CS 207: Discrete Structures

Abstract algebra and Number theory — Modular arithmetic and RSA

Lecture 41
Nov 3 2015

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that a is congruent to b modulo m, denoted $a \equiv b \mod m$.

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that a is congruent to b modulo m, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements?

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that a is congruent to b modulo m, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group?

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that *a is congruent to b modulo m*, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that *a is congruent to b modulo m*, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.
- What about $(\mathbb{Z}_n \setminus \{0\}, \times_n)$? Which elements have inverses?

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that *a is congruent to b modulo m*, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.
- What about $(\mathbb{Z}_n \setminus \{0\}, \times_n)$? Which elements have inverses?
- Only those co-prime to n

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that *a is congruent to b modulo m*, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.
- What about $(\mathbb{Z}_n \setminus \{0\}, \times_n)$? Which elements have inverses?
- Only those co-prime to n because,
  - if $gcd(a,n) = 1$ then $\exists r, s$ s.t., $ar + ns = gcd(a,n) = 1$.
    Again implies $ar \equiv 1 \mod n$, i.e., r is inverse of $a \mod n$.

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that a is congruent to b modulo m, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.
- What about $(\mathbb{Z}_n \setminus \{0\}, \times_n)$? Which elements have inverses?
- Only those co-prime to n because,
  - if $gcd(a,n) = 1$ then $\exists r, s$ s.t., $ar + ns = gcd(a,n) = 1$.
    Again implies $ar \equiv 1 \mod n$, i.e., r is inverse of $a \mod n$.
- Thus, numbers co-prime to n, denoted $Coprime(\mathbb{Z}_n)$ form a group under $\times_n$. Check!

More properties of modular arithmetic & group theory

Definition

For integers a, b and positive integer m, if $m|(a-b)$, then we say that *a is congruent to b modulo m*, denoted $a \equiv b \mod m$.

- $(\mathbb{Z}_p \setminus \{0\}, \times_p)$ is a group.
  - What are its elements? $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$
  - What is the order of this group? $p-1$.
- What about $(\mathbb{Z}_n \setminus \{0\}, \times_n)$? Which elements have inverses?
- Only those co-prime to n because,
  - if $gcd(a, n) = 1$ then $\exists r, s$ s.t., $ar + ns = gcd(a, n) = 1$. Again implies $ar \equiv 1 \mod n$, i.e., r is inverse of $a \mod n$.
- Thus, numbers co-prime to n, denoted $Coprime(\mathbb{Z}_n)$ form a group under $\times_n$. Check!
- The number of elements co-prime to n, i.e., $|Coprime(\mathbb{Z}_n)|$ is denoted $\phi(n)$ – called the Euler totient no./function.

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
2. What is $\phi(p)$?
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
2. What is $\phi(p)$?
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?
4. (Euler's theorem) If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
   – the usual $(\mathbb{Z}_p, \times_p)$
2. What is $\phi(p)$? $p - 1$
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?
   $\phi(pq) = (p-1)(q-1)$
4. (Euler's theorem) If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
2. What is $\phi(p)$?
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?
   $\phi(pq) = (p-1)(q-1)$
4. (Euler's theorem) If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.
   - Let $gcd(a, n) = 1$, $\phi(n) = |(Coprime(\mathbb{Z}_n), \times_n)|$

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
2. What is $\phi(p)$?
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?
   $\phi(pq) = (p-1)(q-1)$
4. (Euler's theorem) If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.
   - Let $gcd(a, n) = 1$, $\phi(n) = |(Coprime(\mathbb{Z}_n), \times_n)|$
   - By Lagrange's theorem, order of element a divides order of this group, i.e., $a^{(ord.of grp)}$=(id of this grp).

Properties of the Euler Totient function

- $\forall n \in \mathbb{Z}^+$, $Coprime(\mathbb{Z}_n)$ denotes numbers coprime to n.
- $(Coprime(\mathbb{Z}_n), \times_n)$ is a group, where $a \times_n b = ab \mod n$.
- Order of this group is $\phi(n)$, no. of elements co-prime to n.

Exercises

1. Suppose p is a prime, what is $(Coprime(\mathbb{Z}_p), \times_p)$?
2. What is $\phi(p)$?
3. Suppose $n = pq$ is a product of primes, what is $\phi(pq)$, i.e., how many numbers are there co-prime to pq in $\{1, \ldots, pq\}$?
   $\phi(pq) = (p-1)(q-1)$
4. (Euler's theorem) If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.
   - Let $gcd(a, n) = 1$, $\phi(n) = |(Coprime(\mathbb{Z}_n), \times_n)|$
   - By Lagrange's theorem, order of element a divides order of this group, i.e., $a^{(ord.of grp)}$=(id of this grp).
   - That is, $a^{\phi(n)} = 1 + kn$ for some k, i.e., $a^{\phi(n)} \equiv 1 \mod n$

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

***Bob* starts by choosing two large primes p, q**

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

1. *Bob* shouts out $N = pq$ and E (encryptor!)...
2. But he keeps p, q and the decryptor D secret.

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

1. Bob shouts out $N = pq$ and E (encryptor!)...
2. But he keeps p, q and the decryptor D secret.
3. $Alice$ wants to send message $M < p, q$ that only Bob understands. What does she send?

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

1. *Bob* shouts out $N = pq$ and E (encryptor!)...
2. But he keeps p, q and the decryptor D secret.
3. *Alice* wants to send message $M < p, q$ that only *Bob* understands. What does she send?
4. *Alice* sends $X = M^E \mod N$

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

1. *Bob* shouts out $N = pq$ and E (encryptor!)...
2. But he keeps p, q and the decryptor D secret.
3. *Alice* wants to send message $M < p, q$ that only *Bob* understands. What does she send?
4. *Alice* sends $X = M^E \mod N$
5. *Bob* can decrypt it by:

Sharing secrets in plain sight! Part 2: Redux

- Alice wants to send a message M (a number, lets say between 1 and 20000) to Bob that only he can figure out.
- But any message can be intercepted (hacker: Carol!)
- How can Bob ensure privacy of messages?

Bob starts by choosing two large primes p, q

Also chooses numbers D and E such that $ED \equiv 1 \mod \phi(pq)$ (i.e., $\phi(pq) \mid (ED - 1)$).

1. *Bob* shouts out $N = pq$ and E (encryptor!)...
2. But he keeps p, q and the decryptor D secret.
3. *Alice* wants to send message $M < p, q$ that only *Bob* understands. What does she send?
4. *Alice* sends $X = M^E \mod N$
5. *Bob* can decrypt it by: $X^D = M^{ED} \mod N = M^{1+m\phi(pq)} \mod pq = M$ (by Euler's theorem)

RSA cryptography

Why does this work?

- Because Carol knows only X, N, E and has to solve $ED \equiv 1 \mod \phi(N)$ to obtain D after computing $\phi(N)$.

RSA cryptography

Why does this work?

- Because Carol knows only X, N, E and has to solve $ED \equiv 1 \mod \phi(N)$ to obtain D after computing $\phi(N)$.
- But there is no known fast way to get $\phi(N)$ from N.

RSA cryptography

Why does this work?

- Because Carol knows only X, N, E and has to solve $ED \equiv 1 \mod \phi(N)$ to obtain D after computing $\phi(N)$.
- But there is no known fast way to get $\phi(N)$ from N.
- Only known way is to factorize N and finding a poly-time algo for this is open!

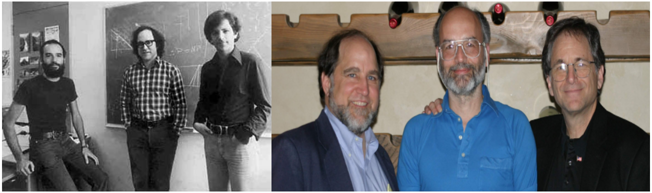

Figure : Rivest, Shamir, Addleman, 1977 - Turing Award in 2002

Compare this to Diffie-hellman

Start with any finite cyclic group G and generator $g \in G$

1. *Alice* picks a random $a \in \mathbb{N}$ and sends g^a to *Bob*.
2. *Bob* picks a random $b \in \mathbb{N}$ and sends g^b to *Alice*.
3. *Alice* computes $(g^b)^a$ and *Bob* computes $(g^a)^b$.
4. Shared key is g^{ab}.

- Of course, we know modular logarithm we could do it!
- i.e., if $g^a = g'$ and g and g' are given, what is a?
- Called the discrete logarithm problem and it is also open!

Summary

What we covered in this course

1. Mathematical proofs and structures
2. Counting and combinatorics
3. Introduction to graph theory
4. Elements of group theory and applications to number theory

Summary: Till half time

- Mathematical proofs and structures

- Counting and Combinatorics

Summary: Till half time

- Mathematical proofs and structures
  - Propositions, proof techniques: contradiction, contrapositive
  - Induction: strong induction, well-ordering principle
  - Sets: finite and infinite sets, countable and uncountable sets
  - Functions: bijections (from e.g., $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$), injections and surjections, Cantor's diagonalization technique
  - Relations: equivalence relations and partitions; partial orders, chains, anti-chains, lattices
- Counting and Combinatorics

Summary: Till half time

- Mathematical proofs and structures
  - Propositions, proof techniques: contradiction, contrapositive
  - Induction: strong induction, well-ordering principle
  - Sets: finite and infinite sets, countable and uncountable sets
  - Functions: bijections (from e.g., $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$), injections and surjections, Cantor's diagonalization technique
  - Relations: equivalence relations and partitions; partial orders, chains, anti-chains, lattices
- Counting and Combinatorics
  - Basic counting principles, double counting
  - Binomial theorem, permutations and combinations, Estimating $n!$
  - Recurrence relations and generating functions
  - Principle of Inclusion-Exclusion (PIE) and its applications.
  - Pigeon-Hole Principle (PHP) and its applications.
  - Some special numbers: Fibonacci, Catalan, Stirling of the second kind ...
  - Introduction to Ramsey theory

Summary: Graph theory

Topics in Graph theory

- Basics: graphs, paths, cycles, walks, trails, ...
- Cliques and independent sets.
- Graph representations, isomorphisms and automorphisms.
- Matchings: perfect, maximal and maximum.

Summary: Graph theory

Graph theory: Characterizations

1. Basics concepts and definitions.
2. Eulerian graphs: Using degrees of vertices.
3. Bipartite graphs: Using odd length cycles.
4. Connected components: Using cycles.
5. Maximum matchings: Using augmenting paths.
6. Perfect matchings in bipartite graphs: Using neighbour sets. – Hall's theorem
7. Maximum matchings in bipartite graphs: Minimum vertex covers. – Konig-Egervary's theorem
8. Stable matchings... and the Gale Shapley Algo

Summary: Abstract Algebra and Number theory

- Definition of an abstract group; basic properties
- Examples:
  - Invertible matrices, Symmetries of a regular polygon
  - Permutation groups, Graph automorphisms
  - $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +n)$, $(\mathbb{Z}_p, \times_p)$, ...
- Abelian groups, Cyclic groups
- Group Isomorphisms and subgroups of a group.
- Order of a group and order of an element.
- Lagrange's theorem; corollaries and some applications

Summary: Abstract Algebra and Number theory

- Definition of an abstract group; basic properties
- Examples:
  - Invertible matrices, Symmetries of a regular polygon
  - Permutation groups, Graph automorphisms
  - $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +n)$, $(\mathbb{Z}_p, \times_p)$, ...
- Abelian groups, Cyclic groups
- Group Isomorphisms and subgroups of a group.
- Order of a group and order of an element.
- Lagrange's theorem; corollaries and some applications

Applications to number theory and cryptography.

- Modular arithmetic
- Diffie-Hellman key exchange
- RSA cryptosystems.

Summary: Abstract Algebra and Number theory

- Definition of an abstract group; basic properties
- Examples:
  - Invertible matrices, Symmetries of a regular polygon
  - Permutation groups, Graph automorphisms
  - $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +n)$, $(\mathbb{Z}_p, \times_p)$, ...
- Abelian groups, Cyclic groups
- Group Isomorphisms and subgroups of a group.
- Order of a group and order of an element.
- Lagrange's theorem; corollaries and some applications

Applications to number theory and cryptography.

- Modular arithmetic
- Diffie-Hellman key exchange
- RSA cryptosystems.

... the end. $\square$