MA426 Elliptic curves

Instructions: The worksheets and other course handouts are available from my website and from the shelves outside my office. The assignments count for 15% of the credit. There are 5 worksheets, and I'll take the total marks by doing best 4 out of 5. Solutions must be handed in by deadline TBA.

I would be grateful for comments on the worksheets or the course material. Miles Reid

Assignment A

A.1. Let $f(x) = x^3 + ax + b$ be a cubic polynomial with coefficients in $\mathbb{R}$. It is known that $f(x)$ has repeated roots if and only if the discriminant $\Delta := 4a^3 + 27b^2 = 0$. If f has a double root α, verify directly that

$$a = -3\alpha^2 \leq 0 \quad \text{and} \quad b = 2\alpha^3,$$

so that α has the same sign as b. [Hint: write the coefficients $0, a, b$ of f in terms of its roots using

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 + ax + b.]$$

Sketch the singular real curve $y^2 = f(x)$ in the two cases $\alpha < 0$ and $\alpha > 0$.

Start from values of a, b giving a double root $\alpha < 0$. Give a plausible argument that increasing b slightly should lead to $\Delta > 0$ and f has one real root only, and decreasing b slightly leads to $\Delta < 0$ and f has 3 real roots. (Another useful mnemonic is that $x^3 - k^2x$ has 3 real roots and obviously $\Delta < 0$, whereas $x^3 + k^2x$ has 1 real and 2 imaginary conjugate roots and $\Delta > 0$.)

Sketch the corresponding nonsingular curves $y^2 = f(x)$ corresponding to the neighbouring values of a.

A.2. Let $S^2 : (x_1^2 + x_2^2 + x_3^2 = 1) \subset \mathbb{R}^3$ be the round sphere. Show that stereographic projection from the N pole $N = (0, 0, 1)$ to the plane $x_3 = 0$ given by $(x_1, x_2, x_3) \mapsto \frac{1}{1-x_3}(x_1, x_2, 0)$ is 1-to-1 from $S^2 \setminus N$ to $\mathbb{R}^2$. Write

$$z = \frac{x_1 + ix_2}{1 - x_3} \in \mathbb{C}.$$

This identifies $S^2 \setminus N$ with $\mathbb{C}$. Now identify $z = w^{-1}$ with an appropriate projection of S^2 from the S pole. [Hint: you just have to change a few signs and make use of the equation of S^2.]

The Riemann sphere is the z-plane and the w-plane (two copies of $\mathbb{C}$) glued by $w = z^{-1}$. The point of the question is to see the abstract identification of these two planes in terms of the standard sphere in $\mathbb{R}^3$.

A.3. Find the proof of Liouville's theorem in your Complex Analysis lecture notes. Give an alternative proof along the following lines: let $f(z)$ be a bounded holomorphic function on $\mathbb{C}$. If $a, b, \in \mathbb{C}$ and Γ is the boundary circle of a big disc of radius $R > |a|, |b|$ then calculate

$$\oint_\Gamma \frac{f(z)\mathrm{d}z}{(z-a)(z-b)}$$

by Cauchy's integral formula. On the other hand, by arguing in the disc of the variable $w = 1/z$, show (again by Cauchy's integral formula) that the integral is zero. Be careful to translate $\mathrm{d}z$ into the appropriate multiple of $\mathrm{d}w$ where $w = z^{-1}$. If you're careless about this point, you might be able to prove that a linear function such as z is constant.

A.4. Consider $y^2 = f(x)$ a cubic with a double root, say for simplicity $y^2 = x(x-1)^2$. Integrate $\int \frac{\mathrm{d}x}{y}$ in terms of elementary functions. [Hints: substitute $t = y/(x-1) = \sqrt{x}$; the answer involves partial fractions and log.]

(The point of the question is historical and etymological. Integrals of the form $\int \frac{\mathrm{d}x}{\sqrt{f}}$ with $f(x)$ a cubic or quartic in x having no repeated roots are called *elliptic integrals*. They cannot be expressed in elementary functions, but instead give rise to elliptic functions and elliptic curves.

The arc length of the ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ leads to the integral

$$\int \mathrm{d}s = \int \sqrt{1 + \left(\tfrac{\mathrm{d}y}{\mathrm{d}x}\right)^2}\, \mathrm{d}x, \quad \text{working out as} \quad a \int \frac{1 - k^2\xi^2}{\sqrt{(1-\xi^2)(1-k^2\xi^2)}}$$

with $k^2 = 1 - \frac{b^2}{a^2}$. Euler found out that this cannot be solved in terms of elementary functions, but has lots of interesting functional equations that led eventually to the group law on the torus $y^2 = (1-\xi^2)(1-k^2\xi^2)$.)

MA426 Elliptic curves

Assignment B

B.1. Let f be an elliptic function of order 2. Use Theorem 2.11, (II) and (III) to prove the following:

1. For all $c \in \mathbb{C}$, the function $f(z) - c$ has either 2 zeros $z = \alpha_1, \alpha_2$ mod L, or one repeated zero $z = \beta$ with multiplicity 2 (so that $f(z) - c \sim (z - \beta)^2 \cdot$ invertible near β).

2. There exists some $d \in \mathbb{C}$ such that $\alpha_1 + \alpha_2 = d$ in the first case, $2\beta = d$ in the second (independently of c).

3. The case of a repeated zero $z = \beta$ must happen for at least 3 distinct values of c. When do you get 3 double zeros, and when 4?

4. If we shift the origin, and think of f as a function of $z' = z - d/2$ then $f(z')$ is an even function.

The point of the question is that you can prove that f has much the same properties as the Weierstrass $\mathfrak{p}$ function by using Theorem 2.11, (II) and (III), without knowing anything about the construction of $\mathfrak{p}$.

B.2. Recall that we write $w_1/2, w_2/2$ and $w_3/2 = w_1/2 + w_2/2$ for the 3 halfperiods of L, and set $\mathfrak{p}(w_i/2) = e_i$.

Figure out for yourself the proof that $\mathfrak{p}(z) - e_i$ has the double zero $w_i/2$ (or read it up). Prove that $e_i \neq e_j$.

Prove that the derivative $\mathfrak{p}'$ of the Weierstrass $\mathfrak{p}$ function satisfies the differential equation

$$(\mathfrak{p}')^2 = 4(\mathfrak{p} - e_1)(\mathfrak{p} - e_2)(\mathfrak{p} - e_3).$$

(Hint: Compare their zeros and poles, and the leading term at the pole.)

The point of the question is to give another derivation of the equation $(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3$. Note that $e_1 + e_2 + e_3 = 0$, $4(e_1e_2 + e_2e_3 + e_3e_1) = g_2$ and $4e_1e_2e_3 = -g_3$.

B.3. Continue the computation of 2.18 (where we derived the equation $(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - 60G_4\mathfrak{p} - 140G_6$), keeping the terms in z^2 and z^4, to deduce that

$$G_8 = \text{multiple of } G_4^2 \quad \text{(to be determined)} \tag{1}$$

$$G_{10} = \frac{5}{3}G_4G_6. \tag{2}$$

In principle you can get a similar formula for every G_{2k}. It would be quite difficult to derive this result just from the definition.

B.4. Let f be an elliptic function, viewed as a map $f\colon E = \mathbb{C}/L \to \mathbb{P}^1_{\mathbb{C}}$. If $z_0 \in \mathbb{C}$ is not a pole of f, set $f(z_0) = c$; we say that f has *ramification of order* m at z_0 if z_0 is an m-fold zero of $f - c$, that is, if

$$f(z) - c = (z - z_0)^m \cdot \text{invertible}.$$

We say that z_0 is a *ramification point* of f is $m \geq 1$. Then f maps a disc around $z_0 \in \mathbb{C}$ to a disc around $c \in \mathbb{C}$ by $z \mapsto (z - z_0)^m$. On the other hand, if z_0 is a pole of f, we say that f has ramification of order m at z_0 if it has pole of order m. Justify this usage (in terms of the parameter at infinity in the image $\mathbb{P}^1_{\mathbb{C}}$).

Suppose that f has order d (defined in 2.12 of lectures). Prove that the sum of $m - 1$ taken over every ramification point equals $2d$.

[Hint: Do something quite different at the multiple zeros of $f - c$ and the poles of f to get this out. Write f' for the derivative; first considering its poles, you calculate order f' as $\sum_{\text{poles}} m + 1$. By the basic property of order, f' also has the same number of zeros counted with multiplicity; the zeros of f' of order $n - 1$ are the ramification points of f of order n. Don't give up just before you get to the end!]

The point of this question is that E has Euler characteristic 0, and $\mathbb{P}^1_C$ has Euler characteristic 2. Suppose we give $\mathbb{P}^1_{\mathbb{C}}$ a sufficiently fine triangulation with vertices including all ramification points. If $E \to \mathbb{P}^1_{\mathbb{C}}$ were an unramified cover, you would find $2d$ for the Euler characteristic of E, and it is not hard to see that a ramification point of order m decreases this by $m - 1$. So we must have $\sum_{\text{branch pts}} m - 1 = 2d$.

MA426 Elliptic curves

Assignment C

C.1. Let $x^3+ax+b = (x-\alpha)(x-\beta)(x-\gamma)$ so that, as usual, the elementary symmetric functions in α, β, γ are

$$\alpha+\beta+\gamma = 0, \quad \alpha\beta+\beta\gamma+\gamma\alpha = a, \quad \alpha\beta\gamma = -b$$

Note that $\Delta = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$ is a symmetric polynomial in α, β, γ. It is known that any symmetric polynomial can be written in terms of the elementary symmetric functions. By calculating this expression explicitly, prove that $\Delta = -(4a^3+27b^2)$.

So (once again), the cubic has distinct roots if and only if $\Delta \neq 0$. (By the way, you can do the same calculations for a general cubic x^3+cx^2+ax+b, but the calculations become unwieldy.)

C.2. Consider the two curves defined (over some field K) by $y^2+y = x^3+x^2+x$ and $y^2+y = x^3-x$. Verify directly that each curve is nonsingular except in one characteristic. [Hint: do 2 and 3 separately. Then complete the square and cube to get $y^2 = x^3+ax+b$ with $a, b \in \mathbf{Q}$, and calculate Δ.]

For each of these curves, write out all their Tate constants (see handout) and calculate their discriminant Δ according to Tate.

C.3. You know from coordinate geometry how to write the line joining $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in the form $y = mx+c$. Suppose C is the curve $y^2 = x^3+ax+b$ and $P_1, P_2 \in C$; substitute $y = mx+c$ to obtain a cubic in x, defining the 3 points of intersection of $L = P_1P_2$ with C. Deduce a formula for P_1+P_2 (in the group law) of the form

$$x_3 = m^2-x_1-x_2, \quad y_3 = -mx_3-c \quad (\text{for } x_1 \neq x_2.)$$

In the same way, write down the tangent line to C at $P = (x_1, y_1)$ in the form $y = mx+c$ [Hint: the slope must be given by $m = \frac{\partial f/\partial x}{\partial f/\partial y}$], and deduce a formula for $2P$ in the group law of the form

$$x_3 = m^2-2x_1, \quad y_3 = -mx_3-c.$$

[Harder] Think through the proof that the group law on C is associative "on general points".

C.4. ([UAG], Ex. 2.11.) Consider the curve $C : (z = x^3) \subset k^2$; C is the image of the bijective map $\varphi\colon k \to C$ by $t \mapsto (t, t^3)$, so it inherits a group law from the additive group k. Prove that this is the unique group law on C such that $(0, 0)$ is the neutral element and

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear}$$

for $P, Q, R \in C$ (with the usual conventions about multiple roots). [Hint: you might find useful the identity

$$\det \begin{vmatrix} 1 & a & a^3 \\ 1 & b & b^3 \\ 1 & c & c^3 \end{vmatrix} = (a-b)(b-c)(c-a)(a+b+c).]$$

In projective terms, C is the curve $Y^2Z = X^3$, our old friend with a cusp at the origin and a flex at $(0, 1, 0)$, and the point of the questions is that the usual construction gives a group law on the complement of the singular points.

MA426 Elliptic curves

Assignment D

D.1. A rational Pythagorean triangle is a triple $a, b, c \in \mathbf{Q}$ with $a^2+b^2 = c^2$. An integer n that is the area $\frac{1}{2}ab$ of a rational Pythagorean triangle is called *congruent*. Prove that n is congruent if and only if there exist an arithmetic progression $x-n, x, x+n$ consisting of three nonzero rational numbers each of which is a perfect square. [Hint: try $x - n = \frac{1}{4}(a-b)^2$.]

If this happens, the elliptic curve $y^2 = x(x-n)(x+n)$ obviously has a rational point with $y \neq 0$. Prove the converse. [Hint: start from a point $P \in C(\mathbf{Q})$ that is not a 2-torsion point. The point $2P \in C(\mathbf{Q})$ is not the point at infinity, and is a double. Now apply the criterion of Theorem 4.4.]

D.2. Fermat proved that $u^4 + v^4 = w^2$ has no integer solutions other than trivial ones: starting from a solution with coprime u, v, w, we mess around, make a couple of normalising assumptions, and eventually get a new solution $r^4 + s^4 = t^2$ with $u = r^4 - s^4$, $v = 2rst$.

Consider the equation

$$u^4 + v^4 = w^2 \quad \text{or} \quad v^4 = (w-u^2)(w+u^2), \tag{3}$$

where we view $(u, v, w) \mapsto (\lambda u, \lambda v, \lambda^2 w)$ as equivalent solutions. Write

$$\frac{v^2}{w-u^2} = \frac{(w+u^2)}{v^2} = \frac{x}{2}, \quad \frac{u}{v} = \frac{y}{2x}.$$

Solve for u^2/v^2 in terms of x, and show that

$$\frac{u^2}{v^2} = \frac{1}{2}\left(\frac{x}{2} - \frac{2}{x}\right)$$

and therefore $y^2 = x(x^2-4)$. (The descent in Fermat's proof can be interpreted as 2-division on this elliptic curve.)

Invert this procedure, to go from a solution of $y^2 = x(x^2-4)$ to a solution of (1). Deduce that the elliptic curve $C : y^2 = x(x^2-4)$ has no rational point with $y \neq 0$, and that 2 is not congruent.

D.3. Let $g(x) = x^3 + ax + b$ and $g_1 = 3x^2 + a = \frac{\mathrm{d}g}{\mathrm{d}x}$. Calculate successively $g_2 = 3g - xg_1$, $g_3 = 3xg_2 - 2ag_1$ and $g_4 = 9bg_2 - 2ag_3$. If you're lucky, you should get $g_4 = 27b^2 + 4a^3 = -\Delta$. Work backwards through the calculation to deduce that

$$Ag + Bg_1 = -\Delta, \quad \text{where} \quad A = -18ax + 27b, \quad B = 6ax^2 - 9bx + 4a^2. \tag{4}$$

Now observe that in turn $B = -9xg + (3x^2 + 4a)g_1$. We can use this to get a simple derivation of $-\Delta$ as a combination of $f = g_1^2 - 8xg$:

$$-\Delta = (3x^2 + 4a)(g_1^2 - 8xg) + (-3x^3 + 5ax + 27b)g. \tag{5}$$

Verify the identity

$$\begin{aligned} -x^6\Delta = &\Big((a^3 + 3b^2)x^2 - a^2bx - 2ab^2\Big)f \\ &+\Big((3a^3 + 24b^2)x^3 + a^2bx^2 - (16ab^2 + a^4)x + 2a^3b\Big)g. \end{aligned} \tag{6}$$

(This can also be derived by the same kind of reasoning.)

The point of the question is to get $-\Delta q^6 = R(p,q)F(p,q) + S(p,q)G(p,q)$ and $-\Delta p^6 = R'(p,q)F(p,q) + S'(p,q)G(p,q)$. This kind of identity (with $6 \mapsto 7$) was used in Lemma 4.12, (iii) to bound the cancellation that can happen in $x(2P) = F(p,q)/G(p,q)$. The textbooks give a bigger formula for $-\Delta q^7$, with a much nastier derivation ([Knapp], p. 96, probably copied from Silverman and Tate).

D.4. Write out all the integral points of $C : y^2 + y = x^3 - x^2$ with $|x|, |y| \leq 2$. Calculate the sum and doubles of all these points, and show they form a subgroup of C. (In fact this is the whole of $C(\mathbf{Q})$.)

MA426 Elliptic curves

Assignment E

E.1. Write

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

for the usual generators of $\mathrm{SL}(2, \mathbf{Z})$. Sketch the fundamental domain

$$D := \Big\{ z \;\Big|\; |z| \geq 1 \text{ and } -1/2 \leq \mathrm{Re}\, z \leq 1/2 \Big\}$$

and its successive translates by

$$T, S, TS, ST, ST^{-1}, ST^{-1}S$$

From the figure (or directly) find the elements of $\mathrm{SL}(2, \mathbf{Z})$ fixing respectively $\omega = \exp(\frac{2\pi i}{3})$ and $-\overline{\omega} = 1 + \omega = -\omega^2$.

Compare [Serre, Cours d'arithmétique, Chapter 7] for the (easy) proof that D is the fundamental domain of $\mathrm{SL}(2, \mathbf{Z})$ and S, T are its generators.

E.2. Calculate the first 3 coefficients of G_4, G_6, Δ and j using the standard table of formulas given in Section 5.9 of the notes.

E.3. If p is a prime, show that $\Gamma_0(p)$ has fundamental domain consisting of the $p+1$ orbits D and $ST^i(D)$ for $i = 0, \ldots, p-1$, and its cusps (the closure at $\{\infty\} \cup \mathbf{Q}$ of the fundamental domain) are just ∞ and 0. It has index $[\mathrm{SL}(2, \mathbf{Z}) : \Gamma_0(p)] = p + 1$.

E.4. Write $\mathrm{SL}(2, \mathbf{Z}/N)$ for the group of matrixes with coefficients in $\mathbf{Z}/N$ with determinant 1 and $\Gamma_0(N)(\mathbf{Z}/N)$ for the subgroup with bottom left entry $= 0$. For $N = 6$, calculate the order of $\mathrm{SL}(2, \mathbf{Z}/6)$ and $\Gamma_0(N)(\mathbf{Z}/N)$.

Deduce that the index $[\mathrm{SL}(2, \mathbf{Z}) : \Gamma_0(6)] = 12$. Write out a set of cosets, and deduce a fundamental domain of $\Gamma_0(6)$ as a union of 12 translates of D

E.5. (Challenge question! compare [Knapp, p. 267, Example 5].) Write

$$\eta(\tau) = \exp\Big(\frac{\pi i \tau}{12}\Big) \prod_{n=1}^{\infty} (1 - q^n)$$

so that $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$. It is known that

$$\eta(\tau+1) = \exp\Big(\frac{\pi i}{12}\Big)\eta(\tau) \quad \text{and} \quad \eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau).$$

Thus, η is *definitely not* a modular form.

Prove that $\left(\eta(\tau)^p/\eta(p\tau)\right)^2$ is a cusp form of weight p for $\Gamma_0(p)$; using Δ deduce that if $p \equiv 11 \bmod 12$ then $\left(\eta(p\tau)\eta(\tau)\right)^2$ is a cusp form of weight 2 for $\Gamma_0(p)$.