# Introduction to number theory-2

March 20, 2017

## 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

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

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

$$a_1x_1 + \cdots + a_kx_k$$

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

If $G$ is a group, written multiplicatively, and $g \in G$, then $g^n \in G$ for all $n \in \mathbf{Z}$ , and $\{g^n : n \in \mathbf{Z}\}$ is a subgroup of $G$.

**Theorem 1.3** *Let $H$ be a subgroup of the integers under addition. There exists a unique nonnegative integer $d$ such that $H$ is the set of all multiples of $d$, that is,*

$$H = \{0, \pm d, \pm 2d, \ldots\} = d\mathbf{Z}.$$

**Proof**. We have $0 \in H$ for every subgroup $H$. If $H = \{0\}$ is the zero subgroup, then we choose $d = 0$ and $H = 0\mathbf{Z}$. Moreover, $d = 0$ is the unique generator of this subgroup.

If $H \neq \{0\}$, then there exists $a \in H, a \neq 0$. Since $-a$ also belongs to $H$, it follows that $H$ contains positive integers. By the minimum principle, $H$ contains a least positive integer $d$. Moreover, $dq \in H$ for every integer $q$, and so $d\mathbf{Z} \subseteq H$.

Let $a \in H$. By the division algorithm, we can write $a = dq + r$, where $q$ and $r$ are integers and $0 \leq r \leq d - 1$.

Since $dq \in H$ and $H$ is closed under subtraction, it follows that

$$r = a - dq \in H.$$

Since $0 \leq r < d$ and $d$ is the smallest positive integer in $H$, we must have $r = 0$, that is, $a = dq \in d\mathbf{Z}$ and $H \subseteq d\mathbf{Z}$.
It follows that $H = d\mathbf{Z}$.

If $H = d\mathbf{Z} = d'\mathbf{Z}$, where $d$ and $d'$ are positive integers,
then $d' \in d\mathbf{Z}$ implies that $d' = dq$ for some integer $q$,
and $d \in d'\mathbf{Z}$ implies that $d = d'q'$ for some integer $q'$.

Therefore, $d = d'q' = dqq'$,
and so $qq' = 1$, hence $q = q' = \pm 1$ and $d = \pm d'$.
Since $d$ and $d'$ are positive, we have $d = d'$,
and $d$ is the unique positive integer that generates the subgroup $H$. □

For example, if $H$ is the subgroup consisting of all integers of the form $35x + 91y$, then $7 = 35(-5) + 91(2) \in H$ and $H = 7\mathbf{Z}$.

Let $A$ be a nonempty set of integers, not all 0. If the integer $d$ divides $a$ for all $a \in A$, then $d$ is called a *common divisor* of $A$.

For example, 1 is a common divisor of every nonempty set of integers.

The positive integer $d$ is called the *greatest common divisor* of the set $A$, denoted by $d = \gcd(A)$,

if

$d$ is a common divisor of $A$

and

every common divisor of $A$ divides $d$.

We shall prove that every nonempty set of integers has a greatest common divisor.

**Theorem 1.4** *Let $A$ be a nonempty set of integers, not all zero. Then $A$ has a unique greatest common divisor, and there exist integers $a_1, \dots, a_k \in A$ and $x_1, \dots, x_k$ such that*

$$\gcd(A) = a_1x_1 + \cdots + a_kx_k.$$

**Proof**. Let $H$ be the subset of $\mathbf{Z}$ consisting of all integers of the form

$$a_1x_1 + \cdots + a_kx_k \qquad \text{with } a_1, \ldots, a_k \in A \text{ and } x_1, \ldots, x_k \in \mathbf{Z}.$$

Then $H$ is a subgroup of $\mathbf{Z}$ and $A \subseteq H$.

By Theorem 1.3, there exists a unique positive integer $d$
such that $H = d\mathbf{Z}$,
that is, $H$ consists of all multiples of $d$.

In particular, every integer $a \in A$ is a multiple of $d$, and so $d$ is a common divisor of $A$.

Since $d \in H$, there exist integers $a_1, \ldots, a_k \in A$ and $x_1, \ldots, x_k$ such that

$$d = a_1x_1 + \cdots + a_kx_k.$$

If $A = \{a_1, \ldots, a_k\}$ is a nonempty, finite set of integers, not all 0, we write $\gcd(A) = (a_1, \ldots, a_k)$. For example,

$$(35, 91) = 7 = 35(-5) + 91(2).$$

**Theorem 1.5** *Let $a_1, \ldots, a_k$ be integers, not all zero.*

*Then $(a_1, \ldots, a_k) = 1$*
*if and only if there exist integers $x_1, \ldots, x_k$ such that*

$$a_1x_1 + \cdots + a_kx_k = 1.$$

The integers $a_1, \ldots, a_k$ are called *relatively prime* if their greatest common divisor is 1, that is, $(a_1, \ldots, a_k) = 1$.

The integers $a_1, \ldots, a_k$ are called *pairwise relatively prime* if $(a_i, a_j) = 1$ for $i \neq j$.

For example, the three integers $6, 10, 15$ are relatively prime but not pairwise relatively prime:

$$\text{since } (6, 10, 15) = 1\,,$$

$$\text{but } (6, 10) = 2,\ (6, 15) = 3, \text{ and } (10, 15) = 5.$$

Let $G$ and $H$ be groups, and denote the group operations by $*$.
A map $f : G \to H$ is called a *group homomorphism* if

$$f(x * y) = f(x) * f(y) \text{ for all } x, y \in G.$$

Thus, a homomorphism $f$ from an additive group $G$ into a multiplicative group $H$ is a map such that $f(x + y) = f(x)f(y)$ for all $x, y \in G$.

# The Euclidean Algorithm and Continued Fractions

Let $a$ and $b$ be integers with $b \geq 1$. There is a simple and efficient method to compute the greatest common divisor of $a$ and $b$ and to express $(a, b)$ explicitly in the form $ax + by$. Define $r_0 = a$ and $r_1 = b$. By the division algorithm, there exist integers $q_0$ and $r_2$ such that

$$r_0 = r_1 q_0 + r_2$$

and

$$0 \leq r_2 < r_1.$$

If an integer $d$ divides $r_0$ and $r_1$, then $d$ also divides $r_1$ and $r_2$.

Similarly, if an integer $d$ divides $r_1$ and $r_2$, then $d$ also divides $r_0$ and $r_1$.
Therefore, the set of common divisors of $r_0$ and $r_1$
is the same as the set of common divisors of $r_1$ and $r_2$, and so

$$(a, b) = (r_0, r_1) = (r_1, r_2).$$

If $r_2 = 0$, then $a = bq_0$ and $(a, b) = b = r_1$.

If $r_2 > 0$, then we divide $r_2$ into $r_1$ and obtain integers $q_1$ and $r_3$ such that

$$r_1 = r_2 q_1 + r_3,$$

where

$$0 \leq r_3 < r_2 < r_1$$

and

$$(a, b) = (r_1, r_2) = (r_2, r_3).$$

Moreover, $q_1 \geq 1$ since $r_2 < r_1$. If $r_3 = 0$, then $(a, b) = r_2$.

If $r_3 > 0$, then there exist integers $q_2$ and $r_4$ such that

$$r_2 = r_3 q_2 + r_4,$$

where $q_2 \geq 1$ and

$$0 \leq r_4 < r_3 < r_2 < r_1$$

and

$$(a, b) = (r_2, r_3) = (r_3, r_4).$$

If $r_4 = 0$, then $(a, b) = r_3$.

Iterating this process $k$ times, we obtain an integer $q_0$, a sequence of positive integers $q_1, q_2, \ldots, q_{k-1}$, and a strictly decreasing sequence of non-negative integers $r_1, r_2, \ldots, r_{k+1}$ such that

$$r_{i-1} = r_i q_{i-1} + r_{i+1}$$

for $i = 1, 2, \ldots, k$, and

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_k, r_{k+1}).$$

If $r_{k+1} > 0$, then we can divide $r_k$ by $r_{k+1}$ and obtain

$$r_k = r_{k+1} q_k + r_{k+2},$$

where $0 \leq r_{k+2} < r_{k+1}$.

Since a strictly decreasing sequence of nonnegative integers must be finite, it follows that there exists an integer $n \geq 1$ such that $r_{n+1} = 0$.

Then we have

an integer $q_0$,

a sequence of positive integers $q_1, q_2, \ldots, q_{n-1}$,

and a strictly decreasing sequence of positive integers $r_1, r_2, \ldots, r_n$,

with $(a, b) = (r_n, r_{n+1}) = r_n$.

The $n$ applications of the division algorithm produce $n$ equations

$$\begin{aligned}
r_0 &= r_1 q_0 + r_2 \\
r_1 &= r_2 q_1 + r_3 \\
r_2 &= r_3 q_2 + r_4 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-2} + r_n \\
r_{n-1} &= r_n q_{n-1}.
\end{aligned}$$

Since $r_n < r_{n+1}$, it follows that $q_{n-1} \geq 2$.

This procedure is called the *Euclidean algorithm.*

We call $n$ the *length* of the Euclidean algorithm for $a$ and $b$.

This is the number of divisions required to find the greatest common divisor.

The sequence $q_0, q_1, \ldots, q_{n-1}$ is called the *sequence of partial quotients.*

The sequence $r_2, r_3, \ldots, r_n$ is called the *sequence of remainders.*

This procedure is called the *Euclidean algorithm.*

We call $n$ the *length* of the Euclidean algorithm for $a$ and $b$.

This is the number of divisions required to find the greatest common divisor.

The sequence $q_0, q_1, \ldots, q_{n-1}$ is called the *sequence of partial quotients.*

The sequence $r_2, r_3, \ldots, r_n$ is called the *sequence of remainders.*

Let us use the Euclidean algorithm to find $(574, 252)$ and express it as a linear combination of 574 and 252. We have

$$\begin{aligned} 574 &= 252 \cdot 2 + 70, \\ 252 &= 70 \cdot 3 + 42, \\ 70 &= 42 \cdot 1 + 28, \\ 42 &= 28 \cdot 1 + 14, \\ 28 &= 14 \cdot 2, \end{aligned}$$

and so

$$(574, 252) = 14.$$

Working backwards through the Euclidean algorithm to express 14 as a linear combination of 574 and 252, we obtain

$$\begin{aligned} 14 &= 42 - 28 \cdot 1 \\ &= 42 - (70 - 42 \cdot 1) \cdot 1 = 42 \cdot 2 - 70 \cdot 1 \\ &= (252 - 70 \cdot 3) \cdot 2 - 70 \cdot 1 = 252 \cdot 2 - 70 \cdot 7 \\ &= 252 \cdot 2 - (574 - 252 \cdot 2) \cdot 7 = 252 \cdot 16 - 574 \cdot 7. \end{aligned}$$

**thank you**

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

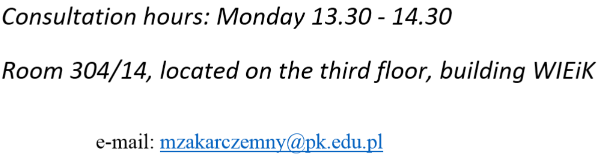
be absent without acceptable documentation justifying the absence is 2.

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