MA 353: Elliptic Curves
Assignment-1

Irish Debbarma, 16696

due: 19th February, 2023

1. $V/\mathbb{Q}$ is the variety $V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2$

   Claim: $V(\mathbb{Q}) = \emptyset$.

   Proof. Since the equation is homogenous, and we are working over rationals $\mathbb{Q}$, can assume that the solutions $[x : y : z]$ have $\gcd(a, b, c) = 1$ and $a, b, c \in \mathbb{Z}$.

   - Observe $\pmod 2$. We have $5X^2 \equiv Z^2 \pmod 2 \Rightarrow X \equiv Z \pmod 2$. If X, Z are both even, then
     - Observe $\pmod 4$. We get $X^2 + 2XY + 2Y^2 = 2YZ + Z^2$. If X, Z are both even, then Y is even as well which contradicts our assumption on the gcd. Thus, we can assume X, Z to be odd.
   - If we consider $\pmod 3$, we have $2X^2 + 2Y^2 = 2YZ + Z^2 \Rightarrow 2X^2 + 3Y^2 = (Y + Z)^2 \Rightarrow X^2 = (Y + Z)^2$. Therefore, $3 \mid X$ and $3 \mid Y + Z$.
     - Now, consider $\pmod 9$. $2Y^2 = 2YZ + Z^2 \Rightarrow 3Y^2 = (Y + Z)^2 \Rightarrow Y^2 = 0$. Thus, $3 \mid Y \Rightarrow 3 \mid Z$. This contradicts our assumption $\gcd(X, Y, Z) = 1$.

   □

2. For each prime $p \geq 3$, let $V_p \subseteq \mathbb{P}^2$ be the variety corresponding to the curve

   $$V_p : X^2 + Y^2 = pZ^2$$

   (a) **Claim**: $V_p \cong \mathbb{P}^1$ over $\mathbb{Q}$ iff $p \equiv 1 \pmod 4$

   Proof. $(\Rightarrow)$

   Suppose $V_p(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$ but $p \equiv 3 \pmod 4$. Consider the equation mod p to get $X^2 + Y^2 \equiv 0 \pmod p \Rightarrow X^2 \equiv -Y^2 \pmod p$. Solving this is equivalent to checking if -1 is a quadratic residue of p but from Euler's criterion -1 is a quadratic residue iff $(-1)^{(p-1)/2} = 1$. Since $p = 4k + 3$, the condition is not satisfied and hence -1 is not a quadratic residue. Thus, $V_p(\mathbb{Q}) = \emptyset$ but clearly $\mathbb{P}^1(\mathbb{Q})$ is non-empty, a contradiction. Hence, our assumption is wrong. p must be congruent $1 \pmod 4$.

$(\Leftarrow)$

Suppose $p \equiv 1 \pmod 4$. Then there exists integers a, b such that $p = a^2+b^2$. Consider the map

$$\begin{aligned} \phi : V_p(\mathbb{Q}) &\longrightarrow \mathbb{P}^1(\mathbb{Q}) \\ [X, Y, Z] &\mapsto [aX + bY + pZ, (aY - bX)] \end{aligned}$$

This map is regular except maybe at the point $aY - bX = 0, aX + bY + Z = 0$, i.e., the point $[a : b : -1]$.

Note that ☐

(b) **Claim**: For $p \equiv 3 \pmod 4$, no two V_ps are isomorphic.

Proof. ☐

3. Let $F(x, y, x) \in k[x, y, z]$ be a homogeneous polynomial polynomial of degree $d \geq 1$ and the curve corresponding to F is non-singular.

Claim:

$$\mathfrak{g}(C) = \frac{(d-1)(d-2)}{2}$$

Proof. ☐

4. (a) $L : 2x + 5y - 1 = 0$

Homogenisation gives us $2x + 5y - Z = 0$. The point at infinity is the point where $z = 0$. Then, $2x + 5y = 0 \Rightarrow [-5 : 2 : 0]$ is the point at infinity.

(b) $C : x^2 - 4xy + 3y^2 - 3x + 5y - 10 = 0$

Homogenisation gives us $x^2 - 4xy + 3y^2 - 3xz + 5yz - 10z^2$. The point at infinity is the point where $z = 0$. Thus,

$$\begin{aligned} x^2 - 4xy + 3y^2 &= 0 \\ (x - 2y)^2 - y^2 &= 0 \\ (x - 2y + y)(x - 2y - y) &= 0 \\ (x - y)(x - 3y) &= 0 \end{aligned}$$

Thus, $x = y$ or $x = 3y$. The points at infinity are thus $[1 : 1 : 0]$ and $[3 : 1 : 0]$.

5. Given $f(x, y) = y^2 - x^3 - ax^2 - bx$

6. Suppose E is an elliptic curve given by the Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ and $P = (x, y)$ a point on E.

   (a) The slope at P is $\lambda = (3x^2 + 2ax + b)/2y$ and the intercept is $\nu = (-x^3 + bx + 2c)/2y$. The line is given by $Y = \lambda X + \nu$. From the formula given in Silverman, the coordinate of $2P$ is given by

   $$\begin{aligned} x_2 &= \lambda^2 - a - 2x \\ y_2 &= -\lambda x_2 - \nu \end{aligned}$$

   Since we want to solve for $3P = 0$, we can just solve for $2P = -P$. Again, using the formula given in Silverman, we want $x_2 = x, y_2 = -y$.

   $$\begin{aligned} -\lambda x_2 - \nu &= -y \\ \lambda x + \nu &= y \\ \lambda &= \frac{y - \nu}{x} \end{aligned}$$

   Using this we can do the following:

   $$\begin{aligned} \lambda^2 - a - 2x &= x \\ \lambda^2 &= a + 3x \\ (y - \nu)^2 &= ax^2 + 3x^3 \\ y^2 + \nu^2 - 2y\nu &= ax^2 + 3x^2 \\ x^3 + ax^2 + bx + c + \nu^2 + x^3 - bx - 2c &= ax^2 + 3x^3 \\ \nu^2 - c &= x^3 \\ (-x^3 + bx + 2c)^2 &= 4(x^3 + c)(x^3 + ax^2 + bx + c) \\ x^6 + b^2x^2 + 4c^2 - 2bx^4 - 4cx^3 + 4bcx &= 4x^6 + 4ax^5 + 4bx^4 + 4cx^3 + \\ &\quad 4cx^3 + 4acx^2 + 4bcx + 4c^2 \end{aligned}$$

   $$3x^6 + 4ax^5 + 6bx^4 + 12x^3c + (4ac - b^2)x^2 = 0$$

   Thus, either $x = 0$ or $3x^4 + 4ax^3 + 6bx^2 + 12xc + (4ac - b^2) = 0$.

   (b) Now, in the particular case of $Y^2 = X^3 + 1$, we have $a = 0 = b, c = 1$. Thus, we have two cases:

   - $x = 0$, then $y^2 = 1$. Hence, the points are $[0 : 1], [0 : -1]$.
   -
     $$\begin{aligned} 3x^4 + 12x &= 0 \\ x^3 &= -4 \end{aligned}$$

     Thus, $x = \sqrt{-4}, \sqrt{-4}\omega$ or $\sqrt{-4}\omega^3$ where ω is primitive 3rd root of unity.
     Now, solve for $y^2 = x^3 + 1 = -2$. Therefore, $y = \sqrt{-2}i, -\sqrt{-2}i$

7. Given $E : y^2 = x^3 + 17$ is an elliptic curve over $\mathbb{Q}$

(a) $P = (-1, 4), Q = (2, 5)$. We wish to find $P + Q$

(b) $P = (-2, 3), Q = (2, 5)$. We wish to find $-P + 2Q$