# Lecture 8 - Properties of Integers

## The Division Algorithm

- Definition $b \mid a$ (b divides a) if and only if $a = bn$
- Theorems, for all $a, b, c \in \mathbb{Z}$:
  - $1 \mid a$ and $a \mid 0$
  - $[(a \mid b) \wedge (b \mid a)] \implies a = \pm b$
  - $[(a \mid b) \wedge (b \mid c)] \implies a \mid c$
  - $(a \mid b) \implies a \mid bx$ for all $x \in \mathbb{Z}$
  - If $x = y + z$ for some $x, y, z \in \mathbb{Z}$ and a divides two of the three integers $x, y$ and $z$ then a divides the remaining integer
  - $[(a \mid b) \wedge (a \mid c)] \implies a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$ (the expression $bx + cy$ is called a linear combination of b and c)
  - For $1 \leq c_i \leq n$, let $c_i \in \mathbb{Z}$. If a divides each $c_i$ then $a \mid (c_1x_1 + c_2x_2 + \ldots + c_nx_n)$ there $x_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.
- If $a, b \in \mathbb{Z}$, then there exist unique $q, r \in \mathbb{Z}$ with $a = qb + r$, $0 \leq r < b$.
  - Here q is called quotient
  - r remainder
  - b divisor and
  - a dividend

## Greatest Common Divisor

- Definition: c is the greatest common divisor of a and b iff:
  - $c \mid a$ and $c \mid b$

    - For any common divisor d of a and b, $d \mid c$

- GCD is unique
- GCD is the smallest positive integer we can write as a linear combination of a and b
- $gcd(a, b) = gcd(b, a)$
- $gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$
- $gcd(a, 0) = |a|$
- $gcd(0, 0)$ is not defined
- We call a and b **relatively prime** (**co-prime**) if $gcd(a, b) = 1$

## Euclidean Algorithm

```
function gcd(a, b)
    while a ≠ b
        if a > b
            a := a − b
        else
            b := b − a
    return a
```

## Least Common Multiple

- Definition: The least common Multiple is the smallest of all positive integers that are common multiples of a and b.
- $lcm(1, n) = lcm(n, 1) = n$
- $lcm(a, na) = na$
- If $n \geq m$, $lcm(a^m, a^n) = a^n$
- If $c = lcm(a, b)$ and d is a common multiple of a and b, then $c \mid d$.
- $a \cdot b = lcm(a, b) \cdot gcd(a, b)$

# Diophantine Equations

- Diophantine equations are of the form
  - $ax^n = by^n = c^n$, where all numbers are integers
- $ax + by = c$ has a solution only if $gcd(a, b)$ is a factor of c
- To solve
  - Find $gcd(a, b) = d$, then $d \mid c$, so $c = d \cdot n$ for some integer n.
  - Express d in the form $d = as + bt$ for some integers s and t
  - Multiply by n to get $x = sn, y = tn$
  - Then, all the solutions can be generated like this:

$$x = x_1 - \frac{rb}{d}$$
$$y = y_1 + \frac{ra}{d}$$

  - Where $x_1$ and $y_1$ are a single solution to this equation.

# Pythagorean Triples

- Pythagorean triples are of the form $a^2 + b^2 = c^2$
- To find these:
  - pick an odd positive number
  - divide its square into two integers which are as close to being equal as possible
  - Example: $7^2 = 49 = 24 + 25$ gives triples $7, 24, 25$
  - Alternatively pick any even integer n
  - triples are $2n, n^2 - 1$ and $n^2 + 1$
  - Example: picking 8 gives $16, 63, 65$