**Mastermath Elliptic Curves, Homework 2**
Martin Bright and Marco Streng
Due: 29th September 2015, 10:15

Students are expected to (try to) solve all problems below. The ones marked with 'H' (that is, 10(a,b,c,e) and 12(a,c,e)) are to be handed in and count towards your grade according to the rules on the web page.

All problems and their solutions are part of the course, and could play a role in the exam. More importantly, they help you digest the material of the previous lecture and help you prepare for the next lecture.

**Problem 10.** A *curve of degree* $a$ in $\mathbb{P}^2$ is the zero set of a non-zero homogeneous polynomial in $k[X, Y, Z]$ of degree $a$. A curve of degree 1 is called a *line*.

(a) Show that for every line $L \subset \mathbb{P}^2(k)$ there is a linear change of variables $T : \mathbb{P}^2 \to \mathbb{P}^2$ (i.e., given by multiplying $(X : Y : Z)$ by some invertible $3 \times 3$ matrix) such that $T(L)$ is given by $Y = 0$. H

You may use the definition of the *intersection number* of curves $C, D \subset \mathbb{A}^2$ in a point $P$ of $\mathbb{A}^2(k)$ from [Milne, Proposition 1.8 for intersection in $(0, 0)$, next page for general points] (or [Fulton, Section 3.3 (1)–(7)] if you prefer). You may also use that this notion extends to a well-defined notion of intersection number for curves in $\mathbb{P}^2$ that does not change upon linear changes of variables of $\mathbb{P}^2$.

(b) Let $F \in k[X, Y, Z]$ be homogeneous and not divisible by $Y$. Show that the intersection number of the curve $F = 0$ with the line $Y = 0$ at $(x : 0 : 1)$ is the order of $x$ as a root of $F(X, 0, 1) \in k[X]$. H

(c) Show that the intersection number of the curve $F = 0$ with the line $Y = 0$ at $(1 : 0 : 0)$ is the number of factors $Z$ in $F(X, 0, Z) \in k[X, Z]$. H

(d) Show that the intersection number of a line $L$ and a curve $C$ at a point $P$ is $\geq 2$ if and only one of the following is true: $P$ is a singular point of $C$ or $L$ is the tangent line of $C$ at $P$.

Let $k$ be an algebraically closed field and let $C$ and $D$ in $\mathbb{P}^2(k)$ be any two curves of degrees $a$ and $b$ that do not have an irreducible component in common. *Bézout's theorem* states that $C$ and $D$ intersect in $ab$ points when counted with multiplicity.

(e) Prove Bézout's theorem in the case where $C$ is a line. H

(f) Think of examples that show that this result fails for affine curves, fails for non-algebraically-closed fields, and fails when the multiplicity is not counted.

**Problem 11.** Let $k$ be an arbitrary field and let $L$ and $D$ be a line and a curve in $\mathbb{P}^2$ given by $G = 0$ respectively $F = 0$, where $G \nmid F$ in $k[X, Y, Z]$. Let $b$ be the degree of $D$, that is, the degree of $F$.

(a) Prove that if $L$ and $D$ intersect in $b - 1$ (rational) points of $\mathbb{P}^2(k)$ with multiplicity, then they intersect in exactly $b$ (rational!) points with multiplicity. [Hint: use Problem 10(a,b,c), and consider the factorization of $F(X, 0, Z) \in k[X, Z]$.]

(b) Let $D^{\mathrm{ns}}(k)$ be the set of non-singular $k$-rational points of $D$. Conclude that if $b = 3$, then there is a well-defined map $* : D^{\mathrm{ns}}(k) \times D^{\mathrm{ns}}(k) \to D^{\mathrm{ns}}(k)$ given by: $P_1 * P_2$ is the third intersection point of the line through $P_1$ and $P_2$, where we take the tangent line if $P_1 = P_2$.

**Problem 12.** Let $k$ be a field of characteristic not 2 or 3, let $A, B \in k$, and let $E$ be the projective curve with affine equation $Y^2 = X^3 + AX + B$.

(a) Let $P = (x, y)$ be a non-singular point on $E$. Show that the slope of the tangent line in $P$ is given by $\lambda = (3x^2 + A)/(2y)$. In particular, if $y = 0$, the tangent line is the vertical line given by the equation $X = x$. H

(b) Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points in $\mathbb{A}^2(k)$. Show that the slope of the line passing through $P$ and $Q$ is given by $\lambda = (y_2 - y_1)/(x_2 - x_1)$. In particular, if $Q = (x_1, -y_1)$, then the line is the vertical line given by the equation $X = x_1$.

Now suppose $4A^3 + 27B^2 \neq 0$. In other words, by Exercise 2(c) of the first homework, the curve $E$ is an elliptic curve.

(c) Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$ be points on $E$ satisfying $P + Q = R$. Show that H

$$x_1 + x_2 + x_3 = \lambda^2, \qquad \text{and} \qquad (-y_3 - y_1)/(x_3 - x_1) = \lambda,$$

where $\lambda$ is the slope of the line in part (a) or (b) depending on whether $P = Q$ or not.

Let $E$ be the elliptic curve over $\mathbb{Q}$ given by the equation $Y^2 = X^3 + 17$ and let $P = (-2, 3)$, $Q = (-1, 4)$.

(d) Check that $P$ and $Q$ are in $E(\mathbb{Q})$.

(e) Use the formulas of (a)–(c) to calculate $P + P$ and $P + Q$. H

**Problem 13.** Let $E$ be the elliptic curve over $\mathbb{F}_7$ given by $Y^2 = X^3 + 2$.

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

(b) How would you decide whether $E(\mathbb{F}_q)$ is cyclic or not?

[Optional problems on page 3.]

**Problem 14.** (Optional: for students who have problems with ideals of $k[X, Y]$.)

(a) Show that the ideal $I \subset \mathbb{R}[X, Y]$ generated by $X(X^2+Y^2-1)$ and $Y(X^2+Y^2-1)$ is not prime.

(b) Make a picture of $V(I) \subset \mathbb{A}^2(\mathbb{R})$.

(c) Show that the ideal $J \subset \mathbb{R}[X, Y]$ generated by $Y^2 + X^2 - X^3$ is prime and make a picture of $V(J)$.

**Problem 15.** (Optional: for students looking for a challenge) [Note: there may still be mistakes in this problem. Solutions of (a)–(g) can be found in [Silverman, Proposition III.2.5], and guidance with (h) can be found in [Silverman, Exercise III.5].] Let $k$ be a field and let $E$ be the plane projective curve with affine equation $y^2 + xy = x^3$, which has a singular point $(0, 0)$.

(a) Homogenise the equation and show that there is an affine part given by $Z + XZ = X^3$ such that the singular point lies at infinity.

(b) Give a change of variables that changes this curve into the affine curve $C : XZ = (X - 1)^3$.

(c) Show that the map $(x, y) \mapsto x$ is a bijection from the set $C(k)$ of affine rational points of $C$ over $k$ to $k^*$.

(d) Show that three points $(x_i, y_i)$ $i = 1, 2, 3$ (with multiplicity) of $C(k)$ lie on a line if and only if $x_1x_2x_3 = 1$. Conclude that $E(k) \setminus \{(0, 0)\}$ with the chord-and-tangent addition is a group isomorphic to $k^*$ and give a formula for an isomorphism $E(k) \setminus \{0, 0\} \to k^*$.

(e) What can you say about the curve $E : y^2 = x^3$? [Hint: use $C : Z = X^3$ and $(k, +)$ instead of $k^*$.]

(f) And what about $E : y^2 + Axy = x^3$ over any algebraically closed field?

(g) What about any singular Weierstrass curve over any algebraically closed field?

(h) What if the field is not algebraically closed?

Source of problems 12 – 14: adapted from Mastermath Elliptic Curves 2013, René Schoof and Peter Stevenhagen.