ARITHMETIC PROOF

zyBooks Chapter: 6.6

LOGISTICS

- HW6 – due next Wednesday, June 24
- Midterm 2
  - Thursday, June 25
  - Practice Exam on Moodle
  - Review Session – Tuesday, June 23
  - Reading + Q&A – Wednesday, June 24

RECAP

- Integer
  - Closure Property
    - $x + y \in Z$, $x \times y \in Z$, $x - y \in Z$, when $x, y \in Z$
  - x = divisor * quotient + remainder, where $0 \leq r < d$
  - divides
    - $x | y$
    - $x \neq 0$, and $y = kx$ for some integer k
  - mod
    - return remainder
  - div:
    - return quotient

RECAP

- Direct proof
  - Assume the hypothesis is true, and the conclusion is proven as the direct result of the assumption
- Proof by cases
  - Break the domain of variable x into classes, and then prove each class

RECAP – PROOF BY CASES

Q: Prove that if x is an integer, then $3x^2 + x + 14$ is even (divisible by 2).

Case 1: x is even, $x = 2a + 0$ for some integer a

Case 2: x is odd, $x = 2a + 1$ for some integer a

Q: Prove that for all integer x, $x^2 + 3x + 1$ is NOT divisible by 3.

Case 1: $x = 3a + 0$ for some integer a

Case 2: $x = 3a + 1$ for some integer a

Case 3: $x = 3a + 2$ for some integer a

Q: Determine if the following statements are True or False. If the statement is true, give a proof. If the statement is false, give a counterexample.

1) If x and y are even integers, then $x + y$ is even

2) If $x + y$ is even for $x, y \in \mathbb{Z}$, then x and y are even

Q: Determine if the following statements are True or False. If the statement is true, give a proof. If the statement is false, give a counterexample.

- If x and y are even integers, then $x + y$ is even

=== TRUE ===

Given x is an even integer, that is, $x = 2a$ for some integer a.

Given y is an even integer, that is, $y = 2b$ for some integer b.

Hence, $x + y = 2a + 2b = 2(a + b)$

Let $c = a + b$, then $x + y = 2c$.

By the properties of integers, we know c is an integer.

Therefore, $x + y$ is even.

Q: Determine if the following statements are True or False. If the statement is true, give a proof. If the statement is false, give a counterexample.

- If $x + y$ is even for $x, y \in \mathbb{Z}$, then x and y are even

=== FALSE ===

Counterexample:

$x = 1$ and $y = 3$

Q: Prove that $3|x \equiv 3|x^2$

Divisibility Lemma

If $a|x$, then $a|kx$ for any integer k

Case 1: $x = 3a$ for some integer a ($3|x \equiv T$).

$x^2 = (3a)^2 = 9a^2 = 3(3a^2)$ ***** $3|x^2 \equiv T$ *****

Let $b = 3a^2$, then $x^2 = 3b$.

Case 2: $x = 3a + 1$ for some integer a ($3|x \equiv F$). ***** $3|x^2 \equiv F$ *****

$x^2 = (3a + 1)^2 = 9a^2 + 6a + 1 = 3(3a^2 + 2a) + 1$

Let $b = 3a^2 + 2a$, then $x^2 = 3b + 1$.

Case 3: $x = 3a + 2$ for some integer a ($3|x \equiv F$). ***** $3|x^2 \equiv F$ *****

$x^2 = (3a + 2)^2 = 9a^2 + 12a + 4 = 3(3a^2 + 4a + 1) + 1$

Let $b = 3a^2 + 4a + 1$, then $x^2 = 3b + 1$.

***** $3|x \equiv 3|x^2$ *****

ARITHMETIC PROOF TECHNIQUES

- Direct proof
- Proof by cases
- Proof by contradiction
- Proof by induction

PROOF BY CONTRACTION

A proof by contradiction is an indirect proof technique which starts by assuming that the theorem is false and then shows that some logical inconsistency arises as a result of the assumption.

Q: Fill in the blanks in the following proof that there is no integer that is BOTH even and odd.

We take the negation of the theorem and suppose it to be true. That is, assume there is an integer n that is _both even and odd_ .

Given n is even, that is, $n =$ __2a__ for some integer a.

Given n is odd, that is, $n =$ __2b + 1__ for some integer b.

Hence, we have $2a = 2b + 1$ by equating the two expressions for n.

$2a - 2b = 2(a - b) = 1$.

That is, $a - b =$ __1/2__.

Since a and b are integers, the difference $a - b$ must also be _an integer_ by closure property. However, $a - b =$ __1/2__ , and __1/2__ is not an integer, which is a contradiction.

Q: If the product of two positive real numbers is larger than 400, then at least one of the two numbers is greater than 20.

Convert to quantified statement:

$$\forall x \forall y\, [\,(xy > 400) \to (x > 20 \vee y > 20)],\, x, y \in \mathbb{R}$$

Assume to the contrary, $\neg\, \forall x \forall y\, [\,(xy > 400) \to (x > 20 \vee y > 20)],\, x, y \in \mathbb{R}$

We have $\exists x \exists y\, \neg[\,(xy > 400) \to (x > 20 \vee y > 20)],\, x, y \in \mathbb{R}$ via De Morgan's

$\equiv \exists x \exists y\, \neg[\,\neg(xy > 400) \;\vee\; (x > 20 \vee y > 20)\,],\, x, y \in \mathbb{R}$ Implication

$\equiv \exists x \exists y\, [\neg\neg\,(xy > 400) \;\wedge \neg(x > 20 \vee y > 20)\,],\, x, y \in \mathbb{R}$ De Morgan's

$\equiv \exists x \exists y\, (\,xy > 400 \wedge\; x \leq 20 \;\wedge y \leq 20\,),\, x, y \in \mathbb{R}$ DN, DeM

However, xy $\leq$ 400 when x $\leq$ 20 and y $\leq$ 20, which contradicts the assumption.

Q: The average of three real numbers, a, b, and c, is greater than or equal to at least one of the numbers.

Assume this theorem is false. That is,

there are three real numbers a, b, and c, such that the average of the three numbers is less than each of the three numbers. Therefore, we have

$$\frac{a+b+c}{3} < a, \qquad \frac{a+b+c}{3} < b, \qquad \frac{a+b+c}{3} < c$$

Adding the three inequalities gives:

$$\frac{a+b+c}{3} + \frac{a+b+c}{3} + \frac{a+b+c}{3} < a+b+c$$

The inequality contradicts the algebraic fact that

$$\frac{a+b+c}{3} + \frac{a+b+c}{3} + \frac{a+b+c}{3} = a+b+c$$

Q: There exist positive integers a, b, such that $\sqrt{a}+\sqrt{b}=\sqrt{a+b}$

Assume this theorem is false. That is,

For all integer a and b, $\sqrt{a}+\sqrt{b}\neq\sqrt{a+b}$

$$(\sqrt{a}+\sqrt{b})^2 = \left(\sqrt{a+b}\right)^2$$

$$a + b + 2\sqrt{ab} = a + b$$

$$2\sqrt{ab} = 0$$

$$\sqrt{ab} = 0$$

$$ab = 0$$

Hence, when 1) either a or b equals 0 or 2) both a and b equal 0, $\sqrt{a}+\sqrt{b}=\sqrt{a+b}$, which contradicts the assumption.

Therefore, the original theorem is true.

Q: $\sqrt{3}$ is an irrational number.

Assume the theorem is false. That is, $\sqrt{3}$ is a rational number.

Hence, $\sqrt{3} = \frac{a}{b}$ for some integers a, b, b $\neq 0$, and in its standard form where a and b have no common factors other than 1.

$$(\sqrt{3})^2 = \left(\frac{a}{b}\right)^2$$

$$3 = \frac{a^2}{b^2}$$

$$3b^2 = a^2$$

Since $3 \mid a^2$, we have $3 \mid a$. That is, a = 3m for some integer m.

Therefore, $3b^2 = (3m)^2 = 9m^2$. That is, $b^2 = 3m^2$.

Hence, $3 \mid b^2$, which means $3 \mid b$.

That is, b = 3n for some integer n.

Hence, we have a common factor 3 for both a and b, which contradicts the assumption.