The solvability of negative Pell equation

Jiaqi Wang, Lide Cai

Mentor: Xiangxue Jia

Beijing National Day School

No.66 Yuquan Road. Haidian Dist. Beijing. China P.C

December 8, 2013

Abstract

Pell equation is an important research object in elementary number theory of indefinite equation. its form is simple, but it is rich in nature. Many number theory problems can be transformed into the problem of Pell equation’s solvability. However, the previous methods in determining the Pell equation’s solvability are sophisticated for calculation, which leads to the lack of efficiency. This paper gives new and more widely used methods to determine the solvability of Pell equation, including several necessary conditions, sufficient conditions and necessary and sufficient conditions.

Keywords

Pell equation, Solvability, Continued fraction expansion, Periodic

1. Introduction

1.1 Background and Motivation

In studying the theory of continued fraction expansions, we noticed the expansion of $\sqrt{\mathrm{D}}$ -type of irrational numbers were periodic, with its parity of period closely related to the solvability of negative Pell equation. Its period is odd if and only if negative Pell equation $Dx^2 - y^2 = 1$ is solvable.

It is well known that the positive Pell equation,

(1.1) $$x^2 - Dy^2 = 1,$$

has infinitely many solutions (x, y) whereas the negative Pell equation,

(1.2) $$Dx^2 - y^2 = 1,$$

does not always have a solution.

Henceforth, D will denote a positive square-free integer, and solution refer to a positive integral solution.

The Pell equation is one of the oldest Diophantine equation that has interested mathematicians all over the world for more than 1000 years. The most essential problem of these two Pell equations is determining their solvability and how to find out the solution to the Pell equations as quickly and concisely as possible. Archimedes' famous "cattle problem" was actually a problem about the solvability of the positive Pell equation.

The solution to positive Pell equation is said to be given by the Indian mathematician Braghmagupta in 6th century. Then, in the 17th century, Lagrange advanced his predecessor's theorem and gave the solution to positive Pell equation by continued fraction expansion theory. His result was that the positive Pell equation is solvable for any given D, and, the solvability of the negative Pell equation is determined by the parity of the period of $\sqrt{D}$'s continued fraction expansion. The equation is solvable if and only if the period is an odd number. The continued fraction expansion is a way to construct solutions.

Not only for huge D may it becomes extremely time consuming, even for some small Ds, the solution to the Pell equation is huge. For example, for D=61, we have $(x, y) = (29718, 3805)$ for negative Pell equation. The solutions of which would have huge time expense. According to [10] and [11], its running time is approaching $O\left(\sqrt{D}\right)$. Besides Lagrange, as [7] shows, many other mathematicians have made minor contributions to the problem relating the solvability of the Pell equation.

The most popular method that has made great progress today is relating the solvability of negative Pell equation to the solvability of other Diophantine equations.

In 1986, Kenneth Hardy and Kenneth.S.Williams proved that $Dx^2 - y^2 = 1$ is solvable if and only if D is the sum of a^2 and b^2, where $a, b \in \mathbb{N}^*$,and a is an odd number such that the Diophantine equation $bV^2 - 2aVW - bW^2 = 1$ of V,W is solvable.

The method above is put into use on [15], which means that for any given D we can determine whether $Dx^2 - y^2 = 1$ is solvable or not. Of course, the calculation must be within the limitation of computational power.

A.Grytczuk, F. Luca and M. W ́ojtowicz [1] proved that the negative Pell equation $Dx^2 - y^2 = 1$ is solvable if and only if there exist a primitive Pythagorean triple (A, B, C) (i.e. A, B, C are positive integers satisfying $A^2 + B^2 = C^2$ and gcd $(A, B) = 1$) and positive integers a, b such that $D = a^2 + b^2$ and $|aA - bB| = 1$.

Of greatest value here is the reduction of the coefficient of the negative Pell equation, which may reduce the time complexity in determining the solvability.

Another approach to this problem involves placing conditions on the modular residues of D which guarantee that (1.2) is solvable or unsolvable. This approach was initiated by Legendre in 1785. Dirichlet[13] observed that if $D = pq$ with $p \equiv q \equiv 1(\bmod 4)$ and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$ (where $\left(\frac{p}{q}\right)_4$ means that p is the power 4 residue modulo q), then (1.2) is solvable. For $D = p_1 p_2 p_3 \cdots p_N$, Tano[8] obtained quadratic residue criteria among the p_i , which when they held would guarantee (1.2) is solvable. Explicit modular residue conditions for particular classes of D are still being found, e.g. Kaplan[6], Pumplün[14].

However, for some huge D s, the previous results are lack of efficiency.

This motivates us to promote the previous results and give a quicker algorithm to determine the solvability of (1.2).

All the methods discussed in this essay are not only capable of determining the solvability of negative Pell equation $Dx^2 - y^2 = 1$, but can also be used to solve many problems relevant to the general Pell equation. For instance, they can be used to determine the parity of the period of the continued fraction expansion of the irrational number $\sqrt{\mathrm{D}}$ etc.

1.2 The content

In section 2, we give the preliminaries, including several important Lemmas in Pell equation and the properties of quadratic residue. We also give some notations that are used in the proof.

In section 3.1, we give a necessary condition for $Dx^2 - y^2 = 1$ to be solvable.

In section 3.2, we give some sufficient conditions for the solvability of $Dx^2 - y^2 = 1$. We give an algorithm to determine the solvability of $Dx^2 - y^2 = 1$ for some particular D s. Then, we define a function, which can be used to present a sufficient condition to the solvability of $Dx^2 - y^2 = 1$ base on the algorithm. We also give a series of corollaries.

In section 3.3, we first arrive at a necessary and sufficient condition for determining the solvability of $Dx^2 - y^2 = 1$ and we give several D s by the condition for which $Dx^2 - y^2 = 1$ is solvable. It forms theorem 6. By theorem 6, we give out several examples to show that there are many types of solvable negative Pell equation with quadratic form *D*.

Secondly, theorem 7 gives a sufficient and necessary condition for determining the solvability of $Dx^2 - y^2 = 1$ when $D \in Y$.

In section 4, we look back on our research, do some numerical experiments and give several types of solvable negative Pell equations.

In the end, we give several comparisons with the previous results.

In section 5, we give the conclusion.

In section 6, we give our plans for future work.

2. Preliminary

Lemma1.*Assume that* p *is an odd prime number, -1 is the quadratic residue of* p *if and only if* $p \equiv 1 \pmod 4$.

Take an odd prime p , we define the function with the integer variable d

$$\left(\frac{d}{p}\right)=\begin{cases}1, & \text{when } d \text{ is the quadratic residue modulo } p,\\ -1, & \text{when } d \text{ isn't the quadratic residue modulo } p,\\ 0, & \text{when } d \mid p.\end{cases}$$

We call $\left(\frac{d}{p}\right)$ the Legendre symbol of d modulo p .

Therefore, Lemma1 can be rewritten as

$$p\equiv 1(\bmod 4)\Leftrightarrow\left(\frac{-1}{p}\right)=1.$$

Lemma2.*Assume that* D *is a positive square-free integer,* $x^2-Dy^2=1$ *is solvable. Its general solution* (x_n,y_n) *can be given by its least positive solution* (x_0,y_0) *through*

(2.1) $$x_n+y_n\sqrt{D}=(x_0+y_0\sqrt{D})^{n+1}, n\in\mathbb{N}^*.$$

The following recursion formula can be proven by (2.1)

$$\begin{cases}x_{n+2}=2x_{n+1}x_0-x_n\\ x_1=2x_0^2-1\end{cases} n\in\mathbb{N}^*.$$

Lemma3.*Assume that* D *is a positive square-free integer, if* $Dx^2-y^2=1$ *is solvable, then its general solution* (x_n,y_n) *can be given by its least positive solution* (x_0,y_0) *through*

$$\sqrt{D}x_n+y_n=(\sqrt{D}x_0+y_0)^{2n+1}, n\in\mathbb{N}^*.$$

Lemma4.*Assume that* p *is an odd prime number, If* $\left(\frac{m}{p}\right)=1$, $r^2\equiv m \pmod p$ *has only two solutions* r_1,r_2 $(0\le r_1<r_2<p)$ *, with* $r_1+r_2=p$ *.*

Lemma5.*Assume that* $m,n,z\in\mathbb{N}$ $(m,n)=1, mn=z^2$ *, then there exist* $u,v\in\mathbb{Z}$ *, such that*

$$\begin{cases}m=u^2,\\ n=v^2,\end{cases},$$

where $(u,v)=1$.

The proof of the above lemmas is available in [2].

3. Main Work

3.1 Necessary conditions

Theorem 1.*If* $Dx^2-y^2=1$ *is solvable, then* D *is not divisible by 4 and* D *doesn't have a prime factor congruent to 3modulo 4.*

Proof. If $\exists$ prime p such that $p\equiv 3 \pmod 4$ and $p\mid D$, taking $Dx^2-y^2=1$ modulo p gives

$$y^2\equiv -1 \pmod p.$$

This means that -1 is the quadratic residue of p , contradicting lemma 1.

If $4\mid D$, taking $Dx^2-y^2=1$ modulo 4 gives

$$y^2 \equiv -1 \pmod 4.$$

However, $y^2 \equiv 0,1 \pmod 4$, leading to a contradiction.

To conclude, it is a necessary condition for D if $Dx^2 - y^2 = 1$ is solvable.

We give the following definition of three sets for simplicity

Definition 1

$Y_s := \{p \mid p \equiv 1 \pmod 4,\ \text{p is a prime number}\}$, we call it set of excellent prime numbers.

$Y := \left\{ x \mid x = \prod_{i=1}^{n} p_i^{a_i}, p_i \in Y_s, a_i, n \in \mathbb{N}^*, 2 \mid \prod_{i=1}^{n}(a_i + 1) \right\}$, we call it set of excellent odd numbers.

$U := \left\{ x \mid x = 2 \cdot \prod_{i=1}^{n} p_i^{a_i}, p_i \in Y_s, a_i \in \mathbb{N}^*, n \in \mathbb{N} \right\}$, we call it set of excellent even numbers.

By definition 1, theorem 1 can be rewritten as

If $Dx^2 - y^2 = 1$ *is solvable, then* $D \in Y$ *or* $D \in U$.

Remark. The necessary condition on D given in [12] is equivalent to theorem 1, by Fermat's theorem on sum of two squares.

3.2 Sufficient conditions

Theorem 2.*If* $D \in Y$ *or* $D \in U$ *, then the general solution* (x_n, y_n) *to* $x^2 - Dy^2 = 1$ *satisfies*

$$2 \nmid x_n, 2 \mid y_n .$$

Proof. Because (x_n, y_n) is a solution to $x^2 - Dy^2 = 1$, we obtain

(3.1) $$x_n^2 - Dy_n^2 = 1.$$

If $D \in Y$, taking(3.1) modulo 4 gives

$$x_n^2 - Dy_n^2 \equiv x_n^2 - y_n^2 \equiv 1 \pmod 4.$$

Since for any integer m , $m^2 \equiv 0,1 (\mathrm{mod}\, 4)$, we obtain

$$2 \nmid x_n, 2 \mid y_n .$$

If $D \in U$ taking (3.1) modulo 4 gives

$$x_n^2 - Dy_n^2 \equiv x_n^2 - 2y_n^2 \equiv 1 \pmod 4$$

Since for any integer m , $m^2 \equiv 0,1 (\mathrm{mod}\, 4)$, we obtain

$$2 \nmid x_n, 2 \mid y_n .$$

Theorem 3. $Dx^2 - y^2 = 1$ *is solvable if*

(i) $D = 2$*;*

(ii) $D = p^a, p \in Y_s, 2 \nmid a$ *;*

(iii) $D = p^a q^b, p, q \in Y_s, 2 \nmid a, \left(\dfrac{p}{q}\right) = -1$*;*

(iv) $D = 2p^a, p \equiv 5 \pmod 8, a \in \mathbb{N}^*$ *, where* p *is a prime.*

*Proof***.** **(i)**For the Pell equation $2x^2 - y^2 = 1$, it's easy to verify that $(x, y) = (1,1)$ is a solution to the equation.

(ii) Applying Theorem2, we obtain the least positive solution (x_0, y_0) to $x^2 - Dy^2 = 1$ satisfying

$$2 \nmid x_0, 2 \mid y_0.$$

Assuming $y_0 = 2k, k \in \mathbb{N}^*$, we rewrite $x_0^2 - Dy_0^2 = 1$ as

(3.2) $$\left(\frac{x_0+1}{2}\right)\left(\frac{x_0-1}{2}\right) = Dk^2.$$

Let $m = \frac{x_0+1}{2}, n = \frac{x_0-1}{2}$, from $2 \nmid x_0$, we obtain $\frac{x_0+1}{2}, \frac{x_0-1}{2} \in N^*$.

Because $\frac{x_0+1}{2} = \frac{x_0-1}{2} + 1$, we obtain

$$(\frac{x_0+1}{2}, \frac{x_0-1}{2})=1.$$

Namely,

$$(m, n) = 1.$$

Then (3.2)is equivalent to

$$mn = p^a k^2.$$

Since $(m, n) = 1$, p is a prime number, by lemma 5, we can get two possible cases for m, n

$$(1)\begin{cases} m = u^2, \\ n = p^a v^2, \end{cases} (2)\begin{cases} m = p^a u^2, \\ n = v^2, \end{cases}.$$

In both cases, $(u, v) = 1$. In case (1), $p \nmid u$. Incase (2), $p \nmid v$.

In case (1), as $m - n = \frac{x_0+1}{2} - \frac{x_0-1}{2} = 1$, we obtain

$$u^2 - p^a v^2 = 1.$$

Namely, (u, v) is a solution to $x^2 - p^a y^2 = 1$.

Recalling $x_0^2 - Dy_0^2 = 1$, we obtain $x_0^2 = Dy_0^2 + 1 > 1$, therefore $x_0 > 1$.Because $2 \nmid x_0$, we obtain $x_0 \geq 3$.

Therefore,

$$u = \sqrt{m} = \sqrt{\frac{x_0+1}{2}} < \sqrt{\frac{x_0+x_0}{2}} = \sqrt{x_0} < x_0.$$

Hence, (u, v) is a solution to $x^2 - p^a y^2 = 1$ and $u < x_0$.

However, (x_0, y_0) is the least positive solution to $x^2 - p^a y^2 = 1$, leading to a contradiction.

Therefore, case (2) holds, which means that $\begin{cases} m = p^a u^2, \\ n = v^2, \end{cases}$, then

$$p^a u^2 - v^2 = m - n = 1.$$

It shows we find a solution (u, v) to $p^a x^2 - y^2 = 1$, here,

$$\begin{cases} u = \sqrt{\frac{x_0+1}{2p^a}}, \\ v = \sqrt{\frac{x_0-1}{2}}, \end{cases}.$$

(iii)Applying Theorem2, we obtain the least positive solution (x_0, y_0) to $x^2 - Dy^2 = 1$satisfying

$$2 \nmid x_0, 2 \mid y_0 .$$

Assume that $y_0 = 2k, k \in \mathbb{N}^*$, we rewrite $x_0^2 - Dy_0^2 = 1$as

$$\left(\frac{x_0+1}{2}\right)\left(\frac{x_0-1}{2}\right) = Dk^2 . \tag{3.3}$$

Let $m = \frac{x_0+1}{2}, n = \frac{x_0-1}{2}$, from $2 \nmid x_0$, we obtain $\frac{x_0+1}{2}, \frac{x_0-1}{2} \in \mathbb{N}^*$.

Because $\frac{x_0+1}{2} = \frac{x_0-1}{2} + 1$, we obtain

$$(\frac{x_0+1}{2}, \frac{x_0-1}{2})=1.$$

Namely,

$$(m,n) = 1.$$

Then (3.3)is equivalent to

$$mn = p^a q^b k^2 .$$

Because $(m,n) = 1$, p,q are prime numbers, by lemma 5,we can get 4 possible cases for m,n

$$(1)\begin{cases} m = p^a q^b u^2, \\ n = v^2, \end{cases} (2)\begin{cases} m = p^a u^2, \\ n = q^b v^2, \end{cases} (3)\begin{cases} m = q^b u^2, \\ n = p^a v^2, \end{cases} (4)\begin{cases} m = u^2, \\ n = p^a q^b v^2, \end{cases} .$$

$(u,v) = 1$ holds in all cases. $p \nmid v, q \nmid v$ holds in case (1); $p \nmid v, q \nmid u$ holds in case (2); $p \nmid u, q \nmid v$ holds in case (3); $p \nmid u, q \nmid u$ holds in case(4).

Since $2 \nmid a$, we obtain

$$p^{a+1} u^2 = (p^{\frac{a+1}{2}} u)^2 .$$

In case (2), from $p^a u^2 - q^b v^2 = m - n = 1$, we obtain

$$p^{a+1} u^2 - pq^b v^2 = p . \tag{3.4}$$

Taking (3.4) modulo q gives $\left(\frac{p}{q}\right) = 1$. However, $\left(\frac{p}{q}\right) = -1$, leading to a contradiction.

Incase (3), $q^b u^2 - p^a v^2 = m - n = 1$, we obtain

$$pq^b u^2 - p^{a+1} v^2 = p . \tag{3.5}$$

Since $2 \nmid a$, we obtain

$$p^{a+1} v^2 = (p^{\frac{a+1}{2}} v)^2 .$$

Taking (3.5) modulo q gives $\left(\frac{-p}{q}\right) = 1$.

However,

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

leading to a contradiction.

In case (4), $u^2 - p^a q^b v^2 = 1$ .Namely, we obtain a solution (u,v) to $x^2 - p^a q^b y^2 = 1$, and $u=\sqrt{m}=\sqrt{\dfrac{x_0+1}{2}}<x_0$, which means that（u,v) is a smaller solution than (x_0,y_0) .However, (x_0,y_0) is the least positive solution to $x^2-Dy^2=1$, contradiction.

In conclusion, case(1) holds, which means that $\begin{cases} m=p^aq^bu^2, \\ n=v^2, \end{cases}$. Therefore,

$$p^aq^bu^2-v^2=1.$$

So we have found a solution（u,v) to $p^aq^bx^2-y^2=1$.

$$(u,v)=(\sqrt{\frac{m}{p^aq^b}},\sqrt{n})=(\sqrt{\frac{x_0+1}{2p^aq^b}},\sqrt{\frac{x_0-1}{2}}).$$

(iv) Applying Theorem2, we obtain the least positive solution (x_0,y_0) to $x^2-Dy^2=1$satisfying

$$2\nmid x_0, 2\mid y_0.$$

Assume that $y_0=2k, k\in\mathbb{N}^*$, we rewrite $x_0^2-Dy_0^2=1$ as

(3.6) $$\left(\frac{x_0+1}{2}\right)\left(\frac{x_0-1}{2}\right)=Dk^2.$$

Let $m=\dfrac{x_0+1}{2}, n=\dfrac{x_0-1}{2}$, from $2\nmid x_0$, we obtain $\dfrac{x_0+1}{2},\dfrac{x_0-1}{2}\in\mathbb{N}^*$.

Because $\dfrac{x_0+1}{2}=\dfrac{x_0-1}{2}+1$, we obtain

$$(\frac{x_0+1}{2},\frac{x_0-1}{2})=1.$$

Namely

$$(m,n)=1.$$

Then (3.6) is equivalent to

$$mn=2p^ak^2.$$

Because $(m,n)=1$, by lemma 5, we obtain four possible cases

$$(1)\begin{cases} m=2p^au^2, \\ n=v^2, \end{cases} (2)\begin{cases} m=p^au^2, \\ n=2v^2, \end{cases} (3)\begin{cases} m=2u^2, \\ n=p^av^2, \end{cases} (4)\begin{cases} m=u^2, \\ n=2p^av^2, \end{cases}.$$

In all cases, $(u,v)=1$. In case(1) $p\nmid v, 2\nmid v$ .In case(2), $p\nmid v, 2\nmid u$. In case(3), $p\nmid u, 2\nmid v$. In case (4), $p\nmid u, 2\nmid u$.

The same procedure in the proof of theorem 1.3 can be adapted to eliminate case (2),(3),(4).To conclude, case (1) holds, namely

$$\begin{cases} m=2p^au^2, \\ n=v^2, \end{cases}.$$

Therefore,

$$2p^au^2-v^2=1.$$

So we have a solution (u,v) to $2p^ax^2-y^2=1$, and

$$(u,v)=(\sqrt{\frac{m}{2p^a}},\sqrt{n})=(\sqrt{\frac{x_0+1}{4p^a}},\sqrt{\frac{x_0-1}{2}}).$$

We hope to generalize Theorem 3 to case in which D has more prime factors. By considering the similarities in the treatment of different cases in theorem 3, we look for a function to determine the solvability of $Dx^2 - y^2 = 1$, where $D \in Y$.

For example, let $D = 5\times 13^2 \times 17^2$, we first break D into A, B, such that $(A,B)=1, AB=D, A\neq D, B\neq D$. There are the following three cases totally.

Case (1): $A=5, B=13^2\times 17^2$,

We know that $\left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=-1$

Implying for case

$$\begin{cases} m=5u^2, \\ n=13^2\cdot 17^2 v^2, \end{cases},$$

we have

$$5u^2 - 13^2\cdot 17^2 v^2 = 1\cdot$$

Multiplying the above equation by 5, we obtain

$$5^2u^2 - 5\cdot 13^2\cdot 17^2 v^2 = 5\cdot$$

Taking the previous equation modulo 13 gives,

$$\left(\frac{5}{13}\right)=1.$$

However,

$$\left(\frac{5}{13}\right)=-1,$$

leading to a contradiction.

Case (2): $A=17^2, B=5\times 13^2$

We know that $\left(\frac{5}{17}\right)=\left(\frac{17}{5}\right)=\left(\frac{2}{5}\right)=-1;$

Case (3): $A=13^2, B=5\times 17^2$

We know that $\left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=-1;$

In case (2) and (3), we can adapt the same procedure in case (1).

Therefore, $5\times 13^2\times 17^2 x^2 - y^2 = 1$ is solvable, we check D on [15], it shows $5\times 13^2\times 17^2 x^2 - y^2 = 1$ is solvable.

Definition 2. $g:\mathbb{N}\setminus\{0,1\}\to\mathbb{N}^*,\ \forall x>1, x\in\mathbb{N}^*,\ x=\prod_{i=1}^{n} p_i^{a_i}$.

$$g(x)=\begin{cases} \prod\limits_{2\nmid a_i}^{n} p_i^{a_i} & \text{if there exists an } i \text{ such that} 2\nmid a_i, \\ 1 & \text{if } x \text{ is a square,} \end{cases}.$$

Theorem 4. *For any* x *in* $\mathbb{N}\setminus\{0,1\}$, $g(x)x$ *is a square.*

Proof. If x is a square, then

$$g(x)x = 1 \bullet x = x .$$

Therefore, $g(x)x$ is a square.

If x is not a square, assuming that $x = \prod_{i=1}^{m} p_i^{a_i} \cdot \prod_{j=1}^{k} q_j^{b_j}$,

where $a_i, b_j \in \mathbb{N}^*, m \in \mathbb{N}^*, k \in \mathbb{N}, 2 \nmid a_i, 2 \mid b_j$. Then

$$g(x)x = \prod_{i=1}^{m} p_i^{a_i} \cdot (\prod_{i=1}^{m} p_i^{a_i} \cdot \prod_{j=1}^{k} q_j^{b_j}) = \prod_{i=1}^{m} p_i^{2a_i} \cdot \prod_{j=1}^{k} q_j^{b_j} .$$

Since for any i , $2a_i$ is an even integer, $g(x)x$ is a square.

For $D \in Y$, we can try to determine the solvability of $Dx^2 - y^2 = 1$ by the following algorithm

Definition 3. $f : N \setminus \{0,1\} \to \{0,1\}$, $f(D)$ *is the output of* ***W.C.J*** *algorithm.*

W.C.J algorithm

```
Input $D \in Y$ ; $f(D) = 0$ ;
for each $(A,B) = 1, AB = D, A \neq D, B \neq D$ {
    possible = true;
    for each prime factor $p$ of $B$ {
        if $\left(\frac{g(A)}{p}\right) == -1$ {
            possible = false;
            break;
        }
    }
    If possible == true
    Return;
}
return $f(D) = 1$ ;
```

Expressing the result by the function, we obtain theorem 5.

Theorem 5. *If* $D \in Y$ *and* $f(D)$ *=1, then* $Dx^2 - y^2 = 1$ *is solvable.*

Proof. For $D \in Y$, assume that its prime factorization is $D = \prod_{i=1}^{n} p_i^{a_i}$.

Therefore, there are $2^n - 2$ kinds of ways to break D into A, B , such that $(A,B) = 1, AB = D, A \neq D, B \neq D$.

For every (A,B) , examine indefinite equation

$$Ax^2 - By^2 = 1 .$$

Multiplying the above equation by $g(A)$, we obtain

$$(g(A)A)x^2 - By^2 = g(A) .$$

By Theorem 4, we obtain $g(A)A$ is a square. Therefore, for any prime factor p of D , we obtain

$$(g(A)A)x^2 \equiv g(A) \pmod{p}.$$

Namely,

$$\left(\frac{g(A)}{p}\right)=1.$$

For every prime factor p of B, we calculate the value of $\left(\frac{g(A)}{p}\right)$. If one of the $\left(\frac{g(A)}{p}\right)$s equals to -1, then $Ax^2 - By^2 = 1$ is unsolvable.

Since $f(D)=1$ means that all the $2^n - 2$ kinds of ways to break D into A, B, $(A,B)=1$, $A \neq D, B \neq D$, $Ax^2 - By^2 = 1$ is unsolvable.

If $(A,B)=(1,D)$, adapt the same procedure in the proof of theorem 3, we will find contradiction. Therefore, the final case holds, it derives that $Dx^2 - y^2 = 1$ is solvable.

Remark1. This method may not eliminate some cases for a given $D \in Y$.

E.g. $D = 5^2 \cdot 13^2 \cdot 17$, we get three possible cases

Case (1) $A = 13^2, B = 5^2 \times 17$, $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1$;

Case (2) $A = 17, B = 5^2 \times 13^2$;

Case (3) $A = 5^2, B = 13^2 \times 17$;

In case (1), none of the value of the Legendre symbols is -1. Therefore, $f(D)=0$. However, we can check $D = 5^2 \cdot 13^2 \cdot 17$ on [15] and actually $5^2 \times 13^2 \times 17x^2 - y^2 = 1$ is solvable.

Remark2. The parity of the power of each prime factor p of D is the only important factor in the algorithm. Therefore, we can reduce the power of enormous D to 1or2. This means that we can construct huge possible D from small D with $f(D)=1$.

By the main idea of the algorithm, we can give the following corollaries:

Corollary 1. Given $D = \prod_{i=1}^{m} p_i^{a_i} \cdot \prod_{j=1}^{k} q_j^{b_j}$, where $a_i, b_j \in \mathbb{N}^*, m \in \mathbb{N}^*, k \in \mathbb{N}, 2 \nmid a_i, 2 \mid b_j$, and $f(D)=1$, then for any $c_i, d_j \in \mathbb{N}^*, m \in \mathbb{N}^*, k \in \mathbb{N}, 2 \nmid c_i, 2 \mid d_j$, $E = \prod_{i=1}^{m} p_i^{c_i} \cdot \prod_{j=1}^{k} q_j^{d_j}$, we have $f(E)=1$. Namely, $Ex^2 - y^2 = 1$ is solvable.

Corollary 2.*Assume that* $p, q \in Y_s, \left(\frac{p}{q}\right) = -1$. $A = \{x \mid x \equiv q \pmod{4p}, x\ is\ a\ prime\}$. $\forall p_1, \cdots, p_n \in A$, $pp_1p_2\cdots p_nx^2 - y^2 = 1$ *is solvable.*

Corollary 3.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 13 modulo 20, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 4.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 17 modulo 20, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 5.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 5 modulo 52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 6.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 21 modulo 52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 7.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 33 modulo 52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 8.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 37 modulo 52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 9.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 41 modulo 52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 10.*Assume that* $p_1,p_2,\cdots,p_n$ *are primes which congruent to 45 modulo52, a is an odd number, then* $5^a p_1p_2\cdots p_nx^2-y^2=1$ *is solvable.*

Corollary 11.*Assume that* $p,q,r_1,r_2,\cdots,r_m,s_1,s_2,\cdots,s_k$ *are all excellent prime numbers,* $\left(\frac{p}{q}\right)=-1$ *,* $\left(\frac{p}{r_i}\right)=-1$*,* $\left(\frac{q}{s_j}\right)=-1$ $i=1,2,\cdots,m$*,* $j=1,2,\cdots,k$*, a and b are both odd numbers, then* $p^aq^br_1r_2\cdots r_ms_1s_2\cdots s_kx^2-y^2=1$ *is solvable.*

Corollary 12. *Assume that* $p_1,p_2,\cdots p_n,p_{1,1},p_{1,2},\cdots p_{1,m_1},p_{2,1},p_{2,2},\cdots p_{2,m_2},\cdots,$ $p_{n,1},p_{n,2},\cdots p_{n,m_n}$ *are all excellent prime numbers,*

$\left(\dfrac{p_i}{p_j}\right)=-1$, $i,j\in\{1,2,3,\cdots,n\}$, $i\neq j$, $\left(\dfrac{p_i}{p_{i,1}}\right)=\left(\dfrac{p_i}{p_{i,2}}\right)=\cdots=\left(\dfrac{p_i}{p_{i,m_i}}\right)=-1$, $i=1,2,\cdots,n$, $a_1,a_2,\cdots,a_n$ are odd numbers, then $\prod_{i=1}^{n}p_i^{a_i}\cdot\prod_{i=1}^{m_1}p_{1,i}\cdot\prod_{i=1}^{m_2}p_{2,i}\cdot\cdots\cdot\prod_{i=1}^{m_n}p_{n,i}x^2-y^2=1$ is solvable.

3.3 Sufficient and necessary conditions

We observe that for a given solution (x,y) to negative Pell equation, we can find a D for which $Dx^2-y^2=1$ is solvable. Therefore, by going through all solutions (x,y) to $Dx^2-y^2=1$, we can obtain every D that for which $Dx^2-y^2=1$ is solvable.

Assume that x is an integer and for any prime factor p of x, $p\in Y_s$ .The solutions to the congruence equation $r^2\equiv-1 \pmod{x^2}$ are

$$r\equiv r_{x,1},r_{x,2},\cdots,r_{x,n_x} \pmod{x^2},(0<r_{x,1}<r_{x,2}...<r_{x,n_x}<x^2).$$

By lemma 4, we can obtain $n_x\geq 2$ .Denote $\dfrac{r_{x,i}^2+1}{x^2}$ by $M_{x,i}$, $i=1,2,\cdots,n_x$, then $M_{x,i}\in\mathbb{N}^*$.

Theorem6. *$Dx^2-y^2=1$ is solvable if and only if ($\exists x\in\mathbb{N}^*$, such that for any prime factor p of x, we have $p\equiv1 \pmod 4$, and $D = x^2k^2+2r_{x,i}k+M_{x,i}$ is suitable for an $i\in\{1,2,\cdots,n_x\}$ and a natural number k) or (there is a k, such that $k\in N^*$ and $D=k^2+1$).*

Proof. Because $Dx^2-y^2=1$ is solvable, assume that (x_0,y_0) is a solution to $Dx^2-y^2=1$, then

$$Dx_0^2-y_0^2=1.$$

It can be rewritten as $D=\dfrac{y_0^2+1}{x_0^2}$ .Since $D\in\mathbb{N}^*$, $x_0^2\mid y_0^2+1$, by lemma1, all prime factors of x congruent to 1 modulo 4.

If $x_0\neq1$, assume that the solutions to the congruence equation are

$$r\equiv r_{x_0,1},r_{x_0,2},\cdots,r_{x_0,n_{x_0}} \pmod{x_0^2},0<r_{x,1}<r_{x,2}...<r_{x,n_x}<x^2.$$

By lemma 4 and the Chinese remainder theorem, we can obtain $n_x\geq 2$.

Then there exist $i\in\{1,2,\cdots,n_x\}$, and $k\in\mathbb{N}$, such that $r_{x_0,i}+kx_0^2=y_0$. Denote $\dfrac{r_{x_0,i}^2+1}{{x_0}^2}$

by $M_{x_0,i}$.

Then

$$D=\frac{y_0^2+1}{x_0^2}=\frac{(r_{x_0,i}+kx_0{}^2)^2+1}{x_0{}^2}=x_0{}^2k^2+2r_{x_0,i}k+M_{x_0,i}.$$

If $x_0=1$, then $D=y_0^2+1$. There is a $k\in\mathbb{N}^*$, such that $D=k^2+1$.

Conversely, when $D=x_0{}^2k^2+2r_{x_0,i}k+M_{x_0,i}$, denote $\begin{cases}x=x_0,\\ y=kx_0^2+r_{x_0,i},\end{cases}$ and substitute it into $Dx^2-y^2=1$. Then

$$\begin{aligned}Dx^2-y^2&=Dx_0^2-(kx_0^2+r_{x_0,i})^2\\&=(x_0{}^2k^2+2r_{x_0,i}k+M_{x_0,i})x_0^2-(kx_0^2+r_{x_0,i})^2\\&=M_{x_0,i}x_0^2-r_{x_0,i}^2=\frac{r_{x_0,i}^2+1}{x_0{}^2}x_0^2-r_{x_0,i}^2\\&=1\end{aligned}$$

Hence, $Dx^2-y^2=1$ is solvable.

When $D=k^2+1$, let $\begin{cases}x=1,\\ y=k,\end{cases}$ and substitute it to $Dx^2-y^2=1$,

$$Dx^2-y^2=D^2-k^2=k^2+1-k^2=1.$$

Therefore, $Dx^2-y^2=1$ is solvable.

By theorem 6, we can construct infinite sequences of numbers such that all terms, represents a D for which $Dx^2-y^2=1$ solvable.

For example,

x^2	r_1,r_2	M_1,M_2
5^2	7,18	2,13
13^2	70,99	29,58
17^2	38,251	5,218
29^2	41,800	2,701
…	…	…

Table 1. the quadratic form *D* by theorem 6

$G(5^2;7;k)=25k^2+14k+2$, $G(5^2;18;k)=25k^2+36k+13$,

$G(13^2;70;k)=169k^2+140k+29$, $G(13^2;99;k)=169k^2+198k+58$,

$G(17^2;38;k)=289k^2+76k+5$, $G(17^2;251;k)=361k^2+502k+218$,

$G(29^2;41;k)=841k^2+82k+2$, $G(29^2;800;k)=841k^2+1600k+701$.

In the above formulae, when $k\in N$, we can find infinitely many D such that $Dx^2-y^2=1$ is solvable.

Namely,

$$(25k^2+14k+2)x^2-y^2=1, \quad (25k^2+36k+13)x^2-y^2=1,$$
$$(169k^2+140k+29)x^2-y^2=1, (169k^2+198k+58)x^2-y^2=1,$$
$$(289k^2+76k+5)x^2-y^2=1, (361k^2+502k+218)x^2-y^2=1,$$
$$(841k^2+82k+2)x^2-y^2=1, (841k^2+1600k+701)x^2-y^2=1,$$

are solvable for any natural number *k*.

When x is a positive odd integer containing a prime factor p which belongs to Y_s or $x=1$, by going through the domain of k, we obtain the union of infinite sequences. For every term in the sequences, the Pell equation $Dx^2-y^2=1$ is solvable and all solvable D are contained in these sequences. That is why this theorem is a necessary and sufficient condition for determining the solvability of $Dx^2-y^2=1$. It also gives a way to construct D in quadratic form.

Theorem7. *Assume that* $D\in Y$ *, the least positive solution to* $x^2-Dy^2=1$ *is* (x_0,y_0) *, then*

$$Dx^2-y^2=1 \textit{ is solvable } \Leftrightarrow \forall p\in Y_s \textit{ and } p\,|\,D\,,\ p\nmid x_0-1$$

Proof. **(**proof by contradiction) If $\exists p\in Y_s$ and $p\,|\,D$, such that $p\,|\,x_0-1$.

Since $Dx^2-y^2=1$ is solvable, suppose (x_n', y_n') is a solution to it, note that

$$\begin{aligned}&(2(y_n')^2+1)^2-4Dx_n'^2y_n'^2\\&=(Dx_n'^2+y_n'^2)^2-4Dx_n'^2y_n'^2\\&=D^2x_n'^4+y_n'^4-2Dx_n'^2y_n'^2\\&=(Dx_n'^2-y_n'^2)^2\\&=1\end{aligned}\quad .$$

Then $(2(y_n')^2+1, 2x_n'y_n')$ is a solution to $x^2-Dy^2=1$.

By lemma 3, for the solutions of $Dx^2-y^2=1$, we have

$$\begin{cases}x_{n+2}=2x_{n+1}x_0-x_n\\x_1=2x_0^2-1\end{cases}.$$

Because $\exists p\in Y_s$ and $p\,|\,D$, such that $p\,|\,x_0-1$, according to our recursion formula, we can obtain

$$x_n\equiv 1 \pmod p, n\in\mathbb{N}.$$

Denote $2y_n'^2+1$ by x_m, then $x_m\equiv 1 \pmod p$, which means that $p\,|\,x_m-1$.

Because $y_n'^2 = \frac{x_m - 1}{2} \equiv 0 \pmod p$, we obtain

$$Dx_n'^2 - y_n'^2 \equiv 0 \pmod p .$$

However, $Dx_n'^2 - y_n'^2 = 1 \equiv 1 \pmod p$, leading to a contradiction.

Conversely, If $\forall p \in Y_s$ and $p \mid D$, $p \nmid x_0 - 1$.Then, by theorem 2, $2 \nmid x_0, 2 \mid y_0$, so

$$\left(\frac{x_0+1}{2}\right)\cdot\left(\frac{x_0-1}{2}\right) = D\left(\frac{y_0}{2}\right)^2 .$$

We obtain

$$p \mid \frac{x_0+1}{2} .$$

Because $(\frac{x_0+1}{2}, \frac{x_0-1}{2}) = 1$, by lemma 5, there are two integers u, v such that $(u, v) = 1$,

and

$$\begin{cases} \frac{x_0+1}{2} = Du^2, \\ \frac{x_0-1}{2} = v^2, \end{cases} .$$

Therefore,

$$Du^2 - v^2 = \frac{x_0+1}{2} - \frac{x_0-1}{2} = 1 .$$

It means that (u, v) is a solution to $Dx^2 - y^2 = 1$. □

By theorem 1, if $Dx^2 - y^2 = 1$ is solvable, then $D \in Y$ or $D \in U$ .when $D \in U$, the solvability of $Dx^2 - y^2 = 1$ is still unknown. Theorem7 gives a sufficient and necessary condition for $Dx^2 - y^2 = 1$ to be solvable when $D \in Y$.

However, this theorem is not suitable for determining the solvability, if $Dx^2 - y^2 = 1$ is solvable, assume that the least positive solution to $Dx^2 - y^2 = 1$ is (x_0', y_0') and the least positive solution to $x^2 - Dy^2 = 1$ is (x_0, y_0) . They satisfy the inequalities

$$x_0' < x_0, y_0' < y_0 .$$

(We will give further illustration in the proof of theorem 8).

If we use this theorem for determining the solvability, we have to find the least positive solution to $x^2 - Dy^2 = 1$. However, as the least positive solution to $x^2 - Dy^2 = 1$ is greater than the least positive solution to $Dx^2 - y^2 = 1$, time complexity of solving $x^2 - Dy^2 = 1$ is greater than solving $Dx^2 - y^2 = 1$ directly.

Despite this, the theorem actually serves as a bridge between the two problems herein, namely the solvability of $Dx^2 - y^2 = 1$ and the determination of a solution of $x^2 - Dy^2 = 1$. It is also a practical method if the least positive solution (x_0, y_0) to $x^2 - Dy^2 = 1$ is obvious since one merely needs to verify whether $p \nmid x_0 - 1$ to determine whether or not the negative Pell equation is solvable.

Theorem 8. *Assume that* $D \in Y$ *, and* $Dx^2 - y^2 = 1$ *is solvable, by lemma 3 its general solution* (x'_n, y'_n) *can be given by its least positive solution* (x'_0, y'_0) *through*

$$\sqrt{D}x'_n + y'_n = (\sqrt{D}x'_0 + y'_0)^{2n+1}, n \in \mathbb{N}^*.$$

Let N_D *be the set of these solutions* (x'_n, y'_n)*. Similarly, by lemma2, let* P_D *be the set of general evenly indexed solutions* (x_{2n}, y_{2n}) *to* $x^2 - Dy^2 = 1$.

We can obtain a one-to-one mapping $g : P_D \to N_D$*.Namely,*

$$\begin{cases} x'_i = \sqrt{\dfrac{x_{2i}+1}{2D}}, \\ y'_i = \sqrt{\dfrac{y_{2i}+1}{2}}, \end{cases}.$$

Proof. Assume that $D \in Y$, the least positive solution to $x^2 - Dy^2 = 1$ is (x_0, y_0), then

(3.14) $$x_0{}^2 - Dy_0{}^2 = 1.$$

Assume that p is a prime factor of D. Taking (3.14) modulo p, we obtain

(3.15) $$x_0{}^2 \equiv 1 \pmod p.$$

(3.15) is equivalent to

$$x_0 \equiv \pm 1 \pmod p.$$

If $x_0 \equiv 1 \pmod p$, apply the recurrence relation of the solution to $x^2 - Dy^2 = 1$ by lemma 2, we obtain

(3.16) $$x_n \equiv 1 \pmod p), n \in \mathbb{N}^*.$$

If $Dx^2 - y^2 = 1$ is solvable, assume that (x'_n, y'_n) is a solution. Note that

$$\begin{aligned} &(2(y'_n)^2 + 1)^2 - 4Dx'^2_n y'^2_n \\ &= (Dx'^2_n + y'^2_n)^2 - 4Dx'^2_n y'^2_n \\ &= D^2 x'^4_n + y'^4_n - 2Dx'^2_n y'^2_n \\ &= (Dx'^2_n - y'^2_n)^2 \\ &= 1 \end{aligned}$$

Then $(2(y'_n)^2 + 1, 2x'_n y'_n)$ is a solution to $x^2 - Dy^2 = 1$.

Denote $2y'^2_n + 1$ by x_m, then by (3.16), $x_m \equiv 1 \pmod p$.

Therefore,

$$2(y'_n)^2 + 1 \equiv 1 \pmod p.$$

Hence,

$$y'_n \equiv 0 \pmod p.$$

Taking $Dx_n'^2 - y_n'^2 = 1$ modulo p, we obtain

$$1 = Dx_n'^2 - y_n'^2 \equiv 0 \times x_n'^2 - 0^2 \equiv 0 \,(\mathrm{mod}\, p).$$

Contradiction.

Therefore, for any prime factor p of D, we have, $x_0 \equiv -1 \pmod{p}$.

By lemma2, we obtain

$$x_{2i} \equiv -1 \pmod{p}, x_{2i+1} \equiv 1 \pmod{p}, \quad \forall i \in \mathbb{N}$$

$\forall i \in \mathbb{N}$, we have $x_{2i}^2 - Dy_{2i}^2 = 1$, by theorem 2, we have $2 \nmid x_{2i}, 2 \mid y_{2i}$. Therefore

$$\left(\frac{x_{2i}+1}{2}\right) \cdot \left(\frac{x_{2i}-1}{2}\right) = D\left(\frac{y_{2i}}{2}\right)^2.$$

Since $x_{2i} \equiv -1 \,(\mathrm{mod}\, p)$, $2 \nmid x_{2i}$, $(p,2) = 1$, we obtain

$$p \mid \frac{x_{2i}+1}{2}$$

holds for any prime factor p of D.

Therefore, by lemma 5, $\exists u_i, v_i \in \mathbb{N}^*$, such that

$$\begin{cases} \dfrac{x_{2i}+1}{2} = Du_i^2, \\ \dfrac{x_{2i}-1}{2} = v_i^2, \end{cases}.$$

Implying

$$Du_i^2 - v_i^2 = 1.$$

Namely, (u_i, v_i) is a solution to $Dx^2 - y^2 = 1$.
Here,

$$\begin{cases} u_i = \sqrt{\dfrac{x_{2i}+1}{2D}}, \\ v_i = \sqrt{\dfrac{y_{2i}+1}{2}}, \end{cases}$$

We obtain a mapping g from P_D to N_D, namely,

$$g : (x_{2i}, y_{2i}) \mapsto \left(\sqrt{\frac{x_{2i}+1}{2D}}, \sqrt{\frac{x_{2i}+1}{2}}\right).$$

Note that, $\forall i < j \in \mathbb{N}$, by lemma2, we obtain

$$x_{2i} < x_{2j}, y_{2i} < y_{2j}.$$

Therefore

$$\sqrt{\frac{x_{2i}+1}{2D}} < \sqrt{\frac{x_{2j}+1}{2D}}, \sqrt{\frac{x_{2i}+1}{2}} < \sqrt{\frac{x_{2j}+1}{2}}.$$

This shows that g is an injection.

$\forall i \in \mathbb{N}$, assume that (x_i', y_i') is a solution to $Dx^2 - y^2 = 1$.Note that

$$\begin{aligned}&(2y_i'^2+1)^2-D(2x_i'y_i')^2\\ &=(Dx_i'^2+y_i'^2)^2-4Dx_i'^2y_i'^2\\ &=D^2x_i'^4+y_i'^4-2Dx_i'^2y_i'^2\\ &=(Dx_i'^2-y_i'^2)^2\\ &=1.\end{aligned}$$

Therefore

$$(2(y_i')^2+1,2x_i'y_i')$$

is a solution to $x^2-Dy^2=1$.

Since

$$\sqrt{\frac{2(y_i')^2+1+1}{2D}}=\sqrt{\frac{y_i'^2+1}{D}}=\sqrt{\frac{Dx_i'^2}{D}}=x_i',\sqrt{\frac{u-1}{2}}=\sqrt{\frac{2y_i'^2}{2}}=y_i',$$

holds for every (x_i',y_i') belonging to N_D, there is an inverse image belonging to P_D.

Therefore, g is a surjection.

To conclude, g is a one-to-one mapping.

4. Related work and experiments

[3][4][5] proved that the following negative Pell equations are solvable:

(4.1) $x^2-5(5n\pm2)y^2=-1(n\equiv-1(\mathrm{mod}\,4))$, where $5n\pm2$ is a prime number;

(4.2) $x^2-5py^2=-1$, where p is a Fermat prime and $p\neq3,5$;

(4.3) $x^2-p(pn\pm2)y^2=-1$, where $n\equiv-1(\mathrm{mod}\,4)$ is a prime, $p\equiv-3(\mathrm{mod}\,8)$ is a prime.

Actually, the solvability of these three negative Pell equations are straightforward from theorem 3, because the given D in the three papers follows from theorem 3. The proofs are shown below.

For $x^2-5(5n\pm2)y^2=-1(n\equiv-1(\mathrm{mod}\,4))$, where $5n\pm2$ is a prime number, since $n\equiv-1(\mathrm{mod}\,4)$, we obtain $5n\pm2\equiv n\pm2\equiv1(\mathrm{mod}\,4)$. Since $5n\pm2$ is a prime number, $5n\pm2$ belongs to Y_s. Because 5 belongs to Y_s, substitute p into 5, q into $5n\pm2$, we obtain

$$\left(\frac{p}{q}\right)=\left(\frac{5}{5n\pm2}\right)=\left(\frac{5n\pm2}{5}\right)=\left(\frac{\pm2}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

Applying theorem 3(ii), the above negative Pell equation (4.1) is solvable.

For $x^2-5py^2=-1$, where p is a Fermat prime and $p\neq3,5$. Denote $2^{2^n}+1$ by p. Because $p\neq3,5$, $n\geq2$. Therefore, $p=2^{2^n}+1\equiv1(\mathrm{mod}\,4)$, namely, p belongs to Y_s. Also,

$$p=2^{2^n}+1=4^{2^{n-1}}+1\equiv(-1)^{2^{n-1}}+1\equiv2(\mathrm{mod}\,5).$$

Hence,

$$\left(\frac{p}{q}\right)=\left(\frac{2^{2^n}+1}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

Applying theorem3(iii), the above negative Pell equation(4.2)is solvable.

For $x^2 - p(pn \pm 2)y^2 = -1$, where $n \equiv -1(\bmod 4)$ is a prime, $p \equiv -3(\bmod 8)$ is a prime. Denote $pn \pm 2$ by q, because $n \equiv -1(\bmod 4)$, $p \equiv -3(\bmod 8)$, we obtain

$$q = pn \pm 2 \equiv (-3)(-1) \pm 2 \equiv 1(\bmod 4).$$

Implying q belongs to Y_s.

Therefore,

$$\left(\frac{q}{p}\right) = \left(\frac{pn \pm 2}{p}\right) = \left(\frac{\pm 2}{p}\right) = \left(\frac{2}{p}\right).$$

Since $p \equiv -3(\bmod 8)$, we obtain

$$\left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Applying theorem 3(iv), the above negative Pell equation (4.3) is solvable.

[9] discussed the solvability of

$$x^2 - (4n+2)y^2 = -1.$$

Actually, the theorems in the paper are straightforward from Theorem 1, Theorem 3 etc.

For $x^2 - (4n+2)y^2 = -1$ in paper [9], the theorem 1 of the paper showed that when n is an odd number and $2n+1$ is a prime, the above negative Pell equation is unsolvable.

Here, $D = 2(2n+1)$ and $2n+1 \equiv 3(\bmod 4)$. Applying theorem1, the above negative Pell equation is unsolvable.

In [12], the theorem revealed that D is solvable if and only if it's the sum of two squares. However, applying Fermat's theorem on sums of two squares, we obtain that the above condition is equivalent to,

$$D \in Y \text{ or } D \in U.$$

When using the continued fraction expansion to calculate the parity of the period, we cannot reduce the power of the prime factors of D to a smaller one, because it may change the parity of its continued fraction expansion, which will affect the solvability. However, our method can reduce the power of each prime factor to 1 or 2. This means that the result can be generalized.

The prime numbers which congruent to 1 modulo4 and smaller than 100 are listed below

5,13,17,29,37,41,53,61,73,89,97

The values of Legendre symbols for all possible pairing of these numbers are listed below.

$\left(\frac{p}{q}\right)$ p q	5	13	17	29	37	41	53	61	73	89	97
5	0										
13	-1	0									
17	-1	1	0								
29	1	1	-1	0							
37	-1	-1	-1	-1	0						
41	1	-1	-1	-1	1	0					
53	-1	1	1	1	1	-1	0				
61	1	1	-1	-1	-1	1	-1	0			
73	-1	-1	-1	-1	1	1	-1	1	0		
89	1	-1	1	-1	-1	-1	1	-1	1	0	
97	-1	-1	-1	-1	-1	-1	1	1	1	1	0

Table 2. the values of Legendre symbols

Here are all the Ds by (iii) of theorem 3 which have two distinct prime factors and both prime factor congruent to 1 modulo 4.(and smaller than 100)

There is at least one odd positive integer in a and b.

$5^a\cdot 13^b$	$5^a\cdot 17^b$	$5^a\cdot 37^b$
$5^a\cdot 53^b$	$5^a\cdot 73^b$	$5^a\cdot 97^b$
$13^a\cdot 37^b$	$13^a\cdot 41^b$	$13^a\cdot 73^b$
$13^a\cdot 89^b$	$13^a\cdot 97^b$	$17^a\cdot 29^b$
$17^a\cdot 37^b$	$17^a\cdot 41^b$	$17^a\cdot 61^b$
$17^a\cdot 73^b$	$17^a\cdot 97^b$	$29^a\cdot 37^b$
$29^a\cdot 41^b$	$29^a\cdot 61^b$	$29^a\cdot 73^b$
$29^a\cdot 89^b$	$29^a\cdot 97^b$	$37^a\cdot 61^b$
$37^a\cdot 89^b$	$37^a\cdot 97^b$	$41^a\cdot 53^b$
$41^a\cdot 89^b$	$41^a\cdot 97^b$	$53^a\cdot 61^b$
$53^a\cdot 73^b$	$53^a\cdot 97^b$	$61^a\cdot 89^b$

Table 3. all the Ds by (iii) of theorem 3 which have two distinct prime factors and both prime factor congruent to 1 modulo 4.(and smaller than 100)

Here are all the Ds by (iv) of theorem3 which have two distinct prime factors where one of the factor is 2 and another prime number congruent to 1 modulo 4 (and smaller than 250).

Here, a is a positive integer.

$2\cdot 5^a$	$2\cdot 13^a$	$2\cdot 29^a$
$2\cdot 37^a$	$2\cdot 53^a$	$2\cdot 61^a$
$2\cdot 101^a$	$2\cdot 109^a$	$2\cdot 149^a$
$2\cdot 157^a$	$2\cdot 173^a$	$2\cdot 181^a$
$2\cdot 197^a$	$2\cdot 229^a$	

Table 4. all the Ds by (iv) of theorem3 which have two distinct prime factors where one of the factor is 2 and another prime number congruent to 1 modulo 4 (and smaller than 250)

Here are some Ds by theorem 4 with more than two distinct prime factors where the prime factors of these Ds congruent to 1 modulo 4.

Here, a is an odd positive integer.

$5^a\cdot 13^b\cdot 17^c$	$5^a\cdot 13^b\cdot 37^c$	$5^a\cdot 13^b\cdot 53^c$
$5^a\cdot 13^b\cdot 73^c$	$5^a\cdot 13^b\cdot 97^c$	$5^a\cdot 17^b\cdot 37^c$
$5^a\cdot 17^b\cdot 53^c$	$5^a\cdot 17^b\cdot 73^c$	$5^a\cdot 17^b\cdot 97^c$
$13^a\cdot 37^b\cdot 41^c$	$13^a\cdot 37^b\cdot 73^c$	$13^a\cdot 37^b\cdot 89^c$
$5^a\cdot 13^b\cdot 17^c\cdot 37^d$	$5^a\cdot 13^b\cdot 17^c\cdot 53^d$	$5^a\cdot 13^b\cdot 17^c\cdot 73^d$
$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 53^e$	$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 73^e$	$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 97^e$
$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 53^e\cdot 73^f$	$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 53^e\cdot 97^f$	$5^a\cdot 13^b\cdot 17^c\cdot 37^d\cdot 73^e\cdot 97^f$
$5^a 13^b 17^c 37^d 53^e 73^f 97^g$	$17^a 29^b 37^c 41^d 61^e 73^f 89^g$	$17^a 29^b 37^c 41^d 61^e 73^f 89^g 97^f$

Table 5. ***D***s by theorem 4 with more than two distinct prime factors where the prime factors of these Ds congruent to 1 modulo 4.

All the numbers in the above 4 tables are D s for which $Dx^2 - y^2 = 1$ is solvable.

5. Conclusion

In section 3.1, by observing the residue of D, we give a necessary condition for $Dx^2 - y^2 = 1$ to be solvable.

Therefore, in section 3.2 we aim to find the prime factorization of D. Probing deeper, we continued our research and proved theorem 3 and theorem 5. In the procedure, we used lemma 5 to sort out the finite cases, and then we used the properties of quadratic residue to eliminate all the cases except two cases. Moreover, we used the minimality of the solutions (x_0, y_0) to the positive Pell equation to eliminate one of two cases remaining. Finally, we construct the solution to the negative Pell equation in the last remaining case.

In section 3.3, we firstly show that for a given solution (x, y) to negative Pell equation, we can find a D for which $Dx^2 - y^2 = 1$ is solvable. Therefore, by going through all solutions (x, y) to $Dx^2 - y^2 = 1$, we can obtain every D that for which $Dx^2 - y^2 = 1$ is solvable. First, with the property of quadratic residue, we obtain x is an odd number without the prime factors congruent to 3 modulo 4; secondly, when $x = 1$, we obtain $D = k^2 + 1$; thirdly, we can use the quadratic congruence equation to find the least positive integer y for every given x such that (x, y) satisfy $Dx^2 - y^2 = 1$; finally, we determine all possible D for which $Dx^2 - y^2 = 1$ is solvable.

When $D \in Y$, we have the least positive solution (x_0, y_0) to $x^2 - Dy^2 = 1$, namely

$$x_0^2 - Dy_0^2 = 1. \tag{5.1}$$

Assuming p is a prime factor of D, taking (5.1) modulo p, gives

$$x_0^2 \equiv 1 \pmod{p}.$$

Namely,

$$p \mid x_0 + 1 \quad \text{or} \quad p \mid x_0 - 1.$$

By lemma 2, we obtain a residue property for every solution to $x^2 - Dy^2 = 1$. This leads to contradiction when $p \mid x_0 - 1$. Therefore, we obtain Theorem 7.

In theorem 8, *we build a one-to-one mapping from a subset of the set of solutions of positive Pell equation to the set of solutions of negative Pell equation.*

6. Future work

When $D \in U$, the solvability of $Dx^2 - y^2 = 1$ is not completely work out. However, we've got results. Such as, theorem3 indicate that, when $D \in U$, if $D = 2p^a, p \in Y_s, a \in \mathbb{N}$, then $D = 2p^a, p \in Y_s, a \in \mathbb{N}$ is solvable.

On the basis of these results, we hope to find a concise theorem to determine the solvability of $Dx^2 - y^2 = 1$, which is a sufficient and necessary condition for $Dx^2 - y^2 = 1$ to be solvable.

Because the solvability of $Dx^2 - y^2 = 1$ can be used to determine the parity of the continued fraction expansion cycle of $\sqrt{D}$ type, we plan to find out a method to determine the parity of the period of the continued fraction expansion for the positive integer D's n times square root.

Also, we plan to write a program of W.C.J algorithm to determine the solvability of negative Pell equation automatically.

Acknowledgement

We thanks toour tutor Mr.Jia for the fully support and help. He’s been accompanied with us during this struggling time all along. Thanks to Professor Yang Jing and Mr. Irvingfor their advice to us in completingthepaper. Thanks to Mr. Qu for his advice. Thanks to our friend Liu Ziyuan for his code. Most importantly, thanks to Cai Lide’s parents and Wang Jiaqi’s parents for their support. They could stand for their children all day long.

Reference

[1] A. Grytczuk, F. Luca, M. W ́ojtowicz, *The negative Pell equation and Pythagorean triples*, Proc. Japan Acad., Volume 76 (2000) 91–94.

[2] C.Pan, C.Pan, *elementary number theory(Beijing, Peking University Public)*2003. (in Chinese)

[3] X. Du, *about Pell equation* $x^2-5(5n+2)y^2=-1(n\equiv-1 \pmod 4)$ Journal of hunan university for nationalities(Natural Science edition)Jun. 2012. 179-181

[4] X. Du, *about Pell equation* $x^2-p(pn\pm2)y^2=-1(p\equiv-3 \pmod 8)$,Journal of southwest university for nationalities(Natural Science edition),2012. 181-182.

[5] X. Du, Determination on solutions in $x^2-(4n+2)y^2=-1$,Journal of Shenyang university,2012. 55-57.

[6] D. Pumplun, *Über die Klassenzahl und die Grundeinheit des reelquadratischen Zahlkorper*, J. Reine Angew. Math. 230 (1968), 167-210.

[7] Edward Everett Whitford, *the Pell equation*, 1912, 71.

[8] F. Tano, *Sur quelques theorems de Dirichlet*, J. Reine Angew. Math. 105 (1889), 160-169.

[9] X. Guan, *about Pell equation* $x^2-5py^2=-1$,Journal of southwest university for nationalities(Natural Science edition)2010. 32-33

[10] H. W. Lenstra Jr. *Solving the Pell Equation*, NOTICES OF THE AMS VOLUME 49, NUMBER 2. 2002 182-192

[11] J.C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $Dx^2-y^2=1$, Trans. Amer. Math. Soc. 260 (1980), 485–508.

[12] K. Hardy, K.S.Williams, *on the solvability of the Diophantine equation* $dV^2-2eVW-dW^2=1$, PACIFIC JOURNAL OF MATHEMATICS Vol. 124, No. 1,1986. 145-157

[13] P. G. L. Dirichlet, *Einige neue S ätze über unbestimmte Gleichungen.* Gesammelte Werke, Chelsea, New York, 219–236.

[14] P. Kaplan, *Sur le 2-groupe des classes d'id éaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), 313-363.

[15] *Testing the solubility of the negative Pell equation*, http://www.numbertheory.org/php/hardy_williams.html, 2013.