Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 2

Divisibility Theorems

Let $a, b, c \in \mathbb{Z}$.

1. Bounds by Divisibility (BBD): $(a \mid b \wedge b \neq 0) \Rightarrow |a| \leq |b|$
2. Transitivity of Divisibility (TD): $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$
3. Divisibility of Integer Combinations (DIC): $(a \mid b \wedge a \mid c) \Rightarrow \forall x, y \in \mathbb{Z}\ a \mid bx + cy$

Proof of DIC: Assume that $a \mid b$ and $a \mid c$. Then there exist integers m and n such that $am = b$ and $an = c$. Then for any x and y integers,

$$bx + cy = amx + any = a(mx + ny)$$

and hence $a \mid bx + cy$.

DIC Example

If $5 \mid a + 2b$ and $5 \mid 2a + b$, then $5 \mid (a + 2b)(2) + (2a + b)(-1)$ and simplifying shows that $5 \mid 3b$.

Converses

Definition: Let A, B be statements. The *converse* of $A \Rightarrow B$ is $B \Rightarrow A$.

Example The converse of Bounds by Divisibility (BBD) is

$$|a| \leq |b| \Rightarrow a \mid b \wedge b \neq 0$$

If and only if

If and only if $A \Leftrightarrow B$, A iff B, A if and only if B.

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Exercise: Show that $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

Sets

A *set* is a collection of elements.

1. $\mathbb{N} = \{1, 2, ...\}$
2. $\mathbb{Q} = \{a/b \in \mathbb{R} : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b \neq 0\}$
3. $\{\}$, $\emptyset$, $\{\emptyset\}$
4. $x \in S$ and $x \notin S$ (Important for proofs with sets)

Other Set Examples

1. Set of even numbers between 5 and 14 (inclusive).

   $\{6, 8, 10, 12, 14\}$ or $\{n \in \mathbb{N} : 5 \leq n \leq 14 \wedge 2 \mid n\}$
2. All odd perfect squares.

   $\{(2k+1)^2 : k \in \mathbb{Z}\}$ (or $\mathbb{N}$ overlap doesn't matter!)

Set Operations

Let S and T be sets. Define

1. $\#S$ or $|S|$. Size of the set S.
2. $S \cup T = \{x : x \in S \vee x \in T\}$ (Union)
3. $S \cap T = \{x : x \in S \wedge x \in T\}$ (Intersection)
4. $S - T = \{x \in S : x \notin T\}$ (Set difference)
5. $\bar{S}$ or S^c (with respect to universe U) the complement of S, that is
$$S^c = \{x \in U : x \notin S\} = U - S$$
6. $S \times T = \{(x, y) : x \in S \wedge y \in T\}$ (Cartesian Product)

More Set Terminology

Let S and T be sets. Then

1. $S \subseteq T$: S is a subset of T. Every element of S is an element of T.
2. $S \subsetneq T$: S is a proper/strict subset of T. Every element of S is an element of T and some element of T is not in S.
3. $S \supseteq T$: S contains T. Every element of T is an element of S.
4. $S \supsetneq T$: S properly/strictly contains T. Every element of T is an element of S and some element of S is not in T.
5. $S = T$ means $S \subseteq T$ and $T \subseteq S$.

Sets and If and Only If

Show $S = T$ if and only if $S \cap T = S \cup T$.

Proof:

- Suppose $S = T$. To show $S \cap T = S \cup T$ we need to show that $S \cap T \subseteq S \cup T$ and that $S \cap T \supseteq S \cup T$.
- First suppose that $x \in S \cap T$. Then $x \in S$ and $x \in T$. Hence $x \in S \cup T$.
- Next, suppose that $x \in S \cup T$. Then $x \in S$ or $x \in T$. Since $S = T$ we have in either case that $x \in S$ and $x \in T$. Thus $x \in S \cap T$. This shows that $S \cap T = S \cup T$ and completes the forward direction.
- Now assume that $S \cap T = S \cup T$. We want to show that $S = T$ which we do by showing that $S \subseteq T$ and $T \subseteq S$.
- First, suppose that $x \in S$. Then $x \in S \cup T = S \cap T$. Hence $x \in T$.
- Next, suppose that $x \in T$. Then $x \in S \cup T = S \cap T$. Hence $x \in S$. Therefore, $S = T$.

Quantified Statements

1. $\forall$ For all
2. $\exists$ There exists

Prove $\forall n \in \mathbb{N}$, $2n^2 + 11n + 15$ is composite.
Proof: Let n be an arbitrary natural number. Then factoring gives $2n^2 + 11n + 15 = (2n+5)(n+3)$. Since $2n + 5 > 1$ and $n + 3 > 1$, we have $2n^2 + 11n + 15$ is composite.

Prove $\exists k \in \mathbb{Z}$ such that $6 = 3k$.
Proof: Since $3 \cdot 2 = 6$, we see that $k = 2$ satisfies the given statement.

Assuming a For All Statement

Let $a, b, c \in \mathbb{Z}$. If $\forall x \in \mathbb{Z}$, $a \mid (bx + c)$ then $a \mid (b + c)$.

Proof: Assume $\forall x \in \mathbb{Z}$, $a \mid (bx + c)$. Then, for example, when $x = 1$, we see that $a \mid (b(1) + c)$. Thus $a \mid (b + c)$.

Domain Is Important!

Let $P(x)$ be the statement $x^2 = 2$ and let

$$S = \{\sqrt{2}, -\sqrt{2}\}.$$

Which of the following are true?

1. $\exists x \in \mathbb{Z}, P(x)$
2. $\forall x \in \mathbb{Z}, P(x)$
3. $\exists x \in \mathbb{R}, P(x)$
4. $\forall x \in \mathbb{R}, P(x)$
5. $\exists x \in S, P(x)$
6. $\forall x \in S, P(x)$

Solution:

1. False
2. False
3. True
4. False
5. True
6. True

Approaching Quantified Statement Problems

1. A single counter example shows $(\forall x \in S, P(x))$ is false.
   Claim: Every positive even integer is composite.
   This claim is false since 2 is even but 2 is prime.
2. A single example does not prove that $(\forall x \in S, P(x))$ is true.
   Claim: Every even integer at least 4 is composite.
   This is true but we cannot prove it by saying "6 is an even integer and is composite." We must show this is true for an arbitrary even integer x. (Idea: $2 \mid x$ so there exists a $k \in \mathbb{N}$ such that $2k = x$ and $k \neq 1$.)
3. A single example does show that $(\exists x \in S, P(x))$ is true.
   Claim: Some even integer is prime.
   This claim is true since 2 is even and 2 is prime.
4. What about showing that $(\exists x \in S, P(x))$ is false?
   Idea: $(\exists x \in S, P(x))$ is false $\equiv \forall x \in S, \neg P(x)$ is true. This idea is central for proof by contradiction which we will see later.

Negating Quantifiers

1. Everybody in this room was born before 2010.
   Solution: Somebody in this room was not born before 2010.
2. Someone in this room was born before 1990
   Solution: Everyone in this room was born after 1990.
3. $\forall x \in \mathbb{R}, |x| < 5$
   Solution: $\neg(\forall x \in \mathbb{R}, |x| < 5) \equiv \exists x \in \mathbb{R}, |x| \geq 5$
4. $\exists x \in \mathbb{R}, |x| \leq 5$
   Solution: $\neg(\exists x \in \mathbb{R}, |x| \leq 5) \equiv \forall x \in \mathbb{R}, |x| > 5$

Order Matters!

1. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$
2. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$
3. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 = 1$
4. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1$

1. False (Choose $x = y = 0$)
2. True (Choose $x = 1$ and $y = 0$)
3. True. **Proof:** Let $x \in \mathbb{R}$ be arbitrary. then choose $y = \sqrt[3]{x^3 - 1}$. Then
$$x^3 - y^3 = x^3 - (\sqrt[3]{x^3 - 1})^3 = x^3 - (x^3 - 1) = 1$$
4. False. Idea: Negate and show the negation is true!
$$\neg(\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x^3 - y^3 = 1) \equiv \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^3 - y^3 \neq 1$$
Proof: Let $x \in \mathbb{R}$ be arbitrary. Take $y = x$. Then $x^3 - y^3 = x^3 - x^3 = 0 \neq 1$.