On the factorization numbers of some finite $p$-groups

Marius Tărnăuceanu

February 17, 2015

Abstract

This note deals with the computation of the factorization number $F_2(G)$ of a finite group $G$. By using the Möbius inversion formula, explicit expressions of $F_2(G)$ are obtained for two classes of finite abelian groups, improving the results of Factorization numbers of some finite groups, Glasgow Math. J. (2012).

MSC (2010): Primary 20D40; Secondary 20D60.
Key words: factorization number, subgroup commutativity degree, Möbius function, finite abelian group.

1 Introduction

Let $G$ be a group, $L(G)$ be the subgroup lattice of $G$ and $H$, $K$ be two subgroups of $G$. If $G = HK$, then $G$ is said to be factored by $H$ and $K$ and the expression $G = HK$ is said to be a factorization of $G$. Denote by $F_2(G)$ the factorization number of $G$, that is the number of all factorizations of $G$.

The starting point for our discussion is given by the paper [3], where $F_2(G)$ has been computed for certain classes of finite groups. The connection between $F_2(G)$ and the subgroup commutativity degree $sd(G)$ of $G$ (see [5, 7]) has been also established, namely

$$sd(G) = \frac{1}{|L(G)|^2} \sum_{H \leq G} F_2(H).$$
Obviously, by applying the well-known Möbius inversion formula to the above equality, one obtains

\[ F_2(G) = \sum_{H \leq G} sd(H) |L(H)|^2 \mu(H, G). \] (1)

In particular, if \( G \) is abelian, then we have \( sd(H) = 1 \) for all \( H \in L(G) \), and consequently

\[ F_2(G) = \sum_{H \leq G} |L(H)|^2 \mu(H, G) = \sum_{H \leq G} |L(G/H)|^2 \mu(H). \] (2)

This formula will be used in the following to calculate the factorization numbers of an elementary abelian \( p \)-group and of a rank 2 abelian \( p \)-group, improving Theorem 1.2 and Corollary 2.5 of [3]. An interesting conjecture about the maximum value of \( F_2(G) \) on the class of \( p \)-groups of the same order will be also presented.

First of all, we recall a theorem due to P. Hall [1] (see also [2]), that permits us to compute explicitly the Möbius function of a finite \( p \)-group.

**Theorem 1.** Let \( G \) be a finite \( p \)-group of order \( p^n \). Then \( \mu(G) = 0 \) unless \( G \) is elementary abelian, in which case we have \( \mu(G) = (-1)^n p^\binom{n}{2} \).

In contrast with Theorem 1.2 of [3] that gives only a recurrence relation satisfied by \( F_2(\mathbb{Z}_p^n), n \in \mathbb{N} \), we are able to determine precise expressions of these numbers.

**Theorem 2.** We have

\[ F_2(\mathbb{Z}_p^n) = \sum_{i=0}^{n} (-1)^i a_{n,p}(i) a_{n-i,p}^2 p^\binom{i}{2}, \] (3)

where \( a_{n,p}(i) \) is the number of subgroups of order \( p^i \) of \( \mathbb{Z}_p^n \), \( a_{n,p} \) is the total number of subgroups of \( \mathbb{Z}_p^n \), and, by convention, \( \binom{i}{2} = 0 \) for \( i = 0, 1 \).

Since the numbers \( a_{n,p}(i), i = 0, 1, \ldots, n \), are well-known, namely

\[ a_{n,p}(i) = \frac{(p^n - 1) \cdots (p - 1)}{(p^i - 1) \cdots (p - 1)(p^{n-i} - 1) \cdots (p - 1)}, \]

the equality (3) easily leads to the following values of \( F_2(\mathbb{Z}_p^n) \) for \( n = 1, 2, 3, 4 \).
Examples.

a) $F_2(\mathbb{Z}_p) = 3$.

b) $F_2(\mathbb{Z}_p^2) = p^2 + 3p + 5$.

c) $F_2(\mathbb{Z}_p^3) = 3p^4 + 4p^3 + 8p^2 + 5p + 7$.

d) $F_2(\mathbb{Z}_p^4) = p^8 + 3p^7 + 9p^6 + 11p^5 + 14p^4 + 15p^3 + 12p^2 + 23p + 9$.

Next we compute the factorization number of a rank 2 abelian $p$-group.

**Theorem 3.** The factorization number of the finite abelian $p$-group $\mathbb{Z}_{p^\alpha_1} \times \mathbb{Z}_{p^\alpha_2}$, $\alpha_1 \leq \alpha_2$, is given by the following equality:

$$F_2(\mathbb{Z}_{p^\alpha_1} \times \mathbb{Z}_{p^\alpha_2}) = \frac{1}{(p-1)^4} \left[ (2\alpha_2 - 2\alpha_1 + 1)p^{2\alpha_1+4} - (6\alpha_2 - 6\alpha_1 + 1)p^{2\alpha_1+3} + (6\alpha_2 - 6\alpha_1 - 1)p^{2\alpha_1+2} - (2\alpha_2 - 2\alpha_1 - 1)p^{2\alpha_1+1} - (2\alpha_1 + 2\alpha_2 + 3)p^3 + (6\alpha_1 + 6\alpha_2 + 7)p^2 - (6\alpha_1 + 6\alpha_2 + 5)p + (2\alpha_1 + 2\alpha_2 + 1) \right].$$

We remark that Theorem 3 gives a generalization of Corollary 2.5 of [3]. Indeed, by taking $\alpha_1 = 1$ and $\alpha_2 = n$ in the above formula, one obtains:

**Corollary 4.** $F_2(\mathbb{Z}_p \times \mathbb{Z}_p^n) = (2n - 1)p^2 + (2n + 1)p + (2n + 3)$.

Finally, we will focus on the minimum/maximum of $F_2(G)$ when $G$ belongs to the class of $p$-groups of order $p^n$. It is easy to see that

$$2n + 1 = F_2(\mathbb{Z}_p^n) \leq F_2(G).$$

For $n \leq 3$ the greatest value of $F_2(G)$ is obtained for $G \cong \mathbb{Z}_p^n$, as shows the following result.

**Theorem 5.** Let $G$ be a finite $p$-group of order $p^n$. If $n \leq 3$, then

$$F_2(G) \leq F_2(\mathbb{Z}_p^n).$$

Inspired by Theorem 5, we came up with the following conjecture, which we also have verified for several $n \geq 4$ and particular values of $p$. 

3
Conjecture 6. For every finite $p$-group $G$ of order $p^n$, we have
\[ F_2(G) \leq F_2(\mathbb{Z}^n_p). \]

We end our note by indicating a natural problem concerning the factorization number of abelian $p$-groups.

**Open problem.** Compute explicitly $F_2(G)$ for an arbitrary finite abelian $p$-group $G$. Given a positive integer $n$, two partitions $\tau, \tau'$ of $n$ and denoting by $G, G'$ the abelian $p$-groups of order $p^n$ induced by $\tau$ and $\tau'$, respectively, is it true that $F_2(G) \geq F_2(G')$ if and only if $\tau \preceq \tau'$ (where $\preceq$ denotes the lexicographic order)?

## 2 Proofs of the main results

**Proof of Theorem 2.** By using Theorem 1 in (2), it follows that
\[
F_2(\mathbb{Z}^n_p) = \sum_{H \leq \mathbb{Z}^n_p} |L(\mathbb{Z}^n_p/H)|^2 \mu(H) = \sum_{i=0}^{n} \sum_{\substack{H \leq \mathbb{Z}^n_p \atop |H|=p^i}} |L(\mathbb{Z}^n_p/H)|^2 \mu(H) =
\]
\[
= \sum_{i=0}^{n} a_{n,p}(i) |L(\mathbb{Z}^{n-i}_p)|^2 (-1)^i p^{i(z)} = \sum_{i=0}^{n} (-1)^i a_{n,p}(i) a_{n-i,p}^2 p^{i(z)},
\]
as desired. $
$

**Proof of Theorem 3.** It is well-known that $G = \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ has a unique elementary abelian subgroup of order $p^2$, say $M$, and that
\[
G/M \cong \mathbb{Z}_{p^{\alpha_1-1}} \times \mathbb{Z}_{p^{\alpha_2-1}}.
\]

Moreover, all elementary abelian subgroups of $G$ are contained in $M$. Denote by $M_i, i = 1, 2, ..., p + 1$, the minimal subgroups of $G$. Then every quotient $G/M_i$ is isomorphic to a maximal subgroup of $G$ and therefore we may assume that
\[
G/M_i \cong \mathbb{Z}_{p^{\alpha_1-1}} \times \mathbb{Z}_{p^{\alpha_2}} \text{ for } i = 1, 2, ..., p
\]
and

\[ G/M_{p+1} \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2-1}}. \]

Clearly, the equality (2) becomes

\[ F_2(G) = \mid L(G/M) \mid^2 \mu(M) + \sum_{i=1}^{p+1} \mid L(G/M_i) \mid^2 \mu(M_i) + \mid L(G) \mid^2 \mu(1), \]

in view of Theorem 1. Since by Theorem 2 we have \( \mu(M) = \mu(\mathbb{Z}_p^2) = p \), \( \mu(M_i) = \mu(\mathbb{Z}_p) = -1 \), for all \( i = 1, p + 1 \), and \( \mu(1) = 1 \), one obtains

\[ F_2(G) = p \mid L(\mathbb{Z}_{p^{\alpha_1-1}} \times \mathbb{Z}_{p^{\alpha_2-1}}) \mid^2 - p \mid L(\mathbb{Z}_{p^{\alpha_1-1}} \times \mathbb{Z}_{p^{\alpha_2}}) \mid^2 - \mid L(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2-1}}) \mid^2 + \mid L(\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}) \mid^2. \]

The total number of subgroups of \( \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \) has been computed in Theorem 3.3 of [6], namely

\[ \frac{1}{(p-1)^2} \left[ (\alpha_2-\alpha_1+1)p^{\alpha_1+2} - (\alpha_2-\alpha_1-1)p^{\alpha_1+1} - (\alpha_1+\alpha_2+3)p + (\alpha_1+\alpha_2+1) \right]. \]

Then the desired formula follows immediately by a direct calculation in the right side of (4).

**Proof of Theorem 5.** For \( n = 2 \) we obviously have

\[ F_2(\mathbb{Z}_{p^2}) = 5 < F_2(\mathbb{Z}_p^2) = p^2 + 3p + 5. \]

For \( n = 3 \) it is well-known (see e.g. (4.13), [III], II) that \( G \) can be one of the following groups:

- \( \mathbb{Z}_2^3, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8, D_8 \) and \( Q_8 \) if \( p = 2 \);
- \( \mathbb{Z}_p^3, \mathbb{Z}_p \times \mathbb{Z}_{p^2}, \mathbb{Z}_p \), \( M(p^3) = \langle x, y \mid x^{p^2} = y^p = 1, y^{-1}xy = x^{p+1} \rangle \) and \( E(p^3) = \langle x, y \mid x^p = y^p = [x, y]^p = 1, [x, y] \in Z(E(p^3)) \rangle \) if \( p \geq 3 \).

By using the results in Section 2 of [III], one obtains

for \( p = 2 \):

\[ F_2(\mathbb{Z}_2^3) = 129 > F_2(\mathbb{Z}_2 \times \mathbb{Z}_4) = 29, F_2(\mathbb{Z}_8) = 7, F_2(D_8) = 41, F_2(Q_8) = 17 \]
and

\[ F_2(\mathbb{Z}_p^3) = 3p^4 + 4p^3 + 8p^2 + 5p + 7 > F_2(\mathbb{Z}_p \times \mathbb{Z}_p^2) = F_2(M(p^3)) = 3p^2 + 5p + 7, \]
\[ F_2(\mathbb{Z}_p^3) = 7. \]

We also observe that \( E(p^3) \) has \( p + 1 \) elementary abelian subgroups of order \( p^2 \), say \( M_1, M_2, \ldots, M_{p+1} \), and that every \( M_i \) contains \( p + 1 \) subgroups of order \( p \), namely \( \Phi(E(p^3)) \) and \( M_{ij}, j = 1, 2, \ldots, p \). Then \( |L(E(p^3))| = p^2 + 2p + 4 \) and so

\[ F_2(E(p^3)) < |L(E(p^3))|^2 = p^4 + 4p^3 + 12p^2 + 16p + 16. \]

On the other hand, we can easily see that this quantity is less than \( F_2(\mathbb{Z}_p^3) \) for all primes \( p \geq 3 \), completing the proof.

**Remark.** It is clear that an explicit formula for \( F_2(E(p^3)) \) cannot be obtained by applying (2), but we are able to determine it by a direct computation. The factorization pairs of \( E(p^3) \) are:

- \((1, E(p^3)), (E(p^3), 1)\);
- \((M_{ij}, M_{ij'}) \forall i' \neq i, (M_{ij}, E(p^3)), (E(p^3), M_{ij}), i = \overline{1, p+1}, j = \overline{1, p};\)
- \((\Phi(E(p^3)), E(p^3)), (E(p^3), \Phi(E(p^3)));\)
- \((M_i, M_{ij'}) \forall i' \neq i, j = 1, 2, \ldots, p, (M_i, M_{ij'}) \forall i' \neq i, (M_i, E(p^3)) \) and \((M_i, E(p^3)), i = \overline{1, p+1};\)
- \((E(p^3), E(p^3)).\)

Hence

\[ F_2(E(p^3)) = 2 + p(p+1)(p+2) + 2 + (p+1)(p^2 + p + 2) + 1 = \]
\[ = 2p^3 + 5p^2 + 5p + 7. \]

**Acknowledgements.** The author is grateful to the reviewer for its remarks which improve the previous version of the paper.
References

[1] Hall, P., *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1933), 29-95.

[2] Hawkes, T., Isaacs, I.M., Özyaydin, M., *On the Möbius function of a finite group*, Rocky Mountain J. Math. **19** (1989), 1003-1033.

[3] Saeedi, F., Farrokhi D.G., M., *Factorization numbers of some finite groups*, to appear in Glasgow Math. J. (2012).

[4] Suzuki, M., *Group theory*, I, II, Springer Verlag, Berlin, 1982, 1986.

[5] Tărnăuceanu, M., *Subgroup commutativity degrees of finite groups*, J. Algebra **321** (2009), 2508-2520, doi: 10.1016/j.jalgebra.2009.02.010.

[6] Tărnăuceanu, M., *An arithmetic method of counting the subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **53/101** (2010), 373-386.

[7] Tărnăuceanu, M., *Addendum to "Subgroup commutativity degrees of finite groups"*, J. Algebra **337** (2011), 363-368, doi: 10.1016/j.jalgebra.2011.05.001.

Marius Tărnăuceanu
Faculty of Mathematics
“Al.I. Cuza” University
Iași, Romania
e-mail: tarnauc@uaic.ro