3rd Week

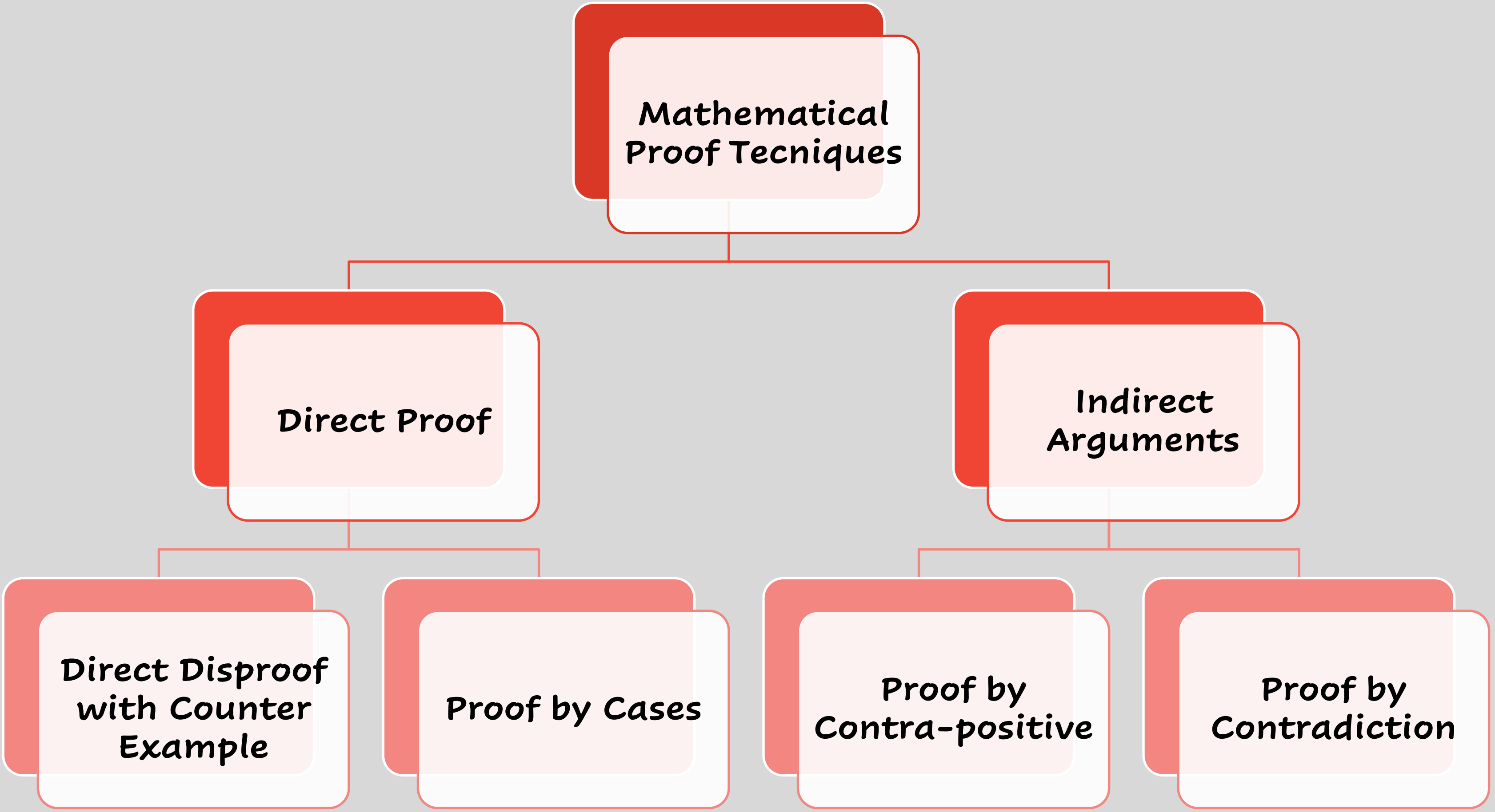
MAT 203E DISCRETE MATH

ınstructor: Dr. Sümeyra BEDİR

#4 Theory of Numbers and Proof Techniques

- Over some number theoretical concepts, we will cover mathematical proof techniques.

Mathematical Proof



Direct Proofs (Even/Odd Numbers)

• Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

$$n\ is\ even \Leftrightarrow \exists k \in \mathbb{Z}: n = 2k$$
$$n\ is\ odd \Leftrightarrow \exists k \in \mathbb{Z}: n = 2k + 1$$

Direct Proofs (Prime Numbers)

• Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

$$1 < n \; is \; prime \Leftrightarrow (n = rs \Leftrightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$$

Example

- $(\forall n \in \mathbb{Z}, n\ even \Rightarrow n^2\ is\ even)$, proove.

Direct Proofs (Rational Numbers)

• Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational.** More formally, if r is a real number, then

$$r \text{ is rational} \quad \Leftrightarrow \quad \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

$$r \in \mathbb{R}\; is\; a\; rational\; number \Leftrightarrow$$
$$(\exists a, b \in \mathbb{Z}: r = a/b \wedge b \neq 0)$$

Example

- Show that the sum of two rational numbers is a rational number.

Direct Proofs (Divisibility)

• Definition

If n and d are integers and $d \neq 0$ then

n **is divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n is a multiple of d, or
d is a factor of n, or
d is a divisor of n, or
d divides n.

The notation **d | n** is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

$$d|n \Leftrightarrow$$
$$(\exists k \in \mathbb{Z}: n = dk)$$

Example

- Prove that for all integers a, b, and c, if $a|b \text{ and } b|c \text{ then } a|c$.

Example

- Prove the expression $(\forall a, b \in \mathbb{Z}, a|b \wedge b|a \Rightarrow a = b)$ or give a counter example.

Direct Proofs (Proof by Cases)

Theorem 4.4.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$