JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

András BIRÓ

On the class number of pairs of binary quadratic forms

Tome 37, nº 3 (2025), p. 897-924.

https://doi.org/10.5802/jtnb.1346

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **37** (2025), 897–924

On the class number of pairs of binary quadratic forms

par András BIRÓ

Résumé. Pour $d_1, d_2, t \in \mathbb{Z}$, soit $h(d_1, d_2, t)$ le nombre de $\mathrm{SL}_2(\mathbb{Z})$-classes d'équivalence des couples (Q_1, Q_2) de formes quadratiques à coefficients entiers tels que le discriminant de Q_i est d_i, et le codiscriminant de Q_1 et Q_2 est t. On donne une formule explicite pour $h(d_1, d_2, t)$ en supposant que d_i n'est pas un carré parfait $(i = 1, 2)$, et $t^2 - d_1 d_2 \neq 0$. Auparavant, de telles formules n'étaient connues que sous certaines conditions de coprimalité.

Abstract. If $d_1, d_2, t \in \mathbb{Z}$, let $h(d_1, d_2, t)$ be the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of pairs (Q_1, Q_2) of quadratic forms with integer coefficients satisfying that the discriminant of Q_i is d_i, and the codiscriminant of Q_1 and Q_2 is t. We give an explicit formula for $h(d_1, d_2, t)$ assuming that d_i is not a square of an integer $(i = 1, 2)$, and $t^2 - d_1 d_2 \neq 0$. Previously such formulas were known only under some coprimality conditions.

1. Introduction

1.1. Basic definitions and motivation. If $\tau = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and Q is a quadratic form, let us define the quadratic form Q^τ by $Q^\tau(X, Y) = Q(aX + bY, cX + dY)$. For $d_1, d_2, t \in \mathbb{Z}$, let $Q_{d_1,d_2,t}$ be the set of pairs (Q_1, Q_2) of quadratic forms

$$\begin{aligned} Q_1(X, Y) &= A_1 X^2 + B_1 XY + C_1 Y^2, \\ Q_2(X, Y) &= A_2 X^2 + B_2 XY + C_2 Y^2 \end{aligned} \tag{1.1}$$

with integer coefficients A_i, B_i, C_i satisfying

$$B_1^2 - 4A_1C_1 = d_1,\ B_2^2 - 4A_2C_2 = d_2,\ B_1B_2 - 2A_1C_2 - 2A_2C_1 = t. \tag{1.2}$$

Here d_1 and d_2 are the discriminants of Q_1 and Q_2, respectively, and t is called the codiscriminant of the pair (Q_1, Q_2).

Manuscrit reçu le 1er juillet 2024, révisé le 25 janvier 2025, accepté le 24 février 2025.

2020 *Mathematics Subject Classification.* 11D09, 11E41.

Mots-clefs. class number of pairs of quadratic forms, Hilbert symbol.

Research partially supported by the NKFIH (National Research, Development and Innovation Office) Grants No. K135885, K143876, and by the MTA HUN-REN RI Lendület Automorphic Research Group.

It is easy to check that if $\tau \in \mathrm{SL}_2(\mathbb{Z})$, and $(Q_1, Q_2) \in Q_{d_1,d_2,t}$, then $(Q_1^\tau, Q_2^\tau) \in Q_{d_1,d_2,t}$. Hence $\mathrm{SL}_2(\mathbb{Z})$ acts on $Q_{d_1,d_2,t}$. Let us denote by $h(d_1, d_2, t)$ the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of $Q_{d_1,d_2,t}$.

Our motivation to study this class number is that it appeared in our recent paper [1] in a formula which expresses the inner product of two automorphic functions, see [1, Lemma 2.1]. Conjugacy classes of pairs of elements of the modular group occur in [1], such pairs correspond to pairs of quadratic forms, this leads us to the class numbers studied here.

In the papers [2] and [3] explicit formulas were given for $h(d_1, d_2, t)$, but only under such coprimality conditions for the parameters which are not satisfied in [1, Lemma 2.1]. An explicit formula without those conditions might be useful, as was mentioned already in [1]. This motivates our present study.

We note that a general upper bound for $h(d_1, d_2, t)$ was proved in [1, Lemma 3.1]. Some parts of the proof of that upper bound are used also in the present paper, but for the sake of completeness we prove everything here. The present paper is independent of automorphic functions, the methods here are elementary.

1.2. Necessary notations and statement of the main result. If p is a prime, let $\mathbb{Q}_p$ be the field of p-adic numbers and let $\mathbb{Z}_p$ be the ring of p-adic integers. If $0 \neq x \in \mathbb{Q}_p$, then let $\nu_p(x) \in \mathbb{Z}$ be such that $xp^{-\nu_p(x)}$ is a p-adic unit, and let $\nu_p(0) = \infty$.

If p is a given prime and $a, b \in \mathbb{Q}_p \backslash \{0\}$, define the Hilbert symbol $(a, b)_p$ in the following way. Let us take $(a, b)_p = 1$ if the equation $z^2 - ax^2 - by^2 = 0$ has a solution $(z, x, y) \neq (0, 0, 0)$ in $\mathbb{Q}_p^3$, and let $(a, b)_p = -1$ otherwise (see [4, Chapter 3]).

If p is a prime, $d \in \mathbb{Z}$, let $s_p(d) = 1$ if d is a square in $\mathbb{Q}_p$, and let $s_p(d) = 0$ otherwise. If $d \in \mathbb{Z}$, then let

$$c(d) := \begin{cases} 0, & \text{if } \nu_2(d) \text{ is even, } \frac{d}{2^{\nu_p(d)}} \equiv 1 \bmod 4, \\ 1, & \text{if } \nu_2(d) \text{ is even, } \frac{d}{2^{\nu_p(d)}} \equiv 3 \bmod 4, \\ 2, & \text{if } \nu_2(d) \text{ is odd.} \end{cases}$$

If c is an integer and $d > 0$ is an odd integer, then let $(\frac{c}{d})$ be the Jacobi symbol. For a real number r let $\lceil r \rceil$ be the least integer not smaller than r.

Let us fix $d_1, d_2, t \in \mathbb{Z}$, we do not denote the dependence on them in the following notations. If p is a prime, let us choose $d_{0,p} \in \{d_1, d_2\}$ such that $\nu_p(d_{0,p}) = \min(\nu_p(d_1), \nu_p(d_2))$, and let $\delta_p = \frac{d_{0,p}}{p^{m_p}}$, where

$$m_p := \min(\nu_p(d_1), \nu_p(d_2), \nu_p(t)).$$

Let $\epsilon_p = 1$ if m_p is even, $\epsilon_p = 0$ otherwise.

If $p > 2$, let $h_p(d_1, d_2, t)$ be

$$(1 + (d_2, t^2 - d_1 d_2)_p) \sum_{0 \le \alpha < \lceil m_p/2 \rceil} p^\alpha + \epsilon_p p^{m_p/2} \sum_{\beta=0}^{\nu_p(t^2 - d_1 d_2) - 2m_p} \left(\frac{\delta_p}{p^\beta}\right).$$

To define $h_2(d_1, d_2, t)$ we need some more notation. Write

$$M := \max(\nu_2(d_1), \nu_2(d_2)),$$

and let

$$A := \begin{cases} \min(\nu_2(d_1) - c(d_1), \nu_2(d_2) - c(d_2)), \\ \qquad\qquad \text{if } \nu_2(d_1) = \nu_2(d_2) = \nu_2(t), \\ \min(\nu_2(d_1) - c(d_1), \nu_2(d_2) - c(d_2), M - 1, \nu_2(t) - 1), \\ \qquad\qquad \text{otherwise,} \end{cases}$$

$$\epsilon := \begin{cases} 1, & \text{if } \nu_2(d_1) = \nu_2(d_2) = \nu_2(t),\ s_2(d_1) = s_2(d_2) = 1, \quad (1.3) \\ 1, & \text{if } \nu_2(d_{0,2}) + 2 \le M,\ \nu_2(d_{0,2}) + 1 \le \nu_2(t),\ s_2(d_{0,2}) = 1, \quad (1.4) \\ 0, & \text{otherwise.} \end{cases}$$

Then let $h_2(d_1, d_2, t)$ be

$$(1 + (d_2, t^2 - d_1 d_2)_2) \left(\sum_{0 \le \alpha \le A} 2^{\alpha - \lceil \alpha/2 \rceil} + \epsilon 2^{m_2/2} (\nu_2(t^2 - d_1 d_2) - 2m_2 - 2) \right).$$

It is easy to see that $h_p(d_1, d_2, t)$ is well-defined, i.e. it is independent of the choice of $d_{0,p}$ in the case $\nu_p(d_1) = \nu_p(d_2)$. It is trivial for $p = 2$, but we will show it also for $p > 2$ in Section 5.

Theorem 1.1. *Assume that $d_1, d_2, t \in \mathbb{Z}$, and d_i is not a square of an integer $(i = 1, 2)$. Assume also that $t^2 - d_1 d_2 \neq 0$ and $4 | t^2 - d_1 d_2$. Then we have*

$$h(d_1, d_2, t) = \prod_{p | t^2 - d_1 d_2} h_p(d_1, d_2, t). \quad (1.5)$$

1.3. Outline of the paper. The basis of the proof is the simple observation that if (1.2) holds, then we have

$$d_2 A_1^2 + d_1 A_2^2 - 2t A_1 A_2 = (A_1 B_2 - A_2 B_1)^2.$$

Hence if $Q_{d_1, d_2, t} \neq \emptyset$, then the equation $d_2 x^2 + d_1 y^2 - 2txy = z^2$ has a nontrivial solution (x, y, z) in integers. So we can assume that there is such a solution, otherwise $h(d_1, d_2, t) = 0$. It can be shown (see Lemma 3.1) that if we fix a nontrivial primitive solution (x, y, z), then in every $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of $Q_{d_1, d_2, t}$ there is an element (Q_1, Q_2) of the form (1.1) such that $A_1 = rx$, $A_2 = ry$ where r is a divisor of $t^2 - d_1 d_2$. Then the goal of determining $h(d_1, d_2, t)$ is reduced in Section 3 to count the possible

pairs (Q_1, Q_2) with given A_1 and A_2, fixing B_1 modulo $2|A_1|$. This leads to the problem of counting the number of solutions of certain systems of congruences, see Lemma 3.4. This is solved in Section 4 by elementary but tedious local calculations. To prepare the proof of Lemma 3.1 we analyze the rational and p-adic points on the quadratic curve $d_2x^2+d_1y^2-2txy=1$ in Section 2. The results of Section 2 are also used in Section 5, where we complete the proof of Theorem 1.1. The proofs are elementary, only basic properties (including the Hasse–Minkowski Theorem) of the Hilbert symbol are used.

2. On a quadratic curve

2.1. Some identities. In the next lemma we collected together some identities needed later. Some of them will be used only in Section 3.

Lemma 2.1. *Let K be a field such that $\mathbb{Q} \subseteq K$ and let $d_1, d_2, t \in K$. Let $A_i, B_i, C_i \in K$ for $i = 1, 2$ such that* (1.2) *holds. Define $Q_1(X, Y)$ and $Q_2(X, Y)$ by the formula* (1.1)*, and let*

$$R(X,Y) = (A_1B_2 - A_2B_1)X^2 + 2XY(A_1C_2 - A_2C_1) + Y^2(B_1C_2 - B_2C_1). \tag{2.1}$$

Then we have the identities

$$d_2(Q_1(X,Y))^2 + d_1(Q_2(X,Y))^2 - 2tQ_1(X,Y)Q_2(X,Y) = (R(X,Y))^2, \tag{2.2}$$

$$d_2A_1^2 + d_1A_2^2 - 2tA_1A_2 = (A_1B_2 - A_2B_1)^2, \tag{2.3}$$

$$(A_1C_2 - A_2C_1)^2 - (A_1B_2 - A_2B_1)(B_1C_2 - B_2C_1) = \frac{t^2 - d_1d_2}{4}, \tag{2.4}$$

and writing

$$a := A_1C_2 - A_2C_1, \quad b := A_2B_1 - A_1B_2 \tag{2.5}$$

we have

$$Q_1(a,b) = A_1\frac{t^2 - d_1d_2}{4}, \quad Q_2(a,b) = A_2\frac{t^2 - d_1d_2}{4}, \tag{2.6}$$

$$R(a,b) = -(A_1B_2 - A_2B_1)\frac{t^2 - d_1d_2}{4}. \tag{2.7}$$

If $\tau = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and

$$\begin{aligned} Q_1^\tau(X,Y) &= A_1^*X^2 + B_1^*XY + C_1^*Y^2, \\ Q_2^\tau(X,Y) &= A_2^*X^2 + B_2^*XY + C_2^*Y^2, \end{aligned} \tag{2.8}$$

then we have

$$A_1^* = Q_1(\alpha,\beta), \quad A_2^* = Q_2(\alpha,\beta), \quad B_2^*A_1^* - B_1^*A_2^* = R(\alpha,\beta). \tag{2.9}$$

Proof. Every statement can be checked by direct computations. The lemma is proved. □

2.2. Parametrization of a quadratic curve. If $d_1, d_2, t \in \mathbb{Z}$ and K is a field such that $\mathbb{Q} \subseteq K$, introduce the notation

$$C_{d_1,d_2,t}(K) := \Big\{(x,y) \in K^2 : \ d_2x^2 + d_1y^2 - 2txy = 1\Big\}. \tag{2.10}$$

Lemma 2.2. *Let d_1, d_2, t be as in Theorem 1.1. Let $A_i, B_i, C_i \in \mathbb{Q}$ for $i = 1, 2$ such that (1.2) is true. Assume that $A_1B_2 - A_2B_1 \neq 0$. Let K be a field such that $\mathbb{Q} \subseteq K$. Introduce the abbreviations*

$$a_1 = \frac{A_1}{A_1B_2 - A_2B_1}, \quad a_2 = \frac{A_2}{A_1B_2 - A_2B_1}. \tag{2.11}$$

Recall the notations (1.1) and (2.1). If $a, b \in K$ are such that $R(a,b) \neq 0$, then write $x_{a,b} := \frac{Q_1(a,b)}{R(a,b)}$, $y_{a,b} := \frac{Q_2(a,b)}{R(a,b)}$.

(i) *Let $a, b \in K$ be such that $R(a,b) \neq 0$. If $(x_{a,b}, y_{a,b}) = (a_1, a_2)$, then we have $b = 0$. $(x_{a,b}, y_{a,b}) = (-a_1, -a_2)$, then we have $a = \lambda(A_1C_2 - A_2C_1)$, $b = \lambda(A_2B_1 - A_1B_2)$ with some nonzero $\lambda \in K$.*

(ii) *For $x, y \in K$ the following two statements are equivalent.*
   (a) *We have $(x,y) \in C_{d_1,d_2,t}(K)$.*
   (b) *There are $a, b \in K$ such that $R(a,b) \neq 0$ and $x = x_{a,b}$, $y = y_{a,b}$.*

Before proving this lemma we need another one.

Lemma 2.3. *Let d_1, d_2, t and K be as in Lemma 2.2, assume that*

$$(x_i, y_i) \in C_{d_1,d_2,t}(K)$$

for $i = 1, 2$ and $(x_1, y_1) \neq (x_2, y_2)$. Then we have

$$S_1 := d_2(x_1 - x_2)^2 + d_1(y_1 - y_2)^2 - 2t(x_1 - x_2)(y_1 - y_2) \neq 0 \tag{2.12}$$

and

$$S_2 := (d_1y_1 - tx_1)(y_1 - y_2) + (d_2x_1 - ty_1)(x_1 - x_2) \neq 0. \tag{2.13}$$

Proof. One can check the identities

$$S_2 = \begin{pmatrix} y_1 & x_1 \end{pmatrix} \begin{pmatrix} d_1 & -t \\ -t & d_2 \end{pmatrix} \begin{pmatrix} y_1 - y_2 \\ x_1 - x_2 \end{pmatrix} \tag{2.14}$$

and

$$2S_2 + \sum_{i=1}^{2} (-1)^i (d_2x_i^2 + d_1y_i^2 - 2tx_iy_i) = S_1.$$

Since $(x_i, y_i) \in C_{d_1,d_2,t}(K)$ for $i = 1, 2$, so $S_1 = 2S_2$. Hence it is enough to show that $S_1 \neq 0$. Assume for a contradiction that $S_1 = 0$. Then the

right-hand side of (2.14) is 0, but this is true also by exchanging the role of (x_1, y_1) and (x_2, y_2), so we get

$$\begin{pmatrix} y_1 & x_1 \\ y_2 & x_2 \end{pmatrix}\begin{pmatrix} d_1 & -t \\ -t & d_2 \end{pmatrix}\begin{pmatrix} y_1 - y_2 \\ x_1 - x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The vector $\left(\begin{smallmatrix} y_1-y_2 \\ x_1-x_2 \end{smallmatrix}\right)$ is nonzero and $\det\left(\begin{smallmatrix} d_1 & -t \\ -t & d_2 \end{smallmatrix}\right) \neq 0$ by $t^2 - d_1 d_2 \neq 0$, so we must have $\det\left(\begin{smallmatrix} y_1 & x_1 \\ y_2 & x_2 \end{smallmatrix}\right) = 0$. Hence $(x_2, y_2) = \lambda(x_1, y_1)$ with some $\lambda \in K$, $\lambda \neq 1$, so $S_1 = (1-\lambda)^2 \neq 0$ by our assumptions. This is a contradiction, the lemma is proved. □

Proof of Lemma 2.2. It is easy to see that if $a, b \in K$, then

$$\begin{pmatrix} Q_1(a,b) - a_1 R(a,b) \\ Q_2(a,b) - a_2 R(a,b) \end{pmatrix} = \frac{b}{A_1 B_2 - A_2 B_1}\begin{pmatrix} a\alpha + b\beta \\ \gamma a + \delta b \end{pmatrix} \tag{2.15}$$

with

$$\alpha := B_1(A_1B_2 - A_2B_1) + 2A_1(A_2C_1 - A_1C_2) = tA_1 - d_1A_2, \tag{2.16}$$

$$\beta := C_1(A_1B_2 - A_2B_1) + A_1(C_1B_2 - C_2B_1), \tag{2.17}$$

$$\gamma := B_2(A_1B_2 - A_2B_1) + 2A_2(A_2C_1 - A_1C_2) = -tA_2 + d_2A_1, \tag{2.18}$$

$$\delta := C_2(A_1B_2 - A_2B_1) + A_2(C_1B_2 - C_2B_1). \tag{2.19}$$

Now, one can compute that

$$\det\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$
$$= 2(A_2B_1 - A_1B_2)((A_1C_2 - A_2C_1)^2 - (A_1B_2 - A_2B_1)(B_1C_2 - B_2C_1)).$$

The last bracket equals $\frac{t^2 - d_1 d_2}{4}$ by (2.4). Hence $t^2 - d_1 d_2 \neq 0$ and $A_1B_2 - A_2B_1 \neq 0$ imply $\det\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \neq 0$. Assume $R(a,b) \neq 0$. If $(x_{a,b}, y_{a,b}) = (a_1, a_2)$, then (2.15) and $\det\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \neq 0$ imply $b = 0$. If $(x_{a,b}, y_{a,b}) = (-a_1, -a_2)$, then (2.15) implies $b \neq 0$, hence from (2.15) we get

$$\begin{pmatrix} a \\ b \end{pmatrix} = \mu\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}\begin{pmatrix} -2a_1 \\ -2a_2 \end{pmatrix}$$

with some nonzero $\mu \in K$. Using (2.11) and

$$\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} A_1C_2 - A_2C_1 \\ A_2B_1 - A_1B_2 \end{pmatrix}$$

we obtain statement (i).

We now turn to (ii). Note that by (2.3) we get $(a_1, a_2) \in C_{d_1,d_2,t}(K)$. We first assume (b). Then (a) follows at once from (2.2).

We now assume (a). If $(x, y) = (a_1, a_2)$, then we can take $a = 1$, $b = 0$. So let us assume that $(x, y) \neq (a_1, a_2)$.

Let us take $a, b \in K$ in the following way:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} x - a_1 \\ y - a_2 \end{pmatrix}. \tag{2.20}$$

By (2.15) and (2.20) we then easily get

$$\begin{pmatrix} Q_1(a,b) - a_1 R(a,b) \\ Q_2(a,b) - a_2 R(a,b) \end{pmatrix} = \frac{b(\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix})}{A_1 B_2 - A_2 B_1} \begin{pmatrix} x - a_1 \\ y - a_2 \end{pmatrix}. \tag{2.21}$$

So this is true if $(x, y) \neq (a_1, a_2)$, and a, b are defined by (2.16)–(2.20).

Assume that $b = 0$. Then by (2.16), (2.18) and (2.20) we get

$$(d_1 A_2 - t A_1)(y - a_2) + (-t A_2 + d_2 A_1)(x - a_1) = 0.$$

By (2.11), $(a_1, a_2), (x, y) \in C_{d_1,d_2,t}(K)$ and $(x, y) \neq (a_1, a_2)$ this contradicts (2.13). So we have $b \neq 0$.

Assume that $R(a, b) = 0$. Then (2.2) and (2.21) imply that

$$d_2(x - a_1)^2 + d_1(y - a_2)^2 - 2t(x - a_1)(y - a_2) = 0.$$

But this contradicts (2.12). So we have $R(a, b) \neq 0$.

Then (2.21) clearly implies

$$\begin{pmatrix} x_{a,b} - a_1 \\ y_{a,b} - a_2 \end{pmatrix} = \frac{b\Big(\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\Big)}{R(a,b)(A_1 B_2 - A_2 B_1)} \begin{pmatrix} x - a_1 \\ y - a_2 \end{pmatrix}.$$

Hence we have $(x_{a,b}, y_{a,b}) \neq (a_1, a_2)$, since we assumed $(x, y) \neq (a_1, a_2)$. We would like to show that $(x, y) = (x_{a,b}, y_{a,b})$. If this is false, then (a_1, a_2), $(x_{a,b}, y_{a,b})$ and (x, y) are three pairwise different points lying on a line and all of these three points belong to $C_{d_1,d_2,t}(K)$. Hence we have that the equation

$$\begin{aligned} d_2(a_1 + q(x - a_1))^2 + d_1(a_2 + q(y - a_2))^2 \\ - 2t(a_1 + q(x - a_1))(a_2 + q(y - a_2)) = 1 \end{aligned} \tag{2.22}$$

has three different solutions $q \in K$. The coefficient of q^2 is nonzero by (2.12), so this is a contradiction. □

2.3. A rational point on the quadratic curve which is prescribed at finitely many places. Our goal here is to prove Lemma 2.5, which will be used in Section 5. We first need a preparatory lemma which is an easy application of Lemma 2.2.

Lemma 2.4. *Let d_1, d_2, t and K be as in Lemma 2.2. Assume that $x_0, y_0, z_0 \in \mathbb{Q}$ are given such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$. Then for $x, y, z \in K$ the following two statements are equivalent.*

(i) *We have $z \neq 0$ and $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(K)$.*

(ii) *There are $c, u, v \in K$ such that $c \neq 0$, $u^2 d_1 z_0 + uv(-2d_1 y_0 + 2tx_0) + v^2 z_0 \neq 0$ and*

$$\begin{aligned} x &= cx_0(u^2 d_1 - v^2), \\ y &= c(u^2(2tx_0 - d_1 y_0) + 2z_0 uv - y_0 v^2), \\ z &= c(u^2 d_1 z_0 + uv(-2d_1 y_0 + 2tx_0) + v^2 z_0). \end{aligned}$$

Proof. This follows at once from Lemma 2.2 (ii) writing

$$\begin{aligned} A_1 &= \frac{d_1}{2}, \qquad B_1 = 0, \quad C_1 = -\frac{1}{2}, \\ A_2 &= t - \frac{d_1 y_0}{2x_0}, \quad B_2 = \frac{z_0}{x_0}, \quad C_2 = -\frac{y_0}{2x_0}. \end{aligned}$$

Note that $x_0 \neq 0$ follows from $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$ and the assumption that d_1 is not a square. □

Lemma 2.5. *Let d_1, d_2, t be as in Lemma 2.2. Assume that $x_0, y_0, z_0 \in \mathbb{Q}$ are given such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$. Let $r \geq 1$, let $p_1, p_2, \ldots, p_r$ be pairwise distinct primes and let $x_i, y_i, z_i \in Z_{p_i}$ for $1 \leq i \leq r$ such that the following conditions are satisfied for every $1 \leq i \leq r$: $z_i \neq 0$, $(\frac{x_i}{z_i}, \frac{y_i}{z_i}) \in C_{d_1,d_2,t}(\mathbb{Q}_{p_i})$ and $\min(\nu_{p_i}(x_i), \nu_{p_i}(y_i)) = 0$. Let $A > 0$ be an integer. Then there are elements $x, y, z \in \mathbb{Z}$ such that $z \neq 0$, $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$, $(x, y) = 1$ and there are p_i-adic units α_i for $1 \leq i \leq r$ such that*

$$\nu_p(x - \alpha_i x_i) \geq A, \quad \nu_p(y - \alpha_i y_i) \geq A, \quad \nu_p(z - \alpha_i z_i) \geq A$$

for $1 \leq i \leq r$.

Proof. We know from Lemma 2.4 that for every $1 \leq i \leq r$ there are $u_i, v_i \in \mathbb{Z}_{p_i}$ and $0 \neq c_i \in \mathbb{Q}_{p_i}$ such that

$$\begin{aligned} x_i &= c_i x_0(u_i^2 d_1 - v_i^2), \\ y_i &= c_i(u_i^2(2tx_0 - d_1 y_0) + 2z_0 u_i v_i - y_0 v_i^2), \\ z_i &= c_i(u_i^2 d_1 z_0 + u_i v_i(-2d_1 y_0 + 2tx_0) + v_i^2 z_0). \end{aligned}$$

Let $B > 0$ be any integer. By the Chinese Remainder Theorem there are elements $u, v \in \mathbb{Z}$ and $0 \neq c \in \mathbb{Q}$ such that

$$\nu_{p_i}(u - u_i) \geq B, \quad \nu_{p_i}(v - v_i) \geq B, \quad \nu_{p_i}(c - c_i) \geq B$$

for $1 \le i \le r$. Let

$$\begin{aligned} x^* &:= cx_0(u^2d_1 - v^2), \\ y^* &:= c(u^2(2tx_0 - d_1y_0) + 2z_0uv - y_0v^2), \\ z^* &:= c(u^2d_1z_0 + uv(-2d_1y_0 + 2tx_0) + v^2z_0). \end{aligned}$$

We have $x^*, y^*, z^* \in \mathbb{Q}$, and if we choose B to be large enough, then we will have

$$\begin{gathered} \nu_{p_i}(x^* - x_i) \ge A, \quad \nu_{p_i}(y^* - y_i) \ge A, \quad \nu_{p_i}(z^* - z_i) \ge A, \\ x^*, y^* \in Z_{p_i}, \quad \min(\nu_{p_i}(x^*), \nu_{p_i}(y^*)) = 0 \end{gathered} \tag{2.23}$$

for $1 \le i \le r$ and we have also $z^* \ne 0$. By Lemma 2.4 we have $(\frac{x^*}{z^*}, \frac{y^*}{z^*}) \in C_{d_1,d_2,t}(\mathbb{Q})$. There is an element $0 \ne \alpha \in \mathbb{Q}$ such that $\alpha x^*, \alpha y^* \in \mathbb{Z}$ and $(\alpha x^*, \alpha y^*) = 1$. It follows from (2.23) that α is a p_i-adic unit for $1 \le i \le r$. Let $(x, y, z) := (\alpha x^*, \alpha y^*, \alpha z^*)$. We clearly have $z \ne 0$ and $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$, and since $x, y \in \mathbb{Z}$, we get $z \in \mathbb{Z}$. □

3. Determining $h(d_1, d_2, t)$ by local data

Let d_1, d_2, t be given as in Theorem 1.1. Assume that $x, y, z \in \mathbb{Z}$ are given such that $z \ne 0$, $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$, $(x, y) = 1$ (see (2.10)). In this section we determine $h(d_1, d_2, t)$ in terms of this given point of $C_{d_1,d_2,t}(\mathbb{Q})$. Our main goal is to prove Lemma 3.4.

Let $\mathcal{P}$ be the set of primes and let $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ be a disjoint union such that if $p \in \mathcal{P}_1$, then $(p, x) = 1$, and if $p \in \mathcal{P}_2$, then $(p, y) = 1$.

Lemma 3.1.

(i) *In every* $\mathrm{SL}_2(\mathbb{Z})$*-equivalence class of* $Q_{d_1,d_2,t}$ *there is an element* (Q_1, Q_2) *with coefficients* $Q_i(X, Y) = A_iX^2 + B_iXY + C_iY^2$ $(i = 1, 2)$ *and an integer* $0 \ne r \in \mathbb{Z}$ *such that* $r | t^2 - d_1d_2$ *and*

$$A_1 = rx, \quad A_2 = ry, \quad B_2A_1 - B_1A_2 = rz, \quad 0 \le B_1 < 2|A_1|. \tag{3.1}$$

(ii) *Assume that* $(Q_1, Q_2) \in Q_{d_1,d_2,t}$, $(Q_1^*, Q_2^*) \in Q_{d_1,d_2,t}$ *with coefficients* $Q_i(X, Y) = A_iX^2 + B_iXY + C_iY^2$, $Q_i^*(X, Y) = A_i^*X^2 + B_i^*XY + C_i^*Y^2$ *for* $i = 1, 2$. *Assume also that* r, r^* *are nonzero integers such that both of them are divisors of* $t^2 - d_1d_2$, *and we have* (3.1) *and*

$$A_1^* = r^*x, \quad A_2^* = r^*y, \quad B_2^*A_1^* - B_1^*A_2^* = r^*z, \quad 0 \le B_1^* < 2|A_1^*|. \tag{3.2}$$

Assume that (Q_1, Q_2) *and* (Q_1^*, Q_2^*) *are* $\mathrm{SL}_2(\mathbb{Z})$*-equivalent. Then* $Q_1 = Q_1^*$, $Q_2 = Q_2^*$.

Proof. We first prove (i). Let $Q_i(X,Y) = A_iX^2 + B_iXY + C_iY^2$ $(i = 1, 2)$ be two quadratic forms such that $(Q_1, Q_2) \in Q_{d_1,d_2,t}$. We first show that replacing (Q_1, Q_2) by an element in its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class we may assume that $(B_1, B_2) \neq (0, 0)$. If $\tau = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, then we have

$$Q_i^\tau(X,Y) = Q_i(X + bY, Y) = A_iX^2 + (B_i + 2A_ib)XY + C_i^*Y^2 \tag{3.3}$$

for $i = 1, 2$ with some C_i^*. If $(B_1 + 2A_1b, B_2 + 2A_2b) = (0, 0)$ for every integer b, then $A_i = B_i = 0$ for $i = 1, 2$. But this is impossible, since this would imply $d_1 = d_2 = t = 0$ which contradicts $t^2 - d_1d_2 \neq 0$.

Hence we may assume that $(B_1, B_2) \neq (0, 0)$. Let $B_1 \neq 0$, say. Assume for a contradiction that $B_2A_1 - B_1A_2 = 0$ and $B_2C_1 - B_1C_2 = 0$. Then $(A_2, C_2) = \lambda(A_1, C_1)$ with $\lambda = B_2/B_1$, hence $C_2A_1 - C_1A_2 = 0$. So the matrix $\left(\begin{smallmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{smallmatrix}\right)$ has rank 1, hence its lines are linearly dependent. But this contradicts $t^2 - d_1d_2 \neq 0$.

So we may assume that $B_2A_1 - B_1A_2 \neq 0$ or $B_2C_1 - B_1C_2 \neq 0$. But applying the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we can exchange the roles of A_i and C_i. So finally, we proved that replacing (Q_1, Q_2) by an element in its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class we can achieve $B_2A_1 - B_1A_2 \neq 0$. Then it follows from Lemma 2.2 that there are $a, b \in \mathbb{Q}$ such that $Q_1(a, b) = qx$, $Q_2(a, b) = qy$ with some $q \in \mathbb{Q}$, $q \neq 0$. We may clearly assume here that $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Taking $\tau = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with some c and d we then see by (2.8) and (2.9) that replacing (Q_1, Q_2) by an element in its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class we may assume that for their coefficients we have $A_1 = mx$, $A_2 = my$ with some $m \in \mathbb{Z}$, $m \neq 0$. By (2.3) and by $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$ we then see that we must have $B_2A_1 - B_1A_2 = \delta mz$ with $\delta = -1$ or $\delta = 1$. If we have $\delta = -1$ here, then we take $\tau = \begin{pmatrix} \frac{a}{(a,b)} & c \\ \frac{b}{(a,b)} & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with a, b as in (2.5). This is possible, since $a = b = 0$ is impossible by (2.4). By (2.6), (2.7), (2.8), (2.9) and Lemma 2.2 we then see that replacing again (Q_1, Q_2) by an element in its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class we may achieve that $\delta = 1$, hence we may assume that for the coefficients we have $A_1 = rx$, $A_2 = ry$, $B_2A_1 - B_1A_2 = rz$ with some $r \in \mathbb{Z}$, $r \neq 0$. Observe also that

$$r = \gcd(A_1, A_2) \Big| t^2 - d_1d_2 \tag{3.4}$$

follows from the definition of d_1, d_2 and t. We have $A_1 \neq 0$ since d_1 is not a square, hence using (3.3) we see that we can achieve also $0 \leq B_1 < 2|A_1|$. Part (i) is proved.

We now turn to part (ii). Assume $(Q_1^*, Q_2^*) = (Q_1^\tau, Q_2^\tau)$ with some $\tau = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. By (2.9) and by $B_2^*A_1^* - B_1^*A_2^* \neq 0$, which follows from our conditions, we get $R(a, b) \neq 0$. By Lemma 2.2 (ii) we have that $(x_{a,b}, y_{a,b}) \in C_{d_1,d_2,t}(\mathbb{Q})$, and $(Q_1^*, Q_2^*) = (Q_1^\tau, Q_2^\tau)$ and (2.9) show that the vectors $(x_{a,b}, y_{a,b})$ and (A_1^*, A_2^*) are constant multiples of each other. By (3.1)

and (3.2) we have that

$$a_1 := \frac{A_1}{A_1B_2 - A_2B_1} = \frac{A_1^*}{A_1^*B_2^* - A_2^*B_1^*},$$
$$a_2 := \frac{A_2}{A_1B_2 - A_2B_1} = \frac{A_2^*}{A_1^*B_2^* - A_2^*B_1^*},$$

and by (2.3) we have $(a_1, a_2) \in C_{d_1,d_2,t}(\mathbb{Q})$. Hence $(a_1, a_2), (x_{a,b}, y_{a,b}) \in C_{d_1,d_2,t}(\mathbb{Q})$ and these vectors are constant multiples of each other. So we have $(x_{a,b}, y_{a,b}) = (a_1, a_2)$ or $(x_{a,b}, y_{a,b}) = (-a_1, -a_2)$. In the latter case we get from Lemma 2.2 (i) and from (2.8), (2.9), (2.5), (2.6), (2.7) that

$$\frac{A_1}{A_1B_2 - A_2B_1} = -\frac{A_1^*}{A_1^*B_2^* - A_2^*B_1^*}, \quad \frac{A_2}{A_1B_2 - A_2B_1} = -\frac{A_2^*}{A_1^*B_2^* - A_2^*B_1^*},$$

which contradicts (3.1) and (3.2). So we must have $(x_{a,b}, y_{a,b}) = (a_1, a_2)$, and then Lemma 2.2 (i) gives $b = 0$. Hence $(Q_1^*, Q_2^*) = (Q_1^\tau, Q_2^\tau)$ with some $\tau = \left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and then using (3.3) we can complete the proof of the lemma. □

Lemma 3.2. *Let $0 \neq r \in \mathbb{Z}$ be such that $r | t^2 - d_1d_2$ and let $A_1 = rx$, $A_2 = ry$. For $B_1, B_2 \in \mathbb{Z}$ satisfying $B_2x - B_1y = z$ the following three conditions are equivalent.*

(i) *There are integers C_1, C_2 such that for the quadratic forms*

$$Q_i(X, Y) = A_iX^2 + B_iXY + C_iY^2$$

have $(Q_1, Q_2) \in Q_{d_1,d_2,t}$.

(ii) *We have $B_i^2 \equiv d_i \bmod (4A_i)$ for $i = 1, 2$.*

(iii) *For every $p \in \mathcal{P}_1$ we have $B_1^2 \equiv d_1 \bmod (p^{\nu_p(4r)})$ and $B_1z + d_1y - tx \equiv 0 \bmod (p^{\nu_p(2r)})$, and for every $p \in \mathcal{P}_2$ we have $B_2^2 \equiv d_2 \bmod (p^{\nu_p(4r)})$ and $-B_2z + d_2x - ty \equiv 0 \bmod (p^{\nu_p(2r)})$.*

Proof. Condition (i) clearly implies condition (ii). If Condition (ii) is true, then we can take integers C_1, C_2 such that for the quadratic forms $Q_i(X, Y) = A_iX^2 + B_iXY + C_iY^2$ we have $B_i^2 - 4A_iC_i = d_i$ for $i = 1, 2$. Let us define $t^* := B_1B_2 - 2A_1C_2 - 2A_2C_1$, we want to show $t^* = t$. By (2.3) we have

$$d_2A_1^2 + d_1A_2^2 - 2t^*A_1A_2 = (A_1B_2 - A_2B_1)^2,$$

and dividing by r^2 this gives

$$d_2x^2 + d_1y^2 - 2t^*xy = (xB_2 - yB_1)^2. \tag{3.5}$$

On the other hand, by the conditions $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$ and $B_2x - B_1y = z$ we have $xy \neq 0$ and

$$d_2x^2 + d_1y^2 - 2txy = (xB_2 - yB_1)^2. \tag{3.6}$$

Formulas (3.5) and (3.6) give $t^* = t$, so (ii) implies (i).

Condition (ii) is true if and only if $B_i^2 \equiv d_i \bmod (p^{\nu_p(4A_i)})$ for $i = 1, 2$ for every $p \in \mathcal{P}$. If $p \in \mathcal{P}_1$, then this condition is equivalent to

$$B_1^2 \equiv d_1 \bmod (p^{\nu_p(4r)}), \quad B_2^2 x^2 \equiv d_2 x^2 \bmod (p^{\nu_p(4ry)}). \tag{3.7}$$

The second condition here is the same as

$$(B_1 y + z)^2 - d_2 x^2 = B_1^2 y^2 + 2B_1 yz + d_1 y^2 - 2txy \equiv 0 \bmod (p^{\nu_p(4ry)}),$$

which is equivalent to

$$B_1^2 y + 2B_1 z + d_1 y - 2tx \equiv 0 \bmod (p^{\nu_p(4r)}). \tag{3.8}$$

The first condition in (3.7) and (3.8) together are equivalent to

$$B_1^2 \equiv d_1 \bmod (p^{\nu_p(4r)}), \quad 2B_1 z + 2d_1 y - 2tx \equiv 0 \bmod (p^{\nu_p(4r)}).$$

We can argue analogously for $p \in \mathcal{P}_2$, hence (ii) is equivalent to (iii). □

Lemma 3.3. *Let $0 \neq r \in \mathbb{Z}$ be such that $r | t^2 - d_1 d_2$ and let $A_1 = rx$, $A_2 = ry$. For every $p \in \mathcal{P}$ let β_p be a given integer satisfying the following properties. If $p \in \mathcal{P}_1$, then we have $\beta_p^2 \equiv d_1 \bmod (p^{\nu_p(4r)})$ and $\beta_p z + d_1 y - tx \equiv 0 \bmod (p^{\nu_p(2r)})$, and if $p \in \mathcal{P}_2$, then we have $\beta_p^2 \equiv d_2 \bmod (p^{\nu_p(4r)})$ and $-\beta_p z + d_2 x - ty \equiv 0 \bmod (p^{\nu_p(2r)})$. Then there is exactly one way of choosing two integers B_1 and B_2 satisfying the following properties: $B_2 x - B_1 y = z$, $0 \leq B_1 < 2|A_1|$ and $B_1 \equiv \beta_p \bmod (p^{\nu_p(2r)})$ for every $p \in \mathcal{P}_1$, $B_2 \equiv \beta_p \bmod (p^{\nu_p(2r)})$ for every $p \in \mathcal{P}_2$.*

Proof. The listed properties of B_1 and B_2 are equivalent to the following: $B_2 x - B_1 y = z$, and we have $B_1 \equiv \beta_p \bmod (p^{\nu_p(2rx)})$ for every $p \in \mathcal{P}_1$, $B_1 \equiv y^{-1}(\beta_p x - z) \bmod (p^{\nu_p(2rx)})$ for every $p \in \mathcal{P}_2$. This shows that there is exactly one possibility for B_1 modulo $2rx = 2A_1$. Since B_1 determines B_2, the uniqueness is proved. For the existence we have to prove that if B_1 satisfies these congruences, then $\frac{B_1 y + z}{x}$ is an integer. This follows from the congruences for $p \in \mathcal{P}_2$. □

Lemma 3.4. *Recall the notations x, y, z, $\mathcal{P}$, $\mathcal{P}_1$ and $\mathcal{P}_2$ from the beginning of Section 3. For $\alpha \geq 0$ and $p \in \mathcal{P}$ define $N_{x,y,z}(p^\alpha)$ in the following way. Let $N_{x,y,z}(p^\alpha)$ be the number of residues $\beta \bmod p^{\alpha + \nu_p(2)}$ satisfying the system of congruences*

$$\beta^2 \equiv d_1 \bmod (p^{\alpha + \nu_p(4)}), \quad \beta z + d_1 y - tx \equiv 0 \bmod (p^{\alpha + \nu_p(2)}) \tag{3.9}$$

in the case $p \in \mathcal{P}_1$, and

$$\beta^2 \equiv d_2 \bmod (p^{\alpha + \nu_p(4)}), \quad \beta z + d_2 x - ty \equiv 0 \bmod (p^{\alpha + \nu_p(2)}) \tag{3.10}$$

in the case $p \in \mathcal{P}_2$. Then we have that

$$h(d_1, d_2, t) = 2 \sum_{0 < r | t^2 - d_1 d_2} \prod_{p^\alpha || r} N_{x,y,z}(p^\alpha). \tag{3.11}$$

If p^α does not divide $t^2 - d_1d_2$, then $N_{x,y,z}(p^\alpha) = 0$.

Proof. Formula (3.11) follows at once from Lemmas 3.1, 3.2 and 3.3, taking into account that the contribution of r and $-r$ is the same for any divisor r of $t^2 - d_1d_2$. We also use that $N_{x,y,z}(p^\alpha)$ remains the same replacing z by $-z$ in (3.10). So (3.11) is proved.

From $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$ and from the congruemces in (3.9) we easily get for $p \in \mathcal{P}_1$ that

$$d_1(d_2x^2 + d_1y^2 - 2txy) = d_1z^2 \equiv \beta^2z^2 \equiv d_1^2y^2 - 2txyd_1 + t^2x^2 \bmod (p^\alpha),$$

hence $(t^2 - d_1d_2)x^2 \equiv 0\ (p^\alpha)$. Completely similarly, from the congruemces in (3.10) we easily get $(t^2 - d_1d_2)y^2 \equiv 0\ (p^\alpha)$ for $p \in \mathcal{P}_2$. The last statement of the lemma follows, so the proof is complete. □

4. Local computations

In this section we use the notations of Lemma 3.4. In the first two lemmas we determine $N_{x,y,z}(p^\alpha)$ under different assumptions on the parameters. In Lemmas 4.3 and 4.4 we compute $\sum_{\alpha\geq 0} N_{x,y,z}(p^\alpha)$ under the conditions of Lemmas 4.1 and 4.2, respectively.

Note that if $x, y, z \in \mathbb{Z}$ are given such that $z \neq 0$, $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$, then

$$d_2x^2 + d_1y^2 - 2txy = z^2. \tag{4.1}$$

Lemma 4.1. *Let $\alpha \geq 0$, $p \in \mathcal{P}$. Assume that d_1 and d_2 are not squares in $\mathbb{Q}_p$. Then we have the following statements.*

(i) *If $\alpha > \min(\nu_p(d_1), \nu_p(d_2), \nu_p(t))$, then $N_{x,y,z}(p^\alpha) = 0$.*

(ii) *If $p \neq 2$ and $\alpha \leq \min(\nu_p(d_1), \nu_p(d_2), \nu_p(t))$, then $N_{x,y,z}(p^\alpha) = p^{\alpha - \lceil \alpha/2 \rceil}$.*

(iii) *Let $p = 2$ and $i = 1$ or $i = 2$. If $\nu_p(d_i) < \alpha + 2$ and $\nu_p(d_i)$ is odd, then $N_{x,y,z}(p^\alpha) = 0$. Furthermore, if $\nu_p(d_i) = \alpha$ and $\frac{d_i}{2^\alpha} \equiv 3 \bmod 4$, then $N_{x,y,z}(p^\alpha) = 0$.*

(iv) *If $p = 2$, $\alpha = \nu_p(t) < \max(\nu_p(d_1), \nu_p(d_2))$, then $N_{x,y,z}(p^\alpha) = 0$.*

(v) *If $p = 2$, $\alpha = \nu_p(t) = \nu_p(d_1) = \nu_p(d_2)$, α is even and $\frac{d_i}{2^\alpha} \equiv 1 \bmod 4$ for $i = 1$ and 2, then $N_{x,y,z}(p^\alpha) = 2^{\frac{\alpha}{2}}$.*

(vi) *Let $p = 2$. Assume that $\nu_p(t) > \alpha$, $\max(\nu_p(d_1), \nu_p(d_2)) > \alpha$, and for $i = 1, 2$ we have that $\nu_p(d_i) \geq \alpha$. Assume also that if $i = 1$ or 2 and $\nu_p(d_i) < \alpha + 2$ then $\nu_p(d_i)$ is even, and if $\nu_p(d_i) = \alpha$ then $\frac{d_i}{2^\alpha} \equiv 1 \bmod 4$. Then $N_{x,y,z}(p^\alpha) = 2^{\alpha - \lceil \alpha/2 \rceil}$.*

(vii) *If $p = 2$, $\nu_p(t) > \alpha = \nu_p(d_1) = \nu_p(d_2)$, then $N_{x,y,z}(p^\alpha) = 0$.*

Proof. Since the statements are symmetric in d_1 and d_2, so we can assume $p \in \mathcal{P}_1$.

Using that d_1 is not a square in $\mathbb{Q}_p$, from the first congruence in (3.9) we get that

$$\nu_p(d_1) \geq \alpha, \tag{4.2}$$

and then

$$\nu_p(\beta) \geq \alpha/2. \tag{4.3}$$

We get from the second congruence in (3.9) that

$$2y(\beta z + d_1 y - tx) \equiv 0 \bmod (p^{\alpha+\nu_p(4)+\nu_p(y)}),$$

and the left-hand side here equals

$$\beta^2 y^2 + 2y\beta z + d_1 y^2 - 2ytx + (d_1 - \beta^2)y^2 = (\beta y + z)^2 - d_2 x^2 + (d_1 - \beta^2)y^2,$$

so using also the first congruence in (3.9) we get

$$(\beta y + z)^2 - d_2 x^2 \equiv 0 \bmod (p^{\alpha+\nu_p(4)+\nu_p(y)}). \tag{4.4}$$

Hence, using that d_2 is not a square in $\mathbb{Q}_p$ and that $(p, x) = 1$, we get that if $N_{x,y,z}(p^\alpha) \neq 0$, then

$$\nu_p(d_2) \geq \alpha + \nu_p(y). \tag{4.5}$$

Assume

$$\nu_p(2t) < \alpha. \tag{4.6}$$

Then using (4.5) and (4.2) we get

$$\nu_p(2txy) < \alpha + \nu_p(y) \leq \nu_p(d_2), \qquad \nu_p(2txy) < \alpha + \nu_p(y) \leq \nu_p(d_1 y^2),$$

hence from (4.1) we get $\nu_p(z) = \frac{\nu_p(2t)+\nu_p(y)}{2}$. By (4.6) and (4.2) we get

$$\nu_p(tx) \leq \nu_p(2t) < \alpha \leq \nu_p(d_1) \leq \nu_p(d_1 y),$$

and using (4.6) and (4.3) we get

$$\nu_p(tx) \leq \nu_p(2t) < \frac{\alpha}{2} + \frac{\nu_p(2t) + \nu_p(y)}{2} \leq \nu_p(\beta z).$$

Therefore, the second congruence in (3.9) cannot hold.

So we see that if $N_{x,y,z}(p^\alpha) \neq 0$, then

$$\nu_p(2t) \geq \alpha. \tag{4.7}$$

From (4.7), (4.2), (4.5) and (4.1) we get that if $N_{x,y,z}(p^\alpha) \neq 0$, then

$$\nu_p(z) \geq \alpha/2. \tag{4.8}$$

Let $p \neq 2$. For this case we get statement (i) from (4.2), (4.5) and (4.7). Under the assumption of (ii) we have (4.8) from (4.1), so (3.9) holds if and only if (4.3) is true. Hence we get (ii).

So let $p = 2$ from now on. If $\nu_p(2t) = \alpha$, then $\nu_p(t) = \alpha - 1$, so from (4.2), (4.3) and (4.8) we see $\nu_p(tx) < \nu_p(d_1 y)$, $\nu_p(tx) < \nu_p(\beta z)$, hence the second congruence in (3.9) cannot be true.

So if $N_{x,y,z}(p^\alpha) \neq 0$, then

$$\nu_p(t) \geq \alpha. \tag{4.9}$$

Hence (i) is proved also for $p = 2$. From the first congruence in (3.9) and from (4.4) we obtain also (iii). It remains to show parts (iv), (v), (vi) and (vii).

If $\nu_p(d_1) > \alpha$, then the first congruence in (3.9) implies $\nu_p(\beta) > \alpha/2$, hence by (4.8) we get $\nu_p(\beta z) > \alpha$. Since $\nu_p(d_1 y) > \alpha$, hence the second congruence in (3.9) holds if and only if $\nu_p(t) > \alpha$.

If $\nu_p(y) > 0$, then by (4.2), (4.5), (4.9) and (4.1) we get $\nu_p(z) > \alpha/2$, hence by (4.3) we get $\nu_p(\beta z) > \alpha$. We see from (4.2) and $\nu_p(y) > 0$ that $\nu_p(d_1 y) > \alpha$. So if $\nu_p(y) > 0$, then the second congruence in (3.9) holds if and only if $\nu_p(t) > \alpha$.

Now let $\nu_p(y) = 0$ and $\nu_p(d_1) = \nu_p(d_2) = \alpha$, then (4.9) and (4.1) imply $\nu_p(z) > \alpha/2$, hence by (4.3) we get $\nu_p(\beta z) > \alpha$. Since $\nu_p(d_1 y) = \alpha$, hence the second congruence in (3.9) holds if and only if $\nu_p(t) = \alpha$.

Assume $\nu_p(y) = 0$, $\nu_p(d_1) = \alpha$ and $\nu_p(d_2) > \alpha$. Then by the first congruence in (3.9) we get $\nu_p(\beta) = \alpha/2$, and from (4.9) and (4.1) we get $\nu_p(z) = \alpha/2$. So $\nu_p(\beta z) = \nu_p(d_1 y) = \alpha$, hence the second congruence in (3.9) holds if and only if $\nu_p(t) > \alpha$.

We see from the last four paragraphs that if $\nu_p(t) = \alpha$ and the first congruence in (3.9) holds, then the second congruence in (3.9) holds if and only if $\nu_p(y) = 0$ and $\nu_p(d_1) = \nu_p(d_2) = \alpha$. Therefore part (iv) is proved. We also see from the last four paragraphs that if $\nu_p(t) > \alpha$ and the first congruence in (3.9) holds, then the second congruence in (3.9) holds if and only if at least one of the following three conditions hold: $\nu_p(d_1) > \alpha$, $\nu_p(y) > 0$ or $\nu_p(d_2) > \alpha$. So (vi) follows at once.

For the proof of (v) it is enough to show that from the conditions of (v) it follows that $\nu_p(y) = 0$. Assume for a contradiction that $\alpha = \nu_p(t) = \nu_p(d_1) = \nu_p(d_2)$, α is even and $\nu_p(y) > 0$. Then $\nu_p(d_1 y^2 - 2txy) \geq \alpha + 3$, which can be seen separately for $\nu_p(y) > 1$ and $\nu_p(y) = 1$. But then (4.1) cannot hold, since d_2 is not a square in $\mathbb{Q}_p$. Therefore (v) is true.

If the conditions of (vii) are satisfied, then we get $\nu_p(y) = 0$ from (4.5). So taking into account (iii) it is enough to show that if $\nu_p(t) > \alpha = \nu_p(d_1) = \nu_p(d_2)$, α is even and $\frac{d_i}{2^\alpha} \equiv 1 \bmod 4$ for $i = 1, 2$, then $\nu_p(y) = 0$ is impossible. Indeed, under these conditions we clearly have

$$\nu_p(2txy) \geq \alpha + 2, \quad \nu_p(d_2 x^2 + d_1 y^2) = \alpha + 1. \tag{4.10}$$

Then (4.1) cannot hold. □

Lemma 4.2. *Let $\alpha \geq 0$, $p \in \mathcal{P}$. Assume that $d_1 = \delta_1^2$ with some $\delta_1 \in \mathbb{Q}_p$. Assume that there is a p-adic unit η such that $\nu_p(x) > \nu_p(t^2 - d_1 d_2) + \nu_p(2)$, $\nu_p(\eta y - 1) > \nu_p(t^2 - d_1 d_2) + \nu_p(2)$ and*

$$\nu_p(\eta z - \delta_1) > \nu_p(t^2 - d_1 d_2) + \nu_p(2).$$

Then we have the following statements.

(i) *If $\alpha + \nu_p(4) \leq \nu_p(d_2)$, $\alpha + \nu_p(2) \leq \nu_p(t)$ and $\alpha \leq \nu_p(d_1)$, then $N_{x,y,z}(p^\alpha) = p^{\alpha - \lceil \alpha/2 \rceil}$.*

(ii) *If $\alpha + \nu_p(4) \leq \nu_p(d_2)$, $\alpha + \nu_p(2) \leq \nu_p(t)$ and $\alpha > \nu_p(d_1)$, then $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$.*

(iii) *Assume that one of the following conditions is true:*
  (a) *We have $\nu_p(d_2) < \alpha$ and d_2 is not a square in $\mathbb{Q}_p$.*
  (b) *We have $\alpha \leq \nu_p(d_2) < \alpha + \nu_p(4)$ and that $\nu_p(d_2)$ is odd.*
  (c) *We have $p = 2$, $\nu_p(d_2) = \alpha$, α is even and $\frac{d_2}{2^\alpha} \equiv 3 \bmod 4$.*
  Then $N_{x,y,z}(p^\alpha) = 0$.

(iv) *Assume $\nu_p(t) \geq \alpha + \nu_p(2)$, $\nu_p(d_2) < \alpha + \nu_p(4)$ and that none of the conditions* (a), (b), (c) *above is true.*
  If $\frac{\nu_p(d_1) + \nu_p(d_2)}{2} < \alpha + \nu_p(2)$, then $N_{x,y,z}(p^\alpha) = 0$.
  If $\frac{\nu_p(d_1) + \nu_p(d_2)}{2} \geq \alpha + \nu_p(2)$, then $N_{x,y,z}(p^\alpha) = 2p^{\nu_p(d_2)/2}$ in the case $\nu_p(d_2) < \alpha$, and $N_{x,y,z}(p^\alpha) = p^{\alpha - \lceil \alpha/2 \rceil}$ in the case $\alpha \leq \nu_p(d_2) < \alpha + \nu_p(4)$.

(v) *If $\nu_p(t) < \alpha + \nu_p(2)$ and $\nu_p(t) < \frac{\nu_p(d_1)}{2}$, then $N_{x,y,z}(p^\alpha) = 0$.*

(vi) *Assume $\frac{\nu_p(d_1)}{2} \leq \nu_p(t) < \alpha + \nu_p(2)$, $\alpha + \nu_p(4) \leq \nu_p(d_2)$.*
  If $\frac{\alpha}{2} + \nu_p(2) + \frac{\nu_p(d_1)}{2} > \nu_p(t)$, then $N_{x,y,z}(p^\alpha) = 0$.
  If $\frac{\alpha}{2} + \nu_p(2) + \frac{\nu_p(d_1)}{2} \leq \nu_p(t)$, then $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$.

(vii) *Assume $\nu_p(t) < \alpha + \nu_p(2)$, $\nu_p(d_2) < \alpha + \nu_p(4)$. If*

$$\nu_p(t) \neq \frac{\nu_p(d_1) + \nu_p(d_2)}{2},$$

then $N_{x,y,z}(p^\alpha) = 0$.

(viii) *Assume $\frac{\nu_p(d_1)}{2} \leq \nu_p(t) < \alpha + \nu_p(2)$, $\nu_p(d_2) < \alpha + \nu_p(4)$ and that none of the conditions* (a), (b), (c) *above is true. Assume $\nu_p(t) = \frac{\nu_p(d_1) + \nu_p(d_2)}{2}$.*
  If $\nu_p(d_1) \leq \nu_p(d_2)$ and $\nu_p(t^2 - d_2 d_1) < \alpha + \nu_p(4) + \nu_p(d_1)$, then

$$N_{x,y,z}(p^\alpha) = 0.$$

  If $\nu_p(d_1) \leq \nu_p(d_2)$ and $\nu_p(t^2 - d_2 d_1) \geq \alpha + \nu_p(4) + \nu_p(d_1)$, then

$$N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}.$$

If $\nu_p(d_1) > \nu_p(d_2)$, $\nu_p(t) < \alpha$, $\nu_p(t^2 - d_2d_1) < \alpha + \nu_p(4) + \nu_p(t)$, *then*

$$N_{x,y,z}(p^\alpha) = 0.$$

If $\nu_p(d_1) > \nu_p(d_2)$, $\nu_p(t) < \alpha$, $\nu_p(t^2 - d_2d_1) \geq \alpha + \nu_p(4) + \nu_p(t)$, *then*

$$N_{x,y,z}(p^\alpha) = p^{\nu_p(d_2)/2}.$$

If $\nu_p(d_1) > \nu_p(d_2)$, $p = 2$, $\nu_p(t) = \alpha$, *then*

$$N_{x,y,z}(p^\alpha) = 2p^{\nu_p(d_2)/2}.$$

Proof. If $\alpha > \nu_p(t^2 - d_1d_2)$, then we know from Lemma 3.4 that $N_{x,y,z}(p^\alpha) = 0$, and so every statement of the present lemma is easy to check.

So we may assume $0 \leq \alpha \leq \nu_p(t^2 - d_1d_2)$. Under our present conditions we have that $p \in \mathcal{P}_2$, and $N_{x,y,z}(p^\alpha)$ is the number of residues $\beta \bmod p^{\alpha+\nu_p(2)}$ satisfying the system of congruences

$$\beta^2 \equiv d_2 \bmod (p^{\alpha+\nu_p(4)}), \tag{4.11}$$

$$\beta\delta_1 \equiv t \bmod (p^{\alpha+\nu_p(2)}). \tag{4.12}$$

Assume the conditions of (i). Then from (4.11) we have $\nu_p(\beta) \geq \frac{\alpha}{2} + \nu_p(2)$, and since $\nu_p(\delta_1) = \frac{\nu_p(d_1)}{2} \geq \frac{\alpha}{2}$, so $\nu_p(\beta\delta_1) \geq \alpha + \nu_p(2)$. Hence if (4.11) is true, then (4.12) is satisfied. Part (i) follows.

Assume the conditions of (ii). Then (4.12) is true if and only if $\nu_p(\beta) \geq \alpha + \nu_p(2) - \frac{\nu_p(d_1)}{2}$, and if this is true, then (4.11) also holds. Part (ii) follows.

Part (iii) follows at once from (4.11).

Part (v) is trivial, since under the conditions of (v), (4.12) cannot be true.

Under the conditions of (vii) we get from (4.11) that $\nu_p(\beta) = \frac{\nu_p(d_2)}{2}$, and then (4.12) cannot hold. So (vii) is proved.

Assume now that $\nu_p(d_2) < \alpha$ and $d_2 = \delta_2^2$ with some $\delta_2 \in \mathbb{Q}_p$. Then (4.11) can be written as

$$\alpha + \nu_p(4) \leq \nu_p(\beta + \delta_2) + \nu_p(\beta - \delta_2). \tag{4.13}$$

Hence one of the terms on the right-hand side must be at least $\frac{\alpha}{2} + \nu_p(2)$. But $\nu_p(2\delta_2) < \frac{\alpha}{2} + \nu_p(2)$, therefore exactly one of these terms is at least $\frac{\alpha}{2} + \nu_p(2)$, the other one equals $\nu_p(2\delta_2)$. Hence if $\nu_p(d_2) < \alpha$ and $d_2 = \delta_2^2$ with some $\delta_2 \in \mathbb{Q}_p$, then (4.11) is true if and only if

$$\nu_p(\beta + \epsilon\delta_2) \geq \alpha + \nu_p(2) - \nu_p(\delta_2) \tag{4.14}$$

with $\epsilon = 1$ or $\epsilon = -1$. Any β can satisfy (4.14) with at most one ϵ, since

$$\nu_p(2\delta_2) < \alpha + \nu_p(2) - \nu_p(\delta_2). \tag{4.15}$$

Now assume that $\alpha \le \nu_p(d_2) < \alpha+\nu_p(4)$ and that none of the conditions (b), (c) given in (iii) is true. Then $p = 2$, and (4.11) is true if and only if $\nu_p(\beta) = \frac{\nu_p(d_2)}{2}$, which can be written as

$$\beta \equiv 2^{\nu_p(d_2)/2} \bmod \left(2^{1+\frac{\nu_p(d_2)}{2}}\right). \tag{4.16}$$

Now assume the conditions of (iv). Then from (4.11) we have $\nu_p(\beta) = \frac{\nu_p(d_2)}{2}$. If $\frac{\nu_p(d_1)}{2} \ge \alpha + \nu_p(2)$, then (4.12) is always true. If $\alpha + \nu_p(2) > \frac{\nu_p(d_1)}{2}$, then (4.12) holds if and only if $\frac{\nu_p(d_1)+\nu_p(d_2)}{2} \ge \alpha + \nu_p(2)$. Assume this last condition. If $\nu_p(d_2) < \alpha$, then by the reasoning between (4.13) and (4.15) we get that $N_{x,y,z}(p^\alpha) = 2p^{\nu_p(d_2)/2}$. If $\alpha \le \nu_p(d_2) < \alpha+\nu_p(4)$, then $\nu_p(d_2)/2 = \lceil \alpha/2 \rceil$, and so by (4.16) we get $N_{x,y,z}(p^\alpha) = p^{\alpha-\lceil\alpha/2\rceil}$. Hence (iv) is proved.

Assume the conditions of (vi). If $\frac{\alpha}{2} + \nu_p(2) + \frac{\nu_p(d_1)}{2} > \nu_p(t)$, then $N_{x,y,z}(p^\alpha) = 0$. Indeed, (4.11) implies that $\nu_p(\beta) \ge \frac{\alpha}{2}+\nu_p(2)$, but then (4.12) cannot be true by our conditions. If $\frac{\alpha}{2}+\nu_p(2)+\frac{\nu_p(d_1)}{2} \le \nu_p(t)$, then if (4.12) is true, then $\nu_p(\beta) = \nu_p(t) - \frac{\nu_p(d_1)}{2}$, and for any such β (4.11) is satisfied. Hence in this case $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$. So (vi) is proved.

From now on we assume the conditions of (viii). Formula (4.12) is true if and only if

$$\nu_p\left(\beta - \frac{t}{\delta_1}\right) \ge \alpha + \nu_p(2) - \nu_p(\delta_1). \tag{4.17}$$

First let $\nu_p(d_2) < \alpha$ and $d_2 = \delta_2^2$ with $\delta_2 \in \mathbb{Q}_p$. Recall that then (4.11) is true if and only (4.14) holds with $\epsilon = 1$ or $\epsilon = -1$, and any β can satisfy (4.14) with at most one ϵ.

If $\nu_p(d_1) \le \nu_p(d_2)$, then (4.14) and (4.17) imply $\nu_p(\epsilon\delta_2+\frac{t}{\delta_1}) \ge \alpha+\nu_p(2)-\nu_p(\delta_2)$. Using (4.15) we then have $\nu_p(-\epsilon\delta_2 + \frac{t}{\delta_1}) = \nu_p(2\delta_2)$. So if (4.12) and (4.11) hold, then (4.17) and

$$\nu_p(t^2 - d_2d_1) \ge \alpha + \nu_p(4) + \nu_p(d_1) \tag{4.18}$$

are true. Conversely, assume that (4.17) and (4.18) are true. It is impossible then that $\nu_p(\epsilon\delta_2 + \frac{t}{\delta_1}) \le \nu_p(2\delta_2)$ for $\epsilon = 1$ and also for $\epsilon = -1$, since then

$$\nu_p(t^2 - d_2d_1) \le \nu_p(d_2) + \nu_p(4) + \nu_p(d_1)$$

would follow, which contradicts (4.18). Hence there is an ϵ for which $\nu_p(\epsilon\delta_2 + \frac{t}{\delta_1}) > \nu_p(2\delta_2)$, which implies $\nu_p(-\epsilon\delta_2 + \frac{t}{\delta_1}) = \nu_p(2\delta_2)$, so we get from (4.18) that

$$\nu_p\left(\epsilon\delta_2 + \frac{t}{\delta_1}\right) \ge \alpha + \nu_p(2) - \nu_p(\delta_2)$$

for this ϵ. Then $\nu_p(d_1) \le \nu_p(d_2)$ and (4.17) imply (4.14), hence (4.12) and (4.11) are true. Hence (4.12) and (4.11) hold if and only if (4.17)

and (4.18) are true. So if $\nu_p(d_1) \le \nu_p(d_2)$ and (4.18) is not true, then $N_{x,y,z}(p^\alpha) = 0$, while if (4.18) is true, then $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$. Hence (viii) is proved for the case $\nu_p(d_2) < \alpha$, $\nu_p(d_1) \le \nu_p(d_2)$.

Still assume $\nu_p(d_2) < \alpha$ and $d_2 = \delta_2^2$ with $\delta_2 \in \mathbb{Q}_p$. If $\nu_p(d_1) > \nu_p(d_2)$, then (4.14) with a given ϵ and (4.17) hold if and only if (4.14) and

$$\nu_p\left(\epsilon\delta_2 + \frac{t}{\delta_1}\right) \ge \alpha + \nu_p(2) - \nu_p(\delta_1) \tag{4.19}$$

are true with the same ϵ.

Assume first that $\nu_p(t) < \alpha$ (if $p \ne 2$, then this follows from the already assumed $\nu_p(t) < \alpha + \nu_p(2)$). Then $\nu_p(2\delta_2) < \alpha + \nu_p(2) - \nu_p(\delta_1)$ using $\nu_p(t) = \nu_p(\delta_1) + \nu_p(\delta_2)$. Hence if (4.19) holds, then $\nu_p(-\epsilon\delta_2 + \frac{t}{\delta_1}) = \nu_p(2\delta_2)$. So (4.19) implies

$$\nu_p(t^2 - d_2 d_1) \ge \alpha + \nu_p(4) + \nu_p(t). \tag{4.20}$$

Conversely, assume that (4.20) is true. We then cannot have

$$\nu_p\left(\epsilon\delta_2 + \frac{t}{\delta_1}\right) \le \nu_p(2\delta_2)$$

for $\epsilon = 1$ and also for $\epsilon = -1$, since then

$$\nu_p(t^2 - d_2 d_1) \le \nu_p(d_2) + \nu_p(4) + \nu_p(d_1) = \nu_p(4) + 2\nu_p(t)$$

would follow, which contradicts (4.20).

Hence there is an ϵ for which $\nu_p(\epsilon\delta_2 + \frac{t}{\delta_1}) > \nu_p(2\delta_2)$, which implies $\nu_p(-\epsilon\delta_2 + \frac{t}{\delta_1}) = \nu_p(2\delta_2)$, so we get from (4.20) that (4.19) is true for this ϵ. Hence we proved that (4.20) is true if and only if (4.19) holds for $\epsilon = 1$ or for $\epsilon = -1$. Moreover, (4.19) cannot hold for $\epsilon = 1$ and also for $\epsilon = -1$.

So if $\nu_p(d_1) > \nu_p(d_2)$, $\nu_p(t) < \alpha$ and (4.20) is not true, then $N_{x,y,z}(p^\alpha) = 0$. If (4.20) is true, then let $\epsilon \in \{-1, 1\}$ be the unique element for which (4.19) holds. From the reasoning above we see that then (4.11) and (4.12) hold if and only if (4.14) holds for this ϵ. Hence if (4.20) is true, then $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_2)/2}$. So (viii) is proved for the case $\nu_p(d_2) < \alpha$, $\nu_p(d_1) > \nu_p(d_2)$, $\nu_p(t) < \alpha$.

Assume now that $\nu_p(d_1) > \nu_p(d_2)$, $\nu_p(t) = \alpha$. This implies $\nu_p(d_2) < \alpha$ and $p = 2$, since we are still in case (viii). Since $\alpha = \nu_p(t) = \nu_p(\delta_1) + \nu_p(\delta_2)$, so (4.19) is true for $\epsilon = 1$ and also for $\epsilon = -1$. Hence (4.11) and (4.12) hold if and only if (4.14) is true with $\epsilon = 1$ or $\epsilon = -1$, and any β can satisfy (4.14) with at most one ϵ. Hence in this case $N_{x,y,z}(p^\alpha) = 2p^{\nu_p(d_2)/2}$. So (viii) is fully proved for the case $\nu_p(d_2) < \alpha$.

Still assuming the conditions of (viii), let us consider finally the case when $p = 2$ and $\alpha \le \nu_p(d_2) < \alpha + \nu_p(4)$. Since $\nu_p(t) \le \alpha$, so we have $\nu_p(d_1) \le \nu_p(d_2)$. We also have $\nu_p(t^2 - d_2 d_1) \ge \alpha + \nu_p(4) + \nu_p(d_1)$. Indeed, if $\nu_p(d_2) = \alpha + \nu_p(2)$, then it is trivial. If $\nu_p(d_2) = \alpha$, then this follows using

that $\frac{d_i}{2^{\nu_p(d_i)}} \equiv 1 \bmod 4$ for $i = 1, 2$ by our conditions. So we have to prove that $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$.

We have seen that (4.11) is true if and only if (4.16) holds, and (4.12) is true if and only if (4.17) holds. It is clear that (4.17) implies (4.16), hence we have indeed $N_{x,y,z}(p^\alpha) = p^{\nu_p(d_1)/2}$. □

Before continuing, we introduce the following notations. For any $p \in \mathcal{P}$ let

$$S_{x,y,z}(p) := \sum_{\alpha \geq 0} N_{x,y,z}(p^\alpha).$$

Lemma 4.3.

(i) *Let $p > 2$ and write $m := \min(\nu_p(d_1), \nu_p(d_2), \nu_p(t))$. Assume that either $s_p(d_1) = s_p(d_2) = 0$, or $s_p(d_1) = 1$, $s_p(d_2) = 0$ and $\nu_p(d_2) = m$. In the latter case assume that x, y, z satisfy the conditions of Lemma 4.2. Then*

$$S_{x,y,z}(p) = \sum_{0 \leq \alpha \leq m} p^{\alpha - \lceil \alpha/2 \rceil}.$$

(ii) *Let $p = 2$ and assume $s_p(d_1) = s_p(d_2) = 0$ and $c(d_1) = c(d_2) = 0$. Then $S_{x,y,z}(p)$ equals*

$$\sum_{0 \leq \alpha < \nu_p(t), \nu_p(d_1)+1, \nu_p(d_2)+1, \max(\nu_p(d_1), \nu_p(d_2))} p^{\alpha - \lceil \alpha/2 \rceil} + \delta_{\nu_p(d_1), \nu_p(t)} \delta_{\nu_p(d_2), \nu_p(t)} 2^{\frac{\nu_p(t)}{2}}.$$

(iii) *Let $p = 2$ and assume $s_p(d_1) = s_p(d_2) = 0$ and $\max(c(d_1), c(d_2)) > 0$. Then $S_{x,y,z}(p)$ equals*

$$\sum_{0 \leq \alpha \leq \nu_p(t) - 1, \nu_p(d_1) - c(d_1), \nu_p(d_2) - c(d_2)} p^{\alpha - \lceil \alpha/2 \rceil}.$$

Proof. Statements (ii), (iii) and the $s_p(d_1) = s_p(d_2) = 0$ part of (i) follow from Lemma 4.1, examining a few cases. Consider now case (i) and assume that $s_p(d_1) = 1$, $s_p(d_2) = 0$ and $\nu_p(d_2) = m$. Then the statement follows from Lemma 4.2 (i) and (iii). □

Lemma 4.4. *Assume that $d_1 = \delta_1^2$ with some $\delta_1 \in \mathbb{Q}_p$. Assume that x, y, z satisfy the conditions of Lemma 4.2.*

(a) *Let $p > 2$, and write $m := \min(\nu_p(d_1), \nu_p(d_2), \nu_p(t))$. Assume that if $\nu_p(d_2) = m$, then $s_p(d_2) = 1$. Then*

$$S_{x,y,z}(p) = \sum_{0 \leq \alpha \leq m} p^{\alpha - \lceil \alpha/2 \rceil} + p^{m/2}(\nu_p(t^2 - d_2 d_1) - 2m). \tag{4.21}$$

(b) *Let $p = 2$ and $\nu_p(d_1) = \nu_p(d_2)$. Then $S_{x,y,z}(p)$ equals*

$$\sum_{0\le\alpha\le\nu_p(t)-1,\nu_p(d_1)-1} p^{\alpha-\lceil\alpha/2\rceil} + \delta_{\nu_p(d_1),\nu_p(t)} p^{\nu_p(d_1)/2}(\nu_p(t^2-d_2d_1)-2\nu_p(d_1)-1).$$

(c) *Let $p = 2$. If $\nu_p(t) \le \nu_p(d_1) < \nu_p(d_2)$, then $S_{x,y,z}(p)$ equals*

$$\sum_{0\le\alpha\le\nu_p(t)-1} p^{\alpha-\lceil\alpha/2\rceil}. \tag{4.22}$$

(d) *Let $p = 2$. If $\nu_p(d_1) < \nu_p(t), \nu_p(d_2)$, then $S_{x,y,z}(p)$ equals*

$$\sum_{\alpha=0}^{\nu_p(d_1)} p^{\alpha-\lceil\alpha/2\rceil} + p^{\nu_p(d_1)/2}(\nu_p(t^2-d_2d_1)-2\nu_p(d_1)-2).$$

(e) *Let $p = 2$. Let d_2 be a square in $\mathbb{Q}_p$. If $\nu_p(t) \le \nu_p(d_2) < \nu_p(d_1)$, then $S_{x,y,z}(p)$ equals* (4.22).

(f) *Let $p = 2$. Let d_2 be a square in $\mathbb{Q}_p$. If $\nu_p(d_2) < \nu_p(t), \nu_p(d_1)$, then $S_{x,y,z}(p)$ equals*

$$\sum_{0\le\alpha\le\nu_p(d_2)} p^{\alpha-\lceil\alpha/2\rceil} + p^{\nu_p(d_2)/2}(\nu_p(t^2-d_2d_1)-2\nu_p(d_2)-2).$$

(g) *Let $p = 2$. Assume that d_2 is not a square in $\mathbb{Q}_p$. If $\nu_p(d_1) > \nu_p(d_2)$, then $S_{x,y,z}(p)$ equals*

$$\sum_{0\le\alpha\le\nu_p(t)-1,\nu_p(d_2)-c(d_2)} p^{\alpha-\lceil\alpha/2\rceil} \tag{4.23}$$

Proof. Consider Lemma 4.2. If in Lemma 4.2 (vi) we have

$$N_{x,y,z}(p^\alpha) \ne 0,$$

then we have

$$\frac{\alpha}{2} + \nu_p(2) + \frac{\nu_p(d_1)}{2} \le \nu_p(t) < \alpha + \nu_p(2),$$

hence $\nu_p(d_1) < \alpha$. The condition $\alpha + \nu_p(4) \le \nu_p(d_2)$ implies $\nu_p(d_1) < \alpha \le \nu_p(d_2) - \nu_p(4)$, so (f) can give nonzero contribution only if $\nu_p(d_2) > \nu_p(d_1) + \nu_p(4)$.

In case Lemma 4.2 (ii) we have

$$\nu_p(d_2) - \nu_p(4) \ge \alpha > \nu_p(d_1),$$

so in Lemma 4.2 (ii) we have $\nu_p(d_2) > \nu_p(d_1) + \nu_p(4)$.

If in Lemma 4.2 (iv) we have $N_{x,y,z}(p^\alpha) \ne 0$, then we have

$$\frac{\nu_p(d_1)+\nu_p(d_2)}{2} \ge \alpha + \nu_p(2) \ge \nu_p(d_2) - \nu_p(2) + 1,$$

hence (d) can give nonzero contribution only if $\nu_p(d_2) \le \nu_p(d_1) + 2\nu_p(2) - 2$.

Assume that d_2 is not a square in $\mathbb{Q}_p$. If $p \neq 2$, then Lemma 4.2(iv), (viii) cannot give nonzero contribution. If $p = 2$, then Lemma 4.2(iv), (viii) can give nonzero contribution only in the case $\alpha + c(d_2) \leq \nu_p(d_2) < \alpha + 2$. This follows from Lemma 4.2(iii).

First let $p \neq 2$. Then the contribution of Lemma 4.2(i) is the first term in (4.21).

Assume besides $p \neq 2$ that $\nu_p(d_1) > \nu_p(d_2)$. We have seen that then the contribution of Lemma 4.2(ii), (vi) is 0. If $\nu_p(t) \leq \nu_p(d_2)$, then the contribution of Lemma 4.2(iv), (viii) is obviously 0, so (a) follows for this case. Let $\nu_p(t) > \nu_p(d_2)$. Then $\nu_p(d_2) = m$, so $s_p(d_2) = 1$ by assumption. Then the contribution of Lemma 4.2(iv) is

$$2p^{\nu_p(d_2)/2}(\min(\nu_p(t), \frac{\nu_p(d_1) + \nu_p(d_2)}{2}) - \nu_p(d_2)). \tag{4.24}$$

If $\nu_p(t) \neq \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$, then the contribution of Lemma 4.2(viii) is 0, hence (a) follows also for this case. Finally, if $\nu_p(t) = \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$, then the contribution of Lemma 4.2(viii) is

$$p^{\nu_p(d_2)/2}(\nu_p(t^2 - d_2 d_1) - 2\nu_p(t)), \tag{4.25}$$

so we get (a) from (4.24) and (4.25). Hence (a) is proved for $\nu_p(d_1) > \nu_p(d_2)$.

Assume besides $p \neq 2$ that $\nu_p(d_1) \leq \nu_p(d_2)$. Then the contribution of Lemma 4.2(iv) is 0. If $\nu_p(t) \leq \nu_p(d_1)$, then the contribution of Lemma 4.2(ii), (vi) is 0, while the contribution of Lemma 4.2(viii) is $p^{\nu_p(d_1)/2}(\nu_p(t^2 - d_2 d_1) - 2\nu_p(t))$. Observe that this expression is nonzero only if $\nu_p(t) = \nu_p(d_1) = \nu_p(d_2)$. So (a) follows for this case. If $\nu_p(t) > \nu_p(d_1)$, then the contribution of Lemma 4.2(ii), (vi) is

$$p^{\nu_p(d_1)/2}(\min(2\nu_p(t) - \nu_p(d_1), \nu_p(d_2)) - \nu_p(d_1)). \tag{4.26}$$

If $\nu_p(t) \neq \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$, then the contribution of Lemma 4.2(viii) is 0, hence (a) follows. If $\nu_p(t) = \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$, then the contribution of Lemma 4.2(viii) is

$$p^{\nu_p(d_1)/2}(\nu_p(t^2 - d_2 d_1) - \nu_p(d_1) - \nu_p(d_2)). \tag{4.27}$$

Observe that this expression is 0 if $s_p(d_2) = 0$. So we get (a) from (4.26) and (4.27). Hence (a) is completely proved.

We assume from now on that $p = 2$.

Assume that $\nu_p(d_1) > \nu_p(d_2)$ and that d_2 is not a square in $\mathbb{Q}_p$. Then the contribution of Lemma 4.2(i), (iv) is (4.23). The contribution of Lemma 4.2(viii) is 0, since we would have

$$\alpha \geq \nu_p(t) = \frac{\nu_p(d_1) + \nu_p(d_2)}{2} > \nu_p(d_2) \geq \alpha + c(d_2),$$

which is a contradiction. Hence (g) is proved.

Assume that d_2 is a square in $\mathbb{Q}_p$ and $\nu_p(t) \le \nu_p(d_2) < \nu_p(d_1)$. Since $\nu_p(t) = \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$ cannot be true, so the contribution of Lemma 4.2 (viii) is 0. We also see that $\nu_p(t) \le \nu_p(d_2)$ can hold in Lemma 4.2 (iv) only in the case $\nu_p(t) = \alpha + \nu_p(2) = \nu_p(d_2)$. We then see that the contribution of Lemma 4.2 (i), (iv) is (4.22), so (e) is proved.

Assume that d_2 is a square in $\mathbb{Q}_p$ and $\nu_p(d_2) < \nu_p(t), \nu_p(d_1)$. Then the contribution of Lemma 4.2 (i) and of the part $\alpha \le \nu_p(d_2) < \alpha + \nu_p(4)$ of Lemma 4.2 (iv) is

$$\sum_{0 \le \alpha \le \nu_p(d_2)} p^{\alpha - \lceil \alpha/2 \rceil}. \tag{4.28}$$

The contribution of the part $\nu_p(d_2) < \alpha$ of Lemma 4.2 (iv) is

$$2p^{\nu_p(d_2)/2}(\min(\nu_p(t) - 1, \frac{\nu_p(d_1) + \nu_p(d_2)}{2} - 1) - \nu_p(d_2)). \tag{4.29}$$

If $\nu_p(t) \ne \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$, then the contribution of Lemma 4.2 (viii) is 0, and so (f) follows for this case. So assume $\nu_p(t) = \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$. Then the contribution of Lemma 4.2(viii) is

$$p^{\nu_p(d_2)/2}((\nu_p(t^2 - d_2 d_1) - \nu_p(4) - 2\nu_p(t)) + 2). \tag{4.30}$$

By (4.28), (4.29) and (4.30) we then get (f) also for this case. Hence (f) is proved.

So it is enough to prove statements (b), (c) and (d).

Assume first $\nu_p(d_1) = \nu_p(d_2)$. We have seen above that the contribution of Lemma 4.2 (ii), (vi) is 0. It is easy to see that the contribution of Lemma 4.2 (iv) is nonzero only in the case $\alpha = \nu_p(d_2) - 1$, $\nu_p(t) \ge \nu_p(d_2)$. Then the contribution of Lemma 4.2 (i), (iv) is

$$\sum_{0 \le \alpha \le \nu_p(t)-1, \nu_p(d_1)-1} p^{\alpha - \lceil \alpha/2 \rceil}.$$

The contribution of Lemma 4.2 (viii) is 0 if $\delta_{\nu_p(d_1),\nu_p(t)} = 0$, hence (b) is proved for this case. Assume $\nu_p(d_1) = \nu_p(d_2) = \nu_p(t)$. Then the contribution of Lemma 4.2 (viii) is

$$p^{\nu_p(d_1)/2}(\nu_p(t^2 - d_2 d_1) - 2\nu_p(d_1) - 1).$$

Indeed, this is clear if d_2 is a square in $\mathbb{Q}_p$, but one can check it also for the cases $s_2(d_2) = 0$, $c(d_2) = 0$ or $c(d_2) = 1$. Hence (b) follows.

We can assume from now on that $\nu_p(d_1) < \nu_p(d_2)$. We have seen that then the contribution of Lemma 4.2 (iv) is 0. The contribution of Lemma 4.2 (i) is

$$\sum_{0 \le \alpha \le \nu_p(t)-1, \nu_p(d_1), \nu_p(d_2)-2} p^{\alpha - \lceil \alpha/2 \rceil}. \tag{4.31}$$

If $\nu_p(t) \le \nu_p(d_1) < \nu_p(d_2)$, then the contribution of Lemma 4.2(ii), (vi), (viii) is 0, so (c) follows. Assume $\nu_p(d_1) < \min(\nu_p(t), \nu_p(d_2))$. Then the contribution of Lemma 4.2(ii), (vi) is

$$p^{\nu_p(d_1)/2}(\min(2\nu_p(t) - \nu_p(d_1) - 2, \nu_p(d_2) - 2) - \nu_p(d_1)) \tag{4.32}$$

in the case $\nu_p(d_2) \ge \nu_p(d_1) + 2$, and the contribution is 0 for $\nu_p(d_2) = \nu_p(d_1) + 1$. We easily get (d) for this latter case using (4.31). So we can assume $\nu_p(d_2) \ge \nu_p(d_1) + 2$, and we easily get (d) for $\nu_p(t) \ne \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$. Assume $\nu_p(t) = \frac{\nu_p(d_1)+\nu_p(d_2)}{2}$. Then the contribution of Lemma 4.2(viii) is

$$p^{\nu_p(d_1)/2}(\nu_p(t^2 - d_2 d_1) - \nu_p(d_1) - \nu_p(d_2)). \tag{4.33}$$

This is clear if d_2 is a square in $\mathbb{Q}_p$, but one can check it also for the cases $s_2(d_2) = 0$, $c(d_2) = 0$ or $c(d_2) = 1$. Using (4.31), (4.32) and (4.33) we get (d) also for this case. □

5. Proof of Theorem 1.1

We first show that $h_p(d_1, d_2, t)$ is independent of the choice of $d_{0,p}$ in the case $\nu_p(d_1) = \nu_p(d_2)$, as was mentioned above Theorem 1.1. It is trivial indeed for $p = 2$, and assuming $p > 2$ it is also trivial in the case $\nu_p(d_1) = \nu_p(d_2) > m_p$. If $p > 2$ and $\nu_p(d_1) = \nu_p(d_2) = m_p$, then our statement is true if $(\frac{d_1 p^{-m_p}}{p}) = (\frac{d_2 p^{-m_p}}{p})$. If $(\frac{d_1 p^{-m_p}}{p}) \ne (\frac{d_2 p^{-m_p}}{p})$, then $\nu_p(t^2 - d_1 d_2) - 2m_p = 0$, so the statement is also true for this case. Hence $h_p(d_1, d_2, t)$ is well-defined.

We also see that

$$h_p(d_1, d_2, t) = h_p(d_2, d_1, t). \tag{5.1}$$

This will follow if we show

$$(d_1, t^2 - d_1 d_2)_p = (d_2, t^2 - d_1 d_2)_p. \tag{5.2}$$

To see (5.2) it is enough to show $(d_1 d_2, t^2 - d_1 d_2)_p = 1$ by the multiplicativity of the Hilbert symbol, see [4, first Remark on p. 20]. Now, if $t = 0$, then this follows from [4, Proposition 2(ii) on p. 19]. If $t \ne 0$, then it is enough to show $(d_1 d_2 t^{-2}, 1 - d_1 d_2 t^{-2})_p = 1$, and it is also true by [4, Proposition 2(ii) on p. 19]. So (5.2) and (5.1) are proved.

Lemma 5.1. *The following three conditions are equivalent.*

1. *There are elements $x_0, y_0, z_0 \in \mathbb{Q}$ such that $z_0 \ne 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$.*
2. *The equation $d_2 x^2 + d_1 y^2 - 2txy - z^2 = 0$ has a solution $(z, x, y) \ne (0, 0, 0)$ in $\mathbb{Q}^3$.*
3. *The equation $x^2 - d_2 z^2 - (t^2 - d_1 d_2) y^2 = 0$ has a solution $(z, x, y) \ne (0, 0, 0)$ in $\mathbb{Q}^3$.*

Proof. From the identity

$$d_2(d_2x^2 + d_1y^2 - 2txy - z^2) = (d_2x - ty)^2 - (t^2 - d_1d_2)y^2 - d_2z^2$$

we see that it is enough to show that if the equation

$$x^2 - d_2z^2 - (t^2 - d_1d_2)y^2 = 0$$

has a solution $(z, x, y) \neq (0, 0, 0)$ in $\mathbb{Q}^3$, then it has also such a solution with $z \neq 0$. Assume that $x^2 - (t^2 - d_1d_2)y^2 = 0$ with $(x, y) \neq (0, 0)$, and $x, y \in \mathbb{Q}$. Then $t^2 - d_1d_2$ is a square, so it is enough to show that $x^2 - d_2z^2 - y^2 = 0$ has a solution in $\mathbb{Q}^3$ with $z \neq 0$. But this follows from the fact that the Pellian equation $x^2 - d_2z^2 = 1$ has a solution with positive integers x and z. □

We first prove Theorem 1.1 assuming that there are elements $x_0, y_0, z_0 \in \mathbb{Q}$ such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$. By Lemma 5.1 and (5.2) we see that this implies

$$(d_2, t^2 - d_1d_2)_p = (d_1, t^2 - d_1d_2)_p = 1 \tag{5.3}$$

for every prime p.

Let $x, y, z \in \mathbb{Z}$ be given such that $z \neq 0$, $(\frac{x}{z}, \frac{y}{z}) \in C_{d_1,d_2,t}(\mathbb{Q})$, $(x, y) = 1$. We get from Lemma 3.4 that

$$h(d_1, d_2, t) = 2 \prod_{p|t^2-d_1d_2} S_{x,y,z}(p), \tag{5.4}$$

where $S_{x,y,z}(p)$ is defined above Lemma 4.3.

We first need three lemmas.

Lemma 5.2. *Assume that d_1 and d_2 are not squares in $\mathbb{Q}_p$. Then*

$$S_{x,y,z}(p) = h_p(d_1, d_2, t) \tag{5.5}$$

for $p > 2$, and

$$2S_{x,y,z}(2) = h_2(d_1, d_2, t). \tag{5.6}$$

Proof. Let us show (5.5). Recall the notations of Section 1. If $\epsilon_p = 0$, let us write $m_p = 2k - 1$. Then by (5.3) and by definition we have

$$h_p(d_1, d_2, t) = 2 \sum_{0 \leq \alpha < k} p^\alpha. \tag{5.7}$$

By Lemma 4.3(i) this equals $S_{x,y,z}(p)$.

If $\epsilon_p = 1$, then let us write $m_p = 2k$. If $\nu_p(d_{0,p}) > m_p$, then by (5.3) and by definition we have

$$h_p(d_1, d_2, t) = 2 \sum_{0 \leq \alpha < k} p^\alpha + p^k. \tag{5.8}$$

If $\nu_p(d_{0,p}) = m_p$, then we must have $(\frac{\delta_p}{p}) = -1$ by the assumption that $d_{0,p}$ is not a square in $\mathbb{Q}_p$. By (5.3) we have that $(d_{0,p}, t^2 - d_1d_2)_p = 1$.

We can now apply the formula for the Hilbert symbol given by Serre, see [4, Theorem 1 on p. 20]. By that theorem and since $\nu_p(d_{0,p})$ is even and $\nu_p(\frac{d_{0,p}/p^{\nu_p(d_{0,p})}}{p}) = -1$, we get that $\nu_p(t^2 - d_1 d_2)$ is even. Then we see that (5.8) is valid also for the case $\nu_p(d_{0,p}) = m_p$. By Lemma 4.3 (i) we see that the right-hand side of (5.8) equals $S_{x,y,z}(p)$. Hence (5.5) is proved.

Let us show (5.6). By (5.3) and by definition we have that

$$h_2(d_1, d_2, t) = 2 \sum_{0 \le \alpha \le A} 2^{\alpha - \lceil \alpha/2 \rceil}.$$

Then (5.6) follows from the definition of A in Section 1 and from Lemma 4.3 (ii) and (iii). □

Lemma 5.3. *Assume that $d_1 = \delta_1^2$ with some $\delta_1 \in \mathbb{Q}_p$. Assume that there is a p-adic unit η such that $\nu_p(x) > \nu_p(t^2 - d_1 d_2) + \nu_p(2)$, $\nu_p(\eta y - 1) > \nu_p(t^2 - d_1 d_2) + \nu_p(2)$ and $\nu_p(\eta z - \delta_1) > \nu_p(t^2 - d_1 d_2) + \nu_p(2)$. Then* (5.5) *and* (5.6) *are true.*

Proof. Let us show (5.5). If $\epsilon_p = 0$ and $m_p = 2k - 1$, then by (5.3) and by definition we have (5.7) also for this case. If $\nu_p(d_2) = m_p$, then we get by Lemma 4.3 (i) that the right-hand side of (5.7) equals $S_{x,y,z}(p)$. If $\nu_p(d_2) > m_p$, then we apply Lemma 4.4 (a). We cannot have $\nu_p(d_1) = m_p$, because m_p is odd. Therefore

$$\nu_p(t^2 - d_2 d_1) = \nu_p(t^2) = 2m_p, \tag{5.9}$$

so we get again that the right-hand side of (5.7) equals $S_{x,y,z}(p)$.

Now let $\epsilon_p = 1$ and $m_p = 2k$. If $\nu_p(d_{0,p}) > m_p$, then by (5.3) and by definition we have (5.8) also for this case, and we have also (5.9). Therefore Lemma 4.4 (a) gives (5.5). If $\nu_p(d_{0,p}) = m_p$ and $(\frac{\delta_p}{p}) = 1$, then by (5.3) and by definition we have

$$h_p(d_1, d_2, t) = 2 \sum_{0 \le \alpha < k} p^\alpha + p^k(1 + \nu_p(t^2 - d_1 d_2) - 2m_p). \tag{5.10}$$

If $s_p(d_2) = 0$ and $\nu_p(d_2) = m_p$, then we cannot have $d_{0,p} = d_2$, so $\nu_p(d_1) = \nu_p(d_2) = m_p$, and since $s_p(d_1) \ne s_p(d_2)$, so we have $\nu_p(t^2 - d_1 d_2) - 2m_p = 0$. Then we see by Lemma 4.3 (i) that (5.10) equals $S_{x,y,z}(p)$. If $s_p(d_2) = 0$ and $\nu_p(d_2) = m_p$ do not hold at the same time, then we get by Lemma 4.4 (a) that (5.10) equals $S_{x,y,z}(p)$. Finally, if $\nu_p(d_{0,p}) = m_p$ and $(\frac{\delta_p}{p}) = -1$, then we must have $d_{0,p} = d_2$. By (5.3) and by [4, Theorem 1 on p. 20] we have that $\nu_p(t^2 - d_1 d_2)$ is even. Hence (5.8) holds also in this case. By Lemma 4.3 (i) we see that this equals $S_{x,y,z}(p)$. We examined every case, so (5.5) is proved.

Let us show (5.6). In case (1.3) we get (5.6) by (5.3) and Lemma 4.4 (b). In case (1.4) we get (5.6) by (5.3) and Lemma 4.4 (d), (f). If (1.3) and (1.4) are false, then in the case $\nu_2(d_1) = \nu_2(d_2) = \nu_2(t)$ we must have $s_2(d_2) = 0$,

$s_2(d_1) = 1$. Then it is easy to see that $\nu_2(t^2 - d_2d_1) - 2\nu_2(d_1) = 2 - c(d_2)$, so Lemma 4.4(b) gives (5.6). Finally, if (1.3), (1.4) and $\nu_2(d_1) = \nu_2(d_2) = \nu_2(t)$ are false, then we get (5.6) by Lemma 4.4(b)(c)(d)(e) and (g). Note that in the case of Lemma 4.4(d) we can have only $\nu_2(d_2) = \nu_2(d_1) + 1$, and then $\nu_2(t^2 - d_2d_1) - 2\nu_2(d_1) - 2 = -1$. So (5.6) is also proved, the lemma follows. □

Lemma 5.4. *Assume that $d_2 = \delta_2^2$ with some $\delta_2 \in \mathbb{Q}_p$. Assume that there is a p-adic unit η such that $\nu_p(\eta x - 1) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$, $\nu_p(y) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$ and $\nu_p(\eta z - \delta_2) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$. Then* (5.5) *and* (5.6) *are true.*

Proof. This follows at once from (5.1) and Lemma 5.3. We apply Lemma 5.3 by the changes $x \leftrightarrow y$, $d_1 \leftrightarrow d_2$. □

We return to the proof of Theorem 1.1 assuming that there are elements $x_0, y_0, z_0 \in \mathbb{Q}$ such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$. Apply Lemma 2.5 such that $p_1, p_2, \dots, p_r$ are the prime divisors of $t^2 - d_1d_2$. If $1 \le i \le r$ and d_1 is a square in $\mathbb{Q}_{p_i}$, $d_1 = \delta_{i,1}^2$ with some $\delta_{i,1} \in \mathbb{Q}_{p_i}$, then let us take $x_i = 0$, $y_i = 1$, $z_i = \delta_{i,1}$. If $1 \le i \le r$, d_1 is not a square in $\mathbb{Q}_{p_i}$ but $d_2 = \delta_{i,2}^2$ with some $\delta_{i,2} \in \mathbb{Q}_{p_i}$, then let us take $x_i = 1$, $y_i = 0$, $z_i = \delta_{i,2}$. Then by Lemma 2.5 we see that we can assume for x, y, z the following properties:

If p divides $t^2 - d_1d_2$ and $d_1 = \delta_{p,1}^2$ with some $\delta_{p,1} \in \mathbb{Q}_p$, then there is a p-adic unit η_p such that $\nu_p(x) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$, $\nu_p(\eta_p y - 1) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$ and $\nu_p(\eta_p z - \delta_{p,1}) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$. If p divides $t^2 - d_1d_2$, d_1 is not a square in $\mathbb{Q}_p$ but $d_2 = \delta_{p,2}^2$ with some $\delta_{p,2} \in \mathbb{Q}_p$, then there is a p-adic unit η_p such that $\nu_p(\eta_p x - 1) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$, $\nu_p(y) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$ and $\nu_p(\eta_p z - \delta_{p,2}) > \nu_p(t^2 - d_1d_2) + \nu_p(2)$.

By Lemmas 5.2, 5.3 and 5.4 we see that if x, y, z satisfy these properties and p divides $t^2 - d_1d_2$, then we have (5.5) and (5.6). We see by (5.4) that this proves Theorem 1.1 for the case when there are elements $x_0, y_0, z_0 \in \mathbb{Q}$ such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$.

Assume now that there are no elements $x_0, y_0, z_0 \in \mathbb{Q}$ such that $z_0 \neq 0$ and $(\frac{x_0}{z_0}, \frac{y_0}{z_0}) \in C_{d_1,d_2,t}(\mathbb{Q})$. By Lemma 5.1 we then see that the equation $z^2 - d_2x^2 - (t^2 - d_1d_2)y^2 = 0$ has no solution $(z, x, y) \neq (0, 0, 0)$ in $\mathbb{Q}^3$. By the Hasse–Minkowski Theorem (see [4, p. 41]) it follows that there is a prime p for which

$$(d_2, t^2 - d_1d_2)_p = -1. \tag{5.11}$$

Assume that this p does not divide $t^2 - d_1d_2$, which implies also $p > 2$. Then by [4, Theorem 1 on p. 20] we get that $(d_2, t^2 - d_1d_2)_p = (\frac{t^2 - d_1d_2}{p})^{\nu_p(d_2)}$. By (5.11) we must have $\nu_p(d_2) > 0$, but then $(\frac{t^2 - d_1d_2}{p}) = 1$, and we get a contradiction. Hence we see that (5.11) holds for a p dividing $t^2 - d_1d_2$. We

show that then we have $h_p(d_1, d_2, t) = 0$. For $p = 2$ this is trivial, so let us assume $p > 2$. We have to show that then we have

$$\epsilon_p \sum_{\beta=0}^{\nu_p(t^2-d_1d_2)-2m_p} \left(\frac{\delta_p}{p^\beta}\right) = 0. \tag{5.12}$$

To show this we may assume that $\epsilon_p = 1$, so m_p is even. We cannot have $\nu_p(d_{0,p}) > m_p$, since in that case we would have that $t^2 - d_1d_2$ is a square in $\mathbb{Q}_p$, which contradicts (5.11). By (5.11) and (5.2) we have $(d_{0,p}, t^2 - d_1d_2)_p = -1$. Since $\nu_p(d_{0,p})$ is even, so [4, Theorem 1 on p. 20] implies that $(d_{0,p}, t^2 - d_1d_2)_p = (\frac{\delta_p}{p})^{\nu_p(t^2-d_1d_2)}$. Hence we must have that $\nu_p(t^2 - d_1d_2)$ is odd and $(\frac{\delta_p}{p}) = -1$, so (5.12) is 0. Hence we proved that the right-hand side of (1.5) is 0, so it is enough to prove that $h(d_1, d_2, t) = 0$. But it follows from (2.3) that if $h(d_1, d_2, t) > 0$, then the equation $d_2x^2 + d_1y^2 - 2txy - z^2 = 0$ has a solution $(z, x, y) \neq (0, 0, 0)$ in $\mathbb{Q}^3$, so condition (1) of Lemma 5.1 is also true, contradicting our present assumption. Theorem 1.1 is proved. □

References

[1] A. Biró, "Local square mean in the hyperbolic circle problem", 2024, https://arxiv.org/abs/2403.16113.

[2] K. Hardy & K. S. Williams, "The class number of pairs of positive-definite binary quadratic forms", *Acta Arith.* **52** (1989), no. 2, p. 103-117.

[3] J. Morales, "The classification of pairs of binary quadratic forms", *Acta Arith.* **59** (1991), no. 2, p. 105-121.

[4] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, 1973, viii+115 pages.

András Biró
HUN-REN Alfréd Rényi Institute of Mathematics
1053 Budapest, Reáltanoda u. 13-15, Hungary
E-mail: biro.andras@renyi.hu