Administrative Information

• Required text: Invitation to Discrete Mathematics
  Jiri Matousek and Jaroslav Nesetril

• Reference: Discrete Mathematics and its Applications
  Kenneth Rosen

• All handouts posted on web page
• Class mailing list
• Homeworks assigned every Wed., due in class next Wed.

• Grading:
  9-10 homeworks (80%), take-home final (20%)
• Collaboration policy

Discussion Sessions/Office Hours

• Discussion Sessions in addition to office hours (perhaps)
• Times announced next week on basis of student choices
• My office hours for next week: Tue, 2:00-4:00 pm
What is Discrete Mathematics?

- Mathematics dealing with finite sets
- Topics: counting, combinatorics, graph theory, probability
- Goals:
  - Develop mathematical maturity
  - Foundation for advanced courses in Computer Science
- Flavor of questions:
  - How many valid passwords on a computer system?
  - What is the probability of winning a lottery?
  - What is the shortest path between two cities?

Toy problems as illustrations

- Puzzle:
  Three houses, three wells:
  Can we connect each house to each well by pathways so that no two pathways cross?

- Real world problem:
  VLSI: Given placement of components of circuit on a board, is it possible to connect them along a board so that no two wires cross?

Proof techniques

Evidence vs. Proof

\[ p(n) = n^2 + n + 41 \]

Claim: \( \forall n \in \mathbb{N}, p(n) \) is prime
Evidence

\[ p(0) = 41 \quad \text{prime} \]
\[ p(1) = 43 \quad \text{prime} \]
\[ p(2) = 47 \quad \text{prime} \]
\[ p(3) = 53 \quad \text{prime} \]
\[ \vdots \]
\[ p(20) = 461 \quad \text{prime} \quad \text{looks promising!} \]
\[ \vdots \]
\[ p(39) = 1601 \quad \text{prime} \quad \text{must be true!} \]

Only prime numbers?

\[ \forall n \in \mathbb{N}, \quad p(n) = n^2 + n + 41 \text{ is prime} \]

- Cannot be a coincidence
- Hypothesis must be true!

But it is NOT!

\[ p(40) = 1681 \quad \text{is NOT PRIME} \]

Evidence vs. Proof

- Euler’s conjecture (1769):
  \[ a^4 + b^4 + c^4 = d^4 \]
  has no solution for \( a, b, c, d \) positive integers

Counterexample: 218 years later by Noam Elkies:

\[ 95800^4 + 217519^4 + 414560^4 = 422481^4 \]

Example courtesy: Prof. Albert R. Meyer’s lecture slides for MIT course 6.042, Fall 02

Evidence vs. Proof

- Hypothesis:
  \[ 313 \cdot (x^3 + y^3) = z^3 \]
  has no positive integer solution

False!

But smallest counterexample has

more than 1000 digits!

Example courtesy: Prof. Albert R. Meyer’s lecture slides for MIT course 6.042, Fall 02
Mathematical Induction

• Find a general formula for $\sum_{i=0}^{n} 2^i$
  
  $2^0 = 1$
  $2^0 + 2^1 = 3$
  $2^0 + 2^1 + 2^2 = 7$
  $2^0 + 2^1 + 2^2 + 2^3 = 15$
  
  $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ ?

Mathematical Induction

1. (Basis step)
   $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ holds for $n = 0$

2. (Inductive step)
   Suppose formula holds for $n = n_0$ (inductive hypothesis)
   We prove that it also holds for $n = n_0 + 1$
   
   $\sum_{i=0}^{n+1} 2^i = \left( \sum_{i=0}^{n} 2^i \right) + 2^{n+1}$
   
   $= (2^{n+1} - 1) + 2^{n+1}$
   
   $= 2^{n+2} - 1$

Show that any $2^n \times 2^n$ chessboard with one square removed can be tiled using L-shaped pieces, each covering three squares.
Template for proof by Induction

- Prove that P(n) is true for all positive integers n
- BASIS STEP: Show that P(1) is true
- INDUCTIVE STEP: Show that P(k) → P(k+1)

Strong Induction

- Prove that P(n) is true for all positive integers n
- BASIS STEP: Show that P(1) is true
- INDUCTIVE STEP: Show that [P(1) ∧ P(2) ∧ … ∧ P(k)] → P(k + 1)

Strong Induction example

- Show that if n is an integer greater than 1, n can be written down as a product of primes
- P(n): n can be written down as a product of primes
  - Basis Step: P(2) is true, 2 = 2
  - Inductive Step: Assume P(j) is true for all j ≤ k
    Need to show that P(k+1) is true
  - Case 1: k+1 is prime, P(k+1) is true
  - Case 2: k+1 = a·b
    By induction hypothesis, both a and b can be written as a product of primes.

Proof by contradiction

Prove that \(\sqrt{2}\) is irrational

Suppose \(\sqrt{2} = \frac{m}{n}\) \(\gcd(m, n) = 1\)

\[2 = \frac{m^2}{n^2}\]

- \(m\) is even
  - \(m = 2k\)
  - \(2 = \frac{4k^2}{n^2}\)

- \(n^2 = 2k^2\)
  - \(n\) is even

Contradiction!