Problem class 7

1. Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 - 16\,x + 16$. Use the reductions at $p = 3$ and $p = 5$ to prove that $E(\mathbb{Q})_{\text{tors}}$ is trivial. Then show that $E(\mathbb{Q})$ is infinite.

Solution: The discriminant of E is 151552 which is neither divisible by 3 nor by 5. So we have good reduction at these primes. For $p = 3$, we find the solutions are:

$$\tilde{E}(\mathbb{F}_3) = \Big\{O,\ (0:1:1),\ (0:2:1),\ (1:1:1),\ (1:2:1),\ (2:1:1),\ (2:2:1)\Big\}$$

and for $p = 5$, we find

$$\tilde{E}(\mathbb{F}_5) = \Big\{O,\ (0:1:1),\ (0:4:1),\ (1:1:1),\\ (1:4:1),\ (3:0:1),\ (4:1:1),\ (4:4:1)\Big\}.$$

Now the group $E(\mathbb{Q})_{\text{tors}}$ injects into $\tilde{E}(\mathbb{F}_5)$ which is a cyclic group of order 7. Therefore the order of $E(\mathbb{Q})_{\text{tors}}$ divides 7. But it also divides $\#\tilde{E}(\mathbb{F}_5) = 8$. Therefore $E(\mathbb{Q})_{\text{tors}}$ is trivial.

It is not hard to spot that $P = (0, 4)$ is a point in $E(\mathbb{Q})$. Since we have shown that there are no points of finite order in $E(\mathbb{Q})$, we conclude that P has infinite order. Therefore $E(\mathbb{Q})$ contains nP for all $n \in \mathbb{Z}$.

(In fact $E(\mathbb{Q})$ is equal to $\mathbb{Z}\,P$.)

2. Show that the torsion subgroup of $E(\mathbb{Q})$ for $E : y^2 = x^3 - 11\,x - 5$ is trivial.

Solution: We count the number of solutions modulo $p = 3$, $p = 5$ and $p = 7$ for which E has good reduction in each case. We find that $\#\tilde{E}(\mathbb{F}_3)$ has 4 elements. Next $\#\tilde{E}(\mathbb{F}_5)$ has 8 elements (as already determined in the notes.) Finally $\#\tilde{E}(\mathbb{F}_7)$ has 9 points. Since 9 and 4 are coprime, we conclude that $E(\mathbb{Q})_{\text{tors}}$ is trivial.

3. Determine $E(\mathbb{Q})_{\text{tors}}$ for the curve $E : y^2 = x^3 - 5005$.

Solution: The discriminant of E is $-16 \cdot 27 \cdot 5005^2$ which factors as $-2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$. The smallest prime of good reduction is $p = 17$, so we better try to use Lutz-Nagell rather than reduction. (In fact modulo 17 there are 18 points and the first order coprime to this is for $p = 31$ where there are 43 points. So this would take a while with this method.)

First there are no points with $y = 0$ as 5005 is not a cube. Hence Lutz-Nagell tells us that y must divide $D = 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$. Suppose first that $y \in \mathbb{Z}$ is divisible

by one of the primes $p \in \{5, 7, 11, 13\}$. Then $x^3 = y^2 + 5005$ has to be divisible by p, too. However p^2 divides x^3 and y^2, yet it does not divide 5005. We conclude that y must divide 27.

For $y = 1$, 3, 9 and 27, we get the equation $x^3 = 5006$, $x^3 = 50032$, $x^3 = 5734$ and $x^3 = 24688$ respectively. But none of these numbers is a cube.

Therefore $E(\mathbb{Q})_{\text{tors}} = \{O\}$.

4. Let B be a square-free integer with $B \neq \pm 1$. Consider the curve $E : y^2 = x^3 + B$.

   (a) Show that $E(\mathbb{Q})$ does not contain a 2-torsion point.

   Solution: If $P = (x_P, y_P)$ is 2-torsion then $y_P = 0$. Then $x_P^3 = -B$ can only be square-free if $B = \pm 1$, but that was excluded.

   (b) Let $P = (x_P, y_P)$ be a torsion point in $E(\mathbb{Q})$. Using Lutz-Nagell show that y_P divides 27.

   Solution: We excluded $y_P = 0$, so Lutz-Nagell says that y_P divides $D = 27B^2$. Now if a prime $p \neq 3$ divides y_P then $p \mid B^2$, so $p \mid B$. Then $p \mid x_P^3 = y_P^2 - B$ so $p \mid x_P$. Therefore $p^2 \mid y_P^2 - x_P^3 = B$ but that contradicts that B is square-free. So y_P divides 27.

   (c) $(*)$ Let p be a prime dividing B. Suppose $p \neq 3$. Use the reduction modulo p to show that $pP = O$ for all torsion points $P \in E(\mathbb{Q})$.

   Solution: By the previous part we know that y_P is a power of 3. Hence it is coprime to p. Because $x_P^3 \equiv y_P^2 \pmod{p}$ also x_P is not divisible by p. We conclude that the reduced point $\tilde{P}$ in $\tilde{E}(\mathbb{F}_p)$ is not the singular point $(0 : 0 : 1)$. We have seen that the group of non-singular points is isomorphic to $(\mathbb{F}_p, +)$; hence $p\tilde{P} = \tilde{O}$. Therefore pP belongs to E_1 for the prime p. This implies $pP = O$ as O is the only torsion point in E_1.

   (d) Show that $\tilde{E}(\mathbb{F}_5)$ is cyclic of order 6 if $5 \nmid B$.

   Solution: If $5 \nmid B$, the reduction is an elliptic curve. The map $x \mapsto x^3$ is a bijection in $\mathbb{F}_5$ because

x	0	1	2	3	4
x^3	0	1	3	2	4

   Therefore when solving $y^2 = x^3 + B$ for various x, we will always encounter each equation $y^2 = z$ for each $z \in \mathbb{F}_5$ exactly once whatever the value of B. For instance for $B = 1$, we will have

   $$\tilde{E}(\mathbb{F}_5) = \Big\{O,\ (0,1),\ (0,4),\ (2,2),\ (2,3),\ (4,0)\Big\}$$

   We always have six solutions and hence the group is cyclic.

   (e) Conclude that $E(\mathbb{Q})$ has no non-zero torsion points.

Solution: If B has more than one prime divisor different from 3, say p_1 and p_2, then the third part implies that all torsion points have order p_1 and also order p_2. Hence in that case $E(\mathbb{Q})$ has only O as a torsion point.

We are left with all numbers B that are either a prime p or $3p$ for some prime p. We also know that the order of $E(\mathbb{Q})_{\text{tors}}$ is a divisor of p. If $p \neq 5$, the previous part implies that p must also divide 6. This is impossible except for $p = 3$ as we already know that there is no 2-torsion.

We are left with $B = 3$, $B = 5$ and $B = 15$. For $B = 3$: The curve has good reduction at $\ell = 7$ and there are 13 points. There cannot be any point of order 3 in $E(\mathbb{Q})$. For $B = 5$: The curve has good reduction at $\ell = 7$ and there are 7 points in the reduction so the curve cannot contain any 5-torsion points. For $B = 15$: The only possibility for the order of a torsion point is again 5, but the reduction at 7 has 12 points.

Here a list of elliptic curves showing that all possible abelian groups in Mazur's theorem can occur as torsion subgroups of $E(\mathbb{Q})$:

Curve A, B	$E(\mathbb{Q})_{\text{tors}}$
-1, 1	O
1, 0	$\mathbb{Z}/2\mathbb{Z}$
0, 4	$\mathbb{Z}/3\mathbb{Z}$
-2, 1	$\mathbb{Z}/4\mathbb{Z}$
-1, 0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
-432, 8208	$\mathbb{Z}/5\mathbb{Z}$
0, 1	$\mathbb{Z}/6\mathbb{Z}$
-3483, 121014	$\mathbb{Z}/7\mathbb{Z}$
-5211, 319734	$\mathbb{Z}/8\mathbb{Z}$
-5211, -31050	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
-17739, 1205766	$\mathbb{Z}/9\mathbb{Z}$
-58347, 3954150	$\mathbb{Z}/10\mathbb{Z}$
-157707, 78888006	$\mathbb{Z}/12\mathbb{Z}$
-24003, 1296702	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
-1386747, 368636886	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$