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:

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