CIMPA school **Elliptic curves**
Gadjah Mada University **14-25 July 2025**
Teachers: Francesco Campagna and Richard Griffon

Exercises for Elliptic curves

Exercise 1

Let $L = \mathbf{Z}\lambda_1 + \mathbf{Z}\lambda_2 \subseteq \mathbf{C}$ be a lattice and let $\wp : \mathbf{C} \to \mathbf{C} \cup \{\infty\}$ be the associated Weierstrass function.

1. Show that $\wp$ and its derivative $\wp'$ are elliptic functions with respect to L.
2. Show that, around 0, the function $\wp$ has Laurent exapansion

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2} \cdot z^{2k}$$

   where for all integers $m \in \mathbf{Z}_{\geq 1}$ we have $G_m := \sum_{\lambda \in L \setminus \{0\}} 1/\lambda^m$.
3. Show that $\wp'(\lambda_1/2) = \wp'(\lambda_2/2) = \wp'((\lambda_1 + \lambda_2)/2) = 0$.
4. Consider the elliptic curve

$$E : y^2 = 4x^3 - g_2 x - g_3, \quad \text{with} \quad g_2 = 60G_4 \text{ and } g_3 = 140G_6.$$

   Show that the three affine points $P \in E(\mathbf{C})$ with $y = 0$ satisfy $2P = O$, where O is the identity element on $E(\mathbf{C})$.

Exercise 2

Let $L \subseteq \mathbf{C}$ be the lattice generated by $(1+i)\omega$ and $(1-i)\omega$, where ω is the lemniscate constant. Denote by $\wp$ the associated Weierstrass function.

In class we saw that the lemniscate sine $\mathrm{sl}(z)$ has the same set of zeroes and poles as $\frac{\wp(z)}{\wp'(z)}$, with the same corresponding multiplicities.

1. Show that there exists a constant $C \in \mathbf{C}$ such that

$$\mathrm{sl}(z) = C \cdot \frac{\wp(z)}{\wp'(z)}.$$

2. Show that $C = -2$.

3. Using the fact that $\mathrm{sl}'(z) = (4\wp(z)^2 - 1)/(4\wp(z)^2 + 1)$ and the functional equation of the lemniscate sine, prove that

$$(\wp')^2 = 4\wp^3 + \wp.$$

4. The previous question shows that, in the notation of Exercise 1, the lattice L has $G_6 = 0$ (why?). Prove this result directly.

Exercise 3

Let ℓ be a prime number and let E be an elliptic curve over $\mathbf{C}$.

1. How many cyclic subgroups of order ℓ does $(\mathbf{Z}/\ell\mathbf{Z})^2$ contain ?
2. Let $\phi : E \to E'$ be an isogeny from E to an elliptic curve E' also defined over $\mathbf{C}$. Assume that $\ker\phi$ contains exactly ℓ elements. Show that $\ker\phi$ is a cyclic subgroup of $E[\ell]$.
3. Let X_ℓ be the set of isogenies $\phi : E \to E'$ from E to another (variable) elliptic curve E' over $\mathbf{C}$ such that $\ker\phi$ is a cyclic group of order ℓ. How many elements are there in X_ℓ ?

Exercise 4

Consider the curve $E/\mathbf{Q}$ given by the projective equation

$$E : Y^2Z = X^3 + XZ^2 + 2Z^3$$

1. Show that E is an elliptic curve. Compute its j-invariant and write its affine equation in the coordinates $x = X/Z$ and $y = Y/Z$.
2. Let $P = [1 : 2 : 1]$. Show that P belongs to $E(\mathbf{Q})$ and compute $n \cdot P$ for all $n \in \mathbf{N}$.
3. Show that

   $$T_2 := \{Q = [X : Y : Z] \in E(\overline{\mathbf{Q}}) : 2Q = 0\} = \{[X : Y : Z] \in E(\overline{\mathbf{Q}}) : Y = 0\} \cup \{O\}.$$

   Determine explicitly this set.
4. Compute $T_2 \cap \langle P \rangle$.