Week 7 Problem Class: Problem Sheet 6

1 (a) Find a point of order 2 in $E(\mathbb{Q})$.

Solution: Order 2 $\iff$ $y=0$

So $(-2,0) \in E(\mathbb{Q})$

is a point of order 2.

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

$a=0, \; b=8$

$\therefore \Delta = -27 \cdot 8^2 = -2^6 \cdot 3^3$

For an odd prime p,
Reduction of E mod p not elliptic

$\iff p \mid \Delta \iff p=3.$

(c) Show T has 2 elements.

Know from (a) that $|T| \geq 2$.

So we need to show $|T| \leq 2$.

From part (b), if p is any odd prime $\neq 3$ then

$$|T| \text{ divides } |\overline{E}(\mathbb{F}_p)|$$

$(\overline{E} = E \bmod p)$.

- $p = 5$: $\overline{E}$ is defined by

$$\overline{E}: \quad y^2 = x^3 + 3$$

Make a table to find solution in $\mathbb{F}_5$:

x	0	1	2	3	4
x^3+3	3	4	1	0	2
y	–	± 2	± 1	0	–

$0^2 = 0$
$1^2 = 4^2 = 1$
$2^2 = 3^2 = 4$

include point at infinity $\mathcal{O}$!

So $|\overline{E}(\mathbb{F}_5)| = 6$

So $|T|$ divides 6. (by Torsion Embedding Theorem)

- Can repeat with $p=7$ and $p=11$.

Find in both cases

$$|\overline{E}(\mathbb{F}_p)| = 12.$$

$\therefore$ Torsion Embedding Theorem $\Rightarrow$ $|T|$ divides 12.

- Reduce mod 13:

$\overline{E}$ is defined $y^2 = x^3 + 8$.

Table of points:

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	-

Squares in $\mathbb{F}_{13}$: $0^2 = 0$, $1^2 = 12^2 = 1$,

$2^2 = 11^2 = 4$, $3^2 = 10^2 = 9$, $4^2 = 9^2 = 3$,

$5^2 = 8^2 = 12$, $6^2 = 7^2 = 10$

The 15 solutions from the table above, together with $\mathcal{O}$, give

$$|\overline{E}(\mathbb{F}_{13})| = 16.$$

So $|T|$ divides 16.

Putting things together $|T|$ divides $\gcd(6, 16) = 2$

$\therefore |T| \leq 2$

from earlier

$\therefore |T| = 2$ $\square$.

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

First step: $\Delta = -4(-39)^3 - 27(70)^2$

$= 104976$

$= 2^4 \cdot 3^8$

So we can apply Torsion Embedding Thm with any prime $p \geq 5$.

- Reduce mod 5:

$\bar{E}: y^2 = x^3 + x$

Make a table to find points on this curve

x	0	1	2	3	4
x^3+x	0	2	0	0	3
y	0	–	0	0	–

So $|\overline{E}(\mathbb{F}_5)| = 4$

$\therefore$ by Torsion Embedding Theorem $|T|$ divides 4.

We found

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

Each non-identity element has $y = 0$

$\therefore$ order 2.

So $\overline{E}(\mathbb{F}_5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Torsion Embedding Theorem says T is a subgroup of $\overline{E}(\mathbb{F}_5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\therefore$ every non-identity element of T must have order 2. These are easy to find: a point $(x,y) \in T$ of order 2 must have $y = 0$ and $x \in \mathbb{Z}$.

So we need to find the integer solutions of $x^3 - 39x + 70 = 0$.

By inspection we see that $x=2$ is a solution: factoring out $x-2$ we get $x^3 - 39x + 70 = (x-2)(x^2+2x-35)$

$$= (x-2)(x-5)(x+7).$$

So $(2,0)$, $(5,0)$, $(-7,0)$ are all points of order 2 in T.

$$\therefore T = \{O, (-7,0), (2,0), (5,0)\}$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$