Proof Techniques and Mathematical Basics for Algorithm Analysis II

Proof Techniques

- P(n): a logical statement for each positive integer n
  - e.g.: P(n): there is a prime larger than n
- Mathematical Induction:
- Suppose that:
  - $P(n_0)$ is true (basis step), and
  - $P(n) \rightarrow P(n+1)$ for each positive integer n. (induction step)
- Then P(n) is true for every positive integer.
- Example: For every positive integer n, we prove that:

$$\sum_{k=1}^{n} k = \binom{n+1}{2}$$

- n=1, assume P(n) true, show that P(n+1) is true.

- Where do we need induction: Chapter 3, 4, 5.

Proof Techniques

- Proof by Contradiction:
  - assume that the statement we want to prove is *false*, and then
  - show that this assumption leads to nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true

- **Proposition** P .
- *Proof.* Suppose $\sim P$.
- . …
- Therefore $C \wedge \sim C$.

Proposition There are infinitely many prime numbers.

Proof. For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as $p_1, p_2, p_3, \ldots p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and so on. Thus p_n is the nth and largest prime number. Now consider the number $a = (p_1 p_2 p_3 \cdots p_n) + 1$, that is, a is the product of all prime numbers, plus 1. Now a, like any natural number, has at least one prime divisor, and that means $p_k \mid a$ for at least one of our n prime numbers p_k. Thus there is an integer c for which $a = cp_k$, which is to say

$$(p_1 p_2 p_3 \cdots p_{k-1} p_k p_{k+1} \cdots p_n) + 1 = cp_k.$$

Dividing both sides of this by p_k gives us

$$(p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) + \frac{1}{p_k} = c,$$

so

$$\frac{1}{p_k} = c - (p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n).$$

The expression on the right is an integer, while the expression on the left is not an integer. This is a contradiction. ■

Limits

Given the functions $f(x)$ and $g(x)$ suppose we have,

$$\lim_{x \to c} f(x) = \infty \qquad \lim_{x \to c} g(x) = L$$

for some real numbers c and L. Then,

1. $\lim_{x \to c} \left[f(x) \pm g(x) \right] = \infty$

2. If $L > 0$ then $\lim_{x \to c} \left[f(x) g(x) \right] = \infty$

3. If $L < 0$ then $\lim_{x \to c} \left[f(x) g(x) \right] = -\infty$

4. $\lim_{x \to c} \frac{g(x)}{f(x)} = 0$

Source: http://tutorial.math.lamar.edu

Simple Series

- Sequence: a set of things (usually numbers) that are in order.
- **Arithmetic Sequence: the difference between one term and the next is a constant.**
  - {a, a+d, a+2d, a+3d, ... }
  - {1, 1+3, 1+2×3, 1+3×3, ... }
  - {1, 4, 7, 10, ... }
- **Summing an Arithmetic Sequence:**

$$\sum_{k=0}^{n-1}(a+kd) = \frac{n}{2}(2a+(n-1)d)$$

- Example: $$\sum_{k=0}^{10-1}(1+k\cdot 3) = \frac{10}{2}(2\cdot 1+(10-1)\cdot 3)$$

- Example: The fifth term of an arithmetic sequence is 11 and the tenth term is 41. What is the first term?

Source: http://www.mathsisfun.com

Simple Series

- Sequence: a set of things (usually numbers) that are in order.
- **Geometric Sequence:** each term is found by **multiplying** the previous term by a **constant**.
  - $\{a, ar, ar^2, ar^3, \dots\}$ //$r \neq 0$, common ratio
  - $\{1, 1\times 2, 1\times 2^2, 1\times 2^3, \dots\} = \{1, 2, 4, 8, \dots\}$
- **Summing a Geometric Sequence**:

$$\sum_{k=0}^{n-1}(ar^k) = a\left(\frac{1-r^n}{1-r}\right) \qquad \sum_{k=0}^{4-1}(10\cdot 3^k) = 10\left(\frac{1-3^4}{1-3}\right) = 400$$

- Example: You put one rice on a chessboard's first square. You double the amount of rice at the next square and so on. How many rice does the last square have?
- Example: Add up the first 10 terms of the Geometric Sequence that halves each time

Source: http://www.mathsisfun.com

Combinatorics

Sets

- Set: an unordered collection of distinct objects (elements)
  - A={1,2,3}, B={2,1,3}, C={2,1,3,4},
    $7 \notin A \quad 3 \in A$
  - n(A) = |A| = 3
  - A=B, A ⊂ C (subset)
  - ∅: Empty set, or null set, ∅⊂X, X any set.
- Union: A ∪ C= {2,1,3,4}
- Intersection: A ∩ C={2,1,3}

Source: Jacques Verstraete, UCSD, class notes, http://www.math.ucsd.edu/~jverstra/154-part1.pdf

Subsets

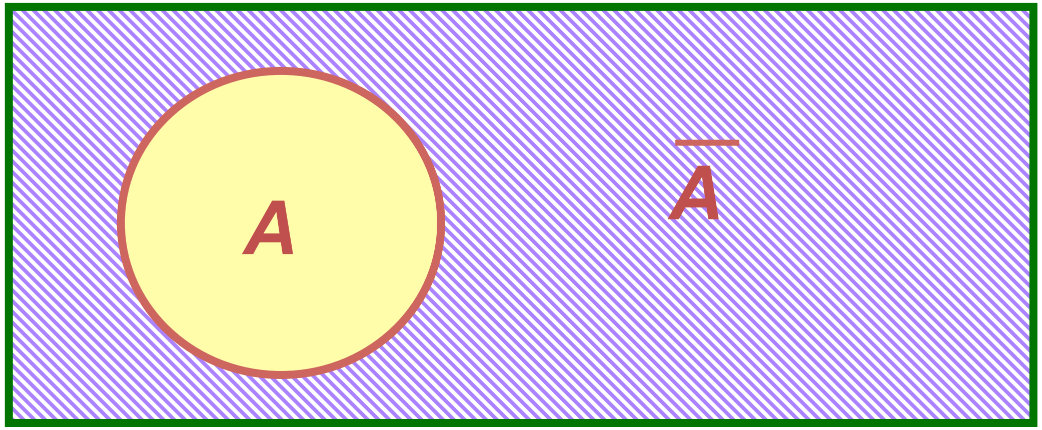
- List all of the subsets of {1, 2, 3}

$\varnothing$ {1} {2} {3} {1, 2} {1, 3} {2, 3} {1, 2, 3}

- If $|A|=n$, there are 2^n possible subsets of A.

Source: Jacques Verstraete, UCSD, class notes, http://www.math.ucsd.edu/~jverstra/154-part1.pdf

Complement

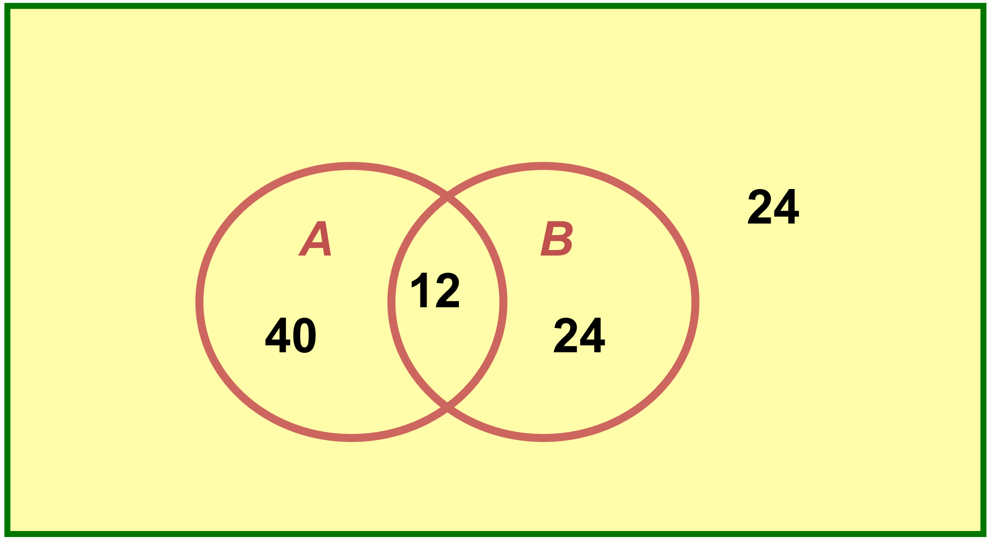


$\overline{A}$: complement of A

$A \cup \overline{A}$ = universal set

Source: www.mathxtc.com

Counting Elements



This is a Venn diagram.

universal set contains 100 elements

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$$=52+36-12=76$$

Source: www.mathxtc.com

Counting Sets and Sequences (Theorems)

- The number of subsets of an n-element set is 2^n.
- The number of sequences of length n from a k-element set is k^n
- The number of permutations of a set of size n is $n! := n(n-1)(n-2)\ldots 1$.
- There are $(n)_k := n(n-1)\ldots(n-k+1)$ sequences of k distinct elements in a set of size n.
- The number of sets of size k *(combinations of size k)* in an n-element set is

$$\binom{n}{k} := \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}$$

Source: Jacques Verstraete, UCSD, class notes, http://www.math.ucsd.edu/~jverstra/154-part1.pdf

Combinatorial Identities

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Source: Jacques Verstraete, UCSD, class notes, http://www.math.ucsd.edu/~jverstra/154-part1.pdf

Probability

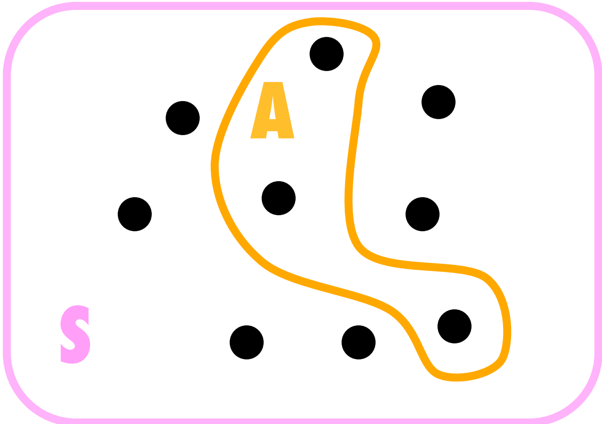
REVIEW

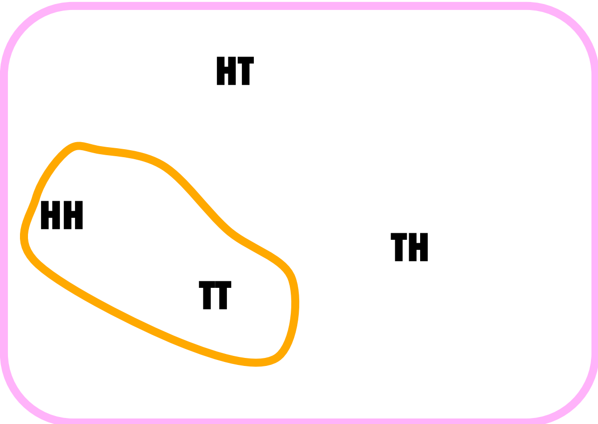
Probability

- Every probabilistic claim ultimately refers to some sample space, which is a set of elementary events
- Think of each elementary event as the outcome of some experiment
  - Ex: flipping two coins gives sample space
    {HH, HT, TH, TT}
- An event is a subset of the sample space
  - Ex: event "both coins flipped the same" is {HH, TT}

REVIEW

Sample Spaces and Events





REVIEW

Probability Distribution

- A probability distribution Pr on a sample space S is a function from events of S to real numbers s.t.
  - Pr[A] $\geq$ 0 for every event A
  - Pr[S] = 1
  - Pr[A U B] = Pr[A] + Pr[B] for every two non-intersecting ("mutually exclusive") events A and B
- Pr[A] is the probability of event A

REVIEW

Properties of Probability Distributions

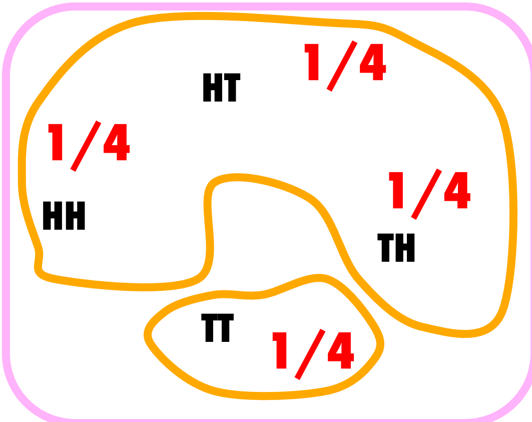
- $\Pr[\varnothing] = 0$
- If $A \subseteq B$, then $\Pr[A] \le \Pr[B]$
- $\Pr[S - A] = 1 - \Pr[A]$ // complement
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$

  $\le \Pr[A] + \Pr[B]$

REVIEW

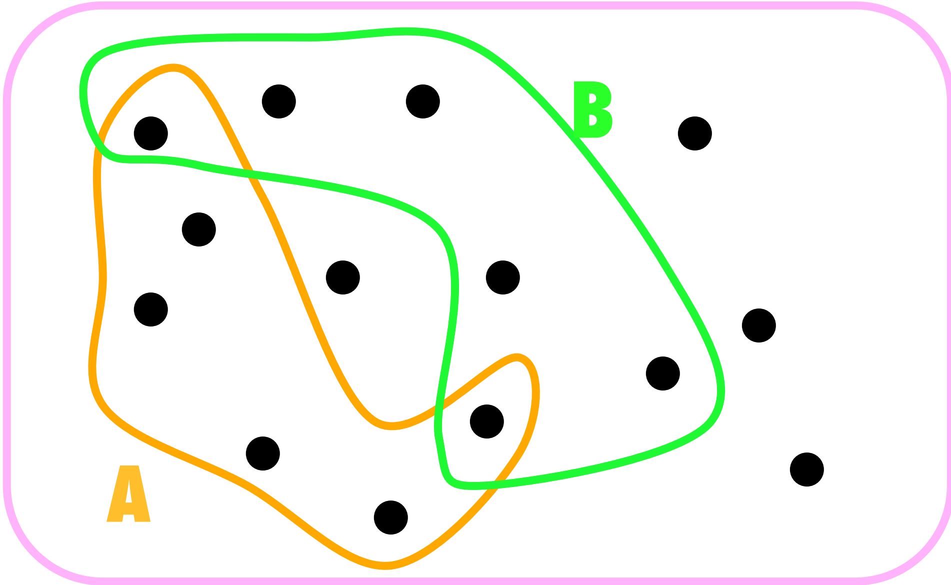
Example

- Suppose Pr[{HH}] = Pr[{HT}] = Pr[{TH}] = Pr[{TT}] = 1/4.
- Pr["at least one head"]
  = Pr[{HH U HT U TH}]
  = Pr[{HH}] + Pr[{HT}] + Pr[{TH}]
  = 3/4.
- Pr["less than one head"]
  = 1 — Pr["at least one head"]
  = 1 — 3/4 = 1/4



REVIEW

Probability Distribution



$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$

REVIEW

Specific Probability Distribution

- Discrete probability distribution: sample space is finite or countably infinite
  - Ex: flipping two coins once; flipping one coin infinitely often
- Continous probability distribution: infinite sample space, e.g. Gaussian

- Uniform probability distribution: every elementary event has the same probability, 1/|S|
  - Ex: flipping two fair coins once, flipping a fair dice
- Nonuniform probability distribution: some elements have different probability, e.g. an unfair coin.

REVIEW

Flipping a Fair Coin

- Suppose we flip a fair coin n times
- Each elementary event in the sample space is one sequence of n heads and tails, describing the outcome of one "experiment"
- Size of sample space is 2^n
- Let A be the event of "k heads and n-k tails occurring"
- Pr[A] = C(n,k)/2^n
  - There are C(n,k) sequences of length n in which k heads and n–k tails occur, and each has probability $1/2^n$.

REVIEW

Example

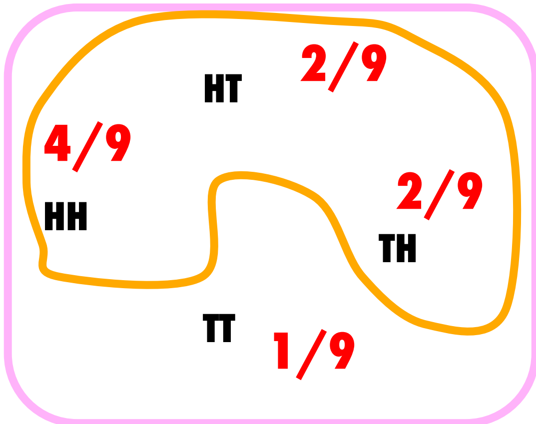
- $n = 5$, $k = 3$
- HHHTT HHTTH HTTHH TTHHH
- HHTHT HTHTH THTHH
- HTHHT THHTH
- THHHT
- Pr(3 heads and 2 tails) = $C(5,3)/2^5$

  = 10/32

REVIEW

Flipping Unfair Coins

- Suppose we flip two coins, each of which gives heads two-thirds of the time
- What is the probability distribution on the sample space?



Pr[at least one head] = 8/9

REVIEW

Independent Events

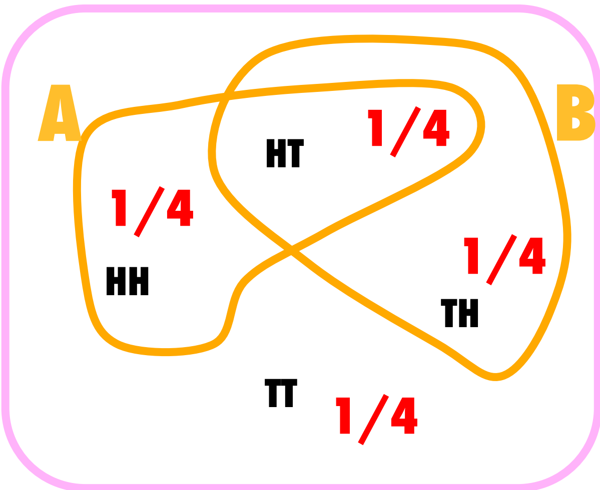
- Two events A and B are independent if $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$
  - i.e., probability that both A and B occur is the product of the separate probabilities that A occurs and that B occurs

REVIEW

Independent Events Example

In two-coin-flip example with fair coins:

- A = "first coin is heads"
- B = "coins are different"



$\Pr[A] = 1/2$
$\Pr[B] = 1/2$
$\Pr[A \cap B] = 1/4 = (1/2)(1/2)$
so A and B are independent

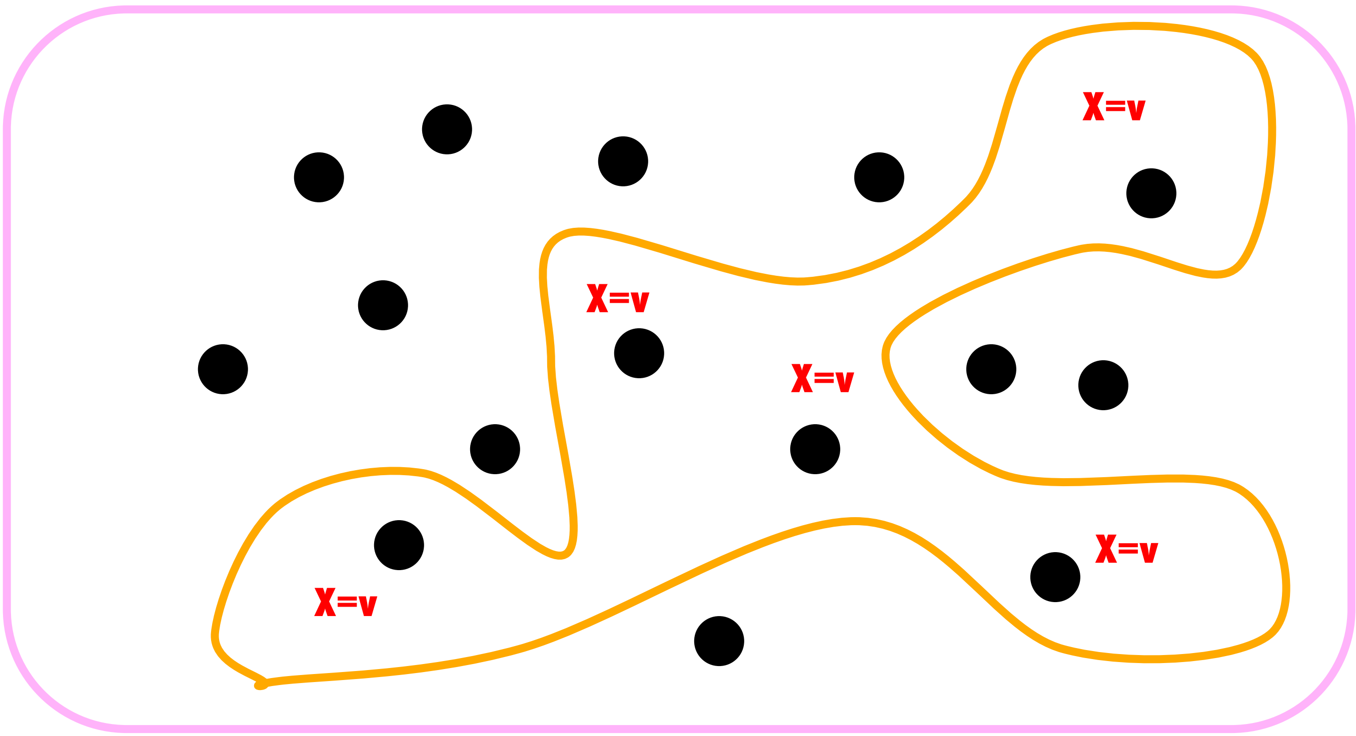
REVIEW

Discrete Random Variables

- A discrete random variable X is a function from a finite or countably infinite sample space to the real numbers
- Associates a real number with each possible outcome of an experiment
- Define the event "X = v" to be the set of all the elementary events s in the sample space with X(s) = v
- So, Pr["X = v"] is the sum of Pr[{s}] over all s with X(s) = v

REVIEW

Discrete Random Variable



Add up the probabilities of all the elementary events in the orange event to get the probability that X = v

REVIEW

Random Variable Example

- Roll two fair 6-sided dice
- Sample space contains 36 elementary events (1:1, 1:2, 1:3, 1:4, 1:5, 1:6, 2:1,…)
- Probability of each elementary event is 1/36
- Define random variable X to be the maximum of the two values rolled
- What is Pr["X = 3"]?
- It is 5/36, since there are 5 elementary events with max value 3 (1:3, 2:3, 3:3, 3:2, and 3:1)

REVIEW

Independent Random Variables

- It is common for more than one random variable to be defined on the same sample space:
  - X is maximum value rolled
  - Y is sum of the two values rolled
- Two random variables X and Y are independent if for all v and w, the events "X = v" and "Y = w" are independent

Expected Value of a Random Variable

REVIEW

- Most common summary of a random variable is its "average", weighted by the probabilities
  - called expected value, or expectation, or mean

- Definition: $E[X] = \sum_{v} v \Pr[X = v]$

REVIEW

Expected Value Example

- Consider a game in which you flip two fair coins
- You get 3TL for each head but lose 2TL for each tail
- What are your expected earnings?
  - i.e., what is the expected value of the random variable X, where X(HH) = 6, X(HT) = X(TH) = 1, and X(TT) = -4?
- Note that no value other than 6, 1, and -4 can be taken on by X (e.g., Pr[X = 5] = 0)
- $E[X] = 6(1/4) + 1(1/4) + 1(1/4) + (-4)(1/4) = 1$

REVIEW

Properties of Expected Values

- $E[X+Y] = E[X] + E[Y]$, for any two random variables X and Y, even if they are not independent!
- $E[a \cdot X] = a \cdot E[X]$, for any random variable X and any constant a
- $E[X \cdot Y] = E[X] \cdot E[Y]$, for any two *independent* random variables X and Y

Study Material (for the Quiz, maybe ☺)

- What is the sum of the squares of integers from k=1 to n? Prove your result.
- Prove that the number of subsets of an n-element set is 2^n.
- Prove that the number of sequences of length n from a k-element set is k^n
- Assume that there is a game where you flip a fair dice and earn as many TL as the square of what you flip (i.e. if you flip a 5, you earn a 25TL). You need to pay a certain amount to enter this game. What is the maximum amount you would pay?

Study Material (for the Quiz, maybe ☺) and Additional Resources

- Prove that $2^{2n} - 1$ is divisible by 3, for integers $n > 0$.
- Prove that $2n + 1 < 2^n$, for all integers $n \geq 3$.
- Prove that square root of 2 is irrational.

Some resources:

http://www.csee.umbc.edu/~stephens/203/PDF/4-3.pdf

http://www.csee.umbc.edu/~stephens/203/PDF/3-6.pdf