Publ. Math. Debrecen
87/1-2 (2015), 133–145
DOI: 10.5486/PMD.2015.7098

Counting invertible sums of squares modulo n and a new generalization of Euler's totient function

By CATALINA CALDERÓN (Leioa), JOSÉ MARÍA GRAU (Oviedo), ANTONIO M. OLLER-MARCÉN (Zaragoza) and LÁSZLÓ TÓTH (Pécs)

Abstract. In this paper we introduce and study a family Φ_k of arithmetic functions generalizing Euler's totient function. These functions are given by the number of solutions to the equation $\gcd(x_1^2+\cdots+x_k^2,n)=1$ with $x_1,\dots,x_k\in\mathbb{Z}/n\mathbb{Z}$ which, for $k=2,4$ and 8 coincide, respectively, with the number of units in the rings of Gaussian integers, quaternions and octonions over $\mathbb{Z}/n\mathbb{Z}$. We prove that Φ_k is multiplicative for every k, we obtain an explicit formula for $\Phi_k(n)$ in terms of the prime-power decomposition of n and derive an asymptotic formula for $\sum_{n\le x}\Phi_k(n)$. As a tool we investigate the multiplicative arithmetic function that counts the number of solutions to $x_1^2+\cdots+x_k^2\equiv\lambda \pmod n$ for λ coprime to n, thus extending an old result that dealt only with the prime n case.

1. Introduction

Euler's totient function φ is one of the most famous arithmetic functions used in number theory. Recall that $\varphi(n)$ is defined as the number of positive integers less than or equal to n that are coprime to n. Many generalizations and analogs of Euler's function are known. See, for instance [5], [6], [8], [9], [13], [16] or the special chapter on this topic in [15]. Among the generalizations, the most significant is probably the Jordan's totient function $\mathbf{J}_k$ given by $\mathbf{J}_k(n)=n^k\prod_{p|n}(1-p^{-k})$ ($n\in\mathbb{N}:=\{1,2,\dots\}$). See [1], [3, pp. 147–155], [18].

Mathematics Subject Classification: 11A25, 11N37.
Key words and phrases: quadratic congruence, multiplicative function, Euler's totient function, asymptotic formula.

In this paper we introduce and study a new generalization of φ. In particular, given $k \in \mathbb{N}$ we define

$$\Phi_k(n) := \text{card } \{(x_1, \ldots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : \gcd(x_1^2 + \cdots + x_k^2, n) = 1\}. \tag{1}$$

Clearly, $\Phi_1(n) = \varphi(n)$ and it is the order of the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$. On the other hand, $\Phi_2(n)$ is the restriction to the set of positive integers of the Euler function defined on the Gaussian integers $\mathbb{Z}[i]$. Thus $\Phi_2(n)$, denoted also by $\mathrm{GIphi}(n)$ in the literature, counts the number of Gaussian integers in a reduced residue system modulo n. See [2]. In the same way, $\Phi_4(n)$ and $\Phi_8(n)$ count, respectively, the number of invertible quaternions and octonions over $\mathbb{Z}/n\mathbb{Z}$.

In order to study the function Φ_k we need to focus on the functions

$$\rho_{k,\lambda}(n) := \text{card } \{(x_1, \ldots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}\} \tag{2}$$

which count the number of points on hyperspheres in $(\mathbb{Z}/n\mathbb{Z})^k$ and, in particular, in the case $\gcd(\lambda, n) = 1$. These functions were already studied in the case when n is an odd prime by Victor-Amédée Lebesgue in 1837. In particular he proved the following result ([4, Chapter X]).

Proposition 1. *Let p be an odd prime and let k, λ be positive integers with $p \nmid \lambda$. Put $t = (-1)^{(p-1)(k-1)/4} p^{(k-1)/2}$ and $\ell = (-1)^{k(p-1)/4} p^{(k-2)/2}$. Then*

$$\rho_{k,\lambda}(p) = \begin{cases} p^{k-1} + t, & \text{if } k \text{ is odd and } \lambda \text{ is a quadratic residue modulo } p; \\ p^{k-1} - t, & \text{if } k \text{ is odd and } \lambda \text{ is a quadratic nonresidue}; \\ p^{k-1} - \ell, & \text{if } k \text{ is even.} \end{cases}$$

The paper is organized as follows. First of all, in Section 2 we study the values of $\rho_{k,\lambda}(n)$ in the case $\gcd(\lambda, n) = 1$, thus generalizing Lebesgue's work. In Section 3 we study the functions Φ_k, in particular we prove that they are multiplicative and we give a closed formula for $\Phi_k(n)$ in terms of the prime-power decomposition of n. Section 4 is devoted to deduce an asymptotic formula for $\sum_{n \le x} \Phi_k(n)$. Finally, we close our work suggesting some ideas that leave the door open for future work.

2. Counting points on hyperspheres $\pmod{n}$

Due to the Chinese Remainder Theorem, the function $\rho_{k,\lambda}$, defined by (2) is multiplicative; i.e., if $n = p_1^{r_1} \cdots p_m^{r_m}$, then $\rho_{k,\lambda}(n) = \rho_{k,\lambda}(p_1^{r_1}) \cdots \rho_{k,\lambda}(p_m^{r_m})$.

Hence, we can restrict ourselves to the case when $n = p^s$ is a prime-power. Moreover, since in this paper we focus on the case $\gcd(\lambda, n) = 1$, we will always assume that $p \nmid \lambda$. The following result will allow us to extend Lebesgue's work to the odd prime-power case.

Lemma 1. *Let p be an odd prime and let $s \in \mathbb{N}$. If $p \nmid \lambda$, then*

$$\rho_{k,\lambda}(p^s) = p^{(s-1)(k-1)}\rho_{k,\lambda}(p).$$

Proof. It is easily seen that any solution to the congruence $x_1^2+\cdots+x_k^2 \equiv \lambda \pmod{p^{s+1}}$ must be of the form $(a_1+t_1p^s, \ldots, a_k+t_kp^s)$, where $0 \le t_1, \ldots, t_k \le p-1$, for some $(a_1, \ldots, a_k)$ such that $a_1^2+\cdots+a_k^2 \equiv \lambda \pmod{p^s}$. Now, $(a_1+t_1p^s)^2+\cdots+(a_k+t_kp^s)^2 \equiv \lambda \pmod{p^{s+1}}$ if and only if $2a_1t_1+\cdots+2a_kt_k \equiv -K \pmod{p}$, where K is such that $a_1^2+\cdots+a_k^2 = Kp^s+\lambda$. Since $a_i \not\equiv 0 \pmod{p}$ for some $i \in \{1, \ldots, k\}$, it follows that there are exactly p^{k-1} possibilities for $(t_1, \ldots, t_k)$. We obtain that $\rho_{k,\lambda}(p^{s+1}) = p^{k-1}\rho_{k,\lambda}(p^s)$, and the result follows inductively. $\square$

If $p = 2$ we have a similar result.

Lemma 2. *Let $s \ge 3$ and let $\lambda \in \mathbb{N}$ be odd. Then,*

$$\rho_{k,\lambda}(2^s) = 2^{(s-3)(k-1)}\rho_{k,\lambda}(8).$$

Proof. In the case $p = 2$ the proof of Lemma 1 does not work since $2a_1t_1+\cdots+2a_kt_k \equiv -K \pmod{2}$ holds only if K is even. Therefore, we use that every solution of the congruence $x_1^2+\cdots+x_k^2 \equiv \lambda \pmod{2^{s+1}}$ is of the form $(a_1+t_12^{s-1}, \ldots, a_k+t_k2^{s-1})$, where $0 \le t_1, \ldots, t_k \le 3$, for some $(a_1, \ldots, a_k)$ satisfying $a_1^2+\cdots+a_k^2 \equiv \lambda \pmod{2^{s-1}}$, that is $a_1^2+\cdots+a_k^2 = L2^{s-1}+\lambda$ with an integer L. Now, taking into account that $s \ge 3$, $(a_1+t_12^{s-1})^2+\cdots+(a_k+t_k2^{s-1})^2 \equiv \lambda \pmod{2^{s+1}}$ if and only if

$$2(a_1t_1+\cdots+a_kt_k) \equiv -L \pmod{4}. \tag{3}$$

Here the condition (3) holds true if and only if L is even, i.e., $a_1^2+\cdots+a_k^2 \equiv \lambda \pmod{2^s}$. Hence we need the solutions $(a_1, \ldots, a_k)$ of the congruence $\pmod{2^s}$, but only those satisfying

$$0 \le a_1, \ldots, a_k < 2^{s-1} \tag{4}$$

It is easy to see that their number is $\rho_{k,\lambda}(2^s)/2^k$, since all solutions of the congruence $\pmod{2^s}$ are $(a_1+u_12^{s-1}, \ldots, a_k+u_k2^{s-1})$ with $(a_1, \ldots, a_k)$ verifying (4) and $0 \le u_1, \ldots, u_k \le 1$. Since a_i must be odd for some $i \in \{1, \ldots, k\}$, for a fixed even L, (3) has $2 \cdot 4^{k-1}$ solutions $(t_1, \ldots, t_k)$. We deduce that $\rho_{k,\lambda}(2^{s+1}) = 2 \cdot 4^{k-1}\rho_{k,\lambda}(2^s)/2^k = 2^{k-1}\rho_{k,\lambda}(2^s)$. Now the result follows inductively on s. $\square$

As we have just seen, unlike when p is an odd prime, the recurrence is now based on $\rho_{k,\lambda}(2^3)$. Hence, the cases $s = 1, 2, 3$; i.e., $n = 2, 4, 8$, must be studied separately. In order to do so, the following general result will be useful.

Lemma 3. *Let k, λ and n be positive integers. Then*

$$\rho_{k,\lambda}(n) = \sum_{\ell=0}^{n-1} \rho_{1,\ell}(n)\rho_{k-1,\lambda-\ell}(n).$$

Proof. Let $(x_1, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k$ be such that $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}$. Then, for some $\ell \in \{0, \dots, n-1\}$ we have that $x_1^2 \equiv \ell \pmod{n}$ and $x_2^2 + \cdots + x_k^2 \equiv \lambda - \ell \pmod{n}$ and hence the result. $\square$

Now, given $k, n \in \mathbb{N}$ let us define the matrix $M(n) = (\rho_{1,i-j}(n))_{0\le i,j\le n-1}$. If we consider the column vector $R_k(n) = (\rho_{k,i}(n))_{0\le i\le n-1}$, then Lemma 3 leads to the following recurrence relation:

$$R_k(n) = M(n) \cdot R_{k-1}(n).$$

In the following proposition we use this recurrence relation to compute $\rho_{k,\lambda}(2^s)$ for $s = 1, 2, 3$ and odd λ.

Lemma 4. *Let k be a positive integer. Then*

i) $\rho_{k,1}(2) = 2^{k-1}$,

ii) $\rho_{k,1}(4) = 4^{k-1} + 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$,

iii) $\rho_{k,3}(4) = 4^{k-1} - 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$,

iv) $\rho_{k,1}(8) = 2^{2k-3}\big(2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) + 2\sin\left(\frac{1}{4}\pi(k+1)\right) - 2\cos\left(\frac{1}{4}\pi(3k+1)\right)\big)$,

v) $\rho_{k,3}(8) = 2^{2k-3}\big(2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2\big(\cos\left(\frac{1}{4}\pi(k+1)\right) + \cos\left(\frac{3}{4}\pi(k+1)\right)\big)\big)$,

vi) $\rho_{k,5}(8) = 2^{2k-3}\big(2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2\sin\left(\frac{1}{4}\pi(k+1)\right) + 2\cos\left(\frac{1}{4}\pi(3k+1)\right)\big)$,

vii) $\rho_{k,7}(8) = 2^{2k-3}\big(2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2\sin\left(\frac{1}{4}(3\pi k+\pi)\right) + 2\cos\left(\frac{1}{4}\pi(k+1)\right)\big)$.

Proof. First of all, observe that

$$M(2) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\ M(4) = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 2 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix},\ M(8) = \begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 0 & 0 & 4 \\ 4 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 4 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 4 & 2 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 4 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 4 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 4 & 2 \end{pmatrix}.$$

Let us compute ii). We know that $R_k(4) = M(4) \cdot R_{k-1}(4)$. Hence, since the eigenvalues of $M(4)$ are $\{4, 2+2i, 2-2i, 0\}$, we know that

$$\rho_{k,1}(4) = C_1 4^k + C_2(2+2i)^k + C_3(2-2i)^k.$$

In order to compute C_1, C_2 and C_3 it is enough to observe that $\rho_{1,1}(4) = 2$, $\rho_{2,1}(4) = 8$ and $\rho_{3,1}(4) = 24$. Hence

$$4C_1 + (2+2i)C_2 + (2-2i)C_3 = 2, \quad 16C_1 + 8iC_2 - 8iC_3 = 8,$$

$$64C_1 - (16-16i)C_2 - (16+16i)C_3 = 24.$$

We deduce

$$\rho_{k,1}(4) = \frac{1}{4}\left(4^k - i(2+2i)^k + i(2-2i)^k\right) = 2^{2k-2} + 2^{\frac{3k}{2}-1}\sin\left(\frac{\pi k}{4}\right),$$

as claimed.

To compute the other cases note that the eigenvalues of $M(2)$ are $\{0, 2\}$ while the eigenvalues of $M(8)$ are

$$\left\{8, 4+4i, 4-4i, \sqrt{2}(-2-2i), \sqrt{2}(2+2i), \sqrt{2}(-2+2i), \sqrt{2}(2-2i), 0\right\}.$$

Thus, in each case we only need to compute the corresponding initial conditions and constants. The final results have been obtained with the help of Mathematica "ComplexExpand" command. □

Note that a different approach to compute the values $\rho_{k,\lambda}(n)$, using the Gauss quadratic sum was given in [20].

3. Counting invertible sums of squares (mod n)

Given positive integers k, n, this section is devoted to computing $\Phi_k(n)$, defined by (1). Let $A(k, \lambda, n)$ denote the set of solutions $(x_1, \ldots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k$ of the congruence $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}$. First of all, let us define the set

$$\mathcal{A}_k(n) := \bigcup_{\substack{1 \le \lambda \le n \\ \gcd(\lambda, n)=1}} A(k, \lambda, n).$$

Hence, $\Phi_k(n) = \operatorname{card} \mathcal{A}_k(n)$ and, since the union is clearly disjoint, it follows that

$$\Phi_k(n) = \sum_{\substack{1 \le \lambda \le n \\ \gcd(\lambda, n)=1}} \rho_{k,\lambda}(n).$$

The following result shows the multiplicativity of Φ_k for every positive k.

Proposition 2. *Let k be a positive integer. Then Φ_k is multiplicative; i.e., $\Phi_k(mn) = \Phi_k(m)\Phi_k(n)$ for every $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$.*

Proof. Let us define a map $F : \mathcal{A}_k(m) \times \mathcal{A}_k(n) \longrightarrow \mathcal{A}_k(mn)$ by

$$F((a_1, \dots, a_k), (b_1, \dots, b_k)) = (na_1 + mb_1, \dots, na_k + mb_k).$$

Note that if $(a_1, \dots, a_k) \in \mathcal{A}_k(m)$, then $a_1^2 + \cdots + a_k^2 \equiv \lambda_1 \pmod{m}$ for some λ_1 with $\gcd(\lambda_1, m) = 1$. In the same way, if $(b_1, \dots, b_k) \in \mathcal{A}_k(n)$, then $b_1^2 + \cdots + b_k^2 \equiv \lambda_2 \pmod{n}$ for some λ_2 with $\gcd(\lambda_2, n) = 1$. Consequently,

$$\begin{aligned}(na_1 + mb_1)^2 + \cdots + (na_k + mb_k)^2 &= n^2(a_1^2 + \cdots + a_k^2) + m^2(b_1^2 + \cdots + b_k^2)\\ &+2mn(b_1a_1 + \cdots + b_ka_k) \equiv n^2\lambda_1 + m^2\lambda_2 \pmod{mn}.\end{aligned}$$

Since it is clear that $\gcd(n^2\lambda_1 + m^2\lambda_2, mn) = 1$, it follows that $(na_1 + mb_1, \dots, na_k + mb_k) \in \mathcal{A}_k(mn)$ and thus F is well-defined.

Now, let $(c_1, \dots, c_k) \in \mathcal{A}_k(mn)$. Then $c_1^2 + \cdots + c_k^2 \equiv \lambda \pmod{mn}$ for some λ such that $\gcd(\lambda, mn) = 1$. Let us define $a_i \equiv c_i \pmod{m}$ and $b_i \equiv c_i \pmod{n}$ for every $i = 1, \dots, k$. It follows that $(a_1, \dots, a_k) \in \mathcal{A}_k(m)$, $(b_1, \dots, b_k) \in \mathcal{A}_k(n)$ and, moreover, $F((a_1, \dots, a_k), (b_1, \dots, b_k)) = (c_1, \dots, c_k)$. Hence, F is surjective.

Finally, assume that

$$(na_1 + mb_1, \dots, na_k + mb_k) \equiv (n\alpha_1 + m\beta_1, \dots, n\alpha_k + m\beta_k) \pmod{mn}$$

for some $(a_1, \dots, a_k), (\alpha_1, \dots, \alpha_k) \in \mathcal{A}_k(m)$ and for some $(b_1, \dots, b_k), (\beta_1, \dots, \beta_k) \in \mathcal{A}_k(n)$. Then, for every $i = 1, \dots, k$ we have that $na_i + mb_i \equiv n\alpha_i + m\beta_i \pmod{mn}$. From this, it follows that $a_i \equiv \alpha_i \pmod{m}$ and that $b_i \equiv \beta_i \pmod{n}$ for every i and hence F is injective.

Thus, we have proved that F is bijective and the result follows. □

Since we know that Φ_k is multiplicative, we just need to compute its values over prime-powers. We do so in the following result.

Proposition 3. *Let k, r be positive integers. Then*

i) $\Phi_k(2^r) = \varphi(2^{kr}) = 2^{kr-1}$.

ii) *If p is an odd prime,*

$$\Phi_k(p^r) = \varphi(p^{kr}) - (-1)^{k(p-1)/4}\varphi(p^{kr-k/2}) = p^{kr-\frac{k}{2}-1}(p-1)\big(p^{k/2} - (-1)^{k(p-1)/4}\big).$$

Proof.

i) If $r = 1, 2, 3$ the result readily follows from Lemma 4 by a simple computation. Now, if $r > 3$ we can apply Lemma 2 to obtain that

$$\begin{aligned}\Phi_k(2^r) &= \sum_{\substack{1\le i\le 2^r\\ 2\nmid i}} \rho_{k,i}(2^r) = 2^{(r-3)(k-1)} \sum_{\substack{1\le i\le 2^r\\ 2\nmid i}} \rho_{k,i}(8)\\ &= 2^{(r-3)(k-1)} \sum_{j=0}^{2^{r-3}-1} \sum_{\substack{8j+1\le i\le 8(j+1)-1\\ 2\nmid i}} \rho_{k,i}(8)\\ &= 2^{(r-3)(k-1)} 2^{r-3} \sum_{\substack{1\le i\le 7\\ 2\nmid i}} \rho_{k,i}(8)\\ &= 2^{(r-3)(k-1)} 2^{r-3} 2^{3k-1} = 2^{rk-1} = \varphi(2^{kr}).\end{aligned}$$

ii) Due to Lemma 1 it can be seen, as is the previous case, that

$$\Phi_k(p^r) = p^{k(r-1)} \sum_{i=1}^{p-1} \rho_{k,i}(p).$$

Thus, it is enough to apply Proposition 1. □

Finally, we summarize the previous work in the following result.

Theorem 1. *Let k be a positive integer. Then the function Φ_k is multiplicative and for every $n \in \mathbb{N}$,*

$$\Phi_k(n) = \begin{cases} n^{k-1}\varphi(n), & \text{if } k \text{ is odd;}\\ n^{k-1}\varphi(n) \prod\limits_{\substack{p\mid n\\ p>2}} \left(1 - \dfrac{(-1)^{k(p-1)/4}}{p^{k/2}}\right), & \text{if } k \text{ is even.}\end{cases}$$

Written more explicitly, we deduce that

$$\Phi_k(n) = \begin{cases} n^{k-1}\varphi(n), & \text{if } k \text{ is odd;}\\ n^{k-1}\varphi(n) \prod\limits_{\substack{p\mid n\\ p>2}} \left(1 - \dfrac{1}{p^{k/2}}\right), & \text{if } k \equiv 0 \pmod 4;\\ n^{k-1}\varphi(n) \prod\limits_{\substack{p\mid n\\ p\equiv 1 \pmod 4}} \left(1 - \dfrac{1}{p^{k/2}}\right) \prod\limits_{\substack{p\mid n\\ p\equiv -1 \pmod 4}} \left(1 + \dfrac{1}{p^{k/2}}\right), & \\ & \text{if } k \equiv 2 \pmod 4.\end{cases}$$

When k is a multiple of 4, Φ_k is closely related to $\mathbf{J}_{k/2}$. The following result, which follows from Theorem 1 and the definition of Jordan's totient function $\mathbf{J}_k$ makes this relation explicit.

Corollary 1. *Let $k \in \mathbb{N}$ be a multiple of 4 and let $n \in \mathbb{N}$. Then,*

$$\Phi_k(n) = n^{k/2-1}\mathbf{J}_{k/2}(n)\varphi(n)\frac{2^{k/2}}{2^{k/2}-1+n \pmod 2}.$$

Moreover, if $k/4$ is odd, then we have

$$\frac{\Phi_k(n)}{\Phi_{k/4}(n)} = n^{k/4}\mathbf{J}_{k/2}(n)\frac{2^{k/2}}{2^{k/2}-1+n \pmod 2}$$

Recall that in the case $k = 4$, $\Phi_4(n)$ is the number of units in the ring $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$. If, in addition, n is odd then $\Phi_4(n) = n\mathbf{J}_2(n)\varphi(n)$ which is the well-known formula for the number of regular matrices in the ring $\mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$. Of course, this is not a surprise since it is known that for an odd n the rings $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ and $\mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$ are isomorphic ([7]).

Some elementary properties of Φ_k, well known for Euler's function (the case $k = 1$) follow at once by Theorem 1. For example, we have

Corollary 2. *Let $k \in \mathbb{N}$ be fixed.*

i) *If $m, n \in \mathbb{N}$ such that $n \mid m$, then $\Phi_k(n) \mid \Phi_k(m)$.*
ii) *If $m, n \in \mathbb{N}$ and let $d = \gcd(m, n)$. Then $\Phi_k(mn)\Phi_k(d) = d^k\Phi_k(m)\Phi_k(m)$.*
iii) *If $n, m \in \mathbb{N}$, then $\Phi_k(n^m) = n^{km-k}\Phi_k(n)$.*

4. The average order of $\Phi_k(n)$

The average order of $\varphi(n)$ is well-known. Namely,

$$\frac{1}{x}\sum_{n\le x}\varphi(n) \sim \frac{3}{\pi^2}x \quad (x \to \infty),$$

see, for example, [10, Th. 330]. In fact, the best known asymptotic formula is due to Walfisz [22]:

$$\sum_{n\le x}\varphi(n) = \frac{3}{\pi^2}x^2 + O(x(\log x)^{2/3}(\log\log x)^{4/3}). \tag{5}$$

We now extend the validity of Walfisz result to Φ_k.

Theorem 2. *Let $k \in \mathbb{N}$ be any fixed integer. Then*

$$\sum_{n \le x} \Phi_k(n) = \frac{C_k}{k+1} x^{k+1} + O(x^k R_k(x)),$$

where

$$C_k = \frac{6}{\pi^2}, \quad R_k = (\log x)^{2/3} (\log\log x)^{4/3}, \quad \text{if } k \text{ is odd};$$

$$C_k = \frac{3}{4} \prod_{p>2} \left(1 - \frac{1}{p^2} - \frac{(-1)^{k(p-1)/4}(p-1)}{p^{k/2+2}}\right), \quad R_k(x) = \log x, \quad \text{if } k \text{ is even.}$$

Proof. If k is odd, then this result follows easily by partial summation from the fact that $\Phi_k(n) = n^{k-1}\varphi(n)$ using Walfisz' formula (5).

Assume now that $k \in \mathbb{N}$ is even. Since the function ϕ_k is multiplicative, we deduce by the Euler product formula that

$$\sum_{n=1}^{\infty} \frac{\Phi_k(n)}{n^s} = \zeta(s-k) G_k(s),$$

where

$$G_k(s) = \left(1 - \frac{1}{2^{s-k+1}}\right) \prod_{p>2} \left(1 - \frac{1}{p^{s-k+1}} - \frac{(-1)^{k(p-1)/4}(p-1)}{p^{s-k/2+1}}\right)$$

is absolutely convergent for $\Re s > k$. This shows that $\Phi_k = \mathrm{id}_k * g_k$ in terms of the Dirichlet convolution, where $\mathrm{id}_k(n) = n^k$ $(n \in \mathbb{N})$ and the multiplicative function g_k is defined by

$$g_k(p^r) = \begin{cases} -2^{k-1}, & \text{if } p = 2,\ r = 1; \\ -p^{k-1} - (-1)^{k(p-1)/4} p^{k/2-1}(p-1), & \text{if } p > 2,\ r = 1; \\ 0, & \text{otherwise.} \end{cases}$$

We obtain

$$\begin{aligned} \sum_{n \le x} \Phi_k(n) &= \sum_{de \le x} g_k(d) e^k = \sum_{d \le x} g_k(d) \sum_{e \le x} e^k = \sum_{d \le x} g_k(d) \left(\frac{(x/d)^{k+1}}{k+1} + O((x/d)^k)\right) \\ &= \frac{x^{k+1}}{k+1} G_k(k+1) + O\left(x^{k+1} \sum_{d > x} \frac{|g_k(d)|}{d^{k+1}}\right) + O\left(x^k \sum_{d \le x} \frac{|g_k(d)|}{d^k}\right). \end{aligned} \tag{6}$$

Here for every $k \ge 4$ we have

$$\sum_{d \le x} \frac{|g_k(d)|}{d^k} \le \prod_{p \le x} \sum_{r=0}^{\infty} \frac{|g_k(p^r)|}{p^{kr}} = \prod_{p \le x} \left(1 + \frac{|g_k(p)|}{p^k}\right) \ll \prod_{p \le x} \left(1 + \frac{p^{k-1} + p^{k/2-1} + p^{k/2}}{p^k}\right)$$

$$< \prod_{p\le x}\sum_{r=0}^{\infty}\frac{1}{p^r} = \prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \ll \log x$$

by Mertens's theorem. In the case $k=2$ this gives

$$\sum_{d\le x}\frac{|g_2(d)|}{d^2} \ll \prod_{\substack{p\le x\\ p\equiv 1 \pmod 4}}\left(1+\frac{2}{p}-\frac{1}{p^2}\right)\prod_{\substack{p\le x\\ p\equiv -1 \pmod 4}}\left(1+\frac{1}{p^2}\right)$$
$$\ll \prod_{\substack{p\le x\\ p\equiv 1 \pmod 4}}\left(1+\frac{1}{p}\right)^2 \ll \log x,$$

using that

$$\prod_{\substack{p\le x\\ p\equiv 1 \pmod 4}}\left(1-\frac{1}{p}\right) \sim c(\log x)^{-1/2},$$

with a certain constant c, cf. [21]. Hence the last last error term of (6) is $O(x^k\log x)$ for every $k\ge 2$ even.

Furthermore, note that for every $k\ge 2$, $|g_k(n)|\le n^{k/2}\sigma_{k/2-1}(n)$ $(n\in\mathbb{N})$, where $\sigma_t(n)=\sum_{d|n}d^t$. Using that $\sigma_t(n)<\zeta(t)n^t$ for $t>1$ we conclude that $|h_k(n)|\ll n^{k-1}$ for $k\ge 4$. Therefore,

$$\sum_{d>x}\frac{|g_k(d)|}{d^{k+1}} \ll \sum_{d>x}\frac{1}{d^2} \ll \frac{1}{x}.$$

In the case $k=2$, using that $\sigma_1(n)\ll n\log n$ (this suffices) we have $h_2(n)\ll n^3\log n$ and

$$\sum_{d>x}\frac{|g_2(d)|}{d^3} \ll \sum_{d>x}\frac{\log d}{d^2} \ll \frac{\log x}{x}.$$

Hence the first error term of (6) is $O(x^k)$ for $k\ge 4$ and it is $O(x^2\log x)$ for $k=2$. This completes the proof. □

Corollary 3 $(k=2,4)$**.**

$$\sum_{n\le x}\Phi_2(n) = \frac{x^3}{4}\prod_{p\equiv 1 \pmod 4}\left(1-\frac{2}{p^2}+\frac{1}{p^3}\right)\prod_{p\equiv -1 \pmod 4}\left(1-\frac{1}{p^3}\right)+O(x^2\log x),$$
$$\sum_{n\le x}\Phi_4(n) = \frac{3x^5}{20}\prod_{p>2}\left(1-\frac{1}{p^2}-\frac{1}{p^3}+\frac{1}{p^4}\right)+O(x^4\log x).$$

5. Conclusions and further work

The generalization of φ that we have presented in this paper is possibly one of the closest to the original idea which consists of counting units in a ring. In addition, both the elementary and asymptotic properties of Φ_k extend those of φ in a very natural way. There are many other results regarding φ that have not been considered here but that, nevertheless, may have their extension to Φ_k. For instance, in 1965 P. Kesava Menon [14] proved the following identity:

$$\sum_{\substack{1\le j\le n\\ \gcd(j,n)=1}} \gcd(j-1,n) = \varphi(n)d(n),$$

valid for every $n \in \mathbb{N}$, where $d(n)$ denotes the number of divisors of n. This identity has been generalized in several ways. See, for example [11], [12], [17], [19]. Also,

$$\sum_{\substack{1\le j\le n\\ \gcd(j,n)=1}} \gcd(j^2-1,n) = \varphi(n)h(n),$$

where h is a multiplicative function given explicitly in [19, Cor. 15]. Our work suggests the following generalization:

$$\sum_{\substack{1\le x_1,\dots,x_k\le n\\ \gcd(x_1^2+\cdots+x_k^2,n)=1}} \gcd(x_1^2+\cdots+x_k^2-1,n) = \Phi_k(n)\Psi_k(n),$$

where Ψ_k is a multiplicative function to be found.

Another question is on minimal order. As well known ([10, Th. 328]), the minimal order of $\varphi(n)$ is $e^{-\gamma}n(\log\log n)^{-1}$, where γ is Euler's constant, that is

$$\liminf_{n\to\infty} \frac{\varphi(n)\log\log n}{n} = e^{-\gamma}.$$

It turns out by Theorem 1 that for every $k \in \mathbb{N}$ odd,

$$\liminf_{n\to\infty} \frac{\Phi_k(n)\log\log n}{n^k} = e^{-\gamma}.$$

Find the minimal order of $\Phi_k(n)$ in the case when k is even.

References

[1] D. Andrica and M. Piticari, On some extensions of Jordan's arithmetic functions, *Acta Univ. Apulensis Math. Inform.* **7** (2004), 13–22.

[2] J. T. Cross, The Euler φ-function in the Gaussian integers, *Amer. Math. Monthly* **90** (1983), 518–528.

[3] L. E. Dickson, History of the theory of numbers, Vol. I: Divisibility and primality, *Chelsea Publishing Co.*, *New York*, 1966.

[4] L. E. Dickson., History of the theory of numbers, Vol. II: Diophantine analysis, *Chelsea Publishing Co.*, *New York*, 1966.

[5] J. Freed-Brown, M. Holden, M. E. Orrison and M. Vrable, Cyclotomic polynomials, symmetric polynomials, and a generalization of Euler's totient function, *Math. Mag.* **85** (2012), 44–50.

[6] P. G. Garcia and S. Ligh, A generalization of Euler's φ-function, *Fibonacci Quart.* **21** (1983), 26–28.

[7] J. M. Grau, C. Miguel and A. M. Oller-Marcén, On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$, *Adv. Appl. Clifford Algebr.* (*to appear*).

[8] J. M. Grau, A. M. Oller-Marcén, M. Rodríguez and D. Sadornil, Fermat test with Gaussian base and Gaussian pseudoprimes, *Czechoslovak Math. J.* (*to appear*).

[9] P. Hall, The Eulerian functions of a group, *Quart. J. Math.* **7** (1936), 134–151.

[10] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles, *Oxford University Press*, *Oxford*, 2008.

[11] P. Haukkanen and J. Wang, A generalization of Menon's identity with respect to a set of polynomials, *Portugal. Math.* **53** (1996), 331–337.

[12] P. Haukkanen, Menon's identity with respect to a generalized divisibility relation, *Aequationes Math.* **70** (2005), 240–246.

[13] J. Kaczorowski, On a generalization of the Euler totient function, *Monatsh. Math.* **170** (2013), 27–48.

[14] P. Kesava Menon, On the sum $\sum(a-1,n), [(a,n)=1]$, *J. Indian Math. Soc. (N.S.)* **29** (1965), 155–163.

[15] J. Sándor and B. Crstici, Handbook of number theory. II, *Kluwer Academic Publishers*, *Dordrecht*, 2004.

[16] R. Sivaramakrishnan, The many facets of Euler's totient. II. Generalizations and analogues, *Nieuw Arch. Wisk.* **8** (1990), 169–187.

[17] M. Tărnăuceanu, A generalization of Menon's identity, *J. Number Theory* **132** (2012), 2568–2573.

[18] S. Thajoddin and S. Vangipuram, A note on Jordan's totient function, *Indian J. Pure Appl. Math.* **19** (1988), 1156–1161.

[19] L. Tóth, Menon's identity and arithmetical sums representing functions of several variables, *Rend. Sem. Mat. Univ. Politec. Torino* **69** (2011), 97–110.

[20] L. Tóth, Counting solutions of quadratic congruences in several variables revisited, *J. Integer Seq.* **14** (2014), Article 14.11.6.

[21] S. Uchiyama, On some products involving primes, *Proc. Amer. Math. Soc.* **28** (1971), 629–630.

[22] A. Walfisz, Weylsche Exponentialsummen in der neueren Zahlentheorie, Mathematische Forschungsberichte, XV, *VEB Deutscher Verlag der Wissenschaften*, *Berlin*, 1963.

CATALINA CALDERÓN
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD DEL PAÍS VASCO
FACULTAD DE CIENCIA Y TECNOLOGÍA
BARRIO SARRIENA, S/N, 48940 LEIOA
SPAIN
E-mail: mtpcagac@lg.ehu.es

ANTONIO M. OLLER-MARCÉN
CENTRO UNIVERSITARIO DE LA DEFENSA
CTRA. DE HUESCA, S/N, 50090 ZARAGOZA
SPAIN
E-mail: oller@unizar.es

JOSÉ MARÍA GRAU
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD DE OVIEDO
AVDA. CALVO SOTELO, S/N, 33007 OVIEDO
SPAIN
E-mail: grau@uniovi.es

LÁSZLÓ TÓTH
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF PÉCS
IFJÚSÁG U. 6, H-7624 PÉCS
HUNGARY
E-mail: ltoth@gamma.ttk.pte.hu

(Received July 1, 2014; revised January 30, 2015)