ACTA ARITHMETICA
147.3 (2011)

On the sum of two integral squares in quadratic fields $\mathbb{Q}(\sqrt{\pm p})$

by

Dasheng Wei (Beijing)

1. Introduction. Gauss first determined which integers can be written as a sum of two integral squares. Niven [5] determined which integers can be written as a sum of two integral squares for the imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$. Nagell further studied the question in [3] and [4] for the twenty quadratic fields $\mathbb{Q}(\sqrt{d})$, where

$$d = \pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 19, \pm 43, \pm 67, \pm 163.$$

His method essentially depends on the fact that the class number of the field $\mathbb{Q}(\sqrt{d}, \sqrt{-d})$ is 1 when d is one of the above integers. However, this method does not apply to general quadratic fields. Recently, Harari [1] showed that the Brauer–Manin obstruction is the only obstruction to existence of integral points of a scheme over the ring of integers of a number field whose generic fiber is a principal homogeneous space of a torus. However, the Brauer–Manin obstruction given in [1] is not constructive and one cannot use that result to determine the existence of integral points for the scheme. Fei Xu and the author gave another, constructive proof of that result in [6] and [7]. In this paper we apply the method of [6] to the quadratic fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$ with p prime.

The notation and terminology are standard if not explained. Let F be a number field, $\mathfrak{o}_F$ the ring of integers of F, Ω_F the set of all primes in F, and ∞ the set of all infinite primes in F. For simplicity, we write $\mathfrak{p} < \infty$ for $\mathfrak{p} \in \Omega_F \setminus \infty$. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$, and $\mathfrak{o}_{F_\mathfrak{p}}$ be the local completion of $\mathfrak{o}_F$ at $\mathfrak{p}$ for each $\mathfrak{p} \in \Omega_F$. Write $\mathfrak{o}_{F_\mathfrak{p}} = F_\mathfrak{p}$ for $\mathfrak{p} \in \infty$. We also denote the adele ring (resp. the idele ring) of F by $\mathbb{A}_F$ (resp. $\mathbb{I}_F$), and set

$$F_\infty = \prod_{\mathfrak{p} \in \infty} F_\mathfrak{p}.$$

2010 *Mathematics Subject Classification*: Primary 11E12; Secondary 11D09.
Key words and phrases: integral points, ring class field, reciprocity law.

DOI: 10.4064/aa147-3-5

Suppose that -1 is not a square in F. Let $E = F(\sqrt{-1})$ and let T be the torus

$$R^1_{E/F}(\mathbb{G}_m) = \mathrm{Ker}[R_{E/F}(\mathbb{G}_{m,E}) \to \mathbb{G}_{m,F}],$$

where R denotes Weil's restriction (see [2, p. 211]). Denote by λ the embedding from T to $R_{E/F}(\mathbb{G}_{m,E})$. Obviously λ induces a natural group homomorphism

$$\lambda_E : T(\mathbb{A}_F) \to \mathbb{I}_E.$$

Let $\mathbf{X}_\alpha$ be the affine scheme over $\mathfrak{o}_F$ defined by the equation $x^2 + y^2 = \alpha$ for a non-zero integer $\alpha \in \mathfrak{o}_F$. The generic fiber of $\mathbf{X}_\alpha$ is a principal homogeneous space of the torus T. The equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$.

Definition 1.1. Let K/E be a finite abelian extension. Let $\psi_{K/E} : \mathbb{I}_E \to \mathrm{Gal}(K/E)$ be the Artin map. We say that α satisfies the *Artin condition of* K if there is

$$\prod_{\mathfrak{p}\le\infty} (x_\mathfrak{p}, y_\mathfrak{p}) \in \prod_{\mathfrak{p}\le\infty} \mathbf{X}_\alpha(\mathfrak{o}_{F_\mathfrak{p}}) \quad \text{such that} \quad \psi_{K/E}\Big(f_E\Big[\prod_{\mathfrak{p}\le\infty} (x_\mathfrak{p}, y_\mathfrak{p})\Big]\Big) = 1$$

where 1 is the identity element of $\mathrm{Gal}(K/E)$ and $f_E : \prod_{\mathfrak{p}\le\infty} \mathbf{X}_\alpha(\mathfrak{o}_{F_\mathfrak{p}}) \to \mathbb{I}_E$ is defined by

$$f_E[(x_\mathfrak{p}, y_\mathfrak{p})] = \begin{cases} (x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, x_\mathfrak{p} - y_\mathfrak{p}\sqrt{-1}) & \text{if } \mathfrak{p} \text{ splits in } E/F, \\ x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1} & \text{otherwise.} \end{cases}$$

By class field theory, it is a necessary condition for $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ that α satisfies the Artin condition of K. In fact there is a finite abelian extension K/E, independent of α, such that the Artin condition of K is also sufficient for $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ (see [6]).

Let $\mathbf{T}$ be the group scheme over $\mathfrak{o}_F$ defined by $x^2 + y^2 = 1$, which is an integral model of T. Since $\mathbf{T}$ is separated over $\mathfrak{o}_F$, we can view $\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subgroup of $T(F_\mathfrak{p})$. Furthermore, the following result is proved in [6].

Proposition 1.2. *Let K/E be a finite abelian extension such that the group homomorphism $\widetilde{\lambda}_E$ induced by λ_E,*

$$\widetilde{\lambda}_E : T(\mathbb{A}_F)/T(F) \prod_{\mathfrak{p}\le\infty} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) \to \mathbb{I}_E/E^* N_{K/E}(\mathbb{I}_K)$$

is well-defined and injective, where well-defined means

$$\lambda_E\Big(T(F) \prod_{\mathfrak{p}\le\infty} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})\Big) \subset E^* N_{K/E}(\mathbb{I}_K).$$

Then $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ if and only if α satisfies the Artin condition of K.

In this paper, we mainly prove the following result.

THEOREM 1.3. *Let p be a prime number and F the quadratic field $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$. Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L, where H_L is the ring class field corresponding to the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$.*

2. The sum of two squares in imaginary quadratic fields. Let d be a square-free positive integer with $d\geq 2$. Let $F=\mathbb{Q}(\sqrt{-d})$, $\mathfrak{o}_F$ be the integral ring of F and $E=F(\sqrt{-1})$. One takes the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$ inside E. Let H_L be the ring class field corresponding to the order L.

PROPOSITION 2.1. *Suppose one of the following conditions holds:*

(1) *The equation $x^2+y^2=-1$ has an integral solution in $\mathfrak{o}_F$.*
(2) *The equation $x^2+y^2=-1$ has no local integral solutions at a place of F.*

Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.

Proof. (1) First we assume $d\neq 3$. Let $\mathfrak{p}$ be a place of F, and $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L inside $E_\mathfrak{p}=E\otimes_F F_\mathfrak{p}$. Recalling that $T=R^1_{E/F}(\mathbb{G}_{m,F})$ and $\mathbf{T}$ is the scheme defined by the equation $x^2+y^2=1$, we have

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

Since the ring class field H_L of the order L corresponds to the open subgroup $E^*(\prod_{\mathfrak{p}\leq\infty}L_\mathfrak{p}^\times)$ of $\mathbb{I}_E$ by class field theory, the natural group homomorphism

$$\widetilde{\lambda}_E: T(\mathbb{A}_F)/T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})\to \mathbb{I}_E/E^*\prod_{\mathfrak{p}\leq\infty}L_p^\times$$

is well-defined. By Proposition 1.2, we only need to show $\widetilde{\lambda}_E$ is injective.

Suppose there are

$$\beta\in E^*\quad\text{and}\quad i\in E_\infty^*\prod_{\mathfrak{p}<\infty}L_\mathfrak{p}^\times$$

such that $\beta i\in T(\mathbb{A}_E)$. Then

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

and

$$N_{E/F}(\beta)\in F^*\cap\prod_{\mathfrak{p}<\infty}\mathfrak{o}_{F_\mathfrak{p}}^\times=\{\pm 1\}.$$

If $N_{E/F}(\beta)=1$, one concludes that $N_{E/F}(\beta)=N_{E/F}(i)=1$, so

$$\beta\in T(F)\quad\text{and}\quad i\in\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}).$$

Hence $\beta i\in T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$.

If $N_{E/F}(\beta) \neq 1$, then $N_{E/F}(\beta) = N_{E/F}(i) = -1$. Thus $x^2 + y^2 = -1$ has local integral solutions at every local place of F. By assumption, $x^2+y^2 = -1$ has an integral solution (x_0, y_0) in $\mathfrak{o}_F$. Let

$$\zeta = x_0 + y_0\sqrt{-1} \quad \text{and} \quad \gamma = \beta\zeta,\ j = i/\zeta.$$

Then $\beta i = \gamma j$ and $N_{E/F}(\gamma) = N_{E/F}(j) = 1$, so

$$\gamma \in T(F) \quad \text{and} \quad j \in \prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}).$$

Hence $\beta i = \gamma j \in T(F)\prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$. Therefore $\widetilde{\lambda}_E$ is injective.

(2) If $d = 3$, then $\mathfrak{o}_F^\times = \langle \pm 1, \zeta_3\rangle$, where ζ_3 is a primitive 3rd root of unity. Since $\zeta_3 = \zeta_3^4$ is a square, the proof for this case is similar. ∎

In the rest of this section we consider the case that d is a prime. First we need the following result that can be found in [8].

Proposition 2.2. *Let p be a prime.*

(1) *If $p \equiv 1 \bmod 4$, then $x^2 - py^2 = -1$ is solvable over $\mathbb{Z}$.*
(2) *If $p \equiv -1 \bmod 8$, then $x^2 - py^2 = 2$ is solvable over $\mathbb{Z}$.*
(3) *If $p \equiv 3 \bmod 8$, then $x^2 - py^2 = -2$ is solvable over $\mathbb{Z}$.*

Now we can prove the following lemma.

Lemma 2.3. *Let p be a prime and $F = \mathbb{Q}(\sqrt{-p})$.*

(1) *If $p \equiv -1 \bmod 8$, then $x^2 + y^2 = -1$ is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$, where $\mathfrak{p} \mid 2$.*
(2) *If $p \not\equiv -1 \bmod 8$, then $x^2 + y^2 = -1$ is solvable over $\mathfrak{o}_F$.*

Proof. (1) If $p \equiv -1 \bmod 8$, then 2 splits into $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in the field $F/\mathbb{Q}$. So the Hilbert symbol satisfies

$$(-1,-1)_{\mathfrak{p}_1} = (-1,-1)_{\mathfrak{p}_2} = -1.$$

Therefore the equation $x^2 + y^2 = -1$ is not solvable over $\mathfrak{o}_{F_{\mathfrak{p}_1}}$ or $\mathfrak{o}_{F_{\mathfrak{p}_2}}$.

If $p \equiv 1 \bmod 4$ or $p = 2$, then $x^2 - py^2 = -1$ has an integral solution (x_0, y_0) in $\mathbb{Z}$ by Proposition 2.2. Hence $x_0^2 + (y_0\sqrt{-p})^2 = -1$.

If $p \equiv 3 \bmod 8$, then $x^2 - py^2 = -2$ has an integral solution (x_0, y_0) in $\mathbb{Z}$ by Proposition 2.2. It is easy to see that $x_0, y_0 \equiv 1 \bmod 2$. So

$$\frac{x_0 \pm y_0\sqrt{-p}}{2} \in \mathfrak{o}_F \quad \text{and} \quad \left(\frac{x_0 + y_0\sqrt{-p}}{2}\right)^2 + \left(\frac{x_0 - y_0\sqrt{-p}}{2}\right)^2 = -1. \ \blacksquare$$

From Proposition 2.1 and Lemma 2.3, we obtain the following result.

Theorem 2.4. *Let p be a prime number and $F = \mathbb{Q}(\sqrt{-p})$. Let H_L be the ring class field corresponding to the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Then the diophantine equation $x^2+y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.*

REMARK 2.5. It is possible that the equation $x^2+y^2=\alpha$ satisfies the Hasse principle for any non-zero integer $\alpha \in \mathfrak{o}_F$ even if the ring class field H_L is not trivial. For example, let $p = 23, 31, 47, 59, 71$ and $F = \mathbb{Q}(\sqrt{-p})$. Then H_L is not trivial and the equation $x^2+y^2=\alpha$ satisfies the Hasse principle for any non-zero integer $\alpha \in \mathfrak{o}_F$. The reason is that $H_L = EH$ for the above p, where $E = F(\sqrt{-1})$ and H is the Hilbert class field of F. If $x^2+y^2=\alpha$ has local solutions for every place, then α automatically satisfies the Artin condition of H_L by class field theory.

Now we use Theorem 2.4 to give an explicit example. Let $F = \mathbb{Q}(\sqrt{-79})$. Write $N_{F/\mathbb{Q}}(\alpha) = 2^{s_1}79^{s_2}p_1^{e_1}\cdots p_g^{e_g}$ for any $\alpha \in \mathfrak{o}_F$. Let $D(n) = \{p_1, \dots, p_g\}$ and $h(x) = x^3 - 307x + 1772$. Denote

$$D_1 = \left\{ p \in D(n) : \left(\frac{79}{p}\right) = \left(\frac{-1}{p}\right) = 1 \right. \\ \left. \text{and } h(x) \equiv 0 \bmod p \text{ is not solvable} \right\},$$

$$D_2 = \left\{ p \in D(n) : \left(\frac{79}{p}\right) = -\left(\frac{-1}{p}\right) = 1 \right. \\ \left. \text{and } h(x) \equiv 0 \bmod p \text{ is not solvable} \right\}.$$

It is easy to see that e_i is even when $p_i \in D_2$.

EXAMPLE 2.6. Let $F = \mathbb{Q}(\sqrt{-79})$ and let α be an integer in F. With the above notation, $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if

(1) $x^2+y^2=\alpha$ has integral solutions at every place of F,
(2) $\displaystyle\sum_{p_i \in D_1} e_i + \sum_{p_i \in D_2} e_i/2 \neq 1.$

3. The sum of two squares in real quadratic fields. Let d be a square-free positive integer and $F = \mathbb{Q}(\sqrt{d})$. Let $\mathfrak{o}_F$ be the ring of integers of F, ε the fundamental unit of $\mathfrak{o}_F$, and $\varepsilon = a + b\sqrt{d}$ with $a, b > 0$. Let $E = F(\sqrt{-1})$. One takes the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$ inside E. Let H_L be the ring class field corresponding to the order L.

PROPOSITION 3.1. *Suppose one of the following conditions holds:*

(1) *$x^2+y^2=\varepsilon$ has an integral solution in $\mathfrak{o}_F$.*
(2) *$x^2+y^2=\varepsilon$ has no local integral solutions at a place of F.*

Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.

Proof. Let $\mathfrak{p}$ be a place of F, and $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L inside $E_\mathfrak{p} = E \otimes_F F_\mathfrak{p}$. Since the ring class field K_L of the order L corresponds to

the open subgroup $E^*(\prod_{\mathfrak{p}\le\infty} L_{\mathfrak{p}}^{\times})$ of $\mathbb{I}_E$ by class field theory, the natural group homomorphism

$$\widetilde{\lambda}_E : T(\mathbb{A}_F)/T(F)\prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) \to \mathbb{I}_E/E^*\prod_{\mathfrak{p}\le\infty} L_p^{\times}$$

is well-defined. By Proposition 1.2, we only need to show $\widetilde{\lambda}_E$ is injective.

Suppose there are

$$\beta \in E^* \quad \text{and} \quad i \in E_\infty^* \prod_{\mathfrak{p}<\infty} L_{\mathfrak{p}}^{\times}$$

such that $\beta i \in T(\mathbb{A}_E)$. Then

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

and

$$N_{E/F}(\beta) \in F^* \cap \prod_{\mathfrak{p}<\infty} \mathfrak{o}_{F_{\mathfrak{p}}}^{\times} = \{\pm\varepsilon^n\}.$$

Since $N_{E/F}(\beta)$ is totally positive, we have $N_{E/F}(\beta) = \varepsilon^n$.

When n is even, let $\gamma = \beta\varepsilon^{n/2}, j = i\varepsilon^{-n/2}$. Then $\beta i = \gamma j$ and $N_{E/F}(\gamma) = N_{E/F}(j) = 1$, so

$$\gamma \in T(F) \quad \text{and} \quad j \in \prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

Hence $\beta i = \gamma j \in T(F)\prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$.

When n is odd, we have $N_{E/F}(i) = \varepsilon^{-n}$. That is, $x^2 + y^2 = \varepsilon^{-n}$ has integral solutions at every local place of F. Since n is odd and $\varepsilon \in \mathfrak{o}_F^{\times}$, $x^2 + y^2 = \varepsilon$ has integral solutions at every place of F. By assumption, this equation has an integral solution (x_0, y_0) in $\mathfrak{o}_F$. Let $\zeta = x_0 + y_0\sqrt{-1}$ and $\gamma = \beta\varepsilon^{(n-1)/2}\zeta$, $j = i\varepsilon^{(1-n)/2}\zeta^{-1}$. Then $\beta i = \gamma j$, and $N_{E/F}(\gamma) = N_{E/F}(j) = 1$, so

$$\gamma \in T(F) \quad \text{and} \quad j \in \prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

Hence $\beta i = \gamma j \in T(F)\prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. Therefore $\widetilde{\lambda}_E$ is injective. ∎

In the following, we consider the case that d is a prime number.

LEMMA 3.2. *Let p be a prime and $F = \mathbb{Q}(\sqrt{p})$. Let ε be the fundamental unit of $\mathfrak{o}_F$ and $\varepsilon = a + b\sqrt{p}$ with $a, b > 0$. Then there is a place $\mathfrak{p}$ of F such that the equation $x^2 + y^2 = \varepsilon$ is not solvable over $\mathfrak{o}_{F_{\mathfrak{p}}}$.*

Proof. If $p \equiv 1 \bmod 4$ or $p = 2$, then $x^2 - py^2 = -1$ has integral solutions by Proposition 2.2. Therefore $N_{F/\mathbb{Q}}(\varepsilon) = -1$. There exists a real place $\mathfrak{p}$ of F such that $|\varepsilon|_{\mathfrak{p}} < 0$. So the equation $x^2 + y^2 = \varepsilon$ is not solvable at $\mathfrak{p}$.

If $p \equiv 3 \bmod 4$, then $x^2 - py^2 = -1$ is not solvable over $\mathbb{Z}$ by Proposition 2.2. Therefore $N_{F/\mathbb{Q}}(\varepsilon) = 1$ and ε is totally positive. Moreover, one

of the equations $x^2 - py^2 = \pm 2$ has an integral solution (x_0, y_0) in $\mathbb{Z}$ by Proposition 2.2. It is easy to see that x_0 and y_0 are odd. Let

$$A = (x_0^2 + py_0^2)/2 \quad \text{and} \quad B = x_0 y_0.$$

Since x_0, y_0 are odd, we see that A, B are integers and B is odd. Moreover,

$$A^2 - pB^2 = (x_0^2 - py_0^2)^2/4 = 1.$$

Let $\varepsilon_1 = A + B\sqrt{p}$. Obviously ε_1 is totally positive and $\varepsilon_1 = \varepsilon^m$ for some $m \in \mathbb{Z}$.

Let $\mathfrak{p}$ be the unique place of F over 2. Assume the equation $x^2 + y^2 = \varepsilon$ is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$. Since $\varepsilon_1 = \varepsilon^m$, the equation $x^2 + y^2 = \varepsilon_1$ is also solvable over $\mathfrak{o}_{F_\mathfrak{p}}$. For any solution $(x_1, y_1) = (a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p})$ of the latter, we have

$$(a_1 + b_1\sqrt{p})^2 + (a_2 + b_2\sqrt{p})^2 = A + B\sqrt{p}.$$

Then

$$2a_1 b_1 + 2a_2 b_2 = B.$$

However, B is odd, a contradiction. ∎

From Proposition 3.1 and Lemma 3.2, we obtain the following result.

THEOREM 3.3. *Let p be a prime number and $F = \mathbb{Q}(\sqrt{p})$. Let H_L be the ring class field corresponding to the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Then the diophantine equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.*

Now we use Theorem 3.3 to give an explicit example. Let $F = \mathbb{Q}(\sqrt{17})$. Write $N_{F/\mathbb{Q}}(\alpha) = 2^{s_1} 17^{s_2} p_1^{e_1} \cdots p_g^{e_g}$ for any $\alpha \in \mathfrak{o}_F$. Let $D(n) = \{p_1, \ldots, p_g\}$ and $h(x) = x^4 - 2x^2 + 17$. Denote

$$D_1 = \left\{ p \in D(n) : \left(\frac{-17}{p}\right) = -\left(\frac{-1}{p}\right) = 1 \right\},$$

$$D_2 = \left\{ p \in D(n) : \left(\frac{-17}{p}\right) = \left(\frac{-1}{p}\right) = 1 \right.$$
$$\left. \text{and } h(x) \equiv 0 \bmod p \text{ is not solvable} \right\}.$$

We can see that e_i is even if $p_i \in D_1$.

EXAMPLE 3.4. Let $F = \mathbb{Q}(\sqrt{17})$ and let α be an integer in F. With the above notation, $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if

(1) $x^2 + y^2 = \alpha$ has integral solutions at every place of F,
(2) $s_1 + \sum_{p_i \in D_1} e_i/2 + \sum_{p_i \in D_2} e_i \equiv 0 \bmod 2$.

Acknowledgements. The author would like to thank Fei Xu and Chungang Ji for many helpful discussions, and the referee for his/her valuable comments. The work is supported by the Morningside Center of Mathematics and NSFC, grant # 10901150 and # 10671104.

References

[1] D. Harari, *Le défaut d'approximation forte pour les groupes algébriques commutatifs*, Algebra Number Theory 2 (2008), 595–611.
[2] J. S. Milne, *Algebraic Geometry*, World Sci., 1998.
[3] T. Nagell, *On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields*, Nova Acta Soc. Sci. Upsal. (4) 15 (1953), no. 11, 77 pp.
[4] —, *On the sum of two integral squares in certain quadratic fields*, Ark. Mat. 4 (1961), 267–286.
[5] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. 48 (1940), 405–417.
[6] D. S. Wei and F. Xu, *Integral points for multi-norm tori*, arXiv:1004.2608.
[7] —, —, *Integral points for groups of multiplicative type*, arXiv:1004.2613.
[8] H. Yokoi, *Solvability of Diophantine equation $x^2 - Dy^2 = \pm 2$ and new invariants for real quadratic fields*, Nagoya Math. J. 134 (1994), 137–149.

Dasheng Wei
Academy of Mathematics and System Science
CAS
Beijing 100190, P.R. China
E-mail: dshwei@amss.ac.cn

Received on 25.10.2009
and in revised form on 28.6.2010 (6188)