Max-Planck-Institut für Mathematik
Bonn

Generalizations of the Markoff-Hurwitz equations over residue class rings

by

Ioulia N. Baoulina

Max-Planck-Institut für Mathematik
Preprint Series 2014 (14)

Generalizations of the Markoff-Hurwitz equations over residue class rings

Ioulia N. Baoulina

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 14-14

GENERALIZATIONS OF THE MARKOFF-HURWITZ EQUATIONS OVER RESIDUE CLASS RINGS

IOULIA N. BAOULINA

ABSTRACT. In this paper, we use evaluations of Gauss sums modulo p^k to derive expressions that allow us for a given generalized Markoff-Hurwitz equation to determine the number of its solutions over $\mathbb{Z}/p^k\mathbb{Z}$ if the number of solutions over $\mathbb{Z}/p\mathbb{Z}$ is known. We also calculate the corresponding Poincaré series.

1. INTRODUCTION

Let $\mathcal{R}$ be a commutative ring. A Markoff-Hurwitz equation over $\mathcal{R}$ is an equation of the type

$$x_1^2 + \cdots + x_n^2 = bx_1 \cdots x_n,$$

where $b \in \mathcal{R} \setminus \{0\}$ and $n \geq 3$. Markoff [21] used continued fractions to find all integer solutions in the case $b = n = 3$ and Hurwitz [18] described the set of integer solutions in the general case. For a history of the problem and related references see [5]. Baragar [6] and Silverman [22] studied solutions to a Markoff-Hurwitz equation when $\mathcal{R}$ is an order in a number field. Recently [4] we considered the case when $\mathcal{R} = \mathbb{Z}/p^k\mathbb{Z}$, where p is a prime and k is a positive integer. Using an elementary algebraic-combinatorial approach, we obtained expressions that allow us for a given Markoff-Hurwitz equation to find the number of its solutions over $\mathbb{Z}/p^k\mathbb{Z}$ if the number of solutions over $\mathbb{Z}/p\mathbb{Z}$ is known.

Carlitz [9] considered a generalized Markoff-Hurwitz equation

$$a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n + c,$$

where $a_1, \ldots, a_n, b \in \mathcal{R} \setminus \{0\}$, $c \in \mathcal{R}$, over $\mathcal{R} = \mathrm{GF}(q)$ with odd q. He found the explicit formulas for the number of solutions when $n = 3$ and when $n = 4$ (under a certain restriction on the coefficients). Some generalizations of Carlitz's results can be found in [2] and [3].

In this paper, we study a generalized Markoff-Hurwitz equation in the case when $\mathcal{R} = \mathbb{Z}/q\mathbb{Z}$, that is, we consider a congruence of the type

$$a_1x_1^2 + \cdots + a_nx_n^2 \equiv bx_1 \cdots x_n + c \pmod{q}, \tag{1.1}$$

where $n \geq 3$, $q > 1$ is an integer and $a_1, \ldots, a_n, b, c$ are integers satisfying $\gcd(a_1 \cdots a_n, q) = 1$. Let $N_q(\bar{a}, b, c)$ denote the number of solutions to (1.1) in $x_1, \ldots, x_n \pmod{q}$. For an integer z and an odd q, let (z/q) denote the generalized

---

2000 *Mathematics Subject Classification.* 11D79, 11G25.

Jacobi symbol. Cohen [10] investigated (1.1) when q is odd and $b \equiv 0 \pmod{q}$. He proved [10, Corollary 1] that

$$N_q(\bar{a},0,0) = \begin{cases} q^{n-1} \sum_{d|q} \Big(\dfrac{(-1)^{n/2}a_1\cdots a_n}{d}\Big)\dfrac{\varphi(d)}{d^{n/2}} & \text{if } 2 \mid n, \\ q^{n-1} \sum_{d^2|q} \dfrac{\varphi(d^2)}{d^n} & \text{if } 2 \nmid n, \end{cases}$$

where φ is the Euler function. For the case $\gcd(c,q)=1$, Cohen [10, Corollary 2] gave the formula

$$N_q(\bar{a},0,c) = \begin{cases} q^{n-1} \sum_{d|q} \Big(\dfrac{(-1)^{n/2}a_1\cdots a_n}{d}\Big)\dfrac{\mu(d)}{d^{n/2}} & \text{if } 2 \mid n, \\ q^{n-1} \sum_{d|q} \Big(\dfrac{(-1)^{(n-1)/2}a_1\cdots a_n c}{d}\Big)\dfrac{\mu^2(d)}{d^{(n-1)/2}} & \text{if } 2 \nmid n, \end{cases}$$

where μ is the Möbius function.

Throughout much of this paper we are particularly interested in the congruence

$$a_1x_1^2 + \cdots + a_nx_n^2 \equiv bx_1\cdots x_n + c \pmod{p^k}, \tag{1.2}$$

where $n \geq 3$, $p > 2$ is a prime, k is a positive integer, $a_1,\dots,a_n,b,c$ are integers with $p \nmid a_1\cdots a_n$. From now on, we assume that $p \nmid c$. The result of Cohen mentioned above yields

$$N_{p^k}(\bar{a},0,c) = p^{k(n-1)} - \Big(\frac{(-1)^{n/2}a_1\cdots a_n}{p}\Big)p^{((2k-1)(n-1)-1)/2}$$

if n is even, and

$$N_{p^k}(\bar{a},0,c) = p^{k(n-1)} + \Big(\frac{(-1)^{(n-1)/2}a_1\cdots a_n c}{p}\Big)p^{(2k-1)(n-1)/2}$$

if n is odd. The special case

$$N_p(\bar{a},0,c) = \begin{cases} p^{n-1} - \Big(\dfrac{(-1)^{n/2}a_1\cdots a_n}{p}\Big)p^{(n-2)/2} & \text{if } 2 \mid n, \\ p^{n-1} + \Big(\dfrac{(-1)^{(n-1)/2}a_1\cdots a_n c}{p}\Big)p^{(n-1)/2} & \text{if } 2 \nmid n, \end{cases} \tag{1.3}$$

is due to Jordan [20] (see also [7, Theorem 10.5.1]). Carlitz [9, Theorem 1] showed that if $n=3$ and $p \nmid b$, then

$$N_p(\bar{a},b,c) = p^2 + 1 + \left(\Big(\frac{a_1}{p}\Big) + \Big(\frac{a_2}{p}\Big) + \Big(\frac{a_3}{p}\Big) + \Big(\frac{c}{p}\Big)\right)\Big(\frac{b^2c - 4a_1a_2a_3}{p}\Big)p. \tag{1.4}$$

Further, if $n=4$ and $p \mid (b^2c^2 - 16a_1a_2a_3a_4)$ then [9, Theorem 3] yields

$$\begin{aligned} N_p(\bar{a},b,c) = {} & p^3 - 1 + \frac{1}{2}\left(\Big(\frac{a_1a_2}{p}\Big) + \Big(\frac{a_1a_3}{p}\Big) + \Big(\frac{a_1a_4}{p}\Big) + \Big(\frac{a_2a_3}{p}\Big)\right. \\ & \left. + \Big(\frac{a_2a_4}{p}\Big) + \Big(\frac{a_3a_4}{p}\Big)\right)\Big(\frac{-1}{p}\Big)p(p-2) - \Big(\frac{-1}{p}\Big)p \\ & - \left(\Big(\frac{a_1}{p}\Big) + \Big(\frac{a_2}{p}\Big) + \Big(\frac{a_3}{p}\Big) + \Big(\frac{a_4}{p}\Big)\right)\Big(\frac{-2c}{p}\Big)p. \end{aligned} \tag{1.5}$$

Also, if $n = 4$, $p \mid (b^2c^2 - 8a_1a_2a_3a_4)$ and $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right) = 0$ then [9, Theorem 2] together with properties of Jacobsthal sums [7, Proposition 6.1.10 and Theorems 6.2.1] imply that

$$N_p(\bar{a}, b, c) = \begin{cases} p^3 - 2p - 1 & \text{if } p \equiv 3 \pmod 4, \\ p^3 + 2(A+1)p - 1 & \text{if } p \equiv 1 \pmod 4, \end{cases} \tag{1.6}$$

where the integer A is uniquely determined by

$$p = A^2 + B^2, \qquad A \equiv -1 \pmod 4. \tag{1.7}$$

In general there is no explicit formula for evaluating $N_{p^k}(\bar{a}, b, c)$. The aim of this paper is to find expressions that allow us to calculate $N_{p^k}(\bar{a}, b, c)$ if $N_p(\bar{a}, b, c)$ is known. Our main results in Section 3 are Theorems 3.1 – 3.3, in which we obtain the desired expressions. In Section 4, we combine our expressions with the results of Carlitz mentioned above to determine explicitly $N_{p^k}(\bar{a}, b, c)$ and $N_q(\bar{a}, b, c)$ for $n = 3$ and for $n = 4$. In Section 5, we compute the corresponding Poincaré series and verify the Q-conjecture of Hayes and Nutt [16]. Poincaré series for more general polynomials are discussed in Section 6.

Throughout this paper, we use the following notation. Let $N^*_{p^k}(\bar{a}, b, c)$ denote the number of solutions to (1.2) with $p \nmid x_1 \cdots x_n$, and $N^{(0)}_{p^k}(\bar{a}, b, c) = N_{p^k}(\bar{a}, b, c) - N^*_{p^k}(\bar{a}, b, c)$. Let r be a nonnegative integer such that

$$p^r \parallel (b^2c^{n-2} - 4(n-2)^{n-2}a_1 \cdots a_n).$$

For $b^2c^{n-2} = 4(n-2)^{n-2}a_1 \cdots a_n$ we use the convention $r = \infty$. Let

$$\theta = \begin{cases} \left(\dfrac{(-1)^{(n-2)/2} \cdot 2(n-2)}{p}\right) & \text{if } 2 \mid n, \\ \left(\dfrac{(-1)^{(n-3)/2} \cdot c(n-2)}{p}\right) & \text{if } 2 \nmid n. \end{cases}$$

For any positive integer q, set $\zeta_q = \exp(2\pi i/q)$.

2. Preliminary Lemmas

First we state our earlier result which will be useful in the sequel. We write $|\mathcal{A}|$ for the number of elements of a finite set $\mathcal{A}$.

Lemma 2.1. *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a nonzero polynomial, and let $k, \alpha_1, \ldots, \alpha_n$ be integers with $k \geq 2$ and $0 \leq \alpha_1, \ldots, \alpha_n \leq [k/2]$. For $\nu \in \{k-1, k\}$, let $\mathcal{A}_{\bar{\alpha},\nu}$ be the set of n-tuples $(u_1, \ldots, u_n)$ of integers such that $1 \leq u_1, \ldots, u_n \leq p^\nu$, $f(u_1, \ldots, u_n) \equiv 0 \pmod{p^\nu}$, and for each j,*

$$p^{\alpha_j} \,\Big\|\, \frac{\partial f}{\partial x_j}(u_1, \ldots, u_n) \quad \text{if} \quad \alpha_j < [k/2],$$
$$p^{\alpha_j} \,\Big|\, \frac{\partial f}{\partial x_j}(u_1, \ldots, u_n) \quad \text{if} \quad \alpha_j = [k/2].$$

Let

$$\mathcal{A}^{(0)}_{\bar{\alpha},\nu} = \{(u_1, \ldots, u_n) \in \mathcal{A}_{\bar{\alpha},\nu} \,:\, p \mid u_1 \cdots u_n\},$$
$$\mathcal{A}^{*}_{\bar{\alpha},\nu} = \{(u_1, \ldots, u_n) \in \mathcal{A}_{\bar{\alpha},\nu} \,:\, p \nmid u_1 \cdots u_n\}.$$

If $\min\{\alpha_1,\dots,\alpha_n\} < [k/2]$ *then*

$$|\mathcal{A}^{(0)}_{\bar{\alpha},k}| = p^{n-1}|\mathcal{A}^{(0)}_{\bar{\alpha},k-1}|, \qquad |\mathcal{A}^{*}_{\bar{\alpha},k}| = p^{n-1}|\mathcal{A}^{*}_{\bar{\alpha},k-1}|.$$

Proof. See [4, Lemma 2.1 and Remark 2.2]. □

Next we recall a few facts about characters. The following lemma gives the orthogonality relation for Dirichlet characters modulo p^k.

Lemma 2.2. *For integers x and y with $p \nmid x$,*

$$\sum_{\chi \pmod{p^k}} \chi(x)\bar{\chi}(y) = \begin{cases} \varphi(p^k) & \text{if } p^k \mid (x-y), \\ 0 & \text{if } p^k \nmid (x-y), \end{cases}$$

where the summation is taken over all Dirichlet characters χ modulo p^k.

Proof. See [1, Theorem 6.16]. □

Since

$$\sum_{\substack{\chi \pmod{p^k} \\ \chi\text{- primitive}}} \chi(x)\bar{\chi}(y) = \sum_{\chi \pmod{p^k}} \chi(x)\bar{\chi}(y) \;-\; \sum_{\chi \pmod{p^{k-1}}} \chi(x)\bar{\chi}(y),$$

for $k \ge 2$, the next lemma is a straightforward consequence of Lemma 2.2.

Lemma 2.3. *Let $k \ge 2$. Then for integers x and y with $p \nmid x$,*

$$\sum_{\substack{\chi \pmod{p^k} \\ \chi\text{- primitive}}} \chi(x)\bar{\chi}(y) = \begin{cases} \varphi(p^k) - \varphi(p^{k-1}) & \text{if } p^k \mid (x-y), \\ -\varphi(p^{k-1}) & \text{if } p^{k-1} \parallel (x-y), \\ 0 & \text{if } p^{k-1} \nmid (x-y). \end{cases}$$

Let χ be a Dirichlet character modulo p^k. The Gauss sum corresponding to χ is defined by

$$G(\chi) = \sum_{x=1}^{p^k} \chi(x)\zeta_{p^k}^{x}.$$

Gauss sums occur in the Fourier expansion of a primitive character.

Lemma 2.4. *Let χ be a primitive Dirichlet character modulo p^k. Then for any integer x,*

$$\chi(x) = \frac{G(\chi)}{p^k} \sum_{y=1}^{p^k} \bar{\chi}(y)\zeta_{p^k}^{-xy}.$$

Proof. See [1, Theorem 8.20]. □

For a Dirichlet character χ modulo p^k, define

$$T(\chi) = \sum_{1 \le x_1,\dots,x_n \le p^k} \chi(x_1^2 \cdots x_n^2)\bar{\chi}^2(a_1x_1^2 + \cdots + a_nx_n^2 - c).$$

In the following lemma we express $T(\chi)$ in terms of Gauss sums, under a certain restriction on the coefficients. For convenience, we also use the notation η for the Jacobi symbol $\left(\frac{\cdot}{p}\right)$.

Lemma 2.5. *Let χ be a primitive character modulo p^k. Assume that $\big(\frac{a_1}{p}\big) = \cdots = \big(\frac{a_n}{p}\big) = \big(\frac{c(n-2)}{p}\big)$. Then*

$$T(\chi) = \frac{\bar{\chi}(a_1 \cdots a_n) G(\bar{\chi}^2)}{p^k} \sum_{y=1}^{p^k} \bar{\chi}^{n-2}(y) \zeta_{p^k}^{-cy} \Big(G(\chi) + \Big(\frac{c(n-2)y}{p}\Big) G(\chi\eta) \Big)^n.$$

Proof. Note that $\bar{\chi}^2$ is primitive. By Lemma 2.4

$$\bar{\chi}^2(a_1 x_1^2 + \cdots + a_n x_n^2 - c) = \frac{G(\bar{\chi}^2)}{p^k} \sum_{y=1}^{p^k} \chi^2(y) \zeta_{p^k}^{-(a_1 x_1^2 + \cdots + a_n x_n^2 - c)y}.$$

Hence

$$\begin{aligned} T(\chi) &= \frac{G(\bar{\chi}^2)}{p^k} \sum_{y=1}^{p^k} \chi^2(y) \zeta_{p^k}^{cy} \sum_{1 \le x_1, \ldots, x_n \le p^k} \chi(x_1^2 \cdots x_n^2) \zeta_{p^k}^{-(a_1 x_1^2 + \cdots + a_n x_n^2)y} \\ &= \frac{G(\bar{\chi}^2)}{p^k} \sum_{\substack{y=1 \\ p \nmid y}}^{p^k} \chi^2(y) \zeta_{p^k}^{cy} \prod_{j=1}^{n} \sum_{x_j=1}^{p^k} \Big(1 + \Big(\frac{x_j}{p}\Big)\Big) \chi(x_j) \zeta_{p^k}^{-a_j x_j y} \\ &= \frac{G(\bar{\chi}^2)}{p^k} \sum_{\substack{y=1 \\ p \nmid y}}^{p^k} \chi^2(y) \zeta_{p^k}^{cy} \prod_{j=1}^{n} \bar{\chi}(-a_j y) \Big(G(\chi) + \Big(\frac{-a_j y}{p}\Big) G(\chi\eta) \Big), \end{aligned}$$

that is

$$T(\chi) = \frac{\bar{\chi}(a_1 \cdots a_n) G(\bar{\chi}^2)}{p^k} \sum_{y=1}^{p^k} \bar{\chi}^{n-2}(y) \zeta_{p^k}^{-cy} \Big(G(\chi) + \Big(\frac{c(n-2)y}{p}\Big) G(\chi\eta) \Big)^n,$$

as desired. □

Let $k \geq 2$, and let ψ be a primitive Dirichlet character modulo p^k of order $\varphi(p^k)$ normalized such that

$$\begin{aligned} &\psi(1 + p^{k/2}) = \zeta_{p^{k/2}}^{-1} && \text{if } 2 \mid k, \\ &\psi\big(1 + p^{(k-1)/2} + \frac{p+1}{2} p^{k-1}\big) = \zeta_{p^{(k+1)/2}}^{-1} && \text{if } 2 \nmid k. \end{aligned}$$

Then every primitive character χ modulo p^k has the form $\chi = \psi^j$ with $p \nmid j$.

Lemma 2.6. *Let $k \geq 2$. For any integer j with $p \nmid j$,*

$$G(\psi^j) = \begin{cases} p^{k/2} \psi^j(j) \zeta_{p^k}^j & \text{if } 2 \mid k, \\ p^{k/2} \psi^j(j) \Big(\dfrac{j}{p}\Big) \zeta_{p^k}^j \zeta_8^{1-p} & \text{if } 2 \nmid k. \end{cases}$$

Proof. See [15, Corollary 2.1]. □

Lemma 2.7. *Let $k \geq 2$. For any integer j with $p \nmid j$,*

$$G(\psi^j \eta) = \Big(\frac{j}{p}\Big) G(\psi^j).$$

Proof. Observe that $\eta = \psi^{p^k(p-1)/2}$. Applying Lemma 2.6, we deduce the asserted result. □

Lemma 2.8. *Let $k\ge 2$ and let j be an integer with $p\nmid j$. Assume that* $\left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right)$. *Then*

$$T(\psi^j)=2^n p^{kn/2}\psi^j(c^{n-2})\bar\psi^j(4(n-2)^{n-2}a_1\cdots a_n)\times\begin{cases}1 & \text{if } 2\mid k,\\ \left(\frac{2}{p}\right)^{n+1}\left(\frac{n-2}{p}\right)\left(\frac{j}{p}\right)^n i^{(n-2)(p-1)^2/4} & \text{if } 2\nmid k.\end{cases}$$

Proof. Appealing to Lemmas 2.5 and 2.7, we obtain

$$\begin{aligned}T(\psi^j)&=\frac{\bar\psi^j(a_1\cdots a_n)G^n(\psi^j)G(\bar\psi^{2j})}{p^k}\sum_{y=1}^{p^k}\bar\psi^{j(n-2)}(y)\zeta_{p^k}^{-cy}\left(1+\left(\frac{jc(n-2)y}{p}\right)\right)^n\\&=\frac{2^{n-1}\bar\psi^j(a_1\cdots a_n)G^n(\psi^j)G(\bar\psi^{2j})}{p^k}\\&\quad\times\left(\sum_{y=1}^{p^k}\bar\psi^{j(n-2)}(y)\zeta_{p^k}^{-cy}+\left(\frac{jc(n-2)}{p}\right)\sum_{y=1}^{p^k}\left(\frac{y}{p}\right)\bar\psi^{j(n-2)}(y)\zeta_{p^k}^{-cy}\right)\\&=\frac{2^{n-1}\bar\psi^j(a_1\cdots a_n)\psi^{j(n-2)}(-c)G^n(\psi^j)G(\bar\psi^{2j})}{p^k}\\&\quad\times\left(G(\bar\psi^{j(n-2)})+\left(\frac{jc(n-2)}{p}\right)\left(\frac{-c}{p}\right)G(\bar\psi^{j(n-2)}\eta)\right),\end{aligned}$$

that is

$$T(\psi^j)=\frac{2^n\bar\psi^j(a_1\cdots a_n)\psi^{j(n-2)}(-c)G^n(\psi^j)G(\bar\psi^{2j})G(\bar\psi^{j(n-2)})}{p^k}. \tag{2.1}$$

Note that

$$\psi^{-2j}(-2j)=\bar\psi^j(4)\psi^{-2j}(j),$$
$$\psi^{-j(n-2)}(-j(n-2))=\bar\psi^{j(n-2)}(-1)\bar\psi^j((n-2)^{n-2})\psi^{2j}(j)\bar\psi^{jn}(j).$$

Combining these relations with Lemma 2.6 and (2.1) and using the fact that $\zeta_8^{1-p}=\left(\frac{2}{p}\right)i^{(p-1)^2/4}$, we deduce the desired result. □

Lemma 2.9. *Let $k\ge 3$ be odd. Then for integers x and y with $p^{k-1}\mid(x-y)$ and $p\nmid x$,*

$$\sum_{j=1}^{\varphi(p^k)}\left(\frac{j}{p}\right)\psi^j(x)\bar\psi^j(y)=\left(\frac{-y}{p}\right)\left(\frac{(x-y)/p^{k-1}}{p}\right)i^{(p-1)^2/4}p^{k-(3/2)}(p-1).$$

Proof. Since $p^{k-1}\mid(x-y)$, there exists a positive integer t such that

$$x\equiv y(1+p^{k-1}t)\equiv y(1+p^{k-1})^t \pmod{p^k}.$$

Note that

$$\left(1+p^{(k-1)/2}+\frac{p+1}{2}p^{k-1}\right)^{p^{(k-1)/2}}\equiv 1+p^{k-1}\pmod{p^k}.$$

Thus, for any integer j,

$$\psi^j(x)\bar\psi^j(y)=\psi^{jtp^{(k-1)/2}}\left(1+p^{(k-1)/2}+\frac{p+1}{2}p^{k-1}\right)=\zeta_{p^{(k+1)/2}}^{-jtp^{(k-1)/2}}=\zeta_p^{-jt}.$$

Hence

$$\sum_{j=1}^{\varphi(p^k)}\Big(\frac{j}{p}\Big)\psi^j(x)\bar{\psi}^j(y)=\sum_{j=1}^{\varphi(p^k)}\Big(\frac{j}{p}\Big)\zeta_p^{-jt}=\frac{\varphi(p^k)}{p}\Big(\frac{-t}{p}\Big)i^{(p-1)^2/4}\sqrt{p}.$$

Since

$$\frac{x-y}{p^{k-1}}\equiv yt \pmod{p},$$

we have

$$\Big(\frac{-t}{p}\Big)=\Big(\frac{-y}{p}\Big)\Big(\frac{(x-y)/p^{k-1}}{p}\Big),$$

and the asserted result follows. □

An immediate consequence of Lemmas 2.3, 2.8 and 2.9 is the following.

Lemma 2.10. *Let $2\le k\le r+1$. Assume that $\big(\frac{a_1}{p}\big)=\cdots=\big(\frac{a_n}{p}\big)=\big(\frac{c(n-2)}{p}\big)$ and $p\nmid b$. If kn is even then*

$$\frac{1}{\varphi(p^k)}\sum_{\substack{\chi \pmod{p^k}\\ \chi\text{- primitive}}}\chi(b^2)T(\chi)=\begin{cases}2^n\theta^k p^{(kn-2)/2}(p-1) & \text{if } k\le r,\\ -2^n\theta^{r+1}p^{((r+1)n-2)/2} & \text{if } k=r+1,\end{cases}$$

If kn is odd then

$$\frac{1}{\varphi(p^k)}\sum_{\substack{\chi \pmod{p^k}\\ \chi\text{- primitive}}}\chi(b^2)T(\chi)=\left(\frac{\frac{b^2c^{n-2}-4(n-2)^{n-2}a_1\cdots a_n}{p^{k-1}}}{p}\right)\cdot 2^n\theta^k p^{(kn-1)/2}.$$

3. Expressions for $N_{p^k}(\bar{a},b,c)$

First we show that the difference $N^{(0)}_{p^k}(\bar{a},b,c)-p^{n-1}N^{(0)}_{p^{k-1}}(\bar{a},b,c)$ vanishes for all $k\ge 2$.

Lemma 3.1. *Let $k\ge 2$. Then $N^{(0)}_{p^k}(\bar{a},b,c)-p^{n-1}N^{(0)}_{p^{k-1}}(\bar{a},b,c)=0$.*

Proof. For $\nu\in\{k-1,k\}$, let $\bar{N}^{(0)}_{p^\nu}(\bar{a},b,c)$ denote the number of solutions to the congruence

$$a_1x_1^2+\cdots+a_nx_n^2\equiv bx_1\cdots x_n+c \pmod{p^\nu} \tag{3.1}$$

in $x_1,\ldots,x_n \pmod{p^\nu}$ such that $p\mid x_1\cdots x_n$ and

$$\begin{aligned}2a_1x_1&\equiv bx_2x_3\cdots x_n \pmod{p^{[k/2]}},\\ 2a_2x_2&\equiv bx_1x_3\cdots x_n \pmod{p^{[k/2]}},\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ 2a_nx_n&\equiv bx_1x_2\cdots x_{n-1} \pmod{p^{[k/2]}}.\end{aligned} \tag{3.2}$$

By Lemma 2.1

$$N^{(0)}_{p^k}(\bar{a},b,c)-p^{n-1}N^{(0)}_{p^{k-1}}(\bar{a},b,c)=\bar{N}^{(0)}_{p^k}(\bar{a},b,c)-p^{n-1}\bar{N}^{(0)}_{p^{k-1}}(\bar{a},b,c).$$

It is readily seen that for each solution $(x_1,\ldots,x_n)$ to the system of congruences (3.2) with $p\mid x_1\cdots x_n$ we have $p\mid x_1,\ \ldots,\ p\mid x_n$. But since $p\nmid c$, none of these solutions satisfy (3.1). Therefore, $\bar{N}^{(0)}_{p^k}(\bar{a},b,c)=\bar{N}^{(0)}_{p^{k-1}}(\bar{a},b,c)=0$, and the result follows. □

Next we show that in many cases $N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c)$ also vanishes.

Lemma 3.2. *Let $k \ge 2$. Then $N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c) = 0$ except possibly when $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $p \nmid b$ and $k \le r+1$.*

Proof. For $\nu \in \{k-1, k\}$, let $\bar{N}^*_{p^\nu}(\bar{a},b,c)$ denote the number of solutions to the congruence (3.1) in $x_1, \dots, x_n \pmod{p^\nu}$ such that $p \nmid x_1 \cdots x_n$ and (3.2) holds. By Lemma 2.1

$$N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c) = \bar{N}^*_{p^k}(\bar{a},b,c) - p^{n-1}\bar{N}^*_{p^{k-1}}(\bar{a},b,c). \tag{3.3}$$

Observe that $\bar{N}^*_{p^k}(\bar{a},b,c) = \bar{N}^*_{p^{k-1}}(\bar{a},b,c) = 0$ for $b \equiv 0 \pmod p$. Further, when $p \nmid x_1 \cdots x_n$, the system of congruences (3.2) can be rewritten as

$$2a_1x_1^2 \equiv \cdots \equiv 2a_nx_n^2 \equiv bx_1 \cdots x_n \pmod{p^{[k/2]}}. \tag{3.4}$$

For any integers $x_1, \dots, x_n$ with $p \nmid x_1 \cdots x_n$ for which (3.1) and (3.4) hold simultaneously, we have

$$(n-2)a_jx_j^2 \equiv c \pmod{p^{[k/2]}}, \qquad j = 1, \dots, n. \tag{3.5}$$

Consequently, $\bar{N}^*_{p^k}(\bar{a},b,c) = \bar{N}^*_{p^{k-1}}(\bar{a},b,c) = 0$ except possibly when $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ and $p \nmid b$.

Now assume that $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $p \nmid b$ and $x_1, \dots, x_n$ are integers with $p \nmid x_1 \cdots x_n$ satisfying (3.1), (3.4) and (3.5). We have

$$(a_1x_1^2 + \cdots + a_nx_n^2 - c)^2 \equiv b^2x_1^2 \cdots x_n^2 \pmod{p^{k-1}}.$$

Multiplying both sides by $(n-2)^n a_1 \cdots a_n \not\equiv 0 \pmod p$, we obtain

$$\begin{aligned}(n-2)^{n-2}a_1 \cdots a_n &\left(\sum_{j=1}^n \big((n-2)a_jx_j^2 - c\big) + 2c\right)^2 \\ &\equiv b^2 \prod_{j=1}^n \big(((n-2)a_jx_j^2 - c) + c\big) \pmod{p^{k-1}}.\end{aligned} \tag{3.6}$$

In view of (3.5),

$$\left(\sum_{j=1}^n \big((n-2)a_jx_j^2 - c\big) + 2c\right)^2 \equiv 4c^2 + 4c\sum_{j=1}^n \big((n-2)a_jx_j^2 - c\big) \pmod{p^{k-1}}$$

and

$$\prod_{j=1}^n \big(((n-2)a_jx_j^2 - c) + c\big) \equiv c^n + c^{n-1}\sum_{j=1}^n \big((n-2)a_jx_j^2 - c\big) \pmod{p^{k-1}}.$$

We can now rewrite (3.6) in the equivalent form

$$(b^2c^{n-2} - 4(n-2)^{n-2}a_1 \cdots a_n)\left(c^2 + c\sum_{j=1}^n \big((n-2)a_jx_j^2 - c\big)\right) \equiv 0 \pmod{p^{k-1}}.$$

By (3.5), this is only possible if $p^{k-1} \mid (b^2c^{n-2} - 4(n-2)^{n-2}a_1 \cdots a_n)$, or, equivalently, if $k \le r+1$. Therefore we have established that $\bar{N}^*_{p^k}(\bar{a},b,c) = \bar{N}^*_{p^{k-1}}(\bar{a},b,c) = 0$ except possibly when $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $p \nmid b$ and $k \le r+1$. The asserted result now follows from (3.3). □

We are now ready to determine $N_{p^k}(\bar{a},b,c)$ in the case $p \mid b$. We obtain immediately from (1.3) and Lemmas 3.1 and 3.2 the following.

Theorem 3.1. *Assume that $p \mid b$. If n is even then*

$$N_{p^k}(\bar{a},b,c) = p^{k(n-1)} - \Big(\frac{(-1)^{n/2}a_1\cdots a_n}{p}\Big)p^{((2k-1)(n-1)-1)/2}.$$

If n is odd then

$$N_{p^k}(\bar{a},b,c) = p^{k(n-1)} + \Big(\frac{(-1)^{(n-1)/2}a_1\cdots a_n c}{p}\Big)p^{(2k-1)(n-1)/2}.$$

Remark. Under the condition $p \mid b$ we have $N_{p^k}(\bar{a},b,c) = N_{p^k}(\bar{a},0,c)$.

It remains to calculate the difference $N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c)$ in the case $\big(\frac{a_1}{p}\big) = \cdots = \big(\frac{a_n}{p}\big) = \big(\frac{c(n-2)}{p}\big)$, $p \nmid b$, $2 \le k \le r+1$.

Lemma 3.3. *Let $2 \le k \le r+1$. Assume that $\big(\frac{a_1}{p}\big) = \cdots = \big(\frac{a_n}{p}\big) = \big(\frac{c(n-2)}{p}\big)$ and $p \nmid b$. If n is even then*

$$N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c) = \begin{cases} 2^{n-1}\theta^k p^{(kn-2)/2}(p-1) & \text{if } k \le r, \\ -2^{n-1}\theta^{r+1}p^{((r+1)n-2)/2} & \text{if } k = r+1. \end{cases}$$

If n is odd and $k \ne r+1$ then

$$N^*_{p^k}(\bar{a},b,c) - p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c) = \begin{cases} 2^{n-1}p^{(kn-2)/2}(p-1) & \text{if } 2 \mid k \text{ and } k \le r, \\ 0 & \text{otherwise.} \end{cases}$$

If n is odd, $r > 0$ and $b^2c^{n-2} \ne 4(n-2)^{n-2}a_1\cdots a_n$ then

$$N^*_{p^{r+1}}(\bar{a},b,c) - p^{n-1}N^*_{p^r}(\bar{a},b,c) = (-1)^r\left(\frac{\frac{b^2c^{n-2}-4(n-2)^{n-2}a_1\cdots a_n}{p^r}}{p}\right)^{r+1} \times 2^{n-1}\theta^{r+1}p^{[((r+1)n-1)/2]}.$$

Proof. For $\nu \in \{k-1,k\}$, let $\hat{N}^*_{p^\nu}(\bar{a},b,c)$ denote the number of solutions to the congruence

$$(a_1x_1^2 + \cdots + a_nx_n^2 - c)^2 \equiv b^2x_1^2\cdots x_n^2 \pmod{p^\nu}$$

in $x_1,\ldots,x_n \pmod{p^\nu}$ such that $p \nmid x_1\cdots x_n$. It is readily seen that

$$\hat{N}^*_{p^\nu}(\bar{a},b,c) = N^*_{p^\nu}(\bar{a},b,c) + N^*_{p^\nu}(\bar{a},-b,c) = 2N^*_{p^\nu}(\bar{a},b,c).$$

Further, by Lemma 2.2,

$$\begin{aligned}\hat{N}^*_{p^k}(\bar{a},b,c) &= \frac{1}{\varphi(p^k)} \sum_{\substack{1\le x_1,\dots,x_n\le p^k\\ p\nmid x_1\cdots x_n}} \sum_{\chi \,(\mathrm{mod}\ p^k)} \chi(b^2x_1^2\cdots x_n^2)\bar{\chi}^2(a_1x_1^2+\cdots+a_nx_n^2-c)\\
&= \frac{1}{\varphi(p^k)} \sum_{\substack{1\le x_1,\dots,x_n\le p^k\\ p\nmid x_1\cdots x_n}} \sum_{\chi \,(\mathrm{mod}\ p^{k-1})} \chi(b^2x_1^2\cdots x_n^2)\bar{\chi}^2(a_1x_1^2+\cdots+a_nx_n^2-c)\\
&\quad+ \frac{1}{\varphi(p^k)} \sum_{1\le x_1,\dots,x_n\le p^k} \sum_{\substack{\chi \,(\mathrm{mod}\ p^k)\\ \chi\text{- primitive}}} \chi(b^2x_1^2\cdots x_n^2)\bar{\chi}^2(a_1x_1^2+\cdots+a_nx_n^2-c)\\
&= p^{n-1}\hat{N}^*_{p^{k-1}}(\bar{a},b,c) + \frac{1}{\varphi(p^k)} \sum_{\substack{\chi \,(\mathrm{mod}\ p^k)\\ \chi\text{- primitive}}} \chi^2(b)T(\chi).\end{aligned}$$

Hence

$$N^*_{p^k}(\bar{a},b,c) = p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c) + \frac{1}{2\varphi(p^k)} \sum_{\substack{\chi \,(\mathrm{mod}\ p^k)\\ \chi\text{- primitive}}} \chi(b^2)T(\chi).$$

The required expressions now follow from Lemma 2.10. □

Corollary 3.1. *Let*

$$k \ge \begin{cases} 3 & \text{if } 2 \mid n,\ \left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right) \text{ and}\\ & b^2c^{n-2}=4(n-2)^{n-2}a_1\cdots a_n,\\ 4 & \text{if } 2 \nmid n,\ \left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right) \text{ and}\\ & b^2c^{n-2}=4(n-2)^{n-2}a_1\cdots a_n,\\ r+2 & \text{if } \left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right) \text{ and}\\ & b^2c^{n-2}\ne 4(n-2)^{n-2}a_1\cdots a_n,\\ 2 & \text{otherwise.}\end{cases}$$

If $2 \mid n$, $\left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right)$ *and* $b^2c^{n-2}=4(n-2)^{n-2}a_1\cdots a_n$ *then*

$$N_{p^k}(\bar{a},b,c) = (p^{n-1}+\theta p^{n/2})N_{p^{k-1}}(\bar{a},b,c) - \theta p^{(3n-2)/2}N_{p^{k-2}}(\bar{a},b,c);$$

if $2 \nmid n$, $\left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right)$ *and* $b^2c^{n-2}=4(n-2)^{n-2}a_1\cdots a_n$ *then*

$$N_{p^k}(\bar{a},b,c) = p^{n-1}N_{p^{k-1}}(\bar{a},b,c) + p^nN_{p^{k-2}}(\bar{a},b,c) - p^{2n-1}N_{p^{k-3}}(\bar{a},b,c);$$

otherwise

$$N_{p^k}(\bar{a},b,c) = p^{n-1}N_{p^{k-1}}(\bar{a},b,c).$$

Appealing to Lemmas 3.1, 3.2 and 3.3, we obtain the following results.

Theorem 3.2. *Let* n *be even and* $p \nmid b$. *If* $\left(\frac{a_1}{p}\right)=\cdots=\left(\frac{a_n}{p}\right)=\left(\frac{c(n-2)}{p}\right)$ *and* $k \le r$ *then*

$$N_{p^k}(\bar{a},b,c) = p^{(k-1)(n-1)}N_p(\bar{a},b,c) + 2^{n-1}p^{(kn-2)/2}(p-1)\cdot\frac{p^{(k-1)(n-2)/2}-\theta^{k-1}}{p^{(n-2)/2}-\theta}.$$

If $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $r > 0$ *and* $k > r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c) + 2^{n-1} p^{((2k-r)(n-1)+r)/2} \cdot \frac{p^{(r-1)(n-2)/2} - \theta^{r-1}}{p^{(n-2)/2} - \theta}$$
$$- 2^{n-1} p^{((2k-r-1)(n-1)+r-1)/2} \cdot \frac{p^{r(n-2)/2} - \theta^{r}}{p^{(n-2)/2} - \theta}.$$

In all other cases

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c).$$

Theorem 3.3. *Let* n *be odd and* $p \nmid b$*. If* $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ *and* $k \leq r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c) + 2^{n-1} p^{k(n-1)-[k/2](n-2)-1} (p-1) \cdot \frac{p^{[k/2](n-2)} - 1}{p^{n-2} - 1}.$$

If $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, r *is odd and* $k > r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c) + 2^{n-1} p^{((2k-r+1)(n-1)+r-1)/2} \cdot \frac{p^{(r-1)(n-2)/2} - 1}{p^{n-2} - 1}$$
$$- 2^{n-1} p^{((2k-r-1)(n-1)+r-1)/2} \cdot \frac{p^{(r+1)(n-2)/2} - 1}{p^{n-2} - 1}.$$

If $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $r > 0$ *is even and* $k > r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c) + 2^{n-1} p^{((2k-r)(n-1)+r-2)/2} (p-1) \cdot \frac{p^{r(n-2)/2} - 1}{p^{n-2} - 1}$$
$$+ \left(\frac{\frac{b^2 c^{n-2} - 4(n-2)^{n-2} a_1 \cdots a_n}{p^r}}{p} \right) \cdot 2^{n-1} \theta p^{((2k-r-1)(n-1)+r)/2}.$$

In all other cases

$$N_{p^k}(\bar{a}, b, c) = p^{(k-1)(n-1)} N_p(\bar{a}, b, c).$$

4. Explicit formulas for $N_{p^k}(\bar{a}, b, c)$ when $n = 3$ and when $n = 4$

In this section, we use the expressions obtained in the previous section together with the results of Carlitz [9] to determine explicitly $N_{p^k}(a)$ for $n = 3$ and for $n = 4$.

Combining (1.4) with Theorem 3.3 leads to the following.

Theorem 4.1. *Let* $n = 3$ *and* $p \nmid b$*. If* $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{c}{p}\right)$ *and* $k \leq r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{2k} + 4p^{2k-1} + p^{2k-2} - 4p^{2k-[k/2]-1}.$$

If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{c}{p}\right)$, r *is odd and* $k > r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{2k} + 4p^{2k-1} + p^{2k-2} - 4p^{2k-((r+1)/2)} - 4p^{2k-((r+3)/2)}.$$

If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{c}{p}\right)$, $r > 0$ *is even and* $k > r$ *then*

$$N_{p^k}(\bar{a}, b, c) = p^{2k} + 4p^{2k-1} + p^{2k-2}$$
$$+ \left(\left(\frac{(b^2 c - 4a_1 a_2 a_3)/p^r}{p} \right) \left(\frac{c}{p} \right) - 1 \right) \cdot 4p^{2k-((r+2)/2)}.$$

In all other cases

$$N_{p^k}(\bar{a},b,c) = p^{2k} + p^{2k-2} + \left(\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{c}{p}\right)\right)\left(\frac{b^2c - 4a_1a_2a_3}{p}\right)p^{2k-1}.$$

Similarly, by combining (1.5) and (1.6) with Theorem 3.2, we arrive at the following results.

Theorem 4.2. *Let $n = 4$ and $p \nmid b$. Assume that $p \mid (b^2c^2 - 16a_1a_2a_3a_4)$. If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{a_4}{p}\right) = \left(\frac{2c}{p}\right)$, $p \equiv 1 \pmod 4$ and $k \le r$ then*

$$N_{p^k}(\bar{a},b,c) = p^{3k} + 3p^{3k-1} - 3p^{3k-2} - p^{3k-3} - 8p^{2k-1}.$$

If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{a_4}{p}\right) = \left(\frac{2c}{p}\right)$, $p \equiv 3 \pmod 4$ and $k \le r$ then

$$N_{p^k}(\bar{a},b,c) = p^{3k} - 3p^{3k-1} + 11p^{3k-2} - p^{3k-3} + 8p^{2k-1}(p-1)\cdot\frac{p^{k-1} - (-1)^{k-1}}{p+1}.$$

If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{a_4}{p}\right) = \left(\frac{2c}{p}\right)$, $p \equiv 1 \pmod 4$ and $k > r$ then

$$N_{p^k}(\bar{a},b,c) = p^{3k} + 3p^{3k-1} - 3p^{3k-2} - p^{3k-3} - 8p^{3k-r-1} - 8p^{3k-r-2}.$$

If $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{a_4}{p}\right) = \left(\frac{2c}{p}\right)$, $p \equiv 3 \pmod 4$ and $k > r$ then

$$\begin{aligned} N_{p^k}(\bar{a},b,c) = {} & p^{3k} - 3p^{3k-1} + 11p^{3k-2} - p^{3k-3} \\ & + 8p^{3k-r}\cdot\frac{p^{r-1} - (-1)^{r-1}}{p+1} - 8p^{3k-r-2}\cdot\frac{p^r - (-1)^r}{p+1}. \end{aligned}$$

In all other cases

$$\begin{aligned} N_{p^k}(\bar{a},b,c) = {} & p^{3k} + \frac{1}{2}\left(\left(\frac{a_1a_2}{p}\right) + \left(\frac{a_1a_3}{p}\right) + \left(\frac{a_1a_4}{p}\right) + \left(\frac{a_2a_3}{p}\right)\right. \\ & \left. + \left(\frac{a_2a_4}{p}\right) + \left(\frac{a_3a_4}{p}\right)\right)\left(\frac{-1}{p}\right)p^{3k-2}(p-2) - \left(\frac{-1}{p}\right)p^{3k-2} \\ & - \left(\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right)\right)\left(\frac{-2c}{p}\right)p^{3k-2} - p^{3k-3}. \end{aligned}$$

Theorem 4.3. *Let $n = 4$ and $p \nmid b$. Assume that $p \mid (b^2c^2 - 8a_1a_2a_3a_4)$ and $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right) = 0$. Then*

$$N_{p^k}(\bar{a},b,c) = \begin{cases} p^{3k} - 2p^{3k-2} - p^{3k-3} & \text{if } p \equiv 3 \pmod 4, \\ p^{3k} + 2(A+1)p^{3k-2} - p^{3k-3} & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where the integer A is uniquely determined by (1.7).

Next we evaluate the number $N_q(\bar{a},b,c)$ of solutions to (1.1), under a certain restriction on q. If $\gcd(a_1\cdots a_nc, q) = 1$ and each prime divisor of q divides b then, by the remark following Theorem 3.1, $N_q(\bar{a},b,c) = N_q(\bar{a},0,c)$. Hence by [10, Corollary 2],

$$N_q(\bar{a},b,c) = \begin{cases} q^{n-1}\sum_{d\mid q}\left(\frac{(-1)^{n/2}a_1\cdots a_n}{d}\right)\frac{\mu(d)}{d^{n/2}} & \text{if } 2 \mid n, \\ q^{n-1}\sum_{d\mid q}\left(\frac{(-1)^{(n-1)/2}a_1\cdots a_nc}{d}\right)\frac{\mu^2(d)}{d^{(n-1)/2}} & \text{if } 2 \nmid n. \end{cases}$$

Using Theorems 4.1 – 4.3, we can easily obtain expressions for $N_q(\bar{a},b,c)$ in some other cases.

Theorem 4.4. *Let $n = 3$ and $q > 1$ be an odd integer coprime with a_1, a_2, a_3 and c. Write $q = q_1q_2q_3q_4q_5$, where q_1, q_2, q_3, q_4, q_5 are pairwise coprime positive integers satisfying the following conditions:*
(a) *each prime divisor of q_1 divides b;*
(b) *b and $q_2q_3q_4q_5$ are coprime;*
(c) *if p is a prime dividing q_2 then $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \left(\frac{c}{p}\right)$, $p^2 \mid q_2$ and $p \parallel (b^2c - 4a_1a_2a_3)$;*
(d) *$b^2c - 4a_1a_2a_3$ and $q_3q_4q_5$ are coprime;*
(e) *if p is a prime dividing $q_3q_4q_5$ then*

$$\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{c}{p}\right) = \left(\frac{b^2c - 4a_1a_2a_3}{p}\right) \cdot \begin{cases} 0 & \text{if } p \mid q_3, \\ 2 & \text{if } p \mid q_4, \\ -2 & \text{if } p \mid q_5. \end{cases}$$

Then

$$N_q(\bar{a}, b, c) = q^2 \left(\sum_{d_1 \mid q_1} \left(\frac{-a_1a_2a_3c}{d_1}\right) \frac{\mu^2(d_1)}{d_1} \right) \left(\sum_{d_2 \mid q_2} \frac{\mu(d_2) 3^{\nu(d_2)}}{d_2^2} \right) \times \left(\sum_{d_3 \mid q_3} \frac{\mu^2(d_3)}{d_3^2} \right) \left(\sum_{d_4 \mid q_4} \frac{\mu^2(d_4)}{d_4} \right)^2 \frac{\varphi^2(q_5)}{q_5^2},$$

where $\nu(d_2)$ denotes the number of distinct prime divisors of d_2. In particular, if $\gcd(b, q) = \gcd(b^2c - 4a_1a_2a_3, q) = 1$ and for each prime p dividing q we have $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{c}{p}\right) = -2 \cdot \left(\frac{b^2c - 4a_1a_2a_3}{p}\right)$ then

$$N_q(\bar{a}, b, c) = \varphi^2(q).$$

Theorem 4.5. *Let $n = 4$ and $q > 1$ be an odd integer coprime with a_1, a_2, a_3, a_4 and c. Write $q = q_1q_2q_3q_4q_5$, where q_1, q_2, q_3, q_4, q_5 are pairwise coprime positive integers satisfying the following conditions:*
(a) *each prime divisor of q_1 divides b;*
(b) *each prime divisor of q_2q_3 divides $b^2c^2 - 8a_1a_2a_3a_4$;*
(c) *each prime divisor of q_4q_5 divides $b^2c^2 - 16a_1a_2a_3a_4$;*
(d) *if p is a prime dividing $q_2q_3q_4$ then $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right) = 0$;*
(e) *if p is a prime dividing q_2 then $p - 1$ is a perfect square;*
(f) *if p is a prime dividing q_3q_5 then $p \equiv 3 \pmod 4$;*
(g) *if p is a prime dividing q_5 then $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right) = -4 \cdot \left(\frac{2c}{p}\right)$.*
Then

$$N_q(\bar{a}, b, c) = q^3 \left(\sum_{d_1 \mid q_1} \left(\frac{a_1a_2a_3a_4}{d_1}\right) \frac{\mu(d_1)}{d_1^2} \right) \left(\sum_{d_2 \mid q_2} \frac{\mu(d_2)}{d_2^3} \right) \left(\sum_{d_3 \mid q_3} \frac{\mu^2(d_3)}{d_3} \right) \times \left(\sum_{d_4 \mid q_3} \frac{\mu(d_4)\sigma(d_4)}{d_4^2} \right) \left(\sum_{d_5 \mid q_4} \left(\frac{-1}{d_5}\right) \frac{\mu(d_5)}{d_5} \right) \left(\sum_{d_6 \mid q_4} \left(\frac{-1}{d_6}\right) \frac{\mu^2(d_6)}{d_6^2} \right) \frac{\varphi^3(q_5)}{q_5^3},$$

where $\sigma(d_4)$ denotes the sum of divisors of d_4. In particular, if for each prime p dividing q we have $p \mid (b^2c^2 - 16a_1a_2a_3a_4)$, $p \equiv 3 \pmod 4$ and $\left(\frac{a_1}{p}\right) + \left(\frac{a_2}{p}\right) + \left(\frac{a_3}{p}\right) + \left(\frac{a_4}{p}\right) = -4 \cdot \left(\frac{2c}{p}\right)$ then

$$N_q(\bar{a}, b, c) = \varphi^3(q).$$

5. Poincaré Series

Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a polynomial and let c_k denote the number of solutions to the congruence $f(x_1, \dots, x_n) \equiv 0 \pmod{p^k}$. The generating function

$$P_f(t) = 1 + \sum_{k=1}^{\infty} c_k t^k$$

is said to be the Poincaré series of f. Borevich and Shafarevich [8, p. 47] raised the question of whether $P_f(t)$ is always a rational function. Igusa [19] and Denef [12] gave an affirmative answer using completely different methods. Both proofs are nonconstructive and don't show how to express $P_f(t)$ as a quotient of two polynomials.

There are, however, certain classes of polynomials for which the corresponding Poincaré series can be computed by elementary means. Goldman [13], [14] derived explicit formulas for the Poincaré series associated with strongly nondegenerate forms and with certain algebraic curves. The case of a diagonal polynomial $f(x_1, \dots, x_n) = a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} + c$, where $a_1, \dots, a_n, c \in \mathbb{Z}$, $d_1, \dots, d_n \in \mathbb{Z}^+$, was treated by Wang [23] (for $c = 0$ and $p \nmid a_1 \cdots a_n$) and Han [17] (for $p \nmid a_1 \cdots a_n d_1 \cdots d_n$), and more recently by Deb [11] (for an arbitrary diagonal polynomial). Recently [4], we calculated explicitly $P_f(t)$ for a Markoff-Hurwitz polynomial $f(x_1, \dots, x_n) = x_1^2 + \cdots + x_n^2 - bx_1 \cdots x_n$, where $b \in \mathbb{Z}$ and $n \geq 3$.

Hayes and Nutt [16] presented a further conjecture: $P_f(t)$ can be written as $P_f(t) = Q_1(t)/Q_2(t)$, where $Q_1(t)$ and $Q_2(t)$ are polynomials in $\mathbb{Z}[t]$ (possibly with common factors) and $Q_2(t)$ is a product of polynomials of the form $1 - p^m t^s$ with $m, s \in \mathbb{Z}$, $m \geq 0$, $s \geq 1$ and $m \leq ns$. They called this assertion the Q-conjecture and proved it in a number of cases. Note that the Q-conjecture holds for the special classes of polynomials mentioned above.

Now consider the case $f(x_1, \dots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2 - bx_1 \cdots x_n - c$, where $a_1, \dots, a_n, b, c \in \mathbb{Z}$, $n \geq 3$. Assume that $p > 2$ and $p \nmid a_1 \cdots a_n c$. Matching up with our previous notation, we have

$$P_f(t) = 1 + \sum_{k=1}^{\infty} N_{p^k}(\bar{a}, b, c) t^k.$$

It is well-known that a power series represents a rational function if and only if the sequence of its coefficients eventually satisfies a linear recurrence relation with constant coefficients. In this case, the denominator is completely determined by the recurrence. The coefficients of the numerator polynomial are determined by the values of the initial terms prior to the recursion. Thus, in view of Corollary 3.1, $P_f(t)$ has the form

$$P_f(t) = \frac{R(t)}{(1 - p^{n-1}t)(1 - \theta p^{n/2} t)}$$

if $2 \mid n$, $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ and $b^2 c^{n-2} = 4(n-2)^{n-2} a_1 \cdots a_n$,

$$P_f(t) = \frac{R(t)}{(1 - p^{n-1}t)(1 - p^n t^2)}$$

if $2 \nmid n$, $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ and $b^2 c^{n-2} = 4(n-2)^{n-2} a_1 \cdots a_n$, and

$$P_f(t) = \frac{R(t)}{1 - p^{n-1}t}$$

otherwise, where $R(t) \in \mathbb{Z}[t]$. We see that the Q-conjecture holds in this case. Further, for $b \equiv 0 \pmod p$, we have $N_{p^k}(\bar{a}, b, c) = N_{p^k}(\bar{a}, 0, c)$, in view of the remark following Theorem 3.1. Thus, combining the result of Han [17, Theorem 5.3] for diagonal polynomials with (1.3), we deduce that in the case $p \mid b$

$$R(t) = 1 + (N_p(\bar{a}, 0, c) - p^{n-1})t = \begin{cases} 1 - \left(\frac{(-1)^{n/2} a_1 \cdots a_n}{p}\right) p^{(n-2)/2} t & \text{if } 2 \mid n, \\ 1 + \left(\frac{(-1)^{(n-1)/2} a_1 \cdots a_n c}{p}\right) p^{(n-1)/2} t & \text{if } 2 \nmid n. \end{cases}$$

The results of Section 3 allow us to determine $R(t)$ in other cases.

Theorem 5.1. *If n is even, $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ and $b^2 c^{n-2} = 4(n-2)^{n-2} a_1 \cdots a_n$ then*

$$R(t) = \big(1 + (N_p(\bar{a}, b, c) - p^{n-1})t\big)(1 - \theta p^{n/2} t) + 2^{n-1} p^{n-1} (p-1) t^2.$$

If n is odd, $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$ and $b^2 c^{n-2} = 4(n-2)^{n-2} a_1 \cdots a_n$ then

$$R(t) = \big(1 + (N_p(\bar{a}, b, c) - p^{n-1})t\big)(1 - p^n t^2) + 2^{n-1} p^{n-1} (p-1) t^2.$$

If $\left(\frac{a_1}{p}\right) = \cdots = \left(\frac{a_n}{p}\right) = \left(\frac{c(n-2)}{p}\right)$, $b^2 c^{n-2} \neq 4(n-2)^{n-2} a_1 \cdots a_n$ and $r > 0$ then

$$\begin{aligned} R(t) =& 1 + (N_p(\bar{a}, b, c) - p^{n-1})t - (-1)^{n(r+1)} \cdot 2^{n-1} \theta^{r+1} p^{[(n(r+1)-1)/2]} t^{r+1} \\ & \times \left(\frac{(b^2 c^{n-2} - 4(n-2)^{n-2} a_1 \cdots a_n)/p^r}{p}\right)^{n(r+1)} \\ & + 2^{n-1} p^{n-1} (p-1) t^2 \cdot \begin{cases} \sum_{j=0}^{r-2} \theta^j p^{jn/2} t^j & \text{if } 2 \mid n, \\ \sum_{j=0}^{[(r-2)/2]} p^{jn} t^{2j} & \text{if } 2 \nmid n. \end{cases} \end{aligned}$$

For all other cases,

$$R(t) = 1 + (N_p(\bar{a}, b, c) - p^{n-1})t.$$

6. Further Generalizations of Markoff-Hurwitz Equations

In this section, we consider a more general congruence

$$a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} \equiv b x_1 \cdots x_n + c \pmod{p^k}, \tag{6.1}$$

where $p > 2$ is a prime, $a_1, \ldots, a_n, b, c$ are integers, $d_1, \ldots, d_n, k$ are positive integers, $p \nmid a_1 \cdots a_n c d_1 \cdots d_n$, $n \geq 2$. Assume in addition that at least one of the following conditions holds:

(a) $p \mid b$;
(b) $\gcd(d_{j_1}, d_{j_2}, p-1) \nmid (\operatorname{ind} a_{j_1} d_{j_1} - \operatorname{ind} a_{j_2} d_{j_2})$ for some $j_1, j_2 \in \{1, \ldots, n\}$;
(c) $p \mid ((D/d_1) + \cdots + (D/d_n) - D)$;
(d) $p \nmid ((D/d_1) + \cdots + (D/d_n) - D)$ and

$$\gcd(d_j, p-1) \nmid (\operatorname{ind} a_j((D/d_1) + \cdots + (D/d_n) - D) - \operatorname{ind} cD/d_j)$$

for some $j \in \{1, \ldots, n\}$;

(e)

$$b^D c^{(D/d_1)+\cdots+(D/d_n)-D}\Big(\frac{D}{d_1}\Big)^{D/d_1}\cdots\Big(\frac{D}{d_n}\Big)^{D/d_n}$$
$$\neq D^D\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)^{(D/d_1)+\cdots+(D/d_n)-D}a_1^{D/d_1}\cdots a_n^{D/d_n},$$

where $\operatorname{ind} z$ denotes the index of the integer $z\not\equiv 0 \pmod p$ with respect to a fixed primitive root modulo p and $D=\operatorname{lcm}[d_1,\ldots,d_n]$.

Throughout this section, $N_{p^k}(\bar a,b,c)$ denotes the number of solutions to (6.1) in $x_1,\ldots,x_n \pmod{p^k}$, $N^*_{p^k}(\bar a,b,c)$ denotes the number of such solutions with $p\nmid x_1\cdots x_n$, and $N^{(0)}_{p^k}(\bar a,b,c)=N_{p^k}(\bar a,b,c)-N^*_{p^k}(\bar a,b,c)$. By the same type of reasoning as in Section 3, we can obtain linear a recurrence relation for $N_{p^k}(\bar a,b,c)$ and calculate the corresponding Poincaré series.

For a fixed $k\geq 2$ and $\nu\in\{k-1,k\}$, let $\bar N^{(0)}_{p^\nu}(\bar a,b,c)$ and $\bar N^*_{p^\nu}(\bar a,b,c)$ denote the number of solutions to the system of congruences

$$\begin{aligned}&a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}\equiv bx_1\cdots x_n+c \pmod{p^\nu},\\&a_1d_1x_1^{d_1-1}\equiv bx_2x_3\cdots x_n \pmod{p^{[k/2]}},\\&a_2d_2x_2^{d_2-1}\equiv bx_1x_3\cdots x_n \pmod{p^{[k/2]}},\\&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&a_nd_nx_n^{d_n-1}\equiv bx_1x_2\cdots x_{n-1} \pmod{p^{[k/2]}},\end{aligned}\tag{6.2}$$

in $x_1,\ldots,x_n \pmod{p^\nu}$ with $p\mid x_1\cdots x_n$ and $p\nmid x_1\cdots x_n$, respectively. From Lemma 2.1 we deduce that

$$\begin{aligned}N^{(0)}_{p^k}(\bar a,b,c)-p^{n-1}N^{(0)}_{p^{k-1}}(\bar a,b,c)&=\bar N^{(0)}_{p^k}(\bar a,b,c)-p^{n-1}\bar N^{(0)}_{p^{k-1}}(\bar a,b,c),\\N^*_{p^k}(\bar a,b,c)-p^{n-1}N^*_{p^{k-1}}(\bar a,b,c)&=\bar N^*_{p^k}(\bar a,b,c)-p^{n-1}\bar N^*_{p^{k-1}}(\bar a,b,c).\end{aligned}$$

By employing the same type of argument as in the proof of Lemma 3.1, we see that $\bar N^{(0)}_{p^k}(\bar a,b,c)=\bar N^{(0)}_{p^{k-1}}(\bar a,b,c)=0$, and so $N^{(0)}_{p^k}(\bar a,b,c)=p^{n-1}N^{(0)}_{p^{k-1}}(\bar a,b,c)$ for $k\geq 2$.

Next we calculate $N^*_{p^k}(\bar a,b,c)-p^{n-1}N^*_{p^{k-1}}(\bar a,b,c)$. When $p\nmid x_1\cdots x_n$, the system of congruences (6.2) can be rewritten as

$$\begin{aligned}&a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}\equiv bx_1\cdots x_n+c \pmod{p^\nu},\\&a_1d_1x_1^{d_1}\equiv\cdots\equiv a_nd_nx_n^{d_n}\equiv bx_1\cdots x_n \pmod{p^{[k/2]}}.\end{aligned}\tag{6.3}$$

Observe that (6.3) yields the congruences

$$\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)a_jx_j^{d_j}\equiv c\cdot\frac{D}{d_j} \pmod{p^{[k/2]}},\quad 1\leq j\leq n.\tag{6.4}$$

It follows easily that if at least one of the conditions (a) – (d) holds then $\bar N^*_{p^k}(\bar a,b,c)=\bar N^*_{p^{k-1}}(\bar a,b,c)=0$, and so $N^*_{p^k}(\bar a,b,c)=p^{n-1}N^*_{p^{k-1}}(\bar a,b,c)$ for $k\geq 2$.

Now suppose that none of (a) – (d) holds. Hence the condition (e) holds. If $\bar N_{p^{k-1}}(\bar a,b,c)=0$ then we are done. Assume that $\bar N_{p^{k-1}}(\bar a,b,c)\neq 0$ and $x_1,\ldots,x_n$ are integers with $p\nmid x_1\cdots x_n$ satisfying (6.2). Then

$$(a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}-c)^D\equiv b^Dx_1^D\cdots x_n^D \pmod{p^{k-1}}.$$

Multiplying both sides by $\left(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\right)^{(D/d_1)+\cdots+(D/d_n)}a_1^{D/d_1}\cdots a_n^{D/d_n}$, we obtain

$$\begin{aligned}\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)^{(D/d_1)+\cdots+(D/d_n)-D}&a_1^{D/d_1}\cdots a_n^{D/d_n}\\ \times\Big(\sum_{j=1}^{n}\Big(\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)a_jx_j^{d_j}-c\cdot\frac{D}{d_j}\Big)+cD\Big)^{D}&\\ \equiv b^D\prod_{j=1}^{n}\Big(\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)^{D/d_j}a_j^{D/d_j}x_j^D\Big)&\pmod{p^{k-1}}.\end{aligned}$$

Further, using (6.4), we find that

$$\begin{aligned}D^D\Big(\frac{D}{d_1}+\cdots+\frac{D}{d_n}-D\Big)^{(D/d_1)+\cdots+(D/d_n)-D}&a_1^{D/d_1}\cdots a_n^{D/d_n}\\ \equiv b^Dc^{(D/d_1)+\cdots+(D/d_n)-D}\Big(\frac{D}{d_1}\Big)^{D/d_1}\cdots\Big(\frac{D}{d_n}\Big)^{D/d_n}&\pmod{p^{[k/2]}}.\end{aligned}$$

In view of the condition (e), the latter is not true if k is sufficiently large. Thus $\bar{N}^*_{p^k}(\bar{a},b,c)=\bar{N}^*_{p^{k-1}}(\bar{a},b,c)=0$ and $N^*_{p^k}(\bar{a},b,c)=p^{n-1}N^*_{p^{k-1}}(\bar{a},b,c)$ for sufficiently large k.

The results may be summarized as follows.

Theorem 6.1. *For sufficiently large k*

$$N_{p^k}(\bar{a},b,c)=p^{n-1}N_{p^{k-1}}(\bar{a},b,c).$$

In particular, if at least one of the conditions (a) – (d) *holds then the number of solutions satisfies the above recurrence relation for all $k\ge 2$.*

Taking into account the fact that $N_p(\bar{a},b,c)=p^{n-1}$ if $\gcd(d_j,p-1)=1$ for some j and $p\mid b$, we obtain

Corollary 6.1. *Let $p>2$ be a prime and*

$$f(x_1,\dots,x_n)=a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}-bx_1\cdots x_n-c,$$

where the integers $a_1,\dots,a_n,b,c,d_1,\dots,d_n$ satisfy the above conditions. Then the Poincaré series $P_f(t)$ is a rational function of the form

$$P_f(t)=\frac{R(t)}{1-p^{n-1}t},$$

where $R(t)\in\mathbb{Z}[t]$; in particular, if $\gcd(d_j,p-1)=1$ for some j and $p\mid b$ then $R(t)=1$.

Finally, we notice that the Q-conjecture of Hayes and Nutt [16] holds for this class of polynomials.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory.* Springer-Verlag, New York-Heidelberg-Berlin, 1976.

[2] I. Baoulina, *On the problem of explicit evaluation of the number of solutions of the equation $a_1x_1^2+\cdots+a_nx_n^2=bx_1\cdots x_n$ in a finite field.* In Current Trends in Number Theory, Edited by S. D. Adhikari, S. A. Katre and B. Ramakrishnan, Hindustan Book Agency, New Delhi, 2002, 27–37.

[3] I. Baoulina, *Generalizations of the Markoff-Hurwitz equations over finite fields.* J. Number Theory **118** (2006), 31–52.

[4] I. N. Baoulina, *On Markoff-Hurwitz equations over residue class rings.* Int. J. Number Theory **10** (2014), 421–454.

[5] A. Baragar, *The Markoff Equation and Equations of Hurwitz.* Ph. D. Thesis, Brown University, 1991.

[6] A. Baragar, *The Markoff-Hurwitz equations over number fields.* Rocky Mountain J. Math. **35** (2005), 695–712.

[7] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums.* Wiley-Interscience, New York, 1998.

[8] Z. I. Borevich, I. R. Shafarevich, *Number Theory.* Academic Press, New York, 1966.

[9] L. Carlitz, *Certain special equations in a finite field.* Monatsh. Math. **58** (1954), 5–12.

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

[11] D. Deb, *Diagonal forms and the rationality of the Poincaré series.* Ph. D. Thesis, University of Kentucky, 2010.

[12] J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety.* Invent. Math. **77** (1984), 1–23.

[13] J. R. Goldman, *Numbers of solutions of congruences: Poincaré series for strongly nondegenerate forms.* Proc. Amer. Math. Soc. **87** (1983), 586–590.

[14] J. R. Goldman, *Numbers of solutions of congruences: Poincaré series for algebraic curves.* Adv. in Math. **62** (1986), 68–83.

[15] S. J. Gurak, *Kloosterman sums for prime powers in P-adic fields.* J. Théor. Nombres Bordeaux **21** (2009), 175–201.

[16] D. Hayes, M. D. Nutt, *Reflective functions on p-adic fields.* Acta Arith. **XL** (1982), 229–248.

[17] Q. Han, *Numbers of solutions of congruences and rationality of generating functions.* Finite Fields Appl. **5** (1999), 266–284.

[18] A. Hurwitz, *Über eine Aufgabe der unbestimmten analysis.* Arch. Math. Phys. **3** (1907), 185–196.

[19] J. Igusa, *Complex powers and asymptotic expansions. II. Asymptotic expansions.* J. Reine Angew. Math. **278/279** (1975), 307–321.

[20] C. Jordan, *Sur les congruences du second degré.* C. R. Acad. Sci. Paris **62** (1866), 687–690.

[21] A. A. Markoff, *Sur les formes quadratiques binaires indéfinies.* Math. Ann. **17** (1880), 379–399.

[22] J. H. Silverman, *The Markoff equation $X^2 + Y^2 + Z^2 = aXYZ$ over quadratic imaginary fields.* J. Number Theory **35** (1990), 72–104.

[23] J. Wang, *On Poincaré series for diagonal forms.* Proc. Amer. Math. Soc. **116** (1992), 607–611.

Ioulia N. Baoulina, Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany

E-mail address: jbaulina@mail.ru, ioulia@mpim-bonn.mpg.de