GENERAL PELL'S EQUATIONS AND ANGLE BISECTORS BETWEEN PLANAR LINES WITH RATIONAL SLOPES

Takashi Hirotsu
Wicks Mitaka #107, Osawa, Mitaka, Tokyo, Japan
twideport@gmail.com

Received: 11/16/23, Accepted: 11/28/24, Published: 12/9/24

Abstract

For a given square-free integer $d > 1$ and a given integer $z > 1$, we describe every integral solution (x, y) of the general Pell's equation $|x^2 - dy^2| = z$, where x and dy are coprime, with the fundamental unit of $\mathbb{Q}(\sqrt{d})$ and elements of $\mathbb{Z}[\sqrt{d}]$ whose absolute value of norms are the smallest prime powers. As one of its applications, we describe all nontrivial rational solutions of $(a-c)^2(b^2+1) = (b-c)^2(a^2+1)$, which is a relational expression between the slopes a and b of two straight lines and the slope c of one of their angle bisectors on the coordinate plane. We also prove an explicit formula for all nontrivial integral solutions of this equation with solutions of negative Pell's equations.

1. Introduction

On the coordinate plane, we consider the following problem, which can be called *the rational angle bisection problem*.

Problem 1. For which rational numbers a and b are the slopes of the angle bisectors between two straight lines with slopes a and b rational?

Remark 1. Given two straight lines, we consider the two angles formed by them, regardless of whether they are acute or not. The bisector of one of the angles and that of the supplementary angle are perpendicular to each other. In the case when they are not parallel to the coordinate axes, if one of the slopes is rational, then so is the other, since the product of the slopes is -1.

Essentially, Problem 1 has the meaning when the bisectors of $\angle AOB$ can be drawn by connecting O and other lattice points for given lattice points O, A, and B. This is important in drawing techniques. Furthermore, in engineering, we can specify the radiation range and the axis of light with a ratio of integers without errors due to approximations to irrational numbers by using a solution to Problem 1.

DOI: 10.5281/zenodo.14340076

The following proposition plays an important role in solving Problem 1.

Proposition 1. (a) *Let a, b, $c \in \mathbb{R}$ with $|a| \neq |b|$. If the slopes of the bisectors of the angles between two straight lines with slopes a and b are c and $-c^{-1}$, then a, b, and c satisfy*

$$(a-c)^2(b^2+1) = (b-c)^2(a^2+1). \tag{1}$$

(b) *Every rational solution (a,b,c) of (1) such that $|a| \neq |b|$ is given by*

$$(a,b,c) = \left(a_1, b_1, \frac{a_1b_2+a_2b_1}{b_2+a_2}\right),\ \left(a_1, b_1, \frac{a_1b_2-a_2b_1}{b_2-a_2}\right)$$

for some rational solutions $(x,y) = (a_1,a_2)$, (b_1,b_2) of

$$x^2 - dy^2 = -1,$$

where d is a positive square-free integer.

The proof is given in Section 2. We say that a solution (a,b,c) of (1) is *trivial* if $|a| = |b|$.

Example 1. The triples

$$(a,b,c) = \left(\frac{3}{4}, \frac{12}{5}, \frac{9}{7}\right),\ \left(\frac{1}{7}, \frac{23}{7}, \frac{6}{7}\right),\ (1,7,2)$$

satisfy (1), and therefore $(a,b) = (3/4, 12/5)$, $(1/7, 23/7)$, $(1,7)$ are solutions to Problem 1 (see Figure 1). The values $a = 3/4$ and $b = 12/5$ are the x-components of rational solutions of $x^2 - y^2 = -1$, since

$$\left(\frac{3}{4}\right)^2 - \left(\frac{5}{4}\right)^2 = -1 \quad \text{and} \quad \left(\frac{12}{5}\right)^2 - \left(\frac{13}{5}\right)^2 = -1.$$

The values $a = 1/7$ and $b = 23/7$ (resp. $a = 1$ and $b = 7$) are the x-components of rational (resp. integral) solutions of $x^2 - 2y^2 = -1$, since

$$\left(\frac{1}{7}\right)^2 - 2\cdot\left(\frac{5}{7}\right)^2 = -1 \quad \text{and} \quad \left(\frac{23}{7}\right)^2 - 2\cdot\left(\frac{17}{7}\right)^2 = -1$$
$$\text{(resp. } 1^2 - 2\cdot 1^2 = -1 \quad \text{and} \quad 7^2 - 2\cdot 5^2 = -1\text{)}.$$

Definition 1. Let $d > 1$ be a square-free integer, and let $z > 0$ be an integer.

(a) Let (x,y) be an integral solution of $|x^2 - dy^2| = z$. We say that (x,y) is *strictly primitive*, if x and dy are coprime.

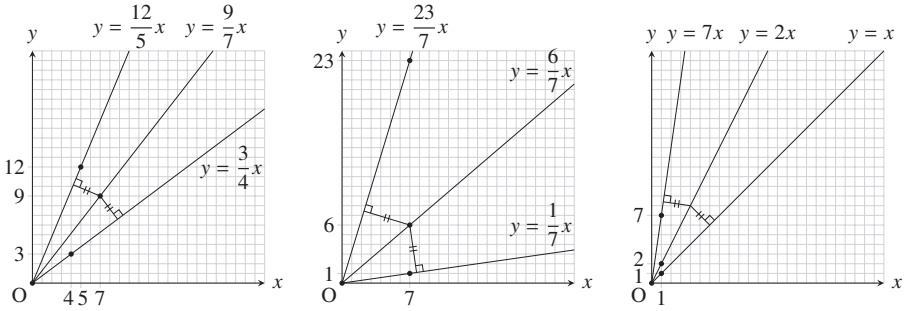

Figure 1: Straight lines and their angle bisectors with rational slopes.

(b) Let $(x, y) = (a_1, a_2)$, (b_1, b_2) be positive integral solutions of $|x^2 - dy^2| = z$. We say (a_1, a_2) is *smaller* than (b_1, b_2), if $a_2 < b_2$, or if $a_1 < b_1$ and $a_2 = b_2$.

(c) For each equation of $x^2 - dy^2 = z$, $x^2 - dy^2 = -z$, and $|x^2 - dy^2| = z$, we call its minimum positive integral solution its *fundamental solution*.

Remark 2. Suppose that z is a square number, and let (x, y) be an integral solution of $|x^2 - dy^2| = z$. If (x, y) is *primitive*, that is, x and y are coprime, then (x, y) is strictly primitive; otherwise, there exists a common prime divisor of x and d dividing $x^2 - dy^2 = \pm z$ twice and also $x^2 \mp z = dy^2$ twice, which contradicts that x and y are coprime, and d is square-free. In particular, every integral solution of $|x^2 - dy^2| = 1$ is strictly primitive.

Throughout this article, we use the following symbols.

Notation 1. Let $\mathbb{N}$ denote the additive monoid of all nonnegative integers. For each prime number p, let $\mathrm{ord}_p : \mathbb{Q}^\times \to \mathbb{Z}$ be the normalized p-adic additive valuation. We denote the greatest common divisor of a, $b \in \mathbb{Z} \setminus \{0\}$ by $\gcd(a, b)$.

Notation 2. Let $d > 1$ be a square-free integer. Let η be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. We denote the n-th smallest positive integral solution of $|x^2 - dy^2| = 1$ by $(x, y) = (f_n^{(d)}, g_n^{(d)})$ or simply $(x, y) = (f_n, g_n)$, and let $\varepsilon = f_1 + g_1\sqrt{d}$. Let $S(d)$ denote the set of every prime number p such that $|x^2 - dy^2| = p^l$ has a strictly primitive integral solution for some integer $l > 0$. For each $p \in S(d)$, let l_p be the minimum integer $l > 0$ such that $|x^2 - dy^2| = p^l$ has a strictly primitive integral solution, and let

$$\xi_p = x_p + y_p\sqrt{d}$$

with the fundamental solution $(x, y) = (x_p, y_p)$ of

$$\begin{cases} x^2 - dy^2 = p^{l_p} & \text{if } x^2 - dy^2 = -1 \text{ has a integral solution,} \\ |x^2 - dy^2| = p^{l_p} & \text{otherwise.} \end{cases}$$

Let $S(d)_-$ denote the set of every $p \in S(d)$ such that ${x_p}^2 - d{y_p}^2 = -p^{l_p}$. Furthermore, for each $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, where a_1, $a_2 \in \mathbb{Q}$, we denote the conjugate and norm of α by

$$\alpha' = a_1 - a_2\sqrt{d} \quad \text{and} \quad N(\alpha) = \alpha\alpha' = {a_1}^2 - d{a_2}^2,$$

respectively.

The first main theorem of this article is the following formula.

Theorem 1. *Let (a, b, c) be a nontrivial rational solution of (1).*

(i) *Suppose that a and b are the x-components of rational solutions of the equation $x^2 - y^2 = -1$. Then (a, b, c) is given by*

$$(a, b, c) = \left(\frac{l^2 - n^2}{2ln}, \frac{m^2 - n^2}{2mn}, \pm \left(\frac{lm - n^2}{(l + m)n} \right)^{\pm 1} \right) \tag{2}$$

for some l, m, $n \in \mathbb{Z}$ such that $|l| \neq |m|$, $lm \neq n^2$,and $lmn \neq 0$, where the double signs correspond.

(ii) *Suppose that a and b are the x-components of rational solutions of a common negative Pell's equation $x^2 - dy^2 = -1$ for some square-free integer $d > 1$. Then (a, b, c) is given by*

$$(a, b, c) = \left(\frac{\alpha + \alpha'}{2}, \frac{\beta + \beta'}{2}, \pm \left(\frac{\alpha\beta - (\alpha\beta)'}{\alpha + \beta - (\alpha + \beta)'} \right)^{\pm 1} \right) \tag{3}$$

for some α, $\beta \in \mathbb{Q}(\sqrt{d})$ such that $N(\alpha) = N(\beta) = -1$ and $\beta \neq \pm\alpha$, where the double signs correspond. In addition, α and β can be written in the form

$$\alpha = \pm\eta^m \prod_{p \in S(d)} {\alpha_p}^{m_p} p^{-l_p m_p/2} \quad \text{and} \quad \beta = \pm\eta^n \prod_{p \in S(d)} {\beta_p}^{n_p} p^{-l_p n_p/2}$$

for some m_p, $n_p \in \mathbb{N}$, α_p, $\beta_p \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$, and m, $n \in \mathbb{Z}$ satisfying

$$l_p m_p \equiv l_p n_p \equiv 0 \pmod 2$$

and

$$1 \equiv \begin{cases} m \equiv n \pmod 2 & \text{if } x^2 - dy^2 = -1 \text{ has an integral solution,} \\ \displaystyle\sum_{p \in S(d)_-} m_p \equiv \sum_{p \in S(d)_-} n_p \pmod 2 & \text{otherwise.} \end{cases}$$

Conversely, every triple (a, b, c) of Form (2) or (3) is a rational solution of (1).

The proof is given in Section 4. For any rational solution (a, b, c) of (1) in (i), each of a and b is a ratio of the leg lengths of some Pythagorean triangle. We find the rational solutions of (1) in (ii) by using the following Theorem. This is the second main theorem of this article.

Theorem 2. (a) *Let $z > 1$ be an integer. Then $|x^2 - dy^2| = z$ has a strictly primitive integral solution if and only if*

$$\mathrm{ord}_p(z) = \begin{cases} l_p n_p & \text{if } p \in S(d), \\ 0 & \text{if } p \notin S(d) \end{cases} \tag{4}$$

for some $n_p \in \mathbb{N}$ for each prime number p, where $l_2 = 2$ and $n_2 \in \{0, 1\}$ if $\eta \notin \mathbb{Z}[\sqrt{d}]$. In this case, its strictly primitive integral solution (x, y) satisfies

$$x + y\sqrt{d} = \pm\eta^n \prod_{p \in S(d)} \xi_p^{*n_p} \tag{5}$$

for some $\xi_p^* \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$ and $n \in \mathbb{Z}$ such that

$$n \equiv \begin{cases} 0,\ \pm 1 \pmod 3 & \text{if } \eta \in \mathbb{Z}[\sqrt{d}] \text{ or } z \equiv 0 \pmod 2, \\ 0 \pmod 3 & \text{if } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ and } z \equiv 1 \pmod 2. \end{cases} \tag{6}$$

(b) *Let $z > 1$ be an integer. Then every integral solution (x, y) of $|x^2 - dy^2| = z^2$ satisfies*

$$x + y\sqrt{d} = \pm\eta^n \prod_{p \in S(d)} \xi_p^{*n_p} p^{\mathrm{ord}_p(z) - l_p n_p/2} \prod_{p \notin S(d)} p^{\mathrm{ord}_p(z)} \tag{7}$$

for some $n_p \in \mathbb{N}$, $\xi_p^* \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$, and $n \in \mathbb{Z}$, where

$$l_p n_p \equiv 0 \pmod 2, \quad n_p \le 2\,\mathrm{ord}_p(z)/l_p, \tag{8}$$

and (6) hold.

The proof is given in Section 3. The integral solutions of (1) are given by the following formula.

Theorem 3. *Every nontrivial integral solution (a, b, c) of (1) is given by*

$$(a, b, c) = \pm \left(f^{(d)}_{(2m-1)(2n-1)}, f^{(d)}_{(2m-1)(2n+1)}, \frac{g^{(d)}_{(2m-1)\cdot 2n}}{g^{(d)}_{2m-1}} \right), \tag{9}$$

$$\pm \left(f^{(2)}_{2n-1}, -f^{(2)}_{2n+1}, f^{(2)}_{2n} \right) \tag{10}$$

for some integers d, m, $n > 0$ such that $x^2 - dy^2 = -1$ has an integral solution, after switching a and b if necessary, where (9) contains the case when $d = 2$. Conversely, every triple (a, b, c) of Form (9) or (10) is an integral solution of (1).

The proof is given in Section 6 after preparation in Section 5.

2. Slopes of Angle Bisectors

In this section, we prove that the slopes of two straight lines and their angle bisectors satisfy Equation (1) and certain properties.

Proof of Proposition 1. (a) It suffices to show the case when $y = cx$ is one of the angle bisectors between $y = ax$ and $y = bx$. Then the distances from a point $(t, ct) \neq (0, 0)$ on $y = cx$ to $ax - y = 0$ and $bx - y = 0$ are equal to each other. This implies

$$\frac{|at - ct|}{\sqrt{a^2 + (-1)^2}} = \frac{|bt - ct|}{\sqrt{b^2 + (-1)^2}},$$

or equivalently,

$$|a - c|\sqrt{b^2 + 1} = |b - c|\sqrt{a^2 + 1}.$$

Squaring both sides, we obtain Equation (1).

(b) Let $(a, b, c) = (a_1, b_1, c_1)$ be a nontrivial rational solution of (1), and let

$$a_1 = \frac{A_1}{Z}, \quad b_1 = \frac{B_1}{Z}, \quad \text{and} \quad c_1 = \frac{C_1}{Z}$$

with A_1, B_1, C_1, $Z \in \mathbb{Z}$ and $Z \neq 0$. Substituting these into (1) and multiplying both sides by Z^4, we obtain

$$(A_1 - C_1)^2({B_1}^2 + Z^2) = (B_1 - C_1)^2({A_1}^2 + Z^2). \tag{11}$$

For any prime number p, the parities of $\mathrm{ord}_p({A_1}^2 + Z^2)$ and $\mathrm{ord}_p({B_1}^2 + Z^2)$ coincide with each other, since $(A_1 - C_1)^2$ and $(B_1 - C_1)^2$ are square numbers. Let d be the product of every prime number p such that these valuations are odd (define $d = 1$ if there are no such prime numbers). Then there exist A_2, $B_2 \in \mathbb{Z}$ such that

$${A_1}^2 + Z^2 = d{A_2}^2 \quad \text{and} \quad {B_1}^2 + Z^2 = d{B_2}^2, \tag{12}$$

where A_1 and B_1 are the X-components of the integral solutions $(X, Y) = (A_1, A_2)$, (B_1, B_2) of $X^2 - dY^2 = -Z^2$. Furthermore, a_1 and b_1 are the x-components of the rational solutions $(x, y) = (a_1, a_2)$, (b_1, b_2) of $x^2 - dy^2 = -1$ with $a_2 = A_2/Z$ and $b_2 = B_2/Z$. Substituting (12) into (11) and dividing both sides by d, we obtain

$$(A_1 - C_1)^2{B_2}^2 = (B_1 - C_1)^2{A_2}^2,$$

or equivalently,

$$(A_1 - C_1)B_2 = \pm(B_1 - C_1)A_2.$$

Solving for C_1, we obtain

$$C_1 = \frac{A_1B_2 + A_2B_1}{B_2 + A_2}, \frac{A_1B_2 - A_2B_1}{B_2 - A_2},$$

since ${B_2}^2 - {A_2}^2 = ({B_1}^2 - {A_1}^2)/d = ({b_1}^2 - {a_1}^2)Z^2/d \neq 0$, and therefore

$$c_1 = \frac{a_1b_2 + a_2b_1}{b_2 + a_2}, \frac{a_1b_2 - a_2b_1}{b_2 - a_2}. \qquad \square$$

Remark 3. Note that (1) is equivalent to $(ac+1)^2(b^2+1) = (bc+1)^2(a^2+1)$, which is derived from the same argument as above and the fact that the other angle bisector is $y = -c^{-1}x$. Statement (a) can also be proven by the addition formula of the tangent function, or the formula for the inner product of two vectors.

For solutions of (1), the following properties are fundamental.

Proposition 2. (a) *If $(a,b,c) = (a_1,b_1,c_1)$ is a real solution of (1), then so are $(a,b,c) = (a_1,b_1,-{c_1}^{-1})$ $(c_1 \neq 0)$ and $(a,b,c) = (-a_1,-b_1,-c_1)$, (b_1,a_1,c_1).*

(b) *If $a = 0$ or $b = 0$, then (1) has no nontrivial integral solutions.*

Proof. (a) See Remark 3 for $(a,b,c) = (a_1,b_1,-{c_1}^{-1})$. The others are obvious.

(b) Let a, $b \in \mathbb{Z}$ with $|a| \neq |b|$. Solving (1) for c, we obtain

$$c = \frac{ab - 1 \pm \sqrt{(a^2+1)(b^2+1)}}{a+b},$$

which is not an integer if $a = 0$ or $b = 0$, since $\sqrt{e^2+1} \notin \mathbb{Q}$ for any $e \in \mathbb{Z} \setminus \{0\}$. This proves the desired assertion. $\square$

3. General Pell's Equations

In this section, we prove Theorem 2. Throughout the section, let $d > 1$ be a square-free integer. We recall the following classical theorems.

Theorem 4 ([1, Theorem 3.2.1])**.** *The positive Pell's equation $x^2 - dy^2 = 1$ has a nontrivial integral solution independently of the value of d.*

Theorem 5. *The negative Pell's equation $x^2 - dy^2 = -1$ has a rational solution, if and only if d has no prime divisors congruent to 3 modulo 4.*

Proof. By Fermat's two squares theorem (see [7, Theorem 2.15]), d can be expressed as $d = a^2 + b^2$ for some a, $b \in \mathbb{N}$, if and only if d has no prime divisors congruent to 3 modulo 4. We can assume $b > 0$, since $d > 1$. Under these conditions, $(x,y) = (a/b, 1/b)$ is a rational solution of $x^2 - dy^2 = -1$.

Conversely, if $x^2 - dy^2 = -1$ has a rational solution $(x,y) = (a/c, b/c)$ with a, b, $c \in \mathbb{Z}$ and $c > 0$, then $db^2 = a^2 + c^2$, which implies that db^2 has no prime divisors congruent to 3 modulo 4 by Fermat's theorem as above, and so does d. $\square$

Remark 4. If $x^2 - dy^2 = -1$ has an integral solution, then d has no prime divisors congruent to 3 modulo 4; however, the converse is false. For example, $x^2 - 34y^2 = -1$ has a rational solution $(x, y) = (5/3, 1/3)$ but no integral solutions.

Let z, $w \in \mathbb{Z} \setminus \{0\}$. If $x^2 - dy^2 = z$ and $x^2 - dy^2 = w$ have integral solutions $(x, y) = (a_1, a_2)$ and $(x, y) = (b_1, b_2)$, respectively, then $x^2 - dy^2 = zw$ has an integral solution

$$(x, y) = (a_1b_1 + da_2b_2, a_1b_2 + a_2b_1),$$

since the norm map $N : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{Q}^\times$ is a group homomorphism. In the case when $w = 1$, such a solution is called a *Pell multiple*.

Theorem 6 ([4, Corollary 3.5])**.** *Let $z \in \mathbb{Z} \setminus \{0\}$. Suppose that $x^2 - dy^2 = z$ has an integral solution. Then, for this equation, there exists a finite number of integral solutions $(x, y) = (a_{1,1}, a_{1,2}), \ldots, (a_{r,1}, a_{r,2})$ such that every integral solution (x, y) satisfies*

$$x + y\sqrt{d} = \pm\varepsilon^n(a_{i,1} + a_{i,2}\sqrt{d})$$

for some $i \in \{1, \ldots, r\}$ and $n \in \mathbb{Z}$.

In this article, we generalize the concept of Pell multiples. The following propositions are fundamental.

Proposition 3. (a) *Let $p_1, \ldots, p_r$ be distinct prime numbers, and let $n_1, \ldots, n_r \in \mathbb{N}$. If $|x^2 - dy^2| = {p_i}^{n_i}$ has a strictly primitive integral solution $(x, y) = (a_{i,1}, a_{i,2})$ for each $i \in \{1, \ldots, r\}$, then $(x, y) \in \mathbb{Z}^2$ defined by*

$$x + y\sqrt{d} = \pm\prod_{i=1}^{r}(a_{i,1} + a_{i,2}\sqrt{d}) \tag{13}$$

is a strictly primitive integral solution of $|x^2 - dy^2| = \prod_{i=1}^{r} {p_i}^{n_i}$.

(b) *Let p be a prime number, and let m, $n > 0$ be integers. If $|x^2 - dy^2| = p^m$ has a strictly primitive integral solution $(x, y) = (a_1, a_2)$, then $(x, y) \in \mathbb{Z}^2$ defined by*

$$x + y\sqrt{d} = \pm(a_1 + a_2\sqrt{d})^n \tag{14}$$

is a strictly primitive integral solution of $|x^2 - dy^2| = p^{mn}$.

Proof. We prove the contrapositions.

(a) For each $i \in \{1, \ldots, r\}$, let $(x, y) = (a_{i,1}, a_{i,2})$ be an integral solution of $|x^2 - dy^2| = {p_i}^{n_i}$, and let $\alpha_i = a_{i,1} + a_{i,2}\sqrt{d}$. Suppose that the integral solution (x, y) of $|x^2 - dy^2| = \prod_{i=1}^{r} {p_i}^{n_i}$ defined by (13) is not strictly primitive. Then $p_j \mid x$ and $p_j \mid dy$ for some $j \in \{1, \ldots, r\}$.

`Case 1:` Suppose that $p_j \mid d$. Then $p_j \mid d{a_{j,2}}^2 \pm {p_j}^{n_j} = {a_{j,1}}^2$, and therefore $p_j \mid a_{j,1}$.

Case 2: Suppose that $p_j \nmid d$. Then $p_j \mid y$. In $\mathbb{Z}[\sqrt{d}]$, this implies that p_j divides

$$(x + y\sqrt{d}) \prod_{i \neq j} \alpha_i' = \pm\alpha_j \prod_{i \neq j} \alpha_i \alpha_i' = \pm\alpha_j \prod_{i \neq j} {p_i}^{n_i}$$

and therefore α_j. Hence $p_j \mid a_{j,1}$ and $p_j \mid a_{j,2}$.

Thus, in each case, $p_j \mid a_{j,1}$ and $p_j \mid da_{j,2}$, which imply that the solution $(x, y) = (a_{j,1}, a_{j,2})$ is not strictly primitive.

(b) Let $(x, y) = (a_1, a_2)$ be an integral solution of $|x^2 - dy^2| = p^m$. Suppose that the solution (x, y) of $|x^2 - dy^2| = p^{mn}$ defined by (14) is not strictly primitive. Then $p \mid x$ and $p \mid dy$.

Case 1: Suppose that $p \mid d$. Then $p \mid d{a_2}^2 \pm p^m = {a_1}^2$, and therefore $p \mid a_1$.

Case 2: Suppose that $p \nmid d$. Then $p \mid y$, and therefore $p \mid x + y\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$. With respect to an extension v of $\mathrm{ord}_p : \mathbb{Q}^\times \to \mathbb{Z}$ to $\mathbb{Q}(\sqrt{d})$, this implies

$$v(a_1 + a_2\sqrt{d}) = \frac{1}{n} v(x + y\sqrt{d}) > 0.$$

Hence $p \mid a_1$ and $p \mid a_2$.

Thus, in each case, $p \mid a_1$ and $p \mid da_2$, which imply that the solution $(x, y) = (a_1, a_2)$ is not strictly primitive. □

Proposition 4. *Let $z \in \mathbb{Z} \setminus \{0\}$. Suppose that $x^2 - dy^2 = -1$ has an integral solution. If $x^2 - dy^2 = z$ has a strictly primitive integral solution, then so does $x^2 - dy^2 = -z$.*

Proof. We prove the contraposition. Suppose that $x^2 - dy^2 = -z$ has no strictly primitive integral solutions. Let $(x, y) = (x_0, y_0)$ be an integral solution of $x^2 - dy^2 = z$. Then $(x, y) \in \mathbb{Z}^2$ defined by $x + y\sqrt{d} = \varepsilon(x_0 + y_0\sqrt{d})$ is an integral solution of $x^2 - dy^2 = -z$, which implies that there exists a prime divisor p of z such that $p \mid x$ and $p \mid dy$.

Case 1: Suppose that $p \mid d$. Then $p \mid d{y_0}^2 + z = {x_0}^2$, and therefore $p \mid x_0$.

Case 2: Suppose that $p \nmid d$. Then $p \mid y$. In $\mathbb{Z}[\sqrt{d}]$, this implies $p \mid x + y\sqrt{d}$, and therefore $p \mid x_0 + y_0\sqrt{d}$ since $p \nmid \varepsilon$. Hence $p \mid x_0$ and $p \mid y_0$.

Thus, in each case, $p \mid x_0$ and $p \mid dy_0$, which imply that $x^2 - dy^2 = z$ has no strictly primitive integral solutions. □

We say that an ideal $\mathfrak{a} \neq (0)$ in a subring of the integer ring of a quadratic field is *primitive* if $\mathfrak{a}$ is not divisible by the ideal (p) for any prime number p.

Theorem 7. *Let p be a prime number. Suppose that $d \not\equiv 5 \pmod 8$ or $p \neq 2$. Then $|x^2 - dy^2| = z$ has a strictly primitive integral solution for some multiple z of p, if and only if p splits in $\mathbb{Q}(\sqrt{d})$.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$. Recall that the integer ring O_K of K is

$$O_K = \begin{cases} \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,\ 3 \pmod 4. \end{cases}$$

Let I be the monoid of all ideals in $\mathbb{Z}[\sqrt{d}]$. For each $(\mathfrak{a}, \mathfrak{b}) \in I \times I$, we define $\mathfrak{a} \sim \mathfrak{b}$ if

$$\mathfrak{b} = (\lambda)\mathfrak{a} \quad \text{or} \quad \mathfrak{a} = (\lambda)\mathfrak{b}$$

for some $\lambda \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}$. Then the relation $\sim$ on I is an equivalence relation which is compatible with the multiplication. Since the ideal class group Cl_K of K is finite, and so is the quotient monoid $I/\sim$ which can be regarded as its submonoid. Furthermore, 2 splits in K if $d \equiv 1 \pmod 8$, and 2 is unramified in K if $d \equiv 5 \pmod 8$.

Suppose that a prime number p splits into prime ideals $\mathfrak{p}$ and $\mathfrak{p}' = \{\alpha' \mid \alpha \in \mathfrak{p}\}$ in O_K, that is, $(p) = \mathfrak{p}\mathfrak{p}' \neq \mathfrak{p}^2$. Then there exist l, x, $y \in \mathbb{Z}$ such that

$$(\mathfrak{p} \cap \mathbb{Z}[\sqrt{d}])^l = (x + y\sqrt{d}) \quad \text{and} \quad 0 < l \leq \#Cl_K \tag{15}$$

by the finiteness of $I/\sim$, where x and y are coprime since $(\mathfrak{p} \cap \mathbb{Z}[\sqrt{d}])^l$ is primitive. Furthermore, x and d are coprime, since $x^2 - dy^2 = \pm p^l$ and $p \nmid d$. These imply that $|x^2 - dy^2| = p^l$ has a strictly primitive integral solution.

To prove the converse, suppose that an integer $z > 1$ has a prime divisor p which does not split in K. Let (x, y) be an integral solution of $|x^2 - dy^2| = z$.

`Case 1:` Suppose that p is unramified in K. Then $p \neq 2$ or "$d \equiv 3 \pmod 4$ and $p = 2$" by assumption. In O_K, the principal ideal (z) is decomposed as

$$(z) = (x + y\sqrt{d})(x - y\sqrt{d}),$$

where both sides are divisible by (p). Therefore $(x+y\sqrt{d})$ and $(x-y\sqrt{d})$ are divisible by (p) in O_K, since the prime ideal (p) divides one of these ideals and also the other because of its self-conjugacy. This implies that $(x+y\sqrt{d})$ and $(x-y\sqrt{d})$ are divisible by (p) in $\mathbb{Z}[\sqrt{d}]$, since

$$p\,O_K \cap \mathbb{Z}[\sqrt{d}] = p\,\mathbb{Z}[\sqrt{d}]. \tag{16}$$

Hence $p \mid x + y\sqrt{d}$, and therefore $p \mid x$ and $p \mid y$.

`Case 2:` Suppose that p ramifies in K. Then $p \mid d$, and therefore p divides $dy^2 \pm z = x^2$, which implies $p \mid x$.

Thus, in each case, (x, y) is not strictly primitive. This proves the desired assertion. □

Corollary 1. *Unless $d \equiv 1 \pmod 4$ and $p = 2$, then l_p is not greater than the ideal class number of $\mathbb{Q}(\sqrt{d})$ for each $p \in S(d)$.*

Proof. The desired assertion follows from (15). □

In the arguments below, we use the following lemma.

Lemma 1. *Suppose that $d \equiv 1 \pmod 4$, and let $z > 1$ be an integer.*

(a) *If $z \equiv 2 \pmod 4$, then $|x^2 - dy^2| = z$ has no integral solutions. Furthermore, if $2 \in S(d)$, then $l_2 \geq 2$.*

(b) *Both $2 \in S(d)$ and $l_2 = 2$ hold if and only if $\eta \notin \mathbb{Z}[\sqrt{d}]$. In this case, $\xi_2 = 2\eta$ holds.*

(c) *If $d \equiv 1 \pmod 8$ and $z \equiv 4 \pmod 8$, then every integral solution of $|x^2 - dy^2| = z$ is a pair of even integers. Furthermore, if $d \equiv 1 \pmod 8$, then $\eta \in \mathbb{Z}[\sqrt{d}]$.*

(d) *If $d \equiv 5 \pmod 8$ and $z \equiv 0 \pmod 8$, then every integral solution of $|x^2 - dy^2| = z$ is a pair of even integers.*

Proof. (a) If $z \equiv 2 \pmod 4$, then $|x^2 - dy^2| = z$ has no integral solutions, since $x^2 - dy^2 \equiv x^2 - y^2 \not\equiv 2 \pmod 4$ by assumption. This implies that $l_2 \geq 2$ if $2 \in S(d)$.

(b) Suppose that $\eta \notin \mathbb{Z}[\sqrt{d}]$. Then the pair (x, y) of odd integers defined by $\eta = (x + y\sqrt{d})/2$ satisfies $|x^2 - dy^2| = 2^2$. This implies that x and dy are coprime, and therefore $2 \in S(d)$ and $l_2 = 2$. In this case, $\xi_2 = 2\eta$ holds by the minimality of η.

Conversely, if $2 \in S(d)$ and $l_2 = 2$, then a strictly primitive integral solution (x, y) of $|x^2 - dy^2| = 2^2$ satisfies $(x + y\sqrt{d})/2 \in O_K^\times \setminus \mathbb{Z}[\sqrt{d}]^\times$, which implies $\eta \notin \mathbb{Z}[\sqrt{d}]$ since

$$O_K^\times = \{\pm\eta^n \mid n \in \mathbb{Z}\}. \tag{17}$$

(c) Suppose that $d \equiv 1 \pmod 8$. Then

$$1^2 - d \cdot 1^2 \equiv 1^2 - d \cdot 3^2 \equiv 3^2 - d \cdot 1^2 \equiv 3^2 - d \cdot 3^2 \equiv 0 \pmod 8,$$

which imply that every integral solution (x, y) of $|x^2 - dy^2| = z$ is a pair of even integers if $z \equiv 4 \pmod 8$. This implies $\eta \in \mathbb{Z}[\sqrt{d}]$ by (b).

(d) If $d \equiv 5 \pmod 8$, then

$$1^2 - d \cdot 1^2 \equiv 1^2 - d \cdot 3^2 \equiv 3^2 - d \cdot 1^2 \equiv 3^2 - d \cdot 3^2 \equiv 4 \pmod 8,$$

which imply that every integral solution (x, y) of $|x^2 - dy^2| = z$ is a pair of even integers if $z \equiv 0 \pmod 8$. □

Now we can determine the elements of $S(d)$.

Theorem 8. (a) *If $d \equiv 1 \pmod 8$, or $d \equiv 5 \pmod 8$ and $\eta \in \mathbb{Z}[\sqrt{d}]$, or $d \equiv 2, 3 \pmod 4$, then $S(d)$ consists of all prime numbers which split in $\mathbb{Q}(\sqrt{d})$.*

(b) *If* $d \equiv 5 \pmod 8$ *and* $\eta \notin \mathbb{Z}[\sqrt{d}]$, *then* $S(d)$ *consists of all prime numbers which split in* $\mathbb{Q}(\sqrt{d})$ *and* 2.

Proof. If $d \equiv 5 \pmod 8$ and $\eta \in \mathbb{Z}[\sqrt{d}]$, then $2 \notin S(d)$, since $|x^2 - dy^2| = 2^l$ has no strictly primitive integral solutions for each integer $l > 0$ by Lemma 1(a), (b), and (d). Combining this fact with Theorem 7 and Lemma 1(b), we obtain (a) and (b). □

We also use the following fact.

Theorem 9. *Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *be pairwise coprime ideals in the integer ring* O_K *of a quadratic field* K. *Then* $\prod_{i=1}^{r} \mathfrak{a}_i$ *is primitive if and only if* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are primitive.*

Proof. For any ideal $\mathfrak{a} \neq (0)$ in O_K, $\mathfrak{a}$ is primitive if and only if the residue group $O_K/\mathfrak{a}$ is cyclic (see [2, Corollary 6.30]). Combining this fact with the Chinese remainder theorem, we obtain the desired assertion. □

Now we are ready to prove Theorem 2.

Proof of Theorem 2. (a) Let $K = \mathbb{Q}(\sqrt{d})$, and let O_K denote the integer ring of K. For each prime number p, we take a prime ideal $\mathfrak{p}$ in O_K lying over (p) in $\mathbb{Z}$, and let $\mathfrak{p}' = \{\alpha' \mid \alpha \in \mathfrak{p}\}$. Note that $\mathfrak{p}^r$ and $\mathfrak{p}'^r$ are primitive for each $r \in \mathbb{N}$ if p splits in K. Let (x, y) be a strictly primitive integral solution of $|x^2 - dy^2| = z$. Let T be the set of all prime divisors of z, and let $T(d) = T \cap S(d)$. For each $p \in T(d)$, let q_p and r_p be the quotient and remainder, respectively, when dividing $\mathrm{ord}_p(z)$ by l_p. For each $p \in T \setminus T(d)$, let $r_p = \mathrm{ord}_p(z)$. The equality $|x^2 - dy^2| = z$ can be expressed as $(x^2 - dy^2) = (z)$ with ideals in O_K, which implies

$$(x + y\sqrt{d})(x - y\sqrt{d}) = \prod_{p \in T(d)} (\xi_p)^{q_p} (\xi_p')^{q_p} \prod_{p \in T} (p)^{r_p},$$

since $(\xi_p)(\xi_p') = (p)^{l_p}$ for each $p \in T(d)$. For each $p \in T$, if $d \equiv 2, 3 \pmod 4$ or $p \neq 2$, then (p) is decomposed as

$$(p) = \mathfrak{p}\mathfrak{p}' \neq \mathfrak{p}^2$$

in O_K by Theorem 7, and therefore the ideal $(x + y\sqrt{d})$ is divisible by either $\mathfrak{p}$ or $\mathfrak{p}'$; otherwise, $(p) = \mathfrak{p}\mathfrak{p}' \mid (x + y\sqrt{d})$ in O_K and also $\mathbb{Z}[\sqrt{d}]$ by (16), and therefore $p \mid x$ and $p \mid y$, which contradict that x and dy are coprime. For each $p \in T(d)$, we can see that (ξ_p) is divisible by either $\mathfrak{p}$ or $\mathfrak{p}'$ by the same argument as above, which implies

$$\{(\xi_p), (\xi_p')\} = \begin{cases} \{\mathfrak{p}^{l_p}, \mathfrak{p}'^{l_p}\} & \text{if } d \equiv 2,\ 3 \pmod 4 \text{ or } p \neq 2, \\ \{\mathfrak{p}^{l_2}, \mathfrak{p}'^{l_2}\},\ \{(2)\mathfrak{p}^{l_2-2}, (2)\mathfrak{p}'^{l_2-2}\} & \text{if } d \equiv 1 \pmod 4 \text{ and } p = 2. \end{cases}$$

The latter case follows from $(2)^2 = \mathfrak{p}^2\mathfrak{p}'^2 \nmid (\xi_2)$, since

$$2^2 O_K \cap \mathbb{Z}[\sqrt{d}] \subset 2\,\mathbb{Z}[\sqrt{d}] \tag{18}$$

and the fundamental solution of $|x^2 - dy^2| = 2^{l_2}$ is strictly primitive.

`Case 1:` Suppose that $d \equiv 2,\ 3 \pmod 4$ or $2 \notin T$. Then $T = T(d)$ by Theorem 8(a), and the ideal $(x + y\sqrt{d})$ is decomposed as

$$(x + y\sqrt{d}) = \left(\prod_{p \in T(d)} \xi_p^{*q_p} \right) \prod_{p \in T(d)} \mathfrak{p}^{*r_p}$$

with $\xi_p^* \in \{\xi_p, \xi_p'\}$ and $\mathfrak{p}^* \in \{\mathfrak{p}, \mathfrak{p}'\}$ in O_K. The ideal

$$\left(\frac{x + y\sqrt{d}}{\prod_{p \in T(d)} \xi_p^{*q_p}} \right) = \prod_{p \in T(d)} \mathfrak{p}^{*r_p}$$

is principal and primitive by Theorem 9, and therefore equal to O_K, which implies that $r_p = 0$ for each $p \in T(d)$. Hence there exists $n \in \mathbb{Z}$ such that

$$x + y\sqrt{d} = \pm \eta^n \prod_{p \in T(d)} \xi_p^{*q_p}.$$

Letting $n_p = q_p$, we obtain (5).

`Case 2:` Suppose that $d \equiv 1 \pmod 4$ and $2 \in T$.

Assume that $2 \notin S(d)$. Then $T \setminus \{2\} = T(d)$, $d \equiv 5 \pmod 8$, 2 is unramified in K, $\eta \in \mathbb{Z}[\sqrt{d}]$ by Theorem 8, and $\mathrm{ord}_2(z) = 2$ by Lemma 1(a) and (d). The prime ideal (2) divides both $(x + y\sqrt{d})$ and $(x - y\sqrt{d})$ only once by its self-conjugacy; otherwise, $(2)^2 \mid (x + y\sqrt{d})$ in O_K, and therefore $(2) \mid (x + y\sqrt{d})$ in $\mathbb{Z}[\sqrt{d}]$ by (18), which contradicts that x and dy are coprime. The ideal $((x+y\sqrt{d})/2)$ is decomposed as

$$\left(\frac{x + y\sqrt{d}}{2} \right) = \left(\prod_{p \in T(d)} \xi_p^{*q_p} \right) \prod_{p \in T(d)} \mathfrak{p}^{*r_p}$$

with $\xi_p^* \in \{\xi_p, \xi_p'\}$ and $\mathfrak{p}^* \in \{\mathfrak{p}, \mathfrak{p}'\}$ in O_K. The ideal

$$\left(\frac{x + y\sqrt{d}}{2\prod_{p \in T(d)} \xi_p^{*q_p}} \right) = \prod_{p \in T(d)} \mathfrak{p}^{*r_p}$$

is principal and primitive by Theorem 9, and therefore equal to O_K, which implies that $r_p = 0$ for each $p \in T(d)$. Hence there exists $n \in \mathbb{Z}$ such that

$$x + y\sqrt{d} = \pm 2\eta^n \prod_{p \in T(d)} \xi_p^{*q_p}.$$

This implies $x+y\sqrt{d} \in 2\mathbb{Z}[\sqrt{d}]$, and therefore $2 \mid x$ and $2 \mid y$, which contradict that x and dy are coprime.

Thus, $2 \in S(d)$, and therefore $T = T(d)$ by Theorem 8.

`Subcase 2-1:` Suppose that $\eta \in \mathbb{Z}[\sqrt{d}]$. Then $d \equiv 1 \pmod 8$, 2 splits in K by Theorem 8(a), and $l_2 \geq 3$ by Lemma 1(a) and (b). By the same argument as Case 1, we can see that $r_p = 0$ for each $p \in T(d)$. Hence there exists $n \in \mathbb{Z}$ such that

$$x + y\sqrt{d} = \pm\eta^n \prod_{p \in T(d)} \xi_p^{*q_p}.$$

Letting $n_p = q_p$, we obtain (5).

`Subcase 2-2:` Suppose that $\eta \notin \mathbb{Z}[\sqrt{d}]$. Then $d \equiv 5 \pmod 8$, 2 is unramified in K by Lemma 1(c), and $\mathrm{ord}_2(z) = 2$, $l_2 = 2$, $q_2 = 1$, $r_2 = 0$, and $\xi_2 = 2\eta$ by Lemma 1(b) and (d). The ideal $((x+y\sqrt{d})/2)$ is decomposed as

$$\left(\frac{x+y\sqrt{d}}{2}\right) = \left(\prod_{p \in T(d)\setminus\{2\}} \xi_p^{*q_p}\right) \prod_{p \in T(d)\setminus\{2\}} \mathfrak{p}^{*r_p}$$

with $\xi_p^* \in \{\xi_p, \xi_p'\}$ and $\mathfrak{p}^* \in \{\mathfrak{p}, \mathfrak{p}'\}$ in O_K. The ideal

$$\left(\frac{x+y\sqrt{d}}{2\prod_{p \in T(d)\setminus\{2\}} \xi_p^{*q_p}}\right) = \prod_{p \in T(d)\setminus\{2\}} \mathfrak{p}^{*r_p}$$

is principal and primitive by Theorem 9, and therefore equal to O_K, which implies that $r_p = 0$ for each $p \in T(d) \setminus \{2\}$. Hence there exists $m \in \mathbb{Z}$ such that

$$\begin{aligned} x + y\sqrt{d} &= \pm 2\eta^m \prod_{p \in T(d)\setminus\{2\}} \xi_p^{*q_p} \\ &= \pm\eta^{m-1}\xi_2 \prod_{p \in T(d)\setminus\{2\}} \xi_p^{*q_p} = \pm\eta^{m+1}\xi_2' \prod_{p \in T(d)\setminus\{2\}} \xi_p^{*q_p}. \end{aligned}$$

Letting $n_2 = 1$, $n_p = q_p$ for each $p \neq 2$, and $n = m \pm 1$, we obtain (5).

In these cases, the exponent n satisfies (6), since

$$\mathbb{Z}[\sqrt{d}]^\times = \begin{cases} \{\pm\eta^n \mid n \in \mathbb{Z}\} & \text{if } \eta \in \mathbb{Z}[\sqrt{d}], \\ \{\pm\eta^n \mid n \in \mathbb{Z},\ n \equiv 0 \pmod 3\} & \text{if } \eta \notin \mathbb{Z}[\sqrt{d}] \end{cases}$$

by (17) and $\eta^3 \in \mathbb{Z}[\sqrt{d}]$ (see [6, Theorem 2.1.4]). We can verify that (4) is satisfied by the argument above. Thus the assertion of (a) holds.

(b) Let (x, y) be an integral solution of $|x^2 - dy^2| = z^2$, and let $g = \gcd(x, y)$. Let T be the set of all prime divisors of zg^{-1}, and let $T(d) = T \cap S(d)$. Let

$$x_0 = \frac{x}{g} \quad \text{and} \quad y_0 = \frac{y}{g}.$$

Then (x_0, y_0) is a strictly primitive integral solution of $|x^2 - dy^2| = z^2 g^{-2}$, and satisfies

$$x_0 + y_0\sqrt{d} = \pm\eta^n \prod_{p\in S(d)} \xi_p^{*n_p} \tag{19}$$

for some $n_p \in \mathbb{N}$, $\xi_p^* \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$, and $n \in \mathbb{Z}$ satisfying (6) and the condition obtained by replacing z with $z^2 g^{-2}$ in (4) because of (a). If $p \in S(d)$, then (8) holds, since $0 \le \mathrm{ord}_p(g) = \mathrm{ord}_p(z) - l_p n_p/2$. If $p \notin S(d)$, then $\mathrm{ord}_p(g) = \mathrm{ord}_p(z)$. Multiplying both sides of (19) by

$$g = \prod_{p\in T(d)} p^{\mathrm{ord}_p(z) - l_p n_p/2} \prod_{p\in T\setminus T(d)} p^{\mathrm{ord}_p(z)},$$

we obtain (7). □

Remark 5. By Theorem 2, it is impossible for both $x^2 - dy^2 = p^n$ and $x^2 - dy^2 = -p^n$ to have strictly primitive integral solutions, if $x^2 - dy^2 = -1$ has no integral solutions.

Example 2. The equation $x^2 - 34y^2 = 1$ has the fundamental solution $(x, y) = (35, 6)$; however, $x^2 - 34y^2 = -1$ has no integral solutions. The fundamental unit of $\mathbb{Q}(\sqrt{34})$ is $\eta = 35 + 6\sqrt{34}$. The equations $x^2 - 34y^2 = -3^2$, $x^2 - 34y^2 = -5^2$, and $x^2 - 34y^2 = -11^2$ have the fundamental solutions $(x, y) = (5, 1)$, $(x, y) = (3, 1)$, and $(x, y) = (27, 5)$, respectively. Every integral solution (x, y) of $x^2 - 34y^2 = -(3\cdot 5\cdot 11)^2$ satisfies one of the conditions

- $x + y\sqrt{d} = \pm\eta^n \cdot (5 \pm \sqrt{34}) \cdot 5 \cdot 11$
- $x + y\sqrt{d} = \pm\eta^n \cdot 3 \cdot (3 \pm \sqrt{34}) \cdot 11$
- $x + y\sqrt{d} = \pm\eta^n \cdot 3 \cdot 5 \cdot (27 \pm 5\sqrt{34})$
- $x + y\sqrt{d} = \pm\eta^n \cdot (5 \pm \sqrt{34}) \cdot (3 \pm \sqrt{34}) \cdot (27 \pm 5\sqrt{34})$

for some $n \in \mathbb{Z}$.

Theorem 2 implies the following formula for rational solutions of Pell's equations.

Theorem 10. *Let $r \in \{0, 1\}$. Every rational solution (x, y) of $x^2 - dy^2 = (-1)^r$ satisfies*

$$x + y\sqrt{d} = \pm\eta^n \prod_{p\in S(d)} \xi_p^{*n_p} p^{-l_p n_p/2} \tag{20}$$

for some $n_p \in \mathbb{N}$, $\xi_p^* \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$, and $n \in \mathbb{Z}$ such that

$$l_p n_p \equiv 0 \pmod 2$$

and

$$r \equiv \begin{cases} n & \pmod 2 \quad \textit{if } x^2 - dy^2 = -1 \textit{ has an integral solution,} \\ \displaystyle\sum_{p \in S(d)_-} n_p & \pmod 2 \quad \textit{otherwise.} \end{cases} \tag{21}$$

Proof. Every integral solution (x, y) of $x^2 - dy^2 = (-1)^r$ satisfies

$$x + y\sqrt{d} = \pm\eta^n$$

for some $n \in \mathbb{Z}$.

Let $(x, y) = (X/Z, Y/Z)$ be a rational solution of $x^2 - dy^2 = (-1)^r$, where X, Y, and Z are coprime integers and $Z > 1$. Then (X, Y) is an integral solution of $X^2 - dY^2 = (-1)^r Z^2$, and satisfies

$$X + Y\sqrt{d} = \pm\eta^n \prod_{p \in S(d)} \xi_p^{*n_p} p^{\mathrm{ord}_p(Z) - l_p n_p/2} \prod_{p \notin S(d)} p^{\mathrm{ord}_p(Z)}$$

for some $n_p \in \mathbb{N}$, $\xi_p^* \in \{\xi_p, \xi_p'\}$ $(p \in S(d))$, and $n \in \mathbb{Z}$, where

$$l_p n_p \equiv 0 \pmod 2, \quad n_p \le 2\,\mathrm{ord}_p(Z)/l_p,$$

and

$$n \equiv \begin{cases} 0,\ \pm 1 & \pmod 3 \quad \text{if } \eta \in \mathbb{Z}[\sqrt{d}] \text{ or } \quad Z \equiv 0 \pmod 2, \\ 0 & \pmod 3 \quad \text{if } \eta \notin \mathbb{Z}[\sqrt{d}] \text{ and } Z \equiv 1 \pmod 2 \end{cases} \tag{22}$$

by Theorem 2. Dividing both sides by Z, we obtain (20). Condition (21) follows from

$$\begin{cases} N(\xi_p^*) < 0 & \text{if } p \in S(d)_-, \\ N(\xi_p^*) > 0 & \text{if } p \in S(d) \setminus S(d)_- \end{cases}$$

and

$$\begin{cases} N(\eta) < 0 & \text{if } x^2 - dy^2 = -1 \text{ has an integral solution,} \\ N(\eta) > 0 & \text{otherwise.} \end{cases}$$

We can remove Condition (22), since x, $y \in \mathbb{Q}$ and $\eta^n \in \mathbb{Z}[(1 + \sqrt{d})/2]$ for each $n \in \mathbb{Z}$. Thus the assertion of the theorem holds. □

4. Angle Bisectors with Rational Slopes

In this section, we prove Theorem 1.

Proof of Theorem 1. (i) Suppose that a and b are the x-components of rational solutions $(x, y) = (a_1, a_2)$ and $(x, y) = (b_1, b_2)$ of $x^2 - y^2 = -1$, respectively. Let

$$(a_1, a_2) = \left(\frac{A_1}{n}, \frac{A_2}{n}\right) \quad \text{and} \quad (b_1, b_2) = \left(\frac{B_1}{n}, \frac{B_2}{n}\right)$$

with A_1, A_2, B_1, B_2, $n \in \mathbb{Z}$ and $n \neq 0$. Then we have

$$A_2{}^2 - A_1{}^2 = B_2{}^2 - B_1{}^2 = n^2.$$

Furthermore, let

$$A_2 + A_1 = l \quad \text{and} \quad B_2 + B_1 = m.$$

Then we have

$$A_2 - A_1 = \frac{n^2}{l} \quad \text{and} \quad B_2 - B_1 = \frac{n^2}{m}.$$

These imply

$$a_1 = \frac{l - n^2/l}{2n} = \frac{l^2 - n^2}{2ln}, \qquad a_2 = \frac{l + n^2/l}{2n} = \frac{l^2 + n^2}{2ln},$$
$$b_1 = \frac{m - n^2/m}{2n} = \frac{m^2 - n^2}{2mn}, \qquad b_2 = \frac{m + n^2/m}{2n} = \frac{m^2 + n^2}{2mn},$$

and therefore

$$\frac{a_1 b_2 + a_2 b_1}{b_2 + a_2} = \frac{1}{2} \cdot \frac{(l^2 - n^2)(m^2 + n^2) + (l^2 + n^2)(m^2 - n^2)}{ln(m^2 + n^2) + mn(l^2 + n^2)} = \frac{lm - n^2}{(l + m)n},$$

which implies

$$\frac{a_1 b_2 - a_2 b_1}{b_2 - a_2} = -\left(\frac{a_1 b_2 + a_2 b_1}{b_2 + a_2}\right)^{-1} = -\frac{(l + m)n}{lm - n^2}.$$

(ii) Suppose that a and b are the x-components of rational solutions $(x, y) = (a_1, a_2)$ and $(x, y) = (b_1, b_2)$ of $x^2 - dy^2 = -1$ for some square-free integer $d > 1$, respectively. In general, if $\alpha = a_1 + a_2\sqrt{d}$ and $\beta = b_1 + b_2\sqrt{d}$ with a_1, a_2, b_1, $b_2 \in \mathbb{Z}$, then

$$a_1 = \frac{\alpha + \alpha'}{2} \quad \text{and} \quad b_1 = \frac{\beta + \beta'}{2},$$

which imply

$$a_1 b_2 + a_2 b_1 = \frac{\alpha\beta - (\alpha\beta)'}{2\sqrt{d}} \quad \text{and} \quad a_2 + b_2 = \frac{(\alpha + \beta) - (\alpha + \beta)'}{2\sqrt{d}}.$$

Combining these identities with Theorem 10, we obtain the desired assertion. □

Example 3. (a) In (2), letting $(l, m, n) = (2, 3, 1)$, we obtain the rational solutions

$$(a, b, c) = \left(\frac{3}{4}, \frac{4}{3}, 1\right), \ \left(\frac{3}{4}, \frac{4}{3}, -1\right)$$

of (1), and letting $(l, m, n) = (2, 5, 1)$, we obtain the rational solutions

$$(a, b, c) = \left(\frac{3}{4}, \frac{12}{5}, \frac{9}{7}\right), \ \left(\frac{3}{4}, \frac{12}{5}, -\frac{7}{9}\right)$$

of (1).

(b) In (3), letting $d = 2$, $\alpha = (1 + 5\sqrt{2})/7$, $\beta = \eta^2\alpha$, and $\eta = 1 + \sqrt{2}$, we obtain the rational solutions

$$(a, b, c) = \left(\frac{1}{7}, \frac{23}{7}, \frac{6}{7}\right), \ \left(\frac{1}{7}, \frac{23}{7}, -\frac{7}{6}\right)$$

of (1), and letting $d = 34$, $\alpha = (5 + \sqrt{34})/3$, $\beta = \eta\alpha$, and $\eta = 35 + 6\sqrt{34}$, we obtain the rational solutions

$$(a, b, c) = \left(\frac{5}{3}, \frac{379}{3}, \frac{32}{9}\right), \ \left(\frac{5}{3}, \frac{379}{3}, -\frac{9}{32}\right)$$

of (1).

5. Integral Solutions of Pell's Equations

Let $d > 1$ be a square-free integer. Assume that $x^2 - dy^2 = -1$ has an integral solution. In this section, we denote $f_n^{(d)}$ and $g_n^{(d)}$ by f_n and g_n, respectively, without the indices (d). For convenience, let $f_0 = 1$ and $g_0 = 0$. In the case when $d = 2$, the terms of (f_n) and (g_n) are known as *half-companion Pell numbers* and *Pell numbers*, respectively. Note that $\varepsilon = f_1 + g_1\sqrt{d}$ satisfies $\varepsilon\varepsilon' = -1$ by assumption.

In this section, we describe the properties of (f_n) and (g_n) used in the proof of Theorem 3 and certain related properties. The following proposition is well-known.

Proposition 5 ([5, Section 2.4])**.** *The sequences (f_n) and (g_n) are strictly increasing, and satisfy*

$$\varepsilon^n = f_n + g_n\sqrt{d} \tag{23}$$

and

$$f_n{}^2 - dg_n{}^2 = (-1)^n. \tag{24}$$

Their general terms are given by

$$f_n = \frac{\varepsilon^n + \varepsilon'^n}{2}, \tag{25}$$

$$g_n = \frac{\varepsilon^n - \varepsilon'^n}{2\sqrt{d}}. \tag{26}$$

Corollary 2. *We have $f_n \geq g_n$, where the equality holds if and only if $d = 2$ and $n = 1$. We also have $f_1 \geq \sqrt{d - 1}$.*

Proof. Identity (24) implies $f_n{}^2 - g_n{}^2 = (d - 1)g_n{}^2 + (-1)^n \geq d - 2 \geq 0$ and $f_1{}^2 = dg_1{}^2 + (-1)^n \geq d - 1$, which prove the desired inequalities. □

The following proposition is also well-known and generalized for the Lucas sequences (see [8, Chapter 2, IV]).

Proposition 6. *Let m, $n \in \mathbb{N}$ with $m \geq n$.*

(a) *Addition formulas: we have*

$$f_{m+n} = f_m f_n + d g_m g_n, \tag{27}$$
$$g_{m+n} = f_m g_n + g_m f_n, \tag{28}$$
$$f_{m-n} = (-1)^n (f_m f_n - d g_m g_n), \tag{29}$$
$$g_{m-n} = (-1)^{n+1} (f_m g_n - g_m f_n). \tag{30}$$

(b) *Double formulas: we have*

$$f_{2n} = f_n^2 + d g_n^2, \tag{31}$$
$$g_{2n} = 2 f_n g_n. \tag{32}$$

Proof. (a) Describing $\varepsilon^{m+n} = \varepsilon^m \varepsilon^n$ and $\varepsilon^{m-n} = (-1)^n \varepsilon^m \varepsilon'^n$ with terms of (f_n) and (g_n) by (23), we obtain

$$\begin{aligned} f_{m+n} + g_{m+n}\sqrt{d} &= (f_m + g_m\sqrt{d})(f_n + g_n\sqrt{d}) \\ &= (f_m f_n + d g_m g_n) + (f_m g_n + g_m f_n)\sqrt{d}, \\ f_{m-n} + g_{m-n}\sqrt{d} &= (-1)^n (f_m + g_m\sqrt{d})(f_n - g_n\sqrt{d}) \\ &= (-1)^n (f_m f_n - d g_m g_n) + (-1)^{n+1} (f_m g_n - g_m f_n)\sqrt{d}. \end{aligned}$$

Comparing both sides, we obtain the desired identities, since 1 and $\sqrt{d}$ are linearly independent over $\mathbb{Q}$.

(b) Letting $m = n$ in (27) and (28), we obtain the desired identities. □

The divisibility in (g_n) depends only on that of the indices (see [3, Theorem IV] and [5, Theorem 8.4]). A certain divisibility property in (f_n) can be proven in a similar way (see [3, Theorem V]). These are summarized as follows. Since most of them are already known, we give a brief proof in a somewhat new way.

Theorem 11. *Let m, $n \in \mathbb{N}$ with $m \geq n > 0$.*

(a) *We have* $\gcd(d, f_n) = \gcd(f_n, g_n) = 1$.

(b) *If m is a multiple of n whose quotient is even, then* $\gcd(f_m, f_n) = 1$.

(c) *The following conditions are equivalent.*

- (f1) *f_m is a multiple of f_n.*
- (f2) *Either we have $d = 2$ and $n = 1$, or m is a multiple of n whose quotient is odd.*

(d) *The following conditions are equivalent.*

(g1) g_m *is a multiple of* g_n.

(g2) m *is a multiple of* n.

Proof. We give the proof in the following order: (a), the implication (f2) to (f1), (b), the implication (f1) to (f2), (d).

(a) Identity (24) implies $\gcd(d, f_n) = \gcd(f_n, g_n) = 1$.

(c) We prove the implication (f2) to (f1).

`Case 1:` Suppose that $d = 2$ and $n = 1$. Then f_m is a multiple of $f_n = 1$, since $\varepsilon = 1 + \sqrt{2}$.

`Case 2:` Suppose that $m = nq$ with an odd integer $q > 0$. Since

$$\frac{\varepsilon^m + \varepsilon'^m}{2} = \frac{\varepsilon^n + \varepsilon'^n}{2} \sum_{i=0}^{q-1} (-1)^i \varepsilon^{n(q-1-i)} \varepsilon'^{ni},$$

we have

$$\frac{f_m}{f_n} = \sum_{i=0}^{q-1} (-1)^i \varepsilon^{n(q-1-i)} \varepsilon'^{ni} \in \mathbb{Z}[\sqrt{d}] \cap \mathbb{Q} = \mathbb{Z}$$

by (25). This implies that f_m is a multiple of f_n.

(b) Suppose that $m = nq$ with an even integer $q > 0$. By (27), we have

$$f_m = f_{n(q-1)+n} = f_{n(q-1)} f_n + d g_{n(q-1)} g_n.$$

Since d and g_n are coprime with f_n by (a), we have $\gcd(f_m, f_n) = \gcd(g_{n(q-1)}, f_n)$, and therefore this is a common divisor of $g_{n(q-1)}$ and $f_{n(q-1)}$ by the implication (f2) to (f1), which implies $\gcd(f_m, f_n) = 1$ by (a).

(c) We prove the implication (f1) to (f2). Suppose that f_m is a multiple of f_n, and $d \neq 2$ or $n \neq 1$. By Corollary 2, we have $f_n > 1$. Let q and r be the quotient and remainder, respectively, when dividing m by n. By (27), we have

$$f_m = f_{nq+r} = f_{nq} f_r + d g_{nq} g_r.$$

Assume that q is even, and let $q = 2^e k$, where e, $k > 0$ are integers and k is odd. By (32), we have $g_{nq} = 2 f_{nq/2} g_{nq/2}$. Repeating this e times, we see that g_{nq} is a multiple of f_{nk}. By the implication (f2) to (f1), f_{nk} is a multiple of f_n. These imply that g_{nq} is a multiple of f_n. Since f_{nq} is coprime with f_n by (b), and f_r is not a multiple of f_n by $0 < f_r < f_n$, we see that f_m is not a multiple of f_n. This is a contradiction.

Therefore q is odd. Since f_{nq} is a multiple of f_n by the implication (f2) to (f1), $d g_{nq} g_r$ is a multiple of f_n. Furthermore, $\gcd(f_n, g_{nq})$ is a common divisor of f_{nq} and g_{nq}, which implies $\gcd(f_n, g_{nq}) = 1$ by (a). Since d and g_{nq} are coprime with f_n, we see that g_r is a multiple of f_n. Since $0 \leq g_r < g_n < f_n$ by Proposition 5 and

Corollary 2, we have $r = 0$ and $m = nq$, which implies that m is a multiple of n whose quotient is odd.

(d) We prove the implication (g2) to (g1). Suppose that $m = nq$ with an integer $q > 0$. Since

$$\frac{\varepsilon^m - \varepsilon'^m}{2\sqrt{d}} = \frac{\varepsilon^n - \varepsilon'^n}{2\sqrt{d}} \sum_{i=0}^{q-1} \varepsilon^{n(q-1-i)} \varepsilon'^{ni},$$

we have

$$\frac{g_m}{g_n} = \sum_{i=0}^{q-1} \varepsilon^{n(q-1-i)} \varepsilon'^{ni} \in \mathbb{Z}[\sqrt{d}] \cap \mathbb{Q} = \mathbb{Z}$$

by (26). This implies that g_m is a multiple of g_n.

We prove the implication (g1) to (g2). Suppose that g_m is a multiple of g_n. Let q and r be the quotient and remainder, respectively, when dividing m by n. By (28), we have

$$g_m = g_{nq+r} = f_{nq} g_r + g_{nq} f_r.$$

Since g_{nq} is a multiple of g_n by the implication (g2) to (g1), $f_{nq} g_r$ is a multiple of g_n. Furthermore, $\gcd(f_{nq}, g_n)$ is a common divisor of f_{nq} and g_{nq}, which implies $\gcd(f_{nq}, g_n) = 1$ by (a). Since f_{nq} is coprime with g_n, we see that g_r is a multiple of g_n. Since $0 \le g_r < g_n$, we have $r = 0$ and $m = nq$, which implies that m is a multiple of n. □

The following formulas enable us to convert sums into products in (f_n) and (g_n).

Proposition 7. *For any m, $n \in \mathbb{N}$ such that $m > n$, we have*

$$f_{m+n} + f_{m-n} = \begin{cases} 2f_m f_n & \text{if} \quad n \equiv 0 \pmod 2, \\ 2d g_m g_n & \text{if} \quad n \equiv 1 \pmod 2, \end{cases} \tag{33}$$

$$f_{m+n} - f_{m-n} = \begin{cases} 2d g_m g_n & \text{if} \quad n \equiv 0 \pmod 2, \\ 2f_m f_n & \text{if} \quad n \equiv 1 \pmod 2, \end{cases} \tag{34}$$

$$g_{m+n} + g_{m-n} = \begin{cases} 2g_m f_n & \text{if} \quad n \equiv 0 \pmod 2, \\ 2f_m g_n & \text{if} \quad n \equiv 1 \pmod 2, \end{cases} \tag{35}$$

$$g_{m+n} - g_{m-n} = \begin{cases} 2f_m g_n & \text{if} \quad n \equiv 0 \pmod 2, \\ 2g_m f_n & \text{if} \quad n \equiv 1 \pmod 2. \end{cases} \tag{36}$$

Proof. For any $n \in \mathbb{N}$, we have $\varepsilon^n \varepsilon'^n = (\varepsilon\varepsilon')^n = (-1)^n$. By (25) and (26), we have

$$\begin{aligned} 2f_m f_n &= \frac{(\varepsilon^m + \varepsilon'^m)(\varepsilon^n + \varepsilon'^n)}{2} = \frac{(\varepsilon^{m+n} + \varepsilon'^{m+n}) + (-1)^n(\varepsilon^{m-n} + \varepsilon'^{m-n})}{2} \\ &= f_{m+n} + (-1)^n f_{m-n}, \\ 2dg_m g_n &= \frac{(\varepsilon^m - \varepsilon'^m)(\varepsilon^n - \varepsilon'^n)}{2} = \frac{(\varepsilon^{m+n} + \varepsilon'^{m+n}) + (-1)^{n+1}(\varepsilon^{m-n} + \varepsilon'^{m-n})}{2} \\ &= f_{m+n} + (-1)^{n+1} f_{m-n}, \end{aligned}$$

$$\begin{aligned} 2f_m g_n &= \frac{(\varepsilon^m + \varepsilon'^m)(\varepsilon^n - \varepsilon'^n)}{2\sqrt{d}} = \frac{(\varepsilon^{m+n} - \varepsilon'^{m+n}) + (-1)^{n+1}(\varepsilon^{m-n} - \varepsilon'^{m-n})}{2\sqrt{d}} \\ &= g_{m+n} + (-1)^{n+1} g_{m-n}, \\ 2g_m f_n &= \frac{(\varepsilon^m - \varepsilon'^m)(\varepsilon^n + \varepsilon'^n)}{2\sqrt{d}} = \frac{(\varepsilon^{m+n} - \varepsilon'^{m+n}) + (-1)^n(\varepsilon^{m-n} - \varepsilon'^{m-n})}{2\sqrt{d}} \\ &= g_{m+n} + (-1)^n g_{m-n}, \end{aligned}$$

which imply the desired identities. □

6. Angle Bisectors with Integral Slopes

In this section, we prove Theorem 3.

Proof of Theorem 3. Every nontrivial integral solution (a, b, c) of (1) can necessarily be written in the form

$$(a, b, c) = \left(a_1, b_1, \frac{a_1 b_2 + a_2 b_1}{b_2 + a_2}\right), \left(a_1, b_1, \frac{a_1 b_2 - a_2 b_1}{b_2 - a_2}\right)$$

for some a_1, a_2, b_1, $b_2 \in \mathbb{Z}$ such that ${a_1}^2 - d{a_2}^2 = {b_1}^2 - d{b_2}^2 = -1$ by Proposition 1. Henceforth, we consider the condition that the rational numbers

$$c_+ = \frac{a_1 b_2 + a_2 b_1}{b_2 + a_2} \quad \text{or} \quad c_- = \frac{a_1 b_2 - a_2 b_1}{b_2 - a_2}$$

are integers. In the general case, we denote $f_n^{(d)}$ and $g_n^{(d)}$ by f_n and g_n, respectively. Suppose that $0 < a_1$ and $0 < a_2 < b_2$. Then $(a_1, a_2) = (f_k, g_k)$ and $(b_1, b_2) = (\pm f_l, g_l)$ for some odd indices k and l such that $k < l$.

`Case 1:` Suppose that

$$(a_1, a_2) = (f_{2i-1}, g_{2i-1}) \quad \text{and} \quad (b_1, b_2) = (f_{(2i-1)+(4j-2)}, g_{(2i-1)+(4j-2)})$$

for some integers i, $j > 0$. Then we have

$$c_+ = \frac{g_{4(i+j-1)}}{2f_{2(i+j-1)}g_{2j-1}} = \frac{g_{2(i+j-1)}}{g_{2j-1}}$$

by (28), (35), and (32). This implies that $c_+ \in \mathbb{Z}$ holds if and only if $g_{2j-1} \mid g_{2(i+j-1)}$, which is equivalent to $2j-1 \mid 2(i+j-1)$ by Theorem 11(d), and to $2j-1 \mid 2i-1$. Letting $j = m$ and $2i-1 = (2m-1)(2n-1)$, we obtain

$$(a_1, b_1, c_+) = \left(f_{(2m-1)(2n-1)}, f_{(2m-1)(2n+1)}, \frac{g_{(2m-1)\cdot 2n}}{g_{2m-1}} \right).$$

Furthermore, $c_- = -{c_+}^{-1} \notin \mathbb{Z}$, since $g_{(2m-1)\cdot 2n} > g_{2m-1}$.

`Case 2:` Suppose that

$$(a_1, a_2) = (f_{2i-1}, g_{2i-1}) \quad \text{and} \quad (b_1, b_2) = (-f_{(2i-1)+(4j-2)}, g_{(2i-1)+(4j-2)})$$

for some integers i, $j > 0$. Then we have

$$c_- = \frac{g_{4(i+j-1)}}{2g_{2(i+j-1)}f_{2j-1}} = \frac{f_{2(i+j-1)}}{f_{2j-1}}$$

by (28), (36), and (32). This implies that $c_- \in \mathbb{Z}$ holds if and only if $f_{2j-1} \mid f_{2(i+j-1)}$, which is equivalent to $d = 2$ and $j = 1$ by Theorem 11(c), since $2(i+j-1)$ is not a multiple of $2j-1$ whose quotient is odd. Letting $i = n$, we obtain

$$(a_1, b_1, c_-) = (f^{(2)}_{2n-1}, -f^{(2)}_{2n+1}, f^{(2)}_{2n}).$$

Furthermore, $c_+ = -{c_-}^{-1} \notin \mathbb{Z}$, since $f^{(2)}_{2n} > 1$.

`Case 3:` Suppose that

$$(a_1, a_2) = (f_{2i-1}, g_{2i-1}) \quad \text{and} \quad (b_1, b_2) = (f_{(2i-1)+4j}, g_{(2i-1)+4j})$$

for some integers i, $j > 0$. Then we have

$$c_+ = \frac{g_{4(i+j)-2}}{2g_{2(i+j)-1}f_{2j}} = \frac{f_{2(i+j)-1}}{f_{2j}}$$

by (28), (35), and (32). In addition, $f_{2(i+j)-1}$ is not a multiple of f_{2j} by Theorem 11(c), since $2(i+j)-1$ is not a multiple of $2j$ whose quotient is odd. These imply $c_+ \notin \mathbb{Z}$. Furthermore, $c_- = -{c_+}^{-1} \notin \mathbb{Z}$, since $f_{2(i+j)-1} > f_{2j}$.

`Case 4:` Suppose that

$$(a_1, a_2) = (f_{2i-1}, g_{2i-1}) \quad \text{and} \quad (b_1, b_2) = (-f_{(2i-1)+4j}, g_{(2i-1)+4j})$$

for some integers i, $j > 0$. Then we have

$$c_- = \frac{g_{4(i+j)-2}}{2f_{2(i+j)-1}g_{2j}} = \frac{g_{2(i+j)-1}}{g_{2j}}$$

by (28), (36), and (32). In addition, $g_{2(i+j)-1}$ is not a multiple of g_{2j} by Theorem 11(d), since $2(i+j)-1$ is not a multiple of $2j$. These imply $c_- \notin \mathbb{Z}$. Furthermore, $c_+ = -{c_-}^{-1} \notin \mathbb{Z}$, since $g_{2(i+j)-1} > g_{2j}$.

Considering the sign changes, it is concluded that every nontrivial integral solution of (1) is given by (9) or (10) after switching a and b if necessary.

It is easy to verify that every triple of Form (9) or (10) is an integral solution of (1). □

Example 4. (a) For a given integer $e > 0$, (1) has integral solutions

$$(a, b, c) = \pm(e, e(4e^2+3), 2e),$$

where e and $e(4e^2+3)$ are the x-components of the first and third smallest solutions $(x, y) = (e, 1)$ and $(x, y) = (e(4e^2+3), 4e^2+1)$ of $|x^2-(e^2+1)y^2| = 1$, respectively.

(b) Integral solutions of $|x^2 - 2y^2| = 1$ produce the following integral solutions of (1): the first few solutions of Form (9) are

$(f_1^{(2)}, f_3^{(2)}, g_2^{(2)}/g_1^{(2)}) = (1, 7, 2)$, $(f_3^{(2)}, f_5^{(2)}, g_4^{(2)}/g_1^{(2)}) = (7, 41, 12)$, $(f_5^{(2)}, f_7^{(2)}, g_6^{(2)}/g_1^{(2)}) = (41, 239, 70)$,

$(f_3^{(2)}, f_9^{(2)}, g_6^{(2)}/g_3^{(2)}) = (7, 1393, 14)$, $(f_9^{(2)}, f_{15}^{(2)}, g_{12}^{(2)}/g_3^{(2)}) = (1393, 275807, 2772)$,

$(f_5^{(2)}, f_{15}^{(2)}, g_{10}^{(2)}/g_5^{(2)}) = (41, 275807, 82)$,

and the first few solutions of Form (10) are

$(f_1^{(2)}, -f_3^{(2)}, f_2^{(2)}) = (1, -7, 3)$, $(f_3^{(2)}, -f_5^{(2)}, f_4^{(2)}) = (7, -41, 17)$, $(f_5^{(2)}, -f_7^{(2)}, f_6^{(2)}) = (41, -239, 99)$.

(c) Integral solutions of $|x^2 - 5y^2| = 1$ produce the following integral solutions of (1): the first few solutions of Form (9) are

$(f_1^{(5)}, f_3^{(5)}, g_2^{(5)}/g_1^{(5)})$ $(f_3^{(5)}, f_5^{(5)}, g_4^{(5)}/g_1^{(5)})$ $(f_5^{(5)}, f_7^{(5)}, g_6^{(5)}/g_1^{(5)})$
$= (2, 38, 4)$, $= (38, 682, 72)$, $= (682, 12238, 1292)$,

$(f_3^{(5)}, f_9^{(5)}, g_6^{(5)}/g_3^{(5)})$ $(f_9^{(5)}, f_{15}^{(5)}, g_{12}^{(5)}/g_3^{(5)})$
$= (38, 219602, 76)$, $= (219602, 1268860318, 439128)$,

$(f_5^{(5)}, f_{15}^{(5)}, g_{10}^{(5)}/g_5^{(5)})$
$= (682, 1268860318, 1364)$.

Acknowledgement. The author is grateful to the managing editor Bruce Landman and the anonymous referee, who read the manuscript with great care and offered many helpful comments and suggestions.

References

[1] T. Andreescu and D. Andrica, *Quadratic Diophantine Equations* (*Developments in Mathematics* **40**), Springer, New York, 2015.

[2] N. Aoki, *Number Theory of Prime Numbers and Quadratic Fields*, Kyoritsu Publ., Tokyo, 2012, in Japanese.

[3] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math. (2)*, **15** (1913-1914), no. 1/4, 30-48.

[4] K. Conrad, Pell's equation, II, `https://api.semanticscholar.org/CorpusID:14314437` (Retrieved November 28, 2024).

[5] T. Koshy, *Pell and Pell–Lucas Numbers with Applications*, Springer, New York, 2014.

[6] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, FL, 1996.

[7] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.

[8] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York, 1996.

Appendix

In Theorem 1, for $d \leq 34$ such that $x^2 - dy^2 = -1$ has a rational solution and $p \leq 29$, the values of η and ξ_p are summarized in Table 1. For reference, we add the values of $N(\eta)$ and $N(\xi_p)$ below the values of η and ξ_p, respectively. We also add the value of the ideal class number h of $\mathbb{Q}(\sqrt{d})$.

d	2	5	10	13
h	1	1	2	1
η	$1+\sqrt{2}$ -1	$(1+\sqrt{5})/2$ -1	$3+\sqrt{10}$ -1	$(3+\sqrt{13})/2$ -1
ξ_2		$3+\sqrt{5}$ 2^2		$11+3\sqrt{13}$ 2^2
ξ_3			$7+2\sqrt{10}$ 3^2	$4+\sqrt{13}$ 3
ξ_5				
ξ_7	$3+\sqrt{2}$ 7			
ξ_{11}		$4+\sqrt{5}$ 11		
ξ_{13}			$23+6\sqrt{10}$ 13^2	
ξ_{17}	$5+2\sqrt{2}$ 17			$15+4\sqrt{13}$ 17
ξ_{19}		$8+3\sqrt{5}$ 19		
ξ_{23}	$5+\sqrt{2}$ 23			$6+\sqrt{13}$ 23
ξ_{29}		$7+2\sqrt{5}$ 29		$9+2\sqrt{13}$ 29

d	17	26	29	34
h	1	2	1	2
η	$4+\sqrt{17}$ -1	$5+\sqrt{26}$ -1	$(5+\sqrt{29})/2$ -1	$35+6\sqrt{34}$ 1
ξ_2	$5+\sqrt{17}$ 2^3		$27+5\sqrt{29}$ 2^2	
ξ_3				$5+\sqrt{34}$ -3^2
ξ_5		$21+4\sqrt{26}$ 5^2	$11+2\sqrt{29}$ 5	$3+\sqrt{34}$ -5^2
ξ_7			$6+\sqrt{29}$ 7	
ξ_{11}		$15+2\sqrt{26}$ 11^2		$27+5\sqrt{34}$ -11^2
ξ_{13}	$9+2\sqrt{17}$ 13		$97+18\sqrt{29}$ 13	
ξ_{17}		$11+2\sqrt{26}$ 17		
ξ_{19}	$6+\sqrt{17}$ 19	$45+8\sqrt{26}$ 19^2		
ξ_{23}		$7+\sqrt{26}$ 23	$38+7\sqrt{29}$ 23	
ξ_{29}				$3+5\sqrt{34}$ -29^2

Table 1: The values of η, $N(\eta)$, ξ_p, and $N(\xi_p)$ for $d \leq 34$ and $p \leq 29$ in Theorem 1.