Finite Fields

Andreas Boulios and Nakul Khambhati

April 12, 2024

Finite fields play a crucial role in the realm of cryptography. Through this worksheet, we aim to understand and explore some of the qualities that make finite fields useful in cryptography as well as to gain some intuition on how to work with them. The finite nature of these constructs along with many properties, some of which are often shared with the real numbers $\mathbb{R}$, make them the perfect tool for solving problems algorithmically with the use of computers. A great example of a shared and crucial property between finite fields and the real numbers is the fundamental theorem of algebra. Before we delve into that however, we should ask:

1 What is a Field?

Let S be some set (e.g. the letters of the English alphabet or the real numbers $\mathbb{R}$.) where $+$ and $\cdot$ are well defined as functions. Their input is any pair of "numbers" in S: (a, b) and their output a single "number": $a + b$ and $a \cdot b$ respectively.
In $\mathbb{R}$, for example, under addition the pair (5,3) goes to 3+5, which we know to be 8.
In order to call such a construction a **Field** it will have to satisfy the following axioms:

Axiom 1.1.
Closure of operations:
For a, $b \in S$ then $a + b$ and $a \cdot b \in S$. In other words, adding or multiplying elements in S gives you elements in S.

Axiom 1.2.
Associativity of operations:
For any two elements a and b in S:

- Addition: $(a + b) + c = a + (b + c)$
- Multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

i.e. we can ignore parentheses in addition and multiplication.

Axiom 1.3.
Commutativity of operations:
For any two elements a and b in S:

- Addition: $a + b = b + a$
- Multiplication: $a \cdot b = b \cdot a$

i.e. order doesn't matter in addition and multiplication.

Axiom 1.4.
Identity of addition:
There exists an element $a \in S$ that has the property: $a + x = x$ for all $x \in S$. In the business this symbol goes by the nickname of "zero". From now on we will use the symbol 0 to denote it.

Axiom 1.5.
Identity of multiplication:
There exists an element $a \in S$ that has the property: $a \cdot x = x$ for all $x \in S$. In the business this symbol goes by the nickname of "one". From now on we will use the symbol 1 to denote it.

Axiom 1.6.
Inverse of addition:
For every element a in S we can find some element b in S such that $a + b = 0$, i.e. they sum to the additive identity. Such an element b can be represented as $-a$.

Axiom 1.7.
Inverse of multiplication:
For every element a in S we can find some element b in S such that $a \cdot b = 1$, i.e. they multiply to the multiplicative identity. Such an element b can be represented as a^{-1}.

Axiom 1.8.
Distributivity:
For any $a, b, c \in S$ we have: $a \cdot (b + c) = a \cdot b + a \cdot c$. This describes the mechanism of how addition and multiplication interact.

Problem 1.1.
Which of the following sets along with the usual addition and multiplication define a field? If they don't, which axioms do they break?

1. Integers $\mathbb{Z}$.
2. Rational numbers $\mathbb{Q}$.
3. Real numbers in the interval from 0 to 1?

Could S be finite?

2 Recalling Modular Arithmetic

Theorem 1.
The Division Algorithm:
Given two integers n and m. I can always write: $n = m \cdot q + r$ with q and r integers and $0 \leq r < m$.

When we write $8 \pmod 5 \equiv 3 \pmod 5$ we mean that 8 and 3 have the same remainder r when we divide by 5. Generally, $x \pmod n =$ the remainder from the integer division of x by n.

2.1 Warm-up

Problem 2.1.
Calculate the following:

- $37 \pmod 5 =$
- $12 \pmod 7 =$
- $7! \pmod 7 =$
- $5! \pmod{10} =$

Problem 2.2.
For some $n \in \mathbb{Z}$ what are the possible values of $n \pmod{12}$?

Think of the operation $a \pmod N$ as placing the integer a in one of N categories depending on the remainder it has when we divide it by N.

2.2 Construction

Consider the set $S = \{0, 1, 2, 3, \cdots, N-1\}$, with addition and multiplication defined as follows:
For a, b in S:

- $a +_o b = a + b \pmod N$
- $a \cdot_o b = a \cdot b \pmod N$

In other words, in order to add or multiply two numbers in S we add or multiply normally and consider the result $\pmod N$. This way the result of addition and multiplications of elements in S will be contained in S.
We denote this construction as $\mathbb{Z}_N$. For the rest of the worksheet we will use the normal $+$ and $\cdot$ symbols to refer to $+_o$ and $\cdot_o$

Problem 2.3.
Find the possible values of x in $\mathbb{Z}_{12}$ in each equation with $+$, and $\cdot$ defined as above.

- $x + 8 = 2$
- $x + 3 = 0$
- $6 \cdot x = 0$

- $3 \cdot x = 2$
- $7 \cdot x = 1$ *i.e. what is* 7^{-1} *in* $\mathbb{Z}_{12}$ *?*
- $x^2 = 4$

Problem 2.4.
Is $\mathbb{Z}_{12}$ a field? If not, which axioms does it break?

Recall last time we showed that for integers a, b if $\gcd(a, b) = 1$ then we can find integers u and v with $au + bv = 1$ and vice versa.

Problem 2.5.
Use the statement above to show that for a in $\mathbb{Z}_n$, a has a multiplicative inverse if and only if $\gcd(n, a) = 1$.

Problem 2.6.
In $\mathbb{Z}_5$ find the multiplicative inverse of every non-zero element.

- $1^{-1} =$
- $2^{-1} =$
- $3^{-1} =$
- $4^{-1} =$

Problem 2.7.
In a field every a "number" (element of the field) has to have a multiplicative inverse. What does n have to be in order for $\mathbb{Z}_n$ to be a field?

We found a finite field!

3 Playing with $\mathbb{Z}_p$

For the rest of the problems with p we will denote some prime number.

Problem 3.1.
Show that in $\mathbb{Z}_p$ if $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Problem 3.2.
Use the result above to prove that in $\mathbb{Z}_p$ for $a \neq 0$ if $a \cdot b = a \cdot c$ then $b = c$. (This gives us the ability to cancel on both sides of equations in the field.)

Problem 3.3.
For some element a in $\mathbb{Z}_p$, consider the function $f_a(x)$ defined on the elements of $\mathbb{Z}_p$ with $f_a(x) = x \cdot a$. Show that $f_a(x)$ is one-to-one. (i.e. if $f_a(x) = f_a(y)$ then $x = y$ in $\mathbb{Z}_p$)

Problem 3.4.
With f_a defined above, is it possible for $f_a(x) = x$?

Problem 3.5.
Start with 1 and consider the sequence emerging by iteratively applying f_a. So, $q_0 = 1$, $q_1 = f_a(q_0) = a$, $q_2 = f_a(q_1) = a^2$, $\cdots$. What is the maximum number of distinct elements this sequence can have? If we continue in this manner will we get repetitions in the sequence?

Problem 3.6.
Construct such sequence in $\mathbb{Z}_7$ for $f_3(x) = 3 \cdot x$.

Problem 3.7.
Suppose we follow the same process above until we get a repeat (we don't include the repeat in the sequence). Our sequence will look like $S_1 = \{1, a, a^2, \cdots, a^n\}$ all of which are distinct in $\mathbb{Z}_p$.Prove that if a^{n+1} is in S_1 then $a^{n+1} = 1$.

Problem 3.8.
What is the maximum value of such n?

So, we know that by repeating this process, for some positive number n, we'll get $a^{n+1} = 1$. Let's find the n that gives us this result.

Suppose n **is less than** $p - 1$, which means that my sequence S doesn't include all of the elements in $\mathbb{Z}_p$. We can then choose some $b \notin S$ and iteratively apply the function $f_a(x)$ again until you get a repeat . From this we'll get another sequence $S_2 = \{b, ba, ba^2, \cdots, ba^m\}$.

Problem 3.9.
Show that S_2 also has exactly n elements.

Problem 3.10.
Show that S_2 can't have any elements in common with S_1.

We now have two disjoint sets S_1 and S_2. Suppose we proceed to select an element c in $\mathbb{Z}_p$ that is in neither of the previously constructed sets, and with it we create yet another sequence $S_3 = \{c, ca, ca^2, \cdots, ca^n\}$ which will be similarly disjoint from S_1 and S_2 and will have n elements.
One could continue this process to create sets $S_1, \cdots, S_M$, until there are no more elements in $\mathbb{Z}_p$ to choose from. i.e. $S_1 \cup S_2 \cup \cdots \cup S_M = \mathbb{Z}_p$.

Problem 3.11.
Using the set equation above reach a contradiction and deduce that n has to be $p - 1$.

What we have shown is that for every element a in $\mathbb{Z}_p$, $a^{p-1} = 1$. Also known as **Fermat's Little Theorem**.

4 Polynomials over $\mathbb{Z}_p$

Problem 4.1.
Solve the equation $x^2 - y^2 = 39$ where x, y are integers.

Polynomials:

- Polynomials are expressions/functions of the form $p(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$.
- The degree of a polynomial: $\deg(p(x))$, is the largest power of n that appears as an exponent of x in the polynomial.
- A root of a polynomial is a "number" x_r such that $p(x_r) = 0$

Usually, we think of the coefficients a_i of these polynomials to be real numbers, and the polynomial itself a function from real numbers to real numbers. It turns out that if we restrict the coefficients to be elements of some finite field like $\mathbb{Z}_p$, we can then think of our polynomial as a function from elements of $\mathbb{Z}_p$ to other elements of $\mathbb{Z}_p$.

In fact polynomials retain many of their nice properties this way.

The fundamental theorem of algebra states that **a degree n** $(n > 0)$ **polynomial in the real numbers has at most n roots.** We will investigate if this is true for polynomial over $\mathbb{Z}_p$.

Problem 4.2.
For $p(x), q(x)$ polynomials in $\mathbb{Z}_p$. What is $\deg(p(x) \cdot q(x))$?

Problem 4.3.
For polynomials with coefficients in $\mathbb{Z}_4$ (not a field) find two non-zero polynomials $p(x), q(x)$ with $p(x) \cdot q(x) = 0$

Problem 4.4.
How many roots does $f(x) = x^2 + 1$ have in the real numbers. What about $\mathbb{Z}_5$?

Problem 4.5.
How many roots does $f(x) = x^p - x$ have in $\mathbb{Z}_p$?

Problem 4.6.
Let $p(x) = a_1 \cdot x + b_1$ be a degree 1 polynomial in $\mathbb{Z}_p$. Suppose I give you another non-zero polynomial $g(x) = c_0 + c_1 x + \cdots + c_m x^m$. Prove that you can always find polynomials $q(x)$ and $r(x)$ with $p(x) = g(x) \cdot q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$.

Problem 4.7.
Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ in $\mathbb{Z}_p$. Also let $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ in $\mathbb{Z}_p$. With $n < m$. Prove that you can always find polynomials $q(x)$ and $r(x)$ such that $p(x) = g(x) \cdot q(x) + r(x)$ with $\deg(r(x)) < n$

Problem 4.8.
Use the above two problems to prove the following by induction:
For any two polynomials $p(x)$ and $g(x)$ in $\mathbb{Z}_p$ I can find $q(x)$ and $r(x)$ with $p(x) = g(x) \cdot q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$.

Problem 4.9.
Show that in $\mathbb{Z}_p$ if $f(a) = 0$ then $f(x) = (x - a) \cdot q(x)$ for some $q(x)$.

Problem 4.10.
According to the result above if the polynomial $f(x)$ in $\mathbb{Z}_p$ has 3 roots what is the minimum degree of $f(x)$.

The fundamental theorem of algebra remains true over the finite fields $\mathbb{Z}_p$ as well!