================#


#include <stdio.h>
#include <math.h>
```

```
#include <stdlib.h>

//***************************************************
void display(long  data[][2]);
void multiply(long  X[2][2],long  Y[2][2],int p);
void inv_X(long  X[2][2]);
void inv_Y(long  Y[2][2]);
void U_2(long  X[2][2],long  Y[2][2],int p);
void U_3(long  X[2][2],long  Y[2][2],int p);
void U_4(long  X[2][2],long  Y[2][2],int p);
void minus_U_4();
void Commutator(long  X[2][2],long  Y[2][2],int p);
int find_number_of_solutions(int p);
bool equal(long  X[2][2],long  Y[2][2],int p);


//***************************************************
//Global variables
static long  C[2][2];
static long  U2[2][2];
static long  U4[2][2];
static long  U3[2][2];
static long  minus_U4[2][2];
static long  M[2][2];
static long  InvX[2][2];
static long  InvY[2][2];
static long  tmp1[2][2];
static long  tmp2[2][2];
static long  tmp3[2][2];
static long  tmp4[2][2];
static long  tmp[2][2];
static long  temp1[2][2];
static long  temp2[2][2];
FILE *output;
//***************************************************

int main(void)   {
int p ;

output = fopen("numbers1.txt", "a+");
fclose(output);
printf("Enter the prime number P: ");
scanf("%d",&p);
```

```
printf("\n");
output = fopen("numbers1.txt", "a+");
fprintf(output, "======");
fprintf(output, "P = ");
fprintf(output, "%d", p," ");
fprintf(output,"\n ");
fprintf(output, "The number of solutions is: ");
fprintf(output, "%d", find_number_of_solutions(p)," ");
fprintf(output, "======");
fprintf(output,"\n ");
fclose(output);
 return(0);
}
//******************************************************************************
void display(long  data[2][2]) {
output = fopen("numbers1.txt", "a+");
   fprintf(output, " \n********************************\n");
   for (int i = 0; i < 2; i++) {
        for (int j = 0; j < 2; j++)
        {
             fprintf(output, "%d", data[i][j]);
             fprintf(output, " ");
          }
             fprintf(output, " \n");

       }
       fprintf(output, " \n********************************\n");
       fclose(output);
   }
//*******************************************************************************

void multiply(long  X[2][2],long  Y[2][2], int p)
{
 M[0][0] = (X[0][0]*Y[0][0]+X[0][1]*Y[1][0])%p;
 M[0][1] = (X[0][0]*Y[0][1]+X[0][1]*Y[1][1])%p;
 M[1][0] = (X[1][0]*Y[0][0]+X[1][1]*Y[1][0])%p;
 M[1][1] = (X[1][0]*Y[0][1]+X[1][1]*Y[1][1])%p;

}
//****************************************************

 void inv_X(long  X[2][2])
 {
  InvX[0][0] =  X[1][1];
  InvX[0][1] = -X[0][1];
  InvX[1][0] = -X[1][0];
  InvX[1][1] =  X[0][0];
  }

  void inv_Y(long  Y[2][2])
 {
  InvY[0][0] =  Y[1][1];
  InvY[0][1] = -Y[0][1];
  InvY[1][0] = -Y[1][0];
  InvY[1][1] =  Y[0][0];
  }
//******************************************************************************
  void Commutator(long  X[2][2],long  Y[2][2],int p)
  {
   //static int temp[2][2];
   //static long  temp1[2][2];
   //static long  temp2[2][2];
   inv_X(X);
   inv_Y(Y);
   multiply(InvX,InvY,p);
   for( int i=0;i<2;i++)
     for(int j=0;j<2;j++)
       temp1[i][j]=M[i][j];
   multiply(temp1,X,p);
   for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
       temp2[i][j]=M[i][j];
   multiply(temp2,Y,p);
   for(i=0;i<2;i++)
     for(int j=0;j<2;j++)
     {
      C[i][j]=M[i][j];
      M[i][j]=0;
     }
   }

//*****************************************************************************
  void U_2(long  X[2][2],long  Y[2][2],int p)
  {
   Commutator(X,Y,p);
    for(int i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp[i][j]=C[i][j];
 multiply(InvX,tmp,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp1[i][j]=M[i][j];
 multiply(tmp1,X,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp2[i][j]=M[i][j];

  multiply(InvY,tmp,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp3[i][j]=M[i][j];
 multiply(tmp3,Y,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp4[i][j]=M[i][j];
  Commutator(tmp2,tmp4,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    U2[i][j]=C[i][j];
  }

void U_3(long  X[2][2],long  Y[2][2],int p)
{
 inv_X(X);
 inv_Y(Y);
 multiply(InvX,U2,p);
  for(int i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp1[i][j]=M[i][j];
 multiply(tmp1,X,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp2[i][j]=M[i][j];

  multiply(InvY,U2,p);
  for( i=0;i<2;i++)
   for(int j=0;j<2;j++)
    tmp3[i][j]=M[i][j];
 multiply(tmp3,Y,p);
```

```
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp4[i][j]=M[i][j];
    Commutator(tmp2,tmp4,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      U3[i][j]=C[i][j];
 }

void U_4(long  X[2][2],long  Y[2][2],int p)
  {
   inv_X(X);
   inv_Y(Y);
   multiply(InvX,U3,p);
    for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp1[i][j]=M[i][j];
   multiply(tmp1,X,p);
    for(i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp2[i][j]=M[i][j];

    multiply(InvY,U3,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp3[i][j]=M[i][j];
   multiply(tmp3,Y,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      tmp4[i][j]=M[i][j];
    Commutator(tmp2,tmp4,p);
    for( i=0;i<2;i++)
     for(int j=0;j<2;j++)
      U4[i][j]=C[i][j];
 }

 void minus_U_4()
  {
   for(int i=0;i<2;i++)
     for(int j=0;j<2;j++)
      minus_U4[i][j]=-U4[i][j];
 }
//******************************************************************************
```

```
bool equal(long  X[2][2],long  Y[2][2],int p)
{
 if((((X[0][0]-Y[0][0])%p)==0)&&
    (((X[0][1]-Y[0][1])%p)==0)&&
    (((X[1][0]-Y[1][0])%p)==0)&&
    (((X[1][1]-Y[1][1])%p)==0))
    return(true);
  else
    return(false);
}

//********************************************************************************

int find_number_of_solutions(int p)
{
 static long E[2][2];
 E[0][0]=1;
 E[0][1]=0;
 E[1][0]=0;
 E[1][1]=1;
 static long minus_E[2][2];
 minus_E[0][0]=-1;
 minus_E[0][1]=0;
 minus_E[1][0]=0;
 minus_E[1][1]=-1;
 static long  X[2][2];
 static long  Y[2][2];
 int counter=0;

 for(int i=(1-p)/2;i<=(p-1)/2;i++)
    for(int j=(1-p)/2;j<=(p-1)/2;j++)
for(int m=(1-p)/2;m<=(p-1)/2;m++)
for(int n=(1-p)/2;n<=(p-1)/2;n++)
for(int k=1;k<=(p-1)/2;k++)
            {
if (((i*n-j*m-1)%p)==0)
               {
                X[0][0]=0;
                X[0][1]=-1;
                X[1][0]=1;
                X[1][1]=k;

                Y[0][0]=i;
                Y[0][1]=j;
                Y[1][0]=m;
                Y[1][1]=n;

                U_2(X,Y,p);
                U_3(X,Y,p);
                U_4(X,Y,p);
                minus_U_4();

  if(((!equal(U4,E,p))&&(!equal(U4,minus_E,p)))&&
  ((equal(U2,U4,p))||
                     (equal(U2,minus_U4,p))))
{
                        counter=counter+1;

                    }
                   }
                }
return(counter);

}
```

FIGURE 2: Program for computing the number of solutions to $e_2 = e_4$ (formulae (2))

References

[1] R. E. Block, *Determination of differentially simple rings with a minimal ideal*, Ann. of Math. (2) **90** (1969), 433–459.

[2] R. E. Block and R. L. Wilson, *Classification of the restricted simple Lie algebras*, J. Algebra **114** (1988), 115–259.

[3] A. Borel, *Linear Algebraic Groups*, 2nd ed., Springer-Verlag, Berlin et al., 1991.

[4] R. Brandl, *On groups with small Engel depth*, Bull. Austral. Math. Soc. **28** (1983), 101–110.

[5] R. Brandl and D. Nikolova, *Simple groups of small Engel depth*, Bull. Austral. Math. Soc. **33** (1986), 245–251.

[6] J. Cossey, S. Oates Macdonald, and A. P. Street, *On the laws of certain finite groups*, J. Austral. Math. Soc. **11** (1970), 441–489.

[7] M. Demazure and P. Gabriel, *Groupes Algébriques*, Masson, Paris & North-Holland, Amsterdam, 1970.

[8] P. Flavell, *Finite groups in which every two elements generate a soluble group*, Invent. Math. **121** (1995), 279–285.

[9] C. K. Gupta, 2-*metabelian groups*, Arch. Math. (Basel) **19** (1968), 584–587.

[10] N. D. Gupta, *Some group laws equivalent to the commutative law*, Arch. Math. (Basel) **17** (1966), 97–102.

[11] N. D. Gupta and H. Heineken, *Groups with a two-variable commutator identity*, Math. Z. **95** (1967), 276–287.

[12] H. Heineken and P. Neumann, *Identical relations and decision procedures for groups*, J. Austral. Math. Soc. **7** (1967), 39–47.

[13] B. Huppert and N. Blackburn, *Finite Groups* III, Springer-Verlag, Berlin et al., 1982.

[14] G. A. Jones, *Varieties and simple groups*, J. Austral. Math. Soc. **17** (1974), 163–173.

[15] S. Lang, *Algebra*, 3rd ed., Addison-Wesley, 1993.

[16] B. H. Neumann, *On a conjecture of Hanna Neumann*, Proc. Glasgoq Math. Assoc. **3** (1956), 13–17.

[17] H. Neumann, *Varieties of Groups*, Springer-Verlag, Berlin et al., 1967.

[18] D. Nikolova, *Groups with a 2-variable commutator identity*, Ph. D. thesis, Sofia Univ., 1983.

[19] D. Nikolova, *Groups with a two-variable commutator identity*, C. R. Acad. Bulgare Sci. **36** (1983), 721–724.

[20] D. Nikolova, *Solubility of finite groups with a two-variable commutator identity*, Serdica **11** (1985), 59–63.

[21] S. Oates and M. B. Powell, *Identical relations in finite groups*, J. of Algebra **1** (1964), 11–39.

[22] V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory*, Nauka, Moscow, 1991; English transl., Academic Press, Boston et al., 1994.

[23] B. Plotkin, E. Plotkin, and A. Tsurkov, *Geometrical equivalence of groups*, Comm. Algebra **27** (1999), 4015–4025.

[24] A. Potapchik and A. Rapinchuk, *Normal subgroups of* $\mathrm{SL}_{1,D}$ *and the classification of finite simple groups*, Proc. Indian Acad. Sci. (Math. Sci.) **106** (1996), 329–368.

[25] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra*, Ann. of Math. (2) **149** (1999), 219–251.

[26] Y. Segev and G. Seitz, *Anisotropic groups of type A_n and the commuting graph of finite simple groups*, to appear.

[27] H. Strade and R. Farnsteiner, *Modular Lie Algebras and Their Representations*, Marcel Dekker, New York–Basel, 1988.

[28] J. Thompson, *Non-solvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968), 383–437.

[29] B. Weisfeiler, *On subalgebras of simple Lie algebras of characteristic $p > 0$*, Trans. Amer. Math. Soc. **286** (1984), 471–503.