INDEX

All decimal numbers (2.25 etc.) without the prefix n (for 'note') refer to questions

addition in modular arithmetic 1.11, 2.25
algebraic number 11.40
algorithm
  division 1.19, 1.23, 1.24, 5.53
  Euclidean 1.39
area of parallelogram 8.5, 9.23
automorph of quadratic form
  definite 8.73–8.77
  indefinite 10.78–10.82

Chevalley's theorem 3.87
Chinese remainder theorem 2.18, 3.44
congruence 1.12, 2.4
  of polynomials 3.78–3.81
congruence class 2.3
congruent modulo n 2.4
conjugate
  graph of partition 7.3
  quadratic irrational 10.43
continued fractions
  convergents to 10.18, 10.24
  finite 10.21, 10.22
  periodic 10.37, 10.53
  for quadratic irrationals 10.76, 10.77
  ultimately periodic 10.76, 10.77
convex 9.35, 9.37, 9.69
coprime 1.60, 1.61
cyclic group 1.33, 2.28, 2.32, 3.58, 3.61, 3.62, 8.76(ii), 10.80

definite quadratic form 8.38, 8.77
degree of polynomial 3.77
descent, method of n 5.20, n 5.67, n 6.51, 10.1
determinant
  of 2×2 matrix n 8.5, 8.32–8.34
  of 3×3 matrix 9.50
direct product of groups 3.63–3.66
Dirichlet's theorem ch. 1 hist. note
discriminant 8.37, 10.46
division algorithm 1.19, 1.23, 1.24, 5.55

ellipse 8.25, 9.44
ellipsoid 9.78, 9.86
equivalent quadratic forms
  properly represent the same integers 8.51
  represent the same set of integers 8.25
Eratosthenes' sieve 1.47
Euclidean algorithm 1.39
Euler's ϕ function
  definition 2.39
  multiplicative property 2.50
Euler's generalisation of Fermat's theorem 3.41
Euler's theorem on partitions 7.47

factorisation
  not unique 1.51
  unique 1.58, 5.56, n 6.15
Farey sequence 8.13, 11.11
Fermat's last theorem n 5.63, ch. 5 hist. note
  $n=3$ 5.67
  $n=4$ 5.21
Fermat's method of descent n 5.20, n 5.67, n 6.51, 10.1
Fermat's theorem 3.19, 3.53, 3.76, 3.78, 4.10
Fermat–Euler theorem 3.41
Ferrers' graph of a partition 7.2
fundamental parallelepiped of a lattice 9.48, 9.57
fundamental parallelogram of a lattice 9.5, 9.23, 9.24
fundamental theorem of arithmetic 1.58

Gauss' lemma 4.43
Gaussian integers 6.15, n 6.36
generating functions for partitions 7.16–7.35
generators
  of parallelogram lattice 9.2–9.5
  of subgroups of $(\mathbf{Z}, +)$ 1.29–1.37
  of subgroups of $\mathbf{Z}^2$ 9.14, 9.15
  of subgroups of $\mathbf{Z}^3$ 9.53–9.55
  of $(\mathbf{Z}_n, +)$ 2.32
graph, Ferrers' 7.2
greatest common divisor (gcd) 1.34, 1.59, 5.54, 8.18
group
  additive 1.22, 2.23
  cyclic 1.33, 3.61, 10.80
  multiplicative 3.17, 3.21, 3.39, 3.40
  non-cyclic 3.65, 8.17, 8.74, 8.75, 9.5, 9.53, 9.55

Hurwitz' theorem 11.31

index of subgroup 8.20, 9.23, 9.66
induction, mathematical n 1.57, 2.18, 2.52, n 5.20
infinite descent, see descent, method of
infinity of primes 1.64
  congruent to 1 (mod 3) 4.28
  congruent to 1 (mod 4) 4.25
  congruent to 2 (mod 3) 1.66
  congruent to 3 (mod 4) 1.65
integral part of x, $[x]$ 4.44
irrational numbers 10.1–10.7
  algebraic of degree $\geqq 2$ 11.40
  quadratic 10.52
  transcendental 11.43
isometric lattice 5.35

Lagrange's theorem on
  continued fractions 10.76
  polynomials 3.57, 3.79, 3.80, 4.10
  quadratic irrationals 10.77
  subgroups 3.18, 3.42, 6.9
  sums of four squares 6.40
lattice points
  in space 9.47–9.86
  in the plane 4.48, 8.1–8.4, 8.9 9.1–9.46
  isometric 5.35
law of quadratic reciprocity 4.62
least common multiple 1.59
Legendre
  symbol 4.15
  theorem 9.86
line segment 9.33, 9.35
Liouville's theorem 11.42

mean value theorem 11.41
mediant of two terms in Farey sequence 11.17
Mersenne prime 1.67
Minkowski's theorem
  in three dimensions 9.71
  in two dimensions 9.39
minus one as a quadratic residue 4.16, 4.19, 4.29, 6.18
$\mathbf{M}_n$ 3.36
modulus 1.11, 2.4
$\mathbf{M}_p$ 3.21
multiplication in modular arithmetic 1.14, 3.4
multiplicative property
  of $\sum_{d|n} \phi(d)$ n 2.63
  of $\phi(n)$ 2.50

negative definite quadratic form 8.38
non-residues, quadratic 4.8, 4.16
norm
  in $\mathbf{Z}[i]$ n 6.15
  in $\mathbf{Z}[\omega]$ 5.41
numerically least residues 4.30

open region 9.29, 9.67
order of element in a group 3.58–3.62

Pell's equation 10.61–10.70
pigeon hole principle ch.11 hist. note
positive definite quadratic from 8.38
prime numbers 1.43, 1.51
  congruent to 1 (mod 4), as the sum of two squares: representable 6.33; uniquely representable 6.36
  congruent to 3 (mod 4) not the sum of two squares 6.4
  factorisation into: in $\mathbf{N}$ 1.58; in $\mathbf{Q}$ 10.5; in $\mathbf{Z}$ n 5.56, n 10.5; in $\mathbf{Z}[\omega]$ 5.51, 5.56
primitive roots 3.62, 3.68, 3.70–3.74
proper representation by quadratic form 8.48
Pythagorean triangles n 5.5
Pythagorean triples 5.5–5.18

$\mathbf{Q}(\sqrt{d})$ 10.44
quadratic irrational 10.52
quadratic
  non-residues 4.8
  residues 4.3
quadratic forms
  equivalent 8.25
  reduced 8.57
quadratic reciprocity, law of 4.62
quaternions 6.38

rational approximation ch. 11
reciprocity, quadratic 4.62
reduced quadratic form
  definition 8.57
  every positive definite form equivalent to 8.66
reduced set of residues 3.36
representation by quadratic form, proper 8.48–8.51
residue class 2.3
residues
  numerically least 4.30–4.36
  quadratic 4.3
RSA codes 3.90–3.95

set of residues
  complete 2.20
  reduced 3.36
simple continued fraction *see* continued fraction
sum of squares
  four 6.52
  three 6.54, 6.57–6.61
  two 6.34
  $x^2 + 2y^2$ 6.60, 8.69, 8.70, 9.45, 9.46
symmetric matrix 8.32, 8.34
symmetry about a point 4.56, 4.60, 9.36, 9.69

transcendental numbers 11.43
triangular numbers 6.55–6.61

unimodular
  group 8.17, 8.19, 8.20
  matrix 8.15
  transformation 8.15, 9.52
unique factorisation 1.24, 1.58
  absence of 1.51
  in $\mathbf{Z}[i]$ n 6.15, n 6.36
  in $\mathbf{Z}[\omega]$ 5.55
units
  in $\mathbf{Z}$ n 5.43
  in $\mathbf{Z}_n$ 3.36
  in $\mathbf{Z}[i]$ 6.15
  in $\mathbf{Z}[\omega]$ 5.43

volume
  of ellipsoid 9.78
  of parallelepiped 9.50

Wilson's theorem 3.25, 3.53, 4.29

$\mathbf{Z}[i]$ n 6.15
$\mathbf{Z}_n$ 1.11, n 2.25
$\mathbf{Z}[\omega]$ 5.37