Counterexamples to congruences in finite p-groups

Benjamin Sambale*

October 24, 2026

Abstract

Let K be a conjugacy class of a finite p-group G. Héthelyi, Külshammer and the author asked whether the number of conjugacy classes contained in KK^{-1} is always congruent to 1 modulo $p-1$, and whether, dually, the number of irreducible constituents of $\chi\overline{\chi}$ is congruent to 1 modulo $p-1$ for every $\chi \in \mathrm{Irr}(G)$. We construct a group of order 7^7 for which both congruences fail.

Keywords: p-groups, products of conjugacy classes, products of characters
AMS classification: 20D15, 20C15, 20E45

Let G be a finite p-group. For a conjugacy class K of G let $K^{-1} := \{a^{-1} : a \in K\}$, and let $\eta(K)$ be the number of conjugacy classes of G contained in KK^{-1}. Since all conjugacy classes have p-power length, $\eta(K) \equiv |KK^{-1}| \pmod{p-1}$. For a complex character ψ of G let $\mathrm{Irr}(\psi)$ be the set of its irreducible constituents. Motivated by sharp lower bounds for $\eta(K)$ and $|\mathrm{Irr}(\chi\overline{\chi})|$ due to Adan-Bante [2, 1], we asked in [4] whether

$$\eta(K) \equiv 1 \pmod{p-1} \tag{P1}$$

for every conjugacy class K of G, and whether

$$|\mathrm{Irr}(\chi\overline{\chi})| \equiv 1 \pmod{p-1} \tag{Q1}$$

for every $\chi \in \mathrm{Irr}(G)$. There, (P1) and (Q1) were proved for $p \leq 3$, for $|G| \leq p^6$, for groups of nilpotency class at most 2 and for metacyclic groups. We show that both congruences fail in general.

Theorem 1. *Let $R := \mathbb{F}_7[s]/(s^5)$, let $P := \langle 1+s, 1+s^2+s^4\rangle \leq R^\times$, and let $G := R \rtimes P$, where P acts on the additive group of R by multiplication. Then $|G| = 7^7$.*

(a) For the conjugacy class K of $1 \in R$ we have $\eta(K) = 33 \equiv 3 \pmod 6$.

(b) Let $\lambda \in \mathrm{Irr}(R)$ be given by $\lambda(a) := \zeta^{\tau(a)}$, where $\zeta := e^{2\pi i/7}$ and $\tau(a) \in \mathbb{F}_7$ is the coefficient of s^4 in a. Then $\chi := \lambda^G \in \mathrm{Irr}(G)$ and $|\mathrm{Irr}(\chi\overline{\chi})| = 81 \equiv 3 \pmod 6$.

In particular, (P1) and (Q1) fail for G.

*Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany, sambale@math.uni-hannover.de

Proof. Since $(1+s)^7 = 1+s^7 = 1$ and $(1+s^2+s^4)^7 = 1$, both generators of P have order 7. The coefficient of s in $(1+s)^i$ is i, so $\langle 1+s\rangle \cap (1+s^2R) = 1$. Hence $|P| = 49$ and $|G| = 7^5 \cdot 7^2 = 7^7$.

For $0 \neq a \in R$ let $\nu(a)$ be the largest k with $a \in s^k R$. For $a, b \neq 0$ we have $ab \neq 0$ whenever $\nu(a)+\nu(b) \leq 4$. Every $r \in P \setminus \{1\}$ has the form $r = (1+s)^i(1+s^2+s^4)^j$, and $\nu(r-1) = 1$ if $7 \nmid i$ and $\nu(r-1) = 2$ otherwise.

Let $P - P := \{a - b : a, b \in P\}$. We claim that P acts freely on $(P-P)\setminus\{0\}$ by multiplication. Let $a, b, c \in P$ with $a \neq b$ and $c(a-b) = a-b$. Since $a-b = b(ab^{-1}-1)$ and b is a unit, we get $(c-1)(ab^{-1}-1) = 0$. As $\nu(ab^{-1}-1) \leq 2$, the previous paragraph forces $c = 1$. A computer calculation shows $|P-P| = 1569$. Thus $(P-P)\setminus\{0\}$ splits into $1568/49 = 32$ orbits of length 49.

(a) Since R is abelian, the conjugacy class in G of an element $a \in R$ is its orbit Pa. In particular $K = P$, $KK^{-1} = P - P$, and the conjugacy classes in KK^{-1} are the P-orbits on $P - P$. Hence $\eta(K) = 1 + 32 = 33$.

(b) The map $\tau\colon R \to \mathbb{F}_7$ is a homomorphism of additive groups. For $r \in R$ let $\lambda_r(a) := \zeta^{\tau(ra)}$. Then $\lambda_r \in \mathrm{Irr}(R)$, and $(R,+) \to \mathrm{Irr}(R)$, $r \mapsto \lambda_r$ is a homomorphism. It is injective, because for $r \neq 0$ we can write $r = s^k u$ with a unit u and get $\tau(r \cdot s^{4-k}u^{-1}) = 1$. Since $|R| = |\mathrm{Irr}(R)|$, it is an isomorphism, and $\lambda = \lambda_1$. For $g \in P$ we have $\lambda_r^g(a) = \lambda_r(ga) = \lambda_{gr}(a)$, so the action of P on $\mathrm{Irr}(R)$ corresponds to multiplication on R. In particular, the stabilizer of λ in P is trivial, and $\chi = \lambda^G$ is irreducible by [5, Theorem 6.11]. Moreover $\chi_R = \sum_{g\in P} \lambda_g$ and $\overline{\chi} = \overline{\lambda}^G$, so [5, Problem 5.3] yields

$$\chi\overline{\chi} = (\chi_R\overline{\lambda})^G = \sum_{g\in P} (\lambda_{g-1})^G.$$

Here $(\lambda_0)^G = (1_R)^G$ is the sum of the 49 linear characters of $G/R \cong P$. For $g \neq 1$ the element $g-1$ lies in $(P-P)\setminus\{0\}$, so λ_{g-1} has trivial stabilizer and $(\lambda_{g-1})^G$ is irreducible of degree 49. By Clifford's theorem [5, Theorem 6.2], $(\lambda_d)^G = (\lambda_{d'})^G$ holds if and only if d and d' lie in the same P-orbit. Since every element of $P-P$ lies in the P-orbit of some $g-1$ with $g \in P$, all 32 orbits on $(P-P)\setminus\{0\}$ occur. Therefore $|\mathrm{Irr}(\chi\overline{\chi})| = 49 + 32 = 81$. □

Analogous constructions yield counterexamples of order p^7 for all primes $p \geq 7$. There are no counterexamples of order 5^7, but there is a counterexample of order 5^{12} with $R := \mathbb{F}_5[s,t]/(s^4, t^2)$ and $P := \langle 1+s,\ 1+t,\ 1+s^2,\ 1+st+s^3\rangle \leq R^\times$.

The group G of Theorem 1 is `SmallGroup`$(7^7, 78341)$ in the Small Groups Library. The file attached to this pdf verifies the counterexamples of order 7^7 and 5^{12} in GAP [3].

Acknowledgment

The work [4] is based on my diploma thesis written in 2008. At the time, I found a counterexample to a stronger conjecture, called (P3) in [4], of order 3^7 (note that (P1) and (Q1) hold for $p = 3$ in general). The groups of order 7^7 were not available at the time. Claude Opus 5.5 (Anthropic) took 30 minutes to find the present counterexample without brute-forcing the Small Groups Library. I have checked all the details and take full responsibility.

References

[1] E. Adan-Bante, *Products of characters and finite p-groups. II*, Arch. Math. (Basel) **82** (2004), 289–297.

[2] E. Adan-Bante, *Conjugacy classes and finite p-groups*, Arch. Math. (Basel) **85** (2005), 297–303.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.16.1*; 2026, `https://www.gap-system.org`.

[4] L. Héthelyi, B. Külshammer and B. Sambale, *Conjugacy classes and characters of finite p-groups*, Comm. Algebra **39** (2011), 657–685.

[5] I. M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006.