COL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Definition (Group)

A group is a set G along with a binary operator $\cdot$ for which the following conditions hold:

1. Closure: For all $g, h \in G$, $g \cdot h \in G$.
2. Identity: There exists an identity $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. Inverse: For all $g \in G$, there exists an $h \in G$ such that $g \cdot h = e = h \cdot g$. Such h is called an *inverse* of g.
4. Associativity: For all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

Definition (Finite Group)

When a group G has finite number of elements, then we say that it is a finite group of *order* $|G|$.

Definition (Abelian Group)

$G$is called an *abelian* group if it is a group and also satisfies the following condition:

- Commutativity: For all $g, h \in G$, $g \cdot h = h \cdot g$.

- Exercise 1: Identity element in any group is unique.
- Exercise 2: Every element in any group has a unique inverse.
- Exercise 3: Let G be a group and $a, b, c \in G$.If $a \cdot c = b \cdot c$, then $a = b$. In particular, is $a \cdot c = c$, then a is the identity element.

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

- Let m be prime and a be an integer such that $1 \leq a < m$. What is the value of a^{m-1}?

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem (Fermat's little theorem)

If p is a prime number, then for any integer a we have: $a^p \equiv a \ (mod \ p)$.

- Let p, q be primes, let $N = pq$, let $\phi(N) = (p-1)(q-1)$, and let e, d be such $ed \equiv 1 \ (mod \ \phi(N))$. Then for any $M \in Z_N^*$, what is the value of $M^{ed} \ (mod \ N)$?

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem (Fermat's little theorem)

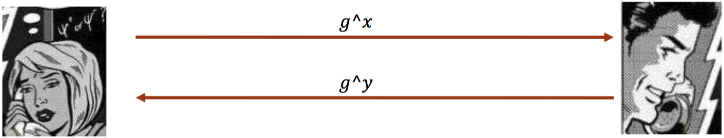
If p is a prime number, then for any integer a we have: $a^p \equiv a \pmod{p}$.

Theorem

Let p, q be primes, let $N = pq$, let $\phi(N) = (p-1)(q-1)$, and let e, d be such $ed \equiv 1 \pmod{\phi(N)}$. Then for any $M \in Z_N$, $M^{ed} \pmod{N} = M$

- The above theorem proves the correctness of the RSA algorithm.
- Question 1: Can we *break* RSA if we can factor N?
- Question 2: Can we factor N if we can *break* RSA?

- Suppose we talk about symmetric schemes. How do two parties exchange secret key?
- Diffie-Hellman Key Exchange.



Both parties share g^{xy} which is the secret key for the session.

- The assumption used here is that there are groups in which computing g^{xy} given just g^x and g^y is difficult.

- Authentication is an issue in the this key exchange protocol.
- Diffie-Hellman Key Exchange: *Man-in-the-middle attack*

Induction and Recursion

- Mathematical induction is used to prove statements that assert that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function.
- A proof by mathematical induction has two parts:
  - **Basis step**: Here we show that $P(1)$ is true.
  - **Inductive step**: Here we show that if $P(k)$ is true, then $P(k+1)$ is true.

Definition (Principle of mathematical induction)

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

- Basis step: We verify that $P(1)$ is true.
- Inductive step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

Definition (Principle of mathematical induction)

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

- Basis step: We verify that $P(1)$ is true.
- Inductive step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

- In the inductive step, we assume that for arbitrary positive integer $P(k)$ is true and then show that $P(k+1)$ must also be true. The assumption that $P(k)$ is true is called the *inductive hypothesis*.
- Induction may be expressed as the following rule of inference:

$$(P(1) \wedge \forall k (P(k) \rightarrow P(k+1))) \rightarrow \forall n \ P(n)$$

Definition (Principle of mathematical induction)

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

- Basis step: We verify that $P(1)$ is true.
- Inductive step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

- Why is mathematical induction valid?
  - Well-ordering principle: Every nonempty subset of the set of positive integers has a least element.
  - Argue the validity of mathematical induction using the axiom above.

End