Proofs, Number Theory

June 18, 2014

Yesterday

- To prove a universal ($\forall$) statement, state the hypothesis, use definitions, and manipulate expressions until you verify the conclusion.
- To prove an existential ($\exists$) statement, just give an example.
- To disprove a statement, prove the negation.
- Try rephrasing the claim or breaking things down into cases if you're stuck.

Proof by contrapositive

Proposition

If a and b are integers and $a + b \geq 15$, then either $a \geq 7$ or $b \geq 8$

Contrapositive

$\forall a, b \in \mathbb{Z}, \neg(a \geq 7 \vee b \geq 8) \rightarrow \neg(a + b \geq 15)$.

1. We must show
   $\forall a, b \in \mathbb{Z}, (\neg(a \geq 7) \wedge \neg(b \geq 15)) \rightarrow \neg(a + b \geq 15)$.
2. ...or $\forall a, b \in \mathbb{Z}, (a < 7 \wedge b < 8) \rightarrow a + b < 15)$.

Proof: If $a < 7$ and $b < 8$, then $a + b < 7 + 8 = 15$.

Proving bi-conditionals

To prove "P if and only if Q," we must prove both "if P, then Q" and "if Q then P."

Proposition

For all integers k, $k^2 + 4k + 6$ is odd if and only if k is odd.

Proof:

Working backwards

Proposition

If x and y are positive real numbers, then $\frac{x+y}{2} \geq \sqrt{xy}$.

Proof:

Statements with both $\forall$ and $\exists$

Proposition

For all real numbers x and y, if x and y are positive, then there exists a real number z such that $x = yz$.

Proof:

Proposition

There exists $n \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, we have $10n \leq m$.

Proof:

Things to prove or disprove

- For any integers j and k, if j is even or k is even, then jk is even.
- Disprove: If k is rational, then k^3/k is rational.
- If m and n are integers and perfect cubes, then mn is a perfect cube.

Number theory

- **Number theory** is the study of integers.
- *"Mathematics is the queen of the sciences and number theory is the queen of mathematics." - Carl Friedrich Gauss*

Divisibility

Definition

If a and b are integers and $b = an$ for some integer n, then a **divides** b, a is a **factor** of b, and b is a **multiple** of a.

- Notation: $a \mid b$.
- Example: $7 \mid 0$, $3 \mid 12$, $-3 \mid 12$, $3 \mid -12$, $-3 \mid -12$.
- Non-example: $0 \nmid 7$, $6 \nmid 10$

Divisibility

Proposition

If a, b, and c are integers, $a \mid b$, and $b \mid c$, then $a \mid c$.

Example: $3 \mid 15$, $15 \mid 30$, and $3 \mid 30$
Proof:

Divisibility

Proposition

If a, b, and c are integers, $a \mid b$, and $a \mid c$, then $a \mid (b+c)$.

Example: $4 \mid 8$, $4 \mid 40$, and $4 \mid 48$.
Proof:

Division Algorithm

Theorem

If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exists a unique pair of integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

"Unique" means that there is only one such pair q, r.

Definition

In the above theorem, q is the **quotient** and r is the **remainder**.
Notation: $q = a$ div b and $r = a$ mod b.

Example: If $a = 98$ and $b = 10$, then $q = 9$ and $r = 8$.
Proof of theorem: Let $q = \lfloor a/b \rfloor$ and $r = a - bq$...

Greatest common divisor

Definition

If a and b are natural numbers, the **greatest common divisor** (GCD) of a and b, denoted $\gcd(a, b)$, is the largest number that divides both a and b.

Definition

Natural numbers a and b are **relatively prime** if $\gcd(a, b) = 1$.

Note: In this class, 0 is a natural number.
Examples:
$\gcd(4, 12) = \gcd(12, 4) = \gcd(-4, 12) = \gcd(-12, 4) = 4$,
$gcd(20, 0) = 20$.

GCD example

Definition

A positive integer $p \geq 2$ is **prime** if its only positive factors are itself and 1.

To find $\gcd(180, 48)$, find prime factorizations of 180 and of 48, and see what's in common...

...but in general, finding factors takes too long.

Euclid's Algorithm

Assume $a \geq b$.

EuclidAlg(a,b)

- If $b = 0$
    - Return a
- Else
    - Return EuclidAlg(b, a mod b)

Reminder: a mod b is the remainder when a is divided by b.
Example: Find $\gcd(662, 414)$