15-251: Great Theoretical Ideas In Computer Science

Recitation 11

Definitions

- **Euler's Totient Function**: $\phi(N) = |\mathbb{Z}_N^*|$, where $\mathbb{Z}_N^* = \{A \in \mathbb{Z}_N : \text{gcd}(A, N) = 1\}$
- **Group**: A group is an ordered pair consisting of a set G, and a binary operation $\circ : G \times G \to G$ that satisfies the following properties: G contains an identity element, every element in G has an inverse, and $\circ$ is associative.

  Abuse of notation: Instead of saying $(G, \circ)$ is a group, we often say G is a group under $\circ$, or just G is a group (especially if the operation is unimportant or obvious from context)
- **Subgroup**: Let G be a group. H is a *subgroup* of G ($H \leq G$) if $H \subseteq G$ and H is a group. H is a *proper subgroup* of G if $H \subsetneq G$.
- **Cyclic subgroup**: Let G be a group, and let $a \in G$. $\{a^k : k \in \mathbb{Z}\}$ is called the *cyclic subgroup generated by* a
- **Group Isomorphism**: Two groups $(G, \circ)$ and $(H, \star)$ are *isomorphic* if there exists a bijection $\psi : G \to H$ satisfying $\psi(a \circ b) = \psi(a) \star \psi(b)$ for all $a, b \in G$.

`fastPow` Redux!

Design an *efficient* algorithm to compute $A^E \mod N$ (modular exponentiation) where A, E, N each have at most n bits, and analyze its time complexity.

All Miixed Up

(a) Let $A, B, C \in \mathbb{N}$. Show that if C is a miix of A and B then C is a multiple of gcd(A, B).

(b) Show how to modify Euclid's Algorithm so that it outputs k and l such that gcd$(A, B) = kA + lB$. Conclude that C is a miix of A and B if and only if C is a multiple of gcd(A, B).

(c) Given A and N such that $A \in Z_N^*$, explain how we can compute A^{-1} in polynomial time.

Group Theory Warm-Up

Which of the following are groups?

(a) $\mathbb{Q}$ under $\div$

(b) $\{3^k : k \in \mathbb{Z}\}$ under multiplication

(c) $\mathbb{Q}$ under $x \star y = xy + x + y$

Prime Time

Let G be a group of prime order p. Prove that G has no non-trivial subgroups. Additionally prove that $(Z_p, +)$ is the unique group, up to isomorphism, of order p for prime p.

Abelian dollar question

Let e be the identity of a group G. Prove that if $a^2 = e$ for every $a \in G$, then G is abelian.