Week 3 Part A highlights

- Determine what evidence is required to establish that a quantified statement is true or false.
- Use logical equivalence to rewrite quantified statements (including negated quantified statements)
- Use universal generalization to prove that universal statements are true
- Define predicates associated with integer factoring and primes
- Define “arbitrary”
- Write proofs in prose form
- Determine whether a proposition is true or false using valid reasoning (proofs) in multiple contexts
- Trace and/or construct a direct proof and proof by contrapositive
- Work to prove/disprove in parallel
- Evaluate which proof technique(s) is appropriate for a given proposition

Some sets of numbers

$\mathbb{N}$	The set of natural numbers	$\{0, 1, 2, 3, \ldots\}$	*Recursively defined by* Basis step: Recursive step:
$\mathbb{Z}$	The set of integers	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$	*Recursively defined by* Basis step: Recursive step:
$\mathbb{Z}^+$	The set of positive integers	$\{1, 2, 3, \ldots\}$	*Set builder notation definition is* $\{x \in \mathbb{N} \mid x > 0\} = \{x \in \mathbb{Z} \mid x > 0\}$
$\mathbb{Z}^{\neq 0}$	The set of nonzero integers		*Set builder notation definition is* $\{x \in \mathbb{Z} \mid (x < 0 \lor x > 0)\}$

Axioms: Statements assumed to be true

Invariant: A property that is true about our algorithm no matter what. Rosen p375

Theorem: Statement that can be shown to be true, usually an important one. Rosen p81

Less important theorems can be called **proposition**, **fact**, **result**.

A less important theorem that is useful in proving a theorem is called a **lemma**.

A theorem that can be proved directly after another one has been proved is called a **corollary**

Proof: Series of steps, each of which follows logically from axioms, or previously proved theorems, whose final step should result in the statement of the theorem being proven.

Some axioms about the numbers (zyBook 4.3.1)

- Rules of Algebra. For example, if x, y, and z are real numbers and $x = y$, then $x + z = y + z$.
- The set of integers is closed under addition, multiplication, and subtraction.
- Every integer is either even or odd.
- If x is an integer, there is no integer between x and $x + 1$. In particular, there is no integer between 0 and 1.
- The relative order of any two real numbers. For example $1/2 < 1$ or $4.2 \geq 3.7$.
- The square of any real number is greater than or equal to

Application: Factoring

Goal: Exchange information (e.g. key for cipher) with a stranger (Amazon, Venmo) without other observers accessing it

Mathematical tool: It is much easier to multiply two large numbers than to factor a large number.

Key idea behind RSA (Rivest Shamir Adelman) Algorithm:

- Amazon picks two primes > 200 digits each, publishes their product
- Anyone can encrypt their credit card using this product.
- There are no known methods to decrypt without factoring into the original primes.
- Current algorithms for factoring products of large primes take billions of years

Definition (Rosen p. 238): When a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$.

Symbolically, $F(a,b) =$ ________________________ and is a predicate over the domain ____________

Other (synonymous) ways to say that $F(a,b)$ is true:

a is a **factor** of b $\quad$ a is a **divisor** of b $\quad$ b is a **multiple** of a $\quad$ $a|b$ $\quad$ b **mod** $a = 0$

Translate these quantified statements by matching to English statement on right.

$\exists a \in \mathbb{Z}^{\neq 0}\ (\ F(a,a)\ )$ ____

$\exists a \in \mathbb{Z}^{\neq 0}\ (\ \neg F(a,a)\ )$ ____

$\forall a \in \mathbb{Z}^{\neq 0}\ (\ F(a,a)\ )$ ____

$\forall a \in \mathbb{Z}^{\neq 0}\ (\ \neg F(a,a)\ )$ ____

Claim: Every nonzero integer is a factor of itself.

Proof:

Claim: The statement "There is a nonzero integer that does not divide its square" is True / False

Circle one

Proof:

New! Proof by universal generalization: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.

An **arbitrary** element of a set or domain is a fixed but unknown element from that set.

Definitions

- An integer x is **even** if ______________________________
- An integer x is **odd** if ______________________________

Prove: If n is even, then n^2 is even

Prove: If x is even integer and y is an odd integer, then $x^2 + y^2$ is an odd integer

New! Proof of conditional by direct proof: To prove that the conditional statement $p \to q$ is true, we can assume p is true and use that assumption to show q is true.

Prove: If n^2 is odd, then n is odd

Prove: For real numbers x and y, if $(x + y) \geq 2$, then $x \geq 1$ or $y \geq 1$

New! Proof of Conditional by Contrapositive: To prove that the implication $p \rightarrow q$ is true, we can assume q is false and use that assumption to show p is also false.

Prove: For any integers, if $x \mid y$ and $x \nmid z$, then $x \nmid (y+z)$

Proof of Conditional by Contrapositive (other forms): To prove that the implication $(p_1 \wedge p_2) \to q$ is true, we can assume q is false and p_1 is true and use that assumption to show p_2 is also false. Alternatively, we can assume q is false and p_2 is true and use that assumption to show p_1 is also false.

Work to prove / disprove statement (sometimes in parallel ...)

Prove or disprove: If x and y are two distinct positive integers, such that xy is a perfect square, then x and y are perfect squares.

Prove or disprove: For every integer n, if n^2 is not divisible by 4, then n is odd.

- Write the logical form: ____________________
- Do you believe the statement? Try a few examples.
- Map out possible strategies to prove the statement
  - Write a strategy to consider: ____________________
  - What assumptions can we make for this strategy? ____________________
  - What evidence do we need to provide? ____________________
- Map out possible strategies to disprove the statement

$(p \to q) \equiv \neg(p \wedge \neg q)$ $\qquad$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\qquad$ $q \vee \neg p \equiv p \to q$ $\qquad$ $\neg \exists x\, P(x) \equiv \forall x\, \neg(P(x))$

To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.

To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true.

To prove that $p \wedge q$ is false, it's enough to prove that p is false.
To prove that $p \wedge q$ is false, it's enough to prove that q is false.