Mastermath Elliptic Curves, Homework sets 7 and 8

Problems marked with a star in the lists are to be handed in and count towards your grade according to the rules on the web page.
All non-optional problems and their solutions are part of the course and could play a role in the exam.

Homework for 3rd November 2015, 10:15: 43*, 44, 45(a)*, 45(d)*, 46*, 48 and 51(b)
Homework for 10th November 2015, 10:15: 45(b)*, 47, 49*, 50*, 53
Optional problems: 45(c), 51(a), 52

We use the notation $\ker(\phi) = \ker(\phi : E(\overline{k}) \to F(\overline{k})) \subset E(\overline{k})$ for $\phi : E \to F$ and $E[m] = \ker([m] : E \to E)$.

Problem 43. Let $\zeta \in \mathbf{F}_4$ denote a primitive 3rd root of unity. Let E be the elliptic curve over $\mathbf{F}_4$ defined by the equation $Y^2 + Y = X^3$. Let $f : E \to E$ be given by $f(x, y) = (\zeta x, y)$ and let $g : E \to E$ be given by $g(x, y) = (x + 1, y + x + \zeta)$. Show that f and g are automorphisms of E and show that they do not commute. Therefore the ring $\operatorname{End} E$ is not commutative in this case.

Problem 44. Let E be the elliptic curve over $\mathbf{Q}$ given by $Y^2 + Y = X^3$ and let Q denote the point $(0, 0)$. Let $\tau : E \longrightarrow E$ denote translation by Q. In other words $\tau(P) = P + Q$ for P a point on E.

(a) Show that τ is a *curve automorphism* of E of order 3, but not an elliptic curve automorphism.

(b) Give a formula for the point τP in terms of the coordinates x and y of $P = (x, y)$. Also give a formula for $\tau^2 P$.

(c) Let H be the subgroup generated by Q and let E' denote the elliptic curve over $\mathbf{Q}$ given by $Y^2 + 3Y = X^3 - 9$. Show that $\phi(x, y) = (x + \frac{1}{x^2}, y - 1 - \frac{2y+1}{x^3})$ defines an isogeny $\phi : E \longrightarrow E'$ whose kernel is H. You may use a computer for part (c).

Problem 45. Let k be a field of characteristic different from 2. Suppose that k contains i, a square root of -1. Let E be the elliptic curve over k given by $Y^2 = X^3 - X$.

(a) Show that the map $[i](x, y) = (-x, iy)$ defines an endomorphism $[i] : E \longrightarrow E$ and that $[i]$ satisfies $[i]^2 + [1] = 0$ in $\operatorname{End}(E)$.

(b) For $a, b \in \mathbf{Z}$, show that the degree of the endomorphism $a + b[i]$ of E is equal to $a^2 + b^2$.

(c) Compute formulas for the isogeny $\phi = [1] + [i]$.

(d) Compute the points in $\ker(\phi)$ for $\phi = [1] + [i]$. Note: this can easily be done without doing (c). If you do use (c), then hand in a solution to (c).

Problem 46. Let E be the elliptic curve over $\mathbf{Q}$ given by the equation $Y^2+Y = X^3$. Compute the coordinates of its 2-torsion points and of its 3-torsion points in $E(\overline{\mathbf{Q}})$. [Hint for the 3-torsion: the curve is not of the form of Problem 12, so the formula in 12(a) is different, but the idea behind 12(c) still works.]

Problem 47. Let E be the elliptic curve over $\mathbf{F}_2$ given by $Y^2 + Y = X^3$. Compute the dual of its Frobenius endomorphism.

Problem 48 (Exercise 3.30 of [Silverman] 2nd Edition)**.** Let A be an abelian group and $r \geq 0$ and $N \geq 1$ integers. Suppose that $\#A[d] = d^r$ for all $d \mid N$, where $A[d]$ denotes the subgroup of elements of order dividing d. Show $A[N] \cong (\mathbf{Z}/N\mathbf{Z})^r$.

Problem 49 (Inspired by Exercise 3.32 of [Silverman] 2nd Edition)**.** Let $\phi \in \mathrm{End}(E)$ be an endomorphism and let

$$d = \deg(\phi), \quad \text{and} \quad t = 1 + \deg(\phi) - \deg(1 - \phi) \in \mathbf{Z}.$$

(a) Prove $t = \phi + \widehat{\phi}$ and $\phi^2 - t\phi + d = 0$ in $\mathrm{End}(E)$.

(b) Give a formula for $\deg(m\phi - n)$ in terms of m, n, d, t.

(c) Prove $|t| \leq 2\sqrt{d}$. [Hint: use $\deg(m\phi - n) \geq 0$ for all $m, n \in \mathbf{Z}$.]

(d) Prove *Hasse's theorem*, which states that for $E/\mathbf{F}_q$ an elliptic curve, we have
$$|\#E(\mathbf{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$
[Hint: show that $E(\mathbf{F}_q) = \ker(1 - \mathrm{Frob}_q)$.]

Problem 50. Let k be a field and let E be an elliptic curve over k.

(a) Show that for $m \geq 3$ not divisible by $\mathrm{char}\, k$, the natural map $\mathrm{Aut}\, E \longrightarrow \mathrm{Aut}(E[m])$ is injective, while for $m = 2$ its kernel is $\{\pm \mathrm{id}\}$.
Notes: this is [Silverman, Exercise 3.12], and you are not allowed to use [Silverman, Theorem III.10.1]. Hint for one approach to this problem: use Problem 49(c).

(b) Show that the order of $\mathrm{Aut}\, E$ is at most 12 when $\mathrm{char}\, k \neq 2$, while it is at most 48 when $\mathrm{char}\, k = 2$. (It is actually ≤ 24.)

(c) Show that the order of an automorphism of E is 1, 2, 3, 4 or 6.
Hint: use Problems 49(a) and 49(b).

Problem 51. Recall from the previous lecture the proof that every elliptic curve (i.e., smooth projective curve of genus 1 with a point) is isomorphic to a smooth projective plane Weierstrass curve with the point at infinity.

(a) Fill in the details.

(b) Prove that every isomorphism of Weierstrass elliptic curves over k is of the form $(x : y : 1) \mapsto (u^2x + r : u^3y + u^2sx + t : 1)$ with $r, s, t \in k$ and $u \in k^*$. [Hint: it is of the form $(x : y : 1) \mapsto (X : Y : 1)$. Show $X \in L(2O)$ and $Y \in L(3O)$.]

Problem 52. Learn about the Weil pairing and use this to prove $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$. For sub-problems to help you towards this goal, see Exercise 3.31 of [Silverman, 2nd Edition].

Problem 53. Let E be an elliptic curve over a finite field $\mathbf{F}_q$ of q elements. Show that we have $E(\mathbf{F}_q) \cong (\mathbf{Z}/m_1\mathbf{Z}) \times (\mathbf{Z}/m_2\mathbf{Z})$, where

(a) m_1 and m_2 are integers with $m_1 \mid m_2$,

(b) m_1 is the largest integer such that $\mathrm{Frob}_q - 1$ is a multiple of $[m_1]$ in the ring $\mathrm{End}(E)$.

Note that the number $m_1 m_2 = \#E(\mathbf{F}_q)$ is as in Problem 49.

Source of most of the problems: adapted from Mastermath Elliptic Curves 2013, René Schoof and Peter Stevenhagen.