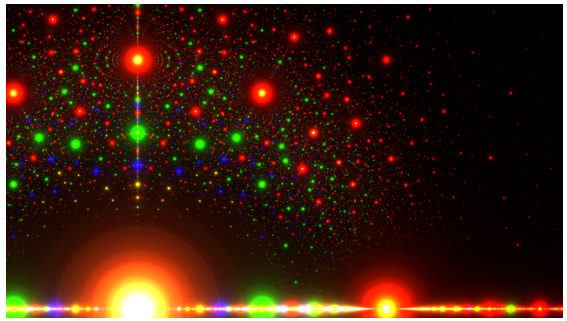
26/08/2022

African Institute for Mathematical Sciences (AIMS), M'Bour, Senegal
CIMPA Research School on cryptography, theoretical
and computational aspects of number theory.
https://indico.math.cnrs.fr/event/5731/



Elementary Approach to Elliptic Curves

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris
http://www.imj-prg.fr/~michel.waldschmidt/

Periods

Group of periods of a meromorphic function $f : \mathbb{C} \to \mathbb{P}_1(\mathbb{C})$:

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

If f is a non constant meromorphic function on $\mathbb{C}$, the group of periods of f is a discrete subgroup of $\mathbb{C}$.

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).*

Exponential and trigonometric functions

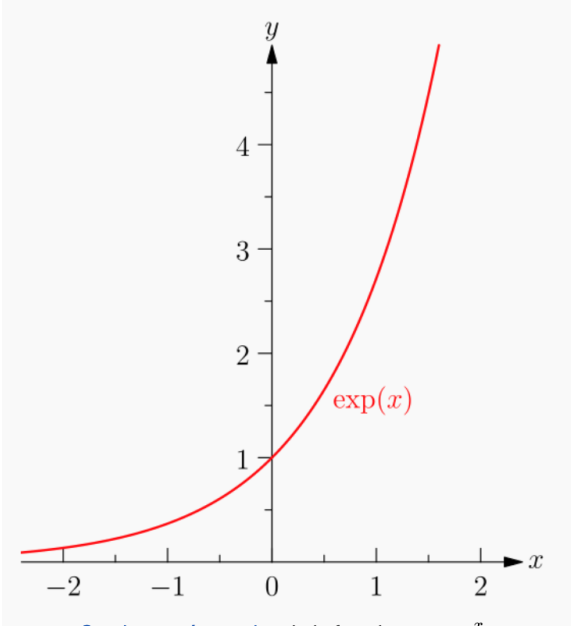
$$\mathrm{e}^z = \sum_{n\geq 0} \frac{z^n}{n!} = \cosh(z) + \sinh(z),$$

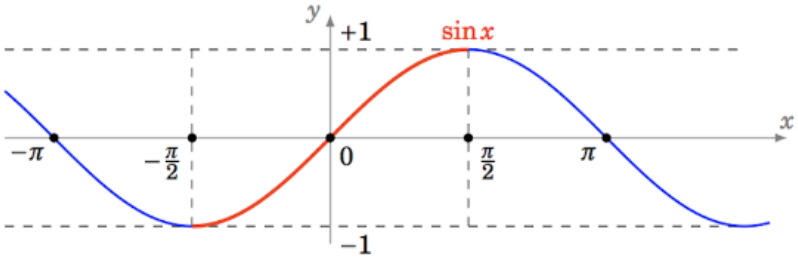
$$\cosh(z) = \sum_{k\geq 0} \frac{z^{2k}}{(2k)!}, \qquad \sinh(z) = \sum_{k\geq 0} \frac{z^{2k+1}}{(2k+1)!}$$

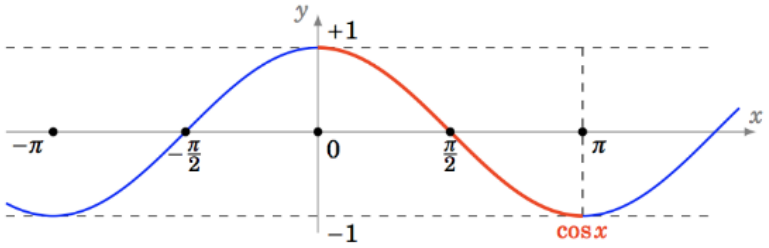
$$\mathrm{e}^{iz} = \cos(z) + i\sin(z),$$

$$\cos(z) = \sum_{k\geq 0} (-1)^k \frac{z^{2k}}{(2k)!}, \qquad \sin(z) = \sum_{k\geq 0} (-1)^k \frac{z^{2k+1}}{(2k+1)!}.$$

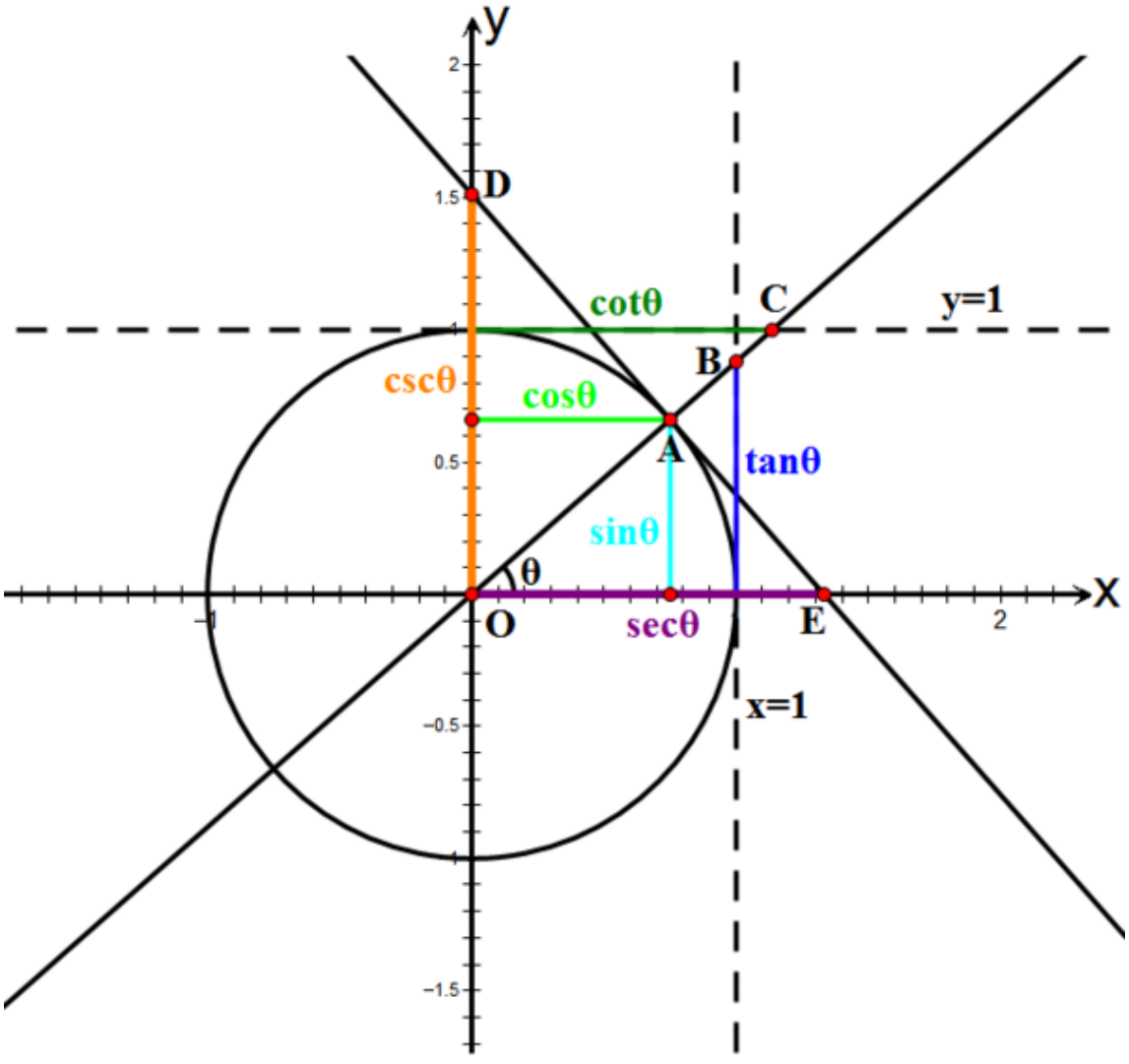
Exponential, sinus, cosinus







The six trigonometric functions



Cotangente

For $0 < |z| < \pi$,

$$\begin{aligned}
\cot z &= \frac{\cos z}{\sin z} \\
&= \frac{\mathrm{d}}{\mathrm{d}z} \log \sin z \\
&= \sum_{n=0}^{\infty} \frac{(-1)^n 2^{2n} B_{2n}}{(2n)!} z^{2n-1} \\
&= z^{-1} - \frac{1}{3} z - \frac{1}{45} z^3 - \frac{2}{945} z^5 - \cdots \\
&= \frac{1}{z} + \sum_{n \in \mathbb{Z} \setminus \{0\}} \left(\frac{1}{z - n\pi} + \frac{1}{n\pi} \right).
\end{aligned}$$

Bernoulli numbers :

$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ \cdots$

$$\frac{z}{\mathrm{e}^z - 1} = \sum_{n \geq 0} \frac{B_n}{n!} z^n.$$

Isomorphisms of topological groups

Line

$$\mathbb{R} \simeq \mathbb{R}_+^\times \simeq \mathbb{R}^\times/\{\pm 1\}.$$

Circle

$$\begin{array}{ccc} \mathbb{R}/\mathbb{Z} & \simeq & \mathbb{U} \\ \cup & & \cup \\ \mathbb{Q}/\mathbb{Z} & \simeq & \mathbb{U}_{\mathrm{tors}}. \end{array}$$

Cylinder

$$\mathbb{C}/2\pi\mathrm{i}\mathbb{Z} \simeq \mathbb{C}^\times.$$

Linear algebraic groups

GL_n, $\mathbb{G}_a$, $\mathbb{G}_m$, Circle $\mathcal{C} : x^2 + y^2 = 1$.

$$\mathrm{GL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \det(M) \neq 0\}.$$

$$\mathbb{G}_m(K) = K^\times = \mathrm{GL}_1(K).$$

$$\mathbb{G}_a(K) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in K \right\} \subset \mathrm{GL}_2(K).$$

$$\mathcal{C}(K) = \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in K \right\} \subset \mathrm{GL}_2(K).$$

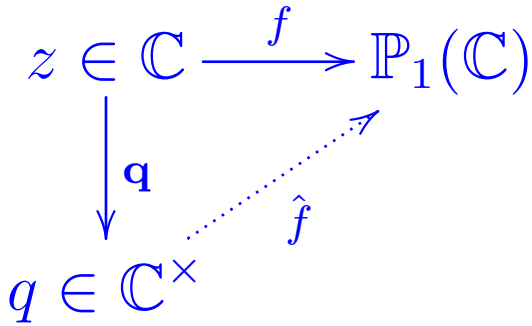
Periodic functions : q–expansion

If f is a periodic meromorphic function with period $\lambda \neq 0$, there exists a function $\hat{f}$ meromorphic on $\mathbb{C}^\times$ such that

$$f(z) = \hat{f}(\mathrm{e}^{2\pi \mathrm{i} z/\lambda})$$

and conversely.

$f = \hat{f} \circ \mathbf{q}$ with $\mathbf{q}(z) = \mathrm{e}^{2\pi \mathrm{i} z/\lambda}$ $\qquad$ $\mathbf{q} : z \mapsto q = \mathrm{e}^{2\pi \mathrm{i} z/\lambda}$.



q–expansion (Fourier) :

$$\hat{f}(q) = \sum_{n \in \mathbb{Z}} a_n q^n.$$

Periods : Maxime Kontsevich and Don Zagier

Maxime Kontsevich

Don Zagier

A *period* is a complex number with real and imaginary parts given by absolutely convergent integrals of rational fractions with rational coefficients on domains of $\mathbb{R}^n$ defined by (in)equalities involving polynomials with rational coefficients

Periods, *Mathematics unlimited—2001 and beyond*, Springer 2001, 771–808.

The numbers $2\pi\mathrm{i}$ and π are periods

$$2\pi\mathrm{i} = \int_{|z|=1} \frac{\mathrm{d}z}{z}.$$

$$\begin{aligned}
\pi &= \iint_{x^2+y^2\leq 1} \mathrm{d}x\mathrm{d}y \\
&= \int_{-1}^{1} \frac{\mathrm{d}x}{\sqrt{1-x^2}} \\
&= \int_{-\infty}^{\infty} \frac{\mathrm{d}x}{1+x^2} \\
&= 4\int_{0}^{1} \frac{\mathrm{d}x}{1+x^2} \\
&= \frac{22}{7} - \int_0^1 \frac{x^4(1-x^4)\mathrm{d}x}{1+x^2}.
\end{aligned}$$

Primitive or reduced pair of periods

Fundamental pair of periods of an elliptic curve : basis (λ_1, λ_2) of the lattice of periods.

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 $\operatorname{Im} \frac{\lambda_2}{\lambda_1} > 0$.

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.

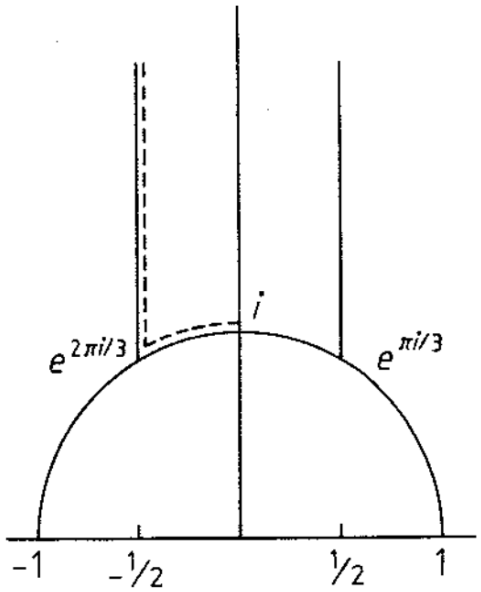
Criterion for a fundamental pair to be primitive

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 any non constant elliptic function f, there exists a pair of fundamental periods (λ_1, λ_2) such that $\tau = \lambda_2/\lambda_1$ satisfies $\operatorname{Im}\tau > 0, \quad |\tau| \geq 1,$ $-\frac{1}{2} \leq \operatorname{Re}\tau < \frac{1}{2},$ with $\operatorname{Re}\tau \leq 0$ 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

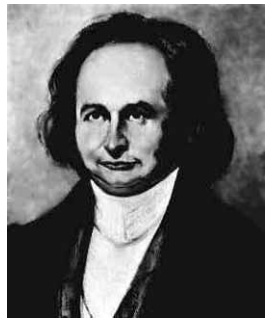
$$S^2 = (ST)^3 = I.$$

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

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*.

Jacobi, Dirichlet's box principle



Karl Jacobi

1804–1851

Lejeune-Dirichlet

1805 - 1859

Exercise.

Let x_1, x_2, x_3 be three complex numbers which are linearly independent over $\mathbb{Q}$. Then there exists a constant $c > 0$ such that for $N \geq 1$,

$$\min\{|a_1x_1 + a_2x_2 + a_3x_3| \ ;$$

$$(a_1, a_2, a_3) \in \mathbb{Z}^3 \setminus \{(0,0,0)\},\ \max\{|a_1|, |a_2|, |a_3|\} \leq N\} \leq \frac{c}{N}.$$

https://mathshistory.st-andrews.ac.uk/Biographies/Jacobi/
https://mathshistory.st-andrews.ac.uk/Biographies/Dirichlet/

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

$$P = \{t_1e_1 + t_2e_2 \mid -1 \leq t_1, t_2 \leq 1\}.$$

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 $x_i = a_iy_i$. □

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 $ad - bc = \pm 1$.

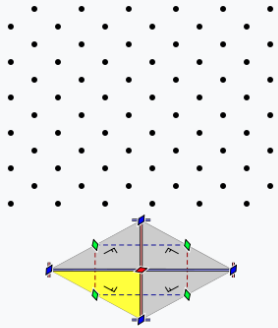
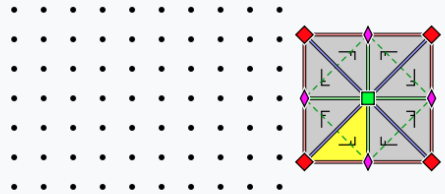
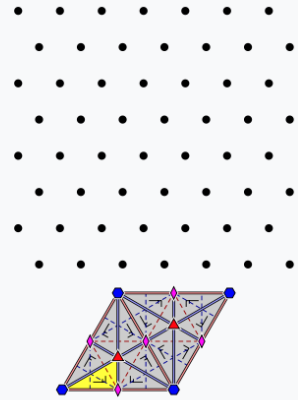
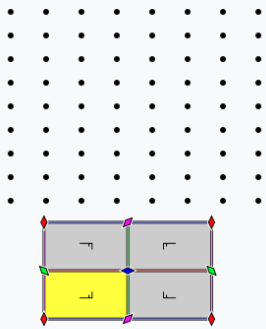
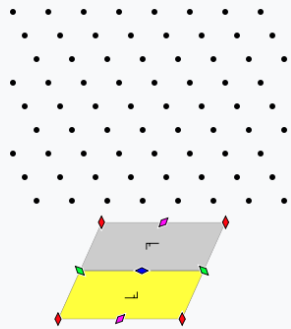
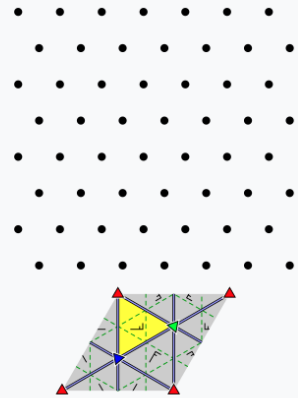
Condition $\mathrm{Im}\,\tau > 0$: $\det = +1$, $\mathrm{SL}_2(\mathbb{Z})$.

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), [∞,2+,∞]	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, [∞,2,∞]	**p2, 2222, [∞,2,∞]+**	**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).

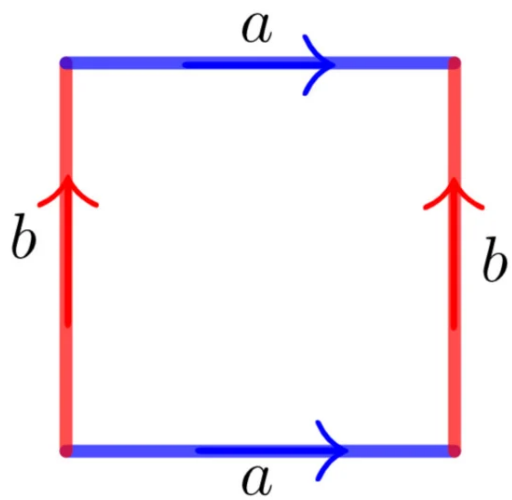
Example : let (λ_1, λ_2) be a basis of Λ as a $\mathbb{Z}$–module. Then the *fundamental parallelogram*

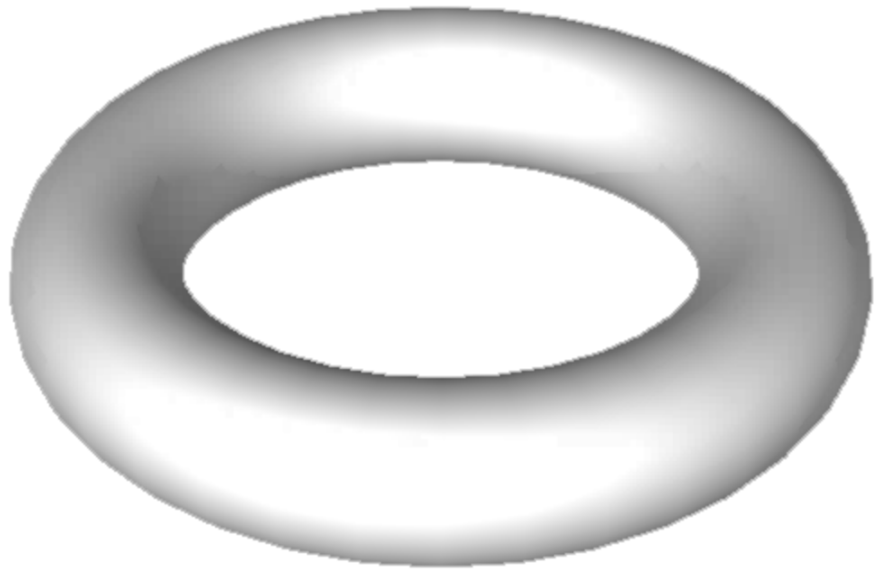
$$\mathcal{P} = \{t_1\lambda_1 + t_2\lambda_2 \mid 0 \leq t_1, t_2 < 1\}$$

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

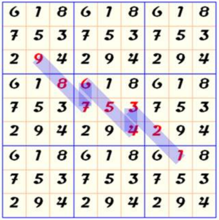
Torus

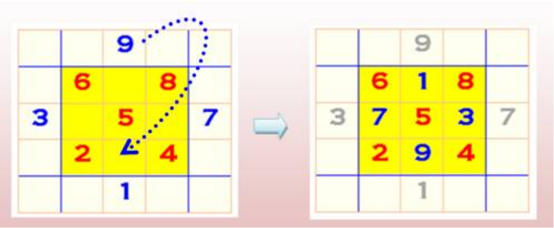
Let Λ be a lattice in $\mathbb{C}$. The quotient $T = \mathbb{C}/\Lambda$ is a torus.





Magic square





http://villemin.gerard.free.fr/Wwwgvmm/CarreMag/CMordre3.htm

Magic square 5×5

3	16	9	22	15	65
20	8	21	14	2	65
7	25	13	1	19	65
24	12	5	18	6	65
11	4	17	10	23	65
65	65	65	65	65	65

http://villemin.gerard.free.fr/Wwwgvmm/CarreMag/CaMagTdM.htm

Magic square 9×9

$$\begin{bmatrix}
47 & 58 & 69 & 80 & 1 & 12 & 23 & 34 & 45 \\
57 & 68 & 79 & 9 & 11 & 22 & 33 & 44 & 46 \\
67 & 78 & 8 & 10 & 21 & 32 & 43 & 54 & 56 \\
77 & 7 & 18 & 20 & 31 & 42 & 53 & 55 & 66 \\
6 & 17 & 19 & 30 & 41 & 52 & 63 & 65 & 76 \\
16 & 27 & 29 & 40 & 51 & 62 & 64 & 75 & 5 \\
26 & 28 & 39 & 50 & 61 & 72 & 74 & 4 & 15 \\
36 & 38 & 49 & 60 & 71 & 73 & 3 & 14 & 25 \\
37 & 48 & 59 & 70 & 81 & 2 & 13 & 24 & 35
\end{bmatrix}$$

http://villemin.gerard.free.fr/Wwwgvmm/CarreMag/aaaMaths/Diagonal.htm

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

The toric section

Intersection of a torus with a plane (worlds of math & physics)

https://www.lucamoroni.it/toric-sections/

https://arxiv.org/pdf/1708.00803 Luca Moroni (2017)

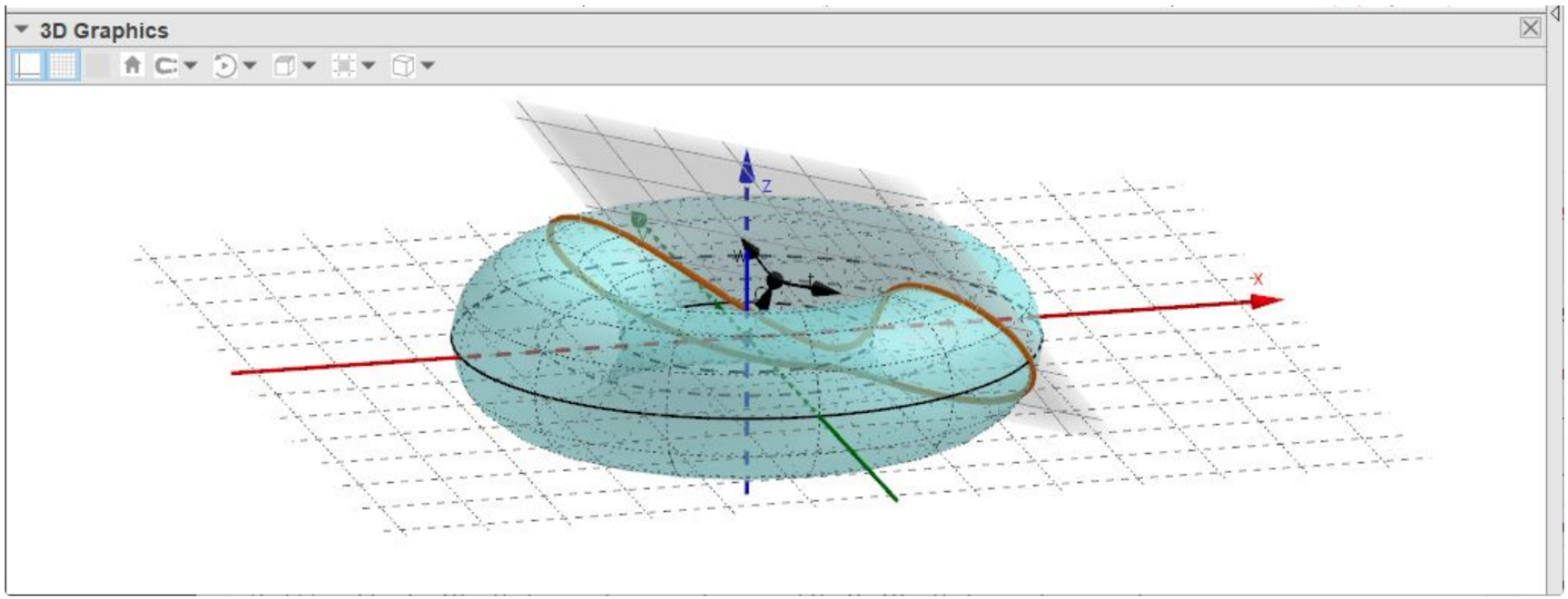


fig. 01 – The torus-Plane Intersection simulation with Geogebra

Cassini ovals

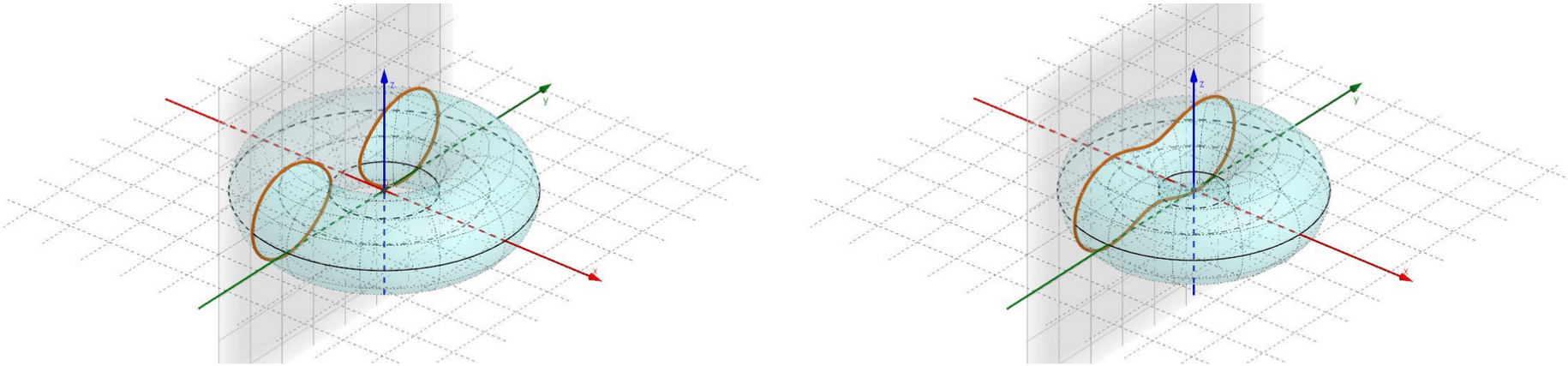
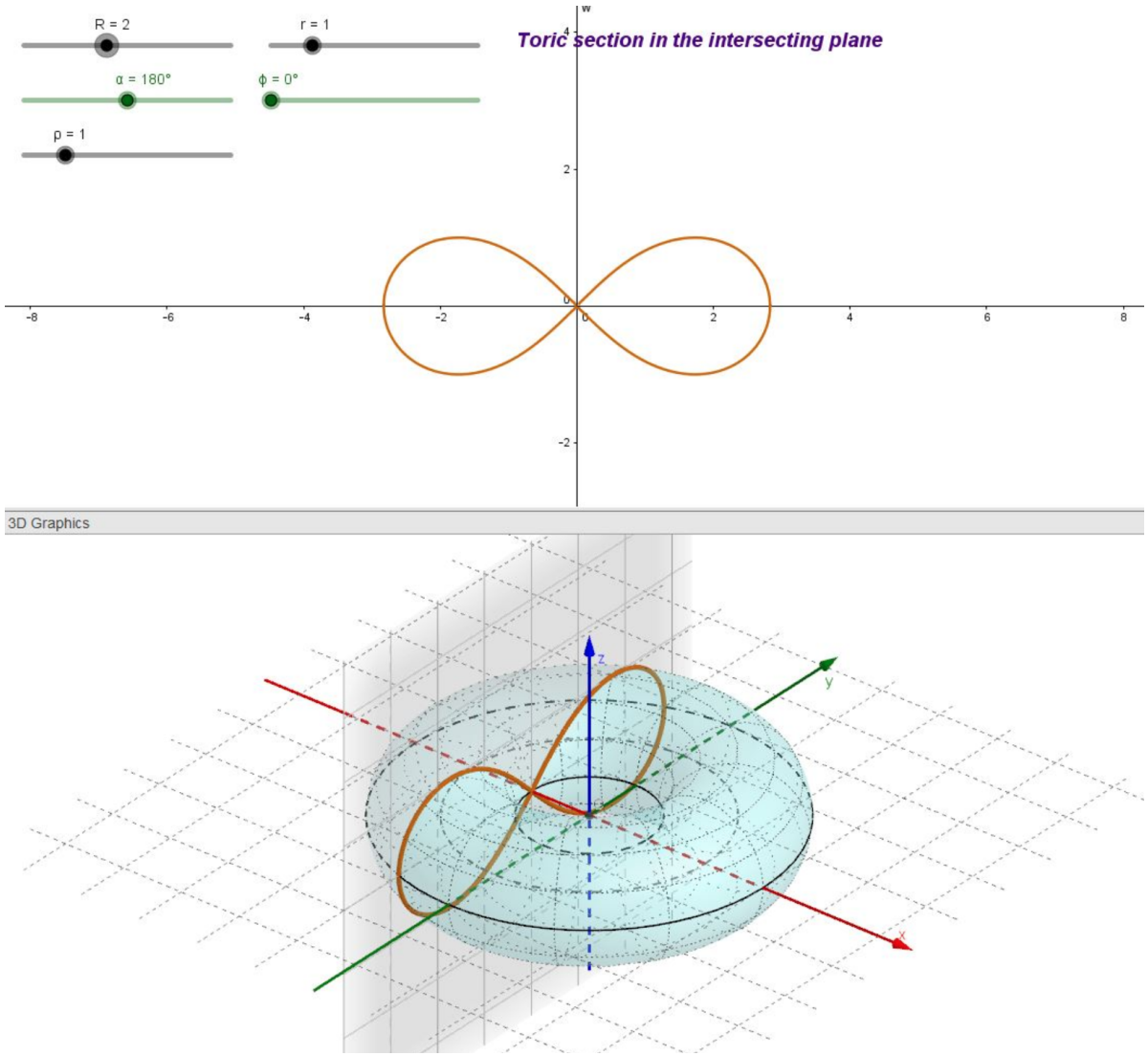


fig. 05 – Two different Cassini's ovals

Lemniscate


R = 2
r = 1
α = 180°
ϕ = 0°
ρ = 1
Toric section in the intersecting plane
3D Graphics
z
y
x

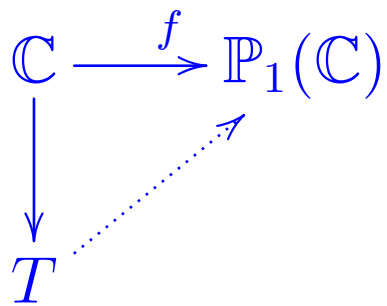
Elliptic function : definition

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 $T := \mathbb{C}/\Lambda$:



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

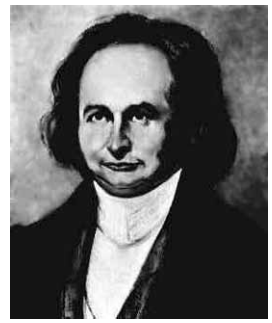
(3) $\sum_{w\in\mathcal{F}} \mathrm{ord}_w(f)\cdot w \in \Lambda$.

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

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

(finite formal sum of points in T 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 $c \in \mathbb{C}^\times$.

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

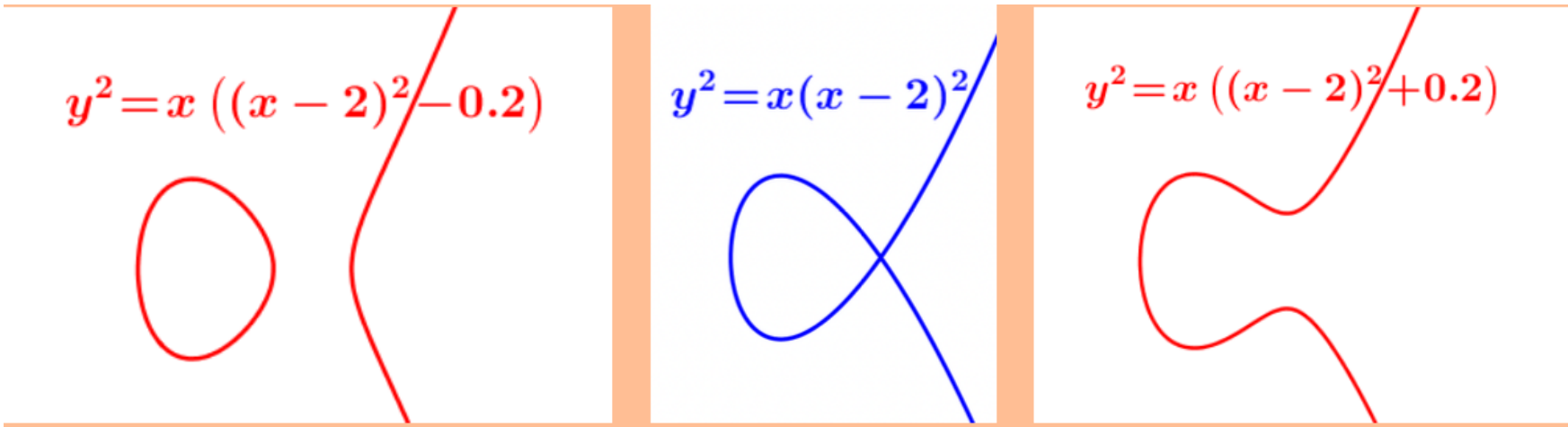
$$e_1 = \wp(\lambda_1/2), \quad e_2 = \wp(\lambda_2/2), \quad e_3 = \wp((\lambda_1 + \lambda_2)/2).$$

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

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

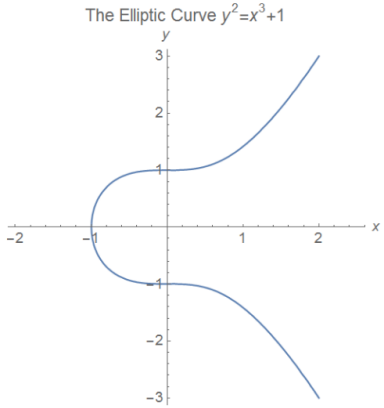
does not vanish.
The curve $y^2t = 4x^3 - g_2xt^2 - g_3t^3$ in $\mathbb{P}_2(\mathbb{C})$ is *smooth* (no singular point).

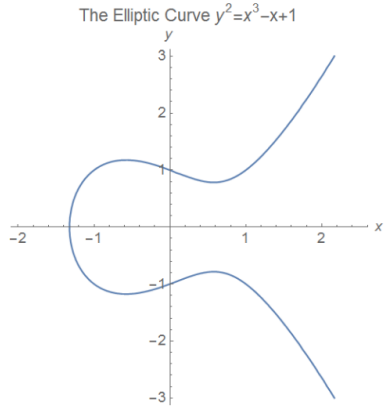
Three real cubics

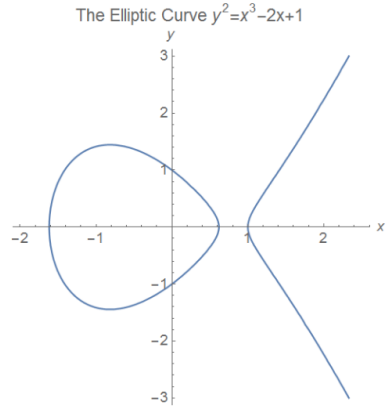


$E(\mathbb{R}) = \{(x : y : t) \in \mathbb{P}_2(\mathbb{R}) \mid y^2 t = 4x^3 - g_2 x t^2 - g_3 t^3\}$.
Point at infinity : $(0 : 1 : 0)$.

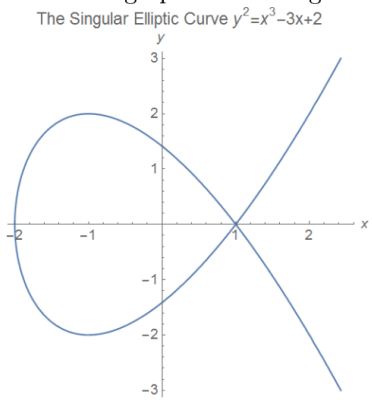
Real cubics

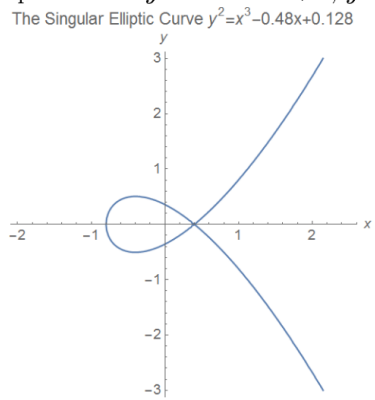


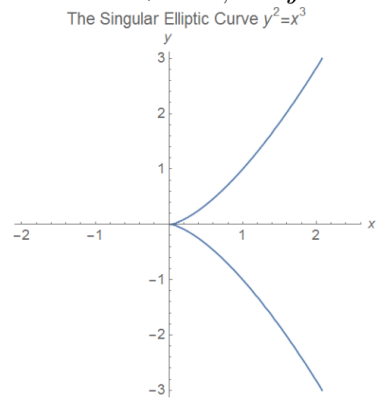




- Here are the graphs of the singular elliptic curves $y^2 = x^3 - 3x + 2$, $y^2 = x^3 - 0.48x + 0.128$, and $y^2 = x^3$:







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

Non degenerate and degenerate elliptic curves

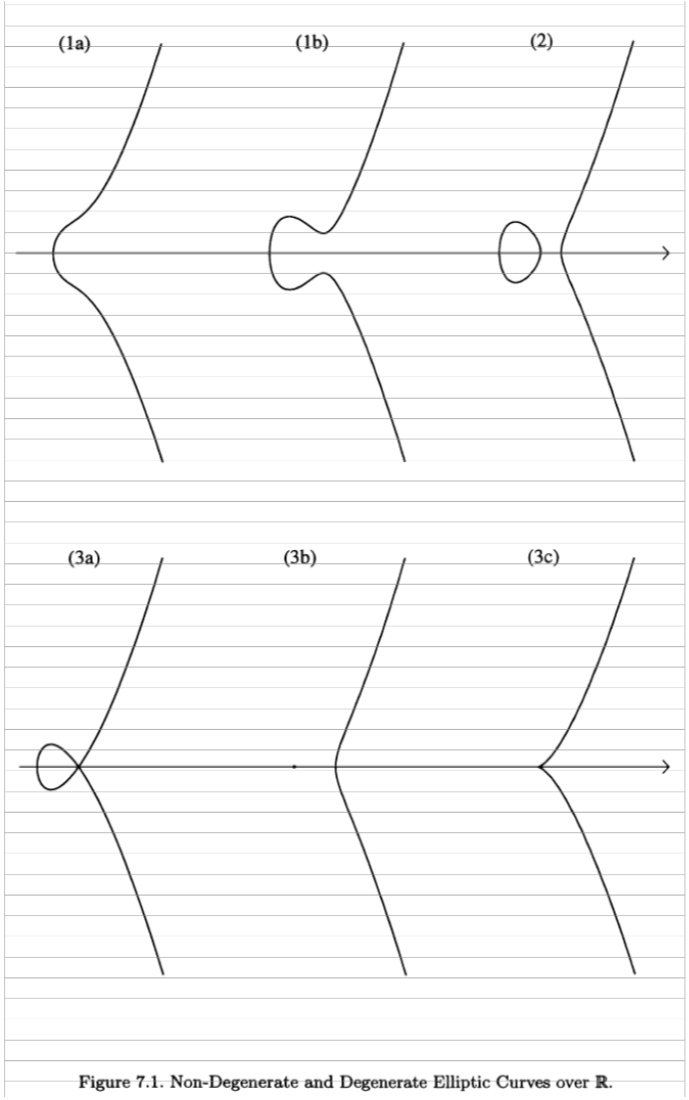


Figure 7.1. Non-Degenerate and Degenerate Elliptic Curves over $\mathbb{R}$.

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

Weierstrass sigma function

K. Weierstrass

Let $\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$ be a lattice in $\mathbb{C}$.
The canonical product of Weierstrass associated with Λ is the Weierstrass *sigma function* σ_Λ defined by

$$\sigma_\Lambda(z) = z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}\right).$$

This function has a simple zero at each point of Λ.

Hadamard canonical products

Jacques Hadamard

1865 - 1963

For $\mathbb{N} = \{0, 1, 2, \ldots\}$:

$$\frac{e^{-\gamma z}}{\Gamma(-z)} = z \prod_{n \geq 1} \left(1 - \frac{z}{n}\right) e^{-z/n}.$$

For $\mathbb{Z}$:

$$\frac{\sin \pi z}{\pi} = z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right).$$

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

Weierstrass zeta function

The logarithmic derivative of the Weierstrass sigma function is the *Weierstrass zeta function*

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

and the derivative of ζ is $-\wp$. The minus sign is selected so that

$$\wp(z) = \frac{1}{z^2} + \text{ a function analytic at } 0.$$

The function ζ is therefore *quasi–periodic* : for any $\lambda \in \Lambda$ there exists $\eta = \eta(\lambda)$ such that

$$\zeta(z+\lambda) = \zeta(z) + \eta.$$

The Weierstrass sigma function

For $\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$ and $\lambda \in \Lambda$,

$$\sigma_\Lambda(z+\lambda) = \chi(\lambda)\mathrm{e}^{\eta(\lambda)(z+\lambda/2)}\sigma_\Lambda(z)$$

where

$$\chi(\lambda) = \begin{cases} -1 & \text{if } \lambda/2 \notin \Lambda, \\ 1 & \text{if } \lambda/2 \in \Lambda. \end{cases}$$

Proof of the Theorem of Abel and Jacobi.

Assume

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

Consider

$$f(z) = \frac{\sigma(z)}{\sigma(z-\ell)} \prod_{w\in\mathcal{F}} \sigma(z-w)^{k_w}.$$

Weierstrass $\wp$ function as a quotient of two entire functions

For $a \in \mathbb{C} \setminus \Lambda$,

$$\wp(z) - \wp(a) = -\frac{\sigma(z-a)\sigma(z+a)}{\sigma(a)^2\sigma(z)^2}.$$

Also

$$\wp'(z) = -\frac{\sigma(2z)}{\sigma(z)^4}.$$

Periods of a Weierstrass elliptic function

A pair of fundamental periods (λ_1, λ_2) is given by

$$\lambda_i = 2\int_{e_i}^{\infty} \frac{\mathrm{d}t}{\sqrt{4t^3 - g_2 t - g_3}}, \qquad (i = 1, 2)$$

where

$$4t^3 - g_2 t - g_3 = 4(t - e_1)(t - e_2)(t - e_3).$$

Examples

Example 1 : $g_2 = 4$, $g_3 = 0$, $j = 1728$

A pair of fundamental periods of the elliptic curve

$$y^2 t = 4x^3 - 4xt^2.$$

is given by

$$\lambda_1 = \int_1^\infty \frac{\mathrm{d}t}{\sqrt{t^3 - t}} = \frac{1}{2}\mathrm{B}(1/4, 1/2) = \frac{\Gamma(1/4)^2}{2^{3/2}\pi^{1/2}} = 2.6220575542\ldots$$

and

$$\lambda_2 = i\lambda_1.$$

Examples (continued)

Example 2 : $g_2 = 0$, $g_3 = 4$, $j = 0$

A pair of fundamental periods of the elliptic curve

$$y^2 t = 4x^3 - 4t^3.$$

is

$$\lambda_1 = \int_1^\infty \frac{\mathrm{d}t}{\sqrt{t^3 - 1}} = \frac{1}{3}\mathrm{B}(1/6, 1/2) = \frac{\Gamma(1/3)^3}{2^{4/3}\pi} = 2.428650648\ldots$$

and

$$\lambda_2 = \varrho\lambda_1$$

where $\varrho = e^{2i\pi/3}$.

Weierstrass sigma function : an example

For $\Lambda = \mathbb{Z} + \mathbb{Z}i$:

$$\sigma_{\mathbb{Z}[i]}(z) = z \prod_{\lambda \in \mathbb{Z}[i] \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2}\right).$$

$$\sigma_{\mathbb{Z}[i]}(1/2) = 2^{5/4}\pi^{1/2}e^{\pi/8}\Gamma(1/4)^{-2} = 0.4749493799\ldots$$

For $\alpha \in \mathbb{Q}(i)$, the number $\sigma_{\mathbb{Z}[i]}(\alpha)$ is algebraic over

$$\mathbb{Q}\big(\pi,\ e^{\pi},\ \Gamma(1/4)\big).$$

Legendre relation

The numbers $\eta(\lambda)$ are the *quasi–periods* of the elliptic curve.
When (λ_1, λ_2) is a pair of fundamental periods, we set $\eta_1 = \eta(\lambda_1)$ and $\eta_2 = \eta(\lambda_2)$.
Legendre relation :

$$\lambda_2\eta_1 - \lambda_1\eta_2 = 2i\pi.$$

this is not Adrien Marie
(1752 – 1833)
but Louis Legendre

Legendre and Fourier

Peter Duren, Changing Faces : The Mistaken Portrait of Legendre.
Notices of American Mathematical Society, **56** (2009) 1440–1443.

Examples

For the curve $y^2t = 4x^3 - 4xt^2$ the quasi–periods associated to the previous fundamental periods are

$$\eta_1 = \frac{\pi}{\lambda_1} = \frac{(2\pi)^{3/2}}{\Gamma(1/4)^2}, \qquad \eta_2 = -i\eta_1,$$

while for the curve $y^2t = 4x^3 - 4t^3$ they are

$$\eta_1 = \frac{2\pi}{\sqrt{3}\lambda_1} = \frac{2^{7/3}\pi^2}{3^{1/2}\Gamma(1/3)^3}, \qquad \eta_2 = \varrho^2\eta_1.$$

Elliptic integrals and ellipses

An ellipse with radii a and b has equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

and the length of its perimeter is

$$2\int_{-b}^{b} \sqrt{1 + \frac{a^2x^2}{b^4 - b^2x^2}}\, \mathrm{d}x.$$

In the same way, the perimeter of a lemniscate

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

is given by an elliptic integral

$$4a\int_{0}^{1} (1 - t^4)^{-1/2}\, \mathrm{d}x.$$

Intersection of two quadratic surfaces

A quartic equation

$$v^2 = au^4 + bu^3 + cu^2 + du + e$$

can be transformed into a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Washington § 2.5.3 : quartic equations.

The intersection of two quadratic surfaces in three dimensional space along with a point in the intersection is usually an elliptic curve. Special case :

$$au^2 + bv^2 = e, \quad cu^2 + dw^2 = f,$$

Washington § 2.5.4 : intersection of two quadratic surfaces

Example :

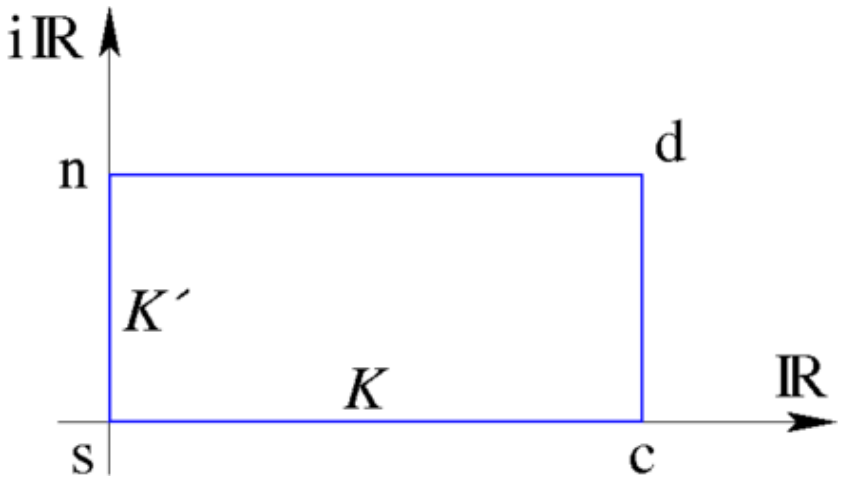
$$u^2 + v^2 = 2, \quad u^2 + 4w^2 = 5$$

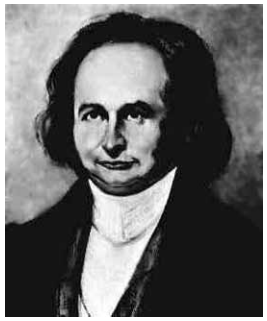
gives

$$y^2 = x^3 + 2x^2 - 5x - 6.$$

Jacobi 12 elliptic functions

Elliptic curve as an intersection of two quadrics : the functions sn and cn.





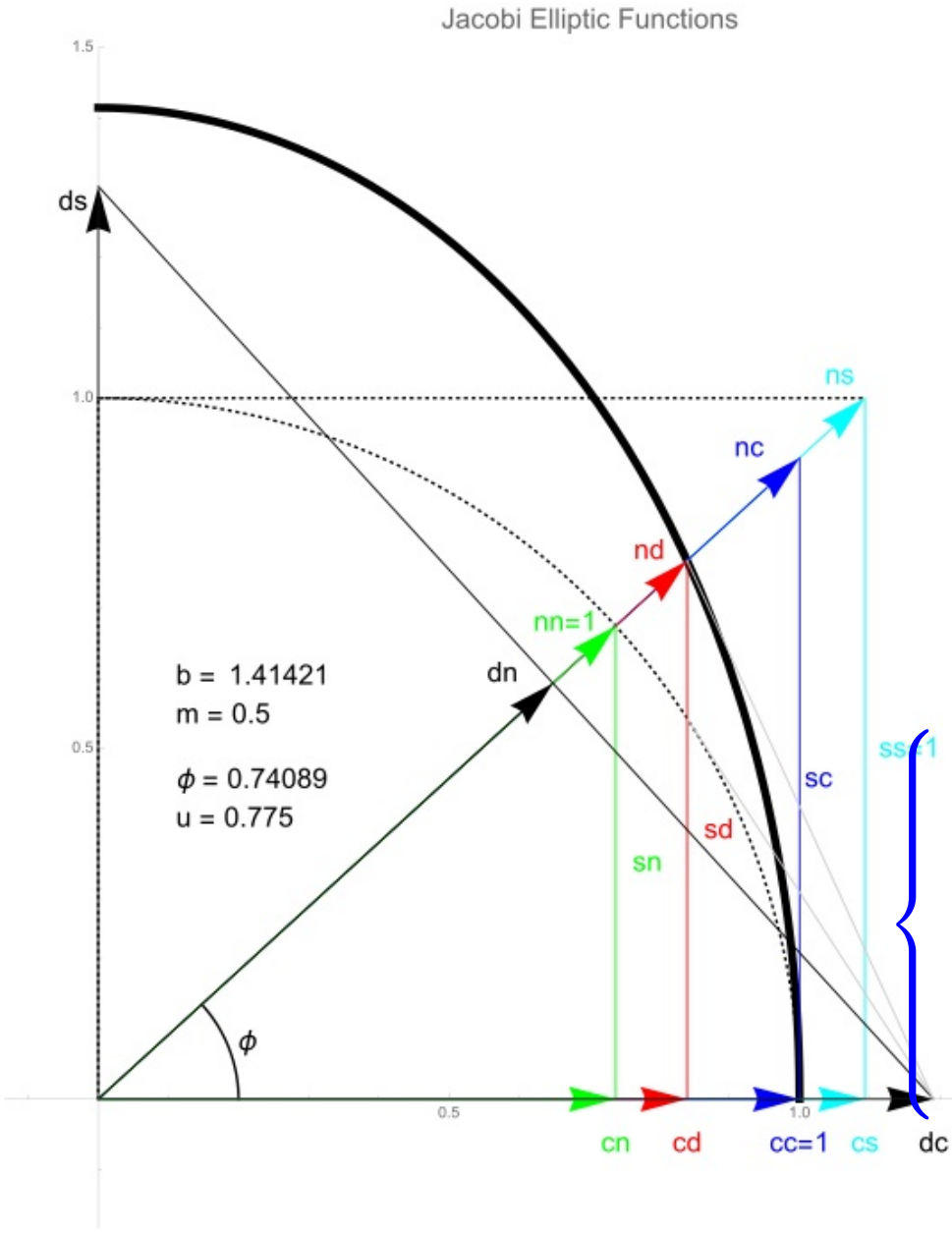
Karl Jacobi

1804–1851

sn sc sd ns nc nd cs cn cd ds dn dc

$$\mathrm{pq} = \frac{\mathrm{pn}}{\mathrm{qn}}.$$

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



$$\mathrm{cn}(s)^2 + \mathrm{sn}(s)^2 = 1,$$

$$\mathrm{dn}(s)^2 + k^2\mathrm{sn}(s)^2 = 1.$$

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}s}\mathrm{sn}(s) = \mathrm{cn}(s)\mathrm{dn}(s), \\ \dfrac{\mathrm{d}}{\mathrm{d}s}\mathrm{cn}(s) = -\mathrm{sn}(s)\mathrm{dn}(s), \\ \dfrac{\mathrm{d}}{\mathrm{d}s}\mathrm{dn}(s) = -k\,\mathrm{sn}(s)\mathrm{cn}(s). \end{cases}$$

The divisor group $\mathrm{Div}(T)$ of a torus T

Let Λ be a lattice, $T = \mathbb{C}/\Lambda$. A *divisor* is a *finite* formal sum of points in T with integer coefficients

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

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.

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.

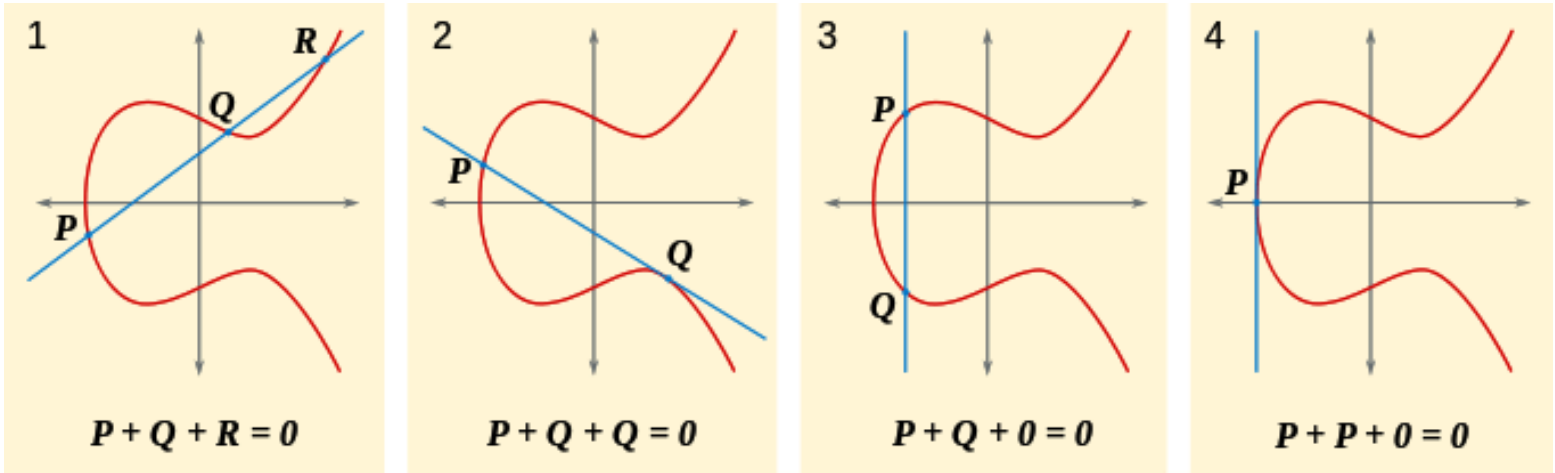
Complex torsion

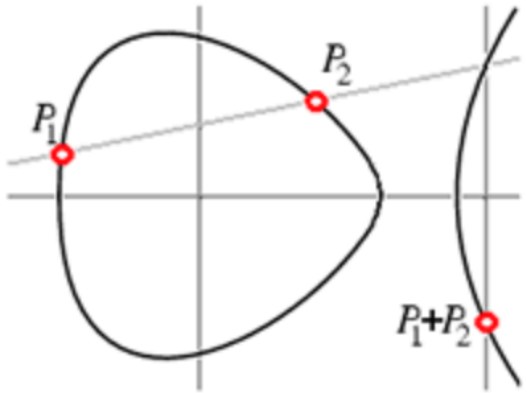
The torsion elements in $E(\mathbb{C})$ are the images under $(\wp : \wp' : 1)$ of the $\mathbb{Q}$–vector space $\mathbb{Q}\Lambda$ spanned by Λ.

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 group law on an elliptic curve

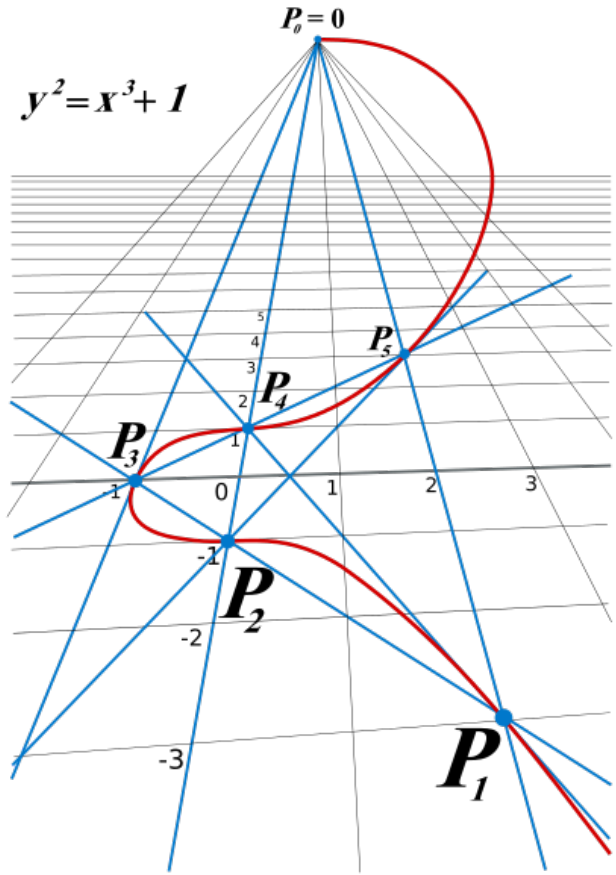




$y^2 = x^3 + 1$

Rational points :

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



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

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.

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

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

Addition formula for the Weierstrass zeta function

Exercise. Addition formula for the Weierstrass zeta function.

$$\zeta(z_1+z_2)=\zeta(z_1)+\zeta(z_2)+\frac{1}{2}\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)},$$

$$\zeta(2z)=2\zeta(z)+\frac{1}{2}\frac{\wp''(z)}{\wp'(z)}.$$

Uniformization Theorem

Theorem. *Let g_2, g_3 be two complex numbers such that ${g_2}^3 \neq 27{g_3}^2$. 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 $\mathbb{C}/\Lambda$.

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

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

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

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

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

Reference : Silverman, Example 4.5 p.74.

Isomorphism between elliptic curves

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

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

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 $\mathbb{Q}$.

q–expansions

Since $j(\tau+1) = j(\tau)$, we can write $j(\tau) = J(\mathrm{e}^{2\pi \mathrm{i} \tau})$.

Set $q = \mathrm{e}^{2\pi \mathrm{i} \tau}$. Then

$$J(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

https://oeis.org/A000521

$$j(\tau) = 1728 \frac{(60G_4)^3}{(60G_4)^3 - 27(140G_6)^2} = 1728 \frac{(20E_4)^3}{\Delta}.$$

q–expansions (continued)

Eisenstein series : $E_{2k}(q)$ is the Fourier expansion of $G_{2k}(\mathbb{Z}+\mathbb{Z}\tau)/(2\zeta(2k))$:

$$P(q) = E_2(q) = 1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n},$$

$$Q(q) = E_4(q) = 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n},$$

$$R(q) = E_6(q) = 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}.$$

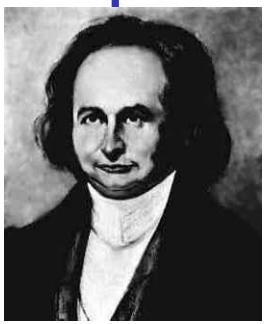
Lambert series

$$\sum_{n=1}^{\infty} q^n\sigma_a(n) = \sum_{n=1}^{\infty}\frac{n^aq^n}{1-q^n}$$

$$\sigma_a(n) = \sum_{d|n} d^a.$$

$$\Delta = 12^{-3}(Q^3 - R^2) \quad \text{and} \quad J = Q^3/\Delta.$$

Jacobi product and Ramanujan function



Karl Jacobi

1804–1851

Srinivasa Ramanujan

1887 – 1920

$$\Delta(q) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

Ramanujan function :

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

$$= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots$$

S. Lang. Elliptic functions. Chap. 18, § 4

W. Kohnen. *A Very Simple Proof of the q-Product Expansion of the Δ-Function*, The Ramanujan Journal, **10** (2005), pp. 71–73.

Ramanujan function

$$(\tau(n))_{n\geq 1} = (1, -24, 252, -1472, 4830, -6048, -16744, 84480, \dots)$$

https://oeis.org/A000594

Ramanujan's Conjecture (1916), Deligne Theorem (1973) : for p prime,

$$|\tau(p)| < 2p^{11/12}.$$

Lehmer's Conjecture : for all $n \geq 1$, $\tau(n) \neq 0$.
Checked for $n < 816212624008487344127999$

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 $A\tau^2 + B\tau + C = 0$.

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

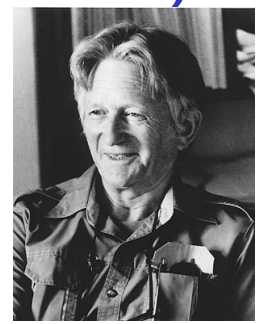
Proof : exercise.

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

Chowla–Selberg Formula (1949, 1967)

SarvadamanChowla

1907 – 1995



Atle Selberg

1917 – 2007

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

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 λ^2 if $\alpha \in \mathbb{Z}$ and $\mathrm{Norm}(\alpha)$ if α is imaginary quadratic ; the degree of the denominator is $\lambda^2 - 1$ and $\mathrm{Norm}(\alpha) - 1$ respectively.

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

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

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

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

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

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 (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.

$$
\begin{aligned}
j((1+i\sqrt{3})/2) &= 0 = 1728 - 3(24)^2 \\
j(i) &= 1728 = 12^3 = 1728 - 4(0)^2 \\
j((1+i\sqrt{7})/2) &= -3375 = (-15)^3 = 1728 - 7(27)^2 \\
j(i\sqrt{2}) &= 8000 = 20^3 = 1728 + 8(28)^2 \\
j((1+i\sqrt{11})/2) &= -32768 = (-32)^3 = 1728 - 11(56)^2 \\
j((1+i\sqrt{19})/2) &= -884736 = (-96)^3 = 1728 - 19(216)^2 \\
j((1+i\sqrt{43})/2) &= -884736000 = (-960)^3 = 1728 - 43(4536)^2 \\
j((1+i\sqrt{67})/2) &= -147197952000 = (-5280)^3 = 1728 - 67(46872)^2 \\
j((1+i\sqrt{163})/2) &= -262537412640768000 = (-640320)^3 \\
&= 1728 - 163(40133016)^2 \\
j(i\sqrt{3}) &= 54000 = 2(30)^3 = 1728 + 12(66)^2 \\
j(2i) &= 287496 = (66)^3 = 1728 + 8(189)^2 \\
j((1+3i\sqrt{3})/2) &= -12288000 = -3(160)^3 = 1728 - 3(2024)^2 \\
j(i\sqrt{7}) &= 16581375 = (255)^3 = 1728 + 7(1539)^2 \\
j((1+i\sqrt{15})/2) &= \frac{-191025 - 85995\sqrt{5}}{2} \\
&= \frac{1-\sqrt{5}}{2}\left(\frac{75+27\sqrt{5}}{2}\right)^3 = 1728 - 3\left(\frac{273+105\sqrt{5}}{2}\right)^2 \\
j((1+i\sqrt{23})/2) &= -(8207500\theta^2 + 10841250\theta + 6167500) \\
&= -(25\theta^2 + 55\theta + 35)^3 \\
&= 1728 - (3\theta^2 - 4)(406\theta^2 + 511\theta + 273)^2,
\end{aligned}
$$

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

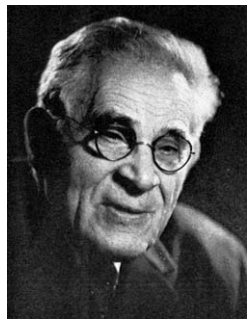
Henri Cohen. *A course in computational algebraic number theory* § 7.2.3 Examples.

The group of rational points on an elliptic curve

Conjecture (Henri Poincaré, 1901) : finitely many points are sufficient to deduce all rational points by the chord and tangent method.

Henri Poincaré

1854 – 1912



Louis Mordell

1888 – 1972

André Weil

1906 – 1998

Theorem (Mordell, 1922). *If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated : there exists a nonnegative integer r (the* Mordell-Weil rank *of the curve over $\mathbb{Q}$) such that*

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

and $E(\mathbb{Q})_{\mathrm{tors}}$ is a finite group.

Mordell–Weil Theorem

If E is an elliptic curve over a number field K, then the abelian group $E(K)$ is finitely generated.

$$E(K) = E(K)_{\text{tors}} \times \mathbb{Z}^r$$

with $r \geq 0$ while $E(K)_{\text{tors}}$ is a finite group.
(André Weil, 1928 : generalization to abelian varieties).

The *weak Mordell–Weil Theorem* : If E is an elliptic curve over K, then for $m \geq 2$ the quotient $E(K)/mE(K)$ is a finite group.

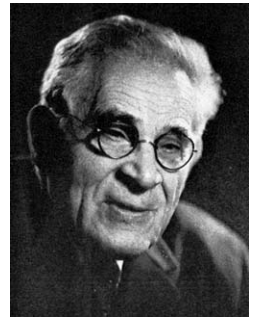
References for the proof : Silverman, Chap. VIII

Mordell's Conjecture, Faltings's Theorem

Mordell's Conjecture : 1922. Faltings's Theorem (1983). The set of rational points on a number field of a curve of genus ≥ 2 is finite.

Jacques Hadamard

1865 - 1963



Louis Mordell

1888 – 1972

Gerd Faltings

Weil's thesis : 1928. Hadamard's comment.

Antoine Chambert-Loir. La conjecture de Mordell : origines, approches, généralisations. Séminaire Betty B., Septembre 2021 5e année, 2021–2022

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

Theorem (Nagell-Lutz). *Suppose E is an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 - Ax - B$ where A and B are integers and let $D = 4A^3 - 27B^2$ be the discriminant of E. If $P = (x, y)$ is a rational point of finite order, then x and y are integers. Furthermore, either $y = 0$ or y^2 divides D.*

Trygve Nagell

1895 – 1988

Journal für die reine und angewandte Mathematik. **177** (1937) : 238–247.

Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques.

Par Mademoiselle *Elisabeth Lutz* à Strasbourg.

Théorème III. *Soit $y^2 = x^3 - Ax - B$ une cubique de genre 1 à coefficients entiers rationnels. Tout point $P(x, y)$ à coordonnées rationnelles, et d'ordre fini dans le groupe des points rationnels sur la cubique, est à coordonnées entières, et tel que y^2 soit égal à 0 ou à un diviseur de $4A^3 - 27B^2$.*

Élisabeth Lutz

1914 – 2008

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

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

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

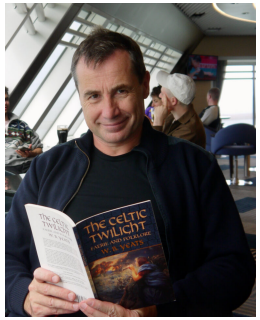
(i) $\mathbb{Z}/n\mathbb{Z}$, with $1 \leq n \leq 10$ or $n = 12$,
(ii) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2m\mathbb{Z})$ with $1 \leq m \leq 4$.

Barry Mazur

The order of $E(\mathbb{Q})_{\text{tors}}$ 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/

Rank of an elliptic curve over $\mathbb{Q}$

The following curve has rank ≥ 28

Noam Elkies

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x$$
$$+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Noam D. Elkies, $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$. May 3, 2006. Email to the NMBRTHRY mailing list.

https://listserv.nodak.edu/cgi-bin/wa.exe?A0=NMBRTHRY

Zev Klagsbrun, Travis Sherman, James Weigandt

The Elkies Curve has Rank 28 Subject only to GRH (2016)

https://arxiv.org/abs/1606.07178

Largest known exact value for the rank of an elliptic curve over $\mathbb{Q}$

The following curve has rank 20 (Elkies-Klagsbrun, 2020)

$$y^2 + xy + y = x^3 - x^2 - 244537673336319601463803487168961769270757573821859853707x + 96171018205318303454622297925880681774327068202896443423895783098989843815112149993 1$$

Andrej Dujella home page

https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html

Heuristic

Jennifer Park, Bjorn Poonen, John Voight, Melanie Matchett Wood

A heuristic for boundedness of ranks of elliptic curves

https://doi.org/10.48550/arXiv.1602.01431
[v3] Tue, 10 Jul 2018

We present a heuristic that suggests that ranks of elliptic curves E over $\mathbb{Q}$ are bounded. In fact, it suggests that there are only finitely many E of rank greater than 21. Our heuristic is based on modeling the ranks and Shafarevich–Tate groups of elliptic curves simultaneously, and relies on a theorem counting alternating integer matrices of specified rank. We also discuss analogues for elliptic curves over other global fields.

https://math.mit.edu/~poonen/papers/bounded-ranks.pdf

$$y^2 = x^3 + 109858299531561$$

$$E(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}^5.$$

$$E(\mathbb{Q})_{\text{tors}} = \{0_E, P, 2P\}, \quad P = (0, 10481331)$$

Five points generating $E(\mathbb{Q})$ modulo torsion :

$$(735532,630902573),$$
$$(49704,15252915),$$
$$(-4578,10476753),$$
$$(-15260,10310419),$$
$$(197379,88314450).$$

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

$$y^2 = x^3 - 36x$$

$E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.

$$E(\mathbb{Q})_{\text{tors}} = \{0_E, (0,0), (6,0), (-6,0)\}$$

$E(\mathbb{Q})$ modulo torsion is generated by the point of infinite order $(12, 36)$.

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

Congruent numbers

A congruent number is a positive integer that is the area of a right triangle with three rational number sides The sequence of (integer) congruent numbers starts with

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, \ldots$$

(sequence A003273 in The On-Line Encyclopedia of Integer Sequences OEIS.)

A positive integer n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2 x$ has a rational point of infinite order.
Assuming BSD, this is equivalent to its L-function having a zero at $s = 1$.

Criterion of J. Tunnell (1983).

Jerrold Bates Tunnell

1950 – 2022

For $n > 0$ odd squarefree, let R be the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ and S the number of triples of integers satisfying $2x^2 + y^2 + 32z^2 = n$.
If $R \neq 2S$, then n is not congruent.
If $R = 2S$, if we assume weak BSD for the curve $y^2 = x^3 - n^2x$, then n is congruent.

Example : for $n \equiv 5, 6, 7 \mod 8$ squarefree, $R = S = 0$.

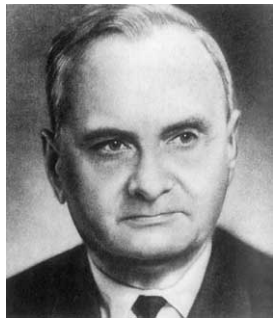
Integer points : Siegel Theorem (1929)

Let g_2 and g_3 be two rational integers with ${g_2}^3 \neq {g_3}^2$. Then the set of $(x, y) \in \mathbb{Z}^2$ such that $y^2 = 4x^3 - g_2 x - g_3$ is finite.

C.L. Siegel

1896 – 1981

Integer points on curves : effective results



A.O. Gel'fond

(1906 – 1968)

Alan Baker

1939 - 2018

- Thue equation $F(x, y) = m$
- Elliptic equation $y^2 = 4x^3 - g_2x - g_3$
- Mordell equation $y^2 = x^3 + k$
- Hyperelliptic equation $y^2 = f(x)$
- Superelliptic equation $y^m = f(x)$

Elliptic curves over finite fields

Equation of a projective plane cubic in any characteristic :

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3.$$

Frobenius endomorphism Φ_q of $E(\mathbb{F}_q)$: $\Phi_q(x, y) = (x^q, y^q)$.

Torsion points on $E(\mathbb{F}_q)$: any rational point is torsion !

For $N \geq 2$ not divisible by the characteristic of $\mathbb{F}_q$, the kernel of the map

$$\begin{array}{ccc} E(\mathbb{F}_q) & \xrightarrow{[N]} & E(\mathbb{F}_q) \\ P & \longmapsto & NP \end{array}$$

is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$.

The Hasse bound

Helmut Hasse

1898 – 1979

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then

$$|\mathrm{Card}E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

There exists an imaginary quadratic integer α satisfying $\alpha\bar{\alpha} = q$ such that

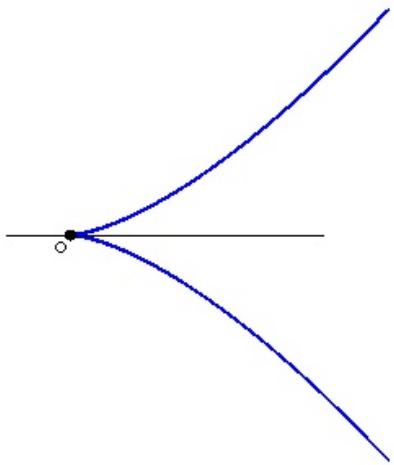
$$\mathrm{Card}E(\mathbb{F}_{q^m}) = q^m + 1 - \alpha^m - \bar{\alpha}^m.$$

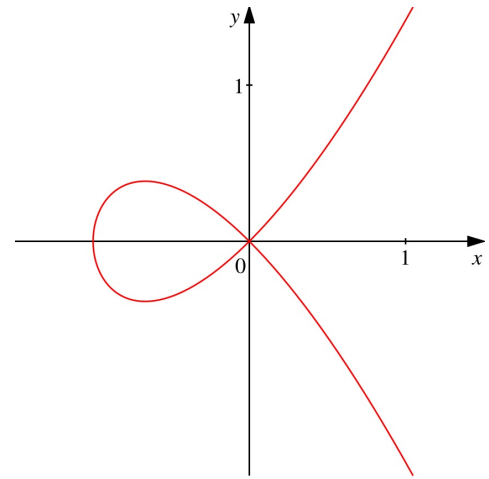
Reduction of an elliptic curve over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$ given as a projective plane cubic with equation

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3.$$

where a_i are integers. Let p be a prime number. The reduction of E modulo p has at most one singular point, which is either a *cusp* or a *node* :





Reduction modulo p

Cusp : a single tangent like $y^2 = x^3$.
Node : two distinct tangents like $y^2 + axy + bx^2 = x^3$ where $y^2 + axy + bx^2 = (y - \alpha x)(y - \alpha' x)$.
The polynomial $y^2 + axy + bx^2 = x^3$ is

- irreducible over $\mathbb{F}_p$ if $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$,
- reducible over $\mathbb{F}_p$ if $\alpha \in \mathbb{F}_p$.

The elliptic curve E over $\mathbb{Q}$ has

- *good reduction at* p if the reduced curve modulo p is smooth,
- *additive reduction at* p if there is a singularity with a single tangent,
- *multiplicative* or *semi–stable reduction at* p if there is a singularity with two distinct tangents.

Reduction modulo p

For $y^2 = x^3 - 27c_4x - 54c_6$, the reduction if

- good if p does not divide the discriminant Δ,
- additive if p divides Δ and c_4,
- multiplicative if p divides Δ but not c_4.

Beware. One needs to consider the *minimal discriminant* of the curve. For $p \notin \{2, 3\}$, the condition is p^4 does not divide c_4 or p^6 does not divide c_6. The invariant j is

$$j = \frac{{c_4}^3}{\Delta}$$

and ${c_4}^3 - {c_6}^2 = 1728\Delta$.
Given an elliptic curve E over $\mathbb{Q}$, the reduction of E at p is good for all but finitely many p.

Multiplicative reduction modulo p

Assume E has multiplicative reduction at p : there are two distinct tangents at the singularity. The multiplicative reduction at p of E is

- *split* if the two tangents are defined over $\mathbb{F}_p$,
- *non* split otherwise (then the two tangents are defined over $\mathbb{F}_{p^2}$).

Reference : M. Hindry, Arithmétique, Chap. V Courbes elliptiques.

Hasse L–function of the curve : local factors

If E has good reduction at p, define $a_p = p + 1 - \mathrm{Card} E(\mathbb{F}_p)$ and

$$L_p(E, s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

If E has split multiplicative reduction at p, define

$$L_p(E, s) = (1 - p^{-s})^{-1}.$$

If E has non split multiplicative reduction at p, define

$$L_p(E, s) = (1 + p^{-s})^{-1}.$$

If E has additive reduction at p, define

$$L_p(E, s) = 1.$$

The conductor of the curve

$$N_E = \prod_p p^{n(E,p)}$$

with

- $n(E,p) = 0$ for p a prime of good reduction,
- $n(E,p) = 1$ for p a prime with multiplicative reduction,
- $n(E,p) = 2 + \delta_{E,p}$ for p a prime with additive reduction.

$\delta_{E,p} = 0$ for $p \geq 5$, $\delta_{E,2} \leq 8$, $\delta_{E,3} \leq 5$
(Ogg's formula for $p \in \{2,3\}$).

Hasse L–function of the curve

$$L(E,s) = \prod_p L_p(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

The Dirichlet series and the Euler product are absolutely convergent for $\operatorname{Re} s > 3/2$.
The function $L(E,s)$ can be analytically continued to an entire function which satisfies a functional equation

$$\Lambda(E,s) = \pm\Lambda(E,2-s)$$

where

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s).$$

Parity conjecture : *the sign of the functional equation determines the parity of the order of the Mordell–Weil group* $E(\mathbb{Q})$.

Birch & Swinnerton-Dyer Conjecture

Bryan J. Birch
Peter Swinnerton-Dyer (1927 – 2018)

Weak BSD Conjecture : *the order of vanishing at* $s = 1$ *of* $L(E, s)$ *is the rank of the Mordell–Weil group* $E(\mathbb{Q})$.

BSD Conjecture : *Let* $P_1, \ldots, P_r$ *be a basis of* $E(\mathbb{Q})$ *modulo torsion. Let* Ω *be the real fundamental period of* E :

$$\Omega = \int_{E(\mathbb{R})} \frac{\mathrm{d}x}{2y + a_1 x + a_3}.$$

Then

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = u \Omega \det(< P_i, P_j >)$$

with $u \in \mathbb{Q}^\times$ *(explicit).*

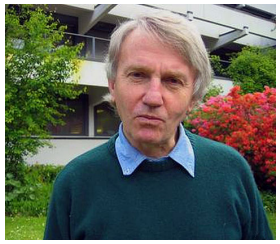
Conjecture BSD - the state of the art

1976 : John Coates, Andrew Wiles
1983 : Benedict Gross, Don Zagier
1990 : Victor Kolyvagin
2001 : Christophe Breuil, Bryan Conrad, Fred Diamond, Richard Taylor
2010 : Manjul Bhargava, Arul Shankar

$L(E,1) \neq 0$ implies $r = 0$
$L(E,1) = 0$, $L'(E,1) \neq 0$ implies $r = 1$
mean value of the rank : $7/6$.

Clay Institute Millenium prize problems 2000, US$ 1 million

Contributions to BSD : trombinoscope



John Coates
1945 - 2022

Andrew Wiles

Benedict Gross

Don Zagier

Victor Kolyvagin

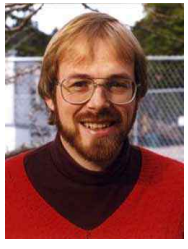
Christophe Breuil

../../ArticlesM

Brian Conrad

/ConradBri

Fred Diamond

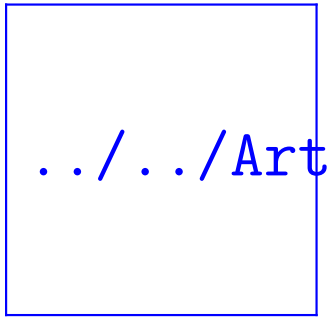


Richard Taylor

Manjul Bhargava

Arul Shankar

Applications of elliptic curves to cryptography



Lawrence C. Washington

L.C. Washington, *Elliptic Curves : Number Theory and Cryptography*

https://www.math.umd.edu/~lcw/

Chap. 5 The discrete logarithm problem

Chap. 6 Elliptic Curve cryptography

- Diffie-Hellman Key Exchange
- Massey-Omura Encryption
- ElGamal Public Key Encryption
- ElGamal Digital Signatures
- The Digital Signature Algorithm
- The Elliptic Curve Integrated Encryption Scheme (ECIES)
- A Public Key Scheme Based on Factoring
- A Cryptosystem Based on the Weil Pairing

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 $f_1, \ldots, f_m$ 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 $\mathbb{K}[f_1, \ldots, f_m]$ for $j = 1, \ldots, m$. Then the set

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

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

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

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.*

Reference :David Masser, *Auxiliary Polynomials in Number Theory* (2016).

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.

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

Chapitre V Courbes elliptiques.

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

• 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

• 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

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.

• Peter Stevenhagen. *Complex elliptic curves* (2019).

http://www.rnta.eu/Montevideo2019/cimpa2019.pdf

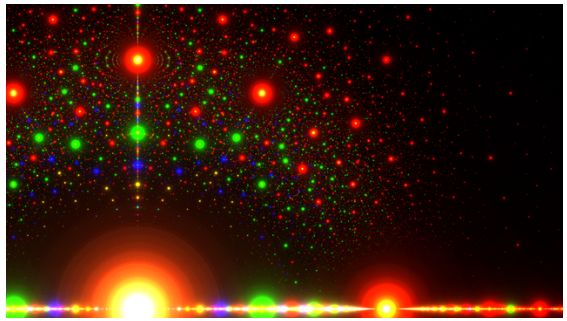
• Lawrence C. Washington. *Elliptic Curves : Number Theory and Cryptography*, Second Edition (Discrete Mathematics and Its Applications) **50**, Taylor & Francis Group, LLC (2008).

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

26/08/2022

African Institute for Mathematical Sciences (AIMS), M'Bour, Senegal
CIMPA Research School on cryptography, theoretical
and computational aspects of number theory.
https://indico.math.cnrs.fr/event/5731/



Elementary Approach to Elliptic Curves

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris
http://www.imj-prg.fr/~michel.waldschmidt/