# ITC8190
# Mathematics for Computer Science
## Preparation for the exam

Aleksandr Lenin

December 18th, 2018

# Equivalence and Order Relations on Sets. Set Partitions.

To show that a given relation $R$ is an equivalence relation on a set $A$, you need to show that $R$ is reflexive, symmetric and transitive.

## Example 1

Equality $(=)$ is an equivalence relation, since

1. Reflexivity: $\forall a \in A : a = a$.
2. Symmetry: $\forall a, b \in A : a = b \implies b = a$.
3. Transitivity: $\forall a, b, c \in A : a = b, b = c \implies a = c$.

## Example 2

The difference relation $\sim$ defined by

$$(a, b) \sim (c, d) \iff a + d = b + c$$

is an equivalence relation on $\mathbb{N} \times \mathbb{N}$, since

1. Reflexivity: $\forall (a, b) \in \mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (a, b) \iff a + b = a + b \quad .$$

2. Symmetry: $\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$:

$$\begin{aligned} (a, b) \sim (c, d) &\implies a + d = b + c = b + c = a + d \\ &\implies (c, d) \sim (a, b) \quad . \end{aligned}$$

## Example 2

The difference relation $\sim$ defined by

$$(a, b) \sim (c, d) \iff a + d = b + c$$

is an equivalence relation on $\mathbb{N} \times \mathbb{N}$, since

3. Transitivity: $\forall (a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$:

$$\begin{aligned}
&(a, b) \sim (c, d) \ \ , \ \ (c, d) \sim (e, f) \implies \\
&a + d = b + c \ \ , \ \ c + f = d + e \implies \\
&a + d = b + d + e - f \implies \\
&a + f = b + e \implies \\
&(a, b) \sim (e, f) \ \ .
\end{aligned}$$

## Example 3

The factor space $\mathbb{Z}_{15} \big/ \bmod 4$ consists of equivalence classes

$$[0] = \{0, 4, 8, 12\} \qquad [1] = \{1, 5, 9, 13\}$$
$$[2] = \{2, 6, 10, 14\} \qquad [3] = \{3, 7, 11\}$$

## Example 4

The factor space $\mathbb{N} \times \mathbb{N} \Big/ \sim$ with $\sim$ defined by $(a, b) \sim (c, d) \Leftrightarrow a - b = c - d$ consists of equivalence classes

$$\mathbb{Z} = \{\dots, [-3], [-2], [-1], [0], [1], [2], [3], \dots\}$$

## Example 5

To show that equivalence classes $[0], [1], [2], [3]$ form a partition on $\mathbb{Z}_{15}$, we need to show that

$$
\begin{aligned}
[0] \cap [1] &= \{0, 4, 8, 12\} \cap \{1, 5, 9, 13\} = \emptyset \\
[0] \cap [2] &= \{0, 4, 8, 12\} \cap \{2, 6, 10, 14\} = \emptyset \\
[0] \cap [3] &= \{0, 4, 8, 12\} \cap \{3, 7, 11\} = \emptyset \\
[1] \cap [2] &= \{1, 5, 9, 13\} \cap \{2, 6, 10, 14\} = \emptyset \\
[1] \cap [3] &= \{1, 5, 9, 13\} \cap \{3, 7, 11\} = \emptyset \\
[2] \cap [3] &= \{2, 6, 10, 14\} \cap \{3, 7, 11\} = \emptyset
\end{aligned}
$$

## Example 5

To show that equivalence classes $[0], [1], [2], [3]$ form a partition on $\mathbb{Z}_{15}$, we need to show that

$$[0] \cup [1] \cup [2] \cup [3] =$$
$$\{0, 4, 8, 12\} \cup \{1, 5, 9, 13\} \cup \{2, 6, 10, 14\} \cup \{3, 7, 11\} =$$
$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\} = \mathbb{Z}_{15} \quad .$$

## Example 6

To show that $\leqslant$ is a partial order on $\mathbb{Z}$, you need to show

1. Reflexivity: $\forall a \in \mathbb{Z} : a \leqslant a$
2. Anti-symmetry: $\forall a, b \in \mathbb{Z} : a \leqslant b \wedge b \leqslant a \implies a = b$
3. Transitivity: $\forall a, b, c \in \mathbb{Z} : a \leqslant b \leqslant c \implies a \leqslant c$

## Example 7

To show that $<$ is a strict partial order on $\mathbb{Z}$, you need to show

1. Anti-reflexivity: $\forall a \in \mathbb{Z} : a \not< a$
2. Asymmetry: $\forall a, b \in \mathbb{Z} : a < b \implies b \not< a$
3. Transitivity: $\forall a, b, c \in \mathbb{Z} : a < b < c \implies a < c$

# Greatest Common Divisor
# Euclidean Algorithm
# Bézout Identity

The greatest common divisor can be calculated using the Euclidean algorithm.

## Example 8

$$\begin{aligned}\gcd(17,25) &= \gcd(17, 25 \bmod 17) = \gcd(8, 17 \bmod 8)\\ &= \gcd(1,8) = \gcd(1, 8 \bmod 1) = 1 \ .\end{aligned}$$

$$\begin{aligned}\gcd(52,36) &= \gcd(36, 52 \bmod 36) = \gcd(16, 36 \bmod 16)\\ &= \gcd(4, 16 \bmod 4) = 4 \ .\end{aligned}$$

$$\begin{aligned}\gcd(11,18) &= \gcd(11, 18 \bmod 11) = \gcd(7, 11 \bmod 7)\\ &= \gcd(4, 7 \bmod 4) = \gcd(3, 4 \bmod 3)\\ &= \gcd(1, 3 \bmod 1) = 1 \ .\end{aligned}$$

## Example 9

To justify that $6 = \gcd(24, 30)$, write out all the divisors

$$\mathrm{Div}(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$
$$\mathrm{Div}(30) = \{1, 2, 3, 5, 6, 10, 15\}$$

Then write out common divisors of both integers

$$\mathrm{Div}(24) \cap \mathrm{Div}(30) = \{1, 2, 3, 6\}$$

Any subset of $\mathbb{N}$ is well ordered by $\leqslant$. In this ordering, 6 is the greatest common divisor, since

$$1 \leqslant 2 \leqslant 3 \leqslant 6 \quad .$$

Table: Extended Euclidean Algorithm

| 11 | 18 | $a$ | $b$ |
|---|---|---|---|
| 11 | 7 | $a$ | $b-a$ |
| 4 | 7 | $2a-b$ | $b-a$ |
| 4 | 3 | $2a-b$ | $2b-3a$ |
| 1 | 3 | $5a-3b$ | $2b-3a$ |
| 1 | 0 | $5a-3b$ | $11b-18a$ |

$$1 = \gcd(11,18) = 5 \cdot 11 + (-3) \cdot 18 \ .$$

# Euler phi function
# Euler Theorem
# Fermat Little Theorem

# Example 10

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = 36 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = \frac{36 \cdot 2}{2 \cdot 3} = 12 \ .$$

Since $\gcd(4, 9) = 1$, then $\varphi(36) = \varphi(4) \cdot \varphi(9)$.

$$\begin{aligned}\varphi(36) = \varphi(4) \cdot \varphi(9) &= 4 \cdot \left(1 - \frac{1}{2}\right) \cdot 9 \cdot \left(1 - \frac{1}{3}\right) \\ &= \frac{4 \cdot 9 \cdot 2}{2 \cdot 3} = 12 \ .\end{aligned}$$

If $p$ is prime, then $\varphi(p) = p - 1$.

$$\begin{aligned}\varphi(11) &= 10 \ , \\ \varphi(38) &= \varphi(2) \cdot \varphi(19) = 18 \ .\end{aligned}$$

Euler Theorem states that if $n$ and $a$ are coprime positive integers, then

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

It follows from the Euler's theorem that the multiplicative modular inverse of $a$ modulo $n$ is $a^{\varphi(n)-1}$.

$$\frac{1}{a} = \frac{a^{\varphi(n)}}{a} = a^{\varphi(n)} \cdot a^{-1} = a^{\varphi n-1} \bmod n \ .$$

Fermat little theorem states that if $n$ and $a$ are coprime positive integers, then

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

Fermat little theorem is a private case of the Euler theorem where $n$ is prime, then $\varphi(n) = n - 1$, and we obtain Fermat little theorem.

Congruences.

Invertibility modulo $n$.

Solutions to $ax \equiv c \bmod n$.

Congruence is an equivalence relation on the ring of integers $\mathbb{Z}$.

Congruence is a surjective ring–homomorphism $\mathbb{Z} \to \mathbb{Z}_n$.

Two integers $a$ and $b$ are congruent modulo $n$ if their difference is a multiple of $n$.

Integers congruent to $n$ belong to the same equivalence class $[n]$.

## Example 11

Equivalence class of 3 modulo 7 is

$$[3] = \{\ldots, -25, -18, -11, -4, 3, 10, 17, 24, \ldots\}$$

An integer $a$ is invertible modulo $n$ iff $a$ is coprime to $n$.

### Example 12

5 is invertible modulo 6. However, 2 and 3 are invertible modulo 5, but not modulo 6.

The number of invertible elements modulo $n$ is exactly $\varphi(n)$.

### Example 13

There are 10 invertible elements modulo 11, since $\varphi(11) = 10$. There are 4 invertible elements modulo 12, since

$$\varphi(12) = \varphi(3) \cdot \varphi(4) = 2 \cdot 4 \cdot \left(1 - \frac{1}{2}\right) = 4 \quad .$$

## Example 14

Every element $a$ has an additive inverse modulo $n$.

$$-2 \equiv 3 \pmod{5} \qquad -3 \equiv 2 \pmod{5}$$

$$-2 \equiv 4 \pmod{6} \qquad -3 \equiv 3 \pmod{6}$$

## Example 15

Equation $2x \equiv 3 \pmod 5$ is solvable, since 2 is invertible modulo 5 (since $\gcd(2,5) = 1$). The solution is $x \equiv 2^{-1} \cdot 3 \bmod 5 = 3 \cdot 3 \bmod 5 = 4$.

## Example 16

Equation $2x \equiv 3 \pmod 6$ is not solvable, since

1. 2 is not invertible modulo 6 (since $\gcd(2,6) = 2 \neq 1$)
2. $\gcd(2,6) = 2 \nmid 3$

## Example 17

Equation $2x \equiv 4 \pmod 6$ is solvable, since

1. 2 is not invertible modulo 6 (since $\gcd(2,6) = 2 \neq 1$)
2. $\gcd(2,6) = 2 | 4$

Every solution satisfying $x \equiv 2 \pmod 3$ also satisfies $2x \equiv 4 \pmod 6$.

# Chinese Remainder Theorem

## Example 18

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases}$$

1. Express the moduli in the form of a Bézout identity

$$\gcd(4, 5) = 1 = (-1) \cdot 4 + 1 \cdot 5$$

2. Obtain the solution

$$x = -3 \cdot 4 + 2 \cdot 5 = -2 \equiv 18 \pmod{20} .$$

## Example 19

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{6} \\ x \equiv 6 \pmod{9} \end{cases}$$

Is not a CRT instance, since $\gcd(6, 9) = 3 \neq 1$.

## Example 20

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 6 \pmod{7} \end{cases}$$

1. Calculate Bézout identities

Table: gcd(5, 42) as B'ezout identity

| 5 | 42 | $a$ | $b$ |
|---|---|---|---|
| 5 | 2 | $a$ | $b-8a$ |
| 1 | 2 | $17a-2b$ | $b-8a$ |
| 1 | 0 | $17a-2b$ | $5b-42a$ |

$\gcd(5,42) = 17 \cdot 5 + (-2) \cdot 42 = 1.$

## Example 20

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 6 \pmod{7} \end{cases}$$

1. Calculate Bézout identities

Table: gcd(6, 35) as B'ezout identity

| 6 | 35 | $a$ | $b$ |
|---|---|---|---|
| 6 | 5 | $a$ | $b-5a$ |
| 1 | 5 | $6a-b$ | $b-5a$ |
| 1 | 0 | $6a-b$ | $6b-35a$ |

$\gcd(6, 35) = 6 \cdot 6 + (-1) \cdot 35 = 1.$

## Example 20

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 6 \pmod{7} \end{cases}$$

1. Calculate Bézout identities

Table: $\gcd(7, 30)$ as B'ezout identity

| 7 | 30 | $a$ | $b$ |
|---|---|---|---|
| 7 | 2 | $a$ | $b - 4a$ |
| 1 | 2 | $13a - 3b$ | $b - 4a$ |
| 1 | 0 | $13a - 3b$ | $7b - 30a$ |

$\gcd(7, 30) = 13 \cdot 7 + (-3) \cdot 30 = 1.$

## Example 20

Solve for $x$.

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 6 \pmod{7} \end{cases}$$

1. Calculate Bézout identities

$$\begin{aligned} \gcd(5, 42) &= 17 \cdot 5 + (-2) \cdot 42 = 1 \\ \gcd(6, 35) &= 6 \cdot 6 + (-1) \cdot 35 = 1 \\ \gcd(7, 30) &= 13 \cdot 7 + (-3) \cdot 30 = 1 \end{aligned}$$

2. Obtain the solution

$$x = 2 \cdot (-2) \cdot 42 - 4 \cdot 35 - 6 \cdot 3 \cdot 30 = 202 \pmod{210}$$

# Mathematical Induction

## Example 21

Show that for all $n \in \mathbb{N}, n > 0$ it holds that

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \quad .$$

It holds for $n = 1$, since $\frac{1 \cdot (1+1)}{2} = 1$.
Suppose it holds for some $n$. Then

$$\begin{aligned} 1 + 2 + 3 + \ldots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

it holds for $n + 1$. By induction, it holds for all $n$.

## Example 22

Show that for all $n \in \mathbb{N}$, every integer in the form $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9.

It holds for $n = 0$, since $10 + 3 + 5 = 18$ and $9|18$.
Suppose that $10^{n+1} + 3 \cdot 10^n + 5$ for some $n$ is divisible by 9.
Then for $n + 1$

$$10 \cdot 10^{n+1} + 10 \cdot 3 \cdot 10^n + 50 - 45 =$$
$$10 \cdot \left(10^{n+1} + 3 \cdot 10^n + 5\right) - 45$$

By assumption $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9, hence also $10 \cdot (10^{n+1} + 3 \cdot 10^n + 5)$ is divisible by 9. Since $9|45$, then also $10 \cdot (10^{n+1} + 3 \cdot 10^n + 5) - 45$ is divisible by 9.

By induction, $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9 for all $n \in \mathbb{N}$.

# Event Probabilities

## Example 23

Given a uniformly distributed random variable $X$ with range $R_X = \{1, 2, 3, 4, 5, 6\}$, what is the probability to get an outcome that is even or greater than 3?

Let event $A$ denote the event of even outcome, and event $B$ denote the event of outcome greater than 3.

## Example 23

Events $A$ and $B$ are not mutually exclusive, since we can get even outcomes that are greater than 3, i.e. 4 or 6. Hence

$$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \underbrace{\Pr[A \cap B]}_{\Pr[A] \cdot \Pr[A|B]} \ .$$

Events $A$ and $B$ are not independent, since even outcome influences the probability of the result being greater than 3, and the result greater than 3 influences the probability of an even outcome. Hence,

$$\begin{aligned} \Pr[A \cup B] &= \Pr[A] + \Pr[B] - \Pr[A] \cdot \Pr[A|B] \\ &= \frac{1}{2} + \frac{1}{2} - \frac{1}{2} \cdot \frac{2}{3} = \frac{2}{3} \ . \end{aligned}$$

## Example 24

Given a uniformly distributed random variable $X$ with range $R_X = \{1, 2, 3, 4, 5, 6\}$, what is the probability to get an outcome 2 or greater than 5?

Let event $A$ denote the event of outcome 2, and event $B$ denote the event of outcome greater than 5. Events $A$ and $B$ are mutually exclusive, hence

$$\Pr[A \cup B] = \Pr[A] + \Pr[B] = \frac{1}{6} + \frac{2}{6} = \frac{1}{2} \ .$$

# Example 25

Given a uniformly distributed random variable $X$ with range $R_X = \{1, 2, 3, 4, 5, 6\}$, and $Y$ with range $R_Y = \{A, B, C, D\}$ what is the probability to get an outcome greater than 2 for $X$ and outcomes $A$ or $C$ for $Y$?

Define events:

- A variable $X$ produces outcome greater than 2
- B variable $Y$ produces outcome $A$
- C variable $Y$ produces outcome $C$

Events $A, B, C$ are all independent, and $B$ and $C$ are mutually exclusive. Hence

$$\Pr[A \cap B \cup C] = \Pr[A] \cdot \Pr[B \cup C] = \Pr[A] \cdot (\Pr[B] + \Pr[C])$$
$$= \frac{2}{3} \cdot \left(\frac{1}{4} + \frac{1}{4}\right) = \frac{2}{3} \cdot \frac{2}{4} = \frac{1}{3} \ .$$

## Example 26

In TUT, the probability that a student attends the information systems' course as well as spanish lessons is 0.087. The probability that a student attends information systems' course is 0.68. What is the probability that a student attends spanish lessons, given that he attends information systems' course?

Define events:

- A the student attends information systems' course
- B the student attends spanish lessons

Applying the chain rule:

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B|A] \implies \Pr[B|A] = \frac{\Pr[A \cap B]}{\Pr[A]} = \frac{0.087}{0.68} \quad .$$

## Example 27

Given two events $A$ and $B$ with the following probabilities

$$\Pr[A \cap B] = 0.2 \qquad \Pr[A] = 0.4 \qquad \Pr[B] = 0.5 \ ,$$

determine if events $A$ and $B$ are independent.

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{0.2}{0.5} = 0.4 = \Pr[A] \ ,$$
$$\Pr[B|A] = \frac{\Pr[A \cap B]}{\Pr[A]} = \frac{0.2}{0.4} = 0.5 = \Pr[B] \ .$$

Events $A$ and $B$ are independent, since conditional and unconditional probabilities are equal. It can also be seen that $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$ is the product of two unconditional probabilities.

## Example 28

The probability that the grass is wet is $\frac{9}{10}$, the probability that the grass is wet, given that it is raining, is $\frac{2}{3}$, and the probability that it is raining is $\frac{3}{10}$. What is the probability that it is raining, given that the grass is wet?

Define the events

A it is raining outside

B the grass is wet

We know that

$$\Pr[A] = \frac{3}{10} \qquad \Pr[B] = \frac{9}{10} \qquad \Pr[B|A] = \frac{2}{3} \ ,$$

we need to calculate $\Pr[A|B]$. By the Bayes rule,

$$\Pr[A|B] = \frac{\Pr[A] \cdot \Pr[B|A]}{\Pr[B]} = \frac{3 \cdot 2 \cdot 10}{10 \cdot 3 \cdot 9} = \frac{2}{9} \ .$$

# Group Theory

## Example 29

Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a group under the addition operation $(a, b) + (c, d) = (a + c, b + d)$.

The group operation above is clearly assiciative, due to associativity of addition in the ring of integers $\mathbb{Z}$.

Element $(0, 0)$ is the is the identity element, since for all $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2 : (0, 0) + (a, b) = (a + 0, b + 0) = (a, b)$. Every element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ has a corresponding inverse element $(-a, -b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, since $(a, b) + (-a, -b) = (0, 0)$. The addition operation is closed, since for every two elements $(a, b), (c, d) \in \mathbb{Z}_2 \times \mathbb{Z}_2$:

$$(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \quad .$$

Hence, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a group under the operation of addition as stated above.

## Example 30

Show that $H = \{(0,0),(0,1)\}$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

It can be seen that $H \subset \mathbb{Z}_2 \times \mathbb{Z}_2$, and the corresponding Cayley table is

Table: Cayley table for $H$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

| $+$ | $(0,0)$ | $(0,1)$ |
|---|---|---|
| $(0,0)$ | $(0,0)$ | $(0,1)$ |
| $(0,1)$ | $(0,1)$ | $(0,0)$ |

## Example 31

Show that $H = \{(0,0),(0,1),(1,0)\}$ is not a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

It can be seen that $H$ is not closed under addition, since

$$(0,1) + (1,0) = (1,1) \notin H \ .$$

What is the structure of $\mathbb{Z}_2 \times \mathbb{Z}_2$? Is it a cyclic group?

$$
\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\} \\
&\langle(0,1)\rangle = \{(0,1),(0,0)\} \\
&\langle(1,0)\rangle = \{(1,0),(0,0)\} \\
&\langle(1,1)\rangle = \{(1,1),(0,0)\}
\end{aligned}
$$

Group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, since there are no element of order 4. Instead it contains 1 element of order 1 and 3 elements of order 2 (every such element is an inverse of itself).

## Example 32

Is $U(9)$ cyclic? How many elements does $U(9)$ contain? What is the structure of $U(9)$?

Group $U(9)$ contains $\varphi(9) = \varphi(3^2) = 9 \cdot \left(1 - \frac{1}{3}\right) = 6$ elements, they are $U(9) = \{1, 2, 4, 5, 7, 8\}$.

$$\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\} \ , \qquad \langle 4 \rangle = \{4, 7, 1\} \ ,$$
$$\langle 5 \rangle = \{5, 7, 8, 4, 2, 1\} \ , \qquad \langle 7 \rangle = \{7, 4, 1\} \ ,$$
$$\langle 8 \rangle = \{8, 1\}$$

Group $U(9)$ is generated by 2 and 5, and hence is cyclic. The structure is 1 element of order 1, 1 element of order 2, 2 elements of order 3 and 2 elements of order 6.

## Example 33

Can $U(9)$ have elements of orders $4, 5$?

No, because by the Lagrange theorem, the order of an element must divide the order of a group. The order of $U(9)$ is $\varphi(9) = 6$, and since 4 and 5 do not divide 6, there cannot be any elements of orders 4 and 5.

Group $U(9)$ can contain elements (and also subgroups) of orders $1, 2, 3, 6$ – all the divisors of 6.

## Example 34

What is the order of 8 in $U(9)$?

Since $|\langle 8\rangle| = 2$ and $\langle 8\rangle = \{8, 1\}$ (element 8 generates a cyclic subgroup of order 2), the order of 8 is 2. In other words, 2 is the minimal integer $k$ such that $8^k \equiv 1 \pmod{9}$.

## Example 35

What is the order of 5 in $U(9)$?

Element 5 generates $U(9)$, and the order of any generator is equal to the order of the group it generates. Hence, the order of 5 is $\varphi(9) = 6$.

## Example 36

Find inverse of 8 in $U(9)$.

Since $|\langle 8 \rangle| = 2$ and $\langle 8 \rangle = \{8, 1\}$ (element 8 generates a cyclic subgroup of order 2), the order of 8 is 2. In other words, 2 is the minimal integer $k$ such that $8^k \equiv 1 \pmod 9$.

Since the order of 8 is 2 in $U(9)$, this element is an inverse of itself. So the inverse of 8 is 8.

## Example 37

What is the inverse of 5 in $U(9)$?

To find an inverse of 5, we can use the Euler's formula

$$5^{-1} = 5^{\varphi(9)-1} \bmod 9 = 5^5 \bmod 9 = 2 \ .$$

Observe that $2 \cdot 5 = 5 \cdot 2 = 10 \equiv 1 \pmod 9$. Hence, the inverse of 5 is 2 in $U(9)$.

## Example 37

What is the inverse of 5 in $U(9)$?

The same result can be obtained by running the Extended Euclidean algorithm

Table: Extended Euclidean Algorithm

| 5 | 9 | $a$ | $b$ |
|---|---|---|---|
| 5 | 4 | $a$ | $b-a$ |
| 1 | 4 | $2a-b$ | $b-a$ |
| 1 | 0 | $2a-b$ | $5b-9a$ |

The inverse of 5 is the Bézout coefficient near 5, which is 2. Hence, 2 is the inverse of 5 in $U(9)$.

## Example 38

Suppose a group $G$ has an element of order 6, and an element of order 7. What is the minimal order of $G$?

By the Largange theorem, the order of $G$ must be at least the least common multiple of 6 and 7, which is 42. Hence, $G$ cannot contain less than 42 elements.

## Example 39

Group $G$ of order 12 contains an element of order 1, eleven elements of order 4. Show that a subgroup of order 6 consists only of the identity element.

By the Lagrange theorem, a) the order of elements in a subgroup must divide the order of a subgroup, and b) the order of a subgroup must divide the order of the group.

Since $6|12$, such a subgroup may exist. However, such a group cannot contain any elements of order 11, since $11 \not| 6$, the only element that fits into such a subgroup is the identity element of order 1.

## Example 40

What are the possible orders of proper non-cyclic subgroups where an element of order 4 could belong to in a group of order 24?

The subgroups of order 8 or 12.

By the Lagrange theorem, an order of a subgroup we are looking for must be a) a multiple of 4 and b) a divisor of 24. Hence, possible orders of such subgroups are $4, 8, 12, 24$.

A subgroup of order 24 is an improper subgroup, contradicting the question of the task.

An element of order 4 would generate the subgroup of order 4, and hence this subgroup would be cyclic, again contradicting the question of the task.

The only subgroups that remain are the subgroups of orders 8 and 12.

?

THANK YOU
FOR
YOUR
ATTENTION
ANY QUESTIONS?