

Lecture  
Thursday Week 5

Discrete Mathematics and  
Probability 2024



There **is** a lecture next week, namely on Thursday, after the class test has been submitted.  
It introduces material from Week 7, on discrete probability.  
There is no lecture on Monday.

## Discrete Math: Covered material

- \* Week 1 (16 Sept; self study): **Epp Chapter 1: Speaking Mathematically**  
Variables; Languages of Sets, of Relations and Functions, of Graphs.  
**Chapter 2: Logic of compound statements**  
2.1 Logical Form and Logical Equivalence  
2.2 Conditional Statements  
**Chapter 3: The logic of Quantified Statements:** All except 3.4, which was covered in Inf1A.
- \* Week 2 (19 & 23 Sept): **Chapter 4: Elementary number theory and methods of proof.**  
Skip Section 4.9 and 4.10 (or 4.8 in the 4<sup>th</sup> edition)  
Direct proof, proof by cases, by contradiction and by contraposition
- \* Week 3 (26 & 30 Sept): **Chapter 5: Induction and Recursion** Skip 5.1 (you know this already), skip 5.7-5.9  
5.1 and 5.6 (self study): recursively defined sequences, sum notation;  $n!$  and “ $n$  choose  $r$ ”.  
5.2-5.4: Proof by induction, and by strong induction.
- \* Week 4 **Chapter 6: Set theory** (treated on 30 Sept), without 6.4  
Basic operators on sets; Venn diagrams; proving set inclusion by element method, and by algebraic method.  
**Chapter 7: Functions** Domain and co-domain; range of a function.  
(3 Oct): Injective, surjective and bijective function. The inverse of a bijective function.  
(7 Oct): Composition of functions. Comparing infinite sets by size. Countably inf., countable, uncountable sets.  
The set of integers, as well as the rationals, are countable. The reals are uncountable.  
Having the same size is an equivalence relation on sets.  
Having a smaller or equal size (defined with injections) is a relation on sets that is reflexive and transitive, and if two sets are smaller or equal in size to each other, they must have the same size.
- \* Week 5 (10 Oct): **Chapter 8: Relations**  
(14 Oct): 8.4: Modular arithmetic and cryptography.

## Discrete Math: Covered material

- \* Week 1 (16 Sept; self study): **Epp Chapters 1-3:**  
Variables; Sets, Relations Functions, Graphs; Logic, Conditional Statements, Quantified Statements.
- \* Week 2 (19 & 23 Sept): **Chapter 4: Elementary number theory and methods of proof.**  
Direct proof, proof by cases, by contradiction and by contraposition
- \* Week 3 (26 & 30 Sept): **Chapter 5: Induction and Recursion** Skip 5.1 (you know this already), skip 5.7-5.9  
**5.1 and 5.6** (self study): recursively defined sequences, sum notation;  $n!$  and “ $n$  choose  $r$ ”.  
**5.2-5.4:** Proof by induction, and by strong induction.
- \* Week 4 **Chapter 6: Set theory** (treated on 30 Sept), without 6.4  
Basic operators on sets; Venn diagrams; proving set inclusion by element method, and by algebraic method.  
**Chapter 7: Functions**  
(3 Oct): Injective, surjective and bijective function. The inverse of a bijective function.  
Domain and co-domain. Range of function.  
(7 Oct): Composition of functions. Comparing infinite sets by size. Countably inf., countable, uncountable sets.  
Having the same size is an equivalence relation on sets.
- \* Week 5 (10 Oct): **Chapter 8: Relations**  
Binary relations; domain and co-domain; 2 kinds of graphs of a relation; inverse of any relation.  
N-ary relations. Reflexivity, symmetry and transitivity of binary relations with domain=co-domain.  
Equivalence relations, equivalence classes, representative of an equivalence class.  
Each equivalence relation induces a partition, and each partition induces an equivalence relation.  
Partial orders. Anti-symmetry. Hasse diagram.  
(14 Oct): **8.4: Modular arithmetic and cryptography**  
Inverse of a number modulo  $n$ . Solving diophantine equations.  
RSA cryptography.

+|

