Geometry in Finite Fields and Beyond

1 Modular Arithmetic

Let $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ denote the integers. If $n > 1$ is an integer, we will say that two integers a and b are *congruent modulo* n if $a - b$ is a multiple of n. This relationship will be written $a \equiv b \pmod{n}$. For example, $17 \equiv 2 \pmod{5}$, since $17 - 2 = 15$ is a multiple of 5.

Let $\mathbb{Z}_n$ denote the set of integers modulo n. This set can be thought of as all the possible remainders one can get when dividing by n. For example, if one takes any integer and divides that integer by 6, one could have a remainder of $0, 1, 2, 3, 4$, or 5. This means that every possible integer will correspond to either $0, 1, 2, 3, 4$, or 5 in $\mathbb{Z}_6$. We can then identity $\mathbb{Z}_n$ with the set $\{0, 1, 2 \ldots, n-1\}$. Furthermore, we can add and multiply two numbers in $\mathbb{Z}_n$ by adding or multiplying those two numbers like usual, and then taking the resulting quantity modulo n. For example, in $\mathbb{Z}_9$, we have

$$4 + 8 = 12 \equiv 3 \pmod{9}$$

and

$$4 \cdot 8 = 32 \equiv 5 \pmod{9}$$

(**Exercises 1 and 2**)

Recall a prime number is a positive integer greater than 1 whose only positive divisors are 1 and itself. The prime numbers $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}$ are at the heart of a great deal of modern research in number theory.

Although we can make sense of addition and multiplication, there are a few differences between arithmetic in $\mathbb{Z}$ and arithmetic in $\mathbb{Z}_n$. First, note that when n is a composite integer (i.e., when n is not prime), we can find two nonzero integers whose product is zero. For instance, $2 \cdot 3 = 0$ in $\mathbb{Z}_6$. A nonzero number a is called a *zero divisor* if there exists another nonzero number b such that $ab = 0$. (**Exercise 3**)

2 How do the primes play a role?

How does the set $\mathbb{Z}_p$ behave when p is a prime number? When p is prime, we will write $\mathbb{F}_p$ instead of $\mathbb{Z}_p$. We will explain this mysterious notation below.

Since p has no divisors other than itself and 1, it turns out that $\mathbb{Z}_p$ has no zero-divisors. Also, unlike $\mathbb{Z}$, every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse. That is to say that for every element a in $\mathbb{Z}_p$, there exists an element b in $\mathbb{Z}_p$ with $ab = 1$. We denote the multiplicative inverse of a by a^{-1} (which we sometimes lazily write as $\frac{1}{a}$). This simple fact that every nonzero element in $\mathbb{F}_p$ has a multiplicative inverse is one of the most important properties of $\mathbb{F}_p$ and is what makes the set so nice! A finite set with no zero divisors is called a *finite field*, which explains the notation $\mathbb{F}_p$. (**Exercise 4**)

Let's take the next step. Write $\mathbb{F}_p^2$ to denote the set of order pairs of elements in $\mathbb{F}_p$.

$$\mathbb{F}_p^2 = \{(x, y) : x, y \text{ are elements of } \mathbb{F}_p\}$$

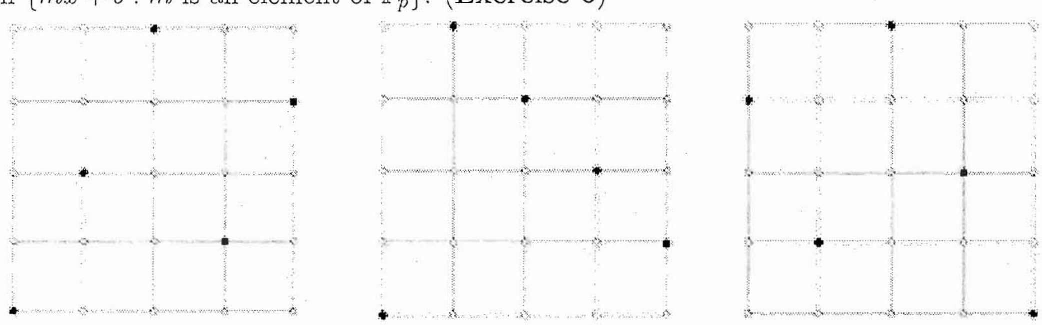
($\mathbb{F}_p^2$ is called a *vector space* over $\mathbb{F}_p$, but do not worry about this if you have not seen the words "vector space" before!) Notice the set $\mathbb{F}_p^2$ has exactly p^2 elements. (**Exercise** 5).

3 Geometry in $\mathbb{F}_p$

We now consider geometric objects in $\mathbb{F}_p^2$. Our goal today is to figure out how to describe geometric objects in $\mathbb{F}_p^2$ and to examine these objects and see what properties they share with their usual analogues.

3.1 Lines

Let's start by discussing lines. Let x and b be elements of $\mathbb{F}_p^2$. A line in $\mathbb{F}_p^2$ is a set of the form $\{mx + b : m \text{ is an element of } \mathbb{F}_p\}$. (**Exercise 6**)



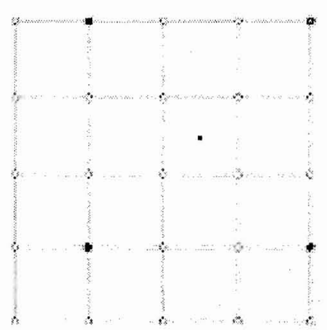
Keep in mind that a "line" in $\mathbb{F}_p^2$ consists only of the points in $\mathbb{F}_p^2$. We can connect the points in $\mathbb{F}_p^2$ with lines, but these line segments are not part of $\mathbb{F}_p^2$!

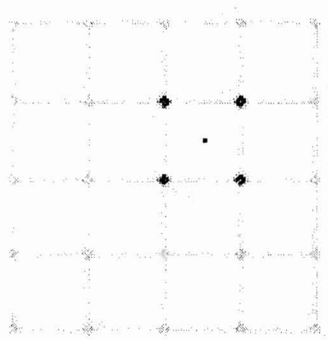
What basic properties do lines have in $\mathbb{F}_p^2$?

- How many points are on a line in $\mathbb{F}_p^2$?
- At how many points can two nonparallel lines intersect?
- Do two points determine a line?
- Is the slope of a line uniquely determined?

3.2 Circles

Recall that a circle in a plane centered at the point (x_0, y_0) with radius r is described by all the solutions (x, y) to $(x - x_0)^2 + (y - y_0)^2 = r^2$. For instance, the set of points $x^2 + y^2 = 1$ describes the circle centered at the origin of radius $\sqrt{1} = 1$. We will take this idea and define a circle in $\mathbb{F}_p^2$ centered at (x_1, y_1) of "radius" t to be all the solutions (x, y) to $(x - x_1)^2 + (y - y_1)^2 = t$. For simplicity, we will always assume that our circles are centered about the origin. We have drawn the circles of radius 2 and 3 in $\mathbb{F}_5$:





Notice that the circles *appear* to be centered at the point $(2.5, 2.5) = (2 + 2^{-1}, 2 + 2^{-1})$. Remembering that $2^{-1} = 3$ in $\mathbb{F}_5$, the circles are really centered at $(2 + 3, 2 + 3) = (0, 0)$ which is the origin! (**Exercises 7 and 8**).

What basic properties do circles have in $\mathbb{F}_p^2$?

- How many points are on a circle in $\mathbb{F}_p^2$?
- At how many points can two circles intersect?
- At how many points can a line and a circle intersect?

4 Exercises

Exercise 1. Write down all the elements of $\mathbb{Z}_{10}$.

Exercise 2. Find:

$$8 + 9 \pmod{10}$$
$$8 \cdot 9 \pmod{10}$$
$$4 + 3 \pmod{10}$$
$$3 \cdot 7 \pmod{10}$$
$$4 \cdot 5 \pmod{10}$$

Exercise 3. Find all the zero divisors of $\mathbb{Z}_8$ and $\mathbb{Z}_7$ (Remember 0 is not a zero divisor!) For what values of n does $\mathbb{Z}_n$ NOT have zero divisors?

Exercise 4. Find the inverse of $2, 3$, and 6 in $\mathbb{F}_7$.

Exercise 5. Write out all the elements of $\mathbb{F}_3^2$ and $\mathbb{F}_5^2$.

Exercise 6. Draw four different lines in $\mathbb{F}_7^2$. How many points does each line have?

Exercise 7. Draw the circles in $\mathbb{F}_7^2$ of radius 3 and 4 centered at the origin

Exercise 8. Draw the circle in $\mathbb{F}_5^2$ of radius 0 centered at the origin. How many points are on this circle?

5 Further Reading in Number Theory and Geometric Combinatorics

- Alex Iosevich, "A View From The Top" (2007)
- Ivan Niven, Herbert Zuckerman, Hugh Montgomery, "An Introduction to the Theory of Numbers" (1991)
- Tom Apostol, "Introduction to Analytic Number Theory (Undergraduate Texts in Mathematics)" (1976)
- Julia Garibaldi, Alex Iosevich, Steven Senger, "The Erdos Distance Problem" (2011)

⋆ Rudolf Lidl, Harald Niederreiter, "Introduction to Finite Fields" (2000)

⋆ Kenneth Ireland, Michael Rosen, "A Classical Introduction to Modern Number Theory (Graduate Texts in Mathematics)" (1990)