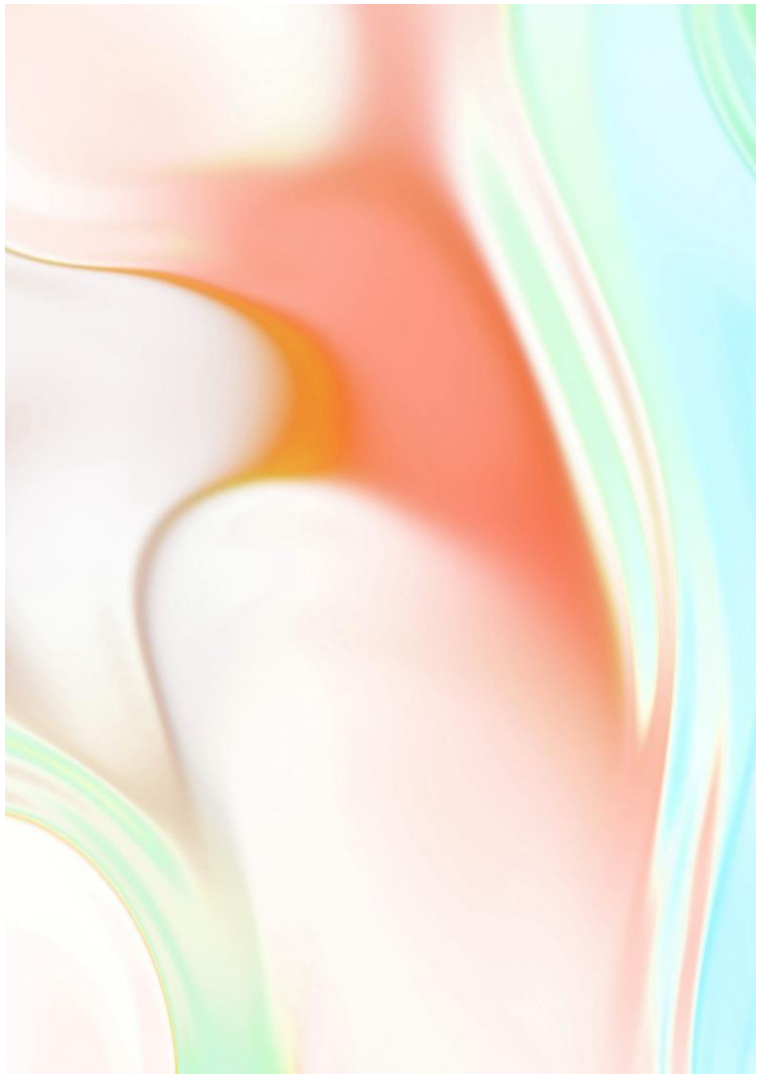
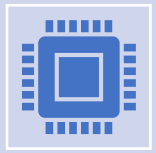
Discrete Mathematics
Lecture 4
Introduction to Number Theory

Lecturer: Kahenya, N.P



Introduction to lecture 4

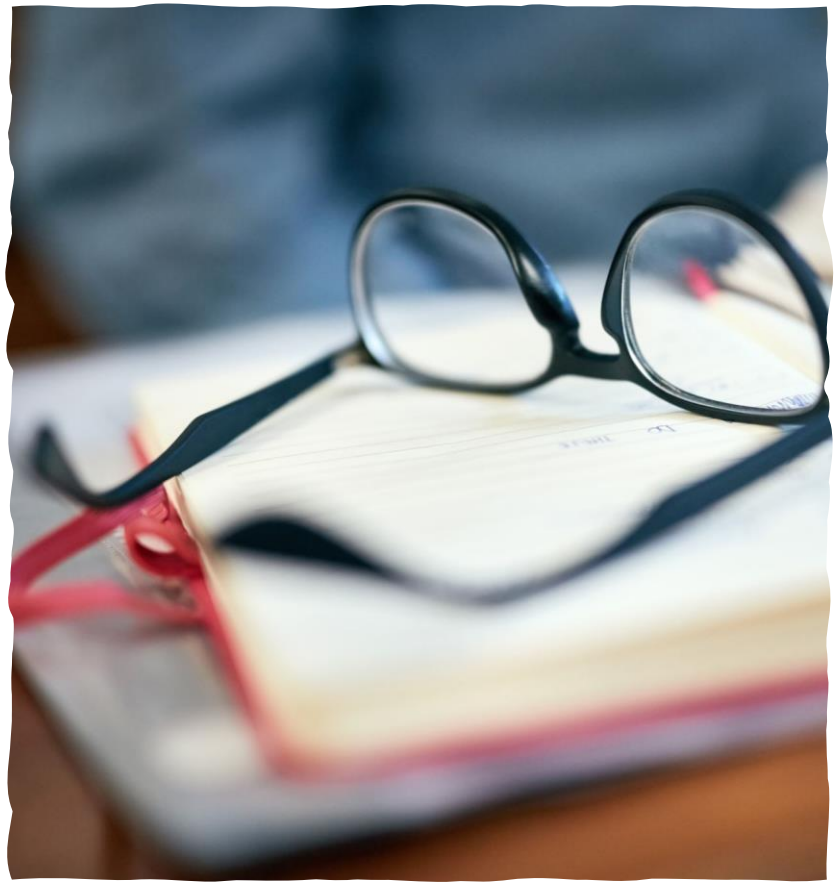


This lecture introduces concepts in basic number theory that are used in computer science.

The lecture will introduce the concepts of modular arithmetic, Euclidean algorithm, linear congruences, and its application in cryptography.

This lecture forms a foundation to a later topic on mathematical proofs.

References



These lecture notes have been derived from the following sources, Susanna (2003), Rosen (2011), and Rosen (2012).

Intended learning outcomes

Be	At the end of this lecture, you will be able to;
Define	Define key concepts in number theory.
Apply	Apply the key concepts in solving problems.

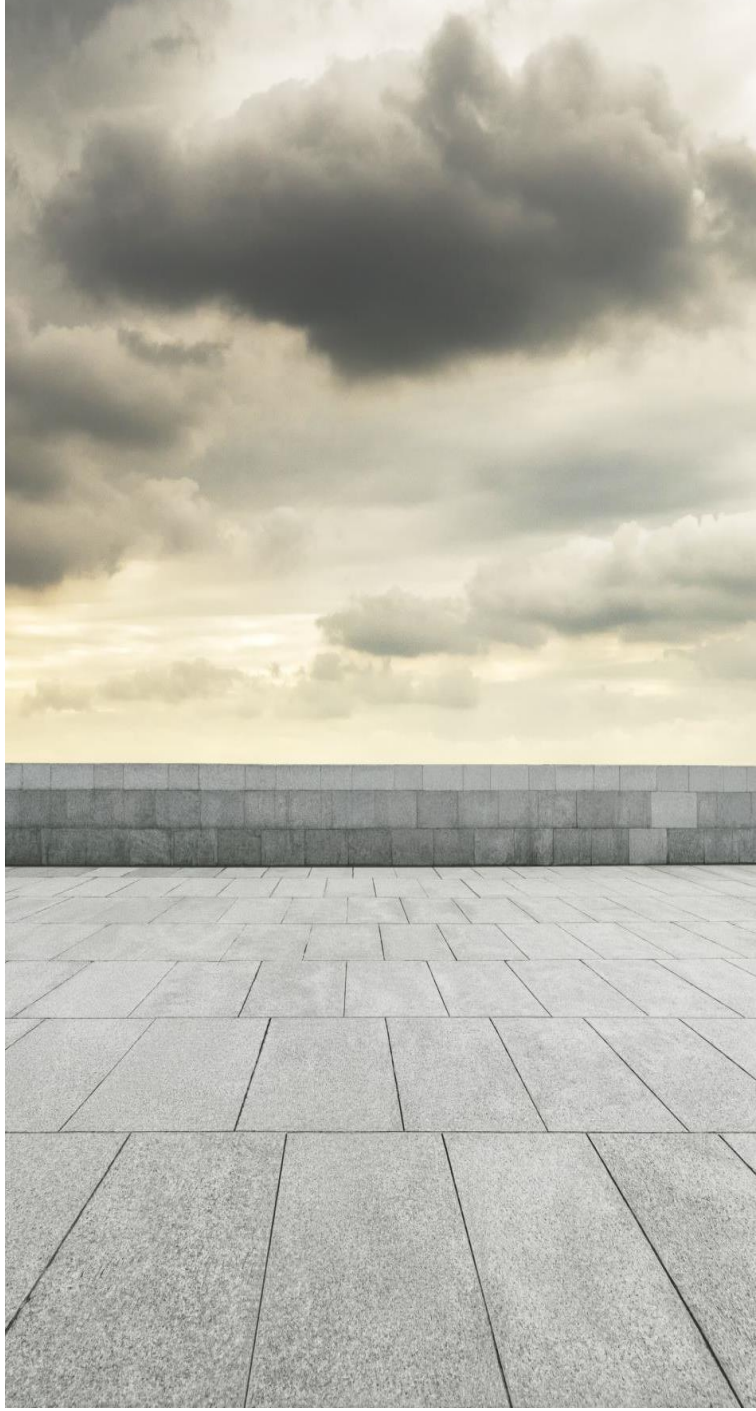
Definition of terms

Division

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.

- Then a is a factor or divisor of b and that b is a multiple of a.

- The notation $a|b$ denotes a divides b. Otherwise $a \nmid b$ i.e., a does not divide b.



Theorem 1: (The Division Algorithm)

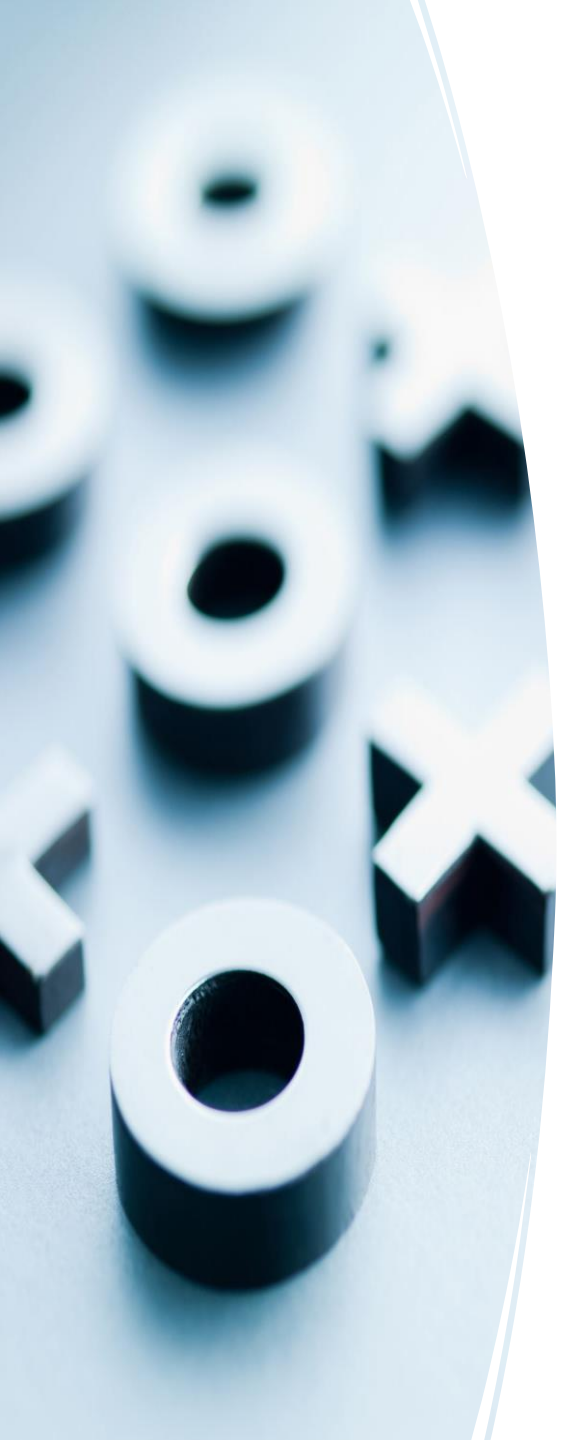
- Let $a \in \mathbb{Z}$ i.e., be an integer and $a \in \mathbb{Z}^+$ i.e., a positive integer. Then there are unique integers q and r with $0 \leq r < d$, such that

$$a = dq + r.$$

- a is called the dividend, d is the divisor, q is the quotient, r is the remainder.

- The algorithm can be used to express the quotient q and the remainder r as follows;

$$\mathrm{q} \equiv \mathrm{a} \operatorname{div} \mathrm{d}$$
$$\mathrm{r} \equiv \mathrm{a} \bmod \mathrm{d}$$



Example 1

Find the quotient and the remainder when 97 is divided by 5

Solution: $97 = 5 \times 19 + 2$

The quotient is $q = 19$ and the remainder $r = 2$.

Thus, we have;

$19 \equiv 97 \text{ div } 5$

$2 \equiv 97 \pmod 5$

Example 2

Find the quotient and the remainder when -17 is divided by 3

Solution: $-17 = 3 \times (-6) + 1$

Quotient is $q = -6$; Remainder $r = 1$.

Thus, we have; $-6 \equiv -17 \text{ div } 3$ or $1 \equiv -17 \pmod 3$.

Remark: We can have $-17 = 3 \times (-5) - 2$.

This is not acceptable since $r < 0$, it cannot be a negative value since from definition of division algorithm we have $0 \leq r < d$.

Definition

If a and b are integers and m is a positive integer, then

$a \equiv b \pmod{m}$ if $m|(a-b)$.

Example: Consider $17 \equiv 3 \bmod 7 \Rightarrow 7|(17-3) = 7|14$.

Theorem

Let a and b be integers and let m be a positive integer.

Then; $a \equiv b \pmod{m}$ iff $a \pmod{m} = b \pmod{m}$

Example : Given $2 \equiv 14 \bmod 12$ is $2 \bmod 12 = 14 \bmod 12$?

Solution: Note that $12|14 - 12 \Rightarrow 12|2$ also $2|14 - 12 \Rightarrow 2|2$.

Hence, True.

Theorem

Let m be a positive integer. The integers a and b congruent modulo m if and only if there is an integer k such that $a = km + b$.

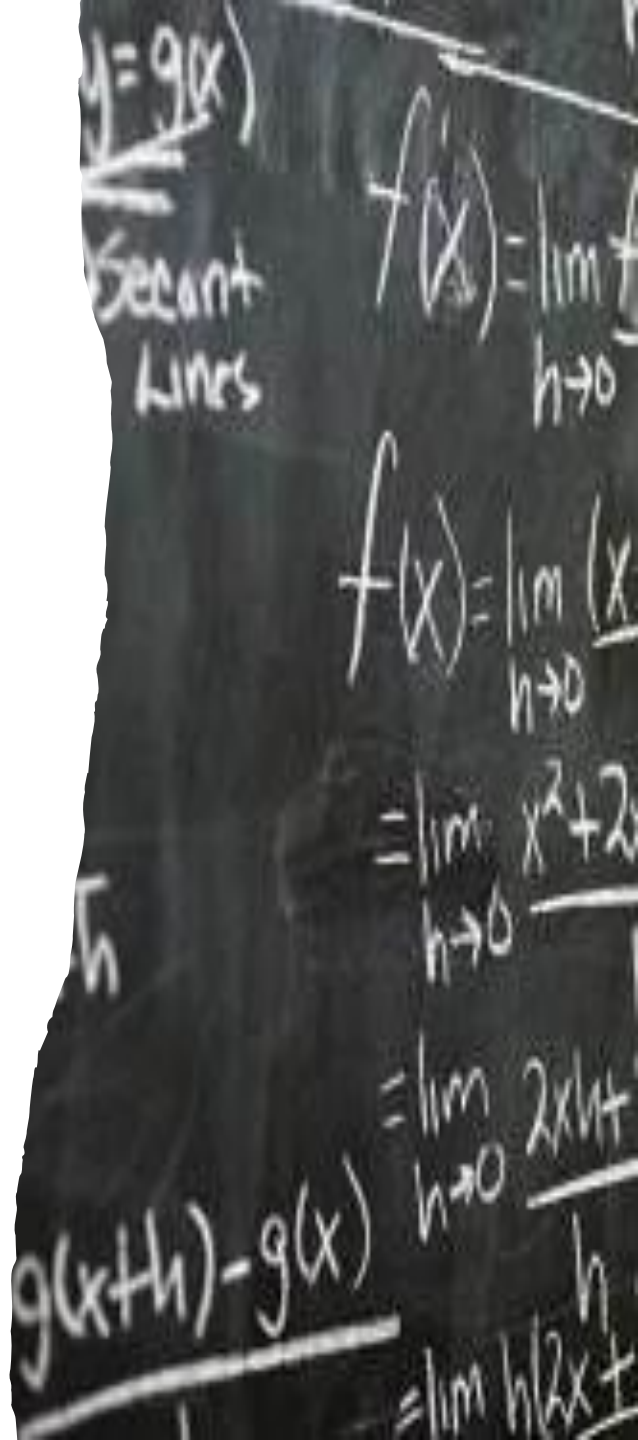
Proof

If $a \equiv b(mod\ m)$ by definition of congruence, we have $m|(a - b)$.

This implies that there exists an integer k such that $(a - b) = km$ => $a = b + km$.

Conversely, if there exists an integer k such that $a = b + km$ then $km = a - b$

Hence m divides $a - b$ such that $a \equiv b(mod\ m)$.

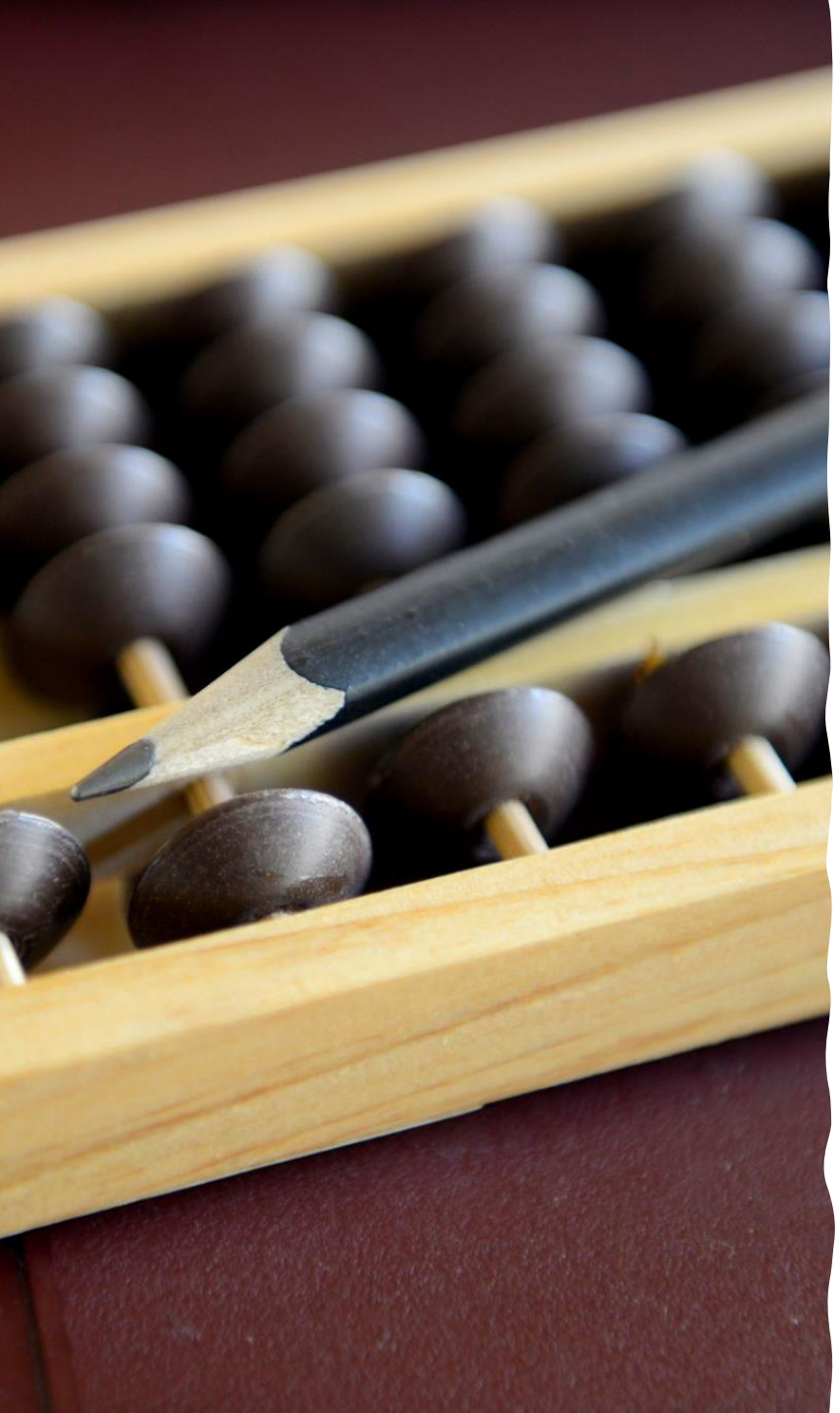


Theorem

Let m be a positive integer.

If a ≡ b(mod m) and c ≡ d(mod m), then a + c ≡ (b +d)(mod m) and

ac ≡ (bd)(mod m)



Arithmetic modulo m

Arithmetic operations on $\mathbb{Z}_m$, the set of nonnegative integers less than m i.e. $\{0,1,\ldots m-1\}$,

the addition of such integers is denoted by $+_m$ and is defined as;

$$a +_m b = (a + b) \bmod m$$

While the multiplication of these integers as $\times_m$ defined by;

$$a \times_m b = (a \times b) mod\ m$$

These two operations are called arithmetic modulo m

Example

Work out; $4 +_5 13$

Solution: $4 +_5 13 = (4 +_5 13) \bmod 5 = 17 \bmod 5 \equiv 2$

Evaluate; $12 \times_7 18$

Solution: $12 \times_7 18 = 12 \bmod 7 \times 18 \bmod 7$

$= (5 \times 4) \bmod 7 = 20 \bmod 7 \equiv 6$

Properties of modular arithmetic operations

The operations $+_m$ and $\times_m$ satisfies the following properties for some integers $a, b, c \in \mathbb{Z}_m$;

Closure property

Suppose $a, b, c \in \mathbb{Z}_m$ then $a +_m b \in \mathbb{Z}_m; a \times_m b \in \mathbb{Z}_m$

For example, consider integers modulo 7 i.e., $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ then

$$5 +_7 6 = 11_7 = 4 \in \mathbb{Z}_7.$$

Again $5 \times_7 6 = 30_7 = 2 \in \mathbb{Z}_7$.

Associative property

Suppose $a, b, c \in \mathbb{Z}_m$ then $a +_m (b +_m c) = (a +_m b) +_m c$ and

$a \times_m (b \times_m c) = (a \times_m b) \times_m c$.

For example, consider integers modulo 5 i.e., $\mathbb{Z}_5 = \{0,1,2,3,4\}$ then

$4 +_5 (3 +_5 2) = 4 +_5 0 = 4_5$.

Again$(4 +_5 3) +_5 2 = 2 +_5 2 = 4_5$

Commutative property

Let $a, b \in \mathbb{Z}_m$ then $a +_m b = b +_m a$ and

$$a \times_m b = b \times_m a$$

For example, consider integers modulo 9 i.e.,

$\mathbb{Z}_9 = \{0,1,2,3,\cdots,8\}$ then

$2 +_9 6 = 6 +_9 2$ and $4 \times_9 5 = 5 \times_9 4$.

Identity Property

Identity elements

The elements 0 and 1 are the additive and multiplicative identify elements respectively modulo m.

Suppose $a \in \mathbb{Z}_m$ then $a +_m 0 = 0 +_m a = a$ and $1 \times_m a = a \times_m 1 = a$.

Distributive property

Suppose $a, b, c \in \mathbb{Z}_m$ then

$a \times_m (b +_m c) = (a \times_m b) +_m (a \times_m c)$ and $(a +_m b) \times_m c = (a \times_m c) +_m (b \times_m c)$.

For example, consider integers modulo 5 i.e., $\mathbb{Z}_5 = \{0,1,2,3,4\}$ then

$$(4 +_5 3) \times_5 2 = (4 \times_5 2) +_5 (3 \times_5 2)$$

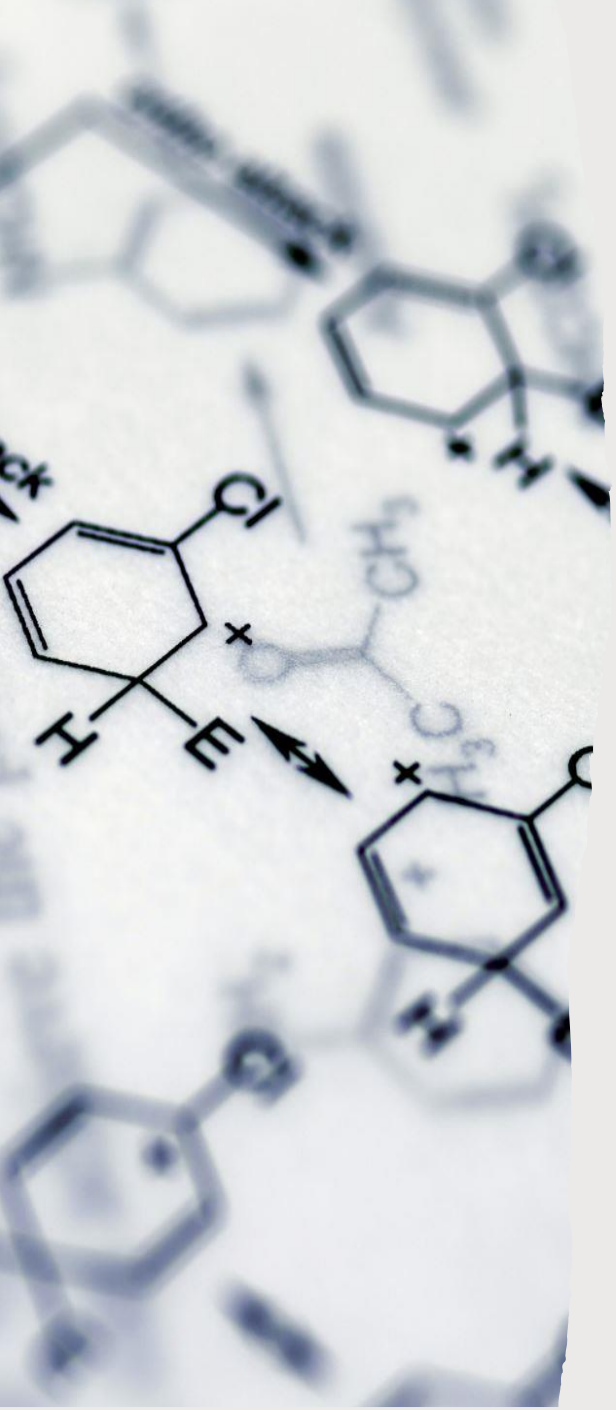
$$2 \times_5 2 = 4$$

$$4 \equiv 4$$

Again; $4 \times_5 (3 +_5 2) = (4 \times_5 3) + (4 \times_5 2)$

$$4 \times 0 = 2 + 3$$

$$0 \equiv 0$$



Additive Inverse

Suppose $a \neq 0$ and $a \in \mathbb{Z}_m$ then $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

then $(m - a)$ is an additive inverse of $a \pmod m$, and 0 is its own additive inverse.

For example,

consider integers modulo 5 i.e., $\mathbb{Z}_5 = \{0,1,2,3,4,5\}$ then the additive inverse of 1 is $5 - 1 = 4$.

Since $1 +_5 4 = 0$ and the additive inverse of 2 is 3.

Multiplicative inverse

Given integers modulo n i.e., $\mathbb{Z}_n$ where n is a prime number , then any non-zero elements a have an inverse such that $a\overline{a} \equiv 1\ (mod\ m)$ with $\overline{a}$ as the multiplicative inverse of a modulo m.

However, given integers modulo m i.e., $\mathbb{Z}_m$ where m is a composite number then any non-zero integer $a \in \mathbb{Z}_m$, that are relatively prime to m have a multiplicative inverse $\overline{a}$ i.e., $a\overline{a} \equiv 1\ (mod\ m)$ with $\gcd(a, m) = 1$

Example

Consider multiplicative Cayley tables integers modulo 5, $\mathbb{Z}_5 = \{0,1,2,3,4\}$.

From the table above the inverse of 1 is 1, the inverse of 2 is 3 and vice versa and the inverse of 4 is itself.

All the non-zero integers modulo 5 have inverses.

$\times_5$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Example

Consider multiplicative Cayley tables integers

modulo 9 i.e., $\mathbb{Z}_9 = \{0,1,2,\cdots,8\}$.

From the table above, 1, 2, 4, 5, 7, and 8 have

multiplicative inverse modulo 9.

While 3 and 6 have no multiplicative inverse modulo 9.

$\times_9$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

Theorem: (Bezout's Theorem)

If a and b are positive integers, then there exists s and t such that;

$$\gcd(a, b) = sa + tb$$

The coefficients s and t are called the Bezout coefficients of a and b i.e., the gcd of two integers a and b can be expressed as a linear combination with integer coefficients of a and b.

GCD and Euclidean Algorithm

Find the gcd(14, 64)

Solution: We apply successive division algorithm to get the gcd.

$$64 = 14 \times 4 + 8 \cdots (\mathrm{i})$$

$$14 = 8 \times 1 + 6 \cdots (\mathrm{ii})$$

$$8 = 1 \times 6 + 2 \cdots (\mathrm{iii})$$

$$6 = 2 \times 3 + 0$$

This is the Euclidean algorithm. It terminates when you get zero as the remainder.

Hence the gcd of 14 and 64 is 2.

GCD as a linear combination

Express the gcd of the following numbers as a linear combination of the two numbers; 399 and 2884

$$2884 = 399 \times 7 + 91$$

$$399 = 91 \times 4 + 35$$

$$91 = 35 \times 2 + 21$$

$$35 = 21 \times 1 + 14$$

$$21 = 14 \times 1 + 7$$

$$14 = 7 \times 2 + 0$$

$$\gcd(399, 2884) = 7$$

Contd...

$$\gcd(399, 2884) = 7$$

$$=> 7 = 21 - 1(14) = 21 - 1[35 - 1(21)] = 2(21) - 1(35)$$

$$7 = 2[91 - 2(35)] - 1(35) = 2(91) - 5(35)$$

$$7 = 2(91) - 5[399 - 4(91)] = 22(91) - 5(399)$$

$$7 = 22[2884 - 7(399)] - 5(399) = 22(2884) - 159(399)$$

$$\therefore 7 = 22(2884) - 159(399)$$

Example

Express the gcd of the following numbers as a linear combination of the two numbers; 732 and 2772

(Pause for some 5 minutes before the next slide for the solution)

Example...contd...

$$2772 = 732 \cdot 3 + 576$$

$$732 = 576 \cdot 1 + 156$$

$$576 = 156 \cdot 3 + 108$$

$$156 = 108 \cdot 1 + 48$$

$$108 = 48 \cdot 2 + 12$$

$$48 = 12 \cdot 4 + 0$$

$$\gcd(732, 2772) = 12$$

$$\therefore 12 = 108 - 2(48) = 108 - 2[156 - 1(108)] = 3(108) - 2(156)$$

$$12 = 3[576 - 3(156)] - 2(156) = 3(576) - 11(156) = 3(576) - 11[732 - 1(576)] = 14(576) - 11(732)$$

$$12 = 14[2772 - 3(732)] - 11(732) = 14(2772) - 53(732)$$

$$\text{i.e. } 12 = 14(2772) - 53(732)$$

References

Rosen, K. (2011). *Elementary Number Theory and Its Application* (6th ed.). Person.

Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.

Susanna, S. E. (2003). *Discrete Mathematics with Application* (3rd ed.). Brooks Cole.