

Index

A page number is underlined (for example: 667) when it represents the definition or the main source of information about the index entry. For several key words that appear frequently only ranges of pages or the most important occurrences are indexed.

- AAECC 21
 Abbott, John 465, 734
 Abel, Niels Henrik 373
 Abelian group 704
 Abramov, Sergei Aleksandrovich (Абрамов
 Сергей Александрович) 7, 641, 671, 675,
 734, 735
 Abramson, Michael 738
 Achilles 162
 ACM ... see Association for Computing Machinery
 active attack 580
 Adam, Charles 729
 Adams, Douglas Noël 729, 796
 addition chain 88
 additive group 250, 578, 703, 713
 Adleman, Leonard Max 16, 421, 509, 531, 576, 735,
 762
 affine part 568
 Agrawal, Manindra 517, 543, 735
 Aho, Alfred Vaino 286, 292, 332, 735
 Ajtai, Miklos 496, 735
 Albanese, Andres 215, 735
 Albert, Abraham Adrian 572, 728
 D'Alembert, Jean le Rond 676, 729
 Alford, William Robert (Red) 529, 532, 735
 algebra
 fundamental theorem of ~ 372, 711
 homomorphism 231
 algebraic 710
 closure 711, 716
 complexity theory 243, 338, 721
 computation problem 97
 curve 11, 172, 174, 175, 696
 degree of an ~ element 710
 equation 696
 field extension see field extension
 geometry 558, 568, 595
 computational ~ 4, 591, 595, 619
 integers 707, 708
 number 203, 640, 663
 field 279, 378, 473, 533
 variety 172, 198, 586, 591, 613, 614
 algebraically closed 172, 595, 617, 621, 711
 ALGOLIB 697
 al-Hajjāj see Hajjāj
 Alice 16–18, 503, 504, 573, 574, 577–580
 al-Kāshī see Kāshī
 al-Khwārizmī see Khwārizmī
 Almkvist, Gert 641, 671, 735
 and Zeilberger integration 632, 637, 643
 Alon, Noga 215, 735
 Amerbach, Bonifatius 25
 Amoroso, Francesco 618, 735
 amplitude 360, 362
 analog signal 360
 analysis of algorithms 29, 278, 697
 analytic number theory 508, 523, 532, 533, 652
 Analytical Engine 312
 Andrews, George Eyre 644, 697, 729, 735
 Queen Anne 219
 annihilating polynomial 341
 annihilator, Ann(·) 343
 annus confusionis 83
 Antoniou, Andreas 353, 735
 Antoniszoon, Adrian (Metius) 82
 Aoki, Kazumaro 542, 751
 Apéry, Roger 671, 684, 697, 761
 number 684
 Apollonius of Perga (Ἀπολλώνιος ὁ Περργάσιος)
 198
 Apostol, Tom Mike 62, 735
 Archimedean valuation 274
 Archimedes of Syracuse (Ἀρχιμήδης ὁ
 Συρακοῦσιος) 24, 82, 218, 294, 358, 372, 374,
 622, 669, 735
 Aristotle (Ἄριστοτέλης) 24
 arithmetic
 circuit ... 36, 39, 43, 88, 101, 199, 223, 224, 234,
 235, 248, 252, 495, 619
 representation 495, 497, 498, 501
 hardware ~ 279, 283
 operation 31, 32, 34, 35, 40
 Artin, Emil 568, 748
 Arwin, Axel 418, 735
 Āryabhaṭa 61, 90
 Āryabhaṭīya 61, 286
 ascending chain condition 604, 610
 Asmuth, Charles A. 131, 735
 associate 46, 147, 518, 707, 708
 associated sequence 669
 Association for Computing Machinery (ACM) .. 533
 Journal of the ~ 21
 SIGSAM 21
 asymmetric cryptosystem 17, 575
 asymptotic complexity 6, 338
 Atkin, Arthur Oliver Lonsdale 532, 735
 authentication 576, 578
 automorphism 441, 713, 714, 715
 Frobenius ~ 398, 420, 465, 713
 average 718
 case analysis 61, 62, 162, 419, 523
 depth
 of a Huffman tree 308
 of a stochastic mobile 306, 307, 308
 Avicenna (Abū 'Alī al-Ḥusayn bin 'Abd Allāh bin
 Sīnā, أبو علي الحسين بن عبد الله بن سيني) .. 88
 AXIOM 20, 24
 axiom
 in a proof system 677, 678, 679
 of choice 63
 Azra, Jean-Pierre 745

- B*-number 550, 551, 553, 556, 557, 568
 Babai, László 198, 724, 736
 Babbage, Charles 312, 676, 725, 727, 729
 baby step/giant step strategy 544
 Babylonians 286, 291
 Bach, Carl Eric 6, 61, 287, 421, 529, 531–535, 568, 736
 Bach, Johann Sebastian 86, 736
 Bachet, Claude Gaspard, sieur de Méziriac 61, 513, 736
 Bachmann, Paul Gustav Heinrich 531, 724
 back-tracking 678
 Bacon, Lord Francis 0, 725
 Bailey, David Harold 2, 83, 337, 736, 737
 Baker, George Allen, Jr. 132, 736
 Ball, Walter William Rouse 531, 534, 736
 Barbour, James Murray 91, 736
 Bareiss, Erwin Hans 132, 736
 Barnett, Michael 7
 Barrau, Théophile 725
 Barrow, Isaac 218
 basis
 Gröbner \sim see Gröbner basis
 Hilbert \sim theorem .. 586, 601, 604, 605, 606, 618
 normal \sim 76, 580
 of a lattice 473, 477
 of a vector space 209, 212, 475, 714, 715, 717
 of an ideal 593, 601, 608, 706
 orthogonal \sim 475, 717
 reduced \sim see reduced basis
 reduction 475, 478, 479, 480, 484, 488, 492, 493, 496, 497, 499, 500, 503, 505–509, 576, 580
 standard \sim 591
 Bauer, Andrej 671, 736
 Baur, Walter 352, 736
 Bayer, David 618, 619, 736
 BCH code 3, 209, 210, 211, 212–215, 325, 332, 377, 412, 416, 417, 756
 designed distance of a \sim 212, 213
 generator polynomial of a \sim 211, 212, 214, 215, 416
 Beame, Paul William 6, 697, 736
 Becker, Thomas 618, 736
 Beiler, Albert H. 534, 736
 Bell, Eric Temple (John Taine) 10, 96, 219, 644, 725, 726, 729, 736
 Beltrami, Eugenio 729, 734
 Benecke, Christof 698, 736
 Ben-Or, Michael 410, 411, 421, 498, 619, 736, 737, 759
 Berenstein, Carlos Alberto 618, 737
 Berggren, Lennart 90, 729, 735, 737, 749, 751, 753, 761, 763
 Berkeley, George 622, 729
 Berlekamp, Elwyn Ralph ... 198, 215, 335, 340, 352, 401, 402, 404, 406, 417, 419–421, 428, 462, 465, 467, 530, 737
 algebra ... 401, 402, 403, 420, 423, 427, 428, 430
 algorithm 161, 198, 335, 402, 403, 404, 405, 407, 420, 424, 427, 428, 530, 745, 751
 -Massey algorithm 325, 742
 matrix see Petr-Berlekamp matrix
 Berman, Benjamin P. 640, 737
 Bernardin, Laurent 469
 Bernoulli, Jakob (1654–1705)
 number 650, 669, 672
 random variable 719
 Bernoulli, Johann (1667–1748) 640, 737
 Bernstein, Daniel Julius 247, 287, 353, 737
 Bernstein, Jeremy 725
 Bert 135
 Bertossi, Leopoldo 6
 Bertrand, Joseph Louis François, postulate 525
 Beschorner, Andreas 7
 Beth, Thomas 747, 760
 Bézier, Pierre Étienne 138, 737
 curve 138
 spline 138
 Bézout, Étienne 172, 197, 590, 724, 728, 737
 -coprime 450, 471
 coefficients 58, 62, 141, 153, 155, 161, 197, 325, 326
 matrix 197, 201
 theorem 157, 172, 173, 175, 198, 560, 692
 Bible 24, 219, 711
 Biermann, Gottlieb 725
 big Oh, $O(\cdot)$ 2, 30, 32, 703, 715, 720, 721, 723, 724
 big prime modular algorithm . see modular algorithm
 bijective 704, 705
 bilinear
 complexity 337, 338
 map 355
 Bimberg, Guido 766
 binary
 calendar 84
 Euclidean Algorithm 61, 65, 738
 rational 200
 representation 75, 88, 100, 262, 283, 408, 504
 tree 296, 303, 305–307, 309
 Binet, Jacques Philippe Marie 61, 737
 Bini, Dario Andrea 352
 binomial 230, 463, 616, 681
 coefficient 76, 166, 658–660, 669, 670, 684, 713, 768
 ideal 616, 681, 697
 theorem 76, 667, 669, 673
 BiPOLAR 3, 279, 281–283, 461, 462
 Birch, Thomas 726
 birthday problem 546, 548
 bit operation 32
 bivariate
 factorization ... 433, 457, 459, 493, 496, 497, 586
 interpolation 134
 modular
 gcd see modular gcd
 EEA see modular EEA
 polynomial ... 141, 162, 178, 182, 186, 203, 205, 206, 246, 254, 289, 332, 457, 473, 493
 black box 101, 340, 351–353, 355, 496, 498
 linear algebra 335, 340, 346, 352, 404, 407
 representation of a polynomial 496
 Black, John Richard 7
 Blake, Ian 580, 737
 Blakley, George Robert (Bob) 131, 735

- Blau, Peter 6
 blocking strategy 422, 461
 Blömer, Johannes Friedrich 215, 735
 boat conformation ... see cyclohexane conformation
 Bob 16, 17, 503, 573, 574, 577–580
 du Bois-Reymond, Emil 588
 Boltzmann, Ludwig 622, 728
 Bolyai, Wolfgang 374
 Bolyai de Bolya, János (Johann) 374
 Bombieri, Enrico 90, 737
 Bonn i, 8
 Bonnet, Ossian Pierre 374
 Bonorden, Olaf 461, 737
 Boole, George 669, 737, 766
 Boolean
 circuit 32
 variable 678
 Borodin, Allan Bertram .. 6, 286, 306, 498, 737, 757
 Borwein, Jonathan Michael .. 83, 90, 729, 735, 737,
 749, 751, 753, 761, 763
 Borwein, Peter Benjamin 83, 90, 729, 735, 737,
 749, 751, 753, 761, 763
 Bos, Joppe Willem 542, 751
 Bose, Nirmal Kumar 738
 Bose, Raj Chandra 215, 737, 756
 Bosma, Wiebren 6, 737, 739
 bound
 Hasse ~ 508, 562, 564, 565, 740
 Mignotte ~ see Mignotte bound
 Weil ~ 568, 736
 Bourgne, Robert 745
 Bouyer, Martine 82
 Boyar, Joan 505, 737
 Boyle, Robert 44, 726
BPP 496, 532, 616, 721, 722, 724
 Brassard, Gilles 41, 720, 737
 Bratley, Paul 41, 720, 737
 Brauer, Alfred Theodor 737
 Bremner, Murray Ronald 7
 Brent, Richard Peirce ... 61, 90, 332, 353, 354, 542,
 567, 738
 Brickell, Ernest Francis 509, 738
 Brieskorn, Egbert 568, 738
 Brillhart, John David 541, 542, 568, 738, 758
 Broda, Engelbert 728
 Bronstein, Manuel 640–642, 671, 735, 738, 760
 Brook, Clifford Hardman (Clive) 729
 Brown, William Stanley 62, 197–199, 332, 738
 Brownawell, Woodrow Dale 618, 738
 Brun, Viggo 758
 Bruns, Winfried 7
 Bshouty, Nader Hanna (نادر حتّا بشوتي) ... 353, 751
 bubble sort 221
 Bucciarelli, Louis 6
 Buchberger, Bruno ... 21, 591, 609, 618, 738, 740, 750,
 753, 757
 algorithm . 591, 608, 609, 610, 611, 612, 617, 747
 Buchmann, Johannes 20
 Budach, Lothar 762
 Buffon, Georges Louis Leclerc, Comte de 198
 Buhler, Joe Peter 759, 764
 Bunch, James Raymond 352, 738
 Bürgisser, Peter . 7, 88, 222, 286, 338, 352, 616, 739
 Burnikel, Christoph 286, 739
 Burrus, Charles Sydney 247, 748
 Buss, Samuel Rudolph 697, 739
 Butler, Michael Charles Richard 420, 739
 butterfly operation 234, 235
 Büttner, J. G. 372
 C, field of complex numbers 768
 Cade, John Joseph 576, 739
 Caesar, Gaius Julius 83, 84, 575
 cipher 573, 574, 580
 Caldwell, Chris Kelly 534
 calendar 11, 69, 83
 Gregorian ~ 84, 91
 Julian ~ 83, 84, 91
 lunar ~ 83
 lunisolar ~ 83
 Camion, Paul Frédéric Roger 419, 420, 739
 cancellation law 706
 Canfield, Earl Rodney 567, 739
 Caniglia, Leandro 618, 619, 739
 Cannon, John 20
 Canny, John Francis 619, 698, 739, 759
 canonical
 form
 of a rational function .. 116, 117, 119, 121, 122,
 124, 138
 of a rational number 126, 127
 representative 398
 ring homomorphism 72, 104, 110, 706, 709
 Cantor, David Geoffrey 245, 247, 280–282, 287,
 405, 406, 417, 418, 466, 739
 and Zassenhaus algorithm 382, 407
 multiplication algorithm 281, 282, 287
 Carathéodory, Constantin 586
 cardinality, # 704, 768
 Carlitz, Leonard 426, 739
 Carlyle, Thomas 726
 Carmichael, Robert Daniel 531, 739
 function, λ 535
 number ... 520, 521–523, 531, 532, 535, 537, 735
 Carmody, Phil 534
 Caron, Thomas R. 531, 567, 739
 le Carré, John (David John Moore Cornwell) ... 220,
 727
 Carroll, Lewis (Rev. Charles Lutwidge Dodgson)
 28, 726
 carry
 flag 30, 41, 42, 222, 262, 280
 look-ahead addition 41
 de Castel'jau, Paul de Faget 138, 739
 Castelfnuovo, Guido, -Mumford regularity 618
 Cataldi, Pietro Antonio 89, 739
 Cauchy, Augustin Louis 131, 132, 197, 286, 373,
 739, 740, 755
 interpolation ... 118, 121, 137, 138, 190, 325, 331
 -Schwarz inequality 485, 500, 555
 sequence 292
 Cavaleri, Bonaventura 622
 Caviness, Bob Forrester 640, 740

- Cayley, Arthur 197, 740, 749
 -Hamilton theorem 341, 716
 center of gravity 592, 612, 613, 652
 Ceres 374
 Cervantes Saavedra, Miguel de 90, 740
 van Ceulen, Ludolph (Ludolf) 82, 90
 Chahal, Jasbir Singh 568, 740
 chain rule 266, 354
 chair conformation ... see cyclohexane conformation
 Chandler, Raymond 729, 734
 change of representation 99, 100, 231, 363
 Char, Bruce Walter 202, 740
 characteristic
 of a ring or field, char 394, 395, 397, 415, 460,
 558, 561, 581, 623, 626, 630, 637, 658, 665,
 710, 712
 polynomial
 of a matrix 337, 346, 420, 716
 of a sequence 341, 342–344, 348, 349, 354, 355
 set 619
 King Charles II of England 218
 Ray-Chaudhuri, Dwijendra Kumar ... 215, 737, 756
 Chebotarev, Nikolai Grigor'evich (Чеботарёв
 Николай Григорьевич) 441, 442, 465,
 740
 theorem .. 441, 442, 443, 465, 467, 753, 759, 764
 Chebyshev, Pafnuti Lvovich' (Чебышев
 Пафнутий Львович) 533, 740
 Chen, Evan Jingchi 7
 Chen, Pehong 8
 Chen, Zhi-Zhong 199, 740
 Cheng, Howard 7
 Chernac, Ladislaus 728
 Chinese Remainder
 Algorithm (CRA) . 3, 19, 100, 101, 106, 104–139,
 170, 171, 189, 190, 244, 246, 286, 295, 332,
 339, 580, 707
 fast ~ 131, 301, 303, 305, 309, 331, 626
 Problem 108, 109, 112, 114, 305, 306
 rational ~ 138
 Theorem (CRT) . 17, 75, 105, 104–139, 231, 243,
 295, 302, 309, 384, 424, 518, 554
 Chistov, Aleksandr Leonidovich (Чистов
 Александр Леонидович) ... 466, 619, 740
 Chor, Ben-Zion (Benny) 509, 740
 Chou, Chung-Chiang 352, 740
 chromatic scale 86
 Chudnovsky, David Vol'fovich (Чудновский
 Давид Вольфович) 90, 750
 Chudnovsky, Gregory Vol'fovich (Чудновский
 Григорий Вольфович) 90
 Ch'ung-chih, Tsu 82
 Church, Alonzo 750
 Chyzak, Frédéric 671, 740, 741
 Cicero, Marcus Tullius 28, 726
 circuit
 arithmetic ~ see arithmetic circuit
 Boolean ~ 32
 Clancy, Tom 376, 572, 728
 Clarke, Arthur A. 746
 Clarke, Arthur Charles 10, 725
 class field theory 586
 classical
 algorithm 36
 polynomial multiplication 34
 Clausen, Michael Hermann ... 7, 88, 222, 286, 338,
 352, 498, 739, 741
 Clebsch, Rudolf Friedrich Alfred 729
 Clegg, Matthew 679, 741
 Clifford, William Kingdon 702, 729
 closed form 1, 66, 645, 673, 675, 697
 von Coburg (Koburgk), Simon Jacob 61
 code 11, 18, 209–212, 214, 215
 BCH ~ see BCH code
 cyclic ~ 416
 dimension of a ~ 209, 210, 211
 erasure ~ 18, 215
 error correcting ~ 18, 209
 Huffman ~ 307, 365–368
 instantaneous ~ 307
 length of a ~ 209, 210–212
 linear ~ 209, 215
 minimal distance of a ~ 210, 211–213, 215
 coding theory 37, 209, 215, 325, 416
 coefficient
 growth 141, 143
 matrix 715
 of a polynomial 32
 representation 100
 Cohen, Henri José 20
 coincide up to 314, 315–317, 322, 323, 332
 Collins, George Edwin . 20, 197–199, 332, 455, 465,
 619, 741, 750, 753, 757
 combinatorial identity 681
 commutative
 group 342, 349, 704, 705, 713
 ring 705, 706, 709, 711, 713
 commute 709
 complete 292, 722
 completion 275
 complexity
 asymptotic ~ 6, 338
 class 721–723
 theory 3, 199, 222, 573, 616, 703, 721
 composite 518
 compositeness test 532
 COMPOSITES 532
 computational
 algebraic geometry 4, 591, 595, 619
 complexity 509, 576
 number theory 3, 4, 517–571, 586
 computational complexity (journal) 21
 computer algebra system 1, 2, 4, 11, 19–21, 197,
 221, 278, 279, 378, 494, 532, 619, 623, 631, 640,
 645
 conditional probability 682, 718
 conformation see cyclohexane conformation
 congruent modulo, mod 69, 706
 conjugacy class 465
 conjugates 713
 co- \mathcal{NP} 722, 723
 construction of irreducible polynomials ... 377, 406,
 410

- content, $\text{cont}(\cdot)$... [147](#), [148](#), [149](#), [150–152](#), [162](#), [192](#),
 199, 200, [433](#), [695](#)
- continuant polynomial ... [65](#), [93](#)
- continued fraction ... [3](#), [69](#), [79–81](#), [84](#), [87](#), [89–91](#), [93](#),
 94, [132](#), [542](#), [768](#)
- expansion ... [79](#), [80](#), [81](#), [84](#), [87](#), [90](#), [568](#)
- factoring method ... [541](#), [568](#)
- control point ... [138](#)
- convergent ... [94](#)
- convex
- body ... [473](#)
- hull ... [198](#)
- convolution
- cyclic ~ ... [230](#), [231](#)
- fast ~ ... [235](#), [240](#), [244](#), [250](#), [251](#), [252](#), [253](#), [254](#)
- negative wrapped ~ ... [238](#), [239](#)
- of polynomials ... [230](#), [235](#), [237](#), [252](#)
- of signals ... [368](#), [369](#)
- property ... [368](#)
- Vandermonde ~ ... [672](#)
- Conway, John Horton ... [533](#)
- Cook, Stephen Arthur ... [6](#), [247](#), [286](#), [722](#), [741](#)
- Cookie Monster ... [135](#)
- Cooley, James William ... [233](#), [247](#), [294](#), [727](#), [741](#)
- Coppersmith, Don ... [352](#), [353](#), [420](#), [741](#), [742](#), [750](#), [765](#)
- coprime ... [46](#), [55](#), [450](#), [707](#)
- Bézout~ ... [450](#), [471](#)
- Cori, Robert ... [756](#)
- Corless, Robert Malcolm ... [7](#), [41](#), [287](#), [741](#), [751](#)
- Cormen, Thomas H. ... [41](#), [368](#), [741](#)
- co- \mathcal{RP} ... [532](#), [722](#), [723](#)
- de Correa, Isabel ... [6](#)
- coset ... [704](#), [715](#)
- cyclotomic ~ ... [415](#)
- of an ideal ... [706](#)
- cosine theorem ... [12](#)
- Cot, Norbert ... [747](#), [760](#)
- Courant, Richard ... [586](#)
- Cowie, James ... [569](#), [741](#)
- Cowles, John Richard ... [199](#), [762](#)
- Cox, David Archibald ... [568](#), [614](#), [617](#), [618](#), [741](#)
- Coxeter, Harold Scott Macdonald ... [531](#), [534](#), [736](#)
- CRA ... see Chinese Remainder Algorithm
- Cramer, Gabriel ... [198](#), [724](#), [741](#)
- rule ... [116](#), [136](#), [157](#), [183](#), [186](#), [200](#), [204](#), [205](#), [485](#),
 716
- Cray ... [337](#)
- Creutzig, Christopher ... [7](#)
- Crichton, Michael ... [208](#), [726](#)
- critical line ... [533](#)
- Cromwell, Oliver ... [208](#), [726](#)
- Crossley, John Newsome ... [727](#), [741](#)
- crossover point ... [221](#), [222](#), [241](#), [251](#), [279](#), [281](#), [282](#),
 337
- CRT ... see Chinese Remainder Theorem
- cryptanalysis ... [503](#), [504](#), [575](#)
- cryptography ... [11](#), [16](#), [18](#), [37](#), [209](#), [503](#), [505](#), [509](#),
 517, [523](#), [525](#), [573–582](#)
- public key ~ ... [3](#), [17](#), [503](#), [575](#), [573–582](#)
- cryptosystem ... [3](#), [17](#), [503](#), [504](#), [541](#), [542](#), [573](#),
 573–582
- asymmetric ~ ... [17](#), [575](#)
- ElGamal ~ ... [579](#), [580](#)
- elliptic curve ~ ... [573](#), [580](#)
- key in a ~ ... [16](#), [18](#), [505](#), [509](#), [573](#), [573–582](#)
- knapsack ~ ... [503](#), [509](#)
- Rabin ~ ... [573](#), [579](#)
- RSA ~ ... see RSA cryptosystem
- short vector ~ ... [573](#)
- subset sum ~ ... [509](#)
- symmetric ~ ... [16](#), [575](#), [578](#)
- cubic spline ... [137](#)
- Cucker, Felipe ... [745](#)
- Cunn, Samuel ... [725](#), [726](#), [758](#)
- Cunningham, Lt.-Col. Allan Joseph Champneys
 ... [541](#), [543](#), [741](#)
- number ... [222](#), [542](#)
- project ... [541](#), [542](#), [569](#)
- curve
- algebraic ~ ... [11](#), [172](#), [174](#), [175](#), [696](#)
- Bézier ~ ... [138](#)
- elliptic ~ ... see elliptic curve
- Gauß bell ~ ... [372](#)
- nonsingular ~ ... [559](#), [568](#), [571](#)
- plane ~ ... [173](#), [198](#), [203](#), [594](#), [615](#)
- projective ~ ... [567](#), [568](#)
- cycle structure of a permutation ... [465](#)
- cyclic
- code ... [416](#)
- convolution ... [230](#), [231](#)
- group ... [250](#), [251](#), [349](#), [422](#), [578](#), [704](#), [713](#)
- module ... [349](#), [350](#)
- cycloheptane ... [694](#), [698](#)
- cyclohexane ... [11](#), [12](#), [14](#), [16](#), [494](#), [619](#), [685–699](#), [725](#)
- conformation of ~ ... [11](#), [12](#), [15](#), [685](#), [687](#), [689](#), [698](#),
 699
- boat ~ ... [12](#), [13](#), [15](#), [16](#), [690](#), [691](#), [696](#)
- chair ~ ... [12](#), [13](#), [16](#), [686](#), [692](#), [693](#)
- flexible ~ ... [12](#), [15](#), [16](#), [696](#), [698](#)
- rigid ~ ... [12](#), [15](#), [16](#), [698](#)
- cyclotomic
- coset ... [415](#)
- polynomial, Φ_n ... [164](#), [201](#), [211](#), [253](#), [412](#), [413](#),
 414, [416](#), [421](#), [441](#), [442](#), [467](#), [568](#)
- D , differential operator ... [624](#), [633](#), [669](#), [673](#)
- D , division time ... [298](#)
- D' Alembert, Jean le Rond ... [676](#), [729](#)
- Damgård, Ivan Bjerre ... [532](#), [742](#)
- Das, Abhijit ... [7](#)
- data
- compression ... [307](#), [363–366](#)
- structure ... [97](#), [493](#)
- database integrity ... [37](#)
- Datta, Ruchira Sreemati ... [7](#)
- Daubert, Katja Elisabeth ... [7](#)
- Davenport, James Harold ... [641](#), [742](#)
- Davies, Charles ... [432](#), [728](#)
- Davis, Martin David, -Putnam procedure ... [678](#)
- DCT, Discrete Cosine Transform ... [363](#), [364](#), [363–369](#)
- Dean, Basil ... [729](#)
- Dèbes, Pierre ... [498](#), [742](#)
- de Casteljau, Paul de Faget ... [138](#), [739](#)

- decimal representation ... 31, 37, 40, 70, 71, 82, 92, 100, 505
- decision problem 721, 722
 hard ~ 722
 instance of a ~ 721
- Decker, Wolfram 7
- de Correa, Isabel 6
- decryption 16, 17, 573–582
- Dedekind, Julius Wilhelm Richard ... 373, 419, 742, 746
- Degeyter, Pierre-Chrétien 727
- degree
 formula 710
 function 63, 94
 of a field extension 384, 710, 711
 of a polynomial, deg 32, 708, 709
 of an algebraic element 710
 sequence ... 92, 93, 142, 178–181, 187, 188, 190, 204, 314, 329, 333
 normal ~ . 51, 53, 59, 60, 65, 93, 195, 314, 317, 319, 321–324, 326, 330, 333
 total ~ 157, 172, 176, 493, 597, 616, 689, 709
 valuation 91, 94, 274
- de Groote, Hans Friedrich 352, 748
- Delaunay, Charles Eugène 20
- Δ , difference operator 646, 647, 660, 671, 673
- DeMillo, Richard Allan 88, 198, 742
- de Moivre, Abraham 353
- De Morgan, Augustus 44, 68, 96, 622, 726, 729
- Deng, Yuefan 352, 740
- dense representation 101, 231, 493, 494
- derivation 197, 624
- derivative .. 113, 114, 122, 133, 156, 213, 259, 265, 266, 267, 289–291, 300, 394, 623, 624, 633, 642, 647, 667, 768
 Hasse-Teichmüller ~ see Hasse-Teichmüller
 logarithmic ~ 633, 635, 636, 639, 641
 trivial ~ 624, 642
- DERIVE 20
- de Sainte-Croix, Jumeau 669
- Descartes, René, du Perron . 334, 512, 622, 727, 729, 796
- designed distance of a BCH code 212, 213
- determinant, det ... 50, 100, 109–111, 113, 136, 157, 172, 197–199, 204, 205, 328, 329, 335, 337, 688, 715, 716
 Gramian ~ 482, 484, 717
 modular ~ 109, 113, 132, 525
 big prime ~ 110, 113, 168, 460, 526
 small primes ~ see modular determinant
- de Weger see Weger
- DFT see Discrete Fourier Transform
- DH see Diffie-Hellman problem
- Diamond, Harold George 745
- diatonic scale 85, 86
- Díaz, Angel Luis 199, 498, 742
- Dickman, Karl Daniel, ρ -function 553
- Dickson, Leonard Eugene 88, 591, 742
 lemma 602, 603, 604, 620
- Didymos of Alexandria (Δίδυμος Ἀλεξανδρέως) 85
- difference
 equation 660, 669, 671, 675
 field 659, 660, 675
 operator, Δ 646, 647, 660, 671, 673
- differential
 algebra 623, 624, 640, 641
 equation ... 1, 4, 90, 353, 428, 633, 640–643, 653, 669, 684
 Risch ~ 641, 738, 742, 750
 field 624, 625, 633, 641
 operator, D 624, 633, 669, 673
- Diffie, Bailey Whitfield 503, 575, 576, 578, 581, 742
- Hellman
 key exchange 573, 578, 579, 756
 Problem 579, 580, 582
- digital
 filter 353
 signal 247, 359, 363, 368
 signature 578
- dimension
 formula 714
 of a code 209, 210, 211
 of a lattice 474, 480
 of a vector space ... 349, 401, 674, 685, 687, 688, 698, 710, 711, 714
- Diophantine
 approximation .. 3, 79, 80, 87, 473, 497, 505, 762
 simultaneous ~ 87, 503, 505, 507–509, 753
 equation 512, 764, 766
 linear 69, 77, 79, 89, 93
- Diophantus of Alexandria (Διόφαντος Ἀλεξανδρέως) 513, 514, 754, 756
- direct product
 of finite probability spaces 718
 of groups 704
 of rings 706
- directed graph 423, 468, 679
- Lejeune Dirichlet, Johann Peter Gustav 62, 506, 507, 509, 528, 588, 707, 742
- Schubfachprinzip 678
- DISCO 21
- Discrete
 Cosine Transform (DCT) 363, 364, 363–369
 Inverse ~ (IDCT) 363, 366, 369
 Fourier Transform (DFT) 229, 221–254, 262, 340, 352, 362, 359–369
 Logarithm Problem (DL) 579, 580, 582
 signal 359, 360–364, 368, 369
- discriminant, disc 156, 207, 435, 441, 443, 454, 455, 466, 467, 470, 471, 537, 689
- dispersion, dis 675
- distinct-degree
 decomposition 381, 392, 400, 422
 factorization 373, 381, 377–421, 461, 462
- distributed
 computing 19, 99, 567
 data structures 18, 19
- divide-and-conquer ... 286, 289, 298, 300, 309, 317, 353
- division
 exact ~ 42, 202, 251, 261, 289, 310

- property 706, 707, 709
 pseudo-~ .. 38, 183, 190, 191, 197, 199, 204–206
 time, D 298
 trial ~ 389, 541, 543, 544, 552
 with remainder 2, 26, 37, 38, 39, 41, 45, 51,
 59–62, 100, 131, 257, 261, 262, 282, 283, 314,
 407, 445
 fast ~ 221, 261, 264, 282, 287, 339
 multivariate ~ 595, 598, 599, 600, 604, 605
 Dixon, Alfred Cardew 671, 743
 Dixon, John Douglas 61, 568, 569, 742
 random squares method . 340, 541, 549, 550, 551,
 556, 558, 567, 569, 570, 579
 DL, Discrete Logarithm Problem 579, 580, 582
 Dodson, Bruce 569, 741, 742
 Don Quixote de la Mancha 90, 740
 Dooley, Samuel Sean 738, 746, 763
 Dörge, Karl 466, 742
 Dornstetter, Jean Louis 215, 742
 double-precision integer 29
 Doughty, Herb 757
 Doyle, Sir Arthur Conan 572, 702, 728, 729
 Dozier, Lamont 728
 Dreker, Stefan 7
 Dresden, Arnold 729
 Dress, Andreas 498, 741
 Drobisch, Moritz Wilhelm 91, 742
 Dubé, Thomas William 618, 742
 Dubner, Harvey Allen 530, 766
 Dubois, Raymond 532, 742
 du Bois-Reymond, Emil 588
 Ducos, Lionel 199, 742
 Dupré, Athanase 61, 742
 Durucan, Emrullah 7
 dynamical systems theory 276

E, shift operator 646, 648, 659, 660, 671
 early abort 382
 Eberly, Wayne Michael 6, 353, 742
 Edmonds, Jeffrey Allen 215, 679, 735, 741
 Edmonds, John Robert (Jack) 132, 742
 EEA see Extended Euclidean Algorithm
 effective univariate factorization see factorization
 eigenvalue 716
 Einstein, Albert 734
 Eisenbrand, Friedrich 7
 Eisenbud, David 617, 697, 742, 743
 Eisenstein, Ferdinand Gotthold Max . 373, 533, 743
 theorem 467
 Ekhad, Shalosh B. 697, 743
 Eleatics 24
 Electronic Frontier Foundation 517
 elementary
 functions 623
 symmetric polynomial 166
 Elements (Euclid) 24, 25, 26, 61, 518, 531, 724, 725
 ElGamal, Taher (طاهر الجمال) see Gamal
 elimination of variables 172
 Elkenbracht-Huizing, Reina Marije 569, 741
 ellipsoid method 473
 elliptic curve 508, 558, 557–568, 571, 580
 cryptosystem 573, 580
 factoring method ... 287, 541, 542, 563, 557–567,
 571
 size of an ~ 561, 565
 smooth ~ 559, 560
 Emiris, Ioannis Zacharias (Ἐμίρης, Ἰωάννης
 Ζαχαρίου) 7, 698, 743
 Encarnación, Mark James 465, 741
 Encke, Johann Franz 746
 encoding map 209
 encryption 16, 17, 573–582
 endomorphism 714, 715
 Frobenius ~ 398, 402, 404, 427, 428, 713, 746
 Eneström, Gustav 743
 Engel, Friedrich 728
 ENIGMA 574
 entropy 298, 324, 452
 equal-degree
 factorization ... 387, 377–421, 424, 461, 462, 554,
 579
 splitting 385, 387, 423, 424
 equivalence relation 92, 314, 332, 430, 673, 707
 Erasmus of Rotterdam 25
 erasure code 18, 215
 Eratosthenes of Cyrene (Ἐρατοσθένης ὁ
 Κυρηναῖος) 24, 518
 sieve 171, 527, 531, 533, 552, 557
 Erdmann, Johann Eduard 726
 Erdős, Pál 512, 567, 739
 ERH see Extended Riemann Hypothesis
 Ernie 135
 error
 correcting code 18, 209
 locator polynomial 213
 Euchner, Martin 497, 762
 Euclid (Εὐκλείδης) 3, 24, 25, 26, 44, 61, 73, 93,
 518, 531, 724, 725, 748
 Euclidean
 Algorithm .. 3, 4, 25, 45–207, 313–333, 530, 612,
 616, 707, 738, 742, 754, 756, 763, 765, 766
 binary ~ 61, 65, 738
 Extended ~ (EEA) see Extended Euclidean
 fast ~ .. 3, 7, 178, 263, 325, 313–333, 345, 626
 monic ~ see monic
 primitive ~ .. 190, 191, 192, 194–197, 199, 206
 quotient in the ~ see quotient
 remainder in the ~ see remainder
 traditional ~ see traditional
 with least absolute remainders 66
 domain .. 45, 45–95, 97, 104, 106, 135, 147, 158,
 159, 186, 257, 352, 595, 707, 708–711
 engine 198
 function 46, 47, 48, 61–64, 257, 707
 minimal ~ 62, 63
 norm, two-norm, $\|\cdot\|_2$ 12, 157, 164, 473, 474,
 480, 487, 497, 717, 768
 number field 724, 755
 representation 64
 Eudoxus of Cnidus (Εὐδόξος Αἰσχίνου Κνίδιος)
 24

- Euler, Leonhard . . . 62, 76, 88–91, 131, 132, 134, 197, 198, 372, 418, 513, 520, 533, 542, 586, 644, 670, 735, 743, 753, 761
 constant, γ 534, 651
 number 669
 theorem 17, 518, 519, 577, 704
 totient function, φ 17, 75, 108, 131, 136, 250, 412, 518, 535, 577
- evaluation
 homomorphism 107, 709
 map 103, 215, 295
 multipoint \sim 19, 97–103, 231–233, 280, 281, 295, 296, 299, 300, 302, 309, 333, 339, 399, 407, 460
 fast \sim 231, 295, 298, 299, 308, 399, 544
 of a matrix 340, 346, 348, 352, 353
- Evdokimov, Sergei Alekseevich (ЕВДОКИМОВ Сергей Алексеевич) 421, 743
- Eve 16, 573, 580, 582
- event 718
- eventually positive 720
- exact division 42, 202, 251, 261, 289, 310
- exp, exponential function 768
- expected value 184, 205, 411, 682, 718
- ΕΧΡΕΧΡΤΙΜΕ* 723
- explicit linear algebra 335, 352, 407
- ΕΧΡSPACE* 616, 697, 723
- ΕΧΡTIME* 723
- Extended
 Euclidean Algorithm (EEA) . . . 17, 48, 57, 45–207, 214, 242, 283, 304, 313–333, 344, 407, 448, 450–452, 505, 577, 710
 big prime modular \sim 189, 190, 195, 206
 bivariate modular \sim 189
 modular \sim 183, 186, 206, 326, 331
 primitive \sim 192
 small primes modular \sim see modular EEA
 traditional \sim see traditional
 Riemann Hypothesis (ERH) . . . 421, 532, 533, 743, 759
- extension field see field extension
- EZ-GCD 460, 466
- factor
 base 550, 557
 combination 434–436, 441, 453, 455, 458, 462, 465, 489, 492, 496, 497
 group 704
- factorial
 falling \sim 647, 649, 654, 669, 670, 673, 768
 greatest \sim factorization, gff . . . see greatest factorial ring 707
 rising \sim 647, 670, 673, 768
- factorization 2, 20
 bivariate \sim 433, 457, 459, 493, 496, 497, 586
 by continued fraction method 541, 568
 by elliptic curve method see elliptic curve
 distinct-degree \sim 373, 381, 377–421, 461, 462
 effective univariate \sim 457, 459, 473, 493, 501
 equal-degree \sim see equal-degree factorization
 greatest factorial \sim , gff see greatest factorial
 irreducible \sim see irreducible factorization
- modular \sim see modular factorization
 of integers 3, 17, 18, 198, 222, 335, 340, 352, 353, 505, 513, 517, 521, 531–533, 541, 541–571, 577–579
 of multivariate polynomials 493, 497, 501
 of polynomials 2, 4, 15, 20, 148, 271, 282, 286, 372, 373, 377, 377–501, 505, 513, 586, 588
 over \mathbb{Z} and \mathbb{Q} 37, 100, 164, 257, 373, 440, 433–471, 473, 474, 487–501, 525, 528
 over finite fields 3, 77, 279, 283, 340, 352, 389, 377–430, 461–463, 488, 493, 569, 724
 of sparse polynomials 497
- pattern 435, 442, 443, 444, 462, 465, 467, 468
- prime \sim 106, 131, 291, 292, 518, 529, 535, 550, 554
- squarefree \sim 377, 379, 389, 393, 395, 397, 416, 426, 658
- unique \sim 706, 707
 domain (UFD) see unique factorization domain
- Faddeev, Dmitrii Konstantinovich (Фаддеев Дмитрий Константинович) 132, 419, 744
- Faddeeva, Vera Nikola'evna (Фаддеева Вера Николаевна) 132, 744
- Fahle, Torsten Klemens 7
- falling factorial 647, 649, 654, 669, 670, 673, 768
- Fano, Robert Mario 307, 744
- fast
 convolution 235, 240, 244, 250, 251, 252, 253, 254
 CRA see Chinese Remainder Algorithm
 division with remainder see division
 Euclidean Algorithm see Euclidean Algorithm
 exponentiation 373, 580
 integer multiplication 221–254
 interpolation 231, 301, 295–310, 331
 matrix multiplication 336, 337, 340
 modular composition 338, 339, 405
 multipoint evaluation see evaluation
 polynomial multiplication 221–254
 sorting 233
- Fast Fourier Transform (FFT) . . . 3, 19, 82, 211, 233, 221–254, 281, 363, 364, 373, 741, 744, 747, 748, 760
- arithmetic circuit 234
- Fermat number \sim 284–286
- multiplication 3, 101, 238, 243, 247, 250, 251, 262, 279, 280, 283, 286, 333
 support the \sim 237, 245, 251, 296, 333
- 3-adic \sim 242, 247, 252, 253
- three primes \sim 243, 246, 247, 283, 284, 286
- Fateman, Richard Jay 640, 737
- Faugère, Jean-Charles 619, 744
- Faulhaber, Johann 670, 752
- feasible matrix multiplication exponent 337, 338, 352
- Feisel, Sandra 6, 7
- Felkel, Anton 540
- Feller, William 717, 744
- Ferdinand, Duke of Braunschweig 372
- Ferdinand von Fürstenberg 514, 725
- Fermat, Clément-Samuel de 514, 725

- Fermat, Pierre de ... 3, 7, 24, 76, 88, 89, 93, 218, 512, 513, 514, 520, 530, 550, 622, 669, 725, 739, 741, 743, 744, 764, 765
 last theorem 514, 595, 761, 766
 liar 519, 534
 little theorem 77, 88, 379, 380, 398, 513, 518, 520, 531, 704, 712, 713, 742, 743
 number, F_n . . . 76, 88, 246, 513, 520, 530, 538, 542, 738, 755
 FFT 284–286
 polynomial 493
 primality test 519, 520, 521, 523, 534
 prime 228, 251, 530, 536
 witness 519, 520, 522, 523, 534
 Feynman, Richard Phillips 220, 540, 727, 728
 FFT see Fast Fourier Transform
 Fibonacci, Leonardo Pisano, son of Bonaccio
 number 53, 54, 61, 66, 89, 742
 sequence 66, 341, 343
 Fich, Faith Ellen 6
 Fiduccia, Charles (Chuck) Michael ... 306, 353, 744
 Fieker, Claus 749
 field 32, 708, 710, 711
 algebraic number ~ 465
 difference ~ 659, 660, 675
 differential ~ 624, 625, 633, 641
 extension 74, 398, 408, 411, 633, 663, 710, 711–713
 algebraic ~ .. 175, 343, 378, 384, 493, 627, 630, 710, 711
 degree of a ~ 384, 710, 711
 finite ~ 710
 Galois ~ 466
 normal ~ 398
 finite ~, \mathbb{F}_q see finite field
 Hilbertian ~ 498
 of constants 627, 659
 of fractions . . . 42, 79, 147, 149, 150, 152, 157, 177, 186, 191, 200, 275, 292, 433, 500, 710
 operation see arithmetic operation
 perfect ~ 397
 splitting ~ 177, 426, 429, 441, 627, 628, 630, 711
 Fields, John Charles, medal 591
 Finck, Pierre Joseph Étienne 61, 744
 fingerprinting 70, 88, 91
 finite
 -dimensional vector space 710, 714
 duration 363, 369
 extension of a field 710
 field, \mathbb{F}_q ... 2, 18, 20, 55, 73, 75, 76, 88, 229, 266, 286, 313, 355, 377–430, 711, 712, 713
 irreducibility test over a ~ 407
 root finding over a ~ 377, 392, 418, 428
 prime field, \mathbb{F}_p . . . 73, 421, 427, 428, 462, 471, 568
 probability space 703, 717, 718, 719
 finitely generated
 ideal 593, 603, 604, 618
 vector space 714
 Fish, Daniel W. 540, 728
 Fitch, John 740, 747, 750, 757
 Fitchas, Noai 619, 744
 Flaccus, Aules Persius 699, 729
 Flajolet, Philippe Patrick Michel 419, 697, 744, 759, 763, 765
 Fleischer, Jochem 736, 748, 760
 flexible conformation see cyclohexane conformation
 floating point
 arithmetic 20, 82, 283, 497
 number 32, 286, 337
 representation 100
 Floyd, Robert W. 546
 cycle detection trick 546, 547, 548, 567
 fluxions 218
 FOCUS 21
 Folkerts, Menso 286, 727, 744
 Ford, Garrett 729
 Fourier, Jean Baptiste Joseph ... 247, 358, 727, 744
 coefficient 362, 369
 prime 99, 243, 246, 528, 529, 536
 series 361, 741
 Transform 247, 359, 361–363, 369, 513
 Continuous ~ 359, 361, 362
 Discrete ~ (DFT) see Discrete Fourier
 Fast ~ (FFT) see Fast Fourier Transform
 \mathbb{F}_p , finite prime field ... 73, 421, 427, 428, 462, 471, 568
 \mathbb{F}_q , finite field 73, 712
 fractal 226, 273, 276–278, 287
 Franke, Jens 542, 751
 Fredet, Anne 641, 738
 Freeman, Timothy Scott 498, 744
 Frege, Friedrich Ludwig Gottlob 588, 739
 -Hilbert proof 678
 Freivalds, Rūsiņš 88, 744
 Frénicle de Bessy, Bernard 513
 frequency 84–86, 359, 360, 361–363, 365, 366
 analysis 574
 Friedman, Philip 472, 572, 728
 Frieze, Alan Michael 505, 744
 FRISCO 619
 Frisé, Adolf 727
 Frobenius, Ferdinand Georg ... 132, 197, 441, 465, 744, 745
 automorphism 398, 420, 465, 713
 density theorem 441, 442, 443, 465
 endomorphism 398, 402, 404, 427, 428, 713, 746
 polynomial representation of the ~ ... 398, 408
 iterated ~ algorithm see iterated Frobenius
 Fröhlich, Albrecht 419, 745, 753
 Fuchssteiner, Benno 7, 20
 Fulton, William 568, 745
 functional decomposition 576, 580, 581
 fundamental
 lemma about gff 657, 658, 661
 period 368
 theorem
 of algebra 372, 711
 of calculus 647
 of number theory 377, 518
 on subresultants 327, 329, 332
 Fürer, Martin 222, 244, 245, 247, 745
 Galileo Galilei 502
 Gallagher, Patrick Ximenes 466, 745

- Galligo, André 618, 619, 739, 744
 Gallo, Giovanni 619, 745
 Gallot, Yves 534
 Galois, Évariste .. 198, 376, 418, 421, 724, 728, 745
 extension 466
 field see finite field
 group 373, 398, 421, 441–443, 465, 762
 theory 398, 414, 441, 713, 745
 ElGamal, Taher (طاهر الجمال) 580, 745
 cryptosystem 579, 580
 gamma function, Γ 659, 660, 670, 673
 Gao, Shuhong 6, 88, 407, 419–421, 580, 745
 Garey, Michael Randolph 509, 722, 745
 Garner, Harvey Louis 132, 745
 von zur Gathen, Désirée Dorothea Sarah Fatima .. 6,
 725
 von zur Gathen, Joachim Paul Rudolf .. 62, 88, 131,
 197–199, 279, 286, 287, 352, 405–407, 419–421,
 425, 461, 466, 467, 497, 498, 500, 580, 581, 669,
 670, 724, 736, 737, 745, 746, 751, 756
 Gaudry, Pierrick 542, 751
 Gauß, Carl Friedrich ... 3, 24, 62, 90, 131, 148, 197,
 247, 256, 358, 372, 373, 374, 376, 417–419, 421,
 444, 466, 497, 529, 533, 540, 586, 670, 699, 724,
 725, 727–729, 746–748
 bell curve 372
 lemma 141, 146, 147, 148, 190, 197, 433, 438
 period 76, 373, 580, 745
 theorem 149, 709
 Gaussian
 elimination 109–113, 131, 132, 137, 190, 340,
 373, 402, 403, 475, 612, 621, 627, 638, 666,
 715, 716, 724, 736, 764
 unimodular ~ 89
 integers 46, 61, 64, 707
 Gautschi, Walter 759
 gcd see greatest common divisor
 gcdE, shift gcd 657
 Geddes, Keith Oliver 6, 20, 202, 740
 Gegenbauer, Leopold Bernhard 62, 747
 Geil, Olav 7
 Gell-Mann, Murray 44, 726
 le Genre, Adrien Marie see Legendre
 generating
 function 697
 set 704, 714
 generator 704
 polynomial of a BCH code ... 211, 212, 214, 215,
 416
 Genovese, Giulio 7
 Gentleman, William Morven 247, 747
 Gentzen, Gerhard, system 678
 genus 568, 618
 Genuys, François 82, 747
 geometric
 elimination theory 175
 series 66, 122, 670
 sum 225, 229, 451, 653, 719
 theorem 612, 618
 geometry
 algebraic ~ 558, 568, 595
 non-Euclidean ~ 25, 373, 374
 of numbers 473
 projective ~ 567
 Georgetown i, 8
 Gergonne, Joseph Diez 465, 747
 Gerhard, Jürgen .. 279, 287, 461, 467, 470, 640, 641,
 669–671, 674, 737, 745–747
 Gerhardt, Carl Immanuel 754
 Gerhold, Stefan 7
 Gericke, Helmuth 764
 Gerstetter, Reinhold 725
 Gesellschaft für Informatik (GI) 21
 gff see greatest factorial factorization
 Gianni, Patrizia 619, 744, 751, 765
 Giesbrecht, Mark William 6, 353, 671, 737, 747, 751
 GIF 368
 Gilchrist, Bruce 744, 767
 Gill, John Thomas, III. 198, 747
 GIMPS 517
 Giovini, Alessandro 619, 747
 Giuliani, Charles-Antoine 7
 Giusti, Marc François 618, 619, 747
 Gleick, James 644, 729
 Glesser, Philippe 198, 757
 Gloor, Oliver 742, 747, 749
 Glover, Roderick Edward 6, 7
 GNU MP 279
 Gō, Nobuhiro 698, 747
 God (الله, deus, Dieu, Gott) 10, 28, 68, 208, 256,
 294, 734
 Gödel, Kurt 588
 Goethe, Johann Wolfgang von ... 140, 358, 726, 727
 Goldbach, Christian 90
 Goldberg, David Marc 7
 golden ratio, ϕ 54, 66, 89, 198
 Goldstine, Hermann Heine 286, 747
 Goldwasser, Shafira 735
 Gonnet Haas, Gaston Henry 20, 202, 740, 746
 Goodman, Jacob Eli 745, 749, 761
 Goodman, Rodney Michael Frederick 509, 747
 Gordan, Paul Albert 199, 332, 747
 Gordon, Daniel Martin 466, 579, 739, 747
 Gosper, Ralph William, Jr. . 641, 662, 670, 671, 675,
 747
 algorithm 641, 658, 662, 665, 670, 671, 736, 755,
 760
 -Petkovšek representation 675, 760
 Göttfert, Rainer 420, 747, 758, 759
 Gourdon, Xavier Richard 419, 744, 747, 759
 Grabmeier, Johannes .. 498, 736, 741, 747, 748, 760
 graded
 lexicographic order 596, 598
 reverse lexicographic order ... 596, 597, 598, 618
 Grafton, Sue Taylor 472, 728
 Graham, Ronald Lewis 509, 571, 669, 670, 717,
 720, 747, 759
 Gram, Jørgen Pedersen 496, 747
 -Schmidt
 orthogonal basis . 475, 476–478, 480, 481, 485,
 498
 orthogonalization (GSO) ... 475, 476, 478–480,
 485, 496, 498, 500, 717

- Gramian
 determinant 482, 484, 717
 matrix 475, 482, 688, 698, 717
 grammar 618
 Granville, Andrew Jam 198, 529, 532, 735, 748
 Graves-Morris, Peter 132, 736
 greatest
 common divisor, gcd 2, 24, 45, 46, 47, 48, 55–57,
 60, 73, 141, 194, 286, 326, 327, 333, 706, 707,
 708
 bivariate modular ~ 141, 162, 168, 203
 heuristic ~ .. 194–196, 202, 206, 317, 320, 333
 modular ~ see modular gcd
 monic ~ . 60, 146, 150–152, 156, 192, 194, 195
 multivariate ~ 190, 198, 202, 466, 496, 501
 normalized ~ 150, 152, 167
 of many integers 199
 of many polynomials 141, 176, 177
 of primitive polynomials 152
 shift ~ 657
 factorial factorization, gff 653, 654, 655–658,
 661, 670, 673
 fundamental lemma about ~ 657, 658, 661
 Gregorian calendar 84, 91
 Pope Gregory XIII 84
 Grigoriev, Dimitrii Yur'evich (Григорьев
 Дмитрий Юрьевич) . 6, 498, 619, 740, 748
 Grimself, Sebastian 7
 Gröbner, Wolfgang Anton Maria 591, 765
 basis ... 3, 15, 101, 175, 604, 591–621, 679, 681,
 694, 697, 736, 738, 740–742, 744, 750, 753,
 756, 757
 minimal ~ 611, 620, 621
 reduced ~ ... 611, 613, 614, 616–618, 620, 621,
 679, 681, 694, 695
 proof system 677, 679, 697, 698
 de Groote, Hans Friedrich 352, 748
 Grotefeld, Andreas Friedrich Wilhelm 279, 286,
 292, 727, 762
 Grötschel, Martin 496, 748, 759
 group 703, 704, 706, 712–715
 additive ~ 250, 578, 703, 713
 commutative ~ 342, 349, 704, 705, 713
 cyclic ~ 250, 251, 349, 422, 578, 704, 713
 factor ~ 704
 Galois ~ 373, 398, 421, 441–443, 465, 762
 homomorphism 554, 704
 isomorphism 105, 704
 Klein ~ 442
 of units 63, 74, 150, 518, 707, 712, 768
 order of a ~ 704
 symmetric ~ 136, 442, 465, 705
 Grund, Roland 698, 736
 Guibas, Leonidas Ioannis (Leo John) 205, 748
 Guillou, Louis Claude 758
 Guilloud, Jean 82
 Gulliver, Lemuel 729
 Gustavson, Fred Gehrung 332, 738
 Guy, Richard Kenneth 568, 569, 748

 H_n , harmonic number 466, 645, 650, 651, 652
 Habicht, Walter 199, 748, 755
 Hadamard, Jacques Salomon 496, 533, 748
 inequality 111, 136, 157, 182, 183, 474, 477
 al-Ḥajjāj bin Yūsuf bin Maṭar
 (الحجاج بن يوسف بن مطر) 25
 Haken, Armin 678, 748
 Halmos, Paul Richard 533, 748
 Halton, John Henry 198, 748
 Hamilton, Sir William Rowan 341, 373, 716
 Hamming, Richard Wesley 308, 748
 weight 75, 210
 Hammurabi (Hammurabi) 766
 Hankel, Hermann 332, 353, 376, 728
 hard decision problem 722
 von Hardenberg see Novalis
 hardware arithmetic 279, 283
 Hardy, Godfrey Harold ... 26, 44, 62, 140, 421, 532,
 534, 535, 572, 726, 728, 748
 harmonic 361, 362
 number, H_n 466, 645, 650, 651, 652
 series 651
 Harris, Mitchell Alan (Mitch) 7
 Hart, William Bruce 497, 748
 Hartlieb, Silke 6, 466, 746
 Hartshorne, Robin 568, 748
 Caliph Ḥārūn al-Rashīd (هارون الرشيد) 25
 hash function 578
 hashing 88, 198
 Haskell, Mellen Woodman 332, 748
 Hasse, Helmut 568, 748
 bound 508, 562, 564, 565, 740
 -Teichmüller derivative 290
 Håstad, Johan Torkel 6, 505, 580, 744, 748
 Havel, Timothy Franklin 698, 748
 Hazebroek, P. 698, 748
 Hearn, Anthony Clem 20
 Heath, Sir Thomas Little 24, 25, 748
 Hecke, Erich 765
 Heegaard, Poul 728
 Hehl, Friedrich Wilhelm 736, 748, 760
 Heiberg, Johan Ludwig 735
 Heideman, Michael Thomas 247, 748
 Heilbronn, Ernst 726
 Heilbronn, Hans 61, 748
 Heintz, Joos 497, 618, 619, 739, 747, 749
 Hellman, Martin Edward ... 503, 504, 509, 573, 575,
 576, 578–582, 742, 756, 757, 763
 Hendriks, Peter Anne 671, 749
 Henry, Alan Sorley 727, 741
 Henry, Charles 744
 Hensel, Kurt Wilhelm Sebastian . 444, 466, 745, 749,
 752, 753, 767
 lemma 447, 449
 lifting 3, 100, 101, 198, 257, 271, 373, 444,
 433–471, 488, 489, 491, 492, 496
 multifactor ~ 450
 step 445, 447, 448, 450, 469
 Hermann, Grete 616, 749
 Hermite, Charles 626, 640, 747, 749
 interpolation 113, 114, 115, 118, 137
 rational ~ 118
 normal form 89, 352, 498, 499
 reduction 625, 626, 627, 631, 640, 642, 673

- Herzog, Dieter 6, 7
 Hessenberg, Gerhard, form 338
 heuristic gcd 194–196, [202](#), 206, [317](#), [320](#), 333
 Higham, Nicholas John 337, 749
 Hilbert, David 3, 24, 25, 89, 90, 140, 373, 419, 495,
 572, [586](#), 587, 588, 591, 616, 618, 678, 725, 726,
 728, 742, 749, 761
 basis theorem 586, 601, [604](#), 605, 606, 618
 class field theory 586
 function 586, 618
 irreducibility theorem 495, 496, 498, 586, 750
 Nullstellensatz . 586, 595, [617](#), 618, 621, 736, 761
 problems 587
 tenth problem 89, 756
 Hilbertian field 498
 Hirn, Andreas 7
 Hironaka, Heisuke 591, 749
 Hocquenghem, Alexis 215, 749, 756
 van Hoeij, Marinus (Mark) Hubertus Franciscus . 7,
 497, 671, 735, 748, 749
 van der Hoeven, Joris 469, 749
 Hoffman, Christoph M. 618, 749
 Hoffman, Dean Gunnar 215, 749
 Hohberger, Reinhard 698, 736
 Holland, Brian 728
 Holland, Eddie 728
 Holliday, Francis 764
 Holmes, Thomas Sherlock Scott 702, 729
 Homer (“Ὅμηρος”) 294
 homogeneous ideal 616
 homomorphism [714](#), 715
 image of a \sim , im [704](#), [706](#), [714](#)
 kernel of a \sim , ker ... 105, 349, 383, 401, [704](#), [706](#),
 709, [714](#)
 of algebras 231
 of groups 554, [704](#)
 of rings ... 104, 107, 133, 295, 302, [705](#), 706, 709
 theorem
 for groups 384, [704](#)
 for modules 349
 for rings 105, [706](#), 711
 Hoover, H. James 6
 Hopcroft, John Edward 286, 332, 352, 735, 738
 Horn, Alfred, clause 678, 679
 Horner, William George, rule ... 88, [101](#), 133, 235,
 270, 289, 296, 306, 338, 346, 348
 Horowitz, Ellis 306, 627, 749
 Horwitz, Jeremy Aaron 567, 749
 Huang, Ming-Deh Alfred 421, 498, 749, 750
 Huang, Xiaohan 353, 405, 420, 750
 Huffman, David Albert 307, 368, 750
 code [307](#), 365–368
 tree [307](#), 308
 average depth of a \sim 308
 Hugenius, Christianus see Huygens, Christiaan
 Hume, David 68, 726
 Hungerford, Thomas William 703, 750
 Hurwitz, Adolf 90, 750
 Huygens (Hugenius, Huyghens), Christiaan . 89, 750
 Huynh, Thiet-Dung 618, 750
 hybrid algorithm . 248, 252, [280](#), 281, 282, 411, 492
 hyperexponential 623, [633](#), 635–637, 639, 641
 integration 3, 632, [633](#), 634, [637](#), 671
 hypergeometric . . 645, [659](#), 660, 665, 667, 669, 674,
 675, 683
 distribution 682
 function 659
 identity 697
 series 373, [670](#)
 summation . 3, 641, [660](#), [665](#), 658–669, 671, 674,
 683, 685
 $I(\cdot, \cdot)$, number of irreducible polynomials 409
 \Im , imaginary part 768
 Iamblichus (Ἰάμβλιχος) of Chalcis 531
 IBM 337
 IDCT, Inverse Discrete Cosine Transform . [363](#), 366,
 369
 ideal 71, 681, [705](#), 706, 709, 710, 716, 768
 binomial \sim 616, [681](#), 697
 containment testing 610
 coset of an \sim [706](#)
 equality testing 610
 finitely generated \sim [593](#), 603, 604, 618
 homogeneous \sim 616
 membership ... [594](#), 600, 601, 605, 610, 616–618
 monomial \sim [601](#), 602, 603, 620
 of polynomials 498, 591–621, 677
 right \sim [705](#)
 variety of an \sim [593](#), 594, 595, 614, 617, 618
 image
 compression 3, 11, 359, [363](#), 364, 368
 of a homomorphism, im [704](#), [706](#), [714](#)
 processing 359
 imaginary quadratic field 707
 Imirzian, Gregory Manug 498, 744
 Immerman, Neil 760
 Impagliazzo, Russell Graham ... 679, 697, 736, 739,
 741
 implicit
 function theorem 618
 linear algebra [352](#)
 implicitization 613, [614](#)
 impulse response sequence [349](#)
 indefinite summation [646](#), 683
 independent
 events [718](#)
 random variables [718](#), 719
 inference rule [677](#), [678](#), 679
 Ingemarsson, Ingemar 747, 760
 injective [704](#), 714
 inner product . 12, 15, 348, 353, [473](#), 485, 498, 685,
 687, 689, 698, [717](#), 768
 insertion sort 221
 instance of a decision problem [721](#)
 instantaneous code [307](#)
 integer
 addition [31](#)
 factorization see factorization
 multiplication see multiplication
 multiprecision \sim . . [29](#), 30–32, 34, 37, 41, 82, 283,
 286
 p -adic \sim 270, 275, 449, 466
 partition 441, 442, [468](#)

- representation of $\sim s$ 29
 root 271, 460
 integral 369, 570, 623, 624, 625, 627, 640, 642, 647, 685
 domain 706, 707–711
 logarithmic \sim 533
 root 392, 393, 635, 641
 integration 4, 20, 101, 199, 264, 395, 623, 625, 631, 640, 647, 650, 653
 Almkvist and Zeilberger \sim 632, 637, 643
 by parts 623, 624, 626, 673
 hyperexponential \sim 3, 632, 633, 634, 637, 671
 Lazard-Rioboo-Trager \sim 627, 630, 631, 640, 758
 of rational functions 3, 626, 630, 632, 640
 Rothstein and Trager \sim . see Rothstein and Trager
 Intel 83
 intermediate expression swell 97, 145, 616
 internal node in a mobile 306, 308
 internet 18, 83, 517, 531, 575
 interpolation ... 18, 19, 97–139, 168, 169, 190, 231, 280, 281, 295, 295–310, 324, 333, 352, 496, 498, 681
 Cauchy \sim 118, 121, 137, 138, 190, 325, 331
 fast \sim 231, 301, 295–310, 331
 formula 134
 Hermite \sim 113, 114, 115, 118, 137
 rational \sim 118
 Lagrange \sim 18, 100, 101, 102, 107, 118, 134, 299, 303, 739
 map 103, 232
 Newton \sim 103, 134, 135, 671
 of bivariate polynomials 134
 of sparse polynomials 498
 polynomial 18, 97–139, 249, 295–310
 rational \sim 101, 118, 119, 120, 132
 intersecting plane curves ... 141, 171, 172, 175, 203
 invariant ring 618
 inversion
 formula 361, 362–364, 369
 Möbius \sim 410, 413, 429
 modular \sim see modular inversion
 Newton \sim see Newton inversion
 of a matrix 337
 p -adic \sim 262
 Iohvidov, Iosif Semenovich (Иохвидов Иосиф Семенович) 334, 727
 irreducibility
 Hilbert \sim theorem 495, 496, 498, 586, 750
 test 406, 408, 461, 497
 over finite fields 407
 irreducible 149, 707, 708, 709, 713
 factor 381, 385, 387, 389, 392, 400, 405, 411, 416, 424
 factorization ... 149, 150, 377, 394, 397, 404, 414, 419, 422, 433, 435, 441, 453, 462, 468, 469, 471, 630, 635
 polynomial 73, 377, 406, 408–412, 414, 421, 710–712
 construction of an \sim 377, 406, 410
 isomorphic 704, 705, 714, 768
 isomorphism 231, 714
 of groups 105, 704
 of rings 705
 ISSAC 21
 iterated Frobenius algorithm 76, 398, 399, 400, 404, 405, 407, 408, 420, 427
 jackpot 161
 Jacob von Coburg (Koburgk), Simon 61
 Jacobi, Carl Gustav Jacob ... 91, 132, 197, 373, 586, 644, 750
 symbol 508, 529, 533, 537, 554, 757, 763
 Jacobian 450, 470, 621
 Jebelean, Tudor 286, 750
 Jeffrey, David John 751
 Jenks, Richard Dimick 20, 750, 757, 765, 767
 Jensen, Christian Albrecht 725
 Jin, Xiaofan 767
 Johnson, David Stiffler 509, 722, 724, 745, 750
 Johnson, Don Herrick 247, 748
 Jones, William 90, 750
 Jordan, Károly (Charles) 669, 750
 Journal
 of Symbolic Computation 21, 41, 618
 of the ACM 21
 SIAM \sim on Computing 21
 JPEG 368
 Julia, Gaston Maurice 276
 set 273, 276
 Julian calendar 83, 84, 91
 Jung, Dirk 7
 Jürgens, Hartmut 278, 760
 Kajler, Norbert 21, 750
 Kalorkoti, Kyriakos (Καλορκότη, Κυριάκος) ... 7, 286, 750
 Kaltofen, Erich Leo 6, 7, 20, 41, 132, 199, 245, 247, 340, 351, 353, 401, 404–407, 419, 420, 465, 495–498, 641, 739, 741, 742, 744, 746, 747, 750, 751
 Kaminski, Michael 353, 751
 Kanada, Yasumasa 82, 247, 751
 Kanellakis, Paris Christos (Κανελλάκης, Πάρις Χρίστος), Award 533
 Kannan, Ravindran 496, 505, 744, 751
 Kanno, Masaaki 7
 Kant, Immanuel 208, 586, 726
 Kao, Ming-Yang 199, 740
 Karatsuba, Anatoliĭ Alekseevich (Карацуба Анатолий Алексеевич) 223, 245, 247, 750, 751
 algorithm 193, 223, 221–254, 278–286, 335
 circuit 224
 Karp, Alan Hersh 286, 751
 Karp, Richard Manning 509, 722, 751
 Karpinski, Marek Mieczysław 6, 198, 498, 741, 746, 748
 Karr, Michael 671, 751
 al-Kāshī, Ghiyāth al-Dīn Jamshīd bin Mas'ūd bin Maḥmūd (غياث الدين جمشيد بن مسعود بن محمود) (الكاشي) 0, 82, 88, 90, 286, 725, 756
 Kasner, Edward 729
 Kayal, Neeraj 517, 543, 735

- Kedlaya, Kiran Sridhara 339, 405, 407, 408, 420, 751
- Keller, Carsten 6
- Keller, Wilfrid 6
- Keller-Gehrig, Walter 352, 751
- Kelley, Colin 8
- Kempfert, Horst 417, 466, 751
- Kepler, Johannes 622
- Kerber, Adalbert 7, 698, 736
- kernel of a homomorphism, ker 105, 349, 383, 401, 704, 706, 709, 714
- Kerschensteiner, Georg 747
- key
 Diffie-Hellman ~ exchange . . . see Diffie-Hellman
 in a cryptosystem . . . 16, 18, 505, 509, 573, 573–582
 private ~ 17, 504, 509, 575, 576–579, 582
 public ~ 17, 503, 509, 575, 577–579, 582
 tonal ~ 85, 86
- al-Khwārizmī, Abū Ja'far Muḥammad bin Mūsā
 (أبو جعفر محمد بن موسى الخوارزمي) 68, 88, 90, 256, 286, 726, 727, 741, 744, 762
- Kipling, Joseph Rudyard 644, 729
- Kirchhoff, Gustav Robert 728
- Kirkpatrick, David Galer 353, 751
- Kiyek, Karl-Heinz 7
- Klapper, Andrew Manoch 7
- Klein, Felix 25, 358, 586, 727
 group 442
- Kleinjung, Thorsten 542, 751
- Klinger, Leslie Stuart 6
- knapsack
 cryptosystem 503, 509
 problem 503
- Kneller, Sir Godfrey, Baronet 725
- Knopfmacher, Arnold 419, 752
- Knopfmacher, John Peter Louis 419, 752
- Knörrer, Horst 568, 738
- Knuth, Donald Ervin 7, 8, 25, 40, 61, 62, 88, 90, 247, 286, 308, 332, 417, 505, 531, 567, 571, 669, 670, 717, 720, 724, 747, 752
- Koblitz, Neal 531, 568, 580, 752
- von Koch, Niels Fabian Helge 287, 752
 snowflake 278, 287
- Koepf, Wolfram 670, 671, 697, 752
- Kohel, David Russell 749
- Kolaitis, Phokion-Gerasimos (Κολαίτης, Φωκίων-Γεράσιμος) 760
- Kollár, János 618, 735, 752
- Kollberg, Lennart 516
- Kolmogorov, Andrei Nikolaevich (Колмогоров Андрей Николаевич) 247
- Kondo, Shigero 82, 90, 767
- Koornwinder, Tom Hendrik 7
- Körner, Heiko 7
- Korselt, Alwin Reinhold 532, 752
 criterion 532
- Kotsireas, Ilias Sotirios (Κοτσιρέας, Ήλιος Σωτηρίου) 7
- Kovalevskaya, Sof'ya Vasil'evna (Sonya Kowalewski, Ковалевская Софья Васильевна) 726
- Koy, Henrik 497, 752
- Kozen, Dexter 576, 581, 619, 736, 752
- Kraft, Leon Gordon, Jr. 307, 752
- Kraitchik, Maurice Borisovitch 376, 540, 567, 727, 728, 752
- Krajíček, Jan 697, 736, 739, 752
- Krandick, Werner Johannes 6, 7
- Kronecker, Leopold 28, 132, 137, 197, 247, 353, 465, 725, 742, 752
 substitution 245, 246, 254, 494, 501
- Krummel, Volker 7
- Kruppa, Alexander 542, 751
- Krylov, Alekseĭ Nikolaevich (Крылов Алексей Николаевич) 353, 753
 subspace 341, 346, 347, 355
- Ku, Yu Hsui 131, 753
- Küchlin, Wolfgang Wilhelm 736, 742, 746, 748–751, 760, 761, 765
- Kuhnert, Martina Ariane 7, 8
- Kühnle, Klaus 616, 617, 753
- Kummer, Ernst Eduard 514
- Kunerle, Jens 7
- Kung, Hsiang Tseng 286, 353, 354, 738, 753
- Kurowski, Scott 517
- Kvashenko, Kirill Yur'evich (Квашенко Кирилл Юрьевич) 641, 735
- Lafon, Jean-Claude 671, 753
- Lagally, Klaus 8
- Lagarias, Jeffrey Clarke 443, 505–507, 509, 580, 744, 753
- Lagrange (la Grange), Joseph Louis, Comte de 90, 91, 131, 419, 590, 728, 753
 interpolant 101, 102, 105, 107, 131, 133, 246, 249, 427
 interpolation 18, 100, 101, 102, 107, 118, 134, 299, 303, 739
 multiplier 621
 theorem 89, 212, 412, 415, 518, 519, 537, 538, 562, 704, 712, 714
- Lakshman, Yagati Narayana 498, 618, 744, 745, 751, 753
- Lalande, Joseph-Jérôme Lefrançais de 728
- LaMacchia, Brian A. 353, 753
- λ , Carmichael function 535
- λ , length of an integer 30, 53, 142
- Lambe, Larry Albert 21, 753
- Lambert, Johann Heinrich 82, 753
- Lamé, Gabriel 61, 753
 theorem 61, 66
- Lamport, Leslie B. 8
- Lanczos, Cornelius 353, 754
 algorithm 353, 741, 742, 758
- Landau, Edmund Georg Hermann 165, 586, 724, 748, 752, 754
 inequality 165, 166
- Landau, Susan Eva 576, 581, 752
- Landrock, Peter 532, 742
- Landry, Fortuné 542, 754
- Lang, Serge 498, 754
- Lange, Tanja 421, 754
- Laplace (la Place), Pierre Simon, Marquis de 294, 432, 724, 725, 727, 728, 754
 expansion 159, 716

- Larson, Richard Gustav 532, 735
 Las Vegas
 algorithm [161](#), 198, 402, 470, 471, 724
 Turing machine [722](#)
 lattice ... 3, 286, 434, [473](#), 473–501, 504, 506–508,
 573, 712
 dimension of a \sim 474, 480
 norm of a \sim [473](#), 474
 Laue, Reinhard 698, 736
 Lauer, Daniel (Daniel Reischert) .. 7, 198, 279, 332,
 466, 754, 761
 Laurent, Pierre Alphonse, series 91, 94, 768
 law of quadratic reciprocity 372, 529, 537, 586
 Lawrence, Thomas Edward 140, 726
 Lazard, Daniel 619, 640, 744, 754, 758
 –Rioboo-Trager integration ... 627, [630](#), 631, 640,
 758
 lc, leading coefficient [32](#), 38, [597](#), [708](#), [709](#)
 lcm, least common multiple [46](#), 57
 le Carré, John see Carré
 leading
 coefficient, lc [32](#), 38, [597](#), [708](#), [709](#)
 digit [30](#), 40
 monomial, lm [598](#)
 principal submatrix 204, 351
 term, lt 595, [598](#), 599, 600, 604, 606–608
 unit, lu [56](#)
 leaf of a mobile [306](#), 307, 308
 leap day [84](#)
 least
 absolute remainder Euclidean Algorithm 66
 absolute residue 72, [550](#)
 common multiple, lcm [46](#), 57
 Lebesgue (Le Besgue), Victor Amédée ... 533, 754
 Lee, King 2, 337, 736
 Lee, Lin-Nan 509, 755
 van Leeuwen, Jan 750, 754, 764, 765
 Legendre (le Gendre), Adrien Marie .. 198, 372, 418,
 420, 466, 468, 516, 533, 569, 728, 754, 766
 symbol [529](#), 537, 562
 Lehmann, Daniel Jean 537, 754
 primality test [537](#), 538
 Lehmer, Derrick Henry 332, 530, 542, 569, 738, 754
 Leibniz, Gottfried Wilhelm, Freiherr von . 26, 88, 89,
 96, 197, 219, 294, 512, 513, 531, 622, 640, 726,
 754, 756
 rule [266](#), 290, 425, 623, 647
 Leighton, Ralph 727, 728
 Leiserson, Charles Eric 41, 368, 741
 Lemmermeyer, Franz 724, 754
 length
 of a code [209](#), 210–212
 of an integer, λ [30](#), 53, 142
 Lenstra, Arjen Klaas .. 279, 465, 474, 475, 497, 506,
 531, 534, 542, 569, 741, 742, 751, 754, 755
 Lenstra, Hendrik Willem, Jr. 419, 421, 441, 474,
 475, 497, 506, 531–534, 541, 542, 557, 558, 563,
 565, 568, 569, 724, 735, 736, 754, 755, 760, 764
 elliptic curve factoring method .. see elliptic curve
 Leonard, Douglas Alan 215, 749
 Levelt, Antonius Henricus Maria (Ton) . 6, 698, 735,
 742, 755
 Levin, Leonid Anatol'evich (Левин Леонид
 Анатольевич) 724, 755
 Lewin, Daniel 199, 755
 lexicographic order ... [596](#), 598, 608, 615, 694, 695
 Leykin, Anton (Лейкін, Антон Геннадійович)
 748
 Leyland, Paul 279
 Li, Gang 352, 740
 Lickteig, Thomas Michael 184, 199, 332, 755
 LIDIA 20, 279
 Lidl, Rudolf 421, 711, 755
 Lie, Marius Sophus 622, 728
 von Lindemann, Carl Louis Ferdinand 82, 755
 Lindner, Charles Curt 215, 749
 line at infinity 568
 linear
 algebra ... 3, 4, 21, 109, 175, 179, 335–356, 373,
 401, 420, 475, 557, 703, [713](#), 714, 715
 black box \sim 335, [340](#), 346, 352, 404, 407
 explicit \sim 335, 352, 407
 sparse \sim 352
 code [209](#), 215
 combination map 153
 congruential generator 503, 505, 574
 Diophantine equation 69, [77](#), 79, 89, 93
 equation ... 1, 3, 66, 129, 175, 197, 340, 346, 685
 feedback shift register [341](#), 342
 map 103, 229, 349, 354, [714](#)
 programming 473
 softly \sim [721](#)
 subspace 209, 210, 280, [714](#), 715, 768
 system of \sim equations 1, 120, 131, 136, 183, 214,
 335–356, 460, 485, 552, 621, 638, 664–666,
 [715](#), 716
 sparse \sim 325, 556
 linearly
 convergent Newton iteration [291](#)
 dependent [714](#), 717
 independent [714](#), 715
 recurrent sequence .. 340, [341](#), 343–347, 349, 353,
 355
 van Lint, Jacobus Hendricus 215, 755
 Liouville, Joseph . 472, 623, 640, 728, 729, 755, 764,
 796
 LIP 279
 Lipson, John David 6, 247, 306, 755
 Lipton, Richard Jay 88, 198, 742
 Lisoněk, Petr 670, 671, 755
 Little, John Brittain 614, 617, 618, 741
 Liu, Zhuojun 376, 727
 LLL algorithm see basis reduction algorithm
 Lloyd, Daniel Boone, Jr. 419, 755
 Lloyd, Daniel Bruce 7
 Lloyd, Stuart Phinney 421, 763
 lm, leading monomial [598](#)
 ln, natural logarithm [768](#)
 Lobachevskii, Nikolai Ivanovich (Лобачевский
 Николай Иванович) 374
 Lobo, Austin 353, 404, 405, 407, 747, 751
 local area network 18
 Locke, John 208, 726
 log, binary logarithm [768](#)

- logarithmic 625
 derivative 633, 635, 636, 639, 641
 integral 533
 part 625, 642
 Lombardi, Henri 199, 755
 Loos, Rüdiger Georg Konrad 466, 750, 753, 755,
 757
 Lotz, Martin Andreas 7
 Lovász, László ... 474, 475, 496, 497, 506, 748, 754,
 759
 Lovelace, Augusta Ada Byron King, Countess of 10,
 725
 Loxton, John Harold 755
 LR-decomposition 337
 lt, leading term ... 595, 598, 599, 600, 604, 606–608
 lu, leading unit 56
 Lu, Shyue-Ching 509, 755
 Luby, Michael George 6, 215, 735
 Lucas, François Édouard Anatole 530, 754, 756
 -Lehmer test 530, 754
 sequence 66
 Lucasian Professor 218
 Lucchesi, Cláudio Leonardo 759
 Luckey, Paul 90, 725, 756
 Luckhardt, Emil 358, 727
 Lücking, Thomas 6, 7, 197, 199, 746
 Ludlum, Robert (Jonathan Ryder) 10, 725
 Luks, Eugene Michael 8, 724, 736
 Lambert, Robert 738
 lunar calendar 83
 van de Lune, Jan 533, 756
 Lüneburg, Heinz 7
 lunisolar calendar 83
 ΛΥΩ (Lambda–Upsilon–Omega) 697
- M, multiplication time 244, 245, 247, 254, 257, 381
 Ma, Keju 6, 62, 756
 Mabbott, Thomas Ollive 728
 MACAULAY 619
 Macaulay, Francis Sowerby 197, 590, 619, 728, 729,
 756, 796
 Mach, Ernst 220, 727
 Machin, John 82
 machine cycle 31, 42, 99
 Mack, Dieter 642, 756
 Maclaurin, Colin 197, 198, 286, 756
 MACSYMA 20
 MacWilliams, Florence Jessie 215, 756
 MAGMA 20
 Mahnke, Dietrich 88, 531, 756
 Makowsky, János 6
 Man, Yiu-Kwong 671, 756
 Manasse, Mark Steven 531, 534, 569, 754, 755
 Mandelbrot, Benoît Baruch 278, 756
 Manin, Yuriĭ Ivanovich (Манин Юрий
 Иванович) 568, 740, 756
 MAPLE i, 8, 20, 21, 65, 82, 143, 173, 181, 192, 201,
 227, 534, 621, 632, 679, 686–697
 Markov, Andreĭ Andreevich (Марков Андрей
 Андреевич) 740
 Markstein, Peter 286, 751
 Massey, James Lee 215, 325, 742, 756
- MATHEMATICA 20
 Mathematics of Computation 21
 Matiyasevich, Yuriĭ Vladimirovich (Матиясевич
 Юрий Владимирович) 89, 640, 756
 Matooane, Mantsika 7
 matrix 337, 714, 768
 Bézout ~ 197, 201
 coefficient ~ 715
 evaluation 340, 346, 348, 352, 353
 Gramian ~ 475, 482, 688, 698, 717
 inversion 337
 multiplication .. 43, 335, 337–339, 411, 715, 720
 exponent 337
 fast ~ 336, 337, 340
 feasible ~ exponent 337, 338, 352
 rectangular ~ 353
 nonsingular ~ ... 89, 109, 116, 212, 213, 346, 351,
 353, 355, 477, 498, 621, 688, 715, 716
 normal form 352
 permutation ~ 483, 715, 716
 Petr-Berlekamp ~ see Petr-Berlekamp matrix
 rank 698, 714, 715
 singular ~ 103, 204, 347, 351, 355, 688, 715, 716
 sparse ~ 335, 340
 Sylvester ~ see Sylvester matrix
 Toeplitz ~ 202, 332, 335, 353, 738
 triangular ~ 329, 638, 666, 716
 unimodular ~ 89, 498, 499
 Vandermonde ~, VDM . see Vandermonde matrix
 Mattson, Harold F. (Skip), Jr. 746
 Maurer, Ulrich Martin (Ueli) 580, 756
 maximum
 likelihood decoding 210
 norm, max-norm, $\|\cdot\|_\infty$.. 158, 166, 183, 191, 202,
 205, 206, 261, 327, 493, 500, 675, 717, 768
 Mayor, Richard 726
 Mayr, Ernst Wilhelm 6, 616–618, 697, 753, 756
 McAuley, Anthony Joseph 509, 747
 McCormack, Thomas Joseph 727
 McCurley, Kevin Snow 580, 757
 McEliece, Robert James 215, 419, 737, 757
 McInnes, James L. 6
 McKenzie, Pierre 6
 mdeg, multidegree of a polynomial 597, 598
 mean value 718
 median in a triangle 592, 593
 MEGA 21
 Mellencamp, John Cougar 208, 726
 Menabrea, Luigi Federico 725
 Mendoza, Olga Lisvet 8
 Menezes, Alfred John 580, 757
 Meng, Sun 6
 mergesort 221
 Merkle, Ralph Charles 503, 504, 509, 576, 757, 763
 Mersenne, Marin 86, 512, 669, 744, 757
 number 251, 517, 530, 534, 754, 766
 prime 517, 530, 531, 534, 535
 Mertens, Franz Carl Joseph 508, 757
 conjecture 503, 508, 759
 method of undetermined coefficients . 627, 638, 639,
 641, 667
 Metropolis, Nicholas 198, 757

- Metzner, Torsten 7
 Meyer, Albert Ronald da Silva 616–618, 756
 Meyer auf der Heide, Friedhelm 744
 Meyer Eikenberry, Shawna 533, 757
 Meyn, Helmut 6–8
 Micali, Silvio 750
 Mierendorff, Eva 7
 Mignotte, Maurice 146, 198, 421, 757
 bound ... 141, 164, 166, 167, 171, 184, 194, 196,
 198, 434, 436, 438, 455, 470, 488, 490, 492
 Mihăilescu, Preda 7
 Mikeladze, Sh. E. 132
 millenium bug 84
 Miller, Gary Lee 532, 533, 535, 736, 755, 757
 Miller, Raymond Edward 744, 751
 Miller, Victor Saul 580, 757
 minimal
 distance of a code 210, 211–213, 215
 Euclidean function 62, 63
 Gröbner basis 611, 620, 621
 polynomial
 of a matrix 343, 346, 355, 404, 716
 of a sequence 343, 344–351, 354–356, 404, 407
 of an algebraic element ... 152, 175, 203, 210,
 211, 343, 354, 415–417, 663, 710, 711
 Minkowski, Hermann 473, 496, 586, 757
 Mishra, Bhubaneswar (Bud) 619, 745
 Mitchell, Joan Laverne 368, 760
 Mittag-Leffler, Gustav Magnus (Gösta) 726
 mixed-radix representation 132, 134
 mobile
 stochastic ~ 306, 307, 308
 Möbius, August Ferdinand
 function, μ 410, 429, 508
 inversion 410, 413, 429
 mod, congruent modulo 69, 706
 mod, residue class 71, 72, 398, 706
 modular
 algorithm .. 3, 19, 97, 97–139, 152, 161, 183, 192,
 339, 408, 433, 444, 505, 517, 523, 525, 526
 big prime ~ .. 97, 100, 152, 161, 289, 444, 460,
 527
 prime power ~ 97, 99, 100, 198, 271, 433, 460,
 470, 528, 536
 small primes ~ 97, 98–100, 112, 137, 247, 310,
 444, 460, 467, 470, 471, 528, 536
 arithmetic 69, 70, 71, 132, 282, 289, 709
 composition ... 338, 339, 354, 356, 407, 408, 427
 fast ~ 338, 339, 405
 determinant 109, 113, 132, 525
 big prime ~ 110, 113, 168, 460, 526
 small primes ~ ... 112, 113, 136, 168, 189, 460,
 526, 528, 536, 537
 EEA
 big prime ~ 189, 190, 195, 206
 bivariate ~ 189
 small primes ~ ... 188, 189, 190, 195, 332, 460,
 526, 528, 537
 exponentiation 75
 factorization 436, 453, 458, 489
 big prime ~ . 433, 435, 436, 467, 526, 528, 529
 prime power ~ ... 435, 453, 457, 466, 467, 526,
 528, 529
 gcd . 141, 146, 152, 158, 161, 163, 164, 190, 196,
 198, 202, 313, 681
 big prime ~ . 162, 166, 168, 169, 171, 193–196,
 206, 411, 460, 526, 529
 bivariate ~ 141, 162, 168, 203
 small primes ~ ... 168, 169, 170, 171, 194–196,
 203, 206, 460, 526, 528
 inversion 69, 73, 76, 77, 111, 115, 124, 138, 163,
 263, 265, 268
 multiplication .. 73, 243, 262, 283, 460, 461, 536
 module 342, 349, 354, 500
 cyclic ~ 349, 350
 \mathbb{Z} -~ 349, 473
 Moenck, Robert Thomas ... 247, 286, 306, 332, 421,
 671, 673, 737, 757
 de Moivre, Abraham 353
 Möller, Hans Michael 199, 618, 757
 monic
 Euclidean Algorithm . 57, 62, 184, 186, 187, 192,
 196, 197, 199, 630, 631
 polynomial 32, 35, 40, 56, 59, 60, 708, 710
 Monien, Burkhard 744, 756
 Monier, Louis Marcel Gino 532, 533, 757
 monomial .. 591, 596, 597, 601, 602, 606, 611, 620,
 709
 ideal 601, 602, 603, 620
 leading ~, lm 598
 order 595, 596, 597–599, 603–605, 610, 620, 621
 Montaigne, Michel Eysquem, Seigneur de . 699, 729
 Monte Carlo
 algorithm 161, 198, 428, 724
 Turing machine
 one-sided ~ 722
 two-sided ~ 721
 Montgomery, Peter Lawrence ... 280, 287, 288, 308,
 353, 542, 569, 741, 751, 757, 758
 Moore, Eliakim Hastings 88, 758
 Mora, Ferdinando Teo 618, 619, 739, 744, 746, 747,
 757
 Morain, François 6
 Moreno-Socías, Guillermo 8
 Morenz, Robert 6
 De Morgan, Augustus 44, 68, 96, 622, 726, 729
 Morgenstern, Jacques 619, 744
 Moritz, Robert Edouard 729, 758
 Morrison, Michael Allan 541, 542, 568, 758
 Moses, Joel 20, 198, 466, 758
 Motwani, Rajeev 88, 198, 758
 Moura, Arnaldo Vieira 759
 Mourrain, Bernard 698, 743
 μ , Möbius function 410, 429, 508
 Mulders, Thom 199, 501, 640, 758
 Mullen, Gary Lee 745, 758, 766
 Müller, Daniel 7
 Müller, Dirk 6
 Müller, Eva-Maria 7
 Müller, Olaf 6–8, 461, 737
 Mullin, Ronald Cleveland 88, 758
 multidegree of a polynomial, mdeg 597, 598
 multifactor Hensel lifting 450

- multiple polynomial quadratic sieve 567
- multiplication
 by scalars 346, 348, 351, 713, 714
 Cantor \sim 281, 282, 287
 FFT \sim see Fast Fourier Transform
 matrix \sim 43, 335, 337–339, 411, 715, 720
 exponent 337
 modular \sim 73, 243, 262, 283, 460, 461, 536
 of integers . 37, 227, 243, 247, 283, 284, 335, 337, 460
 fast \sim 221–254
 of polynomials ... 35, 36, 39, 221–254, 280–282, 284, 285, 319, 323, 335, 460
 classical \sim 34
 fast \sim 221–254
 Schönhage and Strassen \sim see Schönhage
 time, M 244, 245, 247, 254, 257, 381
 multiplicative group ... 93, 105, 133, 211, 212, 250, 280, 384, 535, 578, 580, 703, 704, 713
 multiplicity . 200, 389–392, 394, 419, 440, 460, 470, 552, 560, 630, 656, 692, 711
 multipoint evaluation see evaluation
 multiprecision integer 29, 30–32, 34, 37, 41, 82, 283, 286
- multivariate see also bivariate
 division with remainder .. 595, 598, 599, 600, 604, 605
 factorization 493, 497, 501
 gcd 190, 198, 202, 466, 496, 501
 Newton iteration 449, 450
 polynomial . 3, 4, 21, 60, 101, 191, 198, 199, 254, 378, 493, 586, 591–621, 709, 768
 quotient 600
 remainder 599, 600, 601, 608, 610
- MUMATH 20
 Mumford, David Bryant 618
 Munro, James Ian 306, 737
 MUPAD 8, 20
- musical
 interval 84, 85, 86, 88, 507
 scale 11, 69, 84
 theory 84, 85
- Musil, Robert 256, 727
 Musser, David Rea 465, 751, 758
 Myerson, Gerald 6
- \mathbb{N} , set of nonnegative integers 768
 NAG 20
- Najafi, Seyed Hesameddin 7
 Najfeld, Igor 698, 748
 Napoléon I. Bonaparte 10, 502, 725, 728
 Nash, Stephen Gregory 741
 Näslund, Mats 580, 748, 758
 Newton, Humphrey 218
 Newton, Sir Isaac ... 0, 3, 24, 28, 61, 197, 203, 218, 219, 256, 286, 290, 358, 372, 374, 512, 622, 641, 725–727, 745, 758
 expansion 671
 formula 267, 290, 291
 interpolation 103, 134, 135, 671
 inversion 259, 261, 262, 268–270, 275, 282, 286–289
- iteration 3, 90, 100, 101, 218, 219, 221, 259, 268, 257–292, 295–310, 444, 448, 450, 451, 581, 623
 linearly convergent \sim 291
 multivariate \sim 449, 450
 numerical \sim 262, 271
 p -adic \sim 268, 271, 272, 290, 292
- Nguyen, Phong Quang 509, 580, 758
 Nicely, Thomas Ray 83, 758
 Niederreiter, Harald Günther ... 407, 420, 421, 428, 509, 711, 745, 747, 755, 758, 759
- Niesi, Gianfranco 619, 747
 Nilsson, Bengt Ola Peter 8
 Nöcker, Michael 6, 7, 88, 461, 580, 737, 746
 Noether, Amalie Emmy 586, 604, 750
 Noetherian ring 604
 non-Archimedean valuation 274
 non-Euclidean geometry 25, 373, 374
 nonresidue 418
 nonscalar model of computation 286, 324
- nonsingular
 curve 559, 568, 571
 matrix see matrix
 norm 419, 473, 707, 717
 Euclidean \sim , $\|\cdot\|_2$... 12, 157, 164, 473, 474, 480, 487, 497, 717, 768
 max- \sim , $\|\cdot\|_\infty$ see maximum norm
 of a lattice 473, 474
 one- \sim , $\|\cdot\|_1$ 165, 717, 768
 q - \sim , $\|\cdot\|_q$ 716, 717
- normal
 basis 76, 580
 degree sequence see degree sequence
 field extension 398
 form 56, 57, 59, 60, 63, 64, 150, 191, 200
 Hermite \sim 89, 352, 498, 499
 matrix \sim 352
 Smith \sim 89
- normalized 57, 59, 63, 147, 148, 149
 polynomial 57, 144, 150, 151, 152, 163, 167
- Novalis (Friedrich Leopold Freiherr von Hardenberg) 68, 726, 729, 734
- Novocin, Andrew 497, 748
- \mathcal{NP} ... 215, 474, 496, 503, 504, 509, 576, 579, 616, 722, 723
 co- \sim 722, 723
- NTL 3, 8, 20, 193–196, 279, 283, 284–286, 461–466, 497
- Nullstellensatz
 Hilbert \sim 586, 595, 617, 618, 621, 736, 761
 proof system 679, 697, 698
- number
 field
 algebraic \sim 279, 378, 473, 533
 sieve 541, 542, 569
 theory 529, 530, 533, 724
 analytic \sim 508, 523, 532, 533, 652
 computational \sim 3, 4, 517–571, 586
 fundamental theorem of \sim 377, 518
- numerical
 analysis 1, 32, 118, 119, 121, 132, 259, 621
 Newton iteration 262, 271

- Núñez, Pedro 41, 759
 Nüsken, Michael 6–8
- O , “big Oh” . . . 2, 30, 32, 703, 715, 720, 721, 723, 724
 O^\sim , “soft Oh” 264, 265, 324, 721, 724
 \mathcal{O} , neutral element of an elliptic curve 558
 Odlyzko, Andrew Michael . . . 205, 353, 443, 497, 508,
 509, 533, 580, 697, 739, 744, 748, 753, 759
 Oesterhelt, Andreas Stefan 7
 Oesterlé, Joseph 443, 759
 Ofman, Yuriĭ Pavlovich (Офман Юрий
 Павлович) 223, 245, 247, 751
 ω , feasible matrix multiplication exponent 337
 one-norm, $\|\cdot\|_1$ 165, 717, 768
 one-time pad 574, 578, 580, 581
 Ong, Heidrun 509, 759
 online algorithm 198
 Onyschuk, Ivan Matthew 88, 758
 Oosterhoff, Luitzen Johannes 698, 748, 759
 operation
 arithmetic \sim 31, 32, 34, 35, 40
 bit \sim 32
 butterfly \sim 234, 235
 word \sim 32, 34, 40
 Oppenheim, Alan Victor 368, 759
 Oppenheim, Tan Sri Sir Alexander 739
 optical character recognition (OCR) 623, 640
 order 595, 596, 598, 710
 graded lexicographic \sim 596, 598
 graded reverse lexicographic \sim 596, 597, 598, 618
 lexicographic \sim 596, 598, 608, 615, 694, 695
 monomial \sim . . . 595, 596, 597–599, 603–605, 610,
 620, 621
 of a group 704
 of a group element, ord 518, 704
 partial \sim 595, 596
 recursion \sim 343, 344, 345, 354, 355
 total \sim 595, 596, 602, 603, 620
 well- \sim 596, 603, 608, 620
 ordering information xiii
 Ore, Øystein 741
 orthogonal . . . 473, 476, 477, 480, 482, 486, 497, 506,
 717
 basis 475, 717
 Gram-Schmidt \sim see Gram-Schmidt
 complement 476
 O’Shea, Donal Bartholomew 614, 617, 618, 741
 Osthoff, Johanna 373
 Ostrogradsky, Mikhail Vasil’evich (Остроградский
 Михаил Васильевич) 640, 759
 Ostrowski, Alexander Markus 586
 Osvik, Dag Arne 542, 751
 Oughtred, William 219
- \mathcal{P} , polynomial time . . . 496, 518, 616, 721, 722–724
 \mathbb{P}^2 , projective plane 567
 p_n , n th prime 524
 Padé, Henri Eugène 132, 759
 approximant . . . 81, 121, 122–124, 132, 137, 138,
 204, 214, 215, 332, 353, 736, 738
 approximation . . . 101, 118, 121, 132, 138, 325, 344
 Paderborn . . . i, 6, 20, 365, 514, 725, 744, 746, 756
- p -adic
 completion 449
 expansion 129, 130, 132, 133, 264, 265, 289, 581
 integers, $\mathbb{Z}_{(p)}$ 270, 275, 449, 466
 inversion 262
 lifting see Hensel lifting
 Newton iteration 268, 271, 272, 290, 292
 valuation 273, 274, 275
- Pan, Victor Yakovlevich (Пан Виктор
 Яковлевич) 306, 327, 332, 352, 353, 405,
 420, 750, 759, 766
 Panario Rodríguez, Daniel Nelson . . . 6, 7, 88, 419,
 421, 580, 744–746, 759
- Papadimitriou, Christos Harilaos (Παπαδημητρίου,
 Χρίστος Χαριλάος) 721, 759
 parallel computation . . . 4, 19, 21, 99, 112, 197, 353,
 411, 461, 591, 679
- PARI 20, 279
 Parsons, David 698, 759
 partial
 fraction decomposition . . . 66, 100, 128, 130–132,
 138, 290, 309, 428, 625–627, 631, 640, 642,
 673, 674
 order 595, 596
 partition of an integer 441, 442, 468
- Pascal, Blaise 512
 PASCAL 21
 Patashnik, Oren . . . 8, 571, 669, 670, 717, 720, 747
 Paule, Peter . . . 7, 670, 671, 697, 755, 759, 760
 Peitgen, Heinz-Otto 278, 760
 Pell, John 512
 Pengelley, David 6
 Penk, Michael Alexander 61
 Pennebaker, William Boone, Jr. 368, 760
 Pentium processor 83, 497
 Pepin, Jean François Théophile . . . 530, 534, 538, 760
- perfect
 field 397
 number 531, 535
 power 263, 273, 292, 535, 543, 548, 563
 square 550
 period 360, 362
 periodic
 function 361, 362
 sequence 348
 permutation . . . 89, 109, 136, 441, 573, 574, 672, 694,
 705, 716
 matrix 483, 715, 716
 polynomial 425
 Perron, Oskar 90, 760
 Peterson, James Lyle 697, 760
 Petkovšek, Marko . . . 641, 671, 675, 676, 697, 729,
 735, 736, 760
 Petr, Karel 402, 420, 760
 -Berlekamp matrix . . . 335, 340, 352, 402, 404, 428
 Petri, Carl Adam 679, 760
 net 679, 680, 697, 698, 756, 760, 761
 Petrick, Stanley Roy 749, 755
 Petrovitch, Michel 754
 Pfaff, Johann Friedrich 670
 -Saalschütz identity 671
 Pfeiffer, Rüdiger 766

- Pflügel, Eckhard 641, 760
 PGP 18
 Phelps, Kevin Thomas 215, 749
 φ see Euler totient function
 Φ , totient function for polynomials 93
 Φ_n , cyclotomic polynomial 412
 π 68, 81–83, 89, 90, 198, 221, 247, 588, 710
 rational approximation of \sim 81
 $\pi(\cdot)$, number of primes 524
 piano 86
 Piazzì, Guisepe 374
 Pickering, William Graham 6
 pigeonhole principle 678, 697, 698
 Pilote, Michel 6
 Pinch, Richard Gilmour Eric 532, 760
 Pinzon (née Sharrow), Katherine Rita 8
 Pirastu, Roberto Maria 670, 671, 673, 760
 Pitassi, Toniann 697, 736, 760
 Pitt, François 6
 pivot element 110, 111
 de la Place, Pierre Simon, Marquis see Laplace
 plane curve 173, 198, 203, 594, 615
 intersection 141, 171, 172, 175, 203
 Plato (Πλάτων) 24, 312, 727
 Playboy 372
 Plücker, Julius 729
 plumbing knee 14, 16, 699
 PMS 20
 Pochhammer, Leo, symbol 670
 Pocklington, Henry Cabourn 88, 198, 760
 Poe, Edgar Allan 516, 728
 Poilly, François 725
 point at infinity 558, 561, 564, 567
 Pollack, Richard 745, 749, 761
 Pollard, John Michael 198, 247, 280, 534, 542, 545,
 567–569, 738, 754, 755, 760
 and Strassen method 536, 541, 544, 552, 569
 $p-1$ method 541, 557, 564, 567, 568
 ρ method 541, 542, 545, 547, 548, 567, 569
 polynomial
 addition 33
 annihilating \sim 341
 bivariate \sim see bivariate polynomial
 calculus system 697
 characteristic \sim see characteristic polynomial
 continuant \sim 65, 93
 cyclotomic \sim , Φ_n see cyclotomic polynomial
 degree of a \sim 32, 708, 709
 elementary symmetric \sim 166
 equation 1, 3, 4, 89, 218, 267, 270, 274, 444, 591,
 614, 621, 694, 697
 error locator \sim 213
 factorization see factorization
 ideal 498, 591–621, 677
 interpolation see interpolation
 irreducible \sim see irreducible polynomial
 minimal \sim see minimal polynomial
 monic \sim 32, 35, 40, 56, 59, 60, 708, 710
 multiplication see multiplication
 multivariate \sim see multivariate polynomial
 normalized \sim 57, 144, 150, 151, 152, 163, 167
 part 94, 625–627
 permutation \sim 425
 primitive \sim see primitive polynomial
 random \sim see random polynomial
 remainder sequence 199
 primitive \sim 199
 reduced \sim 199
 subresultant \sim 199
 representation of the Frobenius map 398, 408
 ring 2, 708, 768
 $S\sim$ 604, 606, 608, 610, 619
 separable \sim 397
 splitting \sim 384, 385, 387
 squarefree \sim 377, 397, 426, 453
 summation 3, 645, 649, 650, 658
 Swinnerton-Dyer \sim . 434, 441, 442, 443, 465, 467
 Taylor \sim 123
 time, \mathcal{P} 496, 518, 616, 721, 722–724
 -time
 equivalent 577, 579, 722
 reducible 577, 579, 722
 weight of a \sim 43
 Pomerance, Carl . 520, 529, 532, 557, 567, 569, 735,
 739, 742, 753–755, 757, 759, 760
 van der Poorten, Alfred Jacobus .. 90, 514, 697, 737,
 761
 POSSO 619
 Pottier, Eugène 727
 power series ... 66, 81, 94, 121, 122, 132, 275, 292,
 343, 449, 618, 670, 673, 708, 768
 Powers, Raymond Earnest 569, 754
 pp see primitive part
 Prange, Eugene 419, 430, 761
 pretend field technique 558
 primality
 test 3, 77, 286, 513, 517, 518, 519, 521, 523, 524,
 530, 532, 533, 535, 543, 554
 Fermat \sim 519, 520, 521, 523, 534
 Lehmann \sim 537, 538
 Lucas-Lehmer \sim see Lucas-Lehmer test
 probabilistic \sim 17, 196, 529, 543
 Solovay and Strassen \sim see Solovay
 strong pseudo \sim 520, 521, 523, 532, 536
 prime 149, 707, 708
 element 149, 268, 707, 708
 factorization ... 106, 131, 291, 292, 518, 529, 535,
 550, 554
 Fermat \sim 228, 251, 530, 536
 field 711
 finding 523, 525, 527, 528
 Fourier \sim 99, 243, 246, 528, 529, 536
 Mersenne \sim 517, 530, 531, 534, 535
 number 17, 26, 112, 190, 197, 422, 513, 517,
 517–538, 557, 565, 706
 theorem . 97, 373, 434, 523, 524, 527–529, 532,
 533, 536, 553, 556
 power modular algorithm .. see modular algorithm
 relatively \sim 46, 707
 single precision \sim 69, 113, 243, 246, 528, 529, 536
 twin \sim 83, 221, 534
 PRIMES 532, 721

- primitive
 EEA 192
 element 713
 Euclidean Algorithm 190, 191, 192, 194–197,
 199, 206
 part, pp .. 147, 148, 149, 150, 152, 162, 178, 191,
 192, 200, 433, 434
 polynomial 147, 148, 150, 162, 166, 168, 170,
 191, 199, 200, 202, 206, 433, 695
 greatest common divisor of \sim s 152
 remainder sequence 199
 root of unity see root of unity
 squarefree decomposition 470, 471
 Pritchard, Paul Andrew 533, 761
 private key 17, 504, 509, 575, 576–579, 582
 probabilistic
 algorithm 161, 162, 167, 176, 177, 201, 204, 351,
 378, 421, 423, 434, 438, 536, 569, 576, 722
 primality test 17, 196, 529, 543
 probabilistically checkable proof 88
 probability, $\text{prob}(\cdot)$ 718
 conditional \sim 682, 718
 distribution 523, 718
 finite \sim space 703, 717, 718, 719
 function 717
 uniform \sim 718
 theory 3, 372, 512, 717
 Proclus 24
 product rule 266, 646, 671, 674
 program checking 37
 projection ... 172–174, 476, 483, 499, 652, 689–691,
 693, 699, 718
 projective
 curve 567, 568
 geometry 567
 plane, \mathbb{P}^2 567
 Prolog 678
 proof
 certificate 684
 probabilistically checkable \sim 88
 system 677, 697
 propositional
 calculus 677, 722
 formula 678, 679
 proof system 677, 678
 Pruschke, Thilo 7
 pseudodivision 38, 183, 190, 191, 197, 199, 204–206
 pseudoprimalty test see primality test
 pseudoprime 523
 pseudorandom number generator 503, 505, 509,
 574, 578, 580
PSPACE 616, 617, 723
 Ptolemy, Claudius (Πτολεμαῖος Κλαύδιος) 24
 public key 17, 503, 509, 575, 577–579, 582
 cryptography 3, 17, 503, 575, 573–582
 Pudlák, Pavel 697, 736, 739
 Purdy, George Barry 581, 761
 Putnam, Hilary Whitehall 678
 Pythagorean 85, 518
 triple 567, 570
 \mathbb{Q} , field of rational numbers 768
 q -norm, $\|\cdot\|_q$ 716, 717
 QR-decomposition 337
 quadratic
 character 554, 561
 law of \sim reciprocity 372, 529, 537, 586
 sieve 557, 567
 multiple polynomial \sim 567
 time 36
 quantifier elimination 4
 quicksort 221
 Quisquater, Jean-Jacques 758
 Don Quixote de la Mancha 90, 740
 quotient, quo 38, 40, 41, 46, 47, 261, 707
 in the Euclidean Algorithm 48, 49, 52, 53, 58, 59,
 65, 313, 314, 317, 318, 321, 323, 324, 326
 multivariate \sim 600
 rule 671
 \mathbb{R} , field of real numbers 768
 \Re , real part 768
 Rabin, Michael Oser .. 131, 215, 421, 424, 532, 533,
 759, 761
 cryptosystem 573, 579
 Rabin, Tal 752
 Rabinowitsch, J. L. 618, 761
 Racah, Giulio 764
 Rackoff, Charles Weill 6, 567, 570
 radix
 conversion 264, 265
 representation 29, 33, 41, 129
 Raghavan, Prabhakar 88, 198, 758
 RAM 32
 Ramanujan, Srinivasa Aiyangar . 535, 644, 671, 685,
 737, 743, 748, 759
 Ramos, Bartolomé 86, 761
 random
 element 104, 177, 424, 534, 545
 polynomial 93, 200, 314, 379, 411, 419, 426, 429,
 461
 pseudo \sim number generator ... 503, 505, 509, 574,
 578, 580
 squares method see Dixon
 variable 161, 546, 562, 682, 718, 719, 722
 Bernoulli \sim 719
 walk 562, 571
 rank of a matrix 698, 714, 715
 Raphson, Joseph 219, 725, 726, 758, 761
 Ratdolt, Erhard 25, 725
 rate of a code 209, 210
 rational
 approximation of π 81
 function 710, 768
 canonical form of a \sim . 116, 117, 119, 121, 122,
 124, 138
 integration 3, 626, 630, 632, 640
 reconstruction 115, 117–119, 123, 124, 325
 interpolation 101, 118, 119, 120, 132
 number
 canonical form of a \sim 126, 127
 reconstruction 101, 124, 137, 146, 188–190,
 331

- part 625, 642
 root 456, 466
- Razborov, Aleksandr Aleksandrovich (Разборов Александр Александрович) ... 697, 739, 761
- reachability problem 680, 681, 697
- Recio Muñoz, Tomás Jesús 6, 619, 749
- Recorde, Robert 44, 502, 726, 728, 729, 796
- rectangular matrix multiplication 353
- recurrence 1, 349, 353, 354, 653, 669, 684
- recursion order 343, 344, 345, 354, 355
- recursively enumerable 89
- REDUCE 20
- reduced
 basis 286, 478, 479, 480, 482, 488, 491, 497, 498, 504, 506, 508
 element 611
 Gröbner basis see Gröbner basis
 polynomial remainder sequence 199
- reducible 707
- refutation 678, 679
- Reichel, Horst 756
- Reid, Constance 587, 761
- Reif, John Henry 619, 736
- Reischert, Daniel see Lauer
- Reisig, Wolfgang 697, 761
- Reitwiesner, George Walter 82, 761
- remainder, rem 38, 40, 41, 46, 47, 261, 323, 600, 707
 division with \sim 2, 26, 37, 38, 39, 41, 45, 51, 59–62, 100, 131, 257, 261, 262, 282, 283, 314, 407, 445
 in the Euclidean Algorithm 48, 52, 57, 58, 59, 61, 197, 199, 313, 324, 331, 630, 631
 multivariate \sim 599, 600, 601, 608, 610
- Remmers, Harry 419, 755
- Renegar, James 619, 761
- repeated squaring .. 17, 75, 76, 77, 88, 93, 264, 291, 381, 385, 389, 392, 403, 405, 407, 424, 519, 521, 537
- representative
 canonical \sim 398
 system of \sim s 72, 706, 709
 symmetric \sim 72, 110, 436
- repunit 530, 534, 569
- Research Institute for Symbolic Computation (RISC) 618
- residue
 class, mod 71, 72, 398, 706
 class ring .. 71, 72, 75, 92, 93, 163, 262, 326, 327, 398, 706, 768
- resolution 678
- resultant, res .. 15, 155, 157, 141–207, 327, 331–333, 434, 435, 453, 615, 619, 628, 630, 635, 641, 643, 662, 663, 694
- reversal, rev 203, 258, 262, 287, 343, 424
- Reynaud, Antoine André Louis 61, 761
- Rhind Papyrus 82
- Richardson, Daniel 640, 761
- Richmond, Lawrence Bruce 419, 421, 759
- te Riele, Herman(us) Johannes Joseph 508, 533, 542, 751, 756, 759
- Riemann, Georg Friedrich Bernhard .. 373, 533, 761
 Hypothesis 508, 533, 748, 749, 757
 Extended \sim , (ERH) see Extended Riemann
 zeta function, ζ .. 62, 221, 508, 533, 652, 684, 756, 759
- right ideal 705
- rigid conformation of cyclohexane .. 12, 15, 16, 698
- ring 32, 705, 711
 characteristic of a \sim .. 394, 395, 397, 415, 460, 558, 561, 581, 623, 626, 630, 658, 665, 710, 712
 commutative \sim 705, 706, 709, 711, 713
 factorial \sim 707
 homomorphism 104, 107, 133, 295, 302, 705, 706, 709
 canonical \sim 72, 104, 110, 706, 709
 invariant \sim 618
 isomorphism 705
 Noetherian \sim 604
 of algebraic integers 707, 708
 of constants 624
 of polynomials 2, 708, 768
 operation see arithmetic operation
- Rink, Friedrich Theodor 727
- Rioboo, Renaud 627, 630, 631, 640, 754, 758
- Risch, Robert Henry 640, 641, 761
 differential equation 641, 738, 742, 750
- rising factorial 647, 670, 673, 768
- Ritscher, Stephan 617, 756
- Ritt, Joseph Fels 619, 640, 745, 762
- Rivest, Ronald Linn .. 16, 41, 368, 509, 576, 740, 741, 762
- Robbiano, Lorenzo 617, 619, 742, 747
- robot 591, 592
 kinematics 615, 698
- Rodger, Christopher Andrew 215, 749
- Rogers, Leonard James, -Ramanujan identity ... 671, 685, 743, 759
- Rolletschek, Heinrich Franz 132, 751
- The Rolling Stones 516, 728
- Roman, Steven 669, 762
- Rónyai, Lajos 421, 762
- root
 finding .. 132, 219, 257, 273, 286, 392, 456, 457, 460, 466, 525, 526
 over finite fields 377, 392, 418, 428
 integral \sim 392, 393, 635, 641
 of an integer 271, 460
 of unity 19, 227, 221–254, 262, 373, 384, 412
 primitive \sim .. 211, 209–215, 227, 221–254, 296, 333, 340, 352, 362, 412, 412–417, 536
 rational \sim 456, 466
- Rosen, Frederic 726, 762
- Rosenkranz, Karl 727
- Rosser, John Barkley 527, 532, 536, 750, 762
- Rota, Gian-Carlo 669
- Rothstein, Michael 640, 641, 762
 and Trager integration 627, 640
- rounding error 32
- routing 18, 198
- Rowland, John Hawley 199, 762
- Roy, Marie-Françoise .. 184, 199, 332, 619, 749, 755

- \mathcal{RP} 532, 722, 723
 co~ 532, 722, 723
- RSA
 challenge 542
 cryptosystem 16, 17, 18, 503, 542, 573, 576,
 578–580, 582
 run length encoding 365, 366–368
 Runge, Carl David Tolmé 586
 Russell, Bertrand Arthur William 588
- S-polynomial, $S(\cdot, \cdot)$ 604, 606, 608, 610, 619
 Saalschütz, Louis 671
 Sachse, Hermann 698, 762
 SACLIB 20
 Safey El Din, Mohab 199, 755
 SAGE 20
 de Sainte-Croix, Jumeau 669
 Salvy, Bruno 641, 671, 697, 741, 744, 760, 762
 Samuel, Richard 729
 Sande, G. 247, 747
 Saunders, Benjamin David . 340, 351, 353, 404, 465,
 747, 751
 Sauppe, Dietmar 278, 760
 Saxena, Nitin 517, 543, 735
 scalar 714
 multiplication 346, 348, 351, 713, 714
 scale
 chromatic ~ 86
 diatonic ~ 85, 86
 musical ~ 11, 69, 84
 well-tempered ~ 86, 87, 88
 Schafer, Ronald W. 368, 759
 Scheraga, Harold Abraham 698, 747
 Schering, Ernst Christian Julius 752
 Schloß Neuhaus 365, 725
 Schmidt, August 725
 Schmidt, Erhard . 475–481, 485, 496, 498, 500, 717,
 762
 Schmidt, Friedrich Karl 748
 Schnorr, Claus-Peter .. 421, 497, 509, 567, 752, 757,
 759, 762
 Schoenfeld, Lowell 527, 532, 536, 762
 Schönhage, Arnold . 7, 202, 220–222, 243, 245, 247,
 253, 254, 279, 283, 286, 292, 332, 352, 497, 533,
 727, 759, 762
 and Strassen multiplication algorithm ... 238, 243,
 245, 283, 284, 286
 Schrijver, Alexander 496, 748
 von Schubert, Friedrich Theodor 465, 762
 Schubert, Friedrich Wilhelm 727
 Schwartz, Jacob Theodore 198, 332, 762
 Schwarz, Hermann Amandus 485, 500, 555
 Schwarz (Švarc), Štefan 420, 763
 Schwarz, Robert 8
 Schwenter, Daniel 61, 131, 697, 763
 SCRATCHPAD 20, 640
 secret sharing 3, 11, 18, 19, 100, 103, 131, 134
 Sedgewick, Robert 697, 763
 seed 505, 574, 578
 self-reciprocal 424, 425
 Selfridge, John Lewis 532, 542, 738, 760
 semialgebraic 696
 semigroup 697
 Sendra, Juan Rafael 618, 747, 749
 separable polynomial 397
 sequence
 associated ~ 669
 Cauchy ~ 292
 degree see degree sequence
 Fibonacci ~ 66, 341, 343
 impulse response ~ 349
 linearly recurrent ~ see linearly recurrent
 Lucas ~ 66
 periodic ~ 348
 superincreasing ~ 504
 Seress, Ákos 724, 736
 Serocka, Peter 7
 Seroussi, Gadiel 580, 737
 Serre, Jean-Pierre 744
 Serret, Joseph Alfred 418, 728, 753, 763
 Sesame Street 135
 Sgall, Jiří 697, 739
 Shakespeare, William 0, 725
 Shallit, Jeffrey Outlaw . 6–8, 61, 421, 531–535, 568,
 736, 763
 Shamir, Adi .. 16, 131, 469, 503, 505, 509, 576, 744,
 759, 762, 763
 Shanks, Daniel Charles 82, 763
 Shanks, William 82, 90, 622, 729, 763
 Shannon, Claude Elwood, Jr. 209, 215, 307, 763
 Sharrow, Katherine Rita see Pinzon
 O’Shea, Donal Bartholomew 614, 617, 618, 741
 Shen, Kangsheng 131, 763
 Shepherdson, John Cedric 419, 745
 Shepp, Lawrence Alan 421, 763
 shift
 -equivalence class 655, 656
 gcd, gcdE 657
 operator, E 646, 648, 659, 660, 671
 Shiue, Peter Jau-Shyong 745, 758, 766
 Shokrollahi, Mohammad Amin (محمد أمين شكرالهي)
 88, 222, 286, 338, 352, 739
 short vector ... 3, 434, 435, 473–501, 504–507, 509,
 574
 cryptosystem 573
 shortest vector 480, 493, 497, 500
 Shoup, Victor John ... 3, 6–8, 20, 88, 193, 205, 246,
 278, 279, 283, 286, 354, 401, 405–407, 419–421,
 462, 465–467, 497, 580, 734, 745, 746, 751, 763
 Shparlinski, Igor’ Evgen’ovich (Шпарлинский
 Игорь Евгеньевич) . 6, 198, 199, 419, 746,
 763
 Shparlinski, Irina Igorevna (Шпарлинская
 Ирина Игоревна) 6
 Shpilka, Amir 199, 763
 Shub, Michael Ira 745
 SIAM Journal on Computing 21
 Siegel, Carl Ludwig 586
 sieve
 number field ~ 541, 542, 569
 of Eratosthenes 171, 527, 531, 533, 552, 557
 quadratic ~ 557, 567
 Sieveking, Malte 286, 497, 749, 763
 sign 768

- signal 359–369
 analog ~ 359, 360
 continuous ~ 359, 363
 digital ~ 247, 359, 363, 368
 discrete ~ 359, 360–364, 368, 369
 even ~ 369
 odd ~ 369
 periodic ~ 360, 361–364, 368, 369
 processing 3, 247, 359, 363
 sine ~ 360
- SIGSAM 21
- Silverman, Joseph Hillel 568, 752, 758, 763
- Silverman, Robert David 531, 567, 739, 764
- Simon, Horst Dieter 2, 337, 736
- Simon, Imre 750
- Singer, Michael F. 498, 641, 671, 748, 749, 764
- Singh, Simon 514, 764
- single precision 29, 30, 31, 37, 40–42, 244, 280,
 282, 283
 prime 69, 113, 243, 246, 528, 529, 536
- SINGULAR 20, 619
- singular matrix ... 103, 204, 347, 351, 355, 688, 715,
 716
- singularity 118, 121, 132, 591, 697
- Sipser, Michael 89, 721, 764
- size of an elliptic curve 561, 565
- Sjöwall, Maj 516, 728
- Skopin, Aleksandr Ivanovich (Скопин
 Александр Иванович) 419
- slide rule 1
- Slisenko, Anatol' Oles'evich (Слисенько
 Анатоль Олесьевич) 419, 764
- Sloane, Neil James Alexander 215, 756
- small primes modular algorithm see modular
- Smart, Nigel 580, 737
- Smith, Edson 517
- Smith, Henry John Stephen, normal form 89
- smooth
 elliptic curve 559, 560
 function 121, 361, 368
 number ... 421, 549, 552–555, 557, 558, 564–566,
 568, 570
 point 618
- soft Oh, O^{\sim} 264, 265, 324, 721, 724
- softly linear 721
- Soiffer, Neil 21, 750
- solar calendar 83
- Solovay, Robert Martin 198, 529, 530, 533, 764
 and Strassen primality test 161, 198, 529, 530,
 532, 533, 735
- solution space 351, 638, 666, 685, 698, 715
- Sonin, Nikolai Yakovlevich (Сонин Николай
 Яковлевич) 740
- Sorenson, Jonathan Paul ... 287, 529, 533, 736, 757,
 764
- sorting 198, 221
 fast ~ 233
- Sosigenes of Alexandria 83
- space-bounded complexity class 723
- sparse
 factorization 497
 interpolation 498
- linear
 algebra 352
 system 325, 556
- matrix 335, 340
 representation .. 43, 101, 494, 496, 498, 501, 641
- spline
 Bézier ~ 138
 cubic ~ 137
- splitting
 equal-degree ~ 385, 387, 423, 424
 field 177, 426, 429, 441, 627, 628, 630, 711
 polynomial 384, 385, 387
- Sprindzhuk, Vladimir Gennadievich (Спринджук
 Владимир Геннадиевич) 498, 764
- square
 and multiply 75
 wave 369
- squarefree 55, 419, 435, 558, 559
 decomposition . 395, 396, 397, 425, 426, 460–462,
 470, 471, 492, 625, 626, 630, 631, 634, 635,
 642, 655, 657, 658
 primitive ~ 470, 471
 factorization ... 377, 379, 389, 393, 395, 397, 416,
 426, 658
- part 394, 395, 414, 419, 425, 426, 627, 640, 642,
 663
- polynomial 377, 397, 426, 453
- standard
 basis 591
 deviation 196, 281, 718
 representation 30, 31, 37, 53, 54, 74
- starting solution 265, 268–272, 290, 446, 448
- Steel, Allan Kenneth 8
- Steele, Leroy P., Prize 697
- Steiger, William 745, 749, 761
- Steiglitz, Kenneth 286, 292, 735
- Stein, Clifford 41, 368, 741
- Stein, Josef 61, 764
- Stein, William Arthur 20
- Stern, Jacques 509, 580, 758
- Stetter, Hans Jörg 7, 41, 766
- Stevenhagen, Peter 441, 764
- Stevenson, Robert Louis 28, 726
- Stevin, Simon 41, 61, 764
- Stieltjes, Thomas Joannes 508
- Stillman, Michael 618, 736
- Stirling, James 670, 764
 formula 571
 number 669, 670
 of the first kind 672, 768
 of the second kind 650, 768
- STOC 21
- stochastic mobile 306, 307, 308
- Storjohann, Arne . 353, 497, 501, 671, 747, 758, 764
- Stoutemyer, David 20
- straight-line program 495, 498
- Strang, Gilbert 713, 764
- Strassen, Volker 6, 161, 198, 221, 222, 238, 243,
 245, 247, 254, 283, 284, 286, 324, 332, 335, 337,
 338, 352, 497, 529, 530, 532, 533, 536, 541, 544,
 552, 567, 569, 735, 736, 740, 762, 764
- algorithm 335, 337, 352

- Strehl, Volker 6, 7, 670, 671, 755, 760
- string matching 91
- strong
 liar 523, 532
 pseudoprimalty test 520, 521, 523, 532, 536
 witness 523, 532, 534
- Sturm, Jacques Charles François .. 94, 332, 748, 764
 chain 95, 752, 765
 theorem 95, 198
- Sturmfels, Bernd 697, 743
 subdeterminant 688, 689, 694
 subfield 94, 641, 710, 711, 712
 subgroup 373, 704, 768
 submodule 348
 subproduct tree 296, 297, 298, 302
 subresultant 3, 33, 45, 141, 143, 152, 164, 181,
 178–207, 313, 327–332, 616, 630, 681
 fundamental theorem on \sim s 327, 329, 332
 polynomial remainder sequence 199
- subring 641, 706
- subset sum
 cryptosystem see knapsack cryptosystem
 problem 503, 504, 509, 576
- subspace
 Krylov \sim 341, 346, 347, 355
 linear \sim 209, 210, 280, 714, 715, 768
- substitution 623
- Sudan, Madhu 215, 735
- summation 3, 101, 645–675, 681
 hypergeometric \sim 3, 641, 660, 665, 658–669, 671,
 674, 683, 685
 indefinite \sim 646, 683
 of polynomials 3, 645, 649, 650, 658
- Sun, Xiaoguang 131, 753
- Sun-Tsü 131
 supercomputer 1, 18, 83, 575
- superincreasing sequence 504
- superlinearity 245
- surjective 704, 713, 714
- Svoboda, Antonín 132, 764
- Swan, Richard Gordon 207, 332, 764
- Swift, Jonathan 702, 729
- Swinnerton-Dyer, Sir Henry Peter Francis 465
 polynomial 434, 441, 442, 443, 465, 467
- Sylvester, James Joseph 96, 197, 199, 294, 334, 726,
 727, 736, 755, 765
 matrix, Syl 155, 158, 159, 181, 197, 199, 201,
 204, 205, 335, 340, 435, 470
- symbolic-numeric computation 41
- symmetric
 cryptosystem 16, 575, 578
 group 136, 442, 465, 705
- system of representatives 72, 706, 709
 symmetric \sim 72, 110, 436
- Szabó, Nicholas Sigismund 132, 765
- T , transpose 715
- tableau 678
- Takahashi, Daisuke 82
- Tamura, Yoshiaki 82
- Tanaka, Richard Isamu 132, 765
- tangent function 123, 124
- Taniyama, Yutaka, -Weil conjecture 514
- Tannery, Paul 729, 744
- Tarry, Gaston 531, 765
- Tarski, Alfred (Tajtelbaum) 619, 748, 765
- taxi-cab number 535
- Taylor, Brook 286, 746, 765
 coefficient 114
 expansion 100, 114, 121, 113–131, 259, 264–278,
 286, 289, 290, 292, 353, 623, 671
 generalized \sim 264, 289
 polynomial 123
 series 123
- Taylor, Richard 514, 765
- Teichmüller, Oswald 290
- telescoping 646
- Tenenbaum, Gérald 536, 765
- te Riele, Herman(us) Johannes Joseph see Riele
 term
 ratio 659, 660, 663, 664, 667, 674, 683
 rewriting 591, 618
- Thatcher, James Winthrop 744, 751
- Theaitetus (Θεαιτήτος) 24
- Theiwes, David 7
- theorem in a proof system 677
- Theoretical Computer Science 21
- theory of a proof system 677
- Thijssse, Gérard Philip Antoine 727
- Thomé, Emmanuel 542, 751
- three primes FFT 243, 246, 247, 283, 284, 286
- 3-adic FFT 242, 247, 252, 253
- Thue, Axel 132, 750, 765, 767
- Tijdeman, Robert 760
- van Tilborg, Henricus Carolus Adrianus (Henk) 215,
 737
- Timofeev, Andrey 542, 751
- Tiwari, Prasoon 498, 737
- Toeplitz, Otto, matrix 202, 332, 335, 353, 738
- tonal key 85, 86
- Toom, Andrei Leonovich (Тоом Андрей
 Леонович) 247, 765
- total
 degree 157, 172, 176, 493, 597, 616, 689, 709
 order 595, 596, 602, 603, 620
- Trabb Pardo, Luis Isidoro 567, 752
- trace 382, 419
- traditional
 Euclidean Algorithm .. 47, 51, 54, 57, 79, 94, 95,
 99, 144, 184, 185, 187, 197, 199, 329
 Extended Euclidean Algorithm (EEA) . 48, 49, 51,
 52, 54, 57, 59, 60, 64, 65, 80, 94, 111, 125,
 184, 186, 189, 205, 313, 317, 325, 710
- Trager, Barry Marshall 466, 496, 498, 627, 630,
 631, 640, 751, 758, 765
- transcendental 82, 90, 710
- transmission
 channel 16, 209
 error 209
 rate 210
- transposition principle 340, 353
- trapdoor function 575
- Traub, Joseph Frederick 197, 199, 332, 738, 761
- Traverso, Carlo 619, 734, 747, 765

- Tre, Sol 697, 743
 trial division 389, 541, 543, 544, 552
 triangle 592, 593, 612
 triangular
 matrix 329, 638, 666, 716
 wave 369
 triangulation 198
 trivial derivative 624, 642
 Tropfke, Johannes 88, 765
 tropical year 83, 84
 Trudi, Nicola 199, 765
 Tschirnhaus (Tschirnhausen), Ehrenfried Walther,
 Graf von 197, 754
 Tuckerman, Bryant 542, 738
 Tukey, John Wilder 233, 247, 741
 Túran, Paul 748
 Turing, Alan Mathison 89, 419, 574, 588, 765
 machine 32, 721, 722, 747, 762
 Las Vegas ~ 722
 one-sided Monte Carlo ~ 722
 two-sided Monte Carlo ~ 721
 reduction 722
 Twain, Mark (Samuel Longhorne Clemens) 358, 727
 twin prime 83, 221, 534
 twisted cubic 608, 609, 613, 614
 two-norm, $\|\cdot\|_2$ see Euclidean norm
- UFD see Unique Factorization Domain
 Ulam, Stanisław Marcin 28, 198, 516, 724, 726,
 728, 757
 Ullman, Jeffrey David 286, 292, 332, 735
 ultrametric inequality 274
 Uluġ Beg Muḥammad Tūrghāy bin Shāh Rukh
 (اولغ بگ محمد تورغاي بن شاه رخ) 90
 Umans, Christopher Matthew ... 339, 405, 407, 408,
 420, 751, 765
 umbral calculus 669
 undecidable 419, 640
 Underbakke, David Lee 534
 undetermined coefficients, method of ~ .. see method
 uniform probability function 718
 unimodular
 matrix 89, 498, 499
 transformation 89
 unique factorization domain (UFD) ... 63, 147–150,
 152, 157, 158, 191, 199, 200, 202, 204, 206, 274,
 377, 433, 470, 518, 706, 707, 708, 711
 unit 38, 46, 73, 707, 708–710
 unsatisfiable 678
 Updike, John 702, 729
 Urquhart, Alasdair 697, 765
- $V(\cdot)$, variety 593
 Vacca, Giovanni 88, 765
 Vadhan, Salil 199, 755
 Valach, Miroslav 132, 764
 Valiant, Leslie Gabriel 312, 727
 Vallée, Brigitte 61, 765
 de la Vallée Poussin, Charles Jean Gustave Nicolas
 533, 765
 valuation 94, 257, 273, 274, 275, 292
 Archimedean ~ 274
 degree ~ 91, 94, 274
 non-Archimedean ~ 274
 p -adic ~ 273, 274, 275
 x -adic ~ 91, 94, 274, 275, 292
 value representation 100, 231
 van Ceulen, Ludolph (Ludolf) 82, 90
 van de Lune, Jan 533, 756
 van der Hoeven, Joris 469, 749
 Vandermonde, Alexandre Alexis Théophile 670
 convolution 672
 matrix, VDM .. 103, 213, 231, 232, 249, 335, 340,
 352
 van der Poorten, Alfred Jacobus see Poorten
 van der Waerden, Bartel Leendert see Waerden
 van Hoeij, Marinus (Mark) Hubertus Franciscus .. 7,
 497, 671, 735, 748, 749
 van Leeuwen, Jan 750, 754, 764, 765
 van Lint, Jacobus Hendricus 215, 755
 Vanstone, Scott Alexander 88, 758
 van Tilborg, Henricus Carolus Adrianus . see Tilborg
 variance 718
 variety
 algebraic ~ 172, 198, 586, 591, 613
 of an ideal, $V(\cdot)$ 593, 594, 595, 614, 617, 618
 Vaughan, Robert Charles 198, 201, 765
 VDM see Vandermonde matrix
 vector 714
 addition system 697
 short ~ see short vector
 shortest ~ 480, 493, 497, 500
 space 211, 341, 342, 354, 362, 401, 674, 698,
 710–712, 713, 714, 716, 717
 dimension of a ~ . 349, 401, 674, 685, 687, 688,
 698, 710, 711, 714
 finite-dimensional ~ 710, 714
 finitely generated ~ 714
 Venkatesan, Ramarathnam 567, 749
 Vercauteren, Frederik R. G. 8
 Vernam, Gilbert S. 580, 765
 Vetter, Herbert Dieter Ekkehart .. 279, 286, 292, 727,
 762
 Viehmann, Benjamin Thomas Johannes 7
 Viète, François, Seigneur de la Bigotière 219
 rule 165
 Villard, Gilles 353, 747, 765
 Viola Deambrosis, Alfredo (Tuba) 419, 421, 746,
 759
 Vitter, Jeffrey Scott 697, 765
 Vogel, Kurt 764
 Voltaire (François Marie Arouet) 294, 502, 727, 728
 von Goethe, Johann Wolfgang ... 140, 358, 726, 727
 von Koch, Niels Fabian Helge 287, 752
 von Lindemann, Carl Louis Ferdinand 82, 755
 von Schubert, Friedrich Theodor 465, 762
 Vrbik, Paul 8
- Wade, Leroy Grover (Skip), Jr. 698, 765
 van der Waerden, Bartel Leendert 198, 349, 352,
 419, 465, 586, 588, 703, 729, 734, 765, 766
 Wagstaff, Samuel Standfield, Jr. . 532, 534, 542, 543,
 569, 738, 760, 766
 Wahlöo, Per 516, 728

- Waldeck, Minna 373
 Wall, James Robert 215, 749
 Wallace, Gregory K. 368, 766
 Wallis, John 622
 Walton, Izaak 702, 729
 Wan, Daqing 425, 766
 Wang, Dongming 767
 Wang, Paul Shyh-Horng 376, 727, 759
 Wang, Xinmao 327, 766
 Wang, Yuan 352, 740
 Waring, Edward 131, 286, 588, 766
 Warlimont, Richard Clemens 419, 752
 Waterloo i, 20
 Watson, John H., M. D. 702
 Watt, Stephen Michael . . 41, 735, 738, 741, 747, 766
 weather prediction 1
 Weaver, Warren Eduard 763
 web page . . [xiii](#), 2, 4, 8, 18, 193, 286, 531, 534, 542,
 687, 697, 724
 Weber, Heinrich 725, 761
 Weber, Wilhelm Eduard 374
 Weeks, Dennis 766
 Wegener, Ingo Werner 721, 766
 de Weger, Benjamin Marinus Marnix (Benne) .. 497,
 766
 Wehry, Marianne 6, 7
 Weierstraß, Karl Theodor Wilhelm 68, 373, 726
 coefficients [559](#), 561, 563, 564, 571
 equation [559](#)
 weight
 Hamming ~ [75](#), [210](#)
 of a node in a mobile [306](#), 307, 308
 of a polynomial 43
 Weil, André 198, 513, 514, 766
 bound 568, 736
 Weilert, André 61, 766
 Weispfenning, Volker Bernd . . 7, 618, 736, 741, 747
 well-order [596](#), 603, 608, 620
 well-tempered scale [86](#), 87, 88
 Werckmeister, Andreas 86, 766
 Werner, Markus 699, 729
 Weyl, Claus Hugo Hermann 586
 Whitehead, Alfred North ... 256, 588, 676, 727, 729
 Whiteside, Derek Thomas 725, 726, 758
 Wiedemann, Douglas Henry 340, 346, 351, 352,
 355, 556, 766
 algorithm 340, [346](#), 352, 353, 355, 420, 556, 557,
 741, 750, 751, 765
 Wieland, Thomas 698, 736
 Wiles, Andrew John 514, 765, 766
 Wilf, Herbert Saul 466, 671, 676, 684, 697, 729,
 760, 766
 Kaiser Wilhelm II 587
 Willett, Michael 419, 766
 Williams, Hugh Cowie 530, 542, 568, 569, 757, 766
 Williams, Leland Hendry 20, 766
 Williams, Robert Chadwell 744
 Williams, Thomas 8
 Williams, Virginia Panayotova Vassilevska 352, 766
 Willsky, Alan Steven 368, 759
 Wilson, Richard Michael 88, 758
 Wilson, Sir John, theorem 422, 428
 Winkler, Franz 618, 738, 740, 749
 Winograd, Shmuel 352, 420, 741, 766
 Winter, Dik T. 533, 756
 Winterhof, Arne 421, 754
 witness
 Fermat ~ [519](#), 520, 522, 523, 534
 strong ~ [523](#), 532, 534
 van de Woestijne, Christiaan Evert 8
 Wolf, Stefan 580, 756
 Wolfram, Stephen 20
 Woltman, George Frederick 517
 Wong, Yiu-Chung 498, 750
 Woodall, H. J. 541, 741
 word [29](#), 30, 42
 operation [32](#), 34, 40
 Wrench, John William, Jr. 82, 763
 Wright, Edward Maitland 62, 421, 532, 534, 748
 Wu, Wen-tsün 618, 619, 745, 767
 Wunderlich, Marvin Charles 569, 766
 WZ-pairs 697
 x-adic
 expansion 131
 valuation 91, 94, [274](#), 275, 292
 Yagati Narayana Lakshman see Lakshman
 Yap, Chee Keng 618, 767
 Yee, Alexander Jih-Hing 82, 90, 767
 Yehudayoff, Amir 199, 763
 Yger, Alain 618, 737
 Yong, Huang 8
 Yoshino, S. 82
 Young, Ian Theodore 368, 759
 Yun, David Yuan Yee . . 198, 332, 419, 425, 466, 631,
 640, 738, 758, 767
 algorithm [395](#), 426, 440, 631
 \mathbb{Z} , ring of integers [768](#)
 \mathbb{Z} -module 349, [473](#)
 \mathbb{Z}_m , integers mod m [72](#)
 $\mathbb{Z}_{(p)}$, p -adic integers [275](#), [449](#)
 Zassenhaus, Hans Julius 382, 405–407, 417, 418,
 444, 466, 739, 767
 algorithm [453](#), 455–457, 497
 Zayer, Jörg 569, 741
 Zeilberger, Doron 632, 641, 643, 671, 676, 684,
 697, 729, 735, 740, 760, 766, 767
 Zermelo, Ernst Friedrich Ferdinand 586
 zero divisor 92, [227](#), [706](#), 713
 zeta function, ζ see Riemann zeta function
 Ziegler, Joachim 286, 739
 Ziegler, Konstantin Josef Franzisuks 8
 Zima, Eugene Viktorovich (Зима Евгений
 Викторович) 7, 671, 747
 Zimmermann, Paul 6–8, 465, 542, 697, 734, 744,
 751, 767
 Zimmermann, Philip R. 18, 767
 Zippel, Richard Eliot .. 198, 204, 498, 509, 763, 767
 \mathcal{ZPP} 518, [722](#), 723, 724