CO 480 Lecture 5

Pell's Equation - Brahmagupta and Bhāskara II

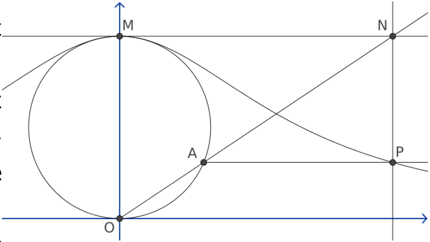
May 16th, 2017

This Day in History - May 16th, 2017

Maria Gaetana Agnesi born in Milan, Italy. Her Instituzioni analitiche of 1748 was an important calculus text. She is most often associated with the cubic curve known as the Witch of Agnesi, which got its name by a mistranslation. Her sister Maria Teresa was a noted composer.

Construction (From Wikipedia)

Starting with a fixed circle, a point O on the circle is chosen. For any other point A on the circle, the secant line OA is drawn. The point M is diametrically opposite to O. The line OA intersects the tangent of M at the point N. The line parallel to OM through N, and the line perpendicular to OM through A intersect at P. As the point A is varied, the path of P is the Witch of Agnesi.



Mistranslation (From Wikipedia)

The curve was studied by Pierre de Fermat in 1630. In 1703, Guido Grandi gave a construction for the curve. In 1718 Grandi suggested the name versoria for the curve, the Latin term for sheet, the rope which turns the sail, and used the Italian word for it, versiera, a hint to sinus versus (versine) that appeared in his construction. In 1748, Maria Gaetana Agnesi published her summation treatise Instituzioni analitiche ad uso della gioventù italiana, in which the curve was named according to Grandi, versiera. Coincidentally, the contemporary Italian word avversiera or versiera, derived from Latin adversarius, a nickname for Devil, "Adversary of God", was synonymous with "witch". Cambridge professor John Colson mistranslated the name of the curve thus.

Announcements

- In question 6b and 6c, I meant to say “Find an integer solution” and not just a solution. Sorry about this.
- Assignment 1 is due Thursday.
- Annotated Bibliography is due Tuesday May 30th
- I will be away for the next two weeks (should be available by email at weird hours).

Archimedes Cattle Problem

- From February 2002 AMS Vol 49 No. 2. article written by Henrik Lenstra Jr. [LJ02]
- Manuscript containing this problem discovered by Lessing in the Wolffenbüttel library and published as follows in 1773.
- Posed at Alexandria in a letter to Eratosthenes.
- See [Bel95] or [Hea64].

Archimedes Cattle Problem (1 of 4)

The Sun god's cattle, friend, apply thy care
to count their number, hast thou wisdom's share.
They grazed of old on the Thrinacian floor
of Sicily's island, herded into four,
colour by colour: one herd white as cream,
the next in coats glowing with ebon gleam,
brown-skinned the third, and stained with spots the last.
Each herd saw bulls in power unsurpassed,
in ratios these: count half the ebon-hued,
add one third more, then all the brown include;
thus, friend, canst thou the white bulls' number tell.
The ebon did the brown exceed as well,
now by a fourth and fifth part of the stained.
To know the spotted-all bulls that remained-
reckon again the brown bulls, and unite
these with a sixth and seventh of the white.

Archimedes Cattle Problem (2 of 4)

Among the cows, the tale of silver-haired
was, when with bulls and cows of black compared,
exactly one in three plus one in four.
The black cows counted one in four once more,
plus now a fifth, of the bespeckled breed
when, bulls withal, they wandered out to feed.
The speckled cows tallied a fifth and sixth
of all the brown-haired, males and females mixed.
Lastly, the brown cows numbered half a third
and one in seven of the silver herd.

Archimedes Cattle Problem (3 of 4)

Tell'st thou unfailingly how many head
the Sun possessed, o friend, both bulls well-fed
and cows of ev'ry colour-no-one will
deny that thou hast numbers' art and skill,
though not yet dost thou rank among the wise.
But come! also the foll'wing recognise.
Whene'er the Sun god's white bulls joined the black,
their multitude would gather in a pack
of equal length and breadth, and squarely throng
Thrinacia's territory broad and long.

Archimedes Cattle Problem (4 of 4)

But when the brown bulls mingled with the flecked,
in rows growing from one would they collect,
forming a perfect triangle, with ne'er
a diff'rent-coloured bull, and none to spare.
Friend, canst thou analyse this in thy mind,
and of these masses all the measures find,
go forth in glory! be assured all deem
thy wisdom in this discipline supreme

...

... what just happened?

Dissecting the Previous Slides

Following the notation in Lenstra's paper, Let x, y, z, t be the number of white, black, spotted and brown bulls. and further let x', y', z', t' be the number of cows of the same respective colours.

Dissecting the Previous Slides

Following the notation in Lenstra's paper, Let x, y, z, t be the number of white, black, spotted and brown bulls. and further let x', y', z', t' be the number of cows of the same respective colours.

On the first slide, we see that the following equations must be satisfied:

$$x = \left(\frac{1}{2} + \frac{1}{3}\right) y + t$$

$$y = \left(\frac{1}{4} + \frac{1}{5}\right) z + t$$

$$z = \left(\frac{1}{6} + \frac{1}{7}\right) x + t$$

Up to this point, this can be solved using linear algebra...

Solving...

$$\begin{aligned} z &= \frac{13}{42}\left(\frac{5}{6}y + t\right) + t \\ &= \frac{65}{252}\left(\frac{9}{20}z + t\right) + \frac{55}{42}t \\ &= \frac{13}{112}z + \frac{395}{252}t \end{aligned}$$

giving $z = \frac{395}{252} \cdot \frac{112}{99}t = \frac{1580}{891}t$. Setting $t = 891m$ for some integer m and unwinding gives the solution

$$(x, y, z, t) = (2226m, 1602m, 1580m, 891m)$$

Dissecting the Previous Slides

On the second slide of the Cattle Problem, we have that

$$x' = \left(\frac{1}{3} + \frac{1}{4}\right)(y + y')$$
$$y' = \left(\frac{1}{4} + \frac{1}{5}\right)(z + z')$$
$$z' = \left(\frac{1}{5} + \frac{1}{6}\right)(t + t')$$
$$t' = \left(\frac{1}{6} + \frac{1}{7}\right)(x + x')$$

Solving...

Up to this point, this is still just a linear algebra problem. We can solve this to see that 4657 divides m and so letting $m = 4657k$, we have the solution

$$(x', y', z', t') = (7206360k, 4893246k, 3515820k, 5439213k)$$

... long but doable by most high school students.

The challenge

On slide three and then on slide four we have the real challenge. We want

$$x + y = 2226m + 1602m = 4657 \cdot 3828 \cdot k$$

to be a square and

$$z + t = 1580m + 891m = 4657 \cdot 2471 \cdot k$$

to be a triangular number. In assignment three, you will prove that a number ℓ is a triangular number if and only if $8\ell + 1$ is a square and will take this for granted for now.

Simplifying the conditions

By Prime Factorization,

$$x + y = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot k$$

and so $x + y$ is a square precisely when $k = a\ell^2$ where $a = 3 \cdot 11 \cdot 29 \cdot 4657 = 4456749$. Further, $z + t$ is a triangular number precisely when $8(z + t) + 1$ is a square, say h^2 ,which when simplified:

$$h^2 = 8(z + t) + 1 = 8(4657 \cdot 2471 \cdot k) + 1 = 8 \cdot 4657 \cdot 2471 \cdot a\ell^2 + 1$$

occurs whenever $h^2 = D\ell^2 + 1$ is solvable where

$$\begin{aligned} D &= 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657)^2 \\ &= 410,286,423,278,424. \end{aligned}$$

or more simply, find integer solutions to $u^2 = dv^2 + 1$ where $d = D/(2 \cdot 4657)^2$ and $2 \cdot 4657 \mid v$. Can we do this?

Definition of Pell's Equation

Pell's Equation

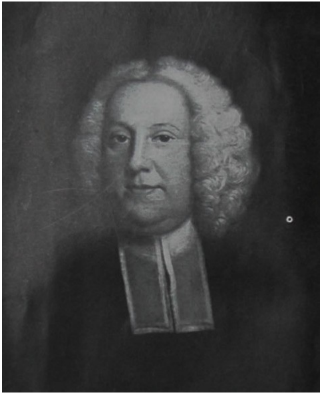
A Pell Equation (or Pell's Equation) is a Diophantine Equation of the form

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

where d is a given fixed positive squarefree integer (that is, no square integer divides d other than 1) and we seek integer solutions for x and y.

History of Pell's Equation [Bar03, p. 22]

- John Pell (c. 1611-1683) was a "minor mathematician".
- Some evidence that Pell worked on the equation $x^2 - 12y^2 = n$.



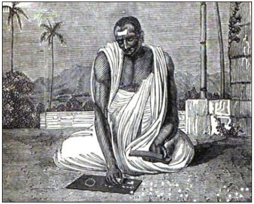
https://commons.wikimedia.org/wiki/File:John_Pell.jpg

More on Misattribution

- These equations were attributed to Pell by Leonhard Euler in a letter to Goldbach dated August 10th, 1730 [Bar03, p. 22].
- Even these references were late as Fermat and his contemporaries also studied these equations.
- Archimedes had an interest in these problem and we will study the Indian influence due to Brahmagupta in the sixth century and in the eleventh century from Jayadeva and Bhāskara II.
- Even earlier to Pell, Pierre de Fermat (1601-1665) made mention of these (I'll mention this later).

Brahmagupta

- Born in 598 AD son of Jiṣṇagupta in Ujjain, India. [OR]
- Died after 665 AD . [Sti03, p. 84] Maybe 670 AD [OR]
- Lived in Bhillamâla, now known as Bhinmal in Gujurat, a state in India [Sti03, p. 84]
- Worked on Linear congruences, Pell's Equation, geometry (cyclic quadrilaterals), astronomy
- Is credited with one of the first uses of zero as a number.

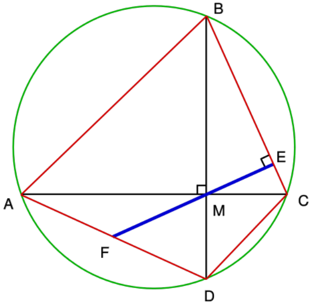


http://www.keywordsuggests.com/
0Cj8NMRlgALxDAehTm02PwQkQkC1ucadWTjwlr\
G3QU6WE2zvCSGHpHy*DqJpQRuc1g6yCA16*DDhkrT4hZxXEg

Brahmagupta's Theorem (From Wikipedia)

Brahmagupta's Theorem

More specifically, let A, B, C and D be four points on a circle such that the lines AC and BD are perpendicular. Denote the intersection of AC and BD by M. Drop the perpendicular from M to the line BC, calling the intersection E. Let F be the intersection of the line EM and the edge AD. Then, F is the midpoint AD.



https://commons.wikimedia.org/wiki/File:Brahmaguptra%27s_theorem.svg

Brahmagupta's Formula

Brahmagupta's Formula

Let $ABCD$ by a cyclic quadrilateral with sides a, b, c, d. Let $s = (a+b+c+d)/2$ be the semi-perimeter. Then

$$|ABCD| = \sqrt{(s-a)(s-b)(s-c)(s-d)}$$

Books

- In 628AD created the Brahmasphutasiddhanta (Brâhma-sphuṭa-siddhânta).
- Literally means “The Opening of the Universe” (See “The Great Mathematicians” by Flood and Wilson)
- Consists of 25 chapters. Topics include astronomy (first 10 chapters) and arithmetic, namely defining zero and negative numbers (debts), multiplication in a place value system, computing square roots, quadratic formula, money and interest computations, summing series, geometry, continued fractions and the first solutions to Pell’s Equations.

Zero (See Wikipedia or [OR])

- The sum of two positive quantities is positive
- The sum of two negative quantities is negative
- The sum of zero and a negative number is negative
- The sum of zero and a positive number is positive
- The sum of zero and zero is zero
- The sum of a positive and a negative is their difference; or, if they are equal, zero

https://en.wikipedia.org/wiki/Br%C4%81hmasphu%E1%B9%ADasiddh%C4%81nta

More on Zero (Subtraction)

- In subtraction, the less is to be taken from the greater, positive from positive
- In subtraction, the less is to be taken from the greater, negative from negative
- When the greater however, is subtracted from the less, the difference is reversed
- When positive is to be subtracted from negative, and negative from positive, they must be added together

Still More on Zero (Multiplication)

- The product of a negative quantity and a positive quantity is negative
- The product of two negative quantities is positive
- The product of two positive quantities is positive
- Positive divided by positive or negative by negative is positive
- Positive divided by negative is negative. Negative divided by positive is negative
- Zero divided by a negative or positive number is either zero or is expressed as a fraction with zero as numerator and the finite quantity as denominator
- A positive or negative number when divided by zero is a fraction with the zero as denominator
- Zero divided by zero is zero

Other Book of Brahmagupta

- Brahmagupta also wrote a second book in astronomy called the Khandakhadyaka in 665 AD (he was 67 years old then).
- Contained problems on eclipses, moons and crescent, conjunctions of planets and longitudes of planets.

Extra Videos

Check out the History of Mathematics series either on Netflix or below by Professor Marcus Du Sautoy

https://www.youtube.com/watch?v=pElvQdcaGXE

https://www.youtube.com/watch?v=DeJbR_FdvFM

Before going into the work of Brahpagupta, let's take a look at the time he lived in.

Back to Alexander [Bur91]

- Back in the time of Alexander the Great, his conquests bordered India which fostered relationships between Asia and the Mediterranean.
- Indian mathematics grew to be far superior to Greek mathematics in all areas except geometry.
- Algebra still in its infancy so more flowery language was used instead of a more formal proof based language.
- In around 500AD, Indian mathematician Aryabhatiya gave an approximation of π:

$$\pi \approx \frac{62832}{20000} = 3.1416$$

Connection to the time in which he worked.

- Back in the time of Alexander the Great, his conquests bordered India which fostered relationships between Asia and the Mediterranean.
- Indian mathematics grew to be far superior to Greek mathematics in all areas except geometry.
- Algebra still in its infancy so more flowery language was used instead of a more formal proof based language.
- Fall of the Roman empire occurs sometime between 500 and 600AD.
- At this point in India, a rather large religious movement, Islam, was in its infancy (the prophet Muhammad lived from about 570-632 AD).

Basics of Islam

Warning: Your instructor is not an expert in religion and most certainly not Islam. However we will discuss a bit about Islam and it's affect on the Indian region during this time.

- Islam means "submission"
- Muslim "one who submits"
- Muslims believe that God revealed the Qu'ran to Muhammad, God's final prophet

Five Pillars of Islam

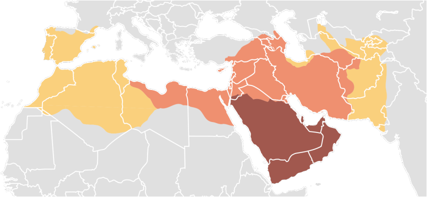
- Shahada: "I profess that there is no god but Allah, and Muhammad is the Prophet of God"
- Salah: daily prayers
- Zakah: alms-giving
- Sawm: fasting
- Hajj: pilgrimage to Mecca

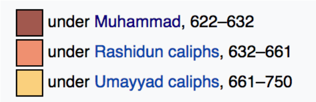
Muhammad's Dates

- Muhammad born in Mecca (570)
- First revelations (610)
- Hijra to Medina (622)
- Capture of Mecca (630)
- Muhammad dies (632)
- Islamic expansion surges

Muslim Conquests

https://www.youtube.com/watch?v=AvFl6UBZLv4





https://en.wikipedia.org/wiki/File:Map_of_expansion_of_Caliphate.svg

Gurjara Dynasty

- During the 600AD time period, Bhinmal was the capital of the lands ruled by the Gurjara dynasty [OR]
- The Gurjara Dynasty (Gurjara-Pratihara Dynasty of the Pratihara Empire) helped to contain armies from the Muslim conquest in north western India.
- Disagreement amongst historians as to whether these were native Indians or foreigners.
- Decline of the Gurjara Dynasty corresponded to the rise of the Muslim conquest.

Brâhma-sphuṭa-siddhânta

- For us this is Brahmagupta's most relevant work where he did most of his algebraic and number theoretic work.
- We will discuss his work in arithmetic with place value, quadratics and his work on Pell's equation

Indian Arithmetic - Multiplication

The following example is how Brahmagupta did multiplication ([Ifr01, p.574]). We do $345 \cdot 265$

$$
\begin{array}{cccccc}
3 & 2 & 6 & 5 & & \\
4 & & 2 & 6 & 5 & \\
5 & & & 2 & 6 & 5 \\
\hline
\end{array}
$$

Indian Arithmetic - Multiplication

The following example is how Brahmagupta did multiplication ([Ifr01, p.574]). We do $345 \cdot 265$

$$\begin{array}{cccccc}
3 & 2 & 6 & 5 & & \\
4 & & 2 & 6 & 5 & \\
5 & & & 2 & 6 & 5 \\
\hline
 & 7 & 9 & 5 & &
\end{array}$$

Indian Arithmetic - Multiplication

The following example is how Brahmagupta did multiplication ([Ifr01, p.574]). We do $345 \cdot 265$

$$
\begin{array}{cccccc}
3 & 2 & 6 & 5 & & \\
4 & & 2 & 6 & 5 & \\
5 & & & 2 & 6 & 5 \\
\hline
 & 7 & 9 & 5 & & \\
 & 1 & 0 & 6 & 0 &
\end{array}
$$

Indian Arithmetic - Multiplication

The following example is how Brahmagupta did multiplication ([Ifr01, p.574]). We do $345 \cdot 265$

$$
\begin{array}{cccccc}
3 & 2 & 6 & 5 & & \\
4 & & 2 & 6 & 5 & \\
5 & & & 2 & 6 & 5 \\
\hline
 & 7 & 9 & 5 & & \\
 & 1 & 0 & 6 & 0 & \\
 & & 1 & 3 & 2 & 5 \\
\hline
 & 9 & 1 & 4 & 2 & 5
\end{array}
$$

Quadratic Equation

- It is said that the Brâhma-sphuṭa-siddhânta contains the first clear description of the quadratic formula
- Usually attributed in its present form to Muhammad ibn Musa al-Khwarizmi (c. 780- c. 850)
- In fact, the word **algebra** is a derivative of al-jabr [completion], one of the two operations used by al-Khwarizmi to solve quadratic equations.
- His book "The Compendious Book on Calculation by Completion and Balancing" is where this is outlined.

Pell's Equation

- Brahmagupta also did some work in two variable indeterminate quadratic equations, namely, Pell's Equations.
- He did not solve them completely but he did give an algorithm for generating solutions.
- In what follows, we follow the outline by [Kat93, p.222-224] and [Sti03, p.75-80]
- Later work by Acarya Jayadeva c. 1000AD and Bhāskara II

The Pell Equation $x^2 - 92y^2 = 1$ according to Brahmagupta

A person solving this problem within a year is a mathematician (Brahmagupta).

Recall from assignment 1

Assignment 1

Show that for any $a, b, c, d, n \in \mathbb{R}$ that $(b^2 - na^2)(d^2 - nc^2) = (bd + nac)^2 - n(bc + ad)^2$.

Extending this result gives:

Composition Rule

Assignment 1

If $b^2 - na^2 = k_1$ and $d^2 - nc^2 = k_2$, then
$(bd + nac)^2 - n(bc + ad)^2 = k_1 k_2$

In this way, we can compose solutions to Pell's Equations of the form $x^2 - dy^2 = k_1$ and $x^2 - dy^2 = k_2$ to get a solution to $x^2 - dy^2 = k_1 k_2$.

In the assignment, you saw when both $k_1 = 1$ and $k_2 = 1$ that this gives a way to compose to larger solutions of $x^2 - dy^2 = 1$. It is less obvious that even when k_1 and k_2 are larger than one, sometimes these solutions can be combined to reduce to a smaller solution!

Composition of Triples

We denote a triple from before as (x_1, y_1, k_1) and (x_2, y_2, k_2) and denote their composition by

$$(x_1, y_1, k_1) \circ (x_2, y_2, k_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1, k_1k_2)$$

Solving $x^2 - 92y^2 = 1$.

We start off with the solution $(10)^2 - 92(1)^2 = 8$ and compose the triple $(10, 1, 8)$ with itself given

$$(10, 1, 8) \circ (10, 1, 8) = (192, 20, 64)$$

This corresponds to

$$192^2 - 92 \cdot (20)^2 = 8^2$$

Dividing through by 8^2 yields

$$24^2 - 92 \cdot (5/2)^2 = 1$$

This is almost an integer solution! We close our eyes and try composing the solution with itself to get...

Final composition

$$\begin{aligned}(24, 5/2, 1) \circ (24, 5/2, 1) &= (24^2 + 92(5/2)^2, 24 \cdot (5/2) + (5/2) \cdot 24, 1) \\ &= (576 + 575, 120, 1) \\ &= (1151, 120, 1).\end{aligned}$$

Therefore $(1151)^2 - 92(120)^2 = 1$. Crazy.

This Day In History May 18th, 1048

Omar Khayyam born in Nishapur, Persia. The mathematician, astronomer, and poet may have been the first to claim cubic equations– and hence angle trisection - could not be solved with straightedge and compass. Pierre Wantzel gave a proof in 1837.

Announcements

- Reminder we will be in different classrooms for the next little bit (sorry!):
- Thursday May 25th, 2017 - in STC 0010.
- Tuesday May 30th, 2017 - in STC 0010.
- Thursday June 1st, 2017 - in EIT 1015.
- Tuesday June 6th (Quiz) - in M3 1006
- Alain is teaching three of these. He will have office hours by appointment as well agamache@uwaterloo.ca

Quiz

- Fill in the blanks
- Short answers
- Long answer
- Math problems

Bhāskara II

- Born in 1114 AD. Died around 1185 AD. [Sti03, p. 85]
- Son of Maheśvara from the city of Bī jāpur.
- Admired work of Brahmagupta.
- Like Brahmagupta, was head of the observatory ad Ujjain [Kat93, p.224]
- Wrote Līlāvatī, said to be named after his daughter "to console her for an astrological forecast that went wrong" [Sti03, p. 85]

Major contributions

- Deducing a way to make sense of $1/0$.
- Idea: Divide a whole by 2, then by 3, then by 4 - each time you shrink the size of the parts you are dividing. Thus, if you divide 1 by something of size 0, you should get a lot of things (namely infinity).
- Also helped improve on the methods of Brahmagupta for Pell's Equation.
- We use [Sti03, p. 78-81] and [Wei84, p. 21-22] for what follows.

Preliminaries

Let (x, y, k) be a solution to $x^2 - dy^2 = k$.
With our composition rule as before, We provide solutions when $k \in \{\pm 1, \pm 2, \pm 4\}$. When $k_1 = 1$, we are done provided we have an integer solution. When $k \in \{-1, \pm 2\}$, all we need to do is perform a composition of the solution with itself. This gives,

$$(x, y, k) = (x^2 + dy^2, 2xy, k^2)$$

When $k = -1$ the above works. When $k = \pm 2$, notice that dividing the x and y coordinates by 2, getting

$$(1/2(x^2 + dy^2), xy, 1),$$

will give a solution (ie. we are dividing the new x and y coordinates by 2; squaring returns the necessary factor of 4).

Final case

If $k = \pm 4$ and x is even, then we see that the above still works after division by 4:

$$(1/4(x^2 + dy^2), 1/2(xy), 1)$$

If however, x is odd, then we perform the following:

$$(x', y', k') = (x/2, y/2, \pm 1) \circ (x/2, y/2, \pm 1) \circ (x/2, y/2, \pm 1)$$

and then we perform this action again if $k' = -1$. One can explicitly derive 3rd and 6th degree equations from this (but we won't).

The Pell Equation $x^2 - 61y^2 = 1$ According to Bhāskara II

So to solve this Pell Equation, it suffices to find some solution (x, y, k) with $d = 61$ and reduce k to be in the set $\{\pm 1, \pm 2, \pm 4\}$ and then from here apply one of the previous rules.

Big idea: Take a close solution, in this case $(8, 1, 3)$ and compose it with the parameterized solution $(m, 1, m^2 - d)$ (which is a solution for any d, not just $d = 61$). This gives $(8m + 61, 8 + m, 3(m^2 - 61))$.

Approximate solution

With our new solution, $(8m+61, 8+m, 3(m^2-61))$, we divide by 3 in the x and y coordinates which forces us to divide by 3^2 in the last coordinate to get the possible non-integral solution:

$$\left(\frac{8m+61}{3}, \frac{8+m}{3}, \frac{m^2-61}{3}\right).$$

An interesting result easily proved in general using modular arithmetic, if $3 \mid 8+m$, then the other two coordinates are also integers (this would be true if 3 were any arbitrary k). We choose m such that $3 \mid 8+m$ and m^2-61 is as small as possible in absolute value. The value $m=7$ accomplishes this and substituting this gives

$$(39, 5, -4)$$

which already gives us our goal.

Final composition

We now perform

$$(39/2, 5/2, -1)^6$$

(where by exponentiation we mean the composition action from before) and this gives

$$(1766319049, 226153980, 1)$$

and by composition this solution with itself, we can get infinitely many solutions as was done in assignment 1.

Pierre de Fermat

The example $x^2 - 61y^2 = 1$ was rediscovered in 1657 by Fermat [Sti03, p. 79]. It was sent in a letter to Frenicle as a challenge. Fermat wrote that he chose small numbers "pour ne vous donner pas trop de peine" (so you don't have too much work) [Con].

Modern Day Pell Equations (See [Con])

We have some unanswered questions:

- Does a Pell Equation always have a solution?
- How do we find one solution?
- How do we find all solutions?

Lagrange Returns!

Lagrange (1768)

The Pell Equation $x^2 - dy^2 = 1$ always has a nontrivial solution (ie. $xy \neq 0$) provided d is a non-square integer.

Idea: Used continued fractions and showed that a solution was related to a convergent of $\sqrt{d}$. Also showed all such $\sqrt{d}$ have periodic expansions. This is really neat but we will not go down this path.

Main Theorem

We will however give a complete classification of all solutions to Pell's Equations as outlined in [Con]:

Main Theorem

We will however give a complete classification of all solutions to Pell's Equations as outlined in [Con]:

Theorem

Let (x_1, y_1) be the positive solution to $x^2 - dy^2 = 1$ where y_1 is minimal. The solutions to $x^2 - dy^2 = 1$ are all generated from $\pm(x_1 + y_1\sqrt{d})^n$ where $n \in \mathbb{Z}$.

Some Lemmas

We have already proven much of the classification theorem.

Lemma 1

If (x, y) and (x', y') are solutions to $x^2 - dy^2 = 1$, then so are the coefficients to

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) = (xx' + dyy') + (x'y + xy')\sqrt{d}.$$

Proof

A simple substitution of the coefficients into Pell's equation yields

$$
\begin{aligned}
&(xx' + dyy')^2 - d(xy' + yx')^2 \\
&= x^2(x')^2 + 2dxx'yy' + d^2y^2(y')^2 - d(x^2(y')^2 + 2xx'yy' + y^2(x')^2) \\
&= x^2(x')^2 + d^2y^2(y')^2 - dx^2(y')^2 - dy^2(x')^2 \\
&= x^2((x')^2 - d(y')^2) - dy^2((x')^2 - d(y')^2) \\
&= (x^2 - dy^2)((x')^2 - d(y')^2) \\
&= 1
\end{aligned}
$$

Lemma 2

Lemma 2

If (x, y) is a solution to $x^2 - dy^2 = 1$, then the coefficients of $(x + y\sqrt{d})^n$ for any $n \in \mathbb{Z}$ also form a solution. So if $y \neq 0$, then a Pell equation has infinitely many solutions.

(This is just rewording the composition rule in the context of $\mathbb{Z}[\sqrt{d}]$).

Proof

The only thing really to consider here is the case when $n < 0$ ($n = 0$ is also easy and positive n were done before). In this case, since (x, y) is a solution to the Pell equation, we have that by the previous lemma (x_{-n}, y_{-n}) is a solution where these are the coefficients to $(x + y\sqrt{d})^{-n}$. Thus...

Proof continued

$$
\begin{aligned}
(x+y\sqrt{d})^n &= \frac{1}{(x+y\sqrt{d})^{-n}} \\
&= \frac{1}{x_{-n}+y_{-n}\sqrt{d}} \\
&= \frac{x_{-n}-y_{-n}\sqrt{d}}{(x_{-n}+y_{-n}\sqrt{d})(x_{-n}-y_{-n}\sqrt{d})} \\
&= \frac{x_{-n}-y_{-n}\sqrt{d}}{x_{-n}^2+dy_{-n}^2} \\
&= x_{-n}-y_{-n}\sqrt{d}
\end{aligned}
$$

and note $(x_{-n}, -y_{-n})$ is also a solution since (x_{-n}, y_{-n}) is.

Lemma 3

Lemma 3

If (x, y) is a solution to $x^2 - dy^2 = 1$, and $x + y\sqrt{d} > 1$, then $x > 1$ and $y > 0$.

Proof

Key Idea: As before, the reciprocal of $x + y\sqrt{d}$ is $x - y\sqrt{d}$. So reciprocating the given inequality, we see that

$$x + y\sqrt{d} > 1 > x - y\sqrt{d} > 0.$$

Thus, from first and third inequalities, $2y\sqrt{d} > 0$ and so $y > 0$ hence $y \geq 1$ (since $y \in \mathbb{Z}$). As

$$x > y\sqrt{d} \geq \sqrt{d} > 1$$

from the last two inequalities, we see that $x > 1$.

Lemma 4

Lemma 4

If (x, y) and (a, b) are solutions to $x^2 - dy^2 = 1$ with $a, b \geq 0$, then

$$a + b\sqrt{d} < x + y\sqrt{d}$$

is true if and only if $a < x$ and $b < y$.

Proof

If $a < x$ and $b < y$ then $a + b\sqrt{d} < x + \sqrt{d}y$. For the converse, suppose that $a + b\sqrt{d} < x + y\sqrt{d}$. Then, reciprocating yields

$$x - y\sqrt{d} < a - b\sqrt{d}.$$

Summing the two inequalities gives $(a + x) + (b - y)\sqrt{d} < (x + a) + (y - b)\sqrt{d}$. By lemma 3, $b - y < y - b$ and so $b < y$. Since

$$a^2 = 1 + db^2 < 1 + dy^2 = x^2$$

we see that $a < x$ (since $x, a > 0$).

Main Theorem

Theorem

Let (x_1, y_1) be the positive solution to $x^2 - dy^2 = 1$ where y_1 is minimal. The solutions to $x^2 - dy^2 = 1$ are all generated from $\pm(x_1 + y_1\sqrt{d})^n$ where $n \in \mathbb{Z}$.

The Easy Claim

By all of the above, we quickly note that $\pm(x_1 + y_1\sqrt{d})^n$ where $n \in \mathbb{Z}$ all form solutions to the Pell Equation $x^2 - dy^2 = 1$.

Harder Claim

Conversely, Suppose that $x^2 - dy^2 = 1$ for some $(x, y) \in \mathbb{Z}^2$ and we suppose that (x, y) are both positive (if $y = 0$ then $x = 1$ and this is an easy case). Let

$$x_1 + \sqrt{d}y_1, x_2 + \sqrt{d}y_2 = (x_1 + \sqrt{d}y_1)^2, \ldots$$

be the sequence of numbers coming from $(x_1 + \sqrt{d}y_1)^n$. These numbers by lemma 3 form an increasing sequence of numbers that tend to infinity. Further, by lemma 4, $x_i + y_i\sqrt{d} < x_{i+1} + y_i\sqrt{d}$ for all positive integers i. Therefore there exists an integer n such that

$$(x_1 + \sqrt{d}y_1)^n \leq x + y\sqrt{d} \leq (x_1 + \sqrt{d}y_1)^{n+1}.$$

Continued Proof

$$(x_1 + \sqrt{d}y_1)^n \leq x + y\sqrt{d} \leq (x_1 + \sqrt{d}y_1)^{n+1}$$

Now, this means that

$$1 \leq (x + y\sqrt{d})(x_1 + \sqrt{d}y_1)^{-n} < x_1 + y_1\sqrt{d}$$

By lemma 1, $(x + y\sqrt{d})(x_1 + \sqrt{d}y_1)^{-n}$ is a solution to the Pell equation, say $a + b\sqrt{d}$. Assuming towards a contradiction that $1 < a + b\sqrt{d}$, by lemma 3, $b < y_1$ but this is a contradiction since y_1 was minimal! Thus, $1 = a + b\sqrt{d}$ and so $x + y\sqrt{d} = (x_1 + \sqrt{d}y_1)^n$. Further, as $y \neq 0$, $n \geq 1$.

Tidying up.

For the negative solutions, notice that

$$\begin{aligned} -x - y\sqrt{d} &= -(x + y\sqrt{d}) \\ x - y\sqrt{d} &= (x + y\sqrt{d})^{-1} \\ -x + y\sqrt{d} &= -(x + y\sqrt{d})^{-1} \end{aligned}$$

so one of these has positive coefficients and hence

$$\pm(x + y\sqrt{d})^{\pm 1} = (x_y + y_1\sqrt{d})^n$$

holding for some value of n. Thus, $x + y\sqrt{d} = \pm(x_y + y_1\sqrt{d})^n$ for some $n \in \mathbb{Z}$. Note that we get the trivial solution when $n = 0$. This completes the proof.

Fundamental Solution

Fundamental Solution

An integer solution (x, y) to a Pell Equation with y minimal is called a *fundamental solution*

Note that the methods of Brahmagupta nor Bhāskara II can be guaranteed to give a minimal solution.

Corollary

Order the solutions as $(x_1, y_1), (x_2, y_2), \ldots$ corresponding to the constant coefficient and the coefficient of $\sqrt{d}$ of $(x_1 + \sqrt{d}y_1)^n$ for each $n \in \mathbb{N}$. Then

$$\begin{aligned} x_{k+1}\sqrt{d}y_{k+1} &= (x_1 + \sqrt{d}y_1)^{k+1} \\ &= (x_k + \sqrt{d}y_k)(x_1 + \sqrt{d}y_1) \\ &= (x_k x_1 + dy_k y_1 + \sqrt{d}(x_k y_1 + y_k x_1)) \end{aligned}$$

Back to the Cattle Problem

So has anyone solved the Cattle Problem?

First General Solution

The general solution to the second part of the problem was first found by A. Amthor in 1880 in his paper "Das Problema Bovinum des Archimedes". He used the simplified version of the Pell equation with d and determined that the continued fraction period was 92. Then using some theory about Legendre symbols (namely that $p = 4657$ is prime and that $\left(\frac{d}{p}\right) = -1$), Amthor determined that the smallest term in the sequence of solutions that satisfies Archimedes problem must divide $p + 1 = 4658$ (recall we need the Pell Equation solution in this case to divide $2 \cdot 4657$. In fact, the term sought after is the 2329th term.

Printed Solution

This term has 206545 digits and was first computed in June of 1965, Gus German, Robert Zarnke, and Hugh Williams right here at the University of Waterloo! Used a combination of the IBM 7040 and 1620 computers

https://cs.uwaterloo.ca/40th/Chronology/printable.shtml

Your turn!

Find an infinite family of solutions to the following Pell Equations. Can you classify all solutions?

- $x^2 - 33y^2 = 1$
- $x^2 - 21y^2 = 1$

References I

E. J. Barbeau.
Pell's equation.
Problem Books in Mathematics. Springer-Verlag, New York, 2003.

A. H. Bell.
The "Cattle Problem." By Archimedies 251 B. C.
Amer. Math. Monthly, 2(5):140–141, 1895.

David M. Burton.
The history of mathematics.
W. C. Brown Publishers, Dubuque, IA, second edition, 1991.
An introduction.

References II

K. Conrad.

Pell equations i and ii.

http://www.math.uconn.edu/~kconrad/blurbs/, visited 2017-05-15.

Check out the Pell Equation I and Pell Equation II blurbs.

T. L. Heath.

Diophantus of Alexandria: A study in the history of Greek algebra.

Second edition. With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler. Dover Publications, Inc., New York, 1964.

References III

Georges Ifrah.
The universal history of computing.
John Wiley & Sons, Inc., New York, 2001.
From the abacus to the quantum computer, Translated from the French and with notes by E. F. Harding, Assisted by Sophie Wood, Ian Monk, Elizabeth Clegg and Guido Waldman.

Victor J. Katz.
A history of mathematics.
HarperCollins College Publishers, New York, 1993.
An introduction.

H. W. Lenstra Jr.
Solving the Pell equation.
Notices Amer. Math. Soc., 49(2):182–192, 2002.

References IV

- J. J. O'Connor and E.F. Robertson.
  Brahmagupta.
  http://www-groups.dcs.st-and.ac.uk/history/Biographies/Brahmagupta.html, visited 2017-05-14.
- J. Stillwell.
  Elements of number theory.
  Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2003.
- André Weil.
  Number theory.
  Birkhäuser Boston, Inc., Boston, MA, 1984.
  An approach through history, From Hammurapi to Legendre.