Chapter 2

Integers

2.1 Integers and Their Properties

Integers are well known numbers. They play a crucial role in mathematics, primarily in the discrete mathematics and its applications. We will use them in the sequel to introduce "new numbers", the residual classes of integers modulo a positive integer n.

First, let us recall some well known facts about division of integers. They are: integer division with remainder, a common divisor, and the greatest common divisor. We present the Euclid's Algorithm for finding the greatest common divisor and its applications, namely for solving Diophantic equations — equations in which only integer solutions are sought.

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

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

$\square$

We will prove later only the uniqueness part of the theorem, the existence of q and r follows from the well known way how to divide two integers.

2.1.2 Remark. 1. The number q is called the *quotient*, and r the *remainder* when we divide a by b.

2. We formulated the division theorem 2.1.1 not only for natural numbers a and b, but also for a negative integer a. In that case, we have to be a little more careful. Assume that a is negative. Divide the absolute value $|a|$ by b. Then $|a| = q'b + r'$ for $0 \le r' < b$, $q' \le 0$, and $a = -q'b - r'$. If $r' = 0$ then $a = -q'b$, and we have $q = -q'$, $r = 0$. Assume $0 < r' < b$, then $a = -q'b - r' = -(q'+1)b + (b - r')$. Moreover, $0 < b - r' < b$, and hence $q = -(q'+1)$ and $r = b - r'$.

We show the procedure on the following example: Let $a = -7$, $b = 3$. We have $7 = 2\cdot 3 + 1$, hence $-7 = -2 \cdot 3 - 1 = -3 \cdot 3 + (3 - 1)$. Therefore, $q = -3$ and $r = 2$.

Let us prove the uniqueness of the quotient and the remainder.

2.1.3 Justification of Uniqueness. Assume that there exist two pairs q and r from 2.1.1, say q_1, r_1 and q_2, r_2, where $0 \le r_1, r_2 < b$. We have

$$a = q_1\,b + r_1, \text{ and } a = q_2\,b + r_2.$$

Then

$$q_1\,b + r_1 = q_2\,b + r_2, \quad \text{i.e.} \quad (q_1 - q_2)\,b = r_2 - r_1.$$

Because $|r_2 - r_1| < b$ and it is a multiple of b, the number $q_1 - q_2$ must be 0 (indeed, otherwise $|(q_1 - q_2)b| \ge b$) . And this means that $q_1 = q_2$ and $r_1 = r_2$. We have shown that the quotient and the remainder are unique. $\square$

2.1.4 Divisibility. Let us recall other well known notions.

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

A positive integer p, $p > 1$, is said to be a *prime* if it satisfies:

$$a \,|\, p,\ a \geq 0, \quad \text{implies} \quad a = 1 \ \text{ or } a = p.$$

A number $n > 1$ is *composite* if it is not a prime, or equivalently, if there exist $r, s \in \mathbb{Z}$ such that $n = r \cdot s$ and $r > 1$ and $s > 1$. □

Notice, that 0 divides 0; indeed, e.g. $0 = 1 \cdot 0$. If $b \neq 0$ then $b \,|\, a$ if and only if the remainder when dividing a by b equals 0. Also, note that 1 has a special role, it is (by definition) neither a composite number nor a prime.

2.1.5 A Common Divisor and the Greatest Common Divisor. Let us recall the definition of a common divisor and the greatest common divisor.

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

The *greatest common divisor* of a, b is the integer c such that

1. $c \geq 0$
2. c is a common divisor of a and b, i.e. $c \,|\, a$ and $c \,|\, b$,
3. and if e is any common divisor of a and b then $e \,|\, c$.

The greatest common divisor of a and b is denoted by $\gcd(a, b)$. Integers a and b are called *relatively prime* (or *coprime*) if $\gcd(a, b) = 1$. □

2.1.6 Remarks.

1. For every natural number a we have $a = \gcd(a, 0)$.
2. If for natural numbers a, b we have $a \,|\, b$ then $\gcd(a, b) = a$.
3. For every integers a, b it holds that $\gcd(a, b)$ is always non-negative and $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.

2.1.7 You know from school mathematics that the greatest common divisor of a and b can be found using a factorization of a and b into products of primes. Unfortunately, finding such factorization for big a (or b) is a very difficult task. (There is not known a tractable algorithm for finding it.) The following fast algorithm, due to Euclid, is based on the division theorem.

2.1.8 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` $c := u$.

2.1.9 Correctness of the Euclid's Algorithm. Notice that the above algorithm will always terminate; indeed, the number t in the next execution of the step 2 is an integer that is always strictly smaller than the previous one. So after a finite number of executions of step 2, we get $t = 0$ and the algorithm terminates.

The fact that the algorithm returns $\gcd(a, b)$ is proved in the following proposition.

Proposition. The pairs of numbers u, t and t, r from the Euclid's algorithm 2.1.8 have the same common divisors. Hence $\gcd(u, t) = \gcd(t, r) = \gcd(a, b)$. □

Justification. Since $r = u - q \cdot t$ for an integer q, any common divisor of u and t is also a divisor of t, r. Indeed, if $u = d \cdot u'$ and $t = d \cdot t'$, then also $r = d \cdot u' - q \cdot d \cdot t' = d(u' - qt')$.

On the other hand, $u = q \cdot t + r$ so any common divisor of t, r is a divisor of u as well. Indeed, if $t = d \cdot t'$ and $r = d \cdot r'$, then also $u = q \cdot d \cdot t' + d \cdot r' = d(qt' + r')$. □

2.1.10 Euclid's Algorithm can be extended in such a way that it finds not only $\gcd(a, b)$ but also **integers** x, y that solve the following equation

$$a\,x + b\,y = \gcd(a, b).$$

Such equations (considered as equations over integers) will play a crucial role when investigating properties of residual classes modulo n.

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

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

□

The proof of the Bezout's theorem will be given by the extended Euclid's algorithm, because the extended Euclid's algorithm not only proves the existence of integers x and y, but it finds them together with the greatest common divisor of a and b.

2.1.12 Extended Euclid's Algorithm.

Input: natural numbers a and b.

Output: $c = \gcd(a, b)$ together with $x, y \in \mathbb{Z}$ 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` $c := u$, $x := x_u$, $y := y_u$.

Justification of the above algorithm is similar to 2.1.8.

1. $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$. So, the step 1 correctly sets x_u, y_u and x_t, y_t.
2. Assume that $u = a\,x_u + b\,y_u$ and $t = a\,x_t + b\,y_t$. Then

$$r = u - q\,t = a\,x_u + b\,y_u - q\,(a\,x_t + b\,y_t) = a\,(x_u - q\,x_t) + b\,(y_u - q\,y_t).$$

   Hence, it is clear that the numbers x_r and y_r are correctly defined.

□

The Bezout's theorem has couple of important corollaries; some of them you have used in school mathematics without justification.

2.1.13 Corollary.

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

□

Justification. We prove the first part of the corollary; the second one is an easy consequence of the first one.

Assume that numbers a and b are relatively prime. By the Bezout's theorem there exist integers x, y such that

$$1 = a\,x + b\,y.$$

Multiplying the equation by c we get

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

Number a divides $a\,c$ and it also divides the product $b\,c$, hence a divides c. □

2.1.14 Prime Factorization. Let us recall another known fact – a factorization of a natural number different from 1 into a product of primes.

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. □

Justification. The existence of a prime factorization is shown using mathematical induction (more precisely, the principle of strong mathematical induction).

To justify the uniqueness one can use the above corollary. Assume that

$$p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots \cdot p_k^{i_k} = q_1^{j_1} \cdot q_2^{j_2} \cdot \ldots \cdot q_m^{j_m}$$

and $p_1 < p_2 < \ldots < p_k$, $q_1 < q_2 < \ldots < q_m$ then p_1 divides $q_1^{j_1} \cdot q_2^{j_2} \cdot \ldots \cdot q_m^{j_m}$ so $p_1 = q_1$. (Indeed, a prime number p divides a prime number q then $p = q$. Hence, p_1 must be equal to the smallest prime among q_j and it is q_1.)

If we divide the equality by p_1 and repeat the argument we get that $i_1 = j_1$. Analogously (after dividing by $p_1^{i_1}$) we get $p_2 = q_2$, $i_2 = j_2$, etc. $k = m$ and $p_k = q_k$, $i_k = j_k$. □

2.1.15 There is a Countably Many Primes. Using the prime factorization theorem one can easily prove that there is an infinite number of primes – see the following theorem. Since every prime is an integer, it means that there is countably many of them.

Theorem. There are infinitely (countably) many primes. □

Justification. Assume that there were only finitely many primes, say $p_1, p_2, \ldots, p_N$ were the only primes. Then the number $n = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$ is a product of primes; namely is divisible by some prime p. But p cannot be among $p_1, \ldots, p_N$, since n is not divisible by any p_i – a contradiction. □

2.1.16 Diophantic Equations. The Bezout's theorem 2.1.11 helps us to solve other linear equations where we are looking for integer solutions – so called *Diophantic equations*.

Definition. Given three integers a, b, c. Find all integers $x, y \in \mathbb{Z}$ which are solutions of the following equation

$$ax + by = c. \tag{2.1}$$

□

2.1.17 When a Diophantic Equation Has Got a Solution. The following proposition characterizes all Diophantic equations that have got at least one solution.

Proposition. Equation 2.1 has got at least one solution if and only if c is divisible by the greatest common divisor of a and b. □

Justification. Denote $d = \gcd(a, b)$. If c is a multiple of d, say $c = k\,d$, then it suffices to find integers x', y' from the Bezout's Theorem for which

$$d = a\,x' + b\,y' \quad \text{and} \quad c = k\,d = a\,k\,x' + b\,k\,y'.$$

Now $x := k\,x'$ and $y := k\,y'$ is one solution of the equation 2.1.