23MAC260 Problem Sheet 5: Solutions

Week 5 Lectures

Last updated March 15, 2024

Throughout these solutions, we will use the terminology "point of finite order" and "torsion point" interchangeably.

1. For each of the following curves, calculate the torsion subgroup $T \subset E(\mathbb{Q})$:

   (a) $y^2 = x^3 - 27$.

   Solution: The Integrality and Nagell–Lutz Theorems says that a torsion point must have integer coordinates (x, y) where $y = 0$ or $y^2 \mid \Delta$.

   Here setting $y = 0$ we get $x^3 - 27 = 0$ which has the integer solution $x = 3$. So we get one point $P = (3, 0)$. Since $y = 0$ we know that $2P = O$, so we know this is really a torsion point.

   If $y \neq 0$ we must have $y^2 \mid \Delta = -27 \cdot 27^2 = 3^9$, so we have $|y| \in \{1, 3, 9, 27, 81\}$. We can tabulate the possibilities as follows:

$\lvert y\rvert$	1	3	9	27	81
$x^3 = y^2 + 27$	28	36	108	756	6588
x	–	–	–	–	–

   In the last row we can see that there were no solutions for x in any case for example by listing the cubes of the integers:

   $$-1, 0, 1, 8, 27, 64, 125, 216, 343, 512, 721, 1000, 1331, 1728,$$
   $$2197, 2744, 3375, 4096, 4913, 5832, 6859 \ldots$$

   Since $x \mapsto x^3$ is monotonic increasing, no value of x^3 outside the given range will match one in the table.

   So the only torsion point other than the idenrtity O is $P = (3, 0)$. Hence

   $$T = \{O, P\} \cong \mathbb{Z}_2.$$

   (b) $y^2 = x^3 + 4x$.

Solution: In this case if $y = 0$ we have $x^3 + 4x = x(x^2 + 4) = 0$; clearly the only solution is $x = 0$. What about $y \neq 0$?

Here $\Delta = -4 \cdot 4^3 = -4^4 = -2^8$. So if $y^2 \mid \Delta$ then $|y| \in \{1, 2, 4, 8, 16\}$.

In this case since our equation has a linear term in x, we can't solve for x^3 purely in terms of y. So we will just put y^2 in the second row of our table:

$\lvert y \rvert$	1	2	4	8	16
$x(x^2+4) = y^2$	1	4	16	64	256
x	$-$	$-$	2	$-$	$-$

To fill in the last row, we need to decide if a given entry in the row above is of the form $x(x^2+4)$ for some integer x. To do this, for example we can note that $x(x^2+4)$ has the same sign as x, so any solution must be positive; moreover $x(x^2 + 4) > x^3$ for positive x, so for a given y^2 we need only look as far as $\sqrt[3]{y^2}$ for solutions. For example, if x satisfies $x(x^2 + 4) = 256$ then x is at most $\sqrt[3]{256} \approx 6.34$, and we can easily check that $x = 1, 2, \ldots, 6$ don't solve the equation.

So the points we found are $(0, 0)$, $(2, \pm 4)$. As always, we need to check whether these candidate torsion points are in fact torsion points, which we now do.

For the point $(0, 0)$ this is easy: any point on E with y-coordinate equal to 0 is a point of order 2, and therefore it is in T.

For the points $(2, \pm 4)$ we have to do a bit of work. Let $P = (2, 4)$. Using the formula from Week 3 we compute

$$\begin{aligned} x(2P) &= \left(\frac{3x^2+4}{2y}\right)^2 |_P - 2x(P) \\ &= 0 \end{aligned}$$

and then using the curve equation $y^2 = x^3 + 4x$ we find that $y(2P) = 0$ also. So $2P = (0, 0)$, and therefore $4P = O$. So P is a point of order 4, and hence $-P$ is a point of order 4 also.

So we get

$$T = \{O, (0, 0), (2, \pm 4)\}.$$

Thiis is a group with 4 elements, so there are two possible isomorphism classes: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. To decide which one our group T actually is, we look at the number of points with order > 2. We see that T contains 2 points (different from O) whose y-coordinate is nonzero. Such a point has order > 2. Of the two possibilities above, only $\mathbb{Z}_4$ has points of order > 2, so we conclude that

$$T \cong \mathbb{Z}_4.$$

(c) $y^2 = x^3 - 16x + 16$.

Solution: Again, Integrality and Nagell–Lutz say that a torsion point other than O must have integer coordinates (x, y) with $y = 0$ or $y^2 \mid \Delta$. Here $\Delta = -4 \cdot (-16)^3 - 27(16)^2 = 16^2 \cdot (64 - 27) = 16^2 \cdot 37$. So a torsion point must have $y = 0$ or $|y| \in \{1, 2, 4, 8, 16\}$. We will deal with both cases directly by tabulating. Our table looks like

$\lvert y\rvert$	0	1	2	4	8	16	
y^2	0	1	4	16	64	256	
x							

and again we need to decide how to fill in the last row.

Denote the cubic $x^3 - 16x + 16$ by $f(x)$. Then $\frac{df}{dx} = 3x^2 - 16$. So the stationary points of f are at $x = \pm\sqrt{16/3}$, hence f is monotic increasing for $|x| \geq \sqrt{16/3} \geq 2$. We will use this to bound the range of values of x we need to consider.

Now $f(-5) = -29 < 0$, so the monotonic property tells us that $f(x) < 0$ for $x \leq -5$. So when $x \leq -5$, the value of $f(x)$ cannot equal y^2 for any y.

We also compute $f(8) = 400$, so again by the monotic property that $f(x) \geq 400$ for $x \geq 8$. So for $x \geq 8$ the value of $f(x)$ cannot equal one of the y^2 values in the table above.

So we can restrict our attention to $-4 \leq x \leq 7$. For integers x in this range we calculate the values of $f(x)$ to be

$$16,\ 37,\ 40,\ 31,\ 16,\ 1,\ -8,\ -5,\ 16,\ 61,\ 136,\ 247$$

The squares in this sequence are $16 = (\pm4)^2 = f(-4) = f(0) = f(4)$ and $1 = (\pm1)^2 = f(1)$. So, along with the identity O, we get candidate torsion points

$$\begin{aligned} \pm P_1 &= (0, \pm4) \\ \pm P_2 &= (-4, \pm4) \\ \pm P_3 &= (4, \pm4) \\ \pm P_4 &= (1, \pm1). \end{aligned}$$

We have to decide which (if any) of these are actual torsion points. We start with P_1. We will compute multiples of the point $2P_1$ using the addition formulas from Week 3. We find

$$\begin{aligned} 2P_1 &= (4, 4) = P_3 \\ 3P_1 &= (-4, -4) = -P_2 \\ 4P_1 &= (8, -20) \end{aligned}$$

At this point we can stop: the y-coordinate of $4P_1$ is does not satisfy the Nagell–Lutz criterion $y^2 \mid \Delta$, so we can conclude that $4P_1$ is not a torsion point, and hence P_1 is not a torsion point.

However, we have shown more: since P_1 is not a torsion point, no multiple of P_1 can be a torsion point either. So our computations above show that $-P_1$, $\pm P_2, \pm P_3$ are not torsion points either.

Finally we must decide if $\pm P_4$ are torsion points. Again using the addition formulas from Week 4 we find

$$x(2P_4) = \frac{161}{4} \notin \mathbb{Z}.$$

The Integrality Theorem tells us that $2P_4$ is not a torsion point, hence the points $\pm P_4$ are not torsion points either.

So finally we have shown that the only torsion point in $E(\mathbb{Q})$ is the identity:

$$T = \{O\}.$$

2. Prove (as stated in the Week 4 lectures) that the torsion subgroup T of the curve defined by

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

is the trivial group $T = \{O\}$.

Solution: Integrality and Nagell–Lutz say that a torsion point other than O must have coordinates (x, y) with $y = 0$ or $y^2 \mid \Delta$.

If $y = 0$, the equation $x^3 + 2 = 0$ has no integral solutions, so we do not get any torsion point in this case.

Computing we find $\Delta = -27 \cdot 2^2 = -2^2 \cdot 3^3$, so the condition $y^2 \mid \Delta$ gives us the cases $|y| = 1, 2, 3, 6$. Tabulating we get

$\lvert y\rvert$	1	2	3	6
$x^3 = y^2 - 2$	-1	2	7	34
x	-1	–	–	–

In this case we can see directly that the only entry in the second row which is the cube of an integer is -1. So we get candidate torsion points

$$P = (-1, \pm 1)$$

and we must decide if they are actual torsion points.

Computing $2P$ using the formulas from Week 3, we compute

$$x(2P) = \frac{17}{4} \notin \mathbb{Z}.$$

The Integrality Theorem implies that $2P$ is not a torsion point, and hence neither are $\pm P$.

So the only torsion point in $E(\mathbb{Q})$ is the identity O: that is

$$T = \{O\}$$

as claimed.

3. What is the torsion subgroup $T \subset E(\mathbb{Q})$ for the following curve?

$$y^2 = x^3 - \frac{15}{16}x + \frac{11}{32}.$$

Solution: Here we don't have an integral equation, so neither the Integrality Theorem nor Nagell-Lutz can be applied directly.

First we have to find an integral model of our curve. To do this we need to find μ such that $\mu^4 \cdot \frac{15}{16}$ and $\mu^6 \cdot \frac{11}{32}$ are integers. The obvious choice is $\mu = 2$: multiplying our x-coefficient by 2^4 and our y-coefficient by 2^6 gives the integral model

$$y^2 = x^3 - 15x + 22.$$

Now we can use Nagell-Lutz. Putting $y = 0$ we get the equation $x^3 - 15x + 22 = 0$. This has a root $x = 2$; factoring out $x - 2$ we get $x^3 - 15x + 22 = (x-2)(x^2 + 2x - 11)$ and the quadratic has no integer roots. So the only integer point with $y = 0$ is $Q = (2, 0)$. Note that since the y-coordinate equals 0, we have $2Q = 0$, so this is an actual torsion point.

To find points with $y \neq 0$, we compute $\Delta = 432 = 2^4 3^3$ so the possibilities for $|y|$ are $2^a 3^b$ where $a \in \{0, 1, 2\}$, $b \in \{0, 1\}$. Tabulating as before we get

$\lvert y \rvert$	1	2	3	4	6	12
y^2	1	4	9	16	36	144
x						

To decide whether a given y^2 equals $x^3 - 15x + 22$ for some integer x we can argue as before. If $f(x) = x^3 - 15x + 22$ then $\frac{df}{dx} = 3x^2 - 15$. So f is monotonic increaing for $x^2 \geq 5$, that is for $|x| \geq \sqrt{5}$.

Now $f(-5) < 0$, so the monotonic property tells us that $f(x) < 0$ for $x \leq -5$. So when $x \leq -5$ the value of $f(x)$ cannot equal y^2 for any y.

Also $f(6) = 148 > 144$, and again the monotonic property says that $f(x) > 144$ for all $x \geq 6$. So for $x \geq 6$ the value of $f(x)$ cannot equal one of the y^2 values in the table above.

So we can restrict our attention to $-4 \leq x \leq 5$. For integer x in this range we calculate the values of $f(x)$ to be:

$$18, 40, 44, 36, 22, 8, 0, 4, 26, 72$$

The only squares in this sequence are $36 = 6^2 = f(-1)$ and $4 = 2^2 = f(3)$. So we get candidate torsion points

$$\pm P_1 = (-1, \pm 6)$$
$$\pm P_2 = (3, \pm 2).$$

Again we must decide which of them are actually torsion points.

Computing multiples of P_1 as in Week 3 shows that

$$\begin{aligned} 2P_1 &= (3, -2) = -P_2 \\ 3P_1 = 2P_1 \oplus P_1 &= (2, 0) = Q. \end{aligned}$$

Hence $6P_1 = 2Q = O$, so P_1 has order 6. We have seen that all the candidate points are multiples of P_1, and hence are in the torsion subgroup T: in other words

$$\begin{aligned} T &= \langle P_1 \rangle = \{O, (2, 0), (-1, \pm 6), (3, \pm 2)\} \\ &\cong \mathbb{Z}_6 \end{aligned}$$

where the last isomorphism comes from the fact (proved for example in the Geometry and Groups module) that any cyclic group with n elements is isomorphic to $\mathbb{Z}_n$.