TOKYO J. MATH.
VOL. 41, NO. 2, 2018
DOI: 10.3836/tjm/1502179249

On the Integral Representation of Binary Quadratic Forms and the Artin Condition

Chang LV, Junchao SHENTU and Yingpu DENG

Institute of Information Engineering (CAS), University of Science and Technology of China, Academy of Mathematics and Systems Science (CAS) and University of Chinese Academy of Sciences

(Communicated by T. Komatsu)

Abstract. For diophantine equations of the form $ax^2 + bxy + cy^2 + g = 0$ over $\mathbf{Z}$ whose coefficients satisfy some assumptions, we show that a condition with respect to the Artin reciprocity map, which we call the Artin condition, is the only obstruction to the local-global principle for integral solutions of the equation. Some concrete examples are presented.

1. Introduction

The main theorem of a book by Cox [1] is a beautiful criterion of the solvability of the diophantine equation $p = x^2 + ny^2$. The specific statement is:

THEOREM 1. *Let n be a positive integer. Then there is a monic irreducible polynomial $f_n(x) \in \mathbf{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then $p = x^2 + ny^2$ is solvable over $\mathbf{Z}$ if and only if $\left(\frac{-n}{p}\right) = 1$ and $f_n(x) = 0$ is solvable over $\mathbf{Z}/p\mathbf{Z}$. Here $h(-4n)$ is the class number of primitive positive definite binary forms of discriminant $-4n$. Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the ring class field of the order $\mathbf{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-n})$.*

There are some generalizations considering the problem over quadratic fields. By using classical results in the class field theory, the first and third authors [3] gave the criterion of the integral solvability of the equation $p = x^2 + ny^2$ for some n over a class of imaginary quadratic fields, where p is a prime element.

Recently, Harari [2] showed that the Brauer-Manin obstruction is the only obstruction for the existence of integral points of a scheme over the ring of integers of a number field, whose generic fiber is a principal homogeneous space (torsor) of a torus. After then Wei and

Received July 20, 2016; revised January 12, 2017
2000 *Mathematics Subject Classification*: 11D09, 11E12, 11D57 (Primary), 14L30, 11R37 (Secondary)
Key words and phrases: binary quadratic forms, integral points, ring class field
The second author was supported by National Natural Science Foundation of China (Grant No. 11501418) and the third author was supported by National Natural Science Foundation of China (Grant No. 11471314).

Xu [9, 10] constructed the idele groups which are the so-called $\mathbf{X}$-*admissible subgroups* for determining the integral points for multi-norm tori, and interpreted the $\mathbf{X}$-admissible subgroup in terms of finite Brauer-Manin obstruction. In [9, Section 3] Wei and Xu also showed how to apply this method to binary quadratic diophantine equations. As applications, they gave some explicit criteria of the solvability of equations of the form $x^2 \pm dy^2 = a$ over $\mathbf{Z}$ in [9, Sections 4 and 5].

Later Wei [7] applied the method in [9] to give some additional criteria of the solvability of the diophantine equation $x^2 - dy^2 = a$ over $\mathbf{Z}$ for some d. He also determined which integers can be written as a sum of two integral squares for some of the quadratic fields $\mathbf{Q}(\sqrt{\pm p})$ (in [6]), $\mathbf{Q}(\sqrt{-2p})$ (in [8]) and so on.

In this article, we apply the method in [9] to diophantine equations of the form

$$ax^2 + bxy + cy^2 + g = 0 \tag{1}$$

over $\mathbf{Z}$, a binary quadratic form representing an integer. With some additional assumptions, by choosing $\mathbf{X}$-admissible subgroups for (1) the same as in [9, Sections 4, 5] and [6], we obtain criteria of the solvability of (1), as a variant of [9, Proposition 4.1] and [9, Proposition 5.1]. In the case $b = 0$, the first and second authors [4] also gave some corresponding results.

Specifically, the main result of this article is:

THEOREM 2. *Let a, b, c and g be integers and suppose that $d = 4ac - b^2 > 0$. Set $E = \mathbf{Q}(\sqrt{-d})$, $L = \mathbf{Z} + \mathbf{Z}\sqrt{-d}$ and H_L the ring class field corresponding to L. Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$. Then $\mathbf{X}(\mathbf{Z}) \neq \emptyset$ if and only if there exists*

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\Big(\tilde{f}_E\Big(\prod_p (x_p, y_p)\Big)\Big) = 1\,.$$

THEOREM 3. *Let a, b, c and g be integers such that $d = 4ac - b^2 < 0$. Suppose $-d = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ where $r > 0, m_k \geq 1$ are not all even and p_k are distinct odd primes such that one of the following assumptions holds*:

(1) $p_i \equiv 3 \pmod 4$ *for some i.*
(2) $r = 2$ *or $r > 3$ is odd, $p_i \equiv 1 \pmod 4, m_i = 1$ for all i and $(p_i/p_j) = -1$ for all $i \neq j$.*

Set $E = \mathbf{Q}(\sqrt{-d})$, $L = \mathbf{Z} + \mathbf{Z}\sqrt{-d}$ and H_L the ring class field corresponding to L. Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$. Then $\mathbf{X}(\mathbf{Z}) \neq \emptyset$ if and only if there exists

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\Big(\tilde{f}_E\Big(\prod_p (x_p, y_p)\Big)\Big) = 1\,.$$

In the above two theorems, $\tilde{f}_E$ is a map from $\prod_{p\le\infty} \mathbf{X}(\mathbf{Z}_p)$ to the idele group $\mathbf{I}_E$ of E which is constructed by using the fact that the generic fiber of $\mathbf{X}$ admits the structure of a torsor of a torus, and $\psi_{H_L/E} : \mathbf{I}_E \to \mathrm{Gal}(H_L/E)$ is the Artin reciprocity map. The condition $\psi_{H_L/E}(\tilde{f}_E(\prod_p (x_p, y_p))) = 1$ is called the Artin condition. See Section 2.1 for details.

In Section 2, we introduce from [9] notation and the general result we mainly use in this paper, but in a modified way which focus on our goal. Then we give our results on the equation (1) in Section 3. If the discriminant d is positive we need no additional assumption. But if d is negative, we add some assumptions on it (as it is done in [9, Section 5]). The results state that the integral local solvability and the Artin condition (see Remark 2) completely describe the global integral solvability. We also give some examples showing the explicit criteria of the solvability.

2. Solvability by the Artin Condition

2.1. Notation. Let F be a number field, $\mathfrak{o}_F$ the ring of integers of F, Ω_F the set of all places in F and ∞_F the set of all infinite places in F. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$ and $\mathfrak{o}_{F_\mathfrak{p}}$ the valuation ring of $F_\mathfrak{p}$ for each $\mathfrak{p} \in \Omega_F \setminus \infty_F$. We also write $\mathfrak{o}_{F_\mathfrak{p}} = F_\mathfrak{p}$ for $\mathfrak{p} \in \infty_F$. The adele ring (resp. idele group) of F is denoted by $\mathbf{A}_F$ (resp. $\mathbf{I}_F$).

Let a, b, c and g be elements in $\mathfrak{o}_F$ and suppose that $-d = b^2 - 4ac$ is not a square in F. Let $E = F(\sqrt{-d})$ and $\mathbf{X} = \mathrm{Spec}(\mathfrak{o}_F[x, y]/(ax^2 + bxy + cy^2 + g))$ be the affine scheme defined by the equation $ax^2 + bxy + cy^2 + g = 0$ over $\mathfrak{o}_F$. The equation

$$ax^2 + bxy + cy^2 + g = 0 \tag{2}$$

is solvable over $\mathfrak{o}_F$ if and only if $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$.

Now we denote

$$\tilde{x} := 2ax + by\,,$$
$$\tilde{y} := y\,,$$
$$n := -4ag\,.$$

Then we can write (2) as

$$\tilde{x}^2 + d\tilde{y}^2 = n\,. \tag{3}$$

Denote by $R_{E/F}(\mathbf{G}_m)$ the Weil restriction of $\mathbf{G}_{m,E}$ to F. Let

$$\varphi : R_{E/F}(\mathbf{G}_m) \longrightarrow \mathbf{G}_m$$

be the homomorphism of algebraic groups which represents

$$x \longmapsto N_{E/F}(x) : (E \otimes_F A)^\times \longrightarrow A^\times$$

for any F-algebra A. Define the torus $T := \ker\varphi$. Let X_F be the generic fiber of $\mathbf{X}$. We can identify elements in $T(A)$ (resp. $X_F(A)$) as $u+\sqrt{-d}v$ with $u^2+dv^2=1$ (resp. $\tilde{x}+\sqrt{-d}\tilde{y}$). Then X_F is naturally a T-torsor by the action:

$$T(A) \times X_F(A) \longrightarrow X_F(A)$$
$$(u+\sqrt{-d}v, \tilde{x}+\sqrt{-d}\tilde{y}) \longmapsto (u+\sqrt{-d}v)(\tilde{x}+\sqrt{-d}\tilde{y})\,.$$

Note that T has an integral model $\mathbf{T} = \mathrm{Spec}(\mathfrak{o}_F[x,y]/(x^2+dy^2-1))$ and we can view $\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subgroup of $T(F_\mathfrak{p})$.

Denote by λ the embedding of T into $R_{E/F}(\mathbf{G}_m)$. Clearly λ induces a natural injective group homomorphism

$$\lambda_E : T(\mathbf{A}_F) \longrightarrow \mathbf{I}_E\,.$$

Let $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$ in E and $L_\mathfrak{p} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_\mathfrak{p}}$ in $E_\mathfrak{p} = E \otimes_F F_\mathfrak{p}$. Then

$$\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) = \{\, \beta \in L_\mathfrak{p}^\times \mid N_{E_\mathfrak{p}/F_\mathfrak{p}}(\beta) = 1 \,\}\,.$$

It follows that $\lambda_E(\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})) \subseteq L_\mathfrak{p}^\times$. Note that $\lambda_E(T(F)) \subseteq E^\times$ in $\mathbf{I}_E$. Let $\mathfrak{Z}_L := \prod_{\mathfrak{p}\in\Omega_F} L_\mathfrak{p}^\times$ which is an open subgroup of $\mathbf{I}_E$. Then the following map induced by λ_E is well-defined:

$$\tilde{\lambda}_E : T(\mathbf{A}_F)/T(F) \prod_{\mathfrak{p}\in\Omega_F} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) \longrightarrow \mathbf{I}_E/E^\times \prod_{\mathfrak{p}\in\Omega_F} L_\mathfrak{p}^\times\,.$$

Now we assume that

$$X_F(F) \neq \emptyset\,, \tag{4}$$

i.e. X_F is a trivial T-torsor. Fixing a rational point $P \in X_F(F)$, for any F-algebra A, we have an isomorphism

$$\phi_P : X_F(A) \xrightarrow{\sim} T(A)$$
$$x \longmapsto P^{-1}x$$

induced by P. Since we can view $\prod_{\mathfrak{p}\in\Omega_F} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subset of $X_F(\mathbf{A}_F)$, the composition $f_E := \lambda_E\phi_P : \prod_\mathfrak{p} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) \longrightarrow \mathbf{I}_E$ makes sense, mapping x to $P^{-1}x$ in $\mathbf{I}_E$. Note that P is in $E^\times \subset \mathbf{I}_E$ since it is a rational point over F. It follows that we can define the map $\tilde{f}_E$ to be the composition

$$\prod_\mathfrak{p} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) \xrightarrow{f_E} \mathbf{I}_E \xrightarrow{\times P} \mathbf{I}_E\,.$$

It can be seen that the restriction to $\mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})$ of $\tilde{f}_E$ is defined by

$$\tilde{f}_E[(x_\mathfrak{p}, y_\mathfrak{p})] = \begin{cases} (\tilde{x}_\mathfrak{p} + \sqrt{-d}\tilde{y}_\mathfrak{p}, \tilde{x}_\mathfrak{p} - \sqrt{-d}\tilde{y}_\mathfrak{p}) \in E_\mathfrak{P} \times E_{\bar{\mathfrak{P}}} & \text{if } \mathfrak{p} = \mathfrak{P}\bar{\mathfrak{P}} \text{ splits in } E/F\,, \\ \tilde{x}_\mathfrak{p} + \sqrt{-d}\tilde{y}_\mathfrak{p} \in E_\mathfrak{P} & \text{otherwise}\,, \end{cases} \tag{5}$$

where $\mathfrak{P}$ and $\bar{\mathfrak{P}}$ (resp. $\mathfrak{P}$) are places of E above $\mathfrak{p}$ and $\tilde{x}_\mathfrak{p} = 2ax_\mathfrak{p} + by_\mathfrak{p}$, $\tilde{y}_\mathfrak{p} = y_\mathfrak{p}$.

Recall that $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$, $L_\mathfrak{p} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_\mathfrak{p}}$ and $\Xi_L = \prod_\mathfrak{p} L_\mathfrak{p}^\times$ is an open subgroup of $\mathbf{I}_E$. By the *ring class field corresponding to* L we mean the class field H_L corresponding to Ξ_L under the class field theory, such that the Artin map gives the isomorphism

$$\psi_{H_L/E} : \mathbf{I}_E/E^\times \Xi_L \xrightarrow{\sim} \mathrm{Gal}(H_L/E)\,.$$

For any $\prod_{\mathfrak{p}\in\Omega_F}(x_\mathfrak{p}, y_\mathfrak{p}) \in \prod_{\mathfrak{p}\in\Omega_F} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})$, noting that P is in E, we have

$$\psi_{H_L/E}\Big(f_E\Big(\prod_\mathfrak{p}(x_\mathfrak{p}, y_\mathfrak{p})\Big)\Big) = 1 \text{ if and only if } \psi_{H_L/E}\Big(\tilde{f}_E\Big(\prod_\mathfrak{p}(x_\mathfrak{p}, y_\mathfrak{p})\Big)\Big) = 1\,. \tag{6}$$

REMARK 1. If $\prod_{\mathfrak{p}\in\Omega_F} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) \neq \emptyset$, then the assumption (4) holds automatically by the Hasse-Minkowski theorem on quadratic equations. Hence we can pick an F-point P of X_F and obtain ϕ_P. But note that the map $\tilde{f}_E$ is independent of P.

2.2. A general result. In the previous section, we choose the subgroup to be $\Xi_L = \prod_\mathfrak{p} L_\mathfrak{p}^\times$ where $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$ and $L_\mathfrak{p} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_\mathfrak{p}}$. By some additional assumptions, we prove that Ξ_L can be viewed as an admissible subgroup for $\mathbf{X} = \mathrm{Spec}(\mathfrak{o}_F[x, y]/(ax^2 + bxy + cy^2 + g))$, that is, the map

$$\tilde{\lambda}_E : T(\mathbf{A}_F)/T(F)\prod \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) \longrightarrow \mathbf{I}_E/E^\times\Xi_L$$

is injective.

LEMMA 1. *Let $\mathcal{U}$ be a complete system of representatives of $\mathfrak{o}_F^\times/(\mathfrak{o}_F^\times)^2$. Suppose for every $u \in \mathcal{U}$, the equation $x^2 + dy^2 = u$ is solvable over $\mathfrak{o}_F$ or is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ for some place $\mathfrak{p}$. Then the map $\tilde{\lambda}_E$ is injective.*

PROOF. Recall that $T = \ker(R_{E/F}(\mathbf{G}_m) \longrightarrow \mathbf{G}_m)$ and $\mathbf{T}$ is the group scheme defined by the equation $x^2 + dy^2 = 1$ over $\mathfrak{o}_F$. Therefore we have

$$T(F) = \{\, \beta \in E^\times \mid N_{E/F}(\beta) = 1 \,\}$$

and

$$\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) = \{\, \beta \in L_\mathfrak{p}^\times \mid N_{E_\mathfrak{p}/F_\mathfrak{p}}(\beta) = 1 \,\}\,.$$

Suppose $t \in T(\mathbf{A}_F)$ such that $\tilde{\lambda}_E(t) = 1$. Write $t = \beta i$ with $\beta \in E^\times$ and $i \in \prod_{\mathfrak{p}} L_{\mathfrak{p}}^\times$. Since $t \in T(\mathbf{A}_F)$ we have

$$N_{E/F}(\beta)N_{E/F}(i) = N_{E/F}(\beta i) = 1\,.$$

It follows that

$$N_{E/F}(i) = N_{E/F}(\beta^{-1}) \in F^\times \cap \prod_{\mathfrak{p}} \mathfrak{o}_{F_{\mathfrak{p}}}^\times = \mathfrak{o}_F^\times\,.$$

So by the definition of $\mathcal{U}$, we have $N_{E/F}(i) = uv^2$ for some $u \in \mathcal{U}$ and $v \in \mathfrak{o}_F^\times$. Then

$$N_{E/F}(iv^{-1}) = u\,,$$

from which we know that the equation $x^2 + dy^2 = u$ is solvable over $\mathfrak{o}_{F_{\mathfrak{p}}}$ for every place $\mathfrak{p}$ of F, since $v^{-1} \in \mathfrak{o}_F$. Thus the assumption tells us that $x^2 + dy^2 = u$ is solvable over $\mathfrak{o}_F$. Let $(x_0, y_0) \in \mathfrak{o}_F^2$ be such a solution and let

$$\begin{aligned} \zeta &= x_0 + y_0\sqrt{-d}\,,\\ \gamma &= \beta v\zeta\,,\\ \text{and } j &= iv^{-1}\zeta^{-1}\,. \end{aligned}$$

Then $N_{E/F}(\gamma) = N_{E/F}(j) = 1$. Note that $\zeta \in L^\times$, and we have $\gamma \in T(F)$ and $j \in \prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. It follows that $t = \beta i = \gamma j \in T(F)\prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. This finishes the proof. □

As a result, we can obtain criteria of the solvability in a more explicit way. We state it in the following proposition, which is a Corollary to [9, Corollary 1.6].

PROPOSITION 1. *Let symbols be as above and $\mathcal{U}$ satisfy the assumption in Lemma* 1. *Then $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$ if and only if there exists*

$$\prod_{\mathfrak{p}\in\Omega_F} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\in\Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$$

such that

$$\psi_{H_L/E}\Big(\tilde{f}_E\Big(\prod_{\mathfrak{p}}(x_{\mathfrak{p}}, y_{\mathfrak{p}})\Big)\Big) = 1\,. \tag{7}$$

PROOF. By the assumption we know from Lemma 1, that

$$\tilde{\lambda}_E : T(\mathbf{A}_F)/T(F)\prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) \longrightarrow \mathbf{I}_E/E^\times \prod_{\mathfrak{p}} L_{\mathfrak{p}}^\times \tag{8}$$

is injective.

If $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$, then

$$\tilde{f}_E\left(\prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})\right) \cap E^\times \prod_{\mathfrak{p}} L_\mathfrak{p}^\times \supseteq \tilde{f}_E(\mathbf{X}(\mathfrak{o}_F)) \cap E^\times \neq \emptyset\,,$$

hence there exists $x \in \prod_{\mathfrak{p}\in\Omega_F} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})$ such that $\psi_{H_L/E}\tilde{f}_E(x) = 1$.

Conversely, suppose there exists $x \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}})$ such that $\psi_{H_L/E}\tilde{f}_E(x) = 1$ (here $\tilde{f}_E$ makes sense by Remark 1), i.e., $\lambda_E\phi_P(x) = f_E(x) \in E^\times \Xi_L = E^\times \prod_{\mathfrak{p}} L_\mathfrak{p}^\times$. Since $\tilde{\lambda}_E$, i.e., (8), is injective, there are $\tau \in T(F)$ and $\sigma \in \prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ such that $\tau\sigma = \phi_P(x) = P^{-1}x$, i.e., $\tau\sigma(P) = x$. Since $P \in X_F(F)$ and

$$g\mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) = \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) \text{ for all } g \in \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})\,, \tag{9}$$

it follows that

$$\tau(P) = \sigma^{-1}(x) \in \mathbf{X}(F) \cap \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_\mathfrak{p}}) = \mathbf{X}(\mathfrak{o}_F)\,.$$

Then the proof is done. □

REMARK 2. The condition (7) is called the *Artin condition* in, for example, Wei's [7, 6, 8]. If the assumption in the proposition holds, the integral local solvability and the Artin condition completely describe the global integral solvability. As a result, in cases where the ring class fields are known it is possible to calculate the Artin condition, and give explicit criteria for the solvability.

3. The Integral Representation of Binary Quadratic Forms over Z

Now we consider the case where $F = \mathbf{Q}$ which is our focus. We now distinguish the sign of the discriminant d.

3.1. The case where the discriminant $d > 0$.

THEOREM 4. *Let a, b, c and g be integers and suppose that $d = 4ac - b^2 > 0$. Set $E = \mathbf{Q}(\sqrt{-d})$, $L = \mathbf{Z} + \mathbf{Z}\sqrt{-d}$ and H_L the ring class field corresponding to L. Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$. Then $\mathbf{X}(\mathbf{Z}) \neq \emptyset$ if and only if there exists*

$$\prod_{p\leq\infty} (x_p, y_p) \in \prod_{p\leq\infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\left(\tilde{f}_E\left(\prod_p (x_p, y_p)\right)\right) = 1\,.$$

PROOF. Since $d > 0$ it is clear that $x^2 + dy^2 = -1$ is not solvable over $\mathbf{R}$, which is to say the assumption in Proposition 1 holds since the only units of $\mathbf{Z}$ are $\{\pm 1\}$. Then the result follows from Proposition 1. □

We now give an example where the explicit criterion is obtained using this result.

EXAMPLE 1. Let g be a negative integer and $l(x) = x^4 - x^3 + x + 1 \in \mathbf{Z}[x]$. Write $g = -2^{s_1} \times 7^{s_2} \times \prod_{k=1}^{r} p_k^{m_k}$, where $s_1, s_2, k \geq 0, m_k \geq 1$, $p_1, p_2, \ldots, p_r \neq 2, 7$ are distinct primes. Define $C = \{3, p_1, p_2, \ldots, p_r\}$ and

$$D = \left\{ p \in C \;\middle|\; \left(\frac{-14}{p}\right) = 1 \text{ and } l(x) \mod p \text{ irreducible} \right\}.$$

Then the diophantine equation $3x^2 + 2xy + 5y^2 + g = 0$ is solvable over $\mathbf{Z}$ if and only if

(1) $3g \times 2^{-s_1} \equiv \pm 1 \pmod 8$,
(2) $\left(\frac{g \times 7^{-s_2}}{7}\right) = 1$,
(3) for all $p \nmid 2 \times 3 \times 7$ with odd $m_p := v_p(g)$, $\left(\frac{-14}{p}\right) = 1$,
(4) and $\sum_{p \in D} v_p(3g) \equiv 0 \pmod 2$.

PROOF. In this example, we have $a = 3,\ b = 2,\ c = 5,\ d = 4ac - b^2 = 4 \times 14$. Let $E = \mathbf{Q}(\sqrt{-d})$. Since $b = 2$, we can simplify the equation (3) by canceling 4 in both sides. Thus we set

$$\begin{aligned} n &= -4ag/4 = -3g\,, \\ \tilde{x} &= (2ax + by)/2 = 3x + y\,, \\ \tilde{y} &= y\,. \end{aligned}$$

We can apply Theorem 4 for $d = 14$ to this example, since we still have $E = \mathbf{Q}(\sqrt{-d})$, $\tilde{x}^2 + d\tilde{y}^2 = n$ and (9) also holds. It follows that $L = \mathbf{Z} + \mathbf{Z}\sqrt{-14} = \mathfrak{o}_E$ and $H_L = H_E = E(\alpha)$ the Hilbert field of E where the minimal polynomial of α is $l(x)$. The Galois group can be calculated:

$$\mathrm{Gal}(H_L/E) = \langle \sqrt{-1} \rangle \cong \mathbf{Z}/4\mathbf{Z}\,.$$

Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(3x^2 + 2xy + 5y^2 + g))$ and

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-14}\tilde{y}_p, \tilde{x}_p - \sqrt{-14}\tilde{y}_p) & \text{if } p \text{ splits in } E/\mathbf{Q}\,, \\ \tilde{x}_p + \sqrt{-14}\tilde{y}_p & \text{otherwise}\,, \end{cases}$$

where $\tilde{x}_p = 3x_p + y_p$ and $\tilde{y}_p = y_p$. Then by Theorem 4, $\mathbf{X}(\mathbf{Z}) \neq \emptyset$ if and only if there exists

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\left(\tilde{f}_E\left(\prod_p (x_p, y_p)\right)\right) = 1\,.$$

Next we verify these conditions in details. Recall that $n = -3g$. By a simple calculation we know the local condition

$$\prod_{p\le\infty} \mathbf{X}(\mathbf{Z}_p) \neq \emptyset$$

is equivalent to

$$\begin{cases} n \times 2^{-s_1} \equiv \pm 1 \pmod 8\,, \\ \left(\frac{n\times 7^{-s_2}}{7}\right) = 1\,, \\ \text{for all } p \nmid 2\times 3\times 7 \text{ with odd } m_p = v_p(n),\ \left(\frac{-14}{p}\right) = 1\,. \end{cases} \tag{10}$$

For the Artin condition, let $(x_p, y_p)_p \in \prod_p \mathbf{X}(\mathbf{Z}_p)$. Then

$$(\tilde{x}_p + \sqrt{-14}\tilde{y}_p)(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) = n \text{ in } E_{\mathfrak{P}} \text{ with } \mathfrak{P} \mid p\,, \tag{11}$$

and since H_L/E is unramified, for any $p \neq \infty$ we have

$$1 = \begin{cases} \psi_{H_L/E}(p_{\mathfrak{P}})\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}), & \text{if } p = \mathfrak{P}\bar{\mathfrak{P}} \text{ splits in } E/\mathbf{Q}\,, \\ \psi_{H_L/E}(p_{\mathfrak{P}}), & \text{if } p = \mathfrak{P} \text{ is inert in } E/\mathbf{Q}\,, \end{cases} \tag{12}$$

where $p_{\mathfrak{P}}$ (resp. $p_{\bar{\mathfrak{P}}}$) is in $\mathbf{I}_E$ such that its $\mathfrak{P}$ (resp. $\bar{\mathfrak{P}}$) component is p and the other components are 1. We calculate $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)])$ separately:

1. If $p = 2$, $2 = \mathfrak{P}_2^2$ in $E/\mathbf{Q}$. Suppose $\mathfrak{P}_2 = \pi_2 \mathfrak{o}_{E_{\mathfrak{P}_2}}$ for $\pi_2 \in \mathfrak{o}_{E_{\mathfrak{P}_2}}$. Noting that H_L/E is unramified, since $\mathfrak{P}_2^2$ is principal in E but $\mathfrak{P}_2$ is not, we have $\psi_{H_L/E}((\pi_2)_{\mathfrak{P}_2}) = -1$. By (11) we have

$$v_{\mathfrak{P}_2}(\tilde{x}_2 + \sqrt{-14}\tilde{y}_2) = v_{\mathfrak{P}_2}(\tilde{x}_2 - \sqrt{-14}\tilde{y}_2) = \frac{1}{2}v_{\mathfrak{P}_2}(n) = v_2(n) = s_1\,.$$

   It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_2, y_2)]) &= \psi_{H_L/E}((\tilde{x}_2 + \sqrt{-14}\tilde{y}_2)_{\mathfrak{P}_2}) \\ &= (-1)^{v_{\mathfrak{P}_2}(\tilde{x}_2+\sqrt{-14}\tilde{y}_2)} = (-1)^{s_1}\,, \end{aligned}$$

   where $\tilde{f}_E[(x_2, y_2)]$ is also regarded as an element in $\mathbf{I}_E$ such that the component above 2 is given by the value of $\tilde{f}_E[(x_2, y_2)]$ and 1 otherwise.
2. If $p = 7$, a similar argument shows that $\psi_{H_L/E}(\tilde{f}_E[(x_7, y_7)]) = (-1)^{s_2}$.
3. If $\left(\frac{-14}{p}\right) = 1$ then by (12) we can distinguish the following cases:

(i) $l(x) \mod p$ splits into linear factors. Then $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\bar{\mathfrak{P}}}) = 1$ and $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$.

(ii) $l(x) \mod p$ splits into two irreducible factors. Then $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\bar{\mathfrak{P}}}) = -1$. It follows that

$$\begin{aligned}\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{-14}\tilde{y}_p)_{\mathfrak{P}})\psi_{H_L/E}((\tilde{x}_p - \sqrt{-14}\tilde{y}_p)_{\bar{\mathfrak{P}}}) \\ &= (-1)^{v_{\mathfrak{P}}(\tilde{x}_p+\sqrt{-14}\tilde{y}_p)+v_{\bar{\mathfrak{P}}}(\tilde{x}_p-\sqrt{-14}\tilde{y}_p)} = (-1)^m,\end{aligned}$$

where $m = v_p(n)$ since

$$\begin{aligned}&v_{\mathfrak{P}}(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_{\bar{\mathfrak{P}}}(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) \\ &\qquad = v_p(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_p(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) = v_p(n)\,.\end{aligned}$$

(iii) $l(x) \mod p$ is irreducible. Then $\psi_{H_L/E}(p_{\mathfrak{P}}) = -\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}) = \pm\sqrt{-1}$. It follows that

$$\begin{aligned}\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{-14}\tilde{y}_p)_{\mathfrak{P}})\psi_{H_L/E}((\tilde{x}_p - \sqrt{-14}\tilde{y}_p)_{\bar{\mathfrak{P}}}) \\ &= (\pm\sqrt{-1})^{v_{\mathfrak{P}}(\tilde{x}_p+\sqrt{-14}\tilde{y}_p)+v_{\bar{\mathfrak{P}}}(\tilde{x}_p-\sqrt{-14}\tilde{y}_p)}(-1)^{v_{\bar{\mathfrak{P}}}(\tilde{x}_p-\sqrt{-14}\tilde{y}_p)} \\ &= (\pm\sqrt{-1})^m(-1)^u\end{aligned}$$

where $m = v_p(n)$ and $u = v_p(\tilde{x}_p - \sqrt{-14}\tilde{y}_p)$ (in $\mathbf{Q}_p$, $0 \le u \le m$). By Hensel's lemma, we can choose a local solution (x_p, y_p) suitably, such that u is taken over any value between 0 and m. Hence $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = \pm(\sqrt{-1})^m$ with the sign chosen freely.

4. If $\left(\frac{-14}{p}\right) = -1$ then p is inert in $E/\mathbf{Q}$. By (12) we have $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$.
5. At last if $p = \infty$, since H_L/E is unramified, we have $\psi_{H_L/E}(\tilde{f}_E[(x_\infty, y_\infty)]) = 1$.

Putting the above argument together, and noting that $D \neq \emptyset$ since $3 \in D$ and that $n = -3g$, we know the Artin condition is

$$\sum_{p\in D} v_p(3g) \equiv 0 \pmod 2\,. \tag{13}$$

The proof is done if we put the local condition (10) and the Artin condition (13) together. □

3.2. The case where the discriminant $d < 0$. In this case, $x^2 + dy^2 = -1$ is solvable over $\mathbf{R}$, so we must look for other place p of $\mathbf{Q}$ such that $x^2 + dy^2 = -1$ is not solvable over $\mathbf{Z}_p$. For a rational prime p that divides d, we observe that, by Hensel's Lemma, $x^2 + dy^2 = -1$ is solvable over $\mathbf{Z}_p$ if and only if it is solvable over $\mathbf{Z}/p\mathbf{Z}$, i.e., $\left(\frac{-1}{p}\right) = 1$. So if d is divisible by some rational prime p where $p \equiv 3 \pmod 4$ then $x^2 + dy^2 = -1$ is not solvable over $\mathbf{Z}_p$. Otherwise if none of the prime divisors of d are congruent to 3 modulo

4, we hope that $x^2 + dy^2 = -1$ is solvable over $\mathbf{Z}$, in order to make the assumption true in Proposition 1. We need the following result by Morris Newman [5].

THEOREM 5. *Let $r > 1$ be 2 or odd, $p_1, p_2, \ldots, p_r$ be distinct primes such that*

$$p_i \equiv 1 \pmod 4, \quad 1 \le i \le r,$$

$$\left(\frac{p_i}{p_j}\right) = -1, \quad 1 \le i \ne j \le r.$$

Then the diophantine equation $x^2 - p_1 p_2 \ldots p_r y^2 = -1$ has a solution in $\mathbf{Z}$.

Now we have the criterion for a certain $d < 0$.

THEOREM 6. *Let a, b, c and g be integers such that $d = 4ac - b^2 < 0$. Suppose $-d = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ where $r > 0, m_k \ge 1$ are not all even and p_k are distinct odd primes such that one of the following assumptions holds*:

(1) $p_i \equiv 3 \pmod 4$ *for some i.*
(2) *$r = 2$ or $r > 3$ is odd, $p_i \equiv 1 \pmod 4, m_i = 1$ for all i and $(p_i/p_j) = -1$ for all $i \ne j$.*

Set $E = \mathbf{Q}(\sqrt{-d})$, $L = \mathbf{Z} + \mathbf{Z}\sqrt{-d}$ and H_L the ring class field corresponding to L. Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$. Then $\mathbf{X}(\mathbf{Z}) \ne \emptyset$ if and only if there exists

$$\prod_{p \le \infty} (x_p, y_p) \in \prod_{p \le \infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\left(\tilde{f}_E\left(\prod_p (x_p, y_p)\right)\right) = 1.$$

PROOF. The units of $\mathbf{Z}$ are $\{\pm 1\}$ so we only need to consider the unit -1. If (1) holds, i.e., $p_i \equiv 3 \pmod 4$ for some i, one can see immediately that $x^2 + dy^2 = -1$ is not solvable over $\mathbf{Z}_{p_i}$. Otherwise (2) holds and then $x^2 + dy^2 = -1$ is solvable over $\mathbf{Z}$ by Theorem 5. Hence the assumption in Proposition 1 holds and we complete the proof by Proposition 1. □

We now give an example for this case.

EXAMPLE 2. Let g be a nonzero integer and $l(x) = x^3 - x^2 - 4x + 2 \in \mathbf{Z}[x]$. Write $g = \pm 2^{s_1} \times 79^{s_2} \times \prod_{k=1}^{r} p_k^{m_k}$, where $s_1, s_2, k \ge 0, m_k \ge 1, p_1, p_2, \ldots, p_r \ne 2, 79$ are distinct primes. Define $C = \{5, p_1, p_2, \ldots, p_r\}$ and

$$D = \left\{ p \in C \;\middle|\; \left(\frac{79}{p}\right) = 1 \text{ and } l(x) \mod p \text{ irreducible} \right\}.$$

Then the diophantine equation $5x^2 + 14xy - 6y^2 + g = 0$ is solvable over $\mathbf{Z}$ if and only if

(1) $\left(\frac{g \times (-79)^{-s_2}}{79}\right) = -1$,

(2) for all $p \nmid 2 \times 5 \times 79$ with odd $m_p := v_p(g)$, $\left(\frac{79}{p}\right) = 1$,
(3) and if $\{\, p \in D \mid v_p(5g) = 1 \,\} \neq \emptyset$ then $r > 1$.

PROOF. In this example, we have $a = 5,\ b = 14,\ c = -6,\ d = 4ac - b^2 = -4 \times 79$. Let $E = \mathbf{Q}(\sqrt{-d})$. Since $2 \mid b$, we may cancel 4 in both sides and assume $d = -79$ as we do in the previous example. Since $79 \equiv 3 \pmod 4$ the assumption (1) in Theorem 6 is correct. It follows that we can apply the theorem for $d = -79$. Thus we set

$$n = -4ag/4 = -5g\,,$$
$$\tilde{x} = (2ax + by)/2 = 5x + 7y\,,$$
$$\tilde{y} = y\,.$$

Now $E = \mathbf{Q}(\sqrt{79})$, $\tilde{x}^2 - 79\tilde{y}^2 = n$ and $L = \mathbf{Z} + \mathbf{Z}\sqrt{79} = \mathfrak{o}_E$ and $H_L = H_E = E(\alpha)$ the Hilbert field of E where the minimal polynomial of α is $l(x)$. The Galois group can be calculated:

$$\mathrm{Gal}(H_L/E) = \langle \omega \rangle \cong \mathbf{Z}/3\mathbf{Z}\,.$$

Let $\mathbf{X} = \mathrm{Spec}(\mathbf{Z}[x, y]/(5x^2 + 14xy - 6y^2 + g))$ and

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{79}\tilde{y}_p, \tilde{x}_p - \sqrt{79}\tilde{y}_p) & \text{if } p \text{ splits in } E/\mathbf{Q}\,, \\ \tilde{x}_p + \sqrt{79}\tilde{y}_p & \text{otherwise}\,, \end{cases}$$

where $\tilde{x}_p = 5x_p + 7y_p$ and $\tilde{y}_p = y_p$. Then by Theorem 6, $\mathbf{X}(\mathbf{Z}) \neq \emptyset$ if and only if there exists

$$\prod_{p \le \infty} (x_p, y_p) \in \prod_{p \le \infty} \mathbf{X}(\mathbf{Z}_p)$$

such that

$$\psi_{H_L/E}\Big(\tilde{f}_E\Big(\prod_p (x_p, y_p)\Big)\Big) = 1\,.$$

By a simple computation the local condition

$$\prod_{p \le \infty} \mathbf{X}(\mathbf{Z}_p) \neq \emptyset$$

is equivalent to the first two conditions (1) and (2) above. For the Artin condition, let $(x_p, y_p)_p \in \prod_p \mathbf{X}(\mathbf{Z}_p)$. Then

$$(\tilde{x}_p + \sqrt{79}\tilde{y}_p)(\tilde{x}_p - \sqrt{79}\tilde{y}_p) = n \text{ in } E_{\mathfrak{P}} \text{ with } \mathfrak{P} \mid p\,,$$

and since H_L/E is unramified, for any $p \neq \infty$ we have

$$1 = \begin{cases} \psi_{H_L/E}(p_{\mathfrak{P}})\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}), & \text{if } p = \mathfrak{P}\bar{\mathfrak{P}} \text{ splits in } E/\mathbf{Q}, \\ \psi_{H_L/E}(p_{\mathfrak{P}}), & \text{if } p = \mathfrak{P} \text{ is inert in } E/\mathbf{Q}. \end{cases} \tag{14}$$

We calculate $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)])$ separately:

1. If $p = 2$, $2 = \mathfrak{P}_2^2$ in $E/\mathbf{Q}$. Suppose $\mathfrak{P}_2 = \pi_2 \mathfrak{o}_{E_{\mathfrak{P}_2}}$ for $\pi_2 \in \mathfrak{o}_{E_{\mathfrak{P}_2}}$. Noting that H_L/E is unramified, since $\mathfrak{P}_2$ is principal in E, we have $\psi_{H_L/E}((\pi_2)_{\mathfrak{P}_2}) = 1$. Hence $\psi_{H_L/E}(\tilde{f}_E[(x_2, y_2)]) = 1$.
2. If $p = 79$, a similar argument shows that $\psi_{H_L/E}(\tilde{f}_E[(x_{79}, y_{79})]) = 1$.
3. If $\left(\frac{79}{p}\right) = 1$ then by (14) we can distinguish the following two cases:
   (i) $l(x) \mod p$ splits into linear factors. Then $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\bar{\mathfrak{P}}}) = 1$ and $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$.
   (ii) $l(x) \mod p$ is irreducible. Then $\psi_{H_L/E}(p_{\mathfrak{P}}) = (\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}))^{-1} = \omega^{\pm 1}$. It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{79}\tilde{y}_p)_{\mathfrak{P}})\psi_{H_L/E}((\tilde{x}_p - \sqrt{79}\tilde{y}_p)_{\bar{\mathfrak{P}}}) \\ &= \omega^{\pm(v_{\mathfrak{P}}(\tilde{x}_p+\sqrt{79}\tilde{y}_p)+v_{\bar{\mathfrak{P}}}(\tilde{x}_p-\sqrt{79}\tilde{y}_p))}/\omega^{\pm 2v_{\bar{\mathfrak{P}}}(\tilde{x}_p-\sqrt{79}\tilde{y}_p)} \\ &= \omega^{\pm(m-2u)} \end{aligned}$$

   where $m = v_p(n)$ and $u = v_p(\tilde{x}_p - \sqrt{79}\tilde{y}_p)$ (in $\mathbf{Q}_p$, $0 \leq u \leq m$). By Hensel's lemma, we can choose a local solution (x_p, y_p) suitably, such that u is taken over any value between 0 and m. Hence

$$\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = \begin{cases} 1 & \text{if } m = 0, \\ \omega^{\pm 1} & \text{if } m = 1, \\ 1 \text{ or } \omega^{\pm 1} & \text{if } m \geq 2, \end{cases}$$

   where the values are chosen freely in each case.
4. If $\left(\frac{79}{p}\right) = -1$ then p is inert in $E/\mathbf{Q}$. By (14) we have $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$.
5. At last if $p = \infty$, since H_L/E is unramified, we have $\psi_{H_L/E}(\tilde{f}_E[(x_\infty, y_\infty)]) = 1$.

Putting the above argument together, and noting that $5 \in D$ and $n = -5g$, we know the Artin condition is exactly the last condition (3) in the example. This completes the proof. □

ACKNOWLEDGMENT. The authors would like to thank Yupeng Jiang and Jianing Li for helpful discussions and the referees for valuable suggestions.

References

[1] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, John Wiley & Sons, 1989.

[2] D. Harari, Le défaut d'approximation forte pour les groupes algébriques commutatifs, Algebra & Number Theory **2**, no. 5 (2008), 595–611.

[3] C. Lv and Y. Deng, On orders in number fields: Picard groups, ring class fields and applications, Science China Mathematics **58**, no. 8 (2015), 1627–1638.

[4] C. Lv and J. Shentu, On the integral representation of $ax^2 + by^2$ and the Artin condition, arXiv preprint arXiv: 1502.07457 (2015), 1–9.

[5] M. Newman, A note on an equation related to the Pell equation, American Mathematical Monthly **84**, no. 5 (1977), 365–366.

[6] D. Wei, On the sum of two integral squares in quadratic fields $\mathbf{Q}(\sqrt{\pm p})$, Acta Arith. **147**, no. 3 (2011), 253–260.

[7] D. Wei, On the diophantine equation $x^2 - Dy^2 = n$, Science China Mathematics **56**, no. 2 (2013), 227–238.

[8] D. Wei, On the sum of two integral squares in the imaginary quadratic field $\mathbf{Q}(\sqrt{-2p})$, Science China Mathematics **57**, no. 1 (2014), 49–60.

[9] D. Wei and F. Xu, Integral points for multi-norm tori, Proceedings of the London Mathematical Society **104**, no. 5 (2012), 1019–1044.

[10] D. Wei and F. Xu, Integral points for groups of multiplicative type, Advances in Mathematics **232**, no. 1 (2013), 36–56.

Present Addresses:
Chang Lv
State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences,
Beijing 100093, P.R. China.
e-mail: lvchang@amss.ac.cn

Junchao Shentu
University of Science and Technology of China,
Hefei 230001, P.R. China.
e-mail: stjc@amss.ac.cn

Yingpu Deng
Key Laboratory of Mathematics Mechanization,
NCMIS, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences,
and School of Mathematical Sciences,
University of Chinese Academy of Sciences,
Beijing 100190, P.R. China.
e-mail: dengyp@amss.ac.cn