Agenda

PROBLEM DOMAIN - NUMBER THEORY

- PROPERTIES OF GROUPS

- PROPERTIES OF Z^*_N :

EULER'S THEOREM AND FERMAT'S THEOREM

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:
    - $x \, \mathbf{R_H} \, y$ **iff** there exists $h \in H$ such that $x = y.h$
  - **Claim 1**: $\mathbf{R_H}$ 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 $\mathbf{f(x) = b.\, a^{-1}.x}$ 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 x^k as follows:
  - $x^0 = 1$ (where 1 is the identity element),
  - $x^k = x \,.\, x^{k-1}$ for $k > 0$
- For any x in G, define the *order* of x as follows:
  - **ord(x)** = *the smallest k > 0 such that* $\boldsymbol{x^k = 1}$ *where 1 is the identity element*
- Proof of existence of a finite order for any finite group:
  - For any x in G, consider $x^1, x^2, \ldots, x^n$ where $n = |G|$
    - If one of them is not 1, are they all distinct?
      - No, by pigeonhole principle and by closure property.
        - i.e. there exist i and j such that i != j and $x^i == x^j$
        - i.e. $x^{i-j} = x^0 = 1$

Properties of Groups

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

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

Properties of Z^*_n : Euler's Theorem

- **Euler's Theorem:**
  - For all n and for x in Z^*_n, $x^{\phi(n)} = 1 \pmod{n}$
  - **Proof:**
    - $|Z^*_n| = \phi(n)$
    - Then by the corollary to the Order Lemma (see previous slide),
      - $x^{\phi(n)} = 1 \pmod{n}$

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, $\phi(p) = p-1$.
    - Then by Euler's Theorem $x^{p-1} = 1 \pmod{p}$