

Cambridge University Press

978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition

H. Davenport

Index

[More information](#)

INDEX

- AKS primality testing, 200–202, 208
 Algebraic Congruences, 41
 Automorphs, 132
- Baker's work on Diophantine equations, 161–164
 Binomial congruences, 49
 Birch–Swinnerton-Dyer algorithm, 151, 163
 Birthday paradox, 174
 Bremner–Cassels elliptic curve, 150, 163
- Carmichael
 conjecture, 212
 function, 169
 numbers, 169, 204–205
- Cattle problem of Archimedes, 94, 102
- Chen's theorem (prime+ P_2), 30
 Chevalley's theorem on congruences, 45, 112
 Chinese Remainder Theorem, 38
 Choi's covering congruences, 47, 48
 Class-number, 128, 133, 134
 Kronecker, 152
 Continued fractions, 68
- complete quotients, 69
 convergents, 74
 Euler's rule, 72
 for \sqrt{N} , 91, 97, 98
 for e , 93, 101
 infinite, 78
 partial quotients, 69
 periodic, 85
- Coppersmith, 200, 208
 Covering set of congruences, 46
 Cryptography, 194–200
 Diffie–Hellman, 196–199
 RSA, 199–200
- Definite forms, 121
 Diffie–Hellman cryptography, 196
 Diophantine approximations, 82, 164
 Diophantine equations, 21
 cubic, 145–154, 157
 higher, 156
 linear, 21, 34, 77
 quadratic, 94, 138, 140, 162
 quartic, 155
- Dirichlet's class number formula, 134, 136
 theorem on primes, 26, 114, 134

Cambridge University Press

978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition

H. Davenport

Index

[More information](#)

238

Index

- Discriminant of elliptic curve, 146
 - of quadratic form, 120
- Divisibility, 5
- Divisors, number of, 13
 - sum of, 14
- Drain's algorithm, 23
- Elliptic curves, 147–154
 - factoring via, 185, 206
 - use in cryptography, 198
- Elliptic equations, 145–154
- Equivalence of elliptic curves, 152
 - of quadratic forms, 117
- Euclid's algorithm, 16
 - theorem on primes, 9
- Euler's criterion, 57
 - function, 37
 - identity, 112
 - rule for continued fractions, 72
- Factorizing a number, 22, 29, 165, 179–194
- Faltings proof of Mordell's conjecture, 156, 163
- Fermat's Last Theorem, 154–156, 163
 - congruence (Little Theorem), 36, 168
 - congruence (polynomial version), 201
 - numbers, 226
 - process for factorization, 22, 199
- Finite fields, 43, 47
- Four cube problem, 159, 164
- Frey curve, 156, 163
- Fundamental theorem of arithmetic, 9, 18
- Gauss's construction (two squares), 109
 - lemma, 58
- Genus of quadratic forms, 129
- Goldbach's problem, 28, 30
- Hasse principle for quadratic forms, 145
 - not for elliptic curves, 151
- Heegner class–number proof, 135, 136
- Heilbronn's theorem, 135, 136
- Hensel's lemma, 223
- Hurwitz's theorem, 82
- Indefinite forms, 122
- Indices (discrete logarithms), 53, 197
- Induction, 6
- Iwaniec's theorem on $n^2 + 1$, 30
- Jacobsthal's construction (two squares), 110
- Karatsuba's algorithm, 167
- Kummer's work on Fermat's Last Theorem, 154
- Lagrange's theorem on congruences, 43
 - continued fractions, 92
 - four squares, 111
- Landau's notation, 202
- Large prime variant, 183, 187, 191, 193
- Legendre's construction (two squares), 108
 - symbol, 56
 - theorem on $ax^2 + by^2 = cz^2$, 144
- Lenstra's elliptic curve method, 185–187, 206
- Linear congruences, 33
 - equations, 21, 34, 77
- Lutz–Nagell theorem, 150, 163
- Mazur's theorem, 150, 163
- Mestre elliptic curve, 150, 163
- Modular elliptic curves, 153, 156
- Mordell
 - conjecture, 156, 163
 - curves, equations, 162
- Mordell–Weil theorem, 150, 153, 163
- Multiplicative functions, 37, 42

Cambridge University Press

978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition

H. Davenport

Index

[More information](#)*Index*

239

- Number field sieve, 193
- Number of representations by a quadratic form, 131
 - by four squares, 115
 - by two squares, 115, 136
- Order to a prime modulus, 35, 50
 - of a torsion point, 150
- Pell's equation, 94
- Perfect numbers, 14, 29
- Periodic continued fractions, 85
- Pollard's ρ method, 179–181
 - $p - 1$ method, 181–184
- Pólya inequality, 67
- Primality, certificates of, 172, 187–188
- Prime Number Theorem, 27, 30
- Primes, 8
 - distribution of, 27
 - in arithmetical progressions, 26, 30, 115, 134
 - infinity of, 9
 - testing for, 168–173, 200–202
- Primitive roots, 50
 - number of, 52
- Principal form, 121
- Proper representation, 122
- Proth's theorem, 173
- Quadratic reciprocity, 60, 61
- Quadratic residues, 55
 - distribution of, 63
- Quadratic sieve, 192–193, 203, 207
- Rabin's
 - algorithm, 170–171
 - theorem, 171
- Random numbers, 173–179
- Rank of an elliptic curve, 151
- Reduced quadratic forms, 128, 130
 - quadratic irrationals, 88
- Reduction of quadratic forms, 126
- Relative primality, 15, 17
- Representation by a quadratic form, 122, 132
 - by four squares, 111, 115
 - by three squares, 114, 115
 - by two squares, 103, 115
- RSA Cryptography, 199–200
- Runge's theorem, 164
- Serret's construction (two squares), 109
- Smooth numbers, 181, 206
 - (B_1, B_2) -smooth, 183, 206
- Stark's theorem on the class-number, 135, 136
- Tables, 97, 130
- Taniyama–Shimura–Weil conjecture, 154, 156
- Thue–Siegel–Roth theorem, 160, 164
- Torsion on elliptic curves, 149
- triangles
 - right-angled, 107
- Unimodular substitution, 118
- Uniqueness of prime factorization, 9, 18
- Vinogradov (sums of three primes), 28, 30
- Weierstrass equation, 145
- Wiles–Taylor proof of Fermat's Last Theorem, 156, 163
- Wilson's Theorem, 40, 57