Amin Zolfagharian - 610002072

Problem 1.

Note that the curve described in the problem is $F(x, y, z) = x^3 + axz^2 + bz^3 - y^2z$. Now first we show that F is smooth iff we have $\Delta = 4a^3 + 27b^2 \neq 0$. First suppose that F is smooth, this means that:

$$\frac{\partial F}{\partial x} = 3x^2 + az^2 \qquad \frac{\partial F}{\partial y} = -2yz \qquad \frac{\partial F}{\partial z} = 3bz^2 + 2axz - y^2$$

at least one of the above is nonzero for any point in the curve. If there were to be a singular point on this curve, $P = (u, v, w)$, then we would have:

$$3u^2 + aw^2 = 0 \qquad -2vw = 0 \qquad 3bw^2 + 2auw - v^2 = 0$$

Since $-2vw = 0$, either $v = 0$ or $w = 0$. But if $w = 0$, we can rewrite $F(u, v, w) = 0$:

$$u^3 = 0$$

Therefore the point P would be $[0 : 1 : 0]$. Which can is non-singular since $\frac{\partial F}{\partial z} = -1$. Then suppose $v = 0$ and $w \neq 0$. We can rewrite the equations:

$$3bw^2 + 2auw - v^2 = 0 \implies w(3bw + 2au) = 0$$
$$\overset{w\neq 0}{\implies} 3bw + 2au = 0 \implies u = -\frac{3bw}{2a}$$

Now if we put this in $3u^2 + aw^2 = 0$, we get:

$$3(-\frac{3bw}{2a})^2 + aw^2 = 0$$
$$\implies w^2(27b^2 + 4a^3) = 0$$

And since $w \neq 0$ then $27b^2 + 4a^3 = 0$. Since we have no sigular-point, then

$$27b^2 + 4a^3 \neq 0$$

The converse is also implied. It only remains to show that this curve has a rational point iff it is smooth.

Problem 2.

If f is of degree $d \geq 4$, then we have:

$$F(x, y, z) = f(x)^* - y^2z^{d-2} = 0$$

Note that $f(x)$ is a polynomial with over only one intermidiate x, therefore all terms in $f(x)^*$ except $a_d x^d$, are multiplied in z. For this curve to have a non-singular point, we must have:

$$\frac{\partial F}{\partial x} = \frac{\partial f(x)^*}{\partial x} = 0 \tag{1}$$

$$\frac{\partial F}{\partial y} = -2z^{d-2}y = 0 \tag{2}$$

$$\frac{\partial F}{\partial z} = -(d-2)y^2 z^{d-3} + \frac{\partial f(x)^*}{\partial z} \tag{3}$$

Since $char K \neq 2$, then (2) shows that either $y = 0$ or $z = 0$. If $z = 0$, then we can replace this in F and have:

$$F(x, y, 0) = f(x)^* = 0 \implies a_d x^d = 0 \implies x = 0$$

Therefore $[0 : 1 : 0]$ is a singular point in this curve. Now if $y = 0$ and $z \neq 0$, then we have $[x : 0 : z] \sim [\frac{x}{z} : 0 : 1]$:

$$\frac{\partial F}{\partial x} = \frac{\partial f(x)^*}{\partial x} = \frac{\partial f(x/y)}{\partial x/y} = 0$$

On the other hand:

$$F(x/y, 0, 1) = f(x/y) = 0$$

Thus, $f(x/y) = f(x/y)' = 0$, But we knew that f does not have a double root. Therefore there is not singular point with $z \neq 0$ and $y = 0$ and $y^2 = f(x)$ has only one singular point.

Problem 3.

(i) First we find the equation of the line connecting P_1 and P_2:

$$\lambda = \frac{v_2 - v_1}{u_2 - u_1} \qquad v = \lambda u + k \quad \text{where} \quad k = v_1 - \lambda u_1 = v_2 - \lambda u_2$$

Now if we substitute u and v from the line we get the intersections:

$$u^3 + v^3 = u^3 + (\lambda u + k)^3 = \alpha$$
$$(\lambda^3 + 1)u^3 + 3k\lambda^2 u^2 + 3k^2 \lambda u + k^3 = \alpha$$

But we know two of these roots are u_1 and u_2, so we want to find u_3. Note that $u_1 + u_2 + u_3 = -3k\lambda^2/\lambda^3 + 1$:

$$u_3 = -\frac{3k\lambda^2}{\lambda^3 + 1} - u_1 - u_2$$

And $v_3 = \lambda u_3 + k$. This gives us the point $P_1 * P_2$. Now we have to find the intersection of the line passing through $P_1 * P_2$ and $\mathcal{O}$ with the curve. A projective line has the form $l = x + by + cz = 0$. If substitute the value for two points we have:

$$1 - b = 0 \implies b = 1$$
$$u_3 + v_3 + c = 0$$

Therefore the line looks like this: $l = x + y - (u_3 + v_3)z = 0$. Now if we substitute this into the curve equation:

$$U^3 + V^3 = \alpha W^3 = \alpha(\frac{U + V}{u_3 + v_3})^3$$

Problem 4.

Problem 5.

Let $F(X, Y, Z) = X^3 + pY^3 + p^2Z^3$. For the sake of contradiction suppose we have some projective point (a, b, c) such that $F(a, b, c) = 0$, where $a, b, c \in \mathbb{Q}$. There exists some $t \in \mathbb{Z}$ such that $ta, tb, tc \in \mathbb{Z}$. Since we have $(a, b, c) \sim (ta, tb, tc)$, then $F(ta, tb, tc) = 0$. This means that F has some integer root (ta, tb, tc). For simplicity put $(a, b, c) = (ta, tb, tc)$. Let us define $\nu_p(a)$ to be the biggest power of p dividing a. In other words, $\nu_p(a) = \alpha$ means that $p^\alpha \mid a$ and $p^{\alpha+1} \nmid a$. Now suppose $\nu_p(a) = \alpha$, $\nu_p(b) = \beta$ and $\nu_p(c) = \gamma$. Then we have $\nu_p(a^3) = 3\alpha$, $\nu_p(pb^3) = 3\beta + 1$ and $\nu_p(p^2c^3) = 3\gamma + 2$. This shows that

$$\nu_p(a^3) \neq \nu_p(pb^3) \neq \nu_p(p^2c^3)$$

WLOG suppose that $\nu_p(a^3) < \nu_p(pb^3) < \nu_p(p^2c^3)$. This means that $\nu_p(a^3 + pb^3 + p^2c^3) = 3\alpha$. Now:

$$\left.\begin{array}{l} a^3 + pb^3 + p^2c^3 = 0 \\ p^{3\beta+1} \mid 0 \\ p^{3\beta+1} \mid pb^3 + p^2c^3 \end{array}\right\} \implies p^{3\beta+1} \mid a^3$$

But since $\nu_p(a^3) = 3\alpha < 3\beta + 1$, we arrive at a contradiction. This shows that we had not rational root in the first place.