Astérisque

YAKOV BERKOVICH

Non-solvable groups with a large fraction of involutions

Astérisque, tome 258 (1999), p. 241-248

<http://www.numdam.org/item?id=AST_1999__258__241_0>

Astérisque **258**, 1999, p. 241–248

NON-SOLVABLE GROUPS WITH A LARGE FRACTION OF INVOLUTIONS

by

Yakov Berkovich

Abstract. — In this note we classify the non-solvable finite groups G such that the class number of G is at least $|G|/16$. Some consequences are derived as well.

C.T.C. Wall classified all finite groups in which the fraction of involutions exceeds 1/2 (see [**1**], Theorem 11.24). In this paper we classify all non-solvable finite groups in which the fraction of involutions is not less than 1/4.

We recall some notation.

Let $k(G)$ be the class number of G. Let $i(G)$ denote the number of all involutions of G, $T(G) = \sum \chi(1)$ where χ runs over the set $\mathrm{Irr}(G)$. Now

$$\mathrm{mc}(G) = k(G)/|G|, \ f(G) = T(G)/|G|, \ i_o(G) = i(G)/|G|.$$

It is well-known (see [**1**], chapter 11) that

$$i(G) < T(G), \ i_o(G) < f(G), \ f(G)^2 \leq \mathrm{mc}(G)$$

(with equality if and only if G is abelian).

In this note we prove the following three theorems.

Theorem 1. — *Let G be a non-solvable group.*

If $mc(G) \geq 1/16$ then $G = G'Z(G)$, where G' is the commutator subgroup of G, $Z(G)$ is the centre of G, $G' \in \{PSL(2,5), SL(2,5)\}$.

Theorem 2. — *Let G be a non-solvable group.*

If $f(G) \geq 1/4$ then $G = G'Z(G)$ and $G' \in \{PSL(2,5), SL(2,5)\}$.

Theorem 3. — *Let G be a non-solvable group.*

Then $i_o(G) \geq 1/4$ if and only if $G = PSL(2,5) \times E$ with $\exp E \leq 2$.

Lemma 1 contains some well-known results.

Lemma 1

(a) If G is simple and a non-linear $\chi \in Irr(G)$ is such that $\chi(1) < 4$, then $\chi(1) = 3$ and $G \in \{PSL(2,5), PSL(2,7)\}$; see [2].

1991 ***Mathematics Subject Classification.*** — Primary 20C15, 20D05, 20E34.
Key words and phrases. — Non-solvable finite groups, class number.

(b) (Isaacs; see **[1]***, Theorem 14.19). If* G *is non-solvable, then* $|cdG| \geq 4$*; here* $cdG = \{\chi(1) | \chi \in Irr(G)\}$.

(c) (see, for example, **[1]***, Chapter 11). If* G *is non-abelian then*

$$mc(G) \leq 5/8, \; f(G) \leq 3/4.$$

Lemma 2. — *Let* $G = G' > 1$, $d \in \{4,5,6\}$. *If* $mc(G) \geq (1/d)^2$ *then there exists a non-linear* $\chi \in Irr(G)$ *such that* $\chi(1) < d$.

Proof. — Suppose that G is a counterexample. Then by virtue of Lemma 1(b) one has

$$\begin{aligned} |G| &= \textstyle\sum_\chi \chi(1)^2 \geq 1 + d^2(k(G)-3) + (d+1)^2 + (d+2)^2 \\ &\geq 1 + d^2(\tfrac{|G|}{d^2} - 3) + 2d^2 + 6d + 5 = |G| - d^2 + 6d + 6 > |G| \end{aligned}$$

since $d \in \{4,5,6\}$, — a contradiction (here χ runs over the set $\mathrm{Irr}(G)$).

Lemma 3 contains the complete classification of all groups G satisfying $i_o(G) = 1/4$.

Lemma 3. — *If* $i_o(G) = 1/4$ *then one and only one of the following assertions holds:*

(a) $G \cong A_4$*, the alternating group of degree* 4.

(b) $G \cong PSL(2,5)$.

(c) G *is a Frobenius group with kernel of index* 4.

(d) G *is a non-cyclic abelian group of order* 12.

(e) G *contains a normal subgroup* R *of order* 3 *such that* $G/R \cong S_3 \times S_3$*; if* x *is an involution in* G *then* $|C_G(x)| = 12$ *(here* S_3 *is the symmetric group of degree* 3*).*

Proof. — By the assumption $|G|$ is even. $i(G)$ is therefore odd by the Sylow Theorem and $|G| = 4i(G)$, $P \in \mathrm{Syl}_2(G)$ has order 4.

(i) Suppose that G has no a normal 2-complement. Then P is abelian of type $(2,2)$ and by the Frobenius normal p-complement Theorem G contains a minimal non-nilpotent subgroup $F = C(3^a) \cdot P$ (here $C(m)$ is a cyclic group of order m and $A \cdot B$ is a semi-direct product of A and B with kernel B). Since all involutions are conjugate in F, all involutions are conjugate in G. Hence $C_G(x) = P$ for $x \in P^\# = P - \{1\}$, $a = 1$. If G is simple then by the Brauer-Suzuki-Wall Theorem (see **[1]**, Theorem 5.20) one has

$$|G| = (2^2 - 1)2^2(2^2 + 1) = 60.$$

Now we assume that G is not simple. Take H, a non-trivial normal subgroup of G. If $|G : H|$ is odd, then

$$\begin{aligned} i(G) = i(H),\; i_o(H) = i(H)/|H| = i(G)/|H| = \\ |G| i_o(G)/|H| = |G : H| i_o(G) = |G : H|/4. \end{aligned}$$

Therefore $|G : H| = 3$ and $i_o(H) = 3/4$. Now $f(H) > i_o(H)$, hence H is abelian (Lemma 1(c)) and $f(H) = 1$. It is easy to see that H is an elementary abelian 2-group, $H = P$. Now $|P| = 4$ implies $|G| = 12$, $F = G \cong A_4$.

Now suppose that H has even index. Since G is not 2-nilpotent (= has no a normal 2-complement) then $|H|$ is odd. In view of $|C_G(x)| = 4$ for $x \in P^\#$ one obtains that PH is a Frobenius group with kernel H, P is cyclic — a contradiction.

(ii) G has a normal 2-complement K.

First assume that P is cyclic. Then all involutions are conjugate in G, and for the involution $x \in P$ one has $C_G(x) = P$. Then G is a Frobenius group with kernel K of index 4.

Assume that $P = \langle\alpha\rangle \times \langle\beta\rangle$ is not cyclic. We have $P = \{1, \alpha, \beta, \alpha\beta\}$, and all elements from $P^{\#}$ are not pairwise conjugate in G. Thus

$$|G : C_G(\alpha)| + |G : C_G(\beta)| + |G : C_G(\alpha\beta)| = i(G) = |G : P|.$$

Note that $C_G(\alpha) = P \cdot C_K(\alpha)$, and similarly for β and $\alpha\beta$. Therefore

$$(1) \qquad |C_K(\alpha)|^{-1} + |C_K(\beta)|^{-1} + |C_K(\alpha\beta)|^{-1} = 1.$$

Since $|K| > 1$ is odd then (1) implies

$$(2) \qquad |C_K(\alpha)| = |C_K(\beta)| = |C_K(\alpha\beta)| = 3.$$

By the Brauer Formula (see **[1]**, Theorem 15.47) one has

$$(3) \qquad |K||C_K(P)|^2 = |C_K(\alpha)||C_K(\beta)||C_K(\alpha\beta)| = 3^3.$$

If $C_K(P) > 1$ then (3) implies $|K| = 3$ and $G = P \times K$ is an abelian non-cyclic group of order 12.

Assume $C_K(P) = 1$. Then $|K| = 3^3$. Now (2) implies that K is not cyclic. By analogy, (2) implies that $\exp K = 3$. From $\exp P = 2$ follows that G is supersolvable. Therefore R, a minimal normal subgroup of G, has order 3. Applying the Brauer Formula to G/R, one obtains $G/R \cong S_3 \times S_3$, and we obtain group (e).

Proof of Theorem 1. — Denote by $S = S(G)$ the maximal normal solvable subgroup of G.

(i) If G is non-abelian simple then $G \cong \mathrm{PSL}(2,5)$.

Proof. — Take $d = 4$ in Lemma 2. Then there exists $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = 3$. Now Lemma 1(a) implies $G \in \{\mathrm{PSL}(2,5), \mathrm{PSL}(2,7)\}$. Since

$$\mathrm{mc}(\mathrm{PSL}(2,7)) = 1/28 < 1/16$$

then $G \cong \mathrm{PSL}(2,5)$ (note that $\mathrm{mc}(\mathrm{PSL}(2,5)) = 1/12$).

(ii) If G is semi-simple then $G \cong \mathrm{PSL}(2,5)$.

Proof. — Take in G a minimal normal subgroup D. Then $D = D_1 \times \cdots \times D_s$ where the D_i's are isomorphic non-abelian simple groups. Since (see **[1]**, Chapter 11) $\mathrm{mc}(D_1) \geq \mathrm{mc}(G) \geq 1/16$, $D \cong \mathrm{PSL}(2,5)$ by (i) and so $\mathrm{mc}(D_1) = 1/12$. Now

$$\mathrm{mc}(D) = \mathrm{mc}(D_1)^s = (1/12)^s \geq 1/16$$

implies that $s = 1$. Therefore $D \cong \mathrm{PSL}(2,5)$. Since $G/C_G(D)$ is isomorphic to a subgroup of $\mathrm{Aut}D \cong S_5$, $\mathrm{mc}(S_5) = 7/120 < 1/16$, then $G/C_G(D) \cong \mathrm{PSL}(2,5)$. Because $D \cap C_G(D) = 1$, $G = D \times C_G(D)$. Now

$$1/16 \leq \mathrm{mc}(G) = \mathrm{mc}(C_G(D))\mathrm{mc}(D) = (1/12)\mathrm{mc}(C_G(D))$$

implies that $\mathrm{mc}(C_G(D)) \geq 3/4 > 5/8$, $C_G(D)$ is abelian (Lemma 1(c)), $C_G(D) = 1$ (since G is semi-simple), and $G \cong \mathrm{PSL}(2,5)$.

(iii) $G/S \cong \mathrm{PSL}(2,5)$.

This follows from $\mathrm{mc}(G/S) \geq \mathrm{mc}(G)$ (P.Gallagher; see [1], Theorem 7.46) and (ii).

(iv) If $G = G'$ then $G \in \mathrm{PSL}(2,5), \mathrm{SL}(2,5)\}$.

Proof. — By virtue of (iii) we may assume that $S > 1$.

Suppose that (iv) is true for all proper epimorphic images of G. Take in S a minimal normal subgroup R of G, and put $|R| = p^n$. Then by the Gallagher Theorem and induction one has $G/R \in \{PSL(2,5), \mathrm{SL}(2,5)\}$.

(1iv) $G/R \cong \mathrm{PSL}(2,5)$, i.e. $R = S$.

If $Z(G) > 1$ then $R = Z(G)$ is isomorphic to a subgroup of the Schur multiplier of G/R so $|R| = 2$ and $G \cong \mathrm{SL}(2,5)$ (Schur). In the sequel we suppose that $Z(G) = 1$.

Then $C_G(R) = R$, so $n > 1$. If $x \in R^\#$ then $|G : C_G(x)| \geq 5$, since index of any proper subgroup of $\mathrm{PSL}(2,5)$ is at least 5. Let $k_G(M)$ denote the number of conjugacy classes of G ($= G$-classes), containing elements from M. Then

$$k_G(R) \leq 1 + |R^\#|/5 = (p^n + 4)/5.$$

If $x \in G - R$ then $Z(G) = 1$, and the structure of G/R imply $|G : C_G(x)| \geq 12p$ (indeed, x does not centralize R and $|G/R : C_{G/R}(xR)| \geq 12$). Hence

$$k_G(G-R) = k(G) - k_G(R) = |G|\mathrm{mc}(G) - k_G(R) \geq \\ 60p^n/16 - (p^n+4)/5 = (71p^n - 16)/20.$$

Now

$$(1) \qquad |G - R| = 59p^n \geq 12pk_G(G-R) \geq 12p(71p^n - 16)/20,$$

$$(2) \qquad 5 \times 59p^{n-1} = 295p^{n-1} \geq 213p^n - 48 \geq 426p^{n-1} - 48 \Rightarrow 131p^{n-1} \leq 48,$$

a contradiction.

(2iv) $G/R \cong \mathrm{SL}(2,5)$.

Proof. — Suppose that $R_1 \neq R$ is a minimal normal subgroup of G. Then (by induction)

$$RR_1 = R \times R_1 = S, \ |R_1| = 2, \ G/R_1 \cong \mathrm{SL}(2,5)$$

and $G' < G$, since the multiplier of $\mathrm{SL}(2,5)$ is trivial, a contradiction. Therefore R is a unique minimal normal subgroup of G. Similarly, one obtains $Z(G) = 1$.

Let $p > 2$. Then $C_G(R) = R$. In this case $Z(S) < R$, so $Z(S) = 1$ and S is a Frobenius group with kernel R of index 2. As in (1iv) one has

$$k_G(S) = k_G(S-R) + k_G(R) \leq 1 + (p^n+4)/5 = (p^n+9)/5.$$

If $x \in G - S$ then $|G : C_G(x)| \geq 12p$ and

$$k_G(G-S) = k(G) - k_G(S) = |G|\mathrm{mc}(G) - k_G(S) \geq \\ 120p^n/16 - (p^n+9)/5 = (73p^n - 18)/10, \\ |G - S| = 118p^n \geq 12pk_G(G-S) \geq 6p(73p^n - 18)/5, \\ 295p^{n-1} \geq 219p^n - 54 \geq 657p^{n-1} - 54, \\ 54 \geq 362p^{n-1},$$

a contradiction.

Let $p = 2$. Since R is the only minimal normal subgroup of G and $Z(G) = 1$ then,

$$\begin{aligned}
k_G(S) &\leq 1 + (2^{n+1} - 1)/5 = (2^{n+1} + 4)/5,\\
k_G(G - S) &\geq 120.2^n/16 - (2^{n+1} + 4)/5 = (71.2^n - 8)/10,\\
59.2^{n+1} = |G - S| &\geq 24 k_G(G - S) \geq 24(71.2^n - 8)/10,\\
295.2^n &\geq 426.2^n - 48,\\
48 &\geq 131.2^n,
\end{aligned}$$

a contradiction.

(v) If D is the last term of the derived series of G then $D \in \{\mathrm{PSL}(2,5), \mathrm{SL}(2,5)\}$.

Proof. — Since $D = D'$ and $\mathrm{mc}(D) \geq \mathrm{mc}(G) \geq 1/16$ the result follows from (iv).

(vi) The subgroup D from (v) coincides with G'.

Proof. — We have $D \in \{\mathrm{PSL}(2,5), \mathrm{SL}(2,5)\}$ by (v). Since $Z(G) < D$ we may, by virtue of the Gallagher Theorem **[1]**, Theorem 7.46, assume that $Z(D) = 1$. Then $D \cong \mathrm{PSL}(2,5)$. Since

$$\mathrm{Aut} D \cong S_5, \ \mathrm{mc}(S_5) = 7/120 < 1/16$$

then

$$G/C_G(D) \cong \mathrm{PSL}(2,5), \ G = D \times C_G(G),$$

and $C_G(D)$ is abelian (see (ii)). So $D = G'$.

(vii) $G = SG'$.

This follows from (iii) and (vi).

(viii) $|S'| \leq 2$. In particular, S is nilpotent and all its Sylow subgroups of odd orders are abelian.

Proof. — In fact, $S' \leq S \cap G' \leq Z(G')$.

(ix) $G = S * G'$, a central product.

Proof. — Take an element x of order 5 in G'. Since $G' \cap S \leq Z(G)$, then

$$G/G' \cap S = G'/G' \cap S \times S/S \cap G'$$

implies that $\langle x, S\rangle$ is nilpotent. Hence $\langle S, x\rangle = P \times A$ where $P \in \mathrm{Syl}_2(S)$ and A is abelian. As $x \in A$ then $x \in C_G(S)$. Since $G' = \langle x \in G' | x^5 = 1\rangle$ it follows that $G = SG' = S * G'$.

(x) S is abelian.

Proof. — We have $G = (S \times G')/Z$ where $|Z| \leq 2$. For $G' \cong \mathrm{PSL}(2,5)$ our assertion is evident. Now let $G' \cong \mathrm{SL}(2,5)$. Then $|Z| = 2$, $Z \geq S'$. Suppose that S is non-abelian. Then $Z = S'$.

Take $\chi \in \mathrm{Irr}(G)$. We consider χ as a character of $G' \times S$ such that $Z \leq \ker\chi$. Then $\chi = \tau\vartheta$ where $\tau \in \mathrm{Irr}(G')$, $\vartheta \in \mathrm{Irr}(S)$ and $\chi_Z = \chi(1)1_Z = \tau(1)\vartheta(1)1_Z$. Now $\tau_Z = \tau(1)\lambda$, $\vartheta_Z = \vartheta(1)\mu$ where $\lambda, \mu \in \mathrm{Irr}(Z)$, $\lambda\mu = 1_Z$. Noting that $|Z| = 2$, one has

$\lambda = \mu$ and $\tau_Z = \tau(1)\lambda, \vartheta_Z = \vartheta(1)\lambda$. Since S is non-abelian then $\mathrm{cd}S = \{1, m\}$ where $m^2 = |S : Z(S)|$.

Suppose that $\lambda = 1_Z$. $\mathrm{Irr}(G')$ has exactly 5 characters containing Z in their kernels, so for τ we have exactly 5 possibilities. Since $Z \le \ker\vartheta$ then $\vartheta \in \mathrm{Lin}(S)$, and for ϑ we have exactly $|\mathrm{Lin}(S)| = |S|/2$ possibilities. Hence for χ we have exactly $5|S|/2$ possibilities if $\lambda = 1_Z$.

Suppose that $\lambda \ne 1_Z$. Then Z is not contained in $\ker\tau$, so for τ we have exactly $|\mathrm{Irr}(G')| - |\mathrm{Irr}(G'/Z)| = 9 - 5 = 4$ possibilities. Since $S' = Z$ is not contained in $\ker\vartheta$, then ϑ is not linear, and for ϑ we have exactly $(|S| - |S/S'|)/m^2 = |S|/2m^2$ possibilities. For χ we have, in this case, exactly $4|S|/2m^2 = 2|S|/m^2$ possibilities.

Finally,

$$k(G) = 5|S|/2 + 2|S|/m^2$$

and

$$\mathrm{mc}(G) = k(G)/|G| = k(G)/60|S| = 1/24 + 1/30m^2.$$

Since $m > 1$ then

$$\mathrm{mc}(G) \le 1/24 + 1/120 = 1/20 < 1/16,$$

a contradiction. Therefore S is abelian, $S = Z(G)$ and $G = G'Z(G)$. In this case $\mathrm{mc}(G) \in \{1/12, 3/40\}$. The theorem is proved.

Let now $f(G) \ge 1/4$. Then $\mathrm{mc}(G) > f(G)^2 \ge 1/16$, and Theorem 2 is a corollary of Theorem 1. It is easy to see that in this case $f(G) = f(G') \in \{4/15, 1/4\}$.

Proof of Theorem 3. — In view of Lemma 3 we may assume that $i_o(G) > 1/4$. Since

$$\mathrm{mc}(G) \ge f(G)^2 > i_o(G)^2 > 1/16$$

we may apply Theorem 1. By this theorem $G = G'Z(G)$ where

$$G' \in \{\mathrm{PSL}(2,5), \mathrm{SL}(2,5)\}.$$

If $G' = G$ then $G \cong \mathrm{PSL}(2,5)$ since $i_0(\mathrm{SL}(2,5)) = 1/120 < 1/4$. Now let $G' < G$.

Suppose that $\exp(G/G') > 2$. Let M/G' be the subgroup generated by all involutions of G/G'. Then $i(M) = i(G)$,

$$i_o(M) = i(M)/|M| = |G : M|i(G)/|G| = \\ |G : M|i_o(G) \ge |G : M|/4 \ge 1/2,$$

and M is solvable by **[1]** Theorem 11.24 (since $f(M) > i_o(M) \ge 1/2$), a contradiction. Thus $\exp(G/G') = 2$.

If $G' = \mathrm{PSL}(2,5)$ then $G = G' \times Z(G)$. If $\exp Z > 2$ and $M = G' \times \Omega_1(Z(G))$ then

$$i(G) = i(M),\ i_o(M) = |G : M|i_o(G) > |G : M|/4 \ge 1/2,$$

and M is solvable (see **[1]**, Theorem 11.24) — a contradiction. Hence if $G' \cong \mathrm{PSL}(2,5)$ then $G = \mathrm{PSL}(2,5) \times E$ with $\exp E \le 2$.

Now suppose that $G = G'Z(G)$, $G' \cong \mathrm{SL}(2,5)$ and $Z(G)$ is a 2-subgroup. Set $\langle z\rangle = Z(G')$.

If $\exp Z(G) = 2$ then $Z(G) = \langle z \rangle \times E$, $G = G' \times E$, and $i_o(G) < 1/4$. Assume that $\exp Z(G) = 4$. Then

$$G' \cap Z(G) = \langle z \rangle = \Phi(G)$$

where $\Phi(G)$ is the Frattini subgroup of G.

Let s be an element of order 4 in $Z(G)$. Then $Z(G) = \langle s \rangle \times E$ and

$$G = (G'\langle s \rangle) \times E, \exp E \leq 2.$$

Let us calculate $i_o(H)$ where

$$H = G'\langle s \rangle,\ Z(H) = \langle s \rangle,\ o(s) = 4.$$

Take $P \in \mathrm{Syl}_2(G')$. Then $P \cong Q(8)$ contains exactly three distinct cyclic subgroups $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$ of order 4, and $a^2 = b^2 = c^2 = s^2 = z$. Hence

$$(as)^2 = (bs)^2 = (cs)^2 = 1$$

and it is easy to see that $i_o(\langle P, s \rangle) = 7$. Now

$$\langle P, s \rangle \in \mathrm{Syl}_2(H),\ |H : N_H(\langle P, s \rangle)| = 5,$$
$$\langle P, s \rangle \cap \langle P, s \rangle^x = \langle s \rangle$$

for all $x \in H - N_H(\langle P, s \rangle)$. Thus

$$i_o(H) = |H : N_H(\langle P, s \rangle)| i_o(\langle P, s \rangle) -$$
$$(|H : N_H(\langle P, s \rangle)| - 1) i_o(\langle s \rangle) = 5 \times 7 - 4 = 31.$$

Since

$$G = H \times E,\ |E| = 2^\alpha,\ \exp E \leq 2,$$

then

$$i(G) = i(H)|E| + |E| - 1 = 31.2^\alpha + 2^\alpha - 1 = 32.2^\alpha - 1,$$
$$i_o(G) = i(G)/|G| = (32.2^\alpha - 1)/240.2^\alpha < 2/15 < 1/4,$$

a contradiction. Therefore $G' \not\cong \mathrm{SL}(2,5)$ and the theorem is proved.

Question. — Find all non-solvable groups G with $i_o(G) = 2^{-n}$, $n > 2$.

There exist four multiplication tables for two-element subsets of group elements (see [**3**]). These multiplication tables afford the following 2×2 squares:

$$\begin{matrix} A & B \\ B & A \end{matrix} \qquad \begin{matrix} A & B \\ B & C \end{matrix} \qquad \begin{matrix} A & B \\ C & A \end{matrix} \qquad \begin{matrix} A & B \\ C & D \end{matrix}$$

Here distinct letters denote distinct elements of a group.

Let us calculate the number $P(1)$ of the squares of the first type in a finite group G. If a pair $\{a, b\}$ of elements of G affords a square of the first type, then $a^2 = b^2$, $ab = ba$. Then $(a^{-1}b)^2 = 1$, so $i = a^{-1}b$ is the involution commuting with a and b. If $i \in \mathrm{Inv}(G)$ (the set of all involutions of G), $x \in C_G(i)$, then the pair (x, xi) affords the square of the first type. Therefore $i \in \mathrm{Inv}(G)$ affords exactly $|C_G(i)|$ squares of the first type. Let

$$\mathrm{Inv}(G) = K(1) \cup \cdots \cup K(r),$$

where $K(1), \dots, K(r)$ are distinct conjugacy classes of G. Then

$$P(1) = \sum_{i \in \mathrm{Inv}(G)} |C_G(i)| = \sum_{j=1}^{r} \sum_{i \in K(j)} |C_G(i)| = r|G|.$$

Thus $P(1) = r|G|$, where r is the number of conjugacy classes of involutions in G.

By analogy, we may prove that the number $P(1,2)$ of commutative squares in the multiplicative table of G is equal to $k(G)|G|$. The number $P(2)$ of squares of the second type in the multiplicative table of G is therefore equal to $P(2) = P(1,2) - P(1) = (k(G) - r)|G|$. If $p(n)$ is the fraction of squares of the n-th type in the multiplicative table of G then

$$p(1) = r/|G|, \ p(2) = (k(G) - r)/|G| = \mathrm{mc}(G) - p(1).$$

It is easy to see that the number $P(1) + P(3)$ of squares of the first and the third type in the multiplicative table of G is equal to $|G|s$ where s is the number of real classes (a class K of G is said to be real if $x \in K \Rightarrow x^{-1} \in K$). Thus

$$P(4) \equiv 0 \pmod{|G|}.$$

References

[1] Berkovich Ya. G., Zhmud' E. M., *Characters of finite groups*, Part 1, Amer. Math. Soc., Providence, Rhode Island, 1998.

[2] Blichfeldt H. F., *Finite collineation groups*, Chicago, 1917.

[3] Freiman G. A., *On two- and three-element subsets of groups*, Æquat. Math., **22**, 1981, 140–152.

Y. Berkovich, Research Institute of Afula, Department of Mathematics and Computer Science, University of Haifa, 31905 Haifa, Israel • *E-mail :* berkov@mathcs2.haifa.ac.il