1. Review of quadratic equations

For $k = \mathbf{Q}$ or $\mathbf{Q}_p$ and $f(x,y) \in \mathbf{Q}[x,y]$, recall that

$$X_f(k) = \left\{(x,y) \in k^2 \mid f(x,y) = 0\right\}.$$

The basic question is to know if $X_f(\mathbf{Q}) \neq \emptyset$. When $f(x,y)$ is a quadratic form, i.e. $f(x,y) = y^2 - ax^2 - b$, Hasse-Minkowski's theorem tells us that

$$\begin{aligned} X_f(\mathbf{Q}) \neq \emptyset &\iff X_f(\mathbf{Q}_p) \neq \emptyset \text{ for all } p \\ &\iff f' = ax^2 - y^2 \text{ represents } b \text{ in } \mathbf{Q}_p \text{ for all } p \\ &\iff (b, -\delta(f'))_p = \mathrm{H}_p(f') = (1,-a)_p \text{ for all } p \\ &\iff (a,b)_p = 1 \text{ for all \textit{odd} } p|ab \text{ and } p = \infty, \\ &\qquad \text{(why don't we need to consider } p = 2\text{?)}. \end{aligned}$$

Therefore, to know if $X_f(\mathbf{Q})$ is empty not not, it boils down to a finite amount of computation of Hilbert symbols at odd primes, which can be computed effectively via Gauss quadratic reciprocity law. We can also ask the following natural questions:

(1) How to obtain a point in $X_f(\mathbf{Q})$ if it is not empty?
(2) How many solutions in $X_f(\mathbf{Q})$?

When $f(x,y) = x^2 - ay^2 - b$, the answers to the above questions is fairly easy. The first one follows from the proof of the proof of Hasse-Minkowski's theorem for $n = 3$. As for the second one, we can show if $X_f(\mathbf{Q}) \neq \emptyset$, then $\#X_f(\mathbf{Q})$ is infinite, and we can write down all solutions.

Example 1.1. Let $f(x,y) = 5x^2 - y^2 - 19$. Write down all solutions in $X_f(\mathbf{Q})$.

2. Cubic equations: Elliptic curves

2.1. Let k be one of the fields $\mathbb{F}_p, \mathbf{Q}_p, \mathbf{Q}, \mathbf{R}, \mathbf{C}$. Take a cubic polynomial

$$g(x) = x^3 + ax^2 + bx + c \text{ with } a,b,c \in k$$

and consider the cubic equations

$$f(x,y) = y^2 - g(x).$$

The homogeneous polynomial $F(X,Y,Z)$ attached to f defined by

$$F(X,Y,Z) := Z^3 \cdot f(\frac{X}{Z}, \frac{Y}{Z}) = ZY^2 - (X^3 + aX^2Z + bXZ^2 + cZ^3).$$

We shall consider the set of k-rational points

$$\begin{aligned} X_f(k) &= \left\{(x,y) \in k^2 \mid y^2 = g(x)\right\}; \\ \mathcal{C}_f(k) &= \left\{[X,Y,Z] \in \mathbf{P}^2(k) \mid F(X,Y,Z) = 0\right\}. \end{aligned}$$

We have an obvious embedding

$$\begin{aligned} X_f(k) &\hookrightarrow \mathcal{C}_f(k) \\ (x,y) &\mapsto [x,y,1]. \end{aligned}$$

It is clear that $\mathcal{C}_f(k)$ contains the point $[0,1,0]$, which is the only point with zero Z-coordinate and that

$$\mathcal{C}_f(k) = X_f(k) \sqcup \{[0,1,0]\}.$$

We can ask the following natural questions regarding the size of $\mathcal{C}_f(\mathbf{Q})$ (or $X_f(\mathbf{Q})$):

(1) When is $\#\mathcal{C}_f(\mathbf{Q}) > 1$?
(2) How to determine *effectively* if $\#\mathcal{C}_f(\mathbf{Q}) = \infty$?

Before we can study the above questions seriously, we need to understand some basic structures of $\mathcal{C}_f(k)$.

2.2. Singular points on $\mathcal{C}_f(k)$.

Definition 2.1. We say a point $P = [a, b, c] \in \mathcal{C}_f(k)$ is a *singular point* if

$$F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0 \quad (F_X := \frac{\partial F}{\partial X}(X, Y, Z)).$$

By definition, the point $[0, 1, 0]$ is not a singular point. If $(a, b) \in X_f(k)$ is a singular point, then

$$\begin{aligned} & f(a, b) = f_x(a, b) = f_y(a, b) = 0 \\ \Longleftrightarrow\ & g'(a) = g(a) = b = 0 \\ \Longleftrightarrow\ & \text{the equation } g(x) = 0 \text{ has a multiple root.} \end{aligned}$$

Therefore, we can conclude that there is at most one singular point in $\mathcal{C}_f(k)$. Let $\alpha_1, \alpha_2, \alpha_3$ are three roots of $g(x) = 0$ and let Δ_g be the discriminant of $g(x)$ given by

$$\Delta_g := (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2.$$

The above discussion shows that

Lemma 2.2. *The cubic curve $\mathcal{C}_f(k)$ has a singular point if and only if $\Delta_g = 0$.*

2.3. The group structure on $\mathcal{C}_f(k)$.

Definition 2.3 (Collinear points)**.** Three points $P, Q, R \in \mathcal{C}_f(k)$ are called *collinear* if there exits a *line*

$$\mathcal{L}_{\lambda,\mu,\nu}(k) := \left\{[X, Y, Z] \in \mathbf{P}^2(k) \mid \lambda X + \mu Y + \nu Z = 0\right\} \quad ([\lambda, \mu, \nu] \in \mathbf{P}^2(k))$$

such that

$$\mathcal{L}_{\lambda,\mu,\nu}(k) \cap \mathcal{C}_f(k) = \{P, Q, R\}.$$

In the class, we explained the following proposition by direct computation:

Proposition 2.4. *Let P and Q be two non-singular points in $\mathcal{C}_f(k)$. There exists a unique point $R \in \mathcal{C}_f(k)$ such that P, Q, R are collinear.*

Proof. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points in $X_f(k) \subset \mathcal{C}_f(k)$. Suppose that $y_1 \neq -y_2$. Let

$$\begin{aligned} \lambda =& \frac{y_1 - y_2}{x_1 - x_2} \text{ if } x_1 \neq x_2, \text{ and} \\ \lambda =& \frac{g'(x_1)}{2y_1} \text{ if } x_1 = x_2,\ y_1 = y_2 \quad (\text{so } P = Q). \end{aligned}$$

and let $\nu = y_1 - \lambda x_1$. Then we have

$$\mathcal{L}_{\lambda,-1,\nu}(k) \cap \mathcal{C}_f(k) = \{P, Q, R\},$$

where $R = (x_3, y_3)$ with

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

If $x_1 = x_2$ and $y_1 = -y_2$, then $R = [0, 1, 0]$ and we have

$$\mathcal{L}_{1,0,-x_1}(k) \cap \mathcal{C}_f(k) = \{P, Q, R\}.$$

We leave the other cases to you as exercises. □

Definition 2.5 (Group law)**.** Suppose that $\mathcal{C}_f(k)$ is non-singular. Namely, $\Delta_g \neq 0$. Then we define the group law on $\mathcal{C}_f(k)$ as follows:

(1) The identity element is $O := [0, 1, 0] \in \mathcal{C}_f(k)$.
(2) For $P \in \mathcal{C}_f(k)$, define $-P$ to be the unique element such that $\{P, O, -P\}$ are collinear.
(3) For $P, Q \in \mathcal{C}_f(k)$, let $P + Q$ be the unique point such that $\{P, Q, -(P + Q)\}$ are collinear.

By definition, if P, Q, R are collinear, then $P + Q + R = O$.

Theorem 2.6. *Suppose $\Delta_g \neq 0$. Then the above definition gives an abelian group structure on $\mathcal{C}_f(k)$ with the identity element O.*

Definition 2.7 (Elliptic curves)**.** The pair $(\mathcal{C}_f(k), O)$ is called an *elliptic curve* defined by $f(x, y) = y^2 - g(x) = 0$. Following the convention, we shall use the notation $E(k)$ to denote the abelian group $\mathcal{C}_f(k)$ with non-zero discriminant $\Delta_g \neq 0$.

Example 2.8. Let $E : y^2 = x^3 + 17$. Let $P = (-1, 4)$ and $Q = (2, 5)$. Compute $P + Q$, $2P$ and $2Q$.

2.4. Torsion points in $E(k)$. Let $E : y^2 = g(x)$ be an elliptic curve over k. For each positive integer $m > 1$, we let $E[m](k)$ be the m-torsion subgroup in $E(k)$ defined by

$$E[m](k) := \{P \in E(k) \mid m \cdot P = O = [0, 1, 0]\}.$$

Proposition 2.9. *If E is an elliptic curve over the complex number $\mathbf{C}$, then we have*

$$E[2](\mathbf{C}) \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}, \quad E[3](\mathbf{C}) \simeq \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}.$$

Using the analytic method, in general one can show that

$$E[m](\mathbf{C}) \simeq \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}.$$

Homework (Due date: 11/25)

Exercise 1 (5 pts)**.** Show the discriminant Δ_g of $g(x) = x^3 + ax^2 + bx + c$ is given by the formula

$$\Delta_g = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Exercise 2 (5 pts)**.** Let $E : y^2 = x^3 + 17$ be an elliptic curve over $\mathbf{Q}$. Let $P = (-2, 3)$ and $Q = (2, 5)$. Compute the following points:

$$2P,\ P - Q,\ 3P - Q.$$

These points all have integral x, y coordinates.

Exercise 3 (5 pts)**.** Let $E : y^2 = x^3 - 2x$. Let $i = \sqrt{-1} \in \mathbf{C}$. Define a map $u : E(\mathbf{C}) \to E(\mathbf{C})$ by

$$u(x, y) := (-x, iy) \text{ and } u(O) := O.$$

Show that the map u is a group homomorphism. In other words,

$$u(P + Q) = u(P) + u(Q).$$

Exercise 4 (10 pts)**.** Consider the point $P = (3, 8)$ on the elliptic curve $E : y^2 = x^3 - 43x + 166$. Compute P, $2P$, $3P$ $4P$ and $8P$. Show that $7P = O$.

Exercise 5 (5 pts)**.** Let $E : y^2 = x^3 + 1$. Find all points $P \in E(\mathbf{C})$ with $3P = O$.