Elliptic Curves, n° 2

Lei Bichang

September 27, 2024

Exercise 1

(a) $-P_1 = (-1, -4)$. The line connecting $P_2 = (-2, 3)$ is

$$y = -7x - 11,$$

so

$$x(P_2 - P_1) = 49 - (-1) - (-2) = 52, \; y(P_2 - P_1) = -(-7 \cdot 52 - 11) = 375.$$

The tangent line at P_2 is

$$y = 2x + 7,$$

so

$$x(2P_2) = 4 - 2 \cdot (-2) = 8, \; y(2P_2) = -(2 \cdot 8 + 7) = 23.$$

The line connecting $2P_2$ and P_1 is

$$y = \frac{19}{9}x + \frac{55}{9},$$

so

$$x(2P_2 + P_1) = -\frac{206}{81}, \; y(2P_2 + P_1) = -\frac{571}{729}.$$

Exercise 2

These three Weierstrass equations satisfy $4a^3 + 27b^2 \neq 0$ in $\mathbb{F}_5$, so they are all elliptic curves over $\mathbb{F}_5$.

(a) For $E : y^2 = x^3 + x$,

$$E(\mathbb{F}_5) = \{O, (0, 0), (2, 0), (-2, 0)\},$$

so all these points have order 2. Therefore, $E(\mathbb{F}_5) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

(b) For $E : y^2 = x^3 + 2x$,

$$E(\mathbb{F}_5) = \{O, (0, 0), (-2, 1), (-2, -1), (-1, 1), (-1, -1)\}.$$

There is only one nonzero element of order 2, so it is not $\mathbb{Z}/2 \times \mathbb{Z}/3$. Therefore, $E(\mathbb{F}_5) \simeq \mathbb{Z}/6$.

(c) For $E : y^2 = x^3 + 1$,

$$E(\mathbb{F}_5) = \{O, (0, 1), (0, -1), (2, 2), (2, -2), (-1, 0)\}.$$

This is also an abelian group of order 6 with one nonzero element of order 2, so $E(\mathbb{F}_5) \simeq \mathbb{Z}/6$.

Exercise 3

(a) We look at the $X = 1$ chart, where the affine equation corresponding to C is

$$1 + y^3 = z^3.$$

At $O = (-1, 0)$, the slope of tangent is

$$\frac{dy}{dz} = 0,$$

so the tangent is $y = -1$. Therefore, the equation of T is

$$X + Y = 0.$$

(b) Such a homography should send O to $[0 : 1 : 0]$ and another point $Q \notin C$ on T to $[1 : 0 : 0]$. Take $Q = [-1 : 1 : 1]$ and let A be the matrix giving this homography, then we can choose

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Under this transformation, the equation becomes

$$(-X + Y + Z)^3 + (X - Y)^3 = X^3,$$

which simplifies to

$$3ZY^2 - 6ZXY + 3Z^2Y = X^3 - 3ZX^2 + 3Z^2X - Z^3.$$

Applying $Z \mapsto \frac{1}{3}Z$ to this equation, we obtain a Weierstrass equation

$$Y^2Z - 2XYZ + \frac{1}{3}YZ^2 = X^3 - X^2Z + \frac{1}{3}XZ^2 - \frac{1}{27}Z^3$$

Then apply $Y \mapsto Y - \left(X - \frac{1}{6}Z\right)$ to this equation, we obtain

$$Y^2Z = X^3 - \frac{1}{108}Z^3. \tag{1}$$

However, the transformation from C to Eq. (1) used above does not send T to $Z = 0$. Suppose that a homography of the form[1]

$$\begin{cases} X \mapsto Z, \\ Y \mapsto \alpha(X - Y), \\ Z \mapsto \beta(X + Y) \end{cases} \tag{2}$$

changes Eq. (1) to C. Substitute them in Eq. (1) and we got

$$\begin{cases} \beta(\alpha^2 + \beta^2 s) = 1, \\ 3\beta^2 s - \alpha^2 = 0, \end{cases}$$

where $s = 1/108$. Take a solution

$$\begin{cases} \alpha = \frac{1}{2}, \\ \beta = 3, \end{cases}$$

then the transformation Eq. (2) is invertible.

[1]This form is inspired by Part (d) of this exercise.

(c) Let L be a line passing O that is tangent to C. Since $Z=0$ intersects C at three different points given that $\operatorname{char} k \neq 3$, we can write

$$L: X+Y+cZ=0.$$

Since O is the only point of C at infinity, we can work in the affine chart $Z \neq 0$, and L is tangent to C iff

$$\begin{cases} x+y+c=0, \\ x^3+y^3=1, \end{cases} \tag{3}$$

has only one solutions. This is to say

$$(x+c)^3 - x^3 + 1 = 0,$$

i.e.,

$$3cx^2 + 3c^2x + (c^3+1) = 0,$$

has discriminant

$$9c^4 - 4 \cdot 3c \cdot (c^3+1) = -3c(c^3+4) = 0.$$

So the tangent lines through O are

$$X+Y+cZ=0,$$

where $c=0$ or $c^3=-4$.

(d) The points of order 2 are the points other than O at which the tangents passing O. So these points are $\left[\frac{r}{2} : \frac{r}{2} : 1\right]$, where $r^3=4$.

On the curve given by Eq. (1), the order two points are of the form $[x:0:z]$, so the points are $[1:0:3r]$ with $r^3=4$. Using Eq. (2), we can solve

$$\begin{cases} 1 = Z, \\ 0 = \frac{X-Y}{2}, \\ 3r = 3(X+Y) \end{cases}$$

to get the point on C correspondingto $[1:0:3r]$, which is exactly $\left[\frac{r}{2} : \frac{r}{2} : 1\right]$.

(e) The inflection points of C are the points where the Hessian of $F = X^3+Y^3-Z^3$ vanishes; i.e,

$$\begin{vmatrix} 6X & & \\ & 6Y & \\ & & -6Z \end{vmatrix} = -6^3XYZ = 0.$$

SO the points P with $3P=0$ are

$$[0:\omega:1],\ [\omega:0:1],\ [-\omega:1:0],$$

where $\omega^3=1$.