Journal of Number Theory 200 (2019) 427–440

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Fast computation of the number of solutions to $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod n$

José María Grau [a], Antonio M. Oller-Marcén [b,*]

[a] Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
[b] Centro Universitario de la Defensa, Ctra. de Huesca, s/n, 50090 Zaragoza, Spain

A R T I C L E   I N F O

Article history:
Received 19 June 2018
Received in revised form 2 July 2018
Accepted 22 September 2018
Available online 18 October 2018
Communicated by L. Smajlovic

Keywords:
Congruence equation
Sum of squares

A B S T R A C T

In this paper we study the multiplicative function $\rho_{k,\lambda}(n)$ that counts the number of solutions of the equation $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod n$ in $(\mathbb{Z}/n\mathbb{Z})^k$. In particular we give closed explicit formulas for $\rho_{k,\lambda}(p^s)$. This leads to an algorithm with an arithmetic complexity of constant order that improves previous work by Tóth [10] and completes the quadratic case considered by Li and Ouyang in [8].

1. Introduction

Let k, λ and n be positive integers and let $\rho_{k,\lambda}(n)$ denote the number of incongruent solutions of the equation

$$P(x_1, \dots, x_k) := x_1^2 + x_2^2 + \cdots + x_k^2 \equiv \lambda \pmod n. \tag{1}$$

In other terms:

$$\rho_{k,\lambda}(n) := \text{card } \{(x_i, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : P(x_1, \dots, x_k) \equiv \lambda \pmod n\}$$

* Corresponding author.
E-mail addresses: grau@uniovi.es (J.M. Grau), oller@unizar.es (A.M. Oller-Marcén).

https://doi.org/10.1016/j.jnt.2018.09.015
0022-314X/

Since the function $\rho_{k,\lambda}$ is multiplicative, it is enough to consider the case when $n = p^s$ is a prime power. Moreover, it is also clear that we can introduce the restriction $0 \leq \lambda < n$.

The computation of $\rho_{k,\lambda}(n)$ by mere exhaustive search is obviously inefficient since its computational complexity has order $\Theta(n^k)$. Thus, the interest to find closed formulas involving a number of operations which is as small as possible.

Identities for $\rho_{k,\lambda}(n)$ can be derived using Gauss and Jacobi sums. In fact, we have (see [7]) a very compact expression like:

$$\rho_{k,\lambda}(n) = \frac{1}{n}\sum_{a=1}^{n} e^{-2\pi i \frac{a\lambda}{n}} \left(\sum_{x=1}^{n} e^{2\pi i \frac{ax^2}{n}}\right)^k. \tag{2}$$

This expression has theoretical value and it could even be practically applied for small values of n. Nevertheless, it is not useful for moderately big values of n, even in the particularly simple case $\lambda = 0$. This is because the arithmetic complexity of that formula is $\Theta(n^2)$.

Another compact expression can be found in [10]. Namely,

$$\rho_{k,\lambda}(n) = n^{k-1}\sum_{d|n}\frac{1}{d^k}\sum_{\substack{l=1\\ \gcd(l,n)=1}}^{d} e^{\frac{-2\pi i l\lambda}{d}} S(l,d)^k, \tag{3}$$

where $S(l,r)$ is the quadratic Gauss sum defined for every natural numbers l, r such that $\gcd(l,r) = 1$ by

$$S(l,r) := \sum_{j=1}^{r} e^{2\pi i \frac{lj^2}{r}}.$$

Formula (3) is more efficient than formula (2) because, if $n = p^s$, its arithmetic complexity is in fact linear $\Theta(n)$. However, it is also inefficient even for small values of s (especially if $\lambda \neq 0$) as we will show in the last section.

Some efficient explicit formulas are known for some particular cases. For instance, V.H. Lebesgue [5] gave in 1837 a closed formula for $\rho_{k,\lambda}(p)$. In [1, p. 46] a formula for $\rho_{k,0}(p^s)$ is given and the case $\gcd(\lambda, p) = 1$ was completely solved in [3]. Furthermore, in [10] and [4] we can find closed formulas for some particular cases of k and λ. Very recently, an algorithm has been provided in [8] to compute the value of $N_J(Q; \lambda, n)$ defined as the number of solutions in $(\mathbb{Z}/n\mathbb{Z})^k$ to the equation

$$Q(x_1,\ldots,x_k) := \alpha_1 x_1^{m_1} + \alpha_2 x_2^{m_2} + \cdots + \alpha_k x_k^{m_k} \equiv \lambda \pmod{n},$$

with the additional restriction that x_i is a unit for every $i \in J \subseteq \{1,...,k\}$.

Note that $\rho_{k,\lambda}(n) = N_{\emptyset}(P; \lambda, n)$. The algorithm given in [8, p. 51] is efficient in many cases, but not for $J = \emptyset$ in general. Even though we are in the quadratic case, the $J = \emptyset$

situation is not covered in (see [8, Theorem 4.4]) and it is only addressed in the more restricted $k = 2$ case. Thus, up to date, no general formula with constant (independent of k, λ and s) complexity for the computation of $\rho_{k,\lambda}(p^s)$ has been given. For example, it is not possible to compute in a reasonable time the value of $\rho_{10,5^{100000}}(5^{1000000})$ with the results that are known today. In this work, using elementary techniques that do not involve Gauss or Jacobi sums, we present explicit general formulas for $\rho_{k,\lambda}(p^s)$ with arithmetic complexity of constant order, $O(1)$.

The paper is organized as follows. In Sections 2 and 3 we present the basic theoretical results of the paper. In Section 4, based on the previous results, we provide the formulas that allow us to efficiently compute $\rho_{k,\lambda}(p^s)$ for any k, λ, p and s. Finally, in Section 5, we analyze and discuss the computational complexity of our algorithm and provide some comparative tables.

2. Known basic cases

The formulas for $\rho_{k,\lambda}(p^s)$ that we are going to present ultimately rely on the values of $\rho_{k,\lambda}(p)$ if p is an odd prime and on the values of $\rho_{k,\lambda}(2^s)$ with $1 \le s \le 3$ if $p = 2$.

As we already pointed out, when p is an odd prime the values of $\rho_{k,\lambda}(p)$ were already studied by V.H. Lebesgue in 1837. In particular he proved the following result [5, Chapter X], where $\left(\frac{\lambda}{p}\right)$ denotes the Legendre symbol defined by

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1, & \text{if } \lambda \text{ is a quadratic residue modulo } p; \\ -1, & \text{if } \lambda \text{ is a not a quadratic residue modulo } p; \\ 0, & \text{if } p \mid \lambda. \end{cases}$$

Proposition 1. *Let p be an odd prime and let k, λ be positive integers with $0 \le \lambda < p$. Put $t = (-1)^{(p-1)(k-1)/4} p^{(k-1)/2}$ and $l = (-1)^{k(p-1)/4} p^{(k-2)/2}$. Then,*

$$\rho_{k,\lambda}(p) = \begin{cases} p^{k-1} + \left(\frac{\lambda}{p}\right) t, & \textit{if } k \textit{ is odd}; \\ p^{k-1} - l + \left(1 - \left|\left(\frac{\lambda}{p}\right)\right|\right) pl, & \textit{if } k \textit{ is even}. \end{cases}$$

In the $p = 2$ case, formulas for $\rho_{k,\lambda}(2^s)$ with $1 \le s \le 3$ were given in [3] when λ is even. Here we complete it.

Proposition 2. *Let k be a positive integer. Then:*

i) $\rho_{k,1}(2) = \rho_{k,0}(2) = 2^{k-1}$,
ii) $\rho_{k,0}(4) = 4^{-1+k} + 2^{-1+\frac{3k}{2}} \cos(\frac{k\pi}{4})$,
iii) $\rho_{k,1}(4) = 4^{k-1} + 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$,
iv) $\rho_{k,2}(4) = 4^{-1+k} - 2^{-1+\frac{3k}{2}} \cos(\frac{k\pi}{4})$
v) $\rho_{k,3}(4) = 4^{k-1} - 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$,

vi) $\rho_{k,0}(8) = 8^{-1+k} + 2^{-2+2\,k}\,\cos(\frac{k\,\pi}{4}) + 2^{-2+\frac{5\,k}{2}}\,\cos(\frac{k\,\pi}{4}) + 2^{-2+2\,k}\,\cos(\frac{3\,k\,\pi}{4})$

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

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

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

x) $\rho_{k,4}(8) = 8^{-1+k} - 2^{-2+2\,k}\,\cos(\frac{k\,\pi}{4}) + 2^{-2+\frac{5\,k}{2}}\,\cos(\frac{k\,\pi}{4}) - 2^{-2+2\,k}\,\cos(\frac{3\,k\,\pi}{4})$

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

xii) $\rho_{k,6}(8) = 8^{-1+k} - 2^{-2+\frac{5\,k}{2}}\,\cos(\frac{k\,\pi}{4}) - 2^{-2+2\,k}\,\sin(\frac{k\,\pi}{4}) + 2^{-2+2\,k}\,\sin(\frac{3\,k\,\pi}{4})$,

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

Proof. 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 $R_k(n) = (\rho_{k,i}(n))_{0\le i\le n-1}$, the following recurrence relation holds:

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

Then, it is enough to apply elementary linear algebra techniques. For details, see [3, Lemma 4]. $\square$

3. Preparatory results

Given positive integers k, n and $0 \le \lambda < n$, let $A(k,\lambda,n)$ denote the set of solutions $(x_1,\dots,x_k) \in (\mathbb{Z}/n\mathbb{Z})^k$ of the congruence $x_1^2+\cdots+x_k^2 \equiv \lambda \pmod{n}$. In particular, if $n = p^s$ is a prime-power, we have that

$$A(k,\lambda,p^s) = \{(x_1,...,x_k) \in (\mathbb{Z}_{p^s})^k : x_1^2+\cdots+x_k^2 \equiv \lambda \pmod{p^s}\}.$$

Now, in this situation, let us define the following sets:

$$A_1(k,\lambda,p^s) = \{(x_1,...,x_k) \in A(k,\lambda,p^s) : p \nmid x_i \text{ for some } 1 \le i \le k\},$$

$$A_2(k,\lambda,p^s) = \{(x_1,...,x_k) \in A(k,\lambda,p^s) : p \mid x_i \text{ for every } 1 \le i \le k\}.$$

Note that $A(k,\lambda,p^s) = A_1(k,\lambda,p^s) \cup A_2(k,\lambda,p^s)$. Hence, since $A_1(k,\lambda,p^s)$ and $A_2(k,\lambda,p^s)$ are disjoint, if we define $\rho^{(1)}_{k,\lambda}(p^s) := \operatorname{card}(A_1(k,\lambda,p^s))$ and $\rho^{(2)}_{k,\lambda}(p^s) := \operatorname{card}(A_2(k,\lambda,p^s))$ it follows that

$$\rho_{k,\lambda}(p^s) = \rho^{(1)}_{k,\lambda}(p^s) + \rho^{(2)}_{k,\lambda}(p^s).$$

Remark 1. If $\gcd(\lambda,p) = 1$; i.e., if $p \nmid \lambda$ then $A_2(k,\lambda,p^s) = \emptyset$. Thus, $\rho^{(2)}_{k,\lambda}(p^s) = 0$ and it follows that $\rho^{(1)}_{k,\lambda}(p^s) = \rho_{k,\lambda}(p^s)$.

This remark implies that the proof of the following result is the same as that of Lemmata 1 and 2 in [3].

Proposition 3.

i) *Let p^s be an odd prime-power with $s \geq 1$ and $0 \leq \lambda < p^s$. Then,*

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

ii) *Let $s \geq 3$ and $0 \leq \lambda < 2^s$. Then, $\rho_{k,\lambda}^{(1)}(2^s) = 2^{(s-3)(k-1)}\rho_{k,\lambda}^{(1)}(8)$.*

Proposition 3 provides us with a recursive relation for $\rho_{k,\lambda}^{(1)}(p^s)$. Note that this result implies that we will have to study the case $p = 2$ separately.

Now we turn to $\rho_{k,\lambda}^{(2)}(p^s)$. In this case, we have the following result.

Proposition 4. *Let p^s be a prime-power, with $s \geq 1$ and let $0 \leq \lambda < p^s$. Then,*

$$\rho_{k,\lambda}^{(2)}(p^s) = \begin{cases} 1, & \text{if } s = 1 \text{ and } \lambda = 0; \\ p^k, & \text{if } s = 2 \text{ and } \lambda = 0; \\ p^k \rho_{k,\lambda/p^2}(p^{s-2}), & \text{if } s \geq 3 \text{ and } p^2 \mid \lambda; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $s = 1$ and $\lambda = 0$, it is obvious that the only k-tuple $(x_1, \dots, x_k)$ such that $x_1^2 + \cdots + x_k^2 \equiv 0 \pmod p$ and $p \mid x_i$ for every i is $(0, \dots, 0)$. Hence, $\rho_{k,\lambda}^{(2)}(p^s) = 1$ in this case.

Secondly, if $s = 2$ and $\lambda = 0$, $\rho_{k,\lambda}^{(2)}(p^2) = \rho_{k,0}^{(2)}(p^2)$ is the number of k-tuples $(x_1, \dots, x_k)$ such that $x_1^2 + \cdots + x_k^2 \equiv 0 \pmod{p^2}$ and $p \mid x_i$ for every i. It is obvious that there are p^k such k-tuples because x_i can be any multiple of p in $\mathbb{Z}/p^2\mathbb{Z}$.

Now, assume that $p^2 \mid \lambda$ and $s \geq 3$. First of all, using Euclid's algorithm, it is easy to see that every element of $A_2(k, \lambda, p^s)$ can be written in the form $(px_1 + \alpha_1 p^{s-1}, \dots, px_k + \alpha_k p^{s-1})$ with $0 \leq \alpha_i \leq p - 1$ and $(x_1 \dots, x_k) \in A(k, \lambda/p^2, p^{s-2})$.

On the other hand, let $(x_1, \dots, x_k) \in A(k, \lambda/p^2, p^{s-2})$; i.e., $x_1^2 + \cdots + x_k^2 \equiv \lambda/p^2 \pmod{p^{s-2}}$. Clearly the set

$$\{(px_1 + \alpha_1 p^{s-1}, \dots, px_k + \alpha_k p^{s-1}) : 0 \leq \alpha_i \leq p - 1 \text{ for every } 1 \leq i \leq k\}$$

is contained in $A_2(k, \lambda, p^s)$ because

$$(px_1 + \alpha_1 p^{s-1})^2 + \cdots + (px_k + \alpha_k p^{s-1})^2 \equiv p^2(x_1^2 + \cdots + x_k^2) \equiv \lambda \pmod{p^s}$$

and all its elements are incongruent modulo p^s. Thus, every element of the set $A(k, \lambda/p^2, p^{s-2})$ gives rise to p^k different elements of $A_2(k, \lambda, p^s)$ and the result follows.

Finally, in the remaining cases (i.e., if $s = 1$ or 2 with $0 < \lambda < p^2$ or if $s \geq 3$ with $p^2 \nmid \lambda$) it is obvious that $A_2(k, \lambda, p^s) = \emptyset$ and hence $\rho^{(2)}_{k,\lambda}(p^s) = 0$, as claimed. □

With the help of Proposition 3 and Proposition 4 we can give recursive formulas that express the value of $\rho_{k,\lambda}(p^s)$. First, we deal with the odd p and non-zero λ case.

Theorem 1. *Let p^s be an odd prime-power and let $0 < \lambda < p^s$ be an integer. Put $\lambda = p^r \lambda'$ with $0 \leq r < s$ and $p \nmid \lambda'$. Then,*

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{\lfloor r/2 \rfloor} p^{ki+(s-2i-1)(k-1)} \cdot \rho^{(1)}_{k,\lambda/p^{2i}}(p).$$

Proof. We have that $\rho_{k,\lambda}(p^s) = \rho^{(1)}_{k,\lambda}(p^s) + \rho^{(2)}_{k,\lambda}(p^s)$. If $r \leq 1$, then Proposition 4 implies that $\rho^{(2)}_{k,\lambda}(p^s) = 0$. Hence, $\rho_{k,\lambda}(p^s) = \rho^{(1)}_{k,\lambda}(p^s) = p^{(s-1)(k-1)}\rho^{(1)}_{k,\lambda}(p)$ due to Proposition 3 and we are done.

Now, if $r \geq 2$ the $s \geq 3$ and Proposition 4 implies that

$$\rho^{(2)}_{k,\lambda}(p^s) = p^k \rho_{k,\lambda/p^2}(p^{s-2}) = p^k \rho^{(1)}_{k,\lambda/p^2}(p^{s-2}) + p^k \rho^{(2)}_{k,\lambda/p^2}(p^{s-2}).$$

Thus, using Proposition 3 again we obtain that

$$\rho_{k,\lambda}(p^s) = p^{(s-1)(k-1)}\rho^{(1)}_{k,\lambda}(p) + p^k p^{(s-3)(k-1)}\rho^{(1)}_{k,\lambda/p^2}(p) + p^k \rho^{(2)}_{k,\lambda/p^2}(p^{s-2}).$$

Since $\lambda/p^2 = p^{r-2}\lambda'$, if $r - 2 \leq 1$, then $\rho^{(2)}_{k,\lambda/p^2}(p^{s-2}) = 0$ by Proposition 4 and we are done.

If, on the other hand, $r \geq 4$ then $s - 2 \geq 3$ and Proposition 4 implies that $\rho^{(2)}_{k,\lambda/p^2}(p^{s-2}) = p^k \rho^{(2)}_{k,\lambda/p^4}(p^{s-4})$. Thus, using Proposition 3 again, it follows that

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{2} \left(p^{ki+(s-2i-1)(k-1)} \rho^{(1)}_{k,\lambda/p^{2i}}(p) \right) + p^{2k} \rho^{(2)}_{k,\lambda/p^4}(p^{s-4}).$$

Clearly this process can be iteratively repeated until we reach the expression

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{\lfloor r/2 \rfloor} \left(p^{ki+(s-2i-1)(k-1)} \cdot \rho^{(1)}_{k,\lambda/p^{2i}}(p) \right) + p^{k\lfloor r/2 \rfloor} \rho^{(2)}_{k,\lambda/p^{2\lfloor r/2 \rfloor}}(p^{s-2\lfloor r/2 \rfloor})$$

and, since $p^2 \nmid \lambda/p^{2\lfloor r/2 \rfloor}$ the result follows from Proposition 4. □

Now, we turn to the $\lambda = 0$ case for an odd prime p.

Theorem 2. *Let p^s be an odd prime-power. Then,*

$$\rho_{k,0}(p^s) = \sum_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(p^{ki} p^{(s-2i-1)(k-1)} \cdot \rho^{(1)}_{k,p^{s-2i}}(p) \right) + p^{\lfloor s/2 \rfloor k}.$$

Proof. First of all, note that $\rho_{k,0}(p^s) = \rho_{k,p^s}(p^s)$. Then we can proceed recursively just like in Theorem 1 because $\rho_{k,p^s}(p^s) = \rho^{(1)}_{k,p^s}(p^s) + \rho^{(2)}_{k,p^s}(p^s)$.

If $s = 1$, then $\rho_{k,p}(p) = \rho^{(1)}_{k,p}(p) + \rho^{(2)}_{k,p}(p) = \rho^{(1)}_{k,p}(p) + 1$ due to Proposition 4.

If $s = 2$, $\rho_{k,p^2}(p^2) = \rho^{(1)}_{k,p^2}(p^2) + \rho^{(2)}_{k,p^2}(p^2) = p^{k-1}\rho^{(1)}_{k,p^2}(p) + p^k$ due to Propositions 3 and 4.

Now, if $s \geq 3$, then Propositions 3 and 4 imply that

$$\rho_{k,p^s}(p^s) = \rho^{(1)}_{k,p^s}(p^s) + \rho^{(2)}_{k,p^s}(p^s) = p^{(s-1)(k-1)}\rho_{k,p^s}(p) + p^k \rho_{k,p^{s-2}}(p^{s-2})$$

If $s - 2 = 1$ or $s - 2 = 2$, then we apply Proposition 4 and the result follows. If, on the other hand, $s - 2 \geq 3$ then

$$\rho_{k,p^s}(p^s) = p^{(s-1)(k-1)}\rho_{k,p^s}(p) + p^k \left(\rho^{(1)}_{k,p^{s-2}}(p^{s-2}) + \rho^{(2)}_{k,p^{s-2}}(p^{s-2}) \right)$$

so applying Propositions 3 and 4 again we get that

$$\rho_{k,p^s}(p^s) = p^{(s-1)(k-1)}\rho_{k,p^s}(p) + p^k p^{(s-3)(k-1)}\rho_{k,p^{s-2}}(p) + p^k \rho_{k,p^{s-4}}(p^{s-4}).$$

To conclude the proof it is enough to observe that the previous process will end after $\lfloor (s-1)/2 \rfloor$ steps and hence after $\lfloor (s-1)/2 \rfloor + 1$ applications of Propositions 3 and 4. $\square$

Now, for the case $p = 2$ and non-zero λ we have the following result.

Theorem 3. *Let 2^s be a power of two ($s \geq 1$) and let $0 < \lambda < 2^s$ be an integer. Put $\lambda = 2^r \lambda'$ with $0 \leq r < s$ and odd λ'. Then,*

$$\rho_{k,\lambda}(2^s) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor - 1} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho^{(1)}_{k,\lambda/2^{2i}}(8) \right) + 2^{k \lfloor \frac{r}{2} \rfloor} \rho^{(1)}_{k,\lambda/2^{2\lfloor \frac{r}{2} \rfloor}}(2^{s-2\lfloor \frac{r}{2} \rfloor}).$$

Proof. The proof goes exactly as in Theorem 1 using Proposition 3 and Proposition 4 repeatedly. Note that, in the cases $r = 0$ and $r = 1$ we consider that if the upper summation limit is -1, the sum is empty. $\square$

And finally, the case $p = 2$, and $\lambda = 0$ is given by the following result.

Theorem 4. *Let 2^s be a power of two ($s \geq 1$). Then,*

$$\rho_{k,0}(2^s) = \sum_{i=0}^{\lfloor \frac{s-1}{2} \rfloor -1} \left(2^{ki} 2^{(s-2i-3)(k-1)} \cdot \rho^{(1)}_{k,2^{s-2i}}(8) \right) + 2^{\lfloor \frac{s-1}{2} \rfloor k} \cdot \rho^{(1)}_{k,0}(2^{s-2\lfloor \frac{s-1}{2} \rfloor}) + 2^{\lfloor \frac{s}{2} \rfloor k}.$$

Proof. The proof goes exactly as in Theorem 2 using Proposition 3 and Proposition 4 repeatedly. Note that, in the cases $s = 1$ and $s = 2$ we consider that if the upper summation limit is -1, the sum is empty. □

4. Fast computation of $\rho_{k,\lambda}(p^s)$

With the results that we have proved in the previous section, we have a procedure to compute $\rho_{k,\lambda}(p^s)$ which has arithmetic complexity of order $\mathcal{O}(s)$. Nevertheless, as we are going to see in this section, it is possible to obtain formulas requiring a constant number of operations.

To do so, given integer numbers k, p, s and N, we define the function

$$\Omega(k, p, s, N) := \sum_{i=0}^{N} p^{ki+(s-2i-1)(k-1)}.$$

Since it is essentially a geometric series, the following result is straightforward.

Lemma 1. *Let k, p, s and N be integer numbers. Then,*

$$\Omega(k, p, s, N) = \begin{cases} \frac{-1+p^{1+N}}{-1+p}, & \textit{if } k = 1; \\ p^{-1+s}(1+N), & \textit{if } k = 2; \\ \frac{p^{(-1+k)\,(-1+s)}\left(p^k - p^2\left(p^{2-k}\right)^N\right)}{-p^2+p^k}, & \textit{otherwise.} \end{cases}$$

The following result will also be useful in the sequel.

Lemma 2.

i) *Let p be any prime and let $0 \leq \lambda < p$. Then,*

$$\rho^{(1)}_{k,\lambda}(p) = \begin{cases} \rho_{k,\lambda}(p) - 1, & \textit{if } \lambda = 0; \\ \rho_{k,\lambda}(p), & \textit{if } \lambda \neq 0. \end{cases}$$

ii) *Let $0 \leq \lambda < 4$. Then,*

$$\rho^{(1)}_{k,\lambda}(4) = \begin{cases} \rho_{k,\lambda}(4) - 2^k, & \textit{if } \lambda = 0; \\ \rho_{k,\lambda}(4), & \textit{if } \lambda \neq 0. \end{cases}$$

iii) *Let* $0 \le \lambda < 8$. *Then,*

$$\rho^{(1)}_{k,\lambda}(8) = \begin{cases} \rho_{k,\lambda}(8) - 2^{2k-1}, & \text{if } \lambda = 0, 4; \\ \rho_{k,\lambda}(8), & \text{if } \lambda \neq 0, 4. \end{cases}$$

Proof. Just recall that $\rho^{(1)}_{k,\lambda}(n) = \rho_{k,\lambda}(n) - \rho^{(2)}_{k,\lambda}(n)$ and apply Proposition 4. $\square$

Corollary 1. *Let* p^s *be an odd prime-power and let* $0 < \lambda < p^s$ *be an integer. Put* $\lambda = p^r\lambda'$ *with* $0 \le r < s$ *and* $p \nmid \lambda'$. *Then,*

$$\rho_{k,\lambda}(p^s) = \begin{cases} \Omega(k,p,s,\frac{r-1}{2}) \cdot (\rho_{k,0}(p) - 1), & \text{if } r \text{ is odd;} \\ \Omega(k,p,s,\frac{r-2}{2}) \cdot (\rho_{k,0}(p) - 1) + p^{k\frac{r}{2}+(s-r-1)(k-1)} \cdot \rho_{k,\lambda'}(p), & \text{if } r \text{ is even .} \end{cases}$$

Proof. Using Lemma 2 the following hold:

- If r is odd, then for every $i \le \lfloor r/2 \rfloor$ we have that $\rho^{(1)}_{k,\lambda/p^{2i}}(p) = \rho^{(1)}_{k,0}(p) = \rho_{k,0}(p) - 1$.
- On the other hand, if r is even then $\rho^{(1)}_{k,\lambda/p^{2i}}(p) = \rho^{(1)}_{k,0}(p) = \rho_{k,0}(p) - 1$ for every $i < r/2$, while $\rho^{(1)}_{k,\lambda/p^{2i}}(p) = \rho_{k,\lambda'}(p)$ for $i = r/2$.

Hence, from Theorem 1 it follows that

$$\rho_{k,\lambda}(p^s) = \sum_{i=0}^{r/2-1} p^{ki+(s-2i-1)(k-1)} \cdot (\rho_{k,0}(p) - 1) + p^{kr/2+(s-r-1)(k-1)} \cdot \rho_{k,\lambda'}(p)$$

and Lemma 1 concludes the proof. $\square$

Corollary 2. *Let* p^s *be an odd prime-power. Then,*

$$\rho_{k,0}(p^s) = \Omega(k,p,s,\lfloor \frac{s-1}{2} \rfloor) \cdot (\rho_{k,0}(p) - 1) + p^{k\lfloor s/2 \rfloor}$$

Proof. First, observe that $s - 2i > 0$ for every $i \le \lfloor \frac{s-1}{2} \rfloor$. Thus, Lemma 2 implies that $\rho^{(1)}_{k,p^{s-2i}}(p) = \rho_{k,0}(p) - 1$. Consequently, it is enough to apply Theorem 2 to get that

$$\rho_{k,0}(p^s) = (\rho_{k,0}(p) - 1) \cdot \sum_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(p^{ki} p^{(s-2i-1)(k-1)} \right) + p^{\lfloor s/2 \rfloor k}$$

and the result follows. $\square$

Corollary 3. *Let* 2^s *be a power of two* ($s \ge 3$) *and let* $0 < \lambda < 2^s$ *be an integer. Put* $\lambda = 2^r\lambda'$ *with* $0 \le r < s$ *and odd* λ'. *Then,*

i) *If r is odd and $s-r>1$,*

$$\rho_{k,\lambda}(2^s)=\frac{\Omega(k,2,s,\frac{r-3}{2})}{2^{2(k-1)}}\cdot(\rho_{k,0}(8)-2^{2k-1})+2^{k\frac{r-1}{2}+(s-r-2)(k-1)}\rho_{k,\lambda'2}(8).$$

ii) *If r is odd and $s-r=1$,*

$$\rho_{k,\lambda}(2^s)=\frac{\Omega(k,2,s,\frac{r-3}{2})}{2^{2(k-1)}}\cdot(\rho_{k,0}(8)-2^{2k-1})+2^{k\frac{r-1}{2}}\rho_{k,2\lambda'}(4).$$

iii) *If r is even and $s-r>2$,*

$$\rho_{k,\lambda}(2^s)=\frac{1}{2^{2(k-1)}}\Omega(k,2,s,\frac{r-4}{2})\cdot(\rho_{k,0}(8)-2^{2k-1})+ \\ +2^{1+r-s+k\,(-2-\frac{r}{2}+s)}(\rho_{k,4\lambda'}(8)-2^{2k-1})+2^{k\frac{r}{2}+(s-r-3)(k-1)}\rho_{k,\lambda'}(8).$$

iv) *If r is even and $s-r=2$,*

$$\rho_{k,\lambda}(2^s)=\frac{1}{2^{2(k-1)}}\Omega(k,2,s,\frac{r-4}{2})\cdot(\rho_{k,0}(8)-2^{2k-1})+ \\ +2^{1+r-s+k\,(-2-\frac{r}{2}+s)}(\rho_{k,4\lambda'}(8)-2^{2k-1})+2^{k\frac{r}{2}}\rho_{k,\lambda'}(4).$$

v) *If r is even and $s-r=1$,*

$$\rho_{k,\lambda}(2^s)=\frac{1}{2^{2(k-1)}}\Omega(k,2,s,\frac{r-4}{2})\cdot(\rho_{k,0}(8)-2^{2k-1})+ \\ +2^{1+r-s+k\,(-2-\frac{r}{2}+s)}(\rho_{k,4\lambda'}(8)-2^{2k-1})+2^{k\frac{r}{2}}\rho_{k,\lambda'}(2).$$

Proof. i) If r is odd and $s-r>1$, then $r-2i\geq 3$ for every $i\leq\lfloor\frac{r}{2}-1\rfloor$. Consequently,

$$\rho^{(1)}_{k,\lambda/2^{2i}}(8)=\rho^{(1)}_{k,0}(8)=\rho_{k,0}(8)-2^{2k-1}$$

due to Lemma 2 and

$$\sum_{i=0}^{\lfloor\frac{r}{2}\rfloor-1}\left(2^{ki}2^{(s-2i-3)(k-1)}\cdot\rho^{(1)}_{k,\lambda/2^{2i}}(8)\right)=\frac{1}{2^{2(k-1)}}\Omega(k,2,s,r,\frac{r-3}{2})\cdot(\rho_{k,0}(8)-2^{2k-1}).$$

Finally, since

$$2^{k\lfloor\frac{r}{2}\rfloor}\rho^{(1)}_{k,\lambda/2^{2\lfloor\frac{r}{2}\rfloor}}(2^{s-2\lfloor\frac{r}{2}\rfloor})=2^{k\lfloor\frac{r}{2}\rfloor}\rho^{(1)}_{k,2\lambda'}(2^{s-r+1})=2^{k\frac{r-1}{2}+(s-r-2)(k-1)}\rho_{k,2\lambda'}(8)$$

the result follows in this case.

ii) If r is odd and $s-r=1$, we proceed like in the previous case but now we have that

$$2^{k\lfloor\frac{r}{2}\rfloor}\rho^{(1)}_{k,2\lambda'}(2^{s-r+1})=2^{k\lfloor\frac{r}{2}\rfloor}\rho^{(1)}_{k,2\lambda'}(4)=2^{k\lfloor\frac{r}{2}\rfloor}\rho_{k,2\lambda'}(4).$$

iii) If r is even and $s-r>2$, then $r-2i\geq 3$ for every $i<\lfloor \frac{r}{2}-1\rfloor$, while $r-2i=2$ for $i=\lfloor \frac{r}{2}-1\rfloor$. Thus,

$$\sum_{i=0}^{\lfloor \frac{r}{2}\rfloor-1}\Big(2^{ki}2^{(s-2i-3)(k-1)}\cdot\rho^{(1)}_{k,\lambda/2^{2i}}(8)\Big)=$$

$$=\sum_{i=0}^{\frac{r-4}{2}}\Big(2^{ki}2^{(s-2i-3)(k-1)}\cdot\rho^{(1)}_{k,0}(8)\Big)+2^{1+r-s+k\,(-2-\frac{r}{2}+s)}(\rho^{1}_{k,4\lambda'}(8))=$$

$$=\sum_{i=0}^{\frac{r-4}{2}}\Big(2^{ki}2^{(s-2i-3)(k-1)}\cdot\rho_{k,0}(8)\Big)+2^{1+r-s+k\,(-2-\frac{r}{2}+s)}(\rho_{k,4\lambda'}(8)-2^{2k-1}).$$

iv) and v) If r is even and $1\leq s-r\leq 2$, we proceed like in the previous case but now we have that

$$2^{k\lfloor\frac{r}{2}\rfloor}\rho^{(1)}_{k,\lambda/2^{2\lfloor\frac{r}{2}\rfloor}}(2^{s-2\lfloor\frac{r}{2}\rfloor})=2^{k\frac{r}{2}}\rho^{(1)}_{k,\lambda'}(2^{s-r})=2^{k\frac{r}{2}}\rho_{k,\lambda'}(2^{s-r}).\quad\square$$

Corollary 4. *Let 2^s be a power of two ($s\geq 3$). Then,*

$$\rho_{k,0}(2^s)=\begin{cases}\frac{1}{2^{2(k-1)}}\Omega(k,2,s,\frac{s-3}{2})\Big(\rho_{k,0}(8)-2^{2k-1}\Big)+2^{\frac{s-1}{2}k}\cdot 2^{k-1}+2^{\frac{s-1}{2}}, \\ \qquad \text{if } r \text{ is odd;}\\ \frac{1}{2^{2(k-1)}}\Omega(k,2,s,\frac{s-4}{2})\Big(\rho_{k,0}(8)-2^{2k-1}\Big)+2^{\frac{s-2}{2}k}\cdot(\rho_{k,0}(4)-2^k)+2^{\frac{s}{2}k}, \\ \qquad \text{if } r \text{ is even.}\end{cases}$$

Proof. For every $i\leq\lfloor\frac{s-1}{2}\rfloor-1$ we have that

$$\rho^{(1)}_{k,2^{s-2i}}(8)=\rho^{(1)}_{k,0}(8)=\rho_{k,0}(8)-2^{2k-1}.$$

Now, if r is odd

$$\rho^{(1)}_{k,0}(2^{s-2\lfloor\frac{s-1}{2}\rfloor})=\rho^{(1)}_{k,0}(2)=2^{k-1}.$$

While, if r is even

$$\rho^{(1)}_{k,0}(2^{s-2\lfloor\frac{s-1}{2}\rfloor}=\rho^{(1)}_{k,0}(4)=\rho_{k,0}(4)-2^k.$$

In any case, it suffices to apply Theorem 4. $\square$

Table 1
Time (in seconds) required to compute $\rho_{3,0}(3^s)$.

s	$\rho_{3,0}(3^s)$	Using (3)	Using Corollary 2
1	9	0.	0.
2	99	0.	0.
3	891	0.	0.
4	8505	0.	0.
5	76545	0.	0.
6	702027	0.	0.
7	6318243	0.14	0.
8	57218481	0.20	0.
9	514966329	1.20	0.
10	4644262899	1.71	0.
11	41798366091	11.18	0.
12	376443575145	15.88	0.
13	3387992176305	32.19	0.
14	30498903155547	43.66	0.
15	274490128399923	189.54	0.
16	2470599441956961	309.78	0.

5. Computational complexity of the computation of $\rho_{k,\lambda}(p^s)$

In this section we analyze the computational complexity of the computation of $\rho_{k,\lambda}(p^s)$ using the results given in Corollaries 1 through 4. In particular, we show that this complexity is $O(1)$. In what follows, the term "arithmetic operation" may refer to either addition, subtraction, product, division or Legendre symbol.

Proposition 5. *The number of arithmetic operations required to compute $\rho_{k,\lambda}(p^s)$ is $O(1)$; i.e., it is bounded by a constant independent of k, λ, p and s.*

Proof. First of all, we note that $\Omega(k, p, s, N)$ can be computed with, at most, 14 arithmetic operations. In addition, if p is odd, Proposition 1 implies that the computation of $\rho_{k,\lambda}(p)$ requires a bounded number of arithmetic operations. In the same way, Proposition 2 implies that the computation of $\rho_{k,\lambda}(2)$, $\rho_{k,\lambda}(4)$ and $\rho_{k,\lambda}(8)$ requires also a bounded number of arithmetic operations.

Finally Corollaries 1 and 2 provide a formula for the computation of $\rho_{k,\lambda}(p^s)$ with a bounded number of arithmetic operations if p is odd, while, for $p = 2$, Corollaries 3 and 4 do the same for the computation of $\rho_{k,\lambda}(p^s)$. □

In order to check the efficiency of our algorithm we are going to present some tables comparing the computation time using our formula versus the most efficient formula known so far (3). Note that if $k > 2$, we cannot apply [8, Theorem 4.4] because we are dealing with the case $J = \emptyset$ as we pointed out in the introduction. If $k = 2$ our results are essentially the same as those in [8, Proposition 4.8].

In Table 1 we compare the computation time (in seconds) required to compute $\rho_{3,0}(3^s)$ for $0 < s < 17$ using (3) and Corollary 2. Although it exceeded our computing capabilities, it is easy to extrapolate that the computation of $\rho_{3,0}(3^{100})$ using (3) would require several millenniums. In Table 2 we make the same kind of comparison using an example

Table 2
Time (in seconds) required to compute $\rho_{4,5}(5^s)$.

s	$\rho_{4,5}(5^s)$	Using (3)	Using Corollary 2
2	18000	0.	0.
3	2250000	0.01	0.
4	281250000	0.03	0.
5	35156250000	0.29	0.
6	4394531250000	1.4	0.
7	549316406250000	17.12	0.
8	68664550781250000	95.19	0.
9	8583068847656250000	426.	0.
10	1072883605957031250000	2101.	0.

Table 3
Time (in seconds) required to compute $\rho_{10^s,0}(9)$.

s	Using (3)	Using Corollary 2	Size of $\rho_{10^s,0}(9)$
1	0.	0.	9
2	0.	0.	95
3	0.	0.	954
4	0.01	0.	9542
5	0.15	0.1	95424
6	3.96	0.57	954242
7	58.09	8.59	9542425
8	745.25	99.25	95424250

with $\lambda \neq 0$. As mentioned in the introduction, we see that for $\lambda \neq 0$ formula (3) performs worse, while our formula behaves essentially in the same way.

With the formulas that we have presented in this paper, the number of required arithmetic operations is of constant order. For example, Table 1 could be extended using just a domestic PC computing, almost instantly, for values of s up to 10^5. However, the mentioned arithmetic operations involve powers of integers as well as the computation of Legendre symbols in order to obtain the value of $\rho_{k,\lambda}(p)$ via Proposition 1. These operations, when considered bit-wise, have a computational cost that increases with the size of the inputs. This becomes apparent when the involved parameters are very big.

If we have a look at the formulas presented in the previous section, those operations whose computational cost dominates over the others are the computation of the power p^{ks} and the computation of the Legendre symbol. Their computational bit-level complexity is, respectively, $O(M(\log(p))\log(ks))$ and $O(M(\log(p))\log\log(p))$, where $M(n)$ represents the computational complexity of the chosen multiplication algorithm [2]. This gives an idea of which is the influence of each parameter over the overall computational cost of our procedure, as well as of its limitations. In fact, this reveals that the influence of the parameters k and s is similar (logarithmic order complexity) and somewhat lower to that of the prime p when considering, for instance, the Schönhage–Strassen multiplication algorithm whose computational complexity for the product of two numbers of size n is $M(n) = O(n\log(n)\log\log(n))$ [9] or Fürer's algorithm [6], which runs in time $O(n\log(n)2^{O(\log^*(n))})$.

In Table 3 we illustrate the impact of the size of k on the computing time of $\rho_{k,\lambda}(p^s)$ in order to clarify our previous comments. Nevertheless, the improvement of our algorithm is still very significant.

References

[1] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, New York, 1998.

[2] R.P. Brent, P. Zimmermann, An $O(M(n)\log n)$ algorithm for the Jacobi symbol, in: Proceedings of ANTS-IX, in: Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 83–95.

[3] C. Calderón, J.M. Grau, A.M. Oller-Marcén, L. Tóth, Counting invertible sums of squares modulo n and a new generalization of Euler's totient function, Publ. Math. Debrecen 87 (1–2) (2015) 133–145.

[4] C. Calderón, M.J. de Velasco, On divisors of a quadratic form, Bol. Soc. Bras. Mat. 31 (1) (2000) 81–91.

[5] L.E. Dickson, History of the Theory of Numbers. Vol. I: Divisibility and Primality, Chelsea Publishing Co., New York, 1966.

[6] M. Fürer, Faster integer multiplication, SIAM J. Comput. 39 (3) (2009) 979–1005.

[7] N.M. Korobov, Las sumas trigonométricas y sus aplicaciones Servicio, Editorial de la Universidad del País Vasco, Bilbao, 1993.

[8] S. Li, Y. Ouyang, Counting the solutions of $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t} \equiv c \pmod{n}$, J. Number Theory 187 (2018) 41–65.

[9] A. Schönhage, V. Strassen, Schnelle Multiplikation großer Zahlen, Computing 7 (1971) 281–292.

[10] L. Tóth, Counting solutions of quadratic congruences in several variables revisited, J. Integer Seq. 17 (2014) Article 14.11.6.