3. Residue Class Rings

In this chapter we will study the conic $\mathcal{H} : XY = 1$ over residue class rings $\mathbb{Z}/m\mathbb{Z}$. The next step will be generalizing these results to general conics. For doing so, we will need some more abstract algebra (finite fields, in particular, which are the topic of the next chapter).

3.1. Fermat's First Theorem

Where we study the group law on the hyperbola over residue class rings.

Our main interest in this chapter lies with understanding the unit groups of the residue class rings $R = \mathbb{Z}/m\mathbb{Z}$. The material presented here is classical (going back to Gauss), and it is presented in the classical language. Later we will prove the results given here for a second time; in fact the properties of $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathcal{H}(\mathbb{Z}/m\mathbb{Z})$ are shared by general conics.

We start by looking at the example of $\mathbb{Z}/5\mathbb{Z}$; the multiplication table for the nonzero elements in $\mathbb{Z}/5\mathbb{Z}$ is given by

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Such multiplication tables contain the full information about a group and its structure, but the structure is not visible. What we can see is the following:

- Every element has a multiplicative inverse because in every row and every column there is a 1;
- The group (if it is one) is abelian: commutativity is displayed by the fact that the table is symmetric with respect to the main diagonal.
- Elements of order 2 (here the residue classes generated by 1 and 4) can be found quickly: all we have to do is look for entries 1 on the diagonal.

On the other hand, checking associativity using the multiplication table is a horrible task. Similarly, such tables do not display subgroups.

Multiplication in residue class rings $\mathbb{Z}/m\mathbb{Z}$ may be represented by a graph; multiplication by 2 in the ring $\mathbb{Z}/7\mathbb{Z}$, for example, is displayed as follows:

Multiplication by 2 produces a fixed point 0 (of course 0 is a fixed point for multiplication by any element) and two cycles of length 3. The cycle containing 1 forms a subgroup H of order 3 of the group G of nonzero elements modulo 7, the other cycle represents its coset G/H.