Introduction to Finite Fields

Srinath Mahankali (smahankali10@stuy.edu)

November 2020

1 Motivating Finite Fields

Consider this problem in the integers:

Problem 1

How many ordered pairs of integers (a, b) satisfy $a^2 - 2b^2 = 1$?

While this problem only has to do with integers, it is helpful to factor as $(a - b\sqrt{2})(a + b\sqrt{2})$.

Solution

There are infinitely many ordered pairs (a, b) satisfying this equation. To show this, first observe that $(a, b) = (1, 0)$ works. Next, we claim that if (a, b) satisfies this equation, so does $(3a + 4b, 2a + 3b)$. To see this, observe that

$$(3a + 4b)^2 - 2(2a + 3b)^2 = (9a^2 + 24ab + 16b^2) - 2(4a^2 + 12ab + 9b^2) = a^2 - 2b^2 = 1.$$

Since $(3a + 4b, 2a + 3b)$ is also a solution, we can get infinitely many ordered pairs satisfying this equation.

How did we know that $(3a + 4b, 2a + 3b)$ would also work? The answer lies in our factorization $a^2 - 2b^2 = (a - b\sqrt{2})(a + b\sqrt{2})$, where $a^2 - 2b^2 = 1$. Using the fact that $(3 - 2\sqrt{2})(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2 = 1$, we can multiply the two equations together:

$$\begin{aligned}
\left((a - b\sqrt{2})(3 - 2\sqrt{2})\right)\left((a + b\sqrt{2})(3 + 2\sqrt{2})\right) &= 1 \\
\left((3a + 4b) - (2a + 3b)\sqrt{2}\right)\left((3a + 4b) + (2a + 3b)\sqrt{2}\right) &= 1 \\
(3a + 4b)^2 - 2(2a + 3b)^2 &= 1.
\end{aligned}$$

This is an example where it is helpful to use irrational numbers in a problem that only has to do with integers. Here is the $\pmod{p}$ version of this problem:

Problem 2

Let $p > 2$ be a prime number such that the congruence $x^2 \equiv 2 \pmod{p}$ has no integer solutions. How many ordered pairs of integers (a, b) with $0 \le a, b \le p - 1$ are there such that $a^2 - 2b^2 \equiv 1 \pmod{p}$?

Let's develop a similar technique to solve this problem.

2 Definitions

Before we study finite fields, let's define some important terms.

Definition 1

A **ring** R is a set with two operations $+$ and $\cdot$ satisfying certain properties:

- R is commutative under both addition and multiplication,
- R is associative under both addition and multiplication,
- Multiplication is distributive over addition,
- Every element in R has an additive inverse, and
- R has an additive identity and a multiplicative identity.

A **field** K is a ring such that every nonzero element of K also has a multiplicative inverse.

Definition 2

Let A and B be rings, and let $f : A \to B$ be a function. We say f is a **homomorphism** if the following properties hold:

- $f(a+b) = f(a) + f(b)$,
- $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1_A) = 1_B$.

If f is also a bijection from A to B, we say f is an **isomorphism**. If $A = B$, then we say f is an **endomorphism**. Finally, if f is an isomorphism and an endomorphism, we say f is an **automorphism**.

2.1 Exercises

Exercise 1. List out as many rings and fields as you can.

Exercise 2. Check that for any positive integer $n, \mathbb{Z}/n\mathbb{Z}$ is a ring.

Exercise 3. Check that $\mathbb{R}[x]/(x^2+1)$ is a ring. What does this ring remind you of?

Exercise 4. What are all the automorphisms of $\mathbb{Z}$? What about $\mathbb{C}$?

Exercise 5. Let f and g be endomorphisms of ring A. Prove that $f \circ g$ is also an endomorphism of A.

Exercise 6. Let A be a ring and suppose $\sigma : A \to A$ is an endomorphism. Let $P(x)$ be a polynomial with coefficients in A such that σ fixes the coefficients of P. Prove that $\sigma(P(a)) = P(\sigma(a))$ for all a in A.

3 Primes

The simplest finite field is $\mathbb{Z}/p\mathbb{Z}$, or the integers $\pmod p$.

Theorem 1

The ring $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof

Since the ring axioms hold for $\mathbb{Z}/p\mathbb{Z}$, the only property we need to check is whether every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. Let a be an integer relatively prime to p. Then, using Bezout's Lemma, there exist integers x and y such that $ax + py = 1$. This means $ax \equiv 1 \pmod{p}$, implying that a has a multiplicative inverse $\pmod{p}$.

This means $\mathbb{Z}/p\mathbb{Z}$ is a field! For this reason, it is sometimes denoted $\mathbb{F}_p$.

3.1 Exercises

Exercise 1. Let p be prime, and let $0 < k < p$ be an integer. Prove that $p|\binom{p}{k}$.

Exercise 2 (Frobenius Endomorphism)**.** Let K be a ring containing $\mathbb{F}_p$ for some prime p.

- Prove that the function $f : K \to K$ satisfying $f(a) = a^p$ for all $a \in K$ is an endomorphism.
- Prove that for any nonnegative integer k, the function $f : K \to K$ satisfying $f(a) = a^{p^k}$ for all $a \in K$ is an endomorphism.

Exercise 3 (Fermat's Little Theorem)**.** Let p be a prime. Prove that $a^p = a$ for all $a \in \mathbb{F}_p$.

Exercise 4 (HMMT)**.** Let $z = a + bi$ be a complex number with integer real and imaginary parts $a, b \in \mathbb{Z}$ where $i = \sqrt{-1}$, (i.e. z is a Gaussian integer). If p is an odd prime number, show that the real part of $z^p - z$ is an integer divisible by p.

4 Polynomials

Just like polynomials in $\mathbb{Q}[x], \mathbb{R}[x]$, or $\mathbb{C}[x]$, we can also work with polynomials in $\mathbb{F}_p[x]$.

Theorem 2 (Unique Factorization of Polynomials in $\mathbb{F}_p$)

Let P be a monic polynomial with coefficients in $\mathbb{F}_p$. Then, P can be written as a product of monic irreducible polynomials in exactly one way.

In fact, a similar unique factorization theorem holds for polynomials in $K[x]$, for any field K! The proof of this is almost identical to the proof of the Fundamental Theorem of Arithmetic. Polynomials in $\mathbb{F}_p[x]$ behave similarly to polynomials in $\mathbb{Q}[x], \mathbb{R}[x]$, or $\mathbb{C}[x]$.

Theorem 3 (Factor Theorem)

Let P be a polynomial such that $P(a) = 0$ for some $a \in \mathbb{F}_p$. Then, $x - a$ is a factor of P.

Proof

Using the division algorithm, we can express $P(x)$ as $P(x) = (x - a)Q(x) + R$ for constant R. Setting x equal to a, we see that $R = P(a) = 0$, implying that $P(x) = (x - a)Q(x)$.

In fact, a modified version of the Fundamental Theorem of Algebra is also true!

Theorem 4 (Lagrange's Theorem)

Let P be a polynomial in $\mathbb{F}_p[x]$ and let $d = \deg(P)$. Then, P has at most d roots, counting multiplicity.

Proof

This follows from the Unique Factorization Theorem. Since we are counting multiplicity, it is enough to show that P has at most d linear factors in its factorization into irreducible polynomials. Because each linear factor contributes 1 to the degree of P, which is equal to d, this is clear.

4.1 Exercises

Exercise 1. Factor the polynomial $x^p - x$ completely in $\mathbb{F}_p$. If p is odd, how does $x^{\frac{p-1}{2}} - 1$ factor?

Exercise 2. Let K be a field containing $\mathbb{F}_p$ and let $a \in K$ satisfy $a^p = a$. Prove that $a \in \mathbb{F}_p$. Generalize this statement.

Exercise 3. Fill in the steps to prove the Unique Factorization Theorem. Hint: prove the division algorithm and Bezout's Lemma for polynomials.

5 Problems

Problem 1. Let $f : \mathbb{F}_p \to \mathbb{F}_p$ be a function. Prove that there is some polynomial $P(x)$ with coefficients in $\mathbb{F}_p$ such that $P(a) = f(a)$ for all a in $\mathbb{F}_p$.

Problem 2 (PUMaC)**.** Let n be the number of polynomial functions from the integers modulo 2010 to the integers modulo 2010. If $n = p_1 p_2 \dots p_k$, where the p_i are not necessarily distinct primes, what is $p_1 + p_2 + \cdots + p_k$?

Problem 3 (PUMaC)**.** Suppose $P(x)$ is a degree n monic polynomial with integer coefficients such that 2013 divides $P(r)$ for exactly 1000 values of r between 1 and 2013 inclusive. Find the minimum value of n.

Problem 4 (PUMaC)**.** Let $p(n) = n^4 - 6n^2 - 160$. If a_n is the least odd prime dividing $q(n) = |p(n-30) \cdot p(n+30)|$, find $\sum_{n=1}^{2017} a_n$. ($a_n = 3$ if $q(n) = 0$.)

Problem 5 (Wilson's Theorem)**.** Let p be a prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.

Problem 6 (Evan Chen)**.** Let $p > 5$ be a prime. In terms of p, compute the remainder when

$$\prod_{m=1}^{p-1} (m^2 + 1)$$

is divided by p.

Problem 7. Let p be a prime. Prove that $\mathbb{F}_p$ has a primitive root.

Problem 8 (PUMaC)**.** Given a positive integer k, let $f(k)$ be the sum of the k-th powers of the primitive roots of 73. For how many positive integers $k < 2015$ is $f(k)$ divisible by 73?

Problem 9 (CMIMC)**.** Suppose $a_0, a_1, \dots, a_{2018}$ are integers such that

$$(x^2 - 3x + 1)^{1009} = \sum_{k=0}^{2018} a_k x^k$$

for all real numbers x. Compute the remainder when $a_0^2 + a_1^2 + \cdots + a_{2018}^2$ is divided by 2017.