Primes in Number Theory

Uwe Kraeft

2005

Berichte aus der Mathematik

Uwe Kraeft

Primes in Number Theory

Shaker Verlag
Aachen 2005

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.ddb.de.

Copyright Shaker Verlag 2005
All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 3-8322-3886-7
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

Without any doubt, primes are the most prominent numbers. They are, to say it in simple words, the base of calculations. All other natural, rational, or irrational numbers are resulting or expressed by them. True primes are natural numbers which can only be divided without remainder or residue by themselves or the number one. The trivial conclusion is that there are no other integer parts in primes. Already Euclid knew that the number of primes is infinite. Eratosthenes gave an algorithm for their construction, which is not surpassed. Today, there exists a comprehensive but in many aspects not sufficient knowledge about these numbers.

There is also a practical aspect of primes in factorisation of natural numbers. Hunting great primes and prime twins is like a sport in mathematics.

While the knowledge about primes can only be called vast and a detailed treatment would fill thousands of pages, in this book, some important basic ideas can be found. The main goal is to show the connections with number theory. A choice of equations and theorems is often only shortly cited.

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

Leimen, in February 2005 Uwe Kraeft

Choice of symbols (see also chapter 5)

$\Rightarrow$	by this follows
$\forall$	for all
$\in$	is element of (is contained in)
$\subset$	is subset of (all elements are contained in)
A={a,b,c}	an example of a set A with elements a, b, and c
a, α ...	in this text mainly natural numbers or integers
N	set of natural numbers 1, 2, 3, ...
N^-	={-N}={-n; n∈N}, set of negative integers -1, -2, -3, ...
N^0	N∪{0}
P	primes of N
P^1	P∪{1}, primes P included 1
p	if not otherwise indicated, generally a prime
p_I, p_{II}	prime I: 4m+1 with m∈N, prime II: 4n-1 with n∈N
p#=p!	product of all primes equal or less p: 2*3*5*7* ... *p
c!	product of all composite numbers equal or less c: 4*6*8* ... *c
n!, (p-1)!	product of all natural numbers equal or less n, (p-1)
Z	=N∪{N^-}∪{0}, set of integers
Q	set of rational numbers a/b with a∈Z, b∈N
Q^+	set of positive rational numbers a/b with a,b∈N
R	set of real number algorithms
Q(R)	Q or R
[...],]...[	closed, open interval
C	complex numbers x+yi with x,y∈Q(R)
M(α)	={α,a+bα; a,b∈M}, f.e. Z(i)⊂C
Q($\sqrt{a}$, ...)	adjunction of $\sqrt{a}$, ... to Q
=	equal (identical) by axioms or definitions
$\cong$	so near as you want but not identical
$\approx$	about, rounded, can f.e. be approximated for great n
~	similar order of magnitude (in [HW p. 7], the meaning of ≈)
$\equiv$	a≡b (mod c) ⇔ $a=b_c$ ⇔ (a-b)/c∈Z for a,b∈Z, c∈N
(a<b)∈Q	a<b and both are elements of Q
(a,b)=c	gcd of a,b∈Z-{0} is c∈N
b|a	b divides a, b is a factor (divisor) of a, $a=0_b$, a∈Z-{0}, b∈N
f.e.	for example (e.g.)
PT	Pythagorean Triple, n nonprimitive, p primitive
FLT	Fermat's Last Theorem

Basic algebraic structures used in this text

Axioms of sets F with inner operations addition „+" or multiplication „*"
$\forall a,b,c,x \in F$ [Kr5 p. 43]

A1 $a+b \in F$ (set F closed with addition)
A2 $(a+b)+c=a+(b+c)$ (associative law of addition)
A3 $a+b=b+a$ (commutative law of addition)
A4a $\exists 0 \in F$ such that $0+a=a$ (existence of a left neutral element: zero)
A4b $\exists x=-a \in F$ such that $x+a=0$ (existence of additive left inverses)
M1 $a*b \in F$ (set F closed with multiplication)
M2 $(a*b)*c=a*(b*c)$ (associative law of multiplication)
M3 $a*b=b*a$ (commutative law of multiplication)
M4a $\exists e \in F$ such that $e*a=a$ (existence of a left neutral element: unity)
M4b $\forall a \neq 0\ \exists x=a^{-1} \neq 0 \in F$ such that $a^{-1}*a=1$ (existence of multiplicative left inverses)
D $a*(b+c)=a*b+a*c$ and $(b+c)*a=b*a+c*a$ (distributive laws)
Z from $a*b=0$ follows at least $a=0$ or $b=0$ (zero divisor free)
U $1 \neq 0$

one inner operation + (or * in **M1**, ...)

groupoid:	**A1**
semigroup:	**A1, A2**
monoid:	**A1, A2, A4a**
group:	**A1, A2, A4a, A4b**
Abelian group AG:	**A1, A2, A3, A4a, A4b**

two inner operations + and *

ring:	**AG, M1, M2,**		**D**
commutative ring:	**AG, M1, M2, M3,**		**D**
ring with unity:	**AG, M1, M2,**	**M4a,**	**D**
zero div. free ring:	**AG, M1, M2,**	**M4a,**	**D, Z**
integral domain:	**AG, M1, M2, M3,**	**M4a,**	**D, Z, U**
skew field:	**AG, M1, M2,**	**M4a, M4b,**	**D, Z, U**
field:	**AG, M1, M2, M3,**	**M4a, M4b,**	**D, Z, U**

For more structures and discussions see chapter 8 of this text

Content

	page
1. Introduction	1
2. Construction of primes	13
3. Divisibility of primes and integers	25
4. Prime tests and factorisation	31
5. Choice of primes and relative primes in functions	41
6. Basic theorems about primes	43
7. Special numbers and primes	51
8. Algebra of primes	61
9. Large primes and applications	75
Choice of literature	83
Supplements to former books of this series	87