On the set of integral solutions of the Pell equation in number fields

Wolfgang A. Schmid*
Institut für Mathematik, Karl-Franzens-Universität Graz
Heinrichstraße 36, 8010 Graz, Austria
wolfgang.schmid@uni-graz.at

Abstract

We investigate the set of integral solutions, over a given number field, of the equation $X^2 - dY^2 = 1$, where d denotes some non-zero integer of this field. We define an operation on this set such that it is an abelian group and determine the structure of this abelian group in terms of the number of complex and real embeddings of the number field, and the number of positive embeddings of d.

Mathematics Subject Classification (2000): 11D09, 11R27
Keywords: Pell equation, Dirichlet's theorem
Abbreviated title: On the Pell equation in number fields

1 Introduction and main result

We want to investigate the set of integral solutions of equations of Pell type

$$X^2 - dY^2 = 1, \tag{$\dagger$}$$

over a given number field K, where d denotes a non-zero algebraic integer of K. Our investigations are motivated by a result of P. Shastri [2, Theorem 1.1] (also cf. Remark 4.2) on integral solutions of the circle equation, that is, ($\dagger$) in the special case $d = -1$. In fact, the methods and results of [2] are, with small modifications, sufficient to establish our result (Theorem 3). For a survey of investigations on Pell type equations in number fields cf. Note 12 to Chapter 9 in [1].

The aim of this paper is to investigate the following set.

Definition 1. For a number field K with ring of integers $\mathcal{O}_K$ and $d \in \mathcal{O}_K \setminus \{0\}$ let

$$C_K^d = \{(x, y) \in \mathcal{O}_K^2 \mid x^2 - dy^2 = 1\}.$$

*Supported by the Austrian Science Fund FWF (Project P16770-N12).

For $(x_1, y_1), (x_2, y_2) \in C_K^d$ let the operation $\times$ be defined via

$$(x_1, y_1) \times (x_2, y_2) = (x_1x_2 + dy_1y_2, x_2y_1 + x_1y_2).$$

We start with a simple lemma on the set C_K^d.

Lemma 2. *Let K be a number field and $d \in \mathcal{O}_K \setminus \{0\}$. Then $(C_K^d, \times)$ is an abelian group.*

Proof. Let $(x_1, y_1), (x_2, y_2) \in C_K^d$. First, we note that

$$(x_1x_2 + dy_1y_2)^2 - d(x_2y_1 + x_1y_2)^2 = x_1^2(x_2^2 - dy_2^2) - dy_1^2(x_2^2 - dy_2^2) = 1.$$

Therefore, C_K^d is closed under the operation $\times$. Clearly, $\times$ is commutative and a direct calculation shows that $\times$ is associative. The neutral element is $(1, 0)$ and the inverse of (x_1, y_1) is given by $(x_1, -y_1)$. □

Our aim is to describe the structure of C_K^d as abelian group. This is done in Theorem 3. First, we recall resp. introduce some notation (cf. [1, Chapter 2.1]). Let K be a number field. Then r_1 denotes the number of real embeddings and r_2 the number of conjugated pairs of complex embeddings. For $a \in K \setminus \{0\}$ let $\rho(a) \in \{0, \dots, r_1\}$ denote the number of real embeddings F_i for which $F_i(a) > 0$, that is, $\rho(a) = (\sum_{i=1}^{r_1} 1 + \epsilon_i(a))/2$ where $(\epsilon_1, \dots, \epsilon_{r_1}) = \mathrm{Sgn}(a)$ is the image of a under the signature map.

For an integral domain R let $R^\times$ denote its group of (multiplicative) units. For j a positive integer let C_j denote the cyclic group with j elements.

Theorem 3. *Let K be a number field and $d \in \mathcal{O}_K \setminus \{0\}$. Then*

$$C_K^d \cong \begin{cases} C_j \times \mathbb{Z}^{\rho(d)+r_2} & \text{if } \sqrt{d} \notin K \\ C_j \times \mathbb{Z}^{r_1+r_2-1} & \text{if } \sqrt{d} \in K \end{cases},$$

where $j = 4$ if $\sqrt{-d} \in \mathcal{O}_K^\times$, and $j = 2$ otherwise.

Remark 4. The theorem contains several interesting special cases.

1. For $K = \mathbb{Q}$ we have $r_1 = 1$ and $r_2 = 0$. Thus, we get the well known result that $X^2 - dY^2 = 1$ has non-trivial solutions in $\mathbb{Z}$ if and only if $d > 0$, that is, $\rho(d) > 0$ and d is not a square in $\mathbb{Z}$.

2. For $d = -1$ we get Theorem 1.1 of [2], the starting point of our investigations, which also provided the pattern for the proof of Theorem 3 (cf. Section 1),

$$C_K^{-1} \cong \begin{cases} C_4 \times \mathbb{Z}^{r_2} & \text{if } \sqrt{-1} \notin K \\ C_4 \times \mathbb{Z}^{r_2-1} & \text{if } \sqrt{-1} \in K \end{cases},$$

since $\rho(-1) = 0$, $\sqrt{-(-1)} \in \mathcal{O}_K^\times$, and if $\sqrt{-1} \in K$, then the field K has no real embeddings.

3. For $d \in \mathbb{Z} \setminus \{-1, 0\}$ we have

$$C_K^d \cong \begin{cases} C_2 \times \mathbb{Z}^{r_2} & \text{if } d < -1 \text{ and } \sqrt{d} \notin K \\ C_2 \times \mathbb{Z}^{r_1+r_2} & \text{if } d > 0 \text{ and } \sqrt{d} \notin K \\ C_2 \times \mathbb{Z}^{r_1+r_2-1} & \text{if } d \neq 1 \text{ and } \sqrt{d} \in K \\ C_2 \times \mathbb{Z}^{r_1+r_2-1} & \text{if } d = 1 \text{ and } \sqrt{-1} \notin K \\ C_4 \times \mathbb{Z}^{r_2-1} & \text{if } d = 1 \text{ and } \sqrt{-1} \in K \end{cases},$$

since $\sqrt{-d} \in \mathcal{O}_K^\times$ implies $d = 1$, and $\rho(d) = r_1$ or $\rho(d) = 0$ holds according as d is positive or negative.

2 Auxiliary results

We establish two lemmata. First, we prove that C_K^d is isomorphic to a certain subgroup of $\mathcal{O}_K[\sqrt{d}]^\times$. This will allow us to use tools from algebraic number theory to investigate the structure of C_K^d.

Lemma 5. *Let K be a number field and $d \in \mathcal{O}_K \setminus \{0\}$. Then the map*

$$\Phi_K^d : \begin{cases} C_K^d & \to \mathcal{O}_k[\sqrt{d}] \\ (x, y) & \mapsto x + \sqrt{d}y \end{cases},$$

is injective and induces an isomorphism of the abelian groups $(C_K^d, \times)$ and $U = \{u \in \mathcal{O}_K[\sqrt{d}]^\times \mid \frac{u+u^{-1}}{2} \in \mathcal{O}_K \text{ and } \frac{u-u^{-1}}{2\sqrt{d}} \in \mathcal{O}_K\}$.

Proof. Let $u \in \Phi_K^d(C_K^d)$. Then $u = x+\sqrt{d}y$ with $x, y \in \mathcal{O}_K$. From the definition of C_K^d we get that $(x+\sqrt{d}y)(x-\sqrt{d}y) = x^2 - dy^2 = 1$. Therefore, $u \in \mathcal{O}_K[\sqrt{d}]^\times$ and $u^{-1} = x - \sqrt{d}y$. Furthermore, we have

$$\frac{u + u^{-1}}{2} = x \in \mathcal{O}_K \text{ and } \frac{u - u^{-1}}{2\sqrt{d}} = y \in \mathcal{O}_K,$$

and thus $\Phi_K^d(C_K^d) \subset U$.

Conversely, for every $u \in U$ we get $(\frac{u+u^{-1}}{2})^2 - d(\frac{u-u^{-1}}{2\sqrt{d}})^2 = 1$. Let

$$\Psi : \begin{cases} U & \to C_K^d \\ u & \mapsto (\frac{u+u^{-1}}{2}, \frac{u-u^{-1}}{2\sqrt{d}}) \end{cases}.$$

Then $\Psi \circ \Phi_K^d$ is the identity on C_K^d and $\Phi_K^d \circ \Psi$ the identity on U. Thus, Φ_K^d is injective and $\Phi_K^d : C_K^d \to U$ is bijective. Via direct calculation we see

$$\Phi_K^d((x_1, y_1) \times (x_2, y_2)) = \Phi_K^d((x_1, y_1))\Phi_K^d((x_2, y_2)).$$

Thus, C_K^d and U are isomorphic. □

Lemma 6. *Let K be a number field of degree n and let $d \in \mathcal{O}_K$ with $\sqrt{d} \notin K$. Further, let $L = K(\sqrt{d})$. Then $\mathcal{O}_K[\sqrt{d}]$ is an order of L and* $\operatorname{rank}(\mathcal{O}_K[\sqrt{d}]^\times) = \operatorname{rank}(\mathcal{O}_L^\times)$. *In particular,*

$$\operatorname{rank}(\mathcal{O}_K[\sqrt{d}]^\times) = \rho(d) + n - 1.$$

Proof. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of $\mathcal{O}_K$. As $[L : \mathbb{Q}] = 2n$ and

$$\{\omega_1, \ldots, \omega_n, \sqrt{d}\omega_1, \ldots, \sqrt{d}\omega_n\} \subset \mathcal{O}_K[\sqrt{d}]$$

is $\mathbb{Q}$-independent, $\mathcal{O}_K[\sqrt{d}]$ is an order of L. Therefore, by [2, Lemma 1.1], we have $\operatorname{rank}(\mathcal{O}_K[\sqrt{d}]^\times) = \operatorname{rank}(\mathcal{O}_L^\times)$.

Let $F : K \to \mathbb{C}$ be an embedding of K. It can be extended in two ways F' and F'' to an embedding of L. Clearly, if F is complex, then F' and F'' are complex. Moreover, if F is real and $F(d) < 0$, then again F' and F'' are complex. However, if F is real and $F(d) > 0$, then F' and F'' are real.

Thus, L has $2\rho(d)$ real and $2(n - \rho(d))$ complex embeddings. Using Dirichlet's unit theorem (see for example [1, Theorem 3.6]) for $\mathcal{O}_L$, the result follows immediately. □

3 Proof of the main result

Now we are ready to prove Theorem 3.

Proof of Theorem 3. We have already established that Φ_K^d is an isomorphism of abelian groups. Therefore, it suffices to investigate $\Phi_K^d(C_k^d)$. First, we prove the result on the rank and then establish the result on the torsion elements.

1. If $\sqrt{d} \notin K$, we consider the relative norm map $\mathcal{N}_{L/K}$, where $L = K(\sqrt{d})$. This leads to the following homomorphism of abelian groups:

$$\mathcal{N}'_{L/K} : \begin{cases} \mathcal{O}_K[\sqrt{d}]^\times & \to \mathcal{O}_K^\times \\ x + \sqrt{d}y & \mapsto (x + \sqrt{d}y)(x - \sqrt{d}y) \end{cases}.$$

   From this it follows immediately that

$$\Phi_K^d(C_K^d) = \ker \mathcal{N}'_{L/K}.$$

   As $(\mathcal{O}_K^\times)^2 \subset \operatorname{im} \mathcal{N}'_{L/K}$ and using Dirichlet's unit theorem again, we get $\operatorname{rank}(\operatorname{im} \mathcal{N}'_{L/K}) = \operatorname{rank}(\mathcal{O}_K^\times) = r_1 + r_2 - 1$. Consequently, as

$$\operatorname{rank}(\mathcal{O}_K[\sqrt{d}]^\times) = \operatorname{rank}(\operatorname{im} \mathcal{N}'_{L/K}) + \operatorname{rank}(\ker \mathcal{N}'_{L/K}),$$

   we get, using Lemma 6, that

$$\operatorname{rank}(\ker \mathcal{N}'_{L/K}) = \rho(d) + r_2.$$

2. If $\sqrt{d} \in K$, then $\mathcal{O}_K[\sqrt{d}] = \mathcal{O}_K$. Therefore, we know

$$\begin{aligned}\Phi_K^d(C_K^d) &= \{u \in \mathcal{O}_K^\times \mid \frac{u+u^{-1}}{2} \in \mathcal{O}_K \text{ and } \frac{u-u^{-1}}{2\sqrt{d}} \in \mathcal{O}_K\} \\ &= \{u \in \mathcal{O}_K^\times \mid u^2 \in 1 + 2\sqrt{d}\mathcal{O}_K\}.\end{aligned}$$

This means that $\Phi_K^d(C_K^d)$ is equal to the kernel of the map

$$\eta : \begin{cases} \mathcal{O}_K^\times & \to (\mathcal{O}_K/2\sqrt{d}\mathcal{O}_K)^\times \\ u & \mapsto u^2 + 2\sqrt{d}\mathcal{O}_K \end{cases}.$$

Since $(\mathcal{O}_K/2\sqrt{d}\mathcal{O}_K)^\times$ is finite, we get

$$\operatorname{rank}(\ker \eta) = \operatorname{rank}(\mathcal{O}_K^\times) = r_1 + r_2 - 1.$$

Next, we establish the result concerning torsion elements. This means we need to determine for which elements of finite order (roots of unity) $\zeta \in \mathcal{O}_K[\sqrt{d}]^\times$

$$\frac{\zeta+\zeta^{-1}}{2} \in \mathcal{O}_K \text{ and } \frac{\zeta-\zeta^{-1}}{2\sqrt{d}} \in \mathcal{O}_K$$

holds. We know that $\frac{\zeta+\zeta^{-1}}{2} \in \mathcal{O}_K$ if and only if $\zeta^4 = 1$ (cf. [2, Proof of the main theorem]). Obviously, for $\zeta = \pm 1$ we have $\frac{\zeta-\zeta^{-1}}{2\sqrt{d}} \in \mathcal{O}_K$. It remains to consider $\zeta = \pm\sqrt{-1}$.

Let $\zeta = \sqrt{-1}$. We need to check whether

$$\frac{\sqrt{-1}}{\sqrt{d}} \in \mathcal{O}_K. \tag{‡}$$

We note that (‡) implies $d \in \mathcal{O}_K^\times$. Thus, (‡) is equivalent to $\sqrt{-d} \in \mathcal{O}_K^\times$. Since the same argument holds for $\zeta = -\sqrt{-1}$, the result concerning torsion elements is established. □

Acknowledgement

The author thanks the referees for their suggestions. In particular, for the advice to extend the considerations from "d a rational integer" to "d an algebraic integer."

References

[1] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers, Second Edition.* Springer-Verlag, Berlin, 1990.

[2] P. Shastri. Integral points on the unit circle. *J. Number Theory*, 91 (2001), no. 1, 67–70.