Week 5
Integers
Discrete Math

Marie Demlová
http://math.fel.cvut.cz/en/people/demlova

March 17, 2022

Integers

Division Theorem. Let a, b, $b > 0$, be two integers. Then there exist unique integers q, r such that

$$a = q\,b + r, \quad 0 \leq r < b.$$

The number q is called the quotient, and r the remainder when we divide a by b.

The division theorem holds also for negative numbers. For example, let $a = -7$, $b = 3$. Then $7 = 2 \cdot 3 + 1$, hence $-7 = -2 \cdot 3 - 1 = -3 \cdot 3 + (3 - 1)$. Therefore, $q = -3$ and $r = 2$.

Given two integers a, b. We say that b divides a if $a = k\,b$ for some integer k. (Also a is a *multiple* of b.) This fact is denoted by $b \,|\, a$.

The Greatest Common Divisor

A positive integer p, $p > 1$, is a prime if
$a \mid p,\ a \geq 0, \quad$ implies $\quad a = 1$ or $a = p$.
A number $n > 1$ is composite if it is not a prime.

Let a and b be two integers. A common divisor of a and b is any integer e for which $e \mid a$ and $e \mid b$.

The greatest common divisor of a, b is the integer $c = \gcd(a, b)$ such that

- $c \geq 0$
- c is a common divisor of a and b, i.e. $c \mid a$ and $c \mid b$,
- and if e is any common divisor of a and b then $e \mid c$.

Integers a and b are called relatively prime (or *coprime*) if $\gcd(a, b) = 1$.

Euclid's Algorithm

Euclid's Algorithm

Input: Positive natural numbers a and b

Output: $c = \gcd(a, b)$.

1. (Initialization.)
   $u := a$, $t := b$;

2. (Divide u by t.)
   `repeat`
   `do` $u = q \cdot t + r$;
   $u := t$, $t := r$.
   `until` $t = 0$.
3. (The greatest common divisor)
   `return` $c := u$.

Euclid's Algorithm

Proposition.
The pairs of numbers u, t and t, r from the Euclid's algorithm have the same common divisors. Hence

$$\gcd(u, t) = \gcd(t, r) = \gcd(a, b).$$

Bezout's Theorem.

Let a and b be two natural numbers. Denote $c = \gcd(a, b)$. Then there exist integers x, y such that

$$a\,x + b\,y = c.$$

Extended Euclid's Algorithm

Input: natural numbers a and b.

Output: $c = \gcd(a, b)$ and $x, y \in \mathbb{Z}$ for which $a\,x + b\,y = c$.

1. (Initialization.)
   $u := a$, $x_u := 1$, $y_u := 0$, $t := b$, $x_t := 0$, $y_t := 1$;
2. (Division.)
   `repeat`
   `do` $u = q \cdot t + r$, $x_r := x_u - q\,x_t$, $y_r := y_u - q\,y_t$;
   $u := t$, $x_u := x_t$, $y_u := y_t$
   $t := r$, $x_t := x_r$, $y_t := y_r$.
   `until` $t = 0$
3. (Greatest common divisor and x, y)
   `return` $c := u$, $x := x_u$, $y := y_u$.

Integers

Corollary of Bezout's theorem.

- Let a and b be two relatively prime numbers. If a divides a product $b \cdot c$ then a divides c.
- If a prime number p divides a product $a \cdot b$ then it divides at least one of the numbers a, b.

Prime Factorization Theorem.

Every natural number n, $n > 1$, factors into a product of primes, i.e.

$$n = p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots \cdot p_k^{i_k},$$

where $p_1, \ldots, p_k$ are distinct primes, and $i_1, \ldots, i_k$ positive natural numbers.

If moreover $p_1 < p_2 < \ldots < p_k$ then the factorization is unique.

Integers

Theorem.

There are infinitely (countably) many primes.

Proposition.

Equation $ax + by = c$ for integers a, b, c has at least one integer solution if and only if c is divisible by the greatest common divisor of a and b.

Diophantic Equations.

By a Diophantic equation we mean equation

$$ax + by = c, \quad a, b, c \in \mathbb{Z},$$

where we are looking only for integers solutions, i.e. $x, y \in \mathbb{Z}$.

Homogeneous Diophantic equation.

A Diophantic equation is homogeneous if the right hand side is 0, i.e. $c = 0$.

Proposition.

If $a \neq 0 \neq b$ then the equation $ax + by = 0$ has infinitely many solutions, more precisely, $x = -k \cdot b_1$, $y = k \cdot a_1$ for any $k \in \mathbb{Z}$, where $a_1 = \frac{a}{\gcd(a,b)}$ and $b_1 = \frac{b}{\gcd(a,b)}$ are all integer solutions of it.

Diophantic Equations.

Proposition.

If c is a multiple of $\gcd(a, b)$ then any solution of $ax + by = c$ is of the form

$$x = x_0 + k \cdot b_1, \quad y = y_0 - k \cdot a_1,$$

where x_0, y_0 is a solution of the equation $ax + by = c$, and $a_1 = \frac{a}{\gcd(a,b)}$, $b_1 = \frac{b}{\gcd(a,b)}$ and $k \in \mathbb{Z}$.

Diophantic Equations.

A Procedure for Solving Diophantic Equations.

- Using the extended Euclid's algorithm we find integers x_0 and y_0 satisfying $ax + by = c$ or find out that the equation does not have a solution.
- If there is at least one integer solution of $ax + by = c$ we find a general integer solution of the equation $a\,x + b\,y = 0$ as follows.
  First, we divide the equation by $\gcd(a, b)$ and obtain an equation $a_1\,x + b_1\,y = 0$ where a_1 and b_1 are relatively prime. The general solution is now $x = b_1\,k$, $y = -a_1\,k$ where $k \in \mathbb{Z}$.
- The general solution of $ax + by = c$ is

$$x = x_0 + b_1\,k, \quad y = y_0 - a_1\,k, \quad k \in \mathbb{Z}.$$