Announcements

- HW #1 is due Tomorrow. Be sure to identify the page where each problem resides.

- HW #2 will be available by tomorrow evening.

- In proofs, work your way from premises toward the conclusion. (Don’t work backwards!)

More Practice Translating

For these examples, the domain is natural numbers ($\mathbb{N}$). We may use quantifiers, variables, the symbols +, -, ×, ÷, =, <, >, and constants like 1 or 57.

Predicates:

- Recall: x is composite
- x is prime
- x is the sum of three primes

Statement (Vinogradov's Theorem):

- Every sufficiently large odd number is the sum of three primes.

Even *More* practice

Let C = {Creatures on Earth}
Let U(x) = "x is a Unicorn", where x $\in$ C

Find statements for these:

- There are no Unicorns
- There is at least one Unicorn
- There is at most one Unicorn
- There are exactly one Unicorn
- There are at least two Unicorns
- There are exactly two Unicorns

Free/Bound variables and Statements

Variables that are not “bound” by quantifiers are called **free variables**.

Let P(x) be some predicate defined over domain $\mathbb{R}$.
Which of these are predicates, and which are statements?

- P(x)
- P(7.2)
- $(\forall x)$ [P(x)]
- $(\exists x)$ [P(x)]
- $(\forall x,y)$[P(x) v P(y)] ^ ~P(z)
- $(\forall x)$[~P(x)] $\rightarrow$ $(\exists y)$ [P(y)] ^ ~P(3.7)

Interpretations

In predicate logic an "Interpretation" is an assignment of meaning to the predicate symbols and a choice of domain(s). Consider:

$(\forall x)(\exists y)\ [P(x,y)]$

- What does this say in English?

- Discuss each assignment for P, below, over each of the domains $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$:

P(a, b) means "$a + b = 0$"
P(a, b) means "b > a and there is no element between a and b"
P(a, b) means "b < a and there is no element between a and b"
P(a, b) means "$a * a = b$"
P(a, b) means "$b * b = a$"

Rules of inference for quantified statements

Existential Generalization

$\underline{P(a) \text{ for some } a \in D}$

$\therefore (\exists x \in D)\,[P(x)]$

Universal Instantiation

$\underline{(\forall x \in D)\,[P(x)]}$

$\therefore P(a) \text{ for any particular } a \in D$

Universal Generalization

Universal Generalization

P(a) for some $a \in D$ (selected arbitrarily)

$\therefore (\forall x \in D)\ [P(x)]$

Is this proof valid?	**Is this proof valid?**
Let $a \in \mathbb{N}$ (selected arbitrarily) ... P(a) $\therefore (\forall x \in \mathbb{N})\ [P(x)]$	Let $a \in \mathbb{N}$ such that a is even. ... P(a) $\therefore (\forall x \in \mathbb{N})\ [P(x)]$

Existential Instantiation

Existential Instantiation

$(\exists x \in D)\ [P(x)]$

$\therefore$ P(a) for *some* $a \in D$

Is proof valid?

Let $a = 7$

…

$(\exists x \in D)\ [P(x)]$

$\therefore P(a)$

Unit 4
Methods of Proof

Definitions

$\mathbb{N}$ – Natural numbers {0, 1, 2, 3…}
$\mathbb{Z}$ – Integers {…−3, −2, −1, 0, 1, 2, 3…}
$\mathbb{R}$ – Real numbers
$\mathbb{Q}$ – Rational numbers (Real numbers than can be expressed as the quotient of two integers, with a non-zero denominator)

What are "irrational numbers"?

What do these mean?

- $\mathbb{R}^+$
- $\mathbb{Q}^-$
- $\mathbb{N}^{>2}$
- $\mathbb{Z}^{\text{even}}$
- $\mathbb{N}^{\text{prime}}$

Closure

We say a set (D) is **closed** under an binary operation (*) if:

$(\forall a,b \in D)[\ a*b \in D]$

Which operations are closed in which domains?

	$\mathbb{R}^+$	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}^{>0}$
+				
-				
*				
/				
exponentiation				

Number Theory

The study of the properties of *Natural Numbers* (ℕ) is called **Number Theory**.

- Number Theory is the perfect environment for learning to write proofs!

- Number Theory is also intertwined with Computer Science
  - Cryptography
  - Data compression
  - Hash functions
  - Random number generation
  - Network protocols
  - "...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations.“
    - Donald Knuth

Divisibility, Multiples and Factors

Let a,b,c $\in \mathbb{N}$ such that a * b = c.

We may say (all of these are equivalent):

“b is a **factor** of c”
“b is a **divisor** of c”
“b **divides** c”
“c is a **multiple** of b”
“c is **divisible** by b”

Even and Odd

We say $n \in \mathbb{Z}$ is **even** when n is a multiple of 2.

More formally:

$n \in \mathbb{Z}$ is even if and only if $(\exists k \in \mathbb{Z})$ [n = 2k]

We say $n \in \mathbb{Z}$ is **odd** when n is not even.

Alternatively:

$n \in \mathbb{Z}$ is odd if and only if $(\exists k \in \mathbb{Z})$ [n = 2k + 1]