1. Basic algebraic properties of integers

1. The origin and foundations of natural numbers

For many centuries mathematicians considered natural numbers as given (by God) and did not bother about their origin. However, in the late 19th and early 20th century, it became evident that one should give a more precise meaning to mathematical objects as well as to mathematical reasoning, and people believed that a foundation of mathematical theories can be given by determining their axioms (and rules of reasoning).

After some trials, a set of such axioms of the theory of natural numbers proposed by Peano were commonly accepted. These axioms can be described in the following way. First, one fixes the primitive notions of

◇ *a natural number and the set* $\mathbb{N}$ *of natural numbers,*
the number $0 \in \mathbb{N}$*, and*
the successor function $s : \mathbb{N} \to \mathbb{N}$

and one admits the following axioms describing the properties of these notions:

1. $\bigwedge\limits_{n,m} (s(n) = s(m) \Rightarrow n = m)$,
2. $\bigwedge\limits_{n} (s(n) \neq 0)$ and
3. Induction Axiom.

The Induction Axiom can either have an elementary, i.e., first order form (where we accept only variables running over $\mathbb{N}$) and is given as a scheme (sequence) of expressions

$$\Big[\Phi(0) \wedge \bigwedge_{n} (\Phi(n) \Rightarrow \Phi(s(n)))\Big] \Rightarrow \bigwedge_{m} \Phi(m),$$

where $\Phi(n)$ is any formula of the theory; or this axiom can have a nonelementary (second order) form (where we accept variables running over the set of subsets of $\mathbb{N}$):

$$\bigwedge_{X\subset\mathbb{N}} [(0 \in X) \wedge (n \in X \Rightarrow s(n) \in X)] \Rightarrow (X = \mathbb{N}).$$

The second way requires having some set theory.

However, the axiomatic way of introducing natural numbers neglects intuitive sources of these numbers. Hence also the construction of a model of natural numbers as composed of the cardinalities of finite sets in some set theory has often been considered.

An equivalent way of constructing a model of numbers in set theory has been proposed by John von Neumann; it consists in defining a specific set of any fixed finite cardinality. First, we let 0 be the empty set, and when we have already chosen a finite set X, then we take the successor of X to be $X \cup \{X\}$. For example, the number 1 is represented by the one-element set $\emptyset \cup \{\emptyset\}$.

The two ways lead to two "theories of numbers", with different sets of theorems. In the axiomatic case, the theorems are the results that can be derived from the axioms; in the set-theoretic case, the theorems are the results that are true in the model.

It is not possible to derive all the results true in a given model of the natural numbers from any given "effectively defined" family of axioms (K. Gödel, 1936). This follows from the fact that in the axiomatic number theory one may prescribe to any of its formulas a natural number and then treat the reasoning steps as functions on the natural numbers.

This leads to the possibility of stating a sentence saying about itself that it is not a consequence of axioms. Then neither this sentence, called the "Gödel sentence", nor its negation, is a consequence of the axioms.

It is very interesting that a sentence which cannot be proved within any effectively given axiomatic number theory can always be found among sentences concerning existence of solutions in $\mathbb{Z}$ of an equation

$$f(x_1, \ldots, x_n) = 0, \tag{$*$}$$

where $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. This result proved by Yurii Matyasevich (1970) answered Hilbert's Tenth Problem. It is known that such a polynomial $f(x_1, \ldots, x_n)$ cannot be of degree 1 or 2; it is not known if it can be of degree 3.

Anyway, *number theory is too rich to be axiomatizable.* However, so far, it seems that this ambiguity of the notion of truth of sentences describing properties of the natural numbers does not concern the properties that mathematicians consider to be interesting within number theory. Nevertheless, studies of different theories of numbers and comparing them is an interesting direction of research, an important part of the foundations of arithmetic.

2. Basic structures in the set $\mathbb{N}$ of natural numbers

All ways of defining natural numbers lead to a set $\mathbb{N}$ of natural numbers with two binary operations (addition and multiplication) and an order $\leq$. The binary operations define a structure of a commutative semiring with 1 and 0 and with an order $\leq$. The Induction Axiom can be formulated (and is often applied) as:

◇ *Every nonempty subset $X \subset \mathbb{N}$ contains an element smallest in that set.*

In the semiring $\mathbb{N}$ we have an algorithm of dividing with a remainder and an algorithm of finding the greatest common divisor (gcd). One can easily define in $\mathbb{N}$ the notion of a prime number and prove the *basic theorem of arithmetic* of the natural numbers saying that:

◇ *Every natural number $n > 1$ can be expressed as a product of prime numbers and such a decomposition is unique up to the order of the factors.*

The proof (by induction) of the first part is easy; the proof of the second part is somewhat cumbersome and is much easier after extending $\mathbb{N}$ to the ring $\mathbb{Z}$ of integers.

3. The ring $\mathbb{Z}$

The formal definition of the ring $\mathbb{Z}$ and of the embedding $\mathbb{N} \to \mathbb{Z}$ can be described in the following way.

In $\mathbb{N} \times \mathbb{N}$ we define an equivalence relation $\equiv$ by

$$(m_1, n_1) \equiv (m_2, n_2) \quad \text{iff} \quad m_1 + n_2 = m_2 + n_1$$

and define $\mathbb{Z}$ to be the set of equivalence classes of $\equiv$. Denote the equivalence class containing (m, n) by $[(m, n)]$. Next define an embedding $\mathbb{N} \to \mathbb{Z}$ by $n \mapsto [(n, 0)]$ and define multiplication and addition in $\mathbb{Z}$ by

$$[(m_1, n_1)] + [(m_2, n_2)] = [(m_1 + m_2, n_1 + n_2)],$$
$$[(m_1, n_1)] \cdot [(m_2, n_2)] = [(m_1 m_2 + n_1 n_2, m_2 n_1 + m_1 n_2)].$$

Then $\mathbb{Z}$ becomes a commutative ring with 1 containing $\mathbb{N}$ as a subsemiring (we identify every natural number with its image in $\mathbb{Z}$). The ring $\mathbb{Z}$ is a domain (does not contain zero divisors).

4. Basic algebraic properties of $\mathbb{Z}$

The ring $\mathbb{Z}$ is a Euclidean ring with respect to the norm function defined as the absolute value. It follows that $\mathbb{Z}$ is a *principal ideal domain* (PID), i.e. a domain such that every ideal is generated by one element. Hence every ideal in $\mathbb{Z}$ is composed of integer multiples nm, $n \in \mathbb{Z}$, of a fixed natural number m. The ideal will be denoted by (m).

Since every PID is a unique factorization domain (UFD), we see that $\mathbb{Z}$ is a UFD. Let us recall that a *unique factorization domain* is a domain such that every nonzero nonunit can be expressed as a product of irreducible elements and such a factorization is unique up to the order of factors and multiplication of factors by units.

The irreducible elements in $\mathbb{Z}$ are the prime numbers and their negatives, hence the basic theorem of the arithmetic of natural numbers follows immediately from the UFD property of $\mathbb{Z}$.

In every UFD ring R, for every pair (a, b) of nonzero elements, one defines the *greatest common divisor* $\gcd(a, b)$ as a divisor of both elements which is divisible by all common divisors of those elements. Then $\gcd(a, b)$ exists and is uniquely determined up to multiplication by an invertible element. This notion can be generalized to any finite system of nonzero elements.

Recall also that two elements are said to be *relatively prime* if their greatest common divisor is 1.

In the case of $\mathbb{Z}$, the greatest common divisor can be (uniquely) defined as the greatest (with respect to $\geq$) common divisor.

If the domain R is a PID (as is $\mathbb{Z}$), then the greatest common divisor of any set of elements is a generator of the ideal generated by these elements. In particular, if elements a, b are relatively prime, then the ideal contains 1, and hence there exist $x, y \in R$ such that $ax + by = 1$.

Next, the property of being a UFD implies that the domain is an integrally closed domain (ICD). Recall that a domain R is said to be *integrally closed* if every element from the field of fractions $Q(R)$ which is a root of a monic polynomial from $R[x]$ belongs to R. (A polynomial $f \in R[x]$ is called *monic* if the coefficient of the highest power of x is 1.)

Studying the properties of integers and of their ring $\mathbb{Z}$ is the basic aim of number theory. However, in the development of the theory it has become clear that studying the properties of some other rings connected in some ways with $\mathbb{Z}$ is of great importance. Nowadays, the study of those rings is considered an important part of number theory, even if their direct relation to the properties of integers is not visible. In Chapters 3, 4 and 5 we are going to describe important examples of such rings (the ring of Gaussian integers, the rings $\mathbb{Z}_m$ for $m \in \mathbb{N}$, the rings O_p of p-adic integers) and show how considering these rings helps in solving some problems concerning $\mathbb{Z}$. In the second part of the book, we shall show how these examples of rings are placed in a far more general and deep theory.

5. Linear Diophantine equations

A great part of the theory of numbers concerns integer solutions of *Diophantine equations*, i.e. equations

$$f(x_1, \dots, x_n) = 0,$$

where $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$. In the present section we will consider the case of linear Diophantine equations

$$a_1x_1 + \cdots + a_nx_n = b,$$

where $a_1, \dots, a_n, b \in \mathbb{Z}$ and at least one a_i is different from 0. We would like to describe all solutions of this equation in $\mathbb{Z}^n$.

First of all, if b does not belong to the ideal generated by $a_1, \dots, a_n$ in $\mathbb{Z}$, then there are no such solutions. If b belongs to that ideal and if d is a generator of the ideal, then $b = dd_0$ for some $d_0 \in \mathbb{Z}$. Moreover, we can find elements $m_1, \dots, m_n$ such that

$$a_1m_1 + \cdots + a_nm_n = d.$$

Finally, we see that $x_1 = d_0m_1, \dots, x_n = d_0m_n$ gives a solution of our equation.

When we find a solution of the equation and we write it as a vector $\alpha \in \mathbb{Z}^n$, then every solution can be represented as a sum $\alpha + \omega$, where ω is a solution of the homogeneous equation $a_1x_1 + \cdots + a_nx_n = 0$. All solutions ω of the last equation form a subgroup of the additive group $\mathbb{Z}^n$. Then we may apply the following:

LEMMA 1. *Let $H \subset \mathbb{Z}^n$ be a subgroup. Then $H \simeq \mathbb{Z}^k$ for some $k \leq n$. Moreover if H is given as*

$$H = \{(c_1, \dots, c_n) \in \mathbb{Z}^n : a_1c_1 + \cdots + a_nc_n = 0\},$$

where $(a_1, \dots, a_n) \in \mathbb{Z}^n \setminus \{0\}$, then $k = n - 1$.

Proof. First notice that the result is true for $n = 0, 1$ (every nonzero subgroup of $\mathbb{Z}$ is infinite cyclic and hence isomorphic to $\mathbb{Z}$).

Then assume that the result is true for subgroups of $\mathbb{Z}^{n-1}$ and assume that $H \subset \mathbb{Z}^n$. Project H onto the last axis. Denote the projection map by π. The image $\pi(H) \subset \mathbb{Z}$ is either zero or nonzero. In the first case $H \subset \mathbb{Z}^{n-1}$ and we may use our inductive assumption. In the second case the image of H is isomorphic to $\mathbb{Z}$. Hence $H = \ker(\pi) \oplus \mathbb{Z}$ (take any $a \in \mathbb{Z}^n$ such that $\pi(a)$ is a generator of $\pi(H)$ and prove that H is a direct sum of two of its subgroups: $\ker(\pi)$ and the subgroup generated by a). But $\ker(\pi) \subset \mathbb{Z}^{n-1}$. Thus from our assumption $\ker(\pi) \simeq \mathbb{Z}^k$ for some $k \leq n-1$, and so H is isomorphic to $\mathbb{Z}^{k+1}$.

Moreover, if H is defined as the set of all solutions in $\mathbb{Z}^n$ of a nonzero linear homogeneous equation, then (by the theory of linear equations) it contains a subset composed of $n-1$ linearly independent (over $\mathbb{Q}$) solutions, hence in this case $k = n-1$. □

Thus we have proved the following:

THEOREM 1. *The equation $a_1x_1 + \cdots + a_nx_n = b$ has a solution in $\mathbb{Z}^n$ iff b belongs to the ideal generated by $a_1, \ldots, a_n$. If this condition is satisfied, then there exist solutions $\omega_1, \ldots, \omega_{n-1}$ of $a_1x_1 + \cdots + a_nx_n = 0$ such that every solution of $a_1x_1 + \cdots + a_nx_n = b$ is of the form*

$$\alpha + m_1\omega_1 + \cdots + m_{n-1}\omega_{n-1},$$

where α is any fixed solution of the equation and $m_1, \ldots, m_{n-1} \in \mathbb{Z}$.

Moreover one can find algorithms for finding α and $\omega_1, \ldots, \omega_{n-1}$.

Problems

1. Prove that all solutions in $\mathbb{Z}^3$ of the equation
$$x^2 + y^2 = z^2$$
are (up to permutation of x and y) of the form
$$x = k(n^2 - m^2), \qquad y = 2knm, \qquad z = k(n^2 + m^2).$$
2. Describe all solutions in $\mathbb{Z}^3$ of the equations:
   - $x + y + z = 1$,
   - $4x + 5y + 6z = 1$,
   - $2x + y + 5z = 2$.
3. Assume that $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Prove that the equation
$$x^m + y^m = z^n$$
has infinitely many solutions in $x, y, z \in \mathbb{N}$.
4. Show that $\gcd(x, y) = 1$ iff $\gcd(4x + 3y, 5x + 4y) = 1$.
5. Show that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ for $a > 1$.
6. Prove that $\sum_{k=1}^{n} 1/k \notin \mathbb{N}$ for $n > 1$.
7. Let $\tau(n)$ denote the number of positive divisors of a number n. Prove that $\sum_{n=1}^{N} \tau(n) \equiv \lfloor\sqrt{N}\rfloor \pmod 2$.
8. Let $\sigma(n)$ be the sum of all positive divisors of n. Prove that the sequence $\sigma(n)/n$ is unbounded.
9. Prove that if integers x, y, z satisfy the equation $x^3 + 2y^3 + 4z^3 = 0$ then $x = y = z = 0$.

10. Let us consider the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0 \qquad \text{with } a, b, c \in \mathbb{Z} \setminus \{0\}.$$

Show that if this equation has a solution $(x_0, y_0, z_0) \neq (0, 0, 0)$ then it has infinitely many nonproportional solutions.

11. Fix a nonempty subset $X \subseteq \mathbb{N}$. A number $a \in X$ will be called *irreducible* if it is not a product of smaller elements of X. We call X *factorial* if any number in X has a unique factorization into irreducibles (up to the order of factors). Prove that:

(a) The set $X_1 := \{n \in \mathbb{N} : n \equiv 1 \pmod 4\}$ is not factorial.

(b) The set $X_2 := \mathbb{N} \setminus \{1, 2\}$ is not factorial.

(c) The family of all factorial sets has the cardinality of the continuum.

Remark. X_1 is closed under multiplication and X_2 is even closed under both addition and multiplication—and despite these regularities, the familiar property of unique factorization does not hold!