Inductive Proofs Must Have

- Base Case (value):
  - where you prove it is true about the base case
- Inductive Hypothesis (value):
  - where you state what will be assume in this proof
- Inductive Step (value):
  - show:
    - where you state what will be proven below
  - proof:
    - where you prove what is stated in the show portion
    - this proof must use the Inductive Hypothesis sometime during the proof

Prove this statement: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Base Case (n=1): $\sum_{i=1}^{1} i = 1$ $\qquad \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{2}{2} = 1$

Inductive Hypothesis (n=p): $\sum_{i=1}^{p} i = \frac{p(p+1)}{2}$

Inductive Step (n=p+1):

Show: $\sum_{i=1}^{p+1} i = \frac{(p+1)((p+1)+1)}{2}$

Proof:(in class)

Variations

- 2+4+6+8+…+20 = ??
- If you can use the fact:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

- Rearrange it into a form that works.
- If you can't – you must prove it from scratch

Less Mathematical Example

- If all we had was 2 and 5 cent coins, we could make any value greater than 3.

- Base Case (n = 4):
- Inductive Hypothesis (n=k):
- Inductive Step (n=k+1):

  show:

  proof:

More Examples to be done in class

- $\forall n \in Z^{\geq 1}, 3 \mid (n^3 - n)$
- $\forall n \in Z^{\geq 0} \sum_{k=0}^{n} 2^k = 2^{n+1} - 1$
- Geometric Progression

$$\forall r \in R^{>1} \forall a \in R \forall n \in Z^{\geq 0}, \sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}$$

Proving Inequalities with Induction

- Inductive Hypothesis
  - has the form y<z
- Inductive Step
  - needs to prove something of the form x<z
- Two methods for the proof part
  - use whichever you like
  - transitivity
    - find a value between (b)
    - prove that b < z
    - prove that x < b
  - book method
    - Substitute "unequals" as long as the signs don't change

    or
    - Add unequals to unequals as long as always adding correct sides

Prove this statement:

$$\forall n \in Z^{\geq 3}, 2n+1 \leq 2^n$$

Base Case (n=3): $LHS: 2(3)+1 = 6+1 = 7$

$RHS: 2^3 = 8$ $\quad LHS \leq RHS$

Inductive Hypothesis (n=k):

$$2k+1 \leq 2^k$$

Inductive Step (n=k+1):

Show:

$$2(k+1)+1 \leq 2^{k+1}$$

Proof:(both methods done in class)

Another Example with inequalities

$$\forall n \in Z^{\geq 2} \forall x \in Z^{>-1}, 1+nx \leq (1+x)^n$$

Strong Induction

- Implication changes slightly
  - if true for all lesser elements, then true for current
- P(i) $\forall i \in Z\ a \leq i < k \rightarrow P(k)$
- P(i) $\forall i \in Z\ a \leq i \leq k \rightarrow P(k+1)$

Regular Induction

- $P(k) \rightarrow P(k+1)$
- $P(k-1) \rightarrow P(k)$

Recurrence Relation Example

- Assume the following definition of a function:

$$a_0 = 1 \qquad a_1 = 1 \qquad a_2 = 3$$

$$\forall k \in Z^{\geq 3}, a_k = a_{k-1} + a_{k-2} - a_{k-3}$$

- Prove the following definition property:

$$\forall n \in Z^{\geq 0}, a_n \in Z^{odd}$$

All Integers greater than 1 are divisible by a prime

Base Case (n=2):

$2|2 \quad 2 \in Z^{prime}$

Inductive Hypothesis (n=i $\forall$i $2 \leq i < k$):

$\exists p \in Z^{prime} \quad p|i$

Inductive Step (n=k):

show: $\exists p \in Z^{prime} \quad p|k$

proof:

A Factorial Example

$$\forall n \in Z^{\geq 2}, \frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$$

Another Example

- Assume the following definition of a recurrence relation:

$$a_1 = 0$$
$$a_2 = 2$$
$$\forall i \in Z^{\geq 3}, a_i = 3a_{\left\lfloor \frac{i}{2} \right\rfloor} + 2$$

- Prove that all elements in this relation have this property:

$$\forall n \in Z^{\geq 1}, a_n \in Z^{even}$$

Well-Ordering Principle

- For any set S of
  - one or more
  - integers
  - all larger than some value
- S has a least element

Use this to prove the Quotient Remainder Theorem

- The quotient-remainder theorem said
  - Given
    - any positive integer n
    - and any positive integer d
  - There exists an r and a q
    - where $n = dq + r$
    - where $0 \leq r < d$
    - which are integers
    - which are unique

Steps to proving the quotient-remainder theorem

- Define S as the set of all non-negative integers in the form n-dk (all integers k)
- Prove that it is non-empty
- Prove that we can apply the Well-Ordering Principle
- Then it has a least element
- Prove that the least element (r) is $0 \leq r < d$