CIMPA School January 2023

http://www.rnta.eu/Manila2022/

University of the Philippines
Diliman, Manila

Introduction to Galois Representations and Modular Forms and their Computational Aspects

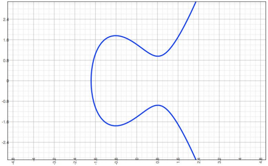
Elliptic curves with complex multiplication.

Michel Waldschmidt

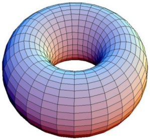
Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

http://www.imj-prg.fr/~michel.waldschmidt/

Which one is an elliptic curve?



Answer $\boxed{1}$



Answer $\boxed{2}$

$$\boxed{y^2 = 4x^3 - 4x}$$

Answer $\boxed{3}$

Right answer: a subset of $\{\boxed{1}, \boxed{2}, \boxed{3}\}$.

René Magritte: la trahison des images (1928–1929)

Left-right reversal illusion

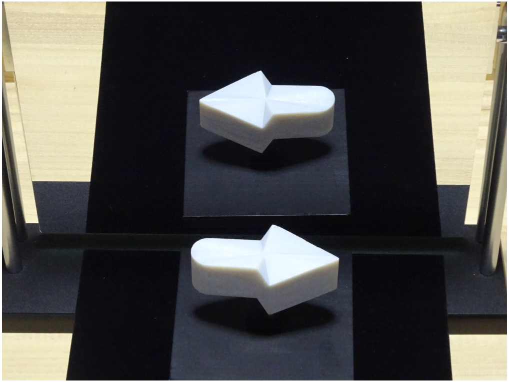
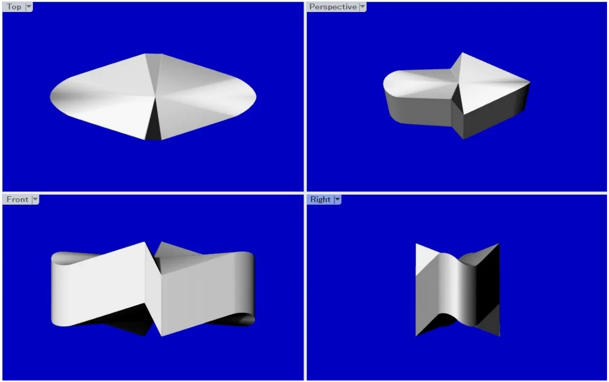


Figure 1. Arrow that changes direction when seen in a mirror.

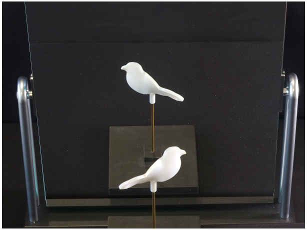
Kokichi Sugihara, Left-right reversal illusion.
Eur. Math. Soc. Mag. **125** (2022), pp. 13–19.
https://doi.org/10.4171/MAG/96

Left-right reversal illusion (2)



Computer graphics images of the object in Figure 1.

Left-right reversal illusion (3)



Object and its mirror image

Front view

Side view

https://en.wikipedia.org/wiki/Elliptic_curve

In mathematics, an elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is defined over a field K and describes points in K^2. If the field's characteristic is different from 2 and 3, then the curve can be described as a plane algebraic curve which consists of solutions (x, y) for:

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

for some coefficients a and b in K.

The curve is required to be non-singular, which means that the curve has no cusps or self-intersections. (This is equivalent to the condition $4a^3 + 27b^2 \neq 0$, that is, being square-free in x.)

It is always understood that the curve is really sitting in the projective plane, with the point O being the unique point at infinity.

https://mathworld.wolfram.com/EllipticCurve.html

Informally, an elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus. The Weierstrass elliptic function $P(z; g_2, g_3)$ describes how to get from this torus to the algebraic form of an elliptic curve.

Formally, an elliptic curve over a field K is a nonsingular cubic curve in two variables, $f(X, Y) = 0$, with a K-rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers $\mathbb{C}$, reals $\mathbb{R}$, rationals $\mathbb{Q}$, algebraic extensions of $\mathbb{Q}$, p-adic numbers $\mathbb{Q}_p$, or a finite field.

Lawrence C. Washington

Elliptic Curves: Number Theory and Cryptography, Second Edition (Discrete Mathematics and Its Applications) 2008

https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/EllipticCurvesNumberTheoryAndCryptography2n.pdf

Chapter 2 The basic theory

For most situations in this book, an **elliptic curve** E is the graph of an equation of the form

$$y^2 = x^3 + Ax + B$$

where A and B are constant. This will be referred to as the **Weierstrass equation** for an elliptic curve.

If K is a field and $A, B \in K$, then we will say that E is **defined over** K.

If we want to consider points with coordinates in some field $L \subset K$, we write $E(L)$.

Henri Cohen

A Course in Computational Algebraic Number Theory.
Graduate Texts in Mathematics, Springer (1993).
https://www.math.u-bordeaux.fr/~hecohen
Chapter V Elliptic curves.

An elliptic curve can be defined as a smooth projective curve of degree 3 in the projective plane, with a point which is the origine: then the set of points has a group structure. A more concrete definition arises from the fact that one can write the affine equation in the form

$$y^2 = x^3 + ax + b \quad \text{with} \quad 4a^3 + 27b^2 \neq 0.$$

Christophe Ritzenthaler.

Introduction to elliptic curves.

https://perso.univ-rennes1.fr/christophe.ritzenthaler/cours/elliptic-curve-course.pdf

Definition 1. A Weierstrass equation of an elliptic curve E over a field K is

$$E : \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$ where Δ is the discriminant of E and is defined as follow

$$\begin{cases} \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ b_2 = a_1^2 + 4a_2, \\ b_4 = 2a_4 + a_1a_3, \\ b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{cases}$$

Definition 2. A (projective) Weierstrass equation of an elliptic curve E over a field K is

$$\tilde{E}: \qquad y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$.

Definition 3. An elliptic curve over a field K is a projective non-singular curve of genus 1 with a K-rational point O.

Other avatars of elliptic curves

1. Quartic equations: $y^2 = f(x)$ with f a degree 4 polynomial without multiple root;
2. Hessian model: $x^3 + y^3 + z^3 = dxyz$;
3. Intersection of quadrics in $\mathbb{P}_3 : x^2 + z^2 = ayt$ and $y^2 + t^2 = axz$;
4. Edwards model: $x^2 + y^2 = 1 + dx^2y^2$.

To keep it simple, we will however often confuse the definition of an elliptic curve and of its (Weierstrass equation) but one has to keep in mind that in general abstract curve $\neq$ a model of a curve $\neq$ an equation of the curve.

https://perso.univ-rennes1.fr/christophe.ritzenthaler/cours/elliptic-curve-course.pdf

Projective plane cubics

$\mathbb{P}_2(K) \ni (x : y : z)$

$$f(x, y, z) = a_{300}x^3 + a_{210}x^2y + a_{120}xy^2 + a_{030}y^3 + a_{201}x^2z + a_{111}xyz + a_{021}y^2z + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3.$$

The generic equation of a projective plane cubic having an inflexion point at $(0 : 1 : 0)$ with tangent $z = 0$ is

$$f(x, y, z) = a_{300}x^3 + a_{201}x^2z + a_{111}xyz + a_{021}y^2z + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3$$

with $a_{300} \neq 0$, $a_{021} \neq 0$.

Projective plane cubics

$$f(x,y,z) = a_{300}x^3 + a_{210}x^2y + a_{120}xy^2 + a_{030}y^3 + \\ a_{201}x^2z + a_{111}xyz + a_{021}y^2z + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3.$$

$$f'_x(x,y,z) = 3a_{300}x^2 + 2a_{210}xy + a_{120}y^2 + 2a_{201}xz + a_{111}yz + a_{102}z^2$$

$$f'_y(x,y,z) = a_{210}x^2 + 2a_{120}xy + 3a_{030}y^2 + a_{111}xz + 2a_{021}yz + a_{012}z^2$$

$$f'_z(x,y,z) = a_{201}x^2 + a_{111}xy + a_{021}y^2 + 2a_{102}xz + 2a_{012}yz + 3a_{003}z^2.$$

$$f(0,1,0) = a_{030},$$

$$f'_x(0,1,0) = a_{120} \quad f'_y(0,1,0) = 3a_{030}, \quad f'_z(0,1,0) = a_{021}.$$

Projective plane cubics passing through $(0:1:0)$

$f(0,1,0) = a_{030} = 0$

Tangent: $xf'_x(0,1,0) + yf'_y(0,1,0) + zf'_z(0,1,0) = 0$

Assume that the tangent at $(0,1,0)$ is $z = 0$:
$f'_x(0,1,0) = f'_y(0,1,0) = 0$, $f'_z(0,1,0) \neq 0$.

$f'_x(0,1,0) = a_{120}$, $f'_y(0,1,0) = 3a_{030}$, $f'_z(0,1,0) = a_{021}$.

Intersection of $z = 0$ with the curve:

$$a_{300}x^3 + a_{210}x^2y + a_{120}xy^2 + a_{030}y^3 = 0$$

Here:

$$(a_{300}x + a_{210}y)x^2 = 0$$

The point $(a_{210} : -a_{300} : 0)$ is on the intersection. Hence $(0:1:0)$ is an inflexion point if and only if $a_{210} = 0$, $a_{300} \neq 0$.

Projective plane cubics

Generic equation of a projective plane cubic with an inflexion point at $(0:1:0)$ with tangent $z=0$:

$$f(x,y,z) = a_{300}x^3 + a_{201}x^2z + a_{111}xyz + a_{021}y^2z + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3$$

with $a_{300} \neq 0$, $a_{021} \neq 0$.

With[1] $a_{300} = 1$, $a_{021} = -1$, setting $a_{ijk} = (-1)^{2k-j} a_{2k-j}$, one gets the equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

[1] Set $z = -a_{300}z'/a_{021}$.

Weierstrass equation

In characteristic $\neq 2$, complete the square by setting

$$Y = y + \frac{1}{2}(a_1 x + a_3).$$

The equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

becomes

$$Y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}.$$

In characteristic $\neq 2$, $\neq 3$, set

$$X = x + \frac{b_2}{12}.$$

The equation becomes

$$Y^2 = X^3 + aX + b.$$

Elliptic curve over a field K

If the coefficients a_i belong to a field K, the elliptic curve is defined over K.

For the Weierstrass model $y^2 = x^3 + ax + b$ with $a_1 = a_2 = a_3 = 0$, $a_4 = a$, $a_6 = b$, we have

$$b_2 = 0, \quad b_4 = 2a, \quad b_6 = 4b, \quad b_8 = -a^2$$

and

$$\Delta = -16(4a^3 + 27b^2).$$

The weight of a_i and b_i is i, of a is 4, of b is 6 and of Δ is 12.

Discriminant

The discriminant of the degree d polynomial

$$a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d = a_0\prod_{i=1}^{d}(x-\alpha_i)$$

is

$$a_0^{2d-2}\prod_{1\le i<j\le d}(\alpha_j-\alpha_i)^2.$$

The cubic polynomial

$$ax^3+bx^2+cx+d$$

has discriminant

$$b^2c^2-4ac^3-4b^3d-27a^2d^2+18abcd\,.$$

For instance the discriminant of the polynomial x^3+ax+b is

$$-4a^3-27b^2\,.$$

Smooth curves

A cubic $y^2z = f(x,z)$ where $f \in K[x,z]$ is homogeneous of degree 3 is smooth if and only if the discriminant of f is not 0.

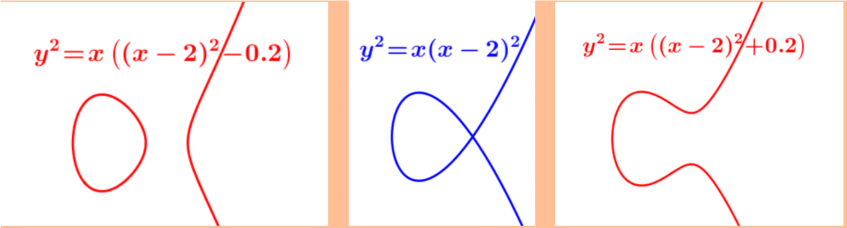
Let $F(x,y,z) = y^2z - f(x,z)$. Assume

$$F(x_0,y_0,z_0) = F'_x(x_0,y_0,z_0) = F'_y(x_0,y_0,z_0) = F'_z(x_0,y_0,z_0) = 0.$$

The condition $F'_y(x_0,y_0,z_0) = 0$, gives $y_0 = 0$, $f(x_0,z_0) = 0$. Then the conditions $f'_x(x_0,z_0) = f'_y(x_0,z_0) = 0$ correspond to a multiple root, hence a vanishing discriminant.

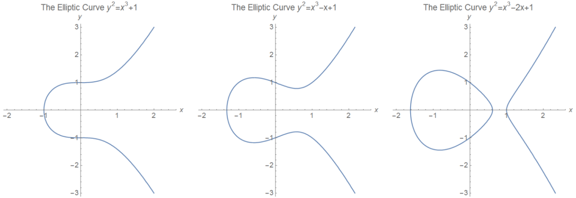
For instance $y^2z = x^3 + axz^2 + bz^3$ is smooth if and only if $4a^3 - 27b^2 \neq 0$.

Three real cubics

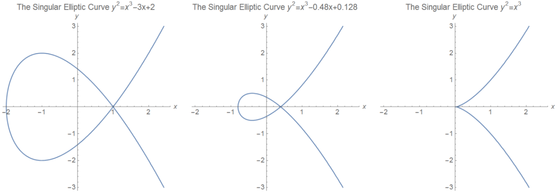


$E(\mathbb{R}) = \{(x : y : t) \in \mathbb{P}_2(\mathbb{R}) \mid y^2 t = 4x^3 - g_2 x t^2 - g_3 t^3\}$.
Point at infinity: $(0 : 1 : 0)$.

Real cubics



- Here are the graphs of the singular elliptic curves $y^2 = x^3 - 3x + 2$, $y^2 = x^3 - 0.48x + 0.128$, and $y^2 = x^3$:



https://web.northeastern.edu/dummit/docs/numthy_7_elliptic_curves.pdf

Non degenerate and degenerate cubics over $\mathbb{R}$

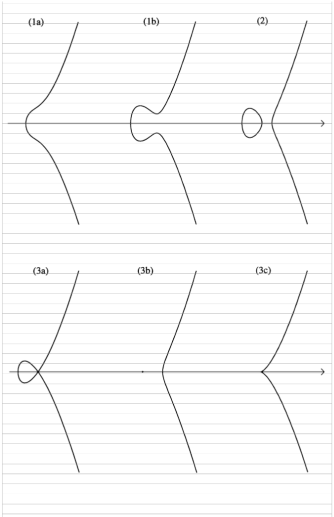


Figure 7.1. Non-Degenerate and Degenerate Elliptic Curves over $\mathbb{R}$.

Henri Cohen. *A course in computational algebraic number theory* § 7.1.4 fig. 7.1.

The group law: chord and tangent

Let $\mathcal{C}$ be a smooth projective plane cubic over an algebraically closed field K.
If P, Q are distinct points on $\mathcal{C}(K)$, the line joining P and Q cuts the cubic in a third point (which may be P or Q), say $P \circ Q \in \mathcal{C}(K)$.
If $P = Q$, let $P \circ P$ be the third point of intersection of the cubic with the tangent to $\mathcal{C}$ at P.
Let O be a point on $\mathcal{C}(K)$. Define

$$P + Q = O \circ (P \circ Q) \quad \text{and} \quad -P = (O \circ O) \circ P.$$

Theorem. *This endows $\mathcal{C}(K)$ of a structure of abelian group with O the neutral element.*

The group law for the Weierstrass model

Let E be the elliptic curve with Weierstrass equation

$$y^2z = x^3 + axz^2 + bz^3.$$

The point $O = (0 : 1 : 0)$ has $O \circ O = O$, $O + O = O$.

For $(x_0 : y_0 : 1)$ on the curve with $y_0 \neq 0$ the line passing through $(x_0 : y_0 : 1)$ and $(x_0 : -y_0 : 1)$ has equation $x = x_0z$ (vertical line) and cuts the curve at O.

Hence $-P$ is the symmetric of P with respect to the real axis.

The group law for the Weierstrass model

Consider the elliptic curve with Weierstrass equation $F(x, y, z) = 0$,

$$F(x, y, z) = y^2 z - x^3 - axz^2 - bz^3.$$

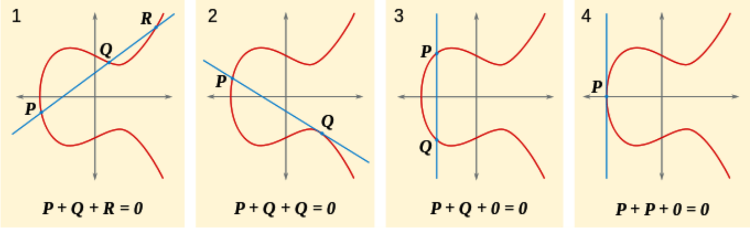
The tangent at a point $(x_0 : 0 : z_0)$ with $x_0^3 + ax_0 z_0^2 + bz_0^3 = 0$ has equation

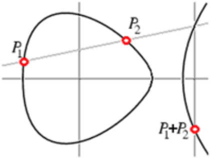
$$xF'_x(x_0, 0, z_0) + yF'_y(x_0, 0, z_0) + zF'_z(x_0, 0, z_0) = 0$$

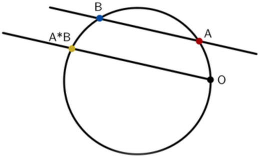
with $F'_y(x_0, 0, z_0) = 0$, hence it is again the vertical line $x = x_0 z$. (Notice that $x_0(3x_0^2 + a) = -(2ax_0 + 3b)$.)

The points P on the curve with $2P = O$ are the three points $(e : 0 : 1)$ with $e^3 + ae + b = 0$.

Chord and tangent





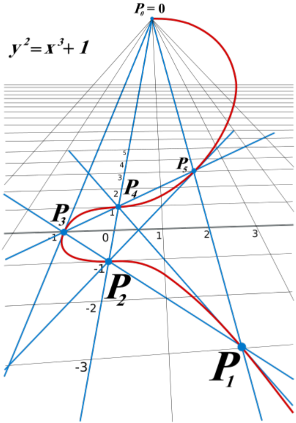


Compare with the group law on the circle.

$y^2 = x^3 + 1$ $\qquad$ $y^2 z = x^3 + z^3$, $O = (0:1:0)$

Rational points :

$P_1 = P = (2, -3)$,
$P_2 = 2P = (0, -1)$,
$P_3 = 3P = (-1, 0)$,
$P_4 = 4P = (0, 1)$,
$P_5 = 5P = (2, 3)$
$P_0 = 6P = O$



https://fr.wikipedia.org/wiki/Courbe_elliptique

The group law for the Weierstrass model

Let E be the elliptic curve with Weierstrass equation

$$y^2 z = x^3 + axz^2 + bz^3$$

with $O = (0:1:0)$.
For $P = (x_0 : y_0 : 1)$, we have $-P = (x_0 : -y_0 : 1)$.
For $P_1 = (x_1 : y_1 : 1)$, $P_2 = (x_2 : y_2 : 1)$ with $P_1 \neq -P_2$, we have $P_1 + P_2 = (x : y : 1)$ with

$$x = \lambda^2 - (x_1 + x_2), \quad y = -\lambda^3 + \lambda(x_1 + x_2) - \mu,$$

where

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_2 = P_1 \\ \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } P_2 \neq P_1 \end{cases}$$

and $\mu = y_1 - \lambda x_1$.

The group law for the Weierstrass model

Proof. Assume first not only $P_1 \neq -P_2$ but also $P_1 \neq P_2$. The point $P_1, P_2, -P$ with $P = P_1 + P_2$ are on a straight line

$$\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x & -y & 1 \end{pmatrix} = 0.$$

$$y_1 = \lambda x_1 + \mu, \quad y_2 = \lambda x_2 + \mu, \quad y = -\lambda x - \mu,$$

with $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$, $\mu = y_1 - \lambda x_1$. The polynomial

$$t^3 + at + b - (\lambda t + \mu)^2$$

has roots x_1, x_2, x, the sum of the roots $x_1 + x_2 + x$ is λ^2.

The group law for the Weierstrass model

Proof (continued). Assume $P_1 = P_2 \neq O$. The equation of the tangent at $P_1 = (x_1 : y_1 : z_1)$ is

$$xF'_x(x_1, y_1, z_1) + yF'_y(x_1, y_1, z_1) + zF'_z(x_1, y_1, z_1) = 0.$$

namely

$$2y_1 z_1 y - (3x_1^2 + az_1)x + 2(y_1^2 - 2ax_1z_1) - 3bz_1^2 = 0.$$

In affine coordinates the equation of the tangent at $P_1 = (x_1 : y_1 : 1)$ is

$$2y_1(y - y_1) - (3x_1^2 + a)(x - x_1) = 0,$$

the slope of which is

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Isomorphisms of elliptic curves

Let E and E' be two elliptic curves with Weierstrass equations

$$y^2 = x^3 + ax + b \quad \text{and} \quad Y^2 = X^3 + a'X + b'.$$

They are called *isomorphic* if there exists a nonzero u with

$$a' = u^4 a, \quad b' = u^6 b.$$

If a, b, a', b' are in a field K and $u \in K^\times$, the two elliptic curves are called *isomorphic over* K.
The map

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (u^2 x, u^3 y) \end{array}$$

is bijective.

x has weight 2, y weight 3, a weight 4, b weight 6.

Isomorphisms of elliptic curves

Let E and E' be two elliptic curves isomorphic over a field K:

$$y^2 = x^3 + ax + b \quad \text{and} \quad Y^2 = X^3 + a'X + b'.$$

Let $u \in K^\times$ satisfy

$$a' = u^4 a, \quad b' = u^6 b.$$

Then the bijective map

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (u^2 x, u^3 y) \end{array}$$

is an isomorphism of algebraic groups.

Torsion points

Over a finite field, all rational points are torsion points.

Over $\mathbb{C}$, the group of torsion points is isomorphic to $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$.

Over a number field, the group of torsion poins is finite.

Over the field of rational numbers, the torsion group has at most 16 elements (B. Mazur).

Let e_1, e_2 and e_3 be the three roots of the polynomial $x^3 + ax + b$ (in an algebraically closure of K):

$$x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3).$$

The three points $Q_i := (e_i : 0 : 1)$ are torsion points of order 2. The group $\{O, Q_1, Q_2, Q_3\}$ is a Klein group of order 4.

Torsion points on an elliptic curve over $\mathbb{Q}$

Theorem (Barry Mazur, 1977). *If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following 15 groups:*

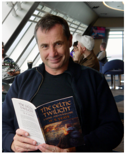
(i) $\mathbb{Z}/n\mathbb{Z}$, with $1 \leq n \leq 10$ or $n = 12$,
(ii) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2m\mathbb{Z})$ with $1 \leq m \leq 4$.

Barry Mazur

The order of $E(\mathbb{Q})_{\mathrm{tors}}$ is ≤ 16.

Torsion points on an elliptic curve over a number field

Merel (1996): the torsion of elliptic curves over number fields is uniformly bounded.



Loïc Merel

https://perso.imj-prg.fr/loic-merel/

Lattices in $\mathbb{C}$

Theorem. *The discrete subgroups of* $\mathbb{C}$ *are*
- $\{0\}$ *(rank* 0*),*
- $\mathbb{Z}\lambda$ *with* $\lambda \neq 0$ *(rank* 1*),*
- $\mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$ *with* (λ_1, λ_2) *a basis of* $\mathbb{C}$ *over* $\mathbb{R}$ *(rank* 2*).*

A *lattice* is a discrete subgroup of $\mathbb{C}$ or rank 2.
Elements of the lattice will be called *periods*.

Primitive or reduced pair of periods

Fundamental pair of periods of a lattice: a basis (λ_1, λ_2) of the $\mathbb{Z}$–module.

Primitive or *reduced* pair of periods: (λ_1, λ_2) with $|\lambda_1|$ minimal among $|\lambda|$, $\lambda \in \Lambda \setminus \{0\}$ and $|\lambda_2|$ minimal among $|\lambda|$, $\lambda \in \Lambda \setminus \mathbb{R}\lambda_1$ and $\mathrm{Im}\, \frac{\lambda_2}{\lambda_1} > 0$.

Theorem. *A primitive pair is fundamental.*

Examples:
$(\mathrm{i}, -1)$ is a pair of primitive periods for the lattice $\mathbb{Z} + \mathbb{Z}\mathrm{i}$,
$(1, 2 + \mathrm{i})$ is a fundamental pair of periods for the same lattice but is not a primitive pair of periods.

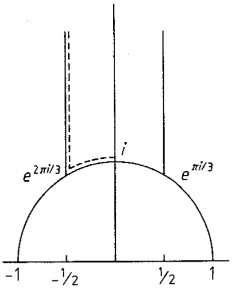
Criterion for a fundamental pair to be primitive

Theorem. *A fundamental pair of periods* (λ_1, λ_2) *is primitive if and only if* $\tau = \lambda_2/\lambda_1$ *satisfies*

$$|\tau| \geq 1, \quad \operatorname{Im} \tau > 0, \quad -\frac{1}{2} \leq \operatorname{Re} \tau \leq \frac{1}{2}.$$

Reference: Chandrasekharan, Chapter I.

Fundamental domain for the modular group



Given a lattice, there exists a pair of fundamental periods (λ_1, λ_2) such that $\tau = \lambda_2/\lambda_1$ satisfies $\mathrm{Im}\,\tau > 0, \quad |\tau| \geq 1,$ $-\frac{1}{2} \leq \mathrm{Re}\,\tau < \frac{1}{2},$ with $\mathrm{Re}\,\tau \leq 0$ if $|\tau| = 1$.

This is a primitive pair of fundamental periods.
If $(\lambda_1^*, \lambda_2^*)$ is an other fundamental pair with $\tau^* = \lambda_2^*/\lambda_1^*$ satisfying these conditions, then $\tau^* = \tau$.

The modular group $\mathrm{SL}_2(\mathbb{Z})$

The subgroup $\mathrm{SL}_2(\mathbb{Z})$ of $\mathrm{GL}_2(\mathbb{Z})$ of matrices of determinant $+1$ is generated by the two elements

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

with the relations

$$S^2 = (ST)^3 = -I.$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \qquad S(\tau) = \frac{-1}{\tau}, \quad T(\tau) = \tau + 1.$$

The subgroup $\{I, S\}$ is the isotropy group of i, while $\{I, ST, (ST)^2\}$ is the isotropy group of $\varrho = \mathrm{e}^{2\pi\mathrm{i}/3}$ and $\{I, TS, (TS)^2\}$ is the isotropy group of $-1/\bar{\varrho} = \mathrm{e}^{\pi\mathrm{i}/3}$.

Reference: J-P. Serre *A course in arithmetic*.

Lattice in $\mathbb{C}$ = discrete subgroup of rank 2

Let G be a discrete subgroup of rank 2 in $\mathbb{C}$. Then there exists a basis (x_1, x_2) of $\mathbb{C}$ over $\mathbb{R}$ such that $G = \mathbb{Z}x_1 + \mathbb{Z}x_2$.

Proof.

By assumption there exists a basis (e_1, e_2) of $\mathbb{C}$ over $\mathbb{R}$ such that $\mathbb{Z}e_1 + \mathbb{Z}e_2 \subset G$.
Let

$$P = \{t_1 e_1 + t_2 e_2 \mid -1 \leq t_1, t_2 \leq 1\}.$$

Then $P \cap G$ is a finite set which generates G as a $\mathbb{Z}$ module and $G \subset \mathbb{Q}e_1 + \mathbb{Q}e_2$.
It follows that there exists $d > 0$ such that G is a subgroup of the free abelian group $G_0 := \mathbb{Z}f_1 + \mathbb{Z}f_2$ with $f_i = e_i/d$.
There is a basis y_1, y_2 of G_0 over $\mathbb{Z}$ and there are two positive integers a_1, a_2 such that a_1 divides a_2, $G_0 = \mathbb{Z}y_1 + \mathbb{Z}y_2$ and $G = \mathbb{Z}x_1 + \mathbb{Z}x_2$ with $x_i = a_i y_i$. $\square$

Lattices in $\mathbb{C}$

Recall: a lattice is a discrete subgroup of $\mathbb{C}$ of maximal rank 2.

The lattices are the subgroups $\mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$ where λ_1, λ_2 is a basis of $\mathbb{C}$ over $\mathbb{R}$.

Examples: $\mathbb{Z} + \mathbb{Z}\mathrm{i}$, $\mathbb{Z} + \mathbb{Z}\mathrm{e}^{2\pi\mathrm{i}/3}$.

Change of basis of a lattice: $\mathrm{GL}_2(\mathbb{Z})$.

$\mathbb{Z} + \mathbb{Z}\mathrm{i} = \mathbb{Z}(a + b\mathrm{i}) + \mathbb{Z}(c + d\mathrm{i})$ when $ad - bc = \pm 1$.

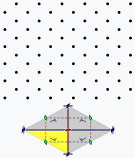
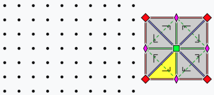
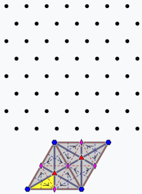
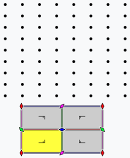
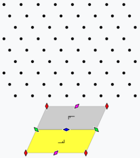
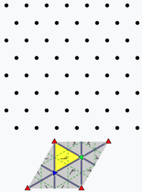
Condition $\operatorname{Im}\tau > 0$: $\det = +1$, $\mathrm{SL}_2(\mathbb{Z})$.

Two main example of lattices

• Let K be an imaginary quadratic number field embedded in $\mathbb{C}$, $\mathcal{R}$ the ring of integers of K.
Any nonzero ideal $\mathfrak{A}$ of $\mathcal{R}$ is a lattice in $\mathbb{C}$.

• Let $\tau \in \mathbb{C} \setminus \mathbb{R}$. Then $\mathbb{Z} + \mathbb{Z}\tau$ is a lattice in $\mathbb{C}$.

Lattices

cmm, (2*22), $[\infty,2^+,\infty]$	p4m, (*442), [4,4]	p6m, (*632), [6,3]
 **rhombic lattice** also **centered rectangular lattice** *isosceles triangular*	 **square lattice** *right isosceles triangular*	 **hexagonal lattice** (equilateral triangular lattice)
pmm, *2222, $[\infty,2,\infty]$	**p2, 2222, $[\infty,2,\infty]^+$**	**p3m1, (*333), $[3^{[3]}]$**
 **rectangular lattice** also **centered rhombic lattice** *right triangular*	 **parallelogrammic lattice** also **oblique lattice** *scalene triangular*	 **equilateral triangular lattice** (hexagonal lattice)

https://en.wikipedia.org/wiki/Lattice_(group)

Fundamental domain

A *fundamental domain* of $\mathbb{C}/\Lambda$ is a subset $\mathcal{F}$ of $\mathbb{C}$ such that the canonical surjection $\mathbb{C} \to \mathbb{C}/\Lambda$ induces a bijective map $\mathcal{F} \to \mathbb{C}/\Lambda$ (i.e. $\mathcal{F}$ is a set of representatives of $\mathbb{C}$ modulo Λ).

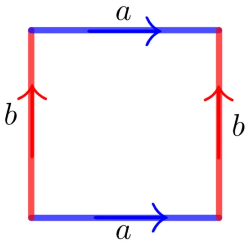
Example: let (λ_1, λ_2) be a basis of Λ as a $\mathbb{Z}$–module. Then the *fundamental parallelogram*

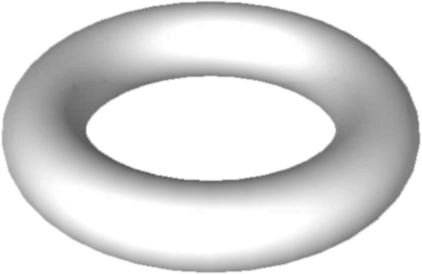
$$\mathcal{P} = \{t_1\lambda_1 + t_2\lambda_2 \mid 0 \leq t_1, t_2 < 1\}$$

is a fundamental domain of $\mathbb{C}/\Lambda$.

Torus

Let Λ be a lattice in $\mathbb{C}$. The quotient $T = \mathbb{C}/\Lambda$ is a torus.





The group of periods of a meromorphic function

Given a meromorphic function $f : \mathbb{C} \to \mathbb{P}_1(\mathbb{C})$, the set

$$\mathrm{Per}(f) = \{\lambda \in \mathbb{C} \mid f(z+\lambda) = f(z)\}$$

is an additive subgroup of $\mathbb{C}$.

If f is constant, then $\mathrm{Per}(f) = \mathbb{C}$.

If f is not constant, then $\mathrm{Per}(f)$ is a discrete subgroup of $\mathbb{C}$.

If the group $\mathrm{Per}(f)$ has rank 2 over $\mathbb{Z}$ (i.e. is a lattice), then f is called an *elliptic function*.

Elliptic function: definition

Given a lattice Λ in $\mathbb{C}$, an *elliptic function with respect to* Λ is a meromorphic function f on $\mathbb{C}$ such that $\Lambda \subset \mathrm{Per}(f)$.

The only entire elliptic functions are the constants (Liouville).

The set of elliptic functions with respect to Λ is a field $\mathcal{M}(\Lambda)$. This field is stable under derivation.

An elliptic function $f : \mathbb{C} \to \mathbb{P}_1(\mathbb{C})$ with respect to Λ induces a map on the torus $T := \mathbb{C}/\Lambda$:

$$\begin{tikzcd} \mathbb{C} \arrow[r, "f"] \arrow[d] & \mathbb{P}_1(\mathbb{C}) \\ T \arrow[ur, dotted] & \end{tikzcd}$$

Elliptic functions: properties

Let Λ be a lattice in $\mathbb{C}$, let f be a non constant elliptic function with respect to Λ and let $\mathcal{F}$ be a fundamental domain for $\mathbb{C}/\Lambda$. Then

(1) $\sum_{w \in \mathcal{F}} \mathrm{res}_w(f) = 0$.

(2) $\sum_{w \in \mathcal{F}} \mathrm{ord}_w(f) = 0$.

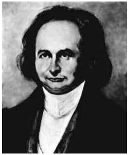
(3) $\sum_{w \in \mathcal{F}} \mathrm{ord}_w(f) \cdot w \in \Lambda$.

The *order* of a non constant elliptic function is the number of poles (counting multiplicities) in a fundamental domain.

Theorem of Abel and Jacobi

Niels Henrik Abel

1802 - 1829



Karl Jacobi

1804–1851

Let Λ be a lattice and $\mathcal{F}$ a fundamental domain of $\mathbb{C}/\Lambda$. For each $w \in \mathcal{F}$, let k_w be a rational integer such that $\{w \in \mathcal{F} \mid k_w \neq 0\}$ is finite. There exists an elliptic function f with respect to Λ satisfying $\mathrm{ord}_w(f) = k_w$ for all $w \in \mathcal{F}$ if and only if

$$\sum_{w \in \mathcal{F}} k_w = 0 \quad \text{and} \quad \sum_{w \in \mathcal{F}} k_w \cdot w \in \Lambda.$$

Divisor of a non constant elliptic function

The *divisor* of a non constant elliptic function $f : T \to \mathbb{P}_1(\mathbb{C})$ is

$$\operatorname{div}(f) := \sum_{w \in T} \operatorname{ord}_w(f)[w] \in \bigoplus_{w \in T} \mathbb{Z}$$

(finite formal sum of points in $T = \mathbb{C}/\Lambda$ with integer coefficients).

If two non constant elliptic functions f, g with respect to Λ have the same divisor, then $f = cg$ for some constant $c \in \mathbb{C}^\times$.

The divisor group $\mathrm{Div}(T)$ of a torus $T = \mathbb{C}/\Lambda$

$$\mathrm{Div}(T) = \bigoplus_{w \in T} \mathbb{Z}.$$

The *summation map* $\Sigma : \mathrm{Div}(T) \to T$ sends $\sum_{w \in T} n_w [w]$ to $\sum_{w \in T} n_w w$.
The *degree map* $\mathrm{Div}(T) \to \mathbb{Z}$ sends $\sum_{w \in T} n_w [w]$ to $\sum_{w \in T} n_w$.
The kernel of the degree map is the subgroup $\mathrm{Div}^0(T)$ of divisors of degree 0.
The *divisor map* $\mathrm{div} : \mathcal{M}(\Lambda)^\times \to \mathrm{Div}^0(T)$ sends a non-zero elliptic function to its associated divisor.

Theorem. *The sequence of abelian groups*

$$1 \longrightarrow \mathbb{C}^\times \longrightarrow \mathcal{M}(\Lambda)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(T) \xrightarrow{\Sigma} T \longrightarrow 1$$

is exact.

Reference: Washington §9.1.

Eisenstein series

For $s \in \mathbb{R}$, the series

$$\sum_{\lambda \in \Lambda \setminus \{0\}} |\lambda|^{-s}$$

converges if and only if $s > 2$.

Lemma. The *Eisenstein series* are

$$G_k(\Lambda) := \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-k}$$

for $k > 2$ an integer.

Gotthold Eisenstein

1823 – 1852

Exercise.

- for k odd, $G_k(\Lambda) = 0$.
- for $\lambda \in \mathbb{C} \setminus \{0\}$ and $\Lambda = \mathbb{Z}\lambda + \mathbb{Z}\mathrm{i}\lambda$, $G_6(\Lambda) = 0$.
- for $\lambda \in \mathbb{C} \setminus \{0\}$ and $\Lambda = \mathbb{Z}\lambda + \mathbb{Z}\varrho\lambda$ with $\varrho = \mathrm{e}^{2\pi\mathrm{i}/3}$, $G_4(\Lambda) = 0$.

Weierstrass $\wp$–function

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

Karl Weierstrass

1815 – 1897

$$\wp'(z) = \sum_{\lambda \in \Lambda} \frac{-2}{(z-\lambda)^3}.$$

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}.$$

The field $\mathcal{M}(\Lambda)$ of elliptic functions for Λ

The field $\mathbb{C}(\wp_\Lambda)$ is the field of even elliptic functions for the lattice Λ.

More precisely, any non constant even elliptic function can be written

$$c \prod_{w \in W} \big(\wp(z) - \wp(w)\big)^{n_w}$$

where $c \in \mathbb{C}^\times$, W is a finite subset of $\mathbb{C} \setminus \Lambda$ and $n_w \in \mathbb{Z}$.

The field $\mathcal{M}(\Lambda)$ is $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$, a quadratic extension of $\mathbb{C}(\wp_\Lambda)$.

Differential equation of $\wp_\Lambda$

$$(\wp_\Lambda')^2 = 4\wp_\Lambda^3 - g_2(\Lambda)\wp_\Lambda - g_3(\Lambda)$$

with

$$g_2(\Lambda) = 60G_4(\Lambda) \quad \text{and} \quad g_3(\Lambda) = 140G_6(\Lambda).$$

Consequence.

$$\wp'' = 6\wp^2 - \frac{g_2}{2}.$$

Smooth cubic curves

We have

$$4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3)$$

with

$$e_1 = \wp(\lambda_1/2), \quad e_2 = \wp(\lambda_2/2), \quad e_3 = \wp((\lambda_1 + \lambda_2)/2).$$

Since e_1, e_2, e_3 are pairwise distinct, the discriminant

$$\Delta = g_2^3 - 27g_3^2 = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$$

does not vanish.
The curve $y^2t = 4x^3 - g_2xt^2 - g_3t^3$ in $\mathbb{P}_2(\mathbb{C})$ is *smooth* (no singular point).

Weierstrass parametrization

Theorem. *Let Λ be a lattice in $\mathbb{C}$. The Weierstrass map*

$$\begin{array}{ccccc} \mathbb{C} & \longrightarrow & \mathbb{P}_2(\mathbb{C}) & & \\ z & \longmapsto & (\wp(z) : \wp'(z) : 1) & & z \notin \Lambda \\ \lambda & \longmapsto & (0:1:0) & & \lambda \in \Lambda \end{array}$$

induces a bijective map from the torus $T := \mathbb{C}/\Lambda$ to the complex elliptic curve E_Λ with projective Weierstrass equation

$$E_\Lambda : \; Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3.$$

Corollary. *The Weierstrass parametrization*

$$\exp_E : \mathbb{C} \longrightarrow E_\Lambda(\mathbb{C})$$

endows $E_\Lambda(\mathbb{C})$ with a group structure isomorphic to $\mathbb{C}/\Lambda$, with zero element $0_E := (0:1:0)$. The inverse of $(X:Y:Z)$ is $(X:-Y:Z)$. Three distinct points on $E_\Lambda(\mathbb{C})$ add to 0_E if and only if they are collinear.

Complex torsion

The torsion elements in $E(\mathbb{C})$ are the images under $(\wp : \wp' : 1)$ of the $\mathbb{Q}$–vector space $\mathbb{Q}\Lambda$ spanned by Λ.

For $N \geq 1$,

$$\{P \in E(\mathbb{C}) \ \mid NP = 0_E\} \simeq \frac{1}{N}\Lambda/\Lambda \simeq (\mathbb{Z}/N\mathbb{Z})^2.$$

The torsion subgroup $E(\mathbb{C})_{\rm tors}$ of $E(\mathbb{C})$ is isomorphic to $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$.

Compare with

$$(\mathbb{C}^\times)_{\rm tors} = \mu \simeq \mathbb{Q}/\mathbb{Z}.$$

where μ is the group of roots of unity in $\mathbb{C}$.

Addition formula for the Weierstrass $\wp$–function

For $u, v, w \in \mathbb{C}$, the condition $u + v + w = 0$ is equivalent to

$$\det \begin{pmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{pmatrix} = 0.$$

This means that three points on $E(\mathbb{C})$ add to O_E if and only if they are on a straight line.

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2.$$

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2.$$

Uniformization Theorem

Theorem. *Let* g_2, g_3 *be two complex numbers such that* $g_2^3 \neq 27g_3^2$*. Then there exists a lattice* Λ *in* $\mathbb{C}$ *such that* $g_2(\Lambda) = g_2$*,* $g_3(\Lambda) = g_3$*. Hence the smooth cubic curve*

$$E : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

is the elliptic curve E_Λ *attached to the torus* $\mathbb{C}/\Lambda$*.*

It suffices to show that there exists a lattice Λ_0 with j invariant $j(E)$. Then there exists α such that $\Lambda = \alpha\Lambda_0$ solves the problem.

Isogenies

Let Λ_1, Λ_2 *be two lattices in* $\mathbb{C}$, $T_1 = \mathbb{C}/\Lambda_1$, $T_2 = \mathbb{C}/\Lambda_2$ *the associated tori and* $\psi : T_1 \to T_2$ *a continuous map. Then there is a continuous map* $\phi : \mathbb{C} \to \mathbb{C}$ *such that the diagram*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\phi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\psi} & \mathbb{C}/\Lambda_2 \end{array}$$

commutes.

The map ϕ is unique up to an additive constant in Λ_2 and satisfies $\phi(\Lambda_1) \subset \Lambda_2$.

If ϕ is analytic and $\psi(0) = 0$, then ψ is called *an isogeny*.

The set of isogenies is an additive group with neutral element the zero isogeny.

Isogenies

Let Λ_1, Λ_2 be two lattices in $\mathbb{C}$ and let $\alpha \in \mathbb{C}$ satisfy $\alpha\Lambda_1 \subset \Lambda_2$. Then the map

$$\begin{array}{rccc} \psi_\alpha : & \mathbb{C}/\Lambda_1 & \longrightarrow & \mathbb{C}/\Lambda_2 \\ & z \bmod \Lambda_1 & \longmapsto & \alpha z \bmod \Lambda_2 \end{array}$$

associated with the analytic map $[\alpha] : z \mapsto \alpha z$:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{[\alpha]} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\psi_\alpha} & \mathbb{C}/\Lambda_2 \end{array}$$

is an isogeny.
Conversely, if $\psi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ is an isogeny, then there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ and $\psi = \psi_\alpha$.

The group of isogenies

Consequence: *Any isogeny* $\mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ *is a group homomorphism and* $\mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$ *is an additive group.*

If $\psi = \psi_\alpha$ is an isogeny associated with $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 \subset \Lambda_2$, then the kernel of ψ is $\Lambda_2/\alpha\Lambda_1$ hence is finite. Its number of elements (the index of $\alpha\Lambda_1$ in Λ_2) is the *degree* of the isogeny.

If ψ is a non zero isogeny of degree n from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$, then $n\Lambda_2$ is a subgroup of index n in $\alpha\Lambda_1$, hence n/α maps Λ_2 to a subgroup of index n in Λ_1 and there exists an isogeny $\hat{\psi}$ of degree n from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$, the *dual isogeny* corresponding to ψ; the composites $\psi \circ \hat{\psi}$ and $\hat{\psi} \circ \psi$ are multiplication by n.

Example of dual isogenies

E_1: $y^2 = x^3 + x^2 + x$
E_2: $Y^2 = X^3 - 2X^2 - 3X$

$$\begin{array}{cccc} \phi & E_1 & \longrightarrow & E_2 \\ & (x,y) & \longmapsto & \left(\dfrac{y^2}{x^2}, \dfrac{y(1-x^2)}{x^2}\right) \end{array}$$

$$\begin{array}{cccc} \hat{\phi} & E_2 & \longrightarrow & E_1 \\ & (X,Y) & \longmapsto & \left(\dfrac{Y^2}{4X^2}, \dfrac{-Y(3+X^2)}{8X^2}\right) \end{array}$$

$$\hat{\phi} \circ \phi = [2].$$

Reference: Silverman, Example 4.5 p.74.

Isomorphism between elliptic curves

Two complex elliptic curves are *isomorphic* iff there is an isogeny of degree 1 between them:

$$E_1 = \mathbb{C}/\Lambda_1, \quad E_2 = \mathbb{C}/\Lambda_2, \quad \Lambda_2 = \alpha\Lambda_1 \quad \text{for some} \quad \alpha \in \mathbb{C}^\times.$$

The two tori $\mathbb{C}/\Lambda$, $\mathbb{C}/\alpha\Lambda$ are said to be *homothetic*.

We have $\wp_{\alpha\Lambda}(z) = \alpha^{-2}\wp_\Lambda(\alpha z)$ and

$$g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda) \quad \text{and} \quad g_3(\alpha\Lambda) = \alpha^{-6}g_2(\Lambda),$$

The modular invariant $j(\Lambda)$

Let Λ be a lattice in $\mathbb{C}$. Recall

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

and

$$g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda), \qquad g_3(\alpha\Lambda) = \alpha^{-6}g_2(\Lambda),$$

Hence $\Delta(\alpha\Lambda) = \alpha^{-12}\Delta(\Lambda)$.
Define

$$j(\Lambda) = 1728\,\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Proposition. *Two lattices are homothetic if and only if they have the same j invariant.*

The modular function $j(\tau)$

For τ_1 and τ_2 in the upper half plane $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$, the two lattices $\mathbb{Z} + \mathbb{Z}\tau_1$ and $\mathbb{Z} + \mathbb{Z}\tau_2$ are homothetic if and only if there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$

The *elliptic modular invariant* is defined for τ in $\mathfrak{H}$ by

$$j(\tau) = j(\mathbb{Z} + \mathbb{Z}\tau).$$

Exercise. Check $j(\tau) \to \infty$ for $\operatorname{Im}(\tau) \to \infty$.

Consequence. $j : \mathfrak{H} \to \mathbb{C}$ is surjective.

$j(\mathfrak{H}) = \mathbb{C}$

Theorem. *The elliptic modular invariant j induces a bijective map $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \longrightarrow \mathbb{C}$.*

Consequence: *proof of the Uniformization Theorem.*
According to the uniformization Theorem, the j invariant gives a bijective map between $\mathbb{C}$ and isomorphism classes of elliptic curves.

For $j \notin \{0, 1728\}$, the j invariant of

$$y^2 = 4x^3 - gx - g \quad \text{with} \quad g = \frac{27j}{j - 1728}$$

is j (notice that $\Delta \neq 0$ since $g \notin \{0, 27\}$).
The j invariants of $y^2 = x^3 + 1$ and $y^2 = x^3 + x$ are 0 and 1728 respectively.

Classes of isomorphism of elliptic curves

For τ and τ' in $\mathfrak{H}$, the two elliptic curves $E = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ and $E' = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau')$ are isomorphic as complex elliptic curves if and only if there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

Remark. The two elliptic curves

$$y^2 = 4x^3 - 4x \quad \text{and} \quad y^2 = 4x^3 + 4x$$

are isomorphic over $\mathbb{C}$, not over $\mathbb{Q}$.

Complex multiplication

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve with $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Then the ring of endomorphisms of E is

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = \begin{cases} \mathbb{Z} & \text{if } [\mathbb{Q}(\tau) : \mathbb{Q}] > 2, \\ \mathbb{Z} + \mathbb{Z}A\tau & \text{if } [\mathbb{Q}(\tau) : \mathbb{Q}] = 2, \end{cases}$$

where, in the second case, A is the leading coefficient in the minimal equation $A\tau^2 + B\tau + C = 0$.

$$\deg \alpha := \operatorname{Card} \ker \alpha = \mathrm{N}(\alpha) = \alpha\bar{\alpha}.$$

Definition. In characteristic 0, E has *complex multiplication* if $\mathrm{End}(E) \neq \mathbb{Z}$.

Chowla–Selberg Formula (1949, 1967)

Sarvadaman Chowla

1907 – 1995

Atle Selberg

1917 – 2007

$$G_4(\mathbb{Z}+\mathbb{Z}\mathrm{i}) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} (m+n\mathrm{i})^{-4} = \frac{\Gamma(1/4)^8}{2^6\cdot 3\cdot 5\cdot \pi^2}$$

and

$$G_6(\mathbb{Z}+\mathbb{Z}\varrho) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} (m+n\varrho)^{-6} = \frac{\Gamma(1/3)^{18}}{2^8\pi^6}$$

Formula of Chowla and Selberg (1966): *the periods of elliptic curves with complex multiplication are products of values of the Gamma function at rational points.*

Endomorphisms of an elliptic curve

Let Λ be a lattice and $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda \subset \Lambda$. Then α is either a rational integer or an imaginary quadratic number. The function $\wp_\Lambda(\alpha z)$ is a rational function of $\wp_\Lambda(z)$ such that the degree of the numerator is α^2 if $\alpha \in \mathbb{Z}$ and $\mathrm{Norm}(\alpha)$ if α is imaginary quadratic; the degree of the denominator is $\alpha^2 - 1$ and $\mathrm{Norm}(\alpha) - 1$ respectively.

Example. $K = \mathbb{Q}(\sqrt{-2})$, $\alpha = \mathrm{i}\sqrt{2}$, $\Lambda = \mathbb{Z} + \mathbb{Z}\alpha$,

$$y^2 = 4x^3 - gx - g, \quad g = \frac{3^3 5^3}{2 \cdot 7^2}, \quad j = 20^3,$$

$$\wp(\alpha z) = \frac{-\frac{1}{2}\wp(z)^2 - \frac{15}{14}\wp(z) - \frac{3^4 5^2}{2^4 7^2}}{\wp(z) + \frac{15}{7}}.$$

Automorphisms of elliptic curves

The map $(x, y) \mapsto (x, -y)$ defines an automorphism of order 2 of the elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$.

The map

$$\begin{array}{rccc} [\mathrm{i}] : & E(\mathbb{C}) & \longrightarrow & E(\mathbb{C}) \\ & (x, y) & \longmapsto & (-x, \mathrm{i}y) \end{array}$$

is an automorphism of order 4 of the elliptic curve $E : y^2 = x^3 - x$:

$$\mathrm{Aut}(E) = \{\pm 1, \pm[\mathrm{i}]\} = \mathbb{Z}[\mathrm{i}]^\times$$

The map

$$\begin{array}{rccc} [\varrho] : & E(\mathbb{C}) & \longrightarrow & E(\mathbb{C}) \\ & (x, y) & \longmapsto & (\varrho x, -y) \end{array}$$

is an automorphism of order 6 of the elliptic curve $E : y^2 = x^3 - 1$:

$$\mathrm{Aut}(E) = \{\pm 1, \pm[\varrho], \pm[\varrho]^2\} = \mathbb{Z}[\varrho]^\times$$

Complex multiplication and imaginary quadratic number field

Let K be an imaginary quadratic number field, $\mathcal{R}$ its ring of integer and $\mathrm{Cl}(\mathcal{R})$ the ideal class group of $\mathcal{R}$. Fix an embedding of K in $\mathbb{C}$. To each ideal of $\mathcal{R}$ is associated a lattice $\Lambda \subset \mathbb{C}$ and an elliptic curve $\mathbb{C}/\Lambda$, so that

$$\mathrm{End}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = \mathcal{R}.$$

Up to isomorphism, $\mathbb{C}/\Lambda$ depends only on the class of Λ in $\mathrm{Cl}(\mathcal{R})$.
One deduces a one to one correspondence between ideal classes in $\mathrm{Cl}(\mathcal{R})$ and elliptic curves E with $\mathrm{End}(E) = \mathcal{R}$.

Reference: Silverman, Appendix C, §11 Complex multiplication.

Fundamental theorem of complex multiplication

Heinrich Weber

1842 – 1913

Karl Rudolf Fueter

1880 – 1950

Let Λ be a lattice associated with an ideal class of $\mathcal{R}$.

Theorem (Weber, Fueter). *The number $j(\Lambda)$ is an algebraic integer of degree over $\mathbb{Q}$ (and over K) the class number h of K. The field $K(j(\Lambda))$ is the maximal unramified extension (Hilbert class field) of K. A complete set of conjugates of $j(\Lambda)$ over K is given by $j(\Lambda_1), \ldots, j(\Lambda_h)$ when $\Lambda_1, \ldots, \Lambda_h$ are representatives of the h classes of ideals of $\mathcal{R}$.*

Complex multiplication (continued)

If K has class number 1, then j is a rational integer.
Discriminants of quadratic fields with class number 1:
$d = -3, -4, -7, -8, -11, -19, -43, -67, -163$

j-invariants for orders of class number 1.
https://oeis.org/A032354

Discriminants for orders: https://oeis.org/A133675

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$$

$$0, 1728 = 12^3, -3375 = -15^3, 8000 = 20^3, -32768 = -32^3,$$
$$54000 = 2 \cdot 30^3, 287496 = 66^3, -884736 = -96^3,$$
$$-12288000 = -3 \cdot 160^3, 16581375 = 255^3,$$
$$-884736000 = -960^3, -147197952000 = -5280^3,$$
$$-262537412640768000 = -640320^3$$

Example: $j((-1+\sqrt{-163})/2) = -262537412640768000 = -640320^3$.
Reference: David Masser
Auxiliary Polynomials in Number Theory, Cambridge University Press 2016

$e^{\pi\sqrt{163}}$

The decimal expansion of $e^{\pi\sqrt{163}}$ starts with

$$262537412640768743.99999999999925007\ldots$$

and the continued fraction expansion starts with

$$[262537412640768743, 1, 1333462407511, 1, 8, 1\ldots].$$

Recall, for $q = e^{2\pi i\tau}$,

$$j(\tau) = J(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

Let $\tau = (-1+\sqrt{-163})/2$ so that $q = e^{2\pi i\tau} = -e^{\pi\sqrt{163}}$. Then

$$\left|j(\tau) - \frac{1}{q} - 744\right| = \left|j(\tau) + e^{\pi\sqrt{163}} - 744\right| = 196884q + \cdots$$

while $|q| < \frac{1}{2}10^{-17}$. Hence the distance of $e^{\pi\sqrt{163}}$ to the nearest integer $|j(\tau)| + 744$ is less than 10^{-12}.

http://oeis.org/A060295 http://oeis.org/A058292

A few special values of j

Examples. Here are a few selected values of j.

$$j((1+i\sqrt{3})/2) = 0 = 1728 - 3(24)^2$$
$$j(i) = 1728 = 12^3 = 1728 - 4(0)^2$$
$$j((1+i\sqrt{7})/2) = -3375 = (-15)^3 = 1728 - 7(27)^2$$
$$j(i\sqrt{2}) = 8000 = 20^3 = 1728 + 8(28)^2$$
$$j((1+i\sqrt{11})/2) = -32768 = (-32)^3 = 1728 - 11(56)^2$$
$$j((1+i\sqrt{19})/2) = -884736 = (-96)^3 = 1728 - 19(216)^2$$
$$j((1+i\sqrt{43})/2) = -884736000 = (-960)^3 = 1728 - 43(4536)^2$$
$$j((1+i\sqrt{67})/2) = -147197952000 = (-5280)^3 = 1728 - 67(46872)^2$$
$$\begin{aligned} j((1+i\sqrt{163})/2) &= -262537412640768000 = (-640320)^3 \\ &= 1728 - 163(40133016)^2 \end{aligned}$$
$$j(i\sqrt{3}) = 54000 = 2(30)^3 = 1728 + 12(66)^2$$
$$j(2i) = 287496 = (66)^3 = 1728 + 8(189)^2$$
$$j((1+3i\sqrt{3})/2) = -12288000 = -3(160)^3 = 1728 - 3(2024)^2$$
$$j(i\sqrt{7}) = 16581375 = (255)^3 = 1728 + 7(1539)^2$$
$$\begin{aligned} j((1+i\sqrt{15})/2) &= \frac{-191025 - 85995\sqrt{5}}{2} \\ &= \frac{1-\sqrt{5}}{2}\left(\frac{75+27\sqrt{5}}{2}\right)^3 = 1728 - 3\left(\frac{273+105\sqrt{5}}{2}\right)^2 \end{aligned}$$
$$\begin{aligned} j((1+i\sqrt{23})/2) &= -(820750\theta^2 + 1084125\theta + 616750) \\ &= -(25\theta^2 + 55\theta + 35)^3 \\ &= 1728 - (3\theta^2 - 4)(406\theta^2 + 511\theta + 273)^2, \end{aligned}$$

where θ is the real root of the cubic equation $X^3 - X - 1 = 0$.

Henri Cohen. *A course in computational algebraic number theory* § 7.2.3 Examples.

Prime values of polynomials

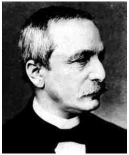
Leonhard Euler
1707 – 1783

Harold Stark

Euler polynomial: $x^2 - x + 41$: produces prime numbers for all integer values of x from 1 to 40.
For $p = 41$ the field $\mathbb{Q}(\sqrt{1-4p}) = \mathbb{Q}(\sqrt{-163})$ has class number 1.

Harold Stark. *A historical note on complex quadratic fields with class-number one.* Proceedings of the American Mathematical Society, (1969) **21** 254–255.
doi:10.1090/S0002-9939-1969-0237461-X
https://en.wikipedia.org/wiki/Lucky_numbers_of_Euler
https://mathworld.wolfram.com/LuckyNumberofEuler.html
https://math.stackexchange.com/questions/169066/polynomials-representing-primes

Kronecker – Weber



Leopold Kronecker
1823 – 1891

Heinrich Weber
1842 – 1913

Kronecker (1853), Weber (1886), Hilbert (1896).
Every finite abelian extension of $\mathbb{Q}$ *is contained in a cyclotomic field* $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/n})$.
Hilbert's twelfth problem asks for generalizations of the Kronecker–Weber theorem to base fields other than the rational numbers, and asks for the analogues of the roots of unity for those fields.

Kronecker Jugendtraum

Kronecker in a letter to Dedekind in 1880 reproduced in volume V of his collected works, page 455

Es handelt sich um meinen liebsten Jugendtraum, nämlich um den Nachweis, dass die Abel'schen Gleichungen mit Quadratwurzeln rationaler Zahlen durch die Transformations-Gleichungen elliptischer Functionen mit singularen Moduln grade so erschöpft werden, wie die ganzzahligen Abel'schen Gleichungen durch die Kreisteilungsgleichungen.

Kronecker Jugendtraum

Kronecker's Jugendtraum is the twelfth of the 23 problems of Hilbert. It asks for an extension of the Kronecker–Weber theorem on abelian extensions of the rational numbers, to any base number field.

The goal is to describe the finite abelian extension of any number field K by means of values of complex functions. For $K = \mathbb{Q}$ this is done by the Kronecker–Weber theorem using the exponential function, for an imaginary quadratic field it is done by using suitably selected elliptic functions.

CM fields, totally real fields

Goro Shimura
1930 – 2019

Samit Dasgupta

Mahesh Kakde

Goro Shimura extended the classical theory of complex multiplication to CM fields.
In the special case of totally real fields, a solution was given by Dasgupta and Kakde. This provides an effective method to construct the maximal abelian extension of any totally real field. The method rests on p–adic integration and the solution it provides for totally real fields is different in nature from what Hilbert had in mind in his original formulation.

Totally real quadratic fields

Henri Darmon

Alice Pozzi

Jan Vonk

A solution in the more special case of totally real quadratic fields, also resting on p–adic methods, was given by Darmon, Pozzi and Vonk.

Hilbert's Twelfth Problem: A Comedy of Errors

Schappacher, Norbert: *On the History of Hilbert's Twelfth Problem: A Comedy of Errors.* Matériaux pour l'histoire des mathématiques au XXème siècle, Nice, 1996, France. Sémin. Congr. 3, Soc. Math. France, Paris (1998), p.243-273.

Nikolaev, Igor: *On algebraic values of function* $\exp(2\pi i x + \log\log y)$*.* Ramanujan J. 47, 417–425 (2018).

M.W. *On a paper by Nikolaev.* The Ramanujan Journal, volume 57, 1517–1518 (2022). Published online: 12 February 2022.

On algebraic values of function $\exp(2\pi i x + \log\log y)$

Nikolaev, Igor. Ramanujan J. **47**, 417–425 (2018).

Remark 2 The absolute value $|z| = (z\bar{z})^{\frac{1}{2}}$ of an algebraic number z is always an "abstract" algebraic number, i.e. a root of the polynomial with integer coefficients; yet Theorem 1 implies that $|\mathcal{J}(\theta_i, \varepsilon)| = \log \varepsilon$ is a transcendental number. This apparent contradiction is false, since quadratic extensions of the field $\mathbb{Q}(z\bar{z})$ have no real embeddings in general; in other words, our extension cannot be a subfield of $\mathbb{R}$.

M.W. Ramanujan Journal, **57**, 1517–1518 (2022).

The abstract of the paper [Nikolaev] starts with the following sentence: *It is proved that, for all but a finite set of the square-free integers, d the value of transcendental function $\exp(2\pi i x + \log\log y)$ is an algebraic number for the algebraic arguments x and y lying in a real quadratic field of discriminant, d.* As a matter of fact, the modulus of this number is $|\log y|$, a transcendental number according to the Hermite–Lindemann Theorem. Theorem 1 of [Nikolaev] contradicts the Hermite–Lindemann Theorem.

Prime numbers of the form $x^2 + ny^2$: Fermat

Pierre de Fermat

1600(?) – 1665

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

Also :

$$p = x^2 + 2y^2 \quad \Longleftrightarrow \quad p \equiv 1, 3 \pmod 8.$$

$$p = x^2 + 3y^2 \quad \Longleftrightarrow \quad p = 3 \quad \text{or} \quad p \equiv 1 \pmod 3.$$

Euler's conjectures

Leonhard Euler

1707 – 1783

An odd prime number p can be written $p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \pmod{20}$.

Johann Carl Friedrich Gauss

1777 – 1865

$$p = x^2 + 27y^2 \quad \Longleftrightarrow$$

$$\begin{cases} p \equiv 1 \pmod 3 \text{ and } 2 \text{ is} \\ \text{a cubic residue modulo } p. \end{cases}$$

History

André Weil
Number theory :
An approach through history. From Hammurapi to Legendre.
Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.

André Weil
1906 – 1998

https://doi.org/10.1007/978-0-8176-4571-7

Class field theory

Let n be a positive integer. There exists an irreducible polynomial $f_n(X) \in /Z[X]$ such that for a prime p dividing neither n nor the discriminant of f_n,

$$p = x^2 + ny^2 \iff \begin{cases} -n \text{ is a quadratic residue modulo } p \text{ and} \\ \text{and there exists } x \in \mathbb{Z} \text{ such that} \\ f_n(x) \equiv 0 \pmod{p}. \end{cases}$$

The polynomial f_n is the minimal polynomial of a primitive element of a ring class field determined by $\mathbb{Z}(\sqrt{-n})$.

David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.*

https://onlinelibrary.wiley.com/doi/book/10.1002/9781118400722

http://www.math.toronto.edu/~ila/Cox-Primes_of_the_form_x2+ny2.pdf

Division of the lemniscate

Johann Carl Friedrich Gauss

1777 – 1865

Niels Henrik Abel

1802 - 1829

Gauss: The regular n–gon can be constructed by a ruler and a compass if and only if n is a product of distinct Fermat primes $2^{2^k}+1$ and a power of 2.

Abel: same result for the lemniscate

$$(x^2+y^2)^2 = x^2 - y^2,$$

the arc length is given by the elliptic integral (Gauss constant)

$$\varpi = 4\int_0^1 \frac{\mathrm{d}t}{\sqrt{1-t^4}} = 2.622\,057\,554\,292\ldots$$

https://handwiki.org/wiki/Lemniscate_constant https://oeis.org/A062539

Lemniscate sine and cosine functions

$$\frac{\mathrm{d}}{\mathrm{d}z}\operatorname{sl} z = \left(1+\operatorname{sl}^2 z\right)\operatorname{cl} z,\ \ \frac{\mathrm{d}}{\mathrm{d}z}\operatorname{cl} z = -\left(1+\operatorname{cl}^2 z\right)\operatorname{sl} z,$$

$\operatorname{sl} 0 = 0,\ \operatorname{cl} 0 = 1$,

$$z = \int_0^{\operatorname{sl} z}\frac{\mathrm{d}t}{\sqrt{1-t^4}} = \int_{\operatorname{cl} z}^{1}\frac{\mathrm{d}t}{\sqrt{1-t^4}}.$$

Compare with

$$\frac{\mathrm{d}}{\mathrm{d}z}\sin z = \cos z,\ \ \frac{\mathrm{d}}{\mathrm{d}z}\cos z = -\sin z,\ \ \sin 0 = 0,\ \ \cos 0 = 1,$$

and

$$z = \int_0^{\sin z}\frac{\mathrm{d}t}{\sqrt{1-t^2}} = \int_{\cos z}^{1}\frac{\mathrm{d}t}{\sqrt{1-t^2}}.$$

Lemniscate elliptic functions

$$\mathrm{cl}^2 z + \mathrm{sl}^2 z + \mathrm{cl}^2 z \,\mathrm{sl}^2 z = 1$$

Parametrization of the quartic curve

$$x^2 + y^2 + x^2 y^2 = 1.$$

The Lemniscate functions cl and sl are elliptic functions with fundamental periods $\omega_1 = (1+\mathrm{i})\varpi$ and $\omega_2 = (1-\mathrm{i})\varpi = \mathrm{i}\omega_1$, like the Weierstrass elliptic function $\wp$ with equation $y^2 = 4x^3 + x$.

Lemniscate vs Weierstrass

$$\mathrm{sl}(z) = -2\frac{\wp(z)}{\wp'(z)}, \qquad \mathrm{sl}'(z) = \frac{4\wp^2(z) - 1}{4\wp^2(z) + 1}.$$

The functions sl and sl' parametrize the curve

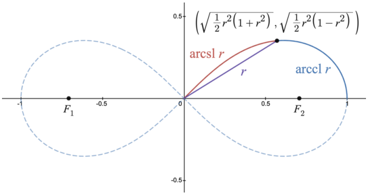
$$y^2 = 1 - x^4.$$

A birational transformation between this curve and the Weierstrass curve is given by

$$x = -2\frac{X}{Y}, \qquad y = \frac{4X^2 - 1}{4X^2 + 1}.$$

David A. Cox and Trevor Hyde, *The Galois theory of the lemniscate.* Journal of Number Theory **135** (2014) 43–59.

Lemnatomic polynomials



The elliptic curve $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}(1+\mathrm{i})\varpi + \mathbb{Z}(1-\mathrm{i})\varpi$ has complex multiplication with ring of endomorphisms $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$.

Let $\beta \in \mathcal{O}$ and $\delta_\beta = (1+\mathrm{i})\varpi/\beta$. The minimal polynomial of δ_β is

$$\Lambda_\beta(x) = \prod_{[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times} (x - \mathrm{sl}(\alpha\delta_\beta))$$

Compare with cyclotomic polynomials :

$$\Phi_n(X) = \prod_{[d] \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \mathrm{e}^{2d\pi\mathrm{i}/n}).$$

Division of the lemniscate

Cyclotomy: $\mathrm{Gal}(\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/n})/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ has order a power of 2 if and only if n is a product of distinct Fermat primes and a power of 2.

Lemniscate: same for $(\mathbb{Z}[\mathrm{i}]/n\mathbb{Z}[\mathrm{i}])^\times$.

References:

B. Sury. *Cyclotomy and Cyclotomic Polynomials. The Story of how Gauss Narrowly Missed Becoming a Philologist.* Resonance, December 1999, 41 – 53.

https://www.isibang.ac.in/~sury/cyclotomy.pdf

Michael Rosen. *Abel's Theorem on the Lemniscate.* The American Mathematical Monthly, 1981, Vol. 88, No. 6, pp. 387-395.

https://www.jstor.org/stable/2321821

Transcendence and elliptic functions

Siegel (1932): elliptic analog of Lindemann's Theorem on the transcendence of π.

Schneider (1937): elliptic analog of Hermite–Lindemann Theorem. General transcendence results on values of elliptic functions, on periods, on elliptic integrals of the first and second kind.

C.L. Siegel
1896 – 1981

Th. Schneider
1911 – 1988

Schneider – Lang Theorem (1949, 1966)

Theodor Schneider

1911 – 1988

Serge Lang

1927 – 2005

Let $f_1, \dots, f_m$ *be meromorphic functions on* $\mathbb{C}$. *Assume* f_1 *and* f_2 *are algebraically independent and of finite order. Let* $\mathbb{K}$ *be a number field. Assume* f_j' *belongs to* $\mathbb{K}[f_1, \dots, f_m]$ *for* $j = 1, \dots, m$. *Then the set*

$$S = \{w \in \mathbb{C} \mid w \text{ not pole of } f_j,\ f_j(w) \in \mathbb{K} \text{ for } j = 1, \dots, m\}$$

is finite.

http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Schneider.html
http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Lang.html

Elliptic analog of Hermite–Lindemann Theorem

Let $w \in \mathbb{C}$, not pole of $\wp$. Then one at least of the numbers g_2, g_3, w, $\wp(w)$ is transcendental.

`Proof` as a consequence of the Schneider–Lang Theorem.
Let $\mathbb{K} = \mathbb{Q}(g_2, w, \wp(w), \wp'(w))$. The two functions $f_1(z) = z$, $f_2(z) = \wp(z)$ are algebraically independent, of finite order. Set $f_3(z) = \wp'(z)$. From ${\wp'}^2 = 4\wp^3 - g_2\wp - g_3$ one deduces

$$f_1' = 1, \quad f_2' = f_3, \quad f_3' = 6f_2^2 - (g_2/2).$$

The set S contains

$$\{\ell w \mid \ell \in \mathbb{Z},\ \ell w \text{ not pole of } \wp\}$$

which is infinite. Hence $\mathbb{K}$ is not a number field. $\square$

Some consequences

If g_2 and g_3 are algebraic, then λ_1 and λ_2 are transcendental.

If $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, then one at least of g_2, g_3 is transcendental.

Theorem (Schneider). *If τ and $j(\tau)$ are algebraic, then τ is quadratic.*

`Hint:` Let $\wp$ with invariant $j(\tau)$ and with g_2, g_3 algebraic. From Schneider–Lang Theorem one deduces that if τ and $j(\tau)$ are algebraic, then the two functions $\wp(z)$ and $\wp(\tau z)$ are algebraically dependent.

Reference: David Masser, *Auxiliary Polynomials in Number Theory* Cambridge Tracts in Mathematics, Cambridge University Press (2016).
doi:10.1017/CBO9781107448018

References

- Komaravolu Chandrasekharan. *Elliptic functions*, Springer Verlag, Grundlehren der mathematischen Wissenschaften (GL **281**) (1985).

https://doi.org/10.1007/978-3-642-52244-4
https://epdf.tips/elliptic-functions452efc21f5fb80b90989bbda54297e5e74666.html

Chapter I Periods of meromorphic functions
Chapter II General properties of elliptic functions
Chapter III Weierstrass's elliptic function $\wp(z)$
Chapter IV The zeta-function and the sigma-function of Weierstrass
Chapter VI The modular function $J(\tau)$

- Henri Cohen. *A course in computational algebraic number theory*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **138**), 3rd ed. (1996).

https://doi.org/10.1007/978-3-662-02945-9
https://www.math.u-bordeaux.fr/~hecohen/

Chapter 7 Introduction to elliptic curves.

• David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.*
(AMS Notices Novembre 2021) AMS Chelsea Publishing, Volume 387 December 2022. Third Edition with Solutions. With contributions by Roger Lipsett
https://onlinelibrary.wiley.com/doi/book/10.1002/9781118400722
http://www.math.toronto.edu/~ila/Cox-Primes_of_the_form_x2+ny2.pdf

• Marc Hindry. *Arithmétique*, Calvage & Mounet (2008). English translation, *Arithmetics*, Universitext, Springer (2011).

http://www.calvage-et-mounet.fr/2022/05/09/arithmetique/
https://webusers.imj-prg.fr/~marc.hindry/enseignement_fr.html
https://doi.org/10.1007/978-1-4471-2131-2

Chapitre V Courbes elliptiques.

• Dale Husemöller. *Elliptic Curves*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **111**), 2nd ed. (2004).
https://doi.org/10.1007/978-1-4757-5119-2
https://people.math.rochester.edu/faculty/doug/otherpapers/Husemoller.pdf
http://www.emule-books.narod.ru/books1.html 8190

Chapter 3 Elliptic curves and their isomorphisms
Chapter 9 Elliptic curves and hypergeometric functions

• K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **84**) 2nd ed.(1998).
https://doi.org/10.1007/978-1-4757-2103-4
http://www.emule-books.narod.ru/books1.html 8169

Chapter 18 Elliptic curves
Chapter 19 The Mordell–Weil Theorem

• Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **97**), (1984).
https://doi.org/10.1007/978-1-4684-0255-1

Chapter I From Congruent Numbers to Elliptic Curves
Chapter II The Hasse—Weil L-Function of an Elliptic Curve
Chapter III Modular Forms

• Serge Lang. *Elliptic functions*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **112**), (1987).

https://doi.org/10.1007/978-1-4612-4752-4
http://www.emule-books.narod.ru/books1.html 8191

Chapter 1 Elliptic functions
Chapter 2 Homomorphisms
Chapter 3 The modular function
Chapter 4 Fourier expansions
Chapter 18 Product expansions

• Serge Lang. *Elliptic curves Diophantine analysis*, Springer Verlag, Grundlehren der mathematischen Wissenschaften, (GL **231**) (1978).

https://doi.org/10.1007/978-3-662-07010-9

Chapter I Elliptic functions

• Álvaro Lozano-Robledo. *Elliptic Curves, Modular Forms, And Their L-functions*, Student Mathematical Library IAS Park City Mathematical subseries Volume **58** (2011).
http://dx.doi.org/10.1090/stml/058
https://vdoc.pub/documents/elliptic-curves-modular-forms-and-their-l-functions-1s4ijp05ad4o
https://www.ams.org/books/stml/058/stml058-endmatter.pdf

Chapter 1 Introduction
Chapter 2 Elliptic curves
Chapter 3 Modular curves

• David Masser. *Auxiliary Polynomials in Number Theory*, (Cambridge Tracts in Mathematics). Cambridge: Cambridge University Press (2016).

doi:10.1017/CBO9781107448018

Chapter 20 Elliptic functions

- James S. Milne

Elliptic Curves.

https://www.jmilne.org/math/Books/ectext6.pdf

- MIT Open Courseware Notes

https://math.mit.edu/classes/18.783/2019/syllabus.html

- Jan Nekovar. *Elliptic functions and elliptic curves (A Classical Introduction)*, (2004).

https://webusers.imj-prg.fr/~jan.nekovar/co/ln/el/el1.pdf

- Jean-Pierre Serre. *A course in arithmetic*, Springer Verlag, Graduate Texts in Mathematics (GTM, volume **7**), (1973).

https://doi.org/10.1007/978-1-4684-9884-4
https://www.math.purdue.edu/~jlipman/MA598/
http://www.emule-books.narod.ru/books1.html 8114

Chapter VII Modular forms

• J. H. Silverman. *The Arithmetic of Elliptic Curves,* Springer Verlag Graduate Texts in Mathematics (GTM, volume **106**) 2nd ed. (2009).
https://doi.org/10.1007/978-1-4757-1920-8
https://www.math.brown.edu/johsilve/AECHome.html
http://www.emule-books.narod.ru/books1.html 8187
https://link.springer.com/book/10.1007/978-1-4757-1920-8

Chapter III The Geometry of Elliptic Curves;
Chapter V Elliptic Curves over Finite Fields,
Chapter VI Elliptic Curves over $\mathbb{C}$
Chapter VIII Elliptic Curves over Global Fields.

• J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. GTM151, Springer, 1994.

https://link.springer.com/book/10.1007/978-1-4612-0851-8

• Peter Stevenhagen. *Complex elliptic curves* (2019).
http://www.rnta.eu/Montevideo2019/cimpa2019.pdf

• Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*, Second Edition (Discrete Mathematics and Its Applications) **50**, Taylor & Francis Group, LLC (2008).
https://doi.org/10.1201/9781420071474
https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/EllipticCurvesNumberTheoryAndCryptography2n.pdf
http://www.emule-books.narod.ru/books1.html 2385

Chapter 1 Introduction
Chapter 2 The basic theory
Chapter 4 Elliptic curves over finite fields
Chapter 6 Elliptic curve cryptography

CIMPA School January 2023

http://www.rnta.eu/Manila2022/

University of the Philippines
Diliman, Manila

Introduction to Galois Representations and Modular Forms and their Computational Aspects

Elliptic curves with complex multiplication.

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

http://www.imj-prg.fr/~michel.waldschmidt/