Georgiana Fasolă; Marius Tărnăuceanu

On a group-theoretical generalization of the Gauss formula

Czechoslovak Mathematical Journal, Vol. 73 (2023), No. 1, 311–317

Persistent URL: `http://dml.cz/dmlcz/151519`

Czechoslovak Mathematical Journal, 73 (148) (2023), 311–317

ON A GROUP-THEORETICAL GENERALIZATION OF THE GAUSS FORMULA

Georgiana Fasolă, Marius Tărnăuceanu, Iaşi

Received May 28, 2022. Published online December 15, 2022.

Abstract. We discuss a group-theoretical generalization of the well-known Gauss formula involving the function that counts the number of automorphisms of a finite group. This gives several characterizations of finite cyclic groups.

Keywords: Gauss formula; Euler's totient function; automorphism group; finite group; cyclic group; abelian group

MSC 2020: 20D60, 11A25, 20D99, 11A99

1. Introduction

Euler's totient function (or, simply, the *totient function*) φ is one of the most famous functions in number theory. The totient $\varphi(n)$ of a positive integer n is defined to be the number of positive integers less than or equal to n that are coprime to n. In algebra this function is important mainly because it gives the order of the group of units in the ring $(\mathbb{Z}_n,+,\cdot)$. Also, $\varphi(n)$ can be seen as the number of generators or as the number of automorphisms of the cyclic group $(\mathbb{Z}_n,+)$. Note that there exist a lot of identities involving the totient function. One of them is the *Gauss formula*

$$\sum_{d\mid n}\varphi(d)=n\quad\forall\,n\in\mathbb{N}^*. \tag{1.1}$$

In the last years there has been a growing interest in extending arithmetical notions to finite groups, see, e.g., [1], [2], [6], [7], [13], [14]. Following this trend, we remark that (1.1) can be rewritten as

$$\sum_{H\leqslant\mathbb{Z}_n}|\mathrm{Aut}(H)|=|\mathbb{Z}_n|\quad\forall\,n\in\mathbb{N}^*.$$

DOI: 10.21136/CMJ.2022.0225-22

It suggests us to consider the functions

$$S(G) = \sum_{H \leqslant G} |\mathrm{Aut}(H)| \quad \text{and} \quad f(G) = \frac{S(G)}{|G|}$$

for any finite group G. Thus, the classical Gauss formula becomes

$$f(\mathbb{Z}_n) = 1 \quad \forall\, n \in \mathbb{N}^*. \tag{1.2}$$

The main goal of our paper is to study the above function f. We start by observing that it is multiplicative, i.e., if G_i, $i = 1, 2, \ldots, m$, are finite groups of coprime orders, then we have

$$f\left(\prod_{i=1}^{m} G_i\right) = \prod_{i=1}^{m} f(G_i).$$

This implies that the computation of $f(G)$ for a finite nilpotent group G is reduced to p-groups.

Our first theorem shows that the cyclic groups are in fact the unique groups satisfying (1.2).

Theorem 1.1. *Let G be a finite group. Then $f(G) \geqslant 1$, and we have equality if and only if G is cyclic.*

The above theorem leads to the following natural question:

Is there a minimum of f on the class of finite noncyclic groups?

In what follows, we give some partial answers to this question by finding the constant c for several particular classes of finite noncyclic groups.

Proposition 1.2. *For any finite noncyclic group G, we have*

$$f(G) \geqslant 1 + \frac{1}{|Z(G)|}.$$

In particular, if G is centerless, then $f(G) \geqslant 2$.

Note that Proposition 1.2 implies

$$f(G) \geqslant 1 + \frac{4}{|G|}$$

for any finite nonabelian group G. Also, by the proof of Proposition 2.1, we infer that small values of $f(G)$ are obtained for finite noncyclic groups G with many cyclic subgroups. This leads to the next proposition. We recall that a finite group G is called a *minimal noncyclic group* if G is not cyclic, but all proper subgroups of G are cyclic.

Proposition 1.3. *Let G be a finite minimal noncyclic group. Then $f(G) \geqslant 2$, and we have equality if and only if $G \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_{2^n}$, $n \in \mathbb{N}^*$.*

The following theorem shows that the constant c can be taken $\frac{5}{2}$ for finite abelian groups.

Theorem 1.4. *Let G be a finite noncyclic abelian group. Then $f(G) \geqslant \frac{5}{2}$, and we have equality if and only if $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_n$, where n is an odd positive integer.*

Inspired by the above results, we came up with the following conjecture, which we have verified by computer for many classes of finite groups.

Conjecture 1.5. *If 2 is the second smallest value of the function f.*

For the proof of Theorem 1.4, we will need to know the number of automorphisms of a finite abelian p-group. This has been explicitly computed e.g., in [3], [9], [12].

Theorem 1.6. *Let $G \cong \prod_{i=1}^{k} \mathbb{Z}_{p^{n_i}}$ be a finite abelian p-group, where $1 \leqslant n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$. Then*

$$|\mathrm{Aut}(G)| = \prod_{i=1}^{k}(p^{a_i} - p^{i-1}) \prod_{u=1}^{k} p^{n_u(k-a_u)} \prod_{v=1}^{k} p^{(n_v-1)(k-b_v+1)}, \tag{1.3}$$

where

$$a_r = \max\{s\colon\ n_s = n_r\} \quad \text{and} \quad b_r = \min\{s\colon\ n_s = n_r\}, \quad r = 1, 2, \ldots, k.$$

In particular, for $k = 2$, we have

$$|\mathrm{Aut}(G)| = (p-1)^2(p+1)^{[n_1/n_2]}p^{3n_1+n_2-[n_1/n_2]-2}. \tag{1.4}$$

We end this paper by indicating a list of open problems concerning our previous results.

Problem 1.1. Determine all finite groups G such that $f(G) = 2$.

Problem 1.2. Find the minimum of f on the class of finite noncyclic p-groups.

Problem 1.3. Is $\mathrm{Im}(f)$ dense in the interval $[2, \infty)$?

Since $f(D_{2n}) = \frac{1}{2}(n+1)$ for any odd integer $n \geqslant 3$, it follows that $\mathbb{N}^* \subseteq \mathrm{Im}(f)$. Thus, the function f takes arbitrarily large values.

Most of our notation is standard and will usually not be repeated here. For basic notions and results on groups we refer the reader to [10].

2. Proof of the main results

First of all, we prove Theorem 1.1.

Proof of Theorem 1.1. Let $C(G)$ be the poset of cyclic subgroups of G. For every divisor d of $|G|$, we denote by n_d the number of cyclic subgroups of order d of G and by n'_d the number of elements of order d in G. Then we have

$$n'_d = n_d\varphi(d)$$

because a cyclic subgroup of order d contains $\varphi(d)$ elements of order d. One obtains

$$\begin{aligned} S(G) &= \sum_{H\leqslant G} |\mathrm{Aut}(H)| \geqslant \sum_{H\in C(G)} |\mathrm{Aut}(H)| = \sum_{H\in C(G)} \varphi(|H|) \\ &= \sum_{d\mid n} \sum_{H\in C(G),\ |H|=d} \varphi(d) = \sum_{d\mid n} n_d\varphi(d) = \sum_{d\mid n} n'_d = |G|, \end{aligned}$$

which shows that $f(G) \geqslant 1$. Moreover, we have equality if and only if $C(G) = L(G)$, i.e., if and only if G is cyclic, as desired. □

Proof of Proposition 1.2. By the proof of Theorem 1.1, it follows that

$$f(G) = 1 + \frac{1}{|G|} \sum_{H\notin C(G)} |\mathrm{Aut}(H)|$$

for any finite group G. If G is noncyclic, then we get

$$f(G) \geqslant 1 + \frac{|\mathrm{Aut}(G)|}{|G|} \geqslant 1 + \frac{|\mathrm{Inn}(G)|}{|G|} = 1 + \frac{1}{|Z(G)|}$$

as desired. □

Note that the ratio $r(G) = |\mathrm{Aut}(G)|/|G|$ is $\geqslant 1$ for many classes of finite groups G. However, there are examples of finite groups G with $Z(G) \neq 1$, but of arbitrarily small $r(G)$, see, e.g., [4], [5], [8].

Proof of Proposition 1.3. By a classical result of Miller and Moreno (see [11]), a finite minimal noncyclic group is of one of the following types:

(1) $\mathbb{Z}_p \times \mathbb{Z}_p$, where p is a prime;

(2) Q_8;

(3) $\langle a, b\colon a^p = b^{q^n} = 1,\ b^{-1}ab = a^r\rangle$, where p, q are distinct primes and $r \not\equiv 1 \pmod p$, $r^q \equiv 1 \pmod p$.

For these groups we easily obtain:

(1) $f(\mathbb{Z}_p \times \mathbb{Z}_p) = 1 + (p+1)(p-1)^2/p > 2$ for all primes p,
(2) $f(Q_8) = 4 > 2$,
(3) $f(\langle a, b\colon\ a^p = b^{q^n} = 1,\ b^{-1}ab = a^r\rangle) = 1 + (p-1)/q \geqslant 2$ because $q \mid p-1$.

Moreover, we have $f(G) = 2$ if and only if G is of type 3 and $p = 3$, $q = 2$, i.e., if and only if $G \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_{2^n}$, $n \in \mathbb{N}^*$. This completes the proof. □

Before proving Theorem 1.4, we establish two auxiliary results.

Lemma 2.1. *Let G be a noncyclic abelian p-group of order p^n. Then* $|\mathrm{Aut}(G)| \geqslant p^n(p-1)^2$.

Proof. Let $G \cong \prod_{i=1}^{k} \mathbb{Z}_{p^{n_i}}$, where $k \geqslant 2$ and $1 \leqslant n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$. For $k = 2$, we have

$$\begin{aligned}|\mathrm{Aut}(G)| &= (p-1)^2(p+1)^{[n_1/n_2]}p^{3n_1+n_2-[n_1/n_2]-2} \geqslant (p-1)^2 p^{3n_1+n_2-2}\\ &\geqslant (p-1)^2 p^{n_1+n_2}\end{aligned}$$

by (1.4). For $k \geqslant 3$, we use the general formula (1.3). Observe that

$$i \leqslant a_i \leqslant k \quad \text{and} \quad 1 \leqslant b_i \leqslant i \quad \forall\, i = 1, 2, \ldots, k.$$

Then

$$\begin{aligned}|\mathrm{Aut}(G)| &= \prod_{i=1}^{k}(p^{a_i} - p^{i-1}) \prod_{u=1}^{k} p^{n_u(k-a_u)} \prod_{v=1}^{k} p^{(n_v-1)(k-b_v+1)}\\ &\geqslant \prod_{i=1}^{k}(p^{i} - p^{i-1}) \prod_{v=1}^{k} p^{(n_v-1)(k-v+1)} = (p-1)^k p^S,\end{aligned}$$

where

$$S = \sum_{i=1}^{k}[i - 1 + (n_i - 1)(k - i + 1)] = (n_1 - 1)k + \sum_{i=2}^{k} n_i(k - i + 1).$$

Since $(p-1)^k > (p-1)^2$, it suffices to show that

$$S \geqslant n_1 + n_2 + \ldots + n_k,$$

which is equivalent to

$$\sum_{i=1}^{k-1} n_i(k-i) \geqslant k.$$

This is true because for $k \geqslant 3$ we have

$$\sum_{i=1}^{k-1} n_i(k-i) \geqslant \sum_{i=1}^{k-1}(k-i) = \frac{k(k-1)}{2} \geqslant k,$$

completing the proof. □

Corollary 2.2. *Let G be a finite abelian group. Then $|\mathrm{Aut}(G)| \geqslant \varphi(|G|)$, and we have equality if and only if G is cyclic.*

P r o o f. Obviously, the result is reduced to finite abelian p-groups. If G is a noncyclic abelian p-group of order p^n, then Lemma 2.1 leads to

$$|\mathrm{Aut}(G)| \geqslant p^n(p-1)^2 > p^{n-1}(p-1) = \varphi(|G|).$$

The proof is completed by the well-known fact that $|\mathrm{Aut}(G)| = \varphi(|G|)$ for all finite cyclic groups G. □

We are now able to prove Theorem 1.4.

P r o o f of Theorem 1.4. Let $G \cong \prod_{i=1}^{m} G_i$ be the decomposition of G as a direct product of abelian p-groups. Then

$$f(G) = \prod_{i=1}^{m} f(G_i).$$

Since G is not cyclic, at least one of the groups G_i, $i = 1, 2, \ldots, m$, is not cyclic. On the other hand, we already know that $f(G_i) \geqslant 1$ for all i by Theorem 1.1. This shows that it suffices to prove the inequality $f(G) \geqslant \frac{5}{2}$ for noncyclic abelian p-groups.

Assume that $G \cong \prod_{i=1}^{k} \mathbb{Z}_{p^{n_i}}$ is an abelian p-group, where $k \geqslant 2$ and $1 \leqslant n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$. By induction on $n = n_1 + n_2 + \ldots + n_k$, we prove that

$$f(G) \geqslant 1 + \frac{(p+1)(p-1)^2}{p}. \tag{2.1}$$

For $n = 2$, we have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and so

$$f(G) = 1 + \frac{|\mathrm{Aut}(G)|}{|G|} = 1 + \frac{|\mathrm{GL}(2,p)|}{p^2} = 1 + \frac{(p+1)(p-1)^2}{p}.$$

Suppose now that $n \geqslant 3$ and that (2.1) holds for any noncyclic abelian p-group of order p^{n-1}. Since G is not cyclic, it possesses at least $p+1$ maximal subgroups $M_0, M_1, \ldots, M_p$. Moreover, at least one of them, say M_0, is noncyclic. Then Lemma 2.1 and Corollary 2.2 imply that

$$S(G) \geqslant S(M_0) + |\mathrm{Aut}(G)| + \sum_{i=1}^{p} |\mathrm{Aut}(M_i)| \geqslant S(M_0) + p^n(p-1)^2 + p\varphi(p^{n-1}).$$

By using the inductive hypothesis, we get

$$f(G) \geqslant \frac{1}{p} f(M_0) + (p-1)^2 + \frac{p-1}{p} \geqslant \frac{1}{p}\Big[1 + \frac{(p+1)(p-1)^2}{p}\Big] + (p-1)^2 + \frac{p-1}{p}$$
$$= 1 + \frac{(p^2+p+1)(p-1)^2}{p^2} > 1 + \frac{(p+1)(p-1)^2}{p}$$

as desired. We can easily see that the minimum value of the right side of (2.1) is $\frac{5}{2}$ and it is attained for $p = 2$. Hence, we have $f(G) \geqslant \frac{5}{2}$, with equality if and only if $p = 2$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This completes the proof. $\square$

Acknowledgments. The authors are grateful to the reviewers for their remarks which improved the previous version of the paper.

References

[1] *S. J. Baishya*: Revisiting the Leinster groups. C. R., Math., Acad. Sci. Paris *352* (2014), 1–6. zbl MR doi

[2] *S. J. Baishya, A. K. Das*: Harmonic numbers and finite groups. Rend. Semin. Mat. Univ. Padova *132* (2014), 33–43. zbl MR doi

[3] *J. N. S. Bidwell, M. J. Curran, D. J. McCaughan*: Automorphisms of direct products of finite groups. Arch. Math. *86* (2006), 481–489. zbl MR doi

[4] *J. N. Bray, R. A. Wilson*: On the orders of automorphism groups of finite groups. Bull. Lond. Math. Soc. *37* (2005), 381–385. zbl MR doi

[5] *J. N. Bray, R. A. Wilson*: On the orders of automorphism groups of finite groups II. J. Group Theory *9* (2006), 537–547. zbl MR doi

[6] *T. De Medts, A. Maróti*: Perfect numbers and finite groups. Rend. Semin. Mat. Univ. Padova *129* (2013), 17–33. zbl MR doi

[7] *T. De Medts, M. Tărnăuceanu*: Finite groups determined by an inequality of the orders of their subgroups. Bull. Belg. Math. Soc. - Simon Stevin *15* (2008), 699–704. zbl MR doi

[8] *J. González-Sánchez, A. Jaikin-Zapirain*: Finite p-groups with small automorphism group. Forum Math. Sigma *3* (2015), Article ID e7, 11 pages. zbl MR doi

[9] *C. J. Hillar, D. L. Rhea*: Automorphisms of finite abelian groups. Am. Math. Mon. *114* (2007), 917–923. zbl MR doi

[10] *I. M. Isaacs*: Finite Group Theory. Graduate Studies in Mathematics 92. AMS, Providence, 2008. zbl MR doi

[11] *G. A. Miller, H. C. Moreno*: Non-abelian groups in which every subgroup is abelian. Trans. Am. Math. Soc. *4* (1903), 398–404. zbl MR doi

[12] *A. Sehgal, S. Sehgal, P. K. Sharma*: The number of automorphism of a finite abelian group of rank two. J. Discrete Math. Sci. Cryptography *19* (2016), 163–171. zbl MR doi

[13] *M. Tărnăuceanu*: A generalization of the Euler's totient function. Asian-Eur. J. Math. *8* (2015), Article ID 1550087, 13 pages. zbl MR doi

[14] *M. Tărnăuceanu*: Finite groups determined by an inequality of the orders of their subgroups II. Commun. Algebra *45* (2017), 4865–4868. zbl MR doi

Authors' address: Georgiana Fasolă, Marius Tărnăuceanu (corresponding author), Faculty of Mathematics, Alexandru Ioan Cuza University, Bulevardul Carol I no. 11, 700506 Iaşi, Romania, e-mail: `georgiana.fasola@student.uaic.ro`, `tarnauc@uaic.ro`.