Introduction to number theory-1

March 13, 2017

Introduction to number theory

Lecturers (30 hours): Maciej Zakarczemny

Exercises (problem sessions 15 hours): Maciej Zakarczemny

Assessment method: two tests during the semester, final exam

The first exam is scheduled for Monday, 26 June 2017, 11.00 – 12:00.

Lectures and a lists of exercises (exercises sheets) will be available online.

My website: maciej.zakarczemny.pl

tab: Introduction to number theory

Topics covered:

Notation and Conventions

Divisibility, GCD, factorization

Fundamental Theorem of Arithmetic

Congruences

Fermat's Little Theorem

Euler's Phi function.

Prime numbers; counting primes, Mersenne and other types of primes

Carmichael numbers

Modular arithmetic and algebra, Chinese Remainder Theorem.

Diophantine equations.

Pythagorean Triples and the Fermat's Last Theorem

"Unbreakable" codes and other applications.

Books:

J. Silverman, A friendly introduction to Number Theory, Prentice Hall, 1997.

Shoup, V. A Computational Introduction to Number Theory and Algebra.

Available at: http://shoup.net/ntb/ntb-v2.pdf

K. Ireland, M. Rosen, A classical introduction in modern number theory, Springer 1990.

W.Narkiewicz, Number Theory, World Scientific, Singapore, 1983.

W.Sierpiński. Elementary theory of numbers, Warszawa-Amsterdam-New York-Oxford 1987.

Z.I. Borevich. I.R.Shafarevich, Number Theory, Academic Press 1966

H. Davenport, The Higher Arithmetic, Cambridge University Press.

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers,
Oxford University Press, 1979.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the course, you need to pass the final exam in the end,

and you need to pass the exercises.

Students must score at least 60 percent on the exam to pass.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the exercises you need to pass:

homework exercises (which will be put on the webpage in due course)

and two tests.

Minimum passing is 60 percent.

The maximum number of lessons that a student may

be absent without acceptable documentation justifying the absence is 2.

Class attendance is required of all undergraduates unless the student has

an official excused absence.

Excused absences are granted for one general reason:

Student has a documented personal reason (illness, injury, health condition etc.).

Consultation hours: Monday 13.30 - 14.30

Room 304/14, located on the third floor, building WIEiK

e-mail: mzakarczemny@pk.edu.pl

Introduction to Number Theory
Institute of Mathematics, Faculty of Physics, Mathematics and Computer Science

is a basic introduction to elementary number theory for undergraduate students with no previous knowledge of the subject.

The only prerequisites are a little calculus and algebra, and the imagination.

The main topics are divisibility and congruences.

Notation and Conventions

We denote the set of positive integers (also called the natural numbers) by $\mathbf{N}$ and the set of nonnegative integers by $\mathbf{N}_0$.

The integer, rational, real numbers are denoted by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, respectively.

The absolute value of $z \in \mathbf{R}$ is $|z|$.

We denote by $\mathbf{Z}^n$ the group of lattice points
in the n-dimensional Euclidean space $\mathbf{R}^n$.

The integer part of the real number x, denoted by $[x]$, is the largest integer that is less than or equal to x.

The fractional part of x is denoted by $\{x\}$.
Then $x = [x] + \{x\}$, where $[x] \in \mathbf{Z}$, $\{x\} \in \mathbf{R}$, and $0 \leq \{x\} < 1$.

In computer science, the integer part of x is often called the *floor* of x, and denoted by $\lfloor x \rfloor$.

The smallest integer that is greater than or equal to x is called the *ceiling* of x, and denoted by $\lceil x \rceil$.

We adopt the standard convention that an empty sum of numbers is equal to 0 and an empty product is equal to 1.

The largest element in a finite set of numbers is denoted by $\max(X)$ and the smallest is denoted by $\min(X)$.

Let a and d be integers.

We write $d|a$ if d divides a, that is, if there exists an integer q such that $a = dq$.

The integers a and b are called *congruent* modulo m, denoted by

$$a \equiv b \pmod{m},$$

if m divides $a - b$.

A *prime number* is an integer $p > 1$ whose only divisors are 1 and p.

The set of prime numbers is denoted by $\mathbf{P}$, and p_k is the kth prime.

Thus, $p_1 = 2, p_2 = 3, \ldots, p_{11} = 31, \ldots$.

Let p be a prime number.

We write $p^r \| n$

if p^r is the largest power of p that divides the integer n,

that is, p^r divides n but p^{r+1} does not divide n.

The *principle of mathematical induction*

states that if $S(k)$ is some statement about integers $k \geq 1$ such that

$S(1)$ is true

and such that

the truth of $S(k)$ implies the truth of $S(k+1)$,

then $S(k)$ holds for all integers $k \geq 1$.

This is equivalent to the *minimum principle*:

A nonempty set of integers bounded below contains a smallest element.

1.1 Division Algorithm

Divisibility is a fundamental concept in number theory. Let a and d be integers. We say that d is a *divisor* of a, and that a is a *multiple* of d, if there exists an integer q such that

$$a = dq.$$

If d divides a, we write

$$d|a.$$

For example, 1001 is divisible by 7 and 13.

Divisibility is transitive:

If a divides b and b divides c, then a divides c .

Theorem 1.1 (Division algorithm) *Let a and d be integers with $d \geq 1$. There exist unique integers q and r such that*

$$a = dq + r \tag{1.1}$$

and

$$0 \leq r \leq d - 1. \tag{1.2}$$

The integer q is called the *quotient* and the integer r is called the *remainder* in the division of a by d.

Proof. Consider the set S of nonnegative integers of the form

$$a - dx$$

with $x \in \mathbf{Z}$. If $a \geq 0$, then $a = a - d \cdot 0 \in S$. If $a < 0$, let $x = -y$, where y is a positive integer. Since d is positive, we have $a - dx = a + dy \in S$ if y is sufficiently large. Therefore, S is a nonempty set of nonnegative integers. By the minimum principle, S contains a smallest element r, and $r = a - dq \geq 0$ for some $q \in \mathbf{Z}$. If $r \geq d$, then

$$0 \leq r - d = a - d(q + 1) < r$$

and $r - d \in S$, which contradicts the minimality of r. Therefore, q and r satisfy conditions (1.1) and (1.2).

Let q_1, r_1, q_2, r_2 be integers such that

$$a = dq_1 + r_1 = dq_2 + r_2 \qquad \text{and} \qquad 0 \leq r_1, r_2 \leq d - 1.$$

Then

$$|r_1 - r_2| \leq d - 1$$

and

$$d(q_1 - q_2) = r_2 - r_1.$$

If $q_1 \neq q_2$, then

$$|q_1 - q_2| \geq 1$$

and

$$d \leq d|q_1 - q_2| = |r_2 - r_1| \leq d - 1,$$

which is impossible. Therefore, $q_1 = q_2$ and $r_1 = r_2$. This proves that the quotient and remainder are unique. $\square$

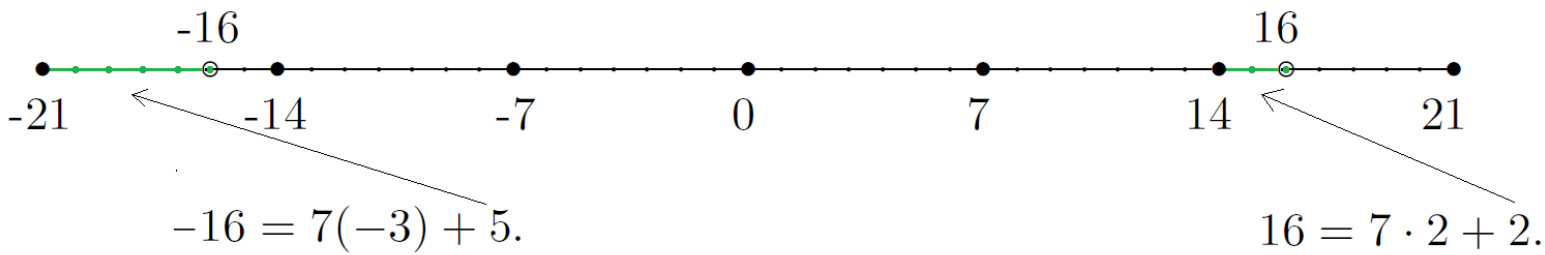
For example, division of 16 by 7 gives the quotient 2 and the remainder 2, that is,

$$16 = 7 \cdot 2 + 2.$$

Division of -16 by 7 gives the quotient -3 and the remainder 5, that is,

$$-16 = 7(-3) + 5.$$

A simple geometric way to picture the division algorithm is to imagine the real number line with dots at the positive integers. Let q be a positive integer, and put a large dot on each multiple of q. The integer a either lies on one of these large dots, in which case a is a multiple of q, or a lies on a dot strictly between two large dots, that is, between two successive multiples of q, and the distance r between a and the largest multiple of q that is less than a is a positive integer no greater than $q - 1$. For example, if $q = 7$ and $a = \pm 16$, we have the following picture.



Using mathematical induction and the division algorithm, we can prove the existence and uniqueness of m-adic representations of integers.

Theorem 1.2 *Let m be an integer, $m \geq 2$. Every positive integer n can be represented uniquely in the form*

$$n = a_0 + a_1 m + a_2 m^2 + \cdots + a_k m^k, \tag{1.3}$$

where k is the nonnegative integer such that $m^k \leq n < m^{k+1}$ and $a_0, a_1, \ldots, a_k$ are integers such that $1 \leq a_k \leq m-1$ and $0 \leq a_i \leq m-1$ for $i = 0, 1, 2, \ldots, k-1$.

This is called the *m-adic representation* of n. The integers a_i are called the *digits* of n to *base* m.

For example, the 2-adic representation of 100 is

$$100 = 1 \cdot 2^2 + 1 \cdot 2^5 + 1 \cdot 2^6, \qquad (1100100)_2$$

and the 3-adic representation of 100 is

$$100 = 1 + 2 \cdot 3^2 + 1 \cdot 3^4. \qquad (10201)_3$$

The 10-adic representation of 217 is

$$217 = 7 + 1 \cdot 10^1 + 2 \cdot 10^2. \qquad (217)_{10}$$

$\binom{n}{k}$ is often read aloud as "n choose k", because there are $\binom{n}{k}$ ways to choose a subset of size k elements, disregarding their order, from a set of n elements.

The binomial formula

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

(valid for any real numbers x,y)

For integers n and k with $n \geq 1$ and $0 \leq k \leq n$, we define the *binomial coefficient*

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Define $\binom{0}{0} = 1$.

Let $\mathbf{N}^k$ denote the set of all k-tuples of positive integers. We define the *lexicographic order* on $\mathbf{N}^k$ as follows. For $(a_1, \ldots, a_k), (b_1, \ldots, b_k) \in \mathbf{N}^k$, we write

$$(a_1, \ldots, a_k) \preceq (b_1, \ldots, b_k)$$

if either $a_i = b_i$ for all $i = 1, \ldots, k$, or there exists an integer j such that $a_i = b_i$ for $i < j$ and $a_j < b_j$.

(a) The relation $\preceq$ is *reflexive* in the sense that if $(a_1, \ldots, a_k) \preceq (b_1, \ldots, b_k)$ and $(b_1, \ldots, b_k) \preceq (a_1, \ldots, a_k)$, then $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$.

(b) The relation $\preceq$ is *transitive* in the sense that if $(a_1, \ldots, a_k) \preceq (b_1, \ldots, b_k)$ and $(b_1, \ldots, b_k) \preceq (c_1, \ldots, c_k)$, then $(a_1, \ldots, a_k) \preceq (c_1, \ldots, c_k)$.

(c) The relation $\prec$ is *total* in the sense that if $(a_1, \ldots, a_k), (b_1, \ldots, b_k) \in \mathbf{N}^k$, then $(a_1, \ldots, a_k) \preceq (b_1, \ldots, b_k)$ or $(b_1, \ldots, b_k) \preceq (a_1, \ldots, a_k)$.

A relation that is reflexive and transitive is called a *partial order*. A partial order that is total is called a *total order*. Thus, the lexicographic order is a total order on the set of k-tuples of positive integers.

1.2 Greatest Common Divisors

Algebra is a natural language to describe many results in elementary number theory.

Let G be a nonempty set, and let $G \times G$ denote the set of all ordered pairs (x, y) with $x, y \in G$. A *binary operation* on G is a map from $G \times G$ into G. We denote the image of $(x, y) \in G \times G$ by $x * y \in G$.

A *group* is a set G with a binary operation that satisfies the following three axioms:

(i) Associativity: For all $x, y, z \in G$,

$$(x * y) * z = x * (y * z).$$

(ii) Identity element: There exists an element $e \in G$ such that for all $x \in G$,

$$e * x = x * e = x.$$

The element e is called the *identity* of the group.

(iii) Inverses: For every $x \in G$ there exists an element $y \in G$ such that

$$x * y = y * x = e.$$

The element y is called the *inverse* of x.

The group G is called *abelian* or *commutative* if the binary operation also satisfies the axiom

(iv) Commutativity: For all $x, y \in G$,

$$x * y = y * x.$$

We can use additive notation and denote the image of the ordered pair $(x, y) \in G \times G$ by $x + y$. We call $x + y$ the *sum* of x and y. In an additive group, the identity is usually written 0, the inverse of x is written $-x$, and we define $x - y = x + (-y)$. We can also use multiplicative notation and denote the image of the ordered pair $(x, y) \in G \times G$ by xy. We call xy the *product* of x and y. In a multiplicative group, the identity is usually written 1 and the inverse of x is written x^{-1}.

Examples of abelian groups are

the integers $\mathbf{Z}$,
the rational numbers $\mathbf{Q}$,
the real numbers $\mathbf{R}$,

with the usual operation of addition.

The nonzero rational, real, denoted by $\mathbf{Q}^\times, \mathbf{R}^\times$, respectively, are also abelian groups, with the usual multiplication as the binary operation.

A *subgroup* of a group G is a nonempty subset of G that is also a group under the same binary operation as G.

If H is a subgroup of G, then

- H is closed under the binary operation in G,
- H contains the identity element of G,
- and the inverse of every element of H belongs to H.

For example, the set of even integers $2\mathbf{Z}$ ={...-6,-4,-2,0,2,4,6...}
is a subgroup of $\mathbf{Z}$.

For example, the set $7\mathbf{Z}$ = {...-28,-21,-14,-7,0,7,14,21,28...}
is a subgroup of $\mathbf{Z}$.

The set $\mathbf{Q}$ of rational numbers is a subgroup of the additive group $\mathbf{R}$.

The set $\mathbf{R}^+$ of positive real numbers is a subgroup of the multiplicative group $\mathbf{R}^\times$.

For every integer d, the set of all multiples of d is a subgroup of $\mathbf{Z}$. We denote this subgroup by $d\mathbf{Z}$.

If $a_1, \ldots, a_k \in \mathbf{Z}$, then the set of all numbers of the form

$$a_1x_1 + \cdots + a_kx_k$$

with $x_1, \ldots, x_k \in \mathbf{Z}$ is also a subgroup of $\mathbf{Z}$.