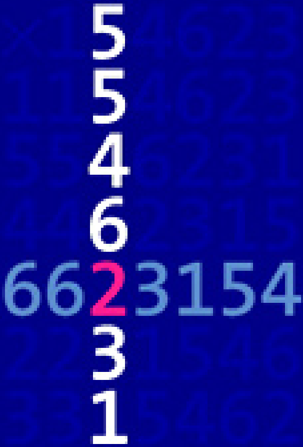

Numbers Groups & Codes

Second Edition

J. F. Humphreys & M. Y. Prest

CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521540506

This page intentionally left blank

Numbers, Groups and Codes

Second Edition

Numbers, Groups and Codes

Second Edition

J. F. HUMPHREYS
Senior Fellow in Mathematics, University of Liverpool

M. Y. PREST
Professor of Mathematics, University of Manchester

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521540506

© Cambridge University Press 2004

This publication is in copyright. Subject to statutory exception and to the provision of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published in print format 2004

ISBN-13 978-0-511-19346-0 eBook (ebrary)
ISBN-10 0-511-19346-7 eBook (ebrary)

ISBN-13 978-0-521-54050-6 paperback
ISBN-10 0-521-54050-X paperback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

To Sarah, Katherine and Christopher *J. F. Humphreys*
To the memory of my parents *M. Y. Prest*

Contents

Preface to first edition *page* ix

Preface to second edition x

Introduction xi

Advice to the reader xiv

1 Number theory 1

1.1 The division algorithm and greatest common divisors 1

1.2 Mathematical induction 15

1.3 Primes and the Unique Factorisation Theorem 25

1.4 Congruence classes 36

1.5 Solving linear congruences 49

1.6 Euler’s Theorem and public key codes 59

Summary of Chapter 1 77

2 Sets, functions and relations 78

2.1 Elementary set theory 78

2.2 Functions 86

2.3 Relations 103

2.4 Finite state machines 117

Summary of Chapter 2 126

3 Logic and mathematical argument 127

3.1 Propositional logic 128

3.2 Quantifiers 137

3.3 Some proof strategies 141

Summary of Chapter 3 146

4 Examples of groups 147

4.1 Permutations 148

4.2 The order and sign of a permutation 159

4.3 Definition and examples of groups 170