Hang Lung Mathematics Awards
Vol. 9 (2021), pp. 55–83

SOLVABILITY OF THE GENERAL PELL'S EQUATION, QUADRATIC RESIDUOSITY, AND REAL QUADRATIC FIELDS OF CLASS NUMBER TWO

A RESEARCH REPORT SUBMITTED TO THE SCIENTIFIC COMMITTEE OF THE HANG LUNG MATHEMATICS AWARDS

TEAM MEMBER
LAI WAI LOK

TEACHER
MR. CHEUNG PAK LEONG

SCHOOL
ST. PAUL'S CO-EDUCATIONAL COLLEGE

AUGUST 2021

Abstract. A new and practical test for determining the solvability of the general Pell's equation $x^2 - Dy^2 = n$ will be offered through proving one necessary condition and one sufficient condition for this renowned quadratic Diophantine equation to be solvable in integers. The test involves only prime factorization and checking of certain simple quadratic residuosity relations. While the necessary condition will be comparatively more straightforward, the sufficient condition in a form of conditional converse of the former will require algebraic number theory tools to formulate and analyze. To prove this sufficient condition, the solvability in question will be transformed into the question of principality of certain well-designed ideal class in a real quadratic field $\mathbb{Q}(\sqrt{D})$ of class number two.

Keywords. General Pell's Equation, Negative Pell's Equation, Quadratic Residue, Real Quadratic Field, Class Number, Ideal Class Group, Principal Ideal

Contents

1. Introduction

1.1. **Research background.** The **general Pell's equation** is the quadratic Diophantine equation

$$x^2 - Dy^2 = n, \tag{1}$$

where D is a positive integer and n is an integer. It has fascinated numerous mathematicians for millennia since its original form $x^2-Dy^2 = 1$ appeared and was studied in 400 BC, and research on this topic is still very active (e.g. [4] on the negative Pell's equation $x^2-Dy^2 = -1$). The reader may consult [1] for an up-to-date survey on quadratic Diophantine equations and the general Pell's equation in particular.

For any Diophantine equation, the foremost topic is whether it is solvable, and if it is, how many solutions are there, and how to find some or certain specific or all of them. Regarding the general Pell's equation, they are described as the *Pell decision problem* and the *Pell search problem* in [1], Section 4.2, p.62. To name a few of the plenty of, from classical to modern, existing results about and methods to tackle the general Pell's equation, they may include certain bounds that limit the sizes of potential solutions, after which brute-force search is enabled, also Brahmagupta's identity that generates new solvable general Pell's equation from other solvable ones, continued fractions method, Lagrange's reduction method, the Lagrange–Matthews–Mollin (LMM) method, etc.. Nevertheless, simple and practical tests for determining its solvability are rather rare — our project is devoted to bridging this deficit, and can be treated as a novel response to the aforementioned decision problem.

1.2. **Our work and paper organization.** In Section 2.1, after some basic observations on the solvability (expressed as **Condition R**) of the general Pell's equation, we will construct two relevant relations (expressed as **Conditions P** and **Q**) between D and n that are number theoretic in nature. These two relations will constitute a necessary condition for the general Pell's equation to be solvable, as stated in our first main result **Theorem A**. In Section 2.2, a minimal amount of algebraic number theory notions will be collected in order to state our second main result **Theorem B**, which is a sufficient condition for the required solvability. **Theorem B** will be a conditional converse of **Theorem A**, and the necessity of the extra assumptions involved will also be explained.

In the short Section 3, we will prove **Theorem A**, painlessly as the needed basic properties of **Conditions P**, **Q** and **R** would have already been collected in Section 2 during introducing our main results.

To prove the much harder **Theorem B**, a lot of preparations will be needed. In this regard, in Section 4, key properties of quadratic residuosity from classical number theory will be collected in Section 4.1, using which further properties of **Conditions P**, **Q** and **R** will be produced in Section 4.2. Section 5 will be devoted to transforming the solvability problem into algebraic number theory terms. For such purpose, a well-designed ideal class in real quadratic fields will be introduced in Section 5.1, as well as proving its many fundamental properties. The transformation will be done in Section 5.2, into the question of principality of this ideal class.

Via the tools developed in Sections 4 and 5, more further properties of **Conditions P**, **Q** and **R** will be derived in Section 6.1. A focused study on the two main scenarios of **Theorem B** will be done in Sections 6.1.1 and 6.1.2, producing two weaker versions of **Theorem B**. Certain sophisticated modifications on n will bridge us towards completing a proof of the full **Theorem B** in Section 6.2.

A couple of final remarks before entering the main body: (i) as far as the solvability of the general Pell's equation is concerned, we will confine ourselves to an unspecified fixed squarefree D, which will be assumed throughout without losing any generality as supported by [3], p.41, Exercise 5.1; also, (ii) n will be assumed nonzero as such case will be trivially solvable. At last, the following notations will be adopted throughout the paper:

Notation	Definition
$\mathbb{Z}$	the set of integers
$\mathbb{Z}^*$	the set of nonzero integers
$\mathbb{N}$	the set of natural numbers
$\mathbb{P}$	the set of prime numbers
$\mathcal{Q}_n$	the set of quadratic residues modulo $n \in \mathbb{Z}^*$ (i.e. $\{m \in \mathbb{Z} \mid a^2 \equiv m \pmod{n}$ for some $a \in \mathbb{Z}\}$)
$\mathbb{M}$	the set of moduli for which D is a quadratic residue (i.e. $\{n \in \mathbb{Z}^* \mid D \in \mathcal{Q}_n\}$)

2. Our solvability tests for the general Pell's equation

2.1. **A necessary condition motivated by quadratic residuosity.**

Being the main concern, we introduce the following shorthand to denote the solvability of the general Pell's equation:

Condition R. (Solvability of general Pell's equation) For $n \in \mathbb{Z}^*$, $\mathbf{R}(n)$ stands for the condition that the general Pell's equation (1) is solvable.

It is natural to begin with investigating necessary conditions for the solvability of the general Pell's equation. If $(x, y) = (x_0, y_0)$ solves the equation, then taking modulo D on (1) would leave us with $x_0^2 \equiv n \pmod{D}$, which means that $n \in \mathcal{Q}_D$. This simple observation has inspired us to formulate the following relation (**Q** stands for quadratic residuosity) between D and n in (1):

Condition Q. (Quadratic residuosity) For $n \in \mathbb{Z}^*$, $\mathbf{Q}(n)$ stands for the condition that $c(n) \in \mathcal{Q}_D$, where c is the function to be defined in Definition 2.1.

Definition 2.1. (Modifications of factors) *Define*

(a) $c(-1) \coloneqq -1$,
(b) $c(p) \coloneqq p$ *for* $p \in \mathbb{P}$ *with* $p \nmid D$,
(c) $c(p) \coloneqq p - \frac{D}{p}$ *for* $p \in \mathbb{P}$ *with* $p \mid D$, *and*
(d) $c(mn) \coloneqq c(m)c(n)$ *for* $m, n \in \mathbb{Z}^*$.

From the definition, the function c can be written explicitly as

$$c(n) = \operatorname{sgn}(n) \prod_{\substack{p \in \mathbb{P} \\ p \nmid D}} p^{\nu_p(n)} \prod_{\substack{p \in \mathbb{P} \\ p \mid D}} \left(p - \frac{D}{p}\right)^{\nu_p(n)} \quad \text{for } n \in \mathbb{Z}^*, \tag{2}$$

where $\nu_p(n)$ denotes the p-adic order of n. It is clear then that $c(n) = n$ iff $(n, D) = 1$. We have chosen the letter c due to the following immediate property:

Lemma 2.2. (Coprimality between $c(n)$ and D) *Suppose* $n \in \mathbb{Z}^*$. *Then,* $(c(n), D) = 1$.

Proof. Suppose the contrary that there exists $q \in \mathbb{P}$ such that $q \mid (c(n), D)$. Then, it follows from the form of (2) that there exists $p \in \mathbb{P}$ such that $p \mid D$ and

$$q \mid \left(p - \frac{D}{p}\right). \tag{3}$$

If $p = q$, then (3) becomes $p \mid \left(p - \frac{D}{p}\right)$, then we would have $p \mid \frac{D}{p}$ and then $p^2 \mid D$, contradicting that D is squarefree. If $p \neq q$, then $p, q \mid D$ would imply $pq \mid D$ as $p, q \in \mathbb{P}$, and then $q \mid \frac{D}{p}$, with which (3) would imply that $q \mid p$, contradicting that $p \neq q$ and $p, q \in \mathbb{P}$. Therefore, $(c(n), D) = 1$. □

It is also natural to investigate how the general Pell's equation (1) with different n are related. On one hand, it is well-known that Condition **R** is multiplicative:

Lemma 2.3. (Multiplicativity of Condition R; Brahmagupta's identity) *Suppose* $m, n \in \mathbb{Z}^*$. *If both of* $\mathbf{R}(m)$ *and* $\mathbf{R}(n)$ *hold, then so does* $\mathbf{R}(mn)$.

Proof. Since both of $\mathbf{R}(m)$ and $\mathbf{R}(n)$ hold, there exist $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $x_1^2 - Dy_1^2 = m$ and $x_2^2 - Dy_2^2 = n$. By Brahmagupta's identity, we have

$$(x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 = (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = mn \tag{4}$$

thus, $(x, y) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1)$ solves $x^2 - Dy^2 = mn$, and $\mathbf{R}(mn)$ holds. □

On the other hand, we have observed the following simple situations where Condition **R** is reducible by squares:

Lemma 2.4. (Reducibility of Condition R by square of prime) *Suppose* $n \in \mathbb{Z}^*$ *and* $(x, y) = (x_0, y_0)$ *solves the general Pell's equation* (1) *so that* $\mathbf{R}(n)$ *holds.*

(a) *If* $p \in \mathbb{P}$ *and* $p \mid D$, *then* $p^2 \mid n$ *and* $(x, y) = \left(\frac{x_0}{p}, \frac{y_0}{p}\right)$ *solves* $x^2 - Dy^2 = \frac{n}{p^2}$ *so that* $\mathbf{R}\left(\frac{n}{p^2}\right)$ *holds.*

(b) *If* $p \in \mathbb{P} \setminus \mathbb{M}$ *and* $p \mid n$, *then* $p^2 \mid n$ *and* $(x, y) = \left(\frac{x_0}{p}, \frac{y_0}{p}\right)$ *solves* $x^2 - Dy^2 = \frac{n}{p^2}$ *so that* $\mathbf{R}\left(\frac{n}{p^2}\right)$ *holds.*

(c) *If* $D \equiv 2, 3 \pmod 4$ *and* $4 \mid n$, *then* $(x, y) = \left(\frac{x_0}{2}, \frac{y_0}{2}\right)$ *solves* $x^2 - Dy^2 = \frac{n}{4}$ *so that* $\mathbf{R}\left(\frac{n}{4}\right)$ *holds.*

Proof. It suffices to show that $p \mid x_0, y_0$ for (a) and (b), and that $2 \mid x_0, y_0$ for (c):

(a) Since $p \mid D$, taking modulo p on (1) yields $x_0^2 \equiv 0 \pmod p$, so $p \mid x_0$ as $p \in \mathbb{P}$, and then

$$p^2 \mid x_0^2. \tag{5}$$

With (5), taking modulo p^2 this time on (1) yields $Dy_0^2 \equiv 0 \pmod{p^2}$. Since D is squarefree, $p^2 \nmid D$, so $p \mid y_0^2$, and then $p \mid y_0$.

(b) Since $p \mid n$, taking modulo p on (1) yields

$$x_0^2 \equiv Dy_0^2 \pmod p. \tag{6}$$

If $p \nmid y_0$, then the inverse $\overline{y_0} \pmod p$ exists as $p \in \mathbb{P}$, and then multiplying (6) by $\overline{y_0}^2$, we would have

$$(x_0\overline{y_0})^2 \equiv Dy_0^2\overline{y_0}^2 = D(y_0\overline{y_0})^2 \equiv D \pmod p.$$

But this means that $D \in \mathcal{Q}_p$, contradicting that $p \notin \mathbb{M}$. Therefore,

$$p \mid y_0. \tag{7}$$

With (7) and $p \mid n$, we have $p \mid (n + Dy_0^2) = x_0^2$, and then $p \mid x_0$ as $p \in \mathbb{P}$.

(c) Since $4 \mid n$, taking modulo 4 on (1) yields

$$x_0^2 \equiv Dy_0^2 \pmod 4. \tag{8}$$

If x_0 is odd, then (8) would cause the following contradiction:

$$\begin{aligned} 1 &\equiv D \cdot 0 \text{ or } D \cdot 1 \\ &= 0 \text{ or } D \\ &\not\equiv 1 \pmod 4. \end{aligned}$$

Now knowing that x_0 has to be even, if y_0 is odd, then (8) would cause another contradiction: $0 \equiv D \cdot 1 = D \equiv 2 \text{ or } 3 \pmod 4$. Hence, both x_0 and y_0 are even.

□

The reducibility phenomenon, especially that from Lemma 2.4(b), has inspired us to formulate the following relation (**P** stands for prime and parity) between D and n in (1):

Condition P. (Parity of prime factor) For $n \in \mathbb{Z}^*$, $\mathbf{P}(n)$ stands for the condition that the p-adic order $\nu_p(n)$ of n is even for all $p \in \mathbb{P} \setminus \mathbb{M}$.

In Section 3, we will prove (not hard indeed) our first main result that Conditions **P** and **Q** are necessary for Condition **R**:

Theorem A. (Necessary condition for solvability of general Pell's equation) *Suppose $n \in \mathbb{Z}^*$. If $\mathbf{R}(n)$ holds, then so do $\mathbf{P}(n)$ and $\mathbf{Q}(n)$.*

Some general Pell's equations that have been tested non-solvable by Theorem A will be tabulated in Section 7 to illustrate the power of our theorem. Next, it is natural to study whether or to what extent the converse of Theorem A holds. In Section 2.2, we will introduce the relevant concepts from algebraic number theory in order to motivate and state our second main result at the end of the section.

2.2. **A sufficient condition motivated by ideal class groups of real quadratic fields.** An algebraic number is a zero of a polynomial with coefficients in $\mathbb{Z}$. The unique polynomial of the least degree with positive leading coefficient satisfied by an algebraic number is called the minimal polynomial of that algebraic number. An algebraic integer is an algebraic number with a monic minimal polynomial. For instance, the algebraic numbers of the form $x + y\sqrt{D}$ with $x, y \in \mathbb{Q}$, where D is a squarefree number, form a field $\mathbb{Q}(\sqrt{D})$ called **real quadratic field**. The algebraic integers in it form a ring called **real quadratic ring** when $D > 0$, which is either $\mathbb{Z}[\sqrt{D}] \coloneqq \{x + y\sqrt{D} \mid x, y \in \mathbb{Z}\}$ when $D = 2, 3 \pmod 4$ or $\{\frac{x}{2} + \frac{y}{2}\sqrt{D} \mid x, y \in \mathbb{Z}\}$ when $D = 1 \pmod 4$ ([2], p.106, Section 10.8).

Every ideal $\mathcal{I}$ in the ring $\mathcal{O}_\mathcal{K}$ of algebraic integers of an algebraic number field $\mathcal{K}$ must be finitely generated ([2], p.112, Theorem 11.1), i.e. $\mathcal{I} = (g_1, ..., g_n) \coloneqq \{r_1 g_1 + \cdots + r_n g_n \mid r_1, ..., r_n \in \mathcal{O}_\mathcal{K}\}$ for some $g_1, ..., g_n \in \mathcal{I}$. For any two ideals $\mathcal{I} = (a_1, ..., a_n)$ and $\mathcal{J} = (b_1, ..., b_m)$ in $\mathcal{O}_\mathcal{K}$, their product $\mathcal{I}\mathcal{J}$ is defined as the ideal

$$(a_1 b_1, ..., a_n b_1, a_1 b_2, ..., a_n b_2, ..., a_1 b_m, ..., a_n b_m)$$

in $\mathcal{O}_\mathcal{K}$ with generators $\{a_i b_j \mid i = 1, ..., n,\ j = 1, ..., m\}$ ([2], p.112, Section 11.2). Given any ideal $\mathcal{I}$ in $\mathcal{O}_\mathcal{K}$, an equivalence relation $\sim$ on $\mathcal{O}_\mathcal{K}$ can be constructed by defining that for any $a, b \in \mathcal{O}_\mathcal{K}$,

$$a \sim b \text{ if } a - b \in \mathcal{I}. \tag{9}$$

The **norm** $N(\mathcal{I})$ of $\mathcal{I}$ is defined as the number of equivalence classes of $\sim$ ([2], p.114, Section 11.5).

Lemma 2.5. (Norm of ideal) *Suppose $\mathcal{I}, \mathcal{J}$ are ideals in $\mathcal{O}_\mathcal{K}$.*

(a) $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$
(b) $N(\mathcal{I}) = 1$ *iff* $\mathcal{I} = \mathcal{O}_\mathcal{K}$
(c) Suppose $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ and $D \equiv 2, 3 \pmod 4$ so that $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{D}]$. For any ideal $\mathcal{I} = (x + y\sqrt{D})$, where $x, y \in \mathbb{Z}$, in $\mathcal{O}_\mathcal{K}$,

$$N(\mathcal{I}) = \left|x^2 - Dy^2\right|. \tag{10}$$

Proof. (a) See [2], p.115, Theorem 11.3.

(b) $N(\mathcal{I}) = 1$ iff $\sim$ has exactly one equivalence class, iff $a \sim b$ for all $a, b \in \mathcal{O}_\mathcal{K}$, or equivalently

$$a - b \in \mathcal{I} \text{ for all } a, b \in \mathcal{O}_\mathcal{K}. \tag{11}$$

If (11) is true, then by taking $b = 0$, we yield $\mathcal{O}_\mathcal{K} \subset \mathcal{I} \subset \mathcal{O}_\mathcal{K}$. If $\mathcal{I} = \mathcal{O}_\mathcal{K}$, then (11) becomes $a - b \in \mathcal{O}_\mathcal{K}$ for all $a, b \in \mathcal{O}_\mathcal{K}$, which is true by the closedness of the addition/subtraction in $\mathcal{O}_\mathcal{K}$.

(c) See [6], p.16, Example following Corollary 2, and p.46, Theorem 22(c).

□

Please take note of how well (10) resembles the left-hand side of the general Pell's equation (1). This phenomenon suggests that one may study the general Pell's equation through considering $\mathbb{Q}(\sqrt{D})$ as we will do for Theorem B, yet, at the cost of confining to $D \equiv 2, 3 \pmod 4$.

Another equivalence relation $\sim$ (same notation as above, but shall be distinguishable by the context) on the set of all ideals in $\mathcal{O}_\mathcal{K}$ can be constructed by defining that for any two ideals $\mathcal{I}$ and $\mathcal{J}$ in $\mathcal{O}_\mathcal{K}$,

$$\mathcal{I} \sim \mathcal{J} \text{ if } (a)\mathcal{I} = (b)\mathcal{J} \text{ for some } a, b \in \mathcal{K} \setminus \{0\}.$$

The equivalence classes of $\sim$ form a group with group operation

$$[\mathcal{I}][\mathcal{J}] = [\mathcal{I}\mathcal{J}]$$

and identity element $[\mathcal{O}_\mathcal{K}]$, which is called the **principal ideal class** as it consists of all the principal ideals (ideals with a single generator) in $\mathcal{O}_\mathcal{K}$. This group is called the **ideal class group** of $\mathcal{K}$ ([2], p.112 and 126, Theorem 11.2 and Section 12.3). The **class number** $h_\mathcal{K}$ of $\mathcal{K}$ is defined as its order, which must be finite ([2], p.127, Theorem 12.4). It is customary to use the shorthand h_D for the class numbers of $\mathbb{Q}(\sqrt{D})$.

Indeed, there were clues that the general Pell's equation has connections with (the class number of) $\mathbb{Q}(\sqrt{D})$ ([1], p.88, Theorem 4.5.5; see also [5]). We will study the general Pell's equation when $h_D = 2$ as assumed in Theorem B as in such case $\mathbb{Q}(\sqrt{D})$ will possess simple structures:

Lemma 2.6. (Class number two: principality, ideal equivalence) *Suppose $h_\mathcal{K} = 2$, and $\mathcal{I}, \mathcal{J}$ are ideals in $\mathcal{O}_\mathcal{K}$.*

(a) $\mathcal{J}^2$ is principal.

(b) $\mathcal{I} \sim \mathcal{J}$ iff $\mathcal{I}\mathcal{J}$ is principal.

Proof. (a) See [2], p.127, Theorem 12.4.

(b) If $\mathcal{I} \sim \mathcal{J}$, then multiplying $\mathcal{J}$ to both sides, we have $\mathcal{I}\mathcal{J} \sim \mathcal{J}^2$, showing the $\mathcal{I}\mathcal{J}$ is principal as $\mathcal{J}^2$ is by Lemma 2.6(a). If $\mathcal{I}\mathcal{J}$ is principal, then $\mathcal{I}\mathcal{J} \sim \mathcal{J}^2$ as $\mathcal{J}^2$ is principal by Lemma 2.6(a), and then multiplying $\mathcal{J}$ to both sides, we have $\mathcal{I}\mathcal{J}^2 \sim \mathcal{J}^3$, which reduces to $\mathcal{I} \sim \mathcal{J}$ as again $\mathcal{J}^2$ is principal by Lemma 2.6(a).

□

In the end, we formulated our second main result as below, and managed to prove it in Section 6, after plenty of preparations in Sections 4 and 5:

Theorem B. (Sufficient condition for solvability of general Pell's equation; conditional converse of Theorem A) *Suppose $n \in \mathbb{Z}^*$, $h_D = 2$ and $D \equiv 2, 3 \pmod 4$. Assume that D also satisfies either*

(i) $\mathbf{R}(-1)$ *holds (i.e. the negative Pell's equation is solvable) or*
(ii) $\mathbf{Q}(-1)$ *does not hold (i.e.* -1 *is a quadratic non-residue modulo* D*).*
If both $\mathbf{P}(n)$ *and* $\mathbf{Q}(n)$ *hold, then so does* $\mathbf{R}(n)$*.*

The class number assumption $h_D = 2$ is necessary, as we have found counter-examples (not shown here) for the theorem when the class number is greater. As remarked after Lemma 2.5, $D \equiv 2, 3 \pmod 4$ is unavoidable for our technique to work. The further assumptions (i) and (ii) will not join our discussion before Section 6. Despite these extra assumptions, it seems that Theorem B would still be applicable to a majority of D with $h_D = 2$ as the following lists of $D \leq 100$ (extracted from OEIS A029702 [8], A031396 [9] and A192450 [10] respectively) suggest. In the lists, D satisfying $h_D = 2$ and either (i) or (ii) are underlined, and non-squarefree D not satisfying $D \equiv 2, 3 \pmod 4$ are crossed out:

- $h_D = 2$: 10, 15, 26, 30, 34, 35, 39, 42, 51, 55, 58, ~~65~~, 66, 70, 74, 78, ~~85~~, 87, 91, 95, ...
- $\mathbf{R}(-1)$ holds: ~~1~~, 2, ~~5~~, 10, ~~13~~, ~~17~~, 26, ~~29~~, ~~37~~, ~~41~~, 50, ~~53~~, 58, ~~61~~, ~~65~~, ~~73~~, 74, 82, ~~85~~, ~~89~~, ~~97~~, ...
- $\mathbf{Q}(-1)$ does not hold: 3, ~~4~~, 6, 7, ~~8~~, ~~9~~, 11, ~~12~~, 14, 15, ~~16~~, 18, 19, ~~20~~, ~~21~~, 22, 23, ~~24~~, 27, ~~28~~, 30, 31, ~~32~~, ~~33~~, 35, ~~36~~, 38, 39, ~~40~~, 42, 43, ~~44~~, ~~45~~, 46, 47, ~~48~~, ~~49~~, 51, ~~52~~, 54, 55, ~~56~~, ~~57~~, 59, ~~60~~, 62, 63, ~~64~~, 66, 67, ~~68~~, ~~69~~, 70, 71, ~~72~~, 75, ~~76~~, ~~77~~, 78, 79, ~~80~~, ~~81~~, 83, ~~84~~, 86, 87, ~~88~~, 90, 91, ~~92~~, ~~93~~, 94, 95, ~~96~~, 98, 99, ~~100~~, ...

Some general Pell's equations that have been tested solvable by Theorem B will be tabulated in Section 7 to illustrate the power of our theorem.

3. Proof of Theorem A

Here we state our first main result again and prove:

Theorem A. (Necessary condition for solvability of general Pell's equation) *Suppose* $n \in \mathbb{Z}^*$*. If* $\mathbf{R}(n)$ *holds, then so do* $\mathbf{P}(n)$ *and* $\mathbf{Q}(n)$*.*

Proof. Assume that $\mathbf{R}(n)$ holds.

To prove that $\mathbf{P}(n)$ holds, suppose the contrary that there exist $p \in \mathbb{P} \setminus \mathbb{M}$ and $k \in \mathbb{N}$ such that $\nu_p(n) = 2k - 1$, i.e. $n = p^{2k-1}n'$ with $n' \in \mathbb{Z}^*$ and $p \nmid n'$. Since $p \in \mathbb{P} \setminus \mathbb{M}$, beginning with that $\mathbf{R}(n)$ holds, Lemma 2.4(b) can be applied $k-1$ times to obtain the following sequence:

$$\mathbf{R}\big(p^{2k-1}n'\big) \text{ holds } \Rightarrow \mathbf{R}\big(p^{2k-3}n'\big) \text{ holds } \Rightarrow \mathbf{R}\big(p^{2k-5}n'\big) \text{ holds } \Rightarrow \cdots \Rightarrow \mathbf{R}(pn') \text{ holds.}$$

Applying Lemma 2.4(b) once more would yield $p^2 \mid pn'$ or $p \mid n'$, which contradicts that $p \nmid n'$. Thus, $\mathbf{P}(n)$ holds.

We move on to prove that $\mathbf{Q}(n)$ also holds. To this end, we will derive that $\mathbf{R}(c(n))$ holds first. If $(n, D) = 1$, then $c(n) = n$ and we are done. If $(n, D) > 1$, write $n = (n, D)n'$ and $(n, D) = \prod_{i=1}^{m} p_i^{e_i}$, where $m \in \mathbb{N}$, $p_i \in \mathbb{P}$ and $e_i \in \mathbb{N}$ for all i. Since $(n', D) = 1$ and all $p_i \mid D$, by using (2), we have

$$n\prod_{i=1}^{m}(p_i^2 - D)^{e_i} = n'\prod_{i=1}^{m} p_i^{e_i}(p_i^2 - D)^{e_i} = n'\prod_{i=1}^{m} p_i^{2e_i}\left(p_i - \frac{D}{p_i}\right)^{e_i} = c(n)\prod_{i=1}^{m} p_i^{2e_i}. \tag{12}$$

Besides that $\mathbf{R}(n)$ holds, all $\mathbf{R}\big(p_i^2 - D\big)$ also hold as $(x, y) = (p_i, 1)$ solves $x^2 - Dy^2 = p_i^2 - D$, thus by using Lemma 2.3 with (12), we have

$$\text{both } \mathbf{R}(n) \text{ and all } \mathbf{R}\big(p_i^2 - D\big) \text{ hold} \quad \Rightarrow \quad \mathbf{R}\left(n \prod_{i=1}^{m} (p_i^2 - D)^{e_i}\right) \text{ holds} \quad \Rightarrow \quad \mathbf{R}\left(c(n) \prod_{i=1}^{m} p_i^{2e_i}\right) \text{ holds.}$$

Moreover, since all $p_i \mid D$, removing squares of primes by using Lemma 2.4(a), we obtain the desired conclusion that $\mathbf{R}(c(n))$ holds. With that $\mathbf{R}(c(n))$ holds, there exist $x_0, y_0 \in \mathbb{Z}$ such that $x_0^2 - Dy_0^2 = c(n)$. Taking modulo D yields $x_0^2 \equiv c(n) \pmod{D}$, thus $c(n) \in \mathcal{Q}_D$, and $\mathbf{Q}(n)$ holds. □

4. Classical Number Theory for Proving Theorem B

4.1. **Key properties of quadratic residuosity.**

Lemma 4.1. (Product of moduli) *Suppose $m, n \in \mathbb{Z}^*$ and $a \in \mathbb{Z}$. Then,*

(a) if $a \in \mathcal{Q}_{mn}$, then $a \in \mathcal{Q}_m, \mathcal{Q}_n$; and
(b) if $a \in \mathcal{Q}_m, \mathcal{Q}_n$ and $(m, n) = 1$, then $a \in \mathcal{Q}_{mn}$.

Proof. (a) If $a \in \mathcal{Q}_{mn}$ with $a \equiv r^2 \pmod{mn}$ for some $r \in \mathbb{Z}$, then $a \equiv r^2 \pmod{m, n}$ so that $a \in \mathcal{Q}_m$ and $a \in \mathcal{Q}_n$.

(b) Suppose $a \in \mathcal{Q}_m, \mathcal{Q}_n$ with $a \equiv r^2 \pmod{m}$ and $a \equiv s^2 \pmod{n}$ for some $r, s \in \mathbb{Z}$. Since $(m, n) = 1$, by the Chinese remainder theorem, $t \equiv r \pmod{m}$ and $t \equiv s \pmod{n}$ for some $t \in \mathbb{Z}$. Then, $t^2 \equiv r^2 \equiv a \pmod{m}$ and $t^2 \equiv s^2 \equiv a \pmod{n}$, and then $t^2 \equiv a \pmod{mn}$ as $(m, n) = 1$, so that $a \in \mathcal{Q}_{mn}$.

□

Lemma 4.2. (Products of quadratic residues and non-residues) *Suppose $n \in \mathbb{Z}^*$ and $a, b \in \mathbb{Z}$.*

(a) If $a, b \in \mathcal{Q}_n$, then $ab \in \mathcal{Q}_n$.
(b) If $a \in \mathcal{Q}_n$ and $(a, n) = 1$, then
(i) the inverse $\overline{a} \in \mathcal{Q}_n$, and
(ii) if $ab \in \mathcal{Q}_n$, then $b \in \mathcal{Q}_n$.
(c) If $ab \in \mathcal{Q}_n$ and $(a, n) = (b, n) = 1$, then either $a, b \in \mathcal{Q}_n$ or $a, b \notin \mathcal{Q}_n$.
(d) Suppose $(a, n) = (b, n) = 1$. Among a, b and ab, if any two of them are in $\mathcal{Q}_n$, then so is the third one.

Proof. (a) If $a, b \in \mathcal{Q}_n$ with $a \equiv r^2 \pmod{n}$ and $b \equiv s^2 \pmod{n}$ for some $r, s \in \mathbb{Z}$, then $ab \equiv (rs)^2 \pmod{n}$ so that and $ab \in \mathcal{Q}_n$.

(b)(i) $\overline{a} \pmod{n}$ exists as $(a, n) = 1$. If $a \in \mathcal{Q}_n$ with $a \equiv r^2 \pmod{n}$ for some $r \in \mathbb{Z}$, then $\overline{a} \equiv \overline{a}(\overline{a}a) \equiv \overline{a}^2 r^2 = (\overline{a}r)^2 \pmod{n}$ so that $\overline{a} \in \mathcal{Q}_n$.

(b)(ii) If $ab \in \mathcal{Q}_n$, then $b \equiv (\overline{a}a)b = \overline{a} \cdot ab \in \mathcal{Q}_n$ by using Lemma 4.2(a) and (b)(i).

(c) The contrary, without loss of generality, that $a \in \mathcal{Q}_n$ but $b \notin \mathcal{Q}_n$ contradicts Lemma 4.2(b)(ii) immediately.

(d) If $a, b \in \mathcal{Q}_n$, then it follows from Lemma 4.2(a) that $ab \in \mathcal{Q}_n$. If, without loss of generality, $a, ab \in \mathcal{Q}_n$, then it follows from Lemma 4.2(b)(ii) that $b \in \mathcal{Q}_n$.

□

Lemma 4.3. (Square roots modulo power of prime) *Suppose $p \in \mathbb{P}$, $p \neq 2$, $k \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $a^2 \equiv b^2 \pmod{p^k}$ and $p \nmid a$ or b, then $a \equiv \pm b \pmod{p^k}$.*

Proof. Suppose the contrary that $a^2 \equiv b^2 \pmod{p^k}$ but $a \not\equiv \pm b \pmod{p^k}$, i.e. $p^k \mid (a^2 - b^2) = (a+b)(a-b)$ and $p^k \nmid (a \pm b)$, then

$$\nu_p(a \pm b) < k \leq \nu_p(a^2 - b^2) = \nu_p(a+b) + \nu_p(a-b),$$

thus $\nu_p(a \pm b) > 0$ so that $p \mid (a \pm b)$. This would imply that $p \mid (a+b) \pm (a-b) = 2a, 2b$, and then $p \mid a, b$ as $p \neq 2$, which contradicts our assumptions. □

Lemma 4.4. (Number of quadratic residues modulo power of prime) *Suppose that $p \in \mathbb{P}$, $p \neq 2$ and $k \in \mathbb{N}$. Then, the set*

$$S = \left\{ n \in \mathcal{Q}_{p^k} \mid 0 \leq n < p^k,\ p \nmid n \right\} \tag{13}$$

has size $\frac{(p-1)p^{k-1}}{2}$.

Proof. In this proof, let $r(n)$ denote the remainder when dividing $n \in \mathbb{N} \cup \{0\}$ by p^k. We prove that $S = S'$ where

$$S' = \left\{ r(m^2) \mid 0 \leq m < \frac{p^k}{2},\ p \nmid m \in \mathbb{Z} \right\},$$

and count its elements.

It is clear from construction that $S' \subset S$. To prove the reversed inclusion, suppose $n \in S$ with $s^2 \equiv n \pmod{p^k}$ for some $s \in \mathbb{N} \cup \{0\}$. First, note that $p^k - r(s), r(s) \geq 0$. Second, since $p \neq 2$ so that $\frac{p^k}{2} \notin \mathbb{Z}$, we have $r(s) \neq \frac{p^k}{2}$, then it follows that $m = \min\left\{p^k - r(s), r(s)\right\} < \frac{p^k}{2}$. Moreover, since $r(s) - p^k \equiv r(s) \equiv s \pmod{p^k}$, we have

$$(p^k - r(s))^2 \equiv r(s)^2 \equiv s^2 \equiv n \pmod{p^k}.$$

As a result, $n = r(m^2) \in S'$.

It remains to count the elements of S'. Indeed, if $r(m_1^2) = r(m_2^2)$ where $0 \leq m_1, m_2 < \frac{p^k}{2}$ and $p \nmid m_1, m_2 \in \mathbb{Z}$, then $m_1^2 \equiv m_2^2 \pmod{p^k}$, and then by Lemma 4.3, $m_1 \equiv \pm m_2 \pmod{p^k}$, and this would force $m_1 = m_2$ as $0 \leq m_1, m_2 < \frac{p^k}{2} < p^k$. Therefore, different elements of S' correspond to different m, and then

$$\begin{aligned} |S| = |S'| &= \left| \left\{ m \mid 0 \leq m < \frac{p^k}{2},\ p \nmid m \in \mathbb{Z} \right\} \right| \\ &= \left| \left\{ m \mid 1 \leq m \leq \frac{p^k - 1}{2},\ p \nmid m \in \mathbb{Z} \right\} \right| \\ &= \frac{p^k - 1}{2} - \left\lfloor \frac{p^k - 1}{2} \Im vp \right\rfloor = \frac{(p-1)p^{k-1}}{2} \end{aligned}$$

as the floor function term $= \left\lfloor \frac{p^{k-1}-1}{2} + \frac{p-1}{2p} \right\rfloor = \frac{p^{k-1}-1}{2}$. □

Lemma 4.5. (Quadratic residuosity modulo power of prime) *Suppose $p \in \mathbb{P}$, $p \neq 2$, $k \in \mathbb{N}$ and $p \nmid a \in \mathbb{Z}$. Then, $a \in \mathcal{Q}_p$ iff $a \in \mathcal{Q}_{p^k}$.*

Proof. The if part follows from Lemma 4.1(a). For the only if part, we shall show from (13) that $S = S''$ where

$$S'' = \left\{ n \in \mathcal{Q}_p \mid 0 \leq n < p^k,\ p \nmid n \right\}.$$

It is clear from construction that $S \subset S''$, so it suffices to show that $|S| = |S''|$. Indeed, partitioning S'' into equal intervals, we have

$$\begin{aligned} |S''| &= \left| \bigsqcup_{i=1}^{p^{k-1}} \{ n \in \mathcal{Q}_p \mid (i-1)p \leq n < ip,\ p \nmid n \} \right| \\ &= \sum_{i=1}^{p^{k-1}} |\{ n \in \mathcal{Q}_p \mid 0 \leq n < p,\ p \nmid n \}| \\ &= \sum_{i=1}^{p^{k-1}} \frac{p-1}{2} \quad \text{(Lemma 4.4 with } k = 1) \\ &= \frac{p-1}{2} \cdot p^{k-1} = |S| \end{aligned}$$

□

4.2. **Further properties of Conditions P, Q and R.**

Lemma 4.6. (Conditions P(m), P(n) and P(mn)) *Suppose $m, n \in \mathbb{Z}^*$. If any two of $\mathbf{P}(m), \mathbf{P}(n)$ and $\mathbf{P}(mn)$ hold, then so does the third one.*

Proof. Suppose the contrary, then there exists $p \in \mathbb{P} \setminus \mathbb{M}$ such that exactly one of $\nu_p(m)$, $\nu_p(n)$ and $\nu_p(mn)$ is odd, but then the parities of the terms in $\nu_p(m)+\nu_p(n) = \nu_p(mn)$ would become inconsistent.

□

Lemma 4.7. (Conditions Q(m), Q(n) and Q(mn)) *Suppose $m, n \in \mathbb{Z}^*$. If any two of $\mathbf{Q}(m), \mathbf{Q}(n)$ and $\mathbf{Q}(mn)$ hold, then so does the third one.*

Proof. By definition, these three conditions are equivalent to $c(m) \in \mathcal{Q}_D$, $c(n) \in \mathcal{Q}_D$ and $c(mn) \in \mathcal{Q}_D$ respectively. Since $(c(m), D) = (c(n), D) = 1$ by Lemma 2.2, the required result follows from replacing n by D and taking $a = c(m)$ and $b = c(n)$ in Lemma 4.2(d). □

Lemma 4.8. (Square factors vs Conditions P, Q and R) *Suppose $n, n', r \in \mathbb{Z}^*$ and $n = r^2 n'$.*

(a) $\mathbf{P}(n)$ holds iff $\mathbf{P}(n')$ holds.
(b) $\mathbf{Q}(n)$ holds iff $\mathbf{Q}(n')$ holds.
(c) If $\mathbf{R}(n')$ holds, then so does $\mathbf{R}(n)$.
(d) Suppose
(i) $r \in \mathbb{P} \setminus \mathbb{M}$ or
(ii) $r \in \mathbb{P}$, $r \mid 2D$ and $D \equiv 2$ or $3 \pmod 4$.
If $\mathbf{R}(n)$ holds, then so does $\mathbf{R}(n')$.

Proof. (a) It is trivial from definition that $\mathbf{P}(r^2)$ holds. Then, apply Lemma 4.6 with $m = r^2$.
(b) It is trivial with Definition 2.1 that $c(r^2) = c(r)^2 \in \mathcal{Q}_D$ so that $\mathbf{Q}(r^2)$ holds. Then, apply Lemma 4.7 with $m = r^2$.
(c) It is trivial that $\mathbf{R}(r^2)$ holds with $(x, y) = (r, 0)$ solving $x^2 - Dy^2 = r^2$. Then, apply Lemma 2.3 with $m = r^2$ and $n = n'$.
(d)(i) Exactly Lemma 2.4(b).
(d)(ii) If $r = 2$, apply Lemma 2.4(c); if not, we have $r \mid D$, then apply Lemma 2.4(a) with $p = r$.

□

Lemma 4.8(d) has motivated us to define the following function s:

Definition 4.9. (Removal of special square factors) *For*

$$n = \prod_i p_i^{2a_i+b_i} \prod_j q_j^{c_j} \in \mathbb{N},$$

where

- $p_i \in \mathbb{P} \setminus \mathbb{M}$ *or* $p_i \mid 2D$,
- $q_j \in \mathbb{P} \cap \mathbb{M}$ *and* $q_j \nmid 2D$ *and*
- $a_i, c_j \in \mathbb{N} \cup \{0\}$ *and* $b_i = 0, 1$,

define

$$s(n) \coloneqq \prod_i p_i^{b_i} \prod_j q_j^{c_j} \in \mathbb{N}.$$

An important property of $s(n)$ related to Condition **P** will be proved in Lemma 5.7(b).

5. Algebraic Number Theory for Proving Theorem B

From now on, we will assume $D \equiv 2, 3 \pmod 4$ in order that we can take $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{D}]$, and incorporate these real quadratic fields and real quadratic rings into our study. Also recall that $\mathbb{M} = \{n \in \mathbb{Z}^* \mid D \in \mathcal{Q}_n\}$ consists of all moduli for which D is a quadratic residue. There are two points to note in advance about $\mathbb{M}$. One is that $n \in \mathbb{M}$ iff $-n \in \mathbb{M}$, so that where appropriate, we may discuss only the positive integers in $\mathbb{M}$ without loss of generality. The other one is that if $n \in \mathbb{M}$ and $k \mid n$, then $k \in \mathbb{M}$ as a consquence of Lemma 4.1(a), and this property will be used frequently and implicitly without being emphasized.

This section is devoted to proving various properties of the following special ideals which will be crucial in proving Theorem B:

Definition 5.1. (Ideal $\mathcal{I}_{n,k}$) *Suppose $D \equiv 2, 3 \pmod 4$. For $n \in \mathbb{M}$ and $k \in \mathbb{Z}$ with $n \mid (k^2 - D)$, define*

$$\mathcal{I}_{n,k} \coloneqq (n, k + \sqrt{D}) = \left\{\alpha n + \beta(k + \sqrt{D}) \mid \alpha, \beta \in \mathcal{O}_\mathcal{K}\right\}$$

which is an ideal in $\mathcal{O}_\mathcal{K}$.

Lemma 5.2. (Ideal multiplication) *Suppose $D \equiv 2, 3 \pmod 4$, $a, b \in \mathbb{M}$, $k \in \mathbb{Z}$ with $a, b \mid (k^2 - D)$. If $(a, b) = 1$, then $\mathcal{I}_{a,k}\mathcal{I}_{b,k} = \mathcal{I}_{ab,k}$.*

Proof. Since $a, b \mid (k^2 - D)$ and $(a, b) = 1$, we have $ab \mid (k^2 - D)$ so that $ab \in \mathbb{M}$ and $\mathcal{I}_{ab,k}$ is also well-defined. On one hand, observe that each generator of

$$\begin{aligned}\mathcal{I}_{a,k}\mathcal{I}_{b,k} &= (a, k + \sqrt{D})(b, k + \sqrt{D}) \\ &= (ab, \underbrace{b}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}), \underbrace{a}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}), \underbrace{(k + \sqrt{D})}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}))\end{aligned}$$

lies in $\mathcal{I}_{ab,k} = (ab, k+\sqrt{D})$, thus $\mathcal{I}_{a,k}\mathcal{I}_{b,k} \subset \mathcal{I}_{ab,k}$. On the other hand, since $(a, b) = 1$, we have $\alpha a + \beta b = 1$ for some $\alpha, \beta \in \mathbb{Z}$, then the second generator of $\mathcal{I}_{ab,k}$

$$\begin{aligned}k + \sqrt{D} &= (\alpha a + \beta b)(k + \sqrt{D}) \\ &= \underbrace{\beta}_{\in\mathcal{O}_\mathcal{K}} b(k + \sqrt{D}) + \underbrace{\alpha}_{\in\mathcal{O}_\mathcal{K}} a(k + \sqrt{D}) \in \mathcal{I}_{a,k}\mathcal{I}_{b,k},\end{aligned}$$

thus $\mathcal{I}_{a,k}\mathcal{I}_{b,k} \supset \mathcal{I}_{ab,k}$. □

Lemma 5.3. (Ideal multiplication) *Suppose $D \equiv 2, 3 \pmod 4$, $n \in \mathbb{M}$ and $r \in \mathbb{N}$. If $(n, 2D) = 1$, then*

(a) $n^r \in \mathbb{M}$, and
(b) $\mathcal{I}_{n^{r+1},k} = \mathcal{I}_{n^r,k}\mathcal{I}_{n,k}$, where $k \in \mathbb{Z}$ and $n^{r+1} \mid (k^2 - D)$.

Proof.

(a) Consider the prime factorization $n = \operatorname{sgn}(n)\prod_i p_i^{e_i}$, where $p_i \in \mathbb{P}$ and $e_i = \nu_{p_i}(n) \geq 1$. Since $(n, 2D) = 1$, we have $p_i \neq 2$ and $p_i \nmid D$ for all i, then we can apply Lemmas 4.1 and 4.5 where appropriate to obtain

$$\begin{aligned}\mathcal{Q}_n = \mathcal{Q}_{\operatorname{sgn}(n)\prod_i p_i^{e_i}} &= \mathcal{Q}_{\operatorname{sgn}(n)}\bigcap_i \mathcal{Q}_{p_i^{e_i}} = \mathcal{Q}_{\operatorname{sgn}(n)}\bigcap_i \mathcal{Q}_{p_i} \\ &= \mathcal{Q}_{\operatorname{sgn}(n)^r}\bigcap_i \mathcal{Q}_{p_i^{e_i r}} = \mathcal{Q}_{\operatorname{sgn}(n)^r\prod_i p_i^{e_i r}} = \mathcal{Q}_{n^r}.\end{aligned}$$

Note that the fact $\mathcal{Q}_1 = \mathcal{Q}_{-1}$ may be needed here. Therefore, $n \in \mathbb{M}$ iff $n^r \in \mathbb{M}$.

(b) Since $n, n^r, n^{r+1} \mid (k^2 - D)$, we have $n, n^r, n^{r+1} \in \mathbb{M}$ so that $\mathcal{I}_{n,k}$, $\mathcal{I}_{n^r,k}$ and $\mathcal{I}_{n^{r+1},k}$ are well-defined. On one hand, observe that each generator of

$$\begin{aligned}\mathcal{I}_{n^r,k}\mathcal{I}_{n,k} &= (n^r, k + \sqrt{D})(n, k + \sqrt{D}) \\ &= (n^{r+1}, \underbrace{n^r}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}), \underbrace{n}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}), \underbrace{(k + \sqrt{D})}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}))\end{aligned}$$

lies in $\mathcal{I}_{n^{r+1},k} = (n^{r+1}, k+\sqrt{D})$, thus $\mathcal{I}_{n^r,k}\mathcal{I}_{n,k} \subset \mathcal{I}_{n^{r+1},k}$. On the other hand, we need to show that the second generator of $\mathcal{I}_{n^{r+1},k}$, namely $k+\sqrt{D}$, lies in $\mathcal{I}_{n^r,k}\mathcal{I}_{n,k}$ so that $\mathcal{I}_{n^r,k}\mathcal{I}_{n,k} \supset \mathcal{I}_{n^{r+1},k}$. To this end, write

$$D = k^2 + mn^{r+1} \tag{14}$$

for some $m \in \mathbb{Z}$. Note that $(k,n) = 1$ as if $p \mid k, n$ for some $p \in \mathbb{P}$, then by (14) we would have $p \mid D$, contradicting that $(n, 2D) = 1$. Moreover, by $(n, 2D) = 1$ again, n must be odd, thus $(2k, n^{r+1}) = 1$, and

$$\alpha(2k) + \beta n^{r+1} = 1 \tag{15}$$

for some $\alpha, \beta \in \mathbb{Z}$. Then, using (14) and (15), we can derive that

$$\begin{aligned}
\alpha(k^2 + D + 2k\sqrt{D}) &= \alpha(2k^2 + mn^{r+1} + 2k\sqrt{D}) \\
&= 2\alpha k(k+\sqrt{D}) + \alpha m n^{r+1} \\
&= (1 - \beta n^{r+1})(k+\sqrt{D}) + \alpha m n^{r+1} \\
k + \sqrt{D} &= \underbrace{(-\alpha m + \beta k + \beta\sqrt{D})}_{\in \mathcal{O}_\mathcal{K}} n^{r+1} + \underbrace{\alpha}_{\in \mathcal{O}_\mathcal{K}} (k+\sqrt{D})^2 \in \mathcal{I}_{n^r,k}\mathcal{I}_{n,k}.
\end{aligned}$$

□

Lemma 5.4. (Ideal multiplication) *Suppose $D \equiv 2, 3 \pmod 4$, $a, b \in \mathbb{Z}^*$, $ab \in \mathbb{M}$, $k \in \mathbb{Z}$ with $ab \mid (k^2 - D)$. If $(a, 2D) = (b, 2D) = 1$, then $\mathcal{I}_{a,k}\mathcal{I}_{b,k} = \mathcal{I}_{ab,k}$.*

Proof. Consider the prime factorizations $a = \operatorname{sgn}(a)\prod_i p_i^{a_i}$ and $b = \operatorname{sgn}(b)\prod_i p_i^{b_i}$ where $a_i = \nu_{p_i}(a)$ and $b_i = \nu_{p_i}(b)$ are allowed to be 0. Since $p_i, a, b, ab \mid (k^2 - D)$, we have $p_i, a, b \in \mathbb{M}$ so that $\mathcal{I}_{a,k}, \mathcal{I}_{b,k}, \mathcal{I}_{p_i,k}, \mathcal{I}_{p_i,k}, \mathcal{I}_{p_i^{a_i},k}$ and $\mathcal{I}_{p_i^{b_i},k}$ are also well-defined. Then, since $(p_i, p_j) = 1$ for $i \neq j$, we can apply Lemma 5.2 to obtain

$$\mathcal{I}_{a,k} = \mathcal{I}_{\prod_i p_i^{a_i},k} = \prod_i \mathcal{I}_{p_i^{a_i},k} \quad \text{and} \quad \mathcal{I}_{b,k} = \mathcal{I}_{\prod_i p_i^{b_i},k} = \prod_i \mathcal{I}_{p_i^{b_i},k}.$$

Moreover, since $(a, 2D) = (b, 2D) = 1$ so that all $(p_i, 2D) = 1$, by Lemma 5.3, they will then equal

$$\prod_i \mathcal{I}_{p_i,k}^{a_i} \quad \text{and} \quad \prod_i \mathcal{I}_{p_i,k}^{b_i}$$

respectively. Combining, we have

$$\mathcal{I}_{a,k}\mathcal{I}_{b,k} = \prod_i \mathcal{I}_{p_i,k}^{a_i} \prod_i \mathcal{I}_{p_i,k}^{b_i} = \prod_i \mathcal{I}_{p_i,k}^{a_i+b_i} = \prod_i \mathcal{I}_{p_i^{a_i+b_i},k} = \mathcal{I}_{ab,k},$$

and note that Lemma 5.3 is used once more in the second last step. □

Lemma 5.5. (Ideal norm) *Suppose $D \equiv 2, 3 \pmod 4$, $n \in \mathbb{M}$, $k \in \mathbb{Z}$ with $n \mid (k^2 - D)$. Then, $N(\mathcal{I}_{n,k}) = |n|$.*

Proof. Write $\mathcal{I} = \mathcal{I}_{n,k}$. Recall that $N(\mathcal{I})$ is defined as the number of equivalence classes of $\sim$ in $\mathcal{O}_\mathcal{K}$ given by (9).

Indeed, $[0], [1], .., [|n|-1]$ are different equivalence classes. If $i, j \in \{0, 1, ..., |n| - 1\}$ with $i \neq j$, then $i \sim j$ requires that $i - j \in \mathcal{I}$, i.e.

$$\begin{aligned} i - j &= (a + b\sqrt{D})n + (c + d\sqrt{D})(k + \sqrt{D}) \text{ for some } a, b, c, d \in \mathbb{Z} \\ &= (an + ck + dD) + (bn + c + dk)\sqrt{D} \\ &\equiv (ck + dD) + (c + dk)\sqrt{D} \pmod{|n|} \\ &= ((-dk)k + dD) + 0\sqrt{D} \quad \text{(by comparing rational and irrational parts)} \\ &= -d(k^2 - D) \equiv 0; \end{aligned}$$

however, since $-|n| < i - j < |n|$, we have $|n| \nmid (i - j)$, thus $i \not\sim j$.

Moreover, $[0], [1], .., [|n| - 1]$ are the only equivalence classes. If $a + b\sqrt{D} \in \mathcal{O}_\mathcal{K}$ where $a, b \in \mathbb{Z}$, then let $q \in \mathbb{Z}$ and $r \in \{0, 1, ..., |n| - 1\}$ be the quotient and the remainder respectively when dividing $a - bk$ by $|n|$, and then

$$(a + b\sqrt{D}) - r = (a - bk) - r + b(k + \sqrt{D}) = \underbrace{\frac{q\,|n|}{n}}_{\in\mathcal{O}_\mathcal{K}} n + \underbrace{b}_{\in\mathcal{O}_\mathcal{K}}(k + \sqrt{D}) \in \mathcal{I},$$

so that $a + b\sqrt{D} \sim r$. □

Lemma 5.6. (Principality of $\mathcal{I}_{n,k}\mathcal{I}_{n,-k}$) *Suppose $n \in \mathbb{M}$, $k \in \mathbb{Z}$ with $n \mid (k^2 - D)$. If $D \equiv 2, 3 \pmod 4$, then $\mathcal{I}_{n,k}\mathcal{I}_{n,-k} = (n)$.*

Proof. Let $k^2 - D = ln$ where $l \in \mathbb{Z}$. On one hand,

$$\begin{aligned} \mathcal{I}_{n,k}\mathcal{I}_{n,-k} &= (n, k + \sqrt{D})(n, -k + \sqrt{D}) \\ &= (n^2, n(-k + \sqrt{D}), n(k + \sqrt{D}), -k^2 + D) \\ &= (\underbrace{n}_{\in\mathcal{O}_\mathcal{K}} n, \underbrace{2k}_{\in\mathcal{O}_\mathcal{K}} n, \underbrace{l}_{\in\mathcal{O}_\mathcal{K}} n, \underbrace{(k + \sqrt{D})}_{\in\mathcal{O}_\mathcal{K}} n), \end{aligned}$$

where each generator lies in (n), thus $\mathcal{I}_{n,k}\mathcal{I}_{n,-k} \subset (n)$. On the other hand, if $(n^2, 2kn, ln) = n$ or $(n, 2k, l) = 1$, then the generator of (n)

$$n = \underbrace{\alpha}_{\in\mathcal{O}_\mathcal{K}} n^2 + \underbrace{\beta}_{\in\mathcal{O}_\mathcal{K}}(2kn) + \underbrace{\gamma}_{\in\mathcal{O}_\mathcal{K}} ln \in \mathcal{I}_{n,k}\mathcal{I}_{n,-k},$$

for some $\alpha, \beta, \gamma \in \mathbb{Z}$, so that $\mathcal{I}_{n,k}\mathcal{I}_{n,-k} \supset (n)$. To this end, suppose $p \mid n, 2k, l$ for some $p \in \mathbb{P}$, then $p^2 \mid (4k^2 - 4ln) = 4D$. Recall that D is squarefree, so $p^2 \nmid D$ but $p^2 \mid 4$, and $p = 2$. But if $p = 2$, then $4 = p^2 \mid ln = (k^2 - D)$, and then $D \equiv k^2 \equiv 0, 1 \pmod 4$, contradicting the assumption that $D \equiv 2, 3 \pmod 4$. □

Restricting to $D \equiv 2, 3 \pmod 4$ will also enable us to apply Lemma 2.4(c) to prove a characterization in the prime factors of the elements of $\mathbb{M}$. This will lay the last step towards the core connection between solvability of the general Pell's

equation and principality of ideal classes in Section 5.2, and an important property of $s(n)$ needed to start the proof of Theorem B in Section 6.2.

Lemma 5.7. (Prime factors of elements of $\mathbb{M}$) *Suppose $n \in \mathbb{Z}^*$. If $D \equiv 2, 3 \pmod 4$, then:*

(a) $n \in \mathbb{M}$ iff there does not exist any $p \in \mathbb{P}$ such that
  (i) $p \mid n$ and $D \notin \mathcal{Q}_p$, or
  (ii) $p^2 \mid n$ and $p \mid 2D$.

(b) if $\mathbf{P}(n)$ holds, then $s(n) \in \mathbb{M}$ (see Definition 4.9).

Proof.

(a) For the only if part, let $n \in \mathbb{M}$, i.e. $D \in \mathcal{Q}_n$ or $rn = k^2 - D$ for some $k, r \in \mathbb{Z}$, and $p \in \mathbb{P}$.
  (i) If $p \mid n$, then by $D \in \mathcal{Q}_n$ and Lemma 4.1(a), we have $D \in \mathcal{Q}_p$.
  (ii) Seeing $rn = k^2 - D$ as that $(x, y) = (k, 1)$ solves $x^2 - Dy^2 = rn$, we have $\mathbf{R}(rn)$ holds. Suppose $p^2 \mid n$ and $p \mid 2D$. No matter $p = 2$ so that $4 = p^2 \mid n$, or $p \neq 2$ so that $p \mid D$ and $p^2 \mid n$, we will have $p^2 \mid rn$ anyway, then by Lemma 2.4(c) (using $D \equiv 2, 3 \pmod 4$) and (a) respectively, in both cases the lemma would produce an integer solution $(x, y) = \left(\frac{k}{p}, \frac{1}{p}\right)$ of $x^2 - Dy^2 = \frac{rn}{p^2}$, which is a contradiction.

  Hence, there does not exist any $p \in \mathbb{P}$ satisfying (i) or (ii).

  For the if part, suppose n does not have any prime factors satisfying (i) or (ii), then n can be factorized into two parts as

(16)
$$n = \underbrace{\prod_i p_i}_{(n,2D)} \quad \underbrace{\prod_j q_j^{e_j}}_{\text{coprime to } 2D},$$

  where
  - $p_i \in \mathbb{P}$ and $p_i \mid 2D$ and
  - $q_j \in \mathbb{P}$, $q_j \nmid 2D$, $D \in \mathcal{Q}_{q_j}$ and $e_j = \nu_{q_j}(n)$.

  On one hand, since $q_j \nmid 2D$ so that $q_j \neq 2$ and $q_j \nmid D$, it follows from $D \in \mathcal{Q}_{q_j}$ and Lemma 4.5 that $D \in \mathcal{Q}_{q_j^{e_j}}$. On the other hand, since $p_i \mid 2D$, we have $p_i = 2$ or $p_i \mid D$. For the first case, by that $p_i = 2 \mid D(D-1)$, we have $D \equiv D^2 \pmod{p_i}$. For the second case, by that $p_i \mid D$, we have $D \equiv 0 = 0^2 \pmod{p_i}$. In both cases, $D \in \mathcal{Q}_{p_i}$. As a result, using Lemma 4.1, we have $D \in \bigcap_i \mathcal{Q}_{p_i} \cap \bigcap_j \mathcal{Q}_{q_j^{e_j}} = \mathcal{Q}_n$ so that $n \in \mathbb{M}$.

(b) If $\mathbf{P}(n)$ holds, then we have prime factorization
$$n = \operatorname{sgn}(n) \prod_i p_i^{2a_i} \prod_j q_j^{b_j} \prod_k r_k^{c_k},$$
  where for each i, $p_i \in \mathbb{P} \setminus \mathbb{M}$ and $a_i \in \mathbb{N}$,
  for each j, $q_j \in \mathbb{P} \cap \mathbb{M}$, $q_j \mid 2D$, $b_j = 2d_j + e_j$, $d_j \in \mathbb{N} \cup \{0\}$ and $e_j = 0, 1$, and

for each k, $r_k \in \mathbb{P} \cap \mathbb{M}$, $r_k \nmid 2D$ and $c_k \in \mathbb{N}$,
and then by definition,

$$s(n) = \operatorname{sgn}(n) \prod_j q_j^{e_j} \prod_k r_k^{c_k}.$$

Check that the two conditions in Lemma 5.7(a) fail, so that $s(n) \in \mathbb{M}$:

(i) if $D \notin \mathcal{Q}_p$ for some $p \in \mathbb{P}$, i.e. $p \notin \mathbb{M}$, then $p = p_i$ for some i, and then $p \nmid s(n)$;
(ii) if $p \mid 2D$ for some $p \in \mathbb{P}$, then $p = q_i$ for some j, and then $\nu_p(s(n)) = e_j = 0, 1$, so that $p^2 \nmid s(n)$.

□

Lemma 5.8. (Product of elements of $\mathbb{M}$) *Suppose $m, n \in \mathbb{M}$. If $D \equiv 2, 3 \pmod 4$, then $mn \in \mathbb{M}$ iff $(m, n, 2D) = 1$.*

Proof. For the if part, suppose $mn \notin \mathbb{M}$, then by Lemma 5.7(a), there exists $p \in \mathbb{P}$ such that

(i) $p \mid mn$ and $D \notin \mathcal{Q}_p$, or
(ii) $p^2 \mid mn$ and $p \mid 2D$.

Case (i) would imply that $p \mid m$ or $p \mid n$, thus with $D \notin \mathcal{Q}_p$, it contradicts that $m, n \in \mathbb{M}$, and then case (ii) must hold. Since $m, n \in \mathbb{M}$ and $p \mid 2D$, by Lemma 5.7(a) again, $p^2 \nmid m, n$. Now, $p^2 \mid mn$ but $p^2 \nmid m, n$, therefore $p \mid m, n$, and then $(m, n, 2D) > 1$.

For the only if part, suppose $p \mid m, n, 2D$ for some $p \in \mathbb{P}$, then $p^2 \mid mn$ and $p \mid 2D$, thus by Lemma 5.7(a) again, we would have $mn \notin \mathbb{M}$.

□

The characterization of $\mathbb{M}$ in Lemma 5.7(a) enables the following extension of Lemma 5.4:

Lemma 5.9. (Ideal multiplication) *Suppose that $a, b \in \mathbb{Z}^*$, $ab \in \mathbb{M}$, $k \in \mathbb{Z}$ with $ab \mid (k^2 - D)$. If $D \equiv 2, 3 \pmod 4$, then $\mathcal{I}_{a,k}\mathcal{I}_{b,k} = \mathcal{I}_{ab,k}$.*

Proof. Since $a, b, ab \mid (k^2 - D)$, we have $a, b \in \mathbb{M}$ so that $\mathcal{I}_{a,k}$ and $\mathcal{I}_{b,k}$ are also well-defined. By Lemma 5.7(a), we have primer factorizations

$$a = \underbrace{\prod_{p_i \mid 2D} p_i}_{a'} \underbrace{\prod_{q_j \nmid 2D} q_j^{a_j}}_{a''} \quad \text{and} \quad b = \underbrace{\prod_{p_i \mid 2D} p_i}_{b'} \underbrace{\prod_{q_j \nmid 2D} q_j^{b_j}}_{b''},$$

where $a', b' \mid 2D$ and $(a'', 2D) = (b'', 2D) = 1$. From above, $(a', a'') = (b', b'') = 1$, so by Lemma 5.2,

$$\mathcal{I}_{a,k} = \mathcal{I}_{a',k}\mathcal{I}_{a'',k} \text{ and } \mathcal{I}_{b,k} = \mathcal{I}_{b',k}\mathcal{I}_{b'',k}.$$

Since $a'b' \mid ab \in \mathbb{M}$ so that $a'b' \in \mathbb{M}$, by Lemma 5.8(b), $(a', b', 2D) = 1$; however, with $a', b' \mid 2D$, actually we have $(a', b') = 1$, thus by Lemma 5.2,

$$\mathcal{I}_{a',k}\mathcal{I}_{b',k} = \mathcal{I}_{a'b',k}.$$

Also, since $(a'', 2D) = (b'', 2D) = 1$, by Lemma 5.4,

$$\mathcal{I}_{a'',k}\mathcal{I}_{b'',k} = \mathcal{I}_{a''b'',k}.$$

Finally, since $a', b' \mid 2D$ and $(a''b'', 2D) = 1$ so that $(a'b', a''b'') = 1$, by Lemma 5.2,

$$\mathcal{I}_{a'b',k}\mathcal{I}_{a''b'',k} = \mathcal{I}_{a'b'a''b'',k}.$$

Combining all,

$$\mathcal{I}_{a,k}\mathcal{I}_{b,k} = \mathcal{I}_{a',k}\mathcal{I}_{a'',k}\mathcal{I}_{b',k}\mathcal{I}_{b'',k} = \mathcal{I}_{a'b',k}\mathcal{I}_{a''b'',k} = \mathcal{I}_{a'b'a''b'',k} = \mathcal{I}_{ab,k}.$$

□

Introducing the condition $h_D = 2$ will allow us to do a good deal more. In particular, Lemma 2.6 is an important tool for establishing ideal equivalence. One important consequence is that we can now show that the ideal class containing $\mathcal{I}_{n,k}$ is independent of k.

Lemma 5.10. (Ideal equivalence) *Suppose $h_D = 2$, $D \equiv 2, 3 \pmod 4$, $n \in \mathbb{M}$ and $k_1, k_2 \in \mathbb{Z}$ with $n \mid (k_1^2 - D), (k_2^2 - D)$. Then, $\mathcal{I}_{n,k_1} \sim \mathcal{I}_{n,k_2}$.*

Proof. If $k_1, k_2 = \pm k$, then $\mathcal{I}_{n,k_1}\mathcal{I}_{n,k_2} = \mathcal{I}_{n,k}\mathcal{I}_{n,-k} = (n)$ is principal, and then by Lemma 2.6, $\mathcal{I}_{n,k_1} \sim \mathcal{I}_{n,k_2}$.

If $n = p^r$ where $p \in \mathbb{P}$, $r \in \mathbb{N}$ and $p \nmid 2D$, then $p \nmid k_1, k_2$, and then by Lemma 4.3, we have $k_1 \equiv \pm k_2 \pmod{p^r}$, i.e. $k_1 = mn \pm k_2$ for some $m \in \mathbb{Z}$. As a result,

$$\mathcal{I}_{n,k_1} = (n, k_1 + \sqrt{D}) = (n, mn \pm k_2 + \sqrt{D}) = (n, \pm k_2 + \sqrt{D}) = \mathcal{I}_{n,\pm k_2},$$

and then $\mathcal{I}_{n,k_1} = \mathcal{I}_{n,k_2}$, or by Lemma 5.6, $\mathcal{I}_{n,k_1}\mathcal{I}_{n,k_2} = \mathcal{I}_{n,-k_2}\mathcal{I}_{n,k_2} = (n)$ is principal. In the second case, by Lemma 2.6, $\mathcal{I}_{n,k_1} \sim \mathcal{I}_{n,k_2}$.

If $n = p^r$ where $p \in \mathbb{P}$, $r \in \mathbb{N}$ and $p \mid 2D$, then by Lemma 5.7(a), $r = \nu_p(n) = 1$. If $p = 2$, then for $i = 1, 2$, $n = p = 2 \mid k_i(k_i - 1) = (k_i^2 - k_i)$ and $n = p = 2 \mid (k_i^2 - D)$ so that $n \mid (k_i - D)$; and if $p \mid D$, then for $i = 1, 2$, $n = p \mid (k_i^2 - D)$ so that $n = p \mid k_i^2$ and $n = p \mid k_i$. In both cases, we have $n \in (k_1 - k_2)$ or $k_1 = mn + k_2$ for some $m \in \mathbb{Z}$, and then

$$\mathcal{I}_{n,k_1} = (n, k_1 + \sqrt{D}) = (n, mn + k_2 + \sqrt{D}) = (n, k_2 + \sqrt{D}) = \mathcal{I}_{n,k_2}.$$

If $n = \prod_{i=1}^m p_i^{e_i}$, where $p_i \in \mathbb{P}$ and $e_i = \nu_{p_i}(n)$. Then, by Lemma 5.2 and above,

$$\mathcal{I}_{n,k_1} = \prod_{i=1}^m \mathcal{I}_{p_i^{a_i},k_1} \sim \prod_{i=1}^m \mathcal{I}_{p_i^{a_i},k_2} = \mathcal{I}_{n,k_2}.$$

□

Due to Lemma 5.10, the following is well-defined:

Definition 5.11. (Ideal class $\mathfrak{I}_n$) *Suppose $h_D = 2$ and $D \equiv 2, 3 \pmod 4$. For $n \in \mathbb{M}$ and $k \in \mathbb{Z}$ with $n \mid (k^2 - D)$, define*

$$\mathfrak{I}_n := [\mathcal{I}_{n,k}]$$

which is an equivalence class of the ideal equivalence $\sim$ on $\mathcal{O}_\mathcal{K}$.

By Definition 5.11 and Lemma 5.9, for $mn \in \mathbb{M}$,

$$\mathfrak{I}_{mn} = \mathfrak{I}_m \mathfrak{I}_n.$$

We shall now establish the equivalence between the principality of this ideal class and a weaker solvability of the general Pell's equation:

Condition $\mathbf{R}^\pm$. (Solvability of general Pell's equation) For $n \in \mathbb{Z}^*$, $\mathbf{R}^\pm(n)$ stands for the condition that at least one of $\mathbf{R}(n)$ and $\mathbf{R}(-n)$ holds.

Lemma 5.12. (Principality of $\mathfrak{I}_n$ vs Condition $\mathbf{R}^\pm$) *Suppose $h_D = 2$, $D \equiv 2, 3 \pmod 4$ and $n \in \mathbb{M}$. Then, $\mathfrak{I}_n$ is the principal ideal class iff $\mathbf{R}^\pm(n)$ holds.*

Proof. If $\mathfrak{I}_n$ is the principal ideal class, then $\mathcal{I}_{n,k} = (x_0 + y_0\sqrt{D})$ for some $k \in \mathbb{Z}$ with $n \mid (k^2 - D)$ and $x_0, y_0 \in \mathbb{Z}$. Taking norm, we have $|n| = N(\mathcal{I}_{n,k}) = \left|x_0^2 - Dy_0^2\right|$ by Lemmas 2.5(c) and 5.5, so that $x_0^2 - Dy_0^2 = \pm n$ and $\mathbf{R}^\pm(n)$ holds.

If $\mathbf{R}^\pm(n)$ holds with $x_0^2 - Dy_0^2 = n$ or $-n$ for some $x_0, y_0 \in \mathbb{Z}$, then let $d = (x_0, y_0)$, $(x_0', y_0') = \left(\frac{x_0}{d}, \frac{y_0}{d}\right)$ and $n = d^2 n'$, so that $x_0'^2 - Dy_0'^2 = n'$ or $-n'$ respectively. Since $(x_0', y_0') = 1$, we have $ux_0' + vy_0' = 1$ for some $u, v \in \mathbb{Z}$. Let $k = vx_0' + Duy_0'$, and we will show that $\mathfrak{I}_{n'} = [\mathcal{I}_{n',k}]$ is the principal ideal class. Indeed by (4), $k^2 - D = (vx_0' + Duy_0')^2 - D(ux_0' + vy_0') = (x_0'^2 - Dy_0'^2)(v^2 - Du^2) = \pm n'(v^2 - Du^2)$, so $n' \mid (k^2 - D)$ and $\mathcal{I}_{n',k}$ is well-defined. Check by expansion that

$$\begin{aligned}
\mathcal{I}_{n',k} &= (n', k + \sqrt{D}) \\
&= (\pm(x_0'^2 - Dy_0'^2), (x_0' + y_0'\sqrt{D})(v + u\sqrt{D})) \\
&= (x_0' + y_0'\sqrt{D})(\pm(x_0' - y_0'\sqrt{D}), v + u\sqrt{D}). \qquad (17)
\end{aligned}$$

Taking norm on both sides of (17), using by Lemmas 2.5(a) and (c) and 5.5, we have

$$\begin{aligned}
N(\mathcal{I}_{n',k}) &= N((x_0' + y_0'\sqrt{D}))N((\pm(x_0' - y_0'\sqrt{D}), v + u\sqrt{D})) \\
|n'| &= |n'|\, N((\pm(x_0' - y_0'\sqrt{D}), v + u\sqrt{D})) \\
N((\pm(x_0' - y_0'\sqrt{D}), v + u\sqrt{D})) &= 1.
\end{aligned}$$

By Lemma 2.5(b), (17) becomes $\mathcal{I}_{n',k} = (x_0' + y_0'\sqrt{D})\mathcal{O}_\mathcal{K} = (x_0' + y_0'\sqrt{D})$ is principal, and $\mathfrak{I}_{n'}$ is the principal ideal class. Finally, since $h_D = 2$, $\mathfrak{I}_{d^2} = \mathfrak{I}_d^2$ is the principal ideal class by Lemmas 2.6, thus $\mathfrak{I}_n = \mathfrak{I}_{d^2}\mathfrak{I}_{n'}$ is also the principal ideal class. □

6. Proof of Theorem B

6.1. Further properties of Conditions P, Q and $\mathbf{R}^{\pm}$.

Lemma 6.1. (Conditions P, Q and $\mathbf{R}^{\pm}$ preserved under c) *Suppose $n \in \mathbb{Z}^*$.*

(a) $\mathbf{P}(n)$ holds iff $\mathbf{P}(c(n))$ holds.
(b) $\mathbf{Q}(n)$ holds iff $\mathbf{Q}(c(n))$ holds.
(c) If $h_D = 2$, $D \equiv 2, 3 \pmod 4$ and $n \in \mathbb{M}$, then $\mathbf{R}^{\pm}(n)$ holds iff $\mathbf{R}^{\pm}(c(n))$ holds.

Proof. (a) Suppose

$$n = \operatorname{sgn}(n) \prod_{\substack{p \in \mathbb{P} \\ p \nmid D}} p^{\nu_p(n)} \prod_{\substack{q \in \mathbb{P} \\ q \mid D}} q^{\nu_q(n)} \text{ and}$$

$$c(n) = \operatorname{sgn}(n) \prod_{\substack{p \in \mathbb{P} \\ p \nmid D}} p^{\nu_p(n)} \prod_{\substack{q \in \mathbb{P} \\ q \mid D}} \left(q - \frac{D}{q}\right)^{\nu_q(n)},$$

so that

$$\frac{c(n)}{n} = \prod_{\substack{q \in \mathbb{P} \\ q \mid D}} \left(1 - \frac{D}{q^2}\right)^{\nu_q(n)}$$

$$c(n) \underbrace{\prod_{\substack{q \in \mathbb{P} \\ q \mid D}} (q^2)^{\nu_q(n)}}_{d(n)} = n \underbrace{\prod_{\substack{q \in \mathbb{P} \\ q \mid D}} (q^2 - D)^{\nu_q(n)}}_{e(n)}. \tag{18}$$

On one hand, $\mathbf{P}(d(n))$ holds trivially as $d(n)$ is a square number. On the other hand, if $r \in \mathbb{P} \setminus \mathbb{M}$, then $D \notin \mathcal{Q}_r$, and then $r \nmid (q^2 - D)$ for any $q \in \mathbb{P}$ with $q \in D$ on the right-hand side of (18), so that $\nu_r(e(n)) = 0$ is even. With both $\mathbf{P}(d(n))$ and $\mathbf{P}(e(n))$ hold, applying Lemma 4.6 twice, we have $\mathbf{P}(c(n))$ holds iff $\mathbf{P}(ne(n))$ holds, iff $\mathbf{P}(n)$ holds.

(b) Note that $c(c(n)) = c(n)$ as $(c(n), D) = 1$ by Lemma 2.2. Then, $\mathbf{Q}(n)$ holds iff $c(n) \in \mathcal{Q}_D$, iff $c(c(n)) \in \mathcal{Q}_D$, iff $\mathbf{Q}(c(n))$ holds.

(c) Define $\sigma = 1$ if $2 \mid D$ and $\sigma = 2$ if $2 \nmid D$, and $g(p) = \left(p - \frac{D}{p}\right)/\sigma$ for $p \in \mathbb{P}$ with $p \mid D$.

First, we show that $g(p)$ is an odd integer. Suppose $2 \mid D$, then $\sigma = 1$, and $g(p) = p - \frac{D}{p}$ is an integer. If p is odd, then $\frac{D}{p}$ will be even as $2 \mid D$; if $p = 2$ is even, then $\frac{D}{p} = \frac{D}{2}$ will be odd, otherwise $4 \mid D$. In both cases, $g(p)$ is odd. Now suppose $2 \nmid D$, then $D \equiv 3 \pmod 4$, $\sigma = 2$ and $g(p) = \left(p - \frac{D}{p}\right)/2$. If $p \equiv 1 \pmod 4$, then $\frac{D}{p} \equiv 3 \pmod 4$; if $p \equiv 3 \pmod 4$, then $\frac{D}{p} \equiv 1 \pmod 4$. In both cases, $p - \frac{D}{p} \equiv 2 \pmod 4$, so $g(p)$ is once again an odd integer.

Next, using Lemma 5.7, consider prime factorization

$$n = \prod_{\substack{i=1 \\ p_i \mid D}}^{m} p_i \underbrace{\prod_{\substack{q_j \mid n \\ q_j \nmid D}} q_j^{b_j}}_{m}.$$

We show that $(g(p_i), 2D) = 1$. Note that $(m, D) = 1$, thus

$$c(n) = c(m) \prod_{i=1}^{k} \left(p_i - \frac{D}{p_i} \right) = m \prod_{i=1}^{k} \sigma g(p_i).$$

Then, $(g(p_i), D) \leq (\sigma g(p_i), D) = \left(p_i - \frac{D}{p_i}, D \right) = (c(p_i), D) = 1$. Plus that $g(p_i)$ is odd, we have $(g(p_i), 2D) = 1$ as claimed.

We will express $\mathfrak{I}_n$ as the product of $\mathfrak{I}_{c(n)/\sigma^k}$ and $(\mathfrak{I}_\sigma)^k$, via working with $\mathfrak{I}_m$, $\mathfrak{I}_{p_i}$, $\mathfrak{I}_{p_i^2 - D}$, $\mathfrak{I}_{\sigma g(p_i)}$, $\mathfrak{I}_{g(p_i)}$ and $\mathfrak{I}_\sigma$. Before proceed, we verify that all of them are well-defined. Indeed, since $m, p_i \mid n \in \mathbb{M}$, we have $m, p_i \in \mathbb{M}$. Also, since $p_i^2 - D = p_i \left(p_i - \frac{D}{p_i} \right) = p_i \sigma g(p_i)$ and trivially $p_i^2 - D \equiv p_i^2 \pmod{D}$, so that $g(p_i), \sigma g(p_i) \mid (p_i^2 - D) \in \mathbb{M}$, we have $g(p_i), \sigma g(p_i) \in \mathbb{M}$. Finally, since $(g(p_i), 2D) = 1$ so that $\left(\prod_{i=1}^{k} g(p_i), 2D \right) = 1$, by Lemma 5.8 we have $\prod_{i=1}^{k} g(p_i) \in \mathbb{M}$. Moreover, as $\left(m, \prod_{i=1}^{k} g(p_i), 2D \right) = 1$, indeed we have $c(n)/\sigma^k = m \prod_{i=1}^{k} g(p_i) \in \mathbb{M}$ by Lemma 5.8 again. Now, noting that $\mathfrak{I}_{p_i^2 - D} = [\mathcal{I}_{p_i^2 - D, p_i}] = [(p_i^2 - D, p_i + \sqrt{D})] = [((p_i + \sqrt{D})(p_i - \sqrt{D}), p_i + \sqrt{D})] = [(p_i + \sqrt{D})]$ is the principal ideal class, we can perform the aforementioned working:

$$\begin{aligned}
\mathfrak{I}_n &= \mathfrak{I}_m \prod_{i=1}^{k} \mathfrak{I}_{p_i} \\
&= \mathfrak{I}_m \prod_{i=1}^{k} \left(\mathfrak{I}_{p_i} \left(\mathfrak{I}_{\sigma g(p_i)} \right)^2 \right), \left(\mathfrak{I}_{\sigma g(p_i)} \right)^2 \text{ is the principal ideal class by Lemma 2.6} \\
&= \mathfrak{I}_m \prod_{i=1}^{k} \left(\mathfrak{I}_{p_i^2 - D} \mathfrak{I}_\sigma \mathfrak{I}_{g(p_i)} \right), \text{ applying Lemma 5.7} \\
&= \mathfrak{I}_m \prod_{i=1}^{k} \mathfrak{I}_\sigma \mathfrak{I}_{g(p_i)}, \mathfrak{I}_{p_i^2 - D} \text{ is the principal ideal class} \\
&= \mathfrak{I}_{c(n)/\sigma^k} (\mathfrak{I}_\sigma)^k
\end{aligned}$$

With this, we can actually find $\ell \in \mathbb{N} \cup \{0\}$ such that $c(n)/2^{2\ell} \in \mathbb{M}$ and $\mathfrak{I}_n = \mathfrak{I}_{c(n)/2^{2\ell}}$:

- Suppose $\sigma = 1$, then with $\ell = 0$, we have $c(n)/2^{2\ell} = c(n)/\sigma^k \in \mathbb{M}$ and $\mathfrak{I}_n = \mathfrak{I}_{c(n)/\sigma^k} (\mathfrak{I}_\sigma)^k = \mathfrak{I}_{c(n)/2^{2\ell}}$.
- Suppose $\sigma = 2$:

– If k is even, then with $\ell = k/2$, we have $c(n)/2^{2\ell} = c(n)/\sigma^k \in \mathbb{M}$ and

$$\mathfrak{I}_n = \mathfrak{I}_{c(n)/\sigma^k}(\mathfrak{I}_\sigma)^k = \mathfrak{I}_{c(n)/2^{2\ell}}.$$

– If k is odd, we have two more cases:
  * Suppose $c(n)/2^k$ is odd, we can take $\ell = (k-1)/2$, then $c(n)/2^{2\ell} = 2(c(n)/2^k) \in \mathbb{M}$ and

$$\mathfrak{I}_n = \mathfrak{I}_{c(n)/2^k}\mathfrak{I}_\sigma(\mathfrak{I}_\sigma)^{2\ell} = \mathfrak{I}_{c(n)/2^{2\ell}}.$$

  * Suppose $c(n)/2^k$ is even, we can take $\ell = (k+1)/2$, then $c(n)/2^{2\ell} = 2(c(n)/2^k) \in \mathbb{M}$ and

$$\mathfrak{I}_n = \mathfrak{I}_{c(n)/2^k}(\mathfrak{I}_\sigma)^{2\ell-1} = \mathfrak{I}_{c(n)/2^{2\ell}}(\mathfrak{I}_\sigma)^{2\ell} = \mathfrak{I}_{c(n)/2^{2\ell}}.$$

As a result, we will have, using Lemma 5.12, $\mathbf{R}^{\pm}(n)$ holds iff $\mathfrak{I}_n$ is principal, iff $\mathfrak{I}_{c(n)/2^{2\ell}}$ is principal, iff $\mathbf{R}^{\pm}\big(c(n)/2^{2\ell}\big)$ holds, and then by Lemma 4.8, iff $\mathbf{R}^{\pm}(c(n))$ holds.

□

Here we collect some properties of the Legendre and the Jacobi symbols which will be used to prove two weaker versions of Theorem B in the next sections:

(a) For $a \in \mathbb{Z}$ and odd $p \in \mathbb{P}$,

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{for } a \equiv 0 \pmod p \\ 1 & \text{for } a \not\equiv 0 \pmod p \text{ and } a \in \mathcal{Q}_p \\ -1 & \text{for } a \not\equiv 0 \pmod p \text{ and } a \notin \mathcal{Q}_p \end{cases}$$

(b) For $a \in \mathbb{Z}$ and odd $n \in \mathbb{N}$ with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$,

$$\left(\frac{a}{n}\right) := \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}.$$

Lemma 6.2. (Properties of Legendre and Jacobi symbols)

(a) **(Multiplicativity)** *Suppose $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$ are odd:*
  (i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
  (ii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

(b) **(Prime denominator)** *Suppose $p \in \mathbb{P}$ is odd:*
  (i) $\left(\frac{-1}{p}\right) = 1$ *if* $p \equiv 1 \pmod 4$
  (ii) $\left(\frac{2}{p}\right) = -1$ *if* $p \equiv \pm 3 \pmod 8$

(c) **(Coprimality)** *Suppose $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ is odd:*
  (i) If $\left(\frac{a}{n}\right) = 0$, *then* $(a, n) > 1$.
  (ii) If $\left(\frac{a}{n}\right) = \pm 1$, *then* $(a, n) = 1$.

(d) **(Quadratic residuosity)** *Suppose $a \in \mathbb{Z}$, $n \in \mathbb{N}$ is odd and $p \in \mathbb{P}$ is odd:*
  (i) If $\left(\frac{a}{n}\right) = -1$, *then* $a \notin \mathcal{Q}_n$.
  (ii) If $\left(\frac{a}{p}\right) = 1$, *then* $a \notin \mathcal{Q}_p$.

(e) **(Law of quadratic reciprocity)** *Suppose $m, n \in \mathbb{N}$ are odd and $(m, n) = 1$. Then,*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = \begin{cases} 1 & \text{if } m \text{ or } n \equiv 1 \pmod 4 \\ -1 & \text{if } m \equiv n \equiv 3 \pmod 4 \end{cases}$$

(f) Suppose $k \in \mathbb{N}$ is odd and squarefree with $k \geq 3$. Then, there exists $r \in \mathbb{Z}^*$ such that $\left(\frac{r}{k}\right) = -1$.

Proof. For part (f), let $p \in \mathbb{P}$ and $p \mid k$. Then $p \geq 3$ as well, there exists quadratic non-residue a modulo p, i.e. $a \notin \mathcal{Q}_p$, and $\left(\frac{a}{p}\right) = -1$. We can then apply the Chinese remainder theorem to take $r \equiv a \pmod p$ and $r \equiv 1 \pmod{k/p}$; this is possible as $(p, k/p) = 1$ by k squarefree. Then we have $\left(\frac{r}{k}\right) = \left(\frac{a}{p}\right)\left(\frac{1}{k/p}\right) = (-1)(1) = -1$. □

We now proceed to prove further properties of $\mathbf{P}$, $\mathbf{Q}$ and $\mathbf{R}^{\pm}$ under assumptions (i) $\mathbf{R}(-1)$ holds and (ii) $\mathbf{Q}(-1)$ does not hold respectively in Theorem B. The treatments for these two cases in Sections 6.1.1 and 6.1.2 are similar and just slightly different.

6.1.1. *When* $\mathbf{R}(-1)$ *holds.*

Lemma 6.3. (Condition P vs Condition Q) *Suppose $h_D = 2$ and $D \equiv 2, 3 \pmod 4$. Assume that D also satisfies that $\mathbf{R}(-1)$ holds. For any $n \in \mathbb{Z}^*$, there exists $p \in \mathbb{P}$ such that $p \nmid D, n$, and $\mathbf{P}(p)$ holds but $\mathbf{Q}(p)$ does not.*

Proof. Suppose that $D \equiv 3 \pmod 4$. Since $\mathbf{R}(-1)$ holds, $x_0^2 - Dy_0^2 = -1$ for some $x_0, y_0 \in \mathbb{Z}$. Taking modulo 4, we would obtain a contradiction that $3 \equiv x_0^2 - Dy_0^2 \equiv x_0^2 + y_0^2 \equiv 0, 1, 2 \pmod 4$. Thus, $D \equiv 2 \pmod 4$.

Let $D = 2k$, where $k \geq 5$ (check from the number lists following the statement of Theorem B at the end of Section 1 that $D \geq 10$ as $h_D = 2$) is odd and squarefree (as D is), and $k \equiv \pm 1 \pmod 4$. Pick any $r \in \mathbb{Z}$ such that $\left(\frac{r}{k}\right) = -1$ by Lemma 6.2(f). By the Chinese remainder theorem, there exists $m \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv \pm 3 \pmod 8 & (\pm \text{ here corresponds to } k \equiv \pm 1 \pmod 4 \text{ resp.}) \\ x \equiv r \pmod k \end{cases}$$

for all $x = m + 8kt$ where $t \in \mathbb{Z}$. Note that $m \equiv \pm 3 \not\equiv 0 \pmod{2, 4, 8}$, and that $m \equiv r \pmod k$ and $\left(\frac{r}{k}\right) = -1$ so that $(m, k) = (r, k) = 1$ by Lemma 6.2(c). Thus, $(m, 8k) = 1$, and then we can apply Dirichlet's theorem on arithmetic progressions to pick a sufficiently large $p \in \mathbb{P}$ of the form $m + 8kt$ such that $p > D, n$ so that $p \nmid D, n$.

To show that $\mathbf{Q}(p)$ does not hold, recall that $p \nmid D$ and $p \equiv r \pmod k$, so

$$\left(\frac{c(p)}{k}\right) = \left(\frac{p}{k}\right) = \left(\frac{r}{k}\right) = -1,$$

and then by Lemmas 6.2(d) and 4.1(a), we have $c(p) \notin \mathcal{Q}_k$ and then $c(p) \notin \mathcal{Q}_D$ as $k \mid D$.

To show that $\mathbf{P}(p)$ holds, recall that $\left(\frac{p}{k}\right) = -1$ so that $(p,k) = 1$ by Lemma 6.2(c). Then, we can apply Lemma 6.2(a), (b) and (e) to obtain

$$\left(\frac{D}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{k}{p}\right) = (-1)(-1)^{\frac{k-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{k}\right) = (-1)(1)(-1) = 1,$$

which infers through Lemma 6.2(d) that $D \in \mathcal{Q}_p$ so that $\nu_q(p)$ is even for all $q \in \mathbb{P}\setminus\mathbb{M}$. □

Lemma 6.4. (Weak version one of Theorem B) *Suppose $h_D = 2$, $D \equiv 2,3 \pmod 4$, $n \in \mathbb{M}$ and $(n,D) = 1$. Assume that D also satisfies that $\mathbf{R}(-1)$ holds. If both $\mathbf{P}(n)$ and $\mathbf{Q}(n)$ hold, then so does $\mathbf{R}^{\pm}(n)$.*

Proof. When $\mathbf{R}(-1)$ holds, by Lemma 2.3, $\mathbf{R}(n)$ holds iff $\mathbf{R}(-n)$ holds. Moreover, by Theorem A, $\mathbf{Q}(-1)$ also holds, then by Lemma 4.7, for any $m \in \mathbb{Z}^*$, $\mathbf{Q}(m)$ holds iff $\mathbf{Q}(-m)$ holds.

Suppose the contrary that both $\mathbf{P}(n)$ and $\mathbf{Q}(n)$ hold but $\mathbf{R}^{\pm}(n)$ does not. Considering $p \in \mathbb{P}$ picked from Lemma 6.3, with Lemma 4.6, we would have:

- $\mathbf{P}(n)$, $\mathbf{P}(p)$ and $\mathbf{P}(pn)$ hold,
- $\mathbf{Q}(n)$ holds but $\mathbf{Q}(p)$ does not,
- $\mathbf{R}^{\pm}(n)$ does not hold, and
- $\mathbf{R}^{\pm}(p)$ does not hold as that at least one of $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ hold is a necessary condition according to Theorem A, but both of them do not hold here.

As a result, by Lemma 5.12, both $\mathfrak{I}_n$ and $\mathfrak{I}_p$ would be the non-principal ideal class, but then by Lemma 2.6, $\mathfrak{I}_{np}$ would be the principal ideal class, and then by Lemma 5.12 again, $\mathbf{R}^{\pm}(np)$ would hold, and then at least one of $\mathbf{Q}(np)$ and $\mathbf{Q}(-np)$ would hold as implied by Theorem A. Yet, $\mathbf{Q}(n)$ holds but $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ do not, so Lemma 4.7 would imply that $\mathbf{Q}(np)$ and $\mathbf{Q}(-np)$ do not hold. Thus, there is a contradiction. □

6.1.2. *When* $\mathbf{Q(-1)}$ *does not hold.*

Lemma 6.5. (Corollary of theorem of Gauss) *Suppose $h_D = 2$ and $D \equiv 2,3 \pmod 4$. If $q \mid D$ for some $q \in \mathbb{P}$ with $q \equiv 3 \pmod 4$, then $4D$ has at least 3 distinct prime factors.*

Proof. The proof follows from realizing that as $h_D = 2$, there are more than one ideal class $\mathfrak{I}$ such that $\mathfrak{I}^2 = [(1)]$, so that on applying the theorem of Gauss in [7], Theorem 3.70, one will have $2^{N-2} \geq 2$, where N is the number of distinct prime factors of $4D$. □

Lemma 6.6. (Condition P vs Condition Q) *Suppose $h_D = 2$ and $D \equiv 2,3 \pmod 4$. Assume that D also satisfies that $\mathbf{Q}(-1)$ does not hold. For any $n \in \mathbb{Z}^*$, there exists $p \in \mathbb{P}$ such that $p \nmid D, n$, and $\mathbf{P}(p)$ holds but both $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ do not.*

Proof. Since $\mathbf{Q}(-1)$ does not hold, $-1 \notin \mathcal{Q}_D$, and we can use it to deduce that $q \mid D$ for some $q \in \mathbb{P}$ and $q \equiv 3 \pmod 4$. Suppose the contrary that $D = \prod_{i=1}^{k} p_i$ for some $p_i \in \mathbb{P}$ where $p_i = 2$ or $p_i \equiv 1 \pmod 4$. Then, by Lemma 6.2(b) and (d), $a_i^2 \equiv -1$

$(\text{mod } p_i)$ for some $a_i \in \mathbb{Z}$. By the Chinese remainder theorem, $a \equiv a_i \ (\text{mod } p_i)$ for some $a \in \mathbb{Z}$, then $a^2 \equiv a_i^2 \equiv -1 \ (\text{mod } p_i)$, and then $a^2 \equiv -1 \ (\text{mod } D)$, getting a contradiction that $-1 \in \mathcal{Q}_D$.

Now, $q \in \mathbb{P}$, $q \equiv 3 \ (\text{mod } 4)$ and $q \mid D$, so by Lemma 6.5, $4D$ has at least three distinct prime factors, so that $4D = 4qk$ for some $k \in \mathbb{N}$ where $k \neq 1, 2^l, q^l$ for all $l \in \mathbb{N}$. We have two cases to consider, namely $D = qk$ is even and odd.

If $D = qk$ is even, then k is even, indeed $k \geq 6$, and then $D = 2qk'$ where $k' = \frac{k}{2} \geq 3$. Pick any $r \in \mathbb{Z}$ such that $\left(\frac{r}{k'}\right) = -1$ by Lemma 6.2(f). By the Chinese remainder theorem, there exists $m \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 5 & (\text{mod } 8) \\ x \equiv 1 & (\text{mod } q) \\ x \equiv r & (\text{mod } k') \end{cases}$$

for all $x = m + 8qk't$ where $t \in \mathbb{Z}$. Note that $m \equiv 5 \not\equiv 0 \ (\text{mod } 2, 4, 8)$, that $m \equiv 1 \not\equiv 0 \ (\text{mod } q)$, and that $m \equiv r \ (\text{mod } k')$ and $\left(\frac{r}{k'}\right) = -1$ so that $(m, k') = (r, k') = 1$ by Lemma 6.2(c). Thus, $(m, 8qk') = 1$, and then we can apply Dirichlet's theorem on arithmetic progressions to pick a sufficiently large $p \in \mathbb{P}$ of the form $m + 8qk't$ such that $p > D, n$ so that $p \nmid D, n$.

To show that $\mathbf{Q}(p)$ does not hold, recall that $p \nmid D$ and $p \equiv r \ (\text{mod } k')$, so

$$\left(\frac{c(p)}{k'}\right) = \left(\frac{p}{k'}\right) = \left(\frac{r}{k'}\right) = -1,$$

and then by Lemma 6.2(d) and Lemma 4.1(a), we have $c(p) \notin \mathcal{Q}_{k'}$ and then $c(p) \notin \mathcal{Q}_D$ as $k' \mid D$.

To show that $\mathbf{Q}(-p)$ does not hold, recall that $c(-p) = -p \equiv -1 \ (\text{mod } q)$. But $\left(\frac{-1}{q}\right) = -1$ by $q \equiv 3 \ (\text{mod } 4)$ and Lemma 6.2(b), so by Lemmas 6.2(d) and 4.1(a), we have $-1 \notin \mathcal{Q}_q$ and $c(-p) \notin \mathcal{Q}_q$ and then $c(-p) \notin \mathcal{Q}_D$ as $q \mid D$.

To show that $\mathbf{P}(p)$ holds, recall that $\left(\frac{p}{k'}\right) = -1$ so that $(p, k') = 1$ by Lemma 6.2(c). Then, we can apply Lemma 6.2(a), (b) and (e) to obtain

$$\begin{aligned} \left(\frac{D}{p}\right) &= \left(\frac{2}{p}\right)\left(\frac{q}{p}\right)\left(\frac{k'}{p}\right) = (-1)(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{q}\right)(-1)^{\frac{k'-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{k'}\right) \\ &= (-1)(1)(-1) = 1, \end{aligned}$$

which infers through Lemma 6.2(d) that $D \in \mathcal{Q}_p$ so that $\nu_q(p) = 0$ is even for all $q \in \mathbb{P} \setminus \mathbb{M}$.

If $D = qk$ is odd, then k is odd and $k \geq 3$.

Pick any $r \in \mathbb{Z}$ such that $\left(\frac{r}{k'}\right) = -1$ by Lemma 6.2(f). By the Chinese remainder theorem, there exists $m \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 3 & (\text{mod } 4) \\ x \equiv 1 & (\text{mod } q) \\ x \equiv r & (\text{mod } k) \end{cases}$$

for all $x = m + 4qkt$ where $t \in \mathbb{Z}$. Note that $m \equiv 3 \not\equiv 0 \ (\text{mod } 2, 4)$, that $m \equiv 1 \not\equiv 0 \ (\text{mod } q)$, and that $m \equiv r \ (\text{mod } k)$ and $\left(\frac{r}{k}\right) = -1$ so that $(m, k) = (r, k) = 1$ by Lemma 6.2(c). Thus, $(m, 4qk) = 1$, and then we can apply Dirichlet's theorem on

arithmetic progressions to pick a sufficiently large $p \in \mathbb{P}$ of the form $m + 4qkt$ such that $p > D, n$ so that $p \nmid D, n$.

To show that $\mathbf{Q}(p)$ does not hold, recall that $p \nmid D$ and $p \equiv r \pmod{k}$, so

$$\left(\frac{c(p)}{k}\right) = \left(\frac{p}{k}\right) = \left(\frac{r}{k}\right) = -1,$$

and then by Lemma 6.2(d) and Lemma 4.1(a), we have $c(p) \notin \mathcal{Q}_k$ and then $c(p) \notin \mathcal{Q}_D$ as $k \mid D$.

To show that $\mathbf{Q}(-p)$ does not hold, recall that $c(-p) = -p \equiv -1 \pmod{q}$. But $\left(\frac{-1}{q}\right) = -1$ by $q \equiv 3 \pmod 4$ and Lemma 6.2(b), so by Lemmas 6.2(d) and 4.1(a), we have $-1 \notin \mathcal{Q}_q$ and $c(-p) \notin \mathcal{Q}_q$ and then $c(-p) \notin \mathcal{Q}_D$ as $q \mid D$.

To show that $\mathbf{P}(p)$ holds, recall that $\left(\frac{p}{k}\right) = -1$ so that $(p, k) = 1$ by Lemma 6.2(c). Then, we can apply Lemma 6.2(a), (b) and (e) to obtain

$$\left(\frac{D}{p}\right) = (-1)^{\frac{D-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{D}\right) = (-1)\left(\frac{p}{q}\right)\left(\frac{p}{k}\right) = (-1)(1)(-1) = 1,$$

which infers through Lemma 6.2(d) that $D \in \mathcal{Q}_p$ so that $\nu_q(p)$ is even for all $q \in \mathbb{P} \setminus \mathbb{M}$. □

Lemma 6.7. (Weak version two of Theorem B) *Suppose $h_D = 2$, $D \equiv 2, 3 \pmod 4$, $n \in \mathbb{M}$ and $(n, D) = 1$. Assume that D also satisfies that $\mathbf{Q}(-1)$ does not hold. If both $\mathbf{P}(n)$ and $\mathbf{Q}(n)$ hold, then so does $\mathbf{R}^{\pm}(n)$.*

Proof. Suppose the contrary that both $\mathbf{P}(n)$ and $\mathbf{Q}(n)$ hold but $\mathbf{R}^{\pm}(n)$ does not. Considering $p \in \mathbb{P}$ picked from Lemma 6.6, with Lemmas 4.6 and 4.7, we would have:

- $\mathbf{P}(n)$, $\mathbf{P}(p)$ and $\mathbf{P}(pn)$ hold,
- $\mathbf{Q}(n)$ holds but $\mathbf{Q}(-1)$ and $\mathbf{Q}(-n)$ do not,
- $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ do not hold,
- $\mathbf{R}^{\pm}(n)$ does not hold, and
- $\mathbf{R}^{\pm}(p)$ does not hold as that at least one of $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ hold is a necessary condition according to Theorem A, but both of them do not hold here.

As a result, by Lemma 5.12, both $\mathfrak{I}_n$ and $\mathfrak{I}_p$ would be the non-principal ideal class, but then by Lemma 2.6, $\mathfrak{I}_{np}$ would be the principal ideal class, and then by Lemma 5.12 again, $\mathbf{R}^{\pm}(np)$ would hold, and then at least one of $\mathbf{Q}(np)$ and $\mathbf{Q}(-np)$ would hold as implied by Theorem A. Yet, $\mathbf{Q}(n)$ holds but $\mathbf{Q}(p)$ and $\mathbf{Q}(-p)$ do not, so Lemma 4.7 would imply that $\mathbf{Q}(np)$ and $\mathbf{Q}(-np)$ do not hold. Thus, there is a contradiction. □

6.2. **Proof of Theorem B.** Here we state our second main result again, for which we have already prepared sufficient tools to prove:

Theorem B. (Sufficient condition for solvability of general Pell's equation; conditional converse of Theorem A) *Suppose $n \in \mathbb{Z}^*$, $h_D = 2$ and $D \equiv 2, 3 \pmod 4$. Assume that D also satisfies either*

(i) $\mathbf{R}(-1)$ holds (i.e. the negative Pell's equation is solvable) or

(ii) $\mathbf{Q}(-1)$ *does not hold (i.e.* -1 *is a quadratic non-residue modulo* D*).*

If both $\mathbf{P}(n)$ *and* $\mathbf{Q}(n)$ *hold, then so does* $\mathbf{R}(n)$*.*

Proof. When $\mathbf{P}(n)$ and $\mathbf{P}(c(s(n)))$ hold, by Lemma 5.7(b), we will have $s(n), s(c(s(n)) \in \mathbb{M}$. Also, since $s(c(s(n))) \mid c(s(n))$ by definition, with $(c(s(n)), D) = 1$ by Lemma 2.2, we will have $(s(c(s(n))), D) = 1$ as well. Then, we have the following sequence of implications:

$$
\begin{array}{lll}
 & \mathbf{P}(n) \text{ and } \mathbf{Q}(n) \text{ hold} & \\
\Rightarrow & \mathbf{P}(s(n)) \text{ and } \mathbf{Q}(s(n)) \text{ hold} & \text{(by Lemma 4.8)} \\
\Rightarrow & \mathbf{P}(c(s(n))) \text{ and } \mathbf{Q}(c(s(n))) \text{ hold} & \text{(by Lemma 6.1)} \\
\Rightarrow & \mathbf{P}(s(c(s(n)))) \text{ and } \mathbf{Q}(s(c(s(n)))) \text{ hold} & \text{(by Lemma 4.8)} \\
\Rightarrow & \mathbf{R}^{\pm}(s(c(s(n)))) \text{ holds} & \text{(by Lemmas 6.4 and 6.7)} \\
\Rightarrow & \mathbf{R}^{\pm}(c(s(n))) \text{ holds} & \text{(by Lemma 4.8)} \\
\Rightarrow & \mathbf{R}^{\pm}(s(n)) \text{ holds} & \text{(by Lemma 6.1)} \\
\Rightarrow & \mathbf{R}^{\pm}(n) \text{ holds} & \text{(by Lemma 4.8)}
\end{array}
$$

To complete the proof, consider the two scenarios in the theorem:

(i) Suppose $\mathbf{R}(-1)$ holds. By Lemma 2.3, no matter which of $\mathbf{R}(n)$ and $\mathbf{R}(-n)$ above holds, so does the other, thus $\mathbf{R}(n)$ holds.

(ii) Suppose $\mathbf{Q}(-1)$ does not hold. But since $\mathbf{Q}(n)$ holds, by Lemma 4.7, $\mathbf{Q}(-n)$ cannot hold, then by Theorem A $\mathbf{R}(-n)$ cannot hold as well. Thus $\mathbf{R}(n)$ holds.

□

7. Appendix

This table shows general Pell's equations that have been tested non-solvable upon applying Theorem A:

n	D																								
	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23	26	29	30	31	33	34	35	37	38	39
−15	P	P	P		P		P	P	P		P		Q	P	P	P	P	Q		P		P	P	P	Q
−14		P	P	P		P	Q	P			P	P	Q	Q		P	Q		P	P	P	Q	Q	P	
−13	P	Q	P	P	P	Q	P			P		P	P		Q	Q		Q	P	P	P	Q	P		Q
−12	P		P	Q		Q	P		P	Q	P			Q	P	P	P	Q		Q	Q	P		P	
−11	P			P	P	P		P	Q		P	P	P	Q		Q	P	P			Q	P	Q	Q	P
−10	P	P	Q	Q	P			P		Q	P		Q	P	P		Q	Q	Q	P	Q		P	P	Q
−9		Q		Q	Q		Q		Q	Q		Q	Q	Q	Q			Q	Q	Q		Q		Q	Q
−8			Q		Q	Q		Q	Q	Q			Q		Q	Q	Q	Q	Q		Q	Q	Q		Q
−7		P	P	P		P		P		Q	P	P	Q			P		Q	P	P	P	Q	Q	P	Q
−6	P	Q	P				P	Q	P		P	Q	Q		P	P	P	Q		Q	Q	P	Q	P	Q
−5	P	P			P	Q	Q	P		Q	P	Q		P	P	Q			Q	P	Q	Q	P	P	Q
−4		Q		Q	Q		Q		Q	Q		Q	Q	Q	Q			Q	Q	Q	Q	Q		Q	Q
−3	P		P	Q		Q	P		P	Q	P			Q	P	P	P	Q		Q	Q	P	Q	P	
−2			Q		Q	Q		Q	Q	Q	Q		Q		Q	Q	Q	Q	Q	Q	Q	Q	Q		Q
−1		Q		Q	Q		Q		Q	Q		Q	Q	Q	Q			Q	Q	Q	Q	Q		Q	Q
0																									
1																									
2		Q	Q	Q		Q	Q	Q		Q	Q	Q	Q	Q		Q	Q	Q		Q		Q	Q	Q	Q
3	P	Q	P		Q	Q	P		P	Q	P	Q	Q		P	P	P	Q	Q		Q	P	Q	P	Q

n	D																								
	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23	26	29	30	31	33	34	35	37	38	39
4																									
5	P	P		Q	P	Q		P	Q	Q	P		Q	P	P	Q		Q		P	Q	Q	P	P	Q
6	P		P	Q	Q		P	Q	P	Q	P		Q	Q	P	P	P		Q	Q	Q	P	Q	P	Q
7		P	P	P	Q	P	Q	P	Q	Q	P	P		Q	Q	P		Q	P	P	P	Q	Q	P	Q
8		Q	Q	Q		Q	Q	Q		Q		Q	Q	Q		Q	Q	Q		Q		Q	Q	Q	Q
9																									
10	P	P	Q		P		Q	P	Q		P	Q	Q	P	P		Q	Q		P	Q	Q	P	P	
11	P	Q		P	P	P	Q	P		Q	P	P	P		Q	Q	P	P	Q	Q	Q	P	Q		P
12	P	Q	P		Q	Q	P		P	Q	P	Q	Q		P	P	P	Q	Q		Q	P		P	Q
13	P		P	P	P	Q	P		Q	P		P	P	Q		Q		Q	P	P	P	Q	P	Q	
14		P	P	P	Q	P		P	Q	Q	P	P	Q		Q	P	Q	Q	P	P	P		Q	P	Q
15	P	P	P	Q	P		P	P	P	Q	P	Q		P	P	P	P	Q	Q	P		P	P	P	Q
16																									
17		P	P	P	P	P	P		P	Q			Q	P	P		P	Q	P	Q	Q	Q	P		P
18		Q	Q	Q		Q	Q	Q		Q	Q	Q	Q	Q		Q	Q	Q		Q		Q	Q	Q	Q
19	P	P			Q	P	Q	P	P	P		Q	P	P	Q	Q	P		P	P	P	Q	P		Q
20	P	P		Q	P	Q		P	Q	Q	P		Q	P	P	Q		Q		P	Q	Q	P	P	Q
21	P	P	P	P		P	P	P	P		P	P	Q	Q	P	P	P	Q	P	P	P	P		P	Q
22	P		Q	P	P	P		P		Q	P	P	P	Q	Q		P	P	Q	Q	Q	P	Q	Q	P
23		Q	P	Q	P	P	P		P	P	P	P	P	P	Q			P	Q	P	P	Q	P	P	Q
24	P		P	Q	Q		P	Q	P	Q	P		Q	Q	P	P	P		Q	Q	Q	P	Q	P	Q
25																									

(P = Condition P fails, Q = Condition Q fails but Condition P holds, blank = both Conditions P and Q hold)

This table shows general Pell's equations that have been tested solvable upon applying Theorem B:

n	D							
	10	15	26	30	35	39	42	51
-15	R	R						R
-14		R		R		R		
-13								
-12						R		
-11		R						
-10	R		R		R			
-9	R		R					
-8								R
-7								
-6	R	R					R	
-5				R				
-4	R		R					
-3						R		
-2								R
-1	R		R					
0	R	R	R	R	R	R	R	R
1	R	R	R	R	R	R	R	R

n	D							
	10	15	26	30	35	39	42	51
2								
3								
4	R	R	R	R	R	R	R	R
5								
6	R			R				
7							R	
8								
9	R	R	R	R	R	R	R	R
10	R	R	R			R		
11								
12								
13						R		R
14					R			
15	R							
16	R	R	R	R	R	R	R	R
17			R					
18								
19				R				
20								
21		R						R
22			R				R	
23			R					
24	R			R				
25	R	R	R	R	R	R	R	R

(R = both Conditions P and Q hold = solvable, blank = at least one of Conditions P or Q fails = non-solvable)

References

[1] T. Andreescu, D. Andrica, *A Quadratic Diophantine Equations*. Springer. ISBN 978-0-387-54109-9.

[2] A. Baker, *A Comprehensive Course in Number Theory*. Cambridge University Press. ISBN 978-1-107-01901-1.

[3] E. J. Barbeau, *Pell's Equation*. Springer. ISBN 978-0-387-22602-6.

[4] É. Fouvry, J. Klüners, *On the negative Pell equation*, Ann. Math. **172** (2010), 2035–2104.

[5] A. Issa, H. Sankari, *Some Criteria for Class Numbers to Be Non-One*, J. Math. **2020** (2020), 1–5.

[6] D. A. Marcus, *Number Fields* (2nd ed.), Springer. ISBN 978-3-319-90233-3.

[7] R. A. Mollin, *Algebraic Number Theory*, Chapman & Hall/CRC. ISBN 0-8493-3989-8.

[8] OEIS Foundation Inc. (2021), The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A029702.

[9] OEIS Foundation Inc. (2021), The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A031396.

[10] OEIS Foundation Inc. (2021), The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A192450.

REVIEWERS' COMMENTS

The main goal of this paper is to give sufficient conditions for the solvability of the diophantine equation (called the general Pell's equation), that is to find integers x, y such that

$$x^2 - Dy^2 = n$$

where n is an integer, $D \equiv 2, 3 \mod 4$, D is square free, and the class number of $\mathbb{Z}[\sqrt{D}]$ is 2.

The paper was reviewed by three reviewers. All reviewers agree that the author demonstrated his mastery of both elementary number theory methods (such as modular arithmetic, Chinese remainder theorem, qaudratic reciprocity), and advanced concepts in algebraic number theory (including concepts of rings of algebraic integers, ideal class group, etc). Reviewers were impressed that the author is only a high school student.