Elliptic curves: homework 5
Due: 12th March 2018, 14:00
Mastermath / DIAMANT, Spring 2018

Solve all problems and hand in Problems 3 and 6.

The solutions to some problems are given as proofs in [Silverman], but you will learn more by solving them yourself.

Problem 1 (Formulas for chord-and-tangent addition)**.** Let K be a field of characteristic not 2 or 3, let $A, B \in K$, let E be the (possibly singular) plane projective curve defined by the affine Weierstrass equation $Y^2 = X^3 + AX + B$.
[This also works for general Weierstrass equations, but the formulas are more complicated. See Silverman, §III.2, Group Law Algorithm 2.3]

(a) Show that $O = (0 : 1 : 0)$ is a non-singular point of E.

For non-singular points P_1 and P_2 of C, let L be the line through P_1 and P_2 (tangent line if $P_1 = P_2$). By Bézout's theorem (Problem 7), there is a unique third intersection point of C with L (counted with multiplicity) and it is a non-singular point of C. Denote this third intersection point by $P_1 * P_2$.

Let $P_1 + P_2 = (P_1 * P_2) * O$.

(b) Show $O + P = P$ for all $P \in E(\overline{K})$.

Now let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be affine non-singular points on E.

(c) If $x_1 = x_2$ and $y_1 = -y_2$, show $P_1 + P_2 = O$.
(Do not forget the case $P_1 = P_2$ with $y_1 = 0$.)

From now on, assume that $x_1 \neq x_2$ or $y_1 \neq -y_2$ holds.

(d) Show $L : y = \lambda x + \nu$ for

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \frac{3x_1^2 + A}{2y_1} & \text{if } x_1 = x_2, \end{cases}$$

and $\nu = y_1 - \lambda x_1$.

(e) Show that $P + Q = (x_3, y_3)$ with

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -(\lambda x_3 + \nu). \end{aligned}$$

(f) If E is smooth, then show that the *translation map*

$$\begin{aligned} \tau_Q : E &\longrightarrow E \\ P &\longmapsto P + Q \end{aligned}$$

is a morphism. Is it a homomorphism of elliptic curves?

Problem 2. Let E be affine plane curve over $\mathbb{Q}$ given by the affine Weierstrass equation $Y^2 = X^3 + 17$ and let $P = (-2, 3)$, $Q = (-1, 4)$. Use the formulas of Problem 1 to calculate $P + P$ and $P + Q$.

Problem 3. Let E be the elliptic curve over $\mathbb{F}_7$ given by the affine Weierstrass equation $Y^2 = X^3 + 2$.

(a) Show that E has precisely nine points defined over $\mathbb{F}_7$.

(b) Decide whether $E(\mathbb{F}_7)$ is cyclic or not.

Problem 4 (Proof of [Silverman, III.1.5 and III.3.1(c)])**.** Let E be a smooth plane projective curve given by a Weierstrass equation

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

over a field K. For the sake of keeping computations simple, you may assume $\mathrm{char}(K) \neq 2, 3$ and hence $a_1 = a_2 = a_3 = 0$. Let

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

(a) Prove

$$\omega = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

(b) Prove that ω has no zeroes or poles.

(c) Show that E has genus 1 and that for every $O \in E(K)$, the pair (E, O) is an elliptic curve. [If a Weierstrass equation is given, but O is not specified, then this is usually understood to mean $O = (0 : 1 : 0)$.]

In last week's homework (Problem 4), you showed that chord-and-tangent addition makes the set of rational points on any *smooth* Weierstrass curve into a group. The following Problem shows that the same is true for the set of non-singular rational points on non-smooth Weierstrass curves.

Problem 5 (Group law for *singular* Weierstrass curves [Silverman, Proposition III.2.5 and Exercise 3.5])**.** Let E be a Weierstrass curve with a cuspidal point S.

(a) Show that there is a change of Weierstrass equation that puts S at $(0,0)$ and makes the generalized tangent line at S horizontal.

(b) Show that after such a change, the Weierstrass equation is

$$Y^2Z = X^3$$

and write down the affine model with coordinates $v = X/Y$ and $z = Z/Y$.

(c) Show that the rational map $v : E_{\mathrm{ns}} \to \mathbb{A}^1 : P \mapsto v(P)$ gives a bijection $E_{\mathrm{ns}}(K) \to K$.

(d) Show that if a line intersects E in three non-singular points P, Q, R counted with multiplicity, then $v(P) + v(Q) + v(R) = 0$.

(e) Conclude that $E_{\mathrm{ns}}(K)$ is a group with chord and tangent addition and that this group is isomorphic to the additive group K.

(f) (Optional). Now let E be a Weierstrass curve with a node at a point S. Show that $E_{\mathrm{ns}}(\overline{K})$ is a group with chord and tangent addition and that this group is isomorphic to the multiplicative group $\overline{K}^*$. Or better: let L/K be the field extension generated by the slopes of the tangent lines at S, and show that either $L = K$ and $E_{\mathrm{ns}}(K) \cong K^*$ or L/K is quadratic and, $E_{\mathrm{ns}}(K) \cong \ker(N_{L/K} : L^* \to K^*)$.
[Hint: Do a change of variables (over $\overline{K}$ or L) such that $S = (0,0)$ and $E : Y^2Z - XYZ = X^3$. Homogenize by setting $Y = 1$, and consider the map $E_{\mathrm{ns}}(\overline{K}) \to \overline{K}^* : (X : Y : Z) \mapsto 1 - X/Y$.]

(g) Conclude (also from (f)) that for singular Weierstrass equations $E/\mathbf{F}_p$, the group $E_{\mathrm{ns}}(\mathbf{F}_p)$ is cyclic of order p, $p-1$, or $p+1$.

Problem 6. (Tate normal form, based on [Silverman, Exercise 8.13].)

(a) Let k be a field and let E/k be an elliptic curve with $P \in E(k)$ a point of order ≥ 4. Show that E can be described by an equation of the form

$$y^2 + uxy + vy = x^3 + vx^2$$

with $u, v \in k$ and $P = (0,0)$.
[Hint: there are two very nice solutions that practise different aspects of the theory.
For solution 1: consider $\mathcal{L}(2O - P)$, $\mathcal{L}(3O - 2P)$ and $\mathcal{L}(6O - 2P)$ similarly to the proof of Proposition III.3.1(a).
For solution 2: start with a general Weierstrass equation and use changes of Weierstrass equation.]

(b) (This problem concerns the *modular curve* $Y^1(5)$.) Show that there is a one-parameter family of elliptic curves over k with a k-rational point of order 5.
[Hint: Set $3P = -2P$ and see how u and v must be related. Note that $3P$ can be computed from $-2P$ and $-P$.]

Problem 7 (Special case of Bézout's theorem)**.** Let $C : F = 0$ be a projective plane curve of degree d and $L \neq C$ a line in the projective plane. Let

$$\phi : \mathbb{P}^1 \to L : (s : t) \mapsto (x_1 s + x_0 t : y_1 s + y_0 t : z_1 s + z_0 t)$$

be an isomorphism. (For non-vertical lines $L : y = \lambda x + y_0$, think of $\phi : x \mapsto (x, \lambda x + y_0)$, which is $x_1 = z_0 = 1$, $x_0 = z_1 = 0$, $y_1 = \lambda$.)

(a) Show that we have $F \circ \phi = \prod_{i=1}^{d} (\beta_i s - \alpha_i t)$ with $\alpha_i, \beta_i \in \overline{K}$.

(b) Show $C(\overline{K}) \cap L(\overline{K}) = \{\phi((\alpha_i : \beta_i)) : i = 1, \ldots, d\}$.

The *multiplicity* of the intersection of C and L in $P = \phi((\alpha : \beta))$ is the number of $i \in \{1, \ldots, d\}$ with $(\alpha : \beta) = (\alpha_i : \beta_i)$.

(c) Conclude that the number of intersection points over $\overline{K}$ of C and L counted with multiplicity is the degree of C.

(d) Show that the intersection multiplicity of C and L in P is ≥ 2 if and only if P is a singular point of C or L is tangent to C at P.
[Hint: make it easier for yourself using changes of variables.]

(e) Show that if $d - 1$ intersection points (counted with multiplicity) are defined over K, then all d are defined over K.

Recommended additional exercises: 3.3, 3.5, 3.21, 3.22, 3.23, 8.13 of [Silverman].