COMP8760 - Lecture 3

Groups and Mutually Prime Numbers

Sanjay Bhattacherjee

University of Kent

Outline

Group

A set and an operation - an abstract algebraic structure.

Mutually Prime Numbers and the Set $\mathbb{Z}_N^\star$

The group that will be used in RSA!

Lagrange's Theorem and Fermat's Little Theorem

Key ideas to be used in RSA!

Study Material for Lecture 3

Book 1 *Cryptography Made Simple*
Author Nigel P. Smart.
Link to eBook

Section 1.1.1 Groups
Section 1.1.3 Euler's Functions
Section 1.1.4 Multiplicative Inverse Modulo N
Section 1.1.5 The Set $\mathbb{Z}_N^\star$

thmmdr

University of Kent

Mutually Prime Numbers

Definition

Two integers a and b are said to be mutually prime if there is no common factor between the two numbers other than 1.

Alternate form

Two integers a and b are said to be mutually prime if $\gcd(a, b) = 1$.

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$
\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4) \\
&= \gcd(4, 1) \\
&= \gcd(1, 4 \mod 1) \\
&= \gcd(1, 0) \\
&= 1
\end{aligned}
$$

So, they are mutually prime.

Euler's phi function: $\phi(n)$

Definition

Let n be a positive integer. We define $\phi(n)$ as the number of integers between 1 and n that are mutually prime to n.

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	1
14	2
15	1

So, $\phi(16) = 8$.

This is a naive enumeration technique, and is costly!!!

We have a very smart mathematical way!

Euler's phi function: $\phi(n)$

Another way for finding the value of $\phi(n)$:

1. Find the prime factorisation of n:

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

2. Use the following formula

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

   This formula can be proved using the principle of inclusion-exclusion.

Find the value of $\phi(100)$

We know $100 = \underbrace{2^2}_{p_1^{\alpha_1}} \times \underbrace{5^2}_{p_2^{\alpha_2}}$

$$\begin{aligned}
\phi(100) &= 100 \prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right) \\
&= 100 \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \\
&= 100 \left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{5}\right) \\
&= 100 \left(\tfrac{1}{2}\right)\left(\tfrac{4}{5}\right) \\
&= 40.
\end{aligned}$$

Find the value of $\phi(1024)$

We know $1024 = \underbrace{2^{10}}_{p_1^{\alpha_1}}$

$$\begin{aligned}\phi(1024) &= 1024 \prod_{i=1}^{1} \left(1 - \frac{1}{p_i}\right) \\ &= 1024 \left(1 - \frac{1}{p_1}\right) \\ &= 1024 \left(1 - \frac{1}{2}\right) \\ &= 512.\end{aligned}$$

thmmdr

University of Kent

The set $\mathbb{Z}_N^\star$

Definition

For a positive integer N, we define $\mathbb{Z}_N^\star$ as the set of all integers between 1 and N that are mutually prime to N.

Examples

- $\mathbb{Z}_2^\star = \{1\}$
- $\mathbb{Z}_3^\star = \{1, 2\}$
- $\mathbb{Z}_4^\star = \{1, 3\}$
- $\mathbb{Z}_5^\star = \{1, 2, 3, 4\}$
- $\mathbb{Z}_6^\star = \{1, 5\}$
- $\mathbb{Z}_{11}^\star = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_{12}^\star = \{1, 5, 7, 11\}$
- $\mathbb{Z}_{13}^\star = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Addition $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication $\pmod 5$ in $\mathbb{Z}_5^\star$

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

Whenever we refer to addition or multiplication
of elements from a set $\mathbb{Z}_N$ or $\mathbb{Z}_N^\star$,
it will mean $+ \pmod N$ and $\times \pmod N$.

We use a general symbol $\star$ to denote both these operations.
So, $\star$ could denote $+ \pmod 5$ or $\times \pmod 5$.
Let us denote the set like $\mathbb{Z}_5$ or $\mathbb{Z}_5^\star$ as G.

thmmdr

University of Kent

Addition $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication $\pmod 5$ in $\mathbb{Z}_5^\star$

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

- Closure:
  For any two elements $x, y \in G$,
  $$x \star y \in G.$$

- Associativity:
  For any three elements $x, y, z \in G$,
  $$x \star (y \star z) = (x \star y) \star z.$$

Addition $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication $\pmod 5$ in $\mathbb{Z}_5^\star$

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

- Identity: (unique for every $\star$)
  There is a unique element $e \in G$ such that, for all $x \in G$,
  $$x \star e = x.$$
  The additive identity is 0 and the multiplicative identity is 1.
- Inverse:
  For any element $x \in G$, there is a unique $\bar{x} \in G$ such that,
  $$x \star \bar{x} = e.$$

Addition $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication $\pmod 5$ in $\mathbb{Z}_5^\star$

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

- Commutativity:
  For any two elements $x, y \in G$,
  $$x \star y = y \star x.$$

- Distributivity:
  For any three elements $x, y, z \in G$,
  $$(x + y) \times z = (x \times z) + (y \times z).$$

Group

A group is a pair $(G, \star)$ that satisfies the following properties.

- Closure:
  For any two elements $x, y \in G$,
  $$x \star y \in G.$$
- Associativity:
  For any three elements $x, y, z \in G$,
  $$x \star (y \star z) = (x \star y) \star z.$$
- Identity: (unique for every $\star$)
  There is a unique element $e \in G$ such that, for all $x \in G$,
  $$x \star e = x.$$
- Inverse:
  For any element $x \in G$, there is a unique $\bar{x} \in G$ such that,
  $$x \star \bar{x} = e.$$

Group: Example 1

$(\underbrace{\mathbb{Z}_{10}}_{\text{The set}}, \underbrace{+ \pmod{10}}_{\text{The operation}})$ satisfies all the properties and hence is a group.

- Closure:
  For any two elements $x, y \in \mathbb{Z}_{10}$, $x + y \pmod{10} \in \mathbb{Z}_{10}$.
  Examples:
  $$3 + 2 = 5 \pmod{10} \in \mathbb{Z}_{10}.$$
  $$3 + 3 = 6 \pmod{10} \in \mathbb{Z}_{10}.$$
  $$9 + 3 = 2 \pmod{10} \in \mathbb{Z}_{10}.$$
  $$9 + 1 = 0 \pmod{10} \in \mathbb{Z}_{10}.$$
- Associativity:
  For any three elements $x, y, z \in \mathbb{Z}_{10}$, $x + (y + z) \pmod{10} = (x + y) + z \pmod{10}$.
  Examples:
  $$1 + (2 + 3) \pmod{10} = (1 + 2) + 3 \pmod{10}.$$
  $$9 + (8 + 7) \pmod{10} = (9 + 8) + 7 \pmod{10}.$$
  $$1 + (7 + 8) \pmod{10} = (1 + 7) + 8 \pmod{10}.$$
  $$0 + (7 + 8) \pmod{10} = (0 + 7) + 8 \pmod{10}.$$

Group: Example 1

$(\underbrace{\mathbb{Z}_{10}}_{\text{The set}}, \underbrace{+ \pmod{10}}_{\text{The operation}})$ satisfies all the properties and hence is a group.

- **Identity**:
  The element $0 \in \mathbb{Z}_{10}$ is unique. For all $x \in \mathbb{Z}_{10}$, $x + 0 \pmod{10} = x$.

$$0 + 0 \pmod{10} = 0.$$

$$1 + 0 \pmod{10} = 1.$$

$$\vdots$$

$$9 + 0 \pmod{10} = 9.$$

- **Inverse**:
  For any element $x \in \mathbb{Z}_{10}$, there is a unique $\bar{x} \in \mathbb{Z}_{10}$ such that, $x + \bar{x} \pmod{10} = 0$. Examples:

$$3 + 7 \pmod{10} = 0.$$

$$4 + 6 \pmod{10} = 0.$$

$$5 + 5 \pmod{10} = 0.$$

Abelian Group

A group pair $(G, \star)$ is abelian if it satisfies the following property as well.

- Commutativity:
  For any two elements $x, y \in G$,
  $$x \star y = y \star x.$$

In other words, a commutative group is called abelian.

$\mathbb{Z}_{12} = \{0, 1, 2, 3, \ldots, 11\}$

For $a, b \in \mathbb{Z}_{12}$, the following table shows all possible $a \times b = a \cdot b$ (except 0's)
(We use the notations $\times$ and $\cdot$ interchangeably to denote multiplication.)

a / b	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Note that the rows of $\mathbb{Z}_{12}^{\star} = \{1, 5, 7, 11\}$ have the element 1 but no 0,
while the other rows have 0 but not 1.

$\mathbb{Z}_{12}^{\star} = \{1, 5, 7, 11\}$

So,

a	1	2	3	4	5	6	7	8	9	10	11
b											
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

- $\mathbb{Z}_{12}^{\star}$ is the set of elements in $\mathbb{Z}_{12}$ that are mutually prime with 12. In other words, for all $a \in \mathbb{Z}_{12}^{\star}$,
$$\gcd(a, 12) = 1.$$
- Note that only if $a \in \mathbb{Z}_{12}^{\star}$, then there is a solution to the equation
$$a \cdot x = 1.$$
In other words, only elements in $\{1, 5, 7, 11\}$ have multiplicative inverses!

$\mathbb{Z}_{13}^{\star} = \{1, 2, 3, \ldots, 12\}$

Here,

a \ b	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

- All positive integers between 1 and 12 are mutually prime with 13. In other words, for all $a \in \mathbb{Z}_{13}^{\star}$,
$$\gcd(a, 13) = 1.$$
- All elements in $\{1, 2, \ldots, 12\}$ have multiplicative inverses!

$\mathbb{Z}_N^\star$ is a Multiplicative Abelian Group

It satisfies the following properties with respect to modular multiplication.

- **Closure**:
  For any two elements $x, y \in \mathbb{Z}_N^\star$,
  $$x \cdot y \in \mathbb{Z}_N^\star$$
- **Associativity**:
  For any three elements $x, y, z \in \mathbb{Z}_N^\star$,
  $$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
- **Identity**:
  The element $1 \in \mathbb{Z}_N^\star$ is the identity such that, for all $x \in \mathbb{Z}_N^\star$,
  $$x \cdot 1 = x$$
- **Inverse**:
  For any element $x \in \mathbb{Z}_N^\star$, there is a unique $\bar{x} \in \mathbb{Z}_N^\star$ such that,
  $$x \cdot \bar{x} = 1$$
- **Commutativity**:
  For any two elements $x, y \in \mathbb{Z}_N^\star$,
  $$x \cdot y = y \cdot x$$

thmmdr

University of Kent

Group: $(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$

where the set $\mathbb{Z}_{11}^{\star} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- **Closure**:
  For any two elements $x, y \in \mathbb{Z}_{11}^{\star}$, $x \times y \pmod{11} \in \mathbb{Z}_{11}^{\star}$.
  Examples:
  $$3 \times 2 = 6 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$3 \times 4 = 1 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$9 \times 3 = 5 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$9 \times 1 = 9 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
- **Associativity**:
  For any three elements $x, y, z \in \mathbb{Z}_{11}^{\star}$, $x \times (y \times z) \pmod{11} = (x \times y) \times z \pmod{11}$.
  Examples:
  $$1 \times (2 \times 3) \pmod{11} = (1 \times 2) \times 3 \pmod{11}.$$
  $$9 \times (8 \times 7) \pmod{11} = (9 \times 8) \times 7 \pmod{11}.$$
  $$1 \times (7 \times 8) \pmod{11} = (1 \times 7) \times 8 \pmod{11}.$$
  $$0 \times (7 \times 8) \pmod{11} = (0 \times 7) \times 8 \pmod{11}.$$

Group: $(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$

$(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$ satisfies all four properties and hence is a group.

- Identity:
  The element $1 \in \mathbb{Z}_{11}^{\star}$ is unique. For all $x \in \mathbb{Z}_{11}^{\star}$, $x \times 1 \pmod{11} = x$.

$$0 \times 1 \pmod{11} = 0.$$

$$1 \times 1 \pmod{11} = 1.$$

$$\vdots$$

$$9 \times 1 \pmod{11} = 9.$$

- Inverse:
  For any element $x \in \mathbb{Z}_{11}^{\star}$, there is a unique $\bar{x} \in \mathbb{Z}_{11}^{\star}$ such that, $x \times \bar{x} \pmod{11} = 1$. Examples:

$$3 \times 7 \pmod{11} = 1.$$

$$4 \times 6 \pmod{11} = 1.$$

$$5 \times 5 \pmod{11} = 1.$$

$\phi(N)$ elements in $\mathbb{Z}_N^\star$

We note here that,

The group $\mathbb{Z}_N^\star$ has all elements of $\mathbb{Z}_N$
that are mutually prime to N.

We recollect here that,

$\phi(N)$ is the number of integers between 1 and N
that are mutually prime to N.

In other words,

$$|\mathbb{Z}_N^\star| = \phi(N).$$

Lagrange's Theorem

Theorem

For any $a \in G$,

$$a^{|G|} = 1.$$

Corollary

We apply this Theorem to the group $\mathbb{Z}_N^\star$.

For any $a \in \mathbb{Z}_N^\star$,

$$a^{\phi(N)} = 1.$$

Fermat's Little Theorem

Theorem

Let p be a prime number and a be an integer. Then,

$$a^p = a \mod p.$$

Proof Idea.

In Lagrange's Theorem, consider the group $(Z_p^\star = \{1, 2, \ldots, p-1\}$.
For any $a \in \mathbb{Z}_p^\star$,

$$a^{p-1} = 1 \mod p.$$

And hence,

$$a^p = a \mod p.$$

Summary

Group

Abstract algebraic structure containing a set and an operation.

Mutually Prime Numbers and the Set $\mathbb{Z}_N^\star$

The group that will be used in RSA!

Lagrange's Theorem and Fermat's Little Theorem

Key ideas to be used in RSA!

Thank you for your kind attention!