Electronic Research Archive

https://www.aimspress.com/journal/era

ERA, 34(10): 7046–7070.
DOI: 10.3934/era.2026305
Received: 15 May 2026
Revised: 28 July 2026
Accepted: 11 August 2026
Published: 17 August 2026

Research article

Explicit formulae for inhomogeneous binary quadratic congruences modulo prime powers

Jiafan Zhang*and Ran Xiong

School of Mathematics and Statistics, Weinan Normal University, Weinan 714099, China

* **Correspondence:** Email: zjfmath@163.com.

Abstract: In this paper, we study the number of solutions to the inhomogeneous binary quadratic congruence $ax^2 + bxy + cy^2 + dx + ey \equiv n \pmod{q}$, where q is a prime power. We treat the cases where q is an odd prime power and a power of 2 separately. By combining exponential sum methods, quadratic Gauss sums, and Hensel's lemma, we obtain exact formulae for the number of unrestricted solutions over $\left(\mathbb{Z}_q\right)^2$ and the number of solutions with both variables restricted to units over $\left(\mathbb{Z}_q^*\right)^2$. This paper simultaneously handles a mixed quadratic term and two separate linear terms, extending several previously studied diagonal, homogeneous, and symmetric special cases.

Keywords: binary quadratic congruences; exponential sums; quadratic Gauss sums; prime powers; Hensel lifting

1. Introduction

Let q be a prime power. Denote by $\mathbb{Z}_q$ the ring of residue classes modulo q, and by $\mathbb{Z}_q^*$ its group of units. Let

$$f(x, y) = ax^2 + bxy + cy^2 + dx + ey \in \mathbb{Z}[x, y]$$

be a binary inhomogeneous quadratic polynomial. For an integer n, we consider the congruence

$$f(x, y) \equiv n \pmod{q}$$

and study the number of its solutions over $(\mathbb{Z}_q)^2$ and over $(\mathbb{Z}_q^*)^2$.

The study of polynomial congruences is a classical problem in number theory, and many scholars have focused on quadratic congruences under various conditions. For example, Yang and Tang [1] systematically investigated the number of solutions of

$$x^2 + y^2 \equiv n \pmod{q}$$

under unit, nonunit, and mixed restrictions on the two variables.

Subsequently, Sun and Cheng [2, 3] investigated weighted quadratic and cubic congruences under similar restrictions, while Xiong [4] studied the quadratic polynomial $g(x) = ax^2 + bx$ and obtained explicit formulae for the number of unit solutions to

$$g(x) + g(y) \equiv n \pmod{q}, \quad x, y \in \mathbb{Z}_q^*.$$

On the other hand, Liu and Ouyang [5] considered congruences of the form

$$ax^2 + bxy + cy^2 \equiv n \pmod{q},$$

thereby treating homogeneous binary quadratic forms with a mixed term. Moreover, Eum [6] studied representation numbers associated with a family of symmetric integral quadratic forms involving both diagonal and mixed terms. Their results show that once the mixed term bxy is present, the structure of the counting problem becomes more complicated than in the diagonal case.

More broadly, quadratic congruences and related exponential sums have been studied from several perspectives, including small solutions of quadratic congruences, character sums associated with binary quadratic forms, and distribution questions for solutions of quadratic congruences. These can be found in the literature [7–10].

However, to the best of our knowledge, exact formulae for the general inhomogeneous binary quadratic congruence

$$ax^2 + bxy + cy^2 + dx + ey \equiv n \pmod{q} \tag{1.1}$$

appear not to have been studied systematically in the literature, especially in the presence of unit restrictions. Compared with previous studies, the simultaneous presence of the mixed term bxy and the two linear terms dx and ey makes the associated counting problem substantially more intricate. Motivated by the works of Xiong [4] and Liu and Ouyang [5], we consider the problem of counting the solutions to (1.1). To this end, we introduce

$$N(f, n; q) := \#\{(x, y) \in (\mathbb{Z}_q)^2 : \ f(x, y) \equiv n \pmod{q}\},$$

and

$$UN(f, n; q) := \#\{(x, y) \in (\mathbb{Z}_q^*)^2 : \ f(x, y) \equiv n \pmod{q}\}.$$

Notation. To state our results, let

$$D = 4ac - b^2, \ C = n + \overline{D}(cd^2 + ae^2 - bde),$$

where $(D, q) = 1$ and $C \in \mathbb{Z}_q$. The quantity C comes from the constant term obtained after completing the square of a binary quadratic polynomial and eliminating the linear terms. $\overline{D}$ denotes the inverse of D modulo q, i.e., $D\overline{D} \equiv 1 \pmod{q}$. Throughout the paper, p is an odd prime, $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, and $\left(\frac{m}{p}\right) = 0$, if $p|m$. For $C \in \mathbb{Z}_{p^\alpha}$, we use the truncated p-adic valuation

$$v_p^{(\alpha)}(C) := \max\{0 \le j \le \alpha : C \equiv 0 \pmod{p^j}\}.$$

Thus, $v_p^{(\alpha)}(C) = \alpha$ when $C \equiv 0 \pmod{p^\alpha}$. For $C \in \mathbb{Z}_{2^\alpha}$, we use

$$v_2^{(\alpha)}(C) = \max\{0 \le j \le \alpha : C \equiv 0 \pmod{2^j}\}.$$

We simply write $v = v_p^{(\alpha)}(C)$ and $v_2 = v_2^{(\alpha)}(C)$ when no confusion can arise. As usual, $e(y) = e^{2\pi i y}$, and a prime on a summation sign indicates that the corresponding variable is restricted to residue classes coprime to the modulus. The quantity ε_{p^α} is defined by

$$\varepsilon_{p^\alpha} = \begin{cases} 1, & p^\alpha \equiv 1 \pmod 4, \\ i, & p^\alpha \equiv 3 \pmod 4. \end{cases}$$

We now state our main theorems.

Theorem 1.1. *Let $q = p^\alpha$ with $\alpha \ge 1$ be an odd prime power, and assume that $(acD, p) = 1$. Then*

$$N(f, n; p^\alpha) = p^\alpha + p^{\alpha-1}\lambda_p(f, n; \alpha),$$

where $\lambda_p(f, n; \alpha)$ is given as follows.

(i) For $\left(\frac{-D}{p}\right) = 1$, we have

$$\lambda_p(f, n; \alpha) = \begin{cases} \alpha(p-1), & v = \alpha, \\ (p-1)v - 1, & 0 \le v \le \alpha - 1. \end{cases}$$

(ii) For $\left(\frac{-D}{p}\right) = -1$, we have

$$\lambda_p(f, n; \alpha) = \begin{cases} 0, & v = \alpha \text{ and } \alpha \text{ is even}, \\ 1 - p, & v = \alpha \text{ and } \alpha \text{ is odd}, \\ 1, & 0 \le v \le \alpha - 1 \text{ and } v \text{ is even}, \\ -p, & 1 \le v \le \alpha - 1 \text{ and } v \text{ is odd}. \end{cases}$$

Theorem 1.2. *Let $q = p^\alpha$ with $\alpha \ge 1$ be an odd prime power, and assume that $(acD, p) = 1$. Then*

$$UN(f, n; p^\alpha) = \begin{cases} p^\alpha - p^{\alpha-1}\left(1 + \left(\frac{4an+d^2}{p}\right) + \left(\frac{4cn+e^2}{p}\right) - \mu_p(f, n; \alpha)\right), & p|n, \\ p^\alpha - p^{\alpha-1}\left(2 + \left(\frac{4an+d^2}{p}\right) + \left(\frac{4cn+e^2}{p}\right) - \mu_p(f, n; \alpha)\right), & p \nmid n, \end{cases}$$

where $\mu_p(f, n; \alpha)$ is given by the following two cases.

(i) If $p \nmid (2ae - bd)$ and $p \nmid (2cd - be)$, then

$$\mu_p(f, n; \alpha) = \lambda_p(f, n; \alpha),$$

where $\lambda_p(f, n; \alpha)$ is defined as in Theorem 1.1.

(ii) If $p \mid (2ae - bd)$ or $p \mid (2cd - be)$, then

$$\mu_p(f, n; \alpha) = \begin{cases} \left(\frac{-D}{p}\right)(p-1), & v \ge 1, \\ -\left(\frac{-D}{p}\right), & v = 0. \end{cases}$$

Theorem 1.3. *Let $q = 2^\alpha$ with $\alpha \geq 1$, and assume that $(acD, 2) = 1$. Then*

$$N(f, n; 2^\alpha) = 2^\alpha + 2^{\alpha-1}\left(\lambda_2(f, n; \alpha) - (-1)^{C_0}\right),$$

where $C_0 \in \{0, 1\}$ is determined by $C \equiv C_0 \pmod 2$ and

$$\lambda_2(f, n; \alpha) = \begin{cases} 0, & v_2 = 0, \text{ or } v_2 = \alpha \text{ and } \alpha \text{ is odd}, \\ 1, & v_2 = \alpha \text{ and } \alpha \text{ is even}, \\ 2, & 1 \leq v_2 \leq \alpha - 1 \text{ and } v_2 \text{ is even}, \\ -1, & 1 \leq v_2 \leq \alpha - 1 \text{ and } v_2 \text{ is odd}. \end{cases}$$

Theorem 1.4. *Let $q = 2^\alpha$ with $\alpha \geq 1$, and assume that $(acD, 2) = 1$. Then*

$$UN(f, n; 2^\alpha) = \begin{cases} N(f, n; 2^\alpha), & n \equiv d \equiv e \equiv 1 \pmod 2, \\ 2^{\alpha-1}, & n \equiv 1 + d + e \pmod 2 \text{ and } (d, e) \not\equiv (1, 1) \pmod 2, \\ 0, & \text{otherwise.} \end{cases}$$

Corollary 1.1. *Let $q = p^\alpha$ with $\alpha \geq 1$ be an odd prime power, and assume that $b = d = e = 0$, and $a = c = 1$. Then we have*

$$N(f, n; p^\alpha) = p^\alpha + p^{\alpha-1}\lambda_p(f, n; \alpha),$$

where

$$\lambda_p(f, n; \alpha) = \begin{cases} (p-1)\sum\limits_{j=1}^{\alpha}\left(\dfrac{-1}{p}\right)^j, & v = \alpha, \\ (p-1)\sum\limits_{j=1}^{v}\left(\dfrac{-1}{p}\right)^j - \left(\dfrac{-1}{p}\right)^{v+1}, & 0 \leq v < \alpha. \end{cases}$$

Moreover,

$$UN(f, n; p^\alpha) = \begin{cases} p^{\alpha-1}(p-1)\left(1 + \left(\dfrac{-1}{p}\right)\right), & v \geq 1, \\ p^{\alpha-1}\left(p - 2 - 2\left(\dfrac{n}{p}\right) - \left(\dfrac{-1}{p}\right)\right), & v = 0. \end{cases}$$

Let $c_l(n)$ be Ramanujan's sum. The above results are equivalent to the following results obtained by Yang and Tang [1]:

$$N(f, n; p^\alpha) = p^\alpha \sum_{l | p^\alpha} (-1)^{\frac{l-1}{2}} \frac{c_l(n)}{l},$$

and

$$UN(f, n; p^\alpha) = \begin{cases} p^{\alpha-1}(p-1)\left(1 + \left(\dfrac{-1}{p}\right)\right), & p | n, \\ p^{\alpha-1}\left(p - 2 - 2\left(\dfrac{n}{p}\right) - \left(\dfrac{-1}{p}\right)\right), & p \nmid n. \end{cases}$$

Thus, upon setting $b = d = e = 0$ and $a = c = 1$, Theorems 1.1 and 1.2 reduce to the corresponding odd prime-power formulas of Yang and Tang [1].

Remark 1.1. *In the present paper, we impose the condition* $(acD, p) = 1$ *in the odd-prime case and* $(acD, 2) = 1$ *in the* 2*-adic case, as required in our proofs. Consequently, our results apply only under the corresponding coprimality assumptions. Determining the number of solutions to inhomogeneous binary quadratic congruences without these restrictions is left for future investigation.*

2. Preliminaries

In this section, we state several lemmas that will be used in the proofs of the main results. The arguments involve quadratic Gauss sums, for which we refer the reader to [11] and [12].

We begin with two standard evaluations of quadratic Gauss sums.

Lemma 2.1. *(See Theorem 1.5.2 and Proposition 1.5.3 in [12].) Let* p *be an odd prime, and let* m *be an integer such that* $p \nmid m$*. Then for any positive integer* α*, we have*

$$\sum_{x=1}^{p^\alpha} e\left(\frac{mx^2}{p^\alpha}\right) = \varepsilon_{p^\alpha} p^{\frac{\alpha}{2}} \left(\frac{m}{p}\right)^\alpha.$$

Let $\alpha \geq 1$*, and let* m *be an odd integer. Then*

$$\sum_{x=1}^{2^\alpha} e\left(\frac{mx^2}{2^\alpha}\right) = \begin{cases} 0, & \alpha = 1, \\ \left(\frac{2^\alpha}{m}\right)(1 + i^m)\, 2^{\frac{\alpha}{2}}, & \alpha \geq 2, \end{cases}$$

where $\left(\frac{2^\alpha}{m}\right)$ *denotes the Kronecker symbol.*

Lemma 2.2. *Let* p *be an odd prime, and let* $\alpha \geq 1$*. Fix an integer* k' *with* $(k', p) = 1$*. Assume that* $(aD, p) = 1$*. Then*

$$\sum_{x=1}^{p^\alpha} \sum_{\substack{y=1 \\ p|y}}^{p^\alpha} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^\alpha}\right)$$

$$= \begin{cases} p^{1/2} \left(\frac{k'a}{p}\right) \varepsilon_p e\left(\frac{-k'\overline{4a}d^2}{p}\right), & \alpha = 1, \\ 0, & \alpha \geq 2,\ p \nmid (2ae - bd), \\ p^\alpha \left(\frac{-D}{p}\right)^\alpha e\left(\frac{-k'K}{p^\alpha}\right), & \alpha \geq 2,\ p \mid (2ae - bd), \end{cases}$$

and

$$\sum_{\substack{x=1 \\ p|x}}^{p^\alpha} \sum_{\substack{y=1 \\ p|y}}^{p^\alpha} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^\alpha}\right)$$

$$= \begin{cases} 1, & \alpha = 1, \\ 0, & \alpha \geq 2,\ p \nmid (2ae - bd) \text{ or } p \nmid (2cd - be), \\ p^\alpha \left(\frac{-D}{p}\right)^\alpha e\left(\frac{-k'K}{p^\alpha}\right), & \alpha \geq 2,\ p \mid (2ae - bd) \text{ and } p \mid (2cd - be), \end{cases}$$

where $K = \overline{D}\left(cd^2 + ae^2 - bde\right)$.

Proof. We first consider

$$S_1 := \sum_{x=1}^{p^\alpha} \sum_{\substack{y=1 \\ p|y}}^{p^\alpha} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^\alpha}\right).$$

If $\alpha = 1$, then $p \mid y$ forces $y \equiv 0 \pmod{p}$, and hence

$$S_1 = \sum_{x=1}^{p} e\left(\frac{k'(ax^2 + dx)}{p}\right).$$

Completing the square and applying Lemma 2.1, we obtain

$$\begin{aligned} S_1 &= \sum_{x=1}^{p} e\left(\frac{k'a\bar{4}(4x^2 + 4\bar{a}dx)}{p}\right) = \sum_{x=1}^{p} e\left(\frac{k'a\bar{4}\left((2x + \bar{a}d)^2 - \bar{a}^2d^2\right)}{p}\right) \\ &= \sum_{x=1}^{p} e\left(\frac{k'a\bar{4}x^2}{p}\right) e\left(\frac{-k'\bar{4}\bar{a}d^2}{p}\right) = p^{1/2}\left(\frac{k'a}{p}\right)\varepsilon_p e\left(\frac{-k'\overline{4a}d^2}{p}\right). \end{aligned}$$

Assume now that $\alpha \geq 2$. Since $p \nmid k'$, we detect the condition $p \mid y$ by additive characters:

$$\mathbf{1}_{p|y} = \frac{1}{p} \sum_{j=1}^{p} e\left(\frac{k'jy}{p}\right).$$

Therefore,

$$\begin{aligned} S_1 &= \frac{1}{p} \sum_{j=1}^{p} \sum_{x=1}^{p^\alpha} \sum_{y=1}^{p^\alpha} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^\alpha}\right) e\left(\frac{k'jy}{p}\right) \\ &= \frac{1}{p} \sum_{j=1}^{p} \sum_{x=1}^{p^\alpha} \sum_{y=1}^{p^\alpha} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + (e + jp^{\alpha-1})y)}{p^\alpha}\right). \end{aligned}$$

Completing the square first in x and then in y, and using Lemma 2.1 to evaluate the resulting quadratic Gauss sums, we obtain

$$\begin{aligned} S_1 &= \frac{1}{p} \sum_{j=1}^{p} \sum_{x=1}^{p^\alpha} \sum_{y=1}^{p^\alpha} e\left(\frac{k'(ax^2 + (by + d)x)}{p^\alpha}\right) e\left(\frac{k'(cy^2 + (e + jp^{\alpha-1})y)}{p^\alpha}\right) \\ &= \frac{1}{p} \sum_{j=1}^{p} \sum_{x=1}^{p^\alpha} \sum_{y=1}^{p^\alpha} e\left(\frac{\bar{4}k'ax^2}{p^\alpha}\right) e\left(\frac{-\overline{4a}k'd^2}{p^\alpha}\right) e\left(\frac{\overline{4a}k'((4ac - b^2)y^2 + 2(2a(e + jp^{\alpha-1}) - bd)y)}{p^\alpha}\right) \\ &= \frac{1}{p} \sum_{x=1}^{p^\alpha} e\left(\frac{\bar{4}k'ax^2}{p^\alpha}\right) \sum_{y=1}^{p^\alpha} e\left(\frac{\overline{4a}k'Dy^2}{p^\alpha}\right) \sum_{j=1}^{p} e\left(\frac{-k'\overline{D}(2ae - bd)j}{p}\right) e\left(\frac{-k'\overline{D}\left(cd^2 + ae^2 - bde\right)}{p^\alpha}\right) \end{aligned}$$

$$= p^{\alpha-1}\left(\frac{-D}{p}\right)^{\alpha} e\left(\frac{-k'K}{p^{\alpha}}\right)\sum_{j=1}^{p} e\left(\frac{-k'\overline{D}(2ae-bd)j}{p}\right),$$

where $K = \overline{D}\left(cd^2 + ae^2 - bde\right)$. The final sum over j vanishes unless $p \mid (2ae - bd)$, in which case it equals p. Hence,

$$S_1 = \begin{cases} 0, & p \nmid (2ae - bd), \\ p^{\alpha}\left(\frac{-D}{p}\right)^{\alpha} e\left(\frac{-k'K}{p^{\alpha}}\right), & p \mid (2ae - bd). \end{cases}$$

By interchanging x and y, we obtain the analogous formula for the sum in which $p|x$ and y is unrestricted.

Next, consider

$$S_2 := \sum_{\substack{x=1 \\ p|x}}^{p^{\alpha}} \sum_{\substack{y=1 \\ p|y}}^{p^{\alpha}} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^{\alpha}}\right).$$

If $\alpha = 1$, then both x and y are congruent to 0 modulo p, so clearly

$$S_2 = 1.$$

Assume now that $\alpha \geq 2$. Since $p \nmid k'$, detecting the conditions $p \mid x$ and $p \mid y$ by orthogonality, we get

$$\begin{aligned} S_2 &= \frac{1}{p^2}\sum_{i=1}^{p}\sum_{j=1}^{p}\sum_{x=1}^{p^{\alpha}}\sum_{y=1}^{p^{\alpha}} e\left(\frac{k'(ax^2 + bxy + cy^2 + dx + ey)}{p^{\alpha}}\right) e\left(\frac{k'ix}{p}\right) e\left(\frac{k'jy}{p}\right) \\ &= \frac{1}{p^2}\sum_{i=1}^{p}\sum_{j=1}^{p}\sum_{x=1}^{p^{\alpha}}\sum_{y=1}^{p^{\alpha}} e\left(\frac{k'(ax^2 + bxy + cy^2 + (d + ip^{\alpha-1})x + (e + jp^{\alpha-1})y)}{p^{\alpha}}\right). \end{aligned}$$

Completing the square in x and y, and then applying Lemma 2.1 as above, we obtain

$$S_2 = p^{\alpha-2}\left(\frac{-D}{p}\right)^{\alpha} e\left(\frac{-k'K}{p^{\alpha}}\right)\sum_{i=1}^{p}\sum_{j=1}^{p} e\left(\frac{-k'\overline{D}((2cd - be)i + (2ae - bd)j)}{p}\right).$$

The double character sum vanishes unless

$$p \mid (2ae - bd) \quad \text{and} \quad p \mid (2cd - be),$$

in which case it equals p^2. Therefore,

$$S_2 = \begin{cases} 0, & \alpha \geq 2,\ p \nmid (2ae - bd) \text{ or } p \nmid (2cd - be), \\ p^{\alpha}\left(\frac{-D}{p}\right)^{\alpha} e\left(\frac{-k'K}{p^{\alpha}}\right), & \alpha \geq 2,\ p \mid (2ae - bd) \text{ and } p \mid (2cd - be). \end{cases}$$

This completes the proof. □

Lemma 2.3 (Hensel's lemma)**.** *(See Theorem 3 in Chapter I, §5 of [13].) Let*

$$F(x) = c_0 + c_1 x + \cdots + c_n x^n$$

be a polynomial whose coefficients are p-adic integers. Let

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \cdots + nc_n x^{n-1}$$

be the derivative of $F(x)$. Let a_0 be a p-adic integer such that $F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p-adic integer a such that

$$F(a) = 0 \quad \textit{and} \quad a \equiv a_0 \pmod{p}.$$

3. Proofs of the main theorems

By the orthogonality of exponential sums, we obtain

$$N(f,n;q) = \frac{1}{q}\sum_{k=1}^{q}\sum_{x=1}^{q}\sum_{y=1}^{q} e\left(\frac{k(ax^2+bxy+cy^2+dx+ey-n)}{q}\right),$$

and

$$UN(f,n;q) = \frac{1}{q}\sum_{k=1}^{q}{\sum_{x=1}^{q}}'{\sum_{y=1}^{q}}' e\left(\frac{k(ax^2+bxy+cy^2+dx+ey-n)}{q}\right).$$

Proof of Theorem 1.1. Let $q = p^\alpha$ be an odd prime power, and assume that $(acD, p) = 1$. By the orthogonality of additive characters,

$$N(f,n;p^\alpha) = \frac{1}{p^\alpha}\sum_{k=1}^{p^\alpha}\sum_{x=1}^{p^\alpha}\sum_{y=1}^{p^\alpha} e\left(\frac{k(f(x,y)-n)}{p^\alpha}\right).$$

Write $(k, p^\alpha) = p^r$ and $k = p^r k'$ with $(k', p) = 1$. Then

$$N(f,n;p^\alpha) = p^\alpha + \frac{1}{p^\alpha}A, \tag{3.1}$$

where

$$A := \sum_{r=0}^{\alpha-1} p^{2r} \sum_{\substack{k'=1\\(k',p)=1}}^{p^{\alpha-r}} e\left(\frac{-k'n}{p^{\alpha-r}}\right)\sum_{x=1}^{p^{\alpha-r}}\sum_{y=1}^{p^{\alpha-r}} e\left(\frac{k'f(x,y)}{p^{\alpha-r}}\right).$$

We now evaluate A. As in the proof of Lemma 2.2, we complete the square in both variables and apply Lemma 2.1 to obtain

$$A = \sum_{r=0}^{\alpha-1} p^{2r} \sum_{\substack{k'=1\\(k',p^{\alpha-r})=1}}^{p^{\alpha-r}} e\left(\frac{-k'n}{p^{\alpha-r}}\right) e\left(\frac{-k'\left(\overline{4a(4ac-b^2)}(2ae-bd)^2+\overline{4a}d^2\right)}{p^{\alpha-r}}\right)$$

$$\cdot \sum_{x=1}^{p^{\alpha-r}} e\left(\frac{\overline{4}k'ax^2}{p^{\alpha-r}}\right)\sum_{y=1}^{p^{\alpha-r}} e\left(\frac{k'\overline{4a}(4ac-b^2)y^2}{p^{\alpha-r}}\right)$$

$$=p^{\alpha}\sum_{r=0}^{\alpha-1} p^r \varepsilon^2_{p^{\alpha-r}}\left(\frac{D}{p}\right)^{\alpha-r} \sum_{\substack{k'=1\\(k',p)=1}}^{p^{\alpha-r}} e\left(\frac{-k'C}{p^{\alpha-r}}\right),$$

where

$$D = 4ac - b^2, \quad C = n + \overline{D}(cd^2 + ae^2 - bde).$$

Let $v = v_p^{(\alpha)}(C)$. Then $0 \le v \le \alpha$. Re-indexing the sum by $m = \alpha - r$ and using the classical evaluation of the Ramanujan sum

$$c_q(n) = \sum_{\substack{k=1\\(k,q)=1}}^{q} e\left(\frac{kn}{q}\right) = \frac{\phi(q)\mu\left(\frac{q}{(n,q)}\right)}{\phi\left(\frac{q}{(n,q)}\right)},$$

we deduce

$$\begin{aligned} A &= p^{\alpha}\sum_{m=1}^{\alpha} p^{\alpha-m}\varepsilon^2_{p^m}\left(\frac{D}{p}\right)^m \sum_{\substack{k'=1\\(k',p^m)=1}}^{p^m} e\left(\frac{-k'C}{p^m}\right) \\ &= p^{2\alpha-1}\left((p-1)\sum_{m=1}^{\min(\alpha,v)} \varepsilon^2_{p^m}\left(\frac{D}{p}\right)^m - \mathbf{1}_{v+1\le\alpha}\varepsilon^2_{p^{v+1}}\left(\frac{D}{p}\right)^{v+1}\right) \\ &= \begin{cases} p^{2\alpha-1}(p-1)\sum_{m=1}^{\alpha}\left(\frac{-D}{p}\right)^m, & v = \alpha, \\ p^{2\alpha-1}\left((p-1)\sum_{m=1}^{v}\left(\frac{-D}{p}\right)^m - \left(\frac{-D}{p}\right)^{v+1}\right), & 1 \le v \le \alpha-1, \\ -p^{2\alpha-1}\left(\frac{-D}{p}\right), & v = 0. \end{cases} \end{aligned} \tag{3.2}$$

Substituting (3.2) into (3.1), we obtain

$$N(f,n;p^{\alpha}) = \begin{cases} p^{\alpha} + p^{\alpha-1}(p-1)\sum_{m=1}^{\alpha}\left(\frac{-D}{p}\right)^m, & v = \alpha, \\ p^{\alpha} + p^{\alpha-1}\left((p-1)\sum_{m=1}^{v}\left(\frac{-D}{p}\right)^m - \left(\frac{-D}{p}\right)^{v+1}\right), & 1 \le v \le \alpha-1, \\ p^{\alpha} - p^{\alpha-1}\left(\frac{-D}{p}\right), & v = 0. \end{cases}$$

It remains to simplify according to the value of the Legendre symbol $\left(\frac{-D}{p}\right)$.

Case 1. $\left(\frac{-D}{p}\right) = 1$.

Then

$$\sum_{m=1}^{t}\left(\frac{-D}{p}\right)^m = t,$$

and therefore

$$N(f,n;p^\alpha) = p^\alpha + p^{\alpha-1}\lambda_p(f,n;\alpha),$$

where

$$\lambda_p(f,n;\alpha) = \begin{cases}\alpha(p-1), & v=\alpha,\\ (p-1)v-1, & 0\le v\le \alpha-1.\end{cases}$$

Case 2. $\left(\frac{-D}{p}\right) = -1$.

In this case,

$$\sum_{m=1}^{t}\left(\frac{-D}{p}\right)^m = \sum_{m=1}^{t}(-1)^m = \begin{cases}0, & t \text{ is even},\\ -1, & t \text{ is odd}.\end{cases}$$

Hence,

$$N(f,n;p^\alpha) = p^\alpha + p^{\alpha-1}\lambda_p(f,n;\alpha),$$

where

$$\lambda_p(f,n;\alpha) = \begin{cases}0, & v=\alpha \text{ and } \alpha \text{ is even},\\ 1-p, & v=\alpha \text{ and } \alpha \text{ is odd},\\ 1, & 0\le v\le \alpha-1 \text{ and } v \text{ is even},\\ -p, & 1\le v\le \alpha-1 \text{ and } v \text{ is odd}.\end{cases}$$

This completes the proof of Theorem 1.1. □

Proof of Theorem 1.2. Let $q = p^\alpha$ be an odd prime power, and assume that $(acD, p) = 1$. By the orthogonality of additive characters,

$$UN(f,n;p^\alpha) = \frac{1}{p^\alpha}\sum_{k=1}^{p^\alpha} e\left(\frac{-kn}{p^\alpha}\right)\sideset{}{'}\sum_{x=1}^{p^\alpha}\sideset{}{'}\sum_{y=1}^{p^\alpha} e\left(\frac{kf(x,y)}{p^\alpha}\right).$$

Write $(k,p^\alpha) = p^r$ and $k = p^r k'$ with $(k',p) = 1$. Then from the inclusion–exclusion decomposition of the unit condition, we have

$$UN(f,n;p^\alpha) = \frac{\phi^2(p^\alpha)}{p^\alpha} + \frac{1}{p^\alpha}(B_1 - B_2 - B_3 + B_4), \tag{3.3}$$

where

$$B_1 = \sum_{r=0}^{\alpha-1} \sum_{\substack{k'=1 \\ (k',p)=1}}^{p^{\alpha-r}} p^{2r} e\left(\frac{-k'n}{p^{\alpha-r}}\right) \sum_{x=1}^{p^{\alpha-r}} \sum_{y=1}^{p^{\alpha-r}} e\left(\frac{k'f(x,y)}{p^{\alpha-r}}\right),$$

$$B_2 = \sum_{r=0}^{\alpha-1} \sum_{\substack{k'=1 \\ (k',p)=1}}^{p^{\alpha-r}} p^{2r} e\left(\frac{-k'n}{p^{\alpha-r}}\right) \sum_{x=1}^{p^{\alpha-r}} \sum_{\substack{y=1 \\ p|y}}^{p^{\alpha-r}} e\left(\frac{k'f(x,y)}{p^{\alpha-r}}\right),$$

$$B_3 = \sum_{r=0}^{\alpha-1} \sum_{\substack{k'=1 \\ (k',p)=1}}^{p^{\alpha-r}} p^{2r} e\left(\frac{-k'n}{p^{\alpha-r}}\right) \sum_{\substack{x=1 \\ p|x}}^{p^{\alpha-r}} \sum_{y=1}^{p^{\alpha-r}} e\left(\frac{k'f(x,y)}{p^{\alpha-r}}\right),$$

$$B_4 = \sum_{r=0}^{\alpha-1} \sum_{\substack{k'=1 \\ (k',p)=1}}^{p^{\alpha-r}} p^{2r} e\left(\frac{-k'n}{p^{\alpha-r}}\right) \sum_{\substack{x=1 \\ p|x}}^{p^{\alpha-r}} \sum_{\substack{y=1 \\ p|y}}^{p^{\alpha-r}} e\left(\frac{k'f(x,y)}{p^{\alpha-r}}\right).$$

As in the proof of Theorem 1.1, we have

$$B_1 = A,$$

where A is the quantity evaluated in (3.2).

We next evaluate B_2, B_3, and B_4 using Lemma 2.2. By the first formula in Lemma 2.2,

$$\begin{aligned}
B_2 &= \sum_{\substack{k'=1 \\ (k',p)=1}}^{p} p^{2\alpha-2} e\left(\frac{-k'n}{p}\right) p^{\frac{1}{2}} \left(\frac{k'a}{p}\right) \varepsilon_p e\left(\frac{-k'\overline{4a}d^2}{p}\right) \\
&\quad + \begin{cases} 0, & p \nmid (2ae-bd), \\ \displaystyle\sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',p^{\alpha-r})=1}}^{p^{\alpha-r}} p^{2r} p^{\alpha-r} \left(\frac{-D}{p}\right)^{\alpha-r} e\left(\frac{-k'n}{p^{\alpha-r}}\right) e\left(\frac{-k'K}{p^{\alpha-r}}\right), & p \mid (2ae-bd) \end{cases} \\
&= \sum_{\substack{k'=1 \\ (k',p)=1}}^{p} p^{2\alpha-2} e\left(\frac{-k'n}{p}\right) p^{\frac{1}{2}} \left(\frac{k'a}{p}\right) \varepsilon_p e\left(\frac{-k'\overline{4a}d^2}{p}\right) \\
&\quad + \begin{cases} 0, & p \nmid (2ae-bd), \\ \displaystyle\sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',p^{\alpha-r})=1}}^{p^{\alpha-r}} p^{2r} p^{\alpha-r} \left(\frac{-D}{p}\right)^{\alpha-r} e\left(\frac{-k'C}{p^{\alpha-r}}\right), & p \mid (2ae-bd) \end{cases} \\
&= \begin{cases} p^{2\alpha-1} \left(\dfrac{4an+d^2}{p}\right), & p \nmid (2ae-bd), \\ p^{2\alpha-1} \left(\dfrac{4an+d^2}{p}\right) + A - A_1, & p \mid (2ae-bd), \end{cases}
\end{aligned}$$

where $C = K + n$ with $K = \overline{D}\left(cd^2 + ae^2 - bde\right)$ in Lemma 2.2, and

$$A_1 := p^{2\alpha-1}\left(\frac{-D}{p}\right)\sum_{\substack{k'=1\\(k',p)=1}}^{p} e\left(\frac{-k'C}{p}\right).$$

By symmetry,

$$B_3 = \begin{cases} p^{2\alpha-1}\left(\dfrac{4cn+e^2}{p}\right), & p \nmid (2cd-be), \\ p^{2\alpha-1}\left(\dfrac{4cn+e^2}{p}\right) + A - A_1, & p \mid (2cd-be). \end{cases}$$

Similarly, by the second formula in Lemma 2.2,

$$B_4 = \begin{cases} p^{2\alpha-2}\displaystyle\sum_{\substack{k'=1\\(k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right), & p \nmid (2ae-bd) \text{ or } p \nmid (2cd-be), \\ p^{2\alpha-2}\displaystyle\sum_{\substack{k'=1\\(k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right) + A - A_1, & p \mid (2ae-bd) \text{ and } p \mid (2cd-be). \end{cases}$$

Now set

$$\delta_1 = \mathbf{1}_{p|(2ae-bd)}, \quad \delta_2 = \mathbf{1}_{p|(2cd-be)}.$$

Then the above three evaluations may be written uniformly as

$$B_2 = p^{2\alpha-1}\left(\frac{4an+d^2}{p}\right) + \delta_1(A - A_1),$$

$$B_3 = p^{2\alpha-1}\left(\frac{4cn+e^2}{p}\right) + \delta_2(A - A_1),$$

and

$$B_4 = p^{2\alpha-2}\sum_{\substack{k'=1\\(k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right) + \delta_1\delta_2(A - A_1).$$

Substituting these into (3.3), we obtain

$$UN(f,n;p^\alpha) = p^{\alpha-2}(p-1)^2 + p^{\alpha-2}\sum_{\substack{k'=1\\(k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right) - p^{\alpha-1}\left(\left(\frac{4an+d^2}{p}\right) + \left(\frac{4cn+e^2}{p}\right)\right) + \frac{1}{p^\alpha}\Omega, \quad (3.4)$$

where

$$\Omega = A - \delta_1(A - A_1) - \delta_2(A - A_1) + \delta_1\delta_2(A - A_1).$$

A simple verification shows that

$$\Omega = \begin{cases} A, & \delta_1 = \delta_2 = 0, \\ A_1, & \delta_1 = 1 \text{ or } \delta_2 = 1. \end{cases}$$

Accordingly, from A and A_1, define

$$\mu_p(f,n;\alpha) = \begin{cases} \lambda_p(f,n;\alpha), & p \nmid (2ae-bd) \text{ and } p \nmid (2cd-be), \\ \left(\dfrac{-D}{p}\right) \displaystyle\sum_{\substack{k'=1 \\ (k',p)=1}}^{p} e\left(\dfrac{-k'C}{p}\right), & p \mid (2ae-bd) \text{ or } p \mid (2cd-be), \end{cases}$$

where $\lambda_p(f,n;\alpha)$ is defined as in Theorem 1.1. Then (3.4) becomes

$$\begin{aligned} UN(f,n;p^\alpha) = {} & p^{\alpha-2}(p-1)^2 + p^{\alpha-2} \sum_{\substack{k'=1 \\ (k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right) \\ & - p^{\alpha-1}\left(\left(\frac{4an+d^2}{p}\right) + \left(\frac{4cn+e^2}{p}\right) - \mu_p(f,n;\alpha)\right). \end{aligned}$$

Finally, by the Ramanujan sum

$$\sum_{\substack{k'=1 \\ (k',p)=1}}^{p} e\left(\frac{-k'n}{p}\right) = \begin{cases} p-1, & p \mid n, \\ -1, & p \nmid n. \end{cases}$$

Therefore

$$UN(f,n;p^\alpha) = \begin{cases} p^\alpha - p^{\alpha-1}\left(1 + \left(\dfrac{4an+d^2}{p}\right) + \left(\dfrac{4cn+e^2}{p}\right) - \mu_p(f,n;\alpha)\right), & p \mid n, \\ p^\alpha - p^{\alpha-1}\left(2 + \left(\dfrac{4an+d^2}{p}\right) + \left(\dfrac{4cn+e^2}{p}\right) - \mu_p(f,n;\alpha)\right), & p \nmid n. \end{cases}$$

It remains to evaluate $\mu_p(f,n;\alpha)$. If

$$p \nmid (2ae-bd) \quad \text{and} \quad p \nmid (2cd-be),$$

then by definition

$$\mu_p(f,n;\alpha) = \lambda_p(f,n;\alpha).$$

If

$$p \mid (2ae-bd) \quad \text{or} \quad p \mid (2cd-be),$$

then using the Ramanujan sum again, we have

$$\mu_p(f,n;\alpha) = \left(\frac{-D}{p}\right) \sum_{\substack{k'=1 \\ (k',p)=1}}^{p} e\left(\frac{-k'C}{p}\right) = \begin{cases} \left(\frac{-D}{p}\right)(p-1), & v \geq 1, \\ -\left(\frac{-D}{p}\right), & v = 0. \end{cases}$$

This completes the proof of Theorem 1.2. □

Proof of Theorem 1.3. Let $q = 2^\alpha$ with $\alpha \geq 1$, and assume that $(acD, 2) = 1$. The case $\alpha = 1$ is immediate by direct counting modulo 2. Hence, we may assume $\alpha \geq 2$ below.

By the orthogonality of additive characters,

$$N(f, n; 2^\alpha) = \frac{1}{2^\alpha} \sum_{k=1}^{2^\alpha} \sum_{x=1}^{2^\alpha} \sum_{y=1}^{2^\alpha} e\left(\frac{k(f(x, y) - n)}{2^\alpha}\right).$$

Write $(k, 2^\alpha) = 2^r$ and $k = 2^r k'$ with $(k', 2) = 1$. Then

$$N(f, n; 2^\alpha) = 2^\alpha + \frac{1}{2^\alpha} \sum_{r=0}^{\alpha-1} 2^{2r} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} e\left(\frac{-k'n}{2^{\alpha-r}}\right) \sum_{x=1}^{2^{\alpha-r}} \sum_{y=1}^{2^{\alpha-r}} e\left(\frac{k' f(x, y)}{2^{\alpha-r}}\right). \tag{3.5}$$

We next eliminate the linear terms. Since $(D, 2) = 1$, the discriminant D is invertible modulo 2^m for every $m \geq 1$. Let $\overline{D}$ denote the inverse of D modulo 2^m. Consider the system

$$\begin{cases} 2ax + by + d \equiv 0 \pmod{2^m}, \\ bx + 2cy + e \equiv 0 \pmod{2^m}. \end{cases} \tag{3.6}$$

Its coefficient matrix

$$H = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$$

has determinant $D = 4ac - b^2$, which is odd, so H is invertible over $\mathbb{Z}/2^m\mathbb{Z}$. Hence (3.6) has a unique solution

$$x_0 = \overline{D}(be - 2cd), \quad y_0 = \overline{D}(bd - 2ae).$$

Setting $x = x_0 + u$ and $y = y_0 + v$, we obtain

$$f(x, y) \equiv f(x_0, y_0) + au^2 + buv + cv^2 \pmod{2^m},$$

since the linear terms in u and v vanish by construction.

Moreover, a direct computation gives

$$f(x_0, y_0) \equiv -\overline{D}(cd^2 + ae^2 - bde) \pmod{2^m}.$$

Recalling that

$$C = n + \overline{D}(cd^2 + ae^2 - bde),$$

we may rewrite (3.5) as

$$N(f, n; 2^\alpha) = 2^\alpha + \frac{1}{2^\alpha} \sum_{r=0}^{\alpha-1} 2^{2r} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} e\left(\frac{-k'C}{2^{\alpha-r}}\right) \sum_{u=1}^{2^{\alpha-r}} \sum_{v=1}^{2^{\alpha-r}} e\left(\frac{k'(au^2 + buv + cv^2)}{2^{\alpha-r}}\right).$$

We now evaluate the inner quadratic sum. Since b is odd, note that

$$\sum_{x=1}^{2^m} e\left(\frac{ax^2+bx}{2^m}\right) = \begin{cases} 2, & m=1, \\ 0, & m \geq 2. \end{cases}$$

Splitting the v-sum according to parity, and replacing b by bv in the above identity, it follows that the odd part contributes

$$\sum_{u=1}^{2^{\alpha-r}} e\left(\frac{k'(au^2+bvu)}{2^{\alpha-r}}\right) = 2$$

if and only if $\alpha - r = 1$; otherwise,

$$\sum_{u=1}^{2^{\alpha-r}} e\left(\frac{k'(au^2+bvu)}{2^{\alpha-r}}\right) = 0.$$

Thus, the odd part contributes

$$\begin{aligned} &\frac{1}{2^\alpha} 2^{2(\alpha-1)} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2} e\left(\frac{-k'C}{2}\right) \sum_{u=1}^{2} e\left(\frac{k'(au^2+bu+c)}{2}\right) \\ =&2^{\alpha-2} \cdot e\left(\frac{-C}{2}\right) \cdot 2 \cdot e\left(\frac{c}{2}\right) = -(-1)^{C_0} 2^{\alpha-1}, \end{aligned}$$

where $C_0 \in \{0,1\}$ is determined by $C \equiv C_0 \pmod 2$. For the even part, writing $v = 2y$ and completing the square in u yields

$$au^2 + buv + cv^2 = au^2 + 2buy + 4cy^2 = a\,(u + \overline{a}\,by)^2 + \overline{a}\,D\,y^2,$$

where $\overline{a}$ denotes the inverse of a modulo $2^{\alpha-r}$. Hence,

$$\begin{aligned} N(f,n;2^\alpha) =& 2^\alpha - (-1)^{C_0} 2^{\alpha-1} \\ &+ \frac{1}{2^\alpha} \sum_{r=0}^{\alpha-2} 2^{2r} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} e\left(\frac{-k'C}{2^{\alpha-r}}\right) \sum_{u=1}^{2^{\alpha-r}} e\left(\frac{k'au^2}{2^{\alpha-r}}\right) \sum_{y=1}^{2^{\alpha-r-1}} e\left(\frac{k'\overline{a}Dy^2}{2^{\alpha-r}}\right). \end{aligned}$$

Note that

$$\sum_{y=1}^{2^m} e\left(\frac{ty^2}{2^m}\right) = \sum_{y=1}^{2^{m-1}} e\left(\frac{ty^2}{2^m}\right) + \sum_{y=1}^{2^{m-1}} e\left(\frac{t(2^{m-1}+y)^2}{2^m}\right) = 2\sum_{y=1}^{2^{m-1}} e\left(\frac{ty^2}{2^m}\right) \qquad (m \geq 2).$$

Using the above formula and Lemma 2.1, we derive

$$N(f,n;2^\alpha) = 2^\alpha - (-1)^{C_0} 2^{\alpha-1} + \frac{1}{2} \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} (1+i^{k'a})(1+i^{k'\overline{a}D}) e\left(\frac{-k'C}{2^{\alpha-r}}\right). \tag{3.7}$$

Let

$$T := \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} (1+i^{k'a})(1+i^{k'\bar{a}D}) e\left(\frac{-k'C}{2^{\alpha-r}}\right).$$

Expanding the product, write

$$T = T_1 + T_2 + T_3 + T_4,$$

where

$$T_1 = \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} e\left(\frac{-k'C}{2^{\alpha-r}}\right),$$

$$T_2 = \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} i^{k'a} e\left(\frac{-k'C}{2^{\alpha-r}}\right),$$

$$T_3 = \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} i^{k'\bar{a}D} e\left(\frac{-k'C}{2^{\alpha-r}}\right),$$

$$T_4 = \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} i^{k'(a+\bar{a}D)} e\left(\frac{-k'C}{2^{\alpha-r}}\right).$$

Since $(acD, 2) = 1$ and $D = 4ac - b^2$, we have $a \equiv 1 \pmod 2$ and $b^2 \equiv 1 \pmod 4$. Therefore, we obtain

$$a + \bar{a}D \equiv a - \bar{a}b^2 \equiv a - a \equiv 0 \pmod 4.$$

Thus $T_4 = T_1$. On the other hand, from $(k'a, 2) = 1$ and

$$\bar{a}D \equiv -a \pmod 4,$$

it follows that the contributions T_2 and T_3 cancel each other, that is,

$$T_2 + T_3 = \sum_{r=0}^{\alpha-2} \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^{\alpha-r}} 2^r \left(\frac{2}{D}\right)^{\alpha-r} e\left(\frac{-k'C}{2^{\alpha-r}}\right)\left(i^{k'a} + i^{-k'a}\right) = 0,$$

where we used the fact that $i^{k'a} + i^{-k'a} = 0$ when $k'a$ is odd. Therefore,

$$T = 2T_1.$$

It remains to evaluate T_1. Writing $v_2 = v_2^{(\alpha)}(C)$ and letting $t = \alpha - r$, we obtain

$$T_1 = \sum_{t=2}^{\alpha} 2^{\alpha-t} \left(\frac{2}{D}\right)^t \sum_{\substack{k'=1 \\ (k',2)=1}}^{2^t} e\left(\frac{-k'C}{2^t}\right).$$

By the Ramanujan sum,

$$c_{2^t}(C) = \sum_{\substack{k'=1\\(k',2)=1}}^{2^t} e\left(\frac{k'C}{2^t}\right) = \begin{cases} 0, & v_2^{(t)}(C) < t-1, \\ -2^{t-1}, & v_2^{(t)}(C) = t-1, \\ 2^{t-1}, & v_2^{(t)}(C) \geq t, \end{cases}$$

and $c_{2^t}(-C) = c_{2^t}(C)$.
For $v_2 = 0$, we always have $v_2 < t-1$, hence $T_1 = 0$.
For $v_2 = \alpha$, we always have $v_2 \geq t$, hence

$$T_1 = 2^{\alpha-1} \sum_{t=2}^{\alpha} \left(\frac{2}{D}\right)^t.$$

For $1 \leq v_2 \leq \alpha - 1$, we have

$$T_1 = 2^{\alpha-1} \sum_{t=2}^{v_2} \left(\frac{2}{D}\right)^t - 2^{\alpha-1} \left(\frac{2}{D}\right)^{v_2+1} = 2^{\alpha-1} \left(\sum_{t=2}^{v_2} \left(\frac{2}{D}\right)^t - \left(\frac{2}{D}\right)^{v_2+1} \right).$$

The above three cases yield

$$T_1 = \begin{cases} 0, & v_2 = 0, \\ 2^{\alpha-1} \displaystyle\sum_{t=2}^{\alpha} \left(\frac{2}{D}\right)^t, & v_2 = \alpha, \\ 2^{\alpha-1} \left(\displaystyle\sum_{t=2}^{v_2} \left(\frac{2}{D}\right)^t - \left(\frac{2}{D}\right)^{v_2+1} \right), & 1 \leq v_2 \leq \alpha - 1. \end{cases}$$

Substituting $T = 2T_1$ into (3.7), we arrive at

$$N(f, n; 2^\alpha) = 2^\alpha - (-1)^{C_0} 2^{\alpha-1} + 2^{\alpha-1} \lambda_2(f, n; \alpha),$$

where $\lambda_2(f, n; \alpha)$ is determined by the above evaluation of T_1.

Since a, c, and D are odd, we have that b is odd and hence

$$D = 4ac - b^2 \equiv 3 \pmod 8.$$

Therefore,

$$\left(\frac{2}{D}\right) = -1.$$

It follows that

$$\lambda_2(f, n; \alpha) = \begin{cases} 0, & v_2 = 0, \text{ or } v_2 = \alpha \text{ and } \alpha \text{ is odd}, \\ 1, & v_2 = \alpha \text{ and } \alpha \text{ is even}, \\ 2, & 1 \leq v_2 \leq \alpha - 1 \text{ and } v_2 \text{ is even}, \\ -1, & 1 \leq v_2 \leq \alpha - 1 \text{ and } v_2 \text{ is odd}. \end{cases}$$

This completes the proof of Theorem 1.3. □

Proof of Theorem 1.4. Let $q = 2^\alpha$ with $\alpha \geq 1$, and assume that $(acD, 2) = 1$. Then a, c, and D are odd. Since

$$D = 4ac - b^2,$$

it follows that b is also odd.

For $(x, y) \in (\mathbb{Z}_{2^\alpha}^*)^2$, both x and y are odd, and hence

$$x^2 \equiv x \equiv 1 \pmod 2, \quad y^2 \equiv y \equiv 1 \pmod 2.$$

Reducing $f(x, y) = ax^2 + bxy + cy^2 + dx + ey$ modulo 2, we obtain

$$f(x, y) \equiv a + b + c + d + e \equiv 1 + d + e \pmod 2,$$

because $a \equiv b \equiv c \equiv 1 \pmod 2$. Therefore, a necessary condition for the congruence

$$f(x, y) \equiv n \pmod{2^\alpha}$$

to have a solution in $(\mathbb{Z}_{2^\alpha}^*)^2$ is

$$n \equiv 1 + d + e \pmod 2.$$

If this condition fails, then clearly

$$UN(f, n; 2^\alpha) = 0.$$

We now assume that

$$n \equiv 1 + d + e \pmod 2,$$

and distinguish cases according to the parity of d and e.

Case 1. $d \equiv e \equiv 1 \pmod 2$.

In this case, $n \equiv 1 \pmod 2$. Reducing $f(x, y)$ modulo 2, we have

$$f(x, y) \equiv x^2 + xy + y^2 + x + y \equiv xy \pmod 2.$$

Hence,

$$f(x, y) \equiv 1 \pmod 2 \iff xy \equiv 1 \pmod 2 \iff x \equiv y \equiv 1 \pmod 2.$$

Since every solution in $(\mathbb{Z}_{2^\alpha})^2$ is automatically a unit solution, and the reverse inclusion is obvious, the two solution sets coincide. Therefore,

$$UN(f, n; 2^\alpha) = N(f, n; 2^\alpha).$$

Case 2. $(d, e) \not\equiv (1, 1) \pmod 2$.

In this case, it suffices to show that

$$UN(f, n; 2^\alpha) = 2^{\alpha-1}.$$

We first treat the three subcases separately.

Subcase 2.1. $d \equiv e \equiv 0 \pmod 2$.

Then $n \equiv 1 \pmod 2$, and

$$f(x, y) \equiv x^2 + xy + y^2 \equiv x + xy + y \pmod 2. \tag{3.8}$$

Fix any odd $y \in \mathbb{Z}_{2^\alpha}^*$, and define

$$F(x, y) = f(x, y) - n.$$

By (3.8), modulo 2 we have

$$F(x, y) \equiv x + xy + y - 1 \pmod 2.$$

Since $y \equiv 1 \pmod 2$, this reduces to

$$F(x, y) \equiv x + x + 1 - 1 \equiv 0 \pmod 2.$$

Hence, the congruence $F(x, y) \equiv 0 \pmod 2$ has the solution

$$x \equiv 1 \pmod 2,$$

which is the unique unit class modulo 2. Moreover,

$$\frac{\partial F}{\partial x} = 2ax + by + d \equiv by \equiv 1 \pmod 2.$$

Therefore, by Hensel's lemma (See Lemma 2.3), the root $x \equiv 1 \pmod 2$ lifts uniquely to a root modulo 2^α. In particular, for each odd y, there exists a unique odd residue class $x \pmod{2^\alpha}$ such that

$$f(x, y) \equiv n \pmod{2^\alpha}.$$

Since there are exactly $2^{\alpha-1}$ odd residue classes modulo 2^α, we obtain

$$UN(f, n; 2^\alpha) = 2^{\alpha-1}.$$

Subcase 2.2. $d \equiv 0 \pmod 2$ and $e \equiv 1 \pmod 2$.

Then $n \equiv 0 \pmod 2$. For fixed odd y, again let

$$F(x, y) = f(x, y) - n.$$

Reducing modulo 2, we obtain

$$F(x, y) \equiv x^2 + xy + y^2 + y \equiv x + xy \pmod 2.$$

Since $y \equiv 1 \pmod 2$, this gives

$$F(x, y) \equiv x + x \equiv 0 \pmod 2.$$

Hence, the congruence $F(x, y) \equiv 0 \pmod 2$ again has the solution

$$x \equiv 1 \pmod 2,$$

which is the unique unit class modulo 2. Also,

$$\frac{\partial F}{\partial x} = 2ax + by + d \equiv by \equiv 1 \pmod 2.$$

By Hensel's lemma, for each odd y, there exists a unique odd lift $x \pmod{2^\alpha}$. Hence,

$$UN(f, n; 2^\alpha) = 2^{\alpha-1}.$$

Subcase 2.3. $d \equiv 1 \pmod 2$ and $e \equiv 0 \pmod 2$.

This case is symmetric to Subcase 2.2, after interchanging the roles of x and y. Therefore,

$$UN(f, n; 2^\alpha) = 2^{\alpha-1}.$$

Combining the above cases, we conclude that

$$UN(f, n; 2^\alpha) = \begin{cases} N(f, n; 2^\alpha), & n \equiv d \equiv e \equiv 1 \pmod 2, \\ 2^{\alpha-1}, & n \equiv 1 + d + e \pmod 2 \text{ and } (d, e) \not\equiv (1, 1) \pmod 2, \\ 0, & \text{otherwise.} \end{cases}$$

This completes the proof of Theorem 1.4. □

4. Examples

In this section, we illustrate Theorems 1.1–1.4 with several concrete examples in the odd prime-power case and the dyadic case. These examples illustrate that the general formulas also include special cases in which the mixed term or the linear terms vanish.

Example 4.1. *Consider*

$$f(x, y) = x^2 + y^2 + x + 2y,$$

and the congruence

$$f(x, y) \equiv 0 \pmod 5.$$

Here,

$$a = c = 1, \quad b = 0, \quad d = 1, \quad e = 2, \quad n = 0,$$

so

$$D = 4ac - b^2 = 4.$$

Hence,

$$\left(\frac{-D}{5}\right) = \left(\frac{-4}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Also,

$$C = n + \overline{D}(cd^2 + ae^2 - bde) = 0 + \overline{4}(1 + 4) = \overline{4} \cdot 5 \equiv 0 \pmod 5,$$

so $v = v_5^{(1)}(C) = 1$. *Since* $\alpha = 1$, *Theorem* 1.1 *gives*

$$\lambda_5(f, 0; 1) = 1 \cdot (5 - 1) = 4,$$

and therefore

$$N(f, 0; 5) = 5 + 4 = 9.$$

Next, we compute the number of unit solutions. We have

$$2ae - bd = 4, \quad 2cd - be = 2,$$

so $5 \nmid (2ae - bd)$ *and* $5 \nmid (2cd - be)$. *Hence, by Theorem* 1.2,

$$\mu_5(f, 0; 1) = \lambda_5(f, 0; 1) = 4.$$

Moreover,

$$\left(\frac{4an + d^2}{5}\right) = \left(\frac{1}{5}\right) = 1, \quad \left(\frac{4cn + e^2}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Since $5 \mid n$, *Theorem* 1.2 *yields*

$$UN(f, 0; 5) = 5 - (1 + 1 + 1 - 4) = 6.$$

Thus,

$$N(f, 0; 5) = 9, \quad UN(f, 0; 5) = 6.$$

In fact, a direct enumeration shows that the nine solutions modulo 5 *are*

$$(0, 0), (0, 3), (1, 1), (1, 2), (2, 4), (3, 1), (3, 2), (4, 0), (4, 3),$$

among which the six unit solutions are

$$(1, 1), (1, 2), (2, 4), (3, 1), (3, 2), (4, 3).$$

Example 4.2. *Consider*

$$f(x, y) = x^2 + xy + y^2,$$

and the congruence

$$f(x, y) \equiv 1 \pmod 8.$$

Here,

$$a = b = c = 1, \quad d = e = 0, \quad n = 1,$$

so

$$D = 4ac - b^2 = 3,$$

and indeed

$$(acD, 2) = 1.$$

Since $d = e = 0$, we have

$$C = n + \overline{D}(cd^2 + ae^2 - bde) = 1.$$

Thus,

$$v_2 = v_2^{(3)}(C) = 0, \quad C_0 \equiv 1 \pmod 2.$$

By Theorem 1.3*,*

$$\lambda_2(f, 1; 3) = 0,$$

and hence

$$N(f, 1; 8) = 2^3 + 2^2(0 - (-1)^1) = 8 + 4 = 12.$$

For the unit-restricted count, we have

$$n \equiv 1 + d + e \pmod 2,$$

and

$$(d, e) \equiv (0, 0) \not\equiv (1, 1) \pmod 2.$$

Therefore, by Theorem 1.4*,*

$$UN(f, 1; 8) = 2^{3-1} = 4.$$

Consequently,

$$N(f, 1; 8) = 12, \qquad UN(f, 1; 8) = 4.$$

A direct computation confirms these values.

Example 4.3. *Consider*

$$f(x, y) = x^2 + y^2,$$

and the congruence

$$f(x, y) \equiv 5 \pmod 9.$$

Here, $p = 3, \alpha = 2$, *and* $a = c = 1, b = d = e = 0, n = 5$, *so* $D = 4ac - b^2 = 4$. *Hence,*

$$\left(\frac{-D}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Moreover,

$$C = n + \overline{D}(cd^2 + ae^2 - bde) = 5,$$

so $v = 0$. *From Theorem* 1.1 *we have*

$$\lambda_3(f, 5; 2) = 1.$$

Therefore,

$$N(f, 5; 9) = 3^2 + 3^{2-1}\lambda_3(f, 5; 2) = 9 + 3 \cdot 1 = 12.$$

Next, we compute the number of unit solutions. We have $2ae - bd = 0$ *and* $2cd - be = 0$. *Thus, by Theorem* 1.2 *we have*

$$\mu_3(f, 5; 2) = 1.$$

Furthermore,

$$\left(\frac{4an + d^2}{3}\right) = \left(\frac{2}{3}\right) = -1, \qquad \left(\frac{4cn + e^2}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Therefore,

$$UN(f, 5; 9) = 9 - 3\,(2 - 1 - 1 - 1) = 12.$$

Thus

$$N(f, 5; 9) = 12, \qquad UN(f, 5; 9) = 12.$$

In fact, a direct enumeration shows that the twelve solutions modulo 9 *are*

$$(1, 2), (1, 7), (2, 1), (2, 8), (4, 4), (4, 5), (5, 4), (5, 5), (7, 1), (7, 8), (8, 2), (8, 7).$$

Since none of the coordinates of these solutions is divisible by 3, *all twelve solutions are unit solutions.*

This example is a specialization of Corollary 1.1, *and the same result can also be derived from Theorem 1.3 of Yang and Tang [1].*

5. Conclusions

In this paper, we obtained explicit formulae for the number of solutions to the inhomogeneous binary quadratic congruence

$$ax^2 + bxy + cy^2 + dx + ey \equiv n \pmod{q},$$

where q is prime powers. Under the assumptions $(acD, p) = 1$ for odd prime powers and $(acD, 2) = 1$ for powers of 2, we derived exact evaluations for the unrestricted counting function $N(f, n; q)$ and the unit-restricted counting function $UN(f, n; q)$, by means of exponential sums, quadratic Gauss sums, and Hensel's lemma. These results unify and extend several earlier counting formulae for diagonal, homogeneous, and special inhomogeneous quadratic congruences modulo prime powers. It would be of interest to investigate whether the present method can be extended to more general quadratic polynomials in several variables or to congruences with additional arithmetic restrictions.

Use of AI tools declaration

During the preparation of this manuscript, the authors used Deepseek (deepseek.com) for language editing and grammar correction. The authors have reviewed and revised all outputs from this tool.

Acknowledgments

We thank the reviewers for their valuable comments.

This study was funded by the Natural Science Basic Research Program of Shaanxi Province (Grant No.2025JC-YBQN-091 and No.2025JC-YBQN-083), the Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No.25JSQ054), the Talent Research Program Initiative 2025 of Weinan Normal University (Grant No.2025RC16), and the Youth Talent Support Program Project of WNU (Grant No.2025XJ-QNRC-02).

Conflict of interest

The authors declare there are no conflicts of interest.

References

1. Q. H. Yang, M. Tang, On the addition of squares of units and nonunits modulo n, *J. Number Theory*, **155** (2015), 1–12. https://doi.org/10.1016/j.jnt.2015.02.019
2. C. F. Sun, Z. Cheng, On the addition of two weighted squares of units mod n, *Int. J. Number Theory*, **12** (2016), 1783–1790. https://doi.org/10.1142/S1793042116501098
3. C. F. Sun, Z. Cheng, On the addition of two cubes of units and nonunits mod p^α, *J. Math. Res. Appl.*, **37** (2017), 274–280. https://doi.org/10.3770/j.issn:2095-2651.2017.03.004
4. R. Xiong, On the addition of values of a quadratic polynomial at units modulo n, *Acta Math. Hung.*, **163** (2021), 62–70. https://doi.org/10.1007/s10474-020-01067-w

5. Y. Liu, Y. Ouyang, On binary quadratic forms modulo n, *Commun. Math. Stat.*, **7** (2019), 61–67. https://doi.org/10.1007/s40304-018-0141-1
6. I. S. Eum, On some representation numbers by $a\sum x_i^2 + b\sum x_i x_j$ representing one, *Indian J. Pure Appl. Math.*, **57** (2026), 321–337. https://doi.org/10.1007/s13226-024-00533-3
7. N. Bag, S. Baier, A. Haldar, Multiple exponential sums and their applications to quadratic congruences, *Math. Nachr.*, **298** (2025), 3599–3612. https://doi.org/10.1002/mana.70063
8. S. Baier, A. Haldar, Asymptotic behavior of small solutions of quadratic congruences in three variables modulo prime powers, *Res. Number Theory*, **8** (2022), 58. https://doi.org/10.1007/s40993-022-00360-7
9. D. R. Heath-Brown, Small solutions of quadratic congruences, and character sums with binary quadratic forms, *Mathematika*, **62** (2016), 551–571. https://doi.org/10.1112/S0025579315000364
10. A. Haldar, Equidistribution of solutions of ternary quadratic congruences modulo prime powers, *Res. Number Theory*, **10** (2024), 47. https://doi.org/10.1007/s40993-024-00535-4
11. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976. https://doi.org/10.1007/978-1-4757-5579-4
12. B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, New York, 1998.
13. N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2^{nd} edition, Springer, New York, 1984. https://doi.org/10.1007/978-1-4612-1112-9

AIMS Press