PERIODICITY OF FREE SUBGROUP NUMBERS MODULO PRIME POWERS

C. KRATTENTHALER† AND T. W. MÜLLER*

Abstract. We characterise when the sequence of free subgroup numbers of a finitely generated virtually free group is ultimately periodic modulo a given prime power.

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 and, for a positive integer λ, let $f_\lambda(\Gamma)$ be the number of free subgroups of index λm_Γ in Γ. In [4], the authors show, among other things, that the number $f_\lambda(\mathrm{PSL}_2(\mathbb{Z}))$ of free subgroups of index 6λ in the inhomogeneous modular group $\mathrm{PSL}_2(\mathbb{Z})$, considered as a sequence indexed by λ, is ultimately periodic modulo any fixed prime power p^α, if p is a prime number with $p \geq 5$. More precise results on the length of the period, and an explicit formula for the linear recurrence satisfied by these numbers modulo p^α are also provided in [4]. As is well known, ultimate periodicity of the sequence $\big(f_\lambda(\Gamma)\big)_{\lambda\geq 1}$ is equivalent to rationality of the corresponding generating function $F_\Gamma(z) = \sum_{\lambda\geq 0} f_{\lambda+1}(\Gamma) z^\lambda$.

The purpose of the present paper is to demonstrate that the periodicity phenomenon discovered in [4] holds in a much wider context, namely that of finitely generated virtually free groups. Indeed, our main result (Theorem 1) provides an explicit characterisation of all pairs (Γ, p^α), where Γ is a finitely generated virtually free group and p^α is a proper prime power, for which the sequence of free subgroup numbers of Γ is ultimately periodic modulo p^α. Roughly speaking, for "almost all" pairs (Γ, p) the sequence $\big(f_\lambda(\Gamma)\big)_{\lambda\geq 0}$ is ultimately periodic modulo p^α for all $\alpha \geq 1$, the only exception occurring when $p \mid m_\Gamma$ and $\mu_p(\Gamma) = 0$, where $\mu_p(\Gamma)$ is a certain invariant defined in (2.10) and discussed in the paragraph following that formula.

In order to further place our results into context, we point out that, for primes p dividing the constant m_Γ, an elaborate theory is presented in [9] for the behaviour of the arithmetic function $f_\lambda(\Gamma)$ modulo p. Recently, this theory has been supplemented by congruences modulo (essentially arbitrary) 2-powers and 3-powers for the number of free subgroups of finite index in lifts of the classical modular group; that is, amalgamated

2010 *Mathematics Subject Classification.* Primary 05A15; Secondary 05E99 11A07 20E06 20E07.
Key words and phrases. virtually free groups, free subgroup numbers, modular group, periodic sequences.
†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.

products of the form

$$\Gamma_\ell = C_{2\ell} \underset{C_\ell}{*} C_{3\ell}, \quad \ell \geq 1;$$

cf. Theorems 19 and 20 in [3, Sec. 8], and Section 16 in [5], in particular, [5, Thms. 49–52]. These results demonstrate a highly non-trivial behaviour of the sequences $\big(f_\lambda(\Gamma_\ell)\big)_{\lambda\geq 1}$ modulo powers of 2 if ℓ is odd (in which case $\mu_2(\Gamma_\ell) = 0$), and modulo powers of 3 for $3 \nmid \ell$ (in which case $\mu_3(\Gamma_\ell) = 0$). For instance, for the sequence $\big(f_\lambda = f_\lambda(\Gamma_1)\big)_{\lambda\geq 1}$ of free subgroup numbers of the group $\mathrm{PSL}_2(\mathbb{Z})$, one finds that:

(1) $f_\lambda \equiv -1 \pmod 3$ if, and only if, the 3-adic expansion of λ is an element of $\{0,2\}^*1$;

(2) $f_\lambda \equiv 1 \pmod 3$ if, and only if, the 3-adic expansion of λ is an element of
$$\{0,2\}^*100^* \cup \{0,2\}^*122^*;$$

(3) for all other λ, we have $f_\lambda \equiv 0 \pmod 3$;

cf. [5, Cor. 53]. Here, for a set Ω, we denote by Ω^* the free monoid generated by Ω. All this is in sharp contrast to "most" of the cases in the classification result in Theorem 1, which exhibit "simple" (ultimate) periodicity.

The proof of Theorem 1 has two main steps. The first consists in showing that, if p is a prime number *not* dividing m_Γ, then the sequence $\big(f_\lambda(\Gamma)\big)_{\lambda\geq 1}$ is ultimately periodic modulo p^α for every integer $\alpha \geq 1$; this is the contents of Theorem 2. Its proof is based on a folklore fact concerning linear recurrence relations with constant coefficients stated in Section 4, on a bound for the p-divisibility of the function $g_\lambda(\Gamma)$ provided by Lemma 6 in Section 5, and the (well-known) classification of virtually infinite-cyclic groups recalled in Section 6. The proof of Theorem 2 appears in Section 7. The second step concerns the case where $p \mid m_\Gamma$, and is largely taken care of by Theorem 3. The proof of the latter theorem in Section 8 is by an inductive argument, which is based on an earlier generating function result in [9]. The proof of Theorem 1 itself is given in Section 9. Precise formulations of our main results are found in Section 3, while the next section collects together definitions as well as some background material on virtually free groups.

2. Some preliminaries on virtually free groups

Our notation and terminology here follows Serre's book [12]; in particular, the category of graphs used is described in [12, §2]. This category deviates slightly from the usual notions in graph theory. Specifically, a *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, 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*.

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 $\pi_1(\Gamma(-), X) \cong \Gamma$. If $\mathfrak{F}$ is a free subgroup of finite index in Γ then, following an idea of C. T. C. Wall, one defines the (rational) Euler characteristic $\chi(\Gamma)$ of Γ as

$$\chi(\Gamma) = -\frac{\mathrm{rk}(\mathfrak{F}) - 1}{(\Gamma : \mathfrak{F})}. \tag{2.1}$$

(This is well-defined in view of Schreier's index formula in [10].) In terms of the above decomposition of Γ, we have

$$\chi(\Gamma) = \sum_{v \in V(X)} \frac{1}{|\Gamma(v)|} - \sum_{e \in \mathcal{O}(X)} \frac{1}{|\Gamma(e)|}. \tag{2.2}$$

Equation (2.2) reflects the fact that, in our situation, the Euler characteristic in the sense of Wall coincides with the equivariant Euler characteristic $\chi_T(\Gamma)$ of Γ relative to the tree T canonically associated with Γ in the sense of Bass–Serre theory; cf. [1, Chap. IX, Prop. 7.3] or [11, Prop. 14].

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

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

(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

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

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

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

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. [8, 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. [7, Prop. 1] or [8, Lemma 2]. We observe that, as a consequence of (2.2), the Euler characteristic of Γ can be expressed in terms of the type $\tau(\Gamma)$ via

$$\chi(\Gamma) = -m_\Gamma^{-1} \sum_{\kappa | m_\Gamma} \varphi(m_\Gamma/\kappa)\, \zeta_\kappa(\Gamma), \tag{2.3}$$

where φ is Euler's totient function. It follows in particular that, if two finitely generated virtually free groups have the same number of free subgroups of index n for every n, then their Euler characteristics must coincide.

The proof of Theorem 2, as given in Section 7, is based on the analysis of a second arithmetic function associated with the group Γ. 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

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

in particular, $g_0(\Gamma)=1$. The sequences $\big(f_\lambda(\Gamma)\big)_{\lambda\ge1}$ and $\big(g_\lambda(\Gamma)\big)_{\lambda\ge0}$ are related via the Hall-type transformation formula[1]

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

Moreover, a careful analysis of the universal mapping property associated with the presentation $\Gamma \cong \pi_1(\Gamma(-), X)$ leads to the explicit formula

$$g_\lambda(\Gamma) = \frac{\prod\limits_{e\in\mathcal{O}(X)} (\lambda m_\Gamma/|\Gamma(e)|)!\,|\Gamma(e)|^{\lambda m_\Gamma/|\Gamma(e)|}}{\prod\limits_{v\in V(X)} (\lambda m_\Gamma/|\Gamma(v)|)!\,|\Gamma(v)|^{\lambda m_\Gamma/|\Gamma(v)|}}, \quad \lambda \ge 0, \tag{2.6}$$

for $g_\lambda(\Gamma)$, where $\mathcal{O}(X)$ is any orientation of X; cf. [8, Prop. 3]. Introducing the generating functions

$$F_\Gamma(z) := \sum_{\lambda\ge0} f_{\lambda+1}(\Gamma) z^\lambda \text{ and } G_\Gamma(z) := \sum_{\lambda\ge0} g_\lambda(\Gamma) z^\lambda,$$

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

$$F_\Gamma(z) = m_\Gamma \frac{d}{dz}\big(\log G_\Gamma(z)\big). \tag{2.7}$$

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). We note that, in view of (2.1), the quantity $\mu(\Gamma)$ is connected with the Euler characteristic of Γ via

$$\mu(\Gamma) + m_\Gamma \cdot \chi(\Gamma) = 1, \tag{2.8}$$

which shows in particular that $\mu(\Gamma)$ is well-defined. Combining Equations (2.3) and (2.8), we see that the free rank $\mu(\Gamma)$ can be expressed in terms of the type of Γ via

$$\mu(\Gamma) = 1 + \sum_{\kappa\mid m_\Gamma} \varphi(m_\Gamma/\kappa)\zeta_\kappa(\Gamma). \tag{2.9}$$

Given a finitely generated virtually free group Γ and a prime number p, we introduce, in analogy with formula (2.9), the *p-rank* $\mu_p(\Gamma)$ of Γ via the equation

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

Clearly, $\mu_p(\Gamma) \ge 0$, with equality occurring in this inequality 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 $\kappa < m_\Gamma$. Similarly, we have $\mu_p(\Gamma)=1$ if, and only if, (i) $\zeta_\kappa(\Gamma)=0$ for all κ with $p\mid\kappa\mid m_\Gamma$, or (ii) Γ is the fundamental group of a tree of groups, m_Γ is even, $p \mid m_\Gamma/2$, $\zeta_{m_\Gamma/2}(\Gamma)=1$,

[1] See [8, Cor. 1], or [2, Prop. 1] for a more general result.

and $\zeta_\kappa(\Gamma) = 0$ for $p \mid \kappa \mid m_\Gamma$ and $\kappa < m_\Gamma/2$. To give some concrete examples, if p is an odd prime number, then the groups

$$\Gamma_{p,\alpha} = C_2 * C_{2p} * \underbrace{C_p * \cdots * C_p}_{\alpha \text{ copies}}, \quad \alpha \geq 0$$

satisfy $\mu_p(\Gamma_{p,\alpha}) = 1$, while the groups

$$\Gamma_{2,\alpha} = C_4 * C_4 * \underbrace{C_2 * \cdots C_2}_{\alpha \text{ copies}}, \quad \alpha \geq 0$$

satisfy $\mu_2(\Gamma_{2,\alpha}) = 1$.

3. Periodicity results for $f_\lambda(\Gamma)$

Here and in the sequel, given power 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; in particular, the phrase "$F_\Gamma(z)$ is rational modulo p^α" means that $F_\Gamma(z)$ equals a certain rational function modulo p^α in the sense of the above definition. (It is well known that rationality of the generating function $F_\Gamma(z)$ is equivalent to ultimate periodicity of its sequence of coefficients $\big(f_\lambda(\Gamma)\big)_{\lambda \geq 1}$.) The main result of this section, which completely characterises rationality of the generating function $F_\Gamma(z)$ modulo prime powers, is as follows.

Theorem 1. *Let Γ be a finitely generated virtually free group, let p be a prime number, and let $F_\Gamma(z)$ denote the generating function $\sum_{\lambda \geq 0} f_{\lambda+1}(\Gamma) z^\lambda$ for the free subgroup numbers of Γ. Then the following assertions are equivalent:*

(I) *the series $F_\Gamma(z)$ is rational modulo p^α for each positive integer α;*

(II) *the series $F_\Gamma(z)$ is rational modulo p;*

(III) *The pair (Γ, p) satisfies one of the following mutually exclusive conditions:*

- $(\mathrm{III})_1$ $p \nmid m_\Gamma$;
- $(\mathrm{III})_2$ $p \mid m_\Gamma$ *and* $\mu_p(\Gamma) > 0$;
- $(\mathrm{III})_3$ Γ *is finite;*
- $(\mathrm{III})_4$ Γ *is virtually infinite-cyclic and* $p = 2$.

The proof of Theorem 1 is broken up into two main steps, each of which is a meaningful result in its own right. Case $(\mathrm{III})_1$ is taken care of by the following result.

Theorem 2. *Let Γ be a finitely generated virtually free group, let p be a prime number not dividing m_Γ, and let α be a positive integer. Then the sequence $\big(f_\lambda(\Gamma)\big)_{\lambda \geq 1}$ is ultimately periodic modulo p^α. Its (minimal) period length is less than*

$$p^{\alpha\left(p\left(\frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 2\right) - 2\right)}. \tag{3.1}$$

Case $(\mathrm{III})_2$, where $p \mid m_\Gamma$ and $\mu_p(\Gamma) > 0$, is dealt with in our last result.

Theorem 3. *Let Γ be a finitely generated virtually free group, let p be a prime number such that $p \mid m_\Gamma$ and $\mu_p(\Gamma) > 0$, and let α be a positive integer. Then the generating function $F_\Gamma(z)$ for the free subgroup numbers of Γ is rational modulo p^α. More precisely,* *if* $\mu_p(\Gamma) = 1$, *then* $F_\Gamma(z)$ *is a proper rational function modulo* p^α, *whose denominator may be chosen as a power of* $1 - z$ *or* $1 + z$, *respectively, depending on whether the expression*

$$(\mu(\Gamma) - \mu_p(\Gamma))/(p - 1)$$

is even or odd. If $\mu_p(\Gamma) \geq 2$, *then* $F_\Gamma(z)$ *is a polynomial modulo* p^α.

Other ingredients in the proof of Theorem 1 (given in Section 9) are Corollary 10, which describes the function $f_\lambda(\Gamma)$ in the case where Γ is virtually infinite-cyclic, as well as [9, Prop. 2] and [9, Theorem 2].

The proof of Theorem 2, as given in Section 7, is based on the analysis of the rational-valued arithmetic function g_λ defined in (2.4). A careful analysis of the expression (2.6) for $g_\lambda(\Gamma)$, combined with Equation (2.5) connecting the $f_\lambda(\Gamma)$'s and the $g_\lambda(\Gamma)$'s, will show that the numbers $f_\lambda(\Gamma)$ satisfy a linear recurrence of finite order with constant coefficients modulo any fixed prime power p^α if p does not divide m_Γ. By a standard result on linear recurring sequences (see Lemma 5 in Section 4), Theorem 2 then follows immediately.

The proof of Theorem 3 is given in Section 8. It is based on a functional equation modulo p (with $p \mid m_\Gamma$) satisfied by the generating function $F_\Gamma(z)$ for the free subgroup numbers $f_\lambda(\Gamma)$ established in [9].

We conclude this section with some remarks.

Remarks 4. (1) It is shown in [9] that, if Γ is a finitely generated virtually free group with $\mu_p(\Gamma) = 0$ for a given prime p, then the function $f_\lambda(\Gamma)$ satisfies the congruence

$$f_\lambda(\Gamma) \equiv (-1)^{\frac{(\mu(\Gamma)-1)}{p-1}} \lambda^{-1} \binom{\frac{\mu(\Gamma)\lambda}{p-1}}{\frac{\lambda-1}{p-1}} \pmod{p};$$

cf. [9, Eqn. (35)]. In general, it remains an open problem how the free subgroup numbers of a finitely generated virtually free group Γ with $\mu_p(\Gamma) = 0$ behave modulo higher p-powers. The only results known in this direction concern (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 $\mathfrak{H}(3) \cong \mathrm{PSL}_2(\mathbb{Z})$ with $p = 3$; see Corollary 34 and Theorem 35 in [3], and [5, Sec. 16].

(2) By a *cyclic cover*, we mean the fundamental group Γ of a finite graph $(\Gamma(-), X)$ of finite cyclic groups. To fix ideas, we shall assume that the canonical embeddings associated with $(\Gamma(-), X)$ are induced by the identity maps of the corresponding vertex stabilisers. Let $\Gamma = \pi_1(\Gamma(-), X)$ be a cyclic cover, and let ℓ be a positive integer. Then we define the *ℓ-th lift* Γ_ℓ *of* Γ as the cyclic cover resulting from $(\Gamma(-), X)$ by multiplying the order of each (vertex or edge) stabiliser by a factor ℓ. The last assertion in Theorem 3 implies that $F_{\Gamma_\ell}(z)$ is a polynomial modulo all proper p-powers for all lifts Γ_ℓ of cyclic covers Γ with $\mu(\Gamma_\ell) = \mu(\Gamma) \geq 2$, and $p \mid \ell$, even if $p \nmid m_\Gamma$.

(3) In order to illustrate Theorem 3, let us consider the case where $\Gamma = \mathfrak{H}(6) \cong C_2 * C_6$ and $p = 3$. Indeed, in this example, we have $3 \mid m_{\mathfrak{H}(6)} = 6$ and $\mu_3(\mathfrak{H}(6)) = 1$. If one applies the algorithm which is implicit in the proof of Theorem 3 given in Section 8,

then, modulo $3^9 = 19683$, one obtains

$$F_{\mathfrak{H}(6)}(z) = \frac{1}{(1+z)^{10}}(19680z^9 + 585z^8 + 1926z^7 + 6165z^6 + 7326z^5 \\ + 1584z^4 + 1566z^3 + 17433z^2 + 1845z + 15) \qquad \text{modulo } 3^9.$$

From this expression, it is not difficult to deduce that the sequence $\big(f_\lambda(\mathfrak{H}(6))\big)_{\lambda\ge1}$, when taken modulo 3^9, is in fact purely periodic with minimal period length $2\cdot 3^{11} = 354294$. Namely, we have

$$\frac{1}{(1+z)^{10}} = \sum_{n\ge0}(-1)^n\binom{n+9}{9}z^n. \tag{3.2}$$

Furthermore,

$$\prod_{\ell=1}^{9}(n+3^{11}+\ell) - \prod_{\ell=1}^{9}(n+\ell) \equiv 3^{11}\left(\prod_{\ell=1}^{9}(n+\ell)\right)\sum_{\ell=1}^{9}\frac{1}{n+\ell} \pmod{3^{13}} \\ \equiv 0 \pmod{3^{13}},$$

since each product $\prod_{\ell=1}^{9}(n+\ell)$ contains at least three factors divisible by 3, at most one of which is divided out by a fraction $\frac{1}{n+\ell}$. Since $9! = 3^4\cdot 4480$ with 4480 not divisible by 3, the above calculation implies

$$\binom{n+3^{11}+9}{9} \equiv \binom{n+9}{9} \pmod{3^9},$$

and it is easy to see that there is no period smaller than 3^{11} of the binomial coefficient $\binom{n+9}{9}$. Using this observation in (3.2), we conclude that the coefficients in the series $1/(1+z)^{10}$ are periodic with minimal period length $2\cdot3^{11}$, implying our claim.

(4) For a finitely generated virtually free group Γ, denote by $\hat\Gamma$ the isomorphism class of Γ. Given a prime number p, define a density $\mathfrak{D}_p$ of isomorphism classes of groups Γ with $\mu_p(\Gamma)=0$ in all isomorphism classes by

$$\mathfrak{D}_p := \lim_{M\to\infty}\frac{\left|\left\{\hat\Gamma : m_\Gamma \le M,\, \mu(\Gamma)\le M,\, \mu_p(\Gamma)=0\right\}\right|}{\left|\left\{\hat\Gamma : m_\Gamma\le M,\, \mu(\Gamma)\le M\right\}\right|}.$$

Note that this definition makes sense in view of [8, Prop. 4] and Equation (2.8). We conjecture that $\mathfrak{D}_p = 0$ for all prime numbers p.

4. Periodicity of sequences over finite rings

In this section we review a standard result on linear recurring sequences (usually only formulated over finite fields), which will be used in a crucial manner in the proof of Theorem 2 in Section 7.

Let Λ be a finite commutative ring with identity, and let $\mathcal{S} = (s_n)_{n\ge0}$ be a sequence of elements of Λ. Suppose that there exist a positive integer d and elements α_0, $\alpha_1,\dots,\alpha_{d-1}\in\Lambda$, such that $\mathcal{S}$ satisfies the relation

$$s_{n+d} = \alpha_{d-1}s_{n+d-1} + \alpha_{d-2}s_{n+d-2} + \cdots + \alpha_0 s_n, \quad n\ge0. \tag{4.1}$$

Then $\mathcal{S}$ is termed a (*homogeneous*) *linear recurring sequence* over Λ *of order* d, a relation of the form (4.1) itself is called a (*homogeneous*) *linear recurrence relation* (or difference relation) *of order* d.

The sequence $\mathcal{S} = (s_n)_{n\ge0}$ is termed *ultimately periodic*, if there exist integers $\omega > 0$ and $n_0 \ge 0$, such that $s_{n+\omega} = s_n$ holds for all $n \ge n_0$. The integer ω is then called a *period* of $\mathcal{S}$. The smallest number among all the possible periods ω of an ultimately periodic sequence $\mathcal{S}$ is called the *least period* $\omega_0 = \omega_0(\mathcal{S})$ of $\mathcal{S}$. If $\mathcal{S} = (s_n)_{n\ge0}$ is ultimately periodic with least period ω_0, then the least non-negative integer n_0 such that $s_{n+\omega_0} = s_n$ for all $n \ge n_0$ is called the *preperiod* of $\mathcal{S}$. An ultimately periodic sequence $\mathcal{S} = (s_n)_{n\ge0}$ with least period $\omega_0(\mathcal{S})$ is termed *purely periodic*, if $s_{n+\omega_0(S)} = s_n$ for all $n \ge 0$. It is easy to see that a sequence $\mathcal{S} = (s_n)_{n\ge0}$ is purely periodic, if, and only if, there exists an integer $\omega > 0$ such that $s_{n+\omega} = s_n$ for all $n \ge 0$. Also, every period of an ultimately periodic sequence is divisible by the least period.

Linear recurring sequences over finite rings are always (ultimately) periodic. The precise fact that we are going to use in the proof of Theorem 2 is the following.

Lemma 5. *Let $\mathcal{S} = (s_n)_{n\ge0}$ be a homogeneous linear recurring sequence of order $d \ge 1$ over a finite commutative ring Λ with identity. Then $\mathcal{S}$ is ultimately periodic with least period $\omega_0(\mathcal{S}) < |\Lambda|^d$.*

The proof of Lemma 5 is virtually identical with that in the case of finite fields; see [6, Theorem 8.7].

5. A bound on the p-divisibility of $g_\lambda(\Gamma)$

We use the standard notation for the p-adic valuation of rational numbers. That is, if $\alpha = r/s$, then $v_p(\alpha) = v_p(r) - v_p(s)$, where $v_p(r)$ is the exponent of the highest p-power dividing r, with $v_p(s)$ being defined in an analogous way.

Lemma 6. *Let Γ be a finitely generated virtually free group of free rank $\mu(\Gamma) \ge 2$, and let p be a prime number not dividing m_Γ. Then we have*

$$v_p\big(g_\lambda(\Gamma)\big) \ge (\mu(\Gamma) - 1) \cdot v_p(\lambda!), \quad \lambda \ge 0. \tag{5.1}$$

In particular, the function $v_p\big(g_\lambda(\Gamma)\big)$ is non-negative, and unbounded as $\lambda \to \infty$.

Proof. Let $(\Gamma(-), X)$ be a Stallings decomposition of Γ, and let $\mathcal{O}(X)$ be any orientation of the graph X. In proving (5.1), we may ignore the factor

$$\frac{\prod\limits_{e\in\mathcal{O}(X)} |\Gamma(e)|^{\lambda m_\Gamma/|\Gamma(e)|}}{\prod\limits_{v\in V(X)} |\Gamma(v)|^{\lambda m_\Gamma/|\Gamma(v)|}} \tag{5.2}$$

in the expression (2.6) for $g_\lambda(\Gamma)$, since $p \nmid m_\Gamma$ by assumption. We shall in fact show that the remaining expression in (2.6) is an integer, and that $(\lambda!)^{-m_\Gamma\cdot\chi(\Gamma)}$ divides that integer. In symbols:

$$(\lambda!)^{-m_\Gamma\cdot\chi(\Gamma)} \quad \text{divides} \quad \frac{\prod\limits_{e\in\mathcal{O}(X)} (\lambda m_\Gamma/|\Gamma(e)|)!}{\prod\limits_{v\in V(X)} (\lambda m_\Gamma/|\Gamma(v)|)!}. \tag{5.3}$$

Since, by (2.8), we have $\mu(\Gamma)-1=-m_\Gamma\cdot\chi(\Gamma)$, in combination with the above remark this would establish (5.1).

For the proof of (5.3), we regard the graph X as undirected, in the sense that each pair $\{e,\bar e\}$ is considered as one (undirected) edge, and we consider the edge and vertex labels as abstract labels satisfying the condition that an edge label divides the vertex labels of the vertices incident with the edge. By abuse of notation, we still write $|\Gamma(e)|$ for the label of the edge e and $|\Gamma(v)|$ for the label of the vertex v.

We shall build up the graph X by adding edges and vertices one by one, and at each step record the contributions of the added edges and vertices to (5.3).

We distinguish two cases, depending on whether X contains a cycle or not. Suppose first that X contains a cycle

$$v_1,e_1,v_2,e_2,\dots,v_m,e_m,v_1,$$

where v_i and v_{i+1} are the vertices incident with the (undirected) edge e_i, $i=1,2,\dots,m$ (where v_{m+1} is identified with v_1), and $v_1,v_2,\dots,v_m$ are pairwise distinct. Since, by the definition of a graph of groups, we have $|\Gamma(e_i)|$ divides $|\Gamma(v_i)|$, $i=1,2,\dots,m$, it follows that

$$\left(m_\Gamma\left(\tfrac{1}{|\Gamma(e_i)|}-\tfrac{1}{|\Gamma(v_i)|}\right)\lambda\right)! \quad\text{divides}\quad \frac{(\lambda m_\Gamma/|\Gamma(e_i)|)!}{(\lambda m_\Gamma/|\Gamma(v_i)|)!},\quad i=1,2,\dots,m, \tag{5.4}$$

by integrality of binomial coefficients.

Let G be the graph consisting of this cycle. If G is already all of X, then our construction stops here. Otherwise, there must be an edge e that is not yet included in G which emanates from some vertex of G. There are two possible cases: either the other vertex incident with e, say v, is not yet in G, in which case we have

$$\left(m_\Gamma\left(\tfrac{1}{|\Gamma(e)|}-\tfrac{1}{|\Gamma(v)|}\right)\lambda\right)! \quad\text{divides}\quad \frac{(\lambda m_\Gamma/|\Gamma(e)|)!}{(\lambda m_\Gamma/|\Gamma(v)|)!}, \tag{5.5}$$

or v is already in G, in which case we have (trivially)

$$\left(m_\Gamma\tfrac{1}{|\Gamma(e)|}\lambda\right)! \quad\text{divides}\quad (\lambda m_\Gamma/|\Gamma(e)|)!. \tag{5.6}$$

We add e and v (in the case it is not yet in G) to G. If G is already all of X, then we stop. Otherwise, we iterate the above step of adding an edge and possibly a vertex to G until we have obtained all of X.

Now we "multiply" all divisor relations (5.4)–(5.6) together, to obtain

$$\left(\prod_{e\in S_1}\left(m_\Gamma\tfrac{1}{|\Gamma(e)|}\lambda\right)!\prod_{(e,v)\in S_2}\left(m_\Gamma\left(\tfrac{1}{|\Gamma(e)|}-\tfrac{1}{|\Gamma(v)|}\right)\lambda\right)!\right)\quad\text{divides}\quad\frac{\prod_{e\in\mathcal{O}(X)}(\lambda m_\Gamma/|\Gamma(e)|)!}{\prod_{v\in V(X)}(\lambda m_\Gamma/|\Gamma(v)|)!}, \tag{5.7}$$

where S_1 is the set of all those edges e of X which, in the above algorithm, were added to G without a vertex being added at the same time, and where S_2 is the set of all pairs (e,v) of an edge e and a vertex v which are either a pair of the form (e_i,v_i), $i=1,2,\dots,m$, or were added together in the same step of the above algorithm. Since $(\lambda!)^m$ divides $(m\lambda)!$ for any positive integer m, our claim (5.3) follows, and thus the assertion (5.1).

If X does not contain a cycle, then we proceed in a similar fashion. The initial step has to be modified, however. To start with, we claim that there must exist an edge e_0 such that $|\Gamma(e_0)|$ is less than $|\Gamma(v_0)|$ *and* less than $|\Gamma(v_1)|$, where v_0 and v_1 are the two vertices incident with e_0. Indeed, any edge e in X with $|\Gamma(e)| = |\Gamma(v)|$ for a vertex v incident with e could actually be contracted "into the other vertex," by which we mean that upon contraction of e the vertex v "disappears" and only the other vertex incident with e is retained. This contraction generates a new graph X' with the same Euler characteristic (cf. (2.2)) and the same associated function g_λ (cf. (2.6)). If the graph X would only consist of such edges, then, after contraction of all the edges, only a single labelled vertex would remain, which has positive Euler characteristic (again, in the sense of (2.2)), namely $1/m_\Gamma$. By (2.8), it would follow that $\mu(\Gamma) = 0$, a contradiction.

Let now e_0 be an edge with $|\Gamma(e_0)| < |\Gamma(v_0)|$ and $|\Gamma(e_0)| < |\Gamma(v_1)|$, where v_0 and v_1 are the vertices incident with e_0. We let G be the graph consisting of e_0, v_0 and v_1. We have

$$\left(m_\Gamma\left(\tfrac{1}{|\Gamma(e_0)|} - \tfrac{1}{|\Gamma(v_0)|} - \tfrac{1}{|\Gamma(v_1)|}\right)\lambda\right)! \quad \text{divides} \quad \frac{(\lambda m_\Gamma/|\Gamma(e_0)|)!}{(\lambda m_\Gamma/|\Gamma(v_0)|)!\,(\lambda m_\Gamma/|\Gamma(v_1)|)!}. \tag{5.8}$$

The subsequent steps are the same as before: that is, if the graph G obtained so far should not yet be all of X, we choose an edge e not yet in G that is incident with one of the vertices in G, and we add it to G together with the other vertex incident with e. In each of these addition steps (5.5) holds. Finally, again, all divisibility relations (5.8) and (5.5), are "multiplied" together. The result is (5.7) (with an empty set S_1), from which the claim (5.3) results in the same way as before. □

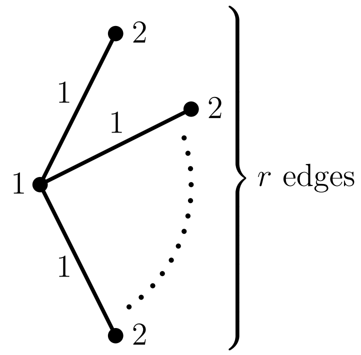

FIGURE 1. The graph of $(C_2)^{*r}$

Remarks 7. (1) It is easy to see that the estimate (5.1) in Lemma 6 is, in general, best possible for odd primes p. For instance, let $\Gamma = (C_2)^{*r}$, where $r \geq 2$. The corresponding graph of groups is shown in Figure 1 together with its vertex and edge labels. We have

$$g_\lambda(\Gamma) = \frac{(2\lambda)!^{r-1}}{\lambda!^r\, 2^{r\lambda}},$$

and, for a prime $p \geq 3$ and $\lambda = p^s$ with $s \geq 0$, we have

$$v_p\big(g_\lambda(\Gamma)\big) = \big(2(r-1) - r\big)\frac{p^s - 1}{p-1} = (r-2)v_p(\lambda!) = (\mu(\Gamma) - 1)v_p(\lambda!).$$

(2) The reader should observe that, in the proof of Lemma 6, we actually proved a slightly stronger result, namely the divisibility relation (5.7), the factor (5.2) not

contributing anything to (5.1). However, since there is no elegant way to write down the result (as a matter of fact, there are *several* inequivalent results that can be derived from different parsings of the graph X), we refrain from exploiting this relation.

6. The classification of virtually infinite-cyclic groups

Virtually infinite-cyclic groups play a certain role in topology as they are precisely the finitely generated groups with two ends. Their structure is well-known; cf. [13, 5.1] or [14, Lemma 4.1].

Proposition 8. *A virtually infinite-cyclic group Γ falls into one of the following two classes:*

(i) Γ *has a finite normal subgroup with infinite-cyclic quotient.*

(ii) Γ *is a free product $\Gamma = G_1 \underset{A}{*} G_2$ of two finite groups G_1 and G_2, with an amalgamated subgroup A of index 2 in both factors.*

Remark 9. In Part (ii) of Proposition 8, A is a finite normal subgroup of Γ with quotient $C_2 * C_2$, the infinite dihedral group.

Corollary 10. *If Γ is virtually infinite-cyclic, then the function $f_\lambda(\Gamma)$ is constant. More precisely, we have $f_\lambda(\Gamma) = m_\Gamma$ for $\lambda \geq 1$ in Case* (i) *of Proposition* 8*, while in Case* (ii) *we have $f_\lambda(\Gamma) = |A| = m_\Gamma/2$.*

Proof. If Γ is as described in Case (i) of Proposition 8, then (2.6) shows that $g_\lambda(\Gamma) = 1$ for $\lambda \geq 0$, leading to $f_\lambda(\Gamma) = m_\Gamma$ for all $\lambda \geq 1$ by (2.5) and an immediate induction on λ.

For Γ as in Case (ii), Equation (2.6) yields

$$g_\lambda(\Gamma) = 2^{-2\lambda}\binom{2\lambda}{\lambda}, \quad \lambda \geq 0.$$

By the binomial theorem applied to the generating function $G_\Gamma(z)$ of the $g_\lambda(\Gamma)$'s, we obtain $G_\Gamma(z) = (1-z)^{-1/2}$, which transforms into the relation

$$F_\Gamma(z) = \frac{|m_\Gamma|}{2(1-z)} = \frac{|A|}{1-z}$$

via (2.7). The desired result follows from this last equation by comparing coefficients. □

7. Proof of Theorem 2

Theorem 2 follows from Lemmas 5 and 6. Indeed, if $\mu(\Gamma) = 0$, then Γ is finite, we have $m_\Gamma = |\Gamma|$, and thus $f_1(\Gamma) = 1$ and $f_\lambda(\Gamma) = 0$ for $\lambda \geq 2$, so that $f_\lambda(\Gamma)$ is ultimately periodic with period and preperiod equal to 1 modulo any prime power. If $\mu(\Gamma) = 1$, then, by Corollary 10, $f_\lambda(\Gamma)$ is constant, thus purely periodic with period equal to 1, again modulo any prime power. Now suppose that $\mu(\Gamma) \geq 2$. Given a positive integer α, let $\lambda_0(\alpha)$ be chosen according to Lemma 6 such that $v_p\big(g_\lambda(\Gamma)\big) \geq \alpha$ for all $\lambda \geq \lambda_0(\alpha)$ and $v_p\big(g_{\lambda_0(\alpha)-1}(\Gamma)\big) < \alpha$. Then consider Equation (2.5) for $\lambda \geq \lambda_0(\alpha)$. All summands on the left-hand side corresponding to indices $\mu \ge \lambda_0(\alpha)$ will vanish modulo p^α, as does the right-hand side, and we obtain the congruence

$$f_{\lambda+\lambda_0(\alpha)}(\Gamma) \equiv -\big(g_1(\Gamma) f_{\lambda+\lambda_0(\alpha)-1}(\Gamma) + \dots + g_{\lambda_0(\alpha)-1}(\Gamma) f_{\lambda+1}(\Gamma)\big) \pmod{p^\alpha}, \quad \lambda \ge 0. \tag{7.1}$$

This provides a homogeneous linear recurrence with constant coefficients in $\mathbb{Z}/p^\alpha\mathbb{Z}$ of order $\lambda_0(\alpha) - 1$ for the sequence $\big(f_\lambda(\Gamma)\big)_{\lambda\ge1}$. Applying Lemma 5 with $\Lambda = \mathbb{Z}/p^\alpha\mathbb{Z}$ and $\mathcal{S} = (f_{\lambda+1}(\Gamma))_{\lambda\ge0}$, we find that, in this last case, $f_\lambda(\Gamma)$ is ultimately periodic modulo p^α with least period $\omega_0 < p^{\alpha(\lambda_0(\alpha)-1)}$.

For proving the claimed upper bound on the (minimal) period length, we need to bound $\lambda_0(\alpha)$ from above. We start by using the estimation (5.1), i.e.,

$$v_p\big(g_\lambda(\Gamma)\big) \ge (\mu(\Gamma) - 1) v_p(\lambda!). \tag{7.2}$$

Thus, we need to bound $v_p(\lambda!)$ from below. We have

$$v_p(\lambda!) = \sum_{\ell\ge1} \left\lfloor \frac{\lambda}{p^\ell} \right\rfloor \ge \sum_{\ell=1}^{\lfloor \log_p \lambda \rfloor} \left(\frac{\lambda}{p^\ell} - \frac{p^\ell - 1}{p^\ell} \right) = \frac{(\lambda+1)}{(p-1)} \frac{(p^{\lfloor \log_p \lambda \rfloor} - 1)}{p^{\lfloor \log_p \lambda \rfloor}} - \lfloor \log_p \lambda \rfloor. \tag{7.3}$$

We claim that, if we substitute

$$\lambda_1(\alpha) := p \left(\frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 2 \right) - 1$$

for λ in the right-hand side of (7.3), then the result is at least $\alpha/(\mu(\Gamma)-1)$. If one then combines (7.2) with (7.3) and observes that the right-hand side of (7.3) is monotone increasing for $\lambda > p$, then one sees that one has proved $v_p\big(g_\lambda(\Gamma)\big) \ge \alpha$ for all $\lambda \ge \lambda_1(\alpha)$. This shows that $\lambda_0(\alpha) \le \lambda_1(\alpha)$, and, in combination with Lemma 5, will establish the upper bound in (3.1) on the period length of the sequences $\big(f_\lambda(\Gamma)\big)_{\lambda\ge1}$.

If one substitutes $\lambda_1(\alpha)$ for λ in the right-hand side of (7.3), then one obtains

$$\left(\frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 2 \right) \frac{p}{(p-1)} \frac{(p^L - 1)}{p^L} - L, \tag{7.4}$$

where $L = \lfloor \log_p \lambda_1(\alpha) \rfloor$. We have

$$\begin{aligned} &\left(\frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 2 \right) \frac{p}{(p-1)} \frac{(p^L - 1)}{p^L} - L \\ &\qquad \ge \left(\frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 2 \right) - \left\lfloor \log_p \left(p \left(\alpha + \lfloor \log_p \alpha \rfloor + 2 \right) \right) \right\rfloor \\ &\qquad \ge \frac{\alpha}{\mu(\Gamma)-1} + \lfloor \log_p \alpha \rfloor + 1 - \left\lfloor \log_p \alpha + \log_p \left(1 + \frac{\lfloor \log_p \alpha \rfloor + 2}{\alpha} \right) \right\rfloor. \end{aligned} \tag{7.5}$$

In order to demonstrate our claim, we have to show

$$\lfloor \log_p \alpha \rfloor + 1 - \left\lfloor \log_p \alpha + \log_p \left(1 + \frac{\lfloor \log_p \alpha \rfloor + 2}{\alpha} \right) \right\rfloor \ge 0. \tag{7.6}$$

If $\alpha = 1$, then, from (7.5), we obtain that the expression (7.6) is bounded below by

$$1 - \lfloor \log_p 3 \rfloor \ge 0.$$

If $\alpha = 2$, then (7.6) becomes

$$\lfloor \log_p 2 \rfloor + 1 - \left\lfloor \log_p 2 + \log_p \left(1 + \frac{\lfloor \log_p 2 \rfloor + 2}{2} \right) \right\rfloor \ge 0,$$

which indeed holds true. (More precisely, the expression on the left-hand side above equals 0 if $p = 2$, and otherwise it equals 1.) On the other hand, if $\alpha \ge 3$, then the left-hand side of (7.6) can be bounded below by

$$\begin{aligned} \lfloor \log_p \alpha \rfloor + 1 - & \left\lfloor \log_p \alpha + \log_p \left(1 + \frac{\lfloor \log_p 3 \rfloor + 2}{3} \right) \right\rfloor \\ & \ge \lfloor \log_p \alpha \rfloor + 1 - \lfloor \log_p \alpha + \log_p 2 \rfloor \\ & \ge \lfloor \log_p \alpha \rfloor + 1 - \lfloor \log_p \alpha + 1 \rfloor \\ & \ge 0. \end{aligned}$$

Thus, in all cases, the expression (7.4) is bounded below by $\alpha/(\mu(\Gamma)-1)$. In combination with (7.2) and (7.3) this establishes the inequality $v_p\big(g_\lambda(\Gamma)\big) \ge \alpha$ for $\lambda \ge \lambda_1(\alpha) \ge \lambda_0(\alpha)$. This completes the proof of the bound (3.1) on the minimal period length and, thus, of the theorem.

8. Proof of Theorem 3

If $p \mid m_\Gamma$, then, by [9, Eq. (3)], the generating function $F_\Gamma(z)$ satisfies the congruence

$$F_\Gamma(z) = z^{\mu_p(\Gamma)} F_\Gamma^{\mu_p(\Gamma)}(z) \left(z^{p-1} F_\Gamma(z)^{p-1} - 1 \right)^{(\mu(\Gamma)-\mu_p(\Gamma))/(p-1)} \quad \text{modulo } p. \tag{8.1}$$

As is argued in [9], if $p \mid m_\Gamma$ and $\mu_p(\Gamma) > 0$, then it is clear from this congruence that $F_\Gamma(z) = 0$ modulo p. We shall now demonstrate by an induction on α that, for all integers $\alpha \ge 1$, the generating function $F_\Gamma(z)$ is rational when coefficients are reduced modulo p^α.

For $\alpha = 1$ this last statement is true due to the above remark. Let us suppose that we have already shown that $F_\Gamma(z)$ is rational when coefficients are reduced modulo p^α, say $F_\Gamma(z) = R(z)$ modulo p^α, for some rational function $R(z)$ over the integers whose denominator is not divisible by p. By [9, Eq. (12)] and (8.1), we know that

$$\begin{aligned} F_\Gamma(z) = z^{\mu_p(\Gamma)} F_\Gamma^{\mu_p(\Gamma)}(z) & \left(z^{p-1} F_\Gamma(z)^{p-1} - 1 \right)^{(\mu(\Gamma)-\mu_p(\Gamma))/(p-1)} \\ & + p \cdot \mathcal{P}(z, F_\Gamma(z), F'_\Gamma(z), F''_\Gamma(z), \dots, F_\Gamma^{(\mu(\Gamma-1))}(z)), \end{aligned} \tag{8.2}$$

where $\mathcal{P}(z, F_\Gamma(z), F'_\Gamma(z), \dots, F_\Gamma^{(\mu(\Gamma)-1)}(z))$ is a polynomial in $z, F_\Gamma(z), F'_\Gamma(z), \dots,$ $F_\Gamma^{(\mu(\Gamma)-1)}(z)$ over the *rationals*. However, it is proven in [9, Sections 3 and 5] that, if $p \mid m_\Gamma$, the rational coefficients can be written with denominators which are relatively prime to p, a fact that we shall tacitly use in the sequel.

We now make the Ansatz $F_\Gamma(z) = R(z) + p^\alpha Y(z)$, for some unknown formal power series $Y(z)$, we substitute in (8.2), and then consider the result modulo $p^{\alpha+1}$. Since

$$(R(z) + p^\alpha Y(z))^e = R^e(z) + e p^\alpha R^{e-1}(z) Y(z) \quad \text{modulo } p^{\alpha+1},$$

we arrive at the congruence

$$\begin{aligned} R(z)+p^\alpha Y(z) &= \sum_{i=0}^{M}(-1)^{M-i}\binom{M}{i} z^{\mu_p(\Gamma)+i(p-1)} \\ &\quad\cdot \big(R^{\mu_p(\Gamma)+i(p-1)}(z)+p^\alpha(\mu_p(\Gamma)+i(p-1))R^{\mu_p(\Gamma)+i(p-1)-1}(z)Y(z)\big)\\ &\quad + p\cdot \mathcal{P}(z,R(z),R'(z),\dots,R^{(\mu(\Gamma)-1)}(z)) \qquad \text{modulo } p^{\alpha+1}, \end{aligned} \tag{8.3}$$

where M is short for $(\mu(\Gamma)-\mu_p(\Gamma))/(p-1)$. By rearranging terms, we transform this congruence into

$$\begin{aligned} p^\alpha Y(z)\cdot\bigg(-1+\sum_{i=0}^{M}(-1)^{M-i}\binom{M}{i} z^{\mu_p(\Gamma)+i(p-1)}(\mu_p(\Gamma)+i(p-1))R^{\mu_p(\Gamma)+i(p-1)-1}(z)\bigg)\\ = R(z)-\sum_{i=0}^{M}(-1)^{M-i}\binom{M}{i} z^{\mu_p(\Gamma)+i(p-1)}R^{\mu_p(\Gamma)+i(p-1)}(z)\\ - p\cdot \mathcal{P}(z,R(z),R'(z),\dots,R^{(\mu(\Gamma)-1)}(z)) \qquad \text{modulo } p^{\alpha+1}. \end{aligned} \tag{8.4}$$

By induction hypothesis, the right-hand side is divisible by p^α. We may hence divide both sides by p^α, to obtain the congruence

$$Y(z)\cdot\bigg(-1+\sum_{i=0}^{M}(-1)^{M-i}\binom{M}{i} z^{\mu_p(\Gamma)+i(p-1)}(\mu_p(\Gamma)-i)R^{\mu_p(\Gamma)+i(p-1)-1}(z)\bigg)=S(z) \qquad \text{modulo } p,$$

where $S(z)$ can be written as an explicit rational function in z over the integers with denominator not divisible by p. If we remember that, from the base case of the induction (see the sentence below (8.1)), it follows that $R(z)=0$ modulo p, then we see that the above congruence simplifies further to

$$Y(z)\cdot\Big(-1+(-1)^M\mu_p(\Gamma)z^{\mu_p(\Gamma)}R^{\mu_p(\Gamma)-1}(z)\Big)=S(z) \qquad \text{modulo } p. \tag{8.5}$$

We can therefore determine $Y(z)$ modulo p by dividing both sides of the congruence by the term in parentheses on the left-hand side. Hence $Y(z)$ is a rational function modulo p, and therefore $F_\Gamma(z)=R(z)+p^\alpha Y(z)$ is rational modulo $p^{\alpha+1}$. This concludes the induction argument.

The additional assertions in Theorem 3 are now obvious: if $\mu_p(\Gamma)=1$, then each time we divide by $1-(-1)^M z$, and the induction hypothesis guarantees that all denominators of fractions in the congruence (8.5) are powers of $1-(-1)^M z$, cf. the implicit definition of $S(z)$ via (8.4). If, on the other hand, $\mu_p(\Gamma)\ge 2$, then let us suppose as induction hypothesis that $R(z)$ is actually a *polynomial* modulo p^α. Again using the fact that $R(z)=0$ modulo p, we see that, since $\mu_p(\Gamma)+i(p-1)>0$ for all $i\ge 0$ in the current case, the congruence (8.5) reduces to

$$-Y(z)=S(z) \qquad \text{modulo } p.$$

Here, the rational function $S(z)$ is actually a *polynomial*. Consequently, $Y(z)$ is a polynomial modulo p, and thus $F_\Gamma(z) = R(z) + p^\alpha Y(z)$ is a polynomial modulo $p^{\alpha+1}$. This completes the proof of the theorem.

9. Proof of Theorem 1

(I) *implies* (II). This is obvious.

(II) *implies* (III). We may have $p \nmid m_\Gamma$ (Case $(\mathrm{III})_1$), or $p \mid m_\Gamma$ and $\mu_p(\Gamma) > 0$ (Case $(\mathrm{III})_2$), or $p \mid m_\Gamma$ and $\mu_p(\Gamma) = 0$. Due to the definition (2.10) of μ_p, the condition $\mu_p(\Gamma) = 0$ already implies that $p \mid m_\Gamma$ (in the sum on the right-hand side of (2.10) only the term for $\kappa = m_\Gamma$ can be negative). Thus, it remains to consider the case where $\mu_p(\Gamma) = 0$. In this case, Theorem A(iii) in [9] says that either $\mu(\Gamma) = 0$, or $\mu(\Gamma) = 1$ and $p = 2$. In the former case, the group Γ is finite (Case $(\mathrm{III})_3$), while in the latter case Γ is virtually infinite-cyclic (Case $(\mathrm{III})_4$).

(III) *implies* (I). We have to distinguish between the various subcases given in this item. In each case, we have to show that the generating function $F_\Gamma(z)$ is rational modulo p^α for every $\alpha \geq 1$.

Case $(\mathrm{III})_1$. This is taken care of by Theorem 2.

Case $(\mathrm{III})_2$. This is dealt with by Theorem 3.

Case $(\mathrm{III})_3$. This is obvious since in this case $F_\Gamma(z) = 1$.

Case $(\mathrm{III})_4$. Corollary 10 says that in this case the sequence of free subgroup numbers $f_\lambda(\Gamma)$ is constant. Consequently, the corresponding generating function $F_\Gamma(z)$ is rational even over the integers.

Acknowledgements

The authors thank the anonymous referee for helpful suggestions which have led to a streamlined and improved version of this paper.

References

[1] K. S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, 1982.

[2] A. Dress and T. W. Müller, Decomposable functors and the exponential principle, *Adv. Math.* **129** (1997), 188–221.

[3] 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.

[4] 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.

[5] C. Krattenthaler and T. W. Müller, A method for determining the mod-3^k behaviour of recursive sequences, preprint, 83 pages; `ar`χ`iv:1308.2856`.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, 2nd edition, Cambridge University Press, 1997.

[7] T. W. Müller, A group-theoretical generalization of Pascal's triangle, *Europ. J. Conbin.* **12** (1991), 43–49.

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

[9] T. W. Müller and J.-C. Schlage-Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.

[10] O. Schreier, Die Untergruppen der freien Gruppen, *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 161–183.
[11] J.-P. Serre, Cohomologie des groupes discrets. In: *Prospects in Mathematics*, Ann. Math. Stud., vol. 70, Princeton University Press, 1971, pp. 77–169.
[12] J.-P. Serre, *Arbres, Amalgames,* SL_2, Astérisque, vol. 46, Société mathématique de France, Paris, 1977.
[13] J. Stallings, On torsion-free groups with infinitely many ends, *Ann. Math.* **88** (1968), 312–334.
[14] C. T. C. Wall, Poincaré complexes: I, *Ann. Math.* **86** (1967), 213–245.

[†]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.