Arithmetic Number Theory

Uwe Kraeft

2003

Berichte aus der Mathematik

Uwe Kraeft

Arithmetic Number Theory

Shaker Verlag
Aachen 2003

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Kraeft, Uwe:
Arithmetic Number Theory / Uwe Kraeft.
Aachen : Shaker, 2003
(Berichte aus der Mathematik)
ISBN 3-8322-1147-0

Printed in Germany.

ISBN 3-8322-1147-0
ISSN 0945-0882

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • eMail: info@shaker.de

Preface

The arithmetic is nowadays the classical and practical part of number theory. There exist several famous and voluminous textbooks from the 19th and beginning of the 20th century. While the methods are elementary, it is this the part of number theory which seems to be difficult and strange for many students. This text tries to give some explanations and shows the application in calculation.

In chronological order with former books on Pythagorean Triples, Euclidean Sequences, Diophantine Equations, Archimedean Approximations, Number Theory of Adjunctions, and Statistical Number Theory this seventh text is a basic treatment of arithmetic number theory and written for all who are interested in basic mathematics. It is also a major aim to show the methods used in number theory. Therefore the reader can find in the here told proofs more syllogisms than usual in textbooks. Especially this may be of interest for the student who begins to study the elements of number theory. The book is dedicated to the memory of Adrien-Marie Legendre and Carl Friedrich Gauß (also Gauss), who laid with the „Essai sur la théorie des nombres" (Legendre) and the „Disquisitiones arithmeticae" (Gauß) the base of higher arithmetic number theory.

I would appreciate discussions, remarks, and hints if there are mistakes.

Leimen, in December 2002 Uwe Kraeft

Symbols

$\Rightarrow$	by this follows
$\forall$	for all
$\exists$	There is/are
$\in$	is element of (is contained in)
$\notin$	is no element of (isn't contained in)
$\subset$	is subset of (all elements are contained in)
$\cup, \cap$	union and intersection of sets
$\varnothing$	the empty set
{a,b,c}	an example of a set with elements a, b, and c
{{a,a,b}}	an example of an assemblage with elements a, a, and b
a, A, α ...	in this text mainly natural numbers or integers
N	set of natural numbers 1, 2, 3, ...
N^-	$=\{-N\}=\{-n; n\in N\}$, set of negative integers -1, -2, -3, ...
N^0	$N\cup\{0\}$
P	primes of N
P^1	$P\cup\{1\}$, primes P included 1
Z	$=N\cup\{N^-\}\cup\{0\}$, set of integers
Q	set of rational numbers a/b with $a\in Z$, $b\in N$
Q^+	set of positive rational numbers a/b with $a,b\in N$
R	set of real number algorithms
Q(R)	Q or R
=	equal (not between rational and irrational numbers)
$\cong$	so near as you want but not identical
$\neq$	not equal
<, >	less, greater
$(a<b)\in Q$	a<b and both are elements of Q
$\sum_{i=1}^{n} a_i$	$=a_1+a_2+ \ldots +a_n$
n!	$=n(n-1)*\ldots*2*1$

$(a,b)=1$	greatest common divisor (factor) $\gcd \in \mathbb{N}$ of a and b is 1
d_i	i^{th} divisor (factor) of n
$\equiv$	$a \equiv b \pmod{m,n,mn}$ if $m,n \in \mathbb{N}$ and $a,b,(a-b)/(mn) \in \mathbb{Z}$; $a \equiv b \pmod{t\ m} \Leftrightarrow a-b=m$
$[a]$	residue class $\{x;\ x \in \mathbb{Z}$ and $x \equiv a \pmod{m}\}$
R_m	set of all residue classes modulo m
G_m	group of prime residue classes modulo m
$\varphi(n)$	number of prime residue classes mod n (Euler's function)
$(a'/p)=b$	$=\left(\frac{a}{p}\right)=b \Leftrightarrow a^{(p-1)/2} \equiv b \pmod{p}$ for $(p>2) \in P$ and normally $(a,p)=1$ (Legendre's symbol)
$\left(\frac{a}{n}\right)$	$=(a'/p_1)(a'/p_2)*...*(a'/p_n)$ with $n=p_1p_2*...*p_n$ for $(p_i>2) \in P$ and normally $(a,p_i)=1$ (Jacobi's symbol)

Content