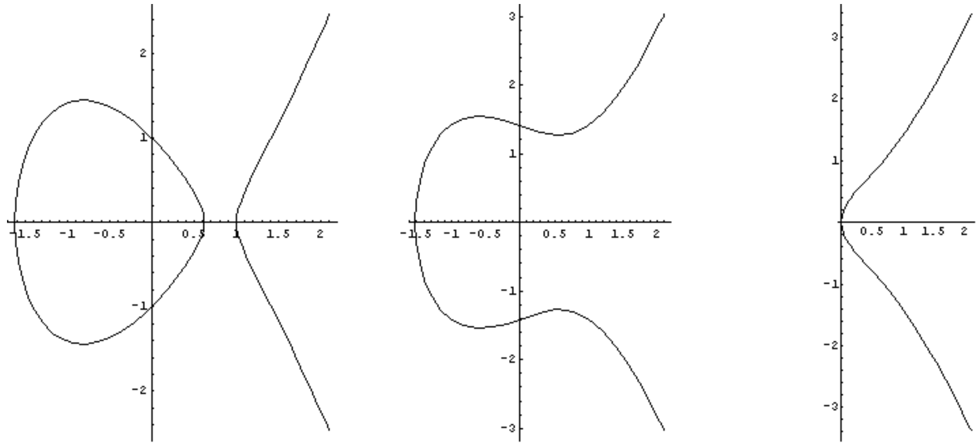

Figure 1: Elliptic curves of the form $E[a, b]$.

... download this document from `www.hakenberg.de`

Contents

The field with a prime number p of elements is denoted $\mathbb{F}_p$.

The **projective space** $\mathbb{P}_n(\mathbb{K})$ is the set of equivalence classes $\{\mathbb{K}^\times(x_0, ..., x_n) : x_i \in \mathbb{K}$ and $x_k \neq 0$ for some $k = 1...n\}$ endowed with the topology induced by $\mathbb{K}^{n+1} - \{0\}$. For a representant $x \in \mathbb{P}_n(\mathbb{K})$ one writes $(x_0 : ... : x_n)$.

$\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is isomorphic to the $\mathbb{F}_2$-vector space with basis -1 and all primes in $\mathbb{N}$.

A polynomial is **homogeneous** of degree d if $f(\lambda\bar{x}) = \lambda^d f(\bar{x})$ for $\lambda \in \mathbb{K}^\times$. We write $f \in \mathbb{K}[\bar{x}]_d$.

Bezout: Let $\mathbb{K}$ be an algebraically closed field. For homogeneous $f \in \mathbb{K}[x, y, w]_n$ and $g \in \mathbb{K}[x, y, w]_m$ without common factor $\#\{(x : y : w) \in \mathbb{P}_2(\mathbb{K}) : f(x, y, w) = g(x, y, w) = 0\} = nm$ counting multiplicities.

1 Elliptic curves

The points on an cubic curve $E_{\mathbb{K}}(\bar{a})$ in **Weierstrass** form are projectively given as

$$(x : y : w) \in \mathbb{P}_2(\mathbb{K}) : y^2w + a_1xyw + a_3yw^2 = x^3 + a_2x^2w + a_4xw^2 + a_6w^3.$$

and by the same argument as in [2] we may also work with $O = \infty$ and points in the affine form

$$(x, y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let f be a cubic homogeneous polynomial over $\mathbb{P}(\mathbb{K})$. The curve C_f is the set of all points $P = (x, y, w)$, which satisfy $f(P) = 0$. C_f is **singular** at $P = (x_0, y_0, w_0)$ of the curve, where the Taylor-expansion of f does not contain terms of first degree. Otherwise there is a unique tangent to the curve at P.

An **elliptic curve** E is the set of points on a nowhere singular cubic curve together with a distinguished point $O \in E$. The chord-tangent rules (see below) endow E with a group structure, O is the **neutral element**.

Usually credited to Poincare: The group law defined via the geometric chord-tangent action: $P + Q := O(PQ)$. The operation is associative, i.e. $(P + Q) + R = (P + Q) + R$. Any choice of a neutral element O produces the same group. An isomorphism $(E, +') \longleftrightarrow (E, +)$ is given by $P \mapsto P - O'$. The proof amounts to show that $(PP')(QQ') = (PQ)(P'Q')$.

Every elliptic curve $E_{\mathbb{K}}(\bar{a})$ can be coordinate transformed into isomorphic $E_{\mathbb{K}}[a, b] := \{(x, y) \in \mathbb{K}^2 : y^2 = x^3 + ax + b\}$ in dependance of the coefficients $a, b \in \mathbb{K}$, with **discriminant** $\Delta = 4a^3 + 27b^2 \neq 0$[1], and $O = \infty$[2]. In this scenario, the group operation has a compact algebraic formulation: Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. The **chord** rule computes $(x, y) = P_1 + P_2$ for the non-trivial combinations and $P_1 \neq P_2$ as

$$\begin{aligned}
x(x_1 - x_2)^2 &= x_1 x_2^2 + x_1^2 x_2 - 2y_1 y_2 + a(x_1 + x_2) + 2b \\
y(x_1 - x_2)^3 &= (3x_2 x_1^2 + x_1^3 + a(3x_1 + x_2) + 4b)y_2 - (3x_1 x_2^2 + x_2^3 + a(x_1 + 3x_2) + 4b)y_1.
\end{aligned}$$

The **tangent** operation yields the coordinates for $(x, y) = P_1 + P_1 = 2P_1$:

$$\begin{aligned}
x(4y_1^2) &= (3x_1^2 + a)^2 - 8x_1 y_1^2 \\
y(2y_1)^3 &= x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2 x_1^2 - 4abc - a^3 - 8b^2
\end{aligned}$$

The **j-invariant** is $j = 1728(4a^3)/\Delta$.

A particularly elegant perspective gives $E_{\mathbb{K}}\langle\alpha, \beta\rangle := E_{\mathbb{K}}[-3\alpha, 2\beta]$ with char $\mathbb{K} \neq 2, 3$ and $\alpha, \beta \in \mathbb{K}$. We derive $\Delta = \alpha^3 - \beta^2$ and $j = \alpha^3/\Delta$. Equip $\mathbb{K}^2$ with a $\mathbb{K}^\times$-action via $\lambda(\cdot, \cdot) = (\lambda^4 \cdot, \lambda^6 \cdot)$. j maps the $\mathbb{K}^\times$-equivariant filtration of $\mathbb{K}^2$ to a filtration of $\mathbb{P}_1(\mathbb{K})$

$$\begin{array}{ccccccc}
\mathbb{K}^2 & \supset & \mathbb{K}^2 - \{0\} & \supset & \mathbb{K}^2 - \{\Delta = 0\} & \supset & (\mathbb{K}^\times)^2 - \{\Delta = 0\} \\
& & \downarrow j & & \downarrow j & & \downarrow j \\
& & \mathbb{P}_1(\mathbb{K}) & \supset & \mathbb{K} & \supset & \mathbb{K} - \{0, 1\}
\end{array}$$

2 Meromorphic functions on a curve

Let $\mathbb{K}$ be algebraically closed. Let $f \in \mathbb{K}[x, y, w]_d$ irreducible define a projective curve $C_{\mathbb{K}}(f)$. We define $\mathbb{K}_f[x, y, w] := \mathbb{K}[x, y, w]/(f) = \bigoplus_k \mathbb{K}[x, y, w]_k$, the field of fractions is $\mathbb{K}_f(x, y, w)$, its subfield the **meromorphic functions** on $C_{\mathbb{K}}(f)$ is $\mathbb{K}(x, y, w)_0 := \{\frac{g}{h} \in \mathbb{K}(x, y, w) : \exists d$ such that $g, h \in \mathbb{K}[x, y, w]_d\}$.

The **group of divisors** is Div C, a free abelian group on $C_{\mathbb{K}}(f)$. Elements $D \in$ Div C are sums akin $D = \sum_{P \in C(\mathbb{K})} m_P[P]$, with coefficients $m_P \in \mathbb{Z}$ and only finitely many non-zero. $\deg D := \sum n_P$. A partial ordering on Div C is given via $D \geq 0 \Leftrightarrow n_P \geq 0$ for all P.

The **intersection number** is $i(P, f \cap g) := \dim_{\mathbb{K}} \mathbb{K}[X, Y]_P/(f, g)$.

For $\varphi = \frac{g}{h} \in \mathbb{K}(x, y, z)_0$ on C we define

$$\text{div } \varphi := \sum_{P: f(P) = g(P) = 0} i(P, C \cap \{g = 0\})[P] - \sum_{P: f(P) = h(P) = 0} i(P, C \cap \{h = 0\})[P].$$

According to Bezout, $\deg f \deg g = \deg f \deg h$ so deg div $\varphi = 0$. For $D \in$ Div C we define the vector space $L(D) := \{\varphi \in \mathbb{K}(x, y, w)_0 : \deg \varphi + D \geq 0\}$. Riemann-Roch: $\exists g \in \mathbb{Z}$ so that $\deg D + 1 - g \leq \dim L(D) < \infty$, equality iff $\deg D > 2g - 2$, g being defined thereby as the genus of the curve C.

[1] arguing with the derivatives, the cubic curve is singular for $\Delta = 0$

[2] projecting down from $E_{\mathbb{K}}(a, b) = \{(x : y : w) \in \mathbb{P}_3(\mathbb{K}) : y^2 w = x^3 + axw^2 + bw^3\}$ via $w \mapsto 1$ while $O = (0 : 1 : 0)$ represents the only class for $w = 0$

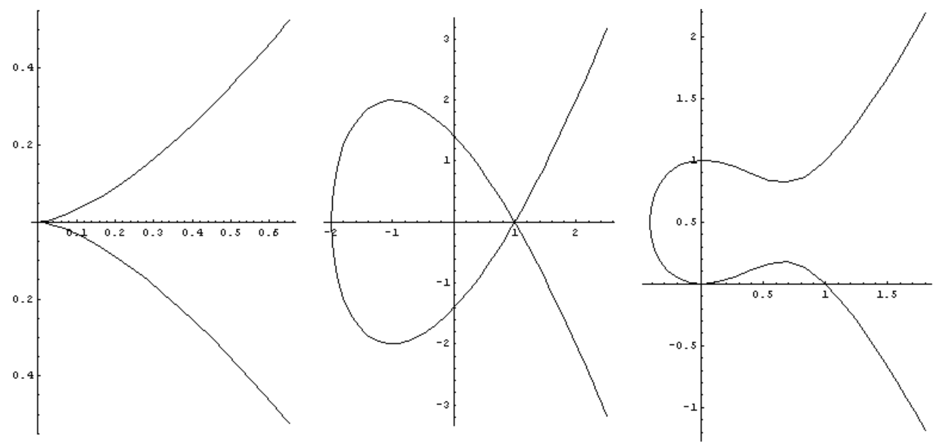

Figure 2: Two examples of singular curves: $E_{\mathbb{K}}\langle 0,0\rangle$ with **cusp**, $E_{\mathbb{K}}\langle -3,2\rangle$ where $\Delta=0$ with **double point**.

Declare $\mathrm{Div}_0\ C := \{D \in \mathrm{Div}\ C : \deg D = 0\}$, and the group of **principle divisors** is $P(C) := \{D \in \mathrm{Div}\ C : \exists\varphi \text{ with } \mathrm{div}\ \varphi = D\}$.

$$P(C) \ \triangleleft\ \mathrm{Div}_0\ C\ \triangleleft\ \mathrm{Div}\ C$$

Let f be an non-singular curve of genus 1, defining $(E_{\mathbb{K}}, O)$, for some selected point O as the neutral element. Then, the **Picard group** $\mathrm{Pic}_0\ C := \mathrm{Div}_0\ C/P(C)$ is isomorphic to $(E_{\mathbb{K}}, O)$, via $P \leftrightarrow [P]-[O]$. To see that $P+S \leftrightarrow [P+S]-[O]$ is compliant, consider the meromorphic function $\varphi = \frac{l_1}{l_2} \in P(C)$, where l_1 is the line going thru P, S and an implied third point R, and l_2 the line intersecting R, O and $P+S$. $\mathrm{div}\ \varphi = [P]+[S]+[R]-[R]-[O]-[P+S]$. Hence, in $\mathrm{Pic}_0\ C$ we have $[P]+[S] \sim [P+S]-[O]$.

3 Algebraic proof for group structure

In projective space, one considers the space of homogeneous cubic forms having 8 fixed points (in general position) in common. This space is spanned by $\lambda F + \mu G = 0$. By Bezout F and G have $3 \cdot 3 = 9$ common intersection points.

As done before, we are concerned showing for points on a $C_{\mathbb{K}}(f)$ the equality $T = S$ for $S = (P+Q)R$ and $T = P(Q+R)$. "Multiplication" with O yields then associativity.

So, we define the form F (G similar) to be the product of three adequate lines, e.g. combines the lines through P/Q, O/QR and $P+Q/R$. Then, we apply Bezouts argument above to pairwise combinations of the cubic curve form itself f, F, and G.

4 p-Reduction

The **p-adic norm** $|\cdot|_p$ assigns $0 \mapsto 0$, and reduced $p^n \frac{u}{v} \in \mathbb{Q} \mapsto p^{-n}$, and satisfies the **ultrametric inequality** • $|r+s|_p \le \max |r|_p\ |s|_p$, and obviously • $|rs|_p = |r|_p|s|_p$. The subring $\mathbb{Q}_{||_p \le 1} := \{r \in \mathbb{Q} : |r|_p \le 1\} \subset \mathbb{Q}$ contains the **p-integral** elements in which analogous $\mathbb{Q}_{||_p<1}$ is an ideal. Hence, we well-define the ring homomorphism $\varrho_p : \mathbb{Q}_{||_p \le 1} \to \mathbb{F}_p$

$$\text{reduced } p^n \frac{u}{v} \mapsto \begin{cases} uv^{-1} \mod p & n = 0 \\ 0 & n > 0 \end{cases}$$

Let prime $p > 2$. The **p-reduction** of $E_{\mathbb{Q}}(\bar{a}) \to E_{\mathbb{F}_p}(\bar{a})$ with $p \nmid \Delta$ works via representing $(x : y : w) \in E_{\mathbb{Q}}(\bar{a})$ with $(\bar{x}, \bar{y}, \bar{w})$ so that • $|\bar{x}|_p, |\bar{y}|_p, |\bar{w}|_p \le 1$ and • at least one of which has $|\cdot|_p = 1$, and • applying the non-obvious group homomorphism

$$\varrho_p(\bar{x},\bar{y},\bar{w}) = (\varrho_p\bar{x},\varrho_p\bar{y},\varrho_p\bar{w}).$$

More intuitive is the equivalent reduction: Let $E_{\mathbb{Q}}[a,b]$ so that $a,b\in\mathbb{Z}$ and $|\Delta|$ minimal [3]. Consider the p-reduction $E_{\mathbb{F}_p}[a,b]\subset\mathbb{F}_p^2\cup\infty$ with a,b and the cubic form being interpreted $\equiv_p$. The following cases can occur:

type of reduction	$\Delta\equiv_p$	$-2ab\equiv_p$	isomorph	$\#E_{\mathbb{F}_p}$
good, non-singular	$\neq 0$		$E_{\mathbb{F}_p}$	?
cusp	0	0	$\mathbb{Z}_p$	p
nodal; rational tangents	0	$\square$	$\mathbb{Z}_p^\times$	$p-1$
nodal; non-rational tangents	0	$\neq\square$	***	$p+1$

$\boxed{\text{Hasse}}$: $|a_p := p+1-\#E_{\mathbb{F}_p}| < 2\sqrt{p}$

Take an elliptic curve $E_{\mathbb{Q}}(\bar{a})$ in Weierstass form with integral coefficients. Then $\Delta\in\mathbb{Z}$. $E_{\mathbb{Q}}(\bar{a})$ is in **global minimal form**, if for all primes p with $p^n\mid\Delta$, the exponent n (equivalently $|\Delta|_p$) is minimal among all admissable coordinate transforms. $\boxed{\text{Neron}}$: for all $E_{\mathbb{Q}}(\bar{a})$ such a global minimal form exists.

Assume $E_{\mathbb{Q}}(\bar{a})$ is in global minimal form. The ***L*-function of** $E_{\mathbb{Q}}(\bar{a})$ is defined as $L_E:\mathbb{C}\to\mathbb{C}$ by

$$L_E(s) := \prod_{p|\Delta}\frac{1}{1-a_pp^{-s}}\prod_{p\nmid\Delta}\frac{1}{1-a_pp^{-s}+p^{1-2s}}.$$

$\boxed{\text{Birch, Swinnerton-Dyer Conjecture}}$: $L_E(s)$ has an analytic continuation to entire $\mathbb{C}$. The order of vanishing at $s=1$ is r the rank[4] of $E_{\mathbb{Q}}$.

5 $E_{\mathbb{Q}}$ is finitely generated

Let $\kappa:\mathbb{Z}\to\mathbb{N}$ obtain the values $m\mapsto\#\{p\in\mathbb{N}\text{ prime}: p|m\}$.

Let G be an abelian group. A norm on G is a map $|\cdot|:G\to\mathbb{R}_0^+$ satisfying • $\#\{g:|g|<n\}<\infty$ for all $n\in\mathbb{N}$ • $|mg|=|m||g|$ for all $m\in\mathbb{Z}$ and • $|g+h|\le|g|+|h|$ for all $g,h\in G$. An abelian group G is finitely generated $\Leftrightarrow$ G is equipped with a norm and the index $(G:nG)<\infty$ for some $n>1$.

In the following $E_{\mathbb{Q}}$ denotes an elliptic curve oringinating from a non-singular cubic curve. The strategy to prove $\boxed{\text{Mordell 1922/23}}$: $E_{\mathbb{Q}}$ is finitely generated, i.e. $E_{\mathbb{Q}}\cong\operatorname{Tors}E_{\mathbb{Q}}\times\mathbb{Z}^r$ where r denotes the **rank** of $E_{\mathbb{Q}}$ follows the above remark.

The 2-isogeny $\varphi:E[a,b]\to E[-2a,a^2-4b]$ which maps $(x,y)\mapsto\frac{1}{x^2}(y^2,y(x^2-b))$ has kernel $\{O,(0,0)\}$.

The homomorphism $\alpha:E[a,b]\to\mathbb{Q}^\times/\mathbb{Q}^{\times2}$ is given by

$$\begin{aligned} O &\mapsto e \\ (0,0) &\mapsto b \quad \mod \mathbb{Q}^{\times 2} \\ (x,y) &\mapsto x \quad \mod \mathbb{Q}^{\times 2} \end{aligned}$$

Then $|\text{im }\alpha|<2^{\kappa(b)+1}$. The sequence $E[a,b]\xrightarrow{\varphi}E[-2a,a^2-4b]\xrightarrow{\alpha}\mathbb{Q}^\times/\mathbb{Q}^{\times2}$ is exact. Furthermore, there is a homomorphism φ' so that $E\xrightarrow{\varphi}E'=E[-2a,a^2-4b]\xrightarrow{\varphi'}E$ is multiplication by 2 on E. We deduce that $(E_{\mathbb{Q}}:2E_{\mathbb{Q}})<2^{\kappa(b)+\kappa(a^2-4b)+2}<\infty$ for non-singular $E=E[a,b]$ with $a,b\in\mathbb{Z}$.

The **naive height** is $h_0:E_{\mathbb{Q}}\to\mathbb{R}_0^+$ with $(\frac{p}{q},y)\mapsto\log\max|p|\ |q| =: |\frac{p}{q}|_\infty$ and $O\mapsto 0$. Under multiplication by 2 we have $h_0(2P)=4h_0(P)+O(1)$, also $\#h_0^{-1}(c)<\infty$. The **canonical height** $h:\mathbb{E}_{\mathbb{Q}}\to\mathbb{R}_0^+$ composes as $P\mapsto\lim\frac{h_0(2^nP)}{4^n}$, which satisfies $(h-h_0)(P)<O(1)$ and $h(2P)=4h(P)$, again $\#h^{-1}(c)<\infty$. h is <u>not</u> a norm on $E_{\mathbb{Q}}$, however either $h(P\pm Q)\le h(P)+h(Q)$ holds. In the proof via contradiction it suffices to go with one.

[3] obtainable via the j-invariant substitutions $a\mapsto\lambda^4a$, $b\mapsto\lambda^6b$

[4] will be defined soon

6 On the rank

Up to today, there exists no effective method to compute the rank for an elliptic curve. Let $E_{\mathbb{Q}} = E[a,b]$ and $a,b \in \mathbb{Z}$. Denote a basis of $E_{\mathbb{Q}}/\text{Tors } E_{\mathbb{Q}} \simeq \mathbb{Z}^r$ with $P_1, ..., P_r$. There exists a unique symmetric positive definite bilinear form $\langle \cdot, \cdot \rangle : \mathbb{Z}^r \times \mathbb{Z}^r \to \mathbb{R}$ with $\langle P, P \rangle = h(P)$. As a consequence $\langle P, Q \rangle = \frac{1}{2}(h(P+Q) - h(P) - h(Q))$. With repect to the basis, the form is described by coefficients $c_{ij} = \langle P_i, P_j \rangle$. The **elliptic regulator** $R_{E/\mathbb{Q}} := \det(c_{ij})$ is independent of the choice of basis. If the rank $r > 0$ then while $T \to \infty$ assymptotically

$$\#\{P \in E_{\mathbb{Q}} : h_0(P) \leq T\} \simeq |\text{Tors } E_{\mathbb{Q}}| \Omega_r \sqrt{\frac{\log^r T}{R_{E/\mathbb{Q}}}},$$

where Ω_r is the volume of the unit ball in $\mathbb{R}^r$. In the limit h_0 can be exchanged by h.

Investigating curves of the form $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with roots in $\mathbb{Z}$, and reducing the image space of a certain homomorphism $E_{\mathbb{Q}}/2E_{\mathbb{Q}} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ but leaving the map injective yields a more sofisticated bound for the rank

$$r \leq \#\{p \in \mathbb{N} \text{ prime} : \text{exactly one of } p|\alpha-\beta, p|\beta-\gamma, p|\alpha-\gamma\} + 2\#\{p \in \mathbb{N} \text{ prime} : p|\alpha-\beta \wedge p|\beta-\gamma \wedge p|\alpha-\gamma\} - 1.$$

The **Hasse principle** is expressed in

$$\prod_{2<p\leq R, p\nmid\Delta} \frac{\#E_{\mathbb{F}_p}}{p} \sim \log^r R$$

A result delivered by Weil: $E(\mathbb{K})$ is finitely generated.

7 Torsion points on $E_{\mathbb{Q}}$

$E_{\mathbb{R}}$ is either $\cong S^1$ or $\cong S^1 \times \mathbb{Z}_2$ [5]. $E_{\mathbb{Q}}$ being a subgroup implies that Tors $E_{\mathbb{Q}} \subset$ Tors $S^1 \times \mathbb{Z}_2$. Mazur 1975 discussed the possible types of the torsion part of $E_{\mathbb{Q}}$:

$$\text{Tors } E_{\mathbb{Q}} \cong \begin{cases} \mathbb{Z}_k & k \in \{1, 2, \ldots, 10, 12\} \\ \mathbb{Z}_2 \times \mathbb{Z}_k & k \in \{2, 4, 6, 8\} \end{cases}$$

Lutz-Nagell 1930: Let $E_{\mathbb{Q}}(\bar{a})$ be given in Weierstrass form with coefficients $\bar{a} \in \mathbb{Z}^5$ and $a_1 = 0$. All torsion points $P = (x,y)$ have integer coordinates. For prime $p \nmid \Delta$ the restriction $\varrho_p|_{\text{Tors } E_{\mathbb{Q}}}$ is injective. For elliptic curves of the form $E_{\mathbb{Q}}[a,b]$ with $a,b \in \mathbb{Z}$ we have moreover $y = 0$ or $y^2|\Delta$.

Example: Consider $E_{\mathbb{Q}}[a,b]$ for different values $a,b \in \mathbb{Z}$, ordered as in figure 1:

a	b	Δ	j	Tors $E_{\mathbb{Q}}[a,b]$	rank
-2	1	-5	$\frac{55296}{5}$		
-1	2	104	$\frac{-864}{13}$		
1	0	4	1728		0

8 Elliptic curves over $\mathbb{C}$

This section needs major revision.

$\mathfrak{H} = \{z \in \mathbb{C} : \text{Im } z > 0\}$. For $\tau \in \mathfrak{H}$ we define the **period lattice** $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$. Every elliptic curve $E(\mathbb{C})$ corresponds to a complex torus $\mathbb{T}_\tau = \mathbb{C}/L_\tau$ in that we find a (unique?) meromorphic L_τ-periodic, i.e. **elliptic function**, $\wp : \mathbb{C} \to \mathbb{C}$ satisfying $\wp'^2 = 4\wp^3 - g_2\wp - g_3\wp$. Evaluating $(\wp, \wp')(z)$ for $z \in \mathbb{T}_\tau$ yields

[5] have a look at the plots

points on .... $\mathbb{T}_\tau$ is the **fundamental parallelogram**. The **Weierstrass** $\wp$ **function** relative to L_τ is given by $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L_\tau - \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$, so that $\wp'(z) = -2\sum_{\omega \in L_\tau} \frac{1}{(z-\omega)^3}$.

Any elliptic function f is in $\mathbb{C}\{\wp, \wp'\}$. For any $u \in \mathbb{C}$ the elliptic function $\wp - u$ has either two simple zeros or one double zero. The latter is the case for $u_1 = \wp(\frac{1}{2})$, $u_2 = \wp(\frac{\tau}{2})$ and $u_3 = \wp(\frac{1+\tau}{2})$. The zeros of $\wp'$ are at $\frac{1}{2}\{1, \tau, 1+\tau\}$, all being simple.

$\wp$ satisfies the differential equation $\wp'^2 = 4\wp^3 - g_2\wp - g_3\wp$, where thru $G_k(L_\tau) = \sum_{\omega \in L_\tau - \{0\}} \frac{1}{\omega^k}$ for $k \geq 3$ the coefficients are $g_2(L_\tau) = 60G_4$ and $g_3(L_\tau) = 140G_6$. In fact $4\omega^3 - g_2\omega - g_3 = 4(\omega - u_1)(\omega - u_2)(\omega - u_3)$ $\Rightarrow$ non-singular.

The map $\varphi : \mathbb{T}_\tau \to E(\mathbb{C}) \subset \mathbb{P}_2(\mathbb{C})$ given by $z \mapsto \begin{cases} (\wp : \wp' : 1)(z) & z \notin L_\tau \\ (0:1:0) & z \in L_\tau \end{cases}$ is a group isomorphism, $\begin{vmatrix} \wp(z_1) & \wp'(z_1) & 1 \\ \wp(z_2) & \wp'(z_2) & 1 \\ \wp(z_1+z_2) & -\wp'(z_1+z_2) & 1 \end{vmatrix} = 0$ for all z_1, z_2. $\Delta = g_2^3 - 27g_3^2$ and $j = 1728g_2^3/\Delta$

In fact $\wp(z) - \frac{1}{z^2} = \sum_{k=1}^{\infty}(k+1)G_{k+2}(L_\tau)z^k$.

9 Modular Forms, Cusp Forms

Let $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. T and S generate $\mathrm{SL}(2,\mathbb{Z})$. The action of $\Gamma = \mathrm{SL}(2,\mathbb{Z})/\{\pm\mathbf{1}\}$ on $\mathfrak{H}$ is defined via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau \to \frac{a\tau+b}{c\tau+d}$. Let $R \subset \mathfrak{H}$ be a fundamental domain with respect to $\mathrm{SL}(2,\mathbb{Z})/\{\pm\mathbf{1}\}$ acting.

An **unrestricted modular form** $f : \mathfrak{H} \to \mathbb{C}$ of weight k satisfies $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Due to the periodicity $f(\tau) = f(\tau+1)$, we put $\tau = \rho + i\sigma$ and may expand f in Fourier series in the variable ρ, to yield the q**-expansion** of f

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q^n \quad \text{with} \quad q = \exp 2\pi i\tau \quad \text{and} \quad c_n = \int_{[-\frac{1}{2},\frac{1}{2}]} f(\rho)q^{-n}\, d\rho.$$

As $\sigma \to \infty$ tends $q \to 0$, hence, we the expansion is around ∞. If $c_{\mathbb{Z}_-} \equiv 0$ then f is a **modular form**. If also $c_0 = 0$, we call f a **cusp form**. Prominent examples are

f	$f \circ \gamma$	q-expansion
j	j	$\frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots$
Δ	$(c\tau + d)^{12}\Delta$	$(2\pi)^{12}(q - 24q^2 + \ldots)$ [alternatively $(2\pi)^{12}q\prod_{\mathbb{N}}(1-q^n)^{24}$]
G_k	$(c\tau + d)^{2k}G_k$	$2\xi(k) *** + \frac{2(2\pi i)^k}{(k-1)!}\sum_{\mathbb{N}} \frac{n^{k-1}q^n}{1-q^n}$

For a modular form f of weight k we have

$$v_\infty + \frac{1}{2}v_i + \frac{1}{3}v_\rho + \sum{}' \, v_\tau = \frac{k}{12}$$

The **Mellin transform** of a nice function $f : \mathbb{R}^+ \to \mathbb{C}$ is a function $g : \mathbb{C} \to \mathbb{C}$ with $g(s) := \int_{\mathbb{R}^+} f(t)t^s \frac{dt}{t}$. The **gamma function** $\Gamma(s)$ is the transform of $\exp -\cdot$. We let a cusp form f undergo the transformation along the line $i\mathbb{R}^+$, and denote the result $\Lambda_f(s) := \int_{\mathbb{R}^+} f(i\sigma)\sigma^s \frac{d\sigma}{\sigma} = (2\pi)^{-s}\Gamma(s)L_f(s)$, where $L_f(s) = \sum_1^\infty \frac{c_n}{n^s}$ is the L**-function of the cusp form** f.

Prove or disproove that every E_Q is **modular**, i.e. L_E equals to E_f for some cusp form f and get 1.000.000$.

References:

D. Husemöller - Elliptic Curves, SK 240 H969 (2)

A. Knapp - Elliptic Curves, SK240 K67 +2

J. Milne - Elliptic Curves, `www.milne.org`