# PLP - 7

## TOPIC 7 —STATEMENT TYPES AND SOME DEFINITIONS

Demirbaş & Rechnitzer

# AFTER LOGIC BUT BEFORE PROOFS

# TYPES OF STATEMENTS

**axiom**

Statements we accept as true without proof.

**fact**

Statements we accept as true, but we won't bother proving for this course

**AXIOM 1.**

Let $m, n$ be integers then $-n, m+n, m-n$ and $m \cdot n$ are also integers.

## FACT:

Let $x \in \mathbb{R}$. Then $x^2 \geq 0$.

# TYPES OF STATEMENTS

**theorem**

An important true statement — Pythagorous' theorem

**corollary**

A true statement that follows from a previous theorem

**lemma**

A true statement that helps us prove a more important result

**result, proposition**

True statements we prove (esp as exercises) we'll call results, or propositions (if more important)

# USEFUL DEFINITIONS

## DEFINITION: EVEN AND ODD NUMBERS.

An integer $n$ is **even** if $n = 2k$ for some $k \in \mathbb{Z}$.

An integer $n$ is **odd** if $n = 2\ell + 1$ for some $\ell \in \mathbb{Z}$.

If two integers are *both even* or *both odd* odd, then they have the **same parity**, else **opposite parity**.

Note:

- The use of *if* in a definition is really *iff*.

  We mean "$n$ is even" if and only if "$n = 2k$ for some $k \in \mathbb{Z}$"
- The number 0 is even (some students are taught otherwise).

# SOME MORE USEFUL DEFINITIONS

## DEFINITION: (DIVISIBILITY).

Let $n, k \in \mathbb{Z}$. We say $k$ **divides** $n$ if there is $\ell \in \mathbb{Z}$ so that $n = \ell k$.

In this case we write $k \mid n$ and say that $k$ is a **divisor** of $n$ and that $n$ is a **multiple** of $k$.

## DEFINITION: (PRIME, COMPOSITE AND 1).

Let $n \in \mathbb{N}$. We say that $n$ is **prime** when it has *exactly* two positive divisors, 1 and itself.

If $n$ has more than two positive divisors then we say that it is **composite**.

Finally, the number 1 is neither prime nor composite.

# GCD, LCM AND EUCLID

## DEFINITION: (GCD AND LCM).

Let $a, b$ be integers

- The **greatest common divisor** of $a, b$ is the largest positive integer that divides both $a, b$
- The **least common multiple** of $a, b$ is the smallest positive integer divisible by both $a, b$
- We denote these $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$

## FACT: (EUCLIDEAN DIVISION).

Let $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique $q, r \in \mathbb{Z}$ so that

$$a = bq + r \qquad \text{with } 0 \leq r < b$$

# CONGRUENCE MODULO $n$

## DEFINITION:

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.

We say that $a$ is **congruent to** $b$ **modulo** $n$ when $n \mid (a-b)$.

The "n" is refered to as the **modulus** and we write the congruence as $a \equiv b \pmod{n}$.

When $n \nmid (a-b)$ we say that $a$ is not congruent to $b$ modulo $n$, and write $a \not\equiv b \pmod{n}$.

For example:

$$5 \equiv 1 \pmod{4} \qquad 17 \equiv 1 \pmod{4} \qquad 3 \not\equiv 9 \pmod{4}$$

$P(\cdot) \Rightarrow$ open sentences

Q) Number 1729 is not a cube; it's however sum of two cubes

p: 1729 is a cube
q: 1729 is the sum of two cubes

$\sim P \wedge Q$

Q1) If $x \in \mathbb{R}$ & the sequence $(x_n)$ converges to $x$, then $(1/x_n)$ converges to $1/x$.

a: $x \in \mathbb{R}$
b: $x_n$ converges to $x$
c: $1/x_n$ converges to $1/x$

$a(x) \wedge b(x_n, x) \Rightarrow c(x_n, x)$

Q2) If an int $n$ is divisible by 6 & 10, then it's | by 2.

x: $6 \mid n$
y: $10 \mid n$
z: $2 \mid n$

$x(n) \vee y(n) \Rightarrow z(n)$

Q) Prove the stmt that: If $n$ is even, then $n^2+4n+5$ is odd

Let $n = 2m$ where $\exists m \in \mathbb{Z}$.
So, for $n^2+4n+5$

$(2m)^2 + 4(2m) + 5$

$4m^2 + 8m + 5$

$\Rightarrow 2(2m^2+4m+2) + 1$

This is of the form $2j+1$ for any $j = 2m^2 + 4m + 2$ where $\exists j \in \mathbb{Z}$

Hence $n^2+4n+5$ is odd.