

# Numbers, groups and codes

---

J. F. Humphreys

*Reader in Pure Mathematics, University of Liverpool*

M. Y. Prest

*Senior Lecturer in Mathematics, University of Manchester*



**CAMBRIDGE**  
UNIVERSITY PRESS

# Contents

---

Preface	ix
Introduction	x
Advice to the reader	xiii
<b>1 Number theory</b>	<b>1</b>
1.1 Mathematical induction	1
1.2 The division algorithm and greatest common divisors	10
1.3 Primes and the Unique Factorisation Theorem	19
1.4 Congruence classes	28
1.5 Solving linear congruences	40
1.6 Euler's Theorem and public key codes	50
<b>2 Sets, functions and relations</b>	<b>67</b>
2.1 Elementary set theory	67
2.2 Functions	75
2.3 Relations	92
2.4 Finite state machines	106
<b>3 Logic, boolean algebra and normal forms</b>	<b>115</b>
3.1 Propositional calculus	115
3.2 Boolean algebras	125
3.3 Karnaugh maps and switching circuits	140
<b>4 Examples of groups</b>	<b>155</b>
4.1 Permutations	155
4.2 The order and sign of a permutation	167
4.3 Definition and examples of groups	178
4.4 Algebraic structures	192

<b>5</b>	<b>Group theory and error-correcting codes</b>	206
5.1	Preliminaries	206
5.2	Cosets and Lagrange's Theorem	215
5.3	Groups of small order	221
5.4	Error-detecting and error-correcting codes	232
	Answers	257
	References and further reading	275
	Biography	278
	Name index	283
	Subject index	285