CS 207: Discrete Structures

Abstract algebra and Number theory

— Lagrange's theorem and its proof

Lecture 39

Oct 29 2015

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

What are the subgroups of the following groups?

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

What are the subgroups of the following groups?

- Symmetries of an eq triangle: $G = \{i, r, s, x, y, z\}$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

What are the subgroups of the following groups?

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \dots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \dots$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \dots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \dots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \dots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \dots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The same sets keep repeating... when multiplied by elements of G

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \ldots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The same sets keep repeating... when multiplied by elements of G
- When do we get back the same subgroup H? And what happens when we don't get back the subgroup?

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \dots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \dots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The sets are disjoint & span G, i.e., form a partition of G.

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \ldots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The sets are disjoint & span G, i.e., form a partition of G.
- But what is the size of each set?

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \ldots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The sets are disjoint & span G, i.e., form a partition of G.
- But what is the size of each set?= size of subgroup
- Thus (size of subgroup) * (no. of such sets)= $|G|$

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \ldots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The sets are disjoint & span G, i.e., form a partition of G.
- But what is the size of each set?= size of subgroup
- Thus (size of subgroup) * (no. of such sets)= $|G|$
- And so $|H|$ divides $|G|$...

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

- $(\mathbb{Z}_6, +_6)$: $\mathbb{Z}_n = \{a \mod n \mid a \in \mathbb{Z}\}$, $a +_n b = a + b \mod n$
  - $H_1 = \{0, 2, 4\}, H_2 = \{0, 3\}$
  - What happens if we add elements to H?
  - $0 + H_1 = \{0, 2, 4\}$, $1 + H_1 = \{1, 3, 5\}$, $2 + H_1 = \{2, 4, 0\} \ldots$
  - $0 + H_2 = \{0, 3\}, 1 + H_2 = \{1, 4\}, 2 + H_2 = \{2, 5\}, \ldots$

What are the properties of such sets obtained?

- We start with a subgroup H of G...
- The sets are disjoint & span G, i.e., form a partition of G.
- But what is the size of each set?= size of subgroup
- Thus (size of subgroup) * (no. of such sets)= $|G|$
- And so $|H|$ divides $|G|$...
- Now, let us generalize and prove this formally!

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Then we can observe several facts:

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Then we can observe several facts:

1. $|gH| = |H|$. Why?

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Then we can observe several facts:

1. $|gH| = |H|$. $gh_1 = gh_2$ implies $h_1 = h_2$ (by left cancellation rule).

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Then we can observe several facts:

1. $|gH| = |H|$. $gh_1 = gh_2$ implies $h_1 = h_2$ (by left cancellation rule).
2. $\bigcup_{g \in G} gH = G$. Why?

Resolving Lagrange's theorem

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof:

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Then we can observe several facts:

1. $|gH| = |H|$. $gh_1 = gh_2$ implies $h_1 = h_2$ (by left cancellation rule).
2. $\bigcup_{g \in G} gH = G$. Each $gH \subseteq G$ and $\forall g \in G$, $g = g * e \in gH$, so $G \subseteq \bigcup_{g \in G} gH$.

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$.

Proof: Exercise.

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$.

Proof:

1. Suppose $x \in g_1 H \cap g_2 H$, i.e.,

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.

Proof:

1. Suppose $x \in g_1H \cap g_2H$, i.e., $x = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$, then we will show $g_1H = g_2H$.

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.

Proof:

1. Suppose $x \in g_1H \cap g_2H$, i.e., $x = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$, then we will show $g_1H = g_2H$.
2. Let $y \in g_1H$, i.e., $y = g_1h$ for some $h \in H$.

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$.

Proof:

1. Suppose $x \in g_1 H \cap g_2 H$, i.e., $x = g_1 h_1 = g_2 h_2$ for some $h_1, h_2 \in H$, then we will show $g_1 H = g_2 H$.
2. Let $y \in g_1 H$, i.e., $y = g_1 h$ for some $h \in H$.
3. Then, $y = g_1 h = (g_2 h_2 h_1^{-1})h = (g_2)(h_2 h_1^{-1} h) = g_2 h' \in g_2 H$

Regarding properties of Cosets

Definition (Left Coset)

Let H be a subgroup of G and $g \in G$. The left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$.

Lemma

Let H be a subgroup of G and $g_1, g_2 \in G$. Then either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.

Proof:

1. Suppose $x \in g_1H \cap g_2H$, i.e., $x = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$, then we will show $g_1H = g_2H$.
2. Let $y \in g_1H$, i.e., $y = g_1h$ for some $h \in H$.
3. Then, $y = g_1h = (g_2h_2h_1^{-1})h = (g_2)(h_2h_1^{-1}h) = g_2h' \in g_2H$
4. Thus $g_1H \subseteq g_2H$. Similarly can show that $g_2H \subseteq g_1H$. $\square$

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a subgroup of G and $g \in G$. Consider the left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$. Then we have,

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a subgroup of G and $g \in G$. Consider the left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$. Then we have,

1. $|gH| = |H|$.
2. $\bigcup_{g \in G} gH = G$.

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a subgroup of G and $g \in G$. Consider the left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$. Then we have,

1. $|gH| = |H|$.
2. $\bigcup_{g \in G} gH = G$.
3. By Lemma, for all $g_1, g_2 \in G$, either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a subgroup of G and $g \in G$. Consider the left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$. Then we have,

1. $|gH| = |H|$.
2. $\bigcup_{g \in G} gH = G$.
3. By Lemma, for all $g_1, g_2 \in G$, either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.
4. From the above, the set of all left cosets $\{gH \mid g \in G\}$ forms a partition of G. Each coset has size $|H|$, so

$$(\text{no. of cosets}) \times |H| = |G|$$

Resuming the proof and summing up

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof: Let H be a subgroup of G and $g \in G$. Consider the left coset $gH = \{x \in G \mid x = gh \text{ for some } h \in H\}$. Then we have,

1. $|gH| = |H|$.
2. $\bigcup_{g \in G} gH = G$.
3. By Lemma, for all $g_1, g_2 \in G$, either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$.
4. From the above, the set of all left cosets $\{gH \mid g \in G\}$ forms a partition of G. Each coset has size $|H|$, so

$$(\text{no. of cosets}) \times |H| = |G|$$

5. Thus $|H|$ divides $|G|$. $\square$

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

- Note that the definition of left cosets, the observations and the Lemma hold even when G is not finite!

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

- Note that the definition of left cosets, the observations and the Lemma hold even when G is not finite!

Right cosets

- What's the fuss about left cosets? Why not right cosets?

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

- Note that the definition of left cosets, the observations and the Lemma hold even when G is not finite!

Right cosets

- What's the fuss about left cosets? Why not right cosets?
- (H.W) Prove that right cosets work too! And no. of left cosets = no. of right cosets.

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

- Note that the definition of left cosets, the observations and the Lemma hold even when G is not finite!

Right cosets

- What's the fuss about left cosets? Why not right cosets?
- (H.W) Prove that right cosets work too! And no. of left cosets = no. of right cosets.
- So, is there a difference? Do they generate the same partition of G?

Some interesting points to note...

Definition

The no. of (distinct) left cosets is called the index of H in G, denoted $|G : H|$. Thus $|G : H| = \frac{|G|}{|H|}$.

- Note that the definition of left cosets, the observations and the Lemma hold even when G is not finite!

Right cosets

- What's the fuss about left cosets? Why not right cosets?
- (H.W) Prove that right cosets work too! And no. of left cosets = no. of right cosets.
- So, is there a difference? Do they generate the same partition of G?
- consider the cosets of $H = \{i, x\}$ in $G = \{i, r, s, x, y, z\}$ ...
  - What are its left-cosets? How many are there?
  - What are its right-cosets? How many are there?

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n =$

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p | (a^{p-1} - 1)$.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p|(a^{p-1} - 1)$.

- Thus if q does not divide $a^{q-1} - 1$, then q is composite.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p|(a^{p-1} - 1)$.

- Thus if q does not divide $a^{q-1} - 1$, then q is composite.
- Is the converse true? That is, does $gcd(a, q) = 1$, $q|a^{q-1} - 1$ imply q is prime?

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p|(a^{p-1} - 1)$.

- Thus if q does not divide $a^{q-1} - 1$, then q is composite.
- Is the converse true? That is, does $gcd(a, q) = 1$, $q|a^{q-1} - 1$ imply q is prime?
- No! There exist composite n such that $n|a^{n-1} - 1$ for all $a \in \mathbb{Z}^+, gcd(a, n) = 1$.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p|(a^{p-1} - 1)$.

- Thus if q does not divide $a^{q-1} - 1$, then q is composite.
- Is the converse true? That is, does $gcd(a, q) = 1$, $q|a^{q-1} - 1$ imply q is prime?
- No! There exist composite n such that $n|a^{n-1} - 1$ for all $a \in \mathbb{Z}^+, gcd(a, n) = 1$. They are called Carmichael numbers.

Corollaries and applications

Exercise Prove the following:

Let g be an element of a finite group G, $|G| = n$.

1. Show that order of the element g divides n.
2. Prove that $g^n = e$.
3. If the order of a group is a prime p, then
   3.1 Is it cyclic (i.e., isomorphic to the cyclic group of order p)?
   3.2 Is it abelian? How many proper subgroups does it have?

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $p|(a^{p-1} - 1)$.

- Thus if q does not divide $a^{q-1} - 1$, then q is composite.
- Is the converse true? That is, does $gcd(a, q) = 1$, $q|a^{q-1} - 1$ imply q is prime?
- No! There exist composite n such that $n|a^{n-1} - 1$ for all $a \in \mathbb{Z}^+, gcd(a, n) = 1$. They are called Carmichael numbers.
- The third Carmichael number is 1729...