

Some elliptic curves from the real world

Bas Edixhoven

Universiteit Leiden

2015/06/18

mathematics colloquium Luxembourg
and the conference

Frontiers in Serre's modularity conjecture"

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),
- classical mechanics (Euler),

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),
- classical mechanics (Euler),
- Bitcoin,

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),
- classical mechanics (Euler),
- Bitcoin,
- the Guggenheim museum in Bilbao (minimal art, Richard Serra).

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),
- classical mechanics (Euler),
- Bitcoin,
- the Guggenheim museum in Bilbao (minimal art, Richard Serra).

The first four examples are well known, but the last one appears to be new.

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in:

- plane geometry (Poncelet),
- Escher's "Print Gallery" (de Smit and Lenstra),
- classical mechanics (Euler),
- Bitcoin,
- the Guggenheim museum in Bilbao (minimal art, Richard Serra).

The first four examples are well known, but the last one appears to be new.

These notes can be downloaded from my homepage (talks/...).

Real Elliptic curves in Weierstrass form

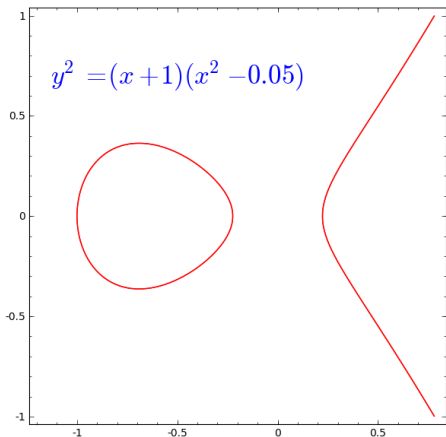
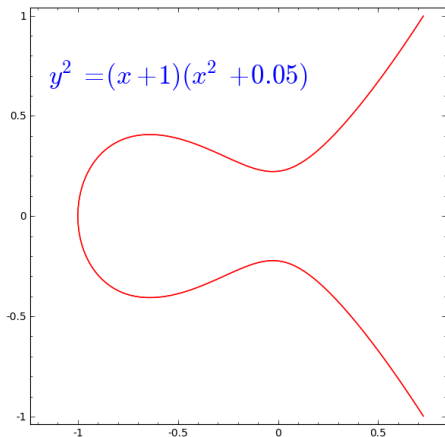
For $a, b \in \mathbb{R}$ with $4a^3 + 27b^2 \neq 0$:

$$\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\}.$$

Real Elliptic curves in Weierstrass form

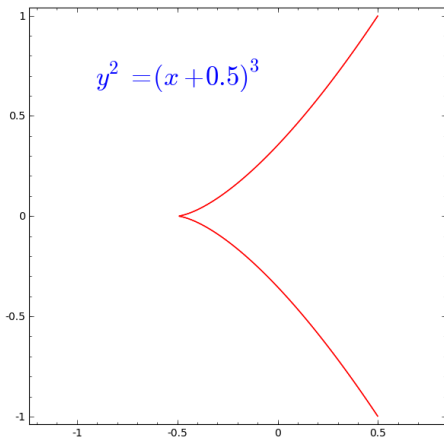
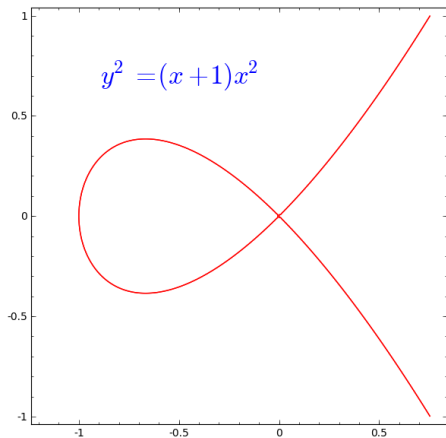
For $a, b \in \mathbb{R}$ with $4a^3 + 27b^2 \neq 0$:

$$\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\}.$$



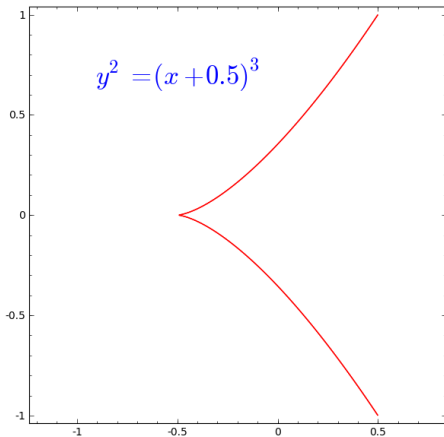
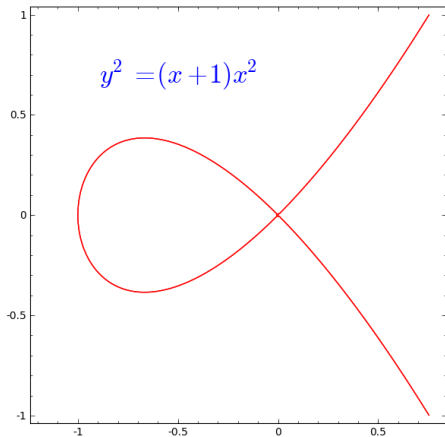
Real Elliptic curves in Weierstrass form

$4a^3 + 27b^2 \neq 0 \Leftrightarrow$ the curve is non-singular.



Real Elliptic curves in Weierstrass form

$4a^3 + 27b^2 \neq 0 \Leftrightarrow$ the curve is non-singular.



All non-singular degree 3 curves in \mathbb{R}^2 can be brought in Weierstrass form by projective transformations.

The algebraic point of view (algebraic geometry)

Closed subvarieties in \mathbb{R}^n : solution sets of systems of polynomial equations.

The algebraic point of view (algebraic geometry)

Closed subvarieties in \mathbb{R}^n : solution sets of systems of polynomial equations.

Maps (morphisms) are “locally” given by rational functions without poles.

The algebraic point of view (algebraic geometry)

Closed subvarieties in \mathbb{R}^n : solution sets of systems of polynomial equations.

Maps (morphisms) are “locally” given by rational functions without poles.

Locally: Zariski topology, the closed subsets are the closed subvarieties.

The algebraic point of view (algebraic geometry)

Closed subvarieties in \mathbb{R}^n : solution sets of systems of polynomial equations.

Maps (morphisms) are “locally” given by rational functions without poles.

Locally: Zariski topology, the closed subsets are the closed subvarieties.

It is often useful to consider $\mathbb{R}^n \subset \mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$: complex projective algebraic geometry.

The algebraic point of view (algebraic geometry)

Closed subvarieties in \mathbb{R}^n : solution sets of systems of polynomial equations.

Maps (morphisms) are “locally” given by rational functions without poles.

Locally: Zariski topology, the closed subsets are the closed subvarieties.

It is often useful to consider $\mathbb{R}^n \subset \mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$: complex projective algebraic geometry.

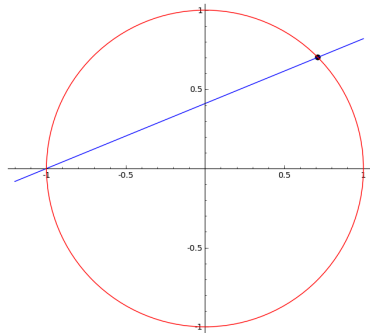
Instead of \mathbb{C} we can use any algebraically closed field, and, in fact, any ring (commutative, with 1).

Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .

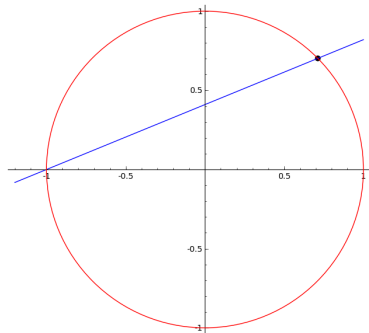
Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .



Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .

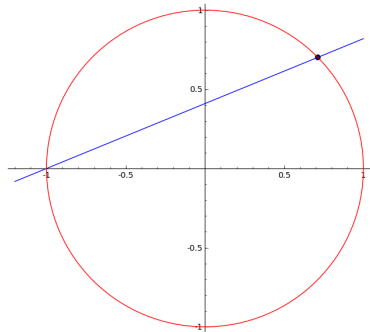


Lines through $(-1, 0)$:

$$y = a \cdot (x + 1).$$

Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .



Lines through $(-1, 0)$:

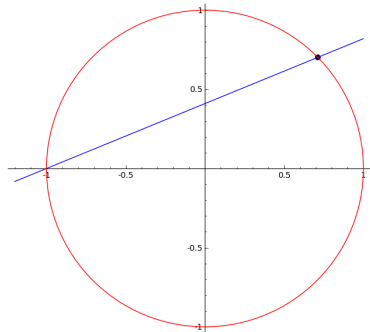
$$y = a \cdot (x + 1).$$

Second intersection point:

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

Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .



Lines through $(-1, 0)$:

$$y = a \cdot (x + 1).$$

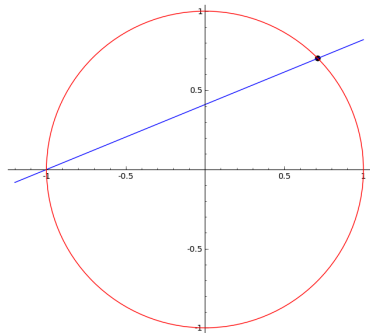
Second intersection point:

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

$$\mathbb{R} \rightarrow \text{circle}, \quad a \mapsto \left(\frac{1 - a^2}{1 + a^2}, \frac{2a}{1 + a^2} \right).$$

Elliptic curves cannot be parametrised

Non-singular degree 2 curves in \mathbb{R}^2 are locally isomorphic to \mathbb{R} .



Lines through $(-1, 0)$:

$$y = a \cdot (x + 1).$$

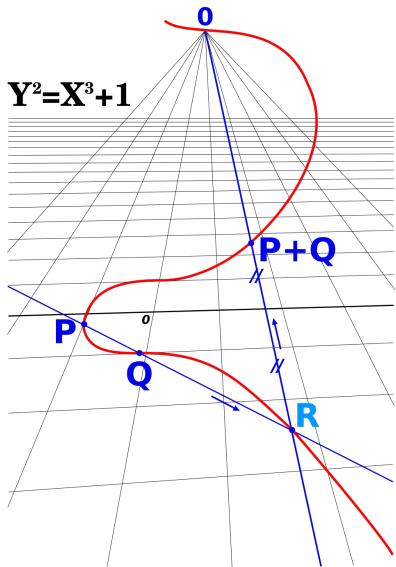
Second intersection point:

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

$$\mathbb{R} \rightarrow \text{circle}, \quad a \mapsto \left(\frac{1 - a^2}{1 + a^2}, \frac{2a}{1 + a^2} \right).$$

Fact: elliptic curves cannot be parametrised, not even locally. Lines intersect them in 1 or 3 points, if we count with multiplicity and use the “projective plane”.

Parallel lines intersect on the horizon: one extra point for each direction in \mathbb{R}^2 .

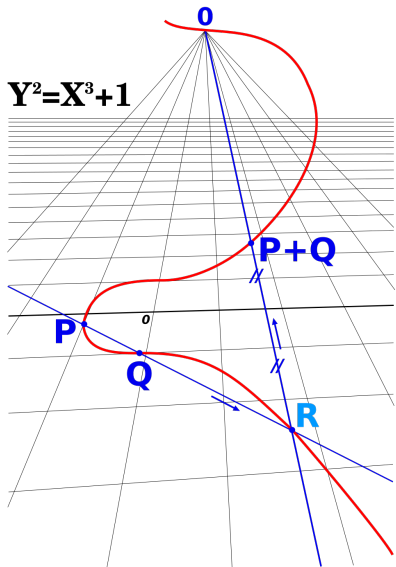


Parallel lines intersect on the horizon: one extra point for each direction in \mathbb{R}^2 .

$E(\mathbb{R})$ has one point “ O ” for the vertical direction.

$E(\mathbb{R})$ (including O) has a *binary operation*:

$$E(\mathbb{R}) \times E(\mathbb{R}) \rightarrow E(\mathbb{R}),$$
$$(P, Q) \mapsto P + Q.$$



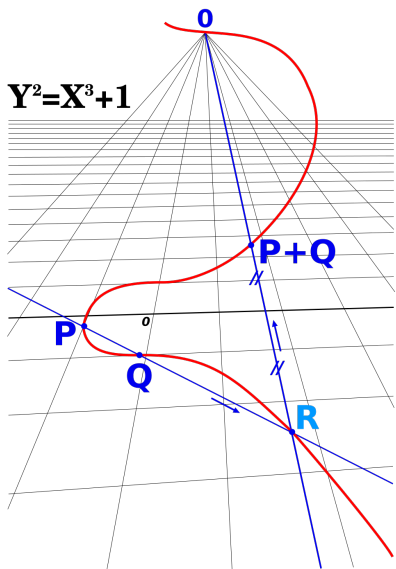
Parallel lines intersect on the horizon: one extra point for each direction in \mathbb{R}^2 .

$E(\mathbb{R})$ has one point “ O ” for the vertical direction.

$E(\mathbb{R})$ (including O) has a *binary operation*:

$$E(\mathbb{R}) \times E(\mathbb{R}) \rightarrow E(\mathbb{R}),$$
$$(P, Q) \mapsto P + Q.$$

This binary operation makes $E(\mathbb{R})$ into *commutative group*. The associativity is not at all obvious.



Parallel lines intersect on the horizon: one extra point for each direction in \mathbb{R}^2 .

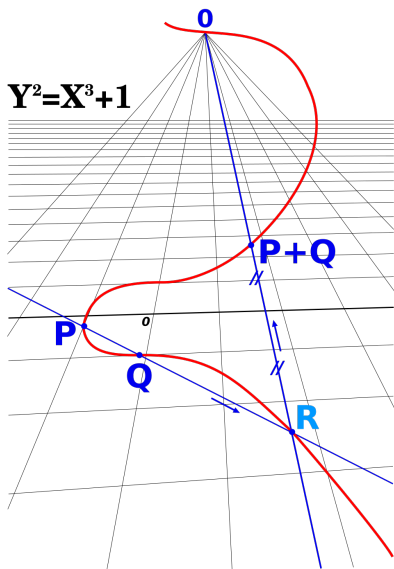
$E(\mathbb{R})$ has one point “ O ” for the vertical direction.

$E(\mathbb{R})$ (including O) has a *binary operation*:

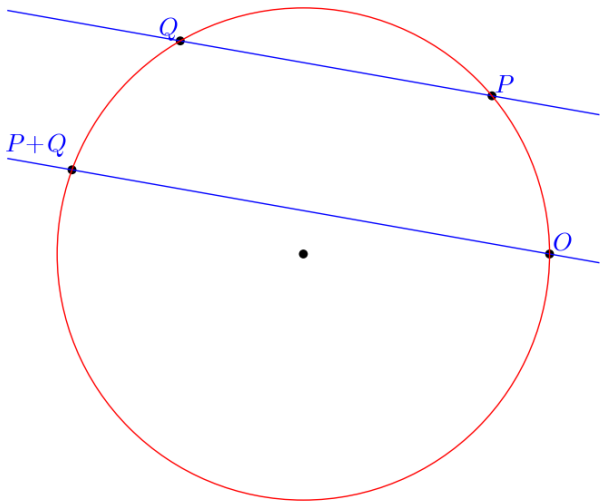
$$E(\mathbb{R}) \times E(\mathbb{R}) \rightarrow E(\mathbb{R}),$$
$$(P, Q) \mapsto P + Q.$$

This binary operation makes $E(\mathbb{R})$ into *commutative group*. The associativity is not at all obvious.

(Picture made by: Jean Brette.)

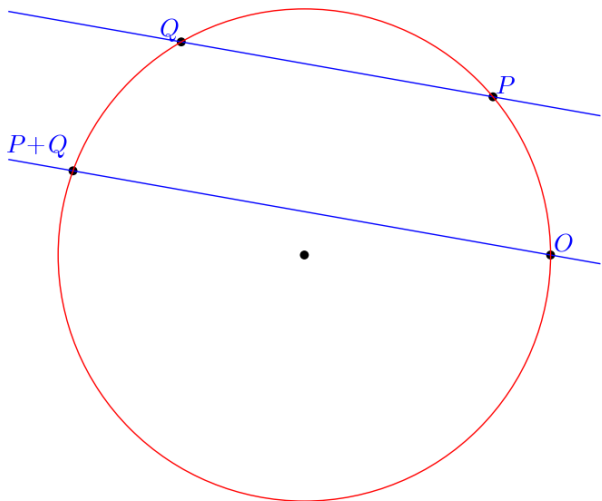


The degenerate case where $E(\mathbb{R})$ is the union of the unit circle and the line at infinity, with $(1, 0)$ as origin.



The degenerate case where $E(\mathbb{R})$ is the union of the unit circle and the line at infinity, with $(1, 0)$ as origin.

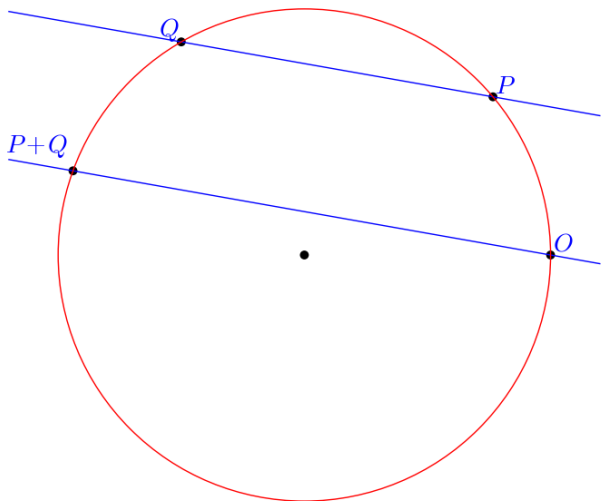
Conclusion: it is addition of angles!



The degenerate case where $E(\mathbb{R})$ is the union of the unit circle and the line at infinity, with $(1, 0)$ as origin.

Conclusion: it is addition of angles!

Hence associative.



Complex elliptic curves, Weierstrass functions

Let $E(\mathbb{C})$ be a complex projective elliptic curve.

Complex elliptic curves, Weierstrass functions

Let $E(\mathbb{C})$ be a complex projective elliptic curve.

Fact: $E(\mathbb{C})$ is homeomorphic to $S^1 \times S^1$, for three reasons.

Complex elliptic curves, Weierstrass functions

Let $E(\mathbb{C})$ be a complex projective elliptic curve.

Fact: $E(\mathbb{C})$ is homeomorphic to $S^1 \times S^1$, for three reasons.

Topology. $E(\mathbb{C})$ is compact, oriented, connected and has a Lie group structure, hence a vector field without zeros, hence (Poincaré-Hopf) its Euler characteristic is zero.

Complex elliptic curves, Weierstrass functions

Let $E(\mathbb{C})$ be a complex projective elliptic curve.

Fact: $E(\mathbb{C})$ is homeomorphic to $S^1 \times S^1$, for three reasons.

Topology. $E(\mathbb{C})$ is compact, oriented, connected and has a Lie group structure, hence a vector field without zeros, hence (Poincaré-Hopf) its Euler characteristic is zero.

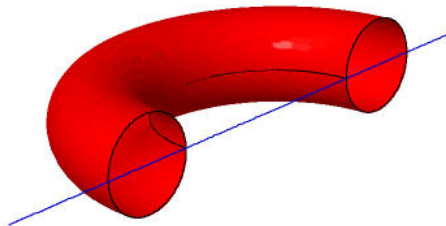
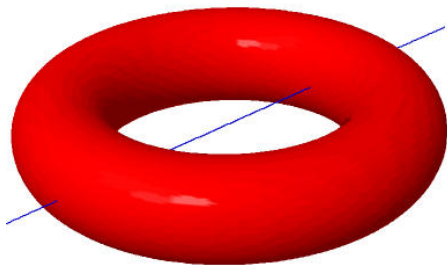
Analysis. Weierstrass functions. Let $L \subset \mathbb{C}$ be a lattice. Then

$$P: \mathbb{C} - L \rightarrow \mathbb{C}, \quad z \mapsto \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

is L -periodic, and $z \mapsto (P(z), P'(z))$ gives $\mathbb{C}/L \rightarrow E_L(\mathbb{C})$.

Elliptic curves as double cover of \mathbb{P}^1

Riemann surfaces. $E(\mathbb{C}) \rightarrow \mathbb{P}^1(\mathbb{C}), (x, y) \mapsto x$ is a 2 to 1 map with 4 ramification points. It is the quotient map for a rotation about 180° .



Automorphisms of elliptic curves

The group of translations acts transitively: all points are equal.

Automorphisms of elliptic curves

The group of translations acts transitively: all points are equal.

Fixing O : automorphisms of E as algebraic group.

Automorphisms of elliptic curves

The group of translations acts transitively: all points are equal.

Fixing O : automorphisms of E as algebraic group.

$\text{Aut}(E, O)$ is cyclic of order 2, 4, or 6: symmetries of 2-dimensional lattices.

Automorphisms of elliptic curves

The group of translations acts transitively: all points are equal.

Fixing O : automorphisms of E as algebraic group.

$\text{Aut}(E, O)$ is cyclic of order 2, 4, or 6: symmetries of 2-dimensional lattices.

$$\text{Aut}(E) = (E, +) \rtimes \text{Aut}(E, O).$$

Automorphisms of elliptic curves

The group of translations acts transitively: all points are equal.

Fixing O : automorphisms of E as algebraic group.

$\text{Aut}(E, O)$ is cyclic of order 2, 4, or 6: symmetries of 2-dimensional lattices.

$$\text{Aut}(E) = (E, +) \rtimes \text{Aut}(E, O).$$

These are affine transformations: $P \mapsto a(P) + B$, with a in $\text{Aut}(E, O)$ and B in E .

Jean-Victor Poncelet (1788–1867) was a French engineer and mathematician who served most notably as the commandant general of the École polytechnique. He is considered a reviver of projective geometry, and his work “*Traité des propriétés projectives des figures*” is considered the first definitive paper on the subject since Gérard Desargues’ work on it in the 17th century.

Source: wikipedia.



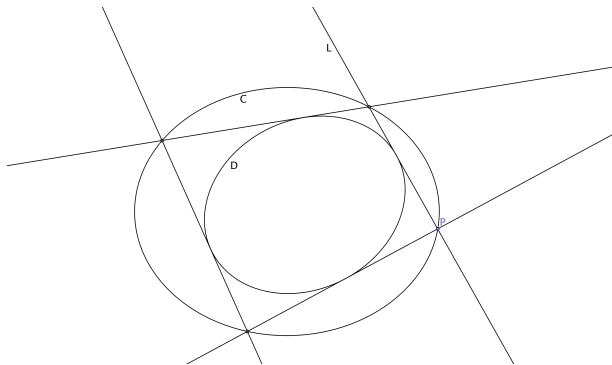
Poncelet's closure theorem, 1822

Let C and D be two plane conics. If it is possible to find, for a given $n > 2$, one n -sided polygon that is simultaneously inscribed in C and circumscribed around D , then it is possible to find infinitely many of them.

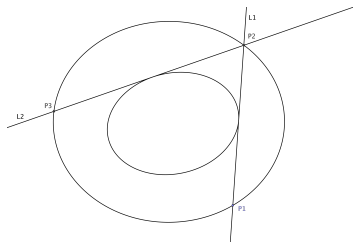
Poncelet's closure theorem, 1822

Let C and D be two plane conics. If it is possible to find, for a given $n > 2$, one n -sided polygon that is simultaneously inscribed in C and circumscribed around D , then it is possible to find infinitely many of them.

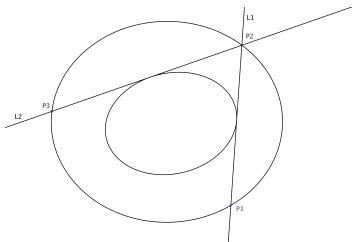
In fact, the construction “moves”: one can move the starting point on C anywhere.



Proof of Poncelet's closure theorem ("Jacobi", 1826)

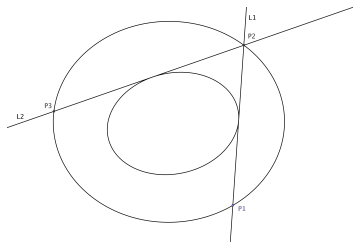


Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}.$

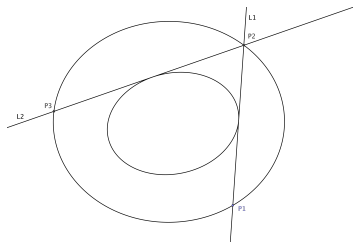
Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}$.

$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$.

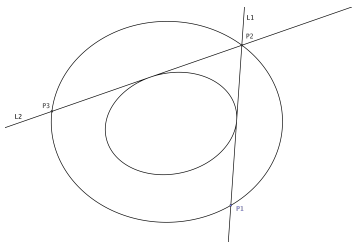
Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}.$

$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere.

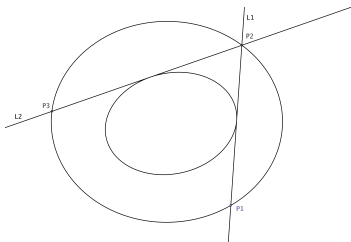
Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}$.

$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere. Hence X is an elliptic curve.

Proof of Poncelet's closure theorem ("Jacobi", 1826)

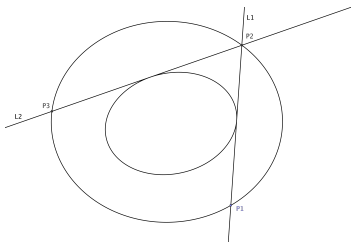


$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}.$

$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere. Hence X is an elliptic curve.

Two involutions: $L \cap C = \{P, P'\}$, $\sigma: (P, L) \mapsto (P', L)$,
 L and L' tangents through P , $\tau: (P, L) \mapsto (P, L')$.

Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}.$

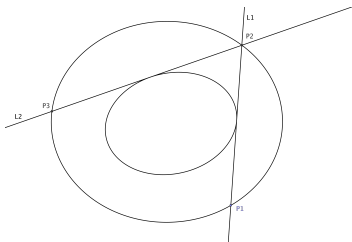
$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere. Hence X is an elliptic curve.

Two involutions: $L \cap C = \{P, P'\}$, $\sigma: (P, L) \mapsto (P', L)$,

L and L' tangents through P , $\tau: (P, L) \mapsto (P, L')$.

In terms of group law: $\sigma(x) = -x + b$, $\tau(x) = -x + c$ for some b and c on X .

Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}.$

$X \rightarrow C, (P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere. Hence X is an elliptic curve.

Two involutions: $L \cap C = \{P, P'\}$, $\sigma: (P, L) \mapsto (P', L)$,
 L and L' tangents through P , $\tau: (P, L) \mapsto (P, L')$.

In terms of group law: $\sigma(x) = -x + b$, $\tau(x) = -x + c$ for some b and c on X . Hence $(\tau \circ \sigma)x = x + (c - b)$, a translation. That explains all.

- 1 If the two ellipses are confocal, then the dynamical system is really an elliptic billiard, with the usual rule of reflection.

- 1 If the two ellipses are confocal, then the dynamical system is really an elliptic billiard, with the usual rule of reflection.
- 2 Bos, Kes, Oort and Raven have written an article on historical aspects: *Poncelet's closure theorem*.

- 1 If the two ellipses are confocal, then the dynamical system is really an elliptic billiard, with the usual rule of reflection.
- 2 Bos, Kes, Oort and Raven have written an article on historical aspects: *Poncelet's closure theorem*.
- 3 Duistermaat has written a whole book on such dynamical systems: *Discrete Integrable Systems, QRT maps and Elliptic Surfaces*.

Classical mechanics: free rotation of a rigid body

At each moment t there is an axis of rotation a .

Classical mechanics: free rotation of a rigid body

At each moment t there is an axis of rotation a .

The movement of this axis with respect to a coordinate system that moves with the body is described by:

Classical mechanics: free rotation of a rigid body

At each moment t there is an axis of rotation a .

The movement of this axis with respect to a coordinate system that moves with the body is described by:

$$\begin{cases} I_1 \dot{a}_1 = (I_2 - I_3) a_2 a_3 \\ I_2 \dot{a}_2 = (I_3 - I_1) a_3 a_1, \\ I_3 \dot{a}_3 = (I_1 - I_2) a_1 a_2 \end{cases} \quad I_1, I_2 \text{ and } I_3 \text{ the moments of inertia.}$$

Classical mechanics: free rotation of a rigid body

At each moment t there is an axis of rotation a .

The movement of this axis with respect to a coordinate system that moves with the body is described by:

$$\begin{cases} l_1 \dot{a}_1 = (l_2 - l_3) a_2 a_3 \\ l_2 \dot{a}_2 = (l_3 - l_1) a_3 a_1, & l_1, l_2 \text{ and } l_3 \text{ the moments of inertia.} \\ l_3 \dot{a}_3 = (l_1 - l_2) a_1 a_2 \end{cases}$$

Two conserved quantities:

$$l_1 a_1^2 + l_2 a_2^2 + l_3 a_3^2, \quad \text{kinetic energy,}$$

$$l_1^2 a_1^2 + l_2^2 a_2^2 + l_3^2 a_3^2, \quad \text{length squared of angular momentum.}$$

Classical mechanics: free rotation of a rigid body

At each moment t there is an axis of rotation a .

The movement of this axis with respect to a coordinate system that moves with the body is described by:

$$\begin{cases} l_1 \dot{a}_1 = (l_2 - l_3) a_2 a_3 \\ l_2 \dot{a}_2 = (l_3 - l_1) a_3 a_1, & l_1, l_2 \text{ and } l_3 \text{ the moments of inertia.} \\ l_3 \dot{a}_3 = (l_1 - l_2) a_1 a_2 \end{cases}$$

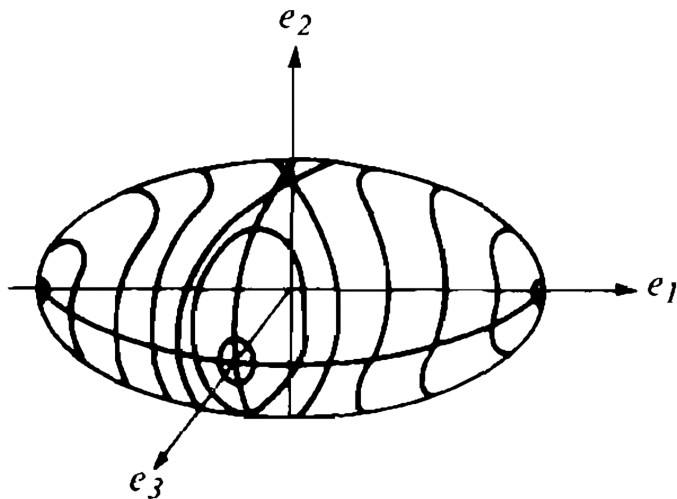
Two conserved quantities:

$$l_1 a_1^2 + l_2 a_2^2 + l_3 a_3^2, \quad \text{kinetic energy,}$$

$$l_1^2 a_1^2 + l_2^2 a_2^2 + l_3^2 a_3^2, \quad \text{length squared of angular momentum.}$$

So the movement is over the intersection of the level surfaces: elliptic curves! Indeed, complex projectively, the first quadric is $\mathbb{P}^1 \times \mathbb{P}^1$, and the intersection with the second quadric is a $(2, 2)$ -curve! So, same situation as with Poncelet.

Intersections of 2 ellipsoids, one fixed



Picture from V.A. Arnold's book "Math. Methods of Class. Mech."

- The vector field on these curves is translation invariant. The group given by the flow *is* the addition law, it is algebraic!

Remarks

- The vector field on these curves is translation invariant. The group given by the flow *is* the addition law, it is algebraic!
- All rotations of the plane that fix the origin are linear maps, hence algebraic. But for the parametrisation of rotation with constant speed one needs sin and cos. That flow is not algebraic.

- The vector field on these curves is translation invariant. The group given by the flow *is* the addition law, it is algebraic!
- All rotations of the plane that fix the origin are linear maps, hence algebraic. But for the parametrisation of rotation with constant speed one needs sin and cos. That flow is not algebraic.
- Explicit solutions for rotation of a rigid body involve Weierstrass functions, or other functions parametrising elliptic curves. That flow is also not algebraic.

- The vector field on these curves is translation invariant. The group given by the flow *is* the addition law, it is algebraic!
- All rotations of the plane that fix the origin are linear maps, hence algebraic. But for the parametrisation of rotation with constant speed one needs sin and cos. That flow is not algebraic.
- Explicit solutions for rotation of a rigid body involve Weierstrass functions, or other functions parametrising elliptic curves. That flow is also not algebraic.
- To prove that the vector field is translation invariant, it suffices to see that on the projective complex elliptic curves it has no poles. A simple but annoying computation, and it makes the outcome look like a miracle. Conversely, if one knew that the translations by the flow are algebraic, then one could deduce (without computation) that the vector field (on the complex projective curves) has no poles.

Source: <http://escherdroste.math.leidenuniv.nl>



Droste-Escher

Escher's print gallery is a transformed Droste picture: the "straight picture" contains a copy of itself, scaled by $q := 1/256$.



A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f: \mathbb{C}^\times \rightarrow X$, where X is the set of colors.

A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f: \mathbb{C}^\times \rightarrow X$, where X is the set of colors.

The self-similarity is then expressed by:

$$\text{for all } t \text{ in } \mathbb{C}^\times, f(qt) = f(t).$$

A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f: \mathbb{C}^\times \rightarrow X$, where X is the set of colors.

The self-similarity is then expressed by:

$$\text{for all } t \text{ in } \mathbb{C}^\times, f(qt) = f(t).$$

So in fact, f induces a function $\bar{f}: \mathbb{C}^\times / q^{\mathbb{Z}} \rightarrow X$.

A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f: \mathbb{C}^\times \rightarrow X$, where X is the set of colors.

The self-similarity is then expressed by:

$$\text{for all } t \text{ in } \mathbb{C}^\times, f(qt) = f(t).$$

So in fact, f induces a function $\bar{f}: \mathbb{C}^\times / q^{\mathbb{Z}} \rightarrow X$.

The quotient $\mathbb{C}^\times / q^{\mathbb{Z}}$ is a complex elliptic curve:

- 1 The annulus $\{t \in \mathbb{C}^\times : q \leq |t| \leq 1\}$ is a fundamental domain.
- 2 $\exp: \mathbb{C} \rightarrow \mathbb{C}^\times, z \mapsto e^z$ gives $\mathbb{C}^\times = \mathbb{C} / 2\pi i \mathbb{Z}$,
hence $\mathbb{C}^\times / q^{\mathbb{Z}} = \mathbb{C} / (\mathbb{Z} \cdot 2\pi i + \mathbb{Z} \cdot \log(q))$.

A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f: \mathbb{C}^\times \rightarrow X$, where X is the set of colors.

The self-similarity is then expressed by:

$$\text{for all } t \text{ in } \mathbb{C}^\times, f(qt) = f(t).$$

So in fact, f induces a function $\bar{f}: \mathbb{C}^\times / q^{\mathbb{Z}} \rightarrow X$.

The quotient $\mathbb{C}^\times / q^{\mathbb{Z}}$ is a complex elliptic curve:

- 1 The annulus $\{t \in \mathbb{C}^\times : q \leq |t| \leq 1\}$ is a fundamental domain.
- 2 $\exp: \mathbb{C} \rightarrow \mathbb{C}^\times, z \mapsto e^z$ gives $\mathbb{C}^\times = \mathbb{C} / 2\pi i \mathbb{Z}$,
hence $\mathbb{C}^\times / q^{\mathbb{Z}} = \mathbb{C} / (\mathbb{Z} \cdot 2\pi i + \mathbb{Z} \cdot \log(q))$.

So, on \mathbb{C} we have the picture $\tilde{f}: \mathbb{C} \rightarrow X$, invariant under the lattice $\mathbb{Z} \cdot 2\pi i + \mathbb{Z} \cdot \log(q) = \mathbb{Z} \cdot i \cdot 6.283 \dots + \mathbb{Z} \cdot 5.545 \dots$

The lattice-invariant picture on \mathbb{C}



Transforming Droste to Escher

Instead of first dividing out by $\mathbb{Z} \cdot 2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

Transforming Droste to Escher

Instead of first dividing out by $\mathbb{Z} \cdot 2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

So, let $a := 2\pi i / z_1 = 0.5621 \dots + i \cdot 0.4961 \dots$,
and consider $\mathbb{C} \rightarrow \mathbb{C}^\times, z \mapsto \exp(az)$.

Transforming Droste to Escher

Instead of first dividing out by $\mathbb{Z} \cdot 2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

So, let $a := 2\pi i/z_1 = 0.5621 \dots + i \cdot 0.4961 \dots$,
and consider $\mathbb{C} \rightarrow \mathbb{C}^\times, z \mapsto \exp(az)$.

This maps $\mathbb{Z} \cdot z_1$ to 1, and $2\pi i$ to

$q_1 := \exp(2\pi ia) = -0.040946 \dots - i \cdot 0.01685 \dots$, with
 $|q_1| = 1/22.58 \dots$ and $\arg(q_1) = -157.6 \dots^\circ$.

Transforming Droste to Escher

Instead of first dividing out by $\mathbb{Z} \cdot 2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

So, let $a := 2\pi i/z_1 = 0.5621 \dots + i \cdot 0.4961 \dots$,
and consider $\mathbb{C} \rightarrow \mathbb{C}^\times, z \mapsto \exp(az)$.

This maps $\mathbb{Z} \cdot z_1$ to 1, and $2\pi i$ to

$q_1 := \exp(2\pi ia) = -0.040946 \dots - i \cdot 0.01685 \dots$, with
 $|q_1| = 1/22.58 \dots$ and $\arg(q_1) = -157.6 \dots^\circ$.

Conclusion: Escher's picture is obtained by applying the multi-valued transformation $t \mapsto t^a = \exp(a \log(t))$ to the Droste picture, that is:
 $g(t) := f(t^a)$.

Transforming Droste to Escher

Instead of first dividing out by $\mathbb{Z} \cdot 2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

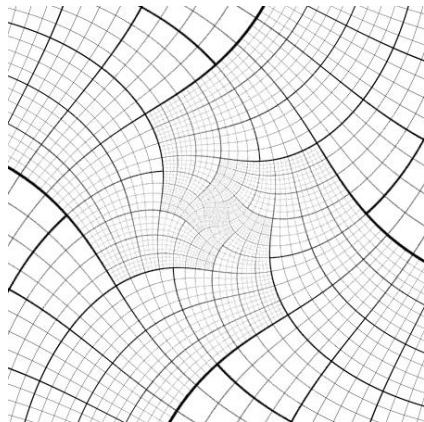
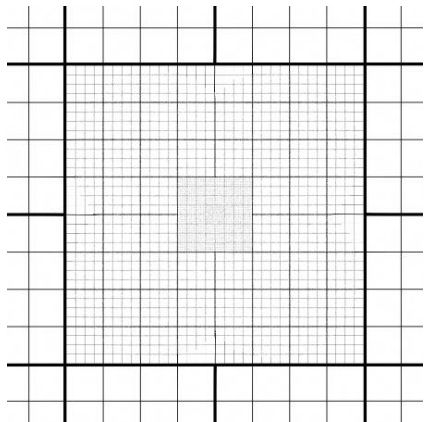
So, let $a := 2\pi i/z_1 = 0.5621 \dots + i \cdot 0.4961 \dots$,
and consider $\mathbb{C} \rightarrow \mathbb{C}^\times$, $z \mapsto \exp(az)$.

This maps $\mathbb{Z} \cdot z_1$ to 1, and $2\pi i$ to

$q_1 := \exp(2\pi ia) = -0.040946 \dots - i \cdot 0.01685 \dots$, with
 $|q_1| = 1/22.58 \dots$ and $\arg(q_1) = -157.6 \dots^\circ$.

Conclusion: Escher's picture is obtained by applying the multi-valued transformation $t \mapsto t^a = \exp(a \log(t))$ to the Droste picture, that is: $g(t) := f(t^a)$. The resulting picture is invariant under $t \mapsto q_1 t$.

The Droste and Escher grids



See the animation

<http://escherdroste.math.leidenuniv.nl/index.php?menu=animation&sub=bmpeg&a=1&b=1>

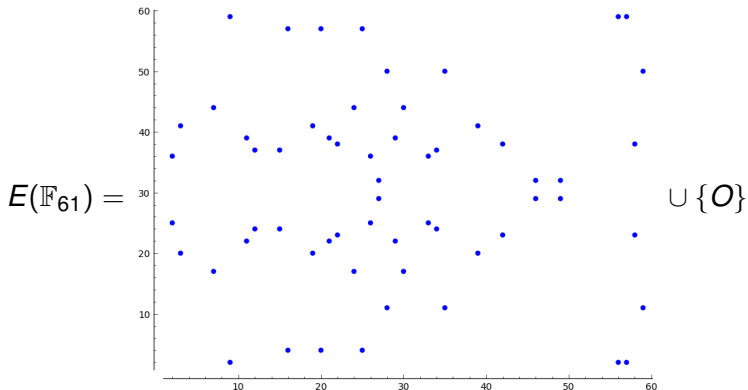
Elliptic curves over finite fields \mathbb{F}_p

For p a prime number and E an elliptic curve $y^2 = x^3 + ax + b$ with a and b in \mathbb{F}_p we have the finite commutative group $E(\mathbb{F}_p)$.

Elliptic curves over finite fields \mathbb{F}_p

For p a prime number and E an elliptic curve $y^2 = x^3 + ax + b$ with a and b in \mathbb{F}_p we have the finite commutative group $E(\mathbb{F}_p)$.

Example: the elliptic curve $y^2 = x^3 + 7$ over \mathbb{F}_{61} :



Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the field \mathbb{F}_p with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the field \mathbb{F}_p with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

$p = 11579208923731619542357098500868790785$
 $3269984665640564039457584007908834671663$.

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the field \mathbb{F}_p with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

$p = 11579208923731619542357098500868790785$
 $3269984665640564039457584007908834671663$.

This is “secp256k1” from the Standards for Efficient Cryptography Group, an international consortium founded in 1998 to develop commercial standards for efficient ECC.

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the field \mathbb{F}_p with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

$$p = 11579208923731619542357098500868790785 \\ 3269984665640564039457584007908834671663.$$

This is “secp256k1” from the Standards for Efficient Cryptography Group, an international consortium founded in 1998 to develop commercial standards for efficient ECC.

$$n := \#E(\mathbb{F}_p) = 11579208923731619542357098500868790785 \\ 2837564279074904382605163141518161494337.$$

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the field \mathbb{F}_p with $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

$$p = 11579208923731619542357098500868790785 \\ 3269984665640564039457584007908834671663.$$

This is “secp256k1” from the Standards for Efficient Cryptography Group, an international consortium founded in 1998 to develop commercial standards for efficient ECC.

$$n := \#E(\mathbb{F}_p) = 11579208923731619542357098500868790785 \\ 2837564279074904382605163141518161494337.$$

This number n is also prime, and that is important.

Richard Serra's "torqued ellipse", Guggenheim, Bilbao



How is this surface made?

Let us watch Serra's explanation in

http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player:
(minutes 16–18).

How is this surface made?

Let us watch Serra's explanation in

http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player:
(minutes 16–18).

So, it is obtained from two ellipses in horizontal planes, one on the ground and one at the top, with their long axes in different directions.

How is this surface made?

Let us watch Serra's explanation in

http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player:
(minutes 16–18).

So, it is obtained from two ellipses in horizontal planes, one on the ground and one at the top, with their long axes in different directions. But Serra did not explain here how the joining is done. The fact however that the side contours of the surfaces are straight lines reveals the joining process.

How is this surface made?

Let us watch Serra's explanation in

http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player:
(minutes 16–18).

So, it is obtained from two ellipses in horizontal planes, one on the ground and one at the top, with their long axes in different directions. But Serra did not explain here how the joining is done. The fact however that the side contours of the surfaces are straight lines reveals the joining process.

Each such side contour corresponds to a plane through our eye. Such a plane “touches” both ellipses. Its intersections with the two horizontal planes containing the ellipses are tangent lines of the ellipses.

How is this surface made?

Let us watch Serra's explanation in

[http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player:](http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player)
(minutes 16–18).

So, it is obtained from two ellipses in horizontal planes, one on the ground and one at the top, with their long axes in different directions. But Serra did not explain here how the joining is done. The fact however that the side contours of the surfaces are straight lines reveals the joining process.

Each such side contour corresponds to a plane through our eye. Such a plane “touches” both ellipses. Its intersections with the two horizontal planes containing the ellipses are tangent lines of the ellipses.

The surface is a part of the boundary of the convex hull of the union of the two ellipses.

How is this surface made?

The surface is the union of lines that join points of the two ellipses where the tangent lines are parallel.

How is this surface made?

The surface is the union of lines that join points of the two ellipses where the tangent lines are parallel.

Serra describes it mechanically:

<http://www.youtube.com/watch?v=G-mBR26bAzA>

Start at 1:35.

How is this surface made?

The surface is the union of lines that join points of the two ellipses where the tangent lines are parallel.

Serra describes it mechanically:

<http://www.youtube.com/watch?v=G-mBR26bAzA>

Start at 1:35.

So he rolls a plane around the ellipses, or rolls his wheel on a sheet of lead.

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

Yes! Well, . . . half.

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

Yes! Well, . . . half.

There is an irreducible F in $\mathbb{R}[x, y, z]$, of degree 8 (I computed this in two ways), such that Serra's surface is half of the zero set of F . I do not know F .

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

Yes! Well, . . . half.

There is an irreducible F in $\mathbb{R}[x, y, z]$, of degree 8 (I computed this in two ways), such that Serra's surface is half of the zero set of F . I do not know F .

The other half consists of lines joining a point below to the “opposite” of the point above: opposite points have parallel tangents.

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

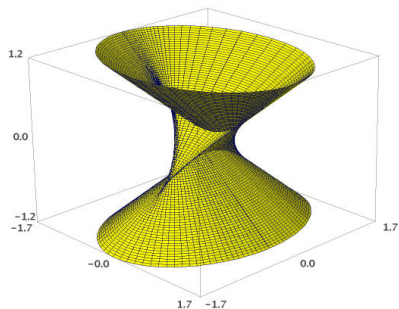
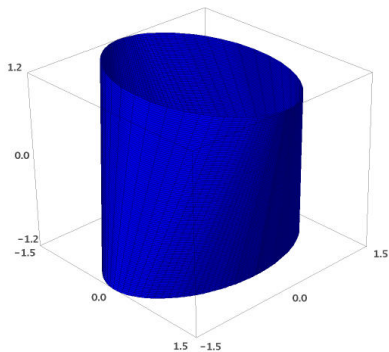
Yes! Well, . . . half.

There is an irreducible F in $\mathbb{R}[x, y, z]$, of degree 8 (I computed this in two ways), such that Serra's surface is half of the zero set of F . I do not know F .

The other half consists of lines joining a point below to the “opposite” of the point above: opposite points have parallel tangents.

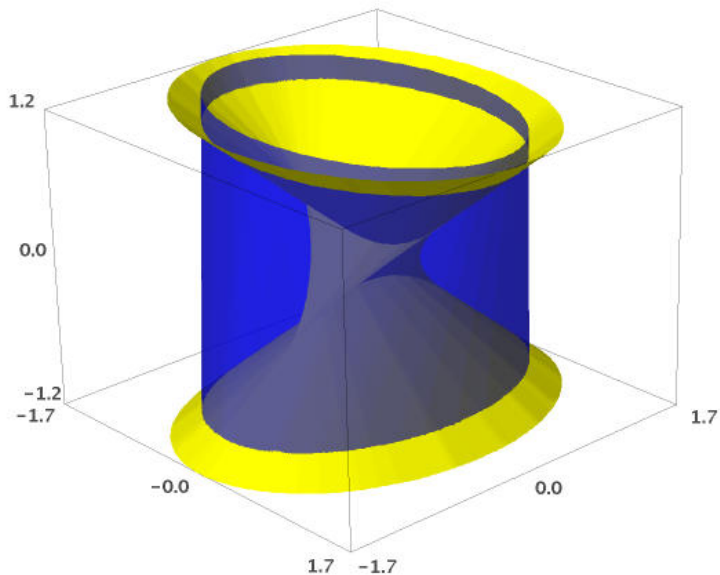
These two halves cannot be separated algebraically, Serra's surface has a siamese twin.

Siamese twins, apart



Pictures and computations by sage.

Siamese twins, together



Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L, \{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.

Hence $E \rightarrow C_i$ is of degree 2, and ramifies over 4 points. Q.E.D.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.

Hence $E \rightarrow C_i$ is of degree 2, and ramifies over 4 points. Q.E.D.

$E(\mathbb{R})$ is homeomorphic to $S^1 \amalg S^1$.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.

Hence $E \rightarrow C_i$ is of degree 2, and ramifies over 4 points. Q.E.D.

$E(\mathbb{R})$ is homeomorphic to $S^1 \amalg S^1$.

Serra's surface S is parametrised by a \mathbb{P}^1 -bundle over E , in fact by $\mathbb{P}^1 \times E$.

Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2 .

For P_i on C_i , let $T_{C_i}(P_i)$ be the tangent of C_i at P_i .

Then $E := \{(P_1, P_2) : P_1 \in C_1, P_2 \in C_2, T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.

Then we have $p_i: C_i \rightarrow L$, $\{p_i(P_i)\} = L \cap T_{C_i}(P_i)$,

p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.

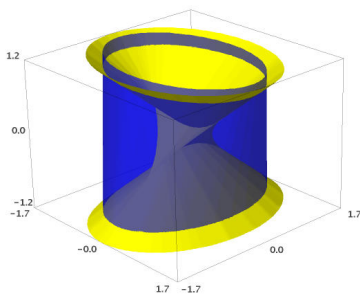
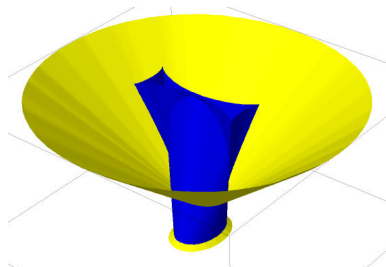
Hence $E \rightarrow C_i$ is of degree 2, and ramifies over 4 points. Q.E.D.

$E(\mathbb{R})$ is homeomorphic to $S^1 \amalg S^1$.

Serra's surface S is parametrised by a \mathbb{P}^1 -bundle over E , in fact by $\mathbb{P}^1 \times E$.

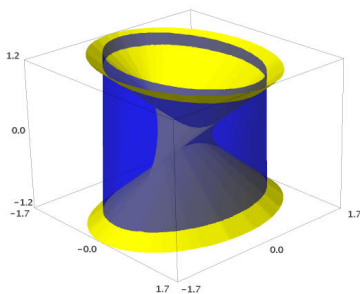
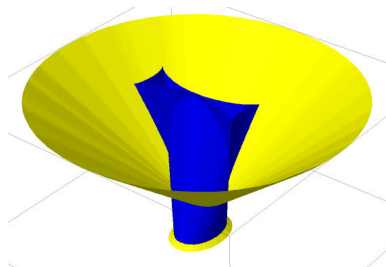
In technical terms: the normalisation is $\mathbb{P}^1 \times E$.

Some more pictures, and an automorphism



The singularities suggest that there is an automorphism of S exchanging blue and yellow.

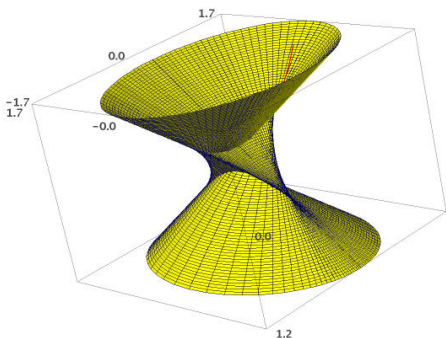
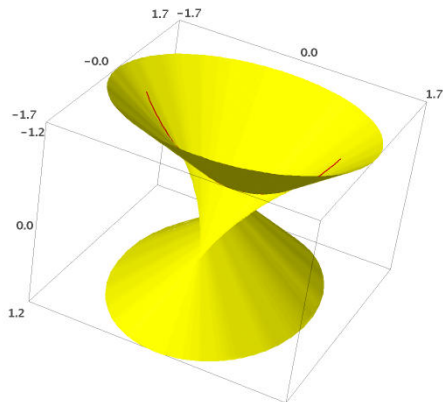
Some more pictures, and an automorphism



The singularities suggest that there is an automorphism of S exchanging blue and yellow.

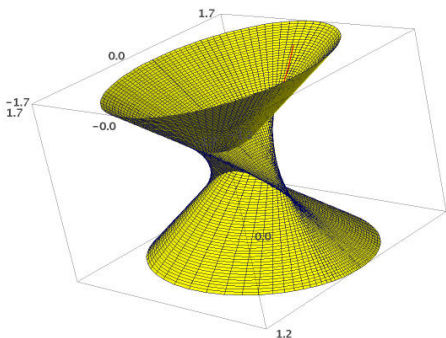
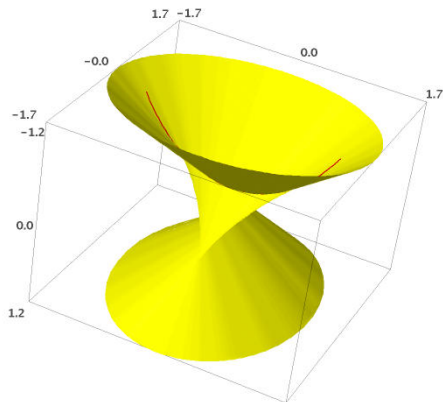
Indeed (Maarten Derickx): the reflection in \mathbb{P}^3 with respect to the plane H_1 and the center of C_2 does this.

A one-dimensional part of $S(\mathbb{R})$



The red ellipse is part of $S(\mathbb{R})$! Only a segment of it is in the yellow part.

A one-dimensional part of $S(\mathbb{R})$



The red ellipse is part of $S(\mathbb{R})$! Only a segment of it is in the yellow part.

It is explained by conjugate intersecting lines.

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally a boundary of their convex hull, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally a boundary of their convex hull, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Minding's theorem (1839) says that locally, the surface is isometric to the plane.

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally a boundary of their convex hull, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Minding's theorem (1839) says that locally, the surface is isometric to the plane.

Intuitively this means: the surface can roll on the plane, giving a mathematical explanation of Serra's wheel.

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally a boundary of their convex hull, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Minding's theorem (1839) says that locally, the surface is isometric to the plane.

Intuitively this means: the surface can roll on the plane, giving a mathematical explanation of Serra's wheel.

The yellow part is obtained by letting one ellipsis roll on top of the paper, and the other below it!

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally a boundary of their convex hull, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Minding's theorem (1839) says that locally, the surface is isometric to the plane.

Intuitively this means: the surface can roll on the plane, giving a mathematical explanation of Serra's wheel.

The yellow part is obtained by letting one ellipsis roll on top of the paper, and the other below it!

Hard to imagine, but we can imagine the case of two circles, giving a cone. The cone can roll on the plane.

Oliver Labs is a mathematician in Mainz, with an interest in computer science and design.

He converted my Sage output to input for a 3d-printer, so that I could have it printed by Shapeways.

Check it out!

<http://www.oliverlabs.net/>

<http://www.shapeways.com/art/mathematical-art?li=nav>

Thanks

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.
- Thanks to Ton Van de Ven for quite a few conversations about Serra's work.

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.
- Thanks to Ton Van de Ven for quite a few conversations about Serra's work.
- To Maarten Derickx for the automorphism exchanging Serra's surface and its twin.

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.
- Thanks to Ton Van de Ven for quite a few conversations about Serra's work.
- To Maarten Derickx for the automorphism exchanging Serra's surface and its twin.
- To Oliver Labs for 3d-printing it from my sage output.

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.
- Thanks to Ton Van de Ven for quite a few conversations about Serra's work.
- To Maarten Derickx for the automorphism exchanging Serra's surface and its twin.
- To Oliver Labs for 3d-printing it from my sage output.
- To you for your attention!