Asian-European Journal of Mathematics
Vol. 10, No. 1 (2017) 1750008 (8 pages)

DOI: 10.1142/S1793557117500085

World Scientific
www.worldscientific.com

On a generalization of the Gauss formula

Marius Tărnăuceanu
Faculty of Mathematics
Alexandru Ioan Cuza University
Bulevardul Carol I 11, Iaşi 700506, Romania
tarnauc@uaic.ro

Communicated by J. Koppitz
Received September 22, 2015
Accepted May 10, 2016
Published June 7, 2016

In this paper, we study a group theoretical generalization of the well-known Gauss formula, that uses the generalized Euler's totient function introduced in [M. Tărnăuceanu, A generalization of the Euler's totient function, *Asian-Eur. J. Math.* **8**(4) (2015) 13, Article ID: 1550087].

Keywords: Gauss formula; Euler's totient function; finite group; order of an element; exponent of a group.

AMS Subject Classification: 20D60, 11A25, 20D99, 11A99

1. Introduction

The *Euler's totient function* (or, simply, the *totient function*) φ is one of the most famous functions in number theory. Notice that 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. The totient function is important mainly, because it gives the order of the group of all units in the ring $(\mathbb{Z}_n, +, \cdot)$. Alternatively, $\varphi(n)$ can be seen as the number of generators or as the number of elements of order n of the finite cyclic group $(\mathbb{Z}_n, +)$.

Recall also a well-known arithmetical identity involving the totient function, namely the *Gauss formula*

$$\sum_{d|n} \varphi(d) = n, \quad \forall\, n \in \mathbb{N}^*. \tag{1}$$

Many generalizations of the totient function are known (for example, see [2, 3, 5, 8] and the special chapter on this topic in [6]). From these, the most significant is probably the *Jordan's totient function* (see [1]).

The starting point for our discussion is given by the paper [11], where a new group theoretical generalization of the totient function has been studied. This is founded on the remark that $\varphi(n)$ counts in fact the number of elements of order $\exp(\mathbb{Z}_n)$ in $(\mathbb{Z}_n, +)$. Consequently, it makes sense to define

$$\varphi(G) = |\{a \in G \mid o(a) = \exp(G)\}|$$

for any finite group G. It is obvious that $\varphi(\mathbb{Z}_n) = \varphi(n)$, for all $n \in \mathbb{N}^*$, and so a generalization of the classical totient function φ is obtained. Remark that unlike Euler's totient function and Jordan's function, the function φ discussed here can vanish (see e.g. [11, Theorems 2.6 and 2.8]). We also remark that for $G \cong \mathbb{Z}_n$ the Gauss formula can be rewritten as

$$\sum_{H \leq G} \varphi(H) = |G|. \tag{2}$$

This leads to the natural problem

which are the finite groups G satisfying the equality (2)?

Its study is the main goal of the current paper. We show that the cyclic groups are the unique abelian groups with this property. Inspired by some particular cases, we conjecture that this is also true for nilpotent groups. Moreover, we give examples of non-nilpotent groups G satisfying (2). Several open problems on this topic are also formulated.

Most of our notation is standard and will not be repeated here. Basic definitions and results on groups can be found in [4, 9]. For subgroup lattice concepts, we refer the reader to [7, 10].

2. Main Results

For a finite group G, let us denote

$$S(G) = \sum_{H \leq G} \varphi(H).$$

In this way, we are interested to describe the class $\mathcal{C}$ consisting of all finite groups G for which $S(G) = |G|$.

Obviously, the finite cyclic groups are contained in $\mathcal{C}$, by the Gauss formula. On the other hand, we easily obtain $S(\mathbb{Z}_2 \times \mathbb{Z}_2) = 7 \neq 4 = |\mathbb{Z}_2 \times \mathbb{Z}_2|$, proving that $\mathcal{C}$ is not closed under direct products or extensions.

For a detailed study of the class $\mathcal{C}$, we must look first at some basic properties of the map S. We remark that it satisfies the inequality

$$S(G) \geq \sum_{H \in C(G)} \varphi(H) = \sum_{H \in C(G)} \varphi(|H|), \tag{3}$$

where $C(G)$ denotes the poset of cyclic subgroups of G. Another easy, but very important property of S is the following.

Proposition 1. *S is multiplicative, that is if $(G_i)_{i=\overline{1,k}}$ is a family of finite groups of coprime orders, then we have*:

$$S\left(\prod_{i=1}^{k} G_i\right) = \prod_{i=1}^{k} S(G_i).$$

Proof. Since the groups $(G_i)_{i=\overline{1,k}}$ are of coprime orders, we infer that every subgroup H of $G = \prod_{i=1}^{k} G_i$ can be written as $H = \prod_{i=1}^{k} H_i$ with $H_i \leq G_i$, $\forall\, i = \overline{1,k}$. By [11, Lemma 2.1], we know that φ is multiplicative and therefore

$$\varphi(H) = \prod_{i=1}^{k} \varphi(H_i).$$

Then, one obtains

$$S\left(\prod_{i=1}^{k} G_i\right) = \sum_{H \leq G} \varphi(H) = \sum_{H_1 \leq G_1} \sum_{H_2 \leq G_2} \cdots \sum_{H_k \leq G_k} \varphi(H_1)\varphi(H_2)\cdots\varphi(H_k)$$
$$= \prod_{i=1}^{k} \left(\sum_{H_i \leq G_i} \varphi(H_i)\right) = \prod_{i=1}^{k} S(G_i)$$

as desired. □

In particular, Proposition 1 shows that the computation of $S(G)$ for a finite nilpotent group G is reduced to p-groups.

Corollary 2. *Let G be a finite nilpotent group and G_i, $i = 1, 2, \ldots, k$, be the Sylow subgroups of G. Then*

$$S(G) = \prod_{i=1}^{k} S(G_i).$$

Proof. The equality follows immediately from Proposition 1, since a finite nilpotent group is the direct product of its Sylow subgroups. □

Notice that for a finite abelian p-group G, the value $\varphi(G)$ has been precisely computed in [11, Theorem 2.3]. This is essential to show the following result.

Theorem 3. *Let G be a finite abelian group. Then $S(G) \geq |G|$, and we have equality if and only if G is cyclic.*

Proof. Remark first that, we can assume G to be a p-group by Corollary 2. Let $(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_r})$ be the type of G and assume that $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_{s-1} < \alpha_s = \alpha_{s+1} = \cdots = \alpha_r$. According to [11, Theorem 2.3], we have

$$\varphi(G) = |G|\left(1 - \frac{1}{p^{r-s+1}}\right) \geq |G|\left(1 - \frac{1}{p}\right).$$

On the other hand, it is wellknown that G has $\frac{p^r-1}{p-1}$ maximal subgroups, namely p^{r-1} subgroups isomorphic to $M_1 = \mathbb{Z}_{p^{\alpha_1-1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r}}$, p^{r-2} subgroups isomorphic to $M_2 = \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2-1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r}}, \ldots,$ and one subgroup isomorphic to $M_r = \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r-1}}$. One obtains

$$\begin{aligned} S(G) &\geq \varphi(G) + \sum_{i=1}^{r} p^{r-i}\varphi(M_i) + 1 \\ &\geq |G|\left(1-\frac{1}{p}\right) + \sum_{i=1}^{r} p^{r-i}\frac{|G|}{p}\left(1-\frac{1}{p}\right) + 1 \\ &= |G|\frac{p^r+p^2-p-1}{p^2} + 1. \end{aligned}$$

If $r \geq 2$, then

$$\frac{p^r+p^2-p-1}{p^2} \geq \frac{2p^2-p-1}{p^2} > 1$$

implying that

$$S(G) > |G| + 1 > |G|.$$

Consequently, G belongs to $\mathcal{C}$, if and only if $r = 1$, i.e. if and only if it is cyclic. □

Next, we will focus on extending the above result from abelian p-groups to arbitrary p-groups, and consequently to arbitrary nilpotent groups. By a direct calculation, we infer that for all non-abelian p-groups G of order p^3 (whose classification is well-known — see e.g. [9, II]) we have

$$S(G) > |G|.$$

This inequality also holds for other classes of non-abelian p-groups G, determined by the existence of abelian subgroups of a given structure.

Theorem 4. *Let G be a non-abelian p-group of order p^n, $n \geq 4$. If G has an abelian subgroup of order p^m and rank r with $m + r \geq n + 2$, then $S(G) > |G|$, i.e. G is not contained in $\mathcal{C}$. In particular, if G has an elementary abelian maximal subgroup, then it does not belong to $\mathcal{C}$.*

Proof. Let A be an abelian subgroup of order p^m and rank r of G, and assume that $m + r \geq n + 2$. By the proof of Theorem 3, we infer that

$$\begin{aligned} S(G) > S(A) &\geq p^m\frac{p^r+p^2-p-1}{p^2} + 1 \\ &= p^{m+r-2} + p^{m-2}\left(p^2-p-1\right) + 1 \\ &\geq p^{m+r-2} + p^{m-2} + 1 > p^{m+r-2} \\ &\geq p^n \end{aligned}$$

as claimed. □

Theorem 5. *Let G be a non-abelian p-group of order p^n, $n \geq 4$. If G has a cyclic maximal subgroup, then $S(G) > |G|$, i.e. G is not contained in $\mathcal{C}$.*

Proof. By [9, II, Theorem 4.1], we know that G is isomorphic to

– $M(p^n) = \langle x, y \,|\, x^{p^{n-1}} = y^p = 1, y^{-1}xy = x^{p^{n-2}+1} \rangle$

when p is odd, or to one of the following groups

– $M(2^n)$
– the dihedral group D_{2^n},
– the generalized quaternion group

$$Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^4 = 1, yxy^{-1} = x^{2^{n-1}-1} \rangle,$$

– the quasi-dihedral group

$$S_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, y^{-1}xy = x^{2^{n-2}-1} \rangle$$

when $p = 2$.

A common property of all these p-groups G is that they have $p + 1$ maximal subgroups, say $M_1, M_2, \ldots, M_{p+1}$, and (at least) one of them is cyclic, say $M_{p+1} \cong \mathbb{Z}_{p^{n-1}}$. Moreover, $\Phi(G)$ is cyclic of order p^{n-2}. Then, by applying the Inclusion–Exclusion Principle, one obtains

$$S(G) = \varphi(G) + \sum_{i=1}^{p+1} S(M_i) - p \cdot S(\Phi(G)) = \varphi(G) + \sum_{i=1}^{p+1} S(M_i) - p^{n-1}. \tag{4}$$

For $M(p^n)$, it is easy to check that p maximal subgroups are cyclic, say $M_i \cong \mathbb{Z}_{p^{n-1}}$, $i = 2, 3, \ldots, p+1$ and $M_1 \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$. Then $\varphi(M(p^n)) = p \cdot \varphi(p^{n-1}) = p^n - p^{n-1}$ and (4) leads to

$$\begin{aligned} S(M(p^n)) &= p^n - p^{n-1} + S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}) + p \cdot p^{n-1} - p^{n-1} \\ &> p^n - p^{n-1} + p^{n-1} + p^n - p^{n-1} = 2 \cdot p^n - p^{n-1} > p^n \end{aligned}$$

according to Theorem 3.

For every $G \in \{D_{2^n}, Q_{2^n}, S_{2^n}\}$, we have $\varphi(G) = 2^{n-2}$. Then (4) can be rewritten as

$$S(G) = 2^{n-2} + S(M_1) + S(M_2). \tag{5}$$

The pair (M_1, M_2) of maximal subgroups of D_{2^n}, Q_{2^n} and S_{2^n} is $(D_{2^{n-1}}, D_{2^{n-1}})$, $(Q_{2^{n-1}}, Q_{2^{n-1}})$ and $(D_{2^{n-1}}, Q_{2^{n-1}})$, respectively. Clearly, in the first two cases (5) becomes a recurrence relation, which easily leads to

$$S(D_{2^n}) = 2^{n+1} + (n-3) \cdot 2^{n-2} > 2^n$$

and

$$S(Q_{2^n}) = (n+4) \cdot 2^{n-2} > 2^n$$

while for $G = S_{2^n}$, one obtains

$$S(S_{2^n}) = 2^{n-2} + S(D_{2^{n-1}}) + S(Q_{2^{n-1}}) = (2n+9) \cdot 2^{n-3} > 2^n.$$

This completes the proof. □

Inspired by the previous results, we came up with the following conjecture.

Conjecture 6. *Let G be a finite nilpotent group. Then $S(G) \geq |G|$, and we have equality if and only if G is cyclic.*

Obviously, Conjecture 6 can be reformulated in the next way: *the cyclic groups are the unique finite nilpotent groups contained in* $\mathcal{C}$. It leads to the natural assumption that, $\mathcal{C}$ consists in fact only of the finite cyclic groups. This is not true, as shows the following elementary example.

Example. Let G be the non-abelian group of order pq, where $p < q$ are primes and $p \mid q-1$. The subgroup structure of G is well-known: it possesses one subgroup of order 1, q subgroups of order p, one subgroup of order q and one subgroup of order pq. Then

$$S(G) = 1 + q\,\varphi(\mathbb{Z}_p) + \varphi(\mathbb{Z}_q) + \varphi(G) = 1 + q(p-1) + q - 1 = pq = |G|$$

i.e. G belongs to $\mathcal{C}$.

In particular, the above example shows that the dihedral group D_6 is contained in $\mathcal{C}$. In fact, we are able to characterize the containment to $\mathcal{C}$ for arbitrary dihedral groups $D_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle$, $n \geq 2$.

Theorem 7. *The dihedral group D_{2n} belongs to $\mathcal{C}$ if and only if n is odd.*

Proof. Let $n = 2^k m$ with $k, m \in \mathbb{N}$ and m odd. Then the lattice of divisors of n can be written as the union of the sets $\mathcal{D}_i = \{\, 2^i m' \mid m' \mid m\}$, $i = 0, 1, \ldots, k$. On the other hand, for every divisor d of n, D_{2n} has one subgroup isomorphic to $\mathbb{Z}_d$, namely $\langle x^{\frac{n}{d}} \rangle$, and $\frac{n}{d}$ subgroups isomorphic to D_{2d}, namely $\langle x^{\frac{n}{d}}, x^{i-1}y \rangle$, $i = 1, 2, \ldots, \frac{n}{d}$. Recall that, we have $\varphi(D_2) = 1$, $\varphi(D_4) = 4$ and

$$\varphi(D_{2n}) = \begin{cases} 0, & n \equiv 1 \pmod 2 \\ \varphi(n), & n \equiv 0 \pmod 2 \end{cases} \quad \forall\, n \geq 3$$

by [11, Theorem 2.6]. It follows that

$$S(D_{2n}) = \sum_{H \leq D_{2n}} \varphi(H) = \sum_{d \mid n} \left(\varphi(\mathbb{Z}_d) + \frac{n}{d} \varphi(D_{2d}) \right)$$

$$= \sum_{d \mid n} \varphi(\mathbb{Z}_d) + \sum_{d \mid n} \frac{n}{d} \varphi(D_{2d}) = \sum_{d \mid n} \varphi(d) + \sum_{i=0}^{k} \sum_{d \in \mathcal{D}_i} \frac{n}{d} \varphi(D_{2d})$$

$$= n + \sum_{m' \mid m} \frac{n}{m'} \varphi(D_{2m'}) + \sum_{i=1}^{k} \sum_{m' \mid m} \frac{n}{2^i m'} \varphi(D_{2^{i+1} m'}) = 2n + \Sigma,$$

where

$$\sum = \sum_{i=1}^{k} \sum_{m'|m} \frac{n}{2^i m'} \varphi(D_{2^{i+1}m'}).$$

Hence $S(D_{2n}) = 2n$, if and only if $\Sigma = 0$. This happens if and only if $k = 0$, i.e. n is odd. □

Remark. By Theorem 7, we have $S(D_{2n}) = 2n$ for n odd. An explicit value of $S(D_{2n})$ for n even can be calculated, too. Let n as above and let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ be the decomposition of m as a product of prime factors. We remark that $\varphi(D_{2^{i+1}m'}) = \varphi(2^i m') = 2^{i-1}\varphi(m')$, excepting the case $i = m' = 1$, when $\varphi(D_{2^{i+1}m'}) = 3$. One obtains

$$\sum = \frac{3n}{2} - \frac{n}{2} + \sum_{i=1}^{k} \sum_{m'|m} \frac{n}{2m'} \varphi(m') = n + \frac{kn}{2} \sum_{m'|m} \frac{\varphi(m')}{m'}$$

$$= n + \frac{kn}{2} \prod_{i=1}^{s} \left(\alpha_i + 1 - \frac{\alpha_i}{p_i}\right)$$

and thus

$$S(D_{2n}) = 3n + \frac{kn}{2} \prod_{i=1}^{s} \left(\alpha_i + 1 - \frac{\alpha_i}{p_i}\right).$$

For example, we can easily check that

$$S(D_{12}) = 23.$$

Next, we observe that both the non-abelian groups of order pq and the dihedral groups D_{2n} with n odd, which we verified to be contained in $\mathcal{C}$, are semidirect products of a cyclic normal subgroup N by a cyclic subgroup H of prime order satisfying $C_N(H) = 1$. The containment of such a group to $\mathcal{C}$ can be also characterized, extending the above results.

Theorem 8. *Let G be a finite non-abelian group and $N \cong \mathbb{Z}_n$ be a normal Hall subgroup of G, which has a complement H of prime order p, such that $C_N(H) = 1$. Then G belongs to $\mathcal{C}$, if and only if the number of complements of N in G is n.*

Proof. Under our hypotheses, $L(G)$ consists of the subgroups of N, say N_d with $d = |N_d|$, $d \,|\, n$ of the complements of N in G, say $H_1 = H, H_2, \ldots, H_{n_p}$, and of the semidirect products $N_d H_i$, with $d \,|\, n$, $d \neq 1$ and $i = \overline{1, n_p}$. Since $C_N(H) = 1$, every $N_d H_i$ with $d \neq 1$ is not cyclic and so it does not contain elements of order $dp = \exp(N_d H_i)$. Consequently, we infer that $\varphi(N_d H_i) = 0$, for all $d \,|\, n$ with $d \neq 1$ and all $i = \overline{1, n_p}$. This leads to

$$S(G) = S(N) + \sum_{i=1}^{n_p} \varphi(H_i) = n + n_p(p-1).$$

It is now obvious that

$$S(G) = np \Leftrightarrow n_p = n$$

which ends the proof. □

We conclude that, at least two important classes of finite groups are contained in $\mathcal{C}$: cyclic groups and semidirect products of type indicated in Theorem 8. Remark that these groups G are supersolvable and that $S(G)$ equals the sum of all values of φ on the cyclic subgroups of G, that is (3) becomes an equality.

Finally, we remark that every subgroup and every quotient of such a group also belong to $\mathcal{C}$, that is $\mathcal{C}$ seems to be closed under subgroups and homomorphic images.

We end this paper by indicating several natural problems on the above class $\mathcal{C}$.

Problem 1. Prove or disprove Conjecture 6.

Problem 2. Give a complete description of $\mathcal{C}$ (in our opinion, it consists of the finite cyclic groups and of non-abelian semidirect products of a certain type, most probably metacyclic groups). Is it true that, $\mathcal{C}$ is contained in the class of finite supersolvable groups?

Problem 3. Study whether $\mathcal{C}$ is closed under subgroups and homomorphic images.

Acknowledgment

The author is grateful to the reviewer for his/her remarks, which improved the previous version of the paper.

References

1. L. Dickson, *History of the Theory of Numbers*, Vol. I (Chelsea Publishing, New York, 1966).
2. P. G. Garcia and S. Ligh, A generalization of Euler's φ-function, *Fibonacci Quart.* **21** (1983) 26–28.
3. P. Hall, The Eulerian functions of a group, *Q. J. Math.* **7** (1936) 134–151.
4. B. Huppert, *Endliche Gruppen*, I (Springer-Verlag, Berlin, 1967).
5. P. J. McCarthy, *Introduction to Arithmetical Functions* (Springer-Verlag, New York, 1986).
6. J. Sándor and B. Crstici, *Handbook of Number Theory*, II (Kluwer Academic, Dordrecht, 2004).
7. R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter Expositions in Mathematics, Vol. 14 (de Gruyter, Berlin, 1994).
8. R. Sivaramakrishnan, The many facets of Euler's totient, II, *Nieuw Arch. Wisk.* **8** (1990) 169–187.
9. M. Suzuki, *Group Theory*, I; II (Springer-Verlag, Berlin, 1982; 1986).
10. M. Tărnăuceanu, *Groups Determined by Posets of Subgroups* (Matrix Rom, Bucureşti, 2006).
11. M. Tărnăuceanu, A generalization of the Euler's totient function, *Asian-Eur. J. Math.* **8**(4) (2015) 13, Article ID: 1550087.