Elliptic curves

Exercises are independent and can be tackled in any order

Exercice 1 Let E be a complex elliptic curve and $\wp$ the associated Weierstraß function. Let z_1, z_2 be complex numbers. Show

$$\begin{vmatrix} \wp(z_1) & \wp'(z_1) & 1 \\ \wp(z_2) & \wp'(z_2) & 1 \\ \wp(z_1+z_2) & -\wp'(z_1+z_2) & 1 \end{vmatrix} = 0 .$$

Exercise 2 Consider the smooth projective curve defined over $\mathbb{Q}$ given by the cubic equation :$E = \{(x:y:z) \in \mathbb{P}_2 : x^3 + y^3 + z^3 = 0\}$.
(i) Show that E is a elliptic curve.
(ii) Find div $\left(\frac{z}{x+y}\right)$ and div $\left(\frac{y-x}{x+y}\right)$.
(iii) Find a Weierstraß normal form for (E, O) with $O = (1 : -1 : 0)$.
(iv) Compute the modular invariant of E.

Exercise 3 For a projective curve C, we say that $P \in C$ is an inflection point of C if the tangent T_P of C at P intersects C with multiplicity ≥ 3. We now assume that $C = C(a, b)$ is a smooth Weierstraß cubic, $y^2 = x^3 + ax + b$.
(i) Check that $p \in C$ is such that $[3]p = O$ if and only if p is an inflection point of C.
(ii) Deduce that $\#C[3] = 9$ (one can assume the Bézout theorem asserting two plane cubics intersect at 9 points counted with multiplicity). ?

Exercise 4 Let Λ be a complex lattice. Show that the following product converges and defines an entire complex function:

$$\sigma(z) = z \prod_{\omega \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\omega}\right) \exp\left[\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right] .$$

Also prove that $\zeta(z) = \sigma'(z)/\sigma(z)$ (σ is a theta function associated to $3(0)$).

Exercise 5 Let $p > 2$ a prime such that $p \equiv 2 \bmod (3)$, $b \in \mathbb{F}_p$ and E the curve over $\mathbb{F}_p$) given by $Y^2 = X^3 + b$.
(i) What condition b needs to meet for E to be elliptic? It is now assumed that E is elliptic.
For questions (ii) to (iv), one may assume that E is supersingular and $\#E(\mathbb{F}_p) = p + 1$.
(ii) Let $n \geq 1$ coprime to p and assume $E[n] \subset E(\mathbb{F}_p)$. Show that $n \mid p - 1$, $n^2 \mid p + 1$, then $n \leq 2$.
(iii) Check $E[2] \subsetneq E(\mathbb{F}_p)$.
(iv) Show $E(\mathbb{F}_p)$ is a cyclic group, what is its cardinality?
(v) Show that E is supersingular.
(vi) Show $\#E(\mathbb{F}_p) = p + 1$. ?

Exercise 6 Let k be a field of characteristic $\neq 2$. Let C_λ the family of cubics $\subset \mathbb{P}_2$ given by $y^2 = x(x-1)(x-\lambda)$, $\lambda \in k$.
(i) Compute the discriminant $\Delta(\lambda)$ of C_λ and its j-invariant (when $\Delta(\lambda) \neq 0$).
(ii) When $\Delta(\lambda) \neq 0$, find $E[2]$.