CPSC/PMAT 629 — Elliptic Curves and Cryptography
ASSIGNMENT 1

Problem 1. *Some fun with fields...*

(1) Construct a multiplication table for the field $\mathbb{F}_{2^3}$.
(2) Let K be any field and α an algebraic element over K. Prove that any automorphism of $K(\alpha)$ that fixes K elementwise is determined uniquely by where it sends α.
(3) Consider the two (isomorphic) fields

$$\mathbb{F}_3(\alpha) \text{ where } \alpha^3 - \alpha + 1 = 0 \qquad \mathbb{F}_3(\beta) \text{ where } \beta^3 - \beta^2 + 1 = 0 \ .$$

Construct an isomorphism from $\mathbb{F}_3(\alpha)$ to $\mathbb{F}_3(\beta)$.

Problem 2. *A proof that, counting multiplicity, every non-vertical line intersects a Weierstrass equation in 3 places*

Consider an elliptic curve with Weierstrass equation given by $y^2 = x^3 + Ax + B$ over some algebraically closed field K of characteristic different from 2 and 3. Furthermore, consider any line of the form $y = mx + b$, with $m, b \in K$.

(1) Show that if the line intersects E in three points, then the line is not tangent to the curve at any point.
(2) Show that if the line intersects E in only two points, then the curve is tangent to the line at exactly one of the points, and it is not an inflection point (we will define an inflection point to mean that the second derivative vanishes at the point).
(3) Show that if the line intersects E in only one point, then the curve is tangent to the line at that point, and this is an inflection point of the curve .

Note: you should *not* simply appeal to Bezout's theorem for this question. You are being asked to *proof* this part of Bezout's theorem for this case!

Problem 3. *Absolute irreducibility of general elliptic curves*

The general equation for an elliptic curve over a field K may be given as

$$y^2 + h(x)y = f(x)$$

where $h(x), f(x) \in K[x]$ and $h(x)$ has degree 0 or 1, $f(x)$ has degree 3 or 4. In addition, this equation must be non-singular; more precisely, there is no point in $\mathbb{A}^2$ that lies on the curve and simultaneously satisfies

$$2y + h(x) = 0 \qquad h'(x)y = f'(x) \ .$$

(1) If the characteristic of K is not 2, show that this is sufficient to prove that the curve is absolutely irreducible (i.e. is not the union of two curves, or equivalently, $y^2 + h(x)y - f(x)$ is irreducible in $\overline{K}[x, y]$).
(2) If the characteristic of K is 2, show that the curve will be absolutely irreducible if $f(x)$ has degree 3, but it can fail if the degree of $f(x)$ is 4.

Problem 4. *Legendre model*

(1) Put the Legendre equation $y^2 = x(x-1)(x-\lambda)$ into Weierstrass form and use this to show that the j-invariant is
$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2} \ .$$
(2) Show that if $j \neq 0, 1728$, then there are six distinct values of λ giving this j, and that if λ is one such value, then the full set is
$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\} \ .$$
(3) Show that if $j = 1728$ then $\lambda = -1, 2, 1/2$ and if $j = 0$ then $\lambda^2 - \lambda + 1 = 0$.

Problem 5. *Automorphisms of curves*

(1) Show that $(x, y) \mapsto (x, -y)$ is a group homomorphism from E to itself for any elliptic curve in the form $y^2 = x^3 + Ax + B$.
(2) Show that $(x, y) \mapsto (-x, iy)$ (where $i^2 = -1$) is an automorphism of the curve $y^2 = x^3 + Ax$ over a field K containing i.

Problem 6. *A partial proof of associativity of point addition*

Let E be an elliptic curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$ over a field K (obviously of characteristic different from 2). Let P, Q and R be three points on E satisfying the property that none of P, Q, R, $P + Q$ and $Q + R$ have the same x-coordinate. Prove that the x-coordinate of $(P + Q) + R$ is the same as $P + (Q + R)$ (i.e. partially prove associativity).