CHAPTER 1

GEOMETRY AND ARITHMETIC

1.1 Rational Points on Conics

We start with the rational numbers, $\mathbb{Q}$. A point (x, y) on the plane is a *rational point* if both $x, y \in \mathbb{Q}$. A *rational line* is a line in the plane whose coefficients are rational, i.e.

$$ax + by + c = 0$$

where $a, b, c \in \mathbb{Q}$. It is easy to show, and left as an exercise to the reader, that given two rational points, the line between them is rational. It is also easy to show that given non-parallel rational lines, their intersection point is rational.

Moving beyond lines, this book aims to study the rational points on curves in the plane, specifically cubic curves. As an introduction however, we will briefly study conics. Let the equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

define a conic. We say this is a *rational conic* if each coefficient $a, b, \ldots, f$ is rational.

Consider the intersection points of a rational line with a rational conic. Are these points also rational? In general, the answer is no. The reason for this is that in the process of solving for the x-coordinates of the intersection points, we end up with a quadratic equation. Assuming a rational coefficients for our line and conic, we obtain a rational quadratic equation, but a such an equation might still have irrational roots, e.g. $x^2 - 2 = 0$, so the intersection points may not be rational. We can show this more rigorously with an example.

Example 1.1.1

Claim: There exists a rational line L and rational conic C such that their intersection points are not rational.

Proof: Define $L : y = 1 - x$ and $C : y = x^2 - 2$. One can readily verify that L and C are both rational. To find the x-coordinates of the intersection points, we set both sides to be equal and solve for x:

$$1 - x = x^2 - 2 \implies x^2 + x - 3 = 0$$

Using the quadratic equation we can find the values of x:

$$x = \frac{-1 \pm \sqrt{13}}{2}$$

Since the x-coordinates are irrational, the intersection points are not rational. ■

But can we find lines and conics that *do* have rational intersection points? It turns out we can. Better yet, if we find one intersection point to be a rational, then it must be that the other point is also rational. We give an example where the intersection points are rational, and then prove our claim of duplicate rational points.

Example 1.1.2

Claim: There exists a rational line L and rational conic C such that their intersection points *are* rational.

Proof: Define $L : y = x$ and $C : x^2 - 2$. We find the x-coordinates of the intersection points as before:

$$x = x^2 - 2 \implies x^2 - x - 2 = (x - 2)(x + 1) = 0 \ ,$$

thus

$$x = 2 \text{ and } x = -1 \ .$$

Using our equation for L, we find that the y-coordinates are $y = 2$ and $y = -1$. Since both points have integer coordinates, they are rational. ■

Theorem 1.1.3

Theorem: Let L and C be a rational line and rational conic respectively, and let P, P' be the intersection points between them, then if P is a rational point, so is P'.

Proof: Let $L : \alpha x + \beta y + \gamma = 0$ and $C : ax^2 + bxy + cy^2 + dx + ey + f = 0$ where all coefficients are rational. In addition, let $P_1 : (x_1, y_1)$ and $P_2 : (x_2, y_2)$ be the intersection points of L and C, and assume P_1 is rational. We can obtain a quadratic equation for x as follows:

$$\alpha x + \beta y + \gamma = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

$$\implies ax^2 + x(by + d - \alpha) + (cy^2 + y(e - \beta) + f - \gamma) = 0 \tag{1}$$

Solving this equation directly would be extremely tedious, but luckily we can use the property that the sum of the roots of the rational quadratic equation $a_0x^2 + a_1x + a_2 = 0$ is equal to $-a_1/a_0$. We know P_1 is an intersection point, so x_1 and y_1 satisfy (1), thus $by_1 + d - \alpha$ and $cy_1^2 + y_1(e - \beta) + f - \gamma$ are both rational, and thus (1) is a rational quadratic equation. Since x_1 and x_2 are roots, we can leverage our property of their sum:

$$x_1 + x_2 = -\frac{by_1 + d - \alpha}{a} \implies x_2 = -\frac{by_1 + d - \alpha}{a} - x_1$$