Amin Zolfagharian - 610002072

Problem 1.

(i) The point $(0, 1)$ always is on the curve, then we have to find the singular points on this curve (If there exists any). Let $F : y^2 = x^3 + x + 1$, if F has a singular point $P = (x, y)$:

$$\frac{\partial F}{\partial x} = 3x^2 + 1 = 0 \qquad \frac{\partial F}{\partial y} = 2y = 0 \qquad \frac{\partial F}{\partial z} = 3z^2 + 2zx - y^2 = 0$$

Then $y = 0$ and $3x^2 = -1$:

$$0 = x^3 + x + 1$$
$$\implies 0 = 3x^3 + 3x + 3 = (-1)x + 3x + 3 \implies x = -\frac{3}{2}$$

Meaning $3(-\frac{3}{2})^2 + 1 \overset{p}{\equiv} 0$, since p is odd:

$$p \mid 3(-\frac{3}{2})^2 + 1 = \frac{27}{4} + 1$$
$$\implies p \mid 27 + 4 = 31$$

Also we have:

$$\frac{\partial F}{\partial z} = 3z^2 + 2zx - y^2 = 3 + 2(-\frac{3}{2}) - 0 = 0$$

Then if P is a singular point, we must be in $\mathbb{F}_{31}$, and for any other p, this is an elliptic curve over $\mathbb{F}_p$. Notice that $p = 3$ is obviously fine since $3x^2 + 1$ can not be 0 in $\mathbb{F}_3$, thus multiplying by 3 is permitted.

(ii) First we find it for $\mathbb{F}_3$:
The points are:

$$(0, 1), (1, 0), (2, 0), \mathcal{O}$$

And since we have two points of order 2 and $(0, 1)$ is not of order 2, then the the group is $\mathbb{Z}/4\mathbb{Z}$.
For $\mathbb{F}_5$:
The points are:

$$(0, \pm 1), (2, \pm 1), (-2, \pm 1), (-1, \pm 2), \mathcal{O}$$

Which are 9 points, we only need to show that there exists one point that doesn't have order 3, which for which we prove that (0, 1) is that point...

Problem 2.

For any $x \in \mathbb{F}_p$, we have $1 + \left(\dfrac{f(x)}{p}\right)$ number of points with x. Since if $f(x)$ is a quadratic residue modules p, then $\left(\dfrac{f(x)}{p}\right) = 1$, and we must have two answers, which we have, since if y is an answer, then $-y$ is also an answer. Now if $f(x) = 0$, then $\left(\dfrac{f(x)}{p}\right) = 0$, giving us the point $(x, 0)$, since $0 = -0$. And if $f(x)$ is not quadratic residue, then there is no point on this curve with such x. We also have $\mathcal{O}$, which we didnt count:

$$|E(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} (1 + \left(\frac{f(x)}{p}\right)) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$$

Problem 3.

Problem 4.

(l) $y^2 = x^3 - 4x$. By Nagell-Lutz Theorem we know that if P is of finite order, either $2P = \mathcal{O}$, which gives us:

$$y = 0, 0 = x^3 - 4x \implies (0,0), (\pm 2, 0)$$

or we have $y^2 \mid \Delta$. Now since $5 \nmid 2\Delta = 2^9$, we have a good reduction modules 5. We get the $\varphi : E(\mathbb{Q}) \to E(\mathbb{F}_5)$:

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

Which has the points:

$$(0,0), (\pm 2, 0), \mathcal{O}$$

Then that's all of the tortion points on this curve, and since all of the elements have order 2, then the resulting group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(m) $y^2 + xy - 5y = x^3 - 5x^2$, First we convert it to a shorter form with substitution $y = y - \frac{1}{2}(x - 5)$:

$$y^2 = x^3 - \frac{19}{4}x^2 - \frac{5}{2}x + \frac{25}{4}$$

Now with another substitution $x = x + \frac{19}{12}$:

$$E : y^2 = x^3 - \frac{481}{48}x - \frac{4879}{864}$$

Now using $\mu = 6$, we get the ismorphic curve $E' : y^2 = x^3 - 12987x - 263466$. Now if we use $\varphi : E'(\mathbb{Q}) \to E'(\mathbb{F}_7)$, since 7 doesn't divide the discriminant; the tortion points are mapped in a 1-1 manner, and we can find them in $E'(\mathbb{F}_7)$. The transitioned form of the equation is:

$$E' : y^2 = x^3 - 2x$$

Which has the points:

$$(0,0), (3,0), (4,0), (-1,\pm 1), (2,\pm 2), \mathcal{O}$$

Which are 8 points, having exactly 3 elements of order 2, meaning that these points are the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and the gruop of tortion points are a subgroup of this group. Now since $(-102,0), (-21,0), (123,0)$ are all the points of order 2 in E', Then the group of tortion points is at least $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now if there is any other tortion point, on this curve, the group would be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and if not it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 5.

(i) Since if $\mu \in \mathbb{Q}$, then $E \cong E'$ if $E : y^2 = x^3 + b$ and $E' : y^2 = x^3 + \mu^6 b$. Then we can strip b out of any a^6 in it.

(ii)

(iii)