1.2: Induction and the Division Algorithm

April 12, 2012

Outline

1. Induction

2. Divisibility
   - What is divisibility?
   - Some Notational Examples
   - The Division Algorithm

Induction overview

In induction we will cover:

- When to use induction
- What is induction
- Examples

When to use Induction

Induction:

- Used to prove incrementally.
- Useful when a fact is parameterizable by an integer.
- Often used to prove formula for sums.
- Can also be used to prove facts about integers of a certain form.

What is induction

- Is a fundamental fact of the natural numbers.
- Statement: If S is a set and
  - $0 \in S$
  - $n \in S$ implies $n + 1 \in S$.

  then S is all natural numbers.

Induction Example

Prove $\sum_{k=0}^{n} k = \binom{n+1}{2}$

- for $n = 1$, $1 = \binom{2}{2} = 1$
-

$$\begin{aligned}
\sum_{k=0}^{n+1} k &= \sum_{k=0}^{n} k + n + 1 \\
&= \binom{n+1}{2} + n + 1 \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+2)(n+1)}{2} \\
&= \binom{n+2}{2}.
\end{aligned}$$

Overview

- Definition: What is divisibility?
- Some notational examples
- The division algorithm

Outline

1. Induction

2. Divisibility
   - What is divisibility?
   - Some Notational Examples
   - The Division Algorithm

Definition

An integer b is divisible by an integer a, not zero, if there is an integer x such that $b = ax$, and we write $a|b$.

Examples

- $1|x$ for all x
- $-1|x$ for all x
- $x|0$ for all $x \neq 0$.
- $a| \pm ab$ for all b and $a \neq 0$.

Proper Divisor

If $a|b$ and $0 < a < b$ then a is a proper divisor of b.

- 12 has $1, 2, 3, 4, 6$ as proper divisors.
- 1 has no proper divisors.

Outline

Arbitrary constants

$$a|b \implies a|bc \text{ for all integer } c.$$

Thus if a divides b, we can add whatever factors we want to b and a will still divide it.

$$3|6 \implies 3|12, 3|18, 3|24, \ldots$$

Proof

$$a|b \implies b = ax$$

$$cb = cax = (cx)a$$

$$a|bc$$

Transitivity

$$a|b, b|c \implies a|c$$

This is the often known transitivitity.

- Note $b \neq 0$ (since 0 divides nothing).
- Otherwise, since $x|0$ for all 0, we could have $x|0$, $0|y$ and thus $x|y$ for all x and y.

Proof

$$a|b, b|c \implies b = ax, c = by$$

$$c = by = axy = a(xy)$$

$$a|c$$

Linear Combinations

$$a|b, a|c \implies a|(bn + cm)$$

Thus a divides the lattice generated by b and c. Hence we can picture this with some geometry if we wanted.

Proof

$$a|b, a|c \implies b = ax, c = ay$$

$$bn = a(xn), cm = a(ym)$$

$$bn + cm = a(xn + ym)$$

$$a|(bn + cm)$$

Trivialities

$$a|b, b|a \implies a = \pm b$$

$$a|b, a > 0, b > 0, \implies a \le b$$

Proof

$$a|b \implies b = ax$$

$$b|a \implies a = by$$

$$a = by = axy$$

$$1 = xy$$

Since x y are integers, then $x, y = \pm 1$.

Multiplicative constants

$$m \neq 0, a|b \implies ma|mb$$

Thus by adding the same factors to both sides, we preserve divisibility. (Golden Rule?)

Proof

$$a|b \implies b = ax$$

$$mb = max$$

$$ma|mb$$

Outline

1. Induction
2. Divisibility
   - What is divisibility?
   - Some Notational Examples
   - The Division Algorithm

Statement

Given integers a, b, with $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r < a$.

$$25 = 7 \cdot 3 + 4$$

Notice that only certain *r*s are possible, and they are unique.

$$a = 4, r = 0, 1, \ldots, 3$$

b	r
0	0
1	1
2	2
3	3
4	0
5	1
6	2