Lecture 1: Conics

Brian Lehmann
Boston College

Introduction

What do theoretical mathematicians study?

Abstract mathematical structures:

- Algebra: discrete structures
- Analysis: continuity and change
- Geometry: shapes and measurement
- Number Theory: integers and primes

Particularly noteworthy: surprising connections between different areas

Goal: study a “surprising connection” between number theory and geometry.

Notation:

- $\mathbb{Z}$ denotes the set of integers: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$.
- $\mathbb{Q}$ denotes the set of rational numbers.
- $\mathbb{R}$ denotes the set of real numbers.
- $\mathbb{C}$ denotes the set of complex numbers.

Introduction

Let's fix:

- a set R of coefficients: either $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- a finite set of variables V: usually $\{x, y, z\}$ or $\{x_1, \ldots, x_n\}$.

Definition

A polynomial over R in the variables V is a finite sum whose terms are products of variables in V and coefficients in R.

Examples of polynomials over $\mathbb{Z}$:

$$x^3 - 27x + 5 \qquad 3xy + 4y^3 - 2x^4 \qquad 3xyz - z^2$$

Introduction

The degree of a polynomial is found in the following way. For each term we take the sum of exponents of the variables. The degree is the largest value of this sum as we vary over all the terms.

$\enclose{circle}{x^3} - 27x + 5$	$3xy + 4y^3 \enclose{circle}{-2x^4}$	$\enclose{circle}{3xyz} - z^2$
degree 3	degree 4	degree 3

Introduction

Suppose P is a polynomial over $\mathbb{Z}$ in n variables. We will be interested in solving the polynomial equation $P(x_1, \ldots, x_n) = 0$. The way we think about the solutions will depend on what type of values we allow for our variables x_i:

- Integer or rational solutions: the solutions will depend on the prime factors of the coefficients (number theory).
  Questions: are there any solutions at all? Infinitely many?
- Real or complex solutions: we can graph the solutions to obtain a shape in $\mathbb{R}^n$ or $\mathbb{C}^n$ (geometry).
  Questions: what does this shape look like? How is it “curved”?

Introduction

Guiding Principle

Let P be a polynomial over $\mathbb{Z}$. The properties of the integer/rational solutions depend on the "curvature" of the real/complex solutions.

This is a fundamental example of a surprising connection between different areas of math! It is currently an active area of research.

History

Definition

A Diophantine equation is an equation of the form $P(x_1, \ldots, x_n) = 0$ where P is a polynomial over $\mathbb{Z}$.

A Diophantine problem asks to find the integer solutions to a Diophantine equation.

Diophantine problems are some of the oldest in mathematics. We start by giving a brief overview of some fun examples.

Pythagorean triples

A Pythagorean triple is a triple of integers (a, b, c) which are not all zero and satisfy

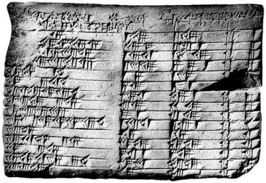
$$a^2 + b^2 = c^2.$$

Some examples of Pythagorean triples are:
$(3, 4, 5)$: $3^2 + 4^2 = 5^2$.
$(6, 8, 10)$: $6^2 + 8^2 = 10^2$.
$(5, 12, 13)$: $5^2 + 12^2 = 13^2$.

Pythagorean triples

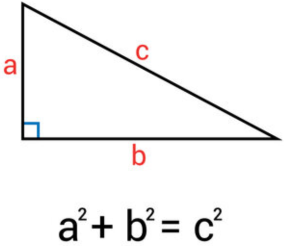
This is the most famous Diophantine problem due to its long history and geometric significance.

Oldest known example: 1800 BC Babylonian tablet (Plimpton 322)



Pythagorean triples

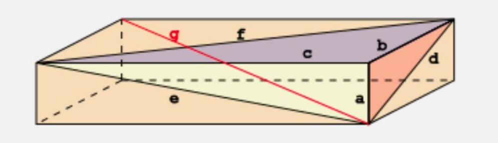
The Pythagorean school was interested in these triples due to their connections with right triangles.



Three-dimensional analogue

What is a “three-dimensional analogue” of a Pythagorean triple?

Each Pythagorean triple gives a rectangle whose sides and diagonal all have integer length. Similarly, we can ask if there is a three-dimensional box such that **every** side and diagonal – including face diagonals and the main diagonal – has integer length.



Three-dimensional analogue

The following problem asks for an analogue in three dimensions:

Problem

Is there a three-dimensional box satisfying the following properties?

- Each side length a, b, c is an integer.
- Each face diagonal d, e, f is an integer.
- The main diagonal g is an integer.

Such a box is called a "perfect Euler brick."

Three-dimensional analogue

One can view this as a type of Diophantine problem:

Problem

Are there non-zero integers a, b, c, d, e, f, p satisfying the following equations?

$$a^2 + b^2 = d^2 \qquad a^2 + c^2 = e^2 \qquad b^2 + c^2 = f^2$$
$$a^2 + b^2 + c^2 = g^2$$

Finding an integer solution is equivalent to finding a perfect Euler brick.

Three-dimensional analogue

This problem has not yet been solved! Computer searches have shown that if there is a perfect Euler brick, the lengths of the edges must be at least $\approx 10^{11}$.

There are heuristics which suggest that there should be no solution. (One such heuristic is our Guiding Principle – curvature controls integer solutions.) However no one has yet developed the techniques to solve this problem.

Cubic equations

Does the equation

$$x^3 + y^3 + z^3 = 29$$

have any integer solutions? Yes; the smallest is $(3, 1, 1)$.

Does the equation

$$x^3 + y^3 + z^3 = 30$$

have any integer solutions? Yes; the smallest is $(-283059965, -2218888517, 2220422932)$.

Cubic equations

More generally, we can look for integer solutions to the equation

$$x^3 + y^3 + z^3 = c$$

for various positive integers c. In other words: which integers c are a sum of three cubes?

We can generate some data for small values of c using a computer.

Cubic equations

Is there an integer solution to

$$x^3 + y^3 + z^3 = c?$$

c	sol?	c	sol?	c	sol?	c	sol?
1	yes	10	yes	19	yes	28	yes
2	yes	11	yes	20	yes	29	yes
3	yes	12	yes	21	yes	30	yes
4	no	13	no	22	no	31	no
5	no	14	no	23	no	32	no
6	yes	15	yes	24	yes	33	yes
7	yes	16	yes	25	yes	34	yes
8	yes	17	yes	26	yes	35	yes
9	yes	18	yes	27	yes	36	yes

Cubic equations

Conjecture

A positive integer c can be written as the sum of three cubes if and only if c is *not* 4 or 5 more than a multiple of 9.

This is currently unsolved! (You might enjoy proving the forward implication.)

Interesting history: prompted by a series of Youtube videos on the Numberphile channel, mathematicians have verified this conjecture for $c \leq 100$. The hardest one was $c = 42$ which was only solved in 2019 by Andrew Booker and Andrew Sutherland using distributed computation:

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$$

More examples

Other famous examples:

Theorem (Fermat's Last Conjecture / Wiles' Theorem)

If p is an integer satisfying $p \geq 3$, there are no non-zero integer solutions to the equation

$$x^p + y^p = z^p.$$

Theorem (Catalan's Conjecture / Mihăilescu's Theorem)

If p, q are integers satisfying $p, q \geq 2$, the only integer solution to the equation

$$x^p - y^q = 1$$

is $3^2 - 2^3 = 1$.

Pythagorean triples

Recall that a Pythagorean triple is a triple of integers (a, b, c) which are not all zero and satisfy

$$a^2 + b^2 = c^2.$$

For the remainder of the lecture, we study this special example at length.

Theorem

There are infinitely many Pythagorean triples and we have a formula for generating all of them.

Modifying solutions

We can construct new Pythagorean triples by modifying old ones:

- If (a, b, c) is a Pythagorean triple, so is (b, a, c).
- If (a, b, c) is a Pythagorean triple, so is $(\pm a, \pm b, \pm c)$.
- If (a, b, c) is a Pythagorean triple and d is any integer, then (da, db, dc) is also a Pythagorean triple:

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2.$$

- Conversely, if (a, b, c) is a Pythagorean triple and d is an integer dividing a, b, c, then $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ is also a Pythagorean triple.

Modifying solutions

Definition

A Pythagorean triple (a, b, c) is primitive if there is no prime p that simultaneously divides a, b, and c.

For example, $(3, 4, 5)$ and $(5, 12, 13)$ are primitive while $(6, 8, 10)$ is not (since every entry is divisible by 2).

Since we can obtain all Pythagorean triples by rescaling the primitive ones, we will focus on finding all primitive Pythagorean triples.

Recasting the problem

It will be helpful to recast the problem in the following way.

$$\begin{array}{c}\text{Integer solutions to}\\ a^2+b^2=c^2\end{array} \quad \leftrightarrow \quad \begin{array}{c}\text{Rational solutions to}\\ x^2+y^2=1\end{array}$$

Let’s explain the connection between the two sides.

Recasting the problem

First, given any Pythagorean triple (a, b, c) the fractions $(\frac{a}{c}, \frac{b}{c})$ solve $x^2 + y^2 = 1$:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = \frac{a^2 + b^2}{c^2} = 1.$$

Note that rescaling (a, b, c) does not affect the resulting (x, y).

Second, suppose we have a rational solution (x, y) to $x^2 + y^2 = 1$. We can put the two fractions over a common denominator: $(x, y) = (\frac{p}{q}, \frac{r}{q})$. If we choose the smallest possible q, we get a primitive Pythagorean triple by clearing denominators:

$$\left(\frac{p}{q}\right)^2 + \left(\frac{r}{q}\right)^2 = 1 \implies p^2 + r^2 = q^2$$

Recasting the problem

More precisely, this argument shows:

Lemma

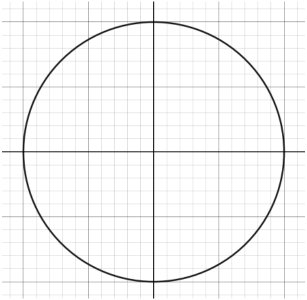
Consider the map

$$\text{Primitive Pythagorean triples} \to \begin{array}{c}\text{Rational solutions to}\\ x^2+y^2=1\end{array}$$
$$(a,b,c) \mapsto (\tfrac{a}{c}, \tfrac{b}{c})$$

This map is surjective and every fiber has exactly two elements: (a,b,c) *and* $(-a,-b,-c)$.

Geometry of the circle

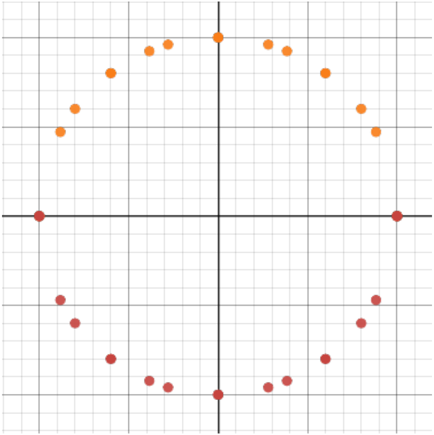
The key advantage of our new perspective is provided by our Guiding Principle: we should think about this problem in terms of geometry! The equation $x^2 + y^2 = 1$ defines a circle in the plane:



Circle of radius 1

Geometry of the circle

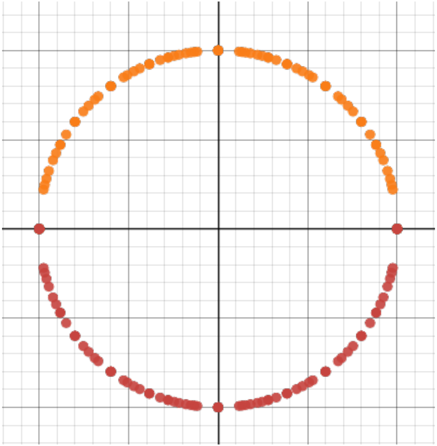
We are looking for points (x, y) on the circle whose coordinates are rational. Here is a picture of the 24 rational solutions with the “simplest” coordinates:



24 rational points

Geometry of the circle

Here is a picture of the 100 rational solutions with the “simplest” coordinates:

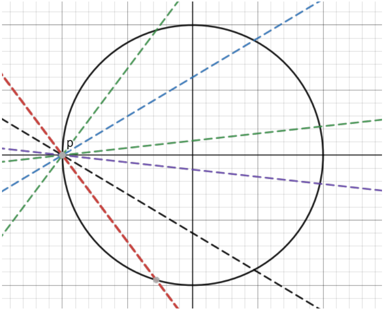


100 rational points

Finding rational points

How can we systematically find the rational solutions to $x^2 + y^2 = 1$?

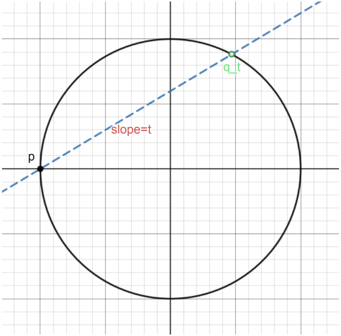
We will use a geometric technique known as "projecting away from a point." We will fix the point $p = (-1, 0)$ and consider the lines going through p.



Projection from p

Finding rational points

Suppose we draw a line of slope t through the point p. This line will meet the circle in exactly one more point which we call q_t. The equation of the line is $y = t(x+1)$.



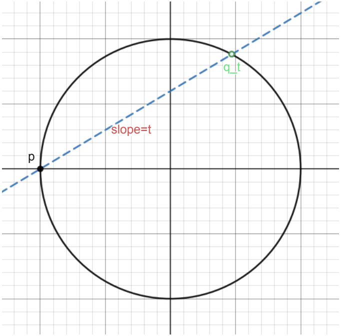
Line of slope t

Finding rational points

Our strategy for finding rational solutions is:

Key Observation

The point q_t has rational coordinates if and only if the slope t is a rational number.



Line of slope t

Finding rational points

If we fix the value of t, we can find the coordinates of the point q_t by solving the two equations:

$$\begin{aligned} y &= t(x+1) \\ x^2 + y^2 &= 1 \end{aligned}$$

We can substitute the first equation into the second:

$$x^2 + t^2(x+1)^2 = 1$$

Since t is fixed we should view this as a quadratic equation in x whose solutions are the x-coordinates of the points where the curves meet.

Finding rational points

Instead of using the quadratic formula, let's remember the following fact:

Theorem

The solutions to the equation $ax^2 + bx + c = 0$ can be found by factoring: if the solutions[1] *are r_1, r_2 then*

$$ax^2 + bx + c = a(x - r_1)(x - r_2).$$

We will solve our quadratic in x by factoring instead.

[1] Here we are allowing the solutions r_1, r_2 to be complex numbers counted with multiplicity.

Finding rational points

We can rewrite our quadratic as:

$$(1+t^2)x^2 + 2t^2x + (t^2-1) = 0.$$

But we already know one solution: $x = -1$ will always work! This comes from the fact that the point $(-1, 0)$ also lies on both curves.

We can find the other solution by factoring:

$$(1+t^2)x^2 + 2t^2x + (t^2-1) = (1+t^2)\left(x-(-1)\right)(x-??)$$

By comparing the coefficient of x on both sides, we see that the other solution is

$$x = 1 - \frac{2t^2}{1+t^2} = \frac{1-t^2}{1+t^2}.$$

Finding rational points

Finally, by plugging our solution x back into one of our original equations

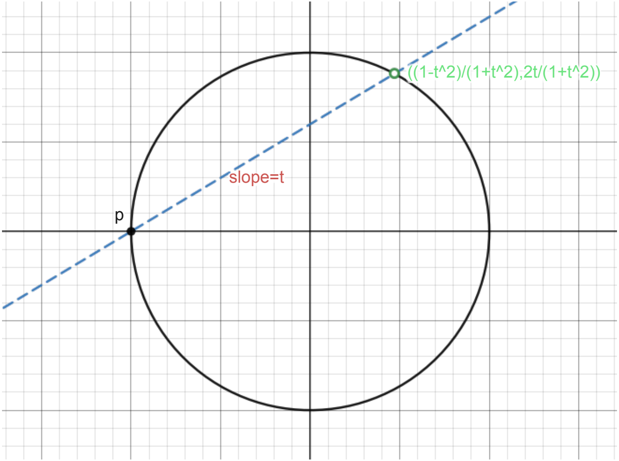
$$\begin{aligned} y &= t(x+1) \\ x^2 + y^2 &= 1 \end{aligned}$$

we can also find the y-coordinate of q_t. The final solution is

$$q_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right).$$

(Double check that if you square these numbers and add you get 1.)

Finding rational points



Line of slope t

Finding rational points

Let's remember our goal: we want to find the points (x, y) on the circle with rational coordinate. We can now explain:

Key Observation

The point q_t has rational coordinates if and only if the slope t is a rational number.

Proof.

Suppose $q_t = (x, y)$ has rational coordinates. The slope of the line between $(-1, 0)$ and q_t is equal to $\frac{y}{x+1}$ which is also rational. Conversely, if t is a rational number then so are $\frac{1-t^2}{1+t^2}$ and $\frac{2t}{1+t^2}$ which are the coordinates of q_t. □

Finding rational points

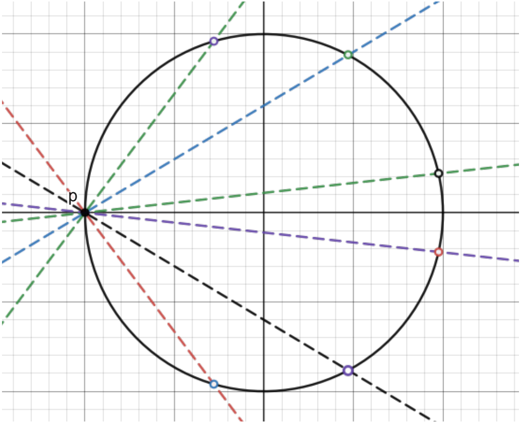
Finally, we have found our solution! We can generate all possible rational solutions (x, y) to $x^2 + y^2 = 1$ by plugging in various rational numbers t into the formula

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

Our key observation shows that we get **all** rational solutions in this way! (Aside from the starting point $(-1, 0)$.)

Examples:
$t = 1$ yields $(0, 1)$, and $0^2 + 1^2 = 1$.
$t = \frac{1}{3}$ yields $(\frac{4}{5}, \frac{3}{5})$, and $\frac{4}{5}^2 + \frac{3}{5}^2 = 1$.
$t = 27$ yields $(-\frac{364}{365}, \frac{27}{365})$, and $(-\frac{364}{365}^2) + \frac{27}{365}^2 = 1$.

Finding rational points



Finding rational points

Finding rational points

If we want to go all the way back to primitive Pythagorean triples, we simply clear denominators. Writing $t = \frac{n}{m}$ in lowest terms, the rational point

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right).$$

yields the primitive triple

$$(a, b, c) = \begin{cases} \left(m^2 - n^2, 2mn, m^2 + n^2\right) & \text{if one of } m, n \text{ is odd} \\ \left(\frac{m^2-n^2}{2}, mn, \frac{m^2+n^2}{2}\right) & \text{if both } m, n \text{ are odd} \end{cases}$$

Here we have implicitly used:

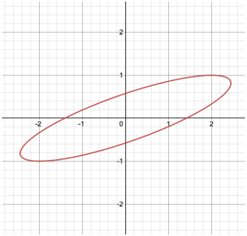
Exercise

If m, n are relatively prime integers then $\gcd(m^2 - n^2, 2mn) \in \{1, 2\}$.

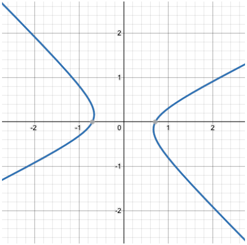
Perspective

Until now we have been focusing on a single equation $x^2 + y^2 = 1$ and finding its rational solutions.

However, the geometric method we developed – projection away from a point – can be used in other situations! Suppose $P(x, y)$ is a degree 2 polynomial and consider the curve C defined by $P(x, y) = 0$.



Ellipse



Hyperbola

Finding rational points on conics

Finding rational solutions to $P(x, y) = 0$:

1. Fix a single rational point p on the curve C.
2. Consider the line ℓ through p with slope t. This will meet the curve C in at most one other point q_t.
3. **Key question:** is it true that q_t has rational coordinates if and only if the slope t is rational?
4. Explicitly find the coordinates of q_t by factoring a quadratic equation.

The only missing piece is the “Key question.”

Finding rational points on conics

We need a result about quadratic equations:

Theorem

Suppose $ax^2 + bx + c = 0$ is a quadratic equation with rational coefficients. If this equation has one rational solution, then every solution is rational.

Proof.

We prove this statement using our factoring method:

$$ax^2 + bx + c = a(x - r_1)(x - r_2).$$

where r_1, r_2 are the solutions to the equation. Without loss of generality suppose that r_1 is rational. By comparing the coefficients of x on both sides, we see that

$$b = a(-r_1 - r_2) \implies r_2 = -r_1 - \frac{b}{a}.$$

Since a, b, r_1 are all rational, r_2 is as well. □

Finding rational points on conics

Key Observation

Let $P(x, y)$ be a degree 2 polynomial over $\mathbb{Q}$ and let C denote the conic $P(x, y) = 0$. Suppose $p \in C$ has rational coordinates. Consider the line ℓ of slope t through p and suppose that $\ell \cap C$ contains a point q_t different from p. Then q_t has rational coordinates if and only if t is rational.

Proof.

If p and q_t both have rational coordinates, then the slope of the line ℓ connecting them is rational. Conversely, if t is rational then we can find the coordinates of q_t by solving the simultaneous equations

$$y = tx + b \qquad\qquad P(x, y) = 0$$

Substituting the first equation into the second, we get a quadratic equation in x. This equation has one rational root corresponding to the x-coordinate of p. Thus the second root – the x-coordinate of q_t – is also rational. Using the linear equation we see that y-coordinate of q_t is again rational. □

Finding rational points on conics

Theorem

Let $P(x, y)$ be a degree 2 polynomial with rational coefficients. Suppose the equation $P(x, y) = 0$ defines a smooth[2] *curve C. If C admits one rational solution p, then it has infinitely many rational solutions.*

We find these infinitely many rational solutions by projecting away from p.

“Proof.”

Let C be the curve $P(x, y) = 0$. Consider the line ℓ through p with rational slope t. Then there is one other point q_t in $\ell \cap C$ besides p. By our Key Observation this point also has rational coordinates. As we vary the slope t we get infinitely many different points. □

[2] To be defined later...

Finding rational points on conics

Aside

We really need the "smooth" assumption. This assumption is what guarantees "$\ell \cap C$ contains one other point besides p." If a curve fails to be smooth, this statement does not need to be true.

For example, consider the degree 2 equation

$$x^2 + y^2 = 0.$$

This has exactly one solution $(x, y) = (0, 0)$. We will see later that it fails to be smooth at $(0, 0)$.

Exercises

Exercises:

1. Linear Diophantine equations: today we discussed finding rational solutions to degree 2 polynomials in two variables. But the simplest example is degree 1 polynomials in two variables. How can we solve such equations?
2. Quadratic Diophantine equations: we discussed a method for finding rational solutions to degree 2 polynomials in two variables. We have seen this in one example: $x^2 + y^2 = 1$. In this problem session you will give more examples and test the boundaries of our method.

Images made using Desmos and taken from Wikipedia, Fermat's Library, Adobe Stock Images.