




A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a dark blue background, resembling a circuit board or a neural network.

ARITHMETIC PROOF

zyBooks Chapter: 6.1~6.3, 6.7, 7.1~7.2



LOGISTICS

- HW5 – due *Monday, June 15*
 - HW6 – released, due *Wednesday, June 24*
- 
- 
- 

PRELIMINARIES – COMMON MATHEMATICAL SETS

- \mathbb{R} – real numbers
- \mathbb{Q} – rational numbers
 - $\{\dots 1/4, 1/2, \dots\}$
 - $\{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$
- \mathbb{Z} – all integers
 - $\{\dots -2, -1, 0, 1, 2, \dots\}$

PRELIMINARIES – PROPERTIES OF INTEGERS

Integer Property	Addition	Multiplication	Subtraction	Division
Commutative	$x + y = y + x$	$x \times y = y \times x$	$x - y \neq y - x$	$x \div y \neq y \div x$
Associative	$x + (y + z) = (x + y) + z$	$x \times (y \times z) = (x \times y) \times z$	$(x - y) - z \neq x - (y - z)$	$(x \div y) \div z \neq x \div (y \div z)$
Identity	$x + 0 = x = 0 + x$	$x \times 1 = x = 1 \times x$	$x - 0 = x \neq 0 - x$	$x \div 1 = x \neq 1 \div x$
Closure	$x + y \in \mathbb{Z}$	$x \times y \in \mathbb{Z}$	$x - y \in \mathbb{Z}$	$x \div y \notin \mathbb{Z}$
Distributive	$x \times (y + z) = x \times y + x \times z$ $x \times (y - z) = x \times y - x \times z$			

INTEGER DIVISION – DIVIDES

$$x \mid y$$

- x divides y
- If and only if $x \neq 0$, and there is an integer k such that $y = kx$.
- If x divides y , then y is said to be a multiple of x , and x is a factor or divisor of y .

For example,

$$3 \mid 6 \rightarrow x = 3 \neq 0, y = 6 = 3k, \text{ where } k = 2.$$

INTEGER DIVISION – DIVISION ALGORITHM

In general, an integer x with any divisor d can be written as

$$x = d * q + r$$

Remainder

Divisor

Quotient

where $0 \leq r < d$

Example:

$$5 = 3 * 1 + 2$$

INTEGER DIVISION – OPERATIONS

$$5 = 3 * 1 + 2$$

- **div**

- $x \text{ div } d = q$
 - $5 \text{ div } 3 = 1$
- returns the **quotient**, the “floor”

- **mod**

- $x \text{ mod } d = r$
 - $5 \text{ mod } 3 = 2$
- returns the **remainder**

INTEGER DIVISION – OPERATIONS

Divisor

Remainder

$$0 \bmod 5 = 0 \quad \leftarrow 0 = 5 * 0 + 0$$

$$1 \bmod 5 = 1 \quad \leftarrow 1 = 5 * 0 + 1$$

$$2 \bmod 5 = 2 \quad \leftarrow 2 = 5 * 0 + 2$$

$$3 \bmod 5 = 3 \quad \leftarrow 3 = 5 * 0 + 3$$

$$4 \bmod 5 = 4 \quad \leftarrow 4 = 5 * 0 + 4$$

$$5 \bmod 5 = 0 \quad \leftarrow 5 = 5 * 1 + 0$$

$$6 \bmod 5 = 1 \quad \leftarrow 6 = 5 * 1 + 1$$

...

$$0 \leq r < d$$

$$x \bmod 5 = \begin{cases} 0 & (0, 5, 10, 15, \dots) \\ 1 & (1, 6, 11, 16, \dots) \\ 2 & (2, 7, 12, 17, \dots) \\ 3 & (3, 8, 13, \dots) \\ 4 & (4, 9, 14, \dots) \end{cases}$$

ARITHMETIC PROOF STRATEGIES

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

DIRECT PROOF

In a direct proof of a conditional statement, the hypothesis **p** is assumed to be **true** and the conclusion **c** is proven as a **direct result** of the assumption

Q: Prove that the product of an **even** integer and an **odd** integer is **even**

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

Given y is an odd integer, that is, $y = 2b + 1$ for some integer b .

Hence, $xy = (2a)(2b + 1)$

$$= 4ab + 2a$$

$$= 2(2ab + 1)$$

Let $c = 2ab + 1$, then $xy = 2c$.

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

Therefore, xy is an even integer.

Q: Prove that for all $x \in \mathbb{Z}$, if x is odd, then x^2 is odd.

Let x be an arbitrary odd number, and $x = 2a + 1$ for some integer a .

$$\text{Hence, } x^2 = (2a + 1)^2$$

$$= 4a^2 + 4a + 1$$

$$= 2(2a^2 + 2a) + 1$$

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

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

Therefore, x^2 is odd.

Q: Prove that if m, n are odd integers, then $m^2 + n^2$ is even.

Given m is an odd integer, that is, $m = 2a + 1$ for some integer a .

Given n is an odd integer, that is, $n = 2b + 1$ for some integer b .

$$\begin{aligned}\text{Hence, } m^2 + n^2 &= (2a + 1)^2 + (2b + 1)^2 \\ &= (4a^2 + 4a + 1) + (4b^2 + 4b + 1) \\ &= 4a^2 + 4a + 4b^2 + 4b + 2 \\ &= 2(2a^2 + 2a + 2b^2 + 2b + 1)\end{aligned}$$

Let $c = 2a^2 + 2a + 2b^2 + 2b + 1$, then $m^2 + n^2 = 2c$.

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

Therefore, $m^2 + n^2$ is even.

PROOF BY CASES

A proof by cases of a universal statement, such as $\forall x P(x)$, **breaks the domain** for the variable x into **different classes** and gives a different **proof for each class**.

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

Case 1: x is even

That is $x = 2a$ for some integer a .

Hence,

$$\begin{aligned} & 3x^2 + x + 14 \\ &= 3(2a)^2 + 2a + 14 \\ &= 3 * 4a^2 + 2a + 14 \\ &= 12a^2 + 2a + 14 \\ &= 2(6a^2 + a + 7) \end{aligned}$$

Let $b = 6a^2 + a + 7$,

then $3x^2 + x + 14 = 2b$

Case 2: x is odd

That is $x = 2a + 1$ for some integer a . Hence,

$$\begin{aligned} & 3x^2 + x + 14 \\ &= 3(2a + 1)^2 + (2a + 1) + 14 \\ &= 3 * (4a^2 + 4a + 1) + 2a + 1 + 14 \\ &= 12a^2 + 12a + 3 + 2a + 1 + 14 \\ &= 12a^2 + 14a + 18 \\ &= 2(6a^2 + 7a + 9) \end{aligned}$$

Let $b = 6a^2 + 7a + 9$, then $3x^2 + x + 14 = 2b$

By the properties of integers, we know b is an integer. Therefore, $3x^2 + x + 14$ is even.

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

Case 1: $x = 3a + 0$

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

$$= 3(3a^2 + 3a) + 1$$

$$= 3Q + 1$$

== NOT divisible by 3 ==

Case 2: $x = 3a + 1$

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

$$= 3(3a^2 + 5a + 1) + 2$$

$$= 3Q + 2$$

== NOT divisible by 3 ==

Case 3: $x = 3a + 2$

$$(3a + 2)^2 + 3(3a + 2) + 1 = 9a^2 + 12a + 4 + 9a + 6 + 1$$

$$= 3(3a^2 + 7a + 3) + 2$$

$$= 3Q + 2$$

== NOT divisible by 3 ==