PARITY PATTERNS ASSOCIATED WITH LIFTS OF HECKE GROUPS

CHRISTIAN KRATTENTHALER† AND THOMAS W. MÜLLER

Abstract. Let q be an odd prime, m a positive integer, and let $\Gamma_m(q)$ be the group generated by two elements x and y subject to the relations $x^{2m} = y^{qm} = 1$ and $x^2 = y^q$; that is, $\Gamma_m(q)$ is the free product of two cyclic groups of orders $2m$ respectively qm, amalgamated along their subgroups of order m. Our main result determines the parity behaviour of the generalized subgroup numbers of $\Gamma_m(q)$ which were defined in [T. W. Müller, *Adv. in Math.* **153** (2000), 118–154], and which count all the homomorphisms of index n subgroups of $\Gamma_m(q)$ into a given finite group H, in the case when $\gcd(m, |H|) = 1$. This computation depends upon the solution of three counting problems in the Hecke group $\mathfrak{H}(q) = C_2 * C_q$: (i) determination of the parity of the subgroup numbers of $\mathfrak{H}(q)$; (ii) determination of the parity of the number of index n subgroups of $\mathfrak{H}(q)$ which are isomorphic to a free product of copies of C_2 and of C_∞; (iii) determination of the parity of the number of index n subgroups in $\mathfrak{H}(q)$ which are isomorphic to a free product of copies of C_q. The first problem has already been solved in [T. W. Müller, in: *Groups: Topological, Combinatorial and Arithmetic Aspects*, (T. W. Müller ed.), LMS Lecture Notes Series 311, Cambridge University Press, Cambridge, 2004, pp. 327–374]. The bulk of our paper deals with the solution of Problems (ii) and (iii).

1. Introduction

1.1. The study of congruences for subgroup numbers and related numerical quantities of groups is almost as old as group theory itself. The reader might think for instance of Frobenius' refinement in [8] of one of Sylow's fundamental theorems:

> (I) *the number $N_{p,r}(G)$ of subgroups of order p^r in a finite group G, whose order is divisible by p^r, satisfies $N_{p,r}(G) \equiv 1 \bmod p$.*

Related results concern the number of solutions of equations in finite groups. The model result here is again due to Frobenius, [9]:

> (II) *the number of solutions of the equation $x^m = 1$ in a finite group G is a multiple of* $\gcd(m, |G|)$.

2000 *Mathematics Subject Classification.* Primary 20E06; Secondary 05A15 05E99 16W22 20E07.

Key words and phrases. modular group, Hecke groups, amalgamated products, generalized subgroup numbers, parity patterns, involution numbers, Fermat primes.

†Research partially supported by the Austrian Science Foundation FWF, grant S9607-N13, in the framework of the National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

The last result was considerably extended and sharpened by P. Hall [14], building heavily on his groundbreaking work [13] concerning the structure of finite p-groups.

From a somewhat more abstract point of view, Frobenius' theorem (II) provides congruences for the number of homomorphisms of a finite cyclic group into a finite group G; and it is this point of view, which explains the connection between results of types (I) and (II). Certain sequences $\{G_n\}_{n\geq 0}$ of finite groups, like the sequence $G_n = S_n$ of symmetric groups or, more generally, a sequence of full monomial groups $G_n = H \wr S_n$, have the power of relating the enumeration of finite index subgroups by index (or similar counting functions) in an arbitrary finitely generated group Γ to the counting of homomorphisms $\Gamma \to G_n$. On the level of generating functions, this relationship is of exponential type; see Formula (5.3) for a concrete example in this direction.

To some extent, divisibility properties of subgroup numbers of a (finitely generated) infinite group may be viewed as a kind of analogue to these classical results for finite groups. Further motivation comes from *subgroup growth theory*, which studies growth, asymptotics, and more delicate number-theoretic properties of subgroup counting functions; cf. the monograph [17] for an overview of results up to about 2002. As far as divisibility properties are concerned, it was a, by now classical, result of Stothers concerning the modular group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, which prompted the quest that led to the delicate congruence patterns exhibited by Hecke groups and other free products. Stothers [33] showed that

> (III) *the number of index n subgroups in the modular group is odd if, and only if, n is of the form 2-power minus 3 or 2-power minus 6.*

The present paper continues this line of research by investigating the parity of (generalized) subgroup numbers of certain free products with amalgamation, which may be viewed as lifts of an underlying Hecke group. We now turn to a more precise description of the contents of this paper.

1.2. For an odd prime q, let

$$\mathfrak{H}(q) = \left\langle x, y \,\middle|\, x^2 = y^q = 1 \right\rangle \cong C_2 * C_q \tag{1.1}$$

be the standard Hecke group attached to q, and for a positive integer m, let

$$\Gamma_m = \Gamma_m(q) = \left\langle x, y \,\middle|\, x^{2m} = y^{qm} = 1,\ x^2 = y^q \right\rangle \cong C_{2m} \underset{C_m}{*} C_{qm}$$

be the associated sequence of lifts in the sense of [22, Eq. (40)]. Moreover, for a finitely generated group Γ, a finite group H, and a positive integer n, set

$$s_\Gamma^H(n) := \sum_{(\Gamma:\Delta)=n} |\operatorname{Hom}(\Delta, H)|.$$

The family $\{s_\Gamma^H(n)\}_{n,H}$ is the collection of *generalized subgroup numbers* of Γ. For $H = \{1\}$, the quantity $s_\Gamma^H(n)$ is the number of index n subgroups of Γ, which we denote by $s_\Gamma(n)$.

The present paper focusses on the parity behaviour of the numbers $s_\Gamma^H(n)$ in the case when $\Gamma = \Gamma_m(q)$ for m, q as above.

The systematic investigation of divisibility properties of subgroup counting functions begins with [28] (which had circulated in the subgroup growth community for some years), where the parity of $s_q(n) := s_{\mathfrak{H}(q)}(n)$ and of the number of free subgroups in $\mathfrak{H}(q)$ of given finite index is determined. These results have been generalized to larger classes of groups and primes not necessarily equal to 2 in [26, 29]. For a survey of these and related developments up to 2001, the reader may consult [27].

The present paper is a first attempt to study divisibility properties of (generalized) subgroup numbers for amalgamated products. Our main result (see Theorem 26 in Section 6) determines the parity behaviour of the generalized subgroup numbers $s^H_{\Gamma_m(q)}(n)$ in the case when $\gcd(m, |H|) = 1$. As Proposition 1 in the next section shows, this computation can be reduced to the solution of three counting problems in the Hecke group $\mathfrak{H}(q) = C_2 * C_q$:

(i) determination of the parity of the subgroup numbers $s_q(n)$ of $\mathfrak{H}(q)$;
(ii) determination of the parity of the numbers $M_q(n)$, where, by definition, $M_q(n)$ is the number of index n subgroups of $\mathfrak{H}(q)$ isomorphic to a free product of copies of C_2 and of C_∞;
(iii) determination of the parity of the numbers $N_q(n)$, where, by definition, $N_q(n)$ is the number of index n subgroups of $\mathfrak{H}(q)$ isomorphic to a free product of copies of C_q.

The first problem has already been solved in [28, Cor. 4]. The corresponding result is recalled here as Theorem 2 in the next section. Problem (ii) is solved in Theorem 16 in Section 4, which, perhaps somewhat surprisingly, shows that the numbers $M_q(n)$ are always even, and Problem (iii) is solved in Theorem 24 in Section 5.

The purpose of Section 3 is to develop in some detail the language of coset diagrams for the groups $\mathfrak{H}(q)$, in order to prepare for the proof of Theorem 16. This proof needs several partial results, which are the subject of Section 4. The first observation is that $M_q(n) = 0$ if q does not divide n, see (4.2). It therefore suffices to investigate the parity of the numbers $M_q(qk)$, where k is some positive integer. The enumerative relation between the coset diagrams and subgroup numbers is made precise in Subsection 4.1. This is done in greater generality than actually needed in our paper, in order to record the corresponding facts for possible use elsewhere. Lemma 6 expresses the numbers of index n subgroups of $\mathfrak{H}(q)$ which are isomorphic to $C_2^{*\lambda} * C_q^{*\mu} * F_\nu$ for fixed λ, μ, ν in terms of the number of certain mixed graphs. The enumeration of these graphs is subsequently reduced in Lemma 7 to graphs where the number of vertices is divisible by q. Then Corollary 8 summarizes specifically the implications for the subgroup numbers $M_q(qk)$ and $s_q(n)$. The main result of Subsection 4.2 is an explicit formula for the number of (mixed) graphs that appear in the corollary, see Proposition 9. This formula allows us to undertake a 2-adic study of the numbers $M_q(qk)$ for $q \geq 5$ in Subsection 4.3, by using known results on the 2-adic valuation of the number of involutions in symmetric groups. The corresponding result, which we prove in Proposition 12, is stronger than actually needed, as it exhibits a rapidly growing lower bound for the 2-adic valuation of the numbers $M_q(qk)$. On the other hand, a similar result cannot be expected for $q = 3$. Moreover, our explicit formula from Subsection 4.2 does not seem to be suited for the 2-adic analysis in this case. Instead, we use results of Stothers [33] to prove in Proposition 15, also in Subsection 4.3, that $M_3(3k)$ is even as well.

Section 5 puts together the ingredients for the proof of Theorem 24. The starting point is the observation that the parity of $N_q(n)$ is the same as the parity of the generalized subgroup numbers $s_q^H(n) := s_{\mathfrak{H}(q)}^H(n)$ with $|H|$ even, see (5.2). Just as subgroup numbers are connected with the enumeration of permutation representations, by [23, Cor. 1] the generalized subgroup numbers $s_\Gamma^H(n)$ of a finitely generated group Γ are related to the function $|\operatorname{Hom}(\Gamma, H \wr S_n)|$, counting monomial representations of Γ, via an identity of exponential type, which is restated here in (5.3). This identity is exploited in Subsections 5.1–5.3 to compute the generalized subgroup numbers $s_q^H(n)$ via a generating function approach, and to determine their parity in the case when H has even order in Subsection 5.5, thereby also determining the parity of $N_q(n)$. As a side result, we actually obtain a formula leading to an integral recurrence relation for the numbers $s_q^H(n)$, $n = 0, 1, \dots$, for each fixed q; see (5.26). This aspect is illustrated in Subsection 5.4 with the modular group $\mathfrak{H}(3)$; see Proposition 23.

Since the proofs of some auxiliary results in Sections 4 and 5 are tedious, involving however relatively straightforward calculations, we have put these proofs in an appendix, so that they do not distract from or obscure the main line of argument.

The final section, Section 6, contains our main result, Theorem 26, determining the parity behaviour of the generalized subgroup numbers $s_{\Gamma_m(q)}^H(n)$ in the case when $\gcd(m, |H|) = 1$, as well as its specialization to the case when q is a Fermat prime, in which case one can be much more precise (see Corollary 27), together with further simplifications when m and/or n satisfy some more specific properties.

2. A reduction result

For an odd prime q, let $\Gamma_m = \Gamma_m(q)$ be as in the introduction. We note that $\Gamma_m(q) \not\cong \Gamma_{m'}(q')$ for $(m, q) \neq (m', q')$. In this section we will show that the parity behaviour of the generalized subgroup numbers of these groups can be computed in terms of certain subgroup numbers pertaining to the base group $\mathfrak{H}(q)$; see Proposition 1.

Set
$$\zeta := x^2 = y^q,$$
so that ζ is a primitive element for the centre of Γ_m. For a positive integer n, a divisor d of m, and a finite group H, define
$$s_{\Gamma_m}^H(d, n) := \sum_{\substack{\Delta \\ (\Gamma_m : \Delta) = n \\ \Delta \cap \langle \zeta \rangle = \langle \zeta^{m/d} \rangle}} |\operatorname{Hom}(\Delta, H)|,$$
so that
$$s_{\Gamma_m}^H(n) = \sum_{d \mid m} s_{\Gamma_m}^H(d, n). \tag{2.1}$$

In what follows, we shall find it necessary to suppose that $\gcd(m, |H|) = 1$. Under the natural projection

$$\pi_d : \Gamma_m \longrightarrow \Gamma_m \big/ \big\langle \zeta^{m/d} \big\rangle \cong \Gamma_{m/d}$$

the subgroups Δ of index n in Γ_m having the property that $\Delta \supseteq \big\langle \zeta^{m/d} \big\rangle$ correspond bijectively to the totality of index n subgroups in $\Gamma_{m/d}$. Moreover, since $\gcd(m, |H|) = 1$, every homomorphism $\varphi : \Delta \to H$ factors through the canonical projection $\pi_d^\Delta : \Delta \to \Delta/\langle \zeta^{m/d} \rangle$. Hence, for $d \mid m$,

$$\begin{aligned} s^H_{\Gamma_{m/d}}(n) &= \sum_{\substack{\bar{\Delta} \\ (\Gamma_{m/d}:\bar{\Delta})=n}} |\operatorname{Hom}(\bar{\Delta}, H)| \\ &= \sum_{\substack{\Delta \\ (\Gamma_m:\Delta)=n \\ \Delta \supseteq \langle \zeta^{m/d} \rangle}} |\operatorname{Hom}(\Delta, H)| \\ &= \sum_{\substack{d' \\ d \mid d' \mid m}} \sum_{\substack{\Delta \\ (\Gamma_m:\Delta)=n \\ \Delta \cap \langle \zeta \rangle = \langle \zeta^{m/d'} \rangle}} |\operatorname{Hom}(\Delta, H)|, \end{aligned}$$

and thus

$$s^H_{\Gamma_{m/d}}(n) = \sum_{\substack{d' \\ d \mid d' \mid m}} s^H_{\Gamma_m}(d', n), \quad d \mid m. \tag{2.2}$$

Fixing q, m, n, and H, and setting

$$g(x) := \left\{ \begin{matrix} s^H_{\Gamma_{m/x}}(n), & x \mid m \\ 0, & \text{otherwise} \end{matrix} \right\} \quad (x \in \mathbb{N}),$$

$$f(x) := \left\{ \begin{matrix} s^H_{\Gamma_m}(x, n), & x \mid m \\ 0, & \text{otherwise} \end{matrix} \right\} \quad (x \in \mathbb{N}),$$

and letting P be the poset with ground-set $\mathbb{N}$ and partial order defined by $x \leq y$ if, and only if, $y \mid x$, Equation (2.2) translates into

$$g(x) = \sum_{y \leq x} f(y), \quad x \in P,$$

and, by definition of the function f, we have $f(x) = 0$ unless $x \geq m$. By Möbius inversion (cf. [31, Propositions 2–3]), we find that

$$s^H_{\Gamma_m}(d, n) = \sum_{\substack{d' \\ d \mid d' \mid m}} \mu_P(d, d')\, s^H_{\Gamma_{m/d'}}(n), \quad d \mid m,$$

where $\mu_P(x, y)$ is the Möbius function in the poset P. It is well-known that $\mu_P(x, y) = \mu(x/y)$ for $x \leq y$ (that is, $y \mid x$), where $\mu(\cdot)$ is the classical Möbius function of number theory. Hence, we have

$$s^H_{\Gamma_m}(d,n) = \sum_{\substack{d' \\ d \mid d' \mid m}} \mu(d'/d)\, s^H_{\Gamma_{m/d'}}(n), \quad d \mid m. \tag{2.3}$$

On the other hand, if we set $d = 1$ in (2.3) and apply Möbius inversion in the other direction, we obtain

$$s^H_{\Gamma_m}(n) = \sum_{d \mid m} s^H_{\Gamma_d}(1,n), \quad \gcd(m, |H|) = 1. \tag{2.4}$$

Our next task is to compute $s^H_{\Gamma_m}(1,n)$ modulo 2. If there exists a subgroup $\Delta \le \Gamma_m$ with $(\Gamma_m : \Delta) = n$ and $\Delta \cap \langle \zeta \rangle = 1$, then

$$\widetilde{\Delta} := \Delta \cdot \langle \zeta \rangle = \Delta \times \langle \zeta \rangle;$$

hence, m must divide n. Thus,

$$s^H_{\Gamma_m}(1,n) = 0, \quad m \nmid n. \tag{2.5}$$

Suppose now that $m \mid n$. Given a subgroup $\Delta \le \Gamma_m$ with $(\Gamma_m : \Delta) = n$ and $\Delta \cap \langle \zeta \rangle = 1$, consider the diagram

$$\begin{tikzcd}
\Delta \arrow[r, "m"] \arrow[d, "\pi_m"'] & \widetilde{\Delta} = \Delta \cdot \langle \zeta \rangle \arrow[r, "n/m"] \arrow[d, "\pi_m"'] & \Gamma_m \arrow[d, "\pi_m"] \\
\bar{\Delta} \arrow[r, "\mathrm{id}"] & \bar{\Delta} \arrow[r, "n/m"'] & \bar{\Gamma} \cong \Gamma_1 = \mathfrak{H}(q)
\end{tikzcd} \tag{2.6}$$

(a number next to an arrow indicates the index of the corresponding embedding). Reading Diagram (2.6) from bottom to top, we can describe Δ as a complement to $\langle \zeta \rangle$ in the lift $\widetilde{\Delta} = \pi_m^{-1}(\bar{\Delta})$ of a subgroup $\bar{\Delta}$ in $\bar{\Gamma} \cong \mathfrak{H}(q)$ with $(\bar{\Gamma} : \bar{\Delta}) = n/m$. Hence,

$$s^H_{\Gamma_m}(1,n) = \sum_{\substack{\bar{\Delta} \\ (\bar{\Gamma}:\bar{\Delta}) = n/m}} |\operatorname{Hom}(\bar{\Delta}, H)| \cdot |\mathfrak{C}(\pi_m^{-1}(\bar{\Delta}); \langle \zeta \rangle)|, \quad m \mid n, \tag{2.7}$$

where $\mathfrak{C}(\pi_m^{-1}(\bar{\Delta}); \langle \zeta \rangle)$ is the (possibly empty) set of complements of $\langle \zeta \rangle$ in $\pi_m^{-1}(\bar{\Delta})$.

Given $\bar{\Delta} \le \bar{\Gamma}$ of index n/m, when does $\langle \zeta \rangle$ split in $\pi_m^{-1}(\bar{\Delta})$? To answer this question, we make use of the long exact (Mayer–Vietoris) sequence

$$\cdots \to H^k(G;A) \underset{(res,res)}{\longrightarrow} H^k(G_1;A) \oplus H^k(G_2;A) \underset{(res,-res)}{\longrightarrow} H^k(S;A) \underset{\delta}{\longrightarrow} H^{k+1}(G;A) \to \cdots \tag{2.8}$$

associated with an amalgamated product $G = G_1 \underset{S}{*} G_2$ and a left RG-module A; cf. [2, Theorem 2.10] or [4, Theorem 2]. By the Kurosh subgroup theorem, $\bar{\Delta}$ is of the form

$$\bar{\Delta} \cong C_2^{*\lambda(\bar{\Delta})} * C_q^{*\mu(\bar{\Delta})} * F_{\nu(\bar{\Delta})}$$

with non-negative integers $\lambda(\bar{\Delta}), \mu(\bar{\Delta}), \nu(\bar{\Delta})$ (these cardinal numbers are seen to be finite through a comparison of Euler characteristics; cf. Equation (3.3) below). Applying (2.8) together with the fact that every extension by a free group splits, we see that

$$H^2(\bar{\Delta}; C_m) \cong \lambda(\bar{\Delta}) H^2(C_2; C_m) \oplus \mu(\bar{\Delta}) H^2(C_q; C_m). \tag{2.9}$$

We now distinguish four cases.

(i) $2 \nmid m$ *and* $q \mid m$. Suppose that, for some subgroup $\bar{\Delta} \leq \bar{\Gamma}$ of index $(\bar{\Gamma} : \bar{\Delta}) = n/m$, $\langle \zeta \rangle$ splits in $\pi_m^{-1}(\bar{\Delta})$, and that $\mu(\bar{\Delta}) > 0$. Then $C_m \times C_q$, an Abelian group of rank 2, would embed into Γ_m, which is impossible. Hence, if $\langle \zeta \rangle$ splits in $\pi_m^{-1}(\bar{\Delta})$, then $\mu(\bar{\Delta}) = 0$. Conversely, if $\mu(\bar{\Delta}) = 0$, then every extension of C_m by $\bar{\Delta}$ splits, since $H^2(C_2; C_m) = 0$ by the Schur–Zassenhaus theorem plus the fact that $2 \nmid m$; cf. for instance [34, Chapter 3]. To summarize, we have shown that

$$\textit{if } 2 \nmid m \textit{ and } q \mid m, \textit{ then } \langle \zeta \rangle \textit{ splits in } \pi_m^{-1}(\bar{\Delta}) \textit{ if, and only if, } \mu(\bar{\Delta}) = 0. \tag{2.10}$$

(ii) $2 \nmid m$ *and* $q \nmid m$. In this case, again by the Schur–Zassenhaus theorem and the isomorphism (2.9), we find that $H^2(\bar{\Delta}; C_m) = 0$. Hence,

$$\begin{aligned}&\textit{if } 2 \nmid m \textit{ and } q \nmid m, \textit{ then the lift } \pi_m^{-1}(\bar{\Delta})\\ &\qquad\qquad\qquad \textit{of every subgroup } \bar{\Delta} \leq_{n/m} \bar{\Gamma} \textit{ splits the centre } \langle \zeta \rangle.\end{aligned} \tag{2.11}$$

(iii) $2 \mid m$ *and* $q \nmid m$. Arguing as in (i), we find that

$$\textit{if } 2 \mid m \textit{ and } q \nmid m, \textit{ then } \langle \zeta \rangle \textit{ splits in } \pi_m^{-1}(\bar{\Delta}) \textit{ if, and only if, } \lambda(\bar{\Delta}) = 0. \tag{2.12}$$

(iv) $2q \mid m$. In this case, we find by similar arguments that

$$\textit{if } 2q \mid m, \textit{ then } \langle \zeta \rangle \textit{ splits in } \pi_m^{-1}(\bar{\Delta}) \textit{ if, and only if, } \lambda(\bar{\Delta}) = \mu(\bar{\Delta}) = 0. \tag{2.13}$$

Given the information in (2.10)–(2.13), we can now evaluate the quantities $s_{\Gamma_m}^H(1, n)$ modulo 2 in terms of data associated with the base group $\bar{\Gamma}$ alone. Denote by $M_q(n)$ the number of index n subgroups $\bar{\Delta}$ in $\bar{\Gamma} = \mathfrak{H}(q)$ with the property that $\mu(\bar{\Delta}) = 0$, by $N_q(n)$ the number of subgroups of index n in $\bar{\Gamma}$ which are isomorphic to a free power of C_q, and recall that $s_q(n)$ denotes the number of index n subgroups in $\mathfrak{H}(q)$.

Proposition 1. *For $m, n \geq 1$, an odd prime q, and a finite group H, we have*

$$s_{\Gamma_m(q)}^H(1, n) \equiv \left\{ \begin{array}{ll} N_q(n/m); & 2 \mid m \mid n \textit{ and } q \nmid m \\ s_q(n/m); & 2 \nmid m, q \nmid m, m \mid n, \textit{ and } 2 \nmid |H| \\ N_q(n/m); & 2 \nmid m, q \nmid m, m \mid n, \textit{ and } 2 \mid |H| \\ M_q(n/m); & q \mid m \mid n, 2 \nmid m, \textit{ and } 2 \nmid |H| \\ 0; & \textit{otherwise} \end{array} \right\} \mod 2.$$

Proof. This is straightforward. For instance, in the first case ($2 \mid m \mid n$ and $q \nmid m$), the computation runs as follows:

$$\begin{aligned}
s^H_{\Gamma_m}(1,n) &= \sum_{\substack{\bar\Delta\\ (\bar\Gamma:\bar\Delta)=n/m}} |\operatorname{Hom}(\bar\Delta,H)|\cdot|\mathfrak{C}(\pi_m^{-1}(\bar\Delta);\langle\zeta\rangle)|\\
&= \sum_{\substack{\bar\Delta\\ (\bar\Gamma:\bar\Delta)=n/m\\ \lambda(\bar\Delta)=0}} |\operatorname{Hom}(\bar\Delta,H)|\cdot|\operatorname{Hom}(\bar\Delta,C_m)|\\
&= \sum_{\substack{\bar\Delta\\ (\bar\Gamma:\bar\Delta)=n/m\\ \lambda(\bar\Delta)=0}} m^{\nu(\bar\Delta)}\,|\operatorname{Hom}(\bar\Delta,H)|\\
&\equiv \sum_{\substack{\bar\Delta\\ (\bar\Gamma:\bar\Delta)=n/m\\ \lambda(\bar\Delta)=\nu(\bar\Delta)=0}} |\operatorname{Hom}(\bar\Delta,H)|\\
&\equiv \sum_{\substack{\bar\Delta\\ (\bar\Gamma:\bar\Delta)=n/m\\ \lambda(\bar\Delta)=\nu(\bar\Delta)=0}} 1\\
&= N_q(n/m),
\end{aligned}$$

where $\bar\Gamma = \mathfrak{H}(q)$, and where we have made use of (2.7), (2.12), and the fact that

$$|\operatorname{Hom}(C_q,H)| = 1 \,+\, (q-1)\cdot\left|\left\{U\le H:\, U\cong C_q\right\}\right|$$

is always odd. Computations for the other cases are similar, and are left to the reader. □

Combining Equation (2.4) with Proposition 1, the calculation of the generalized subgroup numbers $s^H_{\Gamma_m(q)}(n)$ modulo 2 has been reduced to the mod 2 calculation of the numbers $s_q(n)$, $M_q(n)$, and $N_q(n)$. The first problem has already been solved in [28, Cor. 4]. The result reads as follows.

Theorem 2. *Let q be an odd prime. Then*

$$s_q(n)\equiv 1 \pmod 2 \quad \textit{if, and only if,} \quad n=1+2(q-1)\eta \textit{ or } n=2+4(q-1)\eta, \textit{ where}$$
$$\mathfrak{s}_2((q-1)\eta+1)=\mathfrak{s}_2(\eta)+\mathfrak{s}_2((q-2)\eta+1), \quad \textit{and } \eta\in\mathbb{N}_0. \tag{2.14}$$

Here, $\mathfrak{s}_2(x)$ denotes the sum of digits in the binary expansion of the positive integer x. In particular, if q is a Fermat prime, then

$$s_q(n)\equiv 1 \pmod 2 \quad \textit{if, and only if,}$$
$$n=\frac{2(q-1)^\sigma-q}{q-2} \textit{ or } n=\frac{4(q-1)^\sigma-2q}{q-2} \textit{ for some } \sigma\ge 1. \tag{2.15}$$

3. Coset diagrams associated with Hecke groups

There is a well-known connection between the subgroups of index n in a group Γ and the transitive permutation representations of Γ of degree n, which is sometimes useful to obtain information concerning various subgroup numbers of Γ. As the details of this relationship are somewhat hard to find in the literature, we provide a brief discussion of the general facts in Subsection 3.1 for the convenience of the reader, after which we focus on the special case of Hecke groups and their diagrams in Subsection 3.2. This discussion will provide the basis for the mod 2 determination of the numbers $M_q(n)$ in Section 4.

3.1. Transitive permutation representations versus finite-index subgroups. Here, and in the rest of the paper, for a non-negative integer n, the symbol $[n]$ will always denote the standard set $\{1, 2, \ldots, n\}$ of size n. Let $S_n = \mathrm{Sym}([n])$ be the symmetric group of degree n acting on the standard set $[n]$, endowed with geometric multiplication, let $U_n = \mathrm{stab}_{S_n}(1)$ be the stabilizer of the letter 1 in S_n, and, for a group Γ, denote by $T_n(\Gamma)$ the set of all transitive permutation representations $\varphi : \Gamma \to S_n$. For a permutation $\sigma \in S_n$, let ι_σ be the inner automorphism of S_n induced by σ,

$$\iota_\sigma(\pi) = \sigma \circ \pi \circ \sigma^{-1}, \quad \pi \in S_n,$$

and define a left action of U_n on $T_n(\Gamma)$ via the commutative diagram

$$\begin{tikzcd} \Gamma \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_\Gamma"'] & S_n \arrow[d, "\iota_\sigma"] \\ \Gamma \arrow[r, "\sigma\cdot\varphi"'] & S_n \end{tikzcd} \qquad (\sigma \in U_n,\ \varphi \in T_n(\Gamma)),$$

where id_Γ is the identity map on Γ. The basic observation is now the following.

Proposition 3. (i) *The action of U_n on $T_n(\Gamma)$ is free; in particular, each equivalence class of $T_n(\Gamma)$ modulo U_n contains precisely $(n-1)!$ elements.*

(ii) *There is a one-to-one correspondence between the subgroups of index n in Γ and the equivalence classes of $T_n(\Gamma)$ under the action of U_n.*

Proof. (i) Suppose that $\sigma \cdot \varphi = \varphi$ for some $\sigma \in U_n$ and some $\varphi \in T_n(\Gamma)$. By transitivity, given $j \in [n]$, there exists $\gamma_j \in \Gamma$ such that $\varphi(\gamma_j)(1) = j$, and hence

$$\begin{aligned} \sigma(j) &= \sigma(\varphi(\gamma_j)(\sigma^{-1}(1))) \\ &= (\sigma \cdot \varphi)(\gamma_j)(1) \\ &= \varphi(\gamma_j)(1) \\ &= j. \end{aligned}$$

Since j was arbitrary, we conclude that $\sigma = \mathrm{id}_{[n]}$; thus, the action of U_n on $T_n(\Gamma)$ is free as claimed. The particular statement follows from this and the fact that $U_n \cong S_{n-1}$.

(ii) Given $\varphi \in T_n(\Gamma)$, the subgroup

$$\Delta_\varphi := \mathrm{stab}_\varphi(1) = \varphi^{-1}(U_n)$$

has index n in Γ, since a set of elements $\{\gamma_1, \gamma_2, \dots, \gamma_n\}$ chosen as in Part (i) forms a system of (left) coset representatives for Γ modulo Δ_φ. Further, if $\varphi_2 = \sigma \cdot \varphi_1$ for some $\sigma \in U_n$, then

$$\begin{aligned}\Delta_{\varphi_2} &= \varphi_2^{-1}(U_n)\\ &= (\iota_\sigma \circ \varphi_1)^{-1}(U_n)\\ &= \varphi_1^{-1}(\iota_{\sigma^{-1}}(U_n))\\ &= \varphi_1^{-1}(U_n)\\ &= \Delta_{\varphi_1}.\end{aligned}$$

Hence, the assignment $\varphi \mapsto \Delta_\varphi$ induces a well-defined map

$$\Phi : U_n\backslash T_n(\Gamma) \longrightarrow \big\{\Delta :\ \Delta \le \Gamma,\ (\Gamma : \Delta) = n\big\}.$$

A subgroup $\Delta \le \Gamma$ of index n in Γ induces a transitive Γ-action by left multiplication on the n-set Γ/Δ of left cosets which, after suitable renaming, becomes a transitive Γ-action on $[n]$ with the property that $\operatorname{stab}(1) = \Delta$. This shows that Φ is surjective.

To prove injectivity, suppose that $\varphi_1, \varphi_2 \in T_n(\Gamma)$ are two transitive permutation representations of Γ on $[n]$, such that $\Delta_{\varphi_1} = \Delta_{\varphi_2}$. As before, choose elements $\gamma_1, \gamma_2, \dots, \gamma_n \in \Gamma$ such that

$$\varphi_1(\gamma_j)(1) = j, \quad 1 \le j \le n,$$

and define a permutation $\sigma_0 \in U_n$ via

$$\sigma_0(j) := \varphi_2(\gamma_j)(1), \quad 1 \le j \le n.$$

Then, for $\gamma \in \Gamma$ and $j \in [n]$, and with $\gamma\gamma_j \underset{\Delta_{\varphi_1}}{\sim} \gamma_k$, we have

$$\begin{aligned}\sigma_0(\varphi_1(\gamma)(j)) &= \sigma_0(\varphi_1(\gamma)(\varphi_1(\gamma_j)(1)))\\ &= \sigma_0(\varphi_1(\gamma\gamma_j)(1))\\ &= \sigma_0(\varphi_1(\gamma_k)(1))\\ &= \sigma_0(k)\\ &= \varphi_2(\gamma_k)(1)\\ &= \varphi_2(\gamma\gamma_j)(1)\\ &= \varphi_2(\gamma)(\varphi_2(\gamma_j)(1))\\ &= \varphi_2(\gamma)(\sigma_0(j)).\end{aligned}$$

Since j and γ were arbitrary, this shows that $\sigma_0 \cdot \varphi_1 = \varphi_2$; that is, φ_1 and φ_2 are equivalent under the action of U_n, as required. □

3.2. The case of Hecke groups. Now let q be an odd prime number, and let

$$\mathfrak{H}(q) = \big\langle x, y \,\big|\, x^2 = y^q = 1 \big\rangle \tag{3.1}$$

be the standard Hecke group attached to q. By Kurosh's subgroup theorem, a subgroup $\Delta \le \mathfrak{H}(q)$ is of the form

$$\Delta \cong C_2^{*\lambda(\Delta)} * C_q^{*\mu(\Delta)} * F_{\nu(\Delta)} \tag{3.2}$$

with cardinal numbers $\lambda(\Delta), \mu(\Delta)$, and $\nu(\Delta)$. Moreover, if Δ has finite index in $\mathfrak{H}(q)$, comparing the Euler characteristic of Δ with that of $\mathfrak{H}(q)$ shows that $\lambda(\Delta), \mu(\Delta), \nu(\Delta)$ are finite, and are connected to the index $(\mathfrak{H}(q) : \Delta)$ via the relation

$$q\lambda(\Delta) + 2(q-1)\mu(\Delta) + 2q(\nu(\Delta) - 1) = (q-2)(\mathfrak{H}(q) : \Delta). \tag{3.3}$$

Our next result which, in the case of the modular group, goes back to Millington [19, Theorem 1], provides a refinement of the bijection Φ in the proof of Proposition 3(ii) by taking into account the isomorphism type

$$\mathbf{t}(\Delta) = (\lambda(\Delta), \mu(\Delta), \nu(\Delta))$$

of a finite-index subgroup Δ in $\mathfrak{H}(q)$.

Proposition 4. *Let q be an odd prime, let Δ be a subgroup of finite index n in $\mathfrak{H}(q)$, and let $\varphi : \mathfrak{H}(q) \to S_n$ be a transitive permutation representation of $\mathfrak{H}(q)$ such that $\Delta_\varphi = \Delta$. Then $\varphi(x)$ has precisely $\lambda(\Delta)$ fixed points, and $\varphi(y)$ has exactly $\mu(\Delta)$ fixed points, where x, y are as in* (3.1).

Proof. As in the proof of Proposition 3, choose elements $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathfrak{H}(q)$ such that

$$\varphi(\gamma_j)(1) = j, \quad 1 \leq j \leq n;$$

i.e., $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ is a left transversal for $\mathfrak{H}(q)$ modulo Δ. The equation $\varphi(x)(j) = j$ is equivalent to the condition that $x^{\gamma_j} \in \Delta$; in particular, the assignment

$$j \mapsto \mathcal{C}_j := \left\{\delta^{-1} x^{\gamma_j} \delta : \delta \in \Delta\right\}$$

defines a mapping Φ_x from the set of fixed points of $\varphi(x)$ to the set of conjugacy classes of elements of order 2 in Δ. If

$$\mathcal{C} = \left\{\delta^{-1} x' \delta : \delta \in \Delta\right\} \subseteq \Delta$$

is such a conjugacy class, then x' is in Δ and has order 2; thus, by the torsion theorem for free products (cf., for instance, Theorem 1.6 in Chapter IV of [18]), there exists an element $\gamma = \gamma_j \delta$ such that

$$x' = \gamma^{-1} x \gamma = \delta^{-1} x^{\gamma_j} \delta.$$

It follows that $x^{\gamma_j} \in \Delta$, i.e., $\varphi(x)(j) = j$, and $\mathcal{C} = \mathcal{C}_j$; that is, Φ_x is surjective. To prove injectivity, let j and k be fixed points of $\varphi(x)$, and suppose that $\mathcal{C}_j = \mathcal{C}_k$; that is,

$$\delta^{-1} x^{\gamma_j} \delta = x^{\gamma_k}.$$

Consequently, the element $\gamma_j \delta \gamma_k^{-1}$ centralizes the generator x, implying $\gamma_j \delta \gamma_k^{-1} = x^\epsilon$ with $\epsilon \in \{0, 1\}$ by [20, Cor. 4.1.6]. Hence,

$$j = \varphi(\gamma_j \delta \gamma_k^{-1})(k) = \varphi(x^\epsilon)(k) = k,$$

as desired. We conclude that the fixed points of $\varphi(x)$ are in one-to-one correspondence with the $\lambda(\Delta)$ conjugacy classes of elements of order 2 in Δ. By a similar argument, the fixed points of $\varphi(y)$ are in one-to-one correspondence with the $\mu(\Delta)$ conjugacy classes of cyclic subgroups of order q in Δ, completing the proof. $\square$

It is customary to translate these facts into a geometric language. To every transitive permutation representation $\varphi : \mathfrak{H}(q) \to S_n$ there corresponds a diagram D_φ consisting of n labelled vertices, red undirected loops, blue undirected loops, red undirected edges, and blue directed edges, constructed as follows: the vertices of D_φ are labelled with the elements of the standard set $[n]$; for $i, j \in [n]$ such that $\varphi(x)(i) = j$, the vertices labelled i and j are joined by an undirected red edge (a loop if $i = j$); for $i, j \in [n]$ with $i \neq j$ and $\varphi(y)(i) = j$, we draw a directed blue edge from vertex i to vertex j, while, for $i = j$, we attach an undirected blue loop to vertex i. In this way, the set $T_n(\mathfrak{H}(q))$ is in bijective correspondence with the set $\mathcal{D}_{n,q}$ of diagrams on n vertices labelled with the elements of the standard set $[n]$, such that

(a) each vertex has a red loop, or is incident with exactly one red edge,
(b) each vertex has a blue loop, or is contained in precisely one oriented blue q-gon,
(c) the red and blue edges together give a connected figure.

The elements of $\mathcal{D}_{n,q}$ are the *coset diagrams of order* n associated with the Hecke group $\mathfrak{H}(q)$. A permutation $\sigma \in S_n$ induces a map $\sigma : \mathcal{D}_{n,q} \to \mathcal{D}_{n,q}$; two diagrams D_1, D_2 are called equivalent, if $\sigma(D_1) = D_2$ for some permutation $\sigma \in U_n$. The set of orbits $U_n \backslash \mathcal{D}_{n,q}$ is in bijective correspondence with the subgroups of index n in $\mathfrak{H}(q)$, and each equivalence class of diagrams has $(n-1)!$ elements. Further, if D is a diagram corresponding to the index n subgroup $\Delta_D \leq \mathfrak{H}(q)$, then D contains precisely $\lambda(\Delta_D)$ red loops and $\mu(\Delta_D)$ blue loops. Our next result, while spelling out certain numerical constraints, also provides a geometric interpretation for the quantity $\nu(\Delta_D)$.

Proposition 5. *If $D \in \mathcal{D}_{n,q}$ is a diagram containing k blue q-gons and e red edges, and with associated subgroup Δ_D, then*

(i) $\frac{n}{q} \geq k \geq \dfrac{n-e-1}{q-1}$,
(ii) $\frac{n}{2} \geq e \geq n-(q-1)k-1$,
(iii) $e+(q-1)k-n+1 = \nu(\Delta_D)$.

Proof. If $n = 1$, then D consists of one vertex labelled 1, with a red and a blue loop attached to it. Thus, $k = e = 0$ and, by (3.3), $\nu(\Delta_D) = 0$. Similarly, for $n = 2$, the diagram D consists of two vertices labelled 1 and 2, respectively, each having a blue loop attached to it, and joined by a red edge. Thus, $k = 0$, $e = 1$, and, by (3.3), $\nu(\Delta_D) = 0$. One checks that in both cases assertions (i)–(iii) hold true. Hence, for the rest of the proof, we may assume that $n > 2$.

Since, by (b), the q-gons are disjoint, we must have $kq \leq n$; the $n - qk$ vertices not involved in a q-gon must carry blue loops. By (c), there exist at least $k-1$ red edges joining vertices of distinct blue q-gons, and a further $n - qk$ red edges, each joining a vertex with a blue loop to a vertex of a q-gon (here we need that $n > 2$). Thus, there are at least $n-(q-1)k-1$ red edges. Since

$$\mu(\Delta_D) = n - qk$$

and, in view of (a),

$$\lambda(\Delta_D) = n - 2e,$$

Equation (3.3) shows that indeed $e+(q-1)k-n+1 = \nu(\Delta_D)$. The remaining inequalities follow since $\lambda(\Delta_D), \nu(\Delta_D) \geq 0$. $\square$

It is not hard to see that, conversely, whenever inequalities (i) and (ii) are satisfied, a diagram D with specifications as described in Proposition 5 does indeed exist.

4. Counting finite-index subgroups in Hecke groups via coset diagrams

The main purpose of this section is to establish the fact that, for every odd prime q and each integer $n \geq 1$, we have

$$M_q(n) \equiv 0 \bmod 2, \tag{4.1}$$

so that these numbers do in fact not enter into the mod 2 calculation of $s^H_{\Gamma_m(q)}(n)$, despite their appearance in Proposition 1; cf. Theorem 16.

If Δ is a subgroup of index n in $\mathfrak{H}(q)$ with $\mu(\Delta) = 0$, then we must have $q \mid n$ by Equation (3.3) plus the fact that q is a prime. Hence,

$$M_q(n) = 0, \quad q \nmid n; \tag{4.2}$$

in particular, $M_q(n) \equiv 0 \pmod 2$ in this case. We are thus reduced to checking the case where $n = qk$ with $k \geq 1$. Using coset enumeration techniques, the numbers $M_q(qk)$ are expressed as a sum of certain combinatorially defined quantities $M_q(qk; e, k)$ divided by $q^{k-1}(k-1)!$, see Corollary 8(ii). As a next step, an explicit formula for $M_q(qk; e, k)$ is found in Proposition 9. Subsequently, this explicit formula is used to show that $M_q(qk)$ is always even for $q \geq 5$; see Proposition 12. Finally, the corresponding fact for $q = 3$ is established in Proposition 15, building on the work of Stothers [33]. A curious side result is Proposition 10, which provides a closed form product formula for $M_q(qk; e, k)$ in the minimal case $e = k - 1$. As already mentioned in the introduction, the next subsection addresses, in complete generality, the problem of enumerating the index n subgroups in $\mathfrak{H}(q)$ which are isomorphic to $C_2^{*\lambda} * C_q^{*\mu} * F_\nu$ for fixed λ, μ, ν.

4.1. Enumerating finite-index subgroups of given type. Let n, m_1, m_2 be integers with $n > 0$ and $m_1, m_2 \geq 0$. Suppose that we are given a set of m_2 disjoint oriented blue q-gons, the vertices of the i-th one being labelled $q(i-1)+1, \ldots, qi-1, qi$ in order, as well as $n - qm_2$ additional vertices labelled $qm_2 + 1, qm_2 + 2, \ldots, n$. We consider (mixed) graphs resulting from the previously described q-gons and additional vertices by drawing m_1 undirected red edges, such that each vertex is incident with at most one red edge, and such that a connected graph is obtained. (Here, for connectivity, *both* the blue and red edges are taken into account.) Let $\mathcal{M}_q(n; m_1, m_2)$ be the set of all these graphs, and let $M_q(n; m_1, m_2)$ be the cardinality of $\mathcal{M}_q(n; m_1, m_2)$.

Denote by $s_q(n; m_1, m_2)$ the number of index n subgroups Δ in $\mathfrak{H}(q)$ of representation type

$$\mathbf{m}(\Delta) = \begin{pmatrix} m_1 & n - 2m_1 \\ m_2 & n - qm_2 \end{pmatrix}; \tag{4.3}$$

that is, the generator x in (3.1) acts as a product of m_1 2-cycles and $n - 2m_1$ fixed points on the coset space $\mathfrak{H}(q)/\Delta$, while the generator y in (3.1) acts as a product of m_2 q-cycles and $n - qm_2$ fixed points on $\mathfrak{H}(q)/\Delta$. We note that in our situation the representation type $\mathbf{m}(\Delta)$ and the isomorphism type $\mathbf{t}(\Delta)$ of a finite index subgroup

Δ determine each other. More precisely, if Δ is of index n in $\mathfrak{H}(q)$, then $\mathbf{m}(\Delta)$ is given by (4.3) if and only if $\mathbf{t}(\Delta)$ is given by

$$\mathbf{t}(\Delta) = (n - 2m_1, n - qm_2, m_1 + (q-1)m_2 - n + 1). \tag{4.4}$$

The numbers $M_q(n; m_1, m_2)$ and $s_q(n; m_1, m_2)$ are related in the following way.

Lemma 6. *For an odd prime q and integers n, m_1, m_2 with $n > 0$ and $m_1, m_2 \geq 0$, we have*

$$s_q(n; m_1, m_2) = \frac{nM_q(n; m_1, m_2)}{q^{m_2} m_2!\,(n - qm_2)!}. \tag{4.5}$$

Proof. Clearly, a graph $G \in \mathcal{M}_q(n; m_1, m_2)$ can be made into a coset diagam $D \in \mathcal{D}_{n,q}$ by adding a red loop at each vertex not incident with a red edge and a blue loop at each vertex not incident with a blue q-gon. The subgroup Δ_D corresponding to such a diagram has index n and representation type $\left(\begin{smallmatrix} m_1 & n-2m_1 \\ m_2 & n-qm_2 \end{smallmatrix}\right)$. Conversely, such a subgroup leads to a graph $G \in \mathcal{M}_q(n; m_1, m_2)$ for *some* labelling of the vertices by deleting all red and blue loops in a corresponding coset diagram.

In order to construct all possible labellings, first choose labels for the vertices involved in some q-gon in $\binom{n}{qm_2}$ ways. These chosen labels can be used to label the m_2 q-gons in

$$\frac{1}{m_2!}\binom{qm_2}{q, \dots, q}(q-1)!^{m_2} = \frac{(qm_2)!}{m_2!\,q^{m_2}}$$

ways. On the other hand, there is only one way to label the additional $(n - qm_2)$ vertices by the remaining labels, these being completely indistinguishable. Hence, the number of coset diagrams corresponding to subgroups of index n and representation type $\left(\begin{smallmatrix} m_1 & n-2m_1 \\ m_2 & n-qm_2 \end{smallmatrix}\right)$ is

$$\binom{n}{qm_2}\frac{(qm_2)!}{m_2!\,q^{m_2}} M_q(n; m_1, m_2).$$

Our claim follows now from Proposition 3 upon little simplification. $\square$

Relation (4.5) allows us to compute the subgroup numbers $s_q(n; m_1, m_2)$ in terms of the geometrically defined quantities $M_q(n; m_1, m_2)$. As our next result shows, it is enough to consider the latter numbers in the case when $q \mid n$.

Lemma 7. *For an odd prime q and integers n, m_1, m_2 with $n > 0$ and $m_1, m_2 \geq 0$, we have*

$$M_q(n; m_1, m_2) = \frac{(2n - 2m_1 - qm_2)!}{(n - 2m_1)!} M_q(qm_2; m_1 + qm_2 - n, m_2). \tag{4.6}$$

Proof. Given a graph in $\mathcal{M}_q(n; m_1, m_2)$, removal of all vertices not involved in some q-gon together with all incident (red) edges leaves a graph in $\mathcal{M}_q(qm_2; m_1 + qm_2 - n, m_2)$. Conversely, starting from a graph in $\mathcal{M}_q(qm_2; m_1 + qm_2 - n, m_2)$, among the vertices involved in a q-gon there are $qm_2 - 2(m_1 + qm_2 - n) = 2n - 2m_1 - qm_2$ vertices not incident with a red edge. From these vertices we choose $n - qm_2$ vertices in $\binom{2n-2m_1-qm_2}{n-qm_2}$ ways and, having chosen them, we connect each of them by means of a red edge to exactly one of a new set of vertices labelled $\{qm_2 + 1, qm_2 + 2, \dots, n\}$. This last step can be done in $(n - qm_2)!$ different ways. Hence, in total we obtain the relation (4.6). $\square$

Since we shall make use of it later on, we point out that a combination of Lemmas 6 and 7 yields the relation

$$s_q(n;m_1,m_2)=\frac{n\,(2n-2m_1-qm_2)!}{q^{m_2}m_2!\,(n-qm_2)!\,(n-2m_1)!}M_q(qm_2;m_1+qm_2-n,m_2). \tag{4.7}$$

Corollary 8. (i) *Let k and e be integers with $k\ge 1$ and $0\le e\le qk/2$. Then the number of subgroups Δ in $\mathfrak{H}(q)$ of index qk and type*

$$\mathbf{t}(\Delta)=\big(qk-2e,0,e-k+1\big) \tag{4.8}$$

is

$$\frac{M_q(qk;e,k)}{q^{k-1}(k-1)!}.$$

In particular, we have

$$M_q\Big(2q(e-k)/(q-2);e,\frac{2(e-k)}{q-2}\Big)=q^{\frac{2(e-k+1)-q}{q-2}}\Big(\frac{2(e-k+1)-q}{q-2}\Big)!\,f_q\Big(\frac{2q(e-k)}{q-2}\Big),$$
$$e\ge k+1,\ \ e\equiv k\pmod{q-2}, \tag{4.9}$$

where $f_q(n)$ is the number of free subgroups of index n in $\mathfrak{H}(q)$.

(ii) *For $k\ge 1$, the number $M_q(qk)$ of subgroups $\Delta\le\mathfrak{H}(q)$ of index qk and with $\mu(\Delta)=0$ is given by*

$$M_q(qk)=\frac{1}{q^{k-1}(k-1)!}\sum_{0\le e\le\frac{qk}{2}}M_q(qk;e,k). \tag{4.10}$$

(iii) *We have $s_q(1)=s_q(2)=1$, and, for $n>2$,*

$$s_q(n)=\sum_{1\le k\le\frac{n}{q}}\ \sum_{0\le e\le\frac{n}{2}}\frac{n}{q^kk!}\binom{qk-2e}{n-qk}M_q(qk;e,k). \tag{4.11}$$

Proof. Setting $(\mathfrak{H}(q):\Delta)=qk$, $\lambda(\Delta)=qk-2e$, and $\mu(\Delta)=0$ in Equation (3.3), we find that $\nu(\Delta)=e-k+1$, so that $\mathbf{t}(\Delta)$ agrees with (4.8). Hence, setting $n=qk$, $m_1=e$, and $m_2=k$ in (4.7), the first part of (i) follows. The particular statement in (i) as well as Assertion (ii) are immediate consequences. Finally, Assertion (iii) results upon setting $m_1=e+n-qk$ and $m_2=k$ in (4.7) and summing over all e and k. $\square$

4.2. Calculation of the numbers $M_q(qk;e,k)$.

Our next result provides a rather complicated looking but explicit formula for the quantities mentioned in the title. This formula in turn will enable us to determine the parity of the numbers $M_q(n)$ for $q\ge 5$.

Proposition 9. *For $k\ge 1$ and $k-1\le e\le\frac{qk}{2}$, we have*

$$M_q(qk;e,k)=\sum_{\gamma=1}^{k}\frac{(-1)^{\gamma-1}}{\gamma}\sum_{\substack{\alpha_1,\dots,\alpha_\gamma\ge 0\\ \alpha_1+\dots+\alpha_\gamma=e}}\ \sum_{\substack{\rho_1,\dots,\rho_\gamma\ge 1\\ \rho_1+\dots+\rho_\gamma=k}}\binom{k}{\rho_1,\dots,\rho_\gamma}\prod_{i=1}^{\gamma}\frac{(q\rho_i)!}{2^{\alpha_i}\alpha_i!\,(q\rho_i-2\alpha_i)!}. \tag{4.12}$$

Proof. According to the definition of $M_q(qk;e,k)$, we want to enumerate the elements of the set $\mathcal{M}_q(qk;e,k)$; that is, connected graphs consisting of k oriented blue q-gons and e (unoriented) red edges connecting vertices of the q-gons in such a way that no two red edges share a vertex.

Let the q-gons be denoted by $P_1, P_2, \dots, P_k$ in order (according to their smallest vertex label), and let $\Pi(k)$ be the set of all partitions of the standard set $[k]$.

For a partition $\pi \in \Pi(k)$ with γ blocks, we write $M_{=\pi}(k;e_1,e_2,\dots,e_\gamma)$ for the number of ways to draw $e = e_1+e_2+\dots+e_\gamma$ red edges among the vertices of the q-gons in such a way that no two edges share a vertex, and such that the connectivity structure of the resulting graph corresponds to the partition π; that is, if $\{i_1,i_2,\dots,i_j\}$ is the l-th block of π (the blocks can be canonically ordered with respect to their smallest elements), the q-gons $P_{i_1}, P_{i_2}, \dots, P_{i_j}$ form a connected component of the graph and, moreover, there are exactly e_l red edges in this component. Analogously, let $M_{\le\pi}(k;e_1,e_2,\dots,e_\gamma)$ be the number of ways to draw $e = e_1+e_2+\dots+e_\gamma$ red edges such that no two edges share a vertex and such that the connectivity structure of the resulting graph is described by a partition which is equal to or finer than π (in the usual partial order on set partitions; cf., for instance, [32, Example 3.1.1(d)]), and such that the same condition is satisfied with regard to the distribution of the red edges.

Clearly, for fixed e and $\pi \in \Pi(k)$, and denoting by $|\pi|$ the number of blocks of π, we have

$$\sum_{e_1+\dots+e_{|\pi|}=e} M_{\le\pi}(k;e_1,e_2,\dots,e_{|\pi|}) = \sum_{\sigma\le\pi} \sum_{f_1+\dots+f_{|\sigma|}=e} M_{=\sigma}(k;f_1,f_2,\dots,f_{|\sigma|}).$$

Möbius inversion (cf. [31, Propositions 2–3]) yields

$$\sum_{e_1+\dots+e_{|\pi|}=e} M_{=\pi}(k;e_1,e_2,\dots,e_{|\pi|}) = \sum_{\sigma\le\pi} \sum_{f_1+\dots+f_{|\sigma|}=e} \mu(\sigma,\pi)\, M_{\le\sigma}(k;f_1,f_2,\dots,f_{|\sigma|}),$$

where μ denotes the Möbius function of the partition lattice $\Pi(k)$. In particular, for

$$\pi = \{[k]\} =: \hat{1}$$

(the maximum element in the partition lattice $\Pi(k)$), we have

$$M_q(qk;e,k) = M_{=\hat{1}}(k;e) = \sum_{\sigma\in\Pi(k)} \sum_{f_1+\dots+f_{|\sigma|}=e} \mu(\sigma,\hat{1})\, M_{\le\sigma}(k;f_1,f_2,\dots,f_{|\sigma|}). \tag{4.13}$$

The numbers $M_{\le\sigma}(k;f_1,f_2,\dots,f_{|\sigma|})$ are easily determined: if $\{i_1,i_2,\dots,i_j\}$ is the l-th block of σ, then this means that f_l edges are to be drawn *arbitrarily* among the vertices of the q-gons $P_{i_1}, P_{i_2}, \dots, P_{i_j}$, subject only to the restriction that no two edges are allowed to share a vertex. The number of ways to do this is

$$\frac{(jq)(jq-1)\cdots(jq-2f_l+1)}{2^{f_l}\, f_l!}.$$

Hence, if $\rho_1,\rho_2,\dots,\rho_{|\sigma|}$ are the block sizes of σ, we have

$$M_{\le\sigma}(k;f_1,f_2,\dots,f_{|\sigma|}) = \prod_{i=1}^{|\sigma|} \frac{(q\rho_i)!}{2^{f_i}\, f_i!\,(q\rho_i-2f_i)!}.$$

The Möbius function $\mu(\sigma, \hat{1})$ is known as well, namely one has

$$\mu(\sigma, \hat{1}) = (-1)^{|\sigma|-1}(|\sigma|-1)!;$$

cf., for instance, [32, Example 3.10.4]. Finally, for fixed $\rho_1, \rho_2, \dots, \rho_\gamma$ with $\rho_1 + \rho_2 + \cdots + \rho_\gamma = k$, the number of *ordered* partitions of $\{1, 2, \dots, k\}$ (here, "ordered" means that the order of the blocks matters), the block sizes of which are $\rho_1, \rho_2, \dots, \rho_\gamma$, is given by $\binom{k}{\rho_1, \rho_2, \dots, \rho_\gamma}$. Every partition in $\Pi(k)$ with γ blocks giving rise to exactly $\gamma!$ *ordered* partitions of $\{1, 2, \dots, k\}$ by permuting the blocks, we must in the end divide by $\gamma!$ in order to get rid of the overcounting. If everything is put together, (4.13) transforms into (4.12). □

Remark. A combination of (4.7) and Proposition 9 yields an explicit formula for the number $s_q(n; m_1, m_2)$ of index n subgroups in $\mathfrak{H}(q)$ of representation type $\binom{m_1\ n-2m_1}{m_2\ n-qm_2}$.

Although this is not apparent from (4.12), the number $M_q(qk; e; k)$ admits a simple product formula representation in the case when $e = k-1$; that is, when the underlying graph formed by the red edges and the q-gons (collapsed to vertices) is a tree. Rather embarrassingly, we have not been able to deduce Formula (4.14) below directly from the formula of Proposition 9.

Proposition 10. *We have $M_q(q; 0, 1) = 1$, and for $k \geq 2$,*

$$M_q(qk; k-1, k) = q^k((q-1)k)((q-1)k-1)\cdots(qk-2k+3), \tag{4.14}$$

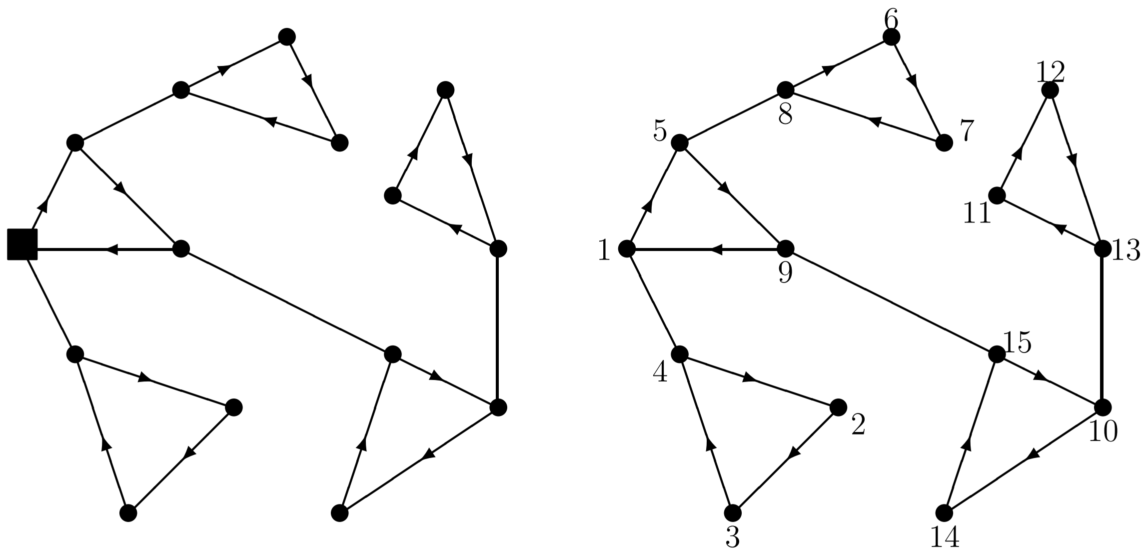
where an empty product must be interpreted as 1.

Proof. The proof consists in converting the problem of counting the elements of $\mathcal{M}_q(qk; k-1, k)$ into a counting problem for certain planar maps. The latter problem has already been solved by Goulden and Jackson in [11] in connection with the computation of connection coefficients for the symmetric group.

Indeed, recall that the set $\mathcal{M}_q(qk; k-1, k)$ consists only of connected graphs. Thus, the only way to generate an element of $\mathcal{M}_q(qk; k-1, k)$ out of k blue q-gons and $k-1$ red edges is by starting from a tree with vertices labelled $v_1, v_2, \dots, v_k$ (and, hence, $k-1$ edges, which we assume to be red), blowing up the vertices of the tree to q-gons, and gluing one end of a red edge originally connecting v_i and v_j to a vertex of the polygon corresponding to v_i, the other to a vertex of the polygon corresponding to v_j, in such a way that no two red edges share a vertex. Finally, we label the vertices of the polygon corresponding to v_i by $qi - q + 1, \dots, qi - 1, qi$ in circular order.

Such an object can be embedded canonically in the plane without crossings of edges by requiring that all polygons are embedded with clockwise circular labelling. Deleting all labels and marking the vertex originally labelled by 1, we obtain a certain set $\widetilde{\mathcal{M}}(q, k)$ of graphs in which one vertex is marked. Figure 1.a shows such a graph in $\widetilde{\mathcal{M}}(3, 5)$; there, the marked vertex is indicated by a black square, red edges are indicated as undirected edges, while the blue edges are the directed edges. We observe that

$$M_q(qk; k-1, k) = q^{k-1}(k-1)!\,\big|\widetilde{\mathcal{M}}(q, k)\big|,$$



a. An element of $\widetilde{\mathcal{M}}(3,5)$ b. The labelling of vertices

FIGURE 1

since, starting with an object from $\widetilde{\mathcal{M}}(q,k)$, we have $(k-1)!$ possibilities to decide from which set of the form $\{qi-q+1,\dots,qi-1,qi\}$ to take the labels for a given unmarked q-gon, and subsequently, for each of the $k-1$ unmarked q-gons, we have q possibilities where to start the clockwise labelling. The problem of counting the elements of $\mathcal{M}_q(qk;k-1,k)$ has thus been reduced to the problem of finding the cardinality of the set $\widetilde{\mathcal{M}}(q,k)$.

To make the link with [11], given an element of $\widetilde{\mathcal{M}}(q,k)$, we translate it into a factorization

$$(1,2,\dots,qk)=\pi_1\circ\pi_2 \tag{4.15}$$

of the "long" cycle $(1,2,\dots,qk)$ into the product of two permutations in S_{qk}, π_1 consisting of k cycles of length q, and π_2 consisting of $k-1$ cycles of length 2 and fixed points otherwise. To explain this translation, consider Figure 1, which illustrates an example for $q=3$ and $k=5$. Given an element of $\widetilde{\mathcal{M}}(q,k)$, we determine labels for all vertices in the following way: the marked vertex is labelled 1. Now we suppose that we already have labelled i vertices by $1,2,\dots,i$. Placing ourselves in the vertex labelled i, v_i say, there are two possibilities: either this vertex is incident to a red edge or not. In the first case, we move from v_i along the red edge, arriving in the vertex u, say, and then continue along the blue edge emanating from u. The vertex which we reach at the other end of this blue edge is labelled $i+1$. In the second case, we simply move along the blue edge emanating from v_i, and we label the vertex which we reach at the other end of this blue edge by $i+1$. Figure 1.b shows the resulting labelling in our example. From the labelling we can read off a factorization (4.15) by interpreting a q-gon with vertices labelled $j_1,j_2,\dots,j_q$ in clockwise order as the cycle $(j_1,j_2,\dots,j_q)$ and letting π_1 be the product of all these cycles, and by interpreting a red edge with end vertices j_1,j_2 as the transposition (j_1,j_2) and letting π_2 be the product of all these transpositions. In this way, our example in Figure 1 corresponds to the factorization

$$(1,2,\dots,15)=\pi_1\circ\pi_2,$$

where

$$\pi_1=(1,5,9)(2,3,4)(6,7,8)(10,14,15)(11,12,13)$$

and

$$\pi_2=(1,4)(5,8)(9,15)(10,13).$$

It is not difficult to see that this translation defines a bijection between elements of $\widetilde{\mathcal{M}}(q,k)$ and factorizations (4.15) where the disjoint cycle factorization of π_1 consists of k cycles of length q, and where the disjoint cycle factorization of π_2 consists of $k-1$ cycles of length 2 and fixed points otherwise. The solution of the enumeration problem for these objects is then found in [11, Theorem 3.2] by specializing $n=qk$, $m=2$, $\alpha_1=(q^k)$, and $\alpha_2=(2^{k-1},1^{qk-2k+2})$. □

4.3. The parity of the numbers $M_q(n)$. Let I_n denote the number of solutions of the equation $x^2=1$ in the symmetric group S_n. It is well known that

$$I_n=\sum_{\alpha\ge0}\frac{n!}{2^\alpha\alpha!\,(n-2\alpha)!},\tag{4.16}$$

if we set $\frac{1}{n!}=0$ for integers $n<0$ in accordance with the behaviour of the gamma function; cf. [5, Equation (4)]. The exact value of the 2-adic valuation of I_n has been determined by Ochiai [30, Sec. 3.2]. The result is that

$$v_2(I_n)=\begin{cases}n/4, & \text{if } n\equiv 0 \pmod 4,\\ (n-1)/4, & \text{if } n\equiv 1 \pmod 4,\\ (n+2)/4, & \text{if } n\equiv 2 \pmod 4,\\ (n+5)/4, & \text{if } n\equiv 3 \pmod 4,\end{cases}$$

where, as usual, $v_2(\alpha)$ stands for the 2-adic valuation of α. For our purposes, the weaker estimate

$$v_2(I_n)\ge\begin{cases}n/4, & \text{if } n\not\equiv 1 \pmod 4,\\ (n-1)/4, & \text{if } n\equiv 1 \pmod 4.\end{cases}\tag{4.17}$$

suffices, which already follows from [5, Theorem 10].

The following auxiliary result (Lemma 11), whose proof will be given in Section A.1 in the appendix, is needed to bound the 2-adic valuation of the numbers $M_q(qk)$ in the case when $q\ge5$; see Proposition 12.

Lemma 11. *If $\rho_1\equiv\rho_2\equiv\cdots\equiv\rho_\alpha\equiv1 \pmod 4$, then*

$$v_2\left(\binom{\rho_1+\rho_2+\cdots+\rho_\alpha}{\rho_1,\rho_2,\dots,\rho_\alpha}\right)\ge v_2(\alpha!).\tag{4.18}$$

If $\rho_1\equiv\rho_2\equiv\cdots\equiv\rho_\alpha\equiv3 \pmod 4$, then

$$v_2\left(\binom{\rho_1+\rho_2+\cdots+\rho_\alpha}{\rho_1,\rho_2,\dots,\rho_\alpha}\right)\ge v_2\big((3\alpha)!\big)-\alpha.\tag{4.19}$$

Proposition 12. *For a prime number $q \ge 5$ and an integer $k \ge 1$, the number $M_q(qk)$ of subgroups in $\mathfrak{H}(q)$ of index qk and with $\mu(\Delta) = 0$ satisfies*

$$v_2(M_q(qk)) \ge \frac{qk-1}{4} - v_2\big((k-1)!\big) - \lfloor \log_2 k \rfloor . \tag{4.20}$$

In particular, $M_q(qk)$ is even for $q \ge 5$ and $k \ge 1$.

Proof. By Part (ii) of Corollary 8, Proposition 9, and (4.16), we have

$$\begin{aligned} M_q(qk) &= \frac{1}{q^{k-1}(k-1)!} \sum_{0 \le e \le \frac{qk}{2}} \sum_{\gamma=1}^{k} \frac{(-1)^{\gamma-1}}{\gamma} \\ &\qquad \cdot \sum_{\substack{\alpha_1,\dots,\alpha_\gamma \ge 0 \\ \alpha_1+\dots+\alpha_\gamma = e}} \sum_{\substack{\rho_1,\dots,\rho_\gamma \ge 1 \\ \rho_1+\dots+\rho_\gamma = k}} \binom{k}{\rho_1,\dots,\rho_\gamma} \prod_{i=1}^{\gamma} \frac{(q\rho_i)!}{2^{\alpha_i}\alpha_i!\,(q\rho_i - 2\alpha_i)!} \\ &= \sum_{\gamma=1}^{k} \sum_{\substack{\rho_1,\dots,\rho_\gamma \ge 1 \\ \rho_1+\dots+\rho_\gamma = k}} \frac{1}{q^{k-1}(k-1)!} \frac{(-1)^{\gamma-1}}{\gamma} \binom{k}{\rho_1,\dots,\rho_\gamma} \prod_{i=1}^{\gamma} I_{q\rho_i}. \end{aligned} \tag{4.21}$$

For fixed γ and $\rho_1, \rho_2, \dots, \rho_\gamma$, we bound the 2-adic valuation of the corresponding summand in the sum in the last line, $S(\gamma; \rho_1, \dots, \rho_\gamma)$ say. Namely, without loss of generality, let $\rho_1, \rho_2, \dots, \rho_\alpha$ be the ρ_j's for which $q\rho_j \equiv 1 \pmod 4$. Then we have

$$\binom{k}{\rho_1,\dots,\rho_\gamma} = \binom{\rho_1+\rho_2+\dots+\rho_\alpha}{\rho_1,\dots,\rho_\alpha} \binom{k}{\rho_1+\dots+\rho_\alpha, \rho_{\alpha+1},\dots,\rho_\gamma},$$

and hence, by a combination of (4.17) and Lemma 11,

$$\begin{aligned} &v_2\big(S(\gamma;\rho_1,\dots,\rho_\gamma)\big) \\ &\qquad \ge -v_2\big((k-1)!\big) - \lfloor \log_2 \gamma \rfloor + v_2\left(\binom{\rho_1+\rho_2+\dots+\rho_\alpha}{\rho_1,\dots,\rho_\alpha}\right) + \sum_{i=1}^{\gamma} v_2(I_{q\rho_i}) \\ &\qquad \ge -v_2\big((k-1)!\big) - \lfloor \log_2 k \rfloor + \frac{\max\{\alpha-1,0\}}{2} + \frac{q(\rho_1+\rho_2+\dots+\rho_\gamma)-\alpha}{4} \\ &\qquad \ge -v_2\big((k-1)!\big) - \lfloor \log_2 k \rfloor + \frac{\max\{\alpha-2,-\alpha\}}{4} + \frac{qk}{4}. \end{aligned}$$

The 2-adic valuation of $M_q(qk)$ is at least the minimum of the expression displayed in the last line taken over all possible choices of α. This minimum is exactly the expression on the right-hand side of (4.20).

To see that the right-hand side of (4.20) is always positive for $q \ge 5$, one observes that $v_2\big((k-1)!\big) \le k-2$ as long as $k \ge 2$, and thus

$$v_2(M_q(qk)) \ge \frac{(q-4)k+7}{4} - \lfloor \log_2 k \rfloor \ge \frac{k+7}{4} - \lfloor \log_2 k \rfloor > 0,$$

provided that $k \ge 2$. For $k = 1$, it can be verified directly that the right-hand side of (4.20) is positive. $\square$

Proposition 12 leaves open the case when $q = 3$, which is settled in Proposition 15 below, making use of results in [33]. The following auxiliary result (Lemma 13) will be used in the proof of Proposition 15; it also bears on the parity of the numbers $M_q(qk; k-1, k)/(k-1)!$ in the case when q is a Fermat prime; see Corollary 14. The (straightforward but somewhat lengthy) proof of Lemma 13 is recorded in Section A.2 in the appendix.

Lemma 13. *Let $\lambda, k \geq 1$ be integers. Then*

$$\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2 \quad \textit{if, and only if,}$$

$$k = \frac{2^{\lambda\sigma}-1}{2^\lambda - 1} \quad \textit{or} \quad k = \frac{2^{\lambda\sigma+1}-2}{2^\lambda-1} \quad \textit{for some } \sigma \geq 1. \tag{4.22}$$

Corollary 14. *Let q be a Fermat prime, and let k be a positive integer. Then*

$$\frac{M_q(qk; k-1, k)}{(k-1)!} \equiv 1 \pmod 2$$

$$\textit{if, and only if,} \quad k = \frac{(q-1)^\sigma - 1}{q-2} \quad \textit{or } k = 2\frac{(q-1)^\sigma-1}{q-2} \quad \textit{for some } \sigma \geq 1.$$

Proof. For $k \geq 2$, Equation (4.14) gives

$$M_q(qk; k-1, k) = q^k\,((q-1)k+1)((q-1)k)\cdots((q-1)k-k+3)\,\frac{1}{(q-1)k+1}$$

so that, modulo 2,

$$\frac{M_q(qk; k-1, k)}{(k-1)!} = q^k \binom{(q-1)k+1}{k-1}\frac{1}{(q-1)k+1} \equiv \binom{(q-1)k+1}{k-1},$$

a congruence which is also seen to hold for $k = 1$. Since q is a Fermat prime, we have $q - 1 = 2^\lambda$ for some $\lambda \geq 1$, and our claim follows from Lemma 13. □

Proposition 15. *For $k \geq 1$, the number $M_3(3k)$ of subgroups Δ of index $3k$ in the modular group $\mathfrak{H}(3) = \mathrm{PSL}_2(\mathbb{Z})$ with the property that $\mu(\Delta) = 0$, is even.*

Proof. Our starting point is again Corollary 8 (ii), more precisely, the fact that

$$M_3(3k) = 3^{-(k-1)} \sum_{k-1 \leq e \leq \frac{3k}{2}} \frac{M_3(3k; e, k)}{(k-1)!}, \quad k \geq 1. \tag{4.23}$$

Concerning the summands occurring on the right-hand side of (4.23), Stothers shows the following:

$$\frac{M_3(3k; k-1, k)}{(k-1)!} = \frac{3^k\,(2k)!}{(k-1)!\,(k+2)!}, \quad k \geq 1, \tag{4.24}$$

$$\frac{M_3(3k; k, k)}{(k-1)!} = 2^{2k-2}\,3^k, \quad k \geq 1, \tag{4.25}$$

$$\frac{M_3(6\ell; 3\ell, 2\ell)}{(2\ell-1)!} = 3^{2\ell-1}\,f_3(6\ell), \quad \ell \geq 1, \tag{4.26}$$

and

$$\frac{M_3(3k;e,k)}{(k-1)!} = 2^{3k-2e-1}\,3^k\,k\,\frac{\prod_{\ell=0}^{3k-2e-2}(3k-e-2\ell-2)}{(3k-2e)!}\,f_3(6(e-k)),\quad k<e<\frac{3k}{2}, \tag{4.27}$$

where $f_3(n)$ is the number of free subgroups of index n in $\mathfrak{H}(3)$, and the product in (4.27) has to be evaluated as 1 if $2e=3k-1$; cf. Propositions 1.7 and 1.8 and Formula (3) in [33]. Of course, Equation (4.24) also follows from our Proposition 10. By (4.27) and Legendre's formula for the p-adic valuation of factorials, we have,

$$v_2\Big(\frac{M_3(3k;e,k)}{(k-1)!}\Big) = \big(\mathfrak{s}_2(3k-2e)-1\big) + v_2(k) + v_2(f_3(6(e-k))) \\ + \sum_{\ell=0}^{3k-2e-2} v_2(3k-e-2\ell-2), \qquad k<e<\frac{3k}{2}, \tag{4.28}$$

where $\mathfrak{s}_2(x)$ is the sum of digits in the binary expansion of x. Further, it is known that $f_3(6\lambda)$ is odd if, and only if, $\lambda+1$ is a non-trivial 2-power; cf. [33, Cor. 1.11] or [21, Proposition 6]. Using this fact together with (4.28), one finds that, for $k<e<\frac{3k}{2}$,

$$\frac{M_3(3k;e,k)}{(k-1)!} \equiv 1 \pmod 2 \text{ if, and only if,}\\ e=2^{\sigma+1}+2^\sigma-2 \text{ and } k=2^{\sigma+1}-1 \text{ for some } \sigma\ge 1. \tag{4.29}$$

Indeed, since $2e<3k$, we have $\mathfrak{s}_2(3k-2e)\ge 1$; hence, all summands on the right-hand side of (4.28) are non-negative. For this right-hand side to vanish, it is thus necessary and sufficient that (i) k is odd, (ii) $e-k+1=2^\sigma$ for some $\sigma\ge1$, and (iii) $3k-2e=2^\lambda$ for some $\lambda\ge 0$. It follows from (ii) and (iii) that $k=2^{\sigma+1}+2^\lambda-2$, which is odd only for $\lambda=0$, whence (4.29).

The parity behaviour of $f_3(6\lambda)$ also gives that

$$\frac{M_3(6\ell;3\ell,2\ell)}{(2\ell-1)!} \equiv 1 \pmod 2 \text{ if, and only if, } \ell+1=2^\sigma \text{ for some } \sigma\ge 1. \tag{4.30}$$

From (4.23)–(4.25), (4.29), and (4.30), we deduce that, modulo 2,

$$M_3(3k) = \frac{3(2k)!}{(k-1)!\,(k+2)!} + 3\cdot 2^{2k-2} \\ + \sum_{k<e<\frac{3k}{2}} \frac{M_3(3k;e,k)}{3^{k-1}\,(k-1)!} + \begin{Bmatrix} \dfrac{M_3\big(3k;\frac{3k}{2},k\big)}{3^{k-1}\,(k-1)!}, & 2\mid k \\ 0, & 2\nmid k \end{Bmatrix} \\ \equiv \binom{2k+1}{k-1} + \begin{Bmatrix} 1; & k=2^\tau-1,\ \tau\ge 2 \\ 0; & \text{otherwise} \end{Bmatrix} + \begin{Bmatrix} 1; & k=2(2^\sigma-1),\ \sigma\ge 1 \\ 0; & \text{otherwise,} \end{Bmatrix}$$

provided that $k\ge 2$. By Lemma 13 with $\lambda=1$, we have

$$\binom{2k+1}{k-1} \equiv 1 \pmod 2 \text{ if, and only if, } k=2^\sigma-1 \text{ or } k=2(2^\sigma-1) \text{ for some } \sigma\ge 1.$$

Combining the last two assertions, we find that

$$M_3(3k) \equiv 0 \bmod 2, \quad k \geq 2.$$

Finally,

$$M_3(3) = M_3(3;0,1) + M_3(3;1,1) = 1 + 3 \equiv 0 \bmod 2,$$

and the proof is complete. □

Putting together the observation that $M_q(n) = 0$ whenever $q \nmid n$ (see the start of this section) with Propositions 12 and 15, we obtain the main result of this section.

Theorem 16. *For each odd prime q and every integer $n \geq 1$, the number $M_q(n)$ of index n subgroups Δ in $\mathfrak{H}(q)$ with the property that $\mu(\Delta) = 0$, is even.*

5. Generalized parity patterns of Hecke groups

The main result of this section computes the parity behaviour of the generalized subgroup numbers of $\mathfrak{H}(q)$, with q an odd prime, in the case when H is of even order; see Theorem 24. Our interest in this computation stems from the fact that, in this setting, $s_q^H(n) := s_{\mathfrak{H}(q)}^H(n) \equiv N_q(n) \pmod 2$, where the $N_q(n)$'s enter into the mod 2 calculation of $s_{\Gamma_m(q)}^H(n)$ via Proposition 1. Indeed, writing

$$\mathfrak{U} \cong C_2^{*\lambda(\mathfrak{U})} * C_q^{*\mu(\mathfrak{U})} * F_{\nu(\mathfrak{U})}$$

for a subgroup $\mathfrak{U}$ in $\mathfrak{H}(q)$, in accordance with Kurosh's subgroup theorem, we have

$$s_q^H(n) = \sum_{(\mathfrak{H}(q):\mathfrak{U})=n} |\operatorname{Hom}(C_2,H)|^{\lambda(\mathfrak{U})} \cdot |\operatorname{Hom}(C_q,H)|^{\mu(\mathfrak{U})} \cdot |H|^{\nu(\mathfrak{U})}.$$

By Frobenius' theorem (cf. [9] or [12, Theorem 9.1.2]) concerning the equation $x^n = 1$ in a finite group, the assumption $|H| \equiv 0 \pmod 2$ implies that $|\operatorname{Hom}(C_2,H)|$ is even. Furthermore, we have

$$|\operatorname{Hom}(C_q,H)| = 1 + (q-1) \times (\text{number of subgroups } U \cong C_q \text{ in } H) \equiv 1 \bmod 2. \tag{5.1}$$

Hence, if $|H|$ is even, it follows that, modulo 2,

$$s_q^H(n) \equiv \sum_{\substack{\mathfrak{U} \\ (\mathfrak{H}(q):\mathfrak{U})=n \\ \lambda(\mathfrak{U})=\nu(\mathfrak{U})=0}} 1 = N_q(n), \tag{5.2}$$

as claimed.

On the other hand, it was shown in particular in [23] that — just as subgroup numbers are connected with the enumeration of permutation representations — the generalized subgroup numbers $s_\Gamma^H(n)$ of a finitely generated group Γ are related to the function $|\operatorname{Hom}(\Gamma, H \wr S_n)|$ counting monomial representations of Γ via the identity

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(\Gamma, H \wr S_n)| \frac{z^n}{|H|^n n!} = \exp\left(\frac{1}{|H|} \sum_{n=1}^{\infty} s_\Gamma^H(n) \frac{z^n}{n}\right), \tag{5.3}$$

or, what comes to the same thing, via the recurrence relation

$$n\,|H|\,h_\Gamma^H(n) = \sum_{k\ge 1} s_\Gamma^H(k) h_\Gamma^H(n-k), \quad n \in \mathbb{Z}, \tag{5.4}$$

where

$$h_\Gamma^H(n) := \begin{cases} |\operatorname{Hom}(\Gamma, H \wr S_n)|/(|H|^n n!), & n \ge 0 \\ 0, & n < 0. \end{cases}$$

This follows from [23, Cor. 1] by setting $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, $M = \mathbb{N}_0$, and replacing the variable z by $z/|H|$. For a (relatively) untechnical account of the theory of generalized permutation representations, which gives rise (among other things) to Formula (5.3), the reader may consult the survey papers [24] and [25]. Introducing the series

$$\mathcal{H}_\Gamma^H(z) := \sum_{n=0}^{\infty} |\operatorname{Hom}(\Gamma, H \wr S_n)| \frac{z^n}{|H|^n n!}$$

and

$$\mathcal{S}_\Gamma^H(z) := \sum_{n=0}^{\infty} s_\Gamma^H(n+1) z^n,$$

Identity (5.3) takes the form

$$\mathcal{H}_\Gamma^H(z) = \exp\left(\frac{1}{|H|} \int \mathcal{S}_\Gamma^H(z)\,dz\right). \tag{5.5}$$

In view of the preceding observations, our next goal will be to derive a linear differential equation with polynomial coefficients for the generating function $\mathcal{H}_{\mathfrak{H}(q)}^H(z)$. Using Relation (5.5) together with the Faà di Bruno formula (see (A.18) below), this linear differential equation will give rise to a Riccati-type differental equation for the generating function $\mathcal{S}_{\mathfrak{H}(q)}^H(z)$. It is the latter differential equation that we are actually interested in; see (5.26).

5.1. A system of linear differential equations for generating functions related to $\mathcal{H}_{\mathfrak{H}(q)}^H(z)$. The starting point for our computations concerning the series $\mathcal{H}_{\mathfrak{H}(q)}^H(z)$ is the observation that, by the universal mapping property of free products,

$$|\operatorname{Hom}(\mathfrak{H}(q), H \wr S_n)| = |\operatorname{Hom}(C_2, H \wr S_n)| \cdot |\operatorname{Hom}(C_q, H \wr S_n)|. \tag{5.6}$$

Setting $h := |H|$, $a := |\operatorname{Hom}(C_2, H)|$, $b := |\operatorname{Hom}(C_q, H)|$,

$$\alpha_n := \begin{cases} |\operatorname{Hom}(C_2, H \wr S_n)|, & n \ge 0 \\ 0, & n < 0, \end{cases}$$

and

$$\beta_n := \begin{cases} |\operatorname{Hom}(C_q, H \wr S_n)|, & n \ge 0 \\ 0, & n < 0, \end{cases}$$

Equation (5.4) specializes to the relations

$$\alpha_{n+1} = a\alpha_n + hn\alpha_{n-1}, \quad n \ne -1 \tag{5.7}$$

and

$$\beta_{n+1} = b\beta_n + h^{q-1}\frac{n!}{(n-q+1)!}\beta_{n-q+1}, \quad n \neq -1, \tag{5.8}$$

where we use the same convention concerning $\frac{1}{n!}$ as in Formula (4.16). For $n, k \in \mathbb{Z}$, let

$$A_k(n) := \frac{\alpha_n\, \beta_{n-k}}{h^{n-k}\,(n-k)!},$$

still making use of the same convention concerning $\frac{1}{n!}$, and set

$$F_k(z) := \sum_{n\in\mathbb{Z}} A_k(n) z^n.$$

The reader should note that, in view of (5.6), we have $F_0(z) = \mathcal{H}^H_{\mathfrak{H}(q)}(z)$.

Multiplying (5.7) by $\beta_{n-k}/(h^{n-k}(n-k)!)$ and (5.8) by $\alpha_{n+k}/(h^n n!)$, we obtain the relations

$$A_{k+1}(n+1) = aA_k(n) + hnA_{k-1}(n-1), \quad n, k \in \mathbb{Z},\, k \geq 0, \tag{5.9}$$

respectively

$$h(n+1)A_{k-1}(n+k) = bA_k(n+k) + A_{k+q-1}(n+k), \quad n, k \in \mathbb{Z}. \tag{5.10}$$

Multiplication by z^{n+1} and summation over $n \in \mathbb{Z}$, transforms Equation (5.9) into the relation

$$F_{k+1}(z) = azF_k(z) + hz^2F_{k-1}(z) + hz^3F'_{k-1}(z), \quad k \geq 0, \tag{5.11}$$

while multiplication by z^{n+k} and summation over $n \in \mathbb{Z}$ turns (5.10) into

$$hzF'_{k-1}(z) = h(k-1)F_{k-1}(z) + bF_k(z) + F_{k+q-1}(z), \quad k \in \mathbb{Z}. \tag{5.12}$$

Clearly, by iterating Relation (5.11), we can express every function F_k with $k \geq 0$ in terms of derivatives of F_0 and F_1 alone; more precisely, define integral coefficient systems $\big(c_k^{(\mu)}\big)$ and $\big(d_k^{(\nu)}\big)$ for $k \geq 0$ and $0 \leq \mu \leq \lfloor \frac{k}{2} \rfloor$, respectively $k \geq 1$ and $0 \leq \nu \leq \lfloor \frac{k-1}{2} \rfloor$, via

$$\begin{aligned} &c_0^{(0)} = 1,\ c_1^{(0)} = 0,\ c_2^{(0)} = h,\ c_2^{(1)} = 1,\\ &d_1^{(0)} = 1,\ d_2^{(0)} = a, \end{aligned}$$

$$c_{k+1}^{(\mu)} = \left\{\begin{array}{ll} ac_k^{(0)} + hkc_{k-1}^{(0)}, & \mu = 0\\ ac_k^{(\mu)} + h(k+\mu)c_{k-1}^{(\mu)} + c_{k-1}^{(\mu-1)}, & 1 \leq \mu \leq \lfloor \frac{k-1}{2} \rfloor\\ c_{k-1}^{(\frac{k-1}{2})}, & \mu = \lfloor \frac{k+1}{2} \rfloor, k \text{ odd}\\ ac_k^{(k/2)} + c_{k-1}^{(\frac{k-2}{2})}, & \mu = \lfloor \frac{k+1}{2} \rfloor, k \text{ even} \end{array}\right\} \quad (k \geq 2),$$

and

$$d_{k+1}^{(\nu)} = \left\{\begin{array}{ll} ad_k^{(0)} + h(k-1)d_{k-1}^{(0)}, & \nu = 0\\ ad_k^{(\nu)} + h(k+\nu-1)d_{k-1}^{(\nu)} + d_{k-1}^{(\nu-1)}, & 1 \leq \nu \leq \lfloor \frac{k-2}{2} \rfloor\\ ad_k^{(\frac{k-1}{2})} + d_{k-1}^{(\frac{k-3}{2})}, & \nu = \lfloor \frac{k}{2} \rfloor, k \text{ odd}\\ d_{k-1}^{(\frac{k-2}{2})}, & \nu = \lfloor \frac{k}{2} \rfloor, k \text{ even} \end{array}\right\} \quad (k \geq 2).$$

Then we have the following.

Lemma 17. *With* $\big(c_k^{(\mu)}\big)$ *and* $\big(d_k^{(\nu)}\big)$ *as above,*

$$F_k(z) = \sum_{\mu=0}^{\lfloor \frac{k}{2} \rfloor} c_k^{(\mu)} h^\mu z^{k+\mu} F_0^{(\mu)}(z) \; + \sum_{\nu=0}^{\lfloor \frac{k-1}{2} \rfloor} d_k^{(\nu)} h^\nu z^{k+\nu-1} F_1^{(\nu)}(z), \quad k \ge 0. \tag{5.13}$$

The proof of Lemma 17, which, again, is straightforward but somewhat technical, will be given in Section A.3 in the appendix.

For later usage, we record evaluations of $c_k^{(\mu)}$ and $d_k^{(\nu)}$ modulo 2 as given by the following two lemmas.

Lemma 18. *For* $h \equiv 0 \pmod 2$, *we have*

$$c_k^{(\mu)} \equiv \delta_{2\mu,k} \bmod 2, \quad \mu \ge 0,\, k \ge 2\mu, \tag{5.14}$$

$$d_k^{(\nu)} \equiv \delta_{2\nu+1,k} \bmod 2, \quad \nu \ge 0,\, k \ge 2\nu+1, \tag{5.15}$$

where $\delta_{s,t}$ *is the Kronecker delta.*

Proof. As we observed at the start of this section, the assumption $h \equiv 0 \bmod 2$ implies that $a \equiv 0 \bmod 2$. Hence, the definition of $c_k^{(\mu)}$ simplifies modulo 2 to

$$c_0^{(0)} \equiv c_2^{(1)} \equiv 1$$

$$c_1^{(0)} \equiv c_2^{(0)} \equiv 0$$

$$c_k^{(\mu)} \equiv \begin{Bmatrix} 0, & \mu = 0 \\ c_{k-2}^{(\mu-1)}, & \mu \ge 1 \end{Bmatrix} \quad (k \ge 3).$$

We now argue by induction on k. For $k \le 2$, Formula (5.14) clearly holds. Supposing that (5.14) holds true for $k < K$ with some $K \ge 3$, the inductive hypothesis gives

$$c_K^{(\mu)} \equiv \begin{Bmatrix} 0, & \mu = 0 \\ \delta_{2(\mu-1),K-2}, & \mu \ge 1 \end{Bmatrix} = \delta_{2\mu,K} \bmod 2, \quad \mu \le \left\lfloor \frac{K}{2} \right\rfloor,$$

as required. The proof of Formula (5.15) is similar. $\square$

Lemma 19. *For* $h \equiv 1 \pmod 2$, *we have*

$$c_k^{(\mu)} \equiv \begin{Bmatrix} \delta_{2\mu,k} + \delta_{2\mu+1,k}; & \text{if } \mu \text{ is odd} \\ \delta_{2\mu,k} + \delta_{2\mu+2,k} + \delta_{2\mu+3,k}; & \text{if } \mu \text{ is even} \end{Bmatrix} \bmod 2, \quad \mu \ge 0,\, k \ge 2\mu, \tag{5.16}$$

$$d_k^{(\nu)} \equiv \begin{Bmatrix} \delta_{2\mu+1,k}; & \text{if } \mu \text{ is odd} \\ \delta_{2\mu+1,k} + \delta_{2\mu+2,k}; & \text{if } \mu \text{ is even} \end{Bmatrix} \bmod 2, \quad \nu \ge 0,\, k \ge 2\nu+1, \tag{5.17}$$

where, again, $\delta_{s,t}$ *is the Kronecker delta.*

Proof. The assumption $h \equiv 1 \pmod 2$ implies that $a = 1$. The rest of the proof is similar to the proof of the preceding lemma, and is omitted. $\square$

Multiplying (5.12) for $k = 0$ by z^2, substituting (5.11) with $k = 0$, and computing $F_{q-1}(z)$ by means of Lemma 17, we find that

$$(d_{q-1}^{(0)} z^q - 1)F_1(z) + \sum_{\nu=1}^{\frac{q-3}{2}} d_{q-1}^{(\nu)} h^\nu z^{q+\nu} F_1^{(\nu)}(z) = -(az + bz^2 + c_{q-1}^{(0)} z^{q+1}) f(z) - \sum_{\mu=1}^{\frac{q-1}{2}} c_{q-1}^{(\mu)} h^\mu z^{q+\mu+1} f^{(\mu)}(z) \quad (5.18)$$

with $f(z) := F_0(z)$. Next, taking $k = 1$ in (5.12) and computing $F_q(z)$ by means of Lemma 17, we obtain the equation

$$(d_q^{(0)} z^{q-1} + b)F_1(z) + \sum_{\nu=1}^{\frac{q-1}{2}} d_q^{(\nu)} h^\nu z^{q+\nu-1} F_1^{(\nu)}(z) = -c_q^{(0)} z^q f(z) - h(c_q^{(1)} z^{q+1} - z) f'(z) - \sum_{\mu=2}^{\frac{q-1}{2}} c_q^{(\mu)} h^\mu z^{q+\mu} f^{(\mu)}(z). \quad (5.19)$$

Similarly, combining Equation (5.12) for $k = 2, 3, \ldots, q-2$ with Lemma 17, we obtain further equations, which together with (5.18) and (5.19) form a system of $q-1$ linear equations over the field $\mathbb{Q}((z))$ in the variables $F_1^{(0)}(z)$, $F_1^{(1)}(z)$, $\ldots$, $F_1^{(q-2)}(z)$. More specifically, we find that

$$\bar{\Delta}_q \begin{pmatrix} F_1^{(0)}(z) \\ \vdots \\ F_1^{(q-2)}(z) \end{pmatrix} = \begin{pmatrix} b_0(z) \\ \vdots \\ b_{q-2}(z) \end{pmatrix}, \quad (5.20)$$

where $\bar{\Delta}_q = (h^\lambda \omega_{\kappa,\lambda})_{0 \le \kappa, \lambda \le q-2}$, with $\omega_{\kappa,\lambda}$ and $b_\kappa(z)$ given explicitly in terms of b, h, the $c_k^{(\nu)}$'s, the $d_k^{(\nu)}$'s, and the derivatives of $f(z)$, as described in Section A.4 in the appendix.

5.2. The determinant of the system, and its minors. Denote by ${}_0\bar{\Delta}_q$ the matrix obtained from $\bar{\Delta}_q$ by replacing the 0-th column with the right-hand side of (5.20), and by ${}_0\Delta_q$ the corresponding matrix obtained from $\Delta_q := (\omega_{\kappa,\lambda})$ via the same operation. Then $\det \bar{\Delta}_q = h^{\binom{q-1}{2}} \det \Delta_q$, $\det {}_0\bar{\Delta}_q = h^{\binom{q-1}{2}} \det {}_0\Delta_q$, and, according to Cramer's Rule and Laplace's expansion theorem,

$$F_1(z) = \frac{\det {}_0\Delta_q}{\det \Delta_q} = (\det \Delta_q)^{-1} \sum_{\kappa=0}^{q-2} (-1)^\kappa (\det \Delta_{\kappa,0}) b_\kappa(z),$$

where $\Delta_{\kappa,0}$ is the matrix obtained from Δ_q by deleting the κ-th row and 0-th column. We are assuming here, of course, that $\det \Delta_q \neq 0$, a fact which follows, among other things, from our next two auxiliary results, whose proofs will be given in Sections A.5 and A.6 in the appendix, respectively.

Lemma 20. *For $h \equiv 0 \pmod 2$, we have*

(i) $\det \Delta_q \equiv \det \Delta_{0,0} \equiv z^{\frac{3q^2-11q+12}{2}} \bmod 2$,

(ii) $\det \Delta_{\kappa,0} \equiv 0 \bmod 2, \quad 1 \le \kappa \le q-2$.

Lemma 21. *For $h \equiv 1 \pmod 2$, we have*

(i) $$\det \Delta_q \equiv \left.\begin{cases} z^{\frac{3q^2-11q+12}{2}}; & \text{if } q \equiv 1 \pmod 4 \\ z^{\frac{3q^2-11q+12}{2}} + z^{\frac{3q^2-8q+9}{2}}; & \text{if } q \equiv 3 \pmod 4 \end{cases}\right\} \bmod 2;$$

(ii) $\det \Delta_{0,0} \equiv z^{\frac{3q^2-11q+12}{2}} \pmod 2$, $\det \Delta_{1,0} \equiv 0 \pmod 2$, *and for $2 \le \kappa \le q-2$,*

$$\det \Delta_{\kappa,0} \equiv \left.\begin{cases} 0; & \text{if } \kappa \ge 2 \text{ and } q \equiv 1 \pmod 4 \\ 0; & \text{if } \kappa \equiv 1 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \\ z^{\frac{3q^2-8q+5-12\kappa'}{2}}; & \text{if } \kappa = 4\kappa'+2 \text{ and } q \equiv 3 \pmod 4 \\ z^{\frac{3q^2-8q+3-12\kappa'}{2}}; & \text{if } \kappa = 4\kappa'+3 \text{ and } q \equiv 3 \pmod 4 \\ z^{\frac{3q^2-8q+1-12\kappa'}{2}}; & \text{if } \kappa = 4\kappa'+4 \text{ and } q \equiv 3 \pmod 4 \end{cases}\right\} \bmod 2.$$

5.3. A functional equation for $\mathcal{S}^H_{\mathfrak{H}(q)}(z)$. The following auxiliary result, whose proof is recorded in Section A.7 in the appendix, is concerned with computing the expressions

$$h^\nu \Big(\frac{d^\nu}{dz^\nu} \mathcal{H}^H_\Gamma(z)\Big) \Big/ \mathcal{H}^H_\Gamma(z), \quad \nu \in \mathbb{N}_0 \tag{5.21}$$

over $\mathbb{Z}$ and modulo 2 in terms of the series $\mathcal{S}^H_\Gamma(z)$. (The reader should recall (5.5).)

Lemma 22. *Let Γ be a finitely generated group, H a finite group, and let $h = |H|$.*

(i) *For each $\nu \in \mathbb{N}_0$, we have*

$$h^\nu \Big(\frac{d^\nu}{dz^\nu} \mathcal{H}^H_\Gamma(z)\Big) \Big/ \mathcal{H}^H_\Gamma(z) = \sum_{\substack{\pi_1,\dots,\pi_\nu \ge 0 \\ \pi_1+2\pi_2+\dots+\nu\pi_\nu=\nu}} h^{\nu-\pi_1-\dots-\pi_\nu} \frac{\nu!}{\prod_{j\ge1}(j!)^{\pi_j}\pi_j!} \prod_{j\ge1}\Big(\big(\mathcal{S}^H_\Gamma(z)\big)^{(j-1)}\Big)^{\pi_j}, \tag{5.22}$$

and the coefficients $\nu! \big/ \big(\prod_{j\ge1}(j!)^{\pi_j}\pi_j!\big)$ are integers.

(ii) *For each $\nu \in \mathbb{N}_0$, the series (5.21) is an integral power series in z, and satisfies the congruence*

$$h^\nu \Big(\frac{d^\nu}{dz^\nu} \mathcal{H}^H_\Gamma(z)\Big) \Big/ \mathcal{H}^H_\Gamma(z) \equiv \sum_{\mu=0}^{\lfloor \frac{\nu}{2} \rfloor} h^\mu \binom{\nu}{2\mu} \Big(\big(\mathcal{S}^H_\Gamma(z)\big)'\Big)^\mu \big(\mathcal{S}^H_\Gamma(z)\big)^{\nu-2\mu} \bmod 2. \tag{5.23}$$

In particular, if $h \equiv 0 \pmod 2$, then

$$h^\nu \Big(\frac{d^\nu}{dz^\nu} \mathcal{H}^H_\Gamma(z)\Big) \Big/ \mathcal{H}^H_\Gamma(z) \equiv \big(\mathcal{S}^H_\Gamma(z)\big)^\nu \bmod 2, \quad \nu \ge 0. \tag{5.24}$$

Write

$$\big((\det\Delta_q)^{-1}\big)^{(\nu)} = \frac{\Theta_\nu(z)}{(\det\Delta_q)^{\nu+1}},\quad \nu\geq 0,$$

where $\{\Theta_\nu(z)\}_{\nu\geq 0}$ is the family of polynomials in z determined recursively via

$$\begin{aligned}\Theta_{\nu+1}(z) &= (\det\Delta_q)\Theta_\nu'(z) - (\nu+1)(\det\Delta_q)'\Theta_\nu(z),\quad \nu\geq 0\\ \Theta_0(z) &= 1.\end{aligned}$$

Then, by Leibniz's formula for the derivatives of a product function, we have

$$F_1^{(\nu)}(z) = \sum_{\lambda=0}^{\nu}\binom{\nu}{\lambda}\frac{\Theta_{\nu-\lambda}(z)}{(\det\Delta_q)^{\nu-\lambda+1}}\,(\det{}_0\Delta_q)^{(\lambda)},\quad \nu\geq 0. \tag{5.25}$$

Inserting (5.25) into (5.19), multiplying throughout by $(\det\Delta_q)^{\frac{q+1}{2}}$, and dividing by the series $f(z)$, we obtain the relation

$$\begin{aligned}c_q^{(0)}z^q(\det\Delta_q)^{\frac{q+1}{2}} &+ z(c_q^{(1)}z^q-1)(\det\Delta_q)^{\frac{q+1}{2}}hf'(z)/f(z)\\ &+\sum_{\mu=2}^{\frac{q-1}{2}}c_q^{(\mu)}z^{q+\mu}(\det\Delta_q)^{\frac{q+1}{2}}h^\mu f^{(\mu)}(z)/f(z)\\ &+(d_q^{(0)}z^{q-1}+b)(\det\Delta_q)^{\frac{q-1}{2}}(\det{}_0\Delta_q)/f(z)\\ +\sum_{\nu=1}^{\frac{q-1}{2}}\sum_{\lambda=0}^{\nu}\binom{\nu}{\lambda}&d_q^{(\nu)}z^{q+\nu-1}\Theta_{\nu-\lambda}(z)(\det\Delta_q)^{\frac{q+1}{2}-(\nu-\lambda+1)}h^\nu(\det{}_0\Delta_q)^{(\lambda)}/f(z)=0,\end{aligned} \tag{5.26}$$

where the reader should recall that $f(z)=F_0(z)=\mathcal{H}^H_{\mathfrak{H}(q)}(z)$. Two kinds of results may be derived from the last identity: first, an integral recurrence relation for the function $s^H_{\mathfrak{H}(q)}(n)$ for each given q in terms of the parameters $h=|H|$, $a=|\operatorname{Hom}(C_2,H)|$, and $b=|\operatorname{Hom}(C_q,H)|$; second, a description of the parity behaviour of $s^H_{\mathfrak{H}(q)}(n)$ for all q. We illustrate the first type of result below with the case of the modular group $\mathfrak{H}(3)$. As concerns the second kind of result, we note that $s^H_{\mathfrak{H}(q)}(n)\equiv s_q(n)$ (mod 2) for $|H|$ odd. Since the parity behaviour of $s_q(n)$ is known (see Theorem 2), we shall concentrate here on the case where $|H|$ is even, which yields the parity of the numbers $N_q(n)$.

5.4. The case of $\mathfrak{H}(3)$. For $q=3$, Eq. (5.26) reduces to

$$\begin{aligned}c_3^{(0)}z^3(\det\Delta_3)^2 &+ z(c_3^{(1)}z^3-1)(\det\Delta_3)^2hf'(z)/f(z)\\ &+\big\{(d_3^{(0)}z^2+b)(\det\Delta_3)+d_3^{(1)}hz^3\Theta_1(z)\big\}(\det{}_0\Delta_3)/f(z)\\ &+d_3^{(1)}z^3(\det\Delta_3)h(\det{}_0\Delta_3)'/f(z)=0.\end{aligned} \tag{5.27}$$

We have

$$
\begin{aligned}
c_3^{(0)} &= ac_2^{(0)} + 2hc_1^{(0)} = ah,\\
c_3^{(1)} &= ac_2^{(1)} + c_1^{(0)} = a,\\
d_3^{(0)} &= ad_2^{(0)} + hd_1^{(0)} = a^2 + h,\\
d_3^{(1)} &= d_1^{(0)} = 1,\\
\det\Delta_3 &= \det\begin{pmatrix} az^3-1 & 0\\ (a^2+h)z^2+b & z^3\end{pmatrix} = z^3(az^3-1),\\
\Theta_1(z) &= -(\det\Delta_3)' = -3z^2(2az^3-1),
\end{aligned}
$$

and

$$
\begin{aligned}
\det{}_0\Delta_3 &= \det\begin{pmatrix} -z(a+bz+hz^3)f(z)-hz^5f'(z) & 0\\ -ahz^3f(z)-hz(az^3-1)f'(z) & z^3\end{pmatrix}\\
&= -z^4(a+bz+hz^3)f(z)-hz^8f'(z).
\end{aligned}
$$

Inserting these values into (5.27), dividing both sides by z^7, and collecting terms, we find that

$$
(z^7-az^{10})h^2f''(z)/f(z)+\big(-1+4az^3+2bz^4+(7h-3a^2)z^6-2abz^7-4ahz^9\big)hf'(z)/f(z)
$$
$$
+ab+b^2z+a(a^2+3h)z^2+4bhz^3-ab^2z^4+(5h^2-a^4)z^5-ab(a^2+h)z^6-2ah^2z^8=0. \tag{5.28}
$$

Substituting

$$
S_3^H(z)=hf'(z)/f(z)
$$

and

$$
h(S_3^H(z))'+(S_3^H(z))^2=h^2f''(z)/f(z)
$$

in (5.28) according to Lemma 22(i), we find the Riccati-type differential equation

$$
\begin{aligned}
&\big(z^7-az^{10}\big)\big(h(\mathcal{S}_3^H(z))'+(\mathcal{S}_3^H(z))^2\big)\\
&\qquad+\big(-1+4az^3+2bz^4+(7h-3a^2)z^6-2abz^7-4ahz^9\big)\mathcal{S}_3^H(z)\\
&+ab+b^2z+a(a^2+3h)z^2+4bhz^3-ab^2z^4+(5h^2-a^4)z^5-ab(a^2+h)z^6-2ah^2z^8=0
\end{aligned} \tag{5.29}
$$

for the generating function $\mathcal{S}_3^H(z):=\mathcal{S}_{\mathfrak{H}(3)}^H(z)$. Comparing coefficients in (5.29), we finally obtain the following result, which generalizes Theorem 1 in [10].

Proposition 23. *The function $s_3^H(n):=s_{\mathfrak{H}(3)}^H(n)$ satisfies the recurrence relation*

$$
s_3^H(n)=4as_3^H(n-3)\,+\,2bs_3^H(n-4)\,+\,(hn-3a^2)s_3^H(n-6)\,-\,2abs_3^H(n-7)
$$
$$
-ah(n-6)s_3^H(n-9)+\sum_{\mu=1}^{n-7}s_3^H(\mu)s_3^H(n-\mu-6)-a\sum_{\mu=1}^{n-10}s_3^H(\mu)s_3^H(n-\mu-9),\quad n\ge 10, \tag{5.30}
$$

with initial values

$$\begin{aligned}
s_3^H(1) &= ab,\\
s_3^H(2) &= b^2,\\
s_3^H(3) &= a(a^2+3h),\\
s_3^H(4) &= 4b(a^2+h),\\
s_3^H(5) &= 5ab^2,\\
s_3^H(6) &= 3a^4+2b^3+5h^2+12a^2h,\\
s_3^H(7) &= 14ab(a^2+2h),\\
s_3^H(8) &= 8b^2(3a^2+2h),\\
s_3^H(9) &= 3a(3a^4+6b^3+15h^2+16a^2h).
\end{aligned}$$

5.5. The parity behaviour of $N_q(n)$. We now use Lemmas 18, 20, and 22(ii) to simplify identity (5.26) under the assumption that $h = |H| \equiv 0 \pmod 2$. Throughout, we set $\mathcal{S}^H_{\mathfrak{H}(q)}(z) =: \mathcal{S}^H_q(z)$ and $\alpha_0 := 3q^2 - 11q + 12$.

First, $c_q^{(0)} \equiv c_q^{(1)} \equiv 0 \pmod 2$, since $q > 2$; hence,

$$c_q^{(0)} z^q (\det \Delta_q)^{\frac{q+1}{2}} \equiv 0 \bmod 2$$

and

$$z(c_q^{(1)} z^q - 1)(\det \Delta_q)^{\frac{q+1}{2}} h f'(z)/f(z) \equiv z^{\frac{q+1}{4}\alpha_0+1} \mathcal{S}^H_q(z) \bmod 2.$$

Similarly, we have $c_q^{(\mu)} \equiv 0 \pmod 2$ for $\mu < q/2$; thus

$$\sum_{\mu=2}^{\frac{q-1}{2}} c_q^{(\mu)} z^{q+\mu} (\det \Delta_q)^{\frac{q+1}{2}} h^\mu f^{(\mu)}(z)/f(z) \equiv 0 \bmod 2.$$

Next, inspection shows that, in view of Lemma 22(ii), $b_\kappa(z)/f(z)$ is always an integral power series; hence, $(\det{}_0\Delta_q)/f(z)$ is an integral power series, and modulo 2 we have

$$\begin{aligned}
(\det{}_0\Delta_q)/f(z) &= \sum_{\kappa=0}^{q-2} (-1)^\kappa (\det \Delta_{\kappa,0}) b_\kappa(z)/f(z)\\
&\equiv (\det \Delta_{0,0}) b_0(z)/f(z)\\
&\equiv z^{\alpha_0/2}\big\{z^2 + z^{\frac{3q+1}{2}} h^{\frac{q-1}{2}} f^{(\frac{q-1}{2})}(z)/f(z)\big\}\\
&\equiv z^{2+\alpha_0/2} + z^{\frac{\alpha_0+3q+1}{2}} \big(\mathcal{S}^H_q(z)\big)^{\frac{q-1}{2}},
\end{aligned}$$

and so, modulo 2,

$$
\begin{aligned}
(d_q^{(0)}z^{q-1}+b)(\det\Delta_q)^{\frac{q-1}{2}}(\det{}_0\Delta_q)/f(z) &\equiv (\det\Delta_q)^{\frac{q-1}{2}}(\det{}_0\Delta_q)/f(z)\\
&\equiv z^{\frac{\alpha_0}{2}(\frac{q+1}{2}-1)}\Big\{z^{2+\alpha_0/2}+z^{\frac{\alpha_0+3q+1}{2}}\big(\mathcal S_q^H(z)\big)^{\frac{q-1}{2}}\Big\}\\
&= z^{2+\frac{q+1}{4}\alpha_0}+z^{(\frac{q+1}{2}\alpha_0+3q+1)/2}\big(\mathcal S_q^H(z)\big)^{\frac{q-1}{2}}.
\end{aligned}
$$

Here we have used Lemma 20 to evaluate $\det\Delta_q$ and $\det\Delta_{\kappa,0}$ modulo 2, the facts, following from Lemma 18, that $d_q^{(0)}\equiv 0 \pmod 2$ and that

$$c_{q-1}^{(\mu)}\equiv 1 \pmod 2 \ \text{ if, and only if, }\ \mu=\frac{q-1}{2},\quad 0\le\mu\le\frac{q-1}{2},$$

plus Part (ii) of Lemma 22 to rewrite the term $h^{\frac{q-1}{2}}f^{(\frac{q-1}{2})}(z)/f(z)$. This leaves the double sum Σ on the right-hand side of (5.26). Clearly, for $0\le\kappa\le q-2$ and $0\le\eta\le\nu$, the term $h^\nu b_\kappa^{(\eta)}(z)/f(z)$ is an integral power series, and we have

$$h^\nu b_\kappa^{(\eta)}(z)/f(z)\equiv 0 \bmod 2,\quad \eta<\nu.$$

From this observation it follows that, for $0\le\lambda\le\nu$, the expression

$$h^\nu(\det{}_0\Delta_q)^{(\lambda)}/f(z)=\sum_{\kappa=0}^{q-2}\sum_{\eta=0}^{\lambda}(-1)^\kappa\binom{\lambda}{\eta}(\det\Delta_{\kappa,0})^{(\lambda-\eta)}h^\nu b_\kappa^{(\eta)}(z)/f(z)$$

is an integral power series, and that

$$h^\nu(\det{}_0\Delta_q)^{(\lambda)}/f(z)\equiv\begin{Bmatrix}z^{\alpha_0/2}h^\nu b_0^{(\nu)}(z)/f(z), & \lambda=\nu\\ 0, & \lambda<\nu\end{Bmatrix} \bmod 2. \tag{5.31}$$

From (5.31) in turn, we conclude that each summand of Σ (and hence Σ itself) is an integral power series, and that

$$\Sigma\equiv\sum_{\nu=1}^{\frac{q-1}{2}}d_q^{(\nu)}z^{q+\nu-1}(\det\Delta_q)^{\frac{q+1}{2}-1}h^\nu(\det{}_0\Delta_q)^{(\nu)}/f(z) \bmod 2. \tag{5.32}$$

Next, using the fact that, by Lemma 18,

$$d_q^{(\nu)}\equiv 1 \pmod 2 \ \text{ if, and only if, }\ \nu=\frac{q-1}{2},\quad 0\le\nu\le\frac{q-1}{2},$$

the right-hand side of (5.32) in its turn is congruent modulo 2 to

$$z^{\frac{3q-3}{2}}(\det\Delta_q)^{\frac{q-1}{2}}h^{\frac{q-1}{2}}(\det{}_0\Delta_q)^{(\frac{q-1}{2})}/f(z),$$

which, in view of (5.31) and Lemmas 20(i) and 22(ii), simplifies further to give

$$
\begin{aligned}
\Sigma &\equiv z^{\frac{\alpha_0+3q-3}{2}}(\det\Delta_q)^{\frac{q-1}{2}}h^{\frac{q-1}{2}}b_0^{(\frac{q-1}{2})}(z)/f(z)\\
&\equiv z^{\frac{\frac{q+1}{2}\alpha_0+3q-3}{2}}\Big\{z^2h^{\frac{q-1}{2}}f^{(\frac{q-1}{2})}(z)/f(z)+z^{\frac{3q+1}{2}}h^{q-1}f^{(q-1)}(z)/f(z)\Big\}\\
&\equiv z^{\frac{\frac{q+1}{2}\alpha_0+3q+1}{2}}\big(\mathcal S_q^H(z)\big)^{\frac{q-1}{2}}+z^{\frac{\frac{q+1}{2}\alpha_0+6q-2}{2}}\big(\mathcal S_q^H(z)\big)^{q-1}.
\end{aligned}
$$

Putting all the pieces together and dividing by $z^{\frac{q+1}{4}\alpha_0+1}$, we obtain the surprisingly elegant congruence

$$z + \mathcal{S}_q^H(z) + z^{3q-2}\big(\mathcal{S}_q^H(z)\big)^{q-1} \equiv 0 \bmod 2, \quad |H| \equiv 0 \pmod 2. \tag{5.33}$$

We are now in a position to establish our second main result.

Theorem 24. *Let q be an odd prime number. Then the number $N_q(n)$ of index n subgroups in the Hecke group $\mathfrak{H}(q)$ isomorphic to a free product of cyclic groups of order q is odd if, and only if, $n = 2 + 4(q-1)\eta$, where η is a non-negative integer satisfying the condition that*

$$\mathfrak{s}_2((q-1)\eta + 1) = \mathfrak{s}_2(\eta) + \mathfrak{s}_2((q-2)\eta + 1). \tag{5.34}$$

Here, as before, $\mathfrak{s}_2(x)$ is the sum of digits in the binary expansion of the positive integer x.

Proof. Recall that, by (5.2), the number $N_q(n)$ is the same modulo 2 as the number $s_q^H(n)$ for a group H of even order. On the other hand, Equation (5.33) is a functional equation for the generating function of the $s_q^H(n)$'s, taken modulo 2. We now use this functional equation to determine $s_q^H(n)$ modulo 2, and thereby $N_q(n)$ modulo 2 as well.

Define an integral power series $\hat{\mathcal{S}}_q^H(z)$ by means of the equation

$$\hat{\mathcal{S}}_q^H(z) = z + z^{3q-2}\big(\hat{\mathcal{S}}_q^H(z)\big)^{q-1}.$$

Then, in view of (5.33), we have

$$\hat{\mathcal{S}}_q^H(z) \equiv S_q^H(z) \bmod 2.$$

Setting

$$\hat{\mathcal{T}}_q^H(z) := z^{-1}\hat{\mathcal{S}}_q^H(z) = 1 + \sum_{n\geq 1} \hat{t}_q^H(n) z^n,$$

we obtain an integral power series with functional equation

$$\hat{\mathcal{T}}_q^H(z) = 1 + z^{4(q-1)}\big(\hat{\mathcal{T}}_q^H(z)\big)^{q-1}. \tag{5.35}$$

From the functional equation it is obvious that $\hat{T}_q^H(z)$ must be a power series in $z^{4(q-1)}$; that is, the coefficients $\hat{t}_q^H(n)$ must satisfy

$$n \not\equiv 0 \bmod 4(q-1) \implies \hat{t}_q^H(n) = 0, \quad n \geq 1. \tag{5.36}$$

Hence, introducing a series $\hat{\mathcal{U}}_q^H(v)$ via

$$\hat{\mathcal{U}}_q^H(v) = \sum_{\eta\geq 1} \hat{t}_q^H(4(q-1)\eta) v^\eta,$$

we have

$$\hat{\mathcal{T}}_q^H(z) - 1 = \hat{\mathcal{U}}_q^H(z^{4(q-1)}),$$

and, setting $v = z^{4(q-1)}$, we find from (5.35) that $\hat{\mathcal{U}}_q^H(v)$ satisfies the functional equation

$$\frac{\hat{\mathcal{U}}_q^H(v)}{(\hat{\mathcal{U}}_q^H(v) + 1)^{q-1}} = v.$$

Using the notation $\langle v^\eta\rangle f(v)$ for the coefficient of v^η in the power series $f(v)$, Lagrange inversion (cf. [32, Theorem 5.4.2]) implies that, for $\eta \ge 1$, we have

$$\begin{aligned}\langle v^\eta\rangle \hat{\mathcal{U}}_q^H(v) &= \eta^{-1}\langle \zeta^{\eta-1}\rangle (1+\zeta)^{(q-1)\eta}\\ &= \eta^{-1}\binom{(q-1)\eta}{\eta-1}\\ &= \frac{1}{(q-1)\eta+1}\binom{(q-1)\eta+1}{\eta}.\end{aligned}$$

Substituting back, $\hat{\mathcal{S}}_q^H(z)$ is found to be given explicitly by

$$\hat{\mathcal{S}}_q^H(z) = \sum_{\eta\ge 0} \frac{1}{(q-1)\eta+1}\binom{(q-1)\eta+1}{\eta} z^{4(q-1)\eta+1},$$

which in turn allows us to deduce that

$$s_q^H(n) \equiv \left.\begin{cases} 0; & n \not\equiv 2 \pmod{4q-4}\\ \frac{1}{(q-1)\eta+1}\binom{(q-1)\eta+1}{\eta}; & n = 2+4(q-1)\eta,\ \eta\ge 0\end{cases}\right\} \bmod 2, \quad n \ge 1. \tag{5.37}$$

Since q is an odd prime, and, hence, $(q-1)\eta+1$ is odd, we have shown that, for $|H|$ even, $s_q^H(n)$ is odd if, and only if, $n = 2+4(q-1)\eta$ for some $\eta \ge 0$ satisfying

$$v_2\left(\binom{(q-1)\eta+1}{\eta}\right) = 0.$$

Applying Kummer's formula (cf. [16, pp. 115–116])

$$v_2\left(\binom{a}{b}\right) = \mathfrak{s}_2(b) + \mathfrak{s}_2(a-b) - \mathfrak{s}_2(a)$$

for the 2-adic valuation of a binomial coefficient, we find that

$$v_2\left(\binom{(q-1)\eta+1}{\eta}\right) = \mathfrak{s}_2(\eta) + \mathfrak{s}_2((q-2)\eta+1) - \mathfrak{s}_2((q-1)\eta+1),$$

and our statement concerning $s_q^H(n)$ can be rewritten as

$s_q^H(n) \equiv 1 \pmod 2$ if, and only if, $n = 2+4(q-1)\eta$ for some $\eta \ge 0$ satisfying (5.34).

In view of (5.2), this establishes the theorem. □

In the case where q is a Fermat prime we can be more explicit.

Corollary 25. *If q is a Fermat prime, then $N_q(n)$ is odd if, and only if, $n = \frac{4(q-1)^{\sigma+1}-2q}{q-2}$ for some $\sigma \ge 0$.*

Proof. If q is a Fermat prime, that is, $q-1 = 2^\lambda$ is a non-trivial 2-power, then

$$\mathfrak{s}_2((q-1)\eta+1) = 1 + \mathfrak{s}_2(\eta),$$

and Equation (5.34) simplifies to

$$\mathfrak{s}_2((q-2)\eta+1) = 1. \tag{5.38}$$

Therefore $(q-2)\eta+1$ must be a 2-power, $(q-2)\eta+1=2^\tau$, say. Equivalently, this is

$$(2^\lambda-1)\eta=2^\tau-1,$$

from which we infer that τ must be a multiple of λ, $\tau=\lambda\sigma$ say. Hence, we find that η must be of the form

$$\eta=\frac{2^{\lambda\sigma}-1}{2^\lambda-1},\quad \sigma\ge 0;$$

and, conversely, for these values of η, Equation (5.38) indeed holds true. We conclude that, in the case when q is a Fermat prime, $N_q(n)$ is odd if, and only if,

$$n=2+4(q-1)\frac{(q-1)^\sigma-1}{q-2}=\frac{4(q-1)^{\sigma+1}-2q}{q-2},\quad \sigma\ge 0,$$

and the corollary is proven. □

Remark. A detailed analysis of (5.26) in the case when $h=|H|$ is odd, making use of Lemma 21, eventually leads to a new proof of Theorem 2, the case where $q\equiv 3 \pmod 4$ being particularly involved.

6. The main result

Here we summarize our findings concerning the parity behaviour of the generalized subgroup numbers of the groups $\Gamma_m(q)$ from the previous sections. If we combine Proposition 1 with Theorems 2, 16, and 24, then we obtain the following result.

Theorem 26. *For $m,n\ge 1$, an odd prime q, and a finite group H with $\gcd(m,|H|)=1$ we have*

$$s^H_{\Gamma_m(q)}(n)=\sum_{d\mid m} s^H_{\Gamma_d(q)}(1,n),$$

where $s^H_{\Gamma_d(q)}(1,n)\equiv 1 \pmod 2$ if, and only if,

$$n=2d(1+2(q-1)\eta)\ \text{with}\ \mathfrak{s}_2((q-1)\eta+1)=\mathfrak{s}_2(\eta)+\mathfrak{s}_2((q-2)\eta+1)\ \text{and}\ q\nmid d,$$

or

$$n=d(1+2(q-1)\eta)\ \text{with}\ \mathfrak{s}_2((q-1)\eta+1)=\mathfrak{s}_2(\eta)+\mathfrak{s}_2((q-2)\eta+1)\ \text{and}\ 2\nmid d,\ q\nmid d,\ 2\nmid |H|.$$

In the case where q is a Fermat prime, we can be more explicit. Namely, if we combine Proposition 1 with the particular statement in Theorem 2, Theorem 16, and Corollary 25, we arrive at the following conclusion.

Corollary 27. *For $m,n\ge 1$, a Fermat prime q, and a finite group H with $\gcd(m,|H|)=1$ we have*

$$s^H_{\Gamma_m(q)}(n)=\sum_{d\mid m} s^H_{\Gamma_d(q)}(1,n),$$

where $s^H_{\Gamma_d(q)}(1,n)\equiv 1 \pmod 2$ if, and only if,

$$n=2d\,\frac{2(q-1)^\sigma-q}{q-2}\ \text{with}\ \sigma\ge 1\ \text{and}\ q\nmid d,$$

or

$$n = d\,\frac{2(q-1)^\sigma - q}{q-2} \quad \textit{with } \sigma \ge 1,\ 2 \nmid d,\ q \nmid d,\ \textit{and } 2 \nmid |H|.$$

Let us fix a Fermat prime $q = 2^\lambda + 1$. Suppose that p is an odd prime with the property that

$$\textit{the multiplicative group generated by } q-1 \textit{ does not contain } 2^{-1}q \textit{ modulo } p. \tag{6.1}$$

Then the equation

$$t_1(2(q-1)^{\sigma_1} - q) = t_2(2(q-1)^{\sigma_2} - q) \tag{6.2}$$

has no solutions $(t_1, t_2, \sigma_1, \sigma_2)$ where $p \mid t_1$, but $p \nmid t_2$, since otherwise we would have

$$2(q-1)^{\sigma_2} \equiv q \bmod p,$$

contrary to our assumption on p. Hence, if q is a Fermat prime, and if the prime divisors of m are among the set consisting of 2, q, and primes p satisfying Condition (6.1), then we obtain for all H with $\gcd(m, |H|) = 1$ that

$$s^H_{\Gamma_m(q)}(n) \equiv 1 \pmod 2 \text{ if, and only if, } n = t\,\frac{2(q-1)^\sigma - q}{q-2} \text{ with } \sigma \ge 1,\ t \mid 2m,\ q \nmid t,$$
$$\text{and } t \text{ even for } |H| \text{ even.} \tag{6.3}$$

Statement (6.3) raises the question which primes satisfy Condition (6.1) for a given Fermat prime q. This problem is addressed in our next result, for $q = 3, 5, 17$. For larger Fermat primes the calculations involved, though essentially trivial, become unwieldy, and are omitted.

Proposition 28.

(i) *All prime numbers* $p \equiv 7, 17 \pmod{24}$ *satisfy Condition* (6.1) *with* $q = 3$.
(ii) *All prime numbers* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$ *satisfy Condition* (6.1) *with* $q = 5$.
(iii) *All prime numbers*

$$p \equiv 7, 13, 19, 21, 23, 31, 35, 39, 41, 43, 53, 57, 59, 63, 65, 67, 69, 71, 73, 77, 79, 83,$$
$$93, 95, 97, 105, 113, 115, 117, 123, 125, 129 \pmod{136}$$

satisfy Condition (6.1) *with* $q = 17$.

Proof. This is a simple application of quadratic reciprocity. Let us first consider the case when $q = 3$. If $p \ne 3$ is an odd prime not satisfying Condition (6.1) with $q = 3$, then we have

$$2^\alpha \equiv 3 \bmod p$$

for some $\alpha \ge 1$, implying $\left(\frac{3}{p}\right) = +1$ or $\left(\frac{6}{p}\right) = +1$, according to whether or not α is even. Hence, every prime $p \equiv \pm 1 \pmod 8$ not satisfying (6.1) with $q = 3$ has the property that $\left(\frac{3}{p}\right) = +1$. By quadratic reciprocity,

$$\left(\frac{p}{3}\right) = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4, \end{cases}$$

for each prime p not satisfying (6.1) with $q = 3$ and such that $p \equiv \pm 1 \pmod 8$. It follows from this that every prime p such that

$$p \equiv \pm 1 \pmod 8 \;\text{ and }\; \left(\frac{p}{3}\right) = \begin{cases} -1, & p \equiv 1 \pmod 4, \\ +1, & p \equiv 3 \pmod 4, \end{cases}$$

will satisfy Condition (6.1) with $q = 3$. Thus, both

$$p \equiv 1 \pmod 8 \;\text{ and }\; p \equiv 2 \pmod 3$$

as well as

$$p \equiv 7 \pmod 8 \;\text{ and }\; p \equiv 1 \pmod 3$$

are hypotheses sufficient to ensure that p meets Condition (6.1) with $q = 3$. The first pair of congruences is equivalent to $p \equiv 17 \pmod{24}$, while the second one is equivalent to $p \equiv 7 \pmod{24}$, whence Assertion (i).

For a Fermat prime q with $q > 3$, we have $q \equiv 1 \pmod 4$, so

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

for any odd prime $p \neq q$ by quadratic reciprocity. Consequently, if p is such that $p \equiv \pm 1 \pmod 8$ and (6.1) does not hold for p, then we find that

$$1 = \left(\frac{2q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

while for $p \equiv \pm 3 \pmod 8$ such that (6.1) does not hold, we obtain $\left(\frac{p}{q}\right) = -1$. Hence, every prime p satisfying either

$$p \equiv \pm 1 \pmod 8 \;\text{ and }\; \left(\frac{p}{q}\right) = -1$$

or

$$p \equiv \pm 3 \pmod 8 \;\text{ and }\; \left(\frac{p}{q}\right) = +1$$

will meet Condition (6.1). Thus, it only remains to translate the statement concerning $\left(\frac{p}{q}\right)$ into a congruence condition modulo q, and to solve the resulting pairs of congruences, each pair leading to an equivalent congruence conditon for p modulo $8q$.

For $q = 5$, we have

$$\left(\frac{p}{5}\right) = +1 \;\text{ if, and only if, }\; p \equiv \pm 1 \pmod 5,$$

so both

$$p \equiv \pm 1 \pmod 8 \;\text{ and }\; p \equiv 2, 3 \pmod 5$$

as well as

$$p \equiv \pm 3 \pmod 8 \;\text{ and }\; p \equiv 1, 4 \pmod 5$$

ensure that p meets Condition (6.1) with $q = 5$. This yields Part (ii), while a corresponding calculation for $q = 17$ gives Assertion (iii). $\square$

For q a Fermat prime and m subject only to the condition that $\gcd(m, |H|) = 1$, we claim that (6.3) holds true for $n \geq \frac{4m^2}{q-2}$. To prove this, it suffices to give an upper bound for non-diagonal solutions of Equation (6.2). Assume that $t_2 > t_1$. Then

$$0 < \sigma_1 - \sigma_2 < \frac{\log t_2/t_1}{\log(q-1)}, \tag{6.4}$$

and we compute:

$$\begin{aligned} t_2\big(2(q-1)^{\sigma_2} - q\big) &= \gcd\Big(t_1\big(2(q-1)^{\sigma_1} - q\big), t_2\big(2(q-1)^{\sigma_2} - q\big)\Big) \\ &\leq \gcd\Big(t_1t_2\big(2(q-1)^{\sigma_1} - q\big) - t_1t_2\big(2(q-1)^{\sigma_1} - q(q-1)^{\sigma_1-\sigma_2}\big), \\ &\qquad\qquad t_2\big(2(q-1)^{\sigma_2} - q\big)\Big) \\ &\leq \gcd\Big(qt_1t_2\big((q-1)^{\sigma_1-\sigma_2} - 1\big), t_2\big(2(q-1)^{\sigma_2} - q\big)\Big) \\ &\leq t_2 \gcd\Big(t_1\big((q-1)^{\sigma_1-\sigma_2} - 1\big), 2(q-1)^{\sigma_2} - q\Big) \\ &< t_2^2, \end{aligned}$$

where we have used (6.4) in the last step. Our claim follows now from Corollary 27 and the fact that $t_2 \leq 2m$.

In particular, we see from the last observation and (6.3), that the parity behaviour of $s_{\Gamma_m}^H(n)$ as a function in n determines m up to a power of q, provided that $\gcd(m, |H|) = 1$.

As a final example, we compute the parity behaviour of $s_{\Gamma_m(q)}^H(n)$ for $q = 3$ and $m = 625$. We have to determine the non-diagonal solutions of the equation

$$t_1(2^{\sigma_1+1} - 3) = t_2(2^{\sigma_2+1} - 3) \tag{6.5}$$

for $\sigma_1, \sigma_2 \geq 1$ and $t_1, t_2 \mid 1250$. We have $t_1 \equiv t_2 \pmod 2$; thus, we may concentrate on the case when both t_1 and t_2 are odd, bearing in mind that each non-diagonal solution of (6.5) with t_1, t_2 odd gives rise to two non-diagonal solutions, namely $(t_1, t_2, \sigma_1, \sigma_2)$ and $(2t_1, 2t_2, \sigma_1, \sigma_2)$.

Suppose without loss of generality that $t_2 > t_1$, and let $\delta := v_5(t_2) - v_5(t_1)$. For $\delta = 1$, we deduce that $2^{\sigma_1+1} \equiv 3 \pmod 5$, which is equivalent to $\sigma_1 \equiv 2 \pmod 4$. The case where $\sigma_1 = 2$ leads to the solutions

$$(t_1, t_2, \sigma_1, \sigma_2) = (5^a, 5^{a+1}, 2, 1), \quad a = 0, 1, 2, 3. \tag{6.6}$$

If $\sigma_1 = 6, 10$, then 2^{σ_2+1} would have to equal 28 respectively 412, which is impossible; while for $\sigma_1 \geq 14$, we deduce that

$$2^{\sigma_2+1} - 3 \geq \frac{2^{15} - 3}{5} = 6553,$$

contradicting the estimate

$$2^{\sigma_2+1} - 3 < t_2 \leq 625$$

obtained above. Hence, the only non-diagonal solutions of (6.5) with t_1 and t_2 odd and $\delta = 1$ are given by (6.6).

For $\delta = 2$, we get that $2^{\sigma_1+1} \equiv 3 \pmod{25}$, which is equivalent to $\sigma_1 \equiv 6 \pmod{20}$. The case where $\sigma_1 = 6$ leads to the solutions

$$(t_1, t_2, \sigma_1, \sigma_2) = (5^a, 5^{a+2}, 6, 2), \quad a = 0, 1, 2. \tag{6.7}$$

If $\sigma_1 \geq 26$, then we deduce that

$$2^{\sigma_2+1} - 3 \geq \frac{2^{27} - 3}{5^2} = 5368709,$$

again contradicting the estimate $2^{\sigma_2+1} - 3 < t_2$. Consequently (6.7) describes the only non-diagonal solutions of (6.5) with t_1, t_2 odd and $\delta = 2$.

For $\delta = 3$, we have $2^{\sigma_1+1} \equiv 3 \pmod{125}$, which is equivalent to $\sigma_1 \equiv 6 \pmod{100}$, leading to the solutions

$$(t_1, t_2, \sigma_1, \sigma_2) = (5^a, 5^{a+3}, 6, 1), \quad a = 0, 1. \tag{6.8}$$

Finally, for $\delta = 4$, we have $2^{\sigma_1+1} \equiv 3 \pmod{625}$, which is equivalent to $\sigma_1 \equiv 106 \pmod{500}$. But 106 is already well above the range allowed for σ_1. Hence, there is precisely one non-diagonal solution of (6.5) for $n = 5, 10, 25, 50, 3125, 6250$; there are exactly three non-diagonal solutions for $n = 125, 250, 625, 1250$; and there are no non-diagonal solutions for other values of n. Consequently, for $\gcd(5, |H|) = 1$, Assertion (6.3) holds true for $n > 6250$, while for $n \leq 6250$ we have

$$\begin{aligned} &s^H_{\Gamma_{625}(3)}(n) \equiv 1 \bmod 2 \text{ if, and only if,} \\ &\qquad n = 1, 2, 13, 26, 29, 58, 61, 65, 122, 125, 130, 145, 250, 253, 290, 305, 325, 506, \\ &\qquad 509, 610, 625, 650, 725, 1018, 1021, 1250, 1265, 1450, 1525, 1625, 2042, 2045, \\ &\qquad\qquad 2530, 2545, 3050, 3250, 3625, 4090, 4093, 5090, 5105 \end{aligned}$$

if $|H|$ is odd, and

$$\begin{aligned} &s^H_{\Gamma_{625}(3)}(n) \equiv 1 \bmod 2 \text{ if, and only if,} \\ &\qquad n = 2, 26, 58, 122, 130, 250, 290, 506, 610, 650, 1018, 1250, 1450, 2042, 2530, \\ &\qquad\qquad 3050, 3250, 4090, 5090 \end{aligned}$$

for $|H|$ even.

Acknowledgements

The authors are indebted to the anonymous referee for a careful reading of the manuscript, and for helpful suggestions concerning the presentation of the material.

Appendix. Proofs of some auxiliary results

A.1. Proof of Lemma 11. Suppose first that $\rho_1 \equiv \rho_2 \equiv \cdots \equiv \rho_\alpha \equiv 1 \pmod 4$. It is well known that the 2-adic valuation of the multinomial coefficient $\binom{\rho_1+\rho_2+\ldots+\rho_\alpha}{\rho_1,\rho_2\ldots,\rho_\alpha}$ is equal to the number of carries, C say, occurring during addition of the numbers $\rho_1, \rho_2 \ldots, \rho_\alpha$. If we assume that, in total, we find E_ℓ 1's as the ℓ-th digit in the binary representations of $\rho_1, \rho_2 \ldots, \rho_\alpha$, then

$$C = \left\lfloor \frac{E_0}{2} \right\rfloor + \left\lfloor \frac{E_1 + \lfloor \frac{E_0}{2} \rfloor}{2} \right\rfloor + \left\lfloor \frac{E_2 + \left\lfloor \frac{E_1 + \lfloor \frac{E_0}{2} \rfloor}{2} \right\rfloor}{2} \right\rfloor + \cdots$$

$$\geq \left\lfloor \frac{E_0}{2} \right\rfloor + \left\lfloor \frac{\lfloor \frac{E_0}{2} \rfloor}{2} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{\lfloor \frac{E_0}{2} \rfloor}{2} \right\rfloor}{2} \right\rfloor + \cdots = \sum_{\ell \geq 1} \left\lfloor \frac{E_0}{2^\ell} \right\rfloor .$$

According to our assumption, we have $E_0 = \alpha$, whence

$$v_2\left(\binom{\rho_1+\rho_2+\ldots+\rho_\alpha}{\rho_1,\rho_2\ldots,\rho_\alpha}\right) = C \geq \sum_{\ell \geq 1} \left\lfloor \frac{\alpha}{2^\ell} \right\rfloor = v_2(\alpha!).$$

The second assertion is established in a similar manner. □

A.2. Proof of Lemma 13. Let $k = \sum_{j\geq 0} k_j 2^j$ be the 2-adic expansion of k. Then

$$2^\lambda k + 1 = 1 \cdot 2^0 + 0 \cdot 2^1 + \cdots + 0 \cdot 2^{\lambda-1} + \sum_{j \geq 0} k_j 2^{j+\lambda}$$

is the 2-adic expansion of $2^\lambda k + 1$. Suppose first that k is odd. Then $k_0 = 1$, and so

$$k - 1 = 0 \cdot 2^0 + \sum_{j\geq 1} k_j 2^j.$$

By Lucas' congruence (cf., for instance, [3, Theorem 3.4.1]), $\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2$ is equivalent to the conjunction of

$$k_1 = k_2 = \cdots = k_{\lambda-1} = 0 \tag{A.1}$$

and

$$k_{\mu+\lambda} \leq k_\mu, \quad \mu \geq 0. \tag{A.2}$$

The conjunction of (A.1) and (A.2) in turn is equivalent to

$$k_j = 0 \ (j \not\equiv 0 \pmod \lambda) \ \text{ and } \ k_{\mu\lambda} \leq k_{(\mu-1)\lambda} \ (\mu \geq 1). \tag{A.3}$$

Let $\sigma \geq 1$ be smallest with the property that $k_{\sigma\lambda} = 0$. Then $k_{\mu\lambda} = 1$ for $\mu = 0, 1, \ldots, \sigma-1$ and $k_{\mu\lambda} = 0$ for $\mu \geq \sigma$, so, by (A.3),

$$k = \sum_{0 \leq \mu \leq \sigma-1} 2^{\lambda\mu} = \frac{2^{\lambda\sigma}-1}{2^\lambda - 1}, \quad \sigma \geq 1.$$

Hence,

$$\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2 \text{ if, and only if, } k = \frac{2^{\lambda\sigma}-1}{2^\lambda - 1} \text{ for some } \sigma \geq 1, \quad k \text{ odd.} \tag{A.4}$$

Now suppose that k is even, and write

$$k = 0 \cdot 2^0 + \cdots + 0 \cdot 2^{r-1} + 1 \cdot 2^r + \sum_{j>r} k_j 2^j$$

with some $r \geq 1$ (such r must exist since $k > 0$). Then

$$k - 1 = 1 \cdot 2^0 + \cdots + 1 \cdot 2^{r-1} + 0 \cdot 2^r + \sum_{j>r} k_j 2^j$$

is the 2-adic expansion of $k-1$ in this case. We now distinguish two cases, according to whether or not $\lambda = 1$.

(i) If $\lambda > 1$, then the coefficient of 2^1 in $2^\lambda k + 1$ vanishes, while, for $r \geq 2$, the corresponding coefficient of $k-1$ equals 1. Hence, $\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2$ together with $\lambda > 1$ forces $r = 1$, so that the expansion of $k-1$ reads

$$k - 1 = 1 \cdot 2^0 + 0 \cdot 2^1 + \sum_{j \geq 2} k_j 2^j.$$

Now, again by Lucas' theorem, $\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2$ is equivalent to the conjunction of

$$k_0 = k_2 = \cdots = k_{\lambda-1} = 0,\ k_1 = 1 \tag{A.5}$$

and

$$k_j \leq k_{j-\lambda}, \quad j \geq \lambda. \tag{A.6}$$

The conjunction of (A.5) and (A.6) in turn is equivalent to

$$k_j = 0\ (j \not\equiv 1 \pmod \lambda) \text{ and } k_{\mu\lambda+1} \leq k_{(\mu-1)\lambda+1}\ (\mu \geq 1). \tag{A.7}$$

Let $\sigma \geq 1$ be smallest with the property that $k_{\sigma\lambda+1} = 0$, so that $k_{\mu\lambda+1} = 1$ for $0 \leq \mu \leq \sigma - 1$ and $k_{\mu\lambda+1} = 0$ for $\mu \geq \sigma$. Thus, by (A.7),

$$k = \sum_{0 \leq \mu \leq \sigma-1} 2^{\lambda\mu+1} = 2\Bigg(\sum_{0 \leq \mu \leq \sigma-1} 2^{\lambda\mu}\Bigg) = \frac{2^{\lambda\sigma+1}-2}{2^\lambda - 1}.$$

Hence,

$$\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2 \text{ if, and only if,}$$

$$k = \frac{2^{\lambda\sigma+1}-2}{2^\lambda - 1} \text{ for some } \sigma \geq 1, \quad (2 \mid k,\ \lambda \geq 2). \tag{A.8}$$

(ii) Now let $\lambda = 1$, so that

$$2^\lambda k + 1 = 1 \cdot 2^0 + \sum_{j \geq 0} k_j 2^{j+1}.$$

Application of Lucas' congruence shows that, in this case, $\binom{2^\lambda k+1}{k-1} \equiv 1 \pmod 2$ is equivalent to the conjunction of

$$k_0 = k_1 = \cdots = k_{r-2} = 1,\ k_{r-1} = 0,\ k_r = 1, \tag{A.9}$$

and

$$k_j \le k_{j-1}, \quad j > r. \tag{A.10}$$

Since, by definition of r, we have $k_j = 0$ for $0 \le j < r$, we again conclude that $r = 1$, so that the conjunction of (A.9) and (A.10) is now equivalent to

$$k_0 = 0,\ k_1 = 1,\ k_j \le k_{j-1}\,(j \ge 2). \tag{A.11}$$

Let $\sigma \ge 1$ be smallest with the property that $k_{\sigma+1} = 0$. Then $k_\mu = 1$ for $1 \le \mu \le \sigma$, and $k_\mu = 0$ for $\mu > \sigma$, and so, by (A.11),

$$k = \sum_{1 \le \mu \le \sigma} 2^\mu = 2^{\sigma+1} - 2.$$

Thus,

$$\binom{2^\lambda k + 1}{k-1} \equiv 1 \pmod 2 \ \text{ if, and only if, } \ k = 2^{\sigma+1} - 2 \ \text{ for some } \sigma \ge 1, \quad (2 \mid k,\ \lambda = 1). \tag{A.12}$$

Our claim (4.22) follows now from (A.4), (A.8), and (A.12). □

A.3. Proof of Lemma 17. We use induction on k. For $k = 0, 1$, Equation (5.13) is trivial, while for $k = 2$ it follows from (5.11) with $k = 1$. Suppose that (5.13) holds for $k \le K$ with some integer $K \ge 2$. Then, by (5.11) with $k = K$, the inductive hypothesis, and the definition of the coefficient systems $\left(c_k^{(\mu)}\right)$ and $\left(d_k^{(\nu)}\right)$, we have

$$\begin{aligned}
F_{K+1} &= azF_K(z) + hz^2F_{K-1}(z) + hz^3F'_{K-1}(z) \\
&= az\Bigg\{\sum_{\mu=0}^{\lfloor\frac{K}{2}\rfloor} c_K^{(\mu)}h^\mu z^{K+\mu}F_0^{(\mu)} + \sum_{\nu=0}^{\lfloor\frac{K-1}{2}\rfloor} d_K^{(\nu)}h^\nu z^{K+\nu-1}F_1^{(\nu)}\Bigg\} \\
&\qquad + hz^2\Bigg\{\sum_{\mu=0}^{\lfloor\frac{K-1}{2}\rfloor} c_{K-1}^{(\mu)}h^\mu z^{K+\mu-1}F_0^{(\mu)} + \sum_{\nu=0}^{\lfloor\frac{K-2}{2}\rfloor} d_{K-1}^{(\nu)}h^\nu z^{K+\nu-2}F_1^{(\nu)}\Bigg\} \\
&\qquad + hz^3\Bigg\{\sum_{\mu=0}^{\lfloor\frac{K-1}{2}\rfloor} c_{K-1}^{(\mu)}h^\mu z^{K+\mu-1}F_0^{(\mu)} + \sum_{\nu=0}^{\lfloor\frac{K-2}{2}\rfloor} d_{K-1}^{(\nu)}h^\nu z^{K+\nu-2}F_1^{(\nu)}\Bigg\}' \\
&= (ac_K^{(0)} + hKc_{K-1}^{(0)})z^{K+1}F_0(z) \\
&\qquad + \sum_{\mu=1}^{\lfloor\frac{K-1}{2}\rfloor}(ac_K^{(\mu)} + h(K+\mu)c_{K-1}^{(\mu)} + c_{K-1}^{(\mu-1)})h^\mu z^{K+\mu+1}F_0^{(\mu)}(z) \\
&\qquad + h^{\lfloor\frac{K+1}{2}\rfloor}z^{K+\lfloor\frac{K+1}{2}\rfloor+1}F_0^{(\lfloor\frac{K+1}{2}\rfloor)}(z) \times \begin{cases} c_{K-1}^{(\frac{K-1}{2})}, & K \text{ odd} \\ ac_K^{(K/2)} + c_{K-1}^{(\frac{K-2}{2})}, & K \text{ even}\end{cases} \\
&\qquad + (ad_K^{(0)} + h(K-1)d_{K-1}^{(0)})z^KF_1(z) \\
&\qquad + \sum_{\nu=1}^{\lfloor\frac{K-2}{2}\rfloor}(ad_K^{(\nu)} + h(K+\nu-1)d_{K-1}^{(\nu)} + d_{K-1}^{(\nu-1)})z^{K+\nu}h^\nu F_1^{(\nu)}(z) \\
&\qquad + h^{\lfloor\frac{K}{2}\rfloor}z^{K+\lfloor\frac{K}{2}\rfloor}F_1^{(\lfloor\frac{K}{2}\rfloor)}(z) \times \begin{cases} ad_K^{(\frac{K-1}{2})} + d_{K-1}^{(\frac{K-3}{2})}, & K \text{ odd} \\ d_{K-1}^{(\frac{K-2}{2})}, & K \text{ even}\end{cases} \\
&= c_{K+1}^{(0)}z^{K+1}F_0(z) + \sum_{\mu=1}^{\lfloor\frac{K-1}{2}\rfloor} c_{K+1}^{(\mu)}h^\mu z^{K+\mu+1}F_0^{(\mu)}(z) \\
&\qquad + c_{K+1}^{(\lfloor\frac{K+1}{2}\rfloor)}h^{\lfloor\frac{K+1}{2}\rfloor}z^{K+\lfloor\frac{K+1}{2}\rfloor+1}F_0^{(\lfloor\frac{K+1}{2}\rfloor)}(z) \\
&\qquad + d_{K+1}^{(0)}z^KF_1(z) + \sum_{\nu=1}^{\lfloor\frac{K-2}{2}\rfloor} d_{K+1}^{(\nu)}h^\nu z^{K+\nu}F_1^{(\nu)}(z) \\
&\qquad + d_{K+1}^{(\lfloor\frac{K}{2}\rfloor)}h^{\lfloor\frac{K}{2}\rfloor}z^{K+\lfloor\frac{K}{2}\rfloor}F_1^{(\lfloor\frac{K}{2}\rfloor)}(z) \\
&= \sum_{\mu=0}^{\lfloor\frac{K+1}{2}\rfloor} c_{K+1}^{(\mu)}h^\mu z^{K+\mu+1}F_0^{(\mu)}(z) + \sum_{\nu=0}^{\lfloor\frac{K}{2}\rfloor} d_{K+1}^{(\nu)}h^\nu z^{K+\nu}F_1^{(\nu)}(z),
\end{aligned}$$

as required. □

A.4. Explicit description of the coefficients $\omega_{\kappa,\lambda}$ and $b_\kappa(z)$. We have

$$
\omega_{\kappa,\lambda}=
\begin{cases}
d_{q-1}^{(0)}z^{q}-1; & \kappa=\lambda=0\\
d_{q-1}^{(\lambda)}z^{\lambda+q}; & \kappa=0,\ \lambda=1,\dots,\frac{q-3}{2}\\
d_{q}^{(0)}z^{q-1}+b; & \kappa=1,\ \lambda=0\\
d_{q}^{(\lambda)}z^{\lambda+q-1}; & \kappa=1,\ \lambda=1,\dots,\frac{q-1}{2}\\
d_{\kappa-1}^{(0)}hz^{\kappa-2}+bd_{\kappa}^{(0)}z^{\kappa-1} & \\
\qquad +d_{\kappa+q-1}^{(0)}z^{\kappa+q-2}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=0\\
-((\lambda-1)d_{\kappa-1}^{(\lambda)}h+d_{\kappa-1}^{(\lambda-1)})z^{\kappa+\lambda-2} & \\
\qquad +bd_{\kappa}^{(\lambda)}z^{\kappa+\lambda-1}+d_{\kappa+q-1}^{(\lambda)}z^{\kappa+\lambda+q-2}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=1,\dots,\frac{\kappa-3}{2}\\
-d_{\kappa-1}^{(\frac{\kappa-3}{2})}z^{\frac{3\kappa-5}{2}}+bd_{\kappa}^{(\frac{\kappa-1}{2})}z^{\frac{3\kappa-3}{2}} & \\
\qquad +d_{\kappa+q-1}^{(\frac{\kappa-1}{2})}z^{\frac{3\kappa+2q-5}{2}}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa-1}{2}\\
d_{\kappa+q-1}^{(\lambda)}z^{\kappa+\lambda+q-2}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa+1}{2},\dots,\frac{\kappa+q-2}{2}\\
d_{\kappa-1}^{(0)}hz^{\kappa-2}+bd_{\kappa}^{(0)}z^{\kappa-1} & \\
\qquad +d_{\kappa+q-1}^{(0)}z^{\kappa+q-2}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=0\\
-((\lambda-1)d_{\kappa-1}^{(\lambda)}h+d_{\kappa-1}^{(\lambda-1)})z^{\kappa+\lambda-2} & \\
\qquad +bd_{\kappa}^{(\lambda)}z^{\kappa+\lambda-1}+d_{\kappa+q-1}^{(\lambda)}z^{\kappa+\lambda+q-2}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=1,\dots,\frac{\kappa-2}{2}\\
-d_{\kappa-1}^{(\frac{\kappa-2}{2})}z^{\frac{3\kappa-4}{2}}+d_{\kappa+q-1}^{(\kappa/2)}z^{\frac{3\kappa+2q-4}{2}}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=\frac{\kappa}{2}\\
d_{\kappa+q-1}^{(\lambda)}z^{\kappa+\lambda+q-2}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=\frac{\kappa+2}{2},\dots,\frac{\kappa+q-3}{2}\\
0; & \text{otherwise,}
\end{cases}
$$

and

$$b_\kappa(z) =$$

$$\begin{cases}
-(az+bz^2+c^{(0)}_{q-1}z^{q+1})f(z) - \sum_{\mu=1}^{\frac{q-1}{2}} c^{(\mu)}_{q-1}h^\mu z^{\mu+q+1}f^{(\mu)}(z); & \kappa=0 \\
-c^{(0)}_q z^q f(z) - h(c^{(1)}_q z^{q+1}-z)f'(z) - \sum_{\mu=2}^{\frac{q-1}{2}} c^{(\mu)}_q h^\mu z^{\mu+q}f^{(\mu)}(z); & \kappa=1 \\
-(bc^{(0)}_\kappa z^\kappa + c^{(0)}_{\kappa+q-1}z^{\kappa+q-1})f(z) & \\
\quad - \sum_{\mu=1}^{\frac{\kappa-1}{2}} ((c^{(\mu-1)}_{\kappa-1} - \mu h c^{(\mu)}_{\kappa-1})z^{\kappa+\mu-1} & \\
\qquad + bc^{(\mu)}_\kappa z^{\kappa+\mu} + c^{(\mu)}_{\kappa+q-1}z^{\kappa+\mu+q-1})h^\mu f^{(\mu)}(z) & \\
\quad -(c^{(\frac{\kappa-1}{2})}_{\kappa-1} z^{\frac{3\kappa-1}{2}} + c^{(\frac{\kappa+1}{2})}_{\kappa+q-1} z^{\frac{3\kappa+2q-1}{2}})h^{\frac{\kappa+1}{2}} f^{(\frac{\kappa+1}{2})}(z) & \\
\quad - \sum_{\mu=\frac{\kappa+3}{2}}^{\frac{\kappa+q-2}{2}} c^{(\mu)}_{\kappa+q-1}h^\mu z^{\kappa+\mu+q-1}f^{(\mu)}(z); & 3\le\kappa\le q-2,\ \kappa \text{ odd} \\
-(bc^{(0)}_\kappa z^\kappa + c^{(0)}_{\kappa+q-1}z^{\kappa+q-1})f(z) & \\
\quad - \sum_{\mu=1}^{\frac{\kappa-2}{2}} ((-\mu h c^{(\mu)}_{\kappa-1} - c^{(\mu-1)}_{\kappa-1})z^{\kappa+\mu-1} & \\
\qquad + bc^{(\mu)}_\kappa z^{\kappa+\mu} + c^{(\mu)}_{\kappa+q-1}z^{\kappa+\mu+q-1})h^\mu f^{(\mu)}(z) & \\
\quad -(-c^{(\frac{\kappa-2}{2})}_{\kappa-1} z^{\frac{3\kappa-2}{2}} + bc^{(\kappa/2)}_\kappa z^{3\kappa/2} + c^{(\kappa/2)}_{\kappa+q-1} z^{\frac{3\kappa+2q-2}{2}})h^{\kappa/2} f^{(\kappa/2)}(z) & \\
\quad - \sum_{\mu=\frac{\kappa+2}{2}}^{\frac{\kappa+q-1}{2}} c^{(\mu)}_{\kappa+q-1}h^\mu z^{\kappa+\mu+q-1}f^{(\mu)}(z); & 2\le\kappa\le q-3,\ \kappa \text{ even.}
\end{cases}$$

A.5. Proof of Lemma 20. Using Lemma 18 plus the facts that h is even and that b is odd (recall (5.1)), we find that, for $0 \le \kappa, \lambda \le q-2$,

$$\omega_{\kappa,\lambda} \equiv \left\{\begin{matrix*}[l] 1; & \kappa=\lambda=0 \\ z^{\frac{3\kappa-3}{2}}; & 1\le\kappa\le q-2,\ \kappa \text{ odd},\ \lambda=\frac{\kappa-1}{2} \\ z^{\frac{3\kappa+3q-6}{2}}; & 1\le\kappa\le q-2,\ \kappa \text{ odd},\ \lambda=\frac{\kappa+q-2}{2} \\ z^{\frac{3\kappa-4}{2}}; & 2\le\kappa\le q-3,\ \kappa \text{ even},\ \lambda=\frac{\kappa}{2} \\ 0; & \text{otherwise} \end{matrix*}\right\} \bmod 2. \tag{A.13}$$

(i) Writing

$$\det \Delta_q \equiv \sum_{\sigma\in \mathrm{Sym}(\{0,1,\ldots,q-2\})} \omega_{0,\sigma(0)}\omega_{1,\sigma(1)}\cdots\omega_{q-2,\sigma(q-2)} \bmod 2, \tag{A.14}$$

we see that the only non-zero contribution on the right-hand side occurs for the permutation σ given by

$$\sigma(\kappa) = \begin{cases} \frac{\kappa+q-2}{2}; & 1\le\kappa\le q-2,\ \kappa \text{ odd} \\ \frac{\kappa}{2}; & 0\le\kappa\le q-3,\ \kappa \text{ even.} \end{cases} \tag{A.15}$$

Indeed, we clearly must have $\sigma(0)=0$, which in turn forces $\sigma(1)=\frac{q-1}{2}$; further, for $\kappa\ge 2$ even, we must have $\sigma(\kappa)=\kappa/2$, and this in turn forces $\sigma(\kappa)=\frac{\kappa+q-2}{2}$ for $\kappa\ge 3$ odd, since the alternative value $\frac{\kappa-1}{2}$ already occurs as image of the even number $\kappa-1$. It follows that, modulo 2,

$$\det\Delta_q\equiv z^{\frac{3q-3}{2}}\cdot\prod_{\substack{3\le\kappa\le q-2\\ \kappa\,\text{odd}}} z^{\frac{3\kappa+3q-6}{2}}\cdot\prod_{\substack{2\le\kappa\le q-3\\ \kappa\,\text{even}}} z^{\frac{3\kappa-4}{2}}\equiv z^e,$$

where

$$\begin{aligned} e&=\frac{3(q-1)}{2}+\sum_{\substack{3\le\kappa\le q-2\\ \kappa\,\text{odd}}}\frac{3\kappa+3q-6}{2}+\sum_{\substack{2\le\kappa\le q-3\\ \kappa\,\text{even}}}\frac{3\kappa-4}{2}\\ &=\frac{3(q-1)}{2}+\frac{9(q-1)(q-3)}{8}+\frac{3(q-1)(q-3)}{8}-(q-3)\\ &=\frac{3q^2-11q+12}{2}. \end{aligned}$$

The fact that

$$\det\Delta_q\equiv\det\Delta_{0,0}\bmod 2$$

follows immediately by expanding $\det\Delta_q$ modulo 2 with respect to the 0-th row.

(ii) For $1\le\kappa\le q-2$, we have

$$\det\Delta_{\kappa,0}\equiv\sum_\sigma \omega_{0,\sigma(0)}\cdots\omega_{\kappa-1,\sigma(\kappa-1)}\omega_{\kappa+1,\sigma(\kappa+1)}\cdots\omega_{q-2,\sigma(q-2)}\equiv 0\bmod 2.$$

Here, σ runs through all bijections of the set $\{0,\dots,\kappa-1,\kappa+1,\dots,q-2\}$ onto the set $\{1,2,\dots,q-2\}$, and $\omega_{0,\sigma(0)}\equiv 0\pmod 2$ for each such σ. $\square$

A.6. Proof of Lemma 21 (sketch). Using Lemma 18 plus the facts that h and b are odd, we find that, for $0\le\kappa,\lambda\le q-2$,

$$\omega_{\kappa,\lambda}\equiv\left\{\begin{matrix}1; & \kappa=\lambda=0\\ z^{\frac{3q-3}{2}}; & \kappa=0,\ \lambda=\frac{q-3}{2}\text{ even}\\ z^{\frac{3\kappa-7}{2}}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa-3}{2}\text{ even}\\ z^{\frac{3\kappa-5}{2}}+z^{\frac{3\kappa-3}{2}}; & 3\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa-1}{2}\text{ odd}\\ z^{\frac{3\kappa-3}{2}}; & 1\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa-1}{2}\text{ even}\\ z^{\frac{3\kappa+3q-6}{2}}; & 1\le\kappa\le q-2,\ \kappa\text{ odd},\ \lambda=\frac{\kappa+q-2}{2}\\ z^{\frac{3\kappa-6}{2}}+z^{\frac{3\kappa-4}{2}}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=\frac{\kappa-2}{2}\text{ even}\\ z^{\frac{3\kappa-4}{2}}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=\frac{\kappa}{2}\\ z^{\frac{3\kappa+3q-7}{2}}; & 2\le\kappa\le q-3,\ \kappa\text{ even},\ \lambda=\frac{\kappa+q-3}{2}\text{ even}\\ 0; & \text{otherwise}\end{matrix}\right\}\bmod 2. \tag{A.16}$$

First suppose that $q \equiv 1 \pmod 4$. For illustration, we display Δ_{13} modulo 2:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & z^{18} & 0 & 0 & 0 & 0 & 0\\
1+z & z & 0 & 0 & 0 & 0 & z^{19} & 0 & 0 & 0 & 0 & 0\\
z & z^2+z^3 & 0 & 0 & 0 & 0 & 0 & z^{21} & 0 & 0 & 0 & 0\\
0 & 0 & z^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & z^6 & 0 & 0 & 0 & 0 & 0 & z^{24} & 0 & 0 & 0\\
0 & 0 & z^6+z^7 & z^7 & 0 & 0 & 0 & 0 & z^{25} & 0 & 0 & 0\\
0 & 0 & z^7 & z^8+z^9 & 0 & 0 & 0 & 0 & 0 & z^{27} & 0 & 0\\
0 & 0 & 0 & 0 & z^{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & z^{12} & 0 & 0 & 0 & 0 & 0 & z^{30} & 0\\
0 & 0 & 0 & 0 & z^{12}+z^{13} & z^{13} & 0 & 0 & 0 & 0 & z^{31} & 0\\
0 & 0 & 0 & 0 & z^{13} & z^{14}+z^{15} & 0 & 0 & 0 & 0 & 0 & z^{33}
\end{pmatrix}$$

In the same way as in the proof of the preceding lemma, it can be seen that there is exactly one permutation in $\mathrm{Sym}(\{0,1,\dots,q-2\})$ leading to a non-zero contribution in the expansion (A.14) of the determinant of Δ_q modulo 2. This permutation is in fact the one in (A.15). The rest of the argument is completely analogous to the one before.

Now let $q \equiv 3 \pmod 4$. We illustrate this situation by displaying Δ_{11} modulo 2:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & z^{15} & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & z^{15} & 0 & 0 & 0 & 0\\
1+z & z & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
z & z^2+z^3 & 0 & 0 & 0 & 0 & z^{18} & 0 & 0 & 0\\
0 & 0 & z^4 & 0 & 0 & 0 & z^{19} & 0 & 0 & 0\\
0 & 0 & z^6 & 0 & 0 & 0 & 0 & z^{21} & 0 & 0\\
0 & 0 & z^6+z^7 & z^7 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & z^7 & z^8+z^9 & 0 & 0 & 0 & 0 & z^{24} & 0\\
0 & 0 & 0 & 0 & z^{10} & 0 & 0 & 0 & z^{25} & 0\\
0 & 0 & 0 & 0 & z^{12} & 0 & 0 & 0 & 0 & z^{27}
\end{pmatrix}. \tag{A.17}$$

Here, there are more permutations leading to non-zero contributions in the expansion (A.14) of $\det \Delta_q$ modulo 2. Namely, there are precisely two non-zero entries modulo 2 in the 0-th row, occurring in columns 0 and $(q-3)/2$. If we decree that $\sigma(0) = 0$, then there is precisely one way to complete this into a permutation leading to a non-zero contribution in the expansion of $\det \Delta_q$ modulo 2, namely the permutation (A.15). If, on the other hand, we set $\sigma(0) = \frac{q-3}{2}$, then the sum of the contributions corresponding to this subset of permutations is given by the minor of Δ_q formed by deleting the 0-th row and the $\frac{q-3}{2}$-th column. This minor can be further reduced by observing that every other column in the right half of the minor contains precisely one non-zero entry modulo 2. (In (A.17), these are the 5-th, 7-th, and 9-th column.) In our running example, it is seen in this way that $\det \Delta_{11}$ modulo 2 equals the determinant

$$\det \begin{pmatrix} 1+z & z & 0 & 0 & 0 & 0 \\ z & z^2+z^3 & 0 & 0 & z^{18} & 0 \\ 0 & 0 & z^4 & 0 & z^{19} & 0 \\ 0 & 0 & z^6+z^7 & z^7 & 0 & 0 \\ 0 & 0 & z^7 & z^8+z^9 & 0 & z^{24} \\ 0 & 0 & 0 & 0 & 0 & z^{25} \end{pmatrix}.$$

From the form of the above matrix, it is obvious that its determinant is equal to

$$\det \begin{pmatrix} 1+z & z \\ z & z^2+z^3 \end{pmatrix} \cdot z^{19} \cdot \det \begin{pmatrix} z^6+z^7 & z^7 \\ z^7 & z^8+z^9 \end{pmatrix} \cdot z^{25} = \pm z^{60}(z^2+2z)^2 \equiv z^{64} \bmod 2.$$

In general, this pattern that the minor under consideration can be expanded as a product of powers of z and 2×2-minors, each of which contributes only a power of z, persists and, in the end, leads to the result asserted in (i).

The argument for establishing the formulae for the minors is similar. □

A.7. Proof of Lemma 22. We shall use the formula

$$\frac{d^\nu}{dz^\nu} A(B(z)) = \sum_{\substack{\pi_1,\dots,\pi_\nu \ge 0 \\ \pi_1+2\pi_2+\dots+\nu\pi_\nu=\nu}} \frac{\nu!}{\prod_{j\ge1}(j!)^{\pi_j}\pi_j!} \left[\prod_{j\ge1} \left(B^{(j)}(z)\right)^{\pi_j}\right] A^{(\pi_1+\dots+\pi_\nu)}(B(z)) \tag{A.18}$$

for the derivatives of a composite function, which is known as the Faà di Bruno formula (cf. [6, Sec. 3.4]; but see also [7, 15]). In view of the left-hand side, Formula (A.18) implies in particular the integrality assertion in Item (i). In fact, the coefficients occurring in (A.18) have a natural combinatorial interpretation (see [1, Theorem 13.2]).

Applying (A.18) with $A(t) = e^t$ and $B(z) = h^{-1} \int \mathcal{S}_\Gamma^H(z)\,dz$, Equation (5.22) follows immediately in view of (5.5).

Finally, using the facts that $\left(\mathcal{S}_\Gamma^H(z)\right)^{(j)} \equiv 0 \pmod 2$ for $j \ge 2$, and that

$$\frac{\nu!}{(\nu-2\mu)!2^\mu\mu!} = \binom{\nu}{2\mu} \cdot \prod_{1\le k\le\mu} (2k-1) \equiv \binom{\nu}{2\mu} \bmod 2,$$

we find from (5.22) that, modulo 2,

$$h^\nu\Big(\frac{d^\nu}{dz^\nu}\mathcal{H}_\Gamma^H(z)\Big)\Big/\mathcal{H}_\Gamma^H(z) \equiv \sum_{\substack{\pi_1,\pi_2\ge0 \\ \pi_1+2\pi_2=\nu}} h^{\nu-\pi_1-\pi_2} \frac{\nu!}{\prod_{j=1}^2 (j!)^{\pi_j}\pi_j!} \prod_{j=1}^2 \Big(\big(\mathcal{S}_\Gamma^H(z)\big)^{(j-1)}\Big)^{\pi_j}$$

$$\equiv \sum_{\mu=0}^{\lfloor \frac{\nu}{2} \rfloor} h^\mu \binom{\nu}{2\mu} \Big(\big(\mathcal{S}_\Gamma^H(z)\big)'\Big)^\mu \big(\mathcal{S}_\Gamma^H(z)\big)^{\nu-2\mu},$$

in accordance with (5.23). Our last claim (5.24) is an immediate consequence of (5.23). □

References

[1] G. E. Andrews, *The Theory of Partitions*, Encyclopedia of Math. and its Applications, Vol. 2, Addison–Wesley, Reading, 1976; reprinted by Cambridge University Press, Cambridge, 1998.

[2] R. Bieri, *Homological Dimension of Discrete Groups*, Queen Mary College Mathematics Notes, second edition, London, 1981 (first edition 1976).

[3] P. J. Cameron, *Combinatorics*, Cambridge University Press, 1994.

[4] I. M. Chiswell, Exact sequences associated with a graph of groups, *J. Pure and Appl. Algebra* **8** (1976), 63–74.

[5] S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups I, *Can. J. Math.* **3** (1951), 328–334.

[6] L. Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, Holland, 1974.

[7] A. D. D. Craik, Prehistory of Faà di Bruno's formula, *Amer. Math. Monthly* **112** (2005), 119–130.

[8] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Sitz.ber. Königl. Preuss. Akad. Wiss. Berlin* (1895), 981–993.

[9] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, *Sitz.ber. Königl. Preuss. Akad. Wiss. Berlin* **44** (1903), 987–991.

[10] C. Godsil, W. Imrich, and R. Razen, On the number of subgroups of given index in the modular group, *Monatshefte Math.* **87** (1979), 273–280.

[11] I. P. Goulden and D. M. Jackson, The combinatorial relationship between trees, cacti and certain connection coefficients for the symmetric group, *Europ. J. Combin.* **13** (1992), 357–365.

[12] M. Hall, *The Theory of Groups*, 2nd edition, Chelsea Publishing Company, New York, 1976.

[13] P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* (2) **36** (1934), 29–95.

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

[15] W. P. Johnson, The curious history of Faà di Bruno's formula, *Amer. Math. Monthly* **109** (2002), 217–234.

[16] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146. Reprinted in: Collected Papers (edited by A. Weil), Vol. I, 485–538, Springer, New York, 1975.

[17] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Math., vol. 212, Birkhäuser, Basel, 2003.

[18] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer, New York, 1977.

[19] M. H. Millington, Subgroups of the classical modular group, *J. London Math. Soc.* (2) **1** (1969), 351–357.

[20] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory*, John Wiley & Sons, New York, 1966.

[21] T. W. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.

[22] T. W. Müller, Subgroup growth of free products, *Invent. math.* **126** (1996), 111–131.

[23] T. W. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118–154.

[24] T. W. Müller, Representations in finite wreath products: Enumerative theory and applications, in: *Proc. Groups Korea '98* (Y. G. Baik, D. L. Johnson, and A. C. Kim eds.), Walter de Gruyter, Berlin, 2000, 243–290.

[25] T. W. Müller, Five lectures on generalized permutation representations, *Mat. Contemp.* **20** (2001), 227–272.

[26] T. W. Müller, Modular subgroup arithmetic in free products, *Forum Math.* **15** (2003), 759–810.

[27] T. W. Müller, Modular subgroup arithmetic, in: *Groups, Combinatorics and Geometry* (Durham 2001; A. A. Ivanov, M. W. Liebeck, and J. Saxl, eds.), World Scientific, Singapore, 2003, pp. 193–225.

[28] T. W. Müller, Parity patterns in Hecke groups and Fermat primes, in: *Groups: Topological, Combinatorial and Arithmetic Aspects*, (T. W. Müller ed.), LMS Lecture Notes Series 311, Cambridge University Press, Cambridge, 2004, 327–374.

[29] T. W. Müller and J.-C. Schlage–Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.
[30] H. Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, *Hokkaido Math. J.* **28** (1999), 71–85.
[31] G.-C. Rota, On the foundations of combinatorial theory I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2** (1964), 340–368.
[32] R. P. Stanley, *Enumerative Combinatorics I*, Wadsworth, Belmont (California), 1986.
[33] W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh, Sec. A* **78** (1977), 105–112.
[34] B. A. F. Wehrfritz, *Finite Groups*, World Scientific, Singapore, 1999.

Fakultät für Mathematik, Universität Wien, Nordbergstrasse 15, A-1090 Vienna, Austria

School of Mathematical Sciences, Queen Mary & Westfield College, University of London, Mile End Road, London E1 4NS, United Kingdom