Field $\mathbb{F}_p$

Number Theory Handout
18 Dec 2022

Definition. A field is a set, equipped with two operations: an **addition operation** $+$, and a **multiplication operation** $\cdot$, such that the following properties are met:

1. $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associativity)
2. $a + b = b + a$ and $a \cdot b = b \cdot a$ (Commutativity)
3. There exists an additive identity (denoted by 0) that satisfies $a + 0 = a$
4. There exists a multiplicative identity (denoted by 1) that satisfies $a \cdot 1 = a$
5. For each a there exists an additive inverse $-a$ such that $a + (-a) = 0$
6. For each $a \neq 0$ there exists a multiplicative inverse a^{-1} such that $a \cdot a^{-1} = 1$
7. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Properties 1 and 2 ensure we can do common sense arithmetic in the set; properties 5 and 6 ensure we can 'invert' elements; property 7 establishes a link between addition and multiplication. Informally,

> **A field is a set in which you can add, subtract, multiply and divide any two elements, except dividing by zero.**

Some obvious fields are $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. However, we did not require a field to have anything to do with $\mathbb{R}$ or $\mathbb{C}$. The definition above allows us to talk about *abstract* sets where $+, \cdot$ may not be exactly the same as those in $\mathbb{C}$. The operations $+, \cdot$ are nothing more than two functions that takes two inputs and spits out an output (and hence, technically, we should write $+(a, b)$ instead of $a + b$, but it doesn't really matter), subject to the conditions required above.

1 The field $\mathbb{F}_p$

Let p be a prime. Consider the set $\{0, \cdots, p-1\}$. Normally, we would write $3 + (p-1) = p + 2$, but let's be sneaky and talk under modulo p, and force $3 + (p-1) = 2$ (i.e. the outputs remain in the same set). This allows us to define a new kind of $+$ and a new kind of $\cdot$, by

$$a + b = (a + b \mod p)$$
$$a \cdot b = (a \cdot b \mod p)$$

where mod p means we take its residue in $\{0, \cdots, p-1\}$. Is this set, under our new $+$ and $\cdot$, considered a field? It certainly obeys properties $1, 2, 3, 4, 5, 7$. How about property 6? Luckily we know for a fact that

> If $p \nmid a$, then there exists b such that $ab \equiv 1 \pmod{p}$. (Why?)

Now that makes this set a field! We denote this set as $\mathbb{F}_p$. We will also rename the elements as $\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$ so that it is clear we are talking about a completely new collection of objects that interact in this new abstract modulo p sense.

Example. Consider $\mathbb{F}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Then

- $\overline{1} + \overline{4} = \overline{5}, \qquad \overline{3} + \overline{6} = \overline{2}, \qquad \overline{4} \cdot \overline{5} = \overline{6}.$
- $\overline{0}$ is the additive identity while $\overline{1}$ is the multiplicative identity.
- $\overline{2}$ and $\overline{4}$ are multiplicative inverses of each other.
- $\overline{2}$ and $\overline{5}$ are additive inverses of each other.

By abstractly defining a field, many properties that may seem obvious have to be re-proven to make sure the common intuition about $\mathbb{R}$ or $\mathbb{C}$ does not mislead us into thinking some property is true:

- $a \cdot 0 = 0$. Proof: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Add $-(a \cdot 0)$ on both sides.
- [1]If $ab = ac$ and $a \neq 0$, then $b = c$. Proof: $b = a^{-1}ab = a^{-1}ac = c$.
- If $ab = 0$ then $a = 0$ or $b = 0$. Proof: Say $a \neq 0$, then multiply a^{-1} on both sides to get $b = 0$. (This property will be called **no zero factors**)

A quick explanation of why the mod 6 integers do not form a field is because $2 \cdot 3 = 0$ in that set, but 2 and 3 are not 0, so it has zero factors!

For any set S, we define $S[x]$ to be the set of polynomials with coefficients in S, i.e. the set of elements in the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

where n is a nonnegative integer (A regular one! Not modulo anything!) and $a_0, \cdots, a_n \in S$.

Proposition. Let F be a field. $F[x]$ is not a field, but it does not have zero factors.

Proof. $F[x]$ is not a field obviously because $x \neq 0$ has no inverse element. To prove that it has no zero factors, let $f(x) = a_n x^n + \cdots$ and $g(x) = b_m x^m + \cdots$ be two nonzero polynomials. Hence $a_n, b_m \neq 0$. Then $f(x)g(x) = (a_n b_m) x^{n+m} + \cdots$, and $a_n b_m \neq 0$ because F has no zero factors! Thus $f(x)g(x)$ cannot be 0. $\square$

[1]If the context is clear we will just write $a \cdot b$ as ab

Also, we can do usual long division on $F[x]$:

Proposition. If $f(x), g(x) \in F[x]$, then there exist unique $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

and $\deg r < \deg g$.

Proof. The existence part comes from the usual procedure of long division. Uniqueness is left as an exercise. $\square$

This leads to a useful theorem that not only applies to $\mathbb{R}$:

Theorem. If $r \in F, f(x) \in F[x]$ satisfies $f(r) = 0$. then $f(x) = (x-r)g(x)$ for some $g(x) \in F[x]$.

Proof. By doing long division we get $f(x) = (x-r)q(x) + r(x)$ where $\deg r < 1$ and thus r is a constant. r must be 0 since $f(r) = 0$. $\square$

Theorem. If $f(x) \in F[x]$, then $f(x) = 0$ has at most $\deg f$ solutions.

Proof. Say r is a root of $f(x) = 0$. Then $f(x) = (x-r)g(x)$. If there were some other root $r_2 \neq r$, then $f(r_2) = (r_2 - r)g(r_2) = 0$ implies $g(r_2) = 0$ since F has no zero factors. But $\deg g = \deg f - 1$. Induction (Every time we have a new root, degree falls by one). $\square$

Example. Let $p > 2$ be prime. Prove that the coefficient of x^{p-2} in $(x-1)\cdots(x-p+1)$ is divisible by p.

Proof. Take $(x-1)\cdots(x-p+1) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_0$ into $\mathbb{F}_p[x]$ by simply replacing 1 by $\overline{1}$ and so on. The resultant polynomial is

$$(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p}+\overline{1}) = \overline{1}x^{p-1} + \overline{a_{p-2}}x^{p-2} + \cdots + \overline{a_0}.$$

However, we know that the polynomial $\overline{1}x^{p-1} - \overline{1}$ also has roots $\overline{1}, \cdots, \overline{p-1}$ by Fermat's Little Theorem. By comparing degrees we must have the following!

$$(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p}+\overline{1}) = \overline{1}x^{p-1} - \overline{1}$$

That means $\overline{a_0} = -\overline{1}$ and $\overline{a_1} = \cdots = \overline{a_{p-2}} = 0$. Taking back to $\mathbb{Z}$ we must have $p \mid a_{p-2}$. $\square$

The above proof also immediately proves that $(p-1)! \equiv -1 \pmod{p}$. Do you see why?

Eisenstein's Criterion for Irreducibility. If $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ satisfies

- $p \nmid a_n$;
- $p \mid a_{n-1}, a_{n-2}, \cdots, a_0$;
- $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Assume $f(x) = g(x)h(x)$. Bring into $\mathbb{F}_p$ gives $\overline{a_n}x^n = \overline{g}(x)\overline{h}(x)$, so by looking at roots and degrees, $\overline{g}(x) = \overline{a}x^k$ and $\overline{h}(x) = \overline{b}x^{n-k}$. This means $g(x) = ax^k + (\text{multiples of } p)$ and $h(x) = bx^{n-k} + (\text{multiples of } p)$. This is impossible if $\deg g, \deg h > 0$ because otherwise p^2 divides the constant term of $f(x)$. $\square$

2 Building Larger Fields

Given a field F, we can insert some new element and generate a bigger field. Such an element must be a root of an irreducible polynomial in $F[x]$. We won't explain this further[2] except giving a few examples:

Example. Consider $\mathbb{F}_7$. Note that $x^2 - \overline{3}$ is irreducible in $\mathbb{F}_7[x]$, so we can let $\sqrt{3}$ be a new element that is a root of $x^2 - \overline{3}$ and add it into $\mathbb{F}_7$. Since we want a field we must also include all numbers of the form $a + b\sqrt{3}$ where $a, b \in \mathbb{F}_7$. Let's check that the set formed

$$\mathbb{F}_7[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{F}_7\}$$

is a field. In fact, that's your job. $\square$

What if we add something like a root of $x^2 - \overline{2}$? Unfortunately that's not possible, because $x^2 - \overline{2} = (x - \overline{3})(x + \overline{3})$ and hence in the end you're just 'adding in $\overline{3}$ (or $\overline{4}$)' after all, keeping $\mathbb{F}_7$ as $\mathbb{F}_7$.

3 An IMO Example

IMOSL2003N7. The sequence $a_0, a_1, a_2, \cdots$ is defined as follows:

$$a_0 = 2, \quad a_{k+1} = 2a_k^2 - 1 \qquad \text{for } k \geq 0$$

Prove that if an odd prime p divides a_n, then 2^{n+3} divides $p^2 - 1$.

Proof. By substituting $a_n = \cosh x_n$ we can simplify (try it) a_n to

$$a_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}$$

Case 1. If $x^2 - 3$ is reducible mod p, we treat $\sqrt{3}$ as that root (so $\sqrt{3}$ is some mod p integer! Weird.) and bring the entire expression above into $\mathbb{F}_p$. Since $p \mid a_n$,

$$(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n} = 0$$

[2]If you're really interested, it's about looking at $F[x]$ mod that irreducible polynomial, so it's like $\mathbb{Z}$ mod primes all over again but with a higher level of abstraction.

Multiply both sides by $(2+\sqrt{3})^{2^n}$, then $(2+\sqrt{3})^{2^{n+1}} = -1$ and thus 2^{n+2} is the order of $2+\sqrt{3}$ in $\mathbb{F}_p$ (see Problem 1 of the Exercises). Therefore $2^{n+2} \mid |\mathbb{F}_p| - 1 = p-1$ and thus $2^{n+3} \mid p^2 - 1$.

Case 2. If $x^2 - 3$ is irreducible, work in the enlarged field $\mathbb{F}[\sqrt{3}]$, which has size p^2. Similarly, we get that the order of $2+\sqrt{3}$ is 2^{n+2}. Therefore $2^{n+2} \mid |\mathbb{F}_p[\sqrt{3}]| - 1 = p^2 - 1$. But this is not enough... Let's find some $u \in \mathbb{F}_p[\sqrt{3}]$ such that $u^2 = 2+\sqrt{3}$. If that's the case then the order of u is 2^{n+3} and it would work. Now $2(2+\sqrt{3}) = (1+\sqrt{3})^2$ and so it suffices to find some v such that $v^2 = \frac{1}{2}$. Notice that in $\mathbb{F}_p[\sqrt{3}]$, $a_n = 0 = 2a_{n-1}^2 - 1$ and thus $a_{n-1}^2 = \frac{1}{2}$. $\square$

4 Exercise

1. Prove that if F is a finite field, then $x^{|F|-1} = 1$ for any nonzero $x \in F$. Also if n is the order of x (the smallest positive integer n such that $x^n = 1$), then n divides $|F| - 1$. (Mimic the proof for Fermat's Little Theorem)

2. Prove that if $p > 3$ is a prime then p^2 divides the numerator of

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

3. Prove that p divides the $2p(p^2-1)$-th Fibonacci number ($F_1 = F_2 = 1, F_{n+1} = F_n + F_{n-1}$).

4. Prove that $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Z}[x]$.

5. Find the remainder of

$$\prod_{k=0}^{p-1}(k^2+1)$$

when divided by p.