

**Characters**  
**in**  
**Number Theory**

**Uwe Kraeft**

2007



Berichte aus der Mathematik

**Uwe Kraeft**

**Characters in Number Theory**

Shaker Verlag  
Aachen 2007

**Bibliographic information published by the Deutsche Nationalbibliothek**

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Copyright Shaker Verlag 2007

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 978-3-8322-6754-4  
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](http://www.shaker.de) • e-mail: [info@shaker.de](mailto:info@shaker.de)

## Preface

The homomorphisms of residue classes or their subgroups onto cyclic subgroups of real or complex numbers, which are called residue class characters, Dirichlet characters, or simply characters, make direct calculations possible; they are also a tool to select special terms in sums. This idea is especially used in the number theory of L-series, f.e. in the zeta function, the Gauss and Jacobi sums, and the proof of Dirichlet's theorem. Characters can be regarded as a step from basic to advanced number theory. Besides these residue class characters, more algebraic characters are defined.

With homomorphisms of finite Abelian groups, characters, the divisor function, von Mangoldt function, and Liouville function in Dirichlet series, Dirichlet series (general), Dirichlet L-series, Gauss , Ramanujan, Kloosterman, and Jacobi sums, and the proof of Dirichlet's theorem by different authors, a choice of applications of characters in number theory is given in this book.

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

Leimen, in October 2007

Uwe Kraeft



### Choice of symbols

|  |  |
|--|--|
| $\Rightarrow, \Leftarrow, \Leftrightarrow$ | by this follows (in the given directions)  |
| $\in$                                      | is element of (is contained in)  |
| $\notin$                                   | is no element of (isn't contained in)  |
| $A=\{a,b,c\}$                              | an example of a set A with elements a, b, and c  |
| $f, \chi$                                  | mappings   |
| $f(x)$                                     | map of the original x  |
| $f^{-1}$                                   | inverse mapping  |
| $a, \alpha, \dots$                         | elements   |
| $-a, \alpha^{-1}$                          | inverse elements (with addition, multiplication)   |
| $\# \{ \dots \}$                           | number of elements   |
| $m, n, \dots$                              | natural numbers  |
| $\mathbb{N}$                               | set of natural numbers 1, 2, 3, ... or any natural number  |
| $p$  | if not otherwise indicated, generally a prime  |
| $\pi(n)$                                   | the number of primes equal or less n   |
| $p_I, p_{II}$                              | prime I: $4m+1$ with $m \in \mathbb{N}$ , prime II: $4n-1$ with $n \in \mathbb{N}$   |
| $P$  | primes of $\mathbb{N}$ ( $P^1$ with the unity)   |
| $\mathbb{N}^0$                             | $\mathbb{N} \cup \{0\}$  |
| $\mathbb{N}^-$                             | $\{-n; n \in \mathbb{N}\}$ , set of negative integers -1, -2, -3, ...  |
| $\mathbb{Z}$                               | $=\mathbb{N} \cup \{\mathbb{N}^-\} \cup \{0\}$ , ring of integers  |
| $\mathbb{Z}/m\mathbb{Z}$                   | ring of congruence classes modulo m  |
| $\mathbb{Q}$                               | field of rational numbers $a/b$ with $a \in \mathbb{Z}, b \in \mathbb{N}$  |
| $\mathbb{Q}^+$                             | set of positive rational numbers $a/b$ with $a, b \in \mathbb{N}$  |
| $\mathbb{R}$                               | field of real number algorithms  |
| $[\dots], ]\dots[, \dots$                  | closed, open interval, ...   |
| $[a,b]$                                    | all x in the closed interval $a \leq x \leq b$   |
| $a = \alpha + i\beta$                      | $= \alpha + \beta i$ complex number with $\alpha, \beta \in \mathbb{Q}(\mathbb{R})$ and $i^2 = -1$   |
| $a^* = \bar{a} = \alpha - i\beta$          | conjugate complex number   |
| $a = \alpha + i\beta$                      | $= r(\cos \varphi + i \sin \varphi)$ in polar coordinates;<br>$r =  a $ modulus or absolute value of a or length of vector $\vec{r}$ ;<br>$\varphi$ is called argument $\arg(a)$ , $\arg a$ , or the phase angle |
| $\mathbb{C} = \mathbb{C}^1$                | $= \mathbb{Q}(i)$ or $\mathbb{R}(i)$ field of complex numbers  |
| $\mathbb{Q}(\mathbb{R}, \mathbb{C})$       | $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$   |
| $\mathbb{C}^G$                             | Gaussian integers with $(\alpha, \beta \neq 0) \in \mathbb{Z}$   |
| $\zeta$                                    | root of unity  |

|                             |   |
|-----------------------------|---|
| $=$                         | equal (identical) by axioms or definitions  |
| $\equiv$                    | $a \equiv b \pmod{c} \Leftrightarrow a \equiv b_c \Leftrightarrow (a-b)/c \in \mathbb{Z}$ for $a, b \in \mathbb{Z}, c \in \mathbb{N}$ |
| $\cong$                     | so near as you want but not identical   |
| $\approx$                   | about, rounded, can f.e. be approximated for great $n$  |
| $\sim$                      | similar order of magnitude  |
| $\neq$                      | not equal   |
| $<, >$                      | less, greater   |
| $n!, (p-1)!$                | product of all natural numbers equal or less $n, (p-1)$   |
| $\binom{a}{b}$              | $\frac{a!}{b!(a-b)!} = \frac{a(a-1)(a-2)*\dots*(a-b+1)}{b(b-1)(b-2)*\dots*1}$ binomial coefficient                                    |
| $\sum_{i=1}^n a_i$          | $= a_1 + a_2 + \dots + a_n$   |
| $L(s, \chi)$                | $= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ Dirichlet L-series (see chapter 5; $\chi$ see chapter 1)                                  |
| $\prod_{i=1}^n a_i$         | $= a_1 * a_2 * \dots * a_n$   |
| $a^n$                       | $n$ th power of $a$   |
| $a^{-n}$                    | $1/a^n$   |
| $a^{1/m}$                   | $m$ th root of $a$ (f.e. $a^{1/2} = \sqrt{a}$ )   |
| $a^{n/m}$                   | $m$ th root of $a^n$  |
| $\{a_i\} = (a_i)$           | $\{a_1, a_2, \dots, a_n\}$ sequence of numbers $a_i$  |
| $b a$                       | $b$ divides $a$ , $b$ is a factor (divisor) of $a$ , $a \equiv 0_b, a \in \mathbb{Z} - \{0\}, b \in \mathbb{N}$                       |
| $p, (q > 1) \in \mathbb{N}$ | $p, q$ are natural numbers and $q > 1$  |
| $(a, b) = d$                | gcd (see below) of $a$ and $b$ is $d$   |
| $\{(a, b)\} = e$            | lcm (see below) of $a$ and $b$ is $e$   |
| $a, b, c$                   | triple of an equation's solution, f.e. PT (see below)   |
| $\frac{p}{q}$               | ratio or common fraction with $p \in \mathbb{Z}, q \in \mathbb{N}$ ,  |
|                             | which can be proper $\left  \frac{p}{q} \right  < 1$ or improper $\left  \frac{p}{q} \right  \geq 1$                                  |

|                              |  |
|------------------------------|--|
| $\left(\frac{a}{p}\right)=1$ | $=(a'/p)=1 \Leftrightarrow a^{(p-1)/2} \equiv 1_p$ (Legendre's symbol)   |
| $\left(\frac{a}{n}\right)$   | $=(a'/p_1)(a'/p_2)(a'/p_3)*\dots$ with $n=p_1p_2p_3*\dots$ , $(p_i>2) \in P$ , and $(a,p_i)=1$ (Jacobi's symbol) |
| $\ln x$                      | natural logarithm of $x$ with $x=e^{\ln x}$  |
| $\text{ind } a$              | index of $a$ with $a \equiv g^{\text{ind } a} \pmod{m}$ , and $(a,m)=1$  |
| $F^*$                        | multiplicative group (without zero) of a field $F$   |
| f.e.                         | for example (e.g.)   |
| gcd                          | greatest common divisor  |
| lcm                          | least common multiple  |
| modulus                      | divisor, from Latin "modulus" measure  |
| PT                           | Pythagorean Triple   |
| $\text{sgn } z$              | $= \frac{z}{ z }$ for $0 \neq z \in C(Q,R)$ or $= 0$ if $z = 0$ , sign function                                  |
| $\chi(n)$                    | character of $n \in N^0$ (see chapter 1)   |
| $\phi(n)$                    | Euler's function, see [Kr19 p. 186]  |
| $\mu(n)$                     | Möbius function, see [Kr19 p. 187]   |
| $\sigma_k(n)$                | divisor function (see chapter 3.1)   |
| $\Lambda(n)$                 | von Mangoldt function (see chapter 3.2)  |
| $\lambda(n)$                 | Liouville function (see chapter 3.3)   |

Many other special symbols and number theoretic functions are explained in the text.

The order of this sequence of texts on number theory is twofold. The order following the date of printing is given at the end of this book. Another grouping is got by the colours of the covers after disciplines as follows:

|                            |              |
|----------------------------|--------------|
| arithmetic number theory:  | light blue   |
| sequences and series:      | dark green   |
| Diophantine Equations:     | orange       |
| algebraic number theory:   | dark red     |
| topological number theory: | purple       |
| analytic number theory:    | dark blue    |
| statistical number theory: | light green  |
| special numbers:           | dark yellow  |
| textbooks:                 | light yellow |

**Content**

|   | page   |
|---|--------|
| 1. Homomorphisms of finite Abelian groups - - - -           | 1      |
| 2. Characters - - - - -                                     | 7      |
| 3. Number theoretic functions in Dirichlet series - - - -   | 19     |
| 3.1 The divisor function - - - - -                          | 19     |
| 3.2 The von Mangoldt function - - - - -                     | 21     |
| 3.3 The Liouville function - - - - -                        | 21     |
| 4. Dirichlet series (general) - - - - -                     | 23     |
| 5. Dirichlet L-series - - - - -                             | 27     |
| 6. Gauss, Ramanujan, Kloosterman, and Jacobi sums - - - -   | 31     |
| 7. The proof of Dirichlet's theorem - - - - -               | 35     |
| 8. Dirichlet's theorem in literature - - - - -              | 49     |
| <br>Choice of relevant literature - - - - -                 | <br>61 |
| <br>Choice of general textbooks about number theory - - - - | <br>63 |
| Choice of journals about number theory - - - - -            | 68     |
| <br>Publications of the author - - - - -                    | <br>69 |
| <br>Supplements to former books of this series - - - - -    | <br>71 |