

Truncated versions of a lemma of Dwork and p -divisibility of arithmetic functions

Christian Krattenthaler and Thomas W. Müller

Universität Wien; Queen Mary, University of London

The number of involutions in S_n

Let I_n denote the number of permutations π with $\pi^2 = \text{id}$.

n	I_n
1	1
2	2
3	$4 = 2^2$
4	$10 = 2 \cdot 5$
5	$26 = 2 \cdot 13$
6	$76 = 2^2 \cdot 19$
7	$232 = 2^3 \cdot 29$
8	$764 = 2^2 \cdot 191$
9	$2620 = 2^2 \cdot 5 \cdot 131$
10	$9496 = 2^3 \cdot 1187$

The number of involutions in S_n

$$\begin{aligned} I_{100} &= 240533474383334789536224332430282328129641198 \backslash \\ &\quad 25419485684849162710512551427284402176 \\ &= 2^{25} \cdot 59 \cdot 616793 \cdot 5258867 \cdot 25964908703 \\ &\quad \cdot 144465705221072755757819 \\ &\quad \cdot 998597411042931968793034681 \end{aligned}$$

The number of “ p -volutions” in S_n

Let $I_n(p)$ denote the number of permutations π with $\pi^p = \text{id}$.

n	$I_n(5)$
5	5^2
10	$5^3 \cdot 17 \cdot 37$
15	$5^3 \cdot 577 \cdot 27197$
20	$5^4 \cdot 11 \cdot 73 \cdot 271 \cdot 1391381$
25	$5^4 \cdot 13 \cdot 281 \cdot 21893792600333$
30	$5^6 \cdot 6337 \cdot 297704663832071017$
35	$5^7 \cdot 29 \cdot 3691 \cdot 2973379 \cdot 1363570115322601$
40	$5^7 \cdot 61 \cdot 113 \cdot 567485839 \cdot 226086986570652945943$
45	$5^8 \cdot 523 \cdot 12893 \cdot 259150543 \cdot 341203128319 \cdot 996775402919$
50	$5^8 \cdot 1459 \cdot 211931 \cdot 299883046539737627 \cdot 33582096306940408147$

The number of “ p -volutions” in S_n

Let $I_n(p)$ denote the number of permutations π with $\pi^p = \text{id}$.

The number of “ p -volutions” in S_n

Let $I_n(p)$ denote the number of permutations π with $\pi^p = \text{id}$.

A fancy way to express $I_n(p)$ is the following:

$$I_n(p) = |\text{Hom}(C_p, S_n)|,$$

where C_N denotes the cyclic group with N elements.

Theorem (Katsurada, Takegahara, Yoshida)

Let C_N denote the cyclic group with N elements. Furthermore, for a finitely generated group G let $h_n(G) := |\text{Hom}(G, S_n)|$. Then

$$v_p(h_n(C_{p^\ell})) \geq \sum_{j=1}^{\ell} \left\lfloor \frac{n}{p^j} \right\rfloor - \ell \left\lfloor \frac{n}{p^{\ell+1}} \right\rfloor,$$

and the bound is sharp for $n \equiv 0 \pmod{p^{\ell+1}}$.

Here, $v_p(\alpha)$ denotes the p -adic valuation of α , i.e., the largest exponent e such that p^e divides α .

Theorem (Katsurada, Takegahara, Yoshida)

Let C_N denote the cyclic group with N elements. Furthermore, for a finitely generated group G let $h_n(G) := |\text{Hom}(G, S_n)|$. Then

$$v_p(h_n(C_{p^\ell})) \geq \sum_{j=1}^{\ell} \left\lfloor \frac{n}{p^j} \right\rfloor - \ell \left\lfloor \frac{n}{p^{\ell+1}} \right\rfloor,$$

and the bound is sharp for $n \equiv 0 \pmod{p^{\ell+1}}$.

Here, $v_p(\alpha)$ denotes the p -adic valuation of α , i.e., the largest exponent e such that p^e divides α .

In particular, for $\ell = 1$ we get

$$v_p(I_n(p)) \geq \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor.$$

Theorem (Katsurada, Takegahara, Yoshida)

Let C_N denote the cyclic group with N elements. Furthermore, for a finitely generated group G let $h_n(G) := |\text{Hom}(G, S_n)|$. Then, for $\ell \geq m$, we have

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

and the bound is sharp for $n \equiv 0 \pmod{p^{\ell+1}}$, except if $\ell = m$ and $p = 2$.

Theorem (Katsurada, Takegahara, Yoshida)

Let C_N denote the cyclic group with N elements. Furthermore, for a finitely generated group G let $h_n(G) := |\text{Hom}(G, S_n)|$. Then, for $\ell \geq m$, we have

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

and the bound is sharp for $n \equiv 0 \pmod{p^{\ell+1}}$, except if $\ell = m$ and $p = 2$.

What can one say about:

$$v_p(h_n(C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}})) ?$$

Let us return to the number I_n of involutions in S_n . Recall that

$$v_2(I_n) = v_2(h_n(C_2)) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor.$$

Let us return to the number I_n of involutions in S_n . Recall that

$$v_2(I_n) = v_2(h_n(C_2)) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor.$$

How to not prove this:

Let us return to the number I_n of involutions in S_n . Recall that

$$v_2(I_n) = v_2(h_n(C_2)) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor.$$

How to not prove this:

Everybody knows that

$$\sum_{n=0}^{\infty} I_n \frac{z^n}{n!} = \exp\left(z + \frac{z^2}{2}\right).$$

Consequently, by comparison of coefficients of $z^n/n!$:

$$I_n = \sum_{k \geq 0} \frac{n!}{2^k k! (n-2k)!}.$$

Let us return to the number I_n of involutions in S_n . Recall that

$$v_2(I_n) = v_2(h_n(C_2)) \geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor.$$

How to not prove this:

Everybody knows that

$$\sum_{n=0}^{\infty} I_n \frac{z^n}{n!} = \exp\left(z + \frac{z^2}{2}\right).$$

Consequently, by comparison of coefficients of $z^n/n!$:

$$I_n = \sum_{k \geq 0} \frac{n!}{2^k k! (n-2k)!}.$$

Now, we “just” have to analyse the 2-divisibility of this sum ...

How to actually do this:

How to actually do this:

Lemma (Dieudonné, Dwork)

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

$$H(z) = \exp(S(z)).$$

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

$$S(z^p) - pS(z) \in p\mathbb{Z}_p[[z]]. \quad (1)$$

How to actually do this:

Lemma (Dieudonné, Dwork)

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

$$H(z) = \exp(S(z)).$$

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

$$S(z^p) - pS(z) \in p\mathbb{Z}_p[[z]]. \quad (1)$$

What does it mean? Let $S(z) = \sum_{n \geq 1} \frac{s_n}{n} z^n$. The condition (1) says that:

- if $p \nmid n$, then $\frac{s_n}{n} \in \mathbb{Z}_p$;
- if $p \mid n$, then $\frac{1}{n}(s_{n/p} - s_n) \in \mathbb{Z}_p$.

How to actually do this:

Lemma (Dieudonné, Dwork)

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

$$H(z) = \exp(S(z)).$$

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

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

How to actually do this:

Lemma (Dieudonné, Dwork)

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

$$H(z) = \exp(S(z)).$$

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

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

Important special case: the *Artin–Hasse exponential*

$$\exp\left(z + \frac{z^p}{p} + \frac{z^{p^2}}{p^2} + \cdots\right)$$

has all its coefficients in \mathbb{Z}_p !

How to actually do this:

How to actually do this:

We have

$$\begin{aligned}\sum_{n=0}^{\infty} I_n \frac{z^n}{n!} &= \exp\left(z + \frac{z^2}{2}\right) \\ &= \exp\left(z + \frac{z^2}{2} + \frac{z^4}{4} + \dots\right) \\ &\quad \times \exp\left(-\frac{z^4}{4} - \frac{z^8}{8} - \dots\right) \\ &= \sum_{i_0=0}^{\infty} H_{i_0} z^{i_0} \times \exp\left(-\frac{z^4}{4} - \frac{z^8}{8} - \dots\right),\end{aligned}$$

with $H_{i_0} \in \mathbb{Z}_2$.

How to actually do this:

We have

$$\begin{aligned}\sum_{n=0}^{\infty} I_n \frac{z^n}{n!} &= \exp\left(z + \frac{z^2}{2}\right) \\ &= \exp\left(z + \frac{z^2}{2} + \frac{z^4}{4} + \dots\right) \\ &\quad \times \exp\left(-\frac{z^4}{4} - \frac{z^8}{8} - \dots\right) \\ &= \sum_{i_0=0}^{\infty} H_{i_0} z^{i_0} \times \exp\left(-\frac{z^4}{4} - \frac{z^8}{8} - \dots\right),\end{aligned}$$

with $H_{i_0} \in \mathbb{Z}_2$. Hence,

$$I_n = \sum_{i_0+4i_4+8i_8+\dots=n} H_{i_0} \frac{n! (-1)^{i_4+i_8+\dots}}{i_4! 4^{i_4} i_8! 8^{i_8} \dots}.$$

How to actually do this:

Hence,

$$I_n = \sum_{i_0+4i_4+8i_8+\dots=n} H_{i_0} \frac{n! (-1)^{i_4+i_8+\dots}}{i_4! 4^{i_4} i_8! 8^{i_8} \dots}$$

How to actually do this:

Hence,

$$I_n = \sum_{i_0+4i_4+8i_8+\dots=n} H_{i_0} \frac{n! (-1)^{i_4+i_8+\dots}}{i_4! 4^{i_4} i_8! 8^{i_8} \dots}$$

We now look at the 2-adic valuation of each summand individually. It is not difficult to see that “the worst that can happen” is in the case where i_4 is as large as possible, that is, $i_4 = \lfloor n/4 \rfloor$:

$$\begin{aligned} v_2 \left(H_{i_0} \frac{n! (-1)^{i_4+i_8+\dots}}{i_4! 4^{i_4} i_8! 8^{i_8} \dots} \right) &\geq v_2 \left(\frac{n!}{i_4! 4^{i_4} i_8! 8^{i_8} \dots} \right) \\ &\geq \sum_{\ell \geq 1} \left\lfloor \frac{n}{2^\ell} \right\rfloor - \sum_{\ell \geq 1} \left\lfloor \frac{n}{4 \cdot 2^\ell} \right\rfloor - 2 \left\lfloor \frac{n}{4} \right\rfloor \\ &\geq \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor. \end{aligned}$$

Back to our problem:

Theorem (Katsurada, Takegahara, Yoshida)

Let C_N denote the cyclic group with N elements. Furthermore, for a finitely generated group G let $h_n(G) := |\text{Hom}(G, S_n)|$. Then, for $\ell \geq m$, we have

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

and the bound is sharp for $n \equiv 0 \pmod{p^{\ell+1}}$, except if $\ell = m$ and $p = 2$.

What can one say about:

$$v_p(h_n(C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}})) ?$$

Back to our problem:

Theorem (Dey)

Let Γ be a finitely generated group, $h_n(\Gamma) := \text{Hom}(\Gamma, S_n)$, and let $s_n(\Gamma)$ be the number of subgroups of Γ of index n . Then

$$\sum_{n \geq 0} \frac{h_n(\Gamma)}{n!} z^n = \exp \left(\sum_{n \geq 1} \frac{s_n(\Gamma)}{n} z^n \right).$$

Back to our problem:

Theorem (Dey)

Let Γ be a finitely generated group, $h_n(\Gamma) := \text{Hom}(\Gamma, S_n)$, and let $s_n(\Gamma)$ be the number of subgroups of Γ of index n . Then

$$\sum_{n \geq 0} \frac{h_n(\Gamma)}{n!} z^n = \exp \left(\sum_{n \geq 1} \frac{s_n(\Gamma)}{n} z^n \right).$$

For example, in the case $\Gamma = C_{p^\ell}$ we have $s_{p^i}(\Gamma) = 1$ for $i = 0, 1, \dots, \ell$, and $s_n(\Gamma) = 0$ otherwise. Hence,

$$\sum_{n \geq 0} \frac{h_n(C_{p^\ell})}{n!} z^n = \exp \left(z + \frac{z^p}{p} + \frac{z^{p^2}}{p^2} + \dots + \frac{z^{p^\ell}}{p^\ell} \right).$$

Back to our problem:

Theorem (Dey)

Let Γ be a finitely generated group, $h_n(\Gamma) := \text{Hom}(\Gamma, S_n)$, and let $s_n(\Gamma)$ be the number of subgroups of Γ of index n . Then

$$\sum_{n \geq 0} \frac{h_n(\Gamma)}{n!} z^n = \exp \left(\sum_{n \geq 1} \frac{s_n(\Gamma)}{n} z^n \right).$$

For example, in the case $\Gamma = C_{p^\ell}$ we have $s_{p^i}(\Gamma) = 1$ for $i = 0, 1, \dots, \ell$, and $s_n(\Gamma) = 0$ otherwise. Hence,

$$\sum_{n \geq 0} \frac{h_n(C_{p^\ell})}{n!} z^n = \exp \left(z + \frac{z^p}{p} + \frac{z^{p^2}}{p^2} + \dots + \frac{z^{p^\ell}}{p^\ell} \right).$$

We see very well that this is a *truncated* Artin–Hasse exponential.

Theorem

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

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

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

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

and that

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

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

Then

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

for all n . If $s_{p^{l-1}} \not\equiv s_{p^l} \pmod{p^{m+1}\mathbb{Z}_p}$, then the bound is sharp for all $n \equiv 0 \pmod{p^l}$.

Then

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

for all n . If $s_{p^{l-1}} \not\equiv s_{p^l} \pmod{p^{m+1}\mathbb{Z}_p}$, then the bound is sharp for all $n \equiv 0 \pmod{p^l}$.

Idea of proof.

We write

$$S(z) = \tilde{S}(z) + R(z),$$

where $\tilde{S}(z)$ satisfies the Dieudonné–Dwork condition (1) and $R(z)$ is a series of order $O(z^{p^\ell})$. Subsequently, we decompose

$$H(z) = \exp(S(z)) = \exp(\tilde{S}(z)) \exp(R(z)).$$

By the lemma of Dieudonné and Dwork, we have $\exp(\tilde{S}(z)) \in \mathbb{Z}_p[[z]]$. It then remains to estimate the “error” created by $\exp(R(z))$.



Corollary

For a prime number p , let $S(z) = \sum_{n \geq 1} \frac{s_n}{n} z^n$ be a formal power series with $s_{p^e} \in \mathbb{Z}_p$ for all non-negative integers e and $s_n = 0$ otherwise, 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

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

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

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

and

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

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

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

for all n . If $s_{p^{l-1}} \not\equiv s_{p^l} \pmod{p^{m+1} \mathbb{Z}_p}$, then the bound is sharp for all $n \equiv 0 \pmod{p^l}$.

Back to our problem:

Theorem (Dey)

Let Γ be a finitely generated group, $h_n(\Gamma) := \text{Hom}(\Gamma, S_n)$, and let $s_n(\Gamma)$ be the number of subgroups of Γ of index n . Then

$$\sum_{n \geq 0} \frac{h_n(\Gamma)}{n!} z^n = \exp \left(\sum_{n \geq 1} \frac{s_n(\Gamma)}{n} z^n \right).$$

Back to our problem:

Theorem (Dey)

Let Γ be a finitely generated group, $h_n(\Gamma) := \text{Hom}(\Gamma, S_n)$, and let $s_n(\Gamma)$ be the number of subgroups of Γ of index n . Then

$$\sum_{n \geq 0} \frac{h_n(\Gamma)}{n!} z^n = \exp \left(\sum_{n \geq 1} \frac{s_n(\Gamma)}{n} z^n \right).$$

We have to control the p -adic valuation of the numbers $s_n(G)$ of subgroups of index n in G !

Proposition

Let $G = C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}}$ with $a_1 \geq a_2 \geq \cdots \geq a_r$. Then the number of subgroups in G of type (b_1, b_2, \dots, b_r) (i.e., those isomorphic to $C_{p^{b_1}} \times C_{p^{b_2}} \times \cdots \times C_{p^{b_r}}$ with $b_1 \geq b_2 \geq \cdots \geq b_r$) equals

$$\prod_{i \geq 1} p^{b'_{i+1}(a'_i - b'_i)} \begin{bmatrix} a'_i - b'_{i+1} \\ b'_i - b'_{i+1} \end{bmatrix}_p.$$

Here,

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \frac{(1 - p^n)(1 - p^{n-1}) \cdots (1 - p^{n-k+1})}{(1 - p^k)(1 - p^{k-1}) \cdots (1 - p)}.$$

Proposition (Butler)

Let $G = C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}}$ with $a_1 \geq a_2 \geq \cdots \geq a_r$. Then

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

where $K_{\lambda, \mu}(t)$ denotes the Kostka–Foulkes polynomial indexed by partitions λ and μ , and where $\alpha = (a_1, a_2, \dots, a_r)$,

$A_1 = (a_1 + a_2 + \cdots + a_r)/2$, and $n(\alpha) = \sum_{i=1}^r (i-1)a_i$.

The *Hall–Littlewood polynomials* $P_\lambda(x_1, \dots, x_n; t)$ are defined by

$$P_\lambda(x_1, \dots, x_n; t) = \frac{1}{v_\lambda(t)} \sum_{w \in S_n} w \left(x_1^{\lambda_1} \cdots x_n^{\lambda_n} \prod_{1 \leq i < j} \frac{x_i - tx_j}{x_i - x_j} \right),$$

where

$$v_\lambda(t) = \prod_{i \geq 1} \prod_{j=1}^{m_i} \frac{1-t^j}{1-t}$$

given that $\lambda = (1^{m_1}, 2^{m_2}, \dots)$.

The *Kostka–Foulkes polynomials* $K_{\lambda,\nu}(t)$ are the coefficients when *Schur functions* $s_{\lambda}(x_1, \dots, x_n)$ are expanded in terms of *Hall–Littlewood polynomials*:

$$s_{\lambda}(x_1, \dots, x_n) = \sum_{\mu} K_{\lambda,\mu}(t) P_{\nu}(x_1, \dots, x_n; t).$$

Here,

$$s_{\lambda}(x_1, \dots, x_n) = \det_{1 \leq i, j \leq r} (h_{\lambda_i - i + j}(x_1, \dots, x_n)),$$

with

$$h_m(x_1, \dots, x_n) = \sum_{1 \leq i_1 \leq i_2 \leq \dots \leq i_m \leq n} x_{i_1} x_{i_2} \cdots x_{i_m}.$$

The Hall–Littlewood polynomials satisfy:

- $P_\mu(\mathbf{x}; t)P_\nu(\mathbf{x}; t) = \sum_\lambda t^{n(\lambda)-n(\mu)-n(\nu)} g_{\mu,\nu}^\lambda(t^{-1})P_\lambda(\mathbf{x}; t)$, where $g_{\mu,\nu}^\lambda(p)$ is the number of subgroups H in a finite Abelian p -group G of type λ , such that H is of type μ and G/H is of type ν ;
- $h_n(\mathbf{x}) = \sum_\lambda t^{n(\lambda)}P_\lambda(\mathbf{x}; t)$;
- $K_{\lambda,\mu}(t) = 0$ unless μ is less than or equal to λ in dominance order;
- in the latter case, $K_{\lambda,\mu}(t)$ is a monic polynomial in t of degree $n(\lambda) - n(\mu)$.

Theorem

Let $G = C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_r}}$ with $a_1 \geq a_2 \geq \cdots \geq a_r$.

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

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

The bound is sharp for all $n \equiv 0 \pmod{p^{a_1+1}}$.

(ii) If $a_1 \leq a_2 + \cdots + a_r$ and $a_1 + a_2 + \cdots + a_r$ is even, then

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

where $A_1 = (a_1 + a_2 + \cdots + a_r)/2$. The bound is sharp for all $n \equiv 0 \pmod{p^{A_1+1}}$, except if $p = 2$.

(iii) If $a_1 \leq a_2 + \cdots + a_r$ and $a_1 + a_2 + \cdots + a_r$ is odd, then

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

where $A_2 = (a_1 + a_2 + \cdots + a_r + 1)/2$. The bound is sharp for all $n \equiv 0 \pmod{p^{A_2+1}}$.

Theorem

Let $G = C_{2^{a_1}} \times C_{2^{a_2}} \times \cdots \times C_{2^{a_r}}$ with $a_1 \geq a_2 \geq \cdots \geq a_r$, $a_1 \leq a_2 + \cdots + a_r$, and $a_1 + a_2 + \cdots + a_r$ being even. Then

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

where $A_1 = (a_1 + a_2 + \cdots + a_r)/2$. The bound is sharp for all n congruent to 0, 2^{A_1+1} , and 2^{A_1+2} modulo 2^{A_1+3} .