Math 145, Problem Set 7. Due Friday, May 30.

You may assume that the ground field is $k = \mathbb{C}$.

1. (*Etymology.*) *Part A - Arclength of the ellipse and elliptic integrals.* Let $0 < a < b$. Consider the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

(i) Show that the arclength of the ellipse equals

$$l = 4b \int_0^{\frac{\pi}{2}} \sqrt{1 - k^2 \sin^2 t}\, dt,$$

for some $k < 1$.

(ii) Prove that this integral can be written as

$$\int_0^1 \sqrt{\frac{1 - k^2u^2}{1 - u^2}}\, du = \int_0^1 \frac{4a(1 - k^2u^2)}{\sqrt{(1 - u^2)(1 - k^2u^2)}}\, du.$$

Remark: The substitution

$$v^2 = (1 - u^2)(1 - k^2u^2)$$

in the denominator comes to mind, but unfortunately it is not helpful in evaluating the integral. The (u, v)-curve defined by the equation above is called a *hyperelliptic quartic.*

(iii) Making a suitable substitution, e.g. $x = (1 + u)^{-1}$, show that the integral above can be put in the form

$$\int \frac{r(x)\, dx}{\sqrt{f(x)}}$$

where $r(x)$ is a rational fraction, and $f(x)$ is a cubic polynomial. An integral of this type is called an *elliptic integral.* The arclength of the ellipse is therefore computed by an elliptic integral. The substitution

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

in the denominator is obviously a cubic curve.

Remark: Elliptic integrals cannot be evaluated by elementary functions. They can be computed in terms of the so-called *elliptic functions* to be introduced below.

Part B - Cubics versus quartics. Show that the hyperelliptic quartic curve

$$v^2 = (1 - u^2)(1 - k^2u^2)$$

is birational to an affine elliptic curve E_λ. For instance, you may want to set $y = v(u+1)^{-1}$.

More historical remarks: Euler asked for solutions $y = y(x)$ of the differential equation

$$\frac{dx}{\sqrt{f(x)}} = \frac{dy}{\sqrt{f(y)}}$$

where f is a cubic polynomial. Note that integrating both sides with respect to x and y leads to *elliptic integrals* which cannot be evaluated in terms of elementary functions. Therefore solutions to the differential equation above are not so easy to write down.

Nonetheless, Euler found solutions $y = y(x)$; in fact he found an entire family $y_\tau = y_\tau(x)$ depending on a parameter τ. It turns out that this family is related to the group law on the elliptic curve $y^2 = f(x)$. The solution y_τ evaluated at a point x was given by the formula

$$(x, \sqrt{f(x)}) \oplus (\tau, \sqrt{f(\tau)}) = (y_\tau, \sqrt{f(y_\tau)}).$$

In addition, Euler proved that for any α, β there exists γ, which can be expressed as a rational function of α and β, such that

$$\int_0^\alpha \frac{dx}{\sqrt{f(x)}} + \int_0^\beta \frac{dx}{\sqrt{f(x)}} = \int_0^\gamma \frac{dx}{\sqrt{f(x)}}.$$

It turns out that these identities are related to the addition on the cubic curve; in fact,

$$(\alpha, \sqrt{f(\alpha)}) \oplus (\beta, \sqrt{f(\beta)}) = (\gamma, \sqrt{f(\gamma)}).$$

2. (*The j-invariant.*) Show that if $j(\lambda) = j(\mu)$ then $E_\lambda \cong E_\mu$.

Hint: First show that if $j(\mu) = c =$ constant then μ can have at most 6 values. If $c = j(\lambda)$ what are the 6 values for μ? Make sure you consider repetitions in the set of 6 values you found. These correspond to the cases $j = 0$ and $j = 1728$.

3. (*Pappus's theorem.*) Let l and m be two projective lines in $\mathbb{P}^2$, and let p_1, p_2, p_3 be points on $l \setminus l \cap m$ and q_1, q_2, q_3 be points on $m \setminus l \cap m$. Let L_{ij} be the line joining p_i and q_j. Show that the three points of intersection of the pairs of lines L_{ij} and L_{ji} are collinear. You may wish to find two cubics intersecting in 9 points.

4. (*The group law on elliptic curves.*)

(i) Consider two points $P([x_1 : y : 1])$ and $Q([x_2 : y_2 : 1])$ on the elliptic curve

$$y^2 z = x(x - z)(x - \lambda z).$$

Prove that the sum

$$P \oplus Q = \begin{cases} [0 : 1 : 0] \text{ if } x_1 = x_2 \text{ but } y_1 \neq y_2 \\ [x_3 : y_3 : 1] \text{ if } x_1 \neq x_2 \end{cases},$$

where

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 + 1 + \lambda - x_1 - x_2$$

$$y_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right) x_3 + \left(\frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}\right).$$

What are the corresponding formulas if $P = Q$?

Hint: First let $y = mx + b$ be the line passing through P and Q. Find m and b in terms of x_1, y_1, x_2, y_2. Then substitute into the equation of the elliptic curve. Note if you know two of the roots of a cubic polynomial, the third one can be determined from one of the coefficients.

(ii) Show that if $\lambda \in \mathbb{Q}$, then the set of points on the elliptic curve with rational coordinates form an abelian group. You only need to check that if P, Q have rational coordinates, so do $-P$ and $P \oplus Q$.

Remark: The abelian group of rational points on the elliptic curve is typically denoted $\overline{E}_\lambda(\mathbb{Q})$. The Mordell-Weil theorem states that this abelian group is finitely generated.

5. (*The group law on the cuspidal cubic.*) Solve problem 2.11 in the textbook.

6. (*Elliptic functions, the Weierstrass function and the parametrization of cubics.*) This question is *entirely optional*, and it requires background in complex analysis. I am happy to explain the necessary background to those who need it.

Let

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$$

be a *complex lattice*. That is, let $\omega_1, \omega_2 \in \mathbb{C}$ be complex numbers with $\omega_1/\omega_2 \notin \mathbb{R}$, and let

$$L = \{m\omega_1 + n\omega_2 : \ m, n \in \mathbb{Z}\}.$$

(i) Show that the infinite series

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

converges to a *meromorphic* function in z with poles of order 2 at the points of L. This is called the *Weierstrass* function.

(ii) Prove that $\wp$ is an even function

$$\wp(z) = \wp(-z),$$

hence its Laurent expansion near 0 contains only even powers of z. Show that its derivative

$$\wp'(z) = -\sum_{\omega \in L} \frac{2}{(z-\omega)^3}$$

is an odd function.

(iii) Moreover, prove that $\wp$ is a *meromorphic elliptic function* e.g.

$$\wp(z+\omega) = \wp(z)$$

for all $\omega \in L$. In other words, $\wp$ is doubly periodic, with periods ω_1 and ω_2.

(iv) Use Liouville's theorem to conclude that *holomorphic* doubly periodic functions are constant.

(v) Show that the $\wp$ function associated to a lattice L satisfies a differential equation

$$\wp'(z)^2 = c_3\wp^3(z) + c_2\wp(z)^2 + c_1\wp(z) + c_0$$

for some constants c_i that depend on L.

Hint: Consider the meromorphic function

$$f(z) = \wp'(z)^2 - c_3\wp^3(z) - c_2\wp(z)^2 - c_1\wp(z) - c_0.$$

Observe that $f(z)$ has a pole of order at most 6 at the origin, and only even powers of z appear in the Laurent expansion. Show that you can pick c_0, c_1, c_2, c_3 such that the Laurent coefficients of $z^{-6}, z^{-4}, z^{-2}, z^0$ in f vanish. Conclude that f is a holomorphic doubly periodic function. Finally, show that $f = 0$.

Remark: With a bit more care, one can show that $c_3 = 4, c_2 = 0$ and c_1, c_0 are given by the *Eisenstein series*

$$c_1 = -60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4}, \ c_0 = -140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6}.$$

(vi) From (v), conclude that the point $(\wp(z) : \wp'(z))$ lies on the cubic curve

$$y^2 = c_3x^3 + c_2x^2 + c_1x + c_0$$

for all values of z. In fact, it turns out that any point on the cubic curve above can be written as $(\wp(z), \wp'(z))$. Therefore $z \mapsto (\wp(z), \wp'(z))$ gives a parametrization of the cubic by *elliptic functions.* Note that we have seen already that a cubic curve does not admit a parametrization by rational functions. It can be shown that the argument can be reversed, e.g. any cubic can be parametrized by the Weierstrass function of some lattice L.