|  |  |
| --- | --- |
| **Lecture 10: Sets and Set Operations** | **Lecture 11: Sets and Set Operations** |
| **Infinite Set** | **Set Identities** |
| **Member of Operator (**∈**)** | **De Morgan’s Law for Sets** |
| **The Empty Set ()** | **Proving Set Identities** |
| **Subset and Superset** | **Method 1: Mutual Subsets** |
| **Proper (strict) Subsets and Supersets** | **Method 2: Set Builder Notation and Logical Equivalence** |
| **Set as Element of a Set** | **Method 3: Membership Tables** |
| **Cardinality of a Set** | **Membership Table Example** |
| **The Power Set Operation** | **Method 4: Venn Diagrams** |
| **Ordered n-tuples** | **Generalized Unions and Intersections** |
| **Cartesian Product of Sets** | **Generalized Union** |
| **The Union Operator (**∪**)** | **Generalized Union Example** |
| **The Intersection Operator** | **Generalized Intersection** |
| **Disjointedness or Exclusive Sets** | **Generalized Intersection Example** |
| **Inclusion-Exclusion Example** | **Bit String Representation of Sets** |
| **Set Difference** | **Examples of Sets as Bit Strings** |
| **Set Complements** |  |
| **Interval Notation** |  |

|  |  |
| --- | --- |
| **Lecture 12: Functions** | **Lecture 13: Functions & Sequences** |
| **Functions** | **Identity Function** |
| **Function: Formal Definition** | **Identity Function Illustration** |
| **Terminology** | **Graphs of Functions** |
| **Range vs Codomain** | **Graphs of Functions: Example** |
| **Function and Non-Function** | **Floor and Ceiling Functions** |
| **Function Operators** | **Visualizing Floor & Ceiling** |
| **Function Composition Operator** | **Plots with Floor Ceiling Example** |
| **Function Composition** | **Plots with Floor & Ceiling** |
| **Function Composition Example** | **Sequences & Summations** |
| **Images of Sets Under Functions** | **Sequences** |
| **One-to-One Function** | **Sequence Examples** |
| **One-to-One Illustration** | **Example With Repetitions** |
| **One-to-one Functions** | **Geometric Series, Sequence or Progression** |
| **Sufficient Conditions for one-to-oneness** | **Arithmetic Series, Sequence or Progression** |
| **Onto (Surjective) Functions** | **Recognizing Sequences (I)** |
| **Illustration of Onto** | **Recognizing Sequences (II)** |
| **Bijections and Inversible Functions** | **Special Integer Sequences** |
| **Inverse Function Illustration** | **Coding: Fibonacci Series** |
| **Inversible Function Examples** | **Coding: Factorial Series** |
| **Mappings in Java** | **Prime Number Series** |
| **Images, Range, Bijection in Java** |  |
|  |  |

|  |  |
| --- | --- |
| **Lecture 15: Sequences & Summations** | **Lecture 16: Mathematical & Strong Induction** |
| **Summation Notation** | **Mathematical Induction** |
| **Generalized Summations** | **The “Domino Effect”** |
| **Summation Manipulations** | **Mathematical Induction Procedure** |
| **Index Shifting** | **Validity of Induction** |
| **Summation Manipulations** | **Outline of the Inductive Proof** |
| **Summation Manipulations** | **Induction Example** |
| **Geometric Progression** | **Induction Example 2** |
| **Geometric Sum Derivation** | **Induction Example 3** |
| **Sum Numbers from 1 to n** | **Generalizing Induction** |
| **Gauss Trick for Summing Numbers (1 to n)** | **Induction Example 4** |
| **Derivation of Gauss Trick** | **Second Principle of Induction (Strong Induction)** |
| **Useful Closed Form Expressions** | **Example of Second Principle** |
| **Using Shortcuts for Evaluating Expressions** | **Generalizing Strong Induction** |
| **Cardinality** | **Example 2: Strong Induction** |
| **Summation Manipulations** | **Example 2: Proof by Mathematical Induction** |
| **Nested Summations** | **Example 3** |
| **Summation’s Conclusion** | **The Well Ordering Property** |
|  | **Well Ordering Property and Mathematical Induction** |
|  | **Well Ordering Property and Induction Example** |

|  |  |
| --- | --- |
| **Lecture 17: Recursive Definitions & Structural Induction** | **Lecture 18: Recursive Definitions, Structural Induction & Recursive Algorithms** |
| **Recursive Definitions** | **Recursive Definitions** |
| **Recursion** | **Full Binary Tree** |
| **Recursively Defined Functions** | **Building Up Full Binary Tree** |
| **Another Example** | **Structural Induction** |
| **Recursive Definition of Factorial** | **Structural Induction Example** |
| **The Fibonacci Numbers** | **Recursive Algorithms** |
| **Inductive Proof about Fibonacci Numbers** | **Example** |
| **A Lower Bound on Fibonacci Numbers** | **Recursive Linear Search** |
| **Recursively Defined Sets** | **Recursive Binary Search** |
| **The Set of All Strings** | **Recursive Fibonacci Algorithm** |
| **String: Example** | **Analysis of Fibonacci Procedure** |
| **Rooted Trees** | **Iterative Fibonacci Algorithm** |
| **Illustrating Rooted Tree Definition** | **Recursive Merge Sort Example** |
| **Building Up Rooted Trees** | **Recursive Merge Sort** |
| **Extended Binary Trees** | **Merging Two Sorted Lists** |
| **Building Up Extended Binary Trees** | **Recursive Merge Method** |

|  |  |
| --- | --- |
| **Lecture 19: The Integers Division Number Theory** | **Lecture 20: Integers Algorithms Number Theory** |
| **The Integers and Division** | **Greatest Common Divisor (GCD)** |
| **Divides, Factor, Multiple** | **Relative Primality** |
| **The Divides Relation** | **GCD Shortcut** |
| **Proof of (2)** | **Least Common Multiple** |
| **The Division Algorithm** | **LCM Shortcut** |
| **The mod Operator** | **LCM Example** |
| **The mod Operator Examples** | **GCD and LCM** |
| **Modular Congruence** | **Spiral Visualization of mod** |
| **Useful Congruence Theorems** | **Pseudorandom Numbers** |
| **Applications of Congruence** | **Linear Congruential Method** |
| **Hashing Functions** | **Prime Numbers: Theorems** |
| **Cryptology (I)** | **Mersenne Primes** |
| **Cryptology (II)** | **Integers and Algorithms** |
| **Prime Numbers** | **Base-b Number Systems** |
| **The Fundamental Theorem of Arithmetic** | **Particular Bases of Interest** |
| **Prime Numbers: Theorems** | **Converting to Base b** |
| **Prime Factorization** | **Binary** ↔ **Hexadecimal** |
| **Greatest Common Divisor (GCD)** | **Addition of Binary Numbers** |
| **Relative Primality** | **Multiplication of Binary Numbers** |
| **GCD Shortcut** |  |

|  |  |
| --- | --- |
| **Lecture 21: Integers Algorithms Number Theory** | **Lecture 22: Linear Congruence & Cryptography Number Theory** |
| **Division with Remainder** | **Uniqueness of Prime Factorization** |
| **Euclid’s Algorithm for GCD** | **Linear Congruences, Inverses** |
| **Euclid’s Algorithm Example** | **Example** |
| **Euclid’s Algorithm Pseudocode** | **Theorem 3** |
| **Proof that Euclid’s Algorithm Works** | **Examples** |
| **Two’s Complement** | **Chinese Remainder Theorem** |
| **Two’s Complement Example** | **Computer Arithmetic with Large Integers** |
| **Subtraction of Binary Numbers** | **Computer Arithmetic Example** |
| **Modular Exponentiation** | **Pseudoprimes** |
| **Algorithm Concept** | **Carmichael Numbers** |
| **Modular Exponentiation** | **Fermat’s Little Theorem** |
| **Modular Exponentiation Examples** | **An Application of Primes** |
| **Modular Exponentiation 3644 to 645** | **Public Key Cryptography** |
| **Miscellaneous Results** | **Rivest-Shamir-Adleman (RSA)** |
| **Theorem 1** | **RSA Encryption** |
| **Proof of Theorem 1** | **RSA Decryption** |
| **Theorem 1 Example** | **Why RSA Works?** |
| **Proof of Lemma 1** |  |
| **Proof of Lemma 2** |
| **Theorem 2** |

|  |  |
| --- | --- |
| **Lecture 23: Combinatorics** | **Lecture 24: Combinatorics** |
| **Combinatorics** | **Permutation Examples** |
| **Sum and Product Rules** | **More Permutation Examples** |
| **The Sum Rule** | **Another Example** |
| **Sum Rule: Example 1** | **Combinations** |
| **The Sum Rule: Example 2** | **Calculate C**(n,r) |
| **The Product Rule** | **Combinations** |
| **The Product Rule Example** | **Combination Examples** |
| **The Product Rule Example 2** | **Binomial Coeffecients** |
| **The Product Rule Example** | **The Binomial Theorem** |
| **IP Address Examples** | **Corollaries** |
| **Set Theoretic Version** | **Generalized Permutations and Combinations** |
| **Inclusion-Exclusion Principle Inclusion-Exclusion Principle Example** | **Permutations with Repetitions**  **Theorem 1**  **Theorem 2:** |
| **Setup of Problem** | **Proof of Theorem 2** |
| **Tree Diagrams** |  |
| **Tree Diagrams Examples** |  |
| **The Pigeonhole Principle** |  |
| **Pigeonhole Principle Example** |  |
| **Generalized Pigeonhole Principle** |  |
| **Proof of Generalized Pigeonhole Principle** |  |
| **Generalized Pigeonhole Principle Example** |  |
| **Fun Pigeonhole Proof** |  |
| **Baseball Example** |  |
| **Baseball Problem Explained** |  |

|  |  |
| --- | --- |
| **Lecture 25: Combinatorics** | **Lecture 26: Relations** |
| **Combinations with Repetitions**  **Theorem 2** | **Introduction** |
| **More Examples** | **Relations**  **Examples** |
| **When to Use Generalized Combinations** | **Functions as Relations** |
| **More Integer Solutions & Restrictions** | **Relations on a Set**  **Example** |
| **Another Perspective to the Example** | **Properties of a Relations** |
| **Distributing Objects into Distinguishable Boxes** | **Reflexive Relations**  **Example** |
| **Distributing Distinguishable Objects into Indistinguishable Boxes** | **Symmetric and Antisymmetric Relations** |
| **Another Perspective of the Example** | **Examples** |
| **Distributing Indistinguishable Objects into Indistinguishable Boxes** | **Transitive Relations**  **Example** |
| **Another Combination Example** | **Combining Relations** |
| **Pascal’s Identity** | **Example** |
| **Pascal’s Triangle** | **Relation Composition** |
| **Vandermonde’s Identity** | **Powers of a Relation** |
| **Proof** | **Theorem** |
| **Corollary** | **n-ary Relations** |
|  | **Examples** |
|  | **Databases and Relations** |
|  | **Operators on n-ary Relations** |
|  | **Selection Operator** |
|  | **Projection Operator** |
|  | **Join Operator** |
|  |  |

|  |  |
| --- | --- |
| **Lecture 27: Relations** | **Lecture 28: Relations** |
| **Representing Relations** | **Partial Ordering: Introduction** |
| **Representing Matrices using Matrices** | **Partial Ordering** |
| **Example** | **Examples** |
| **Matrix of a Reflexive Relation** | **Notations** |
| **Matrix of a Symmetric Relation** | **Comparable Elements** |
| **Antisymmetric Relation and Its Matrix** | **Total Ordering & Well Ordering** |
| **Example** | **Lexicographic Order** |
| **Operations on Relations and Matrices** | **Example** |
| **Matrix of a Composite Relation** | **Lexicographic Ordering** |
| **Example** | **Example** |
| **Power of a relation and Matrix** | **Lexicographic Ordering on Strings** |
| **Represent Relation using Digraphs** |  |
| **Relation Properties and Digraphs** |  |
| **Example** |  |
| **Equivalence Relations** |  |
| **Equivalent Relation** |  |
| **Example** |  |
| **Equivalence Class** |  |
| **Equivalence Classes and Partitions** |  |