TRUNCATED VERSIONS OF DWORK'S LEMMA FOR EXPONENTIALS OF POWER SERIES AND p-DIVISIBILITY OF ARITHMETIC FUNCTIONS

C. KRATTENTHALER† AND T. W. MÜLLER*

Abstract. (Dieudonné and) Dwork's lemma gives a necessary and sufficient condition for an exponential of a formal power series $S(z)$ with coefficients in $\mathbb{Q}_p$ to have coefficients in $\mathbb{Z}_p$. We establish theorems on the p-adic valuation of the coefficients of the exponential of $S(z)$, assuming weaker conditions on the coefficients of $S(z)$ than in Dwork's lemma. As applications, we provide several results concerning lower bounds on the p-adic valuation of the number of permutation representations of finitely generated groups. In particular, we give fairly tight lower bounds in the case of an arbitrary finite Abelian p-group, thus generalising numerous results in special cases that had appeared earlier in the literature. Further applications include sufficient conditions for ultimate periodicity of subgroup numbers modulo p for free products of finite Abelian p-groups, results on p-divisibility of permutation numbers with restrictions on their cycle structure, and a curious "supercongruence" for a certain binomial sum.

1. Introduction

For a finitely generated group Γ and a positive integer n, let $s_n(\Gamma)$ denote the number of subgroups of index n in Γ. Moreover, for a non-negative integer n, set

$$h_n(\Gamma) = |\mathrm{Hom}(\Gamma, S_n)|,$$

the number of representations of Γ in the symmetric group S_n. It is well-known that the sequences $\big(s_n(\Gamma)\big)_{n\ge1}$ and $\big(h_n(\Gamma)\big)_{n\ge0}$ are related via the (formal) identity

$$\sum_{n\ge0} \frac{h_n(\Gamma)}{n!} z^n = \exp\left(\sum_{n\ge1} \frac{s_n(\Gamma)}{n} z^n\right); \tag{1.1}$$

cf., for instance, [4, Prop. 1]. By differentiation of both sides, Equation (1.1) is seen to be equivalent to the recurrence relation

$$h_n(\Gamma) = \sum_{k=1}^{n} (n-k+1)_{k-1}\, s_k(\Gamma)\, h_{n-k}(\Gamma), \qquad n \ge 1, \tag{1.2}$$

2010 *Mathematics Subject Classification.* Primary 20K01; Secondary 05A15 05E99 11A07 20E06 20E07 20E08.

Key words and phrases. divisibility by prime powers, exponential of power series, subgroup numbers, finite Abelian p-groups, Kostka–Foulkes polynomial, supercongruences.

†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.

where, for $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}_0$,

$$(\alpha)_n = \begin{cases} \alpha(\alpha+1)\cdots(\alpha+n-1), & n>0,\\ 1, & n=0, \end{cases}$$

is the Pochhammer symbol.

For a prime number p and a positive integer n, the p-adic valuation $v_p(n)$ is defined as the exponent of the largest power of p dividing n. At the origin of the research presented here stands the aim of deriving good lower bounds for the p-adic valuation $v_p\big(h_n(G)\big)$, where p is a prime and G is a finite Abelian p-group, which are sharp for infinitely many n. As a matter of fact, our main results turn out to be much more general than that.

It would appear that investigation into the above problem started in 1951 with the paper [3] by Chowla, Herstein, and Moore, which, among other things, contains the result that[1]

$$v_2\big(h_n(C_2)\big) \ge \left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor; \tag{1.3}$$

cf. [3, Theorem 10]. The more general result to the effect that

$$v_p\big(h_n(C_p)\big) \ge \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor, \quad n \ge 1, \tag{1.4}$$

for arbitrary prime numbers p, was established several times by various sets of authors, apparently starting with Dress and Yoshida [5] in 1991, followed by Grady and Newman [8], and by Ochiai [18, Sec. 3.2], among others. Ochiai's paper also contains somewhat sharper results for small primes; for instance, he shows that

$$v_2\big(h_n(C_2)\big) = (n+5)/4, \quad \text{for } n \equiv 3 \pmod 4,$$

which is an improvement over (1.4) in that case. The most general results in this direction, prior to the present paper, are due to Katsurada, Takegahara, and Yoshida, who establish lower bounds for the p-adic valuation $v_p\big(h_n(G)\big)$ in the case when G is a finite Abelian p-group of rank (minimal number of generators) at most 2; cf. Theorems 1.3 and 1.4 in [10]. For instance, they show that, for a prime p and integers ℓ, m with $\ell \ge m \ge 0$,

$$v_p\big(h_n(C_{p^\ell} \times C_{p^m})\big) \ge \sum_{j=1}^{\ell} \left\lfloor \frac{n}{p^j} \right\rfloor - (\ell - m) \left\lfloor \frac{n}{p^{\ell+1}} \right\rfloor .$$

In the present paper, we start from an arbitrary sequence $s_1, s_2, s_3, \ldots \in \mathbb{Q}_p$ and define a sequence $h_0, h_1, h_2, \ldots \in \mathbb{Q}_p$ by means of the identity

$$H(z) := \sum_{n\ge 0} \frac{h_n}{n!} z^n = \exp\left(S(z)\right),$$

where $S(z) := \sum_{n\ge1} \frac{s_n}{n} z^n$ is the logarithmic generating function for the sequence $(s_n)_{n\ge1}$; in other words, the sequences $(s_n)_{n\ge1}$ and $(h_n)_{n\ge0}$ are related via (an abstract version of) the recurrence relation (1.2). Our main idea is to establish *truncated versions* of an integrality criterion essentially due to Dwork, sometimes also attributed to Dieudonné and Dwork (cf. [13, Ch. 14, p. 76] and the theorem on p. 409 of [19] with

[1]For an integer $m \ge 2$, we denote by C_m the cyclic group of order m.

$A = \mathbb{Z}_p$ and $B = \mathbb{Q}_p$). We begin by stating this integrality criterion in the precise form needed here.

Lemma 1. *For a prime number p, let $S(z)$ and $H(z)$ be formal power series with coefficients in $\mathbb{Q}_p$ related by*

$$H(z) = \exp\big(S(z)\big). \tag{1.5}$$

Then $H(z)$ has all coefficients in $\mathbb{Z}_p$ if, and only if,

$$S(z^p) - pS(z) \in p\mathbb{Z}_p[[z]]. \tag{1.6}$$

Our results do not attempt to provide necessary and sufficient conditions as in Lemma 1 (that would perhaps seem overly ambitious); rather, they provide *sufficient* conditions for a *certain* p-divisibility. Thus, we obtain sufficient conditions for an exponential of a power series to have coefficients which are divisible by certain scales of powers of a given prime p. Which scales one should think of, we gleaned off the scales one finds in Theorems 1.2–1.4 of [10], which, from our point of view, provide p-divisibility results for the "simplest" cases. Theorems 2 and 6 in Section 2 vastly generalise these results. We would like to point out though that the proofs of our theorems draw on a key idea in the proof of Theorem 1.2 in [10]: the idea of comparison with a reference power series.

In our first main result, Theorem 2, we "truncate" Condition (1.6) in Lemma 1 in the sense that we require (1.6) to hold only up to (and including) the coefficient of z^{p^l-1}, for some given l (see (2.1)), assuming only certain weaker conditions for coefficients of higher powers (see (2.2) and (2.3)). This has the effect of replacing p-integrality of the coefficients of the series $H(z)$ in (1.5) by the weaker p-divisibility result for the coefficients given in (2.4). (These results have to be compared with the bound

$$v_p(h_n) \ge v_p(n!) = \sum_{s\ge1} \left\lfloor \frac{n}{p^s} \right\rfloor \tag{1.7}$$

implied by Lemma 1 provided that (1.6) holds, the equality on the right being due to Legendre's formula [14, p. 10] for the p-adic valuation of $n!$.)

As it turns out, for $p = 2$, there exists a case not covered by Theorem 2 (since Condition (2.3) is violated by a small margin), where one may nevertheless even *improve* on the bound given in (2.4). This is the topic of Theorem 6, which vastly generalises Theorem 1.4 of [10]. Section 2 is devoted to the proofs of Theorems 2 and 6, while also providing considerable further comment as well as several corollaries.

Section 3 addresses the case where we have less precise information on the coefficients s_n of the series $S(z)$ in (1.5). More specifically, what can we say if Condition (2.1) is "truncated" to hold only up to the coefficient of z^{p^l} for some l, while beyond we do not have any additional information, except that $s_n \in \mathbb{Z}_p$? While we cannot expect a result as strong as, say, the bound (2.12) in Corollary 4 with l replaced by $l+1$, p-divisibility of the coefficients of the exponential $H(z)$ in (1.5) still turns out to be higher than one might expect in that situation. Theorems 7, 8, 9, and 12 of Section 3 collectively address this problem. For instance, Theorem 7 provides the bound

$$v_p(h_n) \ge \sum_{s\ge1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-1) \left\lfloor \frac{n}{p^l} \right\rfloor - \sum_{s\ge l} \left\lfloor \frac{n}{2p^s} \right\rfloor, \quad n \ge 1,$$

valid for $p \geq 3$ and $(p,l) \neq (3,1)$. In particular, Theorems 7, 8, and 9, together with the special case of Theorem 2 where $l=1$ and $m=0$, combine to demonstrate existence of a sharp *dividing line* concerning the p-divisibility of the coefficient h_n: if $s_1 \not\equiv s_p \mod p\mathbb{Z}_p$ then, for each N, there exists some $n > N$, such that h_n is not divisible by p; if, on the other hand, $s_1 \equiv s_p \mod p\mathbb{Z}_p$, then $v_p(h_n) \to \infty$ as n tends to infinity; cf. Corollary 11 for more precise statements.

The rest of our paper is devoted to applications of our abstract p-divisibility results in Sections 2 and 3. Sections 4 and 5 address the question what may be said concerning the p-divisibility of the homomorphism numbers $h_n(\Gamma)$ where Γ is a finitely generated group. In Proposition 14, it is shown that $s_p(\Gamma) \equiv 0, 1 \pmod p$. This allows us to rephrase the dividing line concerning p-divisibility outlined above in this specific case as follows: if $s_p(\Gamma) \equiv 1 \pmod p$, then $v_p\big(h_n(\Gamma)\big)$ tends to infinity as $n \to \infty$, whereas for $s_p(\Gamma) \equiv 0 \pmod p$ the prime p does not divide $h_n(\Gamma)$ for infinitely many n; see Theorem 17. Section 5 also contains further p-divisibility results for homomorphism numbers $h_n(G)$, where G is a finite p-group (see Theorem 18) or a finite non-Abelian simple group (see Theorem 19).

Our main applications are contained in Section 6. They provide tight lower bounds for the p-divisibility of homomorphism numbers of arbitrary finite Abelian p-groups. Theorems 25 and 26 generalise the earlier results of Katsurada, Takegahara and Yoshida, which concerned the case of Abelian p-groups of rank at most 2, to arbitrary rank.

We conclude our paper with some further applications. The results in Section 7 provide sufficient conditions for ultimate periodicity modulo p of the subgroup numbers $s_n(\Gamma)$, where p is a prime number and Γ is a free product of finite Abelian p-groups. The corresponding theorem, Theorem 27, generalises earlier findings by Grady and Newman [8]. In Section 8, we apply our abstract p-divisibility results to numbers of permutations with restrictions on their cycle structure. Finally, Section 9 presents a curious three-parameter congruence modulo higher powers of a prime p.

2. p-Divisibility of coefficients in exponentials of power series, I

In this section we present our first set of main results. They concern the case where Condition (1.6) in Lemma 1 is truncated after the term involving z^{p^l-1}, for some given l (see (2.1)), while assuming weaker conditions for coefficients of higher powers (see (2.2) and (2.3)). This results in replacing p-integrality of the coefficients of the series $H(z)$ in (1.5) by the weaker p-divisibility result given in (2.4). The proof of Theorem 2 requires an auxiliary result, which is treated separately in Lemma 3.

Theorem 2. *For a prime number p, let $S(z) = \sum_{n\geq 1} \frac{s_n}{n} z^n$ be a formal power series with $s_n \in \mathbb{Q}_p$ for all n, and let $H(z) = \sum_{n\geq 0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. Given non-negative integers l and m with $m < l$, we assume that*

$$S(z^p) - pS(z) = pJ(z) + (s_{p^{l-1}} - s_{p^l}) \frac{z^{p^l}}{p^{l-1}} + O\left(z^{p^l+1}\right) \tag{2.1}$$

with $J(z) \in \mathbb{Z}_p[z]$, that

$$s_{p^{l-1}} \equiv s_{p^l} \mod p^m\mathbb{Z}_p, \tag{2.2}$$

and that

$$v_p(\lambda_i) \ge -(l-m)\left\lfloor \frac{i}{p^l} \right\rfloor + v_p(i) - \frac{p^{\lfloor \log_p i \rfloor - l} - 1}{p-1} + 1 \tag{2.3}$$

for all $i > p^l$, where $\lambda_i = s_i$ if $i/p^{v_p(i)} \ge p^l$ and $\lambda_i = s_i - s_{i/p^e}$ otherwise, where e is minimal such that $i/p^e < p^l$. Then

$$v_p(h_n) \ge \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-m-1)\left\lfloor \frac{n}{p^l} \right\rfloor \tag{2.4}$$

for all n.

Moreover, writing $e_p(n;l,m) = \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-m-1)\left\lfloor \frac{n}{p^l} \right\rfloor$, under these conditions, the quotient

$$Q_n = \frac{h_n}{p^{e_p(n;l,m)}} \tag{2.5}$$

satisfies

$$Q_n \equiv (-1)^l p^{-m}(s_{p^l} - s_{p^{l-1}})Q_{n-p^l} \mod p\mathbb{Z}_p. \tag{2.6}$$

In particular, if $s_{p^{l-1}} \not\equiv s_{p^l} \mod p^{m+1}\mathbb{Z}_p$, then the bound in (2.4) *is tight for all n which are divisible by p^l.*

Remarks. (1) In order to compare the above truncated version with the original Lemma 1, one must compare the bound in (2.4) with $v_p(n!)$ (recall the parenthetical remark containing (1.7)). More specifically, what we loose by truncating (1.6) to (2.1)–(2.3) is the difference

$$\sum_{s\ge 1} \left\lfloor \frac{n}{p^s} \right\rfloor - \left(\sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-m-1)\left\lfloor \frac{n}{p^l} \right\rfloor \right) = (l-m)\left\lfloor \frac{n}{p^l} \right\rfloor + \sum_{s\ge l+1} \left\lfloor \frac{n}{p^s} \right\rfloor .$$

(2) The degree of the polynomial $J(z)$ may be restricted to $p^l - 1$.

(3) The term $(s_{p^{l-1}} - s_{p^l})\frac{z^{p^l}}{p^{l-1}}$ in (2.1) occurs by the definition of $S(z)$; it does not impose any condition. The condition on that term is formulated in (2.2).

(4) It is worth singling out the special case of Theorem 2 where $l = 1$ and $m = 0$: if $s_1 \not\equiv s_p \mod p\mathbb{Z}_p$, then $h_n \equiv -(s_p - s_1)\, h_{n-p} \mod p\mathbb{Z}_p$. Consequently,

$$h_{ap} \equiv (s_1 - s_p)^a \mod p\mathbb{Z}_p, \quad a \ge 0;$$

thus, for each given N, there exists some $n > N$ such that h_n is not divisible by p. On the other hand, if $s_1 \equiv s_p \mod p\mathbb{Z}_p$, then it follows from Theorems 7, 8, and 9 with $l = 1$ that larger and larger powers of p divide h_n as n grows; see Corollary 11. This says that there is a sharp dividing line concerning the p-divisibility of h_n depending on whether $s_1 \equiv s_p \mod p\mathbb{Z}_p$ or not.

Proof of Theorem 2. We write $n = ap^l + r$ with $0 \le r < p^l$. Assuming (2.1)–(2.3), we have to show the bound (2.4).

We rewrite the series $S(z)$ as

$$S(z) = \widetilde{S}(z) + (s_{p^l} - s_{p^{l-1}})\frac{z^{p^l}}{p^l} + \sum_{i=p^l+1}^{\infty} \lambda_i \frac{z^i}{i}, \tag{2.7}$$

with the coefficients $\lambda_i \in \mathbb{Z}_p$ as in the statement of the theorem. It should be observed that this makes $\widetilde{S}(z)$ satisfy (1.6).

Let us write $\widetilde{H}(z) = \sum_{n\ge0} \widetilde{H}_n z^n = \exp\big(\widetilde{S}(z)\big)$. By taking the exponential of both sides of (2.7), we obtain

$$H(z) = \widetilde{H}(z)\exp\left((s_{p^l}-s_{p^{l-1}})\frac{z^{p^l}}{p^l} + \sum_{i=p^l+1}^{\infty}\lambda_i\frac{z^i}{i}\right). \tag{2.8}$$

We compare coefficients of z^{ap^l+r} on both sides of (2.8). This leads to

$$\frac{h_{ap^l+r}}{(ap^l+r)!} = \sum_{i_0+p^lj_0+\sum_{i=p^l+1}^{\infty} ij_i=ap^l+r} \widetilde{H}_{i_0}\frac{(s_{p^l}-s_{p^{l-1}})^{j_0}}{p^{j_0l}\,j_0!}\prod_{i=p^l+1}^{\infty}\frac{\lambda_i^{j_i}}{i^{j_i}\,j_i!}. \tag{2.9}$$

We now bound the p-adic valuation of the summand from below. By Lemma 1 applied to $\widetilde{S}(z)$, we know that $\widetilde{H}_{i_0}\in\mathbb{Z}_p$. By (2.2), we have

$$v_p\left(\frac{(s_{p^l}-s_{p^{l-1}})^{j_0}}{p^{j_0l}\,j_0!}\right) \ge j_0(m-l) - \sum_{s\ge1}\left\lfloor\frac{j_0}{p^s}\right\rfloor.$$

By (2.3), for $i>p^l$ we have

$$v_p\left(\frac{\lambda_i^{j_i}}{i^{j_i}\,j_i!}\right) \ge -j_i\left((l-m)\left\lfloor\frac{i}{p^l}\right\rfloor + \frac{p^{\lfloor\log_p i\rfloor-l}-1}{p-1}-1\right) - \sum_{s\ge1}\left\lfloor\frac{j_i}{p^s}\right\rfloor.$$

Together, these estimations imply that the p-adic valuation of the summand of the sum on the right-hand side of (2.9) is at least

$$\begin{aligned}
-(l-m)&\left(j_0+\sum_{i=p^l+1}^{\infty} j_i\left\lfloor\frac{i}{p^l}\right\rfloor\right) + \sum_{i=p^l+1}^{\infty} j_i - \sum_{i=p^l+1}^{\infty}\frac{p^{\lfloor\log_p i\rfloor-l}-1}{p-1}j_i\\
&\qquad\qquad -\sum_{s\ge1}\left(\left\lfloor\frac{j_0}{p^s}\right\rfloor+\sum_{i=p^l+1}^{\infty}\left\lfloor\frac{j_i}{p^s}\right\rfloor\right)\\
&\ge -(l-m)\left\lfloor j_0+\sum_{i=p^l+1}^{\infty} j_i\frac{i}{p^l}\right\rfloor - \sum_{i=p^l+1}^{\infty}\frac{p^{\lfloor\log_p i\rfloor-l}-1}{p-1}j_i\\
&\qquad -\sum_{s\ge1}\left(\left\lfloor\frac{j_0}{p^s}\right\rfloor+\sum_{i=p^l+1}^{\infty}\left\lfloor\frac{ij_i}{p^{s+l}}\right\rfloor\right) + \sum_{s\ge1}\sum_{i=p^l+1}^{\infty}\left(\left\lfloor\frac{ij_i}{p^{s+l}}\right\rfloor-\left\lfloor\frac{j_i}{p^s}\right\rfloor\right)\\
&\ge -(l-m)\left\lfloor\frac{1}{p^l}\left(p^lj_0+\sum_{i=p^l+1}^{\infty} ij_i\right)\right\rfloor - \sum_{s\ge1}\left\lfloor\frac{p^lj_0+\sum_{i=p^l+1}^{\infty} ij_i}{p^{s+l}}\right\rfloor\\
&\ge -(l-m)a - \sum_{s\ge1}\left\lfloor\frac{ap^l+r}{p^{s+l}}\right\rfloor,
\end{aligned} \tag{2.10}$$

where we have used Lemma 3 to obtain the next-to-last line, and the dependence of the summation indices of the sum in (2.9) to obtain the last line. Together with Legendre's formula [14, p. 10] applied to the p-adic valuation of $(ap^l + r)!$ on the left-hand side of (2.9), this proves the bound in (2.4), with $n = ap^l + r$.

In order to establish the more precise congruence (2.6), we first observe that equality in (2.10) only holds if $j_i = 0$ for all $i > p^l$ since we discarded the sum of these j_i's when going from the first to the second expression. Hence, it suffices to look more carefully at the summand with $i_0 = r$, $j_0 = a$, and $j_i = 0$ for $i > p^l$, that is, at

$$\widetilde{H}_r \frac{(s_{p^l} - s_{p^{l-1}})^a}{p^{al}\, a!}.$$

More precisely, by the above considerations, we conclude that

$$\begin{aligned} Q_{ap^l+r} &= \frac{h_{ap^l+r}}{p^{e_p(ap^l+r;m,l)}} \\ &\equiv \frac{(ap^l+r)!\, \widetilde{H}_r}{p^{e_p(ap^l+r;m,l)}} \frac{(s_{p^l} - s_{p^{l-1}})^a}{p^{al}\, a!} \mod p\mathbb{Z}_p \\ &\equiv \frac{(ap^l+r)!\, \widetilde{H}_r}{p^{e_p(r;m,l)+ap^{l-1}+\cdots+ap+a}} \frac{\big(p^{-m}(s_{p^l} - s_{p^{l-1}})\big)^a}{a!} \mod p\mathbb{Z}_p \\ &\equiv \frac{(p-1)!^{a(p^{l-1}+\cdots+p+1)}\, r!\, \widetilde{H}_r}{p^{e_p(r;m,l)}} \big(p^{-m}(s_{p^l} - s_{p^{l-1}})\big)^a \mod p\mathbb{Z}_p \\ &\equiv Q_r(-1)^{al}\big(p^{-m}(s_{p^l} - s_{p^{l-1}})\big)^a \mod p\mathbb{Z}_p, \end{aligned}$$

where we have used Wilson's theorem plus the fact that $\widetilde{H}_r = \frac{h_r}{r!}$ in the last line. This is exactly the congruence (2.6).

The above computation with $r = 0$ implies that

$$Q_{ap^l} \equiv \big((-1)^l p^{-m}(s_{p^l} - s_{p^{l-1}})\big)^a \mod p\mathbb{Z}_p$$

for all positive integers a. Thus, if $s_{p^{l-1}} \not\equiv s_{p^l} \mod p^{m+1}\mathbb{Z}_p$, the bound (2.4) is sharp for all n divisible by p^l. This completes the proof of the theorem. $\square$

Lemma 3. *For all non-negative integers i, j, l, and p, with $i \geq p^l$ and $p \geq 2$, we have*

$$\sum_{s \geq 1} \left(\left\lfloor \frac{ij}{p^{s+l}} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right) \geq \frac{p^{\lfloor \log_p i \rfloor - l} - 1}{p-1} j.$$

Proof. We have

$$\begin{aligned} \sum_{s \geq 1} \left(\left\lfloor \frac{ij}{p^{s+l}} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right) &\geq \sum_{s \geq 1} \left(\left\lfloor \frac{p^{\lfloor \log_p i \rfloor} j}{p^{s+l}} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right) \\ &\geq \sum_{s=1}^{\lfloor \log_p i \rfloor - l} p^{\lfloor \log_p i \rfloor - s - l} j = \frac{p^{\lfloor \log_p i \rfloor - l} - 1}{p-1} j, \end{aligned}$$

as desired. $\square$

In the case where $m = 0$, one can formulate a simplified version of Theorem 2 if one assumes in addition that the coefficients s_n are elements of $\mathbb{Z}_p$, since then (2.3) is automatically satisfied.

Corollary 4. *For a prime number p, let $S(z) = \sum_{n\ge1} \frac{s_n}{n} z^n$ be a formal power series with $s_n \in \mathbb{Z}_p$ for all n, and let $H(z) = \sum_{n\ge0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. Given a positive integer l, we assume that*

$$S(z^p) - pS(z) = pJ(z) + O\left(z^{p^l}\right) \tag{2.11}$$

with $J(z) \in \mathbb{Z}_p[z]$. Then

$$v_p(h_n) \ge \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-1) \left\lfloor \frac{n}{p^l} \right\rfloor \tag{2.12}$$

for all n.

Moreover, writing $e_p(n;l) = \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-1) \left\lfloor \frac{n}{p^l} \right\rfloor$, under these conditions, the quotient

$$Q_n = \frac{h_n}{p^{e_p(n;l)}}$$

satisfies

$$Q_n \equiv (-1)^l (s_{p^l} - s_{p^{l-1}}) Q_{n-p^l} \mod p\mathbb{Z}_p. \tag{2.13}$$

In particular, if $s_{p^{l-1}} \not\equiv s_{p^l} \mod p\mathbb{Z}_p$, then the bound in (2.12) *is tight for all n which are divisible by p^l.*

We state another special case of Theorem 2 separately, which is convenient in many applications. More precisely, it addresses the case where the coefficients s_n may be only non-zero for n a power of p. This is the case, for instance, if the coefficient s_n is the number of subgroups of index n in a given p-group, $n \ge 0$; see Sections 5 and 6.

Corollary 5. *For a prime number p, let $S(z) = \sum_{n\ge1} \frac{s_n}{n} z^n$ be a formal power series with $s_{p^e} \in \mathbb{Z}_p$ for all non-negative integers e and $s_n = 0$ otherwise, and let $H(z) = \sum_{n\ge0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. Given non-negative integers l and m with $m < l$, we assume that*

$$S(z^p) - pS(z) = pJ(z) + (s_{p^{l-1}} - s_{p^l}) \frac{z^{p^l}}{p^{l-1}} + O\left(z^{p^l+1}\right) \tag{2.14}$$

with $J(z) \in \mathbb{Z}_p[z]$,

$$s_{p^{l-1}} \equiv s_{p^l} \mod p^m\mathbb{Z}_p, \tag{2.15}$$

and

$$v_p(s_{p^e} - s_{p^{l-1}}) \ge -(l-m)p^{e-l} - \frac{p^{e-l}-1}{p-1} + e + 1 \tag{2.16}$$

for all e with $l < e < l + \log_p(2l+1)$. Then

$$v_p(h_n) \ge \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-m-1) \left\lfloor \frac{n}{p^l} \right\rfloor \tag{2.17}$$

for all n.

Moreover, writing $e_p(n;l,m) = \sum_{s=1}^{l-1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-m-1) \left\lfloor \frac{n}{p^l} \right\rfloor$, under these conditions the quotient

$$Q_n = \frac{h_n}{p^{e_p(n;l,m)}}$$

satisfies

$$Q_n \equiv (-1)^l p^{-m}(s_{p^l} - s_{p^{l-1}})Q_{n-p^l} \mod p\mathbb{Z}_p. \tag{2.18}$$

In particular, if $s_{p^{l-1}} \not\equiv s_{p^l} \mod p^{m+1}\mathbb{Z}_p$, *then the bound in* (2.17) *is tight for all* n *which are divisible by* p^l.

If $p = 2$, there is a case which does not fall under the conditions of Theorem 2 (more precisely, Condition (2.3) is violated by a small margin), in which one may nevertheless even *improve* the bound in (2.4). The corresponding theorem, given below, vastly generalises Theorem 1.4 in [10]. We shall apply it in the proof of Theorem 26.

Theorem 6. *Let* $S(z) = \sum_{n\ge1} \frac{s_n}{n} z^n$ *be a formal power series with* $s_n \in \mathbb{Q}_2$ *for all* n, *and let* $H(z) = \sum_{n\ge0} \frac{h_n}{n!} z^n$ *be the exponential of* $S(z)$. *Given an integer* $l \ge 2$, *we assume that*

$$S(z^2) - 2S(z) = 2J(z) + (s_{2^{l-1}} - s_{2^l})\frac{z^{2^l}}{2^{l-1}} + O\left(z^{2^l+1}\right) \tag{2.19}$$

with $J(z) \in \mathbb{Z}_2[z]$, *that*

$$s_{2^{l-1}} \equiv s_{2^l} \mod 2^{l-1}\mathbb{Z}_2, \quad s_{2^l} \equiv s_{2^{l+1}} \mod 2^{l-2}\mathbb{Z}_2, \tag{2.20}$$

$$s_{2^l} - s_{2^{l-1}} \equiv 2(s_{2^{l+1}} - s_{2^l}) \mod 2^l\mathbb{Z}_2, \tag{2.21}$$

and that

$$v_2(\lambda_i) \ge -\left\lfloor \frac{i}{2^l} \right\rfloor + v_2(i) - 2^{\lfloor \log_2 i \rfloor - l} + \left\lceil \frac{i}{2^{l+2}} \right\rceil + 1 + \chi(i > 2^{l+1}) \tag{2.22}$$

for all $i > 2^l$ *different from* 2^{l+1}, *where* $\lambda_i = s_i$ *if* $i/2^{v_2(i)} \ge 2^l$ *and* $\lambda_i = s_i - s_{i/2^e}$ *otherwise, and with* e *minimal such that* $i/2^e < 2^l$. *Here,* $\chi(\mathcal{A}) = 1$ *if* $\mathcal{A}$ *is true, and* $\chi(\mathcal{A}) = 0$ *otherwise. Then*

$$v_2(h_n) \ge \sum_{s=1}^{l-1} \left\lfloor \frac{n}{2^s} \right\rfloor + \left\lfloor \frac{n}{2^{l+1}} \right\rfloor - \left\lfloor \frac{n}{2^{l+2}} \right\rfloor \tag{2.23}$$

for all n.

Moreover, writing $e_2(n;l) = \sum_{s=1}^{l-1} \left\lfloor \frac{n}{2^s} \right\rfloor + \left\lfloor \frac{n}{2^{l+1}} \right\rfloor - \left\lfloor \frac{n}{2^{l+2}} \right\rfloor$, *under these conditions the quotient*

$$Q_n = \frac{h_n}{2^{e_2(n;l)}}$$

satisfies

$$Q_n \equiv 2^{-l+2}(s_{2^{l+1}} - s_{2^l})Q_{n-2^{l+2}} \mod 2\mathbb{Z}_2. \tag{2.24}$$

If $s_{2^l} \not\equiv s_{2^{l+1}} \mod 2^{l-1}\mathbb{Z}_2$, *then the bound in* (2.23) *is tight for all* n *which are congruent to* 0 *or* 2^l *modulo* 2^{l+2}; *if* $s_{2^{l-1}} \equiv s_{2^{l+1}} + 2^{l-2} \mod 2^l\mathbb{Z}_2$, *then also for all* n *congruent to* 2^{l+1} *modulo* 2^{l+2} *but not for those congruent to* $3 \cdot 2^l$, *while it is the other way round if* $s_{2^{l-1}} \equiv s_{2^{l+1}} + 3 \cdot 2^{l-2} \mod 2^l\mathbb{Z}_2$.

Remark. The reader should observe that, indeed, the conditions of this theorem do not fit into the framework of Theorem 2 with $p = 2$. Namely, the first congruence in (2.20) tells us that we should choose in addition $m = l - 1$ in Theorem 2. But then, for $i = 2^{l+1}$, Condition (2.3) demands $v_2(\lambda_{2^{l+1}}) \ge -2 + l + 1 = l - 1$, while, in that case, we have

$$v_2(\lambda_{2^{l+1}}) = v_2(s_{2^{l+1}} - s_{2^{l-1}}) = v_2\big((s_{2^{l+1}} - s_{2^l}) + (s_{2^l} - s_{2^{l-1}})\big),$$

so that the two congruences in (2.20) only imply $v_2(\lambda_{2^{l+1}})$ to be at least $l-2$, which is less by 1.

Proof of Theorem 6. We proceed in the same manner as in the proof of Theorem 2. Here, we have to bound the 2-adic valuation of

$$\frac{h_{a2^l+r}}{(a2^l+r)!}=\sum_{i_0+2^lj_0+2^{l+1}j_1+\sum_{i=2^l+1}^{2^{l+1}-1}ij_i+\sum_{i=2^{l+1}+1}^{\infty}ij_i=a2^l+r}\widetilde{H}_{i_0}\cdot\frac{(s_{2^l}-s_{2^{l-1}})^{j_0}}{2^{j_0l}\,j_0!}\frac{(s_{2^{l+1}}-s_{2^{l-1}})^{j_1}}{2^{j_1(l+1)}\,j_1!}\prod_{\substack{i=2^l+1\\ i\ne 2^{l+1}}}^{\infty}\frac{\lambda_i^{j_i}}{i^{j_i}\,j_i!}$$

from below. The reader should note that the index formerly called $j_{p^{l+1}}$ has became j_1 here. Refining the previous approach, we rearrange the summation indices according to the sum j_0+2j_1:

$$\frac{h_{a2^l+r}}{(a2^l+r)!}=\sum_{b=0}^{a}\sum_{j_0+2j_1=b}\frac{(s_{2^l}-s_{2^{l-1}})^{j_0}}{2^{j_0l}\,j_0!}\frac{(s_{2^{l+1}}-s_{2^{l-1}})^{j_1}}{2^{j_1(l+1)}\,j_1!}\cdot\sum_{i_0+\sum_{i=2^l+1}^{2^{l+1}-1}ij_i+\sum_{i=2^{l+1}+1}^{\infty}ij_i=(a-b)2^l+r}\widetilde{H}_{i_0}\prod_{\substack{i=2^l+1\\ i\ne 2^{l+1}}}^{\infty}\frac{\lambda_i^{j_i}}{i^{j_i}\,j_i!}. \tag{2.25}$$

The subsum over j_0 and j_1, S_b say, equals

$$\begin{aligned}S_b&=\sum_{j_0+2j_1=b}\frac{(s_{2^l}-s_{2^{l-1}})^{j_0}}{2^{j_0l}\,j_0!}\frac{(s_{2^{l+1}}-s_{2^{l-1}})^{j_1}}{2^{j_1(l+1)}\,j_1!}\\&=\sum_{j_0+2j_1=b}\frac{\big(2^{-l+1}(s_{2^l}-s_{2^{l-1}})\big)^{j_0}}{2^{j_0}\,j_0!}\frac{\big(2^{-l+2}(s_{2^{l+1}}-s_{2^{l-1}})\big)^{j_1}}{2^{3j_1}\,j_1!}\\&=2^{-b}\sum_{j_0+2j_1=b}\frac{\big(2^{-l+1}(s_{2^l}-s_{2^{l-1}})\big)^{j_0}}{j_0!}\frac{\big(2^{-l+2}(s_{2^{l+1}}-s_{2^{l-1}})\big)^{j_1}}{2^{j_1}\,j_1!}.\end{aligned}\tag{2.26}$$

Writing $\mu_0=2^{-l+1}(s_{2^l}-s_{2^{l-1}})$ and $\mu_2=2^{-l+2}(s_{2^{l+1}}-s_{2^{l-1}})$, we observe that the sum in the last line equals the coefficient of z^b in the series $f(z)=\exp\Big(\mu_0z+\mu_2\frac{z^2}{2}\Big)$. Thus, due to (2.20) and (2.21), we may apply Corollary 5 with $p=2$, $l=2$, and $m=0$ to $f(z)$. Consequently, the 2-adic valuation of S_b in (2.26) may be bounded from below by

$$v_2(S_b)\ge -b+\left(\left\lfloor\frac{b}{2}\right\rfloor-\left\lfloor\frac{b}{4}\right\rfloor\right)-v_2(b!)=-b-2\left\lfloor\frac{b}{4}\right\rfloor-\sum_{s\ge 3}\left\lfloor\frac{b}{2^s}\right\rfloor, \tag{2.27}$$

and the quotient $\widehat{Q}_b=b!\,S_b/2^{-b+\lfloor b/2\rfloor-\lfloor b/4\rfloor}$ satisfies

$$\widehat{Q}_b\equiv 2^{-l+2}(s_{2^{l+1}}-s_{2^{l-1}})\widehat{Q}_{b-4}\mod 2\mathbb{Z}_2. \tag{2.28}$$

Next we turn our attention to the second subsum, say $S_{a,b}$,

$$S_{a,b} = \sum_{i_0+\sum_{i=2^l+1}^{2^{l+1}-1} ij_i+\sum_{i=2^{l+1}+1}^{\infty} ij_i=(a-b)2^l+r} \widetilde{H}_{i_0} \prod_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}.$$

By using (2.22), we see that the summand in this sum may be bounded from below in the following manner:

$$\begin{aligned}
-\sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} j_i \left\lfloor \frac{i}{2^l} \right\rfloor &+ \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} \left(-2^{\lfloor \log_2 i\rfloor - l} + \left\lceil \frac{i}{2^{l+2}} \right\rceil + 1 \right) j_i - \sum_{s\ge 1} \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} \left\lfloor \frac{j_i}{2^s} \right\rfloor + \sum_{i=2^{l+1}+1}^{\infty} j_i\\
&\ge - \left\lfloor \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} j_i \frac{i}{2^l} \right\rfloor + \sum_{i=2^l+1}^{2^{l+1}-1} j_i - \sum_{i=2^{l+1}+1}^{\infty} \left(2^{\lfloor \log_2 i\rfloor - l} - \left\lceil \frac{i}{2^{l+2}} \right\rceil - 1 \right) j_i\\
&\qquad - \sum_{s\ge 1} \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} \left\lfloor \frac{ij_i}{2^{s+l}} \right\rfloor + \sum_{s\ge 1} \sum_{i=2^{l+1}+1}^{\infty} \left(\left\lfloor \frac{ij_i}{2^{s+l}} \right\rfloor - \left\lfloor \frac{j_i}{2^s} \right\rfloor \right)\\
&\ge - \left\lfloor \frac{1}{2^l} \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} ij_i \right\rfloor + \sum_{i=2^l+1}^{2^{l+1}-1} \frac{ij_i}{2^{l+2}} + \sum_{i=2^{l+1}+1}^{\infty} \left\lceil \frac{i}{2^{l+2}} \right\rceil j_i - \sum_{s\ge 1} \left\lfloor \sum_{\substack{i=2^l+1\\ i\neq 2^{l+1}}}^{\infty} \frac{ij_i}{2^{s+l}} \right\rfloor\\
&> -(a-b) + \left\lceil \frac{a-b}{4} \right\rceil - \sum_{s\ge 1} \left\lfloor \frac{a-b}{2^s} \right\rfloor - 1, \qquad (2.29)
\end{aligned}$$

where we have used Lemma 3 with $p = 2$ to obtain the next-to-last line, and the dependence of the summation indices of the sum in (2.25) to obtain the last line. Moreover, since, in passing from the first to the second line in (2.29), we left out the last term of the first line, the right-hand side of (2.29) can be increased by 1 as soon as one of the j_i's with $i \ge 2^{l+1} + 1$ is non-zero. Furthermore, when passing from the first estimate to the second, we used the inequality $j_i \ge \frac{ij_i}{2^{l+2}}$ for all i with $2^l+1 \le i \le 2^{l+1}-1$. In particular, for these i we have $j_i - \frac{ij_i}{2^{l+2}} \ge \frac{j_i}{2}$. Hence, the right-hand side of (2.29) can be increased by 1 as soon as the sum $\sum_{i=2^l+1}^{2^{l+1}-1} j_i$ should be at least 2.

We now use the estimates (2.27) for S_b and (2.29) for $S_{a,b}$ in (2.25), to obtain

$$\begin{aligned}
v_2(h_{a2^l+r}) &\ge \sum_{s\ge 1} \left\lfloor \frac{a2^l+r}{2^s} \right\rfloor - b - 2\left\lfloor \frac{b}{4} \right\rfloor\\
&\qquad - \sum_{s\ge 3} \left\lfloor \frac{b}{2^s} \right\rfloor - (a-b) - \sum_{s\ge 1} \left\lfloor \frac{a-b}{2^s} \right\rfloor + \left\lceil \frac{a-b}{4} \right\rceil\\
&\ge \sum_{s=1}^{l-1} \left\lfloor \frac{a2^l+r}{2^s} \right\rfloor + \sum_{s\ge l} \left\lfloor \frac{a2^l+r}{2^s} \right\rfloor - a - 2\left\lfloor \frac{b}{4} \right\rfloor
\end{aligned}$$

$$
\begin{aligned}
&\qquad -\sum_{s\ge3}\left\lfloor\frac{a}{2^s}\right\rfloor-\left\lfloor\frac{a-b}{2}\right\rfloor-\left\lfloor\frac{a-b}{4}\right\rfloor+\left\lceil\frac{a-b}{4}\right\rceil\\
&\ge\sum_{s=1}^{l-1}\left\lfloor\frac{a2^l+r}{2^s}\right\rfloor+\sum_{s\ge l+1}\left\lfloor\frac{a2^l}{2^s}\right\rfloor-2\left\lfloor\frac{b}{4}\right\rfloor-\sum_{s\ge3}\left\lfloor\frac{a}{2^s}\right\rfloor-2\left\lfloor\frac{a-b}{4}\right\rfloor\\
&\ge\sum_{s=1}^{l-1}\left\lfloor\frac{a2^l+r}{2^s}\right\rfloor+\sum_{s\ge1}\left\lfloor\frac{a}{2^s}\right\rfloor-2\left\lfloor\frac{a}{4}\right\rfloor-\sum_{s\ge3}\left\lfloor\frac{a}{2^s}\right\rfloor\\
&\ge\sum_{s=1}^{l-1}\left\lfloor\frac{a2^l+r}{2^s}\right\rfloor+\left\lfloor\frac{a}{2}\right\rfloor-\left\lfloor\frac{a}{4}\right\rfloor.
\end{aligned}\tag{2.30}
$$

This is exactly the bound in (2.23) with $n=a2^l+r$, where $0\le r<2^l$.

It should be noted that the remarks after (2.29) also show that the bound (2.23) for a summand in (2.25) can only be tight if $j_i=0$ for $i\ge 2^{l+1}+1$, if at most one of the j_i's with $2^l+1\le i\le 2^{l+1}-1$ is non-zero, and if such a non-zero j_i does not exceed 1. On the other hand, when passing from the second to the third estimate in (2.30), equality occurs only if $a-b\not\equiv 1 \pmod 4$. Let us suppose that we are in the "adverse" case where $j_{i_0}=1$ for some i_0 between 2^l+1 and $2^{l+1}-1$ and that all other j_i's are zero. Then the first line in chain of inequalities (2.29) says that the p-adic valuation of a summand in the sum $S_{a,b}$ is at least 0, while the last line says that the p-adic valuation of such a summand is at least

$$
-(a-b)+\left\lceil\frac{a-b}{4}\right\rceil-\sum_{s\ge1}\left\lfloor\frac{a-b}{2^s}\right\rfloor.
$$

As soon as $a-b\ge2$, the last expression is ≤ -1, and thus the estimation (2.29) would not be tight. On the other hand, we just saw that $a-b=1$ implies that the estimation (2.30) would not be tight. The only remaining case is $a-b=0$, but this contradicts $j_{i_0}=1$ and the dependence of the summation indices in the sum $S_{a,b}$. Consequently, for the bound (2.23) to be tight for the corresponding summand (multiplied by $(a2^l+r)!$), all j_i's with $i\ge 2^l+1$ must vanish, or, equivalently, $a-b=0$. In other words, remembering (2.27), we have

$$
\frac{h_{a2^l+r}}{(a2^l+r)!}\equiv \widetilde{H}_rS_a \mod 2^{-a-2\lfloor a/4\rfloor-\sum_{s\ge3}\lfloor a/2^s\rfloor+1}\mathbb{Z}_2,
$$

or, recalling that $\widetilde{H}_r=\frac{h_r}{r!}$,

$$
\begin{aligned}
Q_{a2^l+r}&=h_{a2^l+r}2^{-\sum_{s=1}^{l-1}\left\lfloor(a2^l+r)/2^s\right\rfloor-\lfloor a/2\rfloor+\lfloor a/4\rfloor}\\
&\equiv(a2^l+r)!\,\widetilde{H}_rS_a2^{-a\sum_{s=1}^{l-1}2^{l-s}-\sum_{s=1}^{l-1}\lfloor r/2^s\rfloor-\lfloor a/2\rfloor+\lfloor a/4\rfloor}\mod 2\mathbb{Z}_2\\
&\equiv h_r\,2^{-\sum_{s=1}^{l-1}\lfloor r/2^s\rfloor}\,a!\,S_a\,2^{a-\lfloor a/2\rfloor+\lfloor a/4\rfloor}\mod 2\mathbb{Z}_2\\
&\equiv Q_r\widehat{Q}_a\mod 2\mathbb{Z}_2.
\end{aligned}\tag{2.31}
$$

Using (2.28), this chain of congruences can be continued,

$$\begin{aligned}
Q_{a2^l+r} &\equiv 2^{-l+2}(s_{2^{l+1}} - s_{2^{l-1}})Q_r\widehat{Q}_{a-4} \mod 2\mathbb{Z}_2\\
&\equiv 2^{-l+2}(s_{2^{l+1}} - s_{2^{l-1}})Q_{2^l(a-4)+r} \mod 2\mathbb{Z}_2\\
&\equiv 2^{-l+2}(s_{2^{l+1}} - s_{2^l})Q_{2^la+r-2^{l+2}} \mod 2\mathbb{Z}_2,
\end{aligned}$$

where we have used (2.31) with a replaced by $a-4$ in the second line and (2.20) in the last line. This congruence is equivalent to (2.24) with $n = a2^l + r$.

In order to establish the final assertion, we assume $s_{2^l} \not\equiv s_{2^{l+1}} \mod 2^{l-1}\mathbb{Z}_2$. From (2.21), it then follows that also $s_{2^{l-1}} \not\equiv s_{2^l} \mod 2^l\mathbb{Z}_2$. The initial condition $Q_0 = 1$, and the congruence

$$\begin{aligned}
Q_{2^l} &\equiv Q_0\widehat{Q}_1 \mod 2\mathbb{Z}_2\\
&\equiv 2^{-l+1}(s_{2^l} - s_{2^{l-1}}) \mod 2\mathbb{Z}_2\\
&\equiv 1 \mod 2\mathbb{Z}_2,
\end{aligned}$$

together with (2.24) then imply the assertion for n congruent to 0 or 2^l modulo 2^{l+2}. To see the remaining assertions, let us write $s_{2^{l+1}} = s_{2^{l-1}} + 2^{l-2} + \alpha 2^{l-1}$. Then we have the congruences

$$\begin{aligned}
Q_{2^{l+1}} &\equiv Q_0\widehat{Q}_2 \mod 2\mathbb{Z}_2\\
&\equiv \frac{1}{2}\big(2^{-l+1}(s_{2^l} - s_{2^{l-1}})\big)^2 + \frac{1}{2}2^{-l+2}(s_{2^{l+1}} - s_{2^{l-1}}) \mod 2\mathbb{Z}_2\\
&\equiv \frac{1}{2} + \frac{1}{2} + \alpha \mod 2\mathbb{Z}_2\\
&\equiv 1 + \alpha \mod 2\mathbb{Z}_2,
\end{aligned}$$

and

$$\begin{aligned}
Q_{3\cdot 2^l} &\equiv Q_0\widehat{Q}_3 \mod 2\mathbb{Z}_2\\
&\equiv \frac{3!}{2}\Bigg(\frac{1}{3!}\big(2^{-l+1}(s_{2^l} - s_{2^{l-1}})\big)^3\\
&\qquad + \frac{1}{2}2^{-l+1}(s_{2^l} - s_{2^{l-1}})2^{-l+2}(s_{2^{l+1}} - s_{2^{l-1}})\Bigg) \mod 2\mathbb{Z}_2\\
&\equiv 2^{-l+1}(s_{2^l} - s_{2^{l-1}})\left(\frac{1}{2}\big(2^{-l+1}(s_{2^l} - s_{2^{l-1}})\big)^2 + \frac{3}{2}2^{-l+2}(s_{2^{l+1}} - s_{2^{l-1}})\right) \mod 2\mathbb{Z}_2\\
&\equiv \left(\frac{1}{2} + \frac{3}{2} + 3\alpha\right) \mod 2\mathbb{Z}_2\\
&\equiv \alpha \mod 2\mathbb{Z}_2,
\end{aligned}$$

which, together with (2.24), complete the proof of the theorem. □

3. p-Divisibility of coefficients in exponentials of power series, II

In this section we present our second set of main results. They address the case where we have less precise information on the coefficients s_n of the series $S(z)$ in (1.5). More specifically, what can we say if Condition (2.1) is "truncated" to hold only up to the coefficient of z^{p^l}, but beyond this threshold we do not assume any additional information, except that all s_n's should lie in $\mathbb{Z}_p$? While we cannot expect a result as strong as the bound (2.12) in Corollary 4 with l replaced by $l+1$, the next theorem tells us that the p-divisibility of the coefficients of the exponential $H(z)$ in (1.5) is still higher than one might expect.

Theorem 7. *For a prime number $p \ge 3$, let $S(z) = \sum_{n\ge1} \frac{s_n}{n} z^n$ be a formal power series with $s_n \in \mathbb{Z}_p$ for all n, and let $H(z) = \sum_{n\ge0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. Given a positive integer l such that $(p,l) \ne (3,1)$, we assume that*

$$S(z^p) - pS(z) = pJ(z) + O\left(z^{p^l+1}\right) \tag{3.1}$$

with $J(z) \in \mathbb{Z}_p[z]$. Then

$$v_p(h_n) \ge \sum_{s\ge1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-1) \left\lfloor \frac{n}{p^l} \right\rfloor - \sum_{s\ge l} \left\lfloor \frac{n}{2p^s} \right\rfloor \tag{3.2}$$

for all n.

Remarks. (1) We should compare the bound in (3.2) to the one in (2.12), in two different ways.

First, let us consider Corollary 4, and compare it to Theorem 7. The difference in conditions is that, while, under the assumptions of Corollary 4, Condition (1.6) is (potentially) violated starting from the coefficient of z^{p^l} on, under the assumptions of Theorem 7 it is (potentially) violated starting from the coefficient of z^{p^l+1} "only." The "gain" in p-divisibility is given by the difference between (3.2) and (2.12), that is, by

$$\sum_{s\ge l} \left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{n}{2p^s} \right\rfloor \right).$$

On the other hand, let us consider Corollary 4 with l replaced by $l+1$, and compare this to Theorem 7. Now the difference in conditions is that, under the assumptions of Corollary 4, Condition (1.6) is (potentially) violated starting from the coefficient of $z^{p^{l+1}}$ on, while, under the assumptions of Theorem 7, it is still (potentially) violated already starting from the coefficient of z^{p^l+1} on. The "loss" in p-divisibility is then given by the difference between (2.12) with l replaced by $l+1$ and (3.2), that is, by

$$(l-1) \left\lfloor \frac{n}{p^l} \right\rfloor + \left\lfloor \frac{n}{2p^l} \right\rfloor - (l+1) \left\lfloor \frac{n}{p^{l+1}} \right\rfloor + \left\lfloor \frac{n}{2p^{l+1}} \right\rfloor + \sum_{s\ge l+2} \left(\left\lfloor \frac{n}{2p^s} \right\rfloor - \left\lfloor \frac{n}{p^s} \right\rfloor \right).$$

(2) The bound in (3.2) could be further improved, albeit very likely at the cost of having to introduce very complicated arithmetic functions. This is the reason why we have refrained from trying to formulate an improved version of Theorem 7. That the bound (3.2) cannot be tight for infinitely many n, can be seen from the proof: when going from the next-to-last to the last estimate in (3.4), the inequality

$$-\sum_{i=p^l+1}^{\infty} j_i(l-1) \ge -a(l-1)$$

is used. This inequality will be "very far from equality" if $n = ap^l + r$ is large.

Proof of Theorem 7. Following again the proof of Theorem 2, we let $n = ap^l + r$ with $0 \le r < p^l$. Here, instead of (2.9), we obtain

$$\frac{h_{ap^l+r}}{(ap^l+r)!} = \sum_{i_0+\sum_{i=p^l+1}^{\infty} ij_i = ap^l+r} \widetilde{H}_{i_0} \prod_{i=p^l+1}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}, \tag{3.3}$$

with $\widetilde{H}_{i_0} \in \mathbb{Z}_p$ for all i_0, and the λ_i's being defined as in the statement of Theorem 2. Since here we are assuming that all s_i's are in $\mathbb{Z}_p$ (instead of $\mathbb{Q}_p$, as in Theorem 2), we have $\lambda_i \in \mathbb{Z}_p$ for all i. For the p-adic valuation of the summand in the above sum, we then obtain

$$\begin{aligned}
v_p\left(\widetilde{H}_{i_0} \prod_{i=p^l+1}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}\right) &\ge -\sum_{i=p^l+1}^{\infty} j_i \cdot v_p(i) - \sum_{i=p^l+1}^{\infty} \sum_{s\ge 1} \left\lfloor \frac{j_i}{p^s} \right\rfloor \\
&\ge -\sum_{i=p^l+1}^{2p^l-1} j_i(l-1) - \sum_{i=2p^l}^{\infty} j_i \cdot v_p(i) - \sum_{i=p^l+1}^{2p^l-1} \sum_{s\ge 1} \left\lfloor \frac{j_i}{p^s} \right\rfloor - \sum_{i=2p^l}^{\infty} \sum_{s\ge 1} \left\lfloor \frac{j_i}{p^s} \right\rfloor \\
&\ge -\sum_{i=p^l+1}^{2p^l-1} j_i(l-1) - \sum_{i=2p^l}^{\infty} j_i \left(l-1+\frac{i}{2p^l}\right) - \chi(p=3)\frac{j_{p^{l+1}}}{2} \\
&\qquad\qquad - \sum_{i=p^l+1}^{2p^l-1} \frac{j_i}{p-1} - \sum_{s\ge 1} \sum_{i=2p^l}^{\infty} \left\lfloor \frac{ij_i}{2p^{s+l}} \right\rfloor \\
&> -\sum_{i=p^l+1}^{\infty} j_i(l-1) - \left\lfloor \sum_{i=p^l}^{\infty} j_i \frac{i}{2p^l} \right\rfloor - 1 \\
&\qquad + \sum_{i=p^l+1}^{2p^l-1} \left(\frac{ij_i}{2p^l} - \frac{j_i}{p-1}\right) - \sum_{s\ge 1} \left\lfloor \sum_{i=2p^l}^{\infty} \frac{ij_i}{2p^{s+l}} \right\rfloor - \chi(p=3)\frac{j_{p^{l+1}}}{2} \\
&> -a(l-1) + (l-1)j_{p^{l+1}} - \left\lfloor \frac{a}{2} \right\rfloor - \sum_{s\ge 1} \left\lfloor \frac{a}{2p^s} \right\rfloor - \chi(p=3)\frac{j_{p^{l+1}}}{2} - 1.
\end{aligned} \tag{3.4}$$

Here, we have again used Legendre's formula [14, p. 10] in the first step, the estimation

$$\sum_{s\ge 1} \left\lfloor \frac{j}{p^s} \right\rfloor \le \sum_{s\ge 1} \frac{j}{p^s} \le \frac{j}{p-1}$$

in the third step, and the dependence of the summation indices of the sum in (3.3) in the last step. The strict inequality in the fourth step results from the inequality $-\alpha > -\lfloor \alpha \rfloor - 1$. By assumption, we have $(p,l) \ne (3,1)$, and therefore

$$(l-1)j_{p^{l+1}} - \chi(p=3)\frac{j_{p^{l+1}}}{2} \ge 0.$$

Thus, out of (3.4) we obtain exactly the bound in (3.2) with $n = ap^l + r$, as desired. □

By the same approach, we also obtain a corresponding result for the exceptional case where $p = 3$ and $l = 1$.

Theorem 8. *Let $S(z)=\sum_{n\ge1}\frac{s_n}{n}z^n$ be a formal power series with $s_n\in\mathbb{Z}_3$ for all n, and let $H(z)=\sum_{n\ge0}\frac{h_n}{n!}z^n$ be the exponential of $S(z)$. We assume that*

$$S(z^3)-3S(z)=3J(z)+O\left(z^4\right) \tag{3.5}$$

with $J(z)\in\mathbb{Z}_3[z]$. Then

$$v_3(h_n)\ge\sum_{s\ge1}\left(\left\lfloor\frac{n}{3^s}\right\rfloor-\left\lfloor\frac{n}{2\cdot3^s}\right\rfloor\right)-\left\lfloor\frac{n}{18}\right\rfloor \tag{3.6}$$

for all n.

By refining the above approach, and using ideas from the proof of Theorem 6, we also obtain a corresponding result for $p=2$, a case which was excluded in both Theorems 7 and 8. Again, there is a technical auxiliary result which is needed for the proof. It is given separately in Lemma 10.

Theorem 9. *Let $S(z)=\sum_{n\ge1}\frac{s_n}{n}z^n$ be a formal power series with $s_n\in\mathbb{Z}_2$ for all n, and let $H(z)=\sum_{n\ge0}\frac{h_n}{n!}z^n$ be the exponential of $S(z)$. Given a positive integer l, we assume that*

$$S(z^2)-2S(z)=2J(z)+O\left(z^{2^l+1}\right) \tag{3.7}$$

with $J(z)\in\mathbb{Z}_2[z]$. Then

$$v_2(h_n)\ge\begin{cases}\left\lfloor\frac{n}{2}\right\rfloor-\left\lfloor\frac{n}{4}\right\rfloor, & \text{if } l=1,\\ \left\lfloor\frac{n}{2}\right\rfloor, & \text{if } l=2,\\ \sum_{s=1}^{l+1}\left\lfloor\frac{n}{2^s}\right\rfloor-(l-1)\left\lfloor\frac{n}{2^l}\right\rfloor, & \text{if } l\ge3,\end{cases} \tag{3.8}$$

for all n.

Remarks. (1) The bounds in (3.8) in the cases where $l=1$ or $l=2$ are worse than the bound in (3.8) in the generic case (third line on the right-hand side), as can be seen by inspection. The fact that, in the case where $l=1$, the bound cannot be improved is provided for by the observation that, in that case, Corollary 4 with $p=2$ and $l=2$ applies, and hence the tightness assertion given there holds. On the other hand, the fact that, in the case where $l=2$, the bound cannot be improved can be seen by considering e.g. $S(z)=z+\frac{z^2}{2}+\frac{z^4}{4}$. Namely, in that case we have $v_2(h_{8m})=4m$, since in the proof below (see (3.12)) all terms except the one with $j_8=m$ (and all other j_i's equal to zero) have a higher 2-divisibility.

(2) For $l\ge3$, the bound in (3.8) is actually better than the bound in (3.2) with $p=2$. Namely, the difference between the former and the latter is $\left\lfloor n/2^{l+1}\right\rfloor$. For $l=2$, the bound in (3.8) is just barely better than the bound in (3.2), the difference being $\lfloor n/4\rfloor-2\lfloor n/8\rfloor$, which equals 0 or 1, depending on whether $n\equiv0,1,2,3 \pmod 8$ or not. For $l=1$, the bound in (3.8) is worse than the bound in (3.2) with $p=2$.

Proof of Theorem 9. If $l=1$, then we apply Corollary 4 with $p=2$ and $l=2$. Since, for this choice of p and l, Condition (2.11) is equivalent to (3.7) with $l=1$, we immediately get the corresponding bound in (3.8) from (2.12).

We postpone the discussion of the case where $l=2$, and, for the moment, focus on the generic case where $l\ge3$. Proceeding in the same manner as in the proof of

Theorem 7, we let $n = a2^l + r$ with $0 \le r < 2^l$. We then must bound the 2-adic valuation of the summands in the series

$$\frac{h_{a2^l+r}}{(a2^l+r)!} = \sum_{i_0+\sum_{i=2^l+1}^{\infty} ij_i = a2^l+r} \widetilde{H}_{i_0} \prod_{i=2^l+1}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!} \tag{3.9}$$

from below, where we know that $\widetilde{H}_{i_0} \in \mathbb{Z}_2$ for all i_0, and where the λ_i's are defined as in the statement of Theorem 2 with $p = 2$. Again, since we are assuming that all s_i's are in $\mathbb{Z}_2$ (instead of $\mathbb{Q}_2$ as in Theorem 2), we have $\lambda_i \in \mathbb{Z}_2$ for all i. For the 2-adic valuation of the summand in the above sum, we then find that

$$\begin{aligned}
v_2\left(\widetilde{H}_{i_0} \prod_{i=2^l+1}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}\right) &\ge -\sum_{i=2^l+1}^{\infty} j_i \cdot v_2(i) - \sum_{i=2^l+1}^{\infty} \sum_{s\ge 1} \left\lfloor \frac{j_i}{2^s} \right\rfloor \\
&\ge -\sum_{i=2^l+1}^{2^{l+1}-1} j_i(l-2) - j_{3\cdot 2^{l-1}} - \sum_{i=2^{l+1}}^{\infty} j_i(l-1) - \sum_{i=2^{l+1}}^{\infty} j_i(v_2(i)-l+1) \\
&\qquad - \sum_{\substack{i=2^l+1 \\ i\ne 3\cdot 2^{l-1}}}^{2^{l+1}-1} \sum_{s\ge 1} \left\lfloor \frac{j_i}{2^s} \right\rfloor - \sum_{s\ge 1} \left\lfloor \frac{j_{3\cdot 2^{l-1}}}{2^s} \right\rfloor - \sum_{i=2^{l+1}}^{\infty} \sum_{s\ge 1} \left\lfloor \frac{j_i}{2^s} \right\rfloor \\
&\ge -\sum_{i=2^l+1}^{\infty} j_i(l-1) + \sum_{i=2^l+1}^{2^{l+1}-1} j_i - j_{3\cdot 2^{l-1}} - \sum_{i=2^{l+1}}^{\infty} j_i(v_2(i)-l+1) \\
&\qquad - \sum_{\substack{i=2^l+1 \\ i\ne 3\cdot 2^{l-1}}}^{2^{l+1}-1} j_i - \left\lfloor \frac{j_{3\cdot 2^{l-1}}}{2} \right\rfloor - \sum_{s\ge 1} \left\lfloor \frac{3\cdot 2^{l-1} j_{3\cdot 2^{l-1}}}{2^{s+l+1}} \right\rfloor - \sum_{s\ge 1} \sum_{i=2^{l+1}}^{\infty} \left\lfloor \frac{ij_i}{2^{s+l+1}} \right\rfloor \\
&\ge -(l-1)\left(j_{3\cdot 2^{l-1}} + \sum_{\substack{i=2^l+1 \\ i\ne 3\cdot 2^{l-1}}}^{\infty} \left\lfloor \frac{i}{2^l} \right\rfloor j_i \right) + \sum_{i=2^{l+1}}^{\infty} j_i(l-1)\left(\left\lfloor \frac{i}{2^l} \right\rfloor - 1 \right) \\
&\qquad - \sum_{i=2^{l+1}}^{\infty} j_i(v_2(i)-l+1) - \left\lfloor \frac{j_{3\cdot 2^{l-1}}}{2} \right\rfloor \\
&\qquad - \sum_{s\ge 1} \left\lfloor \frac{3\cdot 2^{l-1} j_{3\cdot 2^{l-1}}}{2^{s+l+1}} + \sum_{i=2^{l+1}}^{\infty} \frac{ij_i}{2^{s+l+1}} \right\rfloor \\
&\ge -(l-1)\left(j_{3\cdot 2^{l-1}} + \left\lfloor \sum_{\substack{i=2^l+1 \\ i\ne 3\cdot 2^{l-1}}}^{\infty} \frac{i}{2^l} j_i \right\rfloor \right) - \sum_{s\ge 1} \left\lfloor \frac{a}{2^{s+1}} \right\rfloor \\
&\qquad - \left\lfloor \frac{j_{3\cdot 2^{l-1}}}{2} \right\rfloor + \sum_{i=2^{l+1}}^{\infty} j_i \left(\left\lfloor \frac{i}{2^l} \right\rfloor (l-1) - v_2(i) \right),
\end{aligned} \tag{3.10}$$

where we have used the dependence of the summation indices of the sum in (3.9) in the last line. It is easy to see that

$$2^{x-l}(l-1) \ge x$$

for all real x with $x \ge l+1$ and $l \ge 3$. Hence, with $x = \lfloor \log_2 i \rfloor$, we have

$$\left\lfloor \frac{i}{2^l} \right\rfloor (l-1) - v_2(i) \ge 2^{x-l}(l-1) - x \ge 0,$$

so that the last term in the last line of (3.10) is non-negative. Next, we apply Lemma 10 with $j = j_{3\cdot 2^{l-1}}$ and x equal to the sum $\sum_{i=2^l+1,\, i\ne 3\cdot 2^{l-1}}^{\infty} i j_i/2^l$. This leads to the estimation

$$\begin{aligned} v_2\left(\widetilde H_{i_0} \prod_{i=2^l+1}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}\right) &\ge -(l-1) \left\lfloor \sum_{i=2^l+1}^{\infty} \frac{i}{2^l} j_i \right\rfloor - \sum_{s\ge1} \left\lfloor \frac{a}{2^{s+1}} \right\rfloor + \frac{l-3}{2} \left\lfloor \frac{j_{3\cdot 2^{l-1}}}{2} \right\rfloor \\ &\ge -(l-1)a - \sum_{s\ge1} \left\lfloor \frac{a}{2^{s+1}} \right\rfloor, \end{aligned} \tag{3.11}$$

which is exactly the bound (3.8) with $l \ge 3$ and $n = a2^l + r$, where $0 \le r < 2^l$.

For the remaining case where $l = 2$, a weakened version of the estimation (3.10) suffices. Here, we set $n = 4a + r$, with $0 \le r < 4$. Then

$$\begin{aligned} v_2\left(\widetilde H_{i_0} \prod_{i=5}^{\infty} \frac{\lambda_i^{j_i}}{i^{j_i}\, j_i!}\right) &\ge -\sum_{i=5}^{\infty} j_i \cdot v_2(i) - \sum_{i=5}^{\infty} \sum_{s\ge1} \left\lfloor \frac{j_i}{2^s} \right\rfloor \\ &\ge -j_6 - \sum_{i=8}^{\infty} j_i \cdot v_2(i) - \sum_{i=5}^{7} \sum_{s\ge1} \left\lfloor \frac{j_i}{2^s} \right\rfloor - \sum_{i=8}^{\infty} \sum_{s\ge1} \left\lfloor \frac{j_i}{2^s} \right\rfloor \\ &\ge -\sum_{i=5}^{7} j_i - \sum_{i=8}^{\infty} j_i \left(\left\lfloor \frac{i}{4} \right\rfloor + \left\lfloor \frac{i}{8} \right\rfloor \right) + \sum_{i=8}^{\infty} j_i \left(3 \left\lfloor \frac{i}{8} \right\rfloor - v_2(i) \right) \\ &\qquad - \sum_{i=5}^{7} \left\lfloor \frac{j_i}{2} \right\rfloor - \sum_{i=5}^{7} \sum_{s\ge1} \left\lfloor \frac{i j_i}{2^{s+3}} \right\rfloor - \sum_{s\ge1} \sum_{i=8}^{\infty} \left\lfloor \frac{i j_i}{2^{s+3}} \right\rfloor \\ &\ge -\left\lfloor \sum_{i=5}^{\infty} \frac{i j_i}{4} \right\rfloor - \left\lfloor \sum_{i=5}^{\infty} \frac{i j_i}{8} \right\rfloor + \sum_{i=8}^{\infty} j_i \left(3 \left\lfloor \frac{i}{8} \right\rfloor - v_2(i) \right) - \sum_{s\ge1} \left\lfloor \sum_{i=5}^{\infty} \frac{i j_i}{2^{s+3}} \right\rfloor \\ &\ge -\left\lfloor \frac{n}{4} \right\rfloor - \left\lfloor \frac{n}{8} \right\rfloor - \sum_{s\ge1} \left\lfloor \frac{n}{2^{s+3}} \right\rfloor + \sum_{i=8}^{\infty} j_i \left(3 \left\lfloor \frac{i}{8} \right\rfloor - v_2(i) \right), \end{aligned} \tag{3.12}$$

where we have used the dependence of the summation indices of the sum in (3.9) with $l = 2$ in the last line. To finish up, one applies the inequality

$$3 \left\lfloor \frac{i}{8} \right\rfloor - v_2(i) \ge 3 \cdot 2^{x-3} - x \ge 0, \quad \text{for } i \ge 8,$$

where $x = \lfloor \log_2 i \rfloor$. If this is used in (3.12), then one obtains the bound in (3.8) with $l = 2$. This completes the proof of the theorem. □

Lemma 10. *For all integers j and real numbers x, we have*

$$j + \lfloor x \rfloor \le \left\lfloor \frac{3}{2} j + x \right\rfloor - \frac{1}{2} \left\lfloor \frac{j}{2} \right\rfloor .$$

Proof. If j is even, say $j = 2J$, then

$$\left\lfloor \frac{3}{2} j + x \right\rfloor - \frac{1}{2} \left\lfloor \frac{j}{2} \right\rfloor = \lfloor 3J + x \rfloor - \frac{1}{2} J \ge 2J + \lfloor x \rfloor = j + \lfloor x \rfloor .$$

On the other hand, if j is odd, say $j = 2J + 1$, then

$$\left\lfloor \frac{3}{2} j + x \right\rfloor - \frac{1}{2} \left\lfloor \frac{j}{2} \right\rfloor = \left\lfloor 3J + \frac{3}{2} + x \right\rfloor - \frac{1}{2} J \ge 2J + 1 + \lfloor x \rfloor = j + \lfloor x \rfloor ,$$

as desired. □

As announced in Remark (4) after Theorem 2, there is a sharp dividing line concerning p-divisibility of the coefficients of the series $H(z)$ depending on whether $s_1 \equiv s_p \bmod p\mathbb{Z}_p$ or not.

Corollary 11. *For a prime number p, let $S(z) = \sum_{n \ge 1} \frac{s_n}{n} z^n$ be a formal power series with $s_n \in \mathbb{Q}_p$ for all n, and let $H(z) = \sum_{n \ge 0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. If $s_1 \equiv s_p \bmod p\mathbb{Z}_p$, then, for $p \ge 5$, we have*

$$v_p(h_n) \ge \sum_{s \ge 1} \left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{n}{2p^s} \right\rfloor \right) , \tag{3.13}$$

for $p = 3$, we have

$$v_3(h_n) \ge \sum_{s \ge 1} \left(\left\lfloor \frac{n}{3^s} \right\rfloor - \left\lfloor \frac{n}{2 \cdot 3^s} \right\rfloor \right) - \left\lfloor \frac{n}{18} \right\rfloor , \tag{3.14}$$

while, for $p = 2$, we have

$$v_2(h_n) \ge \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor . \tag{3.15}$$

On the other hand, if $s_1 \not\equiv s_p \bmod p\mathbb{Z}_p$, then for each N there exists some $n > N$ such that h_n is not divisible by p.

If we assume that Condition (1.6) is even satisfied up to the coefficient of $z^{p^{2p^l - 1}}$, then Theorem 7 may be further improved.

Theorem 12. *For a prime number $p \ge 3$, let $S(z) = \sum_{n \ge 1} \frac{s_n}{n} z^n$ be a formal power series with $s_n \in \mathbb{Z}_p$ for all n, and let $H(z) = \sum_{n \ge 0} \frac{h_n}{n!} z^n$ be the exponential of $S(z)$. Given a positive integer l such that $(p, l) \ne (3, 1)$, we assume that*

$$S(z^p) - pS(z) = pJ(z) + O\left(z^{2p^l}\right) \tag{3.16}$$

with $J(z) \in \mathbb{Z}_p[z]$. Then

$$v_p(h_n) \ge \sum_{s \ge 1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l - 1) \left\lceil \frac{n}{2p^l} \right\rceil - \sum_{s \ge l} \left\lfloor \frac{n}{2p^s} \right\rfloor \tag{3.17}$$

for all n.

Remarks. (1) The "gain" effected by the stronger conditions in Theorem 12 over those in Theorem 7 is measured by the difference between the bounds in (3.17) and (3.2), namely

$$(l-1)\left(\left\lfloor \frac{n}{p^l}\right\rfloor - \left\lceil \frac{n}{2p^l}\right\rceil\right).$$

(2) There is no need to have a $p=2$ version of Theorem 12 since this is given by Corollary 4 with $p=2$ and l replaced by $l+1$.

(3) If one would work through the proof below, with $p=3$ and $l=1$, then one would not obtain any improvement over Theorem 8.

Proof of Theorem 12. The proof runs along the lines of the proof of Theorem 7. The relevant computation is:

$$\begin{aligned}
v_p\left(\widetilde{H}_{i_0}\prod_{i=2p^l}^{\infty}\frac{\lambda_i^{j_i}}{i^{j_i}\,j_i!}\right) &\ge -\sum_{i=2p^l}^{\infty} j_i\cdot v_p(i) - \sum_{i=2p^l}^{\infty}\sum_{s\ge1}\left\lfloor\frac{j_i}{p^s}\right\rfloor\\
&\ge -\sum_{i=2p^l}^{\infty} j_i\left(l-1+\frac{i}{2p^l}\right) - \chi(p=3)\frac{j_{p^{l+1}}}{2} - \sum_{s\ge1}\sum_{i=2p^l}^{\infty}\left\lfloor\frac{ij_i}{2p^{s+l}}\right\rfloor\\
&> -\sum_{i=2p^l}^{\infty} j_i\frac{i}{2p^l}(l-1) + (l-1)\left(\frac{p}{2}-1\right)j_{p^{l+1}} - \left\lfloor\sum_{i=2p^l}^{\infty} j_i\frac{i}{2p^l}\right\rfloor - 1\\
&\qquad - \sum_{s\ge1}\left\lfloor\sum_{i=2p^l}^{\infty}\frac{ij_i}{2p^{s+l}}\right\rfloor - \chi(p=3)\frac{j_{p^{l+1}}}{2}\\
&> -(l-1)\left\lceil\frac{a}{2}\right\rceil - \left\lfloor\frac{a}{2}\right\rfloor - \sum_{s\ge1}\left\lfloor\frac{a}{2p^s}\right\rfloor\\
&\qquad + (l-1)\frac{j_{p^{l+1}}}{2} - \chi(p=3)\frac{j_{p^{l+1}}}{2} - 1. \qquad (3.18)
\end{aligned}$$

Again, it is seen that this implies the bound in (3.17). □

4. Counting subgroups in finitely generated groups

Let p be a prime number. The main result of this section, Proposition 14, in particular shows that the number $s_p(\Gamma)$ of subgroups of index p in a finitely generated group Γ is always congruent to 0 or 1 modulo p. As we are going to see in the next section, in combination with Corollary 11, this leads to a sharp dividing line between the two cases concerning the p-divisibility of the homomorphism numbers $h_n(\Gamma)$; see Theorem 17. As illustration of Proposition 14, we exhibit two classes of finite groups G for which $s_p(G)\equiv 0 \pmod p$ (and, more generally, even $s_{p^m}(G)\equiv 0 \pmod p$ for each prime power p^m dividing the order of G) in Corollaries 15 and 16.

Let Γ be a finitely generated group, let p be a prime number, and let m be a positive integer. We write the primary decomposition of the finitely generated Abelian group

$\bar{\Gamma} = \Gamma/[\Gamma, \Gamma]$ as

$$\bar{\Gamma} \cong \bigoplus_{q\in\mathbb{P}} \bigoplus_{\mu=1}^{M_q} C_{q^\mu}^{e_\mu^{(q)}(\Gamma)} \oplus C_\infty^{\bar{r}_\infty(\Gamma)},$$

where $\mathbb{P}$ denotes the set of positive rational primes. For $q \in \mathbb{P}$, the number

$$\bar{r}_q(\Gamma) := e_1^{(q)}(\Gamma) + e_2^{(q)}(\Gamma) + \cdots + e_{M_q}^{(q)}(\Gamma),$$

i.e., the rank (minimal number of generators) of the q-part of $\bar{\Gamma}$, is called the *q-rank* of the finitely generated Abelian group $\bar{\Gamma}$.

For a positive integer k, denote by $n_k(\Gamma)$ the number of normal subgroups of index k in Γ. The following observation will be useful.

Lemma 13. *For a prime number p, we have*

$$n_p(\Gamma) = \frac{p^{\bar{r}_p(\Gamma)+\bar{r}_\infty(\Gamma)} - 1}{p-1}. \tag{4.1}$$

In particular, $n_p(\Gamma)$ either equals zero, or is congruent to 1 modulo p, depending on whether or not $\bar{r}_p(\Gamma) + \bar{r}_\infty(\Gamma)$ vanishes.

Proof. This is [17, Lemma 2]. □

With Lemma 13 at our disposal, we can now show the following.

Proposition 14. *Let Γ be a finitely generated group, and let p be a prime number. The number $s_p(\Gamma)$ of index p subgroups in Γ does not attain the values $2, 3, \ldots, p-1$ modulo p. More precisely, if Γ contains a subgroup of index p, we have*

$$s_p(\Gamma) \equiv \begin{cases} 0 \pmod{p}, & \text{if } \bar{r}_p(\Gamma) + \bar{r}_\infty(\Gamma) = 0, \\ 1 \pmod{p}, & \text{if } \bar{r}_p(\Gamma) + \bar{r}_\infty(\Gamma) > 0. \end{cases} \tag{4.2}$$

Also, if Γ does not contain a normal subgroup of index p^m for some $m \geq 1$, then $s_{p^m}(\Gamma) \equiv 0 \pmod{p}$.

Proof. Let Γ be a finitely generated group, and let p^m be a non-trivial prime power. Let $\mathcal{C}_{p^m}(\Gamma)$ be the complex of subgroups of index p^m in Γ. Since Γ is assumed to be finitely generated, $\mathcal{C}_{p^m}(\Gamma)$ is finite. The group Γ acts from the right on this finite complex by conjugation, i.e., via

$$\Delta \cdot \gamma := \gamma^{-1}\Delta\gamma, \qquad \gamma \in \Gamma,\ \Delta \in \mathcal{C}_{p^m}(\Gamma).$$

Consider a group $\Delta \in \mathcal{C}_{p^m}(\Gamma)$. The orbit of Δ under this Γ-action (i.e., its conjugacy class) has size $(\Gamma : N_\Gamma(\Delta))$. Since $\Delta \subseteq N_\Gamma(\Delta)$, this size must be a power of p, say p^e, with $0 \leq e \leq m$. If $e = 0$, then $N_\Gamma(\Delta)) = \Gamma$, that is, Δ is normal and the size of its orbit is 1. Otherwise the orbit size is divisible by p. Thus,

$$s_{p^m}(\Gamma) \equiv n_{p^m}(\Gamma) \pmod{p}. \tag{4.3}$$

The claims now follow by combining (4.3) with Lemma 13. □

Remark. Similarly, one can show that the number $s_{p^2}(\Gamma)$ does not attain the values $2, 3, \dots, p-1$ modulo p. More precisely, if Γ contains a subgroup of index p^2, then

$$s_{p^2}(\Gamma) \equiv \begin{cases} 0 \pmod p, & \text{if } \bar r_p(\Gamma) + \bar r_\infty(\Gamma) = 0, \text{ or } e_1^{(p)} = \bar r_p(\Gamma) = 1 \text{ and } \bar r_\infty(\Gamma) = 0, \\ 1 \pmod p, & \text{otherwise.} \end{cases} \tag{4.4}$$

We give two illustrations for Proposition 14 from finite group theory.

Corollary 15. *Let G be a finite non-Abelian simple group, and let p^m be a non-trivial prime power dividing the order of G. Then $s_{p^m}(G) \equiv 0 \pmod p$.*

Proof. We have $1 < p^m < |G|$, since otherwise $1 < \zeta_1(G) < G$, a contradiction. Hence, G does not contain a normal subgroup of index p^m, and our assertion follows from the last assertion of Proposition 14. □

Corollary 16. *Let p^m be a prime power with $p^m \ge 3$, let n be positive integer, and suppose that $p^m \mid n!$. Then $s_{p^m}(S_n) \equiv 0 \pmod p$.*

Proof. For $n = 1, 2$ the assertion is empty (thus holds trivially), for $n = 3, 4$ it holds by inspection. For $n \ge 5$, the only non-trivial normal subgroup of S_n is A_n, which has index 2; in particular, S_n does not contain a normal subgroup of index p^m. Our claim follows again from the last assertion of Proposition 14. □

5. p-Divisibility of homomorphism numbers of finitely generated groups

In this section, we present results on the p-divisibility of homomorphism numbers for various classes of finitely generated groups Γ. Our first result, Theorem 17, in particular says that there exists a sharp dividing line for the p-divisibility of the sequence $\big(h_n(\Gamma)\big)_{n\ge0}$: either there is "no increase" in p-divisibility, or there is a considerable p-part in $h_n(\Gamma)$ which tends to infinity as $n \to \infty$. In this context, Proposition 14 shows that the dividing line is given by $s_p(\Gamma) \equiv 1 \pmod p$ as opposed to $s_p(\Gamma) \equiv 0 \pmod p$. This dichotomy is indeed what is needed in the proof of Theorem 17 in order to be able to apply an appropriate abstract result (namely Corollary 11).

Finite p-groups G always have the property that $s_p(G) \equiv 1 \pmod p$. Thus, unbounded growth of p-divisibility must be expected for the homomorphism numbers of such groups. Theorem 18 shows that a growth estimate for $h_n(G)$ can be given which is even better than the one in Theorem 17. Indeed, the bound given there is the same as the one in (1.4) for the cyclic group C_p. Moreover, if p is odd and G is not cyclic, a further improvement is possible, as Theorem 19 shows.

As an example of a non-nilpotent group of mixed order, in Theorem 21 we consider the dihedral group of order $2m$, which turns out to have the property that the 2-divisibility of its homomorphism numbers can be bounded below by bounds which are at least as good as the one for C_2 given in (1.3), and a better bound if $4 \mid m$.

In sharp contrast to these results, we show that a finite non-Abelian simple group G satisfies $h_n(G) \equiv 1 \pmod p$ for all n; see Corollary 23.

Theorem 17. *Let Γ be a finitely generated group, and let p be a prime number. If Γ contains a subgroup of index p and $\bar{r}_p(\Gamma) + \bar{r}_\infty(\Gamma) > 0$, then, for $p \geq 5$, we have*

$$v_p\big(h_n(\Gamma)\big) \geq \sum_{s \geq 1} \left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{n}{2p^s} \right\rfloor \right), \tag{5.1}$$

while, for $p = 3$, we have

$$v_3\big(h_n(\Gamma)\big) \geq \sum_{s \geq 1} \left(\left\lfloor \frac{n}{3^s} \right\rfloor - \left\lfloor \frac{n}{2 \cdot 3^s} \right\rfloor \right) - \left\lfloor \frac{n}{18} \right\rfloor, \tag{5.2}$$

and, for $p = 2$, we have

$$v_2\big(h_n(\Gamma)\big) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor, \tag{5.3}$$

for all n. In all other cases, for each N there exists some $n > N$ such that $h_n(\Gamma)$ is not divisible by p.

Proof. This follows by combining Proposition 14 with Relation (1.1) and Corollary 11. □

Theorem 18. *Let p be a prime number, and let G be a non-trivial finite p-group. Then*

$$v_p\big(h_n(G)\big) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \tag{5.4}$$

for all n.

Proof. By Frobenius' generalisation of Sylow's third theorem in [6], we have $s_{p^i}(G) \equiv 1 \pmod p$ for all i such that $p^i \leq |G|$, while $s_n(G) = 0$ for all n different from a power of p. The claim now follows from Relation (1.1) plus Corollary 4 with $l = 2$. □

Theorem 19. *Let p be a prime number, and let G be a non-cyclic p-group of odd order. Then*

$$v_p\big(h_n(G)\big) \geq \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor - 2 \left\lfloor \frac{n}{p^3} \right\rfloor \tag{5.5}$$

for all n.

Proof. Let p^m be the order of G. By [12] (see also [9, Theorem 1.52]), we know that $s_{p^i} \equiv 1 + p \pmod{p^2}$ for $1 \leq i \leq m - 1$. Thus, remembering again (1.1), we see that the assumptions of Corollary 4 with $l = 3$ are satisfied. The claim now follows from (2.12). □

Next we discuss the family of finite dihedral groups.

Proposition 20. *Let D_m be the dihedral group of order $2m$, and let d be a divisor of $2m$. Then*

$$s_d(G) = \begin{cases} d, & \text{if } d \text{ is odd,} \\ 1 + d, & \text{if } d \text{ is even.} \end{cases}$$

Proof. We regard D_m as a real reflection group acting on $\mathbb{R}^2$ by rotations through angles that are multiples of π/m and reflections in lines that have angles with the x-axis that are also multiples of π/m. Subgroups of D_m are either cyclic or themselves dihedral groups. For each even divisor d of $2m$ there exists exactly one cyclic subgroup of D_m of index d. On the other hand, a dihedral group can be given in terms of two reflections which generate it. It is not difficult to see that a unique way to encode a dihedral subgroup of D_m of index d is in terms of two reflections with respect to the lines l_1 and l_2, the first having an angle of $\alpha\pi/m$ with the x-axis, the second having an angle of $(\alpha+d)\pi/m$ with the x-axis, and $0 \le \alpha < d$. There are d possibilities to choose α. This implies the assertion of the proposition. □

Theorem 21. *Let D_m be the dihedral group of order $2m$. If p is a prime number different from 2, then $h_n(D_m)$ is infinitely often not divisible by p, while we have*

$$v_2\big(h_n(D_m)\big) \ge \begin{cases} \left\lfloor \frac{n}{2} \right\rfloor, & \text{if } 4 \mid m, \\ \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor, & \text{if } 4 \nmid m. \end{cases} \tag{5.6}$$

Proof. First consider an odd prime number p. In that case, Proposition 20 says that $s_p(D_m) = p$ if $p \mid m$ and $s_p(D_m) = 0$ if not. In either case, we have $s_p(D_m) \equiv 0 \pmod p$. The assertion on $h_n(D_m)$ in that case then follows directly from Corollary 11.

In order to establish the second part of the theorem, we observe that, by Proposition 20, we have

$$s_1(D_m) = 1, \quad s_2(D_m) = 3, \quad s_4(D_m) = \begin{cases} 0, & \text{if } 4 \nmid m, \\ 5, & \text{if } 4 \mid m, \end{cases} \quad s_8(D_m) = \begin{cases} 0, & \text{if } 8 \nmid m, \\ 9, & \text{if } 8 \mid m. \end{cases}$$

Consequently, we have $s_2(D_m) - s_1(D_m) = 2 \equiv 0 \pmod 2$ and $s_4(D_m) - s_2(D_m) = 2$ if $4 \mid m$, while $s_4(D_m) - s_2(D_m) = -3$ if $4 \nmid m$. Thus, in the first case, we may apply Corollary 5 with $l = 2$ and $m = 1$, while in the second case we have to choose $m = 0$. The bound on the 2-divisibility of $h_n(D_m)$ then follows from (2.16). □

The following proposition prepares for the result in Corollary 23 on the residue class modulo p of the number of permutation representations of a finite non-Abelian simple group. Given a finitely generated group Γ, we write $T_n(\Gamma)$ for the set of all transitive permutation representations of Γ of degree n. It is well-known (see e.g. [11, Prop. 3]) that

$$|T_n(\Gamma)| = (n-1)!\, s_n(\Gamma), \qquad \text{for } n \ge 1. \tag{5.7}$$

Proposition 22. *Suppose that G is a finite non-Abelian simple group. Then, for each $n \ge 2$, we have $|T_n(G)| \equiv 0 \pmod{|G|}$.*

Proof. It is easy to check that G acts from the left on the set $T_n(G)$ by conjugation, that is,

$$g \cdot \varphi = \varphi \circ \iota_g, \qquad \text{for } g \in G,\ \varphi \in T_n(G).$$

Now suppose that $g \cdot \varphi = \varphi$ for some $g \in G$ and $\varphi \in T_n(G)$. Then we have

$$\varphi(g^{-1}hg) = \varphi(h), \qquad \text{for } h \in G,$$

or, equivalently,

$$[g,h] \in \ker(\varphi), \qquad \text{for } h \in G.$$

However, as φ is transitive on the set $\{1, 2, \dots, n\}$ and $n \ge 2$ by assumption, we have $\ker(\varphi) \ne G$, hence, by simplicity of G, $\ker(\varphi) = 1$. We thus conclude that

$$[g,h] = 1, \qquad \text{for } h \in G,$$

so that $g \in \zeta_1(G)$. Using again simplicity of G, plus the fact that G is non-Abelian, we find that $\zeta_1(G) = 1$, thus $g = 1$. Consequently, the action of G on $T_n(G)$ is free, whence our claim. □

Corollary 23. *Let G be a finite non-Abelian simple group, and let p^m be a prime power dividing the order of G. Then*

$$s_n(G) \equiv 0 \pmod{p^m}, \quad 2 \le n \le p. \tag{5.8}$$

Proof. Since $n \le p$ by assumption, $p \nmid (n-1)!$, so that $(n-1)!$ is invertible modulo p^m. Combining (5.7) with Proposition 22, we get, for $2 \le n \le p$, that

$$s_n(G) \equiv ((n-1)!)^{-1} \, |T_n(G)| \equiv 0 \pmod{p^m},$$

as desired. □

From the above corollary, we see in particular that $s_p(G) \equiv 0 \pmod p$. Thus, by Corollary 11, we conclude that there is no increasing p-divisibility for $h_n(G)$, in the sense that, for each positive integer N, we can find $n > N$ such that $h_n(G)$ is not divisible by p. We now show that the above corollary allows for a sharpening of the last conclusion: $h_n(G)$ is *never* divisible by p, and it is in fact congruent to 1 modulo p.

Corollary 24. *Let G be a finite non-Abelian simple group, and let p be a prime divisor of the order of G. Then we have*

$$h_n(G) \equiv 1 \pmod p, \quad n \ge 1.$$

Proof. Combining the fact that $s_n(G) \equiv 0 \pmod p$ for $2 \le n \le p$, coming from Corollary 23, with the recurrence in (1.2), we find that

$$h_n(G) = \sum_{k=1}^{n} (n-k+1)_{k-1} s_k(G) h_{n-k}(G) \equiv h_{n-1}(G) \pmod p, \quad n \ge 1.$$

Since $h_0(G) = 1$, the result follows. □

6. p-Divisibility of homomorphism numbers for finite Abelian p-groups

In this section, we provide tight bounds on the divisibility by powers of a prime p of the number of permutation representations of finite Abelian p-groups. Theorems 25 and 26 below refine the results of Katsurada, Takegahara and Yoshida [10, Theorems 1.2–1.4] for rank 1 and 2 by adding a periodicity assertion for quotients, while, at the same time, generalising them to arbitrary rank.

Theorem 25. *Let $G = C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}}$ with $a_1 \ge a_2 \ge \cdots \ge a_r$.*

(i) *If $a_1 > a_2 + \cdots + a_r$, then*

$$v_p\big(h_n(G)\big) \ge \sum_{s=1}^{a_1} \left\lfloor \frac{n}{p^s} \right\rfloor - (a_1 - a_2 - \cdots - a_r) \left\lfloor \frac{n}{p^{a_1+1}} \right\rfloor. \tag{6.1}$$

Moreover, the quotient

$$Q_n(G) = \frac{h_n(G)}{p^{e_p(n;a_1,\dots,a_r)}},$$

where $e_p(n; a_1, \dots, a_r)$ denotes the right-hand side of (6.1), satisfies

$$Q_n(G) \equiv (-1)^{a_1} Q_{n-p^{a_1+1}}(G) \pmod p. \tag{6.2}$$

In particular, the bound in (6.1) is tight for all n which are divisible by p^{a_1+1}.

(ii) *If $a_1 \le a_2 + \dots + a_r$ and $a_1 + a_2 + \dots + a_r$ is even, then*

$$v_p\big(h_n(G)\big) \ge \sum_{s=1}^{A_1} \left\lfloor \frac{n}{p^s} \right\rfloor , \tag{6.3}$$

where $A_1 = (a_1 + a_2 + \dots + a_r)/2$. Moreover, if $p > 2$, the quotient

$$Q_n(G) = \frac{h_n(G)}{p^{e_p(n;A_1)}},$$

where $e_p(n; A_1)$ denotes the right-hand side of (6.3), *satisfies*

$$Q_n(G) \equiv (-1)^{A_1} Q_{n-p^{A_1+1}}(G) \pmod p. \tag{6.4}$$

In particular, the bound in (6.3) *is tight for all n which are divisible by p^{A_1+1}, except if $p = 2$.*

(iii) *If $a_1 \le a_2 + \dots + a_r$ and $a_1 + a_2 + \dots + a_r$ is odd, then*

$$v_p\big(h_n(G)\big) \ge \sum_{s=1}^{A_2} \left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{n}{p^{A_2+1}} \right\rfloor , \tag{6.5}$$

where $A_2 = (a_1 + a_2 + \dots + a_r + 1)/2$. Moreover, the quotient

$$Q_n(G) = \frac{h_n(G)}{p^{e_p(n;A_2)}},$$

where $e_p(n; A_2)$ denotes the right-hand side of (6.5), *satisfies*

$$Q_n(G) \equiv (-1)^{A_2} Q_{n-p^{A_2+1}}(G) \pmod p. \tag{6.6}$$

In particular, the bound in (6.5) *is tight for all n which are divisible by p^{A_2+1}.*

Proof. By a short and elegant computation, Butler [2, display on top of p. 773] proved that the difference of "successive" subgroup numbers in a finite Abelian p-group of type $\alpha = (a_1, a_2, \dots, a_r)$ essentially equals a specialised Kostka–Foulkes polynomial. To be precise, taking into account the symmetry relation (cf. e.g. [16, p. 181, Statement (1.5)])

$$s_{p^i} = s_{p^{2A_1-i}}, \tag{6.7}$$

Butler found that

$$s_{p^i}(G) - s_{p^{i-1}}(G) = p^{n(\alpha)} K_{(2A_1-i,i),\alpha}(p^{-1}), \quad \text{for } i \le A_1, \tag{6.8}$$

where $K_{\lambda,\mu}(t)$ denotes the Kostka–Foulkes polynomial indexed by partitions λ and μ (see [16, Ch. III, Sec. 6] for the definition), and where $n(\alpha) = \sum_{i=1}^{r} (i-1)a_i$. It is known (cf. [16, Statement (6.5)(ii) on p. 243]) that $K_{\lambda,\mu}(t)$ vanishes if μ is not less than or equal to λ in dominance order (see [16, p. 7] for the definition), and that it is a monic polynomial of degree $n(\lambda) - n(\mu)$ otherwise. We should observe that α is not less than or equal to $(2A_1 - i, i)$ if, and only if, $2A_1 - i < a_1$, that is, $i > a_2 + \dots + a_r$. If we use all this and the simple fact that $n\big((2A_1 - i, i)\big) = i$ to rewrite (6.8),

$$s_{p^i}(G) - s_{p^{i-1}}(G) = p^i \big(p^{n(\alpha)-n((2A_1-i,i))} K_{(n-i,i),\alpha}(p^{-1})\big),$$

and combine this with the symmetry relation (6.7), then it follows immediately that

$$v_p\big(s_{p^i}(G) - s_{p^{i-1}}(G)\big) = \begin{cases} i, & \text{for } 0 \le i \le \min\{2A_1 - a_1, A_1\}, \\ 2A_1 - i + 1, & \text{for } \max\{a_1, A_1\} + 1 \le i \le 2A_1 + 1, \end{cases} \tag{6.9}$$

and

$$s_{p^i}(G) - s_{p^{i-1}}(G) = 0, \quad \text{for } 2A_1 - a_1 + 1 \le i \le a_1,$$
$$\text{and for } i = A_2 \text{ if } a_1 + \cdots + a_r \text{ is odd.} \quad (6.10)$$

Moreover, we have

$$s_{p^i}(G) - s_{p^{i-1}}(G) = -p^{2A_1 - i + 1} + \text{higher degree terms,}$$
$$\text{for } i = a_1 + 1 \text{ if } a_1 > a_2 + \cdots + a_r,$$
$$\text{for } i = A_1 + 1 \text{ if } a_1 \le a_2 + \cdots + a_r \text{ and } a_1 + \cdots + a_r \text{ is even,}$$
$$\text{and for } i = A_2 + 1 \text{ if } a_1 \le a_2 + \cdots + a_r \text{ and } a_1 + \cdots + a_r \text{ is odd.} \quad (6.11)$$

If we let $a_1 > a_2 + \cdots + a_r$, then (6.9)–(6.11) imply that we may apply Corollary 5 with $l = a_1 + 1$ and $m = 2A_1 - a_1 + 1 = a_2 + \cdots + a_r$. Using Legendre's formula [14, p. 10] for the p-adic valuation of a factorial again, we obtain the bound (6.1), as well as the congruence (6.2) and the corresponding tightness assertion.

Similarly, if $a_1 \le a_2 + \cdots + a_r$ and $a_1 + a_2 + \cdots + a_r$ is even, then (6.9) and (6.11) imply that we may apply Corollary 5 with $l = A_1 + 1$ and $m = A_1$, except if $p = 2$. Indeed, while (2.14) and (2.15) are satisfied for the choice of $l = A_1 + 1$ and $m = A_1$, the inequality (2.16) is satisfied only if we do not have $p = 2$. Namely, if we choose $e = A_1 + 2$ in the latter case, the left-hand side of (2.16) equals $A_1 - 1$, while the right-hand side gives $-2 - 1 + (A_1 + 2) + 1 = A_1$, contradicting (2.16). However, if we exclude the case where $p = 2$, then Corollary 5 together with Legendre's formula [14, p. 10] imply the bound (6.3), as well as the congruence (6.4) and corresponding tightness assertion. In the exceptional case where $p = 2$, the stronger Theorem 26 below fills the hole.

Finally, if $a_1 \le a_2 + \cdots + a_r$ and $a_1 + a_2 + \cdots + a_r$ is odd, then (6.9)–(6.11) imply that we may apply Corollary 5 with $l = A_2 + 1$ and $m = A_2 - 1$. Using Legendre's formula [14, p. 10], we then obtain the bound (6.5), as well as the congruence (6.6) and corresponding tightness assertion.

This completes the proof of the theorem. □

In the exceptional case where $p = 2$, $a_1 \le a_2 + \cdots + a_r$, and $a_1 + a_2 + \cdots + a_r$ is even, we may instead apply Theorem 6 to obtain a stronger 2-divisibility result. Since the proof is straightforward from (6.9)–(6.11), we content ourselves with the statement of the result.

Theorem 26. *Let $G = C_{2^{a_1}} \times C_{2^{a_2}} \times \cdots \times C_{2^{a_r}}$ with $a_1 \ge a_2 \ge \cdots \ge a_r$, $a_1 \le a_2 + \cdots + a_r$, and $a_1 + a_2 + \cdots + a_r$ being even. Then*

$$v_2\big(h_n(G)\big) \ge \sum_{s=1}^{A_1} \left\lfloor \frac{n}{2^s} \right\rfloor + \left\lfloor \frac{n}{2^{A_1+2}} \right\rfloor - \left\lfloor \frac{n}{2^{A_1+3}} \right\rfloor, \quad (6.12)$$

where $A_1 = (a_1 + a_2 + \cdots + a_r)/2$. Moreover, the quotient

$$Q_n(G) = \frac{h_n(G)}{2^{e_2(n;A_1)}},$$

where $e_2(n;A_1)$ *denotes the right-hand side of* (6.12), *satisfies*

$$Q_n(G) \equiv Q_{n-2^{A_1+3}}(G) \pmod 2. \tag{6.13}$$

The bound is tight for all n *congruent to* 0, 2^{A_1+1}, *and* 2^{A_1+2} *modulo* 2^{A_1+3}.

7. Periodicity of Subgroup numbers for free products of finite Abelian groups

In [8], Grady and Newman used their p-divisibility result for the homomorphism number $h_n(C_p)$ of C_p mentioned in the introduction to demonstrate ultimate periodicity modulo p for the subgroup numbers of free powers of C_p. Armed with our much more general p-divisibility results from the previous section, and using the same approach, we may now derive ultimate periodicity modulo p for much larger classes of free products.

Theorem 27. *Let* p *be a prime number. Furthermore, let* Γ_0 *be a finitely generated group, and let* $G_1, G_2, \dots$ *be non-trivial finite Abelian* p*-groups. In each of the following cases, the arithmetic function* $s_n(\Gamma)$ *forms an ultimately periodic sequence modulo* p*:*

(1) $\Gamma = \Gamma_0 * G_1 * G_2$ *and* $p \ge 5$.
(2) $\Gamma = \Gamma_0 * G_1 * G_2$, $p = 3$, *and not both* G_1 *and* G_2 *are isomorphic to* C_3.
(3) $\Gamma = \Gamma_0 * G_1 * G_2 * G_3$ *and* $p = 3$.
(4) $\Gamma = \Gamma_0 * G_1 * G_2$, $p = 2$, *and both* G_1 *and* G_2 *are not isomorphic to* C_2.
(5) $\Gamma = \Gamma_0 * C_2 * G_1$, $p = 2$, *and* G_1 *is not isomorphic to* $C_2, C_4, C_8, C_2 \times C_2$, $C_2 \times C_2 \times C_2$, *or* $C_4 \times C_2$.
(6) $\Gamma = \Gamma_0 * G_1 * G_2 * G_3$, $p = 2$, *and not all of* G_1, G_2, G_3 *are isomorphic to* C_2.
(7) $\Gamma = \Gamma_0 * C_2 * C_2 * C_2 * C_2$ *and* $p = 2$.

Proof. We know that the sequence $\big(s_n(\Gamma)\big)_{n\ge1}$ satisfies the recurrence (1.2). By dividing both sides of the recurrence by $(n-1)!$, we obtain the equivalent form

$$\frac{nh_n(\Gamma)}{n!} = \sum_{k=1}^{n} s_k(\Gamma)\,\frac{h_{n-k}(\Gamma)}{(n-k)!}, \qquad \text{for } n \ge 1. \tag{7.1}$$

Following Grady and Newman [8], our strategy consists in showing that $v_p\big(h_n(\Gamma)/n!\big) > 0$ for almost all n in the cases (1)–(7). Given that p-divisibility property, the recurrence (7.1) reduces to a finite-length linear recurrence with constant coefficients for the sequence $\big(s_n(\Gamma)\big)_{n\ge1}$ when considered modulo p. It then follows (see e.g. [15, Ch. 8]) that $\big(s_n(\Gamma)\big)_{n\ge1}$ is an ultimately periodic sequence modulo p.

(1) We have

$$h_n(\Gamma) = h_n(\Gamma_0)h_n(G_1)h_n(G_2),$$

and hence

$$v_p\left(h_n(\Gamma)\right) \ge v_p\left(h_n(G_1)\right) + v_p\left(h_n(G_2)\right). \tag{7.2}$$

We have to show that

$$v_p\left(h_n(\Gamma)\right) > v_p(n!) = \sum_{s\ge1} \left\lfloor \frac{n}{p^s} \right\rfloor \tag{7.3}$$

for all sufficiently large n. By our p-divisibility results in Theorem 25, we see that

$$v_p\left(h_n(G)\right) \ge \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

for any finite Abelian p-group G. Hence,

$$v_p\left(h_n(G_1)\right) + v_p\left(h_n(G_2)\right) \geq 2\left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right).$$

Now let $n = n_2 p^2 + n_1 p + n_0$ with $0 \leq n_0, n_1 < p$. Then the above inequality becomes

$$v_p\left(h_n(G_1)\right) + v_p\left(h_n(G_2)\right) \geq 2\left(n_2 p + n_1 - n_2\right), \tag{7.4}$$

while

$$\begin{aligned} v_p(n!) &= (n_2 p + n_1) + n_2 + \sum_{s \geq 3} \left\lfloor \frac{n}{p^s} \right\rfloor \\ &= n_2(p+1) + n_1 + \sum_{s \geq 1} \left\lfloor \frac{n_2}{p^s} \right\rfloor \\ &\leq n_2(p+1) + n_1 + \sum_{s \geq 1} \frac{n_2}{p^s} \\ &\leq n_2\left(p + 1 + \frac{1}{p-1}\right) + n_1. \end{aligned} \tag{7.5}$$

Since

$$2(p-1) > p + 1 + \frac{1}{p-1} \tag{7.6}$$

for all $p \geq 5$, a combination of (7.2), (7.4) and (7.5) establishes (7.3) as long as $n_2 > 0$, that is, for $n \geq p^2$.

(2) We proceed as in the proof of Item (1). Without loss of generality, let us assume that G_2 is not isomorphic to C_3. By our 3-divisibility results in Theorem 25, it then follows that

$$v_3\left(h_n(G_2)\right) \geq \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{9} \right\rfloor - 2\left\lfloor \frac{n}{27} \right\rfloor.$$

Hence,

$$v_3\left(h_n(G_1)\right) + v_3\left(h_n(G_2)\right) \geq 2\left(\left\lfloor \frac{n}{3} \right\rfloor - \left\lfloor \frac{n}{27} \right\rfloor\right).$$

Now let $n = 27n_3 + 9n_2 + 3n_1 + n_0$ with $0 \leq n_0, n_1, n_2 < 3$. Then the above inequality becomes

$$\begin{aligned} v_3\left(h_n(G_1)\right) + v_3\left(h_n(G_2)\right) &\geq 2\left(9n_3 + 3n_2 + n_1 - n_3\right) \\ &\geq 16n_3 + 6n_2 + 2n_1, \end{aligned} \tag{7.7}$$

while

$$\begin{aligned} v_3(n!) &= (9n_3 + 3n_2 + n_1) + (3n_3 + n_2) + n_3 + \sum_{s \geq 4} \left\lfloor \frac{n}{3^s} \right\rfloor \\ &= 13n_3 + 4n_2 + n_1 + \sum_{s \geq 1} \left\lfloor \frac{n_3}{3^s} \right\rfloor \\ &\leq 13n_3 + 4n_2 + n_1 + \sum_{s \geq 1} \frac{n_3}{3^s} \\ &\leq \frac{27}{2} n_3 + 4n_2 + n_1. \end{aligned} \tag{7.8}$$

A combination of (7.2), (7.7) and (7.8) establishes (7.3) as long as $n_3 > 0$, that is, for $n \geq 27$.

(3) This is completely analogous to the proof of Item (1). The only difference is that, instead of (7.6), here we rely on

$$3(p-1) > p+1+\frac{1}{p-1},$$

which is valid for all $p \geq 3$, so in particular for $p = 3$.

(4) By our 2-divisibility results in Theorems 25 and 26, one can see that

$$v_2\big(h_n(G_1)\big) \geq \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor .$$

Hence,

$$v_2\big(h_n(C_2)\big) + v_2\big(h_n(G_1)\big) \geq 2\left\lfloor \frac{n}{2} \right\rfloor .$$

Now let $n = 2n_1 + n_0$ with $0 \leq n_0 < 2$. Then the above inequality becomes

$$v_2\left(h_n(C_2)\right) + v_2\left(h_n(G_1)\right) \geq 2n_1, \tag{7.9}$$

while

$$\begin{aligned} v_2(n!) &= n_1 + \sum_{s\geq 2} \left\lfloor \frac{n}{2^s} \right\rfloor \\ &= n_1 + \sum_{s\geq 1} \left\lfloor \frac{n_1}{2^s} \right\rfloor \\ &< 2n_1, \end{aligned} \tag{7.10}$$

as long as $n_1 > 0$. A combination of (7.2), (7.9) and (7.10) establishes (7.3) as long as $n_1 > 0$, that is, for $n \geq 2$.

(5) Again, we proceed as in the proof of Item (1). By our 2-divisibility results in Theorems 25 and 26, it follows that

$$v_2\big(h_n(G)\big) \geq \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor - 2\left\lfloor \frac{n}{8} \right\rfloor$$

for any finite Abelian 2-group not isomorphic to C_2. Hence,

$$v_2\big(h_n(G_1)\big) + v_2\big(h_n(G_2)\big) \geq 2\left\lfloor \frac{n}{2} \right\rfloor + 2\left\lfloor \frac{n}{4} \right\rfloor - 4\left\lfloor \frac{n}{8} \right\rfloor .$$

Now let $n = 8n_3 + 4n_2 + 2n_1 + n_0$ with $0 \leq n_0, n_1, n_2 < 2$. Then the above inequality becomes

$$\begin{aligned} v_2\big(h_n(G_1)\big) + v_2\big(h_n(G_2)\big) &\geq 2(4n_3 + 2n_2 + n_1) + 2(2n_3 + n_2) - 4n_3 \\ &\geq 8n_3 + 6n_2 + 2n_1, \end{aligned} \tag{7.11}$$

while

$$\begin{aligned} v_2(n!) &= (4n_3 + 2n_2 + n_1) + (2n_3 + n_2) + n_3 + \sum_{s\geq 4} \left\lfloor \frac{n}{2^s} \right\rfloor \\ &= 7n_3 + 3n_2 + n_1 + \sum_{s\geq 1} \left\lfloor \frac{n_3}{2^s} \right\rfloor \\ &< 8n_3 + 3n_2 + n_1, \end{aligned} \tag{7.12}$$

as long as $n_3 > 0$. A combination of (7.2), (7.11) and (7.12) establishes (7.3) as long as $n_3 > 0$, that is, for $n \ge 8$.

(6) We proceed as in the proof of Item (1). Here, we have to show that

$$v_2\big(h_n(G_1)\big) + v_2\big(h_n(G_2)\big) + v_2\big(h_n(G_3)\big) > \sum_{s\ge1} \left\lfloor \frac{n}{2^s} \right\rfloor \tag{7.13}$$

for all sufficiently large n. Without loss of generality, we assume that G_3 is not isomorphic to C_2. By our 2-divisibility results in Theorems 25 and 26, it then follows that

$$v_2\big(h_n(G_3)\big) \ge \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor - 2\left\lfloor \frac{n}{8} \right\rfloor .$$

Hence,

$$v_2\big(h_n(G_1)\big) + v_2\big(h_n(G_2)\big) + v_2\big(h_n(G_3)\big) \ge 3\left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor - 2\left\lfloor \frac{n}{8} \right\rfloor .$$

Now let $n = 8n_3 + 4n_2 + 2n_1 + n_0$ with $0 \le n_0, n_1, n_2 < 2$. Then the above inequality becomes

$$\begin{aligned} v_2\big(h_n(G_1)\big) + v_2\big(h_n(G_2)\big) &+ v_2\big(h_n(G_3)\big) \\ &\ge 3(4n_3 + 2n_2 + n_1) - (2n_3 + n_2) - 2n_3 \\ &\ge 8n_3 + 5n_2 + 3n_1, \end{aligned} \tag{7.14}$$

A combination of (7.2), (7.14) and (7.12) establishes (7.3) as long as $n_3 > 0$, that is, for $n \ge 8$.

(7) This can be established in the same manner as before. As a matter of fact, this had already been done earlier in [7, Theorem 1]. In fact, there the stronger result is shown that all $s_n(\Gamma)$'s are odd. Indeed, this is a consequence of considering the relation (1.2), viewed as a recurrence relation for the $s_n(\Gamma)$'s, modulo 2. ☐

8. The p-divisibility of permutation numbers

It is well-known (see e.g. [20, Eq. (5.30)]) that

$$\sum_{n\ge0} \frac{z^n}{n!} \sum_{\sigma\in S_n} \prod_{i\ge1} x_i^{\#(\text{cycles of length } i \text{ in } \sigma)} = \exp\left(\sum_{n\ge1} \frac{x_n}{n} z^n \right). \tag{8.1}$$

In the language of species (cf. [1]), this is the *cycle index series* of the species of permutations. Evidently, there are numerous specialisations of this formula which, in combination with our p-divisibility results in Sections 2 and 3, lead to p-divisibility results for numbers of permutations with restrictions on their cycle lengths. In this section, we present three prototypical such theorems.

Theorem 28. *Let A be a subset of the positive integers, let p be a prime number, and let l be a positive integer. Furthermore, let $\Pi_1(n; p, l, A)$ be the number of permutations of $\{1, 2, \dots, n\}$ whose cycle lengths are in*

$$\{ap^s : a \in A \text{ and } ap^s < p^l\}. \tag{8.2}$$

Then $\Pi_1(n;p,l,A)$ *is divisible by* $p^{e_p(n;l)}$, *where*

$$e_p(n;l)=\sum_{s=1}^{l-1}\left\lfloor\frac{n}{p^s}\right\rfloor-(l-1)\left\lfloor\frac{n}{p^l}\right\rfloor.$$

Proof. In (8.1), we set $x_i=1$ for all i in the set (8.2) and $x_i=0$ for all other i. It is then straightforward to see that all assumptions of Corollary 4 are satisfied. The assertion of the theorem then follows from (2.12). □

Clearly, the special case of Theorem 28 in which we consider permutations in S_n whose cycle lengths are powers p^s of a given prime number p, with $0\le s\le l$, corresponds to the enumeration of representations of C_{p^l} in S_n. Thus, Theorem 25 with $r=1$ — found earlier by Katsurada, Takegahara and Yoshida [10, Theorems 1.2] — is the simplest instance of the above theorem.

Another special case which is worth discussing explicitly is the case of permutations in S_n whose cycle lengths are strictly less than N, where N is some given positive integer. By application of Theorem 29, we conclude that the number of these permutations is divisible by

$$\prod_{\substack{p\le N\\ p\text{ prime}}}p^{\sum_{s=1}^{\lfloor\log_p N\rfloor-1}\lfloor n/p^s\rfloor-\left(\lfloor\log_p N\rfloor-1\right)\left\lfloor n/p^{\lfloor\log_p N\rfloor}\right\rfloor}.$$

Theorem 29. *Let A be a subset of the positive integers, let p be a prime number, and let l be a positive integer. Furthermore, let $\Pi_2(n;p,l,A)$ be the number of permutations of $\{1,2,\dots,n\}$ whose cycle lengths are in*

$$\{ap^s: a\in A\text{ and }ap^s\le p^l\}. \tag{8.3}$$

If $p\ge 3$ and $(p,l)\ne(3,1)$, the number $\Pi_2(n;p,l,A)$ is divisible by $p^{f_p(n;l)}$, where

$$f_p(n;l)=\sum_{s\ge1}\left\lfloor\frac{n}{p^s}\right\rfloor-(l-1)\left\lfloor\frac{n}{p^l}\right\rfloor-\sum_{s\ge l}\left\lfloor\frac{n}{2p^s}\right\rfloor,$$

while the number $\Pi_2(n;3,1,A)$ is divisible by $3^{f_3(n)}$, where

$$f_3(n)=\sum_{s\ge1}\left(\left\lfloor\frac{n}{3^s}\right\rfloor-\left\lfloor\frac{n}{2\cdot3^s}\right\rfloor\right)-\left\lfloor\frac{n}{18}\right\rfloor.$$

Finally, the number $\Pi_2(n;2,l,A)$ is divisible by $2^{f_2(n)}$, where

$$f_2(n)=\begin{cases}\left\lfloor\frac{n}{2}\right\rfloor-\left\lfloor\frac{n}{4}\right\rfloor & \textit{if } l=1,\\ \left\lfloor\frac{n}{2}\right\rfloor & \textit{if } l=2,\\ \sum_{s=1}^{l+1}\left\lfloor\frac{n}{2^s}\right\rfloor-(l-1)\left\lfloor\frac{n}{2^l}\right\rfloor & \textit{if } l\ge3.\end{cases}$$

Proof. This is completely analogous to the proof of Theorem 28. The only difference is that, instead of Corollary 4, one applies Theorems 7–9. □

Theorem 30. *Let A be a subset of the positive integers, let p be a prime number, and let l be a positive integer. Furthermore, let $\Pi_3(n;p,l,A)$ be the number of permutations of $\{1,2,\dots,n\}$ whose cycle lengths are in*

$$\{ap^s: a\in A\text{ and }ap^s<2p^l\}. \tag{8.4}$$

If $p \geq 3$ and $(p,l) \neq (3,1)$, the number $\Pi_3(n;p,l,A)$ is divisible by $p^{g_p(n;l)}$, where

$$g_p(n;l) = \sum_{s\geq 1} \left\lfloor \frac{n}{p^s} \right\rfloor - (l-1) \left\lceil \frac{n}{2p^l} \right\rceil - \sum_{s\geq l} \left\lfloor \frac{n}{2p^s} \right\rfloor .$$

Proof. This is completely analogous to the proof of Theorem 28. Here, we apply Theorem 12. □

9. A supercongruence

In the past few years it has become fashionable to call congruences modulo prime powers p^e, where the exponent e is at least 2, *"supercongruences"*. The specialisation of Corollary 4 where $s_1 = s_p = 1$ and all other s_n's are set equal to zero leads to such a congruence.[2]

Theorem 31. *For all primes p and positive integers a, b, c with $0 \leq b, c < p$, we have*

$$\sum_{s=0}^{pa+b} \frac{(p^2a+pb+c)!}{p^{pa+b-s}\,(pa+b-s)!\,(ps+c)!}$$
$$\equiv (-1)^a p^{(p-1)a} \sum_{s=0}^{b} \frac{(pb+c)!}{p^{b-s}\,(b-s)!\,(ps+c)!} \quad \left(\text{mod } p^{(p-1)a+b+1}\right). \quad (9.1)$$

Proof. Let $S(z) = z + \frac{z^p}{p}$ and $H(z) = \sum_{n\geq 0} \frac{h_n}{n!} z^n = \exp(S(z))$. Expansion of $H(z)$,

$$H(z) = \exp(z)\exp\left(\frac{z^p}{p}\right) = \sum_{s=0}^{\infty} \frac{z^s}{s!} \sum_{t=0}^{\infty} \frac{z^{pt}}{p^t\,t!},$$

and comparison of coefficients lead to

$$h_{p^2a+pb+c} = \sum_{s=0}^{pa+b} \frac{\left(p^2a+pb+c\right)!}{(ps+c)!\,p^{pa+b-s}\,\,(pa+b-s)!}. \quad (9.2)$$

Moreover, by Corollary 4 with $l = 2$ and $n = p^2a + pb + c$, we know that the p-adic valuation of $h_{p^2a+pb+c}$ is at least $(p-1)a + b$, and that the quotient $Q_{p^2a+pb+c} = h_{p^2a+pb+c}/p^{(p-1)a+b}$ satisfies

$$Q_{p^2a+pb+c} \equiv (-1)^a Q_{pb+c} \pmod p. \quad (9.3)$$

Hence, when both sides of (9.2) are reduced modulo $p^{(p-1)a+b+1}$, and (9.3) is used on the left-hand side, the result is (9.1). □

Remark. By taking more terms of the Artin–Hasse exponential $\sum_{n\geq 0} z^{p^n}/p^n$ (cf. [19, Sec. 7.2] for more information), the above theorem can be generalised to supercongruences for multisums.

[2]Since in the modulus of our congruence the exponent of p even grows with p, we are tempted to call this a "supersupercongruence," but refrain from doing so.

References

[1] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and Tree-Like Structures*, Cambridge University Press, Cambridge, 1998.

[2] L. M. Butler, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc.* **101** (1987), 771–776.

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

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

[5] A. W. M. Dress and T. Yoshida, On p-divisibility of the Frobenius numbers of symmetric groups, manuscript, 1991.

[6] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Sitz.ber. Königl.-Preuß. Adad. Wiss. Berlin*, 1895, 981–993.

[7] M. Grady and M. Newman, Some divisibility properties of the subgroup counting function for free products, *Math. Comput.* **58** (1992), 347–353.

[8] M. Grady and M. Newman, Residue periodicity in subgroup counting functions, in: The Rademacher Legacy in Mathematics, *Contemp. Math.* **166** (1994), 265–273.

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

[10] H. Katsurada, Y. Takegahara and T. Yoshida, *The number of homomorphisms from a finite abelian group to a symmetric group*, *Commun. Algebra* **28** (2000), 2271–2290.

[11] C. Krattenthaler and T. W. Müller, Parity patterns associated with lifts of Hecke groups, *Abh. Math. Semin. Univ. Hambg.* **78** (2008), 99–147.

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

[13] S. Lang, *Cyclotomic fields II*, Graduate Texts in Mathematics **69**, Springer–Verlag, 1980.

[14] A. M. Legendre, *Essai sur la théorie des nombres*, 2ed., Courcier, Paris, 1808.

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

[16] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd edition, Oxford University Press, New York/London, 1995.

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

[18] H. Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, *Hokkaido Math. J.* **28** (1999), 71–85.

[19] A. M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics, vol. 198, Springer–Verlag, New York, 2000.

[20] 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.