23MAC260 Problem Sheet 6: Solutions

Week 6 Lectures
Last updated March 22, 2024

1. Let E be the elliptic curve given by

$$y^2 = x^3 + 8.$$

   (a) Find a point of order 2 on E.

   Solution: We know that a point $(x, y) \in E$ has order 2 if any only if $y = 0$. An obvious such point on E is $P = (-2, 0)$.

   (b) Calculate the discriminant Δ of E, and hence find all primes p for which the curve $\overline{E}$ obtained by reducing E mod p is **not** an elliptic curve.

   Solution: We have $\Delta = -4a^3 - 27b^2 = -27 \cdot 8^2 = -3^3 \cdot 2^6$.

   For an odd prime p we have that $\overline{E}$ is not an elliptic curve if and only if $p \mid \Delta$. The only such odd prime is $p = 3$.

   (c) By reducing E mod p for sufficiently many primes, show that the torsion subgroup $T \subset E(\mathbb{Q})$ has only 2 elements.

   Solution: Here we use the Torsion Embedding Theorem, which says that if $\overline{E}$ is an elliptic curve, then T is isomorphic to a subgroup of $\overline{E}(\mathbb{F}_p)$.

   By the previous part, we can apply this with p equal to any odd prime other than 3. First try $p = 5$: then our equation becomes $y^2 = x^3 + 3$. We can find the points in $\overline{E}(\mathbb{F}_5)$ by plugging in the possible values of x in turn and checking whether we get any solutions for $y^2 = x^3 + 3$. Tabulating we find

x	0	1	2	3	4
$x^3 + 3$	3	4	1	0	2
y	$-$	± 2	± 1	0	$-$

   In the last row we used the list of squares in $\mathbb{F}_5$: they are $0^2 = 0,\ 1^2 = 4^2 = 1,\ 2^2 = 3^2 = 4$.

   So we get

$$\overline{E}(\mathbb{F}_5) = \{O, (1, \pm 2), (2, \pm 1), (3, 0)\}.$$

Hence we know that $|T| \mid |\overline{E}(\mathbb{F}_5)| = 6$.

We can try to repeat this process with $p = 7$ and $p = 11$. The sets of points we find are

$$\begin{aligned}
\overline{E}(\mathbb{F}_7) &= \{O, (0, \pm 1), (1, \pm 3), (2, \pm 3), (3, 0), (4, \pm 3), (5, 0), (6, 0)\}. \\
\overline{E}(\mathbb{F}_{11}) &= \{O, (1, \pm 3), (2, \pm 4), (5, \pm 1), (6, \pm 2), (8, \pm 6), (9, 0)\}.
\end{aligned}$$

In both cases we get $|\overline{E}(\mathbb{F}_p)| = 12$: since we already know that $|T| \mid 6$, this gives no new information.

So we move on to $p = 13$. Here the equation of $\overline{E}$ is just $y^2 = x^3 + 8$ and we need to look for points on this curve with coordinates in $\mathbb{F}_{13}$.

Before we start tabulating, it's useful to write down the squares in $\mathbb{F}_{13}$: these are

$$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4, 3^2 = 9,\ 4^2 = 3,\ 5^2 = 12,\ 6^2 = 10$$

and after this since $7 = -6,\ 8 = -5$ etc we don't get any new squares. So now we tabulate:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 + 8$	8	9	3	9	7	3	3	0	0	9	7	0	7
y	$-$	± 3	± 4	± 3	$-$	± 4	± 4	0	0	± 3	$-$	0	$-$

We get 15 points from the table above; together with the identity point O, this gives $|\overline{E}(\mathbb{F}_{13})| = 16$.

Putting our two results together we see that since $|T| \mid 6$ and $|T| \mid 16$ we must have $|T| \mid \gcd(6, 16) = 2$. On the other hand in Part (a) we saw that T contains at least one non-identity point, so $|T| \geq 2$. This gives $|T| = 2$ as required.

2. Use reduction modulo an appropriate prime to compute the torsion subgroup of the curve E given by

$$y^2 = x^3 - 39x + 70.$$

Solution: The first step is always to find and factor Δ. Here $\Delta = -4(-39)^3 - 27(70)^2 = 104976 = 2^4 \cdot 3^8$. So for any odd prime other than $p = 3$, we cam reduce E mod p and apply the torsion embedding theorem.

Reducing mod 5 we get the curve $\overline{E}$ defined by $y^2 = x^3 + x$. Now in $\mathbb{F}_5$ the cubic $x^3 + x$ factors completely:

$$x^3 + x = x^3 - 4x = x(x + 2)(x - 2)$$

So we get 3 points of order 2 in $\overline{E}(\mathbb{F}_5)$, namely $(-2,0)$, $(0,0)$, $(2,0)$. What about the other possible values of x? For $x=1$ we get $x^3+x=2$ and for $x=4$ we get $x^3+x=3$; neither 2 not 3 is a square in $\mathbb{F}_5$, so there are no more rational points.

So $\overline{E}(\mathbb{F}_5)$ is a group with 4 elements, each of order at most 2; hence it is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The Torsion Embedding Theorem tells us that T is therefore isomorphic to a subgroup of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. On the other hand, we can count the elements of order 2 in T: we get one such element $(x,0)$ for each integer root of $x^3-39x+70=0$. This cubic has one evident root $x=2$: factoring out $x-2$ we get the quadratic $x^2+2x-35=(x+7)(x-5)$. So in fact there are 3 integer roots, hence 3 elements of order 2 in T. Therefore T must be the whole grooup $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

3. Let E be the elliptic curve given by

$$y^2 = x^3 + 3x - 11.$$

(a) Calculate the order of the point $P=(3,5)$ on E.

Solution: Computing in the usual way we find

$$\begin{aligned} 2P &= (3,-5) \\ 3P &= O \end{aligned}$$

so P has order 3.

(b) Use reduction mod 7 and 17 to compute the torsion subgroup $T \subset E(\mathbb{Q})$. **Solution:** Note that $\Delta = -3375 = -3^3 \cdot 5^3$ so the reductions mod 7 and 17 are indeed elliptic curves.

Reducing mod 7 we get $\overline{E}$ given by $y^2 = x^3 + 3x - 4$. By the same process as in the previous questions we find

$$\overline{E}(\mathbb{F}_7) = \{O, (1,0), (3,\pm 2), (4,\pm 3)\}$$

and so we know $|T| \mid 6$.

Reducing mod 17 we get $\overline{E}$ given by $y^2 = x^3 + 3x + 6$ and tabulating as before, we find (after lots of calculating!)

$$\begin{aligned} \overline{E}(\mathbb{F}_{17}) = \{&O, (3,\pm 5), (6,\pm 6), (7,\pm 8), (8,\pm 7), (10,\pm 4), (12,\pm 6), (13,\pm 7), \\ &(14,\pm 2), (15,\pm 3), (16,\pm 6)\} \end{aligned}$$

and so we know $|T| \mid 21$.

Putting our two results together we get that $|T| \mid \gcd(6,21) = 3$. On the other hand in Part (a) we found the point P of order 3 in T. Hence we must have $|T| = \langle P \rangle \cong \mathbb{Z}_3$.

4. *(Non-examinable)* Show that if K is an algebraically closed field of characteristic 2, for any short Weierstrass equation

$$f(x, y) = y^2 - x^3 - ax - b$$

there is a point $(x, y) \in K^2$ where

$$f(x, y) = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

Solution: The key point here is that, since we are in characteristic 2, we have $\frac{\partial f}{\partial y} = 2y = 0$ at **every** point (x, y).

Now $\frac{\partial f}{\partial x} = 3x^2 + a = x^2 + a$. Choose a root x_0 of this quadratic (we know it has a root since our field is algebraically closed). Then choose y_0 to be a root of the quadratic $y^2 - x_0^3 - ax_0 - b$ (again, such a y_0 exists because K is algebraically closed). Then we have

$$f(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0.$$

The moral of this story is that equations in Weierstrass form are inappropriate for dealing with elliptic curves in characteristic 2, and one must use a more general form. This is why we simply ignored the prime 2 in our discussion of reduction mod p.