Geometric approaches to solving Diophantine equations

Alex J. Best

Tomorrows Mathematicians Today 2013

16-2-2013

Introduction

Named for Diophantus of Alexandria ($\approx$ 250AD)
Some Diophantine equations:

Introduction

Named for Diophantus of Alexandria ($\approx$ 250AD)
Some Diophantine equations:

- $$x^2 + y^2 = z^2$$

  (Pythagorean triples)

Introduction

Named for Diophantus of Alexandria ($\approx$ 250AD)
Some Diophantine equations:

- $$x^2 + y^2 = z^2$$

  (Pythagorean triples)

- $$x^2 - ny^2 = 1$$

  (Pell's equation)

Introduction

Named for Diophantus of Alexandria ($\approx$ 250AD)
Some Diophantine equations:

- $$x^2 + y^2 = z^2$$
  (Pythagorean triples)
- $$x^2 - ny^2 = 1$$
  (Pell's equation)
- $$x^3 + 48 = y^4$$

Introduction

Named for Diophantus of Alexandria ($\approx$ 250AD)
Some Diophantine equations:

- $$x^2 + y^2 = z^2$$
  (Pythagorean triples)
- $$x^2 - ny^2 = 1$$
  (Pell's equation)
- $$x^3 + 48 = y^4$$
- $$9^x - 8^y = 1$$

What do we want to know?

What do we want to know?

- Are there any solutions?

What do we want to know?

- Are there any solutions?
- How many are there?

What do we want to know?

- Are there any solutions?
- How many are there?
- Can we classify them?

What do we want to know?

- Are there any solutions?
- How many are there?
- Can we classify them?
- How can we compute them?

In this talk

Two general ideas:

In this talk

Two general ideas:

- Geometry of numbers

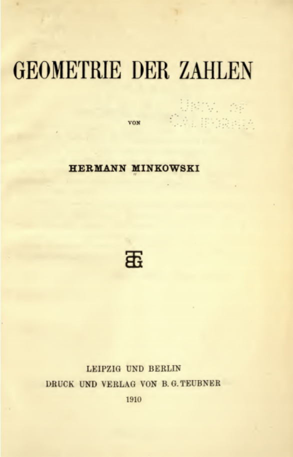
In this talk

Two general ideas:

- Geometry of numbers
- Rational points on surfaces

Minkowski and the Geometry of Numbers

1910 - Hermann Minkowski publishes his paper “Geometrie der Zahlen” and sparks a new field called the Geometry of Numbers.



GEOMETRIE DER ZAHLEN

VON

HERMANN MINKOWSKI

LEIPZIG UND BERLIN
DRUCK UND VERLAG VON B. G. TEUBNER
1910

A motivating example

We want to find when integers x, y such that $x^2 + y^2 = p$ where p is prime.

A motivating example

We want to find when integers x, y such that $x^2 + y^2 = p$ where p is prime.
We can try a few primes, and notice that $2^2 + 1^2 = 5$, $3^2 + 2^2 = 13$, $4^2 + 1^2 = 17$, ... all work.

A motivating example

We want to find when integers x, y such that $x^2 + y^2 = p$ where p is prime.
We can try a few primes, and notice that $2^2 + 1^2 = 5$, $3^2 + 2^2 = 13$, $4^2 + 1^2 = 17$, ... all work.
But 7, 11, 19, ... do not.

A motivating example

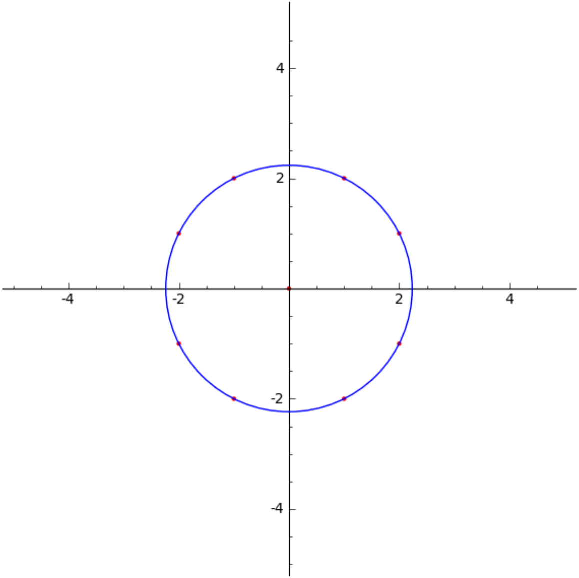
We want to find when integers x, y such that $x^2 + y^2 = p$ where p is prime.
We can try a few primes, and notice that $2^2 + 1^2 = 5$, $3^2 + 2^2 = 13$, $4^2 + 1^2 = 17$, ... all work.
But 7, 11, 19, ... do not.
So maybe $x^2 + y^2 = p$ when $p \equiv 1 \pmod 4$.

Theorem (Fermat's Christmas Theorem)

An odd prime p can be written as $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

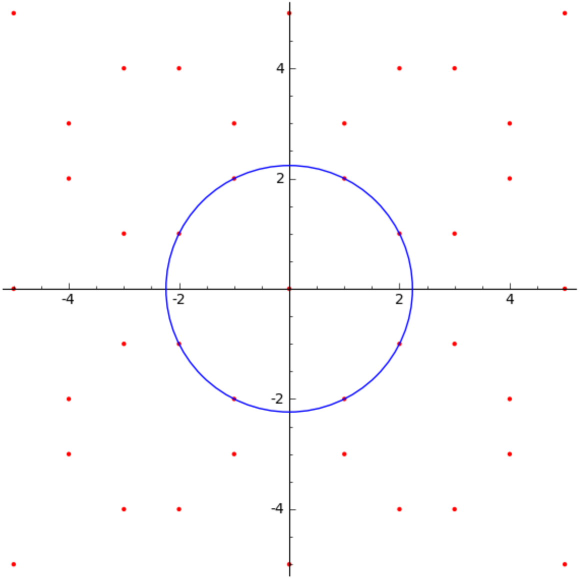
What can geometry do for us?

When $p = 5$ we can look at points satisfying our criteria:



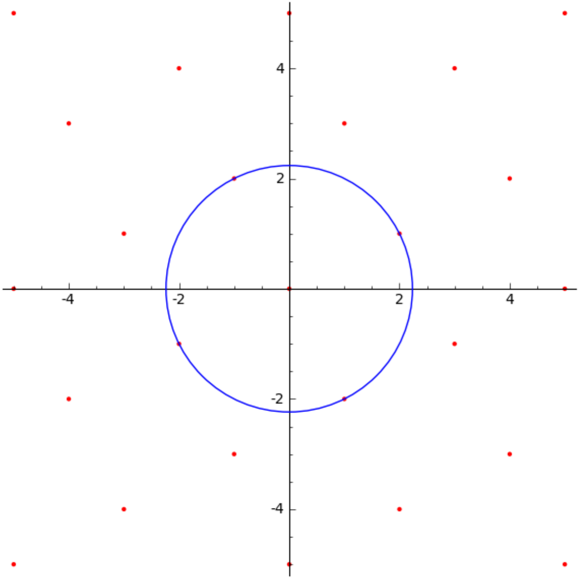
What can geometry do for us?

When $p = 5$ we can look at points satisfying our criteria:



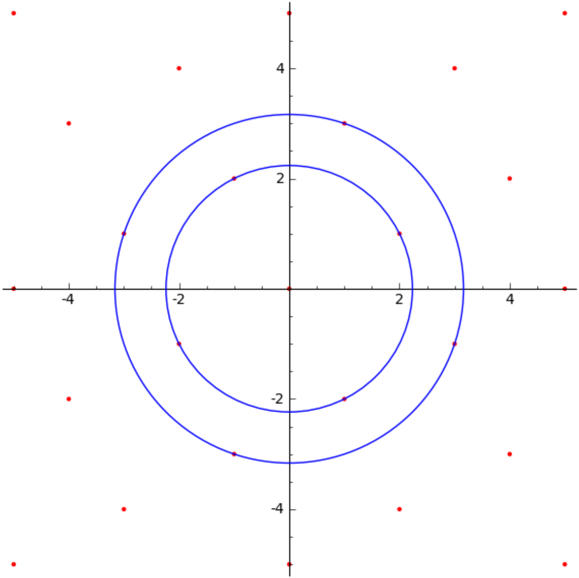
What can geometry do for us?

When $p = 5$ we can look at points satisfying our criteria:



What can geometry do for us?

When $p = 5$ we can look at points satisfying our criteria:



Minkowski's first theorem

We say a set B in $\mathbb{R}^n$ is symmetric if $x \in B \implies -x \in B$.
We say a set B is $\mathbb{R}^n$ is convex if
$x, y \in B \implies x + \lambda(y - x) \in B$ for $0 \leq \lambda \leq 1$.

Minkowski's first theorem

We say a set B in $\mathbb{R}^n$ is symmetric if $x \in B \implies -x \in B$.
We say a set B is $\mathbb{R}^n$ is convex if
$x, y \in B \implies x + \lambda(y - x) \in B$ for $0 \leq \lambda \leq 1$.

Theorem (Minkowski)

If B is a convex symmetric body and Λ a lattice in $\mathbb{R}^n$ then B contains a non-zero point of the lattice if:

$$\mathrm{Vol}(B) > 2^d i$$

Where i is the area of a single cell of the lattice Λ. We can find it using determinants, or the order of our lattice as a subgroup of $\mathbb{Z}^n$ for the more algebraically inclined.

Let's apply it

A circle in $\mathbb{R}^2$ is symmetric and convex, great!

Let's apply it

A circle in $\mathbb{R}^2$ is symmetric and convex, great!
The area of our lattice cell is p.

Let's apply it

A circle in $\mathbb{R}^2$ is symmetric and convex, great!
The area of our lattice cell is p.
The area of our circle is $\pi 2p$

Let's apply it

A circle in $\mathbb{R}^2$ is symmetric and convex, great!
The area of our lattice cell is p.
The area of our circle is $\pi 2p$
So Minkowski tells us that as:

$$\pi 2p = \mathrm{Vol}(B) > 2^d i = 2^2 p = 4p$$

We have a point which satisfies $x^2 + y^2 = kp$ for some $k \geq 1$, and also $x^2 + y^2 < 2p$. So $x^2 + y^2 = p$ and we are done.

Rational points on surfaces

Euler looked at

$$A^4 + B^4 = C^4 + D^4$$

with $A, B, C, D \in \mathbb{Q}$
This defines a surface in $\mathbb{R}^4$.

Rational points on surfaces

Euler looked at

$$A^4 + B^4 = C^4 + D^4$$

with $A, B, C, D \in \mathbb{Q}$
This defines a surface in $\mathbb{R}^4$.
One parametrisation of solutions[1]:

$$\begin{aligned}
a(s,t) &= s^7 + s^5t^2 - 2s^3t^4 + 3s^2t^5 + st^6 \\
b(s,t) &= s^6t - 3s^5t^2 - 2s^4t^3 + s^2t^5 + t^7 \\
c(s,t) &= s^7 + s^5t^2 - 2s^3t^4 - 3s^2t^5 + st^6 \\
d(s,t) &= s^6t + 3s^5t^2 - 2s^4t^3 + s^2t^5 + t^7
\end{aligned}$$

Rational points on surfaces

Euler looked at

$$A^4 + B^4 = C^4 + D^4$$

with $A, B, C, D \in \mathbb{Q}$
This defines a surface in $\mathbb{R}^4$.
One parametrisation of solutions[1]:

$$\begin{aligned}
a(s,t) &= s^7 + s^5t^2 - 2s^3t^4 + 3s^2t^5 + st^6 \\
b(s,t) &= s^6t - 3s^5t^2 - 2s^4t^3 + s^2t^5 + t^7 \\
c(s,t) &= s^7 + s^5t^2 - 2s^3t^4 - 3s^2t^5 + st^6 \\
d(s,t) &= s^6t + 3s^5t^2 - 2s^4t^3 + s^2t^5 + t^7
\end{aligned}$$

Unfortunately this does not give us all solutions.

Counting solutions

Q: How many solutions are there?

Counting solutions

Q: How many solutions are there?
A: ∞
Can we find a better way of counting them?
We want to estimate the density of our solutions.

Heights

We want a different way of describing the size of a rational number.
Take

$$x = \frac{a}{b} \in \mathbb{Q}, \;\; a, b \in \mathbb{Z}$$
$$\gcd(a, b) = 1$$

Heights

We want a different way of describing the size of a rational number.
Take

$$x = \frac{a}{b} \in \mathbb{Q}, \;\; a, b \in \mathbb{Z}$$

$$\gcd(a, b) = 1$$

Then we say height of x is:

$$H(x) := \max\{\log(|a|), \log(|b|)\}$$

Heights

We want a different way of describing the size of a rational number.

Take

$$x = \frac{a}{b} \in \mathbb{Q}, \;\; a, b \in \mathbb{Z}$$

$$\gcd(a, b) = 1$$

Then we say height of x is:

$$H(x) := \max\{\log(|a|), \log(|b|)\}$$

Hurrah! There are only finitely many points with height less than a given value.

Counting points

We now want to count points in a set X with bounded height. We do this in a simple way and define:

$$N(X, B) := \#\{x \in X | H(x) \leq B\}$$

We can analyse the growth of this function as B grows.

Counting points

We now want to count points in a set X with bounded height. We do this in a simple way and define:

$$N(X, B) := \#\{x \in X | H(x) \leq B\}$$

We can analyse the growth of this function as B grows. Manin and others have conjectured that the growth of $N(X, B)$ is asymptotically governed by geometric properties of the surface for many problems[2].

Morals

Geometry can help us show solutions exist to Diophantine equations.
Geometric properties govern the density of the solutions to some problems.

Morals

Geometry can help us show solutions exist to Diophantine equations.
Geometric properties govern the density of the solutions to some problems.
And there is a lot more interplay between these two areas.

References

Hardy, G.H. and Wright, E.M. and Heath-Brown, D.R. and Silverman, J.H., An Introduction to the Theory of Numbers, Oxford University Press, 2008.

Heath-Brown, D.R., Diophantine equations, Algebra, Geometry, Analysis & Logic, Talk at Warwick Mathematics Institute.