

Definitions & Examples of Integral Domains

An **integral domain** D is a **commutative ring with unity** ($1 \neq 0$) that contains **no zero divisors**. This means:

- 1. **Commutative:** $ab = ba$ for all $a, b \in D$.
- 2. **Unity (Multiplicative Identity):** There exists $1 \neq 0$ such that $a \cdot 1 = a$ for all $a \in D$.
- 3. **No Zero Divisors:** If $ab = 0$, then either $a = 0$ or $b = 0$.

This property allows for the **cancellation law**: If $ax = ay$ and $a \neq 0$, then $x = y$.

1. Example: \mathbb{Z} (Integers)

- The integers \mathbb{Z} form a **commutative ring** under usual addition and multiplication.
- It has **unity** 1, since $a \cdot 1 = a$.
- It has **no zero divisors**, because if $ab = 0$ in \mathbb{Z} , then either $a = 0$ or $b = 0$.

✔ Thus, \mathbb{Z} is an **integral domain**.

2. Example: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (Field Examples)

- The rational numbers \mathbb{Q} , real numbers \mathbb{R} , and complex numbers \mathbb{C} are **commutative rings with unity (1)**.
- These fields have **no zero divisors**, since in a field, every nonzero element has a multiplicative inverse.
- Since fields automatically satisfy the integral domain properties, every **field is an integral domain**.

✔ Thus, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are **integral domains**.

3. Example: Polynomials over a Field $F[x]$

- The ring of polynomials $F[x]$ over a field F (e.g., $\mathbb{R}[x]$ or $\mathbb{Q}[x]$) consists of all polynomials with coefficients in F .
- It is **commutative** with **unity** 1.
- It has **no zero divisors**: If $f(x)g(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$.

✔ Thus, $\mathbb{Q}[x], \mathbb{R}[x]$, and $\mathbb{C}[x]$ are **integral domains**.

Non-Examples (Rings that are Not Integral Domains)

- 1. \mathbb{Z}_6 (Integers Modulo 6)
 - It is a **commutative ring** with unity 1.
 - But it has **zero divisors**: $2 \times 3 = 0 \pmod 6$.
 - Since it has zero divisors, it is **not** an integral domain.
- 2. $M_2(\mathbb{R})$ (The Ring of 2×2 Matrices)
 - It is a **ring with unity** (the identity matrix I).
 - But it is **not commutative** (matrix multiplication is not always commutative).
 - It has **zero divisors**: Nonzero matrices can multiply to zero.
 - Since it fails multiple properties, it is **not an integral domain**.

Summary Table

Structure	Commutative?	Unity?	No Zero Divisors?	Integral Domain?
\mathbb{Z} (Integers)	✔	✔	✔	✔
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (Fields)	✔	✔	✔	✔
$\mathbb{Q}[x], \mathbb{R}[x]$ (Polynomials over a Field)	✔	✔	✔	✔
\mathbb{Z}_6 (Integers Mod 6)	✔	✔	✗ (e.g., $2 \times 3 = 0$)	✗
$M_2(\mathbb{R})$ (Matrices)	✗	✔	✗	✗

Section 19: Integral Domains (2025.02.13)

19.8 Example Show that although \mathbb{Z}_2 is an integral domain, the matrix ring $M_2(\mathbb{Z}_2)$ has divisors of zero.

Solution We need only observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \quad \blacktriangle$$

Our next theorem shows that the structure of a field is still the most restrictive (that is, the richest) one we have defined.

To show that \mathbb{Z}_2 (the ring of integers modulo 2) is an integral domain, we need to verify the following properties:

- 1. **Commutativity:** \mathbb{Z}_2 is a commutative ring.
- 2. **Existence of Multiplicative Identity:** \mathbb{Z}_2 has a multiplicative identity.
- 3. **No Zero Divisors:** If $a \cdot b = 0$ in \mathbb{Z}_2 , then either $a = 0$ or $b = 0$.

Step 1: Commutativity

\mathbb{Z}_2 is a commutative ring because multiplication in \mathbb{Z}_2 is commutative. The elements of \mathbb{Z}_2 are $\{0, 1\}$, and the multiplication table is:

\cdot	0	1
0	0	0
1	0	1

From the table, it is clear that $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}_2$.

Step 2: Multiplicative Identity

The multiplicative identity in \mathbb{Z}_2 is 1, because:

$$1 \cdot 0 = 0 \quad \text{and} \quad 1 \cdot 1 = 1.$$

Thus, 1 acts as the multiplicative identity.

Step 3: No Zero Divisors

To show that \mathbb{Z}_2 has no zero divisors, we check all possible products of nonzero elements. The only nonzero element in \mathbb{Z}_2 is 1, and:

$$1 \cdot 1 = 1 \neq 0.$$

Thus, there are no zero divisors in \mathbb{Z}_2 .

Conclusion

Since \mathbb{Z}_2 is a commutative ring with a multiplicative identity and no zero divisors, it is an integral domain.

Additional Note

In fact, \mathbb{Z}_2 is also a field because every nonzero element has a multiplicative inverse. The inverse of 1 is 1 itself, since $1 \cdot 1 = 1$. This further reinforces that \mathbb{Z}_2 is an integral domain.

Section 19: Integral Domains (2025.02.13)

To explain why every field is an integral domain, we need to recall the definitions of a **field** and an **integral domain** and show that the properties of a field satisfy the conditions of an integral domain.

Definitions

- 1. **Field:** A field F is a commutative ring with a multiplicative identity $1 \neq 0$, and every nonzero element in F has a multiplicative inverse. In other words, for every $a \in F$ with $a \neq 0$, there exists $b \in F$ such that $a \cdot b = 1$.
- 2. **Integral Domain:** An integral domain is a commutative ring with a multiplicative identity $1 \neq 0$ and no zero divisors. That is, if $a \cdot b = 0$ in the ring, then either $a = 0$ or $b = 0$.

Why Every Field is an Integral Domain

Let F be a field. We need to show that F satisfies the conditions of an integral domain:

- 1. **Commutativity:** By definition, a field is a commutative ring.
- 2. **Multiplicative Identity:** A field has a multiplicative identity $1 \neq 0$.
- 3. **No Zero Divisors:** Suppose $a \cdot b = 0$ in F . If $a \neq 0$, then a has a multiplicative inverse a^{-1} . Multiplying both sides of $a \cdot b = 0$ by a^{-1} gives:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \implies (a^{-1} \cdot a) \cdot b = 0 \implies 1 \cdot b = 0 \implies b = 0.$$

Thus, if $a \cdot b = 0$, either $a = 0$ or $b = 0$. This shows that F has no zero divisors.

Since F satisfies all the conditions of an integral domain, every field is an integral domain.

Examples of Fields (and Integral Domains)

Here are several examples of fields, which are also integral domains:

- 1. **\mathbb{Q} (Rational Numbers):**
 - \mathbb{Q} is a field because every nonzero rational number $\frac{a}{b}$ has a multiplicative inverse $\frac{b}{a}$.
 - It is also an integral domain because it has no zero divisors.
- 2. **\mathbb{R} (Real Numbers):**
 - \mathbb{R} is a field because every nonzero real number has a multiplicative inverse.
 - It is also an integral domain because it has no zero divisors.

3. \mathbb{C} (Complex Numbers):

- \mathbb{C} is a field because every nonzero complex number $a + bi$ has a multiplicative inverse.
- It is also an integral domain because it has no zero divisors.

4. \mathbb{Z}_p (Integers Modulo p , where p is prime):

- \mathbb{Z}_p is a field because every nonzero element has a multiplicative inverse (since p is prime).
- It is also an integral domain because it has no zero divisors.

5. \mathbb{F}_4 (Finite Field with 4 Elements):

- \mathbb{F}_4 is a field because it is a finite field where every nonzero element has a multiplicative inverse.
- It is also an integral domain because it has no zero divisors.

19.9 Theorem Every field F is an integral domain.

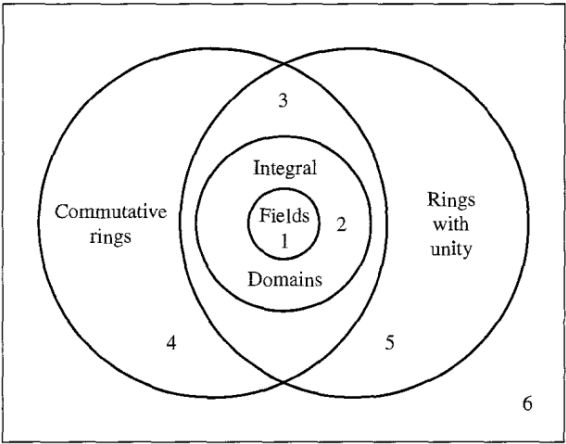
Proof Let $a, b \in F$, and suppose that $a \neq 0$. Then if $ab = 0$, we have

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0.$$

But then

$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b.$$

We have shown that $ab = 0$ with $a \neq 0$ implies that $b = 0$ in F , so there are no divisors of 0 in F . Of course, F is a commutative ring with unity, so our theorem is proved. ♦



19.10 Figure A collection of rings.

19.12 Corollary If p is a prime, then \mathbb{Z}_p is a field.

Proof This corollary follows immediately from the fact that \mathbb{Z}_p is an integral domain and from Theorem 19.11. ♦

To show that \mathbb{Z}_5 is a **field**, we need to verify that every **nonzero element** in \mathbb{Z}_5 has a **multiplicative inverse** (i.e., for each $a \neq 0$, there exists some b such that $a \cdot b \equiv 1 \pmod{5}$).

Step 1: Define \mathbb{Z}_5

The elements of \mathbb{Z}_5 are:

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

with addition and multiplication performed modulo 5.

Since \mathbb{Z}_5 is a ring with unity 1, we now check that every **nonzero** element has a multiplicative inverse.

Step 2: Find Multiplicative Inverses

For each $a \in \{1, 2, 3, 4\}$, we need to find b such that:

$$a \cdot b \equiv 1 \pmod{5}$$

1. Inverse of 1

$$1 \cdot 1 = 1 \equiv 1 \pmod{5}$$

Thus, $1^{-1} \equiv 1 \pmod{5}$.

2. Inverse of 2

We seek b such that:

$$2b \equiv 1 \pmod{5}$$

Checking possible values:

- $2 \times 1 = 2$
- $2 \times 2 = 4$
- $2 \times 3 = 6 \equiv 1 \pmod{5}$

Thus, $2^{-1} \equiv 3 \pmod{5}$.

3. Inverse of 3

We seek b such that:

$$3b \equiv 1 \pmod{5}$$

Checking possible values:

- $3 \times 1 = 3$
- $3 \times 2 = 6 \equiv 1 \pmod{5}$

Thus, $3^{-1} \equiv 2 \pmod{5}$.

4. Inverse of 4

We seek b such that:

$$4b \equiv 1 \pmod{5}$$

Checking possible values:

- $4 \times 1 = 4$
- $4 \times 2 = 8 \equiv 3 \pmod{5}$
- $4 \times 3 = 12 \equiv 2 \pmod{5}$
- $4 \times 4 = 16 \equiv 1 \pmod{5}$

Thus, $4^{-1} \equiv 4 \pmod{5}$.

Step 3: Conclusion

The multiplicative inverses in \mathbb{Z}_5 are:

$$\begin{aligned} 1^{-1} &\equiv 1 \pmod{5}, \\ 2^{-1} &\equiv 3 \pmod{5}, \\ 3^{-1} &\equiv 2 \pmod{5}, \\ 4^{-1} &\equiv 4 \pmod{5}. \end{aligned}$$

Since every nonzero element has an inverse, \mathbb{Z}_5 is a **field**.

19.13 Definition If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring R** . If no such positive integer exists, then R is of **characteristic 0**. ■

We shall be using the concept of a characteristic chiefly for fields. Exercise 29 asks us to show that the characteristic of an integral domain is either 0 or a prime p .

19.14 Example The ring \mathbb{Z}_n is of characteristic n , while \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} all have characteristic 0. ▲

Theorem Explanation

- Characteristic 0:**
 - If $n \cdot 1 \neq 0$ for all positive integers n , then the ring R has **characteristic 0**.
 - This means that no matter how many times you add 1 to itself, you will never get 0. This is typical of infinite rings like \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} .
- Characteristic n :**
 - If $n \cdot 1 = 0$ for some positive integer n , then the **smallest such n** is called the **characteristic of R** .
 - This means that adding 1 to itself n times results in 0. This is typical of finite rings like \mathbb{Z}_n (the ring of integers modulo n).

Key Points

- The characteristic of a ring is determined by the additive order of the multiplicative identity 1.
- If $n \cdot 1 = 0$, then n is the smallest positive integer for which this holds. If no such n exists, the characteristic is 0.
- The characteristic of a ring is always either 0 or a prime number p . This is because if n is composite, the ring would have zero divisors, which is not allowed in integral domains or fields.

Examples

- Characteristic 0:**
 - **Ring:** \mathbb{Z} (integers).
 - Explanation: For any positive integer n , $n \cdot 1 = n \neq 0$. Thus, \mathbb{Z} has characteristic 0.
 - **Ring:** \mathbb{Q} (rational numbers).
 - Explanation: No positive integer n satisfies $n \cdot 1 = 0$, so \mathbb{Q} has characteristic 0.
 - **Ring:** \mathbb{R} (real numbers).
 - Explanation: Similar to \mathbb{Q} , no positive integer n satisfies $n \cdot 1 = 0$, so \mathbb{R} has characteristic 0.

Section 19: Integral Domains (2025.02.13)

2. Characteristic n :

- **Ring:** \mathbb{Z}_n (integers modulo n).
 - Explanation: In \mathbb{Z}_n , $n \cdot 1 = 0$, and n is the smallest such positive integer. Thus, \mathbb{Z}_n has characteristic n .
 - Example: \mathbb{Z}_5 has characteristic 5 because $5 \cdot 1 = 0$ in \mathbb{Z}_5 .
- **Ring:** \mathbb{Z}_p (integers modulo p , where p is prime).
 - Explanation: In \mathbb{Z}_p , $p \cdot 1 = 0$, and p is the smallest such positive integer. Thus, \mathbb{Z}_p has characteristic p .
 - Example: \mathbb{Z}_7 has characteristic 7 because $7 \cdot 1 = 0$ in \mathbb{Z}_7 .

3. Characteristic p (Prime):

- **Ring:** \mathbb{F}_p (finite field with p elements, where p is prime).
 - Explanation: In \mathbb{F}_p , $p \cdot 1 = 0$, and p is the smallest such positive integer. Thus, \mathbb{F}_p has characteristic p .
 - Example: \mathbb{F}_3 has characteristic 3 because $3 \cdot 1 = 0$ in \mathbb{F}_3 .

Why Characteristic is Important

1. Behavior of the Ring:

- The characteristic determines how the ring behaves under repeated addition of the multiplicative identity.
- For example, in a ring of characteristic p , the equation $p \cdot a = 0$ holds for all elements a in the ring.

2. Fields and Integral Domains:

- In fields and integral domains, the characteristic is either 0 or a prime number p . This is because if the characteristic were composite, the ring would have zero divisors, which is not allowed in these structures.

Summary

- The characteristic of a ring R with unity is the smallest positive integer n such that $n \cdot 1 = 0$. If no such n exists, the characteristic is 0.
- Examples of characteristic 0 include \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} .
- Examples of characteristic n include \mathbb{Z}_n and finite fields \mathbb{F}_p (where p is prime).
- The characteristic is a fundamental property that influences the structure and behavior of the ring.

Section 20: Fermat’s and Euler’s Theorems (2025.02.14)

The statement "the order of any element in a group divides the order of the group" is a direct consequence of **Lagrange's Theorem**. Lagrange's Theorem states that for any finite group G , the order (size) of any subgroup H of G divides the order of G . Since the cyclic subgroup generated by an element $a \in G$ is a subgroup of G , the order of a (the size of this cyclic subgroup) must divide the order of G .

Explanation

1. Order of an Element:

- The **order of an element** a in a group G is the smallest positive integer k such that $a^k = e$, where e is the identity element of G .
- If no such k exists, the element has infinite order.

2. Order of a Group:

- The **order of a group** G is the number of elements in G , denoted $|G|$.

3. Lagrange's Theorem:

- If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$.
- The cyclic subgroup generated by a , denoted $\langle a \rangle$, has order equal to the order of a . Thus, the order of a divides $|G|$.

Demonstration in \mathbb{Z}_n

The group \mathbb{Z}_n (integers modulo n under addition) is a cyclic group of order n . The elements of \mathbb{Z}_n are $\{0, 1, 2, \dots, n - 1\}$, and the group operation is addition modulo n .

Key Properties of \mathbb{Z}_n :

1. The **order of** \mathbb{Z}_n is n .
2. The **order of an element** k in \mathbb{Z}_n is the smallest positive integer d such that $d \cdot k \equiv 0 \pmod{n}$.
3. The order of k is $\frac{n}{\gcd(k,n)}$, where $\gcd(k,n)$ is the greatest common divisor of k and n .

Section 20: Fermat’s and Euler’s Theorems (2025.02.14)

Example 1: \mathbb{Z}_6

- The group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has order 6.
- We compute the order of each element:

Element k	$\gcd(k, 6)$	Order $d = \frac{6}{\gcd(k, 6)}$
0	6	$\frac{6}{6} = 1$
1	1	$\frac{6}{1} = 6$
2	2	$\frac{6}{2} = 3$
3	3	$\frac{6}{3} = 2$
4	2	$\frac{6}{2} = 3$
5	1	$\frac{6}{1} = 6$

- Observations:
 - The orders of the elements are 1, 6, 3, 2, 3, 6, all of which divide 6.
 - The identity element 0 has order 1, and the generators of \mathbb{Z}_6 (elements 1 and 5) have order 6

Example 2: \mathbb{Z}_8

- The group $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ has order 8.
- We compute the order of each element:

Element k	$\gcd(k, 8)$	Order $d = \frac{8}{\gcd(k, 8)}$
0	8	$\frac{8}{8} = 1$
1	1	$\frac{8}{1} = 8$
2	2	$\frac{8}{2} = 4$
3	1	$\frac{8}{1} = 8$
4	4	$\frac{8}{4} = 2$
5	1	$\frac{8}{1} = 8$
6	2	$\frac{8}{2} = 4$
7	1	$\frac{8}{1} = 8$

- Observations:
 - The orders of the elements are 1, 8, 4, 8, 2, 8, 4, 8, all of which divide 8.
 - The identity element 0 has order 1, and the generators of \mathbb{Z}_8 (elements 1, 3, 5, 7) have order 8.

Section 20: Fermat’s and Euler’s Theorems (2025.02.14)

- Observations:
 - The orders of the elements are 1, 8, 4, 8, 2, 8, 4, 8, all of which divide 8.
 - The identity element 0 has order 1, and the generators of \mathbb{Z}_8 (elements 1, 3, 5, 7) have order 8.

General Case

For any \mathbb{Z}_n :

- The order of an element k is $\frac{n}{\gcd(k, n)}$.
- Since $\gcd(k, n)$ divides n , the order of k must divide n .

Fermat's Little Theorem

Statement:

If p is a prime number and a is any integer not divisible by p , then:

$$a^{p-1} \equiv 1 \pmod{p}$$

Equivalently, for any integer a :

$$a^p \equiv a \pmod{p}$$

Explanation

The theorem tells us that when we raise an integer a to the power of $p - 1$ and divide by p , the remainder is always 1 (as long as p is prime and a is not a multiple of p).

This property arises from number theory, particularly group theory and modular arithmetic. In simple terms, the theorem leverages the fact that the nonzero integers modulo p form a **multiplicative group** of order $p - 1$, where every element has an inverse.

Examples

Example 1: Verify for $p = 5, a = 2$

$$2^{5-1} = 2^4 = 16$$

$$16 \pmod{5} = 1$$

Since $16 \div 5 = 3$ remainder **1**, we confirm:

$$2^4 \equiv 1 \pmod{5}$$

Example 2: Verify for $p = 7, a = 3$

$$3^{7-1} = 3^6 = 729$$

$$729 \pmod{7} = 1$$

Since $729 \div 7 = 104$ remainder **1**, we confirm:

$$3^6 \equiv 1 \pmod{7}$$

Example 3: Verify for $p = 11, a = 4$

$$4^{11-1} = 4^{10} = 1048576$$

Computing modulo 11:

$$4^2 = 16 \equiv 5 \pmod{11}$$

$$4^4 = (4^2)^2 = 5^2 = 25 \equiv 3 \pmod{11}$$

$$4^8 = (4^4)^2 = 3^2 = 9 \pmod{11}$$

$$4^{10} = 4^8 \cdot 4^2 = 9 \cdot 5 = 45 \equiv 1 \pmod{11}$$

Thus, we confirm:

$$4^{10} \equiv 1 \pmod{11}$$

Example 4: Alternative Form $a^p \equiv a \pmod{p}$ for $p = 7, a = 5$

$$5^7 = 78125$$

Computing modulo 7:

$$5^2 = 25 \equiv 4 \pmod{7}$$

$$5^4 = (5^2)^2 = 4^2 = 16 \equiv 2 \pmod{7}$$

$$5^6 = (5^4) \cdot (5^2) = 2 \cdot 4 = 8 \equiv 1 \pmod{7}$$

Multiplying by 5:

$$5^7 = 5^6 \cdot 5 = 1 \cdot 5 \equiv 5 \pmod{7}$$

Thus, we confirm:

$$5^7 \equiv 5 \pmod{7}$$

Why Fermat's Little Theorem Works

1. **Group Theory Perspective:**

- The nonzero integers modulo p form a multiplicative group of order $p - 1$.
- By Lagrange's Theorem, the order of any element in this group divides $p - 1$. Thus, $a^{p-1} \equiv 1 \pmod{p}$.

2. **Modular Arithmetic:**

- The theorem relies on the properties of modular arithmetic and the fact that prime numbers have no nontrivial divisors.

Section 20: Fermat’s and Euler’s Theorems (2025.02.14)

We need to show that for every integer n , the number $n^{33} - n$ is divisible by 15. This means proving:

$$n^{33} - n \equiv 0 \pmod{15}$$

Since $15 = 3 \times 5$, it suffices to prove:

$$n^{33} - n \equiv 0 \pmod{3} \quad \text{and} \quad n^{33} - n \equiv 0 \pmod{5}.$$

Step 1: Modulo 3

By **Fermat’s Little Theorem**, for any integer n , we know:

$$n^2 \equiv 1 \pmod{3} \quad (\text{if } n \text{ is not divisible by } 3)$$

Raising both sides to the 16th power:

$$n^{32} \equiv 1^{16} \equiv 1 \pmod{3}$$

Multiplying by n :

$$n^{33} \equiv n \pmod{3}$$

Thus,

$$n^{33} - n \equiv 0 \pmod{3}.$$

Step 2: Modulo 5

Similarly, by **Fermat’s Little Theorem**, we have:

$$n^4 \equiv 1 \pmod{5} \quad (\text{if } n \text{ is not divisible by } 5)$$

Raising both sides to the 8th power:

$$n^{32} \equiv 1^8 \equiv 1 \pmod{5}$$

Multiplying by n :

$$n^{33} \equiv n \pmod{5}$$

Thus,

$$n^{33} - n \equiv 0 \pmod{5}.$$


Step 3: Conclusion

Since we have shown:

$$n^{33} - n \equiv 0 \pmod{3} \quad \text{and} \quad n^{33} - n \equiv 0 \pmod{5},$$

it follows that:

$$n^{33} - n \equiv 0 \pmod{15}.$$

Thus, $n^{33} - n$ is always divisible by 15 for any integer n . 

Section 20: Fermat’s and Euler’s Theorems (2025.02.14)

When we say that $p - 1$ is the **order of the multiplicative group of integers modulo p** , we are referring to the group structure formed by the nonzero integers modulo p under multiplication. Let’s break this down in detail:

Multiplicative Group of Integers Modulo p

1. Definition:

- Let p be a prime number.
- The **multiplicative group of integers modulo p** , denoted $(\mathbb{Z}/p\mathbb{Z})^*$ or \mathbb{Z}_p^* , consists of all nonzero integers modulo p :

$$\mathbb{Z}_p^* = \{1, 2, 3, \dots, p - 1\}.$$

- The group operation is **multiplication modulo p** .

2. Group Properties:

- Closure:** For any $a, b \in \mathbb{Z}_p^*$, the product $a \cdot b \pmod{p}$ is also in \mathbb{Z}_p^* .
- Associativity:** Multiplication modulo p is associative.
- Identity Element:** The number 1 is the multiplicative identity, since $a \cdot 1 \equiv a \pmod{p}$ for all $a \in \mathbb{Z}_p^*$.
- Inverses:** For every $a \in \mathbb{Z}_p^*$, there exists a unique $b \in \mathbb{Z}_p^*$ such that $a \cdot b \equiv 1 \pmod{p}$. This b is the **multiplicative inverse** of a .

3. Order of the Group:

- The **order of the group \mathbb{Z}_p^*** is the number of elements in the group, which is $p - 1$ (since 0 is excluded).

Why $p - 1$ is the Order of the Group

- The set $\mathbb{Z}_p^* = \{1, 2, 3, \dots, p - 1\}$ contains $p - 1$ elements.
- Each element in \mathbb{Z}_p^* has a unique multiplicative inverse modulo p , ensuring that the group is well-defined.

Connection to Fermat's Little Theorem

Fermat’s Little Theorem states that for any integer a not divisible by p :

$$a^{p-1} \equiv 1 \pmod{p}.$$

This can be interpreted in terms of the multiplicative group \mathbb{Z}_p^* :

- 1. **Group-Theoretic Interpretation:**
 - The order of the group \mathbb{Z}_p^* is $p - 1$.
 - By **Lagrange’s Theorem**, the order of any element a in \mathbb{Z}_p^* must divide the order of the group, $p - 1$.
 - Therefore, $a^{p-1} \equiv 1 \pmod{p}$.
- 2. **Example:**
 - Let $p = 5$. The multiplicative group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ has order 4.
 - For $a = 2$, compute $2^4 = 16$. Since $16 \equiv 1 \pmod{5}$, Fermat’s Little Theorem holds.

Examples of Multiplicative Groups Modulo p

Example 1: $p = 5$

- The multiplicative group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.
- The order of the group is 4.
- Multiplicative inverses:
 - $2 \cdot 3 \equiv 1 \pmod{5}$, so $2^{-1} \equiv 3 \pmod{5}$.
 - $4 \cdot 4 \equiv 1 \pmod{5}$, so $4^{-1} \equiv 4 \pmod{5}$.

Example 2: $p = 7$

- The multiplicative group $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
- The order of the group is 6.
- Multiplicative inverses:
 - $2 \cdot 4 \equiv 1 \pmod{7}$, so $2^{-1} \equiv 4 \pmod{7}$.
 - $3 \cdot 5 \equiv 1 \pmod{7}$, so $3^{-1} \equiv 5 \pmod{7}$.

Example 3: $p = 11$

- The multiplicative group $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
- The order of the group is 10.
- Multiplicative inverses:
 - $2 \cdot 6 \equiv 1 \pmod{11}$, so $2^{-1} \equiv 6 \pmod{11}$.
 - $3 \cdot 4 \equiv 1 \pmod{11}$, so $3^{-1} \equiv 4 \pmod{11}$.

Key Points

- The multiplicative group \mathbb{Z}_p^* consists of the nonzero integers modulo p , and its order is $p - 1$.
- Fermat’s Little Theorem is a direct consequence of the group structure of \mathbb{Z}_p^* and Lagrange’s Theorem.
- The existence of multiplicative inverses in \mathbb{Z}_p^* is crucial for the theorem to hold.

Summary

The multiplicative group of integers modulo p , denoted \mathbb{Z}_p^* , is a group of order $p - 1$ consisting of the nonzero integers modulo p under multiplication. Fermat’s Little Theorem arises naturally from the properties of this group, and the examples demonstrate how the theorem works in practice.

20.6 Theorem The set G_n of nonzero elements of \mathbb{Z}_n that are not 0 divisors forms a group under multiplication modulo n .

The set G_n of nonzero elements of \mathbb{Z}_n that are not zero divisors forms a group under multiplication modulo n . This group is called the **group of units of \mathbb{Z}_n** and is denoted $(\mathbb{Z}/n\mathbb{Z})^*$ or \mathbb{Z}_n^* . The elements of G_n are precisely the integers modulo n that are **coprime to n** (i.e., their greatest common divisor with n is 1). These elements have multiplicative inverses modulo n , which ensures that G_n is a group.

Properties of G_n

- 1. **Elements:**
 - G_n consists of all integers k in $\{1, 2, \dots, n - 1\}$ such that $\gcd(k, n) = 1$.
- 2. **Group Operation:**
 - The group operation is multiplication modulo n .
- 3. **Identity Element:**
 - The identity element is 1, since $1 \cdot k \equiv k \pmod{n}$ for all $k \in G_n$.
- 4. **Inverses:**
 - Every element $k \in G_n$ has a multiplicative inverse k^{-1} such that $k \cdot k^{-1} \equiv 1 \pmod{n}$.
- 5. **Order of the Group:**
 - The order of G_n is given by Euler's totient function $\phi(n)$, which counts the number of integers in $\{1, 2, \dots, n - 1\}$ that are coprime to n .

Examples

Example 1: $n = 5$

- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
- The nonzero elements that are not zero divisors are $\{1, 2, 3, 4\}$ (since 5 is prime, all nonzero elements are coprime to 5).
- Thus, $G_5 = \{1, 2, 3, 4\}$.
- The group operation is multiplication modulo 5.
- The group is cyclic, and its multiplication table is:

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Observations:
 - Every element has an inverse: $2^{-1} \equiv 3 \pmod{5}$, $3^{-1} \equiv 2 \pmod{5}$, and $4^{-1} \equiv 4 \pmod{5}$.
 - The group is isomorphic to \mathbb{Z}_4 , the cyclic group of order 4.

20.7 Example Let $n = 12$. The positive integers less than or equal to 12 and relatively prime to 12 are 1, 5, 7, and 11, so $\varphi(12) = 4$. ▲

Example 2: $n = 8$

- $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.
 - The nonzero elements that are not zero divisors are those coprime to 8: $\{1, 3, 5, 7\}$.
 - Thus, $G_8 = \{1, 3, 5, 7\}$.
 - The group operation is multiplication modulo 8.
 - The multiplication table is:
- | · | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |
- Observations:
 - Every element has an inverse: $3^{-1} \equiv 3 \pmod{8}$, $5^{-1} \equiv 5 \pmod{8}$, and $7^{-1} \equiv 7 \pmod{8}$.
 - The group is isomorphic to the **Klein four-group** $\mathbb{Z}_2 \times \mathbb{Z}_2$, a non-cyclic group of order 4.

Example 3: $n = 9$

- $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
 - The nonzero elements that are not zero divisors are those coprime to 9: $\{1, 2, 4, 5, 7, 8\}$.
 - Thus, $G_9 = \{1, 2, 4, 5, 7, 8\}$.
 - The group operation is multiplication modulo 9.
 - The group is cyclic, and its multiplication table is:
- | · | 1 | 2 | 4 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 5 | 7 | 8 |
| 2 | 2 | 4 | 8 | 1 | 5 | 7 |
| 4 | 4 | 8 | 7 | 2 | 1 | 5 |
| 5 | 5 | 1 | 2 | 7 | 8 | 4 |
| 7 | 7 | 5 | 1 | 8 | 4 | 2 |
| 8 | 8 | 7 | 5 | 4 | 2 | 1 |
- Observations:
 - Every element has an inverse: $2^{-1} \equiv 5 \pmod{9}$, $4^{-1} \equiv 7 \pmod{9}$, $5^{-1} \equiv 2 \pmod{9}$, $7^{-1} \equiv 4 \pmod{9}$, and $8^{-1} \equiv 8 \pmod{9}$.
 - The group is isomorphic to \mathbb{Z}_6 , the cyclic group of order 6.

Key Points

1. **Formation of G_n :**
 - G_n consists of all integers modulo n that are coprime to n .
 - These elements have multiplicative inverses, making G_n a group under multiplication modulo n .
2. **Order of G_n :**
 - The order of G_n is $\phi(n)$, where ϕ is Euler's totient function.
3. **Structure of G_n :**
 - If n is prime, G_n is cyclic of order $n - 1$.
 - If n is composite, G_n may or may not be cyclic, depending on n .

20.9 Example Let $n = 12$. We saw in Example 20.7 that $\phi(12) = 4$. Thus if we take any integer a relatively prime to 12, then $a^4 \equiv 1 \pmod{12}$. For example, with $a = 7$, we have $7^4 = (49)^2 = 2,401 = 12(200) + 1$, so $7^4 \equiv 1 \pmod{12}$. Of course, the easy way to compute $7^4 \pmod{12}$, without using Euler's theorem, is to compute it in \mathbb{Z}_{12} . In \mathbb{Z}_{12} , we have $7 = -5$ so

$$7^2 = (-5)^2 = (5)^2 = 1 \quad \text{and} \quad 7^4 = 1^2 = 1. \quad \blacktriangle$$

20.8 Theorem (Euler's Theorem) If a is an integer relatively prime to n , then $a^{\phi(n)} - 1$ is divisible by n , that is, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Euler's Theorem

Euler's theorem states that if n is a positive integer and a is an integer such that $\gcd(a, n) = 1$, then:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is Euler's totient function, which counts the number of integers from 1 to n that are coprime to n .

Explanation

Euler's theorem is a generalization of Fermat's Little Theorem, which states that if p is a prime and a is not divisible by p , then:

$$a^{p-1} \equiv 1 \pmod{p}$$

Euler's theorem extends this idea to composite numbers using the Euler totient function.

Proof Outline

1. Consider the set of integers $S = \{x_1, x_2, \dots, x_{\phi(n)}\}$ that are coprime to n .
2. Multiplying all elements by a , which is also coprime to n , produces another set $S' = \{ax_1, ax_2, \dots, ax_{\phi(n)}\}$.
3. Since multiplication by a is a permutation of S modulo n , the product of all elements in S is congruent to the product of all elements in S' modulo n .
4. That is:

$$x_1 x_2 \cdots x_{\phi(n)} \equiv (ax_1)(ax_2) \cdots (ax_{\phi(n)}) \pmod{n}$$

Factoring out $a^{\phi(n)}$, we get:

$$x_1 x_2 \cdots x_{\phi(n)} \equiv a^{\phi(n)} x_1 x_2 \cdots x_{\phi(n)} \pmod{n}$$

5. Since all x_i are coprime to n , their product is also coprime to n , meaning we can cancel it from both sides:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

which proves Euler's theorem.

Examples

Example 1: $n = 10$, $a = 3$

First, compute $\phi(10)$:

$$\phi(10) = 10 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 10 \times \frac{1}{2} \times \frac{4}{5} = 4$$

Now, check Euler's theorem:

$$3^4 \equiv 1 \pmod{10}$$

Computing:

$$\begin{aligned} 3^4 &= 81 \\ 81 \mod 10 &= 1 \end{aligned}$$

Thus, $3^4 \equiv 1 \pmod{10}$, confirming Euler's theorem.

Example 2: $n = 12$, $a = 5$

Compute $\phi(12)$:

$$\phi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4$$

Check Euler's theorem:

$$5^4 \equiv 1 \pmod{12}$$

Computing:

$$\begin{aligned} 5^4 &= 625 \\ 625 \mod 12 &= 1 \end{aligned}$$

Thus, $5^4 \equiv 1 \pmod{12}$, confirming Euler's theorem.

Example 3: $n = 35$, $a = 2$

Compute $\phi(35)$:

$$\phi(35) = 35 \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{7}\right) = 35 \times \frac{4}{5} \times \frac{6}{7} = 24$$

Check Euler's theorem:

$$2^{24} \equiv 1 \pmod{35}$$

Computing:

$$\begin{aligned} 2^{24} &= 16777216 \\ 16777216 \mod 35 &= 1 \end{aligned}$$

Thus, $2^{24} \equiv 1 \pmod{35}$, confirming Euler's theorem.

20.9 Example Let $n = 12$. We saw in Example 20.7 that $\varphi(12) = 4$. Thus if we take any integer a relatively prime to 12, then $a^4 \equiv 1 \pmod{12}$. For example, with $a = 7$, we have $7^4 = (49)^2 = 2,401 = 12(200) + 1$, so $7^4 \equiv 1 \pmod{12}$. Of course, the easy way to compute $7^4 \pmod{12}$, without using Euler's theorem, is to compute it in \mathbb{Z}_{12} . In \mathbb{Z}_{12} , we have $7 = -5$ so

$$7^2 = (-5)^2 = (5)^2 = 1 \quad \text{and} \quad 7^4 = 1^2 = 1. \quad \blacktriangle$$

20.10 Theorem Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m . For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in \mathbb{Z}_m .

Proof By Theorem 20.6, a is a unit in \mathbb{Z}_m and $s = a^{-1}b$ is certainly a solution of the equation. Multiplying both sides of $ax = b$ on the left by a^{-1} , we see this is the only solution. ♦

20.11 Corollary If a and m are relatively prime integers, then for any integer b , the congruence $ax \equiv b \pmod{m}$ has as solutions all integers in precisely one residue class modulo m .

The statement you provided is a fundamental result in modular arithmetic. It says that if m is a positive integer and $a \in \mathbb{Z}_m$ is relatively prime to m (i.e., $\gcd(a, m) = 1$), then for every $b \in \mathbb{Z}_m$, the equation $ax \equiv b \pmod{m}$ has a **unique solution** in \mathbb{Z}_m . This is because a has a **multiplicative inverse** modulo m , which allows us to solve for x .

Explanation

1. Relatively Prime Condition:

- If $\gcd(a, m) = 1$, then a has a multiplicative inverse modulo m . That is, there exists a unique integer a^{-1} such that:

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

2. Solving the Equation:

- The equation $ax \equiv b \pmod{m}$ can be solved by multiplying both sides by a^{-1} :

$$x \equiv a^{-1} \cdot b \pmod{m}.$$

- This gives the unique solution x in \mathbb{Z}_m .

3. Uniqueness:

- The solution is unique because a^{-1} is unique modulo m , and b is fixed.

Examples

Example 1: $m = 5, a = 2, b = 3$

- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
- $a = 2$ is relatively prime to $m = 5$ because $\gcd(2, 5) = 1$.
- The multiplicative inverse of 2 modulo 5 is 3, since $2 \cdot 3 \equiv 6 \equiv 1 \pmod{5}$.
- Solve $2x \equiv 3 \pmod{5}$:

$$x \equiv 2^{-1} \cdot 3 \equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod{5}.$$

- The unique solution is $x = 4$.

Example 2: $m = 7, a = 3, b = 5$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.
- $a = 3$ is relatively prime to $m = 7$ because $\gcd(3, 7) = 1$.
- The multiplicative inverse of 3 modulo 7 is 5, since $3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$.
- Solve $3x \equiv 5 \pmod{7}$:

$$x \equiv 3^{-1} \cdot 5 \equiv 5 \cdot 5 \equiv 25 \equiv 4 \pmod{7}.$$

- The unique solution is $x = 4$.

Example 3: $m = 8, a = 5, b = 7$

- $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.
- $a = 5$ is relatively prime to $m = 8$ because $\gcd(5, 8) = 1$.
- The multiplicative inverse of 5 modulo 8 is 5, since $5 \cdot 5 \equiv 25 \equiv 1 \pmod{8}$.
- Solve $5x \equiv 7 \pmod{8}$:

$$x \equiv 5^{-1} \cdot 7 \equiv 5 \cdot 7 \equiv 35 \equiv 3 \pmod{8}.$$

- The unique solution is $x = 3$.

Example 4: $m = 9, a = 4, b = 2$

- $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
- $a = 4$ is relatively prime to $m = 9$ because $\gcd(4, 9) = 1$.
- The multiplicative inverse of 4 modulo 9 is 7, since $4 \cdot 7 \equiv 28 \equiv 1 \pmod{9}$.
- Solve $4x \equiv 2 \pmod{9}$:

$$x \equiv 4^{-1} \cdot 2 \equiv 7 \cdot 2 \equiv 14 \equiv 5 \pmod{9}.$$

- The unique solution is $x = 5$.

Section 20: Fermat's and Euler's Theorems (2025.02.14)

Why This Works

1. Existence of Inverse:

- If $\gcd(a, m) = 1$, then a has a multiplicative inverse modulo m . This inverse allows us to solve the equation $ax \equiv b \pmod{m}$.

2. Uniqueness:

- The solution $x \equiv a^{-1} \cdot b \pmod{m}$ is unique because a^{-1} is unique modulo m .

3. Relatively Prime Condition:

- If $\gcd(a, m) \neq 1$, then a does not have an inverse modulo m , and the equation $ax \equiv b \pmod{m}$ may have no solution or multiple solutions.

Statement and Explanation

If a and m are relatively prime (i.e., $\gcd(a, m) = 1$), then the congruence equation:

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

has a unique solution modulo m , meaning that all solutions x form a single residue class modulo m .

This result follows from number theory because when $\gcd(a, m) = 1$, a has a multiplicative inverse modulo m , meaning there exists an integer a^{-1} such that:

$$aa^{-1} \equiv 1 \pmod{m}$$

Multiplying both sides of the congruence $ax \equiv b \pmod{m}$ by a^{-1} , we obtain:

$$x \equiv a^{-1}b \pmod{m}$$

Since a^{-1} is unique modulo m , the solution x is unique modulo m as well.

Example 1: $3x \equiv 4 \pmod{7}$

- Since $\gcd(3, 7) = 1$, an inverse of 3 modulo 7 exists.
- The modular inverse of 3 modulo 7 is 5, because:

$$3 \times 5 = 15 \equiv 1 \pmod{7}$$

- Multiplying both sides by 5:

$$x \equiv 5 \times 4 \equiv 20 \pmod{7}$$

$$20 \pmod{7} = 6$$

Thus, the solution is:

$$x \equiv 6 \pmod{7}$$

which means all solutions are of the form:

$$x = 6 + 7k, \quad k \in \mathbb{Z}$$

Section 20: Fermat's and Euler's Theorems (2025.02.14)

Example 2: $7x \equiv 9 \pmod{11}$

- Since $\gcd(7, 11) = 1$, an inverse of 7 modulo 11 exists.
- The modular inverse of 7 modulo 11 is 8, because:

$$7 \times 8 = 56 \equiv 1 \pmod{11}$$

- Multiplying both sides by 8:

$$x \equiv 8 \times 9 \equiv 72 \pmod{11}$$

$$72 \pmod{11} = 6$$

Thus, the solution is:

$$x \equiv 6 \pmod{11}$$

which means all solutions are of the form:

$$x = 6 + 11k, \quad k \in \mathbb{Z}$$

Example 3: $5x \equiv 7 \pmod{12}$

- Since $\gcd(5, 12) = 1$, an inverse of 5 modulo 12 exists.
- The modular inverse of 5 modulo 12 is 5, because:

$$5 \times 5 = 25 \equiv 1 \pmod{12}$$

- Multiplying both sides by 5:

$$x \equiv 5 \times 7 \equiv 35 \pmod{12}$$

$$35 \pmod{12} = 11$$

Thus, the solution is:

$$x \equiv 11 \pmod{12}$$

which means all solutions are of the form:

$$x = 11 + 12k, \quad k \in \mathbb{Z}$$

Examples and Explanation

Example 1: $6x \equiv 9 \pmod{15}$

- Compute $d = \gcd(6, 15) = 3$.
- Since 3 divides 9, solutions exist.
- Divide by 3:

$$2x \equiv 3 \pmod{5}$$

- The modular inverse of 2 modulo 5 is 3, so multiplying both sides by 3:

$$x \equiv 3 \times 3 \equiv 9 \equiv 4 \pmod{5}$$

- Since $d = 3$, the solutions form three residue classes:

$$x \equiv 4, 4 + 5, 4 + 10 \pmod{15}$$

$$x \equiv 4, 9, 14 \pmod{15}$$

So, the solutions are $x = 4, 9, 14$.

20.13 Corollary Let d be the gcd of positive integers a and m . The congruence $ax \equiv b \pmod{m}$ has a solution if and only if d divides b . When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m .

20.14 Example Find all solutions of the congruence $12x \equiv 27 \pmod{18}$.

Solution The gcd of 12 and 18 is 6, and 6 is not a divisor of 27. Thus by the preceding corollary, there are no solutions. ▲

20.15 Example Find all solutions of the congruence $15x \equiv 27 \pmod{18}$.

Solution The gcd of 15 and 18 is 3, and 3 does divide 27. Proceeding as explained before Example 20.14, we divide everything by 3 and consider the congruence $5x \equiv 9 \pmod{6}$, which amounts to solving the equation $5x = 3$ in \mathbb{Z}_6 . Now the units in \mathbb{Z}_6 are 1 and 5, and 5 is clearly its own inverse in this group of units. Thus the solution in \mathbb{Z}_6 is $x = (5^{-1})(3) = (5)(3) = 3$. Consequently, the solutions of $15x \equiv 27 \pmod{18}$ are the integers in the three residue classes.

$$3 + 18\mathbb{Z} = \{\dots, -33, -15, 3, 21, 39, \dots\},$$

$$9 + 18\mathbb{Z} = \{\dots, -27, -9, 9, 27, 45, \dots\}.$$

$$15 + 18\mathbb{Z} = \{\dots, -21, -3, 15, 33, 51, \dots\},$$

Example 2: $8x \equiv 6 \pmod{10}$

- Compute $d = \gcd(8, 10) = 2$.
- Since 2 divides 6, solutions exist.
- Divide by 2:

$$4x \equiv 3 \pmod{5}$$

- The modular inverse of 4 modulo 5 is 4, so multiplying both sides:

$$x \equiv 4 \times 3 \equiv 12 \equiv 2 \pmod{5}$$

- Since $d = 2$, the solutions form two residue classes:

$$x \equiv 2, 2 + 5 \pmod{10}$$

$$x \equiv 2, 7 \pmod{10}$$

So, the solutions are $x = 2, 7$.

Example 3: $9x \equiv 12 \pmod{18}$

- Compute $d = \gcd(9, 18) = 9$.
- Since 9 does **not** divide 12, **no solutions exist**.

Conclusion

- The congruence $ax \equiv b \pmod{m}$ has a solution **if and only if** $\gcd(a, m)$ divides b .
- When a solution exists, there are exactly d different residue classes modulo m , where $d = \gcd(a, m)$.
- The key steps are:
 1. Compute $d = \gcd(a, m)$.
 2. Check if d divides b .
 3. Reduce the equation and solve modulo m/d .
 4. Extend to d distinct solutions in \mathbb{Z}_m .

Understanding the Corollary (20.13)

This corollary is a direct consequence of Theorem 20.12. It states:

- 1. The congruence equation:

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

has a solution **if and only if** $d = \gcd(a, m)$ divides b . This means that if b is not a multiple of d , no solutions exist.

- 2. If d does divide b , then the solutions form exactly d **distinct residue classes modulo** m . That is, the solutions differ by multiples of m/d but cover d different values modulo m .

Explanation of the Claims

- 1. **Why Must d Divide b ?**

- The equation $ax \equiv b \pmod{m}$ is equivalent to the Diophantine equation:

$$ax - b = km$$

- Since d divides both a and m , it must also divide b for a solution to exist.

- 2. **Why Are There Exactly d Residue Classes?**

- If d divides b , we can divide the entire equation by d :

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

- Since $\gcd(a/d, m/d) = 1$, the new equation has a **unique solution modulo** m/d .
- However, in modulo m , solutions will repeat every m/d , forming d distinct residue classes.

20.12 Theorem Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let d be the gcd of a and m . The equation $ax = b$ has a solution in \mathbb{Z}_m if and only if d divides b . When d divides b , the equation has exactly d solutions in \mathbb{Z}_m .

Understanding the Theorem (20.12)

The theorem states that for a given modulus m , an equation of the form:

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

has a solution **if and only if** the greatest common divisor $d = \gcd(a, m)$ divides b . Moreover, if d divides b , then there are exactly d distinct solutions modulo m .

This result generalizes the case when $\gcd(a, m) = 1$, in which case there is always exactly **one** solution modulo m , as guaranteed by the existence of a modular inverse.

Explanation of the Claims

- 1. **Existence of a Solution:**

- The equation $ax \equiv b \pmod{m}$ can be rewritten as:

$$ax - b = km$$

for some integer k .

- This is a linear Diophantine equation in two variables (x and k), which has integer solutions if and only if the greatest common divisor $d = \gcd(a, m)$ divides b .

- 2. **Number of Solutions:**

- If d divides b , we can divide the equation by d , transforming it into a simpler congruence:

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

- Since $\gcd(a/d, m/d) = 1$, the new equation has a unique solution modulo m/d .
- However, the original modulus was m , and since solutions repeat every m/d , there are exactly d solutions in \mathbb{Z}_m .

Examples and Explanation

Example 1: $6x \equiv 9 \pmod{15}$

- Compute $d = \gcd(6, 15) = 3$.
- Since 3 divides 9, the equation has solutions.
- Divide the entire equation by 3:

$$2x \equiv 3 \pmod{5}$$

- Find the unique solution for x modulo 5. The modular inverse of 2 modulo 5 is 3, so multiplying both sides by 3:

$$x \equiv 3 \times 3 \equiv 9 \equiv 4 \pmod{5}$$

- Since the original equation has $d = 3$ solutions, they are:

$$x \equiv 4, 4 + 5, 4 + 10 \pmod{15}$$

$$x \equiv 4, 9, 14 \pmod{15}$$

Thus, the solutions are $x = 4, 9, 14$.

Example 2: $8x \equiv 6 \pmod{10}$

- Compute $d = \gcd(8, 10) = 2$.
- Since 2 divides 6, solutions exist.
- Divide by 2:

$$4x \equiv 3 \pmod{5}$$

- Find the unique solution modulo 5. The inverse of 4 modulo 5 is 4, so multiplying both sides:

$$x \equiv 4 \times 3 \equiv 12 \equiv 2 \pmod{5}$$

- Since $d = 2$, the solutions are:

$$x \equiv 2, 2 + 5 \pmod{10}$$

$$x \equiv 2, 7 \pmod{10}$$

So, the solutions are $x = 2, 7$.

Example 3: $9x \equiv 12 \pmod{18}$

- Compute $d = \gcd(9, 18) = 9$.
- Since 9 divides 12 **is false**, no solutions exist.
- This shows a case where the equation has **no solutions**.

Conclusion

- The congruence $ax \equiv b \pmod{m}$ has a solution **if and only if** $\gcd(a, m)$ divides b .
- If a solution exists, there are exactly d distinct solutions modulo m , where $d = \gcd(a, m)$.
- The key steps in solving these equations involve:
 1. Computing $d = \gcd(a, m)$.
 2. Checking if d divides b .
 3. Reducing the equation and solving modulo m/d .
 4. Using periodicity to find all d solutions.