Pell's Equation

Semin Oh (오 세 민)

2016. 07. 07.

The 80th Open Seminar on Algebras, Combinatorics and Algorithms

Pusan National University

Introduction

Definition

A **Diophantine equation** is an equation in which only integer solutions are allowed. A **Pell's equation** is a kind of Diophantine equations.

Definition. (Pell's Equation)

$$x^2 - Dy^2 = 1, \qquad D \in \mathbb{Z}_{>0}$$

Problem

Euler Project Problem 66 - Pell's Equation

다음과 같은 2차 디오판토스 방정식이 있습니다.

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

$D = \{2, 3, 5, 6, 7\}$ 에 대해서 x를 최소화하는 자연수 해를 찾아 보면 다음과 같습니다.

$$3^2 - 2 \times 2^2 = 1, \qquad 2^2 - 3 \times 1^2 = 1,$$

$$9^2 - 5 \times 4^2 = 1, \qquad 5^2 - 6 \times 2^2 = 1,$$

$$8^2 - 7 \times 3^2 = 1$$

위 경우에 대해 x의 값이 가장 큰 것은 $D = 5$일 때입니다. $D \leq 1000$ 인 경우에 대해 x를 최소화하는 해를 구하면, 가장 큰 x의 값을 갖는 D는 얼마입니까?

A Short History of Pell's Equation

Year	Events
AD 628	**Brahmagupta** described how to use known solutions to Pell's equation to create new solutions.
AD 1150	**Bhaskaracharya** gave an efficient method for finding a minimal positive solution to Pell's equation.
AD 1657	**Fermat** solved the equation $x^2 - 61y^2 = 1$. solution : $(1766319049, 226153980)$
	Brouncker described a general method for solving Pell's equation and solved $x^2 - 313y^2 = 1$ solution : $(32188120829134849, 1819380158564160)$

Brahmagupta (598-670)

A Short History of Pell's Equation

Year	Events
AD 628	**Brahmagupta** described how to use known solutions to Pell's equation to create new solutions.
AD 1150	**Bhaskaracharya** gave an efficient method for finding a minimal positive solution to Pell's equation.
AD 1657	**Fermat** solved the equation $x^2 - 61y^2 = 1$. solution : $(1766319049, 226153980)$ **Brouncker** described a general method for solving Pell's equation and solved $x^2 - 313y^2 = 1$ solution : $(32188120829134849, 1819380158564160)$

A Short History

Bhaskaracharya (1114-1185)

A Short History of Pell's Equation

Year	Events
AD 628	**Brahmagupta** described how to use known solutions to Pell's equation to create new solutions.
AD 1150	**Bhaskaracharya** gave an efficient method for finding a minimal positive solution to Pell's equation.
AD 1657	**Fermat** solved the equation $x^2 - 61y^2 = 1$. solution : $(1766319049, 226153980)$ **Brouncker** described a general method for solving Pell's equation and solved $x^2 - 313y^2 = 1$ solution : $(32188120829134849, 1819380158564160)$

A Short History

Pierre de Fermat
(1601-1665)

William Bouncker
(1585-1645)

Behind Story..

John Wallis described Brouncker's method in a book on algebra and number theory, and Wallis and Fermat both asserted that Pell's equation always has a nontrivial solution.

Leonhard Euler mistakenly thought that the method in Wallis's book was due to **John Pell**, another English mathematician, and it is Euler who assigned the equation the name by which it has since been known.

John Wallis (1616-1703)

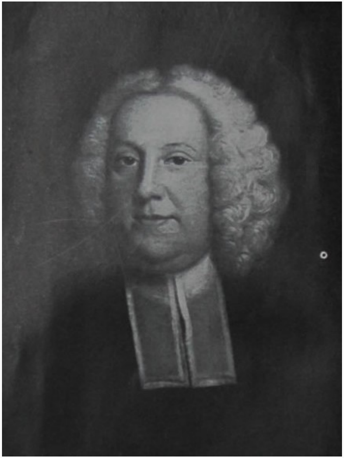
Behind Story..

John Wallis described Brouncker's method in a book on algebra and number theory, and Wallis and Fermat both asserted that Pell's equation always has a nontrivial solution.

Leonhard Euler mistakenly thought that the method in Wallis's book was due to **John Pell**, another English mathematician, and it is Euler who assigned the equation the name by which it has since been known.

A Short History

Loenhard Euler
(1707-1783)



John Pell
(1611-1685)

Preliminaries

Fundamental Theorem.

Theorem 0. (Lagrange 1768)

For every positive integer D that is not a square, the equation $x^2 - Dy^2 = 1$ has a nontrivial solution.

Remarks. If $D = m^2$ for some integer m, then there are only trivial solutions $(x, y) = (\pm 1, 0)$, since

$$x^2 - m^2y^2 = 1 \iff \begin{matrix} x - my = -1 \\ \& \\ x + my = -1 \end{matrix} \quad \text{or} \quad \begin{matrix} x - my = 1 \\ \& \\ x + my = 1 \end{matrix}$$

Note that if (x, y) is a solution, $(-x, -y)$ and $(\mp x, \pm y)$ are also solutions. So it suffice to consider **only positive solutions**.

Fundamental Theorem.

Theorem 0. (Lagrange 1768)

For every positive integer D that is not a square, the equation $x^2 - Dy^2 = 1$ has a nontrivial solution.

Remarks. If $D = m^2$ for some integer m, then there are only trivial solutions $(x, y) = (\pm 1, 0)$, since

$$x^2 - m^2y^2 = 1 \iff \begin{matrix} x - my = -1 \\ \& \\ x + my = -1 \end{matrix} \quad \text{or} \quad \begin{matrix} x - my = 1 \\ \& \\ x + my = 1 \end{matrix}$$

Note that if (x, y) is a solution, $(-x, -y)$ and $(\mp x, \pm y)$ are also solutions. So it suffice to consider **only positive solutions**.

Now we assume that D is not a square number.

Continued Fraction

Definition. (Continued Fraction)

An expression of form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = a_1 + \frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_n}$$

where $a_1 \in \mathbb{Z}$ and $a_i \in \mathbb{Z}_{>0}$ $(i \geq 2)$, is called a **(simple) continued fraction.** We will denote the above fraction by the symbol

$$[a_1, a_2, \ldots, a_n].$$

Continued Fraction

Proposition.

For any $\alpha \in \mathbb{R}$, the expression of the continued fraction of α is uniquely determined.

Examples.

(a) $\frac{5}{7} = 0 + \frac{1}{1+}\frac{1}{2+}\frac{1}{2} = [0, 1, 2, 2]$

(b) $-\frac{9}{7} = -2 + \frac{5}{7} = -2 + [0, 1, 2, 2] = [-2, 1, 2, 2]$

(c) $\sqrt{2} = 1 + \frac{1}{2+}\frac{1}{2+}\cdots = [1, 2, 2, \ldots]$

Continued Fraction

Definition. (Convergent)

A continued fraction $[a_1, a_2, \ldots, a_m]$ by ignoring all of the terms after a given term is called a **convergent** to the original continued fractions. The n**th convergent** is $[a_1, \ldots, a_n]$.

Definition. (Sequences of Convergents)

For a continued fraction $[a_1, a_2, \ldots, a_m]$ with $a_1 \in \mathbb{Z}_{\geq 0}$, define two sequences (p_n) and (q_n) consist of positive integers such that

$$\frac{p_n}{q_n} = [a_1, a_2, \ldots, a_n]$$

and p_n, q_n are coprime for each $1 \leq n \leq m$.

Continued Fraction

Well Known Recurrence Relation:

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \qquad q_{n+2} = a_{n+2}q_{n+1} + q_n$$

Example. ($\sqrt{7}$)

Let $\alpha_1 = \sqrt{7}$ and let $a_n = \lfloor \alpha_n \rfloor$, $\alpha_{n+1} = \dfrac{1}{\alpha_n - a_n}$.

n	1	2	3	4	5	6	$\cdots$
α_n	$\sqrt{7}$	$\frac{1}{\sqrt{7}-2}$	$\frac{\sqrt{7}+1}{2}$	$\frac{\sqrt{7}+1}{3}$	$\sqrt{7}+2$	$\frac{1}{\sqrt{7}-2}$	$\cdots$
a_n	2	1	1	1	4	1	$\cdots$
p_n	2	3	5	8	37	45	$\cdots$
q_n	1	1	2	3	14	17	$\cdots$

Solution to Pell’s Equations

Solution to Pell's Equation

Theorem 1. (Dirichlet's Diophantine Approximation)

Let α be an irrational number. If a/b is a rational number with positive denominator such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

then a/b is one of the convergents to α.

See Chapter 33 in the Silverman's book[1].

[1] Joseph H Silverman. A Friendly Introduction to Number Theory. Pearson, 2013.

Solution to Pell's Equation

Theorem 2.

Let D be a positive integer that is not a square. If x_0, y_0 is a positive solution to

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

then x_0/y_0 is one of the convergents to $\sqrt{D}$.

Proof Since x_0, y_0 is a positive solution to $x^2 - Dy^2 = 1$, then $(x_0 - y_0\sqrt{D})(x_0 + y_0\sqrt{D}) = 1$ which implies that $x_0 > y_0\sqrt{D}$. Therefore,

$$0 < \frac{x_0}{y_0} - \sqrt{D} = \frac{1}{y_0(x_0 + y_0\sqrt{D})} < \frac{1}{y_0(y_0\sqrt{D} + y_0\sqrt{D})} < \frac{\sqrt{D}}{2y_0^2\sqrt{D}}.$$

It follows from Theorem 1 that x_0/y_0 is a convergent to $\sqrt{D}$. ∎

Solution to Generalized Pell's Equations

Solution to Generalized Pell's Equation

Theorem 3.

Let n be an integer and D a nonsquare positive integer with $|n| < \sqrt{D}$. If positive integers x and y satisfy $x^2 - Dy^2 = n$ then x/y is a convergent to the continued fraction of $\sqrt{D}$.

Proof Taking $\alpha = \sqrt{D}$, if $x^2 - Dy^2 = n$ with $|n| < \sqrt{D}$ and $x, y > 0$ then

$$\left|\frac{x}{y} - \sqrt{D}\right| = \frac{|n|}{y^2(x/y + \sqrt{D})} < \frac{\sqrt{D}}{y^2(x/y + \sqrt{D})} = \frac{1}{y^2(x/(y\sqrt{D}) + 1)}.$$

If $n > 0$ then $x^2 - Dy^2 = n > 0 \implies x^2 > Dy^2$, so $x > y\sqrt{D}$ since x and y are positive. Then the blue fraction is less than $\frac{1}{2y^2}$. By Theorem 1, x/y is a convergent of $\sqrt{D}$.

If $n < 0$ then $x^2 - Dy^2 < 0 \implies x < y\sqrt{D}$. Now look at y/x as an approximation to $1/\sqrt{D}$:

$$\left|\frac{y}{x} - \frac{1}{\sqrt{D}}\right| = \frac{|n|}{x\sqrt{D}(y\sqrt{D}+x)} = \frac{|n|}{x^2\sqrt{D}(y\sqrt{D}/x+1)} < \frac{1}{x^2(y\sqrt{D}/x+1)}.$$

Then red fraction is $\boxed{\text{less than } \frac{1}{2x^2}}$ since $x < y\sqrt{D}$. It means that y/x is a convergent to $1/\sqrt{D}$ by Theorem 1.

If $\sqrt{D} = [a_1, a_2, a_3, \ldots]$ then $a_1 \geq 1$ so $1/\sqrt{D} = [0, a_1, a_2, \ldots]$, which means the convergents to $\sqrt{D}$ are the reciprocals of the convergents to $1/\sqrt{D}$. Thus x/y is a convergent to $\sqrt{D}$. ■

If $n < 0$ then $x^2 - Dy^2 < 0 \Longrightarrow x < y\sqrt{D}$. Now look at y/x as an approximation to $1/\sqrt{D}$:

$$\left|\frac{y}{x} - \frac{1}{\sqrt{D}}\right| = \frac{|n|}{x\sqrt{D}(y\sqrt{D} + x)} = \frac{|n|}{x^2\sqrt{D}(y\sqrt{D}/x + 1)} < \frac{1}{x^2(y\sqrt{D}/x + 1)}.$$

Then red fraction is less than $\frac{1}{2x^2}$ since $x < y\sqrt{D}$. It means that y/x is a convergent to $1/\sqrt{D}$ by Theorem 1.

If $\sqrt{D} = [a_1, a_2, a_3, \ldots]$ then $a_1 \geq 1$ so $1/\sqrt{D} = [0, a_1, a_2, \ldots]$, which means the convergents to $\sqrt{D}$ are the reciprocals of the convergents to $1/\sqrt{D}$. Thus x/y is a convergent to $\sqrt{D}$. ■

Comments.

In some case of D and n there is no positive solution to the generalized Pell's equation at all!! (ex. $D = 7$ and $n = -1$) I don't know which conditions guarantee the existence of solutions of generalized Pell's equations likely Lagrange theorem. So, if you know, please let me know. ☺

Implementation

Implementation

Example.

Find the positive solution with the least x to $x^2 - 7y^2 = 1$.
The continued fraction of $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$.

n	1	2	3	4	5	$\cdots$
p_n	2	3	5	**8**	37	$\cdots$
q_n	1	1	2	**3**	14	$\cdots$
$p_n^2 - 7q_n^2$	-3	2	-3	1	-3	$\cdots$

Recall that $p_{n+1} \geq p_n$ for each $n \geq 1$.

Implementation

Example.

Find the positive solution with the least x to $x^2 - 7y^2 = 1$.
The continued fraction of $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$.

n	1	2	3	4	5	$\cdots$
p_n	2	3	5	**8**	37	$\cdots$
q_n	1	1	2	**3**	14	$\cdots$
$p_n^2 - 7q_n^2$	-3	2	-3	1	-3	$\cdots$

Recall that $p_{n+1} \geq p_n$ for each $n \geq 1$.

Let's solve the **Problem 66** with SAGE !

References

- Project Euler @kr. URL: http://euler.synap.co.kr/prob_detail.php?id=66.
- James E Shockley. Introduction to number theory. Holt, Rinehart and Winston, 1967.
- Joseph H Silverman. A Friendly Introduction to Number Theory. Pearson, 2013.
- Seung Hyun Yang. “Continued Fractions and Pell’s Equation”. In: University of Chicago REU Papers (2008).

END

Thank you ❦