Problem 1.1. Deduce from the multiplicativity of the exponential function that for any smooth paths \( \gamma_1, \gamma_2, \gamma_3 : [0,1] \to \mathbb{C}^* \) with \( \gamma_1(t)\gamma_2(t)\gamma_3(t) = 1 \) for all \( t \), one has the identity
\[
\int_{\gamma_1} \frac{dz}{z} + \int_{\gamma_2} \frac{dz}{z} + \int_{\gamma_3} \frac{dz}{z} = 0.
\]

Problem 1.2. Let \( a, b \in \mathbb{R}_{>0} \) with \( a \leq b \). Show that for any \( \varphi_0 \in [0, \frac{\pi}{2}] \) the arclength of the ellipse segment
\[
\mathbb{E}(\varphi_0) = \{ (a \cos(\varphi), b \sin(\varphi)) \in \mathbb{R}^2 \mid \varphi \in [0, \varphi_0] \}
\]
can be written as
\[
\ell(\varphi_0) = \frac{b}{2} \int_{x_0}^{x_1} \frac{1 - cx}{\sqrt{x(1-x)(1-cx)}} \, dx \quad \text{with} \quad x_0, x_1 \in \mathbb{R} \quad \text{and} \quad c = 1 - \frac{a^2}{b^2}.
\]
Problem 2.1. Let $S$ be a Riemann surface.

(a) Show that for any branched cover $p : X \to S$ the topological space $X$ has a unique Riemann surface structure making $p$ a morphism of Riemann surfaces.

(b) For $\Sigma \subset S$ discrete, show that any topological covering map $p_0 : X_0 \to S \setminus \Sigma$ extends uniquely to a branched cover $p : X \to S$.

Problem 2.2. Let $f(x) \in \mathbb{C}[x] \setminus \{0\}$, and put $\Sigma = f^{-1}(0) \cup \{\infty\} \subset S = \mathbb{P}^1(\mathbb{C})$.

(a) Check that

$$p_0 : X_0 = \{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x) \neq 0\} \to S \setminus \Sigma$$

is a double cover. Describe its unique extension $p : X \to S$ over each $s \in \Sigma$.

(b) If $f(x) = x(x + 1)(x - 1)(x - \lambda)$ with $\lambda \in \mathbb{C} \setminus \{0, \pm 1\}$, determine $g(u) \in \mathbb{C}[u]$ such that

$$p^{-1}(S \setminus \{0\}) \simeq \{(u, v) \in \mathbb{C}^2 \mid v^2 = g(u)\}.$$

Problem 2.3. Let $f(x) = x(x - 1)(x - \lambda)$ with $\lambda \in \mathbb{C} \setminus \{0, 1\}$, and consider the branched cover

$$p : E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x)\} \cup \{\infty\} \to \mathbb{P}^1(\mathbb{C}).$$

Show that the differential form

$$\omega = \frac{dx}{\sqrt{f(x)}},$$

which is a priori only well-defined locally on the complement $E \setminus p^{-1}(\{0, 1, \lambda, \infty\})$, extends to a holomorphic differential form on all of $E$. 

www.math.hu-berlin.de/~kraemeth/elliptic-curves/
All elliptic functions on this sheet are for a given lattice $\Lambda \subset \mathbb{C}$. Put $\wp(z) = \wp_{\Lambda}(z)$.

**Problem 3.1.** (a) Show that if $f$ is an elliptic function of degree $\deg(f) = d$, then its derivative is an elliptic function of degree
\[
\deg(f') \in \{d + 1, \ldots, 2d\},
\]
and give examples for the extreme cases $\deg(f') = d + 1$ and $\deg(f') = 2d$.
(b) For $n = 1, 2, 3$, find $h_1, h_2 \in \mathbb{C}(x)$ with $(\wp'(z))^{-n} = h_1(\wp(z)) + h_2(\wp(z)) \cdot \wp'(z)$.

**Problem 3.2.** Show that up to a translation the Weierstrass function is determined uniquely by its differential equation: If $F$ is a meromorphic function on an open domain $\varnothing \neq U \subseteq \mathbb{C}$ satisfying
\[
(F'(z))^2 = 4F(z)^3 - g_2 \cdot F(z) - g_3
\]
for
\[
\begin{align*}
g_2 &= 60G_4(\Lambda), \\
g_3 &= 140G_6(\Lambda),
\end{align*}
\]
then we must have $F(z) = \wp(z + a)$ for some constant $a \in \mathbb{C}$.

**Problem 3.3.** Show that the following properties are equivalent:
(a) We have $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$.
(b) We have $G_{2n}(\Lambda) \in \mathbb{R}$ for all $n \geq 2$.
(c) We have $\wp(\bar{z}) = \overline{\wp(z)}$ for all $z \in \mathbb{C}$.
(d) The lattice $\Lambda \subset \mathbb{C}$ is invariant under complex conjugation.
Put $\mathcal{F} = \{ \tau \in \mathbb{H} \mid \text{Re}(\tau) \leq 1/2 \text{ and } |\tau| \geq 1 \}$.

**Problem 4.1.** Determine all points $\tau \in \mathcal{F}$ that are equivalent modulo $\Gamma = \text{SL}_2(\mathbb{Z})$ to the point $\frac{5i+6}{4i+5}$ respectively $\frac{2+8i}{17} \in \mathbb{H}$.

**Problem 4.2.** Find natural numbers $n_1, \ldots, n_k \in \mathbb{N}$ for which one has the matrix identity

$$
\begin{bmatrix}
4 & 9 \\
11 & 25
\end{bmatrix}
= ST^{n_1} \cdots ST^{n_k}
$$

with $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Is such a representation unique? More generally, show that the modular group has the presentation

$$\text{SL}_2(\mathbb{Z}) \simeq \langle S, T \mid S^2 = (ST)^3 = 1 \rangle.$$ 

**Problem 4.3.** (a) Show that $G_k(\tau) = G_k(\tau)$ for all $\tau \in \mathbb{H}$, $k \geq 4$.

(b) Show that the $j$-function takes real values on the set $\partial \mathcal{F} \cup i \cdot \mathbb{R}_{>0}$.

(c) Conversely, show that any real number arises as $j(\tau_0)$ for some $\tau_0 \in \partial \mathcal{F} \cup i \cdot \mathbb{R}_{>0}$.

**Problem 4.4.** Verify that the derivative of a meromorphic modular form of weight zero is a meromorphic modular form of weight two. Deduce that if $f, g$ are modular forms of a given weight $k$, then $fg' - f'g$ is a modular form of weight $2k + 2$. 
Let $k$ be a field. For elliptic curves with a flex point at infinity we take this flex point as the neutral element for the group structure.

**Problem 5.1.** Let $f \in k[x_0, x_1, x_2]$ be a homogenous polynomial and $C_f \subset \mathbb{P}^2$ the corresponding plane curve. Show that for $\text{char}(k) = 0$, a smooth point $p \in C_f(k)$ is a flex point of the curve iff

$$\det \left( \frac{\partial^2 f}{\partial x_i \partial x_j} \right)(p) = 0.$$ 

What happens if the assumption on the characteristic $\text{char}(k)$ is dropped?

**Problem 5.2.** Find the order of the point $p$ on the elliptic curve $E$ when

(a) $p = (3, 12)$ and $E$ is given by $y^2 = x^3 - 14x^2 + 81x$.

(b) $p = (3, 8)$ and $E$ is given by $y^2 = x^3 - 43x + 166$.

**Problem 5.3.** Put $f(x, y) = y^2 - x^3 + 432c^2$ for fixed $c \in k$.

(a) For which $c$ is the cubic $E = \{(x, y) \mid f(x, y) = 0\} \cup \{\infty\} \subset \mathbb{P}^2$ smooth?

(b) In the smooth case, find $M \in \text{PGL}_3(k)$ that induces on affine coordinates the transformation

$$(x, y) \mapsto (u, v) = \left( \frac{6c}{x} + \frac{y}{6x}, \frac{6c}{x} - \frac{y}{6x} \right).$$

What is the equation for the cubic in the new affine coordinates $(u, v)$?

(c) Now let $k = \mathbb{Q}$. Determine the group $E(\mathbb{Q})$ in the case $c = 1$.

**Problem 5.4.** Let $E \subset \mathbb{P}^2$ be the elliptic curve defined by $y^2 = x^3 - 11$ over $\mathbb{Q}$. Show that

(a) a point $(s, t) \in E(\mathbb{Q})$ is in the image of the map $E(\mathbb{Q}) \rightarrow E(\mathbb{Q}), p \mapsto 2p$ iff the polynomial

$$x^4 - 4sx^3 + 88x + 44s \in \mathbb{Q}[x]$$

has a rational root $x_0 \in \mathbb{Q}$.

(b) the images of $p = (3, 4), q = (15, 58)$ in the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ are distinct and nonzero, hence linearly independent when the quotient is seen as a vector space over the field $F_2 = \mathbb{Z}/2\mathbb{Z}$.

(c) the map $(m, n) \mapsto mp + nq$ gives an embedding $\mathbb{Z}^2 \hookrightarrow E(\mathbb{Q})$. 

www.math.hu-berlin.de/~kraemeth/elliptic-curves/
Problem 6.1. Let \( E \subset \mathbb{P}^2 \) be an irreducible singular cubic over a field \( k \), defined in affine coordinates by a Weierstrass equation.

(a) Show that \( E \) has a unique singular point \( p = (x_0, y_0) \in E(\overline{k}) \).

(b) If \( p \) is a cusp with tangent line given by \( y = \alpha x + \beta \), check that we have an isomorphism

\[
\varphi : E \setminus \{p\} \sim \mathbb{A}^1, \quad (x, y) \mapsto \frac{x - x_0}{y - \alpha x - \beta}
\]

such that \( a, b, c \in E(\overline{k}) \setminus \{p\} \subset \mathbb{P}^2(\overline{k}) \) are collinear iff \( \varphi(a) + \varphi(b) + \varphi(c) = 0 \).

(c) If \( p \) is a node with tangent lines \( y = \alpha_i x + \beta_i \) defined over \( k \), check that we have an isomorphism

\[
\varphi : E \setminus \{p\} \sim \mathbb{A}^1 \setminus \{0\}, \quad (x, y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}
\]

such that \( a, b, c \in E(\overline{k}) \setminus \{p\} \subset \mathbb{P}^2(\overline{k}) \) are collinear iff \( \varphi(a) \cdot \varphi(b) \cdot \varphi(c) = 1 \).

Problem 6.2. Let \( E \) be an elliptic curve over the complex numbers. Which of the following four cases can occur for a subgroup \( H \subset E(\mathbb{C}) \)?

(a) \( H \) is torsion and \( H/2H \) trivial,
(b) \( H \) is torsion and \( H/2H \) infinite,
(c) \( H \) is torsion-free and \( H/2H \) trivial,
(d) \( H \) is torsion-free and \( H/2H \) infinite.

Problem 6.3. Let \( a \in \mathbb{Z} \) be an integer which is not divisible by the fourth power of any prime, and consider the elliptic curve \( E \) defined by \( y^2 = x^3 - ax \).

(a) Show that \( |E(\mathbb{F}_p)| = p + 1 \) for all primes \( p \equiv 3 \pmod{4} \).

(b) Show that

\[
E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} 
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } a \text{ is a square}, \\
\mathbb{Z}/4\mathbb{Z} & \text{if } a = -4, \\
\mathbb{Z}/2\mathbb{Z} & \text{otherwise}. 
\end{cases}
\]

Problem 6.4. Find the 2-power torsion and sets of representatives for \( E(\mathbb{Q})/2E(\mathbb{Q}) \) for the elliptic curves defined by the following equations:

(a) \( y^2 = x(x-3)(x+4) \),
(b) \( y^2 = x(x-1)(x+3) \).

www.math.hu-berlin.de/~kraemeth/elliptic-curves/