Pseudo Frobenius numbers

Benjamin Sambale[*]

September 28, 2019

Abstract

For a prime p, we call a positive integer n a Frobenius p-number if there exists a finite group with exactly n subgroups of order p^a for some $a \geq 0$. Extending previous results on Sylow's theorem, we prove in this paper that every Frobenius p-number $n \equiv 1 \pmod{p^2}$ is a Sylow p-number, i. e., the number of Sylow p-subgroups of some finite group. As a consequence, we verify that 46 is a pseudo Frobenius 3-number, that is, no finite group has exactly 46 subgroups of order 3^a for any $a \geq 0$.

Keywords: Frobenius' theorem, Sylow's theorem, number of p-subgroups
AMS classification: 20D20

1 Introduction

Motivated by Sylow's famous theorem in finite group theory, we investigated *pseudo Sylow p-numbers* in a previous paper [16]. These are positive integers $n \equiv 1 \pmod{p}$, where p is a prime, such that no finite group has exactly n Sylow p-subgroups. It is known that such numbers exist whenever p is odd and we gave an elementary argument for $p = 17$ and $n = 35$.

The present paper is based on Frobenius' extension [5] of Sylow's theorem:

Theorem 1 (Frobenius). *Let p be a prime and $a \geq 0$ such that p^a divides the order of a finite group G. Then the number of subgroups of order p^a of G is congruent to 1 modulo p.*

Nowadays this is usually proved using an argument of Wielandt (see [9, Satz I.7.2], for instance). It is a natural question to ask if every positive integer $n \equiv 1 \pmod{p}$ is a *Frobenius p-number*, i. e., there exists a finite group with exactly n subgroups of order p^a for some $a \geq 0$. The following refinement of Frobenius' theorem, proved by Kulakoff [11] for p-groups and extended to arbitrary finite groups by P. Hall [8], shows that most pseudo Sylow p-numbers cannot be Frobenius p-numbers.

Theorem 2 (Kulakoff–Hall). *Let p be a prime and $a \geq 0$ such that p^{a+1} divides the order of a finite group G. Then the number of subgroups of order p^a of G is congruent to 1 or to $1 + p$ modulo p^2.*

[*] Fachbereich Mathematik, TU Kaiserslautern, 67653 Kaiserslautern, Germany, sambale@mathematik.uni-kl.de

The proof of Theorem 2 uses only elementary group theory, but it lies somewhat deeper than Theorem 1 (Kulakoff [12] pointed out some errors in an earlier proof attempt by Miller [13]).

In view of Theorem 2, we call n a *pseudo Frobenius p-number* if n is congruent to 1 or $1+p$ modulo p^2 and no finite group has exactly n subgroups of order p^a for any $a \geq 0$. Obviously, every pseudo Frobenius p-number is a pseudo Sylow p-number. Since we know from [16] that every odd number is a Sylow 2-number, it is clear that there are no pseudo Frobenius 2-numbers.

Our aim in this paper is to establish the existence of a pseudo Frobenius number. The first choices are $n = 1+p$ and $n = 1+p^2$. However, it can be seen that the general linear group $G = \mathrm{GL}_2(p^a)$ has exactly $1+p^a$ Sylow p-subgroups for any $a \geq 1$ (the upper unitriangular matrices form a Sylow p-subgroup of G and the corresponding normalizer is the Borel subgroup consisting of all upper triangular matrices). The next candidate is $n = 1+p+p^2$, but this is clearly the number of subgroups of order p in the elementary abelian group G of order p^3 (every nontrivial element of G generates a subgroup of order p and two distinct subgroups intersect trivially). Now for $p = 3$ we might consider $n = 1+2\cdot 3^2 = 19$. However, 19 is a prime and we know already from [16] that for any prime $n \equiv 1 \pmod{p}$ there exist (solvable affine) groups with exactly n Sylow p-subgroups. Finally, we have mentioned in [16] (proved by M. Hall [7]) that $n = 1+3+2\cdot 3^2 = 22$ *is* a pseudo Sylow 3-number. On the other hand, the number of subgroups of order 9 in the abelian group $C_9 \times C_3 \times C_3$ is 22 and therefore, 22 is not a pseudo Frobenius number. (In general, the number of subgroups of a given isomorphism type in an abelian p-group is given by a *Hall polynomial.*)

Our first theorem in this paper deals with the case $n \equiv 1 \pmod{p^2}$.

Theorem A. *Every Frobenius p-number $n \equiv 1 \pmod{p^2}$ is a Sylow p-number.*

While our proof is elementary, it relies implicitly on the complicated classification of the finite simple groups (CFSG for short in the following). As an application we obtain our first pseudo Frobenius number.

Corollary B. *The integer 46 is a pseudo Frobenius 3-number.*

With the examples mentioned above, it can be seen that 46 is in fact the smallest pseudo Frobenius number. We do not know if there are any pseudo Frobenius p-numbers congruent to $1+p$ modulo p^2. There are no such numbers below 100 as one can check with the computer algebra system GAP [6] for instance.

2 Proofs

In this section, G always denotes a finite group with identity 1 and p is a prime number. The proof of Theorem A relies on the following more precise version of Theorem 2 for odd primes (see [8, Lemma 4.61 and Theorem 4.6]).

Proposition 3. *Let P be a Sylow p-subgroup of G for some $p > 2$. Then for $1 < p^a < |P|$, the number of subgroups of order p^a in G is congruent to 1 modulo p^2 if and only if P is cyclic.*

Proposition 3 does not hold for $p = 2$. For instance, the dihedral group of order 8 (i. e., the symmetry group of the square) has $5 \equiv 1 \pmod{4}$ subgroups of order 2 (generated by the four reflections and the rotation of degree π). A precise version for $p = 2$ can be found in Murai [14, Theorem D].

Our second ingredient is a consequence of the CFSG by Blau [1].

Proposition 4 (Blau)**.** *If the simple group G has a cyclic Sylow p-subgroup, then every two distinct Sylow p-subgroups of G intersect trivially.*

Proof of Theorem A. We may assume that p is odd. Let $n \equiv 1 \pmod{p^2}$ be a minimal counterexample. Then there exists a group G of minimal order such that the number of subgroups of order p^a for some $a \geq 0$ is n. Since obviously $n > 1$, we have $a \geq 1$. Moreover, since n is not a Sylow p-number, it follows that p^{a+1} divides $|G|$. By Proposition 3, G has a cyclic Sylow p-subgroup P. Since every Sylow p-subgroup contains exactly one subgroup of order p^a, the subgroups $Q = Q_1, \ldots, Q_n \leq G$ of order p^a form a conjugacy class in G. Furthermore, the number of Sylow p-subgroups must be greater than n and this implies that some Q_i is contained in two distinct Sylow p-subgroups. Hence by Proposition 4, G is not simple.

Thus, let N be a nontrivial proper normal subgroup of G. Let n_1 be the number of subgroups of order p^a in QN (note that this number does not depend on the choice of Q, since every Q_iN is conjugate to QN). Since PN/N is a cyclic Sylow p-subgroup of G/N, every subgroup of order $|QN/N|$ in G/N is of the form Q_iN/N for some i. We denote the number of these subgroups by n_2 and conclude that $n = n_1n_2$. By construction, n_1 and n_2 are Frobenius p-numbers.

Suppose that $n_i \not\equiv 1 \pmod{p^2}$ for some $i \in \{1, 2\}$. Then $n_1 \not\equiv 1 \not\equiv n_2 \pmod{p^2}$, since $n_1n_2 = n \equiv 1 \pmod{p^2}$. By Proposition 3, Q must be a Sylow p-subgroup of QN, that is

$$|QN : Q| \not\equiv 0 \pmod{p}. \tag{2.1}$$

Similarly, $QN/N \in \mathrm{Syl}_p(G/N)$ or $QN/N = 1$ according to Proposition 3. In the latter case, N contains $Q_1, \ldots, Q_n$ since they are all conjugate to Q. However, this contradicts the minimality of G. Hence, QN/N is a Sylow p-subgroup of G/N and $|G : QN| = |G/N : QN/N| \not\equiv 0 \pmod{p}$. In combination with (2.1), we obtain

$$|G : Q| = |G : QN||QN : Q| \not\equiv 0 \pmod{p}.$$

But this contradicts the observation that p^{a+1} divides $|G|$.

Consequently, $n_1 \equiv n_2 \equiv 1 \pmod{p^2}$. The minimal choice of G yields $n_2 < n$. Similarly, $n_1 = n$ implies $G = QN$. In this case, $P = QN \cap P = Q(N \cap P)$ (modular law) and since P is cyclic we even have $Q \subseteq N \cap P \subseteq N$ and $G = QN = N$, another contradiction. Thus, $n_1 < n$. Since n is a minimal counterexample to our theorem, n_1 and n_2 must be Sylow p-numbers, since they are Frobenius p-numbers. Let H_i be a finite group with exactly n_i Sylow p-subgroups for $i = 1, 2$. Then

$$\mathrm{Syl}_p(H_1 \times H_2) = \{S_1 \times S_2 : S_i \in \mathrm{Syl}_p(H_i)\}$$

and $n = n_1n_2$ is a Sylow p-number (of $H_1 \times H_2$). This final contradiction completes the proof. □

As in the previous paper [16], we make use of the first principles of group actions. Recall that an *action* of G on a finite nonempty set Ω is a map $G \times \Omega \to \Omega$, $(g, \omega) \mapsto {}^g\omega$ such that ${}^1\omega = \omega$ and ${}^g({}^h\omega) = {}^{gh}\omega$ for $g, h \in G$ and $\omega \in \Omega$. Every action gives rise to a homomorphism $G \to \mathrm{Sym}(\Omega)$ into the symmetric group on Ω, and the action is called *faithful* whenever this homomorphism is injective. In this case G is a *permutation group* of *degree* $|\Omega|$. The *orbit* of $\omega \in \Omega$ under G is the subset ${}^G\omega := \{{}^g\omega : g \in G\} \subseteq \Omega$. The *orbit-stabilizer theorem* states that

$$|{}^G\omega| = |G : G_\omega|$$

where $G_\omega := \{g \in G : {}^g\omega = \omega\}$ is the *stabilizer* of $\omega \in \Omega$. We say that G acts *transitively* on Ω if there is only one orbit, i.e., $\Omega = {}^G\omega$ for any $\omega \in \Omega$. A subset $\Delta \subseteq \Omega$ is called a *block* if

${}^g\Delta\cap\Delta\in\{\Delta,\varnothing\}$ for every $g\in G$. A transitive action is called *primitive* if there are no blocks Δ with $1<|\Delta|<|\Omega|$. This happens if and only if G_ω is a maximal subgroup of G for any $\omega\in\Omega$. Finally, a transitive action is 2-*transitive* if G_ω acts transitively on $\Omega\setminus\{\omega\}$ for any $\omega\in\Omega$. In the following we are mainly interested in the transitive conjugation action of G on $\mathrm{Syl}_p(G)$. Here the stabilizer of $P\in\mathrm{Syl}_p(G)$ is the *normalizer* $\mathrm{N}_G(P):=\{g\in G: gP=Pg\}$.

In the proof of Corollary B we apply two further results. The first appeared in Wielandt [18] and was reproduced in Cameron's book [3, Theorem 3.25].

Proposition 5 (Wielandt). *Let G be a primitive permutation group of degree $2p$. Then G is 2-transitive or $2p-1$ is a square.*

It is another consequence (which we do not need) of the CFSG that the second alternative in Proposition 5 only occurs for $p=5$.

The second tool for Corollary B is a consequence of Brauer's theory of p-blocks of defect 1 [2] and can be extracted from Navarro's book [15, Theorem 11.1]. Here, $\mathrm{Irr}(G)$ is the set of irreducible complex characters of G and the trivial character is denoted by 1_G.

Proposition 6 (Brauer). *Suppose that G has a Sylow p-subgroup P of order p such that $\mathrm{C}_G(P)=P$ and $e:=|\mathrm{N}_G(P)/P|$. Then there exists a set of irreducible characters*

$$B=\{1_G=\chi_1,\ldots,\chi_e,\psi_1,\ldots,\psi_{(p-1)/e}\}\subseteq\mathrm{Irr}(G)$$

and signs $\epsilon_1,\ldots,\epsilon_e\in\{\pm1\}$ such that

$$\begin{aligned}
&\chi_i(1)\equiv\epsilon_i\pmod p && (1\le i\le e),\\
&\psi_j(1)=\Big|\sum_{i=1}^{e}\epsilon_i\chi_i(1)\Big| && (1\le j\le(p-1)/e),\\
&\mu(1)\equiv 0\pmod p && (\forall\mu\in\mathrm{Irr}(G)\setminus B).
\end{aligned}$$

The special case $e=1$ in Proposition 6 leads to $1=1_G(1)=\chi_1(1)=\psi_1(1)=\ldots=\psi_{p-1}(1)$ and $|G:G'|=p$ where G' is the commutator subgroup of G (see [10, Problem 15.6]). In general, Proposition 6 provides information on $|G|$, because it is known that the irreducible character degrees divide the group order (see [10, Problem 28.12]).

Recall that every action of G on Ω gives rise to a *permutation character* π which counts the number of fixed points, that is, $\pi(g):=|\{\omega\in\Omega: {}^g\omega=\omega\}|$ for $g\in G$ (see [3, Section 2.5]). The action is 2-transitive if and only if $\pi=1_G+\chi$ for some $\chi\in\mathrm{Irr}(G)\setminus\{1_G\}$.

Proof of Corollary B. By Theorem A, it suffices to show that 46 is a pseudo Sylow 3-number, because $46\equiv1\pmod 9$. Let G be a minimal counterexample such that $|\mathrm{Syl}_3(G)|=46$. By Sylow's theorem, G acts transitively on $\mathrm{Syl}_3(G)$. If $K\trianglelefteq G$ is the kernel of this action, then it is easy to see that G/K has the same number of Sylow 3-subgroups (see [16, Step 1 of proof of Theorem A]). Thus, by minimality $K=1$ and G acts faithfully on $\mathrm{Syl}_3(G)$. In particular, we can and will regard G as a subgroup of the symmetric group S_{46}. Then, every Sylow 3-subgroup lies in the alternating group A_{46} and minimality implies $G\le A_{46}$. For $P\in\mathrm{Syl}_3(G)$ let $\mathrm{N}_G(P)<M\le G$. Then $P\in\mathrm{Syl}_3(M)$ and

$$|\mathrm{Syl}_3(M)|=|M:\mathrm{N}_M(P)|=|M:\mathrm{N}_G(P)|\in\{2,23,46\}$$

by Lagrange's theorem. Since 2 and 23 are not congruent to 1 modulo 3, we must have $M = G$. Hence, $\mathrm{N}_G(P)$ is a maximal subgroup of G and therefore G acts primitively on $\mathrm{Syl}_3(G)$.

[At this point we could refer to the database of primitive permutation groups of small degree (see for instance Dixon–Mortimer [4, Appendix B] or [6, 17]). However, this database is based on the Aschbacher–O'Nan–Scott theorem and relies ultimately on the CFSG. We prefer to give a classification-free argument along the lines of M. Hall's paper [7].]

Since 45 is not a square, Proposition 5 implies that G acts 2-transitively on $\mathrm{Syl}_3(G)$, i. e., $\mathrm{N}_G(P)$ acts transitively on $\mathrm{Syl}_3(G) \setminus \{P\}$. Hence, for $Q \in \mathrm{Syl}_3(G) \setminus \{P\}$, the 2-point stabilizer $\mathrm{N}_G(P) \cap \mathrm{N}_G(Q)$ has index 45 in $\mathrm{N}_G(P)$ by the orbit-stabilizer theorem. Since $\mathrm{N}_P(Q)$ is a Sylow 3-subgroup of $\mathrm{N}_G(P) \cap \mathrm{N}_G(Q)$, the orbit ${}^PQ$ of P has size

$$|{}^PQ| = |P : \mathrm{N}_P(Q)| = 9.$$

For $g \in \mathrm{N}_G(P)$ we have

$${}^g({}^PQ) = {}^{gP}Q = {}^{Pg}Q = {}^P({}^gQ).$$

Since the orbits of P are disjoint, ${}^PQ$ is a block of $\mathrm{N}_G(P)$. Since $\mathrm{N}_G(P)$ is transitive on $\mathrm{Syl}_3(G) \setminus \{P\}$, the distinct conjugates of ${}^PQ$ form a partition of $\mathrm{Syl}_3(G) \setminus \{P\}$ into five blocks with nine points each. Moreover, $\mathrm{N}_G(P)$ permutes these blocks. Suppose that there exists an element $x \in \mathrm{N}_G(P)$ of order 11. Then x must fix each of the five blocks. On the other hand, x cannot permute nine points nontrivially. Hence, x cannot exist and by Cauchy's theorem, $|G| = 46|\mathrm{N}_G(P)|$ is not divisible by 11. Similarly, $|\mathrm{N}_G(P)|$ is not divisible by 23.

Now let $S \in \mathrm{Syl}_{23}(G)$. Then $|S| = 23$ and S is generated by a product of two disjoint 23-cycles, since $|\mathrm{N}_G(P)|$ is not divisible by 23. It follows that $\mathrm{C}_G(S) \le \mathrm{C}_{A_{46}}(S) = S$ (see [16, Lemma 5]). Moreover, $|\mathrm{N}_G(S)/S|$ divides 22 (see [16, Lemma 6]). By Lagrange's theorem, $|\mathrm{N}_G(S)|$ is not divisible by 11 and therefore $|\mathrm{N}_G(S)/S| \in \{1, 2\}$. In the first case, $|G : G'| = 23$ by the remark after Proposition 6. However, this contradicts the minimal choice of G, since every Sylow 3-subgroup of G lies in G'. Hence, $|\mathrm{N}_G(S)/S| = 2$.

The permutation character of our 2-transitive group G has the form $1_G + \chi$ where $\chi \in \mathrm{Irr}(G)$ has degree 45 (see [3, Section 2.5]). With the notation of Proposition 6 for $p = 23$, we have $\psi_j(1) \equiv \pm 2 \pmod{23}$ for $j = 1, \ldots, 11$ and it follows that $\chi = \chi_2$, $\epsilon_2 = -1$ and $\psi_1(1) = |1 - 45| = 44$. However, the degree of every irreducible character divides the group order, but $|G|$ is not divisible by $44 = 4 \cdot 11$. Contradiction. □

It is possible to prove Corollary B directly without appealing to Theorem A or Proposition 4. To do so, one has to study the conjugation action on the set of 46 subgroups of a fixed 3-power order which is still (2-)transitive by Proposition 3.

Using the database of primitive permutation groups mentioned in the proof, it is easy to show that 51 is a pseudo Frobenius 5-number.

Acknowledgment

The author thanks the anonymous reviewer for pointing out a missing argument in the proof of Theorem A. This work is supported by the German Research Foundation (projects SA 2864/1-1 and SA 2864/3-1).

References

[1] H. I. Blau, *On trivial intersection of cyclic Sylow subgroups*, Proc. Amer. Math. Soc. **94** (1985), 572–576.

[2] R. Brauer, *On groups whose order contains a prime number to the first power. I*, Amer. J. Math. **64** (1942), 401–420.

[3] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, Vol. 45, Cambridge University Press, Cambridge, 1999.

[4] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Vol. 163, Springer-Verlag, New York, 1996.

[5] F. G. Frobenius, *Verallgemeinerung des Sylow'schen Satzes*, Sitzungsber. Preuß. Akad. Wiss. **1895** (1895), 981–993.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.0*; 2018, (`http://www.gap-system.org`).

[7] M. Hall, *On the number of Sylow subgroups in a finite group*, J. Algebra **7** (1967), 363–371.

[8] P. Hall, *On a Theorem of Frobenius*, Proc. London Math. Soc. (2) **40** (1935), 468–501.

[9] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften, Vol. 134, Springer-Verlag, Berlin, 1967.

[10] I. M. Isaacs, *Algebra: a graduate course*, Graduate Studies in Mathematics, Vol. 100, American Mathematical Society, Providence, RI, 2009.

[11] A. Kulakoff, *Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen*, Math. Ann. **104** (1931), 778–793.

[12] A. Kulakoff, *Einige Bemerkungen zur Arbeit: "Form of the number of the subgroups of a prime power group" von G. A. Miller*, Rec. Math. N.S. **8(50)** (1940), 73–75.

[13] G. A. Miller, *Form of the number of the subgroups of a prime power group*, Proc. Nat. Acad. Sci. U.S.A. **9** (1923), 237–238.

[14] M. Murai, *On the number of p-subgroups of a finite group*, J. Math. Kyoto Univ. **42** (2002), 161–174.

[15] G. Navarro, *Characters and blocks of finite groups*, London Mathematical Society Lecture Note Series, Vol. 250, Cambridge University Press, Cambridge, 1998.

[16] B. Sambale, *Pseudo Sylow numbers*, Amer. Math. Monthly **126** (2019), 60–65.

[17] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, Number of primitive permutation groups of degree n*, `https://oeis.org/A000019`.

[18] H. Wielandt, *Primitive Permutationsgruppen vom Grad $2p$*, Math. Z. **63** (1956), 478–485.