Last Time

- Sets
- Union, Intersection, Complement
- Venn Diagrams
- Sequences
- Cartesian Products
- Functions
- Alphabets, Strings, Languages
Proofs

• What is a proof?
  – Logical argument that a statement is true
  – Beyond any doubt
  – Starts with known facts (axioms)
  – Builds to a conclusion with logical steps
  – Deductive reasoning
Other Useful Vocabulary

• **Definition** – describes the objects and notions that we use

• **Theorem** – a mathematical statement proven to be true

• **Lemma** – a mathematical statements that we prove along the way, but aren’t as interesting

• **Corollary** – a mathematical statement related to a theorem proven to be true

• **Conjecture / Hypothesis** – an unproven statement
Proof Design

• “P if and only if Q” \( (P \leftrightarrow Q) \) means you need to prove two parts:
  – “If \( P \) is true, then \( Q \) is true” (forward direction)
  – “If \( Q \) is true, then \( P \) is true” (backward direction)
  – This is usually seen in equality statements (example later).
Proof Strategies

1. Understand the statement that you want to prove.
   – Do you understand the notation?
   – Rewrite the statement in your own words.
   – Break it down and consider each part separately if necessary.
Proof Strategies

2. Try to get a “gut” feeling of why the statement should be true.
   – Experiment with examples.
   – Try to find a counterexample that shows that the statement isn’t true. See where you run into difficulty.
3. Try to prove a simple case.
   – If you need to prove a statement for all natural numbers, start by proving that it’s true for 1 or 2.
   – If the simple case you pick turns out to be too hard, pick a different one.
Proof Strategies

4. Write the proof up properly.
   – The proof should be a sequence of statements, with each statement following from some set of previous statements.
   – Read through a second time to make sure you haven’t introduced an error or omitted an important step.
   – End a proof with Q.E.D. or □.
Proof Strategies

• Other tips:
  – **Be patient** – proofs aren’t the easiest thing in the world to produce.
  – **Come back to it later** – sometimes letting yourself subconsciously consider it is an effective strategy.
  – **Be neat** – it’s easier to organize your thoughts in the end when you can clearly understand the process you took.
  – **Be concise** – the more verbose you are, the more likely you are to introduce an error.
Example

• Prove the following:

For any two sets $A$ and $B$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

**Forward direction:** Suppose that $x$ is an element of $\overline{A \cup B}$. Then $x$ is not in $A \cup B$ from the definition of the complement of a set. Therefore, $x$ is not in $A$, and $x$ is not in $B$, from the definition of the union of two sets. In other words, $x$ is in $\overline{A}$ and $x$ is in $\overline{B}$. By the definition of the intersection of two sets, $x$ is hence in $\overline{A} \cap \overline{B}$.

**Backward direction:** Suppose that $x$ is in $\overline{A} \cap \overline{B}$. Then, $x$ is in both $\overline{A}$ and $\overline{B}$, by the definition of the intersection of two sets. Therefore, $x$ is not in $A$ and $x$ is not in $B$, and thus not in the union of these two sets. Hence, $x$ is in the complement of the union of these sets: $\overline{A \cup B}$. ■
Types of Proof

1. Proof by Construction ("Direct Proof")
2. Proof by Contradiction
3. Proof by Induction

• This is not an exhaustive list.
• Some problems will use more than one of these over the course of the proof.

• Other proof types
1. Proof by Construction

- **Used for:** A conjecture states that a particular type of object exists.
- **Proof goal:** Demonstrate how to construct such an object.
1. Proof by Construction

• Prove the following:
  If $a$ and $b$ are consecutive integers, then the sum $a+b$ is odd.

**Definition:** An integer number is **odd** if and only if there exists an integer $k$ such that $n = 2k+1$.

**Definition:** Two integers $a$ and $b$ are **consecutive** if and only if $b = a+1$.

**Proof:** Assume that $a$ and $b$ are consecutive integers. Because $a$ and $b$ are consecutive, we know that $b = a+1$. Thus, the sum $a+b$ may be re-written as $a+(a+1) = 2a+1$. Thus, there exists a number $k$ such that $a+b = 2k+1$, so the sum $a+b$ is odd. ■
2. Proof by Contradiction

- **Used for:** A conjecture states that a particular statement is true.
- **Proof goal:** Assume that the statement is false, then show that if it were false, it would lead to absurd or unworkable conclusions.
2. Proof by Contradiction

• Prove the following:

\[ \sqrt{2} \text{ is irrational.} \]

**Definition:** A number is **rational** if it can be written as \( m/n \), where \( m, n \in \mathbb{Z} \).

**Definition:** An integer number is **even** if and only if there exists an integer \( k \) such that \( n = 2k \).

**Proof:** Assume to reach a contradiction that \( \sqrt{2} \) is rational. Thus, \( \sqrt{2} = m/n \) for some integers \( m \) and \( n \). If both \( m \) and \( n \) are divisible by the same integer greater than 1, divide both by that integer. Doing so doesn’t change the value of the fraction. Now, at least one of \( m \) and \( n \) must be an odd number.
2. Proof by Contradiction

Without changing the equality of the equation, we can multiply both sides by \( n \) to obtain \( n\sqrt{2} = m \).

Also without changing the equality of the equation, we can square both sides to obtain \( 2n^2 = m^2 \). Because \( m^2 \) is 2 times the integer \( n \), we know that \( m^2 \) is even. Therefore, \( m \) is also even, because the square of an odd number is always odd. So, we can write \( m = 2k \) for some integer \( k \). Then, substituting \( 2k \) for \( m \), we get \( 2n^2 = (2k)^2 = 4k^2 \).

Dividing both sides by 2, we obtain \( n^2 = 2k^2 \). This result shows that \( n^2 \) is even, and hence that \( n \) is even. But we had earlier reduced \( m \) and \( n \) so that they were not both even, yielding a contradiction. \( \blacksquare \)
3. Proof by Induction

- **Used for:** A conjecture states that a particular statement is true for all members of a set.

- **Proof goal:** Demonstrate that the proof is true for one member, and that it also holds for the next member.
  
  - Show that it’s true for \( k = 1 \). (*basis*)
  
  - Show that, if it’s true for \( k \), then it’s true for \( k+1 \). (*induction*)
3. Proof by Induction

• Prove the following:

If $a$ and $b$ are consecutive integers, then the sum $a+b$ is odd.

Proof: Define the function $F(x)$ to be true when the sum of $x$ and its successor is odd.

Basis: Consider the proposition $F(1)$. The sum $1+2 = 3$ is odd because we can demonstrate that $3$ is an odd number: $3 = 2(1) + 1$. Thus, $F(x)$ is true when $x = 1$.

Induction: Assume that $F(x)$ is true for some $x$. Thus, for some $x$, we have that $x+(x+1)$ is odd. We add one to both $x$ and $x+1$, which gives the sum $(x+1) + ((x+1)+1) = (x+1)+(x+2)$. 
3. Proof by Induction

We claim two things. First, we claim that the sum \((x+1)+(x+2) = F(x+1)\).

Second, we claim that adding two to any integer does not change that integer’s evenness or oddness. With these two observations, we claim that \(F(x)\) is odd implies \(F(x+1)\) is odd.

By the principle of mathematical induction, we thus claim that \(F(x)\) is odd for all integers \(x\). Thus, the sum of any two consecutive numbers is odd. ■
Any Questions?

HOMEWORK (due 9/2)

2nd edition: 0.10, 0.11
3rd edition: 0.10, 0.12

Prove: The sum of any two even integers is also even.

Prove: \(1+2+3+\ldots+n = \frac{n(n+1)}{2}\). (HINT: use induction)

Prove: If \(a,b \in \mathbb{Z}\), then \(a^2 - 4b \neq 2\). (HINT: use contradiction)