Amin Zolfagharian - 610002072

Problem 1.

(i) Suppose P is a not an inflation point on the curve E. This means that the tangent line to E on P meets the curve in a third point Q where $Q \neq P$. Now again if we draw the tangent line to E on Q, if it meets the curve in Q 3 times, it means that Q is an inflation point and this case was solved in class. So assume that Q also is not an inflation point, which means that the tangent line on Q meets, the curve in a third point R, where $R \neq Q$ and $R \neq P$. Now consider the matrix:

$$M_\alpha = \begin{bmatrix} P_x & Q_x & R_x \\ P_y & Q_y & R_y \\ P_z & Q_z & R_z \end{bmatrix}$$

Since these three points are not on the same line, then they are linearly independent. This means that $\det(M_\alpha) \neq 0$. Then suppose $\alpha = M_\alpha^{-1}$. Now it is easy to see that α maps P and Q and R respectively to $[1;0;0]$, $[0;1;0]$ and $[0;0;1]$. Suppose that E after transformation with M_α has the form:

$$\begin{aligned} G(u,v,w) = ku^3 + lu^2v + muv^2 + nv^3 + pu^2w + quvw \\ + rv^2w + suw^2 + tvw^2 + fw^3 = 0 \end{aligned}$$

Now since $G(1,0,0) = G(0,1,0) = G(0,0,1) = 0$, then we have $k = n = f = 0$. Now the line tangent to P and passing through Q is now the line that is tangent to $[1;0;0]$ and passing through $[0;1;0]$. It is easy to see that this line is $W = 0$. Now conisder intersections of this line and G:

$$\begin{aligned} G(u,v,0) &= lu^2v + muv^2 = 0 \\ &= uv(lu + mv) = 0 \end{aligned}$$

Now note that uv has roots $[1;0;0]$ and $[0;1;0]$. The third root is also $[1;0;0]$. Therefore $lu + mv$ has root $[1;0;0]$:

$$l \cdot 1 + 0 = 0 \implies l = 0$$

Also since $[0;1;0]$ is not its root, then :

$$l \cdot 0 + m \cdot 1 \neq 0 \implies m \neq 0$$

Also the tangent line to Q which goes through R is now transformed to line tangent to $[0;1;0]$ and goes through $[0;0;1]$. It is not hard to see that this line is $U = 0$. Now if we see the intersections of this line with the curve, we get three points, $[0;1;0]$ two times, and $[0;0;1]$ one time. This means that $[0;1;0]$ is root of the below equation 2 times, and $[0;0;1]$ is the root of it one time:

$$\begin{aligned} G(0,v,w) &= rv^2w + tvw^2 = 0 \\ &= vw(rv + tw) = 0 \end{aligned}$$

Now vw has roots $[0;1;0]$ and $[0;0;1]$, thus $[0;1;0]$ is root of $rv+tw$, and $[0;0;1]$ is not, we have:

$$r \cdot 1 + t \cdot 0 = 0 \implies r = 0$$
$$r \cdot 0 + t \cdot 1 \neq 0 \implies t \neq 0$$

This gives us the form:

$$G(u,v,w) = muv^2 + pu^2w + quvw + suw^2 + tvw^2 = 0$$

Now here if we do the substitution $(u,v,w) \to (K^2, LN, KN)$, we have:

$$mK^2L^2N^2 + pk^5N + qk^3LN^2 + sK^4N^2 + tK^2LN^3 = 0$$

And here dividing by K^2N, we get:

$$mL^2N + pK^3 + qKLN + sK^2N + tLN^2 = 0$$
$$mL^2N + qKLN + tLN^2 = -pK^3 - sK^2N$$

Dehomogenizing in L we get:

$$mL^2 + (qK+t)L = -pK^3 - sK^2$$

Now replace L with $(L - \frac{1}{2}(qK+t))$ we get:

$$L^2 = \text{cubic in } K.$$

The cubic in K might not have leading coefficient 1, but we can adjust that by replacing K and L by λK and $\lambda^2 L$, where λ is the leading coefficient of the cubic. So we do finally get an equation in Weierstrass form.

(ii)

Problem 2.

$C(x,y,z)$ is a projective curve of degree 3:

$$ax^3 + bx^2y + cx^2z + dxy^2 + exz^2 + fy^3 + gy^2z + hyz^2 + iz^3 + jxyz = 0$$

First note that $\mathcal{O}$ is on the curve, then $C(0,1,0) = fy^3 = 0$. Thus $f = 0$. Since the line $z = 0$ intersects with the curve 3 times in $\mathcal{O}$, then:

$$C(x,y,0) = ax^3 + bx^2y + dxy^2 = x(ax^2 + bxy + dy^2) = 0$$

has the root $[0;1;0]$, 3 times. x has one root $[0;1;0]$. Now since $[0;1;0]$ is the root of $ax^2 + bxy + dy^2$, then we have: $d(1)^2 = 0$, which suggests that $d = 0$.

$$C(x,y,0) = ax^3 + bx^2y = x^2(ax+by) = 0$$

Since x^2 has two roots, then $ax+by$ has one root, $[0;1;0]$. This means that $b(1)=0$ and $b=0$. Rewriting $C(x,y,z)$ we have:

$$C(x,y,z) = ax^3 + cx^2z + exz^2 + gy^2z + hyz^2 + iz^3 + jxyz = 0$$

Dividing by g and then replacing x with $x/\sqrt[3]{a}$ we get:

$$y^2z + h'yz^2 + j'xyz = x^3 + c'x^2z + e'xz^2 + i'z^3$$

Which is in Weierstrass form. Note that since $\mathbb{C}$ is algebraicly closed, then $\sqrt[3]{a}$ is also in $\mathbb{C}$, and transformations are all valid.

Problem 3.

First we have to show that the curve is smooth. We Homogenize the equation:

$$y^2z + xyz - x^3 - z^3 = 0$$

Then we calculate all partial derivatives:

$$\frac{\partial F}{\partial x} = -3x^2 + yz \qquad \frac{\partial F}{\partial y} = 2yz + xz \qquad \frac{\partial F}{\partial z} = -3z^2 + y^2 + xy$$

Since we want to find the answers in $\mathbb{F}_2$, then we have:

$$\frac{\partial F}{\partial x} = x^2 + yz \qquad \frac{\partial F}{\partial y} = yz + xz \qquad \frac{\partial F}{\partial z} = z^2 + y^2 + xy$$

If a point is singular, then it vanishes in all three derivatives:

$$\left.\begin{aligned} x^2 + yz = 0 \\ yz + xz = 0 \end{aligned}\right\} \implies x^2 - xz = 0 \implies x(x-z) = 0$$

Then we have two cases:

a) $x = 0$
Then since $x^2 + yz = 0$, we get $yz = 0$. Now either $y = 0$ or $z = 0$, WLOG suppose that $y = 0$. Then since $z^2 + y^2 + xy = 0$, we have $z^2 = 0$ and $z = 0$, but this point (0, 0, 0) is not on the plane.

b) $x = 1, x = z$
In this case note that $x^2 + yz = 0$, then $1 + y = 0$, which means that $y = 1$. But then we have $z^2 + y^2 + xy = 1$, and therefore this point is non-singular. Thus all points on this curve are non-singular and the curve is smooth. Also since the point $(1,1,1)$ is on the curve, then this curve is indeed an elliptic curve.

Now we have to show that the point $(1, 1, 1)$ is of order 4. Only points on this curve are: $\mathcal{O} = [0; 1; 0], [1; 0; 1], [0; 1; 1], [1; 1; 1]$. So we only need to show that $P = (1, 1, 1)$ is not of order 2. For this we find $2P$.

$$\frac{\partial F}{\partial x}(P) = -3x^2 + y = (x^2 + y)(P) = 2 = 0$$
$$\frac{\partial F}{\partial y}(P) = (2y + x)(P) = x(P) = 1$$

Thus the tanget line to P is $1(y - 1) = 0$ or simply $y = 1$. For us to find the third point we find the roots of:

$$1 + x = x^3 + 1$$

This equation has 0 as its roots once and 1 as its roots twice. Thus the third intersection of the line and the curve is $(1, 1)$. In other words $P * P = P$. To find $P + P$ we need to find $P * \mathcal{O}$. Consider the equation in homogenized form:

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

Suppose the line $ax + by + cz = 0$ is passing through P and $\mathcal{O}$. Then $b = 0$ and $a = c$, or $x = z$. Substitution gives us:

$$y^2x + x^2y = x^3 + x^3 = 2x^3 = 0$$
$$\implies xy(y + x) = 0$$

If $x = z = 0$, then gives us the root $\mathcal{O} = [0; 1; 0]$. If $x = z = 1$, then gives us the roots $[1; 0; 1]$ and $[1; 1; 1]$. Therefore we have $P + P = P * \mathcal{O} = [1; 0; 1] \neq \mathcal{O}$. Then P is not of order 2. Therefore P has order 4.

Problem 4.

(i) We have $v(1 \times 1) = v(1) + v(1)$. Which means that $v(1) = 0$. Then $0 = v(1) = v(x \times x^{-1}) = v(x) + v(x^{-1})$, hence $v(x) = -v(x^{-1})$. Suppose that $v(x) > v(y)$.

$$v(x + y) \geq \min\{v(x), v(y)\}$$
$$\exists k \in \mathbb{R},\ v(x + y) = v(y) + k$$

Let $r = y \cdot (x + y)^{-1}$:

$$v(y) = v(r(x + y)) = v(r) + v(x + y) = v(r) + v(y) + k = v(ry) + k = v(\frac{y^2}{x + y}) + k$$
$$v(\frac{y^2}{x + y}) = v(ry) = v(r) + v(y) = v(r) + v(\frac{y^2}{x + y}) + k = v(\frac{y^3}{(x + y)^2}) + k$$

We can repeat this process, and each time find some element in K such that it is smaller than the privious one, and since each step is exactly k, then at some point it must stop, since v has a positive range. This suggests that $k = 0$ and $v(x + y) = v(y)$. **Huge bug**.

(*ii*) Since the sum is finite, WLOG suppose that $a_1 = \min\{a_i\}_{1 \leq i \leq n}$. Then for any a_i, either $v(a_1) = v(a_i)$, and we are done, then assume otherwise, using the first part, we have:

$$\begin{aligned} &\forall i, v(a_1) \neq v(a_i) \\ \implies &\forall i, v(a_1 + a_i) = \min\{a_1, a_i\} = a_1 \end{aligned}$$

Now note that:

$$\begin{aligned} v(a_1 + a_2) &= v(a_1) \\ v(a_1 + a_2) = v(a_1) \neq v(a_2) \implies v(a_1 + a_2 + a_3) &= \min\{v(a_1 + a_2), v(a_3)\} = v(a_1) \\ &\vdots \\ v(a_1 + \cdots + a_{n-2}) = v(a_1) \neq v(a_{n-1}) \implies & \\ v(a_1 + \cdots + a_{n-1}) &= \min\{v(a_1 + \cdots + a_{n-2}), v(a_{n-1})\} \\ &= \min\{v(a_1), v(a_{n-1})\} = v(a_1) \end{aligned}$$

Note that $0 = v(1) = v(-1 \times -1) = v(-1) + v(-1)$, hence $v(-1) = 0$. Then we have:

$$v(-n) = v(-1) + v(n) = v(n)$$

Now note that $a_1 + a_2 + \cdots + a_{n-1} = -a_n$, This means that $v(a_1 + \cdots + a_{n-1}) = v(a_n)$ therefore $v(a_1) = v(a_n)$. Which gives us a contradiction since we assumed there is no i such that $v(a_1) = v(a_i)$.