

# CONTENTS

<i>Foreword by Andrew Wiles</i>	v
<i>Preface to the sixth edition</i>	vii
<i>Preface to the fifth edition</i>	viii
<i>Preface to the first edition</i>	ix
<i>Remarks on notation</i>	xi
I. THE SERIES OF PRIMES (1)	1
1.1. Divisibility of integers	1
1.2. Prime numbers	2
1.3. Statement of the fundamental theorem of arithmetic	3
1.4. The sequence of primes	4
1.5. Some questions concerning primes	6
1.6. Some notations	7
1.7. The logarithmic function	9
1.8. Statement of the prime number theorem	10
II. THE SERIES OF PRIMES (2)	14
2.1. First proof of Euclid's second theorem	14
2.2. Further deductions from Euclid's argument	14
2.3. Primes in certain arithmetical progressions	15
2.4. Second proof of Euclid's theorem	17
2.5. Fermat's and Mersenne's numbers	18
2.6. Third proof of Euclid's theorem	20
2.7. Further results on formulae for primes	21
2.8. Unsolved problems concerning primes	23
2.9. Moduli of integers	23
2.10. Proof of the fundamental theorem of arithmetic	25
2.11. Another proof of the fundamental theorem	26
III. FAREY SERIES AND A THEOREM OF MINKOWSKI	28
3.1. The definition and simplest properties of a Farey series	28
3.2. The equivalence of the two characteristic properties	29
3.3. First proof of Theorems 28 and 29	30
3.4. Second proof of the theorems	31
3.5. The integral lattice	32
3.6. Some simple properties of the fundamental lattice	33
3.7. Third proof of Theorems 28 and 29	35
3.8. The Farey dissection of the continuum	36
3.9. A theorem of Minkowski	37
3.10. Proof of Minkowski's theorem	39
3.11. Developments of Theorem 37	40

IV.	IRRATIONAL NUMBERS	45
4.1.	Some generalities	45
4.2.	Numbers known to be irrational	46
4.3.	The theorem of Pythagoras and its generalizations	47
4.4.	The use of the fundamental theorem in the proofs of Theorems 43–45	49
4.5.	A historical digression	50
4.6.	Geometrical proof of the irrationality of $\sqrt{5}$	52
4.7.	Some more irrational numbers	53
V.	CONGRUENCES AND RESIDUES	57
5.1.	Highest common divisor and least common multiple	57
5.2.	Congruences and classes of residues	58
5.3.	Elementary properties of congruences	60
5.4.	Linear congruences	60
5.5.	Euler's function $\phi(m)$	63
5.6.	Applications of Theorems 59 and 61 to trigonometrical sums	65
5.7.	A general principle	70
5.8.	Construction of the regular polygon of 17 sides	71
VI.	FERMAT'S THEOREM AND ITS CONSEQUENCES	78
6.1.	Fermat's theorem	78
6.2.	Some properties of binomial coefficients	79
6.3.	A second proof of Theorem 72	81
6.4.	Proof of Theorem 22	82
6.5.	Quadratic residues	83
6.6.	Special cases of Theorem 79: Wilson's theorem	85
6.7.	Elementary properties of quadratic residues and non-residues	87
6.8.	The order of $a \pmod{m}$	88
6.9.	The converse of Fermat's theorem	89
6.10.	Divisibility of $2^{p-1} - 1$ by $p^2$	91
6.11.	Gauss's lemma and the quadratic character of 2	92
6.12.	The law of reciprocity	95
6.13.	Proof of the law of reciprocity	97
6.14.	Tests for primality	98
6.15.	Factors of Mersenne numbers; a theorem of Euler	100
VII.	GENERAL PROPERTIES OF CONGRUENCES	103
7.1.	Roots of congruences	103
7.2.	Integral polynomials and identical congruences	103
7.3.	Divisibility of polynomials $\pmod{m}$	105
7.4.	Roots of congruences to a prime modulus	106
7.5.	Some applications of the general theorems	108

7.6.	Lagrange's proof of Fermat's and Wilson's theorems	110
7.7.	The residue of $\{\frac{1}{2}(p-1)\}!$	111
7.8.	A theorem of Wolstenholme	112
7.9.	The theorem of von Staudt	115
7.10.	Proof of von Staudt's theorem	116
VIII.	CONGRUENCES TO COMPOSITE MODULI	120
8.1.	Linear congruences	120
8.2.	Congruences of higher degree	122
8.3.	Congruences to a prime-power modulus	123
8.4.	Examples	125
8.5.	Bauer's identical congruence	126
8.6.	Bauer's congruence: the case $p=2$	129
8.7.	A theorem of Leudesdorf	130
8.8.	Further consequences of Bauer's theorem	132
8.9.	The residues of $2^{p-1}$ and $(p-1)!$ to modulus $p^2$	135
IX.	THE REPRESENTATION OF NUMBERS BY DECIMALS	138
9.1.	The decimal associated with a given number	138
9.2.	Terminating and recurring decimals	141
9.3.	Representation of numbers in other scales	144
9.4.	Irrationals defined by decimals	145
9.5.	Tests for divisibility	146
9.6.	Decimals with the maximum period	147
9.7.	Bachet's problem of the weights	149
9.8.	The game of Nim	151
9.9.	Integers with missing digits	154
9.10.	Sets of measure zero	155
9.11.	Decimals with missing digits	157
9.12.	Normal numbers	158
9.13.	Proof that almost all numbers are normal	160
X.	CONTINUED FRACTIONS	165
10.1.	Finite continued fractions	165
10.2.	Convergents to a continued fraction	166
10.3.	Continued fractions with positive quotients	168
10.4.	Simple continued fractions	169
10.5.	The representation of an irreducible rational fraction by a simple continued fraction	170
10.6.	The continued fraction algorithm and Euclid's algorithm	172
10.7.	The difference between the fraction and its convergents	175
10.8.	Infinite simple continued fractions	177

10.9.	The representation of an irrational number by an infinite continued fraction	178
10.10.	A lemma	180
10.11.	Equivalent numbers	181
10.12.	Periodic continued fractions	184
10.13.	Some special quadratic surds	187
10.14.	The series of Fibonacci and Lucas	190
10.15.	Approximation by convergents	194
XI.	APPROXIMATION OF IRRATIONALS BY RATIONALS	198
11.1.	Statement of the problem	198
11.2.	Generalities concerning the problem	199
11.3.	An argument of Dirichlet	201
11.4.	Orders of approximation	202
11.5.	Algebraic and transcendental numbers	203
11.6.	The existence of transcendental numbers	205
11.7.	Liouville's theorem and the construction of transcendental numbers	206
11.8.	The measure of the closest approximations to an arbitrary irrational	208
11.9.	Another theorem concerning the convergents to a continued fraction	210
11.10.	Continued fractions with bounded quotients	212
11.11.	Further theorems concerning approximation	216
11.12.	Simultaneous approximation	217
11.13.	The transcendence of $e$	218
11.14.	The transcendence of $\pi$	223
XII.	THE FUNDAMENTAL THEOREM OF ARITHMETIC IN $k(1)$ , $k(i)$ , AND $k(\rho)$	229
12.1.	Algebraic numbers and integers	229
12.2.	The rational integers, the Gaussian integers, and the integers of $k(\rho)$	230
12.3.	Euclid's algorithm	231
12.4.	Application of Euclid's algorithm to the fundamental theorem in $k(1)$	232
12.5.	Historical remarks on Euclid's algorithm and the fundamental theorem	234
12.6.	Properties of the Gaussian integers	235
12.7.	Primes in $k(i)$	236
12.8.	The fundamental theorem of arithmetic in $k(i)$	238
12.9.	The integers of $k(\rho)$	241
XIII.	SOME DIOPHANTINE EQUATIONS	245
13.1.	Fermat's last theorem	245
13.2.	The equation $x^2 + y^2 = z^2$	245
13.3.	The equation $x^4 + y^4 = z^4$	247
13.4.	The equation $x^3 + y^3 = z^3$	248

13.5.	The equation $x^3 + y^3 = 3z^3$	253
13.6.	The expression of a rational as a sum of rational cubes	254
13.7.	The equation $x^3 + y^3 + z^3 = t^3$	257
XIV.	QUADRATIC FIELDS (1)	264
14.1.	Algebraic fields	264
14.2.	Algebraic numbers and integers; primitive polynomials	265
14.3.	The general quadratic field $k(\sqrt{m})$	267
14.4.	Unities and primes	268
14.5.	The unities of $k(\sqrt{2})$	270
14.6.	Fields in which the fundamental theorem is false	273
14.7.	Complex Euclidean fields	274
14.8.	Real Euclidean fields	276
14.9.	Real Euclidean fields ( <i>continued</i> )	279
XV.	QUADRATIC FIELDS (2)	283
15.1.	The primes of $k(i)$	283
15.2.	Fermat's theorem in $k(i)$	285
15.3.	The primes of $k(\rho)$	286
15.4.	The primes of $k(\sqrt{2})$ and $k(\sqrt{5})$	287
15.5.	Lucas's test for the primality of the Mersenne number $M_{4n+3}$	290
15.6.	General remarks on the arithmetic of quadratic fields	293
15.7.	Ideals in a quadratic field	295
15.8.	Other fields	299
XVI.	THE ARITHMETICAL FUNCTIONS $\phi(n)$ , $\mu(n)$ , $d(n)$ , $\sigma(n)$ , $r(n)$	302
16.1.	The function $\phi(n)$	302
16.2.	A further proof of Theorem 63	303
16.3.	The Möbius function	304
16.4.	The Möbius inversion formula	305
16.5.	Further inversion formulae	307
16.6.	Evaluation of Ramanujan's sum	308
16.7.	The functions $d(n)$ and $\sigma_k(n)$	310
16.8.	Perfect numbers	311
16.9.	The function $r(n)$	313
16.10.	Proof of the formula for $r(n)$	315
XVII.	GENERATING FUNCTIONS OF ARITHMETICAL FUNCTIONS	318
17.1.	The generation of arithmetical functions by means of Dirichlet series	318
17.2.	The zeta function	320
17.3.	The behaviour of $\zeta(s)$ when $s \rightarrow 1$	321
17.4.	Multiplication of Dirichlet series	323

17.5.	The generating functions of some special arithmetical functions	326
17.6.	The analytical interpretation of the Möbius formula	328
17.7.	The function $\Lambda(n)$	331
17.8.	Further examples of generating functions	334
17.9.	The generating function of $r(n)$	337
17.10.	Generating functions of other types	338
<b>XVIII.</b>	<b>THE ORDER OF MAGNITUDE OF ARITHMETICAL FUNCTIONS</b>	<b>342</b>
18.1.	The order of $d(n)$	342
18.2.	The average order of $d(n)$	347
18.3.	The order of $\sigma(n)$	350
18.4.	The order of $\phi(n)$	352
18.5.	The average order of $\phi(n)$	353
18.6.	The number of squarefree numbers	355
18.7.	The order of $r(n)$	356
<b>XIX.</b>	<b>PARTITIONS</b>	<b>361</b>
19.1.	The general problem of additive arithmetic	361
19.2.	Partitions of numbers	361
19.3.	The generating function of $p(n)$	362
19.4.	Other generating functions	365
19.5.	Two theorems of Euler	366
19.6.	Further algebraical identities	369
19.7.	Another formula for $F(x)$	371
19.8.	A theorem of Jacobi	372
19.9.	Special cases of Jacobi's identity	375
19.10.	Applications of Theorem 353	378
19.11.	Elementary proof of Theorem 358	379
19.12.	Congruence properties of $p(n)$	380
19.13.	The Rogers–Ramanujan identities	383
19.14.	Proof of Theorems 362 and 363	386
19.15.	Ramanujan's continued fraction	389
<b>XX.</b>	<b>THE REPRESENTATION OF A NUMBER BY TWO OR FOUR SQUARES</b>	<b>393</b>
20.1.	Waring's problem: the numbers $g(k)$ and $G(k)$	393
20.2.	Squares	395
20.3.	Second proof of Theorem 366	395
20.4.	Third and fourth proofs of Theorem 366	397
20.5.	The four-square theorem	399
20.6.	Quaternions	401
20.7.	Preliminary theorems about integral quaternions	403

20.8.	The highest common right-hand divisor of two quaternions	405
20.9.	Prime quaternions and the proof of Theorem 370	407
20.10.	The values of $g(2)$ and $G(2)$	409
20.11.	Lemmas for the third proof of Theorem 369	410
20.12.	Third proof of Theorem 369: the number of representations	411
20.13.	Representations by a larger number of squares	415
XXI.	REPRESENTATION BY CUBES AND HIGHER POWERS	419
21.1.	Biquadrates	419
21.2.	Cubes: the existence of $G(3)$ and $g(3)$	420
21.3.	A bound for $g(3)$	422
21.4.	Higher powers	424
21.5.	A lower bound for $g(k)$	425
21.6.	Lower bounds for $G(k)$	426
21.7.	Sums affected with signs: the number $v(k)$	431
21.8.	Upper bounds for $v(k)$	433
21.9.	The problem of Prouhet and Tarry: the number $P(k, j)$	435
21.10.	Evaluation of $P(k, j)$ for particular $k$ and $j$	437
21.11.	Further problems of Diophantine analysis	440
XXII.	THE SERIES OF PRIMES (3)	451
22.1.	The functions $\vartheta(x)$ and $\psi(x)$	451
22.2.	Proof that $\vartheta(x)$ and $\psi(x)$ are of order $x$	453
22.3.	Bertrand's postulate and a 'formula' for primes	455
22.4.	Proof of Theorems 7 and 9	458
22.5.	Two formal transformations	460
22.6.	An important sum	461
22.7.	The sum $\Sigma p^{-1}$ and the product $\Pi(1 - p^{-1})$	464
22.8.	Mertens's theorem	466
22.9.	Proof of Theorems 323 and 328	469
22.10.	The number of prime factors of $n$	471
22.11.	The normal order of $\omega(n)$ and $\Omega(n)$	473
22.12.	A note on round numbers	476
22.13.	The normal order of $d(n)$	477
22.14.	Selberg's theorem	478
22.15.	The functions $R(x)$ and $V(\xi)$	481
22.16.	Completion of the proof of Theorems 434, 6, and 8	486
22.17.	Proof of Theorem 335	489
22.18.	Products of $k$ prime factors	490
22.19.	Primes in an interval	494
22.20.	A conjecture about the distribution of prime pairs $p, p + 2$	495

XXIII. KRONECKER'S THEOREM	501
23.1. Kronecker's theorem in one dimension	501
23.2. Proofs of the one-dimensional theorem	502
23.3. The problem of the reflected ray	505
23.4. Statement of the general theorem	508
23.5. The two forms of the theorem	510
23.6. An illustration	512
23.7. Lettenmeyer's proof of the theorem	512
23.8. Estermann's proof of the theorem	514
23.9. Bohr's proof of the theorem	517
23.10. Uniform distribution	520
XXIV. GEOMETRY OF NUMBERS	523
24.1. Introduction and restatement of the fundamental theorem	523
24.2. Simple applications	524
24.3. Arithmetical proof of Theorem 448	527
24.4. Best possible inequalities	529
24.5. The best possible inequality for $\xi^2 + \eta^2$	530
24.6. The best possible inequality for $ \xi \eta $	532
24.7. A theorem concerning non-homogeneous forms	534
24.8. Arithmetical proof of Theorem 455	536
24.9. Tchebotaref's theorem	537
24.10. A converse of Minkowski's Theorem 446	540
XXV. ELLIPTIC CURVES	549
25.1. The congruent number problem	549
25.2. The addition law on an elliptic curve	550
25.3. Other equations that define elliptic curves	556
25.4. Points of finite order	559
25.5. The group of rational points	564
25.6. The group of points modulo $p$ .	573
25.7. Integer points on elliptic curves	574
25.8. The $L$ -series of an elliptic curve	578
25.9. Points of finite order and modular curves	582
25.10. Elliptic curves and Fermat's last theorem	586
APPENDIX	593
1. Another formula for $p_n$	593
2. A generalization of Theorem 22	593
3. Unsolved problems concerning primes	594



A LIST OF BOOKS	597
INDEX OF SPECIAL SYMBOLS AND WORDS	601
INDEX OF NAMES	605
GENERAL INDEX	611