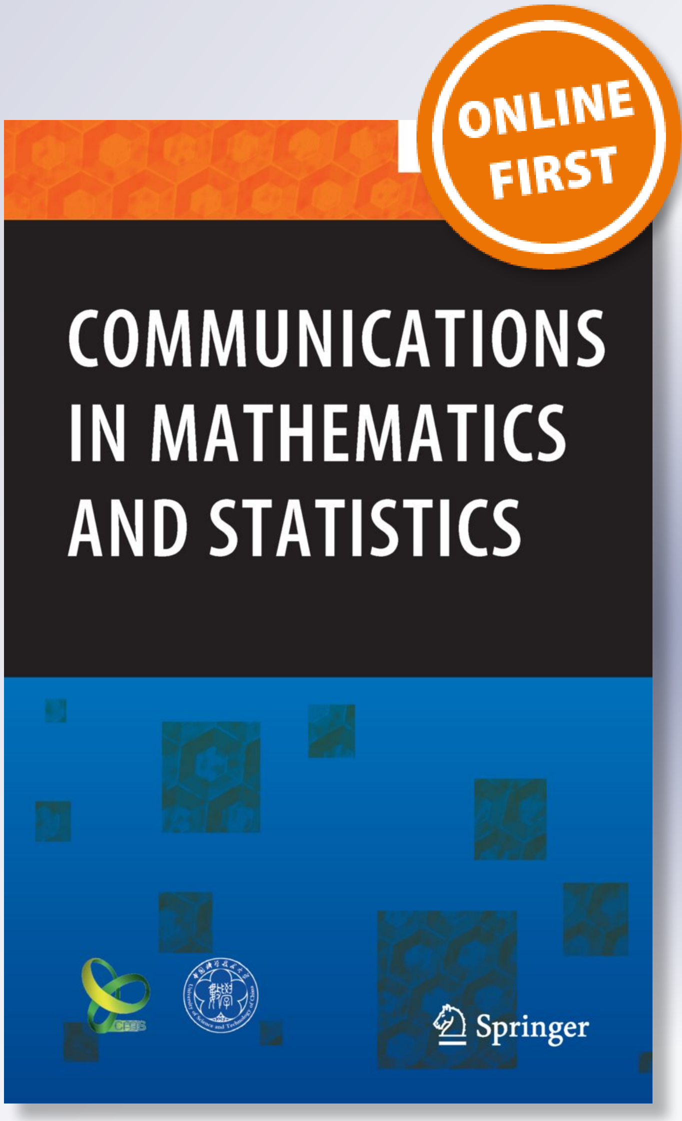
On Binary Quadratic Forms Modulo n

Yang Liu & Yi Ouyang

Communications in Mathematics and Statistics

ISSN 2194-6701

Commun. Math. Stat.
DOI 10.1007/s40304-018-0141-1



Springer

Commun. Math. Stat.
https://doi.org/10.1007/s40304-018-0141-1

On Binary Quadratic Forms Modulo n

Yang Liu[1] · **Yi Ouyang**[1]

Received: 9 January 2018 / Revised: 10 May 2018 / Accepted: 31 May 2018

Abstract Given a binary quadratic polynomial $f(x_1, x_2) = \alpha x_1^2 + \beta x_1 x_2 + \gamma x_2^2 \in \mathbb{Z}[x_1, x_2]$, for every $c \in \mathbb{Z}$ and $n \geq 2$, we study the number of solutions $\mathrm{N}_J(f; c, n)$ of the congruence equation $f(x_1, x_2) \equiv c \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^2$ such that $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ for $i \in J \subseteq \{1, 2\}$.

Keywords Binary quadratic form · Counting solutions · Congruence equation modulo n

Mathematics Subject Classification 11B13, 11L03, 11L05

1 Introduction and Main Result

For an integral polynomial $f(x_1, \ldots, x_t)$ of t variables, following the notations in [1], let $\Gamma_J(f; c, n)$ (or $\Gamma(c, n)$ if f is clear from context) be the set of solutions of $f(x_1, \ldots, x_t) \equiv c \bmod n$ such that $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ for $i \in J \subseteq \{1, \ldots, t\}$ and $N_J(f; c, n)$ be the cardinality of $\Gamma_J(f; c, n)$. When $t = 2$, for simplicity, we write $x = x_1$ and $y = x_2$, and write N, N_1, N_2 and N^* for $N_\emptyset$, $N_{\{1\}}$, $N_{\{2\}}$ and $N_{\{1,2\}}$.

The problem to determine $N_J(f; c, n)$ when f is a diagonal polynomial has drawn extensive studies by many authors recently. Yang and Tang [5] determined $N_J(x^2 + y^2; c, n)$ in 2015, and Sun and Cheng [3] determined $N^*(\alpha x^2 + \gamma y^2; c, n)$ in 2016.

✉ Yang Liu
ooxox@mail.ustc.edu.cn

Yi Ouyang
yiouyang@ustc.edu.cn

1 Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, Anhui, China

Published online: 20 July 2018

Mollahajiaghaei [2] determined $N^*(x_1^2+\cdots+x_t^2; c, n)$. Li and Ouyang [1] completely solved the counting problem of $N_J(f; c, n)$ when f is a diagonal binary quadratic form. Their results can be found in Theorem 4.4, Proposition 4.7 and the remark after the proposition in [1]. Certainly, the results in [1] are far more beyond. They actually determined the values of $N^*(f; c, n)$ for any diagonal quadratic forms of any variables and gave methods to determine essentially $N_J(f; c, n)$ for f of the form $\lambda_1 x_1^{k_1} + \cdots + \lambda_t x_t^{k_t}$. See Toth [4] for more development.

In this note, we shall consider the case that $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ is a non-diagonal binary quadratic form, i.e., $\beta \neq 0$. Our main result is

Theorem 1.1 *For an arbitrary non-diagonal binary quadratic form $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2 \in \mathbb{Z}[x, y]$, for any given J, c and n, $N_J(f; c, n)$ can be determined explicitly as given in Propositions 4.1–4.6.*

2 Basic Reduction

First, by the Chinese Remainder Theorem, suppose n has the prime decomposition $n = \prod_{p|n} p^{n_p}$, then

$$N_J(f; c, n) = \prod_{p|n} N_J(f; c, p^{n_p}). \tag{2.1}$$

Hence we only need to compute $N_J(f; c, p^a)$ for any prime number p and any integer $a \geq 1$. From now on, we let $v_p(x)$ be the p-adic valuation of x. In particular, for $0 \neq c \in \mathbb{Z}/p^a\mathbb{Z}$, $c_p = v_p(c) < a$ is well defined.

Fix p. Write $\alpha = p^{e_1}\alpha'$, $\beta = p^{e_2}\beta'$ and $\gamma = p^{e_3}\gamma'$ with $e_1, e_2, e_3 \geq 0$ and $p \nmid \alpha'\beta'\gamma'$. Then to compute $N_J(f; c, p^a)$,

- we may assume $\min\{e_1, e_2, e_3\} = 0$ by [1, Proposition 2.1(2)];
- we may assume $e_1 \leq e_3$ by symmetry;
- the map $\Gamma_J(f; c, p^a) \to \Gamma_J(p^{e_1}x^2 + p^{e_2}xy + p^{e_3}\alpha'\gamma'\beta'^{-2}y^2; \alpha'c, p^a)$, $(x, y) \mapsto (\alpha'x, \beta'y)$ is a bijection, so we may assume $\alpha' = \beta' = 1$.

From now on, if not stated otherwise, we assume

$$f(x, y) = p^{e_1}x^2 + p^{e_2}xy + p^{e_3}\lambda y^2 \tag{2.2}$$

satisfying the conditions

$$e_1 \leq e_3, \ \min\{e_1, e_2\} = 0, \ p \nmid \lambda, \text{ and } c \in \mathbb{Z}/p^a\mathbb{Z}. \tag{2.3}$$

3 Two Useful Lemmas

Lemma 3.1 *For $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$, one has*

$$N^*(c, p^a) = (N_1 + N_2 - N)(c, p^a) + \overline{N}, \tag{3.1}$$

where $\overline{N}$ *is* $p^2N(\frac{c}{p^2}, p^{a-2})$ *if* $a > 2$ *and* $c_p \geq 2$, *is* $p^{2(a-1)}$ *if* $a \leq 2$ *and* $c = 0$, *and is* 0 *in other occasions.*

Proof We see that $\Gamma_1 \cap \Gamma_2 = \Gamma^*$, and the complement of $\Gamma_1 \cup \Gamma_2$ in Γ is the set $\{(px, py) \in (\mathbb{Z}/p^a)^2 \mid f(px, py) \equiv c \bmod p^a\}$. Thus (3.1) follows from the Inclusion-Exclusion Principle immediately. □

Lemma 3.2 *Suppose* $f'(x, y) = x^2 + (2^e\lambda - 1)y^2$ *with* $e > 0$ *and* $2 \nmid \lambda$.

(1) *For c odd,*

$$N(f'; c, 2^a) = \begin{cases} 2^a, & \text{if } a = 1 \text{ or } e \geq 2; \\ 2^{a+1}, & \text{if } e = 1,\ a \geq 2 \text{ and } c \equiv 1 \bmod 4; \\ 0, & \text{if } e = 1,\ a \geq 2 \text{ and } c \equiv 3 \bmod 4. \end{cases} \tag{3.2}$$

(2) *For general c,*

$$N_2(f'; c, 2^a) = \begin{cases} 2^a, & \text{if } a \geq 2,\ c \equiv 2^e\lambda - 1 \bmod 4; \\ 2^{a+1}, & \text{if } a \geq 3,\ c \equiv 2^e\lambda \bmod 8; \\ 4, & \text{if } a = 2,\ c \equiv 2^e\lambda \bmod 4; \\ 1, & \text{if } a = 1; \\ 0, & \text{if otherwise}. \end{cases} \tag{3.3}$$

Proof By [1, Theorem C], we have $N(f'; c, 2^a) = 2^{a-3}N(f'; c, 8)$ for $a \geq 3$ if $2 \nmid c$. By [1, Theorem B], we have $N_2(f'; c, 2^a) = 2^{a-3}N_2(f'; c, 8)$ for $a \geq 3$. Now we just have to manually compute $N(f'; c, 2^a)$ and $N(f'; c, 2^a)$ for $a \leq 3$. □

4 Case by Case Study

We shall discuss the counting problem in six cases.

Proposition 4.1 *If* $e_1 > 0$ *and hence* $f(x, y) = p^{e_1}x^2 + xy + p^{e_3}\lambda y^2$, *then*

$$N(f; c, p^a) = \begin{cases} p^{a-1}(p-1)(c_p+1), & \text{if } c \neq 0; \\ p^{a-1}(pa + p - a), & \text{if } c = 0, \end{cases} \tag{4.1}$$

$$N_1(f; c, p^a) = N_2(f; c, p^a) = p^{a-1}(p-1), \tag{4.2}$$

$$N^*(f; c, p^a) = \begin{cases} p^{a-1}(p-1), & \text{if } p \nmid c; \\ 0, & \text{if } p \mid c. \end{cases} \tag{4.3}$$

Proof Define d_n recursively by $d_0 = 1$ and $d_{n+1} = 1 + p^{e_1+e_3}\lambda d_n^2$. Since $d_{n+2} - d_{n+1} = p^{e_1+e_3}\lambda(d_{n+1} + d_n)(d_{n+1} - d_n)$, the sequence $\{d_n\}$ is a Cauchy sequence and converges to a p-adic unit $d \in \mathbb{Z}_p$. Note that $d = 1 + p^{e_1+e_3}\lambda d^2$, then $p^{e_1}x^2 + xy + p^{e_3}\lambda y^2 \equiv c \bmod p^a$ if and only if $d(p^{e_1}x^2 + xy + p^{e_3}\lambda y^2) = (x + dp^{e_3}\lambda y)(dp^{e_1}x + y) \equiv dc \bmod p^a$ for any e_1 and e_3.

Let $(u, v) = (x + dp^{e_3}\lambda y, dp^{e_1}x + y)$. Then $(x, y) = (u - dp^{e_3}\lambda v)/(1 - p^{e_1+e_3}\lambda d^2), (v - dp^{e_1}u)/(1 - p^{e_1+e_3}\lambda d^2)$. If $e_1 > 0$, then $x \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ (resp. $y \in (\mathbb{Z}/p^a\mathbb{Z})^\times$) if and only if $u \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ (resp. $v \in (\mathbb{Z}/p^a\mathbb{Z})^\times$), we have a well-defined bijective map $\varphi : \Gamma_J(f; c, p^a) \to \Gamma_J(uv; dc, p^a)$, $(x, y) \mapsto (u, v)$ for any J. Now it is not difficult to prove the following formulas:

$$N(uv; dc, p^a) = \begin{cases} p^{a-1}(p-1)(c_p+1), & \text{if } c \neq 0; \\ p^{a-1}(pa+p-a), & \text{if } c = 0, \end{cases}$$
$$N_1(uv; dc, p^a) = N_2(uv; dc, p^a) = p^{a-1}(p-1),$$
$$N^*(uv; dc, p^a) = \begin{cases} p^{a-1}(p-1), & \text{if } p \nmid c; \\ 0, & \text{if } p \mid c. \end{cases}$$

□

Remark We only need $e_3 > 0$ to get the equivalence of x and $u \in (\mathbb{Z}/p^a\mathbb{Z})^\times$, thus for $J = \emptyset$ or $\{1\}$, $N_J(f; c, p^a) = N_J(uv; c, p^a)$ if $e_3 > 0$ (even if $e_1 = 0$).

Proposition 4.2 *If $e_2 > v_p(2)$ and hence $f(x, y) = x^2 + p^{e_2}xy + p^{e_3}\lambda y^2$, let $\lambda' = p^{e_3}\lambda - \frac{p^{2e_2}}{4}$ and $f'(x, y) = x^2 + \lambda' y^2$, then*

$$N_J(f; c, p^a) = N_J(f'; c, p^a). \tag{4.4}$$

Proof This is because the map $\psi : \Gamma_J(f; c, p^a) \to \Gamma_J(f'; c, p^a)$ which sends (x, y) to $(x + \frac{p^{e_2}}{2}y, y)$ is a bijection. □

Remark For $J = \{1\}$ or $\{1, 2\}$, the value $N_J(f'; c, p^a) = p^{a-1}N_J(f'; c, p)$ is given by a simple explicit formula in [1, Theorem 4.4]. For $J = \emptyset$ or $\{2\}$, one can find the (more complicated) explicit formulas in [1, Proposition 4.7].

Proposition 4.3 *Suppose p is odd, $e_1 = e_2 = 0$, i.e., $f(x, y) = x^2 + xy + p^{e_3}\lambda y^2$.*

(1) *If $e_3 = 0$, let $f'(x, y) = x^2 + (4\lambda - 1)y^2$, then*

$$\begin{aligned} N(c, p^a) = N(f'; c, p^a),\ N_1(c, p^a) \\ = N_2(f'; \lambda c, p^a),\ N_2(c, p^a) = N_2(f'; c, p^a). \end{aligned} \tag{4.5}$$

(2) *If $e_3 > 0$, then*

$$N(c, p^a) = \begin{cases} p^{a-1}(p-1)(c_p+1), & \text{if } c \neq 0; \\ p^{a-1}(pa+p-a), & \text{if } c = 0, \end{cases} \tag{4.6}$$

$$N_1(c, p^a) = p^{a-1}(p-1), \tag{4.7}$$

$$N_2(c, p^a) = \begin{cases} p^{a-1}\left(p-2-\left(\frac{c}{p}\right)\right), & \text{if } p \nmid c; \\ 2p^{a-1}(p-1), & \text{if } p \mid c. \end{cases} \tag{4.8}$$

(3) *In both cases,* $N^*(c, p^a)$ *is obtained by the values* N_1, N_2 *and* N *through the relation* (3.1).

Proof If $J = \emptyset$ or $\{2\}$, the map $\Gamma_J(f; c, p^a) \to \Gamma_J(x^2 + (4p^{e_3}\lambda - 1)y^2; c, p^a)$, $(x, y) \mapsto (x + \frac{y}{2}, \frac{y}{2})$ is a bijection. If $e_3 = 0$, the map $\Gamma_1(c, p^a) \to \Gamma_2(\lambda c, p^a)$, $(x, y) \mapsto (\lambda y, x)$ is also a bijection. We get (4.5).

If $e_3 > 0$, then $N_2(c, p^a) = p^{a-1} N_2(x^2 - y^2; c, p)$ by [1, Theorem B] and (4.8) is easily obtained. The formulas for $N(c, p^a)$ and $N_1(c, p^a)$ follow from the remark after Proposition 4. □

Remark The values of $N(f'; c, p^a)$ and $N_2(f'; c, p^a)$ (and $N_2(f'; \lambda c, p^a)$) in (4.5) are given explicitly in [1, Proposition 4.7].

Proposition 4.4 *Suppose* $p = 2$, $(e_1, e_2) = (0, 1)$, *i.e.,* $f(x, y) = x^2 + 2xy + 2^{e_3}\lambda y^2$. *Set* $f'(x, y) = x^2 + (2^{e_3}\lambda - 1)y^2$.

(1) *If* $e_3 = 0$, *then*

$$\begin{aligned} N(c, 2^a) &= N(f'; c, 2^a), \ N_1(c, 2^a) \\ &= N_2(f'; \lambda c, 2^a), \ N_2(c, 2^a) = N_2(f'; c, 2^a). \end{aligned} \tag{4.9}$$

(2) *If* $e_3 > 0$, *then* $N(c, 2^a) = N(f'; c, 2^a)$; $N_1(c, 2^a) = 0$ *if* c *is even and* $N_1(c, 2^a) = N(f'; c, 2^a)$ *which is given by* (3.2) *in Lemma* 3.2(1) *if* c *is odd;* $N_2(c, 2^a) = N_2(f'; c, 2^a)$ *which is given by* (3.3) *in Lemma* 3.2(2).

(3) *In both cases,* N^* *is obtained by the values* N_1, N_2 *and* N *through the relation* (3.1).

Proof If $J = \emptyset$ or $\{2\}$, the map $\Gamma_J(f; c, 2^a) \to \Gamma_J(x^2 + (2^{e_3}\lambda - 1)y^2; c, 2^a)$, $(x, y) \mapsto (x + y, y)$ is a bijection. In particular, if $e_3 > 0$, $N_2(c, 2^a) = N_2(f'; c, 2^a)$ is given by Lemma 3.2(2).

For N_1, if $e_3 = 0$, the map $\Gamma_1(c, 2^a) \to \Gamma_2(\lambda c, 2^a)$, $(x, y) \mapsto (\lambda y, x)$ is a bijection; if $e_3 > 0$, then x is odd if and only if $x^2 + 2xy + 2^{e_3}\lambda y^2$ is odd, which means $N_1(c, 2^a) = N(c, 2^a) = N(f'; c, 2^a)$ which is given by Lemma 3.2(1) if c is odd or 0 if c is even. □

Remark The remaining values of $N(f'; c, 2^a)$ and $N_2(f'; c, 2^a)$ in Proposition 4.4 are given in the remark after [1, Proposition 4.7].

Proposition 4.5 *Suppose* $p = 2$ *and* $e_1 = e_2 = e_3 = 0$, *i.e.,* $f(x, y) = x^2 + xy + \lambda y^2$.

(1) *If* c *is odd, then*

$$N^*(c, 2^a) = 2^{a-1}, \ N_1(c, 2^a) = N_2(c, 2^a) = 2^a, \ N(c, 2^a) = 3 \cdot 2^{a-1}. \tag{4.10}$$

(2) *If* c *is even, then*

$$N^*(c, 2^a) = N_1(c, 2^a) = N_2(c, 2^a) = 0, \tag{4.11}$$

$$N(c, 2^a) = \begin{cases} 3 \cdot 2^{a-1}, & \text{if } c \neq 0 \text{ and } 2 \mid c_2; \\ 0, & \text{if } c \neq 0 \text{ and } 2 \nmid c_2; \\ 4^{\lfloor \frac{a}{2} \rfloor}, & \text{if } c = 0. \end{cases} \tag{4.12}$$

Proof (1) Suppose c is odd. Let $f'(x, y) = x^2 + (4\lambda - 1)y^2$, then $N(f'; c, 2^a) = 2^a$ by Lemma 3.2(1). Note that any element $(u, v) \in \Gamma(f'(u, v); \lambda c, 2^a)$ satisfies $u - v$ odd, thus

$$x = \frac{u-v}{\lambda} + 2v, \ \ y = 2v - x = \frac{v-u}{\lambda}$$

are both odd. We have a map from $\Gamma(f'(u, v); \lambda c, 2^a)$ to $\Gamma^*(c, 2^a)$ by sending (u, v) to (x, y). This map is surjective and 2-to-1: only $(w-\lambda y, w)$ with w satisfying $2w = x + y \bmod 2^a$ maps to (x, y). In this way, we have $N^*(c, 2^a) = \frac{1}{2}N(f'; \lambda c, 2^a) = 2^{a-1}$.

We know $\Gamma_1(c, 2^a)$ is a disjoint union of $\Gamma^*(c, 2^a)$ and the set $\{(x, 2y) \mid x \text{ odd}, \ f(x, 2y) \equiv c \bmod 2^a\}$. The latter is 1-to-2 correspondent to $\Gamma_1(x^2 + 2xy + 4\lambda y^2; c, 2^a)$, and $\Gamma_1(x^2+2xy+4\lambda y^2; c, 2^a) = \Gamma(x^2+2xy+4\lambda y^2; c, 2^a)$ if c is odd. Now $\Gamma(x^2 + 2xy + 4\lambda y^2; c, 2^a) \to \Gamma(f'; c, 2^a)$, $(x, y) \mapsto (x + y, y)$ is bijective, so the result for Γ_1 follows.

For Γ_2, the map $\Gamma_2(c, 2^a) \to \Gamma_1(\lambda c, 2^a)$, $(x, y) \mapsto (\lambda y, x)$ is a bijection. For $N(c, 2^a)$, we just use (3.1).

(2) If c is even, since $x^2 + xy + \lambda y^2$ is odd if one of x or y is odd, hence $N_1 = N_2 = N^* = 0$. Then N follows from (3.1). □

Proposition 4.6 *If* $p = 2$, $e_1 = e_2 = 0$ *and* $e_3 > 0$, *i.e.*, $f(x, y) = x^2 + xy + 2^{e_3}\lambda y^2$, *then*

$$N(c, 2^a) = \begin{cases} 2^{a-1}(c_2 + 1), & \textit{if } c \neq 0; \\ 2^{a-1}(a + 2), & \textit{if } c = 0, \end{cases} \tag{4.13}$$

$$N_1(c, 2^a) = 2^{a-1}, \tag{4.14}$$

$$N^*(c, 2^a) = \begin{cases} 0, & \textit{if } 2 \nmid c; \\ 2^{a-1}, & \textit{if } 2 \mid c, \end{cases} \tag{4.15}$$

$$N_2(c, 2^a) = \begin{cases} 0, & \textit{if } 2 \nmid c; \\ 2^a, & \textit{if } 2 \mid c. \end{cases} \tag{4.16}$$

Proof The first two equations are from the remark after Proposition 4.1.

As $f(x, y)$ is even if y is odd, $N^*(c, 2^a) = N_2(c, 2^a) = 0$ if c is odd. If c is even, $\Gamma^*(c, 2^a) = \Gamma_1(c, 2^a)$ is obvious, hence $N^*(c, 2^a) = N_1(c, 2^a) = 2^{a-1}$.

Now for c even, $\Gamma_2(c, 2^a)$ is a disjoint union of Γ^* and $X = \{(2x, y) \mid y \text{ odd}, \ 4x^2 + 2xy + 2^{e_3}y^2 \equiv c \bmod 2^a$. As usual we have $|X| = 2N_2(2x^2 + xy + 2^{e_3-1}\lambda y^2; \frac{c}{2}, 2^{a-1}) = 2N_2(uv; \frac{c}{2}, 2^{a-1}) = 2^{a-1}$. □

Acknowledgements Research is partially supported by National Natural Science Foundation of China (Grant No. 11571328).

References

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

2. Mollahajiaghaei, M.: On the addition of squares of units modulo n. J. Number Theory **170**, 35–45 (2017)
3. Sun, C.F., Cheng, Z.: On the addition of two weighted squares of units mod n. Int. J. Number Theory **12**(7), 1783–1790 (2016)
4. Tóth, L.: *Counting solutions of quadratic congruences in several variables revisited*. J. Integer Seq. **17** (2014), Article 14.11.6
5. Yang, Q.H., Tang, M.: On the addition of squares of units and nonunits modulo n. J. Number Theory **155**, 1–12 (2015)