Pell's Equation and Diophantine Approximation

Yunseo Choi, Aneesha Manne, Poonam Sahoo

December 10, 2019

MIT Primes Program

Table of Contents

Introduction

The Pell's Equation

Definition of Pell's Equation

The Pell equation is the equation of the form $x^2 - Dy^2 = 1$ for positive integer pairs (x, y) and positive integers D.

The Pell's Equation

Definition of Pell's Equation

The Pell equation is the equation of the form $x^2 - Dy^2 = 1$ for positive integer pairs (x, y) and positive integers D.

Sidenote

We will refer to D as a positive integer that is not a square of an integer.

- If D is a square number, the equation has no solutions except $(x, y) = (\pm 1, 0)$

History

Brief History

- The equation was studied extensively by Joseph-Louis Lagrange and John Wallis in the 1700s.
- However, it was named Pell's equation after John Pell because Euler miscredited who discovered them first.

Natural Questions

Natural Questions

1. Is it always possible to find a solution (x, y) given any D?
2. If so, how can we describe all such solutions?
3. What if the right hand side is -1 instead of 1?
4. Given D, how do we obtain a solution such that $x^2 - Dy^2 = 1$?

Theorem 1

Theorem 1

There always exists a pair of integers (x, y) such that $x^2 - Dy^2 = 1$.

Theorem 2

When (x_1, y_1) are the positive integer solutions with smallest x_1 such that $x^2 - Dy^2 = 1$, every subsequent solutions (x_k, y_k) can be obtained through

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k.$$

Theorem 3

Theorem 3

For a given D, there does not always exist a pair of integers (x, y) such that $x^2 - Dy^2 = -1$.

Theorem 4

Theorem 4

When the continued fraction $\sqrt{D} = [a_1, \overline{a_2, a_3, ..., a_{n-1}, a_n}]$, let p and q be co-prime integers such that $\frac{p}{q} = [a_1, a_2, a_3, ...a_{n-1}]$. Then, an integer solution (x, y) to Pell's equation $x^2 - Dy^2 = 1$ is given by

$$(x, y) = (p, q) \text{ when } n \text{ is odd}$$

$$(x, y) = (p^2 + q^2 D, 2pq) \text{ when } n \text{ is even.}$$

Nuts and Bolts

Auxiliary Lemma 1

Note

$x^2 - Dy^2 = (x - y\sqrt{D})(x + y\sqrt{D})$

Auxiliary Lemma 1

Note

$x^2 - Dy^2 = (x - y\sqrt{D})(x + y\sqrt{D})$

Lemma 1

For m that is a given positive number and a fixed D, there exists a pair of integers (x, y) such that $0 < y \leq m$, and

$$| x - y\sqrt{D} | < \frac{1}{m}.$$

Proof Sketch of Lemma 1

Set up

- We will be proving this by contradiction and using pigeon-hole principle
- Set the pigeons as the solutions $(x_k, y_k) = (\lceil k\sqrt{D}\rceil, k)$
- Set the holes as the intervals the solutions fall into

Proof Sketch of Lemma 1

Set up

- We will be proving this by contradiction and using pigeon-hole principle
- Set the pigeons as the solutions $(x_k, y_k) = (\lceil k\sqrt{D}\rceil, k)$
- Set the holes as the intervals the solutions fall into

Concluding Step

Since there are m pairs of (x_k, y_k) but only $m - 1$ intervals, there is an interval that contains two pairs.

Auxiliary Lemma 2

Lemma 2

For any given D, there are infinitely many pairs of positive integers (x, y) such that

$$| x - y\sqrt{D} | < \frac{1}{y}.$$

Proof of Lemma 2

Set Up

- Select arbitrary positive integer m to be m_1
- There exists some integer pair (x_1, y_1) such that $\mid x_1 - y_1\sqrt{D} \mid < \frac{1}{m}$ (lemma 1)

Proof of Lemma 2

Set Up

- Select arbitrary positive integer m to be m_1
- There exists some integer pair (x_1, y_1) such that $\mid x_1 - y_1\sqrt{D} \mid < \frac{1}{m}$ (lemma 1)

Next Steps

- $\mid x - y\sqrt{D} \mid < \frac{1}{m} \neq 0$ because $\sqrt{D}$ is an irrational number
- There exists m_2 such that $\mid x_1 - y_1\sqrt{D} \mid > \frac{1}{m_2}$
- Repeat the same process with m_2 instead of m_1
- There are infinite pairs of (x, y) such that $\mid x - y\sqrt{D} \mid < \frac{1}{y}$

Auxiliary Lemma 3

Lemma 3

For any given D, there exists infinite number of pairs of positive integers (x, y) such that

$$\mid x^2 - Dy^2 \mid < 3\sqrt{D}.$$

Proof of Lemma 3

Set Up

- $x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y)$
- There are infinitely many pairs of integers (x, y) such that $\mid x - y\sqrt{D} \mid < \frac{1}{y}$ (Lemma 2)

Proof of Lemma 3

Set Up

- $x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y)$
- There are infinitely many pairs of integers (x, y) such that $| x - y\sqrt{D} |< \frac{1}{y}$ (Lemma 2)

Next Steps

- For pairs (x, y), $(x + \sqrt{D}y)(x - \sqrt{D}y) < \frac{x+\sqrt{D}y}{y} = \frac{x}{y} + \sqrt{D}$.
- $x < y\sqrt{D} + 1$ since $| x - y\sqrt{D} |< \frac{1}{y} \leq 1$
- Simplify to $\frac{x}{y} < \sqrt{D} + \frac{1}{y} < \sqrt{D} + \sqrt{D}$
- $x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y) < 3\sqrt{D}$

Auxiliary Lemma 4

Lemma 4

For some non-negative integer k, there exists infinitely many pairs of positive integer pairs (x, y) such that

$$x^2 - Dy^2 = k.$$

Proof of Lemma 4

Set Up

There exists infinite number of pairs of positive integers (x, y) such that $\mid x^2 - Dy^2 \mid < 3\sqrt{D}$ (Lemma 3)

Proof of Lemma 4

Set Up

There exists infinite number of pairs of positive integers (x, y) such that $\mid x^2 - Dy^2 \mid < 3\sqrt{D}$ (Lemma 3)

Next Steps

- Only a finite number of integers whose absolute value is less than $3\sqrt{D}$
- Some integer in this interval, k, should have infinite number of integers that satisfy $x^2 - Dy^2 = k$.

Introduction to Auxiliary Lemmas for Theorem 4

- First we will introduce continued fractions
- Then we will prove lemmas that lead up to Theorem 4:

- First we will introduce continued fractions
- Then we will prove lemmas that lead up to Theorem 4:

Theorem 4

When the continued fraction $\sqrt{D} = [a_1, \overline{a_2, a_3, ..., a_{n-1}, a_n}]$, let p and q be co-prime integers such that $\frac{p}{q} = [a_1, a_2, a_3, ...a_{n-1}]$. Then, an integer solution (x, y) to Pell's equation $x^2 - Dy^2 = 1$ is given by

$$(x, y) = (p, q) \text{ when } n \text{ is odd}$$

$$(x, y) = (p^2 + q^2D, 2pq) \text{ when } n \text{ is even.}$$

What is a Continued Fraction?

Definition

A **continued fraction** for a real number x is formed by

$$x_1 = x, a_n = \lfloor x_n \rfloor, x_{n+1} = \frac{1}{x_n - a_n}$$

for $n \in \mathbb{N}$. Following the conventional notation, we write $x = [a_1, a_2, ...]$.

Continued Fractions

Example

Construct the continued fraction for $\sqrt{2}$.

Continued Fractions

Example

Construct the continued fraction for $\sqrt{2}$.

First Term

$1 < \sqrt{2} < 2$, so taking the floor, $a_1 = 1$

Example

Construct the continued fraction for $\sqrt{2}$.

First Term

$1 < \sqrt{2} < 2$, so taking the floor, $a_1 = 1$

Recursion

- $x_2 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$, so $a_2 = 2$.
- Also, $x_3 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$
- Then $x_i = \sqrt{2}+1$ for $i > 1$, so $\sqrt{2} = [1, 2, 2, ., , ,] = [1, \overline{2}]$

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\dots}}}}$$

Proof Sketch of Lemma 5

Lemma 5

The continued fraction expansion of a real number x is periodic if and only if x is quadratic irrational.

Proof Sketch of Lemma 5

Lemma 5

The continued fraction expansion of a real number x is periodic if and only if x is quadratic irrational.

Definition

A real number is **quadratic irrational** if it is the solution to some integer-coefficient quadratic equation, i.e., the number can be expressed as $\frac{P \pm \sqrt{D}}{Q}$ for some integers P, Q and positive integer D.

Proof Sketch of Lemma 5

Lemma 5

The continued fraction expansion of a real number x is periodic if and only if x is quadratic irrational.

Forward Direction

- Must show that real number $A = [a_1, ..a_\ell, \overline{b_1, ..., b_n}]$ can be expressed as

$$A = \frac{P \pm \sqrt{D}}{Q}$$

- Let $B = [\overline{b_1, b_2, ..., b_n}]$

Proof Sketch of Lemma 5

Deal with B

- $$B = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \ldots + \cfrac{1}{b_n + \cfrac{1}{B}}}}$$
- Then $B = \frac{uB+v}{wB+z}$ for u, v, w, z integers
- Cross multiply, solve for B using quadratic formula
- $B = \frac{i+j\sqrt{D}}{k}$ quadratic irrational

Proof Sketch of Lemma 5

Deal with B

- $$B = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \ldots + \cfrac{1}{b_n + \frac{1}{B}}}}$$
- Then $B = \frac{uB+v}{wB+z}$ for u, v, w, z integers
- Cross multiply, solve for B using quadratic formula
- $B = \frac{i+j\sqrt{D}}{k}$ quadratic irrational

Substitution

$$A = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_\ell + \cfrac{1}{\frac{i+j\sqrt{D}}{k}}}}$$

$$A = \frac{e + f\sqrt{D}}{g + h\sqrt{D}} \text{ for } e, f, g, h \text{ integers}$$

Rationalizing, $A = \frac{r+s\sqrt{D}}{t}$ for integers r, s, t as desired

Proof Sketch of Lemma 5

Reverse Direction

- Must show only finitely many x_i given x_1
- Let $x_1 = \frac{P+\sqrt{D}}{Q}$
- Suffices to show that such x_i are periodic
- The following lemma completes proof

Proof Sketch of Lemma 6

Lemma 6

A reduced quadratic irrational number is purely periodic.

Additional Definitions

Definition

A continued fraction is **purely periodic** if $x = [\overline{a_1, a_2, ..a_n}]$ for some n.

Additional Definitions

Definition

A continued fraction is **purely periodic** if $x = [\overline{a_1, a_2, ..a_n}]$ for some n.

Definition

A quadratic irrational number is **reduced** if it is greater than 1 and its conjugate is between 0 and -1.

Additional Definitions

Definition

A continued fraction is **purely periodic** if $x = [\overline{a_1, a_2, ..a_n}]$ for some n.

Definition

A quadratic irrational number is **reduced** if it is greater than 1 and its conjugate is between 0 and -1.

Note

- every irrational quadratic number can be reduced by adding or subtracting an integer
- suffices to prove for reduced quadratic irrationals

Proof Sketch of Lemma 6

Lemma 6

A reduced quadratic irrational number is purely periodic.

Set Up

- $x_1 = x = \frac{P+\sqrt{D}}{Q}$ reduced quadratic irrational, $x' = \frac{P-\sqrt{D}}{Q}$ conjugate
- From definitions, bound $P + \sqrt{D}$

$$x = \frac{P+\sqrt{D}}{Q} > 1, \text{ so } Q < P + \sqrt{D} < 2\sqrt{D}$$

- Only finitely many (P, Q) such that $\frac{P+\sqrt{D}}{Q}$ reduced quadratic irrational

Proof Sketch of Lemma 6

Recursive Step

- Use recursive formula, plug in $x_1 = \frac{P+\sqrt{D}}{Q}$,

$$x_2 = \frac{P_1 + \sqrt{D}}{Q_1}$$

- Using $x' = a_1 + \frac{1}{x_2'}$, show x_2 reduced quadratic irrational, holds for all x_i

Proof Sketch of Lemma 6

Recursive Step

- Use recursive formula, plug in $x_1 = \frac{P+\sqrt{D}}{Q}$,

$$x_2 = \frac{P_1 + \sqrt{D}}{Q_1}$$

- Using $x' = a_1 + \frac{1}{x_2'}$, show x_2 reduced quadratic irrational, holds for all x_i

Periodic

- Finitely many (P, Q) such that $\frac{P+\sqrt{D}}{Q}$ reduced quadratic irrational
- $x_i = x_j$ for some $i \neq j$
- By recursion, $x_1 = x_{j-i+1}$, $x_2 = x_{i+j+2}$, ... $x_i = x_j$, $x_{i+1} = x_{j+1}$, $x_{i+2} = x_{i+3}$, ...
- Sequence periodic with first term x_1, thus continued fraction x purely periodic

Corollary of Lemma 6

Corollary 1

For some sequence of integers a_i, $\sqrt{D} = [a_1, \overline{a_2, a_3, ..a_n}]$.

Corollary of Lemma 6

Corollary 1

For some sequence of integers a_i, $\sqrt{D} = [a_1, \overline{a_2, a_3, ..a_n}]$.

Proof

- $\sqrt{D}$ quadratic irrational, solution to $x^2 - D = 0$
- $\sqrt{D} + \left\lfloor \sqrt{D} \right\rfloor$ purely periodic
- Thus $\sqrt{D}$ periodic from second term from Lemma 6

Recursive Sequence

Definition

We define a recursive sequence p_n and q_n for continued fraction $[a_1, a_2, ..., a_n]$. Note that a_i here are not specific numbers, but variables.

$$\frac{p_n}{q_n} = [a_1, ...a_n].$$

Recursive Sequence

Definition

We define a recursive sequence p_n and q_n for continued fraction $[a_1, a_2, ..., a_n]$. Note that a_i here are not specific numbers, but variables.

$$\frac{p_n}{q_n} = [a_1, ...a_n].$$

Example

We list the first two terms of p_i and q_i. $p_1 = a_1$, $p_2 = a_1a_2 + 1$. $q_1 = 1, q_2 = a_2$.

Auxiliary Lemmas

Lemma 7

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ..a_n}]$ and p_n and q_n as defined above. Then,

1. For $n \geq 2$, $p_n = a_n p_{n-1} + p_{n-2}$.
2. For $n \geq 2$, $q_n = a_n q_{n-1} + q_{n-2}$.
3. For $n \geq 1$, $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$.
4. For $n \geq 2$, $x = \frac{x_{n+1} P_n + P_{n-1}}{x_{n+1} Q_n + Q_{n-1}}$.

Auxiliary Lemmas

Lemma 7

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ..a_n}]$ and p_n and q_n as defined above. Then,

1. For $n \geq 2$, $p_n = a_n p_{n-1} + p_{n-2}$.
2. For $n \geq 2$, $q_n = a_n q_{n-1} + q_{n-2}$.
3. For $n \geq 1$, $p_{n-1} q_n - p_n q_{n-1} = (-1)^n$.
4. For $n \geq 2$, $x = \frac{x_{n+1} P_n + P_{n-1}}{x_{n+1} Q_n + Q_{n-1}}$.

- Use induction to verify
- Important for the following lemma

Proof Sketch of Lemma 8

Lemma 8

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ...a_n}]$ and let $\frac{p}{q} = [a_1, ..a_{n-1}]$. Then, (p, q) is a solution to the equation $x^2 - Dy^2 = (-1)^{n-1}$.

Proof Sketch of Lemma 8

Lemma 8

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ...a_n}]$ and let $\frac{p}{q} = [a_1, ..a_{n-1}]$. Then, (p, q) is a solution to the equation $x^2 - Dy^2 = (-1)^{n-1}$.

From Lemma 7 #4

$$\sqrt{D} = \frac{x_{n+1}P_n + P_{n-1}}{x_{n+1}Q_n + Q_{n-1}}$$

Proof Sketch of Lemma 8

Lemma 8

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ...a_n}]$ and let $\frac{p}{q} = [a_1, ..a_{n-1}]$. Then, (p, q) is a solution to the equation $x^2 - Dy^2 = (-1)^{n-1}$.

From Lemma 7 #4

$$\sqrt{D} = \frac{x_{n+1}P_n + P_{n-1}}{x_{n+1}Q_n + Q_{n-1}}$$

Substitution

Substitute $x_{n+1} = \sqrt{D} + \left\lfloor \sqrt{D} \right\rfloor$, get

$$\sqrt{D}(\sqrt{D} + \left\lfloor \sqrt{D} \right\rfloor)Q_n + \sqrt{D}Q_{n-1} = (\sqrt{D} + \left\lfloor \sqrt{D} \right\rfloor)P_n + P_{n-1}$$

Proof Sketch of Lemma 8

Since $\sqrt{D}$ is Irrational

$$P_{n-1} = DQ_n - \left\lfloor \sqrt{D} \right\rfloor P_n$$

$$Q_{n-1} = P_n - \left\lfloor \sqrt{D} \right\rfloor Q_n$$

Proof Sketch of Lemma 8

Since $\sqrt{D}$ is Irrational

$$P_{n-1} = DQ_n - \left\lfloor \sqrt{D} \right\rfloor P_n$$

$$Q_{n-1} = P_n - \left\lfloor \sqrt{D} \right\rfloor Q_n$$

From Lemma 7 #3

- $P_n(P_n - \left\lfloor \sqrt{D} \right\rfloor Q_n) - Q_n(DQ_n - \left\lfloor \sqrt{D} \right\rfloor P_n) = (-1)^{n-1}$
- Simplifies to $(P_n)^2 - D(Q_n)^2 = (-1)^{n-1}$
- So $p^2 - Dq^2 = (-1)^{n-1}$ as desired

Proofs

Proof of Theorem 1

Proof of Theorem 1

Theorem 1

There always exists a pair of integers (x, y) such that $x^2 - Dy^2 = 1$.

Proof of Theorem 1

Theorem 1

There always exists a pair of integers (x, y) such that $x^2 - Dy^2 = 1$.

Lemma 8

For some non-negative integer k, there exists infinitely many pairs of positive integer pairs (x, y) such that

$$x^2 - Dy^2 = k.$$

Proof of Theorem 1

Theorem 1

There always exists a pair of integers (x, y) such that $x^2 - Dy^2 = 1$.

Lemma 8

For some non-negative integer k, there exists infinitely many pairs of positive integer pairs (x, y) such that

$$x^2 - Dy^2 = k.$$

From Lemma 8

For some i and j, there is an infinite number of solutions (x, y) such that $x^2 - Dy^2 = k$ while $x \equiv i \pmod{k}$, and $y \equiv j \pmod{k}$.

Set up

Let (x_1, y_1) and (x_2, y_2) be such solutions.

- $x_1^2 - Dy_1^2 = k$, $x_2^2 - Dy_2^2 = k$,
- $x_1 \equiv x_2 \pmod{k}$,
- $y_1 \equiv y_2 \pmod{k}$.

Division

$$\frac{x_1^2 - Dy_1^2}{x_2^2 - Dy_2^2} = \frac{(x_1 + \sqrt{D}y_1)(x_1 - \sqrt{D}y_1)}{(x_2 + \sqrt{D}y_2)(x_2 - \sqrt{D}y_2)} = 1.$$

Simplification

$$\begin{aligned}
\frac{x_1 \pm \sqrt{D}y_1}{x_2 \pm \sqrt{D}y_2} &= \frac{(x_1 \pm \sqrt{D}y_1)(x_2 \mp \sqrt{D}y_2)}{(x_2 \pm \sqrt{D}y_2)(x_2 \mp \sqrt{D}y_2)} \\
&= \frac{(x_1x_2 - Dy_1y_2) \pm (x_2y_1 - x_1y_2)\sqrt{D}}{x_2^2 - Dy_2^2} \\
&= \frac{(x_1x_2 - Dy_1y_2) \pm (x_2y_1 - x_1y_2)\sqrt{D}}{k}.
\end{aligned}$$

Proof of Theorem 1

Simplification

$$\begin{aligned}\frac{x_1 \pm \sqrt{D}y_1}{x_2 \pm \sqrt{D}y_2} &= \frac{(x_1 \pm \sqrt{D}y_1)(x_2 \mp \sqrt{D}y_2)}{(x_2 \pm \sqrt{D}y_2)(x_2 \mp \sqrt{D}y_2)} \\ &= \frac{(x_1x_2 - Dy_1y_2) \pm (x_2y_1 - x_1y_2)\sqrt{D}}{x_2^2 - Dy_2^2} \\ &= \frac{(x_1x_2 - Dy_1y_2) \pm (x_2y_1 - x_1y_2)\sqrt{D}}{k}.\end{aligned}$$

Solution to $x^2 - Dy^2 = 1$

$$(x, y) = (\frac{x_1x_2 - Dy_1y_2}{k}, \frac{x_2y_1 - x_1y_2}{k})$$

Proof of Theorem 1

Integers?

$y = \frac{x_2 y_1 - x_1 y_2}{k}$.

Proof of Theorem 1

Integers?

$y = \frac{x_2 y_1 - x_1 y_2}{k}$.

$x_1 \equiv x_2 \pmod{k}$, $y_1 \equiv y_2 \pmod{k}$. So, $x_2 y_1 \equiv x_1 y_2 \pmod{k}$.

Therefore, y and thus x are integers.

Proof of Theorem 2

Theorem 2

When (x_1, y_1) are the positive integer solutions with smallest x_1 such that $x^2 - Dy^2 = 1$, every subsequent solutions (x_k, y_k) can be obtained through

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k.$$

Proof of Theorem 2

Theorem 2

When (x_1, y_1) are the positive integer solutions with smallest x_1 such that $x^2 - Dy^2 = 1$, every subsequent solutions (x_k, y_k) can be obtained through

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k.$$

Part 1

(x_k, y_k) are solutions to $x^2 - Dy^2 = 1$.

Proof of Theorem 2

Theorem 2

When (x_1, y_1) are the positive integer solutions with smallest x_1 such that $x^2 - Dy^2 = 1$, every subsequent solutions (x_k, y_k) can be obtained through

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k.$$

Part 1

(x_k, y_k) are solutions to $x^2 - Dy^2 = 1$.

Part 2

(x_k, y_k) are **all** the solutions to $x^2 - Dy^2 = 1$.

Proof of Theorem 2

Part 1 - Base Case

(x_1, y_1) are solutions to $x^2 - Dy^2 = 1$ by set-up.

Proof of Theorem 2

Part 1 - Base Case

(x_1, y_1) are solutions to $x^2 - Dy^2 = 1$ by set-up.

Part 1 - Inductive Step: k to $k+1$

$(x_k + y_k\sqrt{D})(x_1 + y_1\sqrt{D}) = (x_1x_k + Dy_1y_k) + (x_1y_k + x_ky_1)\sqrt{D} = x_{k+1} + y_{k+1}\sqrt{D}$.

Proof of Theorem 2

Part 1 - Base Case

(x_1, y_1) are solutions to $x^2 - Dy^2 = 1$ by set-up.

Part 1 - Inductive Step: k to $k+1$

$(x_k + y_k\sqrt{D})(x_1 + y_1\sqrt{D}) = (x_1x_k + Dy_1y_k) + (x_1y_k + x_ky_1)\sqrt{D} = x_{k+1} + y_{k+1}\sqrt{D}$.

$$(x_{k+1}, y_{k+1}) = (x_1x_k + Dy_1y_k, x_1y_k + x_ky_1)$$

Proof of Theorem 2

Part 1- Inductive Step: k to $k+1$

$$\begin{aligned}
1 &= (x_1^2 - Dy_1^2)(x_k^2 - Dy_k^2) \\
&= (x_1 + y_1\sqrt{D})(x_k + y_k\sqrt{D})(x_1 - y_1\sqrt{D})(x_k - y_k\sqrt{D}) \\
&= [(x_1x_k + Dy_1y_k) + (x_1y_k + x_ky_1)\sqrt{D}][(x_1x_k + Dy_1y_k) - (x_1y_k + x_ky_1)\sqrt{D}] \\
&= (x_1x_k + Dy_1y_k)^2 - D(x_1y_k + x_ky_1)^2 \\
&= x_{k+1}^2 - Dy_{k+1}^2
\end{aligned}$$

Proof of Theorem 2

Part 2- Assume Contrary

Let (X, Y) be the smallest solution to $X^2 - DY^2 = 1$ that cannot be described as in theorem statement.

Proof of Theorem 2

Part 2- Assume Contrary

Let (X, Y) be the smallest solution to $X^2 - DY^2 = 1$ that cannot be described as in theorem statement.

Part 2- Building down

$$\begin{aligned}1 = (X^2 - DY^2)(x_1 - Dy_1^2) &= (X + Y\sqrt{D})(x_1 - y_1\sqrt{D})(X - Y\sqrt{D})(x_1 + y_1\sqrt{D}) \\ &= [(Xx_1 - Yy_1D) + (Yx_1 - Xy_1)\sqrt{D}][(Xx_1 - Yy_1D) - (Yx_1 - Xy_1)\sqrt{D}] \\ &= (Xx_1 - Yy_1D)^2 - D(Yx_1 - Xy_1)^2.\end{aligned}$$

Proof of Theorem 2

Part 2- Assume Contrary

Let (X, Y) be the smallest solution to $X^2 - DY^2 = 1$ that cannot be described as in theorem statement.

Part 2- Building down

$$\begin{aligned}1 = (X^2 - DY^2)(x_1 - Dy_1^2) = (X + Y\sqrt{D})(x_1 - y_1\sqrt{D})(X - Y\sqrt{D})(x_1 + y_1\sqrt{D})\\ = [(Xx_1 - Yy_1D) + (Yx_1 - Xy_1)\sqrt{D}][(Xx_1 - Yy_1D) - (Yx_1 - Xy_1)\sqrt{D}]\\ = (Xx_1 - Yy_1D)^2 - D(Yx_1 - Xy_1)^2.\end{aligned}$$

So, $(Xx_1 - Yy_1D, Yx_1 - Xy_1)$ are solutions.

Proof of Theorem 2

Part 2- Assume Contrary

Let (X, Y) be the smallest solution to $X^2 - DY^2 = 1$ that cannot be described as in theorem statement.

Part 2- Building down

$$\begin{aligned}1 = (X^2 - DY^2)(x_1 - Dy_1^2) &= (X + Y\sqrt{D})(x_1 - y_1\sqrt{D})(X - Y\sqrt{D})(x_1 + y_1\sqrt{D}) \\ &= [(Xx_1 - Yy_1D) + (Yx_1 - Xy_1)\sqrt{D}][(Xx_1 - Yy_1D) - (Yx_1 - Xy_1)\sqrt{D}] \\ &= (Xx_1 - Yy_1D)^2 - D(Yx_1 - Xy_1)^2.\end{aligned}$$

So, $(Xx_1 - Yy_1D, Yx_1 - Xy_1)$ are solutions.
By assumption, $(Xx_1 - Yy_1D, Yx_1 - Xy_1)$ should be larger than (X, Y).

Proof of Theorem 2

Part 2- Minimality

By minimality assumption, $Xx_1 - Yy_1 \geq X$. So, $\frac{X}{Y} \geq \frac{y_1}{x_1 - 1}$.

Proof of Theorem 2

Part 2- Minimality

By minimality assumption, $Xx_1 - Yy_1 \geq X$. So, $\frac{X}{Y} \geq \frac{y_1}{x_1-1}$.

$X^2 - DY^2 = 1$. So, $\frac{X}{Y} = \sqrt{D + \frac{1}{Y^2}}$.

Proof of Theorem 2

Part 2- Minimality

By minimality assumption, $Xx_1 - Yy_1 \geq X$. So, $\frac{X}{Y} \geq \frac{y_1}{x_1 - 1}$.

$X^2 - DY^2 = 1$. So, $\frac{X}{Y} = \sqrt{D + \frac{1}{Y^2}}$.

As Y increases, $\frac{X}{Y}$ decreases.

Proof of Theorem 2

Part 2- Minimality

By minimality assumption, $Xx_1 - Yy_1 \geq X$. So, $\frac{X}{Y} \geq \frac{y_1}{x_1 - 1}$.
$X^2 - DY^2 = 1$. So, $\frac{X}{Y} = \sqrt{D + \frac{1}{Y^2}}$.
As Y increases, $\frac{X}{Y}$ decreases.
Even when $(x, y) = (x_1, y_1)$, the minimal solution, $\frac{Dy_1}{x_1 - 1} > \frac{x_1}{y_1}$.
Contradiction.

Proof of Theorem 3

Theorem 3

For a given D, there does not always exist a pair of integers (x, y) such that $x^2 - Dy^2 = -1$.

Counterexample

$D = 4$. $x^2 - 4y^2 = -1$. Therefore, $X^2 = 4y^2 - 1$.
$x^2 \equiv 3 \pmod{4}$. Contradiction.

Proof of Theorem 4

Theorem 4

When the continued fraction $\sqrt{D} = [a_1, \overline{a_2, a_3, ..., a_{n-1}, a_n}]$, let p and q be co-prime integers such that $\frac{p}{q} = [a_1, a_2, a_3, ...a_{n-1}]$. Then, an integer solution (x, y) to Pell's equation $x^2 - Dy^2 = 1$ is given by

$$(x, y) = (p, q) \text{ when } n \text{ is odd}$$

$$(x, y) = (p^2 + q^2 D, 2pq) \text{ when } n \text{ is even.}$$

Proof of Theorem 4

Lemma 8

Let $\sqrt{D} = [a_1, \overline{a_2, a_3, ...a_n}]$ and let $\frac{p}{q} = [a_1, ..a_{n-1}]$. Then, (p, q) is a solution to the equation $x^2 - Dy^2 = (-1)^{n-1}$.

Solutions

- $n \equiv 1 \pmod 2$: $p^2 - Dq^2 = 1$.
- $n \equiv 0 \pmod 2$: $p^2 - Dq^2 = -1$. Squaring each side, $(p^2 - Dq^2)^2 = (p^2 + Dq^2)^2 - D(2pq)^2 = 1$.

Summary

Summary

Question

For every D that is not a perfect square, is there always a nontrivial solution?

Summary

Question

For every D that is not a perfect square, is there always a nontrivial solution?

Theorem 1

There always exists a pair of integers (x, y) such that $x^2 - Dy^2 = 1$.

Summary

Question

How do we generate all such solutions?

Summary

Question

How do we generate all such solutions?

Theorem 2

When (x_1, y_1) are the positive integer solutions with smallest x_1 such that $x^2 - Dy^2 = 1$, every subsequent solutions (x_k, y_k) can be obtained through

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k.$$

Summary

Question

What if the right hand side is -1?

Summary

Question

What if the right hand side is -1?

Theorem 3

For a given D, there does not always exist a pair of integers (x, y) such that $x^2 - Dy^2 = -1$.

Summary

Question

How do we find a solution?

Summary

Question

How do we find a solution?

Theorem 4

When the continued fraction $\sqrt{D} = [a_1, \overline{a_2, a_3, ..., a_{n-1}, a_n}]$, let p and q be co-prime integers such that $\frac{p}{q} = [a_1, a_2, a_3, ...a_{n-1}]$. Then, an integer solution (x, y) to Pell's equation $x^2 - Dy^2 = 1$ is given by

$$(x, y) = (p, q) \text{ when } n \text{ is odd}$$

$$(x, y) = (p^2 + q^2 D, 2pq) \text{ when } n \text{ is even.}$$

Acknowledgments

We would like to thank:

- Zhulin Li, our mentor
- The MIT PRIMES program
- Our parents