From Conic Sections to Isogeny Graphs

Chloe Martindale

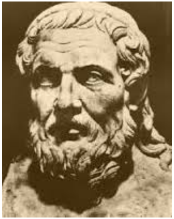
Universiteit Leiden and Université de Bordeaux

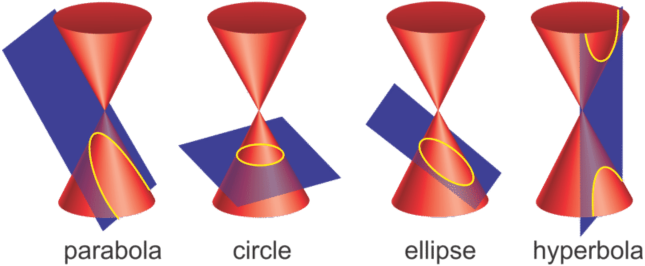
General Colloquium, Mathematics and Statistics, University College Dublin

29th June, 2016

Diophantine equations through the ages

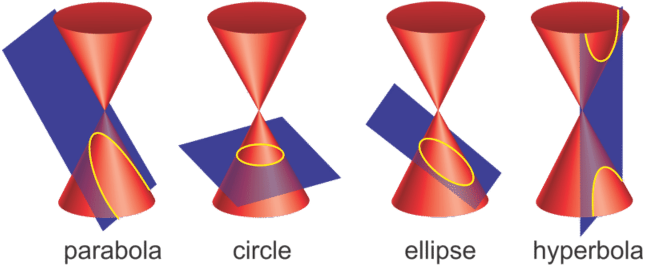
- **c. 360-350 BC: Menachmus**
- c. 350 BC: Euclid
- c. 250 AD: Diophantus writes *Arithmetica*





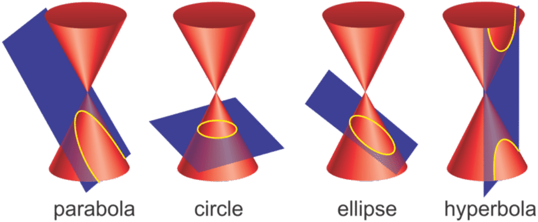
Diophantine equations through the ages

- c. 360-350 BC: Menachmus
- **c. 350 BC: Euclid**
- c. 250 AD: Diophantus writes *Arithmetica*

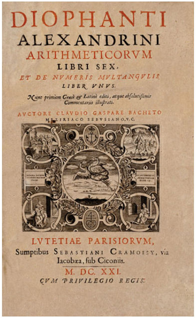


Diophantine equations through the ages

- c. 360-350 BC: Menachmus
- c. 350 BC: Euclid
- **c. 250 AD: Diophantus writes Arithmetica**



$$ax^2 + by^2 = 1$$


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantine equations through the ages: two variables

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

Diophantine equations through the ages: two variables

Definition

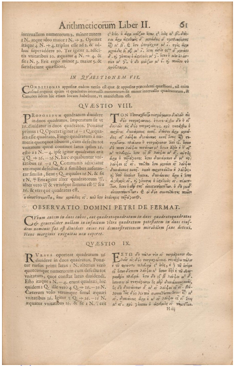
We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

Pierre de Fermat (1601-1665)

- Showed that all algebraic curves over $\mathbb{Q}$ of degree 2 are conics
- Claimed to have a proof that there are no non-trivial rational solutions to the algebraic curve $x^n + y^n = 1$ for $n \geq 3$.



Arithmeticorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

Isaac Newton (1643-1727)

- 1710: classifies algebraic curves over $\mathbb{Q}$ of degree 3, showing by that by applying rational transformations to x and y, these curves can always be written as

$$y^2 = x^3 + ax + b$$

for some $a, b \in \mathbb{Z}$.

Examples of algebraic curves of degree 3

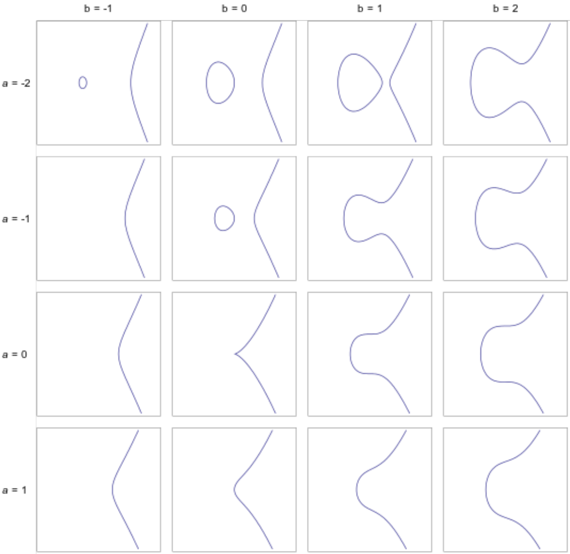


Image credits: "EllipticCurveCatalog" by Tos - Own work. Licensed under Public Domain via Commons

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

c.1829: Abel and Jacobi construct the Jacobian of a curve.

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

c.1829: Abel and Jacobi construct the Jacobian of a curve.

- The Jacobian is an additive group containing the curve itself

Diophantine equations through the ages: two variables

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

c.1829: Abel and Jacobi construct the Jacobian of a curve.

- The Jacobian is an additive group containing the curve itself
- Jacobians are examples of *abelian varieties*

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Definition

If μ is a solution of an equation as above for which *all* the solutions are positive, then μ is *totally positive*.

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Definition

If μ is a solution of an equation as above for which *all* the solutions are positive, then μ is *totally positive*.

Non-Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$,

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Definition

If μ is a solution of an equation as above for which *all* the solutions are positive, then μ is *totally positive*.

Non-Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$, for which the other solution is $1 - \sqrt{2}$.

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Definition

If μ is a solution of an equation as above for which *all* the solutions are positive, then μ is *totally positive*.

Non-Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$, for which the other solution is $1 - \sqrt{2}$.

Example: $\mu = 2 + \sqrt{2}$ is a solution of $x^2 - 4x + 2$,

Interlude: Algebraic integers

Definition

An *algebraic integer* μ is a solution of an equation

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$.

Definition

If μ is a solution of an equation as above for which *all* the solutions are positive, then μ is *totally positive*.

Non-Example: $\mu = 1 + \sqrt{2}$ is a solution of $x^2 - 2x - 1$, for which the other solution is $1 - \sqrt{2}$.

Example: $\mu = 2 + \sqrt{2}$ is a solution of $x^2 - 4x + 2$, for which the other solution is $2 - \sqrt{2}$.

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that
  - μ is real, and

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that
  - μ is real, and
  - μ is totally positive,

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that
  - μ is real, and
  - μ is totally positive,

  we can construct an abelian variety A'

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that
  - μ is real, and
  - μ is totally positive,

  we can construct an abelian variety A' and a map to it called a *μ-isogeny*.

Playing with algebraic curves

Definition

We define an *algebraic curve* over $\mathbb{Q}$ to be a curve that can be written as

$$f(x, y) = 0,$$

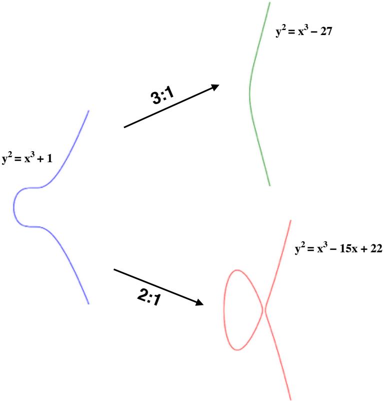
where $f \in \mathbb{Z}[x, y]$.

- The Jacobian of a curve contains the curve itself
- Jacobians are examples of abelian varieties

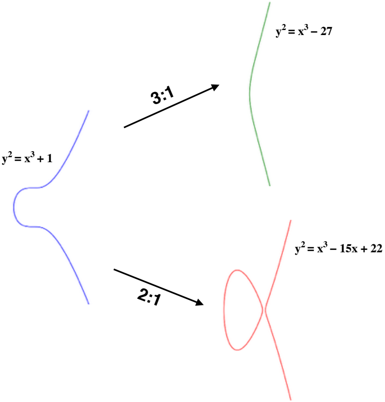
- Q: When can we construct a 'nice' map between 2 abelian varieties?
- A: Take an abelian variety A. Then given an algebraic integer μ (of the right degree) such that
  - μ is real, and
  - μ is totally positive,

  we can construct an abelian variety A' and a map to it called a *μ-isogeny*.

Two μ-isogenies of algebraic curves of degree 3



Two μ-isogenies of algebraic curves of degree 3



These maps are explicit, for example the top map is:

$$(x, y) \mapsto \left(\frac{x^3 + 4}{x^2}, \frac{x^3 y - 8y}{x^3} \right).$$

Playing with algebraic curves

- The Jacobian of a curve contains the curve.
- Jacobians of algebraic curves are examples of abelian varieties.
- In some cases we can construct a map between abelian varieties called a μ-isogeny.

Playing with algebraic curves

- The Jacobian of a curve contains the curve.
- Jacobians of algebraic curves are examples of abelian varieties.
- In some cases we can construct a map between abelian varieties called a μ-isogeny.

Definition

A *μ-isogeny graph* over $\mathbb{F}_p$ is a graph with

Playing with algebraic curves

- The Jacobian of a curve contains the curve.
- Jacobians of algebraic curves are examples of abelian varieties.
- In some cases we can construct a map between abelian varieties called a μ-isogeny.

Definition

A *μ-isogeny graph* over $\mathbb{F}_p$ is a graph with

- vertices given by abelian varieties over $\mathbb{F}_p$

Playing with algebraic curves

- The Jacobian of a curve contains the curve.
- Jacobians of algebraic curves are examples of abelian varieties.
- In some cases we can construct a map between abelian varieties called a μ-isogeny.

Definition

A *μ-isogeny graph* over $\mathbb{F}_p$ is a graph with

- vertices given by abelian varieties over $\mathbb{F}_p$ (e.g. algebraic curves of degree 3 mod p)

Playing with algebraic curves

- The Jacobian of a curve contains the curve.
- Jacobians of algebraic curves are examples of abelian varieties.
- In some cases we can construct a map between abelian varieties called a μ-isogeny.

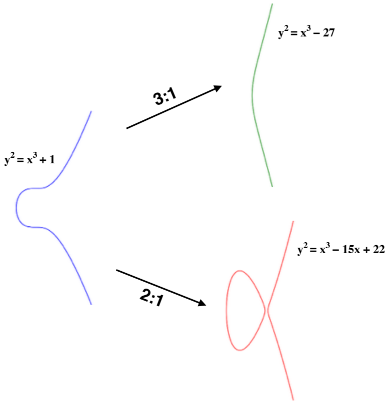
Definition

A *μ-isogeny graph* over $\mathbb{F}_p$ is a graph with

- vertices given by abelian varieties over $\mathbb{F}_p$ (e.g. algebraic curves of degree 3 mod p), and
- edges given by μ-isogenies.

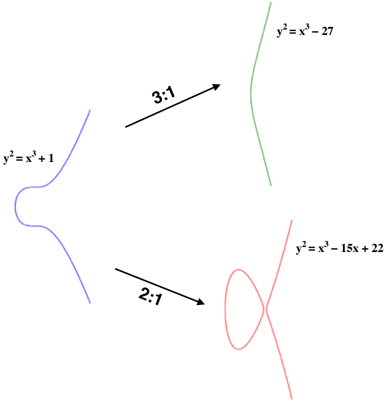
Playing with algebraic curves

Example



Playing with algebraic curves

Example



We can draw a 3-isogeny graph of the top isogeny:

And a 2-isogeny graph of the bottom isogeny:

Playing with algebraic curves

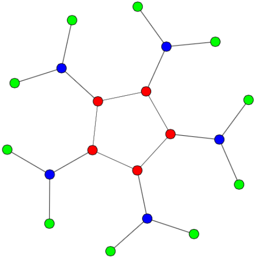
Definition

We define a *volcano graph* to be a symmetric graph that:

Playing with algebraic curves

Definition

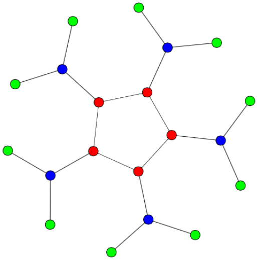
We define a *volcano graph* to be a symmetric graph that:



Playing with algebraic curves

Definition

We define a *volcano graph* to be a symmetric graph that:

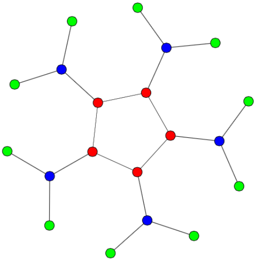


- contains a unique cycle

Playing with algebraic curves

Definition

We define a *volcano graph* to be a symmetric graph that:



- contains a unique cycle, and
- has exactly v edges from every vertex, except for the vertices joined to the cycle by a path of exactly d edges, from which there is exactly 1 edge.

Playing with algebraic curves

Definition

For μ a real totally positive algebraic integer, we define G to be the μ-isogeny graph over $\mathbb{F}_p$ with the maximum number of vertices and edges.

Playing with algebraic curves

Definition

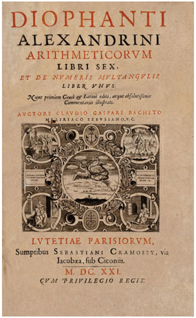
For μ a real totally positive algebraic integer, we define G to be the μ-isogeny graph over $\mathbb{F}_p$ with the maximum number of vertices and edges.

Theorem (Kohel 1996)

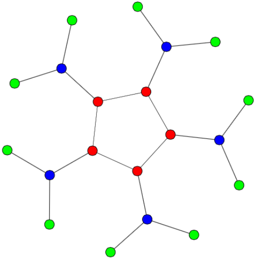
If $\mu \in \mathbb{Z}$, then the connected components of G are volcano graphs.

Theorem (M. 2016)

The connected components of G are volcano graphs.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
LVTETIAE PARISIORVM,
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Thank you!



Future research plans

- In my thesis, we see how to ‘walk around’ these graphs

Future research plans

- In my thesis, we see how to ‘walk around’ these graphs
- Starting point for many projects extending ideas for degree 3

Future research plans

- In my thesis, we see how to ‘walk around’ these graphs
- Starting point for many projects extending ideas for degree 3, for example
  - Work in progress: counting points on algebraic curves of degree 5 and 6

Future research plans

- In my thesis, we see how to 'walk around' these graphs
- Starting point for many projects extending ideas for degree 3, for example
  - Work in progress: counting points on algebraic curves of degree 5 and 6
  - Construction of elliptic units for algebraic curves of degree 5 and 6 (and higher?)

Future research plans

- In my thesis, we see how to 'walk around' these graphs
- Starting point for many projects extending ideas for degree 3, for example
  - Work in progress: counting points on algebraic curves of degree 5 and 6
  - Construction of elliptic units for algebraic curves of degree 5 and 6 (and higher?)
- Explicit descent via μ-isogeny