09/21/2022

→ STYLE CHANGES
→ INTRO TO SETS cont.
→ NUMBER THEORY
→ THING I DIDN'T KNOW WHERE TO PUT

STYLE CHANGES

We are changing how we want you to format multiple quantifiers. Earlier, we had asked for...

$$(\forall s \in S, \exists t \in T)[P(s,t)] \quad \times$$

However, we feel that this format implies some seperation between the quantifiers and predicate which is... inaccurate.

We would rather have our format imply that a predicate + inner-quantifier is itself a predicate which the outer-quantifier acts on. The following format is more representative of this...

$$(\forall s \in S(\exists t \in T(P(s,t)))) \quad \checkmark$$

But, this is kinda ugly, so we're recommending you submit your answers formatted as...

$$\forall s \in S, \exists t \in T, P(s,t) \quad \checkmark \text{ - preferred}$$

This isn't as bad to look at and doesn't imply any false seperation. This is the recommeded format and the one instructors will stick to. We will also accept...

$$(\forall s \in S)(\exists t \in T)[P(s,t)] \quad \checkmark$$

Again, we are most up-to-date via the Style Guide on the class website, which you should be checking frequently.

INTRO TO SETS (cont.)

Last discussion we introduced multiple ways to define sets. We now define operations/operators we use with sets. We define $U :=$ universal set:

INTERSECTION $\quad A \cap B \equiv \{x \in U \mid x \in A \wedge x \in B\}$

UNION $\quad A \cup B \equiv \{x \in U \mid x \in A \vee x \in B\}$

COMPLIMENT $\quad A^c \equiv \{x \in U \mid x \notin A\}$

SET MINUS $\quad A \setminus B \vee A - B \equiv \{x \in U \mid x \in A \wedge x \notin B\}$

Take note that 3 of the operations above are analogous to our $\wedge, \vee, \neg$ operators in propositional logic.

EQUIVALENCE $\quad A \equiv B \iff \forall x \in U, x \in A \iff x \in B$

EMPTY SET $\quad \emptyset \equiv \{\}$, the set with no elements

SUBSET $\quad A \subseteq B \iff \forall x \in U, x \in A \Rightarrow x \in B$

PROPER SUBSET $\quad A \subset B \iff A \subseteq B \wedge A \not\equiv B$

the biconditional is equivalent to equivalence which is why I've used them interchangebly

PRACTICE

$74.5 \in \mathbb{Z}$ FALSE

$\{3,4\} \in \{\emptyset, \{3,4\}\}$ TRUE

$\emptyset \in \{\}$ FALSE

$\emptyset \subseteq \emptyset$ TRUE

NUMBER THEORY

We're about to start proofs, but we need something to write proofs about right? We introduce number theory, the study of numbers, primarily the integers.

Today we introduce key concepts, namely parity, modular arithmetic, divisibility, and primes/composites, as a rich canvas for you to understand and perform proofs on later.

PARITY

This simply refers to if an integer is even or odd:

$$x \text{ is even} \iff \exists k \in \mathbb{Z},\ x = 2k$$

$$x \text{ is odd} \iff \exists k \in \mathbb{Z},\ x = 2k+1$$

MODULAR ARITHMETIC

We define the mod operator such that for an integer x,

$$x \bmod m = y \quad \text{s.t} \quad y \in \mathbb{N}^{<m} \wedge \exists k \in \mathbb{Z},\ x = y + mk$$

We say that two integers x, y are equivalent mod m if and only if there exists some integer k such that $x = y + km$.

$$x \equiv y \pmod{m} \iff \exists k \in \mathbb{Z},\ x = y + km$$

You are probably familiar with mod via % infix operator from programming languages. It's worth stressing that equivalent mod m is a <u>statement</u>. You can prove that

$$x \equiv y \pmod{m} \iff x \,\%\, m = y \,\%\, m$$

Note, we will NOT use nor accept % as mod in this class, it is utilized here to bridge the gap between your background understanding and where we need you to be.

DIVISIBILITY

Given two integers a, b we say that a divides b or b is divisible by a if and only if there exists an integer k such that $b = ak$:

$$a \mid b \iff \exists k \in \mathbb{Z},\ b = ak$$

PRIMES / COMPOSITES

We classify an integer n as prime if and only if it is divisible only by 1 and n. We classify n as a composite if it is not prime:

$$n \text{ is prime} \iff \forall x \in \mathbb{Z},\ x = 1 \lor x = n \lor x \nmid n$$

$$n \text{ is composite} \iff \exists x \in \mathbb{Z},\ x \neq 1 \land x \neq n \land x \mid n$$

THING I DIDN'T KNOW WHERE TO PUT

Something you need to be aware of is the idea of closure. I wasn't sure where to classify it since it technically applicable to any set, but in this course its most often seen in regard to number theory.

We say a set is closed under a given operation if performing said operation on members of that set produces an output also in said set. For binary operators (2 inputs, by far the most common), we can quantify this as...

$$S \text{ is closed under } * \iff \forall a, b \in S,\ a * b \in S$$

Note, the integers $\mathbb{Z}$ are closed under addition and multiplication. This is an important fact which we won't have you prove, but will require you cite when relevant.

PRACTICE

Give an equivalent statement for $x|n$ using modular arithmetic.

$$x|n \iff 0 \equiv n \pmod{x} \iff n \bmod x = 0$$

State if $\mathbb{Z}^{EVEN}$ and $\mathbb{Z}^{ODD}$ are closed under addition and multiplication.

$\mathbb{Z}^{EVEN}$ closed under $+, \times$

$\mathbb{Z}^{ODD}$ closed under $\times$

Get creative and define $\mathbb{Z}^{EVEN}$ and $\mathbb{Z}^{ODD}$ in as many unique ways as you can using the set definition methodologies from last discussion:

$\mathbb{Z}^{EVEN}$: $\{2n \mid n \in \mathbb{Z}\}$, $\mathbb{Z} \setminus \mathbb{Z}^{ODD}$, $\{\ldots, -4, -2, 0\ 2, 4, \ldots\}$

$\{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\}$, $\{x \in \mathbb{Z} \mid 2|x\}$

$\mathbb{Z}^{ODD}$: $\{2n+1 \mid n \in \mathbb{Z}\}$, $\mathbb{Z} \setminus \mathbb{Z}^{EVEN}$, $\{\ldots, -3, -1\ , 1, 3, \ldots\}$

$\{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\}$, $\{x \in \mathbb{Z} \mid 2|x+1\}$