FREE SUBGROUP NUMBERS MODULO PRIME POWERS: THE NON-PERIODIC CASE

C. KRATTENTHALER[†] AND T. W. MÜLLER[*]

Abstract. In [*J. Algebra* **452** (2016), 372–389], we characterise when the sequence of free subgroup numbers of a finitely generated virtually free group Γ is ultimately periodic modulo a given prime power. Here, we show that, in the remaining cases, in which the sequence of free subgroup numbers is not ultimately periodic modulo a given prime power, the number of free subgroups of index λ in Γ is — essentially — congruent to a binomial coefficient times a rational function in λ modulo a power of a prime that divides a certain invariant of the group Γ, respectively to a binomial sum involving such numbers. These results, apart from their intrinsic interest, in particular allow for a much more efficient computation of congruences for free subgroup numbers in these cases compared to the direct recursive computation of these numbers implied by the generating function results in [*J. London Math. Soc.* (2) **44** (1991), 75–94].

1. Introduction

For a finitely generated virtually free group Γ, denote by m_Γ the least common multiple of the orders of the finite subgroups in Γ. Moreover, for a positive integer λ, let $f_\lambda(\Gamma)$ be the number of free subgroups of index λm_Γ in Γ. A concrete example of a (non-free) finitely generated virtually free group that the reader may want to keep in mind is the inhomogeneous modular group $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$, where C_m denotes the cyclic group of order m. Here, we have $m_{\Gamma_0} = \mathrm{lcm}\{2,3\} = 6$, and the first few terms of the sequence $(f_\lambda(\Gamma_0))_{\lambda\ge1}$ are

$$5,\ 60,\ 1105,\ 27120,\ 828250,\ 30220800,\ 1282031525,\ 61999046400,\ 3366961243750,\ \dots$$

In [6], a complete characterisation is given of all pairs (Γ, p^α) for which the sequence $(f_\lambda(\Gamma))_{\lambda\ge1}$ is ultimately periodic modulo p^α, where Γ is a finitely generated virtually free group, p is a prime number, and α is a positive integer. As it turns out, somewhat surprisingly, this is always the case, unless $\mu_p(\Gamma) = 0$ and $\mu(\Gamma) \ge 2$,[1] where $\mu_p(\Gamma)$ and $\mu(\Gamma)$ are certain invariants of Γ defined in Section 2. In our running example $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z})$, we have $\mu(\Gamma_0) = 2$, $\mu_2(\Gamma_0) = \mu_3(\Gamma_0) = 0$, and $\mu_p(\Gamma_0) = 1$ for $p \ge 5$. Indeed, the sequence $(f_\lambda(\mathrm{PSL}_2(\mathbb{Z})))_{\lambda\ge1}$ is ultimately periodic modulo p^α for $p \ge 5$ and all α, and non-periodic for $p = 2, 3$; see [3], [2, Sec. 8], [4, Sec. 16], where more precise

---

2010 *Mathematics Subject Classification.* Primary 05A15; Secondary 05E99 11A07 20E06 20E07 68W30.

Key words and phrases. virtually free groups, free subgroup numbers, congruences, Gosper–Zeilberger algorithm.

[†]Research partially supported by the Austrian Science Foundation FWF, grants Z130-N13 and S50-N15, the latter in the framework of the Special Research Program "Algorithmic and Enumerative Combinatorics"

[*]Research supported by Lise Meitner Grant M1661-N25 of the Austrian Science Foundation FWF.

[1]The condition $\mu(\Gamma) \ge 2$ is equivalent to the assertion that Γ contains a non-Abelian free subgroup.

results are obtained for the free subgroup numbers of the inhomogeneous modular group and certain lifts thereof.

Our present paper focuses on the case of non-periodic behaviour. It is shown in [10] that, for $\mu_p(\Gamma) = 0$ and $\mu(\Gamma) \geq 2$, the function $f_\lambda(\Gamma)$ satisfies the congruence

$$f_\lambda(\Gamma) \equiv (-1)^{\frac{(\mu(\Gamma)-1)\lambda+1}{p-1}} \frac{1}{\lambda} \binom{\frac{\mu(\Gamma)\lambda}{p-1}}{\frac{\lambda-1}{p-1}} \pmod p, \tag{1.1}$$

where the binomial coefficient is defined to be zero whenever the lower argument is not an integer; cf. [10, Eqn. (35)].

The purpose of the present paper is to demonstrate that, under the same assumptions, the function $f_\lambda(\Gamma)$ satisfies a very similar congruence modulo an *arbitrary* p-power. More precisely, if $\mu(\Gamma) \equiv 0, 1 \pmod p$, the function $f_\lambda(\Gamma)$, when reduced modulo any fixed p-power, is congruent to a (quasi-)rational factor in λ times a binomial coefficient (see Corollary 8 in Section 6), while in the remaining cases the right-hand side takes the form of a sum of such expressions (see Corollary 12 in the same section). A remarkable consequence of these results is that, while it may be safely conjectured that the generating function for the free subgroup numbers (which satisfies a highly non-linear differential equation obtained from (2.8) via (2.6)) is not D-finite, implying that the sequence of free subgroup numbers itself is not P-recursive,[2] its reduction modulo any fixed p-power is (see Corollary 7).

While the result obtained in Corollary 8 for arbitrary p-powers is 'as good as' the mod p result (1.1), we show in Proposition 13 that the sum described in Corollary 12 satisfies an inhomogeneous linear recurrence of finite depth with constant coefficients and leading coefficient 1 (which may be found automatically by means of the Gosper–Zeilberger algorithm; cf. [11]). This leads again to an efficient computation of $f_\lambda(\Gamma)$ modulo p^α. All these results are presented in Section 6, and are illustrated there by concrete examples.

The only known earlier results concerning congruences of free subgroup numbers modulo prime powers in the non-periodic case covered the following scenarios: (i) lifts of Hecke groups $\mathfrak{H}(q) \cong C_2 * C_q$ with q a Fermat prime and $p = 2$, and (ii) lifts of the classical modular group $\mathfrak{H}(3) \cong \mathrm{PSL}_2(\mathbb{Z})$ and $p = 3$; see Section 8, Corollary 34 and Theorem 35 in [2], and [4, Sec. 16]. In particular, the behaviour of $f_\lambda(\Gamma)$ modulo p-powers in these known cases fits into the framework of the semi-automatic method for obtaining congruences developed in [2, 4, 5], and further (unpublished) work. As we show in this paper, for finitely generated virtually free groups Γ and primes p with $\mu_p(\Gamma) = 0$ and $\mu(\Gamma) \geq 2$, this is always the case.

This semi-automatic method is based on a generating function approach, featuring a basic series — to be adapted for each class of applications — which is then used to express the generating function for the sequence of numbers we have in mind, reduced modulo a given p-power, as a polynomial in this basic series. We show in Theorem 6 in Section 5 that, if $\mu_p(\Gamma) = 0$ and $\mu(\Gamma) \geq 2$, we may choose the series

$$\Phi(z) = \sum_{n=1}^{\infty} (-1)^{\frac{(\mu(\Gamma)-1)n+1}{p-1}} \frac{1}{n} \binom{\frac{\mu(\Gamma)n}{p-1}}{\frac{n-1}{p-1}} z^n \tag{1.2}$$

[2]The reader is referred to [13, Ch. 6] for information on D-finite series and P-recursive sequences.

as basic series (i.e., the series formed out of the coefficients on the right-hand side of (1.1)) in order to express the generating function $\sum_{\lambda=1}^{\infty} f_\lambda(\Gamma)\, z^\lambda$ modulo p-powers as a polynomial in $\Phi(z)$. Corollaries 8 and 12 alluded to above are consequences of Theorem 6. The proof of the theorem requires some auxiliary results which are presented in Section 4. These include some interesting determinant evaluations, see Lemmas 4 and 5.

A remarkable feature of the present application of our semi-automatic generating function method is that the degree of the polynomial in the basic series $\Phi(z)$ expressing the generating function $\sum_{\lambda=1}^{\infty} f_\lambda(\Gamma)\, z^\lambda$ modulo p^α does not increase with α. As a consequence, the complexity of the computation only mildly increases with α. This is in sharp contrast to our previous applications of this method. The reason for the above phenomenon lies in the fact that $\Phi(z)$ satisfies an *exact* functional equation over the integers, namely (4.1), while in our previous applications the basic series satisfied functional equations modulo p^α of complexity increasing with α.

Our results concerning the function $f_\lambda(\Gamma)$ are complemented by Theorem 2 in Section 3, which precisely characterises those finitely generated virtually free groups Γ with $\mu(\Gamma) \geq 2$ and $\mu_p(\Gamma) = 0$ for a given prime number p.

2. Some preliminaries on finitely generated virtually free groups

Our notation and terminology concerning virtually free groups and their decomposition in terms of a graph of groups follows Serre's book [12]; in particular, the category of graphs used in the context of graphs of groups is described in [12, §2]. This category deviates slightly from the usual notions in graph theory. In order to distinguish the objects of this category from graphs in the sense of graph theory, we call them *S-graphs*. Specifically, an *S-graph* X consists of two sets: $E(X)$, the set of (directed) *edges*, and $V(X)$, the set of *vertices*. The set $E(X)$ is endowed with a fixed-point-free involution $^- : E(X) \to E(X)$ (*reversal of orientation*), and there are two functions $o, t : E(X) \to V(X)$ assigning to an edge $e \in E(X)$ its *origin* $o(e)$ and *terminus* $t(e)$, such that $t(\bar{e}) = o(e)$. The reader should note that, according to the above definition, S-graphs may have loops (that is, edges e with $o(e) = t(e)$) and multiple edges (that is, several edges with the same origin and the same terminus). An *orientation* $\mathcal{O}(X)$ consists of a choice of exactly one edge in each pair $\{e, \bar{e}\}$ (this is indeed always a pair – even for loops – since, by definition, the involution $^-$ is fixed-point-free). Such a pair is called a *geometric edge*. For our running example $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$, we may choose $V(X) = \{v_1, v_2\}$ and $E(X) = \{e, \bar{e}\}$. Figure 1.a shows the corresponding S-graph X.

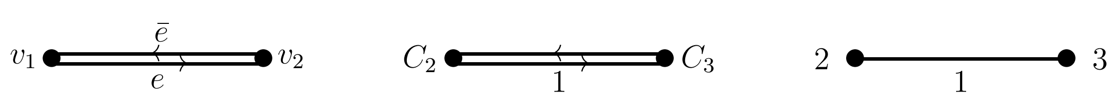

Figure 1. a. An S-graph, for $\mathrm{PSL}_2(\mathbb{Z})$ b. a graph of groups, c. an order graph

Let Γ be a finitely generated virtually free group with Stallings decomposition $(\Gamma(-), X)$; that is, $(\Gamma(-), X)$ is a finite graph of finite groups with fundamental group $\pi_1(\Gamma(-), X) \cong \Gamma$. Figure 1.b shows a graph of groups with fundamental group

$\mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$. Replacing the stabiliser groups of vertices and edges by their respective group orders and replacing each pair $(e, \bar{e})$ by one unoriented edge, we obtain the corresponding *order graph* of Γ. Abstractly, an *order graph* is a finite connected unoriented graph (in the sense of graph theory; multiple edges and loops are allowed) whose vertices v and edges e carry positive integers, $n(v)$, respectively $n(e)$, as labels such that $n(e) \mid n(v)$ if v is incident to e. The labels of vertices and edges will frequently be referred to as their respective *order*. Figure 1.c shows the order graph for $\mathrm{PSL}_2(\mathbb{Z})$ corresponding to the graph of groups in Figure 1.b.

As in the introduction, denote by m_Γ the least common multiple of the orders of the finite subgroups in Γ, so that, in terms of the above Stallings decomposition of Γ,

$$m_\Gamma = \operatorname{lcm}\big\{|\Gamma(v)| :\, v \in V(X)\big\}. \tag{2.1}$$

(This formula essentially follows from the well-known fact that a finite group has a fixed point when acting on a tree.) The *type* $\tau(\Gamma)$ of a finitely generated virtually free group $\Gamma \cong \pi_1(\Gamma(-), X)$ is defined as the tuple

$$\tau(\Gamma) = \big(m_\Gamma; \zeta_1(\Gamma), \dots, \zeta_\kappa(\Gamma), \dots, \zeta_{m_\Gamma}(\Gamma)\big),$$

where the $\zeta_\kappa(\Gamma)$'s are integers indexed by the divisors κ of m_Γ, given by

$$\zeta_\kappa(\Gamma) = \big|\big\{e \in \mathcal{O}(X) :\, |\Gamma(e)| \,\big|\, \kappa\big\}\big| - \big|\big\{v \in V(X) :\, |\Gamma(v)| \,\big|\, \kappa\big\}\big|. \tag{2.2}$$

(Here, $\mathcal{O}(X)$ is any orientation of the S-graph X.) It can be shown that the type $\tau(\Gamma)$ is in fact an invariant of the group Γ, i.e., independent of the particular decomposition of Γ in terms of a graph of groups $(\Gamma(-), X)$, and that two finitely generated virtually free groups Γ_1 and Γ_2 contain the same number of free subgroups of index n for each positive integer n if, and only if, $\tau(\Gamma_1) = \tau(\Gamma_2)$; cf. [9, Theorem 2]. We have $\zeta_\kappa(\Gamma) \geq 0$ for $\kappa < m_\Gamma$ and $\zeta_{m_\Gamma}(\Gamma) \geq -1$ with equality occurring in the latter inequality if, and only if, Γ is the fundamental group of a tree of groups; cf. [8, Prop. 1] or [9, Lemma 2]. In our running example of the inhomogeneous modular group $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z})$, we have $m_{\Gamma_0} = \operatorname{lcm}\{2, 3\} = 6$, $\zeta_1(\Gamma_0) = 1$, $\zeta_2(\Gamma_0) = \zeta_3(\Gamma_0) = 0$, and $\zeta_6(\Gamma_0) = -1$.

Inspection of (2.1) and (2.2) reveals the noteworthy fact that all ingredients of the type (that is, m_Γ and the ζ_κ's) depend only on the orders but not on the internal structure of the stabilisers of vertices and edges of $(\Gamma(-), X)$. Therefore it makes sense to attach the same invariants to the order graph obtained from the graph of groups $(\Gamma(-), X)$ in the way described earlier, or, more generally, to an abstract order graph. Specifically, given an order graph G, we define m_G to be the least common multiple of the vertex orders $n(v)$, taken over all vertices of G, and, for a divisor κ of m_G, we let

$$\zeta_\kappa(G) = \big|\big\{e \in E(G) :\, n(e) \mid \kappa\big\}\big| - \big|\big\{v \in V(G) :\, n(v) \mid \kappa\big\}\big|, \tag{2.3}$$

where $V(G)$ denotes the set of vertices of G and $E(G)$ the set of edges.

Define a *torsion-free* Γ*-action* on a set Ω to be a Γ-action on Ω which is free when restricted to finite subgroups, and let

$$g_\lambda(\Gamma) := \frac{\text{number of torsion-free } \Gamma\text{-actions on a set with } \lambda m_\Gamma \text{ elements}}{(\lambda m_\Gamma)!}, \quad \lambda \geq 0; \tag{2.4}$$

in particular, $g_0(\Gamma) = 1$. (There exists an explicit product formula for $g_\lambda(\Gamma)$ in terms of a corresponding graph of groups, see [9, Prop. 3].) The sequences $\big(f_\lambda(\Gamma)\big)_{\lambda \geq 1}$ and

$\big(g_\lambda(\Gamma)\big)_{\lambda\geq 0}$ are related via the Hall-type transformation formula[3]

$$\sum_{\mu=0}^{\lambda-1} g_\mu(\Gamma) f_{\lambda-\mu}(\Gamma) = m_\Gamma \lambda g_\lambda(\Gamma), \quad \lambda \geq 1. \tag{2.5}$$

Introducing the generating functions

$$F_\Gamma(z) := \sum_{\lambda=1}^{\infty} f_\lambda(\Gamma) z^\lambda \text{ and } G_\Gamma(z) := \sum_{\lambda=0}^{\infty} g_\lambda(\Gamma) z^\lambda,$$

Equation (2.5) is seen to be equivalent to the relation

$$F_\Gamma(z) = m_\Gamma z \frac{d}{dz}\big(\log G_\Gamma(z)\big). \tag{2.6}$$

Define the *free rank* $\mu(\Gamma)$ of a finitely generated virtually free group Γ to be the rank of a free subgroup of index m_Γ in Γ (existence of such a subgroup follows, for instance, from Lemmas 8 and 10 in [12]; it need not be unique, though). It can be shown that the free rank $\mu(\Gamma)$ may be expressed in terms of the type of Γ via

$$\mu(\Gamma) = 1 + \sum_{\kappa \mid m_\Gamma} \varphi(m_\Gamma/\kappa)\zeta_\kappa(\Gamma), \tag{2.7}$$

where φ is Euler's totient function. This formula implies in particular that $\mu(\Gamma)$ is well-defined. In our running example $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z})$, we have

$$\mu(\Gamma_0) = 1 + \varphi(6)\zeta_1(\Gamma_0) + \varphi(3)\zeta_2(\Gamma_0) + \varphi(2)\zeta_3(\Gamma_0) + \varphi(1)\zeta_6(\Gamma_0) = 2.$$

It is known that the sequence $g_\lambda(\Gamma)$ is of hypergeometric type and that its generating function $G_\Gamma(z)$ satisfies a homogeneous linear differential equation

$$\theta_0(\Gamma)G_\Gamma(z) \;+\; (\theta_1(\Gamma)z - m_\Gamma)G'_\Gamma(z) \;+\; \sum_{\mu=2}^{\mu(\Gamma)} \theta_\mu(\Gamma) z^\mu G_\Gamma^{(\mu)}(z) = 0 \tag{2.8}$$

of order $\mu(\Gamma)$ with integral coefficients $\theta_\mu(\Gamma)$ given by

$$\theta_\mu(\Gamma) = \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j} m_\Gamma(j+1) \prod_{\kappa\mid m_\Gamma} \prod_{\substack{1\leq k\leq m_\Gamma \\ (m_\Gamma,k)=\kappa}} (jm_\Gamma + k)^{\zeta_\kappa(\Gamma)}, \quad 0 \leq \mu \leq \mu(\Gamma); \tag{2.9}$$

cf. [9, Prop. 5]. The linear differential equation (2.8) can subsequently be translated into a Riccati-type differential equation for $F(z)$ via the relation (2.6). In our running example $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z})$, the differential equation (2.8) becomes

$$5G(z) + (72z - 6)G'(z) + 36z^2 G''(z) = 0,$$

which translates into the differential equation

$$5z + (6z - 1)F(z) + zF^2(z) + 6z^2 F'(z) = 0$$

satisfied by the generating function $F(z)$ for the free subgroup numbers $f_\lambda(\mathrm{PSL}_2(\mathbb{Z}))$.

[3]See [9, Cor. 1], or [1, Prop. 1] for a more general result.

For a finitely generated virtually free group Γ and a prime number p, we introduce, in formal analogy with formula (2.7), the *p-rank* $\mu_p(\Gamma)$ of Γ via the equation

$$\mu_p(\Gamma) = 1 + \sum_{p|\kappa|m_\Gamma} \varphi(m_\Gamma/\kappa)\zeta_\kappa(\Gamma). \tag{2.10}$$

Clearly, $\mu_p(\Gamma) \geq 0$, with equality occurring if, and only if, Γ is the fundamental group of a tree of groups, $p \mid m_\Gamma$, and $\zeta_\kappa(\Gamma) = 0$ for $p \mid \kappa \mid m_\Gamma$ and $\kappa < m_\Gamma$. As already mentioned in the introduction, for $\Gamma_0 = \mathrm{PSL}_2(\mathbb{Z})$ we have $\mu(\Gamma_0) = 2$, $\mu_2(\Gamma_0) = \mu_3(\Gamma_0) = 0$, and $\mu_p(\Gamma_0) = 1$ for $p \geq 5$. Since the free rank $\mu(\Gamma)$ and the p-rank $\mu_p(\Gamma)$ only depend on the type invariants m_Γ and the ζ_κ's, in view of our earlier discussion they may also be defined for abstract order graphs and, in particular, for an order graph G of a finitely generated virtually free group Γ. Doing so, one has $\mu(\Gamma) = \mu(G)$ and $\mu_p(\Gamma) = \mu_p(G)$. These conventions will be used in the proof of Theorem 2.

In what follows, it will be important to be able to represent a finitely generated virtually free group Γ by a graph of groups avoiding trivial amalgamations along a maximal tree. This is achieved via the following auxiliary result.

Lemma 1 (Normalisation)**.** *Let $(\Gamma(-), X)$ be a (connected) graph of groups with fundamental group Γ, and suppose that X has only finitely many vertices. Then there exists a graph of groups $(\Delta(-), Y)$ with $|V(Y)| < \infty$ and a spanning tree T in Y, such that $\pi_1(\Delta(-), Y) \cong \Gamma$, and such that*[4]

$$\Delta(e)^e \neq \Delta(t(e)) \text{ and } \Delta(e)^{\bar{e}} \neq \Delta(o(e)), \quad \text{for } e \in E(T). \tag{2.11}$$

Moreover, if $(\Gamma(-), X)$ satisfies the finiteness condition

(F_1) $\quad$ *X is a finite S-graph,*

or

(F_2) $\quad$ *$\Gamma(v)$ is finite for every vertex $v \in V(X)$,*

then we may choose $(\Delta(-), Y)$ so as to enjoy the same property.

See [7, Sec. 3] for a proof of this useful result. Subsequently, we shall call a graph of groups $(\Delta(-), Y)$ *normalised*, if it satisfies the conditions of the lemma for some spanning tree T of Y. In our situation, normalised graphs of groups will always be trees, so coincide with their respective spanning trees. We shall therefore suppress the reference to the spanning trees from now on.

3. Characterisation of finitely generated virtually free groups Γ with $\mu_p(\Gamma) = 0$

Recall (see paragraph below (2.10)) that, if a finitely generated virtually free group satisfies $\mu_p(\Gamma) = 0$ for a given prime p, then, in particular, Γ is the fundamental group of a tree of groups. Theorem 2 below tells us how a normalised (in the sense of Lemma 1) order tree[5] X underlying the Stallings decomposition $(\Gamma(-), X)$ of a finitely generated virtually free group Γ must be constructed so as to satisfy $\mu_p(\Gamma) = 0$.

[4] The notation used in Equation (2.11) follows Serre; see Déf. 8 in [12, Sec. 4.4].

[5] Here, *order tree* means an order graph which has the form of a tree.

Given a fixed prime number p, the starting point of our construction are certain finite rooted vertex-labelled trees which we call *divisor trees*. By definition, vertices of divisor trees are labelled by positive integers coprime to p. Moreover, any two adjacent vertices, say v_1 and v_2, with v_1 closer to the root than v_2, satisfy $\ell(v_2) \mid \ell(v_1)$ and $\ell(v_2) < \ell(v_1)$, where $\ell(v_1)$ and $\ell(v_2)$ denote the labels of v_1 and v_2. See Figure 2 for an example of such a divisor tree. There, the prime number to be fixed from the very beginning is $p = 5$. In the figure, the root is indicated by a square.

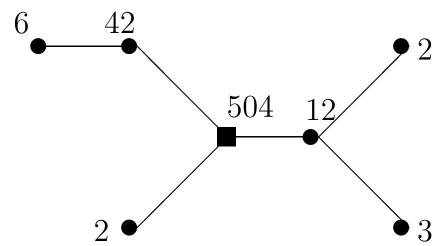

FIGURE 2. A divisor tree for $p = 5$

Given a divisor tree D, we fix a map f from the set of vertices of D into the set of (ordinary, unlabelled) finite rooted trees with the property that non-root vertices are mapped to non-trivial[6] trees rooted at a leaf and, in case D consists of just the root, this root must be mapped to a non-trivial tree (with no restriction on the location of the root). Figure 3 shows an example of such a map f defined on the vertices of the divisor tree in Figure 2. There, the roots of the image trees are indicated by little circles.

From D and f, we construct a certain class of order graphs. The reader is advised to consult Figure 4 while reading the description of this construction in the following paragraph. We remind the reader that, in that example, the fixed prime number is $p = 5$.

If v_1 and v_2 are adjacent in D, where v_1 is closer to the root than v_2, then we glue the root of $f(v_2)$ to one of the leaves of $f(v_1)$. If this is done for all edges of D, we obtain a rooted tree, U say, where the root of U is by definition the root of $f(r)$, with r being the root of D. In Figure 4, the root is again indicated by a square. Given some vertex v in D, we label the edges in $f(v)$ by $\ell(v)$ and the non-root vertices in $f(v)$ by $p \cdot \ell(v)$. The root of U (that is, the root of $f(r)$) is assigned a number which is a multiple of

$$p \cdot \operatorname{lcm}\{\ell(v) : v \in D\}.$$

Abusing notation, we write $f(D)$ for the set of order graphs resulting from this construction. All of them are trees. We shall occasionally use the term *order tree* for these order graphs.

Theorem 2. *Let $\Gamma \cong \pi_1(\Gamma(-), X)$ be a finitely generated virtually free group with $\mu(\Gamma) \geq 2$, where X is an S-graph which is assumed to be normalised in the sense of Lemma 1. Then $\mu_p(\Gamma) = 0$ if, and only if, there exist a divisor tree D and a map f as above from the set of vertices of D into the set of finite rooted trees such that the order tree corresponding to $(\Gamma(-), X)$ is in $f(D)$.*

[6]Here, 'non-trivial' means 'at least two vertices'.

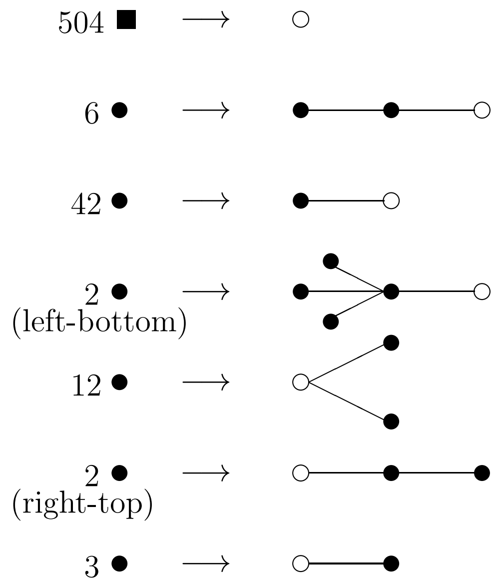

FIGURE 3. A function f on the vertices of the divisor tree of Figure 2

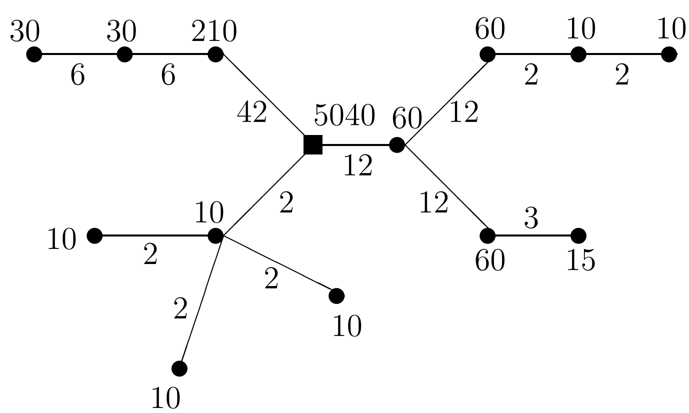

FIGURE 4. An order tree resulting from the divisor tree of Figure 2 and the function f from Figure 3

Proof. We start with the proof of the forward implication. We consider the order graph of $(\Gamma(-), X)$, which we denote by G. By the characterisation of groups Γ with $\mu_p(\Gamma) = 0$ given in the paragraph after (2.10), we know that G is a tree, that, using the identification of invariants of Γ and G discussed in Section 2, $p \mid m_G$, and that $\zeta_\kappa(G) = 0$ for $p \mid \kappa \mid m_G$ and $\kappa < m_G$. Also, since $(\Gamma(-), X)$ is normalised, we have $n(e) < n(v)$ if $v \in V(G)$ is incident with $e \in E(G)$.

Let m be the minimal order of vertices and edges in G. Since $(\Gamma(-), X)$ is assumed to be normalised and $\mu(\Gamma) \geq 2$, this order must be the order of an edge. Furthermore, m cannot be divisible by p since otherwise we would have

$$0 = \zeta_m(G) = \left|\left\{e \in E(G) : n(e) = m\right\}\right| > 0,$$

a contradiction.

In order to proceed, we need to introduce an auxiliary object. Let ℓ be a positive integer. We let $S_\ell(G)$ be the collection of subtrees of G consisting of those vertices and edges with orders dividing ℓ. It should be noted that the connected components of $S_\ell(G)$ need not be trees in the classical sense since they may contain edges with one or both of their vertices removed.

Next we consider $S_{pm}(G)$. We claim that $S_{pm}(G)$ consists of all vertices and edges with orders m or pm, but no other vertices or edges. Let us assume for a contradiction that there is a vertex v^* with $n(v^*) = pm'$ or an edge e^* with $n(e^*) = pm'$, $m' \mid m$ and $m' < m$, where m' is minimal with this property. If there should be such a vertex v^*, then it is incident with an edge $\tilde{e}$ with $n(\tilde{e})$ properly dividing $n(v^*) = pm'$. The order $n(\tilde{e})$ cannot be m' since this would contradict minimality of m. Thus, $n(\tilde{e}) = pm''$ with $m'' \mid m'$ and $m'' < m'$, contradicting the minimality of m'. On the other hand, if there is an edge e^* as above, then we have

$$0 = \zeta_{pm'}(G) = \left|\left\{e \in E(G) : n(e) \mid pm'\right\}\right| - \left|\left\{v \in V(G) : n(v) \mid pm'\right\}\right|.$$

Thus, there must be at least one vertex v with $n(v) \mid pm'$. If $n(v) < pm'$, then we have again a contradiction to the minimality of m'. If $n(v) = pm'$, then the above argument for v^* also produces a contradiction to the minimality of m'.

If $pm = m_G$, then $S_{pm}(G) = G$ and indeed $\mu_p(\Gamma) = \mu_p(G) = 0$.

If $pm < m_G$, then the connected components of $S_{pm}(G)$ might be of two kinds: either an edge with order pm without vertices, or a subtree of G consisting of edges with order m and of some vertices of these edges, which have order pm. If all vertices of the edges would be part of the component, then this would already be the complete tree G, which is impossible by our assumption that $pm < m_G$. We may therefore assume that in each component there is at least one vertex of some edge missing. This vertex must be a leaf of the tree structure. (If not, the subtree would actually decompose into smaller trees.) In that case, each component contributes a non-negative number to

$$\zeta_{pm}(G) = \left|\left\{e \in E(G) : n(e) \mid pm\right\}\right| - \left|\left\{v \in V(G) : n(v) \mid pm\right\}\right|.$$

Since $\zeta_{pm}(G) = 0$, all components must actually contribute zero. This implies that components of the first kind cannot exist, and all components consist of edges of order m and an equal number of vertices with order pm, that is, exactly one of the vertices is missing from the tree component.

We now remove $S_{pm}(G)$ from G. What remains is another order tree, say G'. It is easy to see that our construction guarantees that $\zeta_\kappa(G') = \zeta_\kappa(G)$ for all κ.

We repeat the above construction for G', with a new minimal order $m' > m$. This process is continued until nothing remains from the original order tree G.

We now form a divisor tree out of the pieces of this construction. Each connected component of $S_{pm}(G)$, of $S_{pm'}(G')$, ... is interpreted as a vertex labelled by m, by m', ..., respectively, and two vertices, v_1 and v_2 say, are connected by an edge if the (incomplete) tree, $C(v_2)$ say, corresponding to v_2 was attached to the (incomplete) tree, $C(v_1)$ say, corresponding to v_1 in the original order tree G. The label of v_2 divides the one of v_1 since the order of the leaf of $C(v_1)$ on which $C(v_2)$ was attached must be a multiple of the order of the edges of $C(v_2)$.

Finally, to see the reverse implication, one has to convince oneself that the divisor tree construction of the theorem always yields order trees G with $\mu_p(G) = 0$, and that we have $\mu_p(\Gamma)=0$ for any group Γ of the theorem with order graph equal to G, which is not difficult. □

4. Auxiliary results

The purpose of this section is to provide the means for the proof of Theorem 6 in the next section. Lemma 3 below demonstrates that the derivatives of our basic series $\Phi(z)$ in (1.2) can be expressed as a polynomial in $\Phi(z)$ with rational coefficients, which is one of the fundamental facts needed in the proof of Theorem 6. The proof of the lemma is based on the evaluation of the determinant of a block matrix given in Lemma 4, which itself uses another determinant evaluation, provided in Lemma 5. The determinant evaluation of Lemma 4 also plays a crucial role in the proof of Theorem 6.

Let p be a given prime number. In all of this section, we write N for $\mu(\Gamma)/(p-1)$. Using this notation, the series $\Phi(z)$ in (1.2) becomes

$$\Phi(z)=\sum_{n=1}^{\infty}(-1)^{Nn-\frac{n-1}{p-1}}\frac{1}{n}\binom{Nn}{\frac{n-1}{p-1}}z^n.$$

A straightforward application of the Lagrange inversion formula (cf. [13, Theorem 5.4.2]) shows that $\Phi(z)$ is the unique formal power series solution of the equation

$$\Phi(z)-z\left(\Phi^{p-1}(z)-1\right)^N=0. \tag{4.1}$$

Lemma 3. *We have*

$$\Phi'(z)=\frac{\operatorname{Pol}(z,\Phi(z))}{(-1)^{(p-1)N}\big((p-1)N\big)^{(p-1)N}z^{p-1}+\big((p-1)N-1\big)^{(p-1)N-1}}, \tag{4.2}$$

where $\operatorname{Pol}(z,t)$ *is a polynomial in* z *and* t *over the integers.*

Proof. Differentiating both sides of (4.1), we obtain

$$\Phi'(z)-\left(\Phi^{p-1}(z)-1\right)^N-zN(p-1)\Phi'(z)\Phi^{p-2}(z)\left(\Phi^{p-1}(z)-1\right)^{N-1}=0.$$

Hence,

$$\Phi'(z)=\frac{\left(\Phi^{p-1}(z)-1\right)^N}{1-zN(p-1)\Phi^{p-2}(z)\left(\Phi^{p-1}(z)-1\right)^{N-1}}. \tag{4.3}$$

We must now express the reciprocal of the denominator as a polynomial in $\Phi(z)$. In order to do this, we make the Ansatz

$$\left(1-zN(p-1)\Phi^{p-2}(z)\left(\Phi^{p-1}(z)-1\right)^{N-1}\right)\sum_{i=0}^{(p-1)N-1}b_i(z)\Phi^i(z)=1, \tag{4.4}$$

with at this point undetermined coefficients $b_i(z)$, where the sum represents the reciprocal of the denominator in (4.3). We multiply both sides of the last equation by $(\Phi^{p-1}(z)-1)$. Then, using (4.1), we obtain

$$\Big(\big(1-N(p-1)\big)\Phi^{p-1}(z)-1\Big)\sum_{i=0}^{(p-1)N-1}b_i(z)\Phi^i(z)=\Phi^{p-1}(z)-1. \tag{4.5}$$

We expand the product on the left-hand side and use (4.1) again to reduce $\Phi^{(p-1)N}(z)$ to a linear combination of lower powers of $\Phi(z)$. This leads to

$$\begin{aligned}
&\big(1-N(p-1)\big)\sum_{i=0}^{(p-1)N-p} b_i(z)\Phi^{i+p-1}(z)\\
&+\big(1-N(p-1)\big)\sum_{i=0}^{p-2} b_{i+(p-1)(N-1)}(z)\left(z^{-1}\Phi^{i+1}(z)-\sum_{k=0}^{N-1}\binom{N}{k}(-1)^{N-k}\Phi^{i+(p-1)k}(z)\right)\\
&\qquad\qquad\qquad\qquad-\sum_{i=0}^{(p-1)N-1} b_i(z)\Phi^i(z)=\Phi^{p-1}(z)-1.
\end{aligned}$$

Comparison of powers of $\Phi(z)$ then yields a system of equations of the form

$$M\cdot b=c, \tag{4.6}$$

where $b=(b_i(z))_{0\le i\le (p-1)N-1}$ is the column vector of unknowns, $c=(c_i)_{0\le i\le (p-1)N-1}$ with $c_0=-1$, $c_{p-1}=1$, and $c_i=0$ otherwise, and M is the $(p-1)N\times(p-1)N$ matrix given by

$$M_{i,j}=\begin{cases}-1 & \text{if } 0\le i=j\le (p-1)N-p,\\ X & \text{if } p-1\le i=j+p-1\le (p-1)N-1,\\ Xz^{-1} & \text{if } 1\le i=j-(p-1)(N-1)+1\le p-1,\\ (-1)^{N-k-1}\binom{N}{k}X & \text{if } 0\le i-(p-1)k=j-(p-1)(N-1)\le p-2,\\ & \qquad\qquad\text{for some } k \text{ with } 0\le k\le N-1,\end{cases}$$

X being short for $1-(p-1)N$. The structure of the matrix M becomes clearer if we reorder the rows and columns of the matrix simultaneously so that first come the rows and columns indexed by i and j which are $\equiv 0 \pmod{p-1}$, respectively, then those which are $\equiv 1 \pmod{p-1}$, …, and finally those which are $\equiv p-2 \pmod{p-1}$. The result is the matrix

$$\begin{pmatrix} A & 0 & 0 & \dots & 0 & C\\ B & A & 0 & \dots & 0 & 0\\ 0 & B & A & \dots & 0 & 0\\ \vdots & & \ddots & \ddots & & \vdots\\ 0 & \dots & 0 & B & A & 0\\ 0 & \dots & 0 & 0 & B & A\end{pmatrix}, \tag{4.7}$$

where the block A is the $N\times N$ matrix given by

$$A=\begin{pmatrix} -1 & 0 & 0 & \dots & 0 & (-1)^{N-1}X\\ X & -1 & 0 & \dots & 0 & (-1)^{N-2}X\binom{N}{1}\\ 0 & X & -1 & \dots & 0 & (-1)^{N-3}X\binom{N}{2}\\ \vdots & & \ddots & \ddots & & \vdots\\ 0 & \dots & 0 & X & -1 & -X\binom{N}{N-2}\\ 0 & \dots & & 0 & X & X\binom{N}{N-1}-1\end{pmatrix}, \tag{4.8}$$

B is the $N \times N$ matrix given by

$$B = \begin{pmatrix} 0 & \dots & 0 & Xz^{-1} \\ 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{pmatrix},$$

and C is the $N \times N$ matrix given by

$$C = \begin{pmatrix} 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & Xz^{-1} \\ 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{pmatrix}.$$

The determinant of M (that is, of the matrix in (4.7)) is computed in Lemma 4. It is obviously non-zero, therefore the system of linear equations satisfied by the coefficients $b_i(z)$, $i = 0, 1, \dots, N-1$, has a unique solution. In the end, we obtain (4.2). $\square$

Lemma 4. *The determinant of the matrix in* (4.7) *equals*

$$(-1)^{(p-1)N}\big((p-1)N\big)^{(p-1)N} + \big((p-1)N-1\big)^{(p-1)N-1} z^{-p+1}.$$

Proof. We write the last column of (4.7) as the sum $c_1 + c_2$, where c_1 is the column with Xz^{-1} as index-1 entry (the reader should remember that our indexing starts with 0) and 0's otherwise, and c_2 is the "rest," that is, the index i entry equals

$$(-1)^{N-(i-(p-2)N)-1}\binom{N}{i-(p-2)N}X - \delta_{i,(p-1)N-1}$$

for $i = (p-2)N, (p-2)N+1, \dots, (p-1)N-1$ and 0's otherwise. Then, by linearity in the last column, the determinant $\det M$ equals the sum of

$$\det \begin{pmatrix} A & 0 & 0 & \dots & 0 & 0 \\ B & A & 0 & \dots & 0 & 0 \\ 0 & B & A & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & B & A & 0 \\ 0 & \dots & 0 & 0 & B & A \end{pmatrix}, \tag{4.9}$$

and the determinant of a second matrix, which arises from (4.7) by replacing the last column by c_1. Since the matrix in (4.9) is a lower triangular block matrix, its determinant equals

$$(\det A)^{p-1}. \tag{4.10}$$

We are going to evaluate the determinant of A in Lemma 5.

In order to evaluate the determinant of the second matrix, we expand it along the last column. This leads to the expression

$$(-1)^{(p-1)N} X z^{-1} \det \begin{pmatrix} A' & 0 & 0 & \dots & 0 & 0 \\ B & A & 0 & \dots & 0 & 0 \\ 0 & B & A & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & B & A & 0 \\ 0 & \dots & 0 & 0 & B & A'' \end{pmatrix}, \tag{4.11}$$

where A' is the matrix which arises from A by deleting its row with index 1 (it should be remembered again that our indexing of rows starts with the index 0), and A'' is the matrix which arises from A be deleting its last column. Inspection of the matrix in (4.11) reveals that it is an upper (sic!) triangular matrix, hence its determinant equals the product of its diagonal entries, so that (4.11) equals

$$(-1)^{(p-1)N} X z^{-1} \left(X z^{-1}\right)^{p-2} (-1) X^{(p-1)(N-1)-1} = \left((p-1)N-1\right)^{(p-1)N-1} z^{-p+1}. \quad \square$$

Lemma 5. *With the matrix A given by* (4.8)*, We have*

$$\det A = (-1)^N \big((p-1)N\big)^N.$$

Proof. We replace the 0-th row of A by

$$\sum_{j=0}^{N-1} X^{-j} \cdot (\text{row } j).$$

This is an operation which does not change the determinant. For the entry in the 0-th row and $(N-1)$-st column of the new matrix, we obtain

$$\begin{aligned} \sum_{j=0}^{N-1} X^{-j} (-1)^{N-j-1} \binom{N}{j} X - X^{-N+1} &= -X^{-N+1} \sum_{j=0}^{N} X^{N-j} (-1)^{N-j} \binom{N}{j} \\ &= -X^{-N+1} (1-X)^N = -\frac{\big((p-1)N\big)^N}{X^{N-1}}. \end{aligned} \tag{4.12}$$

Thus, after the operation described above, the new matrix reads

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & Y \\ X & -1 & 0 & \dots & 0 & (-1)^{N-2} X \binom{N}{1} \\ 0 & X & -1 & \dots & 0 & (-1)^{N-3} X \binom{N}{2} \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & X & -1 & -X \binom{N}{N-2} \\ 0 & \dots & & 0 & X & X \binom{N}{N-1} - 1 \end{pmatrix},$$

where Y denotes the quantity in (4.12). The determinant of this matrix, and thus the determinant of A, equals

$$(-1)^{N-1} X^{N-1} Y = (-1)^N \big((p-1)N\big)^N,$$

establishing the claim. $\square$

5. A generating function approach

Given a finitely generated virtually free group Γ, in this section we write $F(z)$ for the generating function $F_\Gamma(z)=\sum_{\lambda=1}^\infty f_\lambda(\Gamma)\,z^\lambda$ of the number $f_\lambda(\Gamma)$ of subgroups of index λm_Γ in Γ. The theorem below shows that, under the conditions of Theorem 2, the series $F(z)$, when coefficients are reduced modulo any given p-power, can be expressed as a polynomial in $\Phi(z)$.

Theorem 6. *Let p be a prime and α a positive integer. Furthermore, let Γ be a finitely generated virtually free group with $\mu_p(\Gamma)=0$ and $\mu(\Gamma)\ge 2$. As before, let $\Phi(z)$ be the series in* (1.2). *Then the generating function $F(z)$ for the free subgroup numbers of Γ, when reduced modulo p^α, can be expressed as a polynomial in $\Phi(z)$ of degree at most $\mu(\Gamma)-1$, with coefficients in $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$, where*

$$Y(z)=\begin{cases} z^{p-1}-\left(\frac{\mu(\Gamma)}{p-1}+1\right)^{-1}, & \text{if } p\ge 3 \text{ and } \mu(\Gamma)\not\equiv 0,1 \pmod p,\\ 1, & \text{otherwise.}\end{cases}$$

Proof. It is known from [10, Prop. 2] that $F(z)$ satisfies a differential equation of the form

$$F(z)=z\left(F^{p-1}(z)-1\right)^{\mu(\Gamma)/(p-1)}+p\mathcal{P}\left(z,F(z),F'(z),\dots,F^{(\mu(\Gamma)-1)}(z)\right), \tag{5.1}$$

where $\mathcal{P}(z,t_0,t_1,\dots,t_{\mu(\Gamma)-1})$ is a polynomial in $z,t_0,t_1,\dots,t_{\mu(\Gamma)-1}$ over the integers. (To be precise, this is the result of a careful p-adic analysis of the differential equation arising from a combination of (2.6) and (2.8).) It is our goal to express $F(z)$ modulo p^α as a polynomial in $\Phi(z)$ with coefficients in $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$. Since $\Phi(z)$ satisfies the functional equation (4.1) with $N=\mu(\Gamma)/(p-1)$, we have

$$F(z)=\Phi(z)\quad\text{modulo } p.$$

Here, given integral power series (or Laurent series) $f(z)$ and $g(z)$, we write

$$f(z)=g(z)\text{ modulo } p^\gamma$$

to mean that the coefficients of z^i in $f(z)$ and $g(z)$ agree modulo p^γ for all i.

We now suppose that we have already found a polynomial

$$F_\beta(z)=\sum_{i=0}^{\mu(\Gamma)-1}a_{i,\beta}(z)\Phi^i(z),$$

with coefficients $a_{i,\beta}(z)$ in $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$, so that

$$F(z)=F_\beta(z)\quad\text{modulo } p^\beta. \tag{5.2}$$

We then make the Ansatz

$$F(z)=F_{\beta+1}(z)=F_\beta(z)+p^\beta\sum_{i=0}^{\mu(\Gamma)-1}b_{i,\beta+1}(z)\Phi^i(z)\qquad\text{modulo } p^{\beta+1}, \tag{5.3}$$

for certain, at this point undetermined, rational functions $b_{i,\beta+1}(z)$ over the integers. We substitute this Ansatz in the differential equation (5.1) and reduce the result modulo $p^{\beta+1}$, to obtain

$$\begin{aligned} F_\beta(z) + p^\beta \sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z) \\ - z\left(F_\beta^{p-1}(z) + (p-1)F_\beta^{p-2}(z)p^\beta \sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z) - 1\right)^{\mu(\Gamma)/(p-1)} \\ - p\mathcal{P}\left(z, F_{\beta+1}(z), F'_{\beta+1}(z), \dots, F_{\beta+1}^{(\mu(\Gamma)-1)}(z)\right) = 0 \quad \text{modulo } p^{\beta+1}. \end{aligned} \tag{5.4}$$

By Lemma 3, we have

$$F_{\beta+1}^{(j)}(z) = F_\beta^{(j)}(z) + p^\beta \sum_{i=0}^{\mu(\Gamma)-1} c_{i,\beta+1;j}(z)\Phi^i(z) \tag{5.5}$$

for all non-negative integers j and certain rational functions $c_{i,\beta+1;j}(z)$. It should be noted that the denominators of these rational functions are powers of

$$(-1)^{(p-1)N}\big((p-1)N\big)^{(p-1)N} z^{p-1} + \big((p-1)N-1\big)^{(p-1)N-1}, \tag{5.6}$$

where we wrote again $N = \mu(\Gamma)/(p-1)$ for short. Since we are considering (5.4) modulo $p^{\beta+1}$, and since the sum on the right-hand side of (5.5) has the prefactor p^β, we may reduce these denominators modulo p. Explicitly, we have

$$\begin{aligned} (-1)^{(p-1)N}\big((p-1)N\big)^{(p-1)N} z^{p-1} + \big((p-1)N-1\big)^{(p-1)N-1} \\ = \begin{cases} 1 \pmod p, & \text{if } p=2 \text{ and } N \text{ is even,} \\ z \pmod p, & \text{if } p=2 \text{ and } N \text{ is odd,} \\ -1 \pmod p, & \text{if } p\ge 3 \text{ and } N\equiv 0 \bmod p \\ z^{p-1} \pmod p, & \text{if } p\ge 3 \text{ and } N\equiv -1 \bmod p \\ z^{p-1} - (N+1)^{-1} \pmod p, & \text{if } p\ge 3 \text{ and } N\not\equiv 0,1 \bmod p \end{cases} \end{aligned} \tag{5.7}$$

In all cases, the reciprocals of the polynomials on the right-hand side of (5.7) are elements of $\mathbb{Z}[z, z^{-1}, Y^{-1}(z)]$. (Here we use that $N \equiv -1 \pmod p$ and $\mu(\Gamma) \equiv 1 \pmod p$ are equivalent.) Hence, in our computation, the coefficients $c_{i,\beta+1;j}(z)$ may be assumed to lie in $\mathbb{Z}[z, z^{-1}, Y^{-1}(z)]$.

If relation (5.5) is substituted in (5.4), then one sees that this congruence reduces to

$$\begin{aligned} F_\beta(z) + p^\beta \sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z) \\ - z\left((F_\beta^{p-1}(z)-1)^N + p^\beta(p-1)NF_\beta^{p-2}(z)(F_\beta^{p-1}(z)-1)^{N-1} \sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z)\right) \\ - p\mathcal{P}\left(z, F_\beta(z), F'_\beta(z), \dots, F_\beta^{(\mu(\Gamma)-1)}(z)\right) = 0 \quad \text{modulo } p^{\beta+1}. \end{aligned}$$

By definition of $F_\beta(z)$, we may divide both sides by p^β. This leads to the congruence

$$G_\beta(z)+\sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z)\\ -(p-1)NzF_\beta^{p-2}(z)(F_\beta^{p-1}(z)-1)^{N-1}\sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z)=0 \quad \text{modulo } p,$$

for some explicitly given polynomial $G_\beta(z)$ in $\Phi(z)$ with coefficients in $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$. By construction, we have

$$F_\beta(z)=\Phi(z)\quad \text{modulo } p.$$

Using this in the above congruence, we arrive at

$$G_\beta(z)+\big(1-(p-1)Nz\Phi^{p-2}(z)(\Phi^{p-1}(z)-1)^{N-1}\big)\sum_{i=0}^{\mu(\Gamma)-1} b_{i,\beta+1}(z)\Phi^i(z)=0 \quad \text{modulo } p. \tag{5.8}$$

By reducing "high" powers of $\Phi(z)$ by means of (4.1) and subsequently comparing coefficients of powers of $\Phi(z)$, we obtain a system of linear equations over $\mathbb{Z}/p\mathbb{Z}$ for the unknown rational functions $b_{i,\beta+1}(z)$, $i=0,1,\dots,\mu(\Gamma)-1$. As inspection shows, the coefficient matrix of the system is exactly the same as the one arising from (4.5). (The reader should in particular compare (5.8) and (4.4).) We have computed the determinant of this coefficient matrix in the proof of Lemma 3. As a matter of fact, it equals (5.6) divided by z^{p-1}. Since (5.8) is a congruence modulo p, we have to reduce (5.6) modulo p, which we did in (5.7). We observed that the reciprocals of the reduced expressions lie in $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$ in all cases. In particular, they are all non-zero. Hence, there are unique rational functions $b_{i,\beta+1}(z)$, $i=0,1,\dots,\mu(\Gamma)-1$, solving (5.8), and all of them are elements of $\mathbb{Z}[z,z^{-1},Y^{-1}(z)]$. This completes the proof of the theorem. □

Theorem 6 has a remarkable consequence concerning the nature of the generating function $F(z)$ for the free subgroup numbers of a finitely generated virtually free group Γ. In the proof of the theorem, we used that $F(z)$ satisfies an algebraic differential equation of the form (5.1). The technical term which is commonly used for this situation is that the generating function $F(z)$ is *differentially algebraic*. On the other hand, it may be safely conjectured that it does not belong to the more restrictive class of *D-finite* power series, that is, it does not satisfy a linear differential equation with polynomial coefficients. Equivalently, we conjecture that the sequence of free subgroup numbers of Γ is not P-recursive, that is, it does not satisfy a linear recurrence with polynomial coefficients. (The reader is referred to [13, Ch. 6] for information on D-finite series and P-recursive sequences.) Theorem 6 implies that the situation changes drastically when one reduces the free subgroup numbers modulo a given prime power. (The reader should recall that algebraic power series are automatically D-finite.)

Corollary 7. *Under the assumptions of Theorem* 6*, we have*

$$F(z)=A_{p,\alpha}(z)\quad \text{modulo } p^\alpha,$$

where $A_{p,\alpha}(z)$ is an algebraic power series, that is, it satisfies an equation of the form $\operatorname{Pol}(A_{p,\alpha}(z), z) = 0$*, where* $\operatorname{Pol}(y, z)$ *is a polynomial in y and z.*

Proof. Theorem 6 says that $F(z)$ can be expressed as a polynomial in $\Phi(z)$, z, z^{-1}, and $Y^{-1}(z)$. The series $\Phi(z)$ is algebraic by (4.1), as are z, z^{-1}, and $Y^{-1}(z)$. The assertion of the corollary then follows from the closure properties of the class of algebraic series. ☐

6. The main results

Let again Γ be a finitely generated virtually free group and p a prime such that $\mu_p(\Gamma) = 0$ and $\mu(\Gamma) \geq 2$. We are now in the position to derive the main results of this paper, which say that the number of free subgroups of index λm_Γ in Γ, when reduced modulo any given p-power, is congruent to a binomial coefficient involving λ times a rational function in λ, respectively a sum involving these quantities. These results are made precise in Corollaries 8 and 12 below. We accompany these results by concrete examples, given in Example 9 and 10, which illustrate Corollary 8, respectively Example 14, illustrating Corollary 12. Moreover, we explain in Remarks 11 and 15 how the earlier results in [2, 4] fit into the more general picture that we present here.

Corollary 8. *Let r be a non-negative integer. With the assumptions of Theorem* 6*, if* $\mu(\Gamma) \equiv 0, 1 \pmod p$*, then*

$$f_\lambda(\Gamma) \equiv R_{\Gamma,p,r}(\lambda) \binom{\frac{\mu(\Gamma)\lambda}{p-1}}{\frac{\lambda-r}{p-1}} \pmod{p^\alpha}, \quad \text{for } \lambda \equiv r \pmod{p-1}, \tag{6.1}$$

where, $R_{\Gamma,p,r}(\lambda)$ is a rational function in λ. Furthermore, the right-hand side of the above congruence is always integral.

Proof. By Theorem 6, the generating function $\sum_{\lambda=1}^{\infty} f_\lambda(\Gamma)\, z^\lambda$ equals

$$\sum_{i=0}^{\mu(\Gamma)-1} b_{i,\alpha}(z)\Phi^i(z) \qquad \text{modulo } p^\alpha, \tag{6.2}$$

and the coefficients $b_{i,\alpha}(z)$ are elements of $\mathbb{Z}[z, z^{-1}, Y^{-1}(z)]$. According to the definition of $Y(z)$, under our assumption $\mu(\Gamma) \equiv 0, 1$ we have $Y(z) = 1$. Consequently, the coefficients $b_{i,\alpha}(z)$ are actually Laurent polynomials over the integers.

We must now extract the coefficient of z^λ in (6.2). In order to do so, we appeal again to the Lagrange inversion formula (cf. [13, Theorem 5.4.2]), which shows that

$$\left\langle z^n \right\rangle \Phi^m(z) = (-1)^{\frac{(\mu(\Gamma)-1)n+m}{p-1}} \frac{m}{n} \binom{\frac{\mu(\Gamma)n}{p-1}}{\frac{n-m}{p-1}}. \tag{6.3}$$

If this is used to extract the coefficient of z^λ in (6.2) for $\lambda \equiv r \pmod{p-1}$, then one arrives at the assertion (6.1). The integrality claim follows from the fact that the expression on the right-hand side of (6.1) is an integral linear combination of terms (6.3), all of which are integral. ☐

Example 9. We let $p = 3$ and Γ_1 a finitely generated virtually free group with order graph given by the normalised tree in Figure 5. In this situation, we have $m_{\Gamma_1} = 6$, $\zeta_1(\Gamma_1) = 2$, $\zeta_2(\Gamma_1) = 4$, $\zeta_3(\Gamma_1) = 0$, and $\zeta_6(\Gamma_1) = -1$, and thus

$$\mu_3(\Gamma_1) = 1 + \varphi\left(\tfrac{6}{3}\right) \zeta_3(\Gamma_1) + \varphi\left(\tfrac{6}{6}\right) \zeta_6(\Gamma_1) = 1 + 0 + (-1) = 0$$

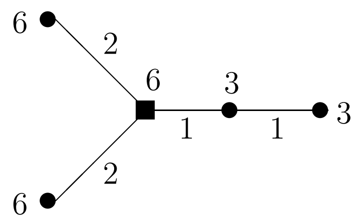

FIGURE 5. The order graph of the group Γ_1 in Example 9

and

$$\mu(\Gamma_1) = 1+\varphi\left(\tfrac{6}{1}\right)\zeta_1(\Gamma_1)+\varphi\left(\tfrac{6}{2}\right)\zeta_2(\Gamma_1)+\varphi\left(\tfrac{6}{3}\right)\zeta_3(\Gamma_1)+\varphi\left(\tfrac{6}{6}\right)\zeta_6(\Gamma_1) = 1+4+8+0-1 = 12.$$

The functional equation for $F(z) = F_{\Gamma_1}(z)$ that we get from (2.6) and (2.8), after reduction of the coefficients modulo 81, is

$$\begin{multlined}63z^3F^9(z)F''(z) + 72z^3F^3(z)F''(z) + 27z^3F(z)F''(z) + 72z^2F^{10}(z)F'(z)\\ + 36z^2F^9(z)F'(z) + 9z^2F^4(z)F'(z) + 18z^2F^3(z)F'(z) + 27z^2F^2(z)F'(z)\\ + 27z^2F(z)F'(z) + 54z^2F'(z) + zF^{12}(z) + 36zF^{11}(z) + 15zF^{10}(z) + 72zF^9(z)\\ + 54zF^8(z) + 46zF^6(z) + 18zF^5(z) + 21zF^4(z) + 63zF^3(z)\\ + 9zF^2(z) + 54zF(z) + 80F(z) + 16z = 0 \qquad \text{modulo } 81.\end{multlined}$$

The algorithm given in the proof of Theorem 6 to find a solution to this congruence yields

$$\begin{multlined}F(z) = 15z + (27z+1)\Phi(z) + 69z\Phi^2(z) + 9z\Phi^3(z) + 42z\Phi^4(z) + 27z\Phi^5(z)\\ + 39z\Phi^6(z) + 27z\Phi^7(z) + 66z\Phi^8(z) + 72z\Phi^9(z) + 12z\Phi^{10}(z) \qquad \text{modulo } 81.\end{multlined}$$

Coefficient extraction then yields

$$f_{2L+1}(\Gamma_1) \equiv (-1)^{L+1}\frac{P_1(L)}{(12L+1)_6}\binom{12L+6}{L} \pmod{81}, \quad \text{for } L \ge 1,$$

where

$$P_1(L) = 18(473007L^5 + 969687L^4 + 765456L^3 + 308998L^2 + 72732L + 9080),$$

and

$$f_{2L}(\Gamma_1) \equiv (-1)^{L+1}\frac{P_2(L)}{(12L-6)\,(11L-4)_4}\binom{12L-6}{L-1} \pmod{81}, \quad \text{for } L \ge 1,$$

where

$$P_2(L) = 324(48L^6 - 528L^5 + 6079L^2 + 9091L^4 - 10582L^3 - 1874L + 286),$$

with the Pochhammer symbol $(\alpha)_m$ being defined by $(\alpha)_m := \alpha(\alpha+1)\cdots(\alpha+m-1)$ for $m \ge 1$, and $(\alpha)_0 := 1$.

Example 10. We let $p = 2$ and Γ_2 a finitely generated virtually free group with order graph given by the normalised tree in Figure 6. In this situation, we have $m_{\Gamma_2} = 30$,

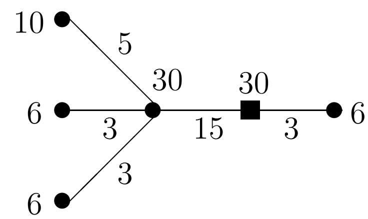

FIGURE 6. The order graph of the group Γ_2 in Example 10

$\zeta_1(\Gamma_2)=0$, $\zeta_2(\Gamma_2)=0$, $\zeta_3(\Gamma_2)=3$, $\zeta_5(\Gamma_2)=1$, $\zeta_6(\Gamma_2)=0$, $\zeta_{10}(\Gamma_2)=0$, $\zeta_{15}(\Gamma_2)=5$, and $\zeta_{30}(\Gamma_2)=-1$, and thus

$$\begin{aligned}\mu_2(\Gamma_2)&=1+\varphi\big(\tfrac{30}{2}\big)\,\zeta_2(\Gamma_2)+\varphi\big(\tfrac{30}{6}\big)\,\zeta_6(\Gamma_2)+\varphi\big(\tfrac{30}{10}\big)\,\zeta_{10}(\Gamma_2)+\varphi\big(\tfrac{30}{30}\big)\,\zeta_{30}(\Gamma_2)\\&=1+0+0+(-1)=0\end{aligned}$$

and

$$\begin{aligned}\mu(\Gamma_2)&=1+\varphi\big(\tfrac{30}{1}\big)\,\zeta_1(\Gamma_2)+\varphi\big(\tfrac{30}{2}\big)\,\zeta_2(\Gamma_2)+\varphi\big(\tfrac{30}{3}\big)\,\zeta_3(\Gamma_2)+\varphi\big(\tfrac{30}{5}\big)\,\zeta_5(\Gamma_2)+\varphi\big(\tfrac{30}{6}\big)\,\zeta_6(\Gamma_2)\\&\qquad+\varphi\big(\tfrac{30}{10}\big)\,\zeta_{10}(\Gamma_2)+\varphi\big(\tfrac{30}{15}\big)\,\zeta_{15}(\Gamma_2)+\varphi\big(\tfrac{30}{30}\big)\,\zeta_{30}(\Gamma_2)\\&=1+0+0+12+2+0+0+5+(-1)=19.\end{aligned}$$

The functional equation for $F(z)=F_{\Gamma_2}(z)$ that we get from (2.6) and (2.8), after reduction of the coefficients modulo 16, is

$$\begin{aligned}&4z^3F^{16}(z)F''(z)+8z^3F^8(z)F''(z)+4z^3F''(z)+10z^2F^{17}(z)F'(z)+10z^2F^{16}(z)F'(z)\\&\quad+8z^2F^{13}(z)F'(z)+8z^2F^{12}(z)F'(z)+12z^2F^9(z)F'(z)+12z^2F^8(z)F'(z)\\&\quad+8z^2F^5(z)F'(z)+8z^2F^4(z)F'(z)+10z^2F(z)F'(z)+10z^2F'(z)+zF^{19}(z)\\&\quad+13zF^{18}(z)+11zF^{17}(z)+7zF^{16}(z)+4zF^{15}(z)+4zF^{14}(z)+12zF^{13}(z)\\&\quad+12zF^{12}(z)+14zF^{11}(z)+6zF^{10}(z)+10zF^9(z)+2zF^8(z)+4zF^7(z)+4zF^6(z)\\&+12zF^5(z)+12zF^4(z)+9zF^3(z)+5zF^2(z)+3zF(z)+15F(z)+15z=0\qquad\text{modulo }16.\end{aligned}$$

The algorithm given in the proof of Theorem 6 to find a solution to this congruence yields

$$\begin{aligned}F(z)&=4z+5\Phi(z)+(12z+2)\Phi^2(z)+8\Phi^3(z)+12\Phi^4(z)+8\Phi^5(z)+8z\Phi^8(z)\\&\qquad+8z\Phi^{10}(z)+4z\Phi^{16}(z)+12z\Phi^{18}(z)\qquad\text{modulo }16.\end{aligned}$$

Coefficient extraction then yields

$$f_\lambda(\Gamma_2)\equiv\frac{Q(\lambda)}{3\lambda(6\lambda+1)(9\lambda+1)(9\lambda+2)(18\lambda+5)(19\lambda-18)_{19}}\binom{19\lambda}{\lambda-1}\pmod{16},\qquad\text{for }\lambda\ge2,$$

where

$$\begin{aligned}
Q(\lambda) = {} & 414873816131174400000 + 1687131469740810240000\lambda \\
& + 11694465019743123456000\lambda^2 + 29282454431920413411 8400\lambda^3 \\
& - 29202846796468767574333 44\lambda^4 + 29139678526675320716647104\lambda^5 \\
& - 208744430518331785363075776\lambda^6 + 1109655351908161743775529040\lambda^7 \\
& - 4529445293042933659974133664\lambda^8 + 13823323659414730061860809764\lambda^9 \\
& - 27457006500072077685531953836\lambda^{10} + 13774006864417015570820956495\lambda^{11} \\
& + 106285230034124606189268827556\lambda^{12} - 297352958635465036740864629691\lambda^{13} \\
& - 141581261268484414672371284786\lambda^{14} + 3042215815187103665497014434600\lambda^{15} \\
& - 10200061275321550038724683325744\lambda^{16} + 20246947276823841509192253805174\lambda^{17} \\
& - 27403542237122957637017406285816\lambda^{18} + 26128885491619758888717502991655\lambda^{19} \\
& - 17392298204833244937049876124804\lambda^{20} + 7727636538613299232368005827649\lambda^{21} \\
& - 2065181275328822431645181305786\lambda^{22} + 251508577253835734501825269810\lambda^{23}.
\end{aligned}$$

Remark 11. More generally, if $p = 2$, $\mu_2(\Gamma) = 0$ and $\mu(\Gamma) \geq 2$, then we are always in the case covered by Corollary 8, since, trivially, $\mu(\Gamma) \equiv 0 \pmod 2$ or $\mu(\Gamma) \equiv 1 \pmod 2$. In particular, we see that the discussion of the subgroup numbers of lifts of Hecke groups $\mathfrak{H}(q) \cong C_2 * C_q$ with q a Fermat prime modulo powers of 2 in [2, Sec. 8 and second part of Sec. 13] fits into the framework of Corollary 8, which can be regarded as a vast generalisation. It has to be emphasised yet that the results for lifts of Hecke groups in [2] go slightly further than Corollary 8 in that case as the basic series used there — which is the mod-2-reduction of our basic series $\Phi(z)$ — allows for a very efficient coefficient extraction, a point that we did not touch in the present paper.

Now we turn to the somewhat more complicated case when $\mu(\Gamma) \not\equiv 0, 1 \pmod p$.

Corollary 12. *Let r be an integer with $0 \leq r \leq p-2$. With the assumptions of Theorem 6, if $\mu(\Gamma) \not\equiv 0, 1 \pmod p$, then*

$$\begin{aligned}
f_\lambda(\Gamma) \equiv {} & \left(\frac{\mu(\Gamma)}{p-1} + 1\right)^{\lambda/(p-1)} R^{(1)}_{\Gamma,p,r}(\lambda) \\
& + \sum_{k=0}^{\lfloor \lambda/(p-1) \rfloor} \left(\frac{\mu(\Gamma)}{p-1} + 1\right)^{k} R^{(2)}_{\Gamma,p,r}(\lambda,k) \binom{\frac{\mu(\Gamma)\lambda}{p-1} - \mu(\Gamma)k}{\frac{\lambda-r}{p-1} - k} \pmod{p^\alpha}, \\
& \qquad\qquad\qquad\qquad\qquad\qquad \text{for } \lambda \equiv r \pmod{p-1}, \qquad (6.4)
\end{aligned}$$

where $R^{(1)}_{\Gamma,p,r}(\lambda)$ and $R^{(2)}_{\Gamma,p,r}(\lambda,k)$ are rational functions in their respective arguments. Moreover, $R^{(2)}_{\Gamma,p,r}(\lambda,k)$ depends only on $\frac{\lambda}{p-1} - k$, and the right-hand side of the above congruence is always integral.

Proof. We begin as in the proof of Corollary 12 by quoting Theorem 6, which tells us that the generating function $\sum_{\lambda=1}^\infty f_\lambda \, z^\lambda$ is given by (6.2) modulo p^α. However, here we have $Y(z) = z^{p-1} - (N+1)^{-1}$, with $N = \mu(\Gamma)/(p-1)$.

Again, we must now extract the coefficient of z^λ in (6.2). Here, we must first expand fractions,

$$\frac{1}{Y^q(z)} = \frac{1}{\big(z^{p-1}-(N+1)^{-1}\big)^q} = (-1)^q(N+1)^q\sum_{k=0}^{\infty}\binom{q+k-1}{k}(N+1)^k z^{(p-1)k}.$$

Subsequent coefficient extraction using (6.3) leads to the result in (6.4), where the term containing $R^{(1)}_{\Gamma,p,r}(\lambda)$ comes from the summand $b_{0,\alpha}(z)$ in (6.2), while the term containing $R^{(2)}_{\Gamma,p,r}(\lambda,k)$ is generated by the remaining summands in (6.2). The integrality claim follows from the fact that the expression on the right-hand side of (6.4) is an integral linear combination of terms, all of which are integral. □

We now show that the sum on the right-hand side of (6.4) satisfies a linear recurrence with constant coefficients, so that the computation of this sum modulo p^α can be achieved in essentially linear time with growing λ by reducing results modulo p^α after each iteration of the recurrence. (We say "essentially" since the computation of the inhomogeneous part of the recurrence does grow super-linearly.)

Proposition 13. *Let r be an integer with $0\le r\le p-2$, and let $S_r(\lambda)$ denote the sum on the right-hand side of* (6.4)*. Then we have*

$$\sum_{j=0}^{d+1}(-1)^j\binom{d+1}{j}M^{d+1-j}S_r(\lambda+(p-1)j)=g_r(\lambda),\quad \textit{for } \lambda\equiv r \pmod{p-1}, \tag{6.5}$$

where d is the numerator degree of $R^{(2)}_{\Gamma,p,r}(\lambda,k)$ in λ, $M=\frac{\mu(\Gamma)}{p-1}+1$, and $g_r(\lambda)$ is a hypergeometric term, that is, $g_r(\lambda+1)/g_r(\lambda)$ equals a rational function in λ.

Proof. We fix r, and we write $\lambda=(p-1)L+r$. Using this notation, the sum $S_r(\lambda)$ has the form

$$S_r(\lambda)=S_r((p-1)L+r)=\sum_{k=0}^{L}M^kA(L-k,L)\,f(L-k), \tag{6.6}$$

where $A(x,y)$ is a polynomial in x and y of degree d in y, and $f(L-k)$ comprises the binomial coefficient on the right-hand side of (6.4) as well as the denominator of $R^{(2)}_{\Gamma,p,r}(\lambda,k)$. We chose to parametrise the polynomial $A(L-k,L)$ in this slightly unusual form since it will be of advantage during the following computation.

Let E denote the shift operator in L, that is, $(Eh)(L):=h(L+1)$. We now apply $(E-M\cdot\mathrm{id})^{d+1}$ to (6.6). We obtain

$$\begin{aligned}
&(E-M\cdot\mathrm{id})^{d+1}S_r((p-1)L+r)\\
&\qquad=\sum_{j=0}^{d+1}(-1)^{d+1-j}\binom{d+1}{j}M^{d+1-j}\sum_{k=0}^{L+j}M^kA(L+j-k,L+j)\,f(L+j-k)\\
&\qquad=\sum_{j=0}^{d+1}(-1)^{d+1-j}\binom{d+1}{j}M^{d+1-j}\sum_{k=-j}^{L}M^{k+j}A(L-k,L+j)\,f(L-k)\\
&\qquad=\sum_{k=0}^{L}M^{d+k+1}f(L-k)\sum_{j=0}^{d+1}(-1)^{d+1-j}\binom{d+1}{j}A(L-k,L+j)+G_r(L),
\end{aligned}$$

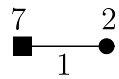

FIGURE 7. The order graph of the group $\mathfrak{H}(7)$ in Example 14

where $G_r(L)$ is the hypergeometric term resulting from summands that we split off when passing from the summation over k running from $-j$ to L in the next-to-last line to the summation over k running from 0 to L in the last line. Using the difference operator Δ_t defined by $(\Delta_t h)(t) := h(t+1) - h(t)$, this last expression can be rewritten as

$$(E-M\cdot\mathrm{id})^{d+1} S_r((p-1)L+r) = \sum_{k=0}^{L} M^{d+k+1} f(L-k)\, \Delta_t^{d+1} A(L-k,t)\big|_{t=L} + G_r(L). \tag{6.7}$$

We assumed that $A(x,y)$ is a polynomial of degree d in y, hence Δ_t^{d+1} kills $A(L-k,t)$. Consequently, on the right-hand side in (6.7) there remains only $G_r(L)$, while, after expansion of $(E-M\cdot\mathrm{id})^{d+1}$, the left-hand side becomes the left-hand side of (6.5), as desired. $\square$

Example 14. We consider the Hecke group $\mathfrak{H}(7) = C_2 * C_7$, whose order graph is shown in Figure 7, and the prime $p = 7$. We have $m_{\mathfrak{H}(7)} = 14$, $\zeta_1(\mathfrak{H}(7)) = 1$, $\zeta_2(\mathfrak{H}(7)) = 0$, $\zeta_7(\mathfrak{H}(7)) = 0$, and $\zeta_{14}(\mathfrak{H}(7)) = -1$, and thus $\mu_7(\mathfrak{H}(7)) = 0$ and $\mu(\mathfrak{H}(7)) = 6$.

The functional equation for $F(z) = F_{\mathfrak{H}(7)}(z)$ that we get from (2.6) and (2.8) is sufficiently small to be displayed here:

$$\begin{gathered}
537824z^6F^{(5)}(z) + 230496z^5F(z)F^{(4)}(z) + 6991712z^5F^{(4)}(z) + 41160z^4F(z)^2F^{(3)}(z)\\
+ 1959216z^4F(z)F^{(3)}(z) + 24989608z^4F^{(3)}(z) + 384160z^5\big(F''(z)\big)^2 + 3920z^3F^3(z)F''(z)\\
+ 205800z^3F^2(z)F''(z) + 3874528z^3F(z)F''(z) + 25988424z^3F''(z) + 41160z^4\big(F'(z)\big)^3\\
+ 8820z^3F^2(z)\big(F'(z)\big)^2 + 288120z^3F(z)\big(F'(z)\big)^2 + 2512132z^3\big(F'(z)\big)^2\\
+ 210z^2F^4(z)F'(z) + 9800z^2F^3(z)F'(z) + 180516z^2F^2(z)F'(z) + 1561336z^2F(z)F'(z)\\
+ 5336394z^2F'(z) + 576240z^5F^{(3)}(z)F'(z) + 164640z^4F(z)F'(z)F''(z)\\
+ 3649520z^4F'(z)F''(z) + zF^6(z) + 42zF^5(z) + 679zF^4(z) + 5292zF^3(z)\\
+ 20335zF^2(z) + 34986zF(z) - F(z) + 19305z = 0.
\end{gathered}$$

The algorithm in the proof of Theorem 6 to find a solution to this congruence gives

$$\frac{\begin{aligned}7\big(8z^{18} + 12z^{17} + 7z^{15} + 7z^{13} + 48z^{12} + 16z^{11}&\\ +7z^{10} + 35z^9 + 42z^7 + 23z^6 + 24z^5 + 21z^4 + 42z^3 + 14z\big)&\end{aligned}}{(1-2z^6)^3}$$
$$+ \left(1 + \frac{\begin{aligned}7\big(35z^{18} + 11z^{17} + 30z^{16} + 14z^{14} + 14z^{12} + 17z^{11}&\\ +47z^{10} + 14z^9 + 42z^8 + 21z^6 + z^5 + 32z^4 + 42z^3\big)&\end{aligned}}{(1-2z^6)^3}\right)\Phi(z)$$

$$
\begin{aligned}
&+\frac{7\left(28z^{17}+36z^{16}+31z^{15}+14z^{14}+7z^{13}+21z^{11}+20z^{10}\right.\\
&\qquad\left.+18z^{9}+35z^{8}+28z^{7}+7z^{5}+30z^{4}+41z^{3}+28z^{2}+21z\right)}{\left(1-2z^{6}\right)^{3}}\Phi^{2}(z)\\
&+\frac{7\left(42z^{16}+29z^{15}+22z^{14}+7z^{13}+7z^{12}+7z^{10}+27z^{9}\right.\\
&\qquad\left.+48z^{8}+35z^{7}+21z^{6}+35z^{4}+16z^{3}+2z^{2}+42z\right)}{\left(1-2z^{6}\right)^{3}}\Phi^{3}(z)\\
&+\frac{7\left(42z^{17}+14z^{15}+41z^{14}+19z^{13}+7z^{12}+42z^{11}\right.\\
&\qquad\left.+35z^{9}+z^{8}+23z^{7}+21z^{6}+42z^{5}+28z^{3}+26z^{2}+31z\right)}{\left(1-2z^{6}\right)^{3}}\Phi^{4}(z)\\
&+\frac{7\left(22z^{18}+21z^{17}+21z^{16}+21z^{14}+34z^{12}+7z^{11}\right.\\
&\qquad\left.+7z^{10}+28z^{8}+9z^{6}+28z^{5}+28z^{4}+42z^{2}\right)}{\left(1-2z^{6}\right)^{3}}\Phi^{5}(z)\\
&\hspace{20em}\text{modulo } 343. \qquad (6.8)
\end{aligned}
$$

Finally, we have to extract coefficients. We content ourselves with displaying here the results for $f_\lambda(\mathfrak{H}(7))$ for $\lambda \equiv 0 \pmod 6$; for the other congruence classes for λ, similar results are available. By comparing coefficients of $z^{6\lambda}$ on both sides of (6.8), we obtain

$$
\begin{aligned}
f_{6\lambda}(\mathfrak{H}(7)) &\equiv 7\cdot 2^{\lambda-2}(49\lambda^2-7\lambda+4)\\
&\quad+7\sum_{k=0}^{\infty}(-1)^{k+\lambda}2^{k-4}\frac{5\,(5k-5\lambda+1)\,(k-\lambda)P(\lambda)}{3\,(6\lambda-6k-5)_5}\binom{6\lambda-6k}{\lambda-k} \pmod{343}, \qquad (6.9)
\end{aligned}
$$

where

$$
\begin{aligned}
P(\lambda) = 22661k^4-45322k^3\lambda+70594k^3+22661k^2\lambda^2-110545k^2\lambda+92331k^2+39951k\lambda^2\\
-110913k\lambda+56014k+28424\lambda^2-38696\lambda+12528.
\end{aligned}
$$

Let us denote the sum on the right-hand side of the congruence (6.9) by $S(\lambda)$. Applying Proposition 13 (or, more precisely, its proof; alternatively, one may use the Gosper–Zeilberger algorithm; cf. [11]), we see that $S(\lambda)$ satisfies the recurrence

$$
S(\lambda+3)-6S(\lambda+2)+12S(\lambda+1)-8S(\lambda)=7\,(-1)^{\lambda+1}\,T(\lambda)\frac{(6\lambda)!}{\lambda!\,(5\lambda+13)!},
$$

where

$$
\begin{aligned}
T(\lambda) &= 7578375074183\lambda^{12}+110764942152696\lambda^{11}+719438896272607\lambda^{10}\\
&\quad+2739679993093800\lambda^{9}+6794561274739329\lambda^{8}+11525824255968648\lambda^{7}\\
&\quad+13662933657289381\lambda^{6}+11354903297697240\lambda^{5}+6532000464773588\lambda^{4}\\
&\quad+2520106018198656\lambda^{3}+613697061412512\lambda^{2}+83672481893760\lambda+4738762828800.
\end{aligned}
$$

Remark 15. The discussion of free subgroup numbers of lifts $\Gamma_m(3)$ of the classical modular group $\mathfrak{H}(3)\cong \mathrm{PSL}_2(\mathbb{Z})$ in [4, Sec. 16] taken modulo powers of 3 fits into the framework of Corollary 12. Indeed, for these lifts, we have $\mu_{\Gamma_m(3)}=2$, which is not congruent to $0,1 \pmod 3$. Consequently, according to Theorem 6, we must be prepared to encounter denominators in the coefficients of the polynomial in $\Phi(z)$ that expresses the generating function for the free subgroup numbers when coefficients are reduced modulo a power of 3. This is exactly what happened in [4], and this is also the reason why coefficient extraction was considerably harder in [4] than in [2].

Acknowledgement

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

References

[1] A. Dress and T. W. Müller, Decomposable functors and the exponential principle, *Adv. Math.* **129** (1997), 188–221.
[2] M. Kauers, C. Krattenthaler, and T. W. Müller, A method for determining the mod-2^k behaviour of recursive sequences, with applications to subgroup counting, *Electron. J. Combin.* **18** (2012), Art. #P37, 83 pp.
[3] C. Krattenthaler and T. W. Müller, A Riccati differential equation and free subgroup numbers for lifts of $\mathrm{PSL}_2(\mathbb{Z})$ modulo prime powers, *J. Combin. Theory Ser. A* **120** (2013), 2039–2063.
[4] C. Krattenthaler and T. W. Müller, A method for determining the mod-3^k behaviour of recursive sequences, preprint, 83 pages; arχiv:1308.2856.
[5] C. Krattenthaler and T. W. Müller, A method for determining the mod-p^k behaviour of recursive sequences, preprint, 35 pages; arχiv:1508.02580.
[6] C. Krattenthaler and T. W. Müller, Periodicity of free subgroup numbers modulo prime powers, *J. Algebra* **452** (2016), 372–389.
[7] C. Krattenthaler and T. W. Müller, Normalising graphs of groups, *Monatsh. Math.* (to appear).
[8] T. W. Müller, A group-theoretical generalization of Pascal's triangle, *Europ. J. Combin.* **12** (1991), 43–49.
[9] T. W. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.
[10] T. W. Müller and J.-C. Schlage-Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.
[11] M. Petkovšek, H. Wilf, and D. Zeilberger, *A=B*, A. K. Peters, Wellesley, 1996.
[12] J.-P. Serre, *Arbres, Amalgames,* SL_2, Astérisque, vol. 46, Société mathématique de France, Paris, 1977.
[13] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge, 1999.

† Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria. WWW: http://www.mat.univie.ac.at/~kratt.

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