

---

# Index

- abc*-conjecture, 117, 120, 216, 218
- Binary quadratic forms, 176, 180, 181, 227, 228, 230–236, 240, 242, 243
- Binomial coefficients, 4, 36, 61, 98, 129
- Carmichael numbers, 133, 138, 202
- Catalan equation, 117, 219
- Chinese Remainder Theorem, 54, 59, 72, 161, 190
- Class group and composition, 240–245, 247, 248
- Class number, 232–235
- Computation and running times, 143, 144, 190, 194, 196, 202
- Congruent number problem, 115
- Constructibility and pre-Galois theory, 65
- Continued fractions, 17, 25
- Convolutions, 76
- Cryptography, 190, 192, 194
- Cyclotomic polynomials, 136
- Descent, 113, 117, 212
- Diophantine problems, 109, 112, 114, 137, 161, 175, 208, 212, 215, 216, 228, 236
- Divisibility tests, 34, 134
- Divisors (incl. gcds), 12, 47, 69
- Dynamics, 26, 222
- Elliptic curves, 114
- Euclidean algorithm, 11, 18, 19, 23, 25, 52
- Euler's  $\phi$ -function, 68
- Euler's criterion, 150, 157
- Factoring methods, 197
- Fermat numbers, 8, 58, 65, 82, 128, 137, 155, 165, 196, 203
- Fermat's Last Theorem, 58, 112, 115, 119, 137
- Fermat's Little Theorem, 126, 142, 149
- Fermat-Catalan conjecture, 117, 122, 219
- Fibonacci numbers, 1, 20, 25, 37, 58
- Fundamental discriminants, 228, 229, 232, 234, 235
- Fundamental Theorem of Arithmetic, 43, 44
- Groups, 39, 42, 210, 238
- Heuristics, xxii
- Ideals, 15, 21, 25, 244
- Irrational numbers, 49, 59, 117, 206, 220
- Jacobi symbol, 159, 163
- Lattice points, 169, 174, 183–185, 187, 206, 222, 239
- Legendre symbol, 148
- Lifting solutions mod  $p^k$ , 162
- Linear algebra, 13, 15, 27, 52, 58, 120, 198, 227, 229
- Local-global principle, 54, 59, 178, 179, 181, 184, 186, 187, 231
- Lucas sequence, 2

- Matrices and matrix groups, 23, 25, 27,  
106, 229, 231, 238, 246
- Mersenne numbers, 8, 22, 37, 58, 70, 83,  
128, 155
- Möbius function, 75, 103, 137
- Orders (of elements), 41, 124, 128, 130,  
134, 140
- Pascal's triangle, 5, 61
- Pell's equation, 208, 210
- Pell's equation; negative, 212
- Perfect numbers, 69, 71
- Polynomial properties, 34, 49, 58, 94,  
117, 119, 120, 128, 151, 163, 197
- Power residues, 123, 150
- Primality testing, 83, 195, 196, 199
- Prime  $k$ -tuplets conjecture, 104
- Primes in arithmetic progressions, 85,  
89, 95, 105, 136, 164
- Primes: infinitely many, 81, 82, 86
- Primes: number of, 83, 86, 89, 97
- Primitive roots, 130, 131, 134, 165, 195
- Pseudoprimes, 133, 138, 199–203
- Pythagorean triangle, 109, 115, 117, 183
- Quadratic fields, 244, 245
- Quadratic forms, 179
- Quadratic reciprocity (Law of), 152,  
153, 155, 157, 161, 165, 167, 177
- Quadratic residues / non-residues, 148,  
151
- Quadratic residues and non-residues;  
least, 149, 162
- Residues (mod  $n$ ), 29, 39, 51, 124, 126,  
147, 157, 167, 207
- Rings and fields, 41
- Second-order linear recurrence  
sequences, 2, 7, 22, 37, 58
- Square roots (mod  $n$ ), 56, 151,  
161–163, 189, 200
- Sums of powers of integers, 3
- Sums of two squares, 173, 175, 183, 207,  
240
- Tiling, 19
- Transcendental numbers, 213, 214, 218
- Waring's problem, 118
- Wilson's Theorem, 129