Bibliography


[58] E. Brown, Sets in which $xy + k$ is always a square, Math. Comp. 45 (1985), 613–620.


[200] Great Internet Mersenne Prime Search (GIMPS) 
https://www.mersenne.org/


[244] M. Kiseljak, Contributions to the theory of perfect numbers, Kr. zemaljska tiskara, Zagreb, 1911 (in Croatian).


REFERENCES


### Notation Index

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{N}$</td>
<td>set of positive integers</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>set of integers</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>set of rational numbers</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>set of real numbers</td>
</tr>
<tr>
<td>$\mathbb{C}$</td>
<td>set of complex numbers</td>
</tr>
<tr>
<td>□</td>
<td>symbol for the end of a proof</td>
</tr>
<tr>
<td>♦</td>
<td>symbol for the end of a solution</td>
</tr>
<tr>
<td>$n!$</td>
<td>factorial</td>
</tr>
<tr>
<td>$\binom{n}{k}$</td>
<td>binomial coefficient</td>
</tr>
<tr>
<td>$L_n$</td>
<td>$n$-th Lucas number</td>
</tr>
<tr>
<td>$F_n$</td>
<td>$n$-th Fibonacci number</td>
</tr>
<tr>
<td>$a \mid b$</td>
<td>$a$ divides $b$</td>
</tr>
<tr>
<td>$a \notmid b$</td>
<td>$a$ does not divide $b$</td>
</tr>
<tr>
<td>$a^k \parallel b$</td>
<td>$a^k$ is the largest power of $a$ dividing $b$</td>
</tr>
<tr>
<td>$\gcd(a,b)$</td>
<td>greatest common divisor of $a$ and $b$</td>
</tr>
<tr>
<td>$\log_b(x)$</td>
<td>logarithm to the base $b$</td>
</tr>
<tr>
<td>$\ln(x)$</td>
<td>natural logarithm</td>
</tr>
<tr>
<td>$\text{lcm}(a,b)$</td>
<td>least common multiple of $a$ and $b$</td>
</tr>
<tr>
<td>$\min(a,b)$</td>
<td>minimum of $a$ and $b$</td>
</tr>
<tr>
<td>$\max(a,b)$</td>
<td>maximum of $a$ and $b$</td>
</tr>
<tr>
<td>$f_n$</td>
<td>Fermat number $2^{2^n} + 1$</td>
</tr>
<tr>
<td>$M_p$</td>
<td>Mersenne number $2^p - 1$</td>
</tr>
<tr>
<td>$a \equiv b \pmod{m}$</td>
<td>$a$ is congruent $b$ modulo $m$</td>
</tr>
<tr>
<td>$a \not\equiv b \pmod{m}$</td>
<td>$a$ is not congruent $b$ modulo $m$</td>
</tr>
<tr>
<td>$\varphi(m)$</td>
<td>Euler function</td>
</tr>
<tr>
<td>$\text{ind}_g a$</td>
<td>index of $a$ with respect to a primitive root $g$</td>
</tr>
<tr>
<td>$\text{pseudoprime}(b)$</td>
<td>pseudoprime to the base $b$</td>
</tr>
<tr>
<td>$\text{strong pseudoprime}(b)$</td>
<td>strong pseudoprime to the base $b$</td>
</tr>
<tr>
<td>$(\frac{a}{b})$</td>
<td>Legendre symbol</td>
</tr>
</tbody>
</table>
\(|A|\) \quad \text{number of elements of a finite set } A

\left(\frac{a}{Q}\right) \quad \text{Jacobi symbol}

\text{lpsp}(a, b) \quad \text{Lucas pseudoprime}

A^\top \quad \text{transpose of a matrix } A

h(d) \quad \text{class number of the discriminant } d

t_m \quad m\text{-th triangular number}

\lfloor x \rfloor \quad \text{the largest integer } \leq x

\lceil x \rceil \quad \text{the smallest integer } \geq x

\{x\} \quad \text{fractional part of } x

\mu(n) \quad \text{Möbius function}

\sigma(n) \quad \text{sum of divisors of } n

\tau(n) \quad \text{number of divisors of } n

f(x) = O(g(x)) \quad |f(x)| \leq Cg(x) \text{ for a constant } C

f(x) = o(g(x)) \quad \lim_{x \to \infty} \frac{f(x)}{g(x)} = 0

f(x) \ll g(x) \quad |f(x)| \leq Cg(x) \text{ for a constant } C

f(x) \gg g(x) \quad \text{same as } f(x) \ll g(x)

\gamma \quad \text{Euler-Mascheroni constant}

f \ast g \quad \text{Dirichlet product}

\omega(n) \quad \text{number of prime divisors of } n

\pi(x) \quad \text{number of primes which are } \leq x

\text{li}(x) \quad \text{logarithmic integral function}

\Lambda(n) \quad \text{von Mangoldt function}

\psi(x) \quad \text{Chebyshev function } \psi

\psi(x) \quad \text{Chebyshev function } \psi

\zeta(s) \quad \text{Riemann zeta function}

\text{Re}(s) \quad \text{real part of a complex number } s

\text{Im}(s) \quad \text{imaginary part of a complex number } s

\Gamma(s) \quad \text{gamma-function}

B_n \quad n\text{-th Bernoulli number}

\chi(n) \quad \text{Dirichlet character}

L(s, \chi) \quad \text{Dirichlet } L\text{-function}

\|\alpha\| \quad \text{distance from } \alpha \text{ to the nearest integer}

\mathcal{F}_n \quad \text{Farey sequence of order } n

[a_0, a_1, \ldots, a_n] \quad \text{finite continued fraction}

[a_0, a_1, \ldots] \quad \text{infinite continued fraction}

\frac{p}{q} \quad i\text{-th convergent of a continued fraction}

\frac{p_i}{q_{n,i}} \quad \text{secondary convergent of a continued fraction}

M(\alpha) \quad \text{Markov constant}

\|x\| \quad \max(|x_1|, \ldots, |x_n|), \text{ for } x = (x_1, \ldots, x_n)
nearest integer to a real number $x$

$g(a_1,\ldots,a_n)$ Frobenius number

$p$-adic valuation

$p$-adic norm

Hilbert symbol

polynomial ring on $R$

content of a polynomial $f$

resultant of polynomials $f$ and $g$

discriminant of a polynomial $f$

Dickson polynomial

Chebyshev polynomial of the first kind

Chebyshev polynomial of the second kind

Fibonacci polynomial

elementary symmetric polynomials

algebraic number field

norm of an algebraic number

trace of an algebraic number

norm of $\alpha$ with respect to $K$

trace of $\alpha$ with respect to $K$

set of all algebraic integers in $K$

principal ideal generated by $\alpha$

norm of an ideal $a$

class number of a number field $K$

Dedekind zeta function

hypergeometric function

height of a polynomial $P$

Mahler measure of a polynomial $P$

logarithmic Weil height of a polynomial $P$

separation exponent of a polynomial $P$

$k$-th Catalan number

algebraic closure of a field $K$

Weierstrass $\wp$-function

torsion group of an elliptic curve $E$

rank of an elliptic curve $E$

canonical height

Néron-Tate pairing

finite field with $q$ elements

radical of a polynomial $f$

radical of a positive integer $m$
## Subject Index

2-Selmer rank, 512

abc conjecture, 576

abc theorem for polynomials, 574

AKS algorithm, 548

algebraic integer, 368
  irreducible, 372, 393
  prime, 372, 393

algebraic number, 366
  degree, 368

algebraic number field, 378

analytic rank, 516

Artin’s conjecture, 65

Artin’s constant, 65

associated algebraic numbers, 392

badly approximable numbers, 216

Baker, Alan, 408

Baker-Davenport reduction, 445

Baker-Wüstholz theorem, 444

Bernoulli numbers, 174

Bernoulli, Jacob, 174

Bertrand’s postulate, 163

binary quadratic form, 111
  positive definite, 112
  primitive, 116
  principal, 111
  reduced, 114

Binet’s formula, 17

binomial coefficient, 8

binomial theorem, 8

Birch and Swinnerton-Dyer (BSD) conjecture, 515

Blichfeldt’s theorem, 235

BSGS method, 532

canonical decomposition, 32

canonical height, 500

Carmichael numbers, 75

Carmichael’s theorem, 104

Cassini’s identity, 15

Catalan numbers, 426

Chebyshev functions, 164

Chebyshev polynomials
  of the first kind, 352
  of the second kind, 356

Chebyshev, Pafnuti Lvovich, 159

Chevalley-Warning theorem, 321

Chinese remainder theorem (CRT), 51

class number
  of a number field, 396
  of binary quadratic forms, 115

compact set, 235

complete residue system, 44

completely multiplicative function, 140

composite numbers, 31

conductor, 485

congruence, 42

congruence method, 458

congruent number, 556

continued fraction
  complete quotient, 205, 208
  convergent, 205, 208
  partial quotient, 205, 208
  secondary convergent, 214
INDEX

continued fractions, 202
  finite, 205
  infinite, 208
  periodic, 222
  period length, 222
  purely periodic, 222
convex set, 235
Coppersmith’s theorem, 267
coprime integers, 24
cryptography, 250
cryptosystem, 251
cyclotomic field, 399
discriminant
  of a polynomial, 346
  of a quadratic form, 111
  of an algebraic number field, 382
  of an elliptic curve, 467
divisor, 22, 336
Doud’s algorithm, 491
ECDLP, 540
Edwards curves, 479
Eisenstein’s irreducibility criterion, 349
elementary symmetric polynomials, 358
ElGamal cryptosystem, 536
elliptic curve, 466
  anomalous, 531, 542
  induced by a Diophantine triple, 578
  supersingular, 531, 542
equivalent decompositions, 351
equivalent numbers, 217
equivalent quadratic forms, 112, 125
Erdős, Paul, 162
Erdős-Strauss conjecture, 140
Euclid, 26
Euclid’s algorithm, 25
  extended, 28
Euclidean field, 373
Euler function, 54
Euler’s criterion, 84
Euler’s product formula, 176
Euler’s theorem, 54
Euler, Leonhard, 54
Euler-Maclaurin formula, 168
Euler-Mascheroni constant, 150
factor basis, 538
factorial, 8
Farey sequence, 194
Faulhaber’s formula, 174
Fermat numbers, 37
Fermat’s Last Theorem for polynomials, 575
Fermat's little theorem, 55
Fermat, Pierre de, 37
Fibonacci numbers, 11
Fibonacci polynomials, 356
Fibonacci, Leonardo Pisano, 10
field, 334
    algebraically closed, 344
formal derivative, 342
fraction field, 348
Frobenius automorphism, 521
Frobenius endomorphism, 533
Frobenius number, 273
function
    analytic, 172
    ceiling, 136
    differentiable, 172
    fractional part, 136
    greatest integer, 136
    meromorphic, 173
Fundamental theorem of arithmetic, 32
Fundamental theorem of symmetric polynomials, 359
fundamental unit, 371
Galois extension, 378
Galois, Évariste, 378
gamma-function, 173
Gauss hypergeometric function, 409
Gauss sum, 525
Gauss' lemma, 89
Gauss' lemma for polynomials, 339
Gauss' quadratic reciprocity law, 91
Gauss, Carl Friedrich, 42
Gaussian rationals, 369
GCD-domain, 336
genus of a curve, 472
Goldbach's conjecture, 39
good approximation, 215
greatest common divisor, 23, 336
group homomorphism, 178
Hardy-Ramanujan number, 586
Hasse's theorem, 527
Hasse-Minkowski principle, 325
Hasse-Minkowski theorem, 325
height
    of a polynomial, 422
    of an algebraic number, 417
height determinant, 505
Hensel's lemma, 61
Hilbert symbol, 326
    product formula, 326
Holzer's theorem, 313
Hurwitz's theorem, 198
Håstad's attack, 263
ideal, 385
    maximal, 387
    norm, 390
    prime, 387
    principal, 385
totally ramified, 392
unramified, 392
ideal class group, 395
index, 66
index calculus method, 538
infinite product
    absolutely convergent, 175
    convergent, 175
integral basis, 382
integral domain, 334
    characteristic, 343
irreducible element, 336
isogeny, 507

j-invariant, 481
Jacobi symbol, 96
Jacobi's formula, 123
Jacobian projective coordinates, 478
Koblitz curves, 534
Korselt's criterion, 75
Kronecker symbol, 97
Kronecker's algorithm, 348
Kummer, Ernst Eduard, 384
López-Dahab coordinates, 529
Lagrange's four-square theorem, 121
Lagrange’s theorem
  on the best approximations, 214
  on the number of congruence solutions, 59
Lagrange, Joseph-Louis, 121
lattice, 240
  basis, 240
least common multiple, 33
Legendre symbol, 84
Legendre’s theorem
  on continued fractions, 210
  on ternary equations, 309
Legendre, Adrien-Marie, 84
Lenstra’s algorithm for factorization (ECM), 549
Liouville numbers, 403
Liouville’s theorem, 402
Liouville, Joseph, 402
LLL algorithm, 243
LLL-reduced basis, 241
local-global principle, 325
logarithmic integral function, 159
logarithmic Weil height, 423
Lucas numbers, 11
Lucas pseudoprime (lpsp), 103
Lucas sequences, 103
Lucas, Edouard, 10
Lucas-Lehmer algorithm, 545
Lutz, Élisabeth, 488
Lutz-Nagell theorem, 488
Mahler measure, 423
Mahler, Kurt, 422
Markov constant, 219
Matiyasevich’s lemma, 106
Mazur’s bound, 517
Menezes-Vanstone cryptosystem, 537
Mersenne numbers, 38
Mertens constant, 170
Mestre polynomial method, 514
Midi’s theorem, 72
Miller-Rabin primality test, 78
minimal polynomial, 368
  over integers, 368
minimal Weierstrass equation, 483
Minkowski’s theorem
  on convex bodies, 237
  on linear forms, 238
Minkowski, Hermann, 235
Möbius function, 141
Möbius inversion formula, 142
Mordell’s equation, 559
Mordell, Louis Joel, 486
Mordell-Weil basis, 505
Mordell-Weil theorem, 486
multiple, 22, 336
multiplicative function, 55
NAF representation, 530
Nagell, Trygve, 488
Néron-Tate pairing, 504
Newton’s approximant, 230
Newton’s formulas, 362
Newton’s method, 229
Noetherian ring, 400
norm
  of an algebraic number, 379
  normal basis, 524
order, 62

$p$-adic integers, 324
$p$-adic norm, 323
$p$-adic numbers, 324
$p$-adic valuation, 323
pairwise coprime integers, 24
parallelogram low, 500
partial summation formula, 168
Pascal’s formula, 8
Pell’s equation, 284
  fundamental solution, 286
Pellian equation, 296
  ambiguous class, 297
  class of solutions, 297
perfect numbers, 143
perfect square, 33
Pocklington’s theorem, 544
Pollard’s $p$-method, 541
Pollard’s $p−1$ method, 548
polynomial, 335
  coefficients, 335
  degree, 335
  indecomposable, 351
  irreducible, 347
  monic, 335
  primitive, 339
  reducible, 347
  symmetric, 358
  total degree, 358
polynomial basis, 523
polynomial content, 339
polynomial resultant, 345
polynomial ring, 335
power integral basis, 383
prime number theorem (PNT), 159
prime numbers, 31
primitive prime divisor, 104
primitive root, 63
principal character, 178
principal ideal domain, 397
principle of mathematical induction, 4
product of ideals, 385
pseudoprime (psp), 74
Pythagorean triple, 274
  primitive, 274
quadfield, 368
  imaginary, 370
  real, 370
quadform, 125
  positive definite, 126
quadirrat, 222
  reduced, 225
quadnr, 83
quadres, 83
radical
  of a polynomial, 574
  of a positive integer, 576
ramindex, 392
rank of an elliptic curve, 486
rational Diophantine $m$-tuple, 454
reduced residue system, 54
reduction
  additive, 483
  good, 483
  multiplicative, 483
  non-split, 483
  split, 483
regulator
  of a number field, 394
  of an elliptic curve, 505
residuum, 173
Riemann hypothesis (RH), 174
  extended (ERH), 182
  generalized (GRH), 183
Riemann zeta function, 173
Riemann, Bernhard, 172
ring, 334
  commutative with unity, 334
root of a polynomial, 342
  order (multiplicity), 342
root of unity, 524
  primitive, 524
Roth’s theorem, 404
Roth, Klaus Friedrich, 404
RSA cryptosystem, 254
  rebalanced, 262
Schmidt’s subspace theorem, 406
Schönherrmann’s irreducibility criterion, 349
Segre’s theorem, 199
Selberg’s formula, 172
separation exponent, 424
Shanks-Mestre method, 532
Siegel’s identity, 569
Sierpiński, Wacław, 274
sieve of Eratosthenes, 34
signed digit representation, 530
singularity, 172
  essential, 172
  isolated, 172
  pole of order $n$, 172
  removable, 172
Sophie Germain primes, 38
square-free integer, 33
strong Diophantine $m$-tuple, 456
strong pseudoprime (spsp), 75
twin primes, 38
sum of ideals, 387
twist of an elliptic curve, 533
sums of powers, 359
unimodular matrices, 113
Sun Tzu, 50
unique factorization domain, 336
Sylvester’s theorem, 273
unique factorization property, 373
symmetric set, 234
unit, 392
Tate normal form, 494
Vandermonde matrix, 423
Tate, John, 494
Vinogradov, Ivan Matveevich, 86
taylor series, 172
von Mangoldt function, 164
taylor’s formula, 344
ternary quadratic form, 307
W eierstrass form, 467
torsion group, 486
short, 467
Thue equation, 431
Weierstrass, Karl, 470
Thue’s theorem, 432
Weierstrass \( \wp \)-function, 470
Thue, Alex, 431
Weil, André, 486
torsion group, 486
Wiener’s attack, 257
trace of an algebraic number, 379
Wilson’s theorem, 57
trace of Frobenius, 527
Wirsing’s theorem, 417
transcendental numbers, 366
Worley’s theorem, 212
triangular numbers, 131
zero of a polynomial, 342
trinomial basis, 523
zero polynomial, 335
Tunnell’s theorem, 558
Translator
Petra Švob

Lector
Maria Jurjevich

Cover by
Tanja Pružek Šimpović

Graphics preparation
Graphic-art redaction of Školska knjiga

Press
Grafički zavod Hrvatske, d.o.o., Zagreb


CIP copy is available in the catalogue of the National and University Library in Zagreb, under the number 001092040.