22MAC260 Problem Sheet 4: Solutions

Week 4 Lectures

Last updated March 8, 2024

1. Let a and b be complex numbers such that $-4a^3 - 27b^2 \neq 0$. Let E and E' be the elliptic curves given the by two equations

$$E\colon\ y^2 = x^3 + ax + b$$
$$E'\colon\ y^2 = x^3 + ax - b.$$

   (a) Show that $E \simeq E'$.

   Solution: By our definition of isomorphism in Week 4, we need to find a complex number μ satisfying

$$\mu^4 a = a$$
$$\mu^6 b = -b.$$

   For any value of a, the first equation has solutions $\mu = \pm 1, \pm i$. To satisfy the second equation, we can then choose $\mu = \pm i$.

   (b) If a, $b \in \mathbb{R}$, show that E and E' are not isomorphic over $\mathbb{R}$ unless $b = 0$.

   Solution: If $b \neq 0$ then the second equation above becomes $\mu^6 = -1$. This equation has no solutions $\mu \in \mathbb{R}$, so E and E' are not isomorphic over $\mathbb{R}$.

2. Consider the family of curves

$$E_t: \quad y^2 = x^3 + a(t)x + b(t)$$

   where $a(t)$ and $b(t)$ are polynomials in the parameter t. Suppose that

$$\Delta(t) = -4a(t)^3 - 27b(t)^2$$

   is not identically zero.

   (a) Show that there is a finite (possibly empty) set V of values for t such that E_t is an elliptic curve for all $t \in \mathbb{C} \setminus V$.

Solution: The point here is just that for any chosen value of t, the value of $\Delta(t)$ as defined above is the discriminant of the curve E_t. So E_t is an elliptic curve if and only if $\Delta(t) \neq 0$. Now $\Delta(t)$ is a polynomial which by assumption is not identically zero, hence it has finitely many roots $t_1, \dots, t_n$. Define V to be the set $\{t_1, \dots, t_n\}$: then for any $t \in \mathbb{C} \setminus V$, we have that $\Delta(t) \neq 0$, hence E_t is an elliptic curve.

(b) Suppose that neither of a and b is identically zero, that a and b have no common root, and that $3 \deg a \neq 2 \deg b$. Show that for every $c \neq 0$, -1728 there is an elliptic curve E_t in the family with $j(E_t) = c$.

Solution: Let c be a fixed complex number, not equal to either 0 or 1728. To find a value of t such that $j(E_t) = c$ we have to solve the equation

$$1728 \frac{4a(t)^3}{\Delta(t)} = c.$$

Writing $\Delta(t) = -4a(t)^3 - 27b(t)^2$ and rearranging, this becomes

$$4(c + 1728)a(t)^3 + 27cb(t)^2 = 0. \qquad (*)$$

Since by assumption $c \neq 0, -1728$, the coefficients of $a(t)^3$ and $b(t)^2$ in equation $(*)$ are both nonzero.

Moreover, since $\deg(a(t)^3) = 3 \deg a(t) \neq 2 \deg b(t) = \deg(b(t)^2)$, the terms on the left-hand side of $(*)$ have different degrees, and hence the degree of the left-hand side is $\max\{3 \deg a(t), 2 \deg b(t)\} > 0$. So in particular we see that the left-hand side of $(*)$ is not a constant polynomial, and hence Equation $(*)$ has at least one solution t_0.

To finish, we need to check that our solution t_0 actually corresponds to an elliptic curve: in other words, that $\Delta(t_0) \neq 0$. Now if t_o is a common solution of $(*)$ and $\Delta = 0$, then it must also be a root of

$$\gcd\left(4(c + 1728)a(t)^3 + 27cb(t)^2, -4a(t)^3 - 27b(t)^2\right) = a(t)^3$$

But then t_0 is a common root of $a(t)$ and $\Delta(t)$, hence also a root of $b(t)$. This contradicts the assumption that $a(t)$ and $b(t)$ have no common roots.

3. *Legendre form.* A cubic is in **Legendre form** if it is given as

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

for some number $\lambda \neq 0$, 1.

(a) Show that every cubic in Legendre form defines an elliptic curve.

Solution: There is not really anything to show here. Since by assumption $\lambda \neq 0$, the right-hand side of the equation defining E_λ is a cubic with 3 distinct roots 0, 1, λ, hence it satisfies our definition of elliptic curve.

(b) Transform the Legendre equation into Weierstrass form.

Solution: According to the lectures from Week 3, if we transform the cubic

$$y^2 = x^3 + \beta x^2 + \gamma x + \delta$$

to Weierstrass form, we get the cubic

$$\begin{aligned} y^2 &= x^3 + \gamma' x + \delta' \quad \text{where} \\ \gamma' &= \gamma - \frac{1}{3}\beta^2, \\ \delta' &= \delta - \frac{1}{3}\beta\gamma + \frac{2}{27}\beta^3. \end{aligned}$$

Multiplying out the Legendre equation above we get

$$y^2 = x^3 + (-\lambda - 1)x^2 + \lambda x$$

so we have

$$\beta = -\lambda - 1,\ \gamma = \lambda,\ \delta = 0.$$

Putting these into the formulas above we get the Weierstrass form

$$\begin{aligned} y^2 = x^3 &+ \left(\lambda - \frac{1}{3}(\lambda+1)^2\right) x \\ &+ \left(\frac{1}{3}\lambda(\lambda+1) - \frac{2}{27}(\lambda+1)^3\right). \end{aligned}$$

(c) Use the previous part to show that for every $j \neq 0$, 1728, there are exactly 6 values of λ such that $j(E_\lambda) = j$.

Solution: This turns out to be a fairly difficult computation, so don't worry too much if you weren't able to work through the whole solution.

First we have to compute the j-invariant as a function of λ. Taking the coefficients of our short Weierstrass form from above

$$\begin{aligned} a &= \lambda - \frac{1}{3}(\lambda+1)^2 = \frac{1}{3}\left(3\lambda - (\lambda+1)^2\right) \\ b &= \frac{1}{3}\lambda(\lambda+1) - \frac{2}{27}(\lambda+1)^3 = \frac{1}{27}\left(9\lambda(\lambda+1) - 2(\lambda+1)^3\right) \end{aligned}$$

Plugging these into our formula $j = -1728\frac{4a^3}{4a^3+27b^2}$ we get

$$j = -1728\,\frac{4\cdot\frac{1}{27}(3\lambda - (1+\lambda)^2)^3}{\frac{4}{27}(3\lambda-(1+\lambda)^2)^3 + \frac{1}{27}(9\lambda(1+\lambda) - 2(1+\lambda)^3)^2}$$

We can multiply by 27 above and below to get rid of fractions in numberator and denominator. The numerator then simplifies to give

$$1728 \cdot 4(\lambda^2 - \lambda + 1)^3.$$

For the denominator we get

$$\begin{aligned}
&4(3\lambda - (1+\lambda)^2)^3 + (9\lambda(1+\lambda) - 2(1+\lambda)^3)^2 \\
=& -4(\lambda^2 - \lambda + 1)^3 + (-2\lambda^3 + 3\lambda^2 + 3\lambda - 2)^2 \\
=& -27\lambda^2(\lambda - 1)^2.
\end{aligned}$$

Putting everything back together we get

$$\begin{aligned}
j &= -\frac{1728 \cdot 4}{27} \frac{(\lambda^2 - \lambda + 1)^2}{\lambda^2(\lambda - 1)^2} \\
&= -256 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.
\end{aligned} \tag{**}$$

Now to prove the claim, we observe (check it!) that our formula for j is invariant under the two substitutions

$$\begin{aligned}
\lambda &\mapsto 1 - \lambda \\
\lambda &\mapsto \frac{1}{\lambda}.
\end{aligned}$$

Applying these substitutions repeatedly, we end up with the 6 values

$$\lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}.$$

For a fixed value of j, the formula $(**)$ above gives a degree-6 polynomial in λ. This polynomial has (at most) 6 roots, so if the 6 values above are distinct, they must be all the roots, so we get exactly 6 values of λ for which E_λ has the given j-invariant.

Let us analyse the cases when the 6 values above are not distinct. We find the following possibilities: first

$$\begin{aligned}
\lambda &= \frac{1}{\lambda}, \\
1 - \lambda &= \frac{\lambda - 1}{\lambda}, \\
\frac{1}{1 - \lambda} &= \frac{\lambda}{\lambda - 1}
\end{aligned}$$

which happens exactly when $\lambda = -1$. Next,

$$\begin{aligned}\lambda &= 1 - \lambda,\\ \frac{1}{\lambda} &= \frac{1}{1-\lambda},\\ \frac{\lambda}{\lambda - 1} &= \frac{\lambda - 1}{\lambda}\end{aligned}$$

which happens exactly when $\lambda = \frac{1}{2}$.
Next,

$$\begin{aligned}\lambda &= \frac{\lambda}{\lambda - 1},\\ 1 - \lambda &= \frac{1}{1-\lambda},\\ \frac{1}{\lambda} &= \frac{\lambda - 1}{\lambda}\end{aligned}$$

which happens exactly when $\lambda = 2$.
In each of these case, plugging in the value of λ in $(**)$ we get $j(E_\lambda) = -1728$.

Finally, we can also have

$$\begin{aligned}\lambda &= \frac{1}{1-\lambda} = \frac{\lambda - 1}{\lambda}\\ 1 - \lambda &= \frac{1}{\lambda} = \frac{\lambda}{\lambda - 1}\end{aligned}$$

which happens when $\lambda^2 - \lambda + 1 = 0$, in other words when $j(E_\lambda) = 0$. Writing the values out explicitly we get

$$\lambda = \frac{1 \pm \sqrt{3}i}{2}.$$

(d) Which values of λ give $j(E_\lambda) = 0$? Which give $j(E_\lambda) = -1728$?
Solution: answered in the previous part.

4. Starting from the right-angled triangle with sides of length $(5, 12, 13)$, use the method described in the Week 4 lectures to produce another right-angled triangle with rational sides and area 30.

Solution: Using formula (1) in Theorem 3.1 of the Week 4 notes with $q = 30$, the triple $(5, 12, 13)$ maps to the point

$$\begin{aligned} P &= \left(\frac{30 \cdot 12}{13 - 5}, \frac{2 \cdot 30^2}{13 - 5}\right) \\ &= (45,\ 225) \end{aligned}$$

on the curve

$$E\colon y^2 = x^3 - 900x.$$

Now we apply the formulas for point addition from the Week 3 notes. We compute

$$\begin{aligned} m' &= \left(\frac{3x^2 - 900}{2y}\right)_{|P} \\ &= \frac{23}{2} \end{aligned}$$

and hence

$$\begin{aligned} x(2P) &= \left(\frac{23}{2}\right)^2 - 2x(P) \\ &= \frac{169}{4} \\ y(2P) &= -\left(y(P) + m'(x(2P) - x(P))\right) \\ &= -\frac{1547}{8}. \end{aligned}$$

Since $y(2P) < 0$, applying formula (2) from Theorem 3.1 of the Week 4 notes would give us a triple (a, b, c) with $a < 0$, $b < 0$, $c < 0$. So instead of $2P$, we use the point $-2P = P * P$. We have

$$-2P = \left(\frac{169}{4}, \frac{1547}{8}\right)$$

and plugging these coordinates into formula (2) from the Week 3 notes, we get

$$(a, b, c) = \left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right).$$