Counting Solutions of Quadratic Congruences in Several Variables Revisited

László Tóth

Journal of Integer Sequences, Vol. 17 (2014), Article 14.11.6

Abstract

Let $N_k(n,r,\boldsymbol{a})$ denote the number of incongruent solutions of the quadratic congruence $a_1x_1^2+\ldots+a_kx_k^2 \equiv n \pmod r$, where $\boldsymbol{a}=(a_1,\ldots,a_k)\in \mathbb{Z}^k$, $n\in \mathbb{Z}$, $r\in \mathbb{N}$. We give short direct proofs for certain less known compact formulas on $N_k(n,r,\boldsymbol{a})$, valid for r odd, which go back to the work of Minkowski, Bachmann and Cohen. We also deduce some other related identities and asymptotic formulas which do not seem to appear in the literature.

2010 Mathematics Subject Classification: 11D79, 11A25, 11N37

Key Words and Phrases: quadratic congruence in many variables, number of solutions, Jacobi symbol, Ramanujan sum, character sum, Gauss quadratic sum, asymptotic formula

1 Introduction

Let k and n be positive integers and let $r_k(n)$ denote the number of representations of n as a sum of k squares. More exactly, $r_k(n)$ is the number of solutions $(x_1,\ldots,x_k)\in \mathbb{Z}^k$ of the equation

$$x_1^2+\cdots+x_k^2=n. \tag{1}$$

The problem of finding exact formulas or good estimates for $r_k(n)$ and to study other related properties is one of the most fascinating problems in number theory. Such results were obtained by several authors, including Euler, Gauss, Liouville, Jacobi, Legendre and many others. Some of these results are now well known and are included in several textbooks. See, e.g., Grosswald [13], Hardy and Wright [14, Ch. XX], Hua [15, Ch. 8], Ireland and Rosen [17, Ch. 17], Nathanson [20, Ch. 14]. See also Dickson [10, Ch. VI–IX, XI].

For example, one has the next exact formulas. Let n be of the form $n=2^\nu m$ with $\nu \ge 0$ and m odd. Then

$$r_2(n)=4\sum_{d\mid m}(-1)^{(d-1)/2}, \tag{2}$$

$$r_4(n)=8(2+(-1)^n)\sum_{d\mid m} d. \tag{3}$$

Exact formulas for $r_k(n)$ are known also for other values of k. These identities are, in general, more complicated for k odd than in the case of k even.

Now consider the equation (1) in the ring $\mathbb{Z}/r\mathbb{Z}$ of residues (mod r), where r is a positive integer. Equivalently, consider the quadratic congruence

$$x_1^2 + \cdots + x_k^2 \equiv n \pmod{r}, \tag{4}$$

where $n \in \mathbb{Z}$. Let $N_k(n,r)$ denote the number of incongruent solutions $(x_1,\ldots,x_k) \in \mathbb{Z}^k$ of (4). The function $r \mapsto N_k(n,r)$ is multiplicative. Therefore, it is sufficient to consider the case $r = p^s$, a prime power. Identities for $N_k(n,p^s)$ can be derived using Gauss and Jacobi sums. For example, we refer to the explicit formulas for $N_k(0,p^s)$ given in [4, p. 46] and for $N_k(1,p)$ given in [17, Prop. 8.6.1]. See also Dickson [10, Ch. X] for historical remarks.

Much less known is that for k even and r odd, $N_k(n,r)$ can be expressed in a compact form using Ramanujan's sum. Furthermore, for k odd, r odd and $\gcd(n,r)=1$, $N_k(n,r)$ can be given in terms of the Möbius μ function and the Jacobi symbol. All these formulas are similar to (2) and (3). Namely, one has the following identities:

0) For $k \equiv 0 \pmod 4$, r odd, $n \in \mathbb{Z}$:

$$N_k(n,r) = r^{k-1} \sum_{d \mid r} \frac{c_d(n)}{d^{k/2}}. \tag{5}$$

1) For $k \equiv 1 \pmod 4$, r odd, $n \in \mathbb{Z}$, $\gcd(n,r)=1$:

$$N_k(n,r) = r^{k-1} \sum_{d \mid r} \frac{\mu^2(d)}{d^{(k-1)/2}} \left(\frac{n}{d}\right). \tag{6}$$

2) For $k \equiv 2 \pmod 4$, r odd, $n \in \mathbb{Z}$:

$$N_k(n,r) = r^{k-1} \sum_{d \mid r} (-1)^{(d-1)/2} \, \frac{c_d(n)}{d^{k/2}}. \tag{7}$$

3) For $k \equiv 3 \pmod 4$, r odd, $n \in \mathbb{Z}$, $\gcd(n,r)=1$:

$$N_k(n,r) = r^{k-1} \sum_{d \mid r} (-1)^{(d-1)/2} \, \frac{\mu^2(d)}{d^{(k-1)/2}} \left(\frac{n}{d}\right). \tag{8}$$

These are special cases of the identities deduced by Cohen in the paper [6] and quoted later in his papers [7, 8, 9]. The proofs given in [6] are lengthy and use the author's previous work, although in Section 7 of [6] a direct approach using finite Fourier sums is also described. According to Cohen the formulas (5)–(8) are due in an implicit form by Minkowski [18, pp. 45–58, 166–171]. Cohen [6, p. 27] says: "We mention the work of Minkowski as an important example of the use of Fourier sums in treating quadratic congruences. While Minkowski's approach was quite general, his results were mainly of an implicit nature." Cohen [9] refers also to the book of Bachmann [2, Part 1, Ch. 7].

Another related compact formula, which seems to not appear in the literature is the following: If $k \equiv 0 \pmod 4$, r is odd and $n \in \mathbb{Z}$, then

$$N_k(n,r) = r^{k/2-1} \sum_{d \mid \gcd(n,r)} d \, J_{k/2}(r/d), \tag{9}$$

where J_m is the Jordan function of order m.

It is the first main goal of the present paper to present short direct proofs of the identities (5)–(9). Slightly more generally, we will consider — as Cohen did — the quadratic congruence

$$a_1x_1^2 + \cdots + a_kx_k^2 \equiv n \pmod r, \tag{10}$$

where $n \in \mathbb{Z}$, $\boldsymbol{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$ and derive formulas for the number $N_k(n, r, \boldsymbol{a})$ of incongruent solutions $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ of (10), assuming that r is odd. For the proofs we only need to express $N_k(n, r, \boldsymbol{a})$ by a trigonometric sum and to use the evaluation of the Gauss quadratic sum. No properties concerning finite Fourier expansions or other algebraic arguments are needed. The proof is quite simple if k is even and somewhat more involved if k is odd. We also evaluate $N_k(n, 2^\nu)$ ($\nu \in \mathbb{N}$) for certain values of k and n and consider some special cases of (10).

Our second main goal is to establish asymptotic formulas — not given in the literature, as far as we know — for the sums $\sum_{r\le x} N_k(n, r)$, taken over all integers r with $1 \le r \le x$, in the cases $(k, n) = (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1), (4, 0), (4, 1)$. Similar formulas can be deduced also for other special choices of k and n. Note that the mean values of the functions $r \mapsto N_k(n, r)/n^{k-1}$ were investigated by Cohen [7], but only over the odd values of r.

We remark that a character free method to determine the number of solutions of the equation $x^2 + my^2 = k$ in the finite field $\mathbb{F}_p$ (p prime) was presented in a recent paper by Girstmair [12].

2 Notation

Throughout the paper we use the following notation: $\mathbb{N} := \{1, 2, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$; $e(x) = \exp(2\pi i x)$; $\left(\frac{\ell}{r}\right)$ is the Jacobi symbol ($\ell, r \in \mathbb{N}$, r odd), with the conventions $\left(\frac{\ell}{1}\right) = 1$ ($\ell \in \mathbb{N}$), $\left(\frac{\ell}{r}\right) = 0$ if $\gcd(\ell, r) > 1$; $c_r(n)$ denotes Ramanujan's sum (see, e.g., [1, Ch. 8], [14, Ch. XVI]) defined as the sum of n-th powers of the primitive r-th roots of unity, i.e.,

$$c_r(n) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} e(jn/r) \quad (r, n \in \mathbb{N}), \tag{11}$$

where $c_r(0) = \varphi(r)$ is Euler's function and $c_r(1) = \mu(r)$ is the Möbius function; $S(\ell, r)$ is the quadratic Gauss sum defined by

$$S(\ell, r) = \sum_{j=1}^{r} e(\ell j^2/r) \quad (\ell, r \in \mathbb{N}, \gcd(\ell, r) = 1). \tag{12}$$

Furthermore, $*$ is the Dirichlet convolution of arithmetical functions; $\mathbf{1}$, id and id_k are the functions given by $\mathbf{1}(n) = 1$, $\mathrm{id}(n) = n$, $\mathrm{id}_k(n) = n^k$ ($n \in \mathbb{N}$); $\tau(n)$ is the number of divisors of n; $J_k = \mu * \mathrm{id}_k$ is the Jordan function of order k, $J_k(n) = n^k \prod_{p|n}(1 - 1/p^k)$ ($n \in \mathbb{N}$), where $J_1 = \varphi$. Also, $\psi_k = \mu^2 * \mathrm{id}_k$ is the generalized Dedekind function, $\psi_k(n) = n^k \prod_{p|n}(1 + 1/p^k)$ ($n \in \mathbb{N}$); ζ is the Riemann zeta function; γ stands for the Euler constant; $\chi = \chi_4$ is the nonprincipal character (mod 4) and $G = L(2, \chi) \doteq 0.915956$ is the Catalan constant given by

$$G = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2} = \prod_{p\equiv 1 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p\equiv -1 \pmod 4} \left(1 + \frac{1}{p^2}\right)^{-1}. \tag{13}$$

3 General results

We evaluate $N_k(n,r,\boldsymbol{a})$ using the quadratic Gauss sum $S(\ell,r)$ defined by (12).

Proposition 1. *For every $k,r\in\mathbb{N}$, $n\in\mathbb{Z}$, $\boldsymbol{a}=(a_1,\ldots,a_k)\in\mathbb{Z}^k$ we have*

$$N_k(n,r,\boldsymbol{a})=r^{k-1}\sum_{d\mid r}\frac{1}{d^k}\sum_{\substack{\ell=1\\(\ell,d)=1}}^{d}e(-\ell n/d)S(\ell a_1,d)\cdots S(\ell a_k,d).$$

Proof. As is well known (see e.g., [19, Th. 1.31]), the number of solutions of a congruence can be expressed using the familiar identity

$$\sum_{j=1}^{r}e(jt/r)=\begin{cases}r, & \text{if } \ r\mid t;\\ 0, & \text{if } \ r\nmid t.\end{cases}\tag{14}$$

valid for every $r\in\mathbb{N},t\in\mathbb{Z}$. In our case we obtain

$$N_k(n,r,\boldsymbol{a})=\frac{1}{r}\sum_{x_1=1}^{r}\cdots\sum_{x_k=1}^{r}\sum_{j=1}^{r}e((a_1x_1^2+\cdots+a_kx_k^2-n)j/r),$$

that is,

$$N_k(n,r,\boldsymbol{a})=\frac{1}{r}\sum_{j=1}^{r}e(-jn/r)\sum_{x_1=1}^{r}e(ja_1x_1^2/r)\cdots\sum_{x_k=1}^{r}e(ja_kx_k^2/r).\tag{15}$$

By grouping the terms of (15) according to the values $(j,r)=d$ with $j=d\ell$, $(\ell,r/d)=1$, we obtain

$$N_k(n,r,\boldsymbol{a})=\frac{1}{r}\sum_{d\mid r}\sum_{\substack{\ell=1\\(\ell,r/d)=1}}^{r/d}e(-\ell n/(r/d))\sum_{x_1=1}^{r}e(\ell a_1x_1^2/(r/d))\cdots\sum_{x_k=1}^{r}e(\ell a_kx_k^2/(r/d)),\tag{16}$$

where, as it is easy to see, for every $j\in\{1,\ldots,k\}$,

$$\sum_{x_j=1}^{r}e(\ell a_jx_j^2/(r/d))=dS(\ell a_j,r/d).\tag{17}$$

By inserting (17) into (16) and by putting d instead of r/d, we are ready. □

Proposition 2. *Assume that $k,r\in\mathbb{N}$, r is odd, $n\in\mathbb{Z}$ and $\boldsymbol{a}=(a_1,\ldots,a_k)\in\mathbb{Z}^k$ is such that* $\gcd(a_1\cdots a_k,r)=1$. *Then*

$$N_k(n,r,\boldsymbol{a})=r^{k-1}\sum_{d\mid r}\frac{i^{k(d-1)^2/4}}{d^{k/2}}\left(\frac{a_1\cdots a_k}{d}\right)\sum_{\substack{\ell=1\\(\ell,d)=1}}^{d}\left(\frac{\ell}{d}\right)^k e(-\ell n/d).\tag{18}$$

Proof. We use that for every r odd and $\ell \in \mathbb{N}$ such that $\gcd(\ell, r) = 1$,

$$S(\ell, r) = \begin{cases} \left(\frac{\ell}{r}\right)\sqrt{r}, & \text{if } \ r \equiv 1 \pmod 4; \\ i\,\left(\frac{\ell}{r}\right)\sqrt{r}, & \text{if } \ r \equiv -1 \pmod 4, \end{cases} \tag{19}$$

cf., e.g., [4, Th. 1.5.2], [15, Th. 7.5.6]. Now the result follows immediately from Proposition 1. ∎

Proposition 3. *Assume that $k \in \mathbb{N}$, $r = 2^\nu$ ($\nu \in \mathbb{N}$), $n \in \mathbb{Z}$ and $\boldsymbol{a} = (a_1, \dots, a_k) \in \mathbb{Z}^k$ is such that $a_1, \dots, a_k$ are odd. Then*

$$N_k(n, 2^\nu, \boldsymbol{a}) = 2^{\nu(k-1)} \left(1 + \sum_{t=1}^{\lfloor \nu/2 \rfloor} \frac{1}{2^{kt}} \sum_{\substack{\ell=1 \\ \ell \text{ odd}}}^{2^{2t}} e(-\ell n/2^{2t})(1+i^{\ell a_1}) \cdots (1+i^{\ell a_k}) \right.$$
$$\left. + \sum_{t=1}^{\lfloor (\nu-1)/2 \rfloor} \frac{1}{2^{kt}} \sum_{\substack{\ell=1 \\ \ell \text{ odd}}}^{2^{2t+1}} e(-\ell n/2^{2t+1} + \ell(a_1 + \cdots + a_k)/8) \right).$$

Proof. Using Proposition 1 and putting $d = 2^s$,

$$N_k(n, 2^\nu, \boldsymbol{a}) = 2^{\nu(k-1)} \sum_{s=0}^{\nu} \frac{1}{2^{ks}} \sum_{\substack{\ell=1 \\ \ell \text{ odd}}}^{2^s} e(-\ell n/2^s) S(\ell a_1, 2^s) \cdots S(\ell a_k, 2^s).$$

We apply that for every ℓ odd,

$$S(\ell, 2^\nu) = \begin{cases} 0, & \text{if } \ \nu = 1; \\ (1+i^\ell) 2^{\nu/2}, & \text{if } \ \nu \text{ is even}; \\ 2^{(\nu+1)/2} e(\ell/8), & \text{if } \ \nu > 1 \text{ is odd}, \end{cases}$$

cf., e.g., [4, Th. 1.5.1, 1.5.3], [15, Th. 7.5.7]. Separating the terms corresponding to $s = 2t$ even and $s = 2t+1$ odd, respectively we obtain the given formula. ∎

4 The case k even, r odd

Suppose that k is even and r is odd. In this case we deduce for $N_k(n, r, \boldsymbol{a})$ formulas in terms of the Ramanujan sums.

Proposition 4. ([6, Th. 11 and Eq. (5.2)]) *Assume that $k = 2m$ ($m \in \mathbb{N}$), $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$, $\boldsymbol{a} = (a_1, \dots, a_k) \in \mathbb{Z}^k$, $\gcd(a_1 \cdots a_k, r) = 1$. Then*

$$N_{2m}(n, r, \boldsymbol{a}) = r^{2m-1} \sum_{d \mid r} \frac{c_d(n)}{d^m} \left(\frac{(-1)^m a_1 \cdots a_{2m}}{d} \right).$$

Proof. This is a direct consequence of Proposition 2. For k even the inner sum of (18) is exactly $c_d(n)$, by its definition (11), and applying that $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2}$ the proof is complete. ∎

In the special case $k = 2$, $a_1 = 1$, $a_2 = -D$, r odd, $\gcd(D, r) = \gcd(n, r) = 1$ Proposition 4 was deduced by Rabin and Shallit [21, Lemma 3.2].

Corollary 5. *If $k = 4m$ $(m \in \mathbb{N})$, $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ and $a_1 \cdots a_k = 1$ (in particular $a_1 = \cdots = a_k = 1$), then*

$$N_{4m}(n, r, \boldsymbol{a}) = r^{4m-1} \sum_{d \mid r} \frac{c_d(n)}{d^{2m}}.$$

Corollary 6. *If $k = 4m + 2$ $(m \in \mathbb{N}_0)$, $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ and $a_1 \cdots a_k = 1$ (in particular $a_1 = \cdots = a_k = 1$), then*

$$N_{4m+2}(n, r, \boldsymbol{a}) = r^{4m+1} \sum_{d \mid r} (-1)^{(d-1)/2} \frac{c_d(n)}{d^{2m+1}}. \tag{20}$$

Therefore, the identities (5) and (7) are proved. In particular, the next simple formulas are valid: for every r odd,

$$N_2(0, r) = r \sum_{d \mid r} (-1)^{(d-1)/2} \, \frac{\varphi(d)}{d}, \tag{21}$$

$$N_4(1, r) = r^3 \sum_{d \mid r} \frac{\mu(d)}{d^2} = r J_2(r). \tag{22}$$

Remark 7. In the case k even and $a_1 = \cdots = a_k = 1$ for the proof of Proposition 4 it is sufficient to use the formula $S^2(\ell, r) = (-1)^{(r-1)/2} r$ (r odd, $\gcd(\ell, r) = 1$) instead of the much deeper result (19) giving the precise value of $S(\ell, r)$.

In the case $k = 4m$ and $a_1 \cdots a_k = 1$ the next representation holds as well (already given in (9) in the case $a_1 = \cdots = a_k = 1$).

Corollary 8. *If $k = 4m$ $(m \in \mathbb{N})$, $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ and $a_1 \cdots a_k = 1$ (in particular $a_1 = \cdots = a_k = 1$), then*

$$N_{4m}(n, r, \boldsymbol{a}) = r^{2m-1} \sum_{d \mid \gcd(n, r)} d \, J_{2m}(r/d). \tag{23}$$

Proof. We use Corollary 5 and apply that for every fixed n, $c_{\bullet}(n) = \mu * \eta_{\bullet}(n)$, where $\eta_r(n) = r$ if $r \mid n$ and 0 otherwise. Therefore,

$$\begin{aligned} N_{4m}(n, r, \boldsymbol{a}) &= r^{2m-1} \sum_{d \mid r} c_d(n) (r/d)^{2m} \\ &= r^{2m-1} \left(c_{\bullet}(n) * \mathrm{id}_{2m}\right)(r) \\ &= r^{2m-1} \left(\mu * \mathrm{id}_{2m} * \eta_{\bullet}(n)\right)(r) \\ &= r^{2m-1} \left(J_{2m} * \eta_{\bullet}(n)\right)(r) \\ &= r^{2m-1} \sum_{d \mid \gcd(n, r)} d \, J_{2m}(r/d). \end{aligned}$$

□

Remark 9. The identity (23) shows that for every r odd, the function $n \mapsto N_{4m}(n,r)$ is even (mod r). We recall that an arithmetic function $n \mapsto f(n)$ is said to be even (mod r) if $f(n) = f(\gcd(n,r))$ holds for every $n \in \mathbb{N}$. We refer to [24] for this notion. In fact, for every k even the function $n \mapsto N_k(n,r,\boldsymbol{a})$ is even (mod r), where r is a fixed odd number and $\gcd(a_1 \cdots a_k, r) = 1$, since according to Proposition 4, $N_k(n,r,\boldsymbol{a})$ is a linear combination of the values $c_d(r)$ with $d \mid r$. See also [8].

A direct consequence of (23) is the next result:

Corollary 10. *If $k = 4m$ $(m \in \mathbb{N})$, $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ such that $\gcd(n,r) = 1$, then*

$$N_{4m}(n,r) = r^{2m-1} J_{2m}(r) = r^{4m-1} \prod_{p \mid r} \left(1 - \frac{1}{p^{2m}}\right).$$

Another consequence of Proposition 4 is the following identity, of which proof is similar to the proof of Corollary 8:

Corollary 11. *If $k = 4m+2$ $(m \in \mathbb{N}_0)$, $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ and $a_1 \cdots a_k = -1$, then*

$$N_{4m+2}(n,r,\boldsymbol{a}) = r^{2m} \sum_{d \mid \gcd(n,r)} d\, J_{2m+1}(r/d).$$

In the case $r = p^\nu$ $(p > 2$ prime) and for special choices of k and n one can deduce explicit formulas from the identities of above. For example (as is well known):

Corollary 12. *For every prime $p > 2$ and every $n \in \mathbb{N}$,*

$$N_2(n,p) = \begin{cases} 2p-1, & \text{if } p \mid n,\ p \equiv 1 \pmod 4; \\ 1, & \text{if } p \mid n,\ p \equiv -1 \pmod 4; \\ p-1, & \text{if } p \nmid n,\ p \equiv 1 \pmod 4; \\ p+1, & \text{if } p \nmid n,\ p \equiv -1 \pmod 4, \end{cases}$$

$$N_2(n,p^2) = \begin{cases} p(p-1), & \text{if } p \nmid n,\ p \equiv 1 \pmod 4; \\ 2p(p-1), & \text{if } p \mid n,\ p^2 \nmid n,\ p \equiv 1 \pmod 4; \\ 3p^2 - 2p, & \text{if } p^2 \mid n,\ p \equiv 1, \pmod 4; \\ p(p+1), & \text{if } p \nmid n,\ p \equiv -1 \pmod 4; \\ 0, & \text{if } p \mid n,\ p^2 \nmid n,\ p \equiv -1 \pmod 4; \\ p^2, & \text{if } p^2 \mid n,\ p \equiv -1 \pmod 4. \end{cases}$$

5 The case k odd, r odd

Now consider the case k odd, r odd. In order to apply Proposition 2 we need to evaluate the character sum

$$T(n,r) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} \left(\frac{j}{r}\right) e(jn/r).$$

Lemma 13. *Let $r, n \in \mathbb{N}$, r odd such that* $\gcd(n,r) = 1$.

i) If r is squarefree, then

$$T(n,r) = \begin{cases} \left(\frac{n}{r}\right)\sqrt{r}, & \text{if } r \equiv 1 \pmod 4; \\ i\left(\frac{n}{r}\right)\sqrt{r}, & \text{if } r \equiv -1 \pmod 4. \end{cases} \tag{24}$$

ii) If r is not squarefree, then $T(n,r) = 0$.

Proof. For every r odd the Jacobi symbol $j \mapsto \left(\frac{j}{r}\right)$ is a real character (mod r) and $T(n,r) = \left(\frac{n}{r}\right) T(1,r)$ holds if $\gcd(n,r) = 1$. See, e.g., [15, Ch. 7].

i) If r is squarefree, then $j \mapsto \left(\frac{j}{r}\right)$ is a primitive character (mod r). Thus, $T(1,r) = \sqrt{r}$ for $\left(\frac{-1}{r}\right) = 1$ and $T(1,r) = i\sqrt{r}$ for $\left(\frac{-1}{r}\right) = -1$ ([15, Th. 7.5.8]), giving (24).

ii) We show that if r is not squarefree, then $T(1,r) = 0$. Here r can be written as $r = p^2 s$, where p is a prime and by putting $j = ks + q$,

$$T(1,r) = \sum_{q=1}^{s} \sum_{k=0}^{p^2-1} \left(\frac{ks+q}{r}\right) e((ks+q)/r),$$

where

$$\left(\frac{ks+q}{r}\right) = \left(\frac{ks+q}{p^2}\right)\left(\frac{ks+q}{s}\right) = \left(\frac{q}{s}\right)$$

and deduce

$$T(1,r) = \sum_{q=1}^{s} \left(\frac{q}{s}\right) e(q/(p^2 s)) \sum_{k=0}^{p^2-1} e(k/p^2) = 0,$$

since the inner sum is zero using (14). $\square$

Note that properties of the sum $T(n,r)$, including certain orthogonality results were obtained by Cohen [6] using different arguments.

Proposition 14. ([6, Cor. 2]) *Assume that $k = 2m+1$ ($m \in \mathbb{N}_0$), $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$ such that* $\gcd(n,r) = 1$, $\boldsymbol{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$, $\gcd(a_1 \cdots a_k, r) = 1$. *Then*

$$N_{2m+1}(n,r,\boldsymbol{a}) = r^{2m} \sum_{d \mid r} \frac{\mu^2(d)}{d^m} \left(\frac{(-1)^m n a_1 \cdots a_{2m+1}}{d}\right).$$

Proof. Apply Proposition 2. For k odd the inner sum of (18) is $T(-n,d)$, where $T(n,r)$ is given by (24). Since r is odd and $\gcd(n,r) = 1$, if $d \mid r$, then d is also odd and $\gcd(d,r) = 1$. We deduce by Lemma 13 that

$$\begin{aligned} N_k(n,r,\boldsymbol{a}) &= r^{k-1} \sum_{d \mid r} \frac{i^{k(d-1)^2/4}}{d^{k/2}} \left(\frac{a_1 \cdots a_k}{d}\right) T(-n,d) \\ &= r^{k-1} \sum_{\substack{d \mid r \\ d \text{ squarefree}}} \frac{i^{k(d-1)^2/4}}{d^{k/2}} \left(\frac{a_1 \cdots a_k}{d}\right) i^{(d-1)^2/4} \left(\frac{-n}{d}\right) \sqrt{d} \\ &= r^{k-1} \sum_{d \mid r} \frac{\mu^2(d)}{d^{(k-1)/2}} i^{(k+1)(d-1)^2/4} \left(\frac{-n a_1 \cdots a_k}{d}\right), \end{aligned}$$

which gives the result by evaluating the powers of i. $\square$

Corollary 15. *If $k = 4m + 1$ ($m \in \mathbb{N}_0$), $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$, $\gcd(n, r) = 1$ and $a_1 \cdots a_k = 1$ (in particular if $a_1 = \cdots = a_k = 1$), then*

$$N_{4m+1}(n, r, \boldsymbol{a}) = r^{4m} \sum_{d \mid r} \frac{\mu^2(d)}{d^{2m}} \left(\frac{n}{d}\right).$$

Corollary 16. *If $k = 4m + 3$ ($m \in \mathbb{N}_0$), $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$, $\gcd(n, r) = 1$ and $a_1 \cdots a_k = 1$ (in particular if $a_1 = \cdots = a_k = 1$), then*

$$N_{4m+3}(n, r, \boldsymbol{a}) = r^{4m+2} \sum_{d \mid r} \frac{\mu^2(d)}{d^{2m+1}} (-1)^{(d-1)/2} \left(\frac{n}{d}\right).$$

This proves the identities (6) and (8).

Corollary 17. *If $k = 4m + 3$ ($m \in \mathbb{N}_0$), $r \in \mathbb{N}$ is odd, $n \in \mathbb{Z}$, $\gcd(n, r) = 1$ and $a_1 \cdots a_k = -1$, then*

$$N_{4m+3}(n, r, \boldsymbol{a}) = r^{2m+1} \psi_{2m+1}(r).$$

To prove the next result we need the evaluation of

$$V(r) = T(0, r) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} \left(\frac{j}{r}\right),$$

not given by Lemma 13.

Lemma 18. *If $r \in \mathbb{N}$ is odd, then*

$$V(r) = \begin{cases} \varphi(r), & \text{if } r \text{ is a square;} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $r = t^2$ is a square, then $\left(\frac{j}{r}\right) = \left(\frac{j}{t^2}\right) = 1$ for every j with $\gcd(j, r) = 1$ and deduce that $V(r) = \varphi(r)$.

Now assume that r is not a square. Then, since r is odd, there is a prime $p > 2$ such that $r = p^\nu s$, where ν is odd and $\gcd(p, s) = 1$. First we show that there exists an integer j_0 such that $(j_0, r) = 1$ and $\left(\frac{j_0}{r}\right) = -1$. Indeed, let c be a quadratic nonresidue (mod p) and consider the simultaneous congruences $x \equiv c \pmod{p}$, $x \equiv 1 \pmod{s}$. By the Chinese remainder theorem there exists a solution $x = j_0$ satisfying

$$\left(\frac{j_0}{r}\right) = \left(\frac{j_0}{p}\right)^\nu \left(\frac{j_0}{s}\right) = \left(\frac{c}{p}\right)^\nu \left(\frac{1}{s}\right) = (-1)^\nu = -1,$$

since ν is odd. Hence

$$V(r) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} \left(\frac{j j_0}{r}\right) = \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} \left(\frac{j}{r}\right) \left(\frac{j_0}{r}\right) = - \sum_{\substack{j=1 \\ \gcd(j,r)=1}}^{r} \left(\frac{j}{r}\right) = -V(r),$$

giving that $V(r) = 0$. $\square$

Proposition 19. ([6, Cor. 1]) *Assume that $k, r \in \mathbb{N}$ are odd, $n = 0$ and $\boldsymbol{a} = (a_1, \dots, a_k) \in \mathbb{Z}^k$, $\gcd(a_1 \cdots a_k, r) = 1$. Then*

$$N_k(0, r, \boldsymbol{a}) = r^{k-1} \sum_{d^2 \mid r} \frac{\varphi(d)}{d^{k-1}},$$

which does not depend on $\boldsymbol{a}$.

Proof. From Proposition 2 we have

$$N_k(0, r, \boldsymbol{a}) = r^{k-1} \sum_{d \mid r} \frac{i^{k(d-1)^2/4}}{d^{k/2}} \left(\frac{a_1 \cdots a_k}{d} \right) V(d),$$

where $V(d)$ is given by Lemma 18. We deduce

$$N_k(0, r, \boldsymbol{a}) = r^{k-1} \sum_{d^2 \mid r} \frac{i^{k(d^2-1)^2/4}}{d^k} \left(\frac{a_1 \cdots a_k}{d^2} \right) \varphi(d^2) = r^{k-1} \sum_{d^2 \mid r} \frac{\varphi(d^2)}{d^k}.$$

□

Remark 20. For all the results of this section it was assumed that $\gcd(n, r) = 1$. See [9] for certain special cases of $\gcd(n, r) > 1$.

6 The case k even, $r = 2^\nu$

In this section let $a_1 = \cdots = a_k = 1$.

Proposition 21. *If $k \in \mathbb{N}$ is even and $n \in \mathbb{Z}$ is odd, then $N_k(n, 2) = 2^{k-1}$ and for every $\nu \in \mathbb{N}$, $\nu \geq 2$,*

$$N_k(n, 2^\nu) = 2^{\nu(k-1)} \left(1 - \frac{1}{2^{k/2-1}} \cos\left(\frac{k\pi}{4} + \frac{n\pi}{2} \right) \right).$$

Proof. We obtain from Proposition 3 by separating the terms according to $\ell = 4u + 1$ and $\ell = 4u + 3$, respectively,

$$N_k(n, 2^\nu) = 2^{\nu(k-1)} \left(1 + \sum_{t=1}^{\lfloor \nu/2 \rfloor} \frac{1}{2^{kt}} A_t + \sum_{t=1}^{\lfloor (\nu-1)/2 \rfloor} \frac{1}{2^{kt}} B_t \right),$$

where

$$\begin{aligned} A_t &= (1+i)^k \sum_{u=0}^{2^{2t-2}-1} e(-(4u+1)n/2^{2t}) + (1-i)^k \sum_{u=0}^{2^{2t-2}-1} e(-(4u+3)n/2^{2t}) \\ &= \left((1+i)^k e(-n/2^{2t}) + (1-i)^k e(-3n/2^{2t}) \right) \sum_{u=0}^{2^{2t-2}-1} e(-un/2^{2t-2}), \end{aligned}$$

and

$$B_t = \sum_{u=0}^{2^{2t-1}-1} \left(e(-(4u+1)n/2^{2t+1} + (4u+1)k/8) + e(-(4u+3)n/2^{2t+1} + (4u+3)k/8)\right)$$

$$= \left(e(k/8 - n/2^{2t+1}) + e(3k/8 - 3n/2^{2t+1})\right) \sum_{u=0}^{2^{2t-1}-1} e(-un/2^{2t-1} + ku/2).$$

Since n is odd, $n/2^{2t-2} \notin \mathbb{Z}$ for every $t \geq 2$. It follows that $A_t = 0$ for every $t \geq 2$. Also,

$$A_1 = (1+i)^k e(-n/4) + (1-i)^k e(-3n/4) = -2^{k/2+1} \cos(k\pi/4 + n\pi/2).$$

Similarly, since k is even and n is odd, $k/2 - n/2^{2t-1} \notin \mathbb{Z}$ for every $t \geq 1$. It follows that $B_t = 0$ for every $t \geq 1$. This completes the proof. $\square$

Corollary 22. *If $k = 4m$ ($m \in \mathbb{N}$) and $n \in \mathbb{Z}$ is odd, then for every $\nu \in \mathbb{N}$,*

$$N_{4m}(n, 2^\nu) = 2^{\nu(4m-1)}.$$

Corollary 23. *If $k = 4m+2$ ($m \in \mathbb{N}_0$) and $n = 2t+1 \in \mathbb{Z}$ is odd, then $N_{4m+2}(n, 2) = 2^{4m+1}$ and for every $\nu \geq 2$,*

$$N_{4m+2}(n, 2^\nu) = 2^{\nu(4m+1)} \left(1 + \frac{(-1)^{m+t}}{2^{2m}}\right).$$

By similar arguments one can deduce from Proposition 3:

Proposition 24. ([4, p. 46]) *If $k = 4m$ ($m \in \mathbb{N}$) and $n = 0$, then for every $\nu \in \mathbb{N}$,*

$$N_{4m}(0, 2^\nu) = 2^{\nu(4m-1)} \left(1 + \frac{(-1)^m (2^{(\nu-1)(2m-1)} - 1)}{2^{(\nu-1)(2m-1)}(2^{2m-1} - 1)}\right).$$

Proposition 25. ([4, p. 46]) *If $k = 4m+2$ ($m \in \mathbb{N}_0$) and $n = 0$ for every $\nu \in \mathbb{N}$,*

$$N_{4m+2}(0, 2^\nu) = 2^{\nu(4m+1)}.$$

7 The case k odd, $r = 2^\nu$

Now let k be odd, $r = 2^\nu$, $a_1 = \cdots = a_k = 1$. By similar arguments as in the previous sections we have

Proposition 26. ([4, p. 46]) *If $k \in \mathbb{N}$ is odd and $n = 0$, then for every $\nu \in \mathbb{N}$,*

$$N_k(0, 2^\nu) = 2^{\nu(k-1)} \left(1 + \frac{(-1)^{(k^2-1)/8} \cdot (2^{(k-2)\lfloor \nu/2 \rfloor} - 1)}{2^{(k-2)\lfloor \nu/2 \rfloor - (k-3)/2}(2^{k-2} - 1)}\right).$$

Other cases can also be considered, for example:

Proposition 27. *If $k = 4m+3$ and $n = 4t+1$ ($m, n \in \mathbb{N}_0$), then for every $\nu \in \mathbb{N}$,*

$$N_{4m+3}(n, 2^\nu) = 2^{\nu(4m+2)} \left(1 + \frac{(-1)^m}{2^{2m+1}}\right).$$

8 Special cases

In this section we consider some special cases and deduce asymptotic formulas for $k = 1, 2, 3, 4$ and $\boldsymbol{a} = (1, \ldots, 1)$.

8.1 The congruence $x^2 \equiv 0 \pmod{r}$

For $k = 1$ and $n = 0$ we have the congruence $x^2 \equiv 0 \pmod{r}$. Its number of solutions, $N_1(0, r)$ is the sequence A000188 in [22]. It is well known and can be deduced directly that $N_1(0, p^\nu) = p^{\lfloor \nu/2 \rfloor}$ for every prime power p^ν ($\nu \in \mathbb{N}$). This leads to the Dirichlet series representation

$$\sum_{r=1}^{\infty} \frac{N_1(0,r)}{r^s} = \frac{\zeta(2s-1)\zeta(s)}{\zeta(2s)}. \tag{25}$$

Our next result corresponds to the classical asymptotic formula of Dirichlet

$$\sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + O(x^{1/2}).$$

Proposition 28. *We have*

$$\sum_{r \le x} N_1(0,r) = \frac{3}{\pi^2} x \log x + cx + O(x^{2/3}), \tag{26}$$

where $c = \frac{3}{\pi^2}\left(3\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)}\right)$.

Proof. By the identity (25) we infer that for every $r \in \mathbb{N}$,

$$N_1(0,r) = \sum_{a^2 b^2 c = r} \mu(a) b.$$

Using Dirichlet's hyperbola method we have

$$E(x) := \sum_{b^2 c \le x} b = \sum_{b \le x^{1/3}} b \sum_{c \le x/b^2} 1 + \sum_{c \le x^{1/3}} \sum_{b \le (x/c)^{1/2}} b - \sum_{b \le x^{1/3}} b \sum_{c \le x^{1/3}} 1,$$

which gives by the trivial estimate (i.e., $|x - \lfloor x \rfloor| < 1$),

$$E(x) = \frac{1}{2} x \log x + \frac{1}{2}(3\gamma - 1)x + O(x^{2/3}).$$

Now,

$$\sum_{r \le x} N_1(0,r) = \sum_{a \le x^{1/2}} \mu(a) E(x/a^2)$$

and easy computations complete the proof. ∎

Remark 29. The error term of (26) can be improved by the method of exponential sums (see, e.g., [5, Ch. 6]). Namely, it is $O(x^{2/3-\delta})$ for some explicit δ with $0 < \delta < 1/6$.

8.2 The congruence $x^2 \equiv 1 \pmod r$

It is also well known, that in the case $k = 1$ and $n = 1$ for the number of solutions of the congruence $x^2 \equiv 1 \pmod r$ one has $N_1(1, p^\nu) = 2$ for every prime $p > 2$ and every $\nu \in \mathbb{N}$, $N_1(1, 2) = 1$, $N_1(1, 4) = 2$, $N_1(1, 2^\nu) = 4$ for every $\nu \geq 3$ (sequence A060594 in [22]). The Dirichlet series representation

$$\sum_{r=1}^{\infty} \frac{N_1(1,r)}{r^s} = \frac{\zeta^2(s)}{\zeta(2s)} \left(1 - \frac{1}{2^s} + \frac{2}{2^{2s}}\right) \tag{27}$$

shows that estimating the sum $\sum_{r \leq x} N_1(1,r)$ is closely related to the squarefree divisor problem. Let $\tau^{(2)}(n) = 2^{\omega(n)}$ denote the number of squarefree divisors of n. Then

$$\sum_{n=1}^{\infty} \frac{\tau^{(2)}(n)}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}. \tag{28}$$

By this analogy we deduce

Proposition 30.

$$\sum_{r \leq x} N_1(1,r) = \frac{6}{\pi^2} x \log x + c_1 x + O(x^{1/2} \exp(-c_0 (\log x)^{3/5} (\log\log x)^{-1/5})),$$

where $c_0 > 0$ is a constant and $c_1 = \frac{6}{\pi^2}\left(2\gamma - 1 - \frac{\log 2}{2} - \frac{2\zeta'(2)}{\zeta(2)}\right)$. If the Riemann hypothesis (RH) is true, then the error term is $O(x^{4/11+\varepsilon})$ for every $\varepsilon > 0$.

Proof. By the identities (27) and (28) it follows that for every $r \in \mathbb{N}$,

$$N_1(1,r) = \sum_{ab=r} \tau^{(2)}(a) h(b),$$

where the multiplicative function h is defined by

$$h(p^\nu) = \begin{cases} -1, & \text{if } \ p = 2,\ \nu = 1; \\ 2, & \text{if } \ p = 2,\ \nu = 2; \\ 0, & \text{otherwise.} \end{cases}$$

Now the convolution method and the result

$$\sum_{n \leq x} \tau^{(2)}(n) = \frac{6}{\pi^2} x \left(\log x + 2\gamma - 1 - \frac{2\zeta'(2)}{\zeta(2)}\right) + O(R(x)),$$

where $R(x) \ll x^{1/2} \exp(-c_0 (\log x)^{3/5} (\log\log x)^{-1/5})$ (see [23]) conclude the proof. If RH is true, then the estimate $R(x) \ll x^{4/11+\varepsilon}$ due to Baker [3] can be used. $\square$

Remark 31. See [11] for asymptotic formulas on the number of solutions of the higher degree congruences $x^\ell \equiv 0 \pmod n$ and $x^\ell \equiv 1 \pmod n$, respectively, where $\ell \in \mathbb{N}$. The results of our Propositions 28 and 30 are better than those of [11] applied for $\ell = 2$.

8.3 The congruence $x^2 + y^2 \equiv 0 \pmod{r}$

This is the case $k = 2$, $n = 0$. $N_2(0, r)$ is the sequence A086933 in [22] and for r odd it is given by (21). Furthermore, $N_2(0, 2^\nu)$ is given by Proposition 25. We deduce

Corollary 32. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_2(0, p^\nu) = \begin{cases} p^\nu(\nu + 1 - \nu/p), & \text{if } p \equiv 1 \pmod{4},\ \nu \ge 1; \\ p^\nu, & \text{if } p \equiv -1 \pmod{4},\ \nu \text{ is even}; \\ p^{\nu-1}, & \text{if } p \equiv -1 \pmod{4},\ \nu \text{ is odd}; \\ 2^\nu, & \text{if } p = 2,\ \nu \ge 1. \end{cases}$$

Corollary 33. $N_2(0, \centerdot) = \mathrm{id} \cdot (\mathbf{1} * \chi) * \mu\chi$, *where χ is the nonprincipal character* (mod 4).

Proof. From Corollary 32 we obtain the Dirichlet series representation

$$\sum_{r=1}^{\infty} \frac{N_2(0, r)}{r^s} = \zeta(s-1) \prod_{p>2} \left(1 - \frac{(-1)^{(p-1)/2}}{p^s}\right) \left(1 - \frac{(-1)^{(p-1)/2}}{p^{s-1}}\right)^{-1}$$

$$= \zeta(s-1) L(s-1, \chi) L(s, \chi)^{-1},$$

where $L(s, \chi)$ is the Dirichlet series of χ. This gives the result. □

Observe that $4(\mathbf{1} * \chi)(n) = r_2(n)$ is the number of ways n can be written as a sum of two squares, quoted in the Introduction. This shows that the sum $\sum_{r \le x} N_2(0, r)$ is closely related to the Gauss circle problem. The next result corresponds to the asymptotic formula due to Huxley [16]

$$\sum_{n \le x} r_2(n) = \pi x + O(x^a (\log x)^b), \tag{29}$$

where $a = 131/416 \doteq 0.314903$ and $b = 26947/8320$.

Proposition 34. *We have*

$$\sum_{r \le x} N_2(0, r) = \frac{\pi}{8G} x^2 + O(x^{a+1} (\log x)^b),$$

where G is the Catalan constant defined by (13).

Proof. Since $N_2(0, \centerdot) = (\mathrm{id} \cdot r_2/4) * (\mu\chi)$, we have

$$\sum_{r \le x} N_2(0, r) = \frac{1}{4} \sum_{d \le x} \mu(d)\chi(d) \sum_{n \le x/d} n r_2(n).$$

Now partial summation on (29) and usual estimates give the result. □

8.4 The congruence $x^2 + y^2 \equiv 1 \pmod{r}$

This is the case $k = 2$, $n = 1$. $N_2(1, r)$ is sequence A060968 in [22]. For every r odd we have by (20),

$$N_2(1, r) = r \sum_{d|r} (-1)^{(d-1)/2} \frac{\mu(d)}{d},$$

and deduce (cf. Corollary 23).

Corollary 35. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_2(1, p^\nu) = \begin{cases} p^\nu(1 - 1/p), & \text{if } p \equiv 1 \pmod 4, \ \nu \geq 1; \\ p^\nu(1 + 1/p), & \text{if } p \equiv -1 \pmod 4, \ \nu \geq 1; \\ 2, & \text{if } p = 2, \ \nu = 1; \\ 2^{\nu+1}, & \text{if } p = 2, \ \nu \geq 2. \end{cases}$$

Proposition 36. *We have*

$$\sum_{r \leq x} N_2(1, r) = \frac{5}{8G} x^2 + O(x \log x).$$

Proof. One has the Dirichlet series representation

$$\sum_{r=1}^{\infty} \frac{N_2(1, r)}{r^s} = \zeta(s - 1) \left(1 + \frac{4}{2^{2s}}\right) L(s, \chi)^{-1},$$

and the asymptotic formula is obtained by usual elementary arguments. □

8.5 The congruence $x^2 + y^2 + z^2 \equiv 0 \pmod{r}$

This is the case $k = 3$, $n = 0$. $N_3(0, r)$ is the sequence A087687 in [22]. By Proposition 19 we have for every $r \in \mathbb{N}$ odd,

$$N_3(0, r) = r^2 \sum_{d^2|r} \frac{\varphi(d)}{d^2} \tag{30}$$

and using also Proposition 26 we deduce

Corollary 37. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_3(0, p^\nu) = \begin{cases} p^{3\beta-1}(p^{\beta+1} + p^\beta - 1), & \text{if } p > 2, \ \nu = 2\beta \text{ is even;} \\ p^{3\beta-2}(p^\beta + p^{\beta-1} - 1), & \text{if } p > 2, \ \nu = 2\beta - 1 \text{ is odd;} \\ 2^{3\beta}, & \text{if } p = 2, \ \nu = 2\beta \text{ is even;} \\ 2^{3\beta-1}, & \text{if } p = 2, \ \nu = 2\beta - 1 \text{ is odd.} \end{cases}$$

Proposition 38.

$$\sum_{r \leq x} N_3(0, r) = \frac{24\zeta(3)}{\pi^4} x^3 + O(x^2 \log x).$$

Proof. The Dirichlet series of the function $r \mapsto N_3(0,r)$ is

$$\sum_{r=1}^{\infty} \frac{N_3(0,r)}{r^s} = \zeta(s-2)G(s),$$

where

$$G(s) = \frac{\zeta(2s-3)}{\zeta(2s-2)} \frac{2^{2s}-16}{2^{2s}-4} \tag{31}$$

is the Dirichlet series of the multiplicative function g given by

$$g(p^\nu) = \begin{cases} p^{3\beta-1}(p-1), & \text{if } \; p>2,\; \nu=2\beta \geq 2; \\ -2^{3\beta}, & \text{if } \; p=2,\; \nu=2\beta \geq 2; \\ 0, & \text{if } \; p \geq 2,\; \nu=2\beta-1 \geq 1. \end{cases}$$

Therefore, $N_3(0, \centerdot) = \mathrm{id}_2 * g$ and obtain

$$\begin{aligned} \sum_{r\leq x} N_3(0,r) &= \sum_{d \leq x} g(d) \left(\frac{x^3}{3d^3} + O(\frac{x^2}{d^2}) \right) \\ &= \frac{x^3}{3} G(3) + O\left(x^3 \sum_{d>x} \frac{|g(d)|}{d^3} \right) + O\left(x^2 \sum_{d \leq x} \frac{|g(d)|}{d^2} \right). \end{aligned} \tag{32}$$

Here a direct computation shows that

$$\sum_{d\leq x} \frac{|g(d)|}{d^2} \leq \prod_{p \leq x} \sum_{\nu=0}^{\infty} \frac{|g(p^\nu)|}{p^\nu} \ll \prod_{p} \left(1+\frac{1}{p}\right) \ll \log x \tag{33}$$

by Mertens' theorem.

Furthermore, by (31), $g(n) = \sum_{ab^2=n} h(a) b^3$, where the Dirichlet series of the function h is absolutely convergent for $\Re s > 3/2$. Hence

$$\sum_{n \leq x} h(n) = c_2 x^2 + O(x^{3/2+\varepsilon})$$

with a certain constant c_2, and by partial summation we deduce that

$$\sum_{d>x} \frac{|g(d)|}{d^3} \ll \frac{1}{x}. \tag{34}$$

Now the result follows from (32), (33) and (34). □

8.6 The congruence $x^2 + y^2 + z^2 \equiv 1 \pmod r$

$N_3(1,r)$ is the sequence A087784 in [22]. Using Corollary 16 and Proposition 27 we have

Corollary 39. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_3(1,p^\nu) = \begin{cases} p^{2\nu}(1+1/p), & \textit{if } \; p \equiv 1 \pmod 4,\; \nu \geq 1; \\ p^{2\nu}(1-1/p), & \textit{if } \; p \equiv -1 \pmod 4,\; \nu \geq 1; \\ 4, & \textit{if } \; p=2,\; \nu=1; \\ 3 \cdot 2^{2\nu-1}, & \textit{if } \; p=2,\; \nu \geq 2. \end{cases}$$

Proposition 40. *We have*

$$\sum_{r \le x} N_3(1, r) = \frac{36G}{\pi^4} x^3 + O(x^2 \log x).$$

Proof. Now the corresponding Dirichlet series is

$$\sum_{r=1}^{\infty} \frac{N_3(1, r)}{r^s} = \zeta(s-2) \left(1 + \frac{8}{2^{2s}}\right) \prod_{p \equiv 1 \pmod 4} \left(1 + \frac{1}{p^{s-1}}\right) \prod_{p \equiv -1 \pmod 4} \left(1 - \frac{1}{p^{s-1}}\right).$$

Hence, $N_3(1, \boldsymbol{.}) = \mathrm{id}_2 * f$, where f is the multiplicative function defined for prime powers p^ν by

$$f(p^\nu) = \begin{cases} p, & \text{if } \ p \equiv 1 \pmod 4, \ \nu = 1; \\ -p, & \text{if } \ p \equiv -1 \pmod 4, \ \nu = 1; \\ 8, & \text{if } \ p = 2, \ \nu = 2; \\ 0, & \text{otherwise}, \end{cases}$$

and the given asymptotic formula is obtained by the convolution method. □

8.7 The congruence $x^2 + y^2 + z^2 + t^2 \equiv 0 \pmod r$

This is the case $k = 4$, $n = 0$ (sequence A240547 in [22]). For every r odd,

$$N_4(0, r) = r^3 \sum_{d \mid r} \frac{\varphi(d)}{d^2}$$

by Corollary 5 and using also Proposition 24 we conclude

Corollary 41. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_4(0, p^\nu) = \begin{cases} p^{2\nu-1}(p^{\nu+1} + p^\nu - 1), & \textit{if } \ p > 2, \ \nu \ge 1; \\ 2^{2\nu+1}, & \textit{if } \ p = 2, \ \nu \ge 1. \end{cases}$$

Proposition 42. *We have*

$$\sum_{r \le x} N_4(0, r) = \frac{5\pi^2}{168\zeta(3)} x^4 + O(x^3 \log x).$$

Proof. The corresponding Dirichlet series is

$$\sum_{r=1}^{\infty} \frac{N_4(0, r)}{r^s} = \zeta(s-2)\zeta(s-3) \left(1 - \frac{4}{2^s} - \frac{32}{2^{2s}}\right) \prod_{p > 2} \left(1 - \frac{1}{p^{s-1}}\right).$$

□

8.8 The congruence $x^2 + y^2 + z^2 + t^2 \equiv 1 \pmod{r}$

This is the case $k = 4$, $n = 1$. $N_4(1, r)$ is sequence A208895 in [22]. By the identity (22) giving its values for r odd and by Corollary 22 we obtain

Corollary 43. *For every prime power p^ν ($\nu \in \mathbb{N}$),*

$$N_4(1, p^\nu) = \begin{cases} p^{3\nu}(1 - 1/p^2), & \text{if } p > 2,\ \nu \geq 1; \\ 8^\nu, & \text{if } p = 2,\ \nu \geq 1. \end{cases}$$

Proposition 44. *We have*

$$\sum_{r \leq x} N_4(1, r) = \frac{2}{7\zeta(3)} x^4 + O(x^3).$$

Proof. Here

$$\sum_{r=1}^{\infty} \frac{N_4(1, r)}{r^s} = \zeta(s - 3) \prod_{p>2} \left(1 - \frac{1}{p^{s-1}}\right).$$

□

Finally, we deal with two special cases corresponding to $\boldsymbol{a} \neq (1, \ldots, 1)$.

8.9 The congruence $x^2 - y^2 \equiv 1 \pmod{r}$

Here $k = 2$, $n = 1$, $\boldsymbol{a} = (1, -1)$. $N_2(1, r, (1, -1))$ is sequence A062570 in [22]. Corollary 11 tells us that for every $r \in \mathbb{N}$ odd, $N_3(1, r, (1, -1)) = \varphi(r)$. Furthermore, from Proposition 1 one can deduce, similar to the proof of Proposition 21 that for every $\nu \in \mathbb{N}$, $N_3(1, 2^\nu, (1, -1)) = 2^\nu$. Thus,

Corollary 45. *For every $r \in \mathbb{N}$ one has*

$$N_3(1, r, (1, -1)) = \varphi(2r).$$

8.10 The congruence $x^2 + y^2 \equiv z^2 \pmod{r}$

This Phythagorean congruence is obtained for $k = 3$, $n = 0$, $a_1 = a_2 = 1$, $a_3 = -1$. $N_3(0, r, (1, 1, -1))$ is sequence A062775 in [22]. Proposition 19 shows that for every $r \in \mathbb{N}$ odd, $N_3(0, r, (1, 1, -1)) = N_3(0, r)$ given by (30). From Proposition 1 one can deduce that for every $\nu \in \mathbb{N}$,

$$N_3(0, 2^\nu, (1, 1, -1)) = 2^{2\nu} \left(2 - \frac{1}{2^{\lfloor \nu/2 \rfloor}}\right).$$

Consequently,

Corollary 46.

$$N_3(0, p^\nu, (1, 1, -1)) = \begin{cases} p^{3\beta-1}(p^{\beta+1} + p^\beta - 1), & \text{if } p > 2,\ \nu = 2\beta \text{ is even;} \\ p^{3\beta-2}(p^\beta + p^{\beta-1} - 1), & \text{if } p > 2,\ \nu = 2\beta - 1 \text{ is odd;} \\ 2^{3\beta}(2^{\beta+1} - 1), & \text{if } p = 2,\ \nu = 2\beta \text{ is even;} \\ 2^{3\beta-1}(2^\beta - 1), & \text{if } p = 2,\ \nu = 2\beta - 1 \text{ is odd.} \end{cases}$$

9 Acknowledgement

The author gratefully acknowledges support from the Austrian Science Fund (FWF) under the project Nr. M1376-N18. The author thanks Olivier Bordellès, Steven Finch and Wenguang Zhai for their valuable comments on the asymptotic formulas included in Section 8. The author is thankful to the referee for some corrections and remarks that have improved the paper.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[2] P. Bachmann, *Zahlentheorie*, vol. 4: Arithmetik der quadratischen Formen, Leipzig, 1898.

[3] R. C. Baker, The square-free divisor problem II, *Quart. J. Math. (Oxford)* (2) **47** (1996), 133–146.

[4] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, New York, NY: John Wiley & Sons, 1998.

[5] O. Bordellès, *Arithmetic Tales*, Springer, 2012.

[6] E. Cohen, Rings of arithmetic functions. II: The number of solutions of quadratic congruences, *Duke Math. J.* **21** (1954), 9–28.

[7] E. Cohen, A generalization of Axer's theorem and some of its applications, *Math. Nachr.* **27** (1963/1964), 163–177.

[8] E. Cohen, Arithmetical notes, VII: Some classes of even functions (mod r), *Collect. Math.* **16** (1964), 81–87.

[9] E. Cohen, Quadratic congruences with an odd number of summands, *Amer. Math. Monthly* **73** (1966), 138–143.

[10] L. E. Dickson, *History of the Theory of Numbers*, vol. II, reprinted by Chelsea, New York, 1966.

[11] S. Finch, G. Martin, and P. Sebah, Roots of unity and nullity modulo n, *Proc. Amer. Math. Soc.* **138** (2010), 2729–2743.

[12] K. Girstmair, The equation $x^2 + \overline{m}y^2 = \overline{k}$ in $\mathbb{Z}/p\mathbb{Z}$, *Amer. Math. Monthly* **120** (2013), 546–552.

[13] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, 1985.

[14] G. H, Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Sixth Edition, Edited and revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

[15] L. K. Hua, *Introduction to Number Theory*, Springer, 1982.

[16] M. N. Huxley, Exponential sums and lattice points III., *Proc. London Math. Soc.* **87** (2003), 591–609.

[17] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics 84, Springer, 1990.

[18] H. Minkowski, *Gesammelte Abhandlungen*, Leipzig, 1911.

[19] W. Narkiewicz, *Number Theory*, World Scientific, Singapore, 1983.

[20] M. B. Nathanson, *Elementary Methods in Number Theory*, Graduate Texts in Mathematics 195, Springer, 2000.

[21] M. O. Rabin and J. O. Shallit, Randomized algorithms in number theory, *Comm. in Pure and Applied Math.* **39** (supplement) (1986), S239–S256.

[22] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`

[23] D. Suryanarayana and V. Siva Rama Prasad, The number of k-free divisors of an integer, *Acta Arith.* **17** (1971), 345–354.

[24] L. Tóth and P. Haukkanen, The discrete Fourier transform of r-even functions, *Acta Univ. Sapientiae, Math.* **3** (2011), 5–25.

L. Tóth
Department of Mathematics, University of Pécs
Ifjúság útja 6, H-7624 Pécs, Hungary
and
Institute of Mathematics, Universität für Bodenkultur
Gregor Mendel-Straße 33, A-1180 Vienna, Austria
E-mail: ltoth@gamma.ttk.pte.hu