MAT4006: Introduction to Coding Theory

Lecture 04: The Ring $\mathbb{Z}_m$, Field Characteristic, Finite Field Sizes

Instructor: Zitan Chen
Scribe: Siqi Yao

Spring 2025

1 The Ring $\mathbb{Z}_m$

Definition 4.1 (Congruence)

Let $a, b, m > 1$ be integers (a, b are arbitrary). We say a is **congruent** to b modulo m, written as

$$a \equiv b \pmod{m}$$

if $m \mid (a - b)$, i.e., m divides $(a - b)$.

Remarks

1. **Division with remainder:** Given a and $m > 1$, we have

$$a = qm + b,$$

   where $q, b \in \mathbb{Z}$, $0 \leq b \leq m - 1$, and b is **uniquely** determined by a and m.

   Note: $a - b = qm$

   Therefore, any integer a is congruent to exactly one of $0, 1, \ldots, m - 1$ modulo m.

2. The integer b is called the **remainder** of a divided by m, denoted by $(a \pmod{m})$.

   We also have

$$a \equiv (a \pmod{m}) \pmod{m}.$$

3. **Properties of the modulo operation:**

   If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\begin{cases} a \pm c \equiv b \pm d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

Definition 4.2 (The Ring $\mathbb{Z}_m$)

For $m > 1$, we denote by $\mathbb{Z}_m$ (also written as $\mathbb{Z}/(m)$ or $\mathbb{Z}/m\mathbb{Z}$) the set

$$\{0, 1, \dots, m-1\}$$

and define addition "+" and multiplication "·" in $\mathbb{Z}_m$ by

- For $a, b \in \mathbb{Z}_m$,

$$\begin{aligned} a + b &:= \text{the remainder of } a + b \text{ divided by } m \\ &= (a + b \pmod{m}) \\ a \cdot b &:= (a \cdot b \pmod{m}) \end{aligned}$$

One can show that $(\mathbb{Z}_m, +, \cdot)$ is a ring.

Example: The Ring $\mathbb{Z}_4$

We consider the ring $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Addition table in $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication table in $\mathbb{Z}_4$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Is $\mathbb{Z}_4$ a field?

No. To be a field, every nonzero element must have a multiplicative inverse.
The set of nonzero elements of $\mathbb{Z}_4$ is

$$\mathbb{Z}_4^* = \mathbb{Z}_4 \setminus \{0\} = \{1, 2, 3\}.$$

$\mathbb{Z}_4^*$ has a multiplicative identity: 1.

We need to check whether every element in $\mathbb{Z}_4^*$ has a multiplicative inverse in $\mathbb{Z}_4$:

- $1 \cdot 1 \equiv 1 \pmod{4}$, so 1 has inverse 1.
- $3 \cdot 3 \equiv 9 \equiv 1 \pmod{4}$, so 3 has inverse 3.
- $2 \cdot x$ equals 2 or 0 for $x = 1, 2, 3$, so 2 does **not** have a multiplicative inverse in $\mathbb{Z}_4$.

Therefore, not every nonzero element has a multiplicative inverse, so $\mathbb{Z}_4$ is **not** a field.

Theorem 4.1

$\mathbb{Z}_m$ is a field if and only if m is a prime.

Proof. Suppose m is composite, i.e.,

$$m = a \cdot b \quad \text{where} \quad 0 < a, b < m.$$

Note that

$$m \equiv 0 \pmod{m}.$$

Then,

$$a \cdot b \equiv 0 \pmod{m}$$

$\Rightarrow a \cdot b = 0$ ("$\cdot$" is the multiplication defined in $\mathbb{Z}_m$)
Since $a \neq 0$, $b \neq 0$, but for any field, $a \cdot b = 0$ implies $a = 0$ or $b = 0$, which is a contradiction. Thus, $\mathbb{Z}_m$ cannot be a field when m is composite.

Suppose m is prime.
We need to show $\mathbb{Z}_m^*$ (the set of nonzero elements in $\mathbb{Z}_m$) is an abelian group under multiplication.
It suffices to show that for every $a \in \mathbb{Z}_m^*$, the element a has a multiplicative inverse.
Since $\gcd(m, a) = 1$ (because m is prime and $a \neq 0$), by Bézout's identity, there exist integers u, v such that

$$ua + vm = \gcd(a, m) = 1.$$

Taking both sides mod m, we get

$$ua \equiv 1 \pmod{m}$$

so u is the multiplicative inverse of a in $\mathbb{Z}_m$.
Therefore, every nonzero element in $\mathbb{Z}_m$ has a multiplicative inverse, and thus $\mathbb{Z}_m$ is a field when m is prime. $\square$

2 Field Characteristic

Recall

For a ring $(R, +, \cdot)$, an integer $n \geq 1$ (where n not necessarily $\in R$) and $a \in R$, we denote the n-th additive power of a by $n \cdot a$, i.e.,

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ times}} = \sum_{i=1}^{n} a$$

Definition 4.3 (Characteristic)

Let F be a field. The **characteristic** of F, denoted $\text{char}(F)$, is the least positive integer p such that

$$p \cdot 1 = 0$$

where 1 is the multiplicative identity of F.
If no such positive integer exists, then the characteristic is defined to be 0.
Note: $p \cdot 1 = 0 \implies p \cdot a = 0$ for all $a \in F$

Theorem 4.2

$\text{char}(F)$ is either 0 or a prime.

Proof. We will show that $\text{char}(F)$ cannot be 1 or any composite number.

It is clear that $1 \cdot 1 \neq 0$, so 1 cannot be the characteristic of any field.

Suppose $p = \text{char}(F)$, and p is composite. Then $p = nm$ for integers $1 < n, m < p$.

Let $a = n \cdot 1$, $b = m \cdot 1$. Clearly, $a, b \in F$ (n, m themselves are not necessarily elements of F!)

Now,

$$a \cdot b = (n \cdot 1)(m \cdot 1) = \left(\sum_{i=1}^{n} 1\right)\left(\sum_{j=1}^{m} 1\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} 1 = nm \cdot 1 = p \cdot 1 = 0.$$

Since F is a field, $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

But if $a = 0$, this means $n \cdot 1 = 0$ in F, so the characteristic of F would be $n < p$, contradicting minimality of p. Similarly for b.

Therefore, p cannot be composite, so the characteristic of any field is either 0 or a prime. □

3 Finite Field Sizes

Theorem 4.3

A finite field F of characteristic p contains p^n elements for some integer $n \geq 1$.

Proof. Let $F \neq \varnothing$, so $F \supseteq \{0, 1\}$.

Choose $\alpha_1 \in F^* = F \setminus \{0\}$.

We claim that $0 \cdot \alpha_1, 1 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1$ are all distinct (Note the repetition: $p \cdot \alpha_1 = 0, \quad (p+1) \cdot \alpha_1 = 1 \cdot \alpha_1$).

Indeed, suppose $i \cdot \alpha_1 = j \cdot \alpha_1$ for $0 \leq i \leq j \leq p-1$. Then

$$(j - i) \cdot \alpha_1 = 0.$$

As $\text{char}(F) = p$, $\alpha_1 \neq 0$, we must have $j - i = 0$. Otherwise $j - i$ should be the characteristic of F since $0 < j - i < p$. Thus, $i = j$, so all p elements are distinct.

If $F = \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1\}$, then $|F| = p$ and we are done.

Otherwise, choose $\alpha_2 \in F \setminus \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \dots, (p-1) \cdot \alpha_1\}$.

We claim that all elements of the form $a_1\alpha_1 + a_2\alpha_2$, for $0 \le a_1, a_2 \le p-1$, are distinct.

Suppose $a_1\alpha_1 + a_2\alpha_2 = b_1\alpha_1 + b_2\alpha_2$ for some $0 \le a_1, b_1, a_2, b_2 \le p-1$. Then

$$(a_1 - b_1)\alpha_1 = (b_2 - a_2)\alpha_2.$$

Suppose $b_2 - a_2 \neq 0$. Then

$$\alpha_2 = (b_2 - a_2)^{-1}(a_1 - b_1)\alpha_1,$$

which contradicts the choice of α_2 (since it would then be in the span of α_1). Thus, $b_2 = a_2$ and $a_1 = b_1$.

Since $|F| < \infty$, we can continue in this way to obtain $\alpha_1, \dots, \alpha_n$ such that

$$\alpha_i \in F \setminus \{a_1\alpha_1 + \dots + a_{i-1}\alpha_{i-1} \mid a_1, \dots, a_{i-1} \in \mathbb{Z}_p\}$$

for all $2 \le i \le n$ and

$$F = \{a_1\alpha_1 + \dots + a_n\alpha_n \mid a_1, \dots, a_n \in \mathbb{Z}_p\}.$$

Thus,

$$|F| = p^n.$$

$\square$