INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Stefanos Aivazidis and Thomas Müller

Congruences associated with families of nilpotent subgroups and a theorem of Hirsch

Volume 361 (2023), p. 1585-1592

https://doi.org/10.5802/crmath.514

CENTRE MERSENNE

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2023, Vol. 361, p. 1585-1592
https://doi.org/10.5802/crmath.514

Group theory / *Théorie des groupes*

Congruences associated with families of nilpotent subgroups and a theorem of Hirsch

Stefanos Aivazidis [*, a] **and Thomas Müller** [b]

[a] Department of Mathematics & Applied Mathematics, University of Crete, Greece
[b] Department of Mathematics, University of Vienna, Austria
E-mails: s.aivazidis@uoc.gr, muellet4@univie.ac.at

Abstract. Our main result associates a family of congruences with each suitable system of nilpotent subgroups of a finite group. Using this result, we complete and correct the proof of a theorem of Hirsch concerning the class number of a finite group of odd order.

Keywords. Nilpotent systems of subgroups, congruences.

2020 Mathematics Subject Classification. 20D20, 20D60.

Funding. The first author is partially supported by the Hellenic Foundation for Research and Innovation, Project HFRI-FM17-1733. This research was supported through the program “Research in Pairs” by the Mathematisches Forschungsinstitut Oberwolfach in 2019.

Manuscript received 28 April 2023, revised and accepted 13 May 2023.

1. Introduction

A celebrated result of Burnside [1, p. 295], established using the then still recent (ordinary) character theory of finite groups, states that if G is a group of odd order then the class number $k(G)$ of G satisfies the congruence $k(G) \equiv |G| \pmod{16}$. The starting point of the work reported here was our desire to correct and complete the proof of an apparently little known theorem of Hirsch [7] providing a beautiful non-trivial refinement of Burnside's result.

Theorem 1. *Let $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the order of a group G, where $p_1, p_2, \dots, p_k$ are odd primes, and $\alpha_1, \alpha_2, \dots, \alpha_k$ are positive integers. Let d be the greatest common divisor of the numbers $p_i^2 - 1$ with $1 \leqslant i \leqslant k$. Then $N \equiv k(G) \pmod{2d}$.*

Burnside's result follows from Theorem 1, since $p^2 \equiv 1 \pmod 8$ for p odd, so that $8 \mid d$. To quickly finish our description of this line of development, we mention that, using some of the easier ideas of Hirsch [7], Poland [8] subsequently obtains an alternative congruence for $k(G)$ which, when combined with Theorem 1, yields the following further strengthening of Burnside's theorem.

[*] Corresponding author.

Theorem 2 ([8, Cor. 3.10]). *In the notation of Theorem 1, we have, for $N = |G|$ odd,*

$$k(G) \equiv N \pmod{\operatorname{lcm}\{2d, \tau\}}, \tag{1}$$

where $\tau = \operatorname{gcd}_{i \leqslant i \leqslant k}(p_i - 1)^2$.

Hirsch's proof of Theorem 1, though ingenious and mostly correct, exhibits several gaps, and one non-trivial error. The most serious gap we found is the lack of any justification offered for the following claim, which Hirsch [7] makes in passing, and then bases the more subtle final part of his argument on:

Claim 3. *The number of Sylow p-subgroups of a group G of odd order, containing a given p-element, is odd.*

It is not too hard (though not completely trivial) to supply a proof of Claim 3, if one is willing to invoke the Odd Order Theorem, and to exploit the solubility of G; however, the paper [4] establishing Burnside's Odd Order Conjecture only appeared in 1963, hence was not available to Hirsch in the late 1940's. This raises the question whether an elementary proof of Claim 3 can be given, which does not presuppose solubility of the group involved. This is indeed the case but, as often happens, starting out with a rather specialised problem has led us to the discovery of a more general result, relating congruences to certain systems of nilpotent subgroups in an arbitrary finite group, which appears to be of interest in itself; cf. Section 2, in particular Theorem 7.

2. Set-up and main result

Let G be a finite group, and let $\mathfrak{F}_G$ be a collection of nilpotent subgroups of G satisfying:

(a) $1 \in \mathfrak{F}_G$ and $G \notin \mathfrak{F}_G$;

(b) $S \in \mathfrak{F}_G$ and $g \in G$ implies $S^g \in \mathfrak{F}_G$;

(c) $S \in \mathfrak{F}_G$ and $R \leqslant S$ implies $R \in \mathfrak{F}_G$;

(d) for each subgroup $K \leqslant G$ (in particular for G itself), the maximal elements of the subposet

$$\mathfrak{F}_K := \{S \in \mathfrak{F}_G : S \leqslant K\} \subseteq \mathfrak{F}_G$$

(with inclusion as partial order) form a single K-conjugacy class $\mathscr{M}_K$;

(e) for any two subgroups K, L of G with $K \leqslant L$, we have $(K:S)\big|(L:T)$, where $S \in \mathscr{M}_K$ and $T \in \mathscr{M}_L$.

For clarification, we note that the concept of a maximal element used here refers to the context of *poset theory*: if $(P, \leqslant)$ is a poset, an element $a \in P$ is termed *maximal*, if $a \leqslant p$ for some $p \in P$ implies $a = p$ (i.e., a is not strictly covered). In particular, if P has a greatest element a_0, then a_0 is the only maximal element of P.

The following is now easily checked.

Lemma 4. *Let G be a finite group, and let $\mathfrak{F}_G$ be a system of nilpotent subgroups of G satisfying Conditions* (a)–(e). *Let $K \leqslant G$, and suppose that $K \notin \mathfrak{F}_G$. Then the pair $(K, \mathfrak{F}_K)$ again satisfies Conditions* (a)–(e), *where $\mathfrak{F}_K$ is defined as above.*

Examples 5.

(1) Suppose that $|\pi(G)| > 1$. For a prime $p \in \pi(G)$, let $\mathfrak{F}_G$ be the collection of all p-subgroups of G. For $K \leqslant G$, the collection $\mathscr{M}_K$ of maximal elements of the poset $(\mathfrak{F}_K, \subseteq)$ consists precisely of the Sylow p-subgroups of K. Conditions (a)–(c) are clear, while Conditions (d)–(e) hold by Sylow's theorem.

(2) Let π be a set of primes, and let G be a soluble group whose order is not a π-number. Suppose that G contains a nilpotent Hall π-subgroup H. Then each π-subgroup of G is nilpotent, and is contained in some conjugate of H; in particular, the Hall π-subgroups of G form a single conjugacy class (by Wielandt's corresponding theorem in [9]). Let $\mathfrak{F}_G$ be the collection of all π-subgroups of G. For $K \leqslant G$, the maximal elements of the poset $(\mathfrak{F}_K, \subseteq)$ are the Hall π-subgroups of K. Again, Conditions (a)–(c) are clear, while Conditions (d) and (e) hold thanks to P. Hall's characterisation of soluble groups; cf. in particular [5].

Let $\mathbb{P}$ denote the set of all positive rational primes. Given a finite group G and a system $\mathfrak{F}_G$ of nilpotent subgroups of G, we set

$$m_G := \gcd\left\{p-1 : p \in \mathbb{P},\, p \mid (G:M) \text{ for some } M \in \mathscr{M}_G\right\}.$$

If

$$\left\{p \in \mathbb{P} : p \mid (G:S) \text{ for some } S \in \mathscr{M}_G\right\} = \emptyset,$$

then $|S| = |G|$ for $S \in \mathscr{M}_G$, so $G = S \in \mathfrak{F}_G$, contradicting the second part of Condition (a). Hence, assuming $G \notin \mathfrak{F}_G$, the constant m_G is well defined.

We note the following.

Lemma 6. *Let G be a finite group and let $\mathfrak{F}_G$ be a system of nilpotent subgroups of G satisfying Conditions* (a) *and* (e). *If $K \leqslant G$ and $K \notin \mathfrak{F}_G$, then $m_G \mid m_K$.*

Proof. Since $K \notin \mathfrak{F}_G$, we have $K \notin \mathfrak{F}_K$, so that m_K is defined. Suppose that $p \in \mathbb{P}$ is such that $p \mid (K:S)$ for some $S \in \mathscr{M}_K$. Then $p \mid (G:T)$ for $T \in \mathscr{M}_G$ by Condition (e), so that $m_G \mid p-1$. Hence, $m_G \mid m_K$, as claimed. □

Our main result is now as follows.

Theorem 7. *Let G be a finite group, and let $\mathfrak{F}_G$ be a system of nilpotent subgroups of G satisfying Conditions* (a)–(e). *For $S \in \mathfrak{F}_G$, set*

$$\mathfrak{F}_G(S) := \{T \in \mathscr{M}_G : S \leqslant T\}.$$

Then $|\mathfrak{F}_G(S)| \equiv 1 \pmod{m_G}$ for all $S \in \mathfrak{F}_G$.

Combining Theorem 7 with Example (1), we derive an arithmetic property of the collection of Sylow p-subgroups of a finite group G containing a fixed p-subgroup.

Corollary 8. *Let G be a finite group such that $|\pi(G)| > 1$, let p be a prime number dividing the order of G, and let H be a fixed p-subgroup of G. Then the number $n_p(G,H)$ of Sylow p-subgroups of G containing H satisfies the congruence*

$$n_p(G,H) \equiv 1 \pmod{m_G}, \tag{2}$$

where

$$m_G = \gcd\left\{p-1 : p \in \pi(G) \setminus \{p\}\right\}.$$

Remark 9. Hirsch's original Claim 3 follows from the special case of Corollary 8, where G has odd order, and H is cyclic.

Similarly, by combining Theorem 7 with Example (2), we find the following.

Corollary 10. *Let G be a finite soluble group, let π be a non-empty set of prime numbers such that $|G|$ is not a π-number, and let H be a fixed π-subgroup of G. If G contains a nilpotent Hall π-subgroup, then the number $n_\pi(G,H)$ of Hall π-subgroups of G containing H satisfies the congruence*

$$n_\pi(G,H) \equiv 1 \pmod{m_G}, \tag{3}$$

where

$$m_G = \gcd\{p-1 : p \in \pi(G) - \pi\}.$$

Remark 11. The condition in Corollary 10 that the group G should contain a nilpotent Hall π-subgroup can in fact be disposed of, leading to the following general result for finite π-separable groups.

Theorem 12. *Let π be a non-empty set of primes, let G be a finite π-separable group such that $|G|$ is not a π-number, and let H be a fixed π-subgroup of G. Then the number $n_\pi(G,H)$ of Hall π-subgroups of G containing H satisfies the congruence*

$$n_\pi(G,H) \equiv 1 \pmod{m_G},$$

where

$$m_G = \gcd\{p-1 : p \in \pi(G) - \pi\}.$$

The proof of Theorem 12, whose proper setting is the theory of projectors relative to Schunck classes, will be discussed in a separate publication, together with certain related results.

3. Proof of Theorem 7

We begin with two easy reductions.

First, suppose that $S \in \mathfrak{F}_G$ is such that $S \trianglelefteq G$. Then $\mathfrak{F}_G(S) = \mathscr{M}_G$ by (d) with $G = K$, and so

$$|\mathfrak{F}_G(S)| = |\mathscr{M}_G| = (G : \mathbf{N}_G(T)),$$

where $T \in \mathscr{M}_G$. Consequently, if p is a prime dividing the cardinality of the set $\mathfrak{F}_G(S)$, then $p \mid (G:T)$, hence $p \equiv 1 \pmod{m_G}$ by definition of m_G, implying $|\mathfrak{F}_G(S)| \equiv 1 \pmod{m_G}$. Therefore, we may suppose that $\mathbf{N}_G(S) < G$.

Second, if $S \in \mathscr{M}_G$, then $\mathfrak{F}_G(S) = \{S\}$, so $|\mathfrak{F}_G(S)| = 1 \equiv 1 \pmod{m_G}$. Thus, we may assume that $S \notin \mathscr{M}_G$.

Suppose for a contradiction that Theorem 7 is false, and let G be a counterexample of least possible order. Fix a system $\mathfrak{F}_G$ of nilpotent subgroups satisfying Conditions (a)–(e) for which G fails, and, among the elements $S \in \mathfrak{F}_G$ with $|\mathfrak{F}_G(S)| \not\equiv 1 \pmod{m_G}$, let S_0 be one of largest possible order. By the observations above, we have $K := \mathbf{N}_G(S_0) < G$ and $S_0 \notin \mathscr{M}_G$.

Let $K_1, K_2, \ldots, K_t$ be the pairwise distinct elements of $\mathfrak{F}_K$ occurring as intersections $S \cap K$ for $S \in \mathfrak{F}_G(S_0)$, and set

$$\mathfrak{F}_j(S_0) := \{S \in \mathfrak{F}_G(S_0) : \mathbf{N}_S(S_0) = K_j\}, \quad 1 \leqslant j \leqslant t,$$

so that

$$\mathfrak{F}_G(S_0) = \bigsqcup_{j=1}^{t} \mathfrak{F}_j(S_0)$$

for some $t > 0$, where $\sqcup$ denotes disjoint union. We note that, for $j \in [t]$ and $S \in \mathfrak{F}_j(S_0)$,

$$S_0 < K_j = \mathbf{N}_S(S_0) \leqslant S$$

since $S_0 < S$ by our second reduction, so that its normaliser in the nilpotent group S grows.

Each of these elements K_j may or may not lie in $\mathscr{M}_K$, i.e., be a maximal element of $\mathfrak{F}_K$. After permuting indices if necessary, we may suppose that

$$K_j \in \mathscr{M}_K \iff j \in [s]$$

for some s with $0 \leqslant s \leqslant t$. We claim that

$$\mathscr{M}_K = \{K_1, K_2, \ldots, K_s\}.$$

To see this, we first note that $\mathscr{M}_K = \mathfrak{F}_K(S_0)$ by Condition (d), since $S_0 \trianglelefteq K$. Hence, a given element $S \in \mathscr{M}_K$ is contained in some $T \in \mathfrak{F}_G(S_0)$, and we have $S \leqslant T \cap K \in \mathfrak{F}_K$ by Condition (c), so that

$$T \cap K = S = K_j$$

for some $j \in [s]$. It follows that $\mathscr{M}_K \subseteq \{K_1, \dots, K_s\}$, and the reverse inclusion holds by definition of s.

It follows now that $s \equiv 1 \pmod{m_G}$. Indeed, by Condition (d), we have

$$s = |\mathscr{M}_K| = (K : \mathbf{N}_K(S)) \,\big|\, (K : S)$$

for some $S \in \mathscr{M}_K$. If $K \in \mathfrak{F}_G$, then $\mathscr{M}_K = \{K\}$, so $s = 1 \equiv 1 \pmod{m_G}$. Suppose, on the other hand, that $K \notin \mathfrak{F}_G$ (so that $K \notin \mathfrak{F}_K$ and m_K is defined), and let $p \in \mathbb{P}$ be such that $p \mid s$. Then $p \mid (K : S)$, so $p \equiv 1 \pmod{m_K}$ by definition of m_K, implying $s \equiv 1 \pmod{m_K}$. Furthermore, by Lemma 6, $m_G \mid m_K$ in this case, and we again deduce that $s \equiv 1 \pmod{m_G}$.

For $j \in [s]$, we have $\mathfrak{F}_j(S_0) = \mathfrak{F}_G(K_j)$, thus $\left|\mathfrak{F}_j(S_0)\right| \equiv 1 \pmod{m_G}$ by choice of S_0, since $K_j > S_0$. Hence,

$$\left| \bigsqcup_{j=1}^{s} \mathfrak{F}_j(S_0) \right| = \sum_{j=1}^{s} \left|\mathfrak{F}_j(S_0)\right| \equiv s \equiv 1 \pmod{m_G}. \tag{4}$$

In order to obtain the desired contradiction (to the existence of a counterexample G), it remains to show that

$$\left| \bigsqcup_{j=s+1}^{t} \mathfrak{F}_j(S_0) \right| \equiv 0 \pmod{m_G}. \tag{5}$$

In fact, we shall establish the stronger property that

$$\left|\mathfrak{F}_j(S_0)\right| \equiv 0 \pmod{m_G}, \quad s < j \leqslant t. \tag{6}$$

Suppose for a contradiction that (6) is false. Then, among the indices j with $s < j \leqslant t$ and $\left|\mathfrak{F}_j(S_0)\right| \not\equiv 0 \pmod{m_G}$, we may choose one, j_0 say, such that $\mathbf{N}_S(S_0) = K_{j_0}$ is of largest order among the subgroups K_j of K corresponding to these indices j. Consider the complex $\mathfrak{F}_G(K_{j_0})$. Since $K_{j_0} > S_0$, we have $\left|\mathfrak{F}_G(K_{j_0})\right| \equiv 1 \pmod{m_G}$ by our choice of S_0. We now split the set $\mathfrak{F}_G(K_{j_0})$ according to the intersections of its elements with the normaliser $K = \mathbf{N}_G(S_0)$. Let $K_{j_0}, L_1, L_2, \dots, L_r$ be the distinct elements of $\mathfrak{F}_K$ arising in this way, so that

$$\mathfrak{F}_G(K_{j_0}) = \mathfrak{F}_{j_0}(S_0) \sqcup \bigsqcup_{\rho=1}^{r} \left\{S \in \mathscr{M}_G : \mathbf{N}_S(S_0) = L_\rho\right\}, \tag{7}$$

where $L_\rho > K_{j_0}$ for all $\rho \in [r]$, with some r such that $0 \leqslant r < t$. Since $\mathfrak{F}_G(K_{j_0}) \subseteq \mathfrak{F}_G(S_0)$, the groups L_ρ we encounter in this way are among the subgroups $K_1, \dots, K_t$ of K which occurred earlier on in the proof, so that $L_\rho = K_{\psi(\rho)}$ for a suitable injective map $\psi : [r] \to [t]$. We thus have

$$\left\{S \in \mathscr{M}_G : \mathbf{N}_S(S_0) = L_\rho\right\} = \mathfrak{F}_{\psi(\rho)}(S_0), \quad 1 \leqslant \rho \leqslant r,$$

and (7) may be written more briefly in the form

$$\mathfrak{F}_G(K_{j_0}) = \mathfrak{F}_{j_0}(S_0) \sqcup \bigsqcup_{\rho=1}^{r} \mathfrak{F}_{\psi(\rho)}(S_0). \tag{8}$$

Now, as before, a given L_ρ may or may not be a maximal element of $\mathfrak{F}_K$, while $K_{j_0} \notin \mathscr{M}_K$ since $j_0 > s$. After permuting indices if necessary, we may suppose that

$$L_\rho \in \mathscr{M}_K \iff \rho \in [q]$$

for some integer q with $0 \leqslant q \leqslant r$. We have

$$\mathfrak{F}_{\psi(\rho)}(S_0) = \left\{S \in \mathscr{M}_G : \mathbf{N}_S(S_0) = L_\rho\right\} = \mathfrak{F}_G(L_\rho), \quad 1 \leqslant \rho \leqslant q,$$

so $\left|\mathfrak{F}_{\psi(\rho)}(S_0)\right| \equiv 1 \pmod{m_G}$ for $1 \leqslant \rho \leqslant q$ by our choice of S_0, since $L_\rho > K_{j_0} > S_0$. Hence,

$$\left|\bigsqcup_{\rho=1}^{q} \mathfrak{F}_{\psi(\rho)}(S_0)\right| = \sum_{\rho=1}^{q} \left|\mathfrak{F}_{\psi(\rho)}(S_0)\right| \equiv q \pmod{m_G}. \tag{9}$$

Next, we claim that

$$\mathfrak{F}_K(K_{j_0}) = \left\{L_1, L_2, \ldots, L_q\right\}. \tag{10}$$

Indeed, let $S \in \mathfrak{F}_K(K_{j_0})$. Then there exists some $S' \in \mathscr{M}_G$ such that $S' \geqslant S$, a fortiori $S' \in \mathfrak{F}_G(K_{j_0})$, and

$$S' \cap K = S = L_\rho$$

for some $\rho \in [q]$. This proves the forward inclusion of (10), while the reverse inclusion holds by definition of q.

It now follows that $q \equiv 1 \pmod{m_G}$. Indeed, if $K \in \mathfrak{F}_G$, then $\mathscr{M}_K = \{K\}$, and

$$q = \left|\mathfrak{F}_K(K_{j_0})\right| = 1 \equiv 1 \pmod{m_G}.$$

If, on the other hand, $K \notin \mathfrak{F}_G$, then $K \notin \mathfrak{F}_K$, so that m_K is defined, and the pair $(K, \mathfrak{F}_K)$ satisfies Conditions (a)–(e) by Lemma 4. Consequently, we have

$$q = \left|\mathfrak{F}_K(K_{j_0})\right| \equiv 1 \pmod{m_K}$$

by choice of G, since $K < G$. Furthermore, $m_G \mid m_K$ by Lemma 6, so that $q \equiv 1 \pmod{m_G}$ follows again.

Combining (9) with our last observation, we now conclude that

$$\left|\bigsqcup_{\rho=1}^{q} \mathfrak{F}_{\psi(\rho)}(S_0)\right| \equiv 1 \pmod{m_G}.$$

Moreover, for ρ in the range $q < \rho \leqslant r$, we have $\psi(\rho) > s$ and $K_{\psi(\rho)} > K_{j_0}$. Hence, by our choice of the index j_0, it follows that

$$\left|\mathfrak{F}_{\psi(\rho)}(S_0)\right| \equiv 0 \pmod{m_G}, \quad q < \rho \leqslant r.$$

We deduce that

$$1 \equiv \left|\mathfrak{F}_G(K_{j_0})\right| \equiv \left|\mathfrak{F}_{j_0}(S_0)\right| + 1 \not\equiv 1 \pmod{m_G},$$

since $\left|\mathfrak{F}_{j_0}(S_0)\right| \not\equiv 0 \pmod{m_G}$ by our choice of j_0. This contradiction shows that (6) holds; thus also (5) holds true. Combining (4) with (5), we now deduce that

$$|\mathfrak{F}_G(S_0)| \equiv 1 \pmod{m_G},$$

contradicting our choice of the data G, $\mathfrak{F}_G$, and S_0. This final contradiction shows that no counterexample to our theorem exists, and the result is proven. □

4. Some remarks concerning the proof of Theorem 1

Let G be a group of odd order N. If $x \in G$ lies in a conjugacy class of size h, then the number of elements $y \in G$ commuting with x is N/h. Thus, the total number of solutions $(x, y) \in G^2$ of the equation

$$x^{-1}y^{-1}xy = 1 \tag{11}$$

is

$$\sum_{\rho=1}^{k(G)} h_\rho N/h_\rho = Nk(G).$$

Hirsch's principal idea is to recount the non-trivial solutions (x, y) of (11) in batches according to the subgroup $\langle x, y\rangle$ they generate. Hence, we need to compute $\varphi_2(\langle x, y\rangle)$. Here, for a finite group G and a positive integer n, $\varphi_n(G)$, the nth Eulerian number of G, is the number of n-tuples $(x_1, x_2, \ldots, x_n) \in G^n$ such that $G = \langle x_1, x_2, \ldots, x_n \rangle$. These numbers were introduced by Philip Hall [6], who shows among other things that

$$\varphi_n(G) = \sum_{H \leqslant G} \mu_G(H, G)|H|^n, \tag{12}$$

where μ_G is the Möbius function for the lattice of subgroups of G; cf. [6, Eqn. (3.12)]. Let $x = x_1 x_2 \cdots x_k$ and $y = y_1 y_2 \cdots y_k$, where x_i and y_i are p_i-elements. Then

$$\varphi_2(\langle x, y \rangle) = \varphi_2(\langle x_1, y_1 \rangle)\varphi_2(\langle x_2, y_2 \rangle) \cdots \varphi_2(\langle x_k, y_k \rangle).$$

Now $\langle x_i, y_i \rangle$, if non-trivial, is either cyclic of order p_i^m, say, or an abelian group of the form $C_{p_i^m} \times C_{p_i^n}$, where $m \geqslant n$. For a prime p and a positive integer m, we have

$$\varphi_2(C_{p^m}) = p^{2m} - p^{2m-2} = p^{2m-2}(p^2 - 1), \tag{13}$$

since we only need to rule out those pairs in which the orders of both components are less than p^m. In dealing with the case of an abelian p-group of rank 2, Hirsch offers, essentially without proof, the formulae

$$\varphi_2(C_{p^m} \times C_{p^m}) = (p^{2m} - p^{2m-2})[(p^{2m} - p^{2m-2}) - (p^m - p^{m-1})], \tag{14}$$

$$\varphi_2(C_{p^m} \times C_{p^n}) = \varphi(p^m)p^n\varphi(p^n)(p^m + p^{m-1}), \quad m > n, \tag{15}$$

where φ is Euler's totient function. Of these, (14) is false (the right-hand side overcounts whenever $m > 1$), while (15) turns out to be correct. The fact that Hirsch distinguishes the cases $m = n$ and $m > n$ suggests that what he had in mind here is a direct enumeration of pairs of generators in these groups. Viewed in this way, the proof of (15) is considerably harder than that of (14), so that the correctness of (15), against the backdrop of (14) being erroneous, comes as somewhat of a surprise. In any case, Hall's formula (12) suggests a more elegant and uniform approach to the computation of the Eulerian numbers of a finite abelian p-group, which we explain next.

If G is a finite abelian p-group, then, by duality,

$$\mu_G(H, G) = \mu_G(1, G/H), \quad H \leqslant G.$$

Moreover, Delsarte [3] shows in this case that, for $H \leqslant G$,

$$\mu_G(1, H) = \begin{cases} (-1)^s p^{\binom{s}{2}}, & H \cong C_p^s, \\ 0, & \text{otherwise.} \end{cases}$$

Hence, for

$$G = C_{p^{\lambda_1}} \times C_{p^{\lambda_2}} \times \cdots \times C_{p^{\lambda_\ell}}$$

of type $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ with $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_\ell \geqslant 1$, we have

$$\begin{aligned} \varphi_n(G) &= \sum_{s=0}^{\ell} \sum_{\substack{H \leqslant G \\ G/H \cong C_p^s}} \mu_G(1, G/H)|H|^n \\ &= \sum_{s=0}^{\ell} \sum_{\substack{H \leqslant G \\ G/H \cong C_p^s}} (-1)^s p^{\binom{s}{2}} p^{n(\lambda_1 + \cdots + \lambda_\ell - s)}. \end{aligned}$$

Again by duality, the number of subgroups $H \leqslant G$ with $G/H \cong C_p^s$ equals the number of subgroups $K \leqslant G$ with $K \cong C_p^s$. By a well-known result, the number of subgroups of type $\nu = (\nu_1, \ldots, \nu_\ell)$ in an abelian p-group of type $\lambda = (\lambda_1, \ldots, \lambda_\ell)$ is given by the formula

$$\prod_{i \geqslant 1} p^{\nu'_{i+1}(\lambda'_i - \nu'_i)} \begin{bmatrix} \lambda'_i - \nu'_{i+1} \\ \nu'_i - \nu'_{i+1} \end{bmatrix}_p, \tag{16}$$

where λ', ν' are the conjugates of the partitions λ and ν, respectively, and

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \prod_{i=0}^{k-1} \frac{1-p^{n-i}}{1-p^{i+1}} \tag{17}$$

is the number of k-dimensional subspaces of an n-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$; see, for instance, [2, Eqn. (1)]. If $H \leqslant G$ is such that $H \cong C_p^s$, then its type ν takes the form

$$\nu = (\underbrace{1,1,\dots,1}_{s}, \underbrace{0,0,\dots,0}_{\ell-s}),$$

and, consequently,

$$\nu' = (s, \underbrace{0,0,\dots,0}_{\ell-1}).$$

It thus follows from (16) that the number of subgroups H in a group G of type λ with $H \cong C_p^s$ is simply given by the Gauß coefficient $\left[\begin{smallmatrix} \ell \\ s \end{smallmatrix}\right]_p$. We thus obtain

$$\varphi_n(G) = \sum_{s=0}^{\ell} (-1)^s p^{\binom{s}{2}} \begin{bmatrix} \ell \\ s \end{bmatrix}_p p^{n(\lambda_1+\cdots+\lambda_\ell - s)}.$$

Applying the q-binomial theorem

$$(1+z)(1+qz)\cdots(1+q^{\ell-1}z) = \sum_{s=0}^{\ell} \begin{bmatrix} \ell \\ s \end{bmatrix}_q q^{\binom{s}{2}} z^s$$

with $q = p$ and $z = -p^{-n}$, we find the following.

Proposition 13. *Let*

$$G = C_{p^{\lambda_1}} \times C_{p^{\lambda_2}} \times \cdots \times C_{p^{\lambda_\ell}}$$

be a finite abelian p-group of type $\lambda = (\lambda_1, \dots, \lambda_\ell)$, where $\ell \geqslant 1$ and $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_\ell \geqslant 1$, and let n be a positive integer. Then the nth Eulerian number $\varphi_n(G)$ of G is given by the formula

$$\varphi_n(G) = p^{n(\lambda_1+\cdots+\lambda_\ell) - \binom{n+1}{2} + \binom{n-\ell+1}{2}} \prod_{i=0}^{\ell-1} (p^{n-i} - 1). \tag{18}$$

In particular, for $\ell = n = 2$, Equation (18) yields

$$\varphi_2(C_{p^m} \times C_{p^r}) = p^{2m+2r-3}(p^2-1)(p-1), \quad m \geqslant r, \tag{19}$$

which is what Hirsch needs at this point.

Since $\langle x, y\rangle$ is non-trivial by assumption, at least one of its Sylow subgroups $\langle x_i, y_i\rangle$ must be non-trivial, thus $d \mid \varphi_2(\langle x, y\rangle)$ by (13) and (19), so $Nk(G) \equiv 1 \pmod{d}$. Since $N^2 \equiv 1 \pmod{d}$ by definition of d, we find that $k(G) \equiv N \pmod{d}$. The second (and more subtle) part of Hirsch's argument then deals with the task of strengthening the modulus d by a factor 2, and is correct, apart from relying on the unsubstantiated Claim 3.

References

[1] W. Burnside, *Theory of Groups of Finite Order*, Dover Publications, 1955.

[2] L. M. Butler, "A unimodality result in the enumeration of subgroups of a finite abelian group", *Proc. Am. Math. Soc.* **101** (1987), no. 4, p. 771-775.

[3] J. Delsarte, "Fonctions de Möbius sur les groupes abeliens finis", *Ann. Math.* **49** (1948), p. 600-609.

[4] W. Feit, J. G. Thompson, "Solvability of groups of odd order", *Order* **13** (1963), p. 775-1029.

[5] P. Hall, "A note on soluble groups", *J. Lond. Math. Soc.* **3** (1928), p. 98-105.

[6] ———, "The eulerian functions of a group", *Q. J. Math., Oxf. Ser.* **7** (1936), p. 134-151.

[7] K. A. Hirsch, "On a theorem of Burnside", *Q. J. Math.* **1** (1950), p. 97-99.

[8] J. Poland, "Two problems of finite groups with k conjugate classes", *J. Aust. Math. Soc.* **8** (1968), p. 49-55.

[9] H. Wielandt, "Zum Satz von Sylow", *Math. Z.* **60** (1954), p. 407-408.