Days 11&12

Chapter 4

Vocabulary

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

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 $a|b$, 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.

Proof

Theorem. A true statement that has been proved to be true.

These mean the same:

Proposition. Prop.

Lemma. a mini-theorem.

Corollary

Proof. of a theorem is a written verification that a theorem is definitely true.

Proof is about communication

Definitions are of paramount importance

WHAT CAN WE USE IN PROOFS?

sets: $\mathbb{N}$

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{Q}$

$\mathbb{R}$

$\mathbb{C}$

Arithmetic $+, -, \times, \div, <$

Algebra $2x+4 = 2(x+2)$

Any definitions we give.

Defn An integer n is **even** if $n = 2a$ for some integer a.

Ques is 12 even?

$a = 6$, note $6 \in \mathbb{Z}$

$2 \cdot 6 = 12$

Is 0 even?

is $0 \in \mathbb{Z}$? Yes

$a = 0$, $0 \in \mathbb{Z}$

$2 \times 0 = 0$

Defn n is **even** iff

$$\forall n \in \mathbb{Z} \exists a \in \mathbb{Z},\ 2a = n$$

$$\forall n \in \mathbb{Z} \left(\overbrace{\cancel{n \text{ is even}}}^{E(n)} \iff \exists a \in \mathbb{Z},\ n = 2a \right)$$

$E(n) =$ n is even

Defn An integer n is **odd** if $n = 2a + 1$ for some integer a.

Even/odd | Positive/negative

parity | sign

Parity = evenness or oddness of a number.

What is the parity of 24?

Even

Defn "divides"

If a, b are integers, we say a divides b, or $a|b$, if $b = a \cdot n$, where n is an integers.

Ex: T/F $2|6$ True $n=3$

"Axiom" "Theorem"

Fact: If a, b are integers,
then $a+b$ is an integer,
$a-b$ "
$a \cdot b$ "

$a = 5, \; b = 16 \quad \in \mathbb{Z}$

* addition: $a+b = 5+16 = 21 \in \mathbb{Z}$

* subtraction: $a-b = 5-16 = -11 \in \mathbb{Z}$

mult. $a \cdot b = 5 \cdot 16 = 80 \in \mathbb{Z}$

divide $a \div b = \frac{5}{16} \notin \mathbb{Z}$

Direct Proof

used to Conditional Statement

prove Conditional Statements

$P \rightarrow Q$

Outline for Direct Proof

Proposition. $P \rightarrow Q$. If P then Q

Proof. Suppose P.

⋮

Therefore Q. QED, □

P: "an integer x is odd"

Q: "x^2 is odd"

Proposition If an integer x is odd, then x^2 is odd.

Proof. Suppose an integer x is odd.

Given an odd integer x,

Thus $x = 2a+1$ for some integer a, by the definition of odd

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

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

$x^2 = 2(2a^2+2a) + 1$, let $b = 2a^2 + 2a$.

So $x^2 = 2b + 1$, by substitution.

Also, b is an integer, by closure of $\mathbb{Z}$ under integer operations

Therefore x^2 is odd by the definition of odd. □

$x = 3$

$x = 2a+1 \rightarrow a = 1$, $1 \in \mathbb{Z}$

$3 = 2 \cdot 1 + 1$

$x^1 = 3^1 = 9$

$9 = 2 \cdot 4 + 1$

4

TWO MATHEMATICAL THEOREMS THAT WE WILL ACCEPT WITHOUT PROOF (for now)

- **Theorem (The Division Algorithm).** Given integers a and b with b>0, there exist unique integers q and r for which a=qb+r and 0r<b.
- **Theorem (Unique Factorization).** Every natural number greater than 1 has a unique factorization into primes. *NOTE: Also called the "Fundamental Theorem of Arithmetic"*

WHAT AM I ALLOWED TO USE IN PROOFS?

Any definitions given in class or in the book, plus
Basic mathematical knowledge including:

- the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and the meaning of $\in$, $\subseteq$
- arithmetic for numbers in the above sets (facts about addition, subtraction, multiplication, division, exponents)
- algebra (for example for solving equations and simplifying expressions)
- the meaning of "<"

Outline for Direct Proof

Proposition. If P, then Q.
Proof. Suppose P.
…
Therefore Q.

Proposition. If x is odd, then x^2 is odd.

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

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