Agenda

PROBLEM DOMAIN - NUMBER THEORY
- PROPERTIES OF GROUPS
- PROPERTIES OF Z^*_N :
EULER'S THEOREM AND FERMAT'S THEOREM

Lagrange’s Theorem – Proof Step 1

- Lagrange’s Theorem:
  - For any finite group (G, .) and any subgroup H of G :
    - $|H| \mid |G|$
- Proof:

Sub-Groups: Lagrange's Theorem

- **Lagrange's Theorem:**
  - For any finite group (**G**, **.**) and any subgroup **H** of **G** :

    $|H| \mid |G|$
- **Proof:**
  - Define $\mathbf{R_H}$ on **G**:
    - $\mathbf{x\ R_H\ y}$ **iff** there exists $\mathbf{h \in H}$ such that $\mathbf{x = y.h}$
  - **Claim 1**: $\mathbf{R_H}$ is an *equivalence relation*.
    - **Exercise:** *Prove this claim!*

Lagrange's Theorem – Proof Step 2

- Lagrange's Theorem:
  - For any finite group (**G**, **.**) and any subgroup **H** of **G** :

    |H| | |G|
- Proof:
  - Define $\mathbf{R_H}$ on **G**:
    - **x** $\mathbf{R_H}$ **y** **iff** there exists **h** ∊ **H** such that **x = y.h**
  - **Claim 1**: $\mathbf{R_H}$ is an <u>*equivalence relation*</u>.
  - **Claim 2**: **H** is one of the <u>equivalence classes of $\mathbf{R_H}$</u>
    - **Exercise:** *Prove this claim!*

Lagrange's Theorem – Proof Step 3

- Lagrange's Theorem:
  - For any finite group (**G**, **.**) and any subgroup **H** of **G** :
    $|H| \mid |G|$
- Proof:
  - Define **R_H** on **G**:
    - **$x \ R_H \ y$** **iff** there exists **$h \in H$** such that **$x = y.h$**
  - **Claim 1**: **R_H** is an *equivalence relation*.
  - **Claim 2**: **H** is one of the equivalence classes of **R_H**
  - **Claim 3**:
    - If **H_a** and **H_b** are two equivalences classes of **R_H**
    - then **$f(x) = b.\ a^{-1}.x$** is bijective.
      - **Exercise:** *Prove this claim!*

Lagrange's Theorem – Proof

- **Lagrange's Theorem:**
  - For any finite group (**G**, **.**) and any subgroup **H** of **G** :

    $|H| \mid |G|$
- **Proof:**
  - Define R_H on **G**:
    - $x \; R_H \; y$ **iff** there exists $h \in H$ such that $x = y.h$
  - **Claim 1**: R_H is an *equivalence relation*.
  - **Claim 2**: **H** is one of the equivalence classes of R_H
  - **Claim 3**: If H_a and H_b are two equivalences classes of R_H then $f(x) = b.\, a^{-1}.x$ is bijective.
  - **Conclusion from Claims 2 and 3**:
    - *All equivalence classes of* R_H *are of the same size* $|H|$
      - and so $|H| \mid |G|$

Groups: Order of an element

- For any group (**G**,**.**) and for any **x** in **G**, define $\mathbf{x}^{\mathbf{k}}$ as follows:
  - $\mathbf{x^0 = 1}$ (where **1** is the identity element),
  - $\mathbf{x^k = x \,.\, x^{k-1}}$ for $\mathbf{k > 0}$

- For any **x** in **G**, define the ***order*** of **x** as follows:
  - **ord(x)** = <u>*the smallest **k > 0***</u>

    such that $\mathbf{x^k = 1}$ *where* <u>*1 is the identity element*</u>

Finite Groups have Finite Orders

- **Proof** of *existence of a finite order for any finite group*:
  - For any **x** in **G**, consider $\mathbf{x^1}$, $\mathbf{x^2}$, …, $\mathbf{x^n}$ where $\mathbf{n = |G|}$
    - If one of them is not **1**, are they all distinct?
      - No!
      - By *pigeonhole principle* and by *closure property*
        - there exist **i** and **j** such that **i != j** and $\mathbf{x^i == x^j}$
        - i.e. $\mathbf{x^{i-j} = 1}$

Properties of Groups: Order Lemma

- **Order Lemma :**
  - For any finite group (**G**, **.**), and any **x** in **G**, **ord(x)** divides **|G|**.
  - **Proof:**
    - The elements $\mathbf{x^1}$, $\mathbf{x^2}$, …, $\mathbf{x^k}$, where **k** is **ord(x)**, *form a subgroup of* **G**.
      - Why?
    - Therefore, by Lagrange's Theorem, **k** divides **|G|**.

- **Corollary (to Order Lemma):**
  - $\mathbf{x^{|G|} = 1}$ (the identity element of **G**)

Properties of Z^*_n : Euler's Theorem

- **Euler's Theorem:**
  - For all **n** and for **x** in $\mathbf{Z^*_n}$, $\mathbf{x^{\phi(n)} = 1 \ (\mathrm{mod}\ n)}$
- **Proof:**
  - Recall that $\mathbf{|Z^*_n| = \phi(n)}$
  - By the corollary to the Order Lemma
    - $\mathbf{x^{\phi(n)} = 1 \ (\mathrm{mod}\ n)}$

Fermat's Theorem

- **Fermat's Theorem:**
  - *For all primes* **p** and *for* **x** *in* **Z^*_n**

    $$x^{p-1} = 1 \pmod{p}.$$
- **Proof:**
  - For prime **p**

    $$\phi(p) = p-1.$$
  - By Euler's Theorem

    $$x^{p-1} = 1 \pmod{p}$$