

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Number Theory and Cryptography

Group Theory and Cryptography

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 $g \cdot g \cdot \dots \cdot g$ (m operations).)

Theorem (Fermat's little theorem)

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

- 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 $M \in \mathbb{Z}_N^*$, what is the value of $M^{ed} \pmod{N}$?

Number Theory and Cryptography

Group Theory and Cryptography

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 $g \cdot g \cdot \dots \cdot g$ (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

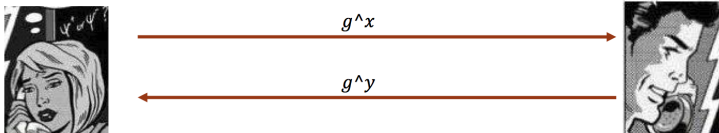
Let p, q be primes, let $N = pq$, let $\phi(N) = (p-1)(q-1)$, and let e, d be such $ed \equiv 1 \pmod{\phi(N)}$. Then for any $M \in \mathbb{Z}_N$, $M^{ed} \pmod{N} = M$

- 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?

Number Theory and Cryptography

Diffie-Hellman key exchange

- 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.

Number Theory and Cryptography

Diffie-Hellman key exchange

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



Induction and Recursion

Induction and Recursion

Mathematical Induction

- 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 .

Induction and Recursion

Mathematical Induction

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:

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

Induction and Recursion

Mathematical Induction

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.

Induction and Recursion

Mathematical Induction: Examples

- Show that the sum of the first n odd integers is n^2 .

Induction and Recursion

Mathematical Induction: Examples

- Show that the sum of the first n odd integers is n^2 .
- Show that for all n , $n < 2^n$.

Induction and Recursion

Mathematical Induction: Examples

- Show that the sum of the first n odd integers is n^2 .
- Show that for all n , $n < 2^n$.
- Show that $2^n < n!$ for every integer n with $n \geq 4$.

Induction and Recursion

Mathematical Induction: Examples

- Show that the sum of the first n odd integers is n^2 .
- Show that for all n , $n < 2^n$.
- Show that $2^n < n!$ for every integer n with $n \geq 4$.
- Prove the following generalization of De Morgan's laws:

$$\overline{\cap_{j=1}^n A_j} = \cup_{j=1}^n \overline{A_j}$$

whenever $A_1, A_2, \dots, A_n$ are subsets of a universal set U and $n \geq 2$.

End