# Chapter 4

**Vocabulary**

| | |
|---|---|
| - theorem | - parity |
| - proof | - divides |
| - definition | - divisor |
| - proposition, lemma, corollary | - multiple |
| - even | - direct proof |
| - odd | |

**Definitions**

- A **theorem** is a statement that is true, and has been proved to be true.
- A **proof** of a theorem is a written verification that a theorem is definitely and unequivocally true.
- A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word, phrase, or symbol.
- *Words that mean the same thing as "theorem", but are used in special ways:*
    - *A statement that is true (and proven), but is not as significant as a theorem is sometimes called a* ***proposition***
    - *A* ***lemma*** *is a theorem whose main purpose is to help prove another theorem (a "little theorem, used along the way")*
    - *A* ***corollary*** *is a result that is an immediate consequence of a theorem or proposition ("a little something extra, that we get for free, having completed the theorem")*

**Mathematical Definitions & Facts**

- Definition. An integer $n$ is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.
- Definition. An integer $n$ is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.
- Definition. Two integers have the **same parity** if they are both even or both odd. Otherwise they have **opposite parity**.
- Definition. Suppose $a$ and $b$ are integers. We say that $a$ **divides** $b$, written $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that $a$ is a **divisor** of $b$, and that $b$ is a **multiple** of $a$.
- Definition. A natural number $n$ is **prime** if it has exactly two distinct positive divisors, 1 and $n$.
- Definition. A natural number $n$ is **composite** if it factors as $n = ab$ where $a, b > 1$.
- Fact. Suppose $a$ and $b$ are integers. Then so are $a+b$, $a-b$, and $ab$. (closure of $\mathbb{Z}$)

Does $3 \mid 15$?
$15 = 3 \cdot 5$
$5 \in \mathbb{Z}$

word/term

$\boxed{x \text{ is odd}}$

definition

property

$\boxed{x \in \mathbb{Z},\ x = 2a+1 \text{ for some } a \in \mathbb{Z}}$

**Proposition:** $P \to Q$

Direct Proof.

**Proof.** Suppose $P$.

⋮

Therefore $Q$.

**Ex:**

**Prop.** If $x$ is odd, then $x^2$ is odd.

**Proof:** Suppose $x$ is odd

so $x$ is an integer and $x = 2a+1$ for some $a \in \mathbb{Z}$, by the definition of odd.

$x \cdot x \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication

since $x = 2a+1$,

$x^2 = (2a+1)^2$ by rules of algebra

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

$x^2 = (4a^2 + 4a) + 1$

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

let $b = 2a^2 + 2a$, so $x^2 = 2b+1$

then $b \in \mathbb{Z}$, since $a \in \mathbb{Z}$, $2 \in \mathbb{Z}$, and $\mathbb{Z}$ is closed under multiplication and addition.

~~$x = 7$~~

$x \in \mathbb{Z}$ $a = 3$

$7 = 2 \cdot 3 + 1$, $3 \in \mathbb{Z}$

thus 7 is odd

$x^2 = \underline{49}$

$x^2 = 2 \cdot 24 + 1$

$24 \in \mathbb{Z}$

thus $x^2$ is odd.

Thus $x^2 \in \mathbb{Z}$ and $x^2 = 2b+1$ for $b \in \mathbb{Z}$

Therefore, $x^2$ is odd, by the definition of odd

QED

$\square$

$\boxed{\checkmark}$

Ex: $\boxed{a|b}$ (term) $\xrightarrow{\text{definition}}$ $\boxed{a, b \in \mathbb{Z} \text{ and } b = a \cdot d \text{ for some } d \in \mathbb{Z}}$ (property)

$a = 2$
$b = 4$
$c = 8$

$2|4$ T
$4|8$ T
then two divides eight
$2|8$ T
$\underline{\underline{8 = 2 \cdot 4}}$
eight divides two
$8|2$ ~~F~~
$2 = 8 \cdot c$
$c \in \mathbb{Z}$

Proposition. Let $a$, $b$, and $c$ be integers. If $a|b$ and $b|c$, then $a|c$.

Proof. Suppose $a, b, c$ are integers, and $a|b$ and $b|c$.
Thus $b = a \cdot h$ for some $h \in \mathbb{Z}$
and $c = b \cdot i$ for some $i \in \mathbb{Z}$,
by definition of "divides".
By substitution,

[illegible]

$$c = b \cdot i = (a \cdot h)\, i$$

$$c = ahi$$

is $m \in \mathbb{Z}$?
why?

let $m = h \cdot i$.

then $m \in \mathbb{Z}$ because $h \in \mathbb{Z}$, $i \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under multiplication.

$c = a \cdot m$ for some $m \in \mathbb{Z}$

Therefore, $a \mid c$, by defn of divides $\square$

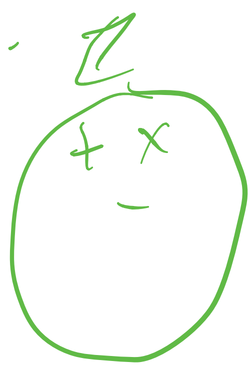
---

$\mathbb{Z}$ is closed under multiplication, addition, subtraction.

means you cannot escape from $\mathbb{Z}$ by performing these operations.

if $a, b \in \mathbb{Z}$

$$\left.\begin{aligned} a \cdot b &\in \mathbb{Z} \\ a + b &\in \mathbb{Z} \\ a - b &\in \mathbb{Z} \end{aligned}\right\}$$



$P \to Q$

**Prop** if $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

$n=4$

$1+(-1)^4(2\cdot 4-1)$

$1+1(8-1)$

$1+7$

$8$

8 is a multiple of 4.

**Proof:** Suppose $n \in \mathbb{N}$.

Case 1 n is even

then $n \in \mathbb{Z}$, $n = 2a$, for some $a \in \mathbb{Z}$ by defn of even.

by substitution

$1+(-1)^n(2n-1) =$

$1+(-1)^{2a}(2(2a)-1) =$ $\quad (-1)^{2a} = 1$

$1+1(4a-1) = 1+4a-1 = 4a$

$1+(-1)^n(2n-1) = 4\cdot a$, $a \in \mathbb{Z}$

Therefore, $1+(-1)^n(2n-1)$ is a

multiple of 4, by definition of multiple. ☑

<u>case 2</u> n is odd

Therefore $1+(-1)^n(2n-1)$ is a multiple of 4.

Office Hours

# Assignment5-Sec3.1-3.4: Problem 7

**(6 points) Library/Rochester/setProbability1Combinations/ur_pb_1_9.pg**

This set is **visible to students.**

In how many ways can 5 different novels, 2 different mathematics books, and 1 biology book be arranged on a bookshelf if

(a) the books can be arranged in any order?

Answer: $8!$

(b) the mathematics books must be together and the novels must be together?

Answer: $5! \cdot 2! \cdot 1 \cdot 3!$

(c) the mathematics books must be together but the other books can be arranged in any order?

Answer: $5! \cdot 3! \cdot 2!$