

Literaturverzeichnis

- [Abr2003] Abramov, S. A.: When does Zeilberger's algorithm succeed? *Advances in Applied Mathematics* **30**, 2003, 424–441.
- [AKS2004] Agarwal, M., Kayal, N., Saxena, N.: Primes is in P . *Annals of Mathematics* **160**, 2004, 781–793.
- [AGP1994] Alford, W. R., Granville, A., Pomerance, C.: There are infinitely many Carmichael numbers. *J. Ann. Math. II. Ser.* **139**, 1994, 703–722.
- [AZ1991] Almkvist, G., Zeilberger, D.: The method of differentiating under the integral sign. *J. Symbolic Computation* **10**, 1990, 571–591.
- [Bai1935] Bailey, W. N.: *Generalized Hypergeometric Series*. Cambridge University Press, England, 1935. Nachdruck 1964 durch Stechert-Hafner Service Agency, New York/London.
- [BDG1988] Balcázar, J. L., Díaz, J., Gabarró, J.: *Structural Complexity*. Springer, Heidelberg, 1988.
- [BHKS2005] Belabas, K., van Hoeij, M., Klüners, J., Steel, A.: *Factoring polynomials over global fields*, <http://www.mathematik.uni-kassel.de/~klueners/factor.pdf>.
- [Ber1967] Berlekamp, E. R.: Factoring polynomials over finite fields. *Bell System Technical Journal* **46**, 1967, 1853–1859.
- [BFKWZ1998] Betten, A., Fripertinger, H., Kerber, A., Wassermann, A., Zimmermann, K.-H.: *Codierungstheorie*. Springer, Berlin–Heidelberg, 1998.
- [Beu2005] Beutelspacher, A.: *Kryptologie*. Vieweg, Braunschweig/Wiesbaden, 7. Auflage, 2005. Erstauflage 1987.
- [Böi1998] Böing, H.: *Theorie und Anwendungen zur q -hypergeometrischen Summation*. Diplomarbeit, 1998, Freie Universität Berlin.
- [BW1963] Boveri, Th., Wasserrab, Th.: *Das Fischer-Lexikon Technik 4*, Fischer-Taschenbuch-Verlag, 1963.
- [Bro1997] Bronstein, M.: *Symbolic Integration I*. Springer, Berlin, 1997.
- [Buc1999] Buchmann, J.: *Einführung in die Kryptographie*. Springer, Berlin–Heidelberg, 1999.
- [BCS1997] Bürgisser, P., Clausen, M., Shokrollahi, M. A.: *Algebraic Complexity Theory*. Grundlehren der mathematischen Wissenschaften 315. Springer, Berlin–Heidelberg–New York, 1997.
- [Chi2000] Childs, L.: *A Concrete Introduction to Higher Algebra*. Springer, New York, 2. Auflage, 2000. Erstauflage 1979.
- [CC1986] Chudnovski, D. V., Chudnovski, G. V.: On expansion of algebraic functions in power and Puiseux series I. *Journal of Complexity* **2**, 1986, 271–294.
- [CC1987] Chudnovski, D. V., Chudnovski, G. V.: On expansion of algebraic functions in power and Puiseux series II. *Journal of Complexity* **3**, 1987, 1–25.
- [CLO1997] Cox, D., Little, J., O'Shea, D.: *Ideals, Varieties and Algorithms*. Springer, New York, 1997.
- [DeB1984] De Branges, L.: A proof of the Bieberbach conjecture. *Acta Math.* **154**, 1985, 137–152.

- [DH1976] Diffie, W., Hellman, M. E.: New directions in Cryptography. *IEEE Transactions on Information Theory* **6**, 1976, 644–654.
- [Eng1995] Engel, A.: Kann man mit DERIVE geometrische Sätze beweisen? In: Koepf, W. (Hg.): *Der Mathematik-Unterricht* 41, Heft 4, Juli 1995: *DERIVE-Projekte im Mathematikunterricht*, 38–47.
- [Erm1982] Ermolaev, H.: *Mikhail Sholokhov and his Art*. Princeton University Press, 1982.
- [Fas1945] Fasenmyer, M. C.: *Some Generalized Hypergeometric Polynomials*. Ph. D. Dissertation, University of Michigan, 1945.
- [For1996] Forster, O.: *Algorithmische Zahlentheorie*. Vieweg, Braunschweig/Wiesbaden, 1996.
- [GG1999] von zur Gathen, J., Gerhard, J.: *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.
- [GCL1992] Geddes, K. O., Czapor, S. R., Labahn, G.: *Algorithms for Computer Algebra*. Kluwer, Boston/Dordrecht/London, 1992.
- [Gos1978] Gosper Jr., R. W.: Decision procedure for indefinite hypergeometric summation. *Proc. Natl. Acad. Sci. USA* **75**, 1978, 40–42.
- [GKP1994] Graham, R. L., Knuth, D. E., Patashnik, O.: *Concrete Mathematics. A Foundation for Computer Science*. Addison-Wesley, Reading, Massachusetts, 2. Auflage, 1994. Erstaufgabe 1988.
- [Henn2003] Henn, H.-W.: *Elementare Geometrie und Algebra*. Vieweg, Braunschweig/Wiesbaden, 2003.
- [Her1975] Herstein, I. N.: *Topics in Algebra*. Wiley, New York, 1975.
- [Hoe2002] van Hoeij, M.: Factoring polynomials and the knapsack problem. *Journal of Number Theory* **95**, 2002, 167–189.
- [JS1992] Jenks, R. D., Sutor, R. S.: *AXIOM – The Scientific Computation System*. Springer, New York und NAG, Ltd., Oxford, 1992.
- [Jun1995] Jungnickel, D.: *Codierungstheorie*. Spektrum Akademischer Verlag, Heidelberg, 1995.
- [Kap2004] Kaplan, W.: *Computeralgebra*. Springer, Berlin–Heidelberg–New York, 2004.
- [Kar1962] Karatsuba, A.: Multiplication of multidigit numbers on automata. *Soviet Physics Doklady* **7**, Englische Ausgabe 1967, 595–596.
- [Karr1981] Karr, M.: Summation in finite terms. *J. of the ACM* **28**, 1981, 305–350.
- [Klü2005] Klüners, J.: Neuere Entwicklungen bei der Faktorisierung von Polynomen. *Rundbrief der Fachgruppe Computeralgebra* **37**, Oktober 2005, 16–20.
- [Kob2001] Koblitz, N.: Cryptography. In: Engquist, B., Schmid, W. (Hg.): *Mathematics Unlimited – 2001 and Beyond*, Springer, Berlin–Heidelberg–New York, 2001, 749–769.
- [Koe1992] Koepf, W.: Power series in computer algebra. *J. Symbolic Computation* **13**, 1992, 581–603.
- [Koe1993a] Koepf, W.: *Mathematik mit DERIVE*. Vieweg, Braunschweig/Wiesbaden, 1993.

- [Koe1993b] Koepf, W.: Eine Vorstellung von Mathematica und Bemerkungen zur Technik des Differenzierens. *Didaktik der Mathematik* **21**, 1993, 125–139.
- [Koe1994] Koepf, W.: *Höhere Analysis mit DERIVE*. Vieweg, Braunschweig/Wiesbaden, 1994.
- [Koe1996] Koepf, W.: Closed form Laurent-Puiseux series of algebraic functions. *Applicable Algebra in Engineering, Communication and Computing* **7**, 1996, 21–26.
- [Koe1998] Koepf, W.: *Hypergeometric Summation*. Vieweg, Braunschweig/Wiesbaden, 1998.
- [KBM1995] Koepf, W., Bernig, A., Melenk, H.: Trigsimp, a REDUCE Package for the Simplification and Factorization of Trigonometric and Hyperbolic Functions. In: Koepf, W. (Hg.): *REDUCE Packages on Power Series, Z-Transformation, Residues and Trigonometric Simplification*. Konrad-Zuse-Zentrum Berlin (ZIB), Technical Report TR 95–3, 1995.
- [Kro1882] Kronecker, L.: Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. Reine Angew. Math.* **92**, 1–122.
- [Kro1883] Kronecker, L.: Die Zerlegung der ganzen Grössen eines natürlichen Rationalitäts-Bereichs in ihre irreduciblen Factoren. *J. Reine Angew. Math.* **94**, 344–348.
- [Lam1844] Lamé, G.: Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nobres entiers. *Comptes Rendues Acad. Sci. Paris* **19**, 1944, 867–870.
- [LLL1982] Lenstra, A. K., Lenstra, H. W., Jr., Lovász, L.: Factoring polynomials with rational coefficients, *Math. Ann.* **261**, 1982, 515–534.
- [Lint2000] van Lint, J. H.: Die Mathematik der Compact Disc. In: Aigner, M., Behrends, E. (Hg.): *Alles Mathematik*, Vieweg, Braunschweig/Wiesbaden, 2000, 11–19.
- [Mae1997] Maeder, R. E.: *Programming in Mathematica*. Addison Wesley, Reading, Massachussets, 3. Auflage, 1997. Erstauflage 1990.
- [Mig1992] Mignotte, M.: *Mathematics for Computer Algebra*. Springer, New York, 1992.
- [MM2005] Mohammed, M., Zeilberger, D.: Sharp upper bounds for the orders of the recurrences outputted by the Zeilberger and q -Zeilberger algorithms. *J. Symbolic Computation* **39**, 2005, 201–207.
- [MM2001] Mulholland, J., Monagan, M.: Algorithms for trigonometric polynomials. *Proc. of ISSAC 2001*, ACM Press, New York, 2001, 245–252.
- [Nor1975] A. C. Norman: Computing with formal power series. *Transactions on Mathematical Software* **1**, ACM Press, New York, 1975, 346–356.
- [Ost1845] Ostrogradsky, M. W.: De l'intégration des fractions rationelles. Bulletin de la Classe Physico-Mathématiques de l'Académie Impériale des Sciences de St. Pétersbourg **IV**, 145–167, 286–300.
- [PS1995] Paule, P., Schorn, M.: A Mathematica version of Zeilberger's algorithm for proving binomial coefficient identities. *J. Symbolic Computation* **20**, 1995, 673–698.

- [PS1993] Petkovšek, M., Salvy, B.: Finding all hypergeometric solutions of linear differential equations. *Proc. of ISSAC 1993*, ACM Press, New York, 1993, 27–33.
- [PGP] PGP Homepage:
<http://www.pgpi.org>.
- [Ric1968] Richardson, D.: Some unsolvable problems involving elementary functions of a real variable. *J. Symbolic Logic* **33**, 1968, 511–520.
- [Rie1994] Riesel, Hans: *Prime Numbers and Computer Methods for Factorization*. Progress in Mathematics, Birkhäuser, Boston, 2. Auflage, 1994. Erstauflage 1985.
- [Rio1991] Rioboo, R.: *Quelques aspects du calcul exact avec des nombres réels*. Thèse de Doctorat de l'Université de Paris 6, Informatiques.
- [Ris1969] Risch, R.: The problem of integration in finite terms. *Trans. Amer. Math. Soc.* **139**, 1969, 167–189.
- [Ris1970] Risch, R.: The solution of the problem of integration in finite terms. *Bull. Amer. Math. Soc.* **76**, 1970, 605–608.
- [RSA1978] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public key cryptosystems. *Comm. ACM* **21**, 1978, 120–126.
- [Rob1936] Robertson, M. S.: A remark on the odd schlicht functions. *Bull. Amer. Math. Soc.* **42**, 1936, 366–370.
- [Rob1978] Robertson, M. S.: Complex powers of p -valent functions and subordination. *Complex Anal.*, Proc. S.U.N.Y. Conf., Brockport 1976, Lect. Notes Math. **36**, 1978, 1–33.
- [Rob1989] Robertson, M. S.: A subordination problem and a related class of polynomials. In: Srivastava, H. M., Owa, Sh. (Hg.): *Univalent Functions, Fractional Calculus, and Their Applications*. Ellis Horwood Limited, Chichester, 1989, 245–266.
- [Rot1976] Rothstein, M.: *Aspects of Symbolic Integration and Simplification of Exponential and Primitive Functions*. Dissertation, Univ. of Wisconsin, Madison, 1976.
- [Sal1990] Salomaa, A.: *Public-Key Cryptography*. Springer, Berlin, 1990.
- [SK2000] Schmersau, D., Koepf, W.: *Die reellen Zahlen als Fundament und Baustein der Analysis*. Oldenbourg, München, 2000.
- [SS1971] Schönhage, V., Strassen, A.: Schnelle Multiplikation großer Zahlen. *Computing*, 1971, 281–292.
- [Sch2003] Schulz, R. H.: *Codierungstheorie*. Vieweg, Braunschweig/Wiesbaden, 2. Auflage, 2003. Erstauflage 1991.
- [Spr2004] Sprenger, T.: Algorithmen für mehrfache Summen. Diplomarbeit, 2004, Universität Kassel.
- [Tef1999] Tefera, A.: A multiple integral evaluation inspired by the multi-WZ method. *Electronic J. Combinatorics* **6(1)**, 1999, 1–7.
- [Tef2002] Tefera, A.: MultInt, a MAPLE package for multiple integration by the WZ method. *J. Symbolic Computation* **34**, 2002, 329–353.
- [Tra1976] Trager, B.: Algebraic factoring and rational function integration. *Proc. SYMSAC 1976*, ACM Press, New York, 1976, 219–226.

- [Tro2004a] Trott, M.: *The Mathematica Guidebook for Graphics*. Springer, New York, 2004.
- [Tro2004b] Trott, M.: *The Mathematica Guidebook for Programming*. Springer, New York, 2004.
- [Tro2005] Trott, M.: *The Mathematica GuideBook for Symbolics*. Springer, New York, 2005.
- [Ver1976] Verbaeten, P.: *Rekursiebetrekkingen voor lineaire hypergeometrische functies*. Proefschrift voor het doctoraat in de toegepaste wetenschappen. Katholieke Universiteit te Leuven, Heverlee, België, 1976.
- [Wal2000] Walter, W.: *Gewöhnliche Differentialgleichungen*. Springer, Berlin/Heidelberg, 7. Auflage, 2000. Erstauflage 1972.
- [Wan1978] Wang, P. S.: An improved multivariate polynomial factorization algorithm. *Math. Comp.* **32**, 1978, 1215–1231.
- [Weg1997] Wegschaider, K.: *Computer Generated Proofs of Binomial Multi-Sum Identities*. Diplomarbeit, RISC Linz, 1997.
- [Wei2005a] Weisstein, E. W.: RSA Number. *MathWorld—A Wolfram Web Resource*. <http://mathworld.wolfram.com/RSANumber.html>.
- [Wei2005b] Weisstein, E. W.: RSA-200 Factored. *MathWorld—A Wolfram Web Resource*. <http://mathworld.wolfram.com/news/2005-05-10/rsa-200>.
- [Wei2005c] Weisstein, E. W.: RSA-640 Factored. *MathWorld—A Wolfram Web Resource*. <http://mathworld.wolfram.com/news/2005-11-08/rsa-640>.
- [Wes1999] Wester, M. (Hg.): *Computer Algebra Systems*. Wiley, Chichester, 1999.
- [WZ1992] Wilf, H. S., Zeilberger, D.: An algorithmic proof theory for hypergeometric (ordinary and “ q ”) multiset/integral identities. *Invent. Math.* **108**, 1992, 575–633.
- [Wie1999] Wiesenbauer, J.: Public-Key-Kryptosysteme in Theorie und Programmierung. *Schriftenreihe zur Didaktik der ÖMG* **30**, 1999, 144–159.
- [Wie2000] Wiesenbauer, J.: Using DERIVE to explore the Mathematics behind the RSA cryptosystem. In: Etchells, T., Leinbach, C., Pountney, D. (Hg.): *Proceedings of the 4th International DERIVE & TI-89/92 Conference Computer Algebra in Mathematics Education (Liverpool 2000)*, CD-ROM, bk-teachware, 2000.
- [Wol2003] Wolfram, St.: *The Mathematica Book*. Wolfram Media, 5. Auflage, 2003. Erstauflage 1988.
- [Zas1969] Zassenhaus, H.: On Hensel factorization I. *J. Number Theory* **1**, 1969, 291–311.
- [Zei1990a] Zeilberger, D.: A fast algorithm for proving terminating hypergeometric identities. *Discrete Math.* **80**, 1990, 207–211.
- [Zei1990b] Zeilberger, D.: A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.* **32**, 1990, 321–368.
- [Zip1993] Zippel, R.: *Effective Polynomial Computation*. Kluwer, Boston/Dordrecht/London, 1993.

Symbolverzeichnis

- π (Kreiszahl) 3
 $n!$ (Fakultät) 4
 \sqrt{x} (Quadratwurzel) 7
 $\sin x$ (Sinusfunktion) 7
 $\cos x$ (Kosinusfunktion) 7
 i, i (imaginäre Einheit) 8
 e, e (Eulersche Zahl) 8
 $\exp x$ (Exponentialfunktion) 8
 \mathbb{Z} (ganze Zahlen) 9, 64
 $R[x]$ (Polynomring) 9, 154
 \mathbb{Q} (rationale Zahlen) 10, 64
 \mathbb{Z}_p (Restklassenring) 10, 87, 90
 $\tan x$ (Tangensfunktion) 17
 $\arctan x$ (Arkustangensfunktion) 20, 469
 \mathbb{N} (natürliche Zahlen) 23, 55
 $\log x, \ln x$ (Logarithmusfunktion) 28, 40, 44, 447
 $\mathbb{N}_{\geq 0}$ (nichtnegative ganze Zahlen) 36
 $O(f(n))$ (Ordnungsterm, Landau-Symbol) 37, 53
 \mathbb{R} (reelle Zahlen) 45
 $\cot x$ (Kotangensfunktion) 47
 $\sec x$ (Sekansfunktion) 47, 314
 $\csc x$ (Kosekansfunktion) 47
 $z_n z_{n-1} \dots z_1 z_0$ (Zahldarstellung) 51
 $\log_B x$ (Logarithmus zur Basis B) 59
 $[r]$ (ganzzahliger Anteil) 64
 $\text{quotient}(x, y)$ (ganzzahlige Division) 65
 $\text{rest}(x, y), \text{mod}(x, y)$ (Rest bei der ganzzahligen Division) 65
 $a \mid b$ (a teilt b) 67
 $\text{gcd}(a, b), \text{gcd}(a_1, a_2, \dots, a_n)$ (größter gemeinsamer Teiler) 67
 $a \sim b$ (assozierte Zahlen) 67
 $\text{lcm}(a, b)$ (kleinstes gemeinsames Vielfaches) 68
 $\text{eukl}(a, b)$ (Euklidische Länge) 68
 \mathbb{P} (Primzahlen) 73
 $\mathbb{N}_{\geq 2}$ etc. (Teilmengennotation) 73
 $\text{sort}(p_1, \dots, p_n)$ (sortierte Liste) 73
 $(\mathbb{Z}, +, \cdot)$ (Ring der ganzen Zahlen) 87
 $a \equiv b \pmod{p}$ 87
 $[a]_p$ (Restklasse) 87
 $a \oplus b$ (modulare Addition) 89
 $a \otimes b$ (modulare Multiplikation) 89
 $(\mathbb{Z}_p, \oplus, \otimes)$ (Restklassenring) 89
 $a^{-1} \pmod{p}$ (modulares Inverses) 91
 $\text{char}(R)$ (Charakteristik) 91
 \mathbb{Z}_p^* (multiplikative Gruppe in \mathbb{Z}_p) 91
 $\text{GF}(q), \mathbb{F}_q$ (Galoisfeld) 91, 227
 $\sqrt{a} \pmod{p}$ (modulare Quadratwurzel) 93
 $\text{ord}(a)$ (Ordnung) 102
 $\log_a b \pmod{p}$ (modularer Logarithmus) 104
 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ (Alphabete) 121
 \mathcal{W} (Menge aller Wörter) 121
 $\mathbb{Z}[i]$ (Gaußsche ganze Zahlen) 153
 $\text{deg}(a(x), x)$ (Grad eines Polynoms) 154
 $\text{lcoeff}(a(x), x)$ (führender Koeffizient eines Polynoms) 155
 $\text{lterm}(a(x), x)$ (führender Term eines Polynoms) 155
 $R[x_1, \dots, x_n]$ (Polynomring in mehreren Variablen) 157
 $\text{quotient}(a(x), b(x), x)$ (Polynomquotient) 174
 $\text{rest}(a(x), b(x), x)$ (Polynomrest) 174
 $\text{gcd}(a(x), b(x))$ (größter gemeinsamer Teiler zweier Polynome) 181
 $\text{content}(a(x), x)$ (Inhalt eines Polynoms) 188, 261
 $\text{qf}(a(x), x)$ (quadratfreier Teil eines Polynoms) 193, 196
 $a'(x)$ (Ableitung) 193
 D, D_x (Differentialoperator) 194, 344, 397, 443
 $\mathbb{K}(x)$ (Körper der rationalen Funktionen) 198
 $\mathbb{K}(x_1, \dots, x_n)$ (Körper der rationalen Funktionen in mehreren Variablen) 198
 $a(x) \equiv b(x) \pmod{p(x)}$ (Kongruenz modulo eines Polynoms) 205
 $[a(x)]_{p(x)}$ (Restklasse modulo eines Polynoms) 205
 $\mathbb{K}[x]/\langle p(x) \rangle$ (Restklassenring modulo eines Polynoms) 205

- $\mathbb{K}(\alpha)$ (einfache Körpererweiterung durch Adjunktion) 207, 213
 $\mathbb{R}(i)$ (komplexe Zahlen als algebraischer Erweiterungskörper) 208
 $A \cong B$ (Isomorphie) 208
 $\mathbb{K}(\alpha, \beta, \dots)$ (mehrfache Körpererweiterung durch Adjunktion) 213
 $[\mathbb{E} : \mathbb{K}]$ (Grad einer endlichen Körpererweiterung) 215
 $\text{minpol}(\alpha, x)$, $\text{minpol}_{\mathbb{K}}(\alpha, x)$ (Minimalpolynom einer algebraischen Zahl) 218
 $\text{grad}(\alpha)$, $\text{grad}_{\mathbb{K}}(\alpha)$ (Grad einer algebraischen Zahl) 218
 \bar{z} (Konjugiertes einer komplexen Zahl) 220
 $\text{Re } z$ (Realteil einer komplexen Zahl) 220
 $\text{Im } z$ (Imaginärteil einer komplexen Zahl) 220
 $|z|$ (Absolutbetrag einer komplexen Zahl) 220
 \mathbb{K}^* (multiplikative Gruppe in einem Körper) 231
 $S(a(x), b(x), x)$ (Sylvestermatrix) 236
 $|M|$ (Determinante einer Matrix) 236
 $\text{res}(a(x), b(x), x)$ (Resultante) 237
 $\text{primpart}(a(x), x)$ (primitiver Teil eines Polynoms) 262
 $\dim V$ (Dimension eines Vektorraums) 272
 $\text{kern } A$ (Kern einer Matrix) 272
 $\text{arctanh } x$ (inverse hyperbolische Tangensfunktion) 297
 M/\sim (Quotientenmenge) 298
 $a \equiv b$ (Gleichheit) 298
 $R[x, y]/\langle x^2 + y^2 - 1 \rangle$ (Ring trigonometrischer Polynome) 305
 $\text{arcsinh } x$ (inverse hyperbolische Sinusfunktion) 314
 $\text{ord}(a(x), x)$ (Ordnung einer Potenzreihe) 317
 $R[[x]]$ (Potenzreihenring) 317
 $\mathbb{K}((x))$ (Körper formaler Laurentreihen) 322
 $\text{holgrad}(f(x), x)$ (holonomer Grad einer Funktion) 332
 $\Gamma(x)$ (Gammafunktion) 339, 375
 $\text{Ai}(x)$, $\text{Bi}(x)$ (Airyfunktionen) 339
 $\text{holgrad}(a_k, k)$ (holonomer Grad einer Folge) 343
 S_k (Vorwärtsshiftoperator) 344
 $(a)_k$ (Pochhammer-Symbol) 345
 ${}_pF_q \left(\begin{matrix} \text{upper} \\ \text{lower} \end{matrix} \middle| x \right)$ (allgemeine hypergeometrische Funktion) 350
 $H_n(x)$ (Hermitepolynome) 353
 $m \ll n$ (m wesentlich kleiner als n) 357
 $\text{algrad}(y(x), x)$ (Grad einer algebraischen Funktion) 359
 $L_n^{(\alpha)}(x)$ (Laguerrepolynome) 380
 $\theta F(x) = \theta_x F(x) = x F'(x)$ (Differentialoperator) 381, 398
 $P_n(x)$ (Legendrepolynome) 394
 I_a^b (Integraloperator) 397
 \int_x (Stammfunktion) 397
 Δ, Δ_k (Vorwärtsdifferenzenoperator) 397
 ∇, ∇_k (Rückwärtsdifferenzenoperator) 397
 \sum_k (unbestimmte Summe, diskrete Stammfunktion) 398
 $k^{\overline{n}}$ (steigende Faktorielle) 399
 $k^{\underline{n}}$ (fallende Faktorielle) 399
 H_k (harmonische Zahlen) 400
 \mathbb{K}_0 (Konstantenkörper) 443
 $\int g$ (Integral) 443
 $\mathbb{K}_{d(x)}$ (kleinster Zerfällungskörper) 456

Mathematica Stichwortverzeichnis

- eingebaute Funktionen
- \geq , $>=$ (größer gleich) 70
 - ∞ , Infinity (unendlich) 37
 - !, Factorial (Fakultät) 4, 344
 - !, Not (logisches „nicht“) 70, 128
 - #, Slot (Variable einer reinen Funktion) 29
 - #1, #2 (Variablen einer reinen Funktion) 34
 - %, Out (Ausgabe) 4, 44
 - &&, And (logisches „und“) 33
 - &, Function (reine Funktion) 29, 30, 34
 - ', Derivative (Ableitung einer Funktion) 35, 335
 - *, Times (Multiplikation) 7, 27, 31, 339
 - +, Plus (Addition) 3, 27
 - , (Argumenttrennung) 31
 - >, \rightarrow , Rule (Ersetzen) 9, 12
 - , Subtract (Subtraktion) 4, 28
 - . (Dezimalpunkt) 3
 - ., Dot (Skalarprodukt) 465
 - /., ReplaceAll (Einsetzen) 12
 - //., ReplaceRepeated (rekursives Einsetzen) 44, 70
 - // (Postfixform) 5
 - /;, Condition (Bedingung) 6
 - /, Divide (Division) 3, 27
 - ::, MessageName (Fehlermeldung) 112
 - :=, SetDelayed (verzögerte Zuweisung) 6, 30
 - :>, RuleDelayed (verzögertes Ersetzen) 43, 225
 - ;, (Anweisungstrennung) 31
 - <>, StringJoin (Verbinden einer Zeichenkette) 137
 - =, Set (Zuweisung) 7
 - ==, Equal (Gleichheit) 12, 43, 183, 298
 - ===, SameQ (syntaktische Gleichheit) 183, 298
 - ?, (Hilfestellung) 37
 - ?? (erweiterte Hilfestellung) 41, 463
 - [] (Funktionsaufruf) 3
 - [[]], Part (Element einer Liste) 15, 34
 - ^^ (*B*-adische Zahldarstellung) 52
 - ^, Power (Potenz) 4, 27
 - _, Blank (Variable, Muster) 6, 29
 - _. , Optional (erweitertes Muster) 40
 - _? (Fragemuster) 29
 - ' 1 ' (Variable für Fehlermeldung) 112
 - {}, List (Liste) 5, 27
 - () (Klammerung mathematischer Ausdrücke) 39
 - Abs (Absolutbetrag) 128, 305
 - AiryAi (Airyfunktion) 339, 380
 - AiryBi (Airyfunktion) 339, 380
 - And, && (logisches „und“) 33
 - Apart (Partialbruchzerlegung) 311
 - Append (Anhängen an eine Liste) 46, 48
 - AppendTo (Anhängen und Zuweisen) 70
 - Apply (Ersetzen des Kopfs) 31, 110, 132, 189, 262
 - ArcSin (Arkussinusfunktion) 42
 - ArcSinh (inverse hyperbolische Sinusfunktion) 314
 - ArcTan (Arkustangensfunktion) 42
 - ArcTanh (inverse hyperbolische Tangensfunktion) 297, 342
 - AspectRatio (Plot-Option) 35
 - Automatic (Wert einiger Optionen) 35, 466
 - BaseForm (*B*-adische Zahldarstellung) 52
 - BernoulliB (Bernoullische Zahlen) 328
 - Binomial (Binomialkoeffizient) 135, 159, 344, 389
 - Blank, _ (Variable, Muster) 6, 29
 - Cases (Fälle) 29
 - Ceiling (nächstgrößere ganze Zahl) 281
 - ChebyshevT (Chebyshevpolynome) 254
 - ChineseRemainder (chinesischer Restsatz) 97
 - Chop (Unterdrücken kleiner Dezimalzahlen) 165
 - Clear (Löschen einer Variablen/Funktion) 8, 44, 56

- Coefficient (Koeffizient eines Polynoms) 70, 156
 CoefficientList (Koeffizientenliste eines Polynoms) 156, 160, 214
 Collect (Sammeln nach Potenzen einer Variablen) 158, 302
 Complement (Mengenkomplement) 186
 Complex (komplexe Zahl) 27
 ComplexExpand (Auswertung über \mathbb{C}) 8, 471
 ComposeList (Iterationsliste) 32
 ComposeSeries (Komposition von Reihen) 324, 375
 Condition, /; (Bedingung) 6
 ContinuedFraction (Kettenbruch) 82
 ContourPlot (Höhenliniendiagramm) 18
 Cos (Kosinusfunktion) 7, 42, 297
 Count (Anzahl) 30
 Cyclotomic (zyklotomische Polynome) 293
 D (Ableitung eines Ausdrucks) 19, 40, 47
 DeleteCases (Teillöschung) 30
 Denominator (Nenner einer rationalen Funktion) 262
 Derivative, ' (Ableitung einer Funktion) 35, 47, 335
 Det (Determinante) 11
 \$DisplayFunction (Ausgabemedium) 257
 DisplayFunction (Plot-Option) 257
 Divide, / (Division) 3, 27
 Divisors (Teiler) 154, 189
 Do (Zählschleife) 31
 Dot, . (Skalarprodukt) 465
 DSolve (Lösung von Differentialgleichungen) 339, 379, 435
 ElementToPolynomial (Format endlicher Körper) 229
 Eliminate (Elimination von Variablen) 337
 Equal, == (Gleichheit) 12, 43, 183, 298
 Evaluate (Auswertung erzwingen) 470
 EvenQ (gerade?) 39
 Exp (Exponentialfunktion) 8, 27
 Expand (Ausmultiplizieren) 9, 45, 158, 297, 300, 303
 ExpandAll (Ausmultiplizieren) 407
 Exponent (Grad eines Polynoms) 241
 ExtendedGCD (erweiterter Euklidischer Algorithmus) 71, 92
 Extension (algebraischer Erweiterungskörper) 10, 466
 Factor (Polynomfaktorisierung) 9, 187, 192
 Factorial, ! (Fakultät) 4, 344
 FactorInteger (Faktorisierung ganzer Zahlen) 5, 75, 154
 FactorSquareFree (quadratfreie Faktorisierung eines Polynoms) 196, 275, 478
 FactorSquareFreeList (quadratfreie Faktorisierung eines Polynoms) 478
 Fibonacci (Fibonaccizahlen und -polynome) 38, 45
 FieldIrreducible (irreduzibles Polynom in \mathbb{Z}_p) 229
 First (erstes Element einer Liste) 46, 48
 FixedPoint (Fixpunktiteration) 32, 35, 368
 FixedPointList (Fixpunktiterationsliste) 32, 257, 368
 Flat (assoziativ) 41
 Flatten (Flachmachen von Listen) 29, 57, 95
 Floor (ganzzahliger Anteil) 65
 Fold (Iteration) 32, 34
 FoldList (Iterationsliste) 32
 For (for-Schleife) 32
 Fourier (diskrete Fouriertransformation) 165
 FourierParameters (diskrete Fouriertransformation) 165
 FreeQ (Unabhängigkeit) 40, 181
 FromCharacterCode (Zeichen aus ASCII-Code) 123

- FromContinuedFraction (Kettenbruch) 82
- FromDigits (periodische Dezimaldarstellung) 84
- FullForm (interne Darstellung) 27
- FullSimplify (Vereinfachung) 7, 214, 297, 310, 342
- Function, & (reine Funktion) 29, 30, 34
- FunctionExpand (Vereinfachung spezieller Funktionen) 389, 436
- FunctionOfCode (Format endlicher Körper) 228
- Gamma (Gammafunktion) 339, 375
- GaussianIntegers (komplexe Ganzzahlen) 10, 154
- GCD (größter gemeinsamer Teiler) 82, 262
- Graphics (Graphikroutine) 257
- Head (Kopf) 27
- Hold (Verhindern der Auswertung) 43
- Horner (Hornerverfahren) 83
- Hue (Farbfunktion) 18
- Hypergeometric2F1 (Gaußsche hypergeometrische Reihe) 351
- HypergeometricPFQ (allgemeine hypergeometrische Reihe) 351
- Identity (Plot-Option) 257
- IdentityMatrix (Einheitsmatrix) 273
- If (wenn, dann) 30, 298
- ImplicitPlot (impliziter Plot) 15
- In (Eingabe) 44
- Infinity, ∞ (unendlich) 37
- InputForm (Eingabeformat) 27, 300
- Integer (ganze Zahl) 27
- IntegerDigits (Ziffernfolge) 52
- IntegerExponent (Exponent der Primfaktorzerlegung) 112
- IntegerQ (ganze Zahl?) 29
- Integers (Vereinfachungsoption) 377
- Integrate (Integral) 19, 28, 309, 451
- InterpolatingPolynomial (Interpolationspolynom) 180, 190
- Inverse (inverse Matrix) 10
- InverseFourier (diskrete Fouriertransformation) 166
- InverseSeries (Inversion einer Reihe) 324, 374, 375
- IrreduciblePolynomial (irreduzibles Polynom in \mathbb{Z}_p) 229
- Join (Verbinden zweier Listen) 160, 241, 452
- LaguerreL (Laguerrepolynome) 380, 426
- LCM (kleinstes gemeinsames Vielfaches) 110, 262
- LegendreP (Legendrepolynome) 426
- Length (Länge einer Liste, Argumentanzahl) 52
- Limit (Grenzwert) 19, 159, 325, 436
- Line (Graphikroutine) 257
- LinearSolve (Lösen linearer Gleichungssysteme) 245
- List, {} (Liste) 5, 27
- Listable (Attribut einer Funktion) 463
- Log (Logarithmusfunktion) 28, 42, 44, 314, 342, 476
- Map (Anwendung einer Funktion auf die Teile eines Ausdrucks) 48
- MatrixForm (Matrizendarstellung) 5, 57, 92
- MatrixPower (Matrizenpotenz) 44
- Max (Maximum) 47
- Message (Fehlermeldung) 112
- MessageName, : : (Fehlermeldung) 112
- Mod (Divisionsrest) 65, 88, 279
- Module (Programmgruppe) 32
- Modulus (modulares Rechnen) 9, 92, 95, 132
- MultiplicativeOrder (multiplikative Ordnung) 103, 106, 118, 234
- N (numerischer Wert) 3
- Nest (Verkettung) 32, 34
- NestList (Verkettungsliste) 32, 241, 325
- NestWhile (bedingte Verkettung) 32
- NestWhileList (bedingte Verkettungsliste) 32
- NextPrime (nächste Primzahl) 98
- Normal (Umformung in ein Polynom) 323
- Not, ! (logisches „nicht“) 70, 128

- NSolve (numerisches Lösen von Gleichungen) 13
 Null (leeres Ergebnis) 31, 32, 138
 NullSpace (Kern einer Matrix) 245, 273
 Numerator (Zähler einer rationalen Funktion) 334
 O (Abbruchordnung) 321
 OddQ (ungerade?) 39
 Optional, _ . (erweitertes Muster) 40
 Options (Optionen) 17
 Orderless (kommutativ) 41
 Out, % (Ausgabe) 4, 44
 Outer (äußeres Produkt) 186, 189
 PadLeft (Anhängen führender Nullen) 160
 PadRight (Anhängen von Nullen) 166, 170, 241
 Part, [[]] (Element einer Liste) 15, 34
 Partition (Zerlegung einer Liste) 84, 123, 170, 189
 Plot (zweidimensionale Graphik) 17
 Plot3D (dreidimensionale Graphik) 17
 PlotPoints (Plot-Option) 18
 PlotRange (Plot-Option) 17
 PlotStyle (Plot-Option) 17
 Plus, + (Addition) 3, 27
 Pochhammer (Pochhammer-Symbol) 345
 PolynomialExtendedGCD (erweiterter Euklidischer Algorithmus) 184, 200, 211, 479
 PolynomialGCD (größter gemeinsamer Teiler von Polynomen) 181
 PolynomialMod (modulares Rechnen mit Polynomen) 209, 229
 PolynomialPowerMod (modulare Potenz eines Polynoms) 252
 PolynomialQuotient (Polynomdivision) 175, 182, 186
 PolynomialRemainder (Rest bei der Polynomdivision) 175, 182, 186, 209, 307
 Position (Position) 29, 95, 186, 191
 Power, ^ (Potenz) 4, 27
 PowerMod (modulare Potenz) 92, 100
 Prepend (Anhängen vorn) 46, 48
 PrependTo (Anhängen vorn und Zuweisen) 128
 Prime (n -te Primzahl) 114, 200, 285
 PrimeQ (prim?) 6, 76, 77, 154
 Print (Druckbefehl) 138, 412
 Product (Produkt) 15, 28, 31
 ProductLog (Lambertsche W -Funktion) 367
 ProvablePrimeQ (nachgewiesene Primzahl) 116
 Quotient (ganzzahlige Division) 65
 Random (Zufallszahl) 29, 62
 Range (Iterationsliste) 34
 Rational (rationale Zahl) 27
 Re (Realteil) 8
 Real (Dezimalzahl) 27
 RealDigits (periodische Dezimaldarstellung) 84
 \$RecursionLimit (Rekursionstiefe) 37, 44
 Remove (Löschen einer Variablen/Funktion) 334
 ReplaceAll, /. (Einsetzen) 12
 ReplaceRepeated, //. (rekursives Einsetzen) 44, 70
 Rest (Liste ohne erstes Element) 46, 48
 Resultant (Resultante) 239, 459
 Return (Abbruch einer Kontrollstruktur) 104
 Reverse (Umkehrung einer Liste) 47, 160, 241
 RGBColor (Rot-Grün-Blau-Farbenwert) 17
 Root (Nullstelle eines Polynoms) 15, 217, 226, 249
 RootReduce (algebraische Vereinfachung) 15, 214, 221, 226, 253
 RootSum (Summe über die Nullstellen eines Polynoms) 458
 RotateRight (zyklische Vertauschung einer Liste) 241
 Round (Runden reeller Zahlen) 45

- Rule, \rightarrow , \Rightarrow (Ersetzen) 9, 12
 RuleDelayed, $:=$ (verzögertes Ersetzen) 43, 225
 SameQ, $===$ (syntaktische Gleichheit) 183, 298
 Sec (Sekansfunktion) 314
 Select (Auswahl) 29
 Sequence (Argumentfolge) 189, 262, 264
 Series (Taylorpolynom) 19, 326
 SeriesData (interne Darstellung von Potenzreihen) 324, 374
 Set, = (Zuweisung) 7
 SetDelayed, $:=$ (verzögerte Zuweisung) 6, 30
 SetFieldFormat (Format endlicher Körper) 228
 Simplify (Vereinfachung) 7, 297, 310, 314
 Sin (Sinusfunktion) 7, 28, 42, 297
 Slot, # (Variable einer reinen Funktion) 29
 Solve (Lösen von Gleichungen) 12
 Sort (Sortieren) 73, 128
 Sqrt (Quadratwurzel) 7
 StringDrop (Ende einer Zeichenkette) 137
 StringJoin, <> (Verbinden einer Zeichenkette) 137
 StringReplace (Ersetzen in einer Zeichenkette) 134
 StringTake (Anfang einer Zeichenkette) 137
 Subtract, - (Subtraktion) 4, 28
 Sum (Summe) 4, 28
 Symbol (Symbol) 27
 Table (Listenerzeugung) 10, 31, 34
 Take (Teil einer Liste) 160
 Tan (Tangensfunktion) 17, 297
 Thickness (Graphikroutine) 257
 Times, * (Multiplikation) 7, 27, 31, 339
 Timing (Zeitmessung) 36, 44
 ToCharacterCode (ASCII-Nummer eines Zeichens) 123
 Together (rationale Normalform) 9, 198, 297, 304
 Trace (Ablaufprotokoll) 33, 57
 Transpose (Transponieren von Matrizen) 110, 190
 TrigExpand (trigonometrische Vereinfachung) 254, 307
 TrigFactor (trigonometrische Vereinfachung) 307, 314
 TrigFactorList (trigonometrische Vereinfachung) 307
 TrigReduce (trigonometrische Vereinfachung) 307, 309
 TrigToExp (trigonometrische Vereinfachung) 307
 Union (Vereinigung) 48, 74
 Unprotect (Löschen des Überschreibschutzes) 241
 Variables (Variablen eines Ausdrucks) 306
 Which (Fallunterscheidung) 31
 While (while-Schleife) 32, 70
- Konstanten**
 E (Eulersche Zahl e) 8
 False (falsch) 6
 I (imaginäre Einheit i) 8, 27
 Pi (Kreiszahl π) 3
 True (wahr) 6
- Menüs**
Abort Evaluation \rightarrow **Kernel, Abort Evaluation** 77
Palettes \rightarrow **File, Palettes** 3
TraditionalForm \rightarrow **Cell, Default Output Format Type, TraditionalForm** 5, 158, 300, 304, 321, 345
- Packages**
 "Algebra`FiniteFields`" 228, 254
 "Algebra`Horner`" 83
 "Algebra`PolynomialExtendedGCD`" 184, 211, 476, 479
 "Algebra`PolynomialPowerMod`" 186, 252
 "Algebra`SymmetricPolynomials`" 217, 278

- "Calculus`Limit`" 159
- "DiscreteMath`Combinatorica`" 128
- "Graphics`ImplicitPlot`" 15
- "NumberTheory`NumberTheory-Functions`" 97, 98
- "NumberTheory`PrimeQ`" 116
- "SpecialFunctions`" 329, 409
 - AlgebraicDE (Differentialgleichung einer algebraischen Funktion) 362, 382
 - DEtoRE (Differentialgleichung zu Rekursion) 348, 381
 - DiskreteStammfunktion (diskrete Stammfunktion) 431, 436
 - DispersionsMenge (Dispersionsmenge) 418, 436
 - FPS (formale Potenzreihen) 330, 380, 435
 - Gosper (Gosper-Algorithmus) 406, 409
 - GradSchranke (Gradschranke beim Gosper-Algorithmus) 412
 - holonomicDE (holonome Differentialgleichung) 334
 - HolonomicDE (holonome Differentialgleichung) 338
 - HolonomicRE (holonome Rekursionsgleichung) 344
 - hypergeometricPFQ (unevaluierete hypergeometrische Reihe) 352
 - HyperTerm (hypergeometrischer Term) 380
 - PowerDE (Differentialgleichung einer Potenz) 379
 - PrimDispersion (Primdispersion) 417
 - ProductDE (Differentialgleichung eines Produkts) 339, 378
 - ProductRE (Rekursionsgleichung eines Produkts) 344
 - REtoDE (Rekursion zu Differentialgleichung) 348, 382
 - REtoPol (Polynomlösung der Gosperrekursion) 414, 436
 - SimplifyCombinatorial (Vereinfachung kombinatorischer Ausdrücke) 423, 436
 - specfunprint (Verbosemodus) 330
 - specfunprintoff (Verbosemodus abstellen) 331
 - SumDE (Differentialgleichung einer Summe) 338
 - SumRE (Rekursionsgleichung einer Summe) 344
 - SumRekursion (Zeilberger-Algorithmus) 423
 - SumToHypergeometric (Umwandlung in hypergeometrische Notation) 352, 380, 435
 - Taylor (Taylorpolynom) 358
 - WZCertificate (Zertifikat der WZ-Methode) 431
 - Zb (Zeilberger-Algorithmus) 425
 - "zb_alg`" 330
 - Gosper (Gosper-Algorithmus) 406
 - Zb (Zeilberger-Algorithmus) 425
- selbstdefinierte Funktionen
 - Abbruchordnung (Abbruchordnung einer Potenzreihe) 374
 - Add (Langzahladdition) 81
 - AddZ (Additionstafel \mathbb{Z}_p) 92
 - AnzahlFaktoren (Berlekamp-Algorithmus) 273
 - AnzahlIrreduzibel (Anzahl irreduzibler Polynome) 255
 - Berlekamp (Berlekamp-Algorithmus) 269
 - CR (chinesischer Restsatz) 98
 - CaesarE (Entschlüsselung mit Caesarcode) 137
 - CaesarV (Verschlüsselung mit Caesarcode) 137
 - CheckISBNPrüfziffer (Testen einer ISBN-Nummer) 147
 - Content (Inhalt eines Polynoms) 201
 - Delta (Δ -Operator) 400
 - DEOrder (Ordnung einer Differentialgleichung) 47

- detore (Differentialgleichung zu Rekursion) 381
- Diff (Differentiation) 40, 47
- Digitalisiere (Buchstabennummer) 131
- digitstonumber (Zahlkonversion) 46
- DiskreterLogarithmus (diskreter Logarithmus) 104
- divisors (Teiler) 189
- DSolveTaylor (Taylorapproximation eines Anfangswertproblems) 383
- EANPrüfziffer (EAN-Prüfziffer) 148
- Eisenstein (Eisensteinkriterium) 201
- Entschlüssele (RSA-Entschlüsselung) 144
- Eratosthenes (Primzahlsieb) 84
- extendedgcd (erweiterter Euklidischer Algorithmus) 70, 182
- factorinteger (Faktorisierung ganzer Zahlen) 76, 77, 84
- Fak1 (Fakultät) 32
- Fak2 (Fakultät) 32
- Fak3 (Fakultät) 32
- Fak4 (Fakultät) 33
- Fak5 (Fakultät) 34
- Fak6 (Fakultät) 34
- Fak7 (Fakultät) 34
- Faktoren (Faktoren eines Polynoms modulo p) 186, 265
- fallendeFaktorielle (fallende Faktorielle) 400
- FallendeFaktorielle (fallende Faktorielle) 401
- FasenmyerDE (Differentialgleichung einer definiten Summe) 434, 435
- FasenmyerRE (Rekursionsgleichung einer definiten Summe) 393, 435
- FastImplicitTaylor (Taylorpolynom) 372
- FastNextCarmichael (Carmichaelzahl) 110
- FFT (schnelle Fouriertransformation) 170
- Fib1 (Fibonaccizahlen) 36
- Fib2 (Fibonaccizahlen) 37
- FixedPointGraph (graphische Darstellung des Fixpunktverfahrens) 257
- FixedPointRestGraph (graphische Darstellung des Fixpunktverfahrens) 257
- Grad (Polynomgrad) 47
- HenselLifting (Hensel-Lifting) 286
- HilbertMatrix (Hilbertmatrix) 10
- Horner (Hornerverfahren) 83
- Huffman (Huffman-Code) 128
- HuffmanList (Huffman-Code) 128
- hypDE (hypergeometrische Differentialgleichung) 381
- hyperTerm (hypergeometrischer Term) 380
- IFFT (schnelle Fouriertransformation) 170
- ImplicitTaylor (Taylorpolynom) 365
- ImplicitTaylor2 (Taylorpolynom) 370
- ImplicitTaylor3 (Taylorpolynom) 371
- InitialisiereRSA (Initialisierung des RSA-Verfahrens) 144
- InverseReedSolomon (Reed-Solomon-Code) 134, 150, 255
- inverseSeries (Inversion einer Reihe) 375
- ISBNPrüfziffer (ISBN-Prüfziffer) 147
- Karatsuba (Langzahlmultiplikation) 60
- Kehrwert (Kehrwert einer Potenzreihe) 374
- kfreieDE (k -freie Differentialgleichung) 434
- kfreieRE (k -freie Rekursionsgleichung) 390
- Kronecker (Kronecker-Algorithmus zur Polynomfaktorisierung) 201
- Lagrange (Interpolationspolynom) 180
- lcoeff (führender Koeffizient eines Polynoms) 255
- ListKaratsuba (Multiplikation von Polynomen) 160
- ListToNumber (Konversion von ASCII-Nummern in Zahl) 143
- LogToArcTan (Rioboo-Algorithmus) 476
- makemoniC (normiertes Polynom) 463
- MinErzeuger (minimaler Erzeuger) 103

- ModularLog (modularer Logarithmus) 118
 ModularSqrt (modulare Quadratwurzel) 95
 Multiply (Langzahlmultiplikation) 56
 MultZ (Multiplikationstafel \mathbb{Z}_p^*) 92
 MultZ0 (Multiplikationstafel \mathbb{Z}_p) 92
 NewtonListe (Newtonverfahren) 368
 NewtonVerfahren (Newtonverfahren) 35, 368
 NextCarmichael (Carmichaelzahl) 108
 NextPrime (nächste Primzahl) 6, 76, 200
 Nullstellen (Nullstellen eines Polynoms über \mathbb{Z}_p) 291
 numbertodigits (Zahlkonversion) 46
 NumberToList (Konversion einer Zahl in ASCII-Nummern) 143
 NumberToText (Konversion einer Zahl in einen Text) 143
 Ordnung (Ordnung einer Potenzreihe) 374
 PolynomialCR (chinesischer Restsatz für Polynome) 211
 PolynomialKaratsuba (Multiplikation von Polynomen) 160
 PolynomialModInverse (modulares Inverses eines Polynoms) 252
 Potenzmenge (Potenzmenge) 47
 power (ganzzahlige Potenz) 117
 powermod (modulare Potenz) 100, 117
 PowerSeriesQ (Potenzreihe?) 374
 PrimitiverTeil (Erzeugung eines primitiven Polynoms) 262
 QuadratfreieFaktorisierung (quadratfreie Faktorisierung eines Polynoms) 202
 QuadratfreierTeil (quadratfreier Teil eines Polynoms) 202
 RabinMillerPrime (Rabin-Miller-Test) 112
 RationaleNullstellen (rationale Nullstellen eines Polynoms) 291
 RationaleZerlegung (Zerlegung eines rationalen Integrals) 453, 479
 ReedSolomon (Reed-Solomon-Code) 132, 150, 255
 resultant (Resultante) 239
 retode (Rekursion zu Differentialgleichung) 382
 reverse (Umkehrung einer Liste) 47
 RothsteinTrager (Rothstein-Trager-Algorithmus) 465
 SeriesSqrt (Quadratwurzel einer Potenzreihe) 375
 Summation (diskrete Stammfunktion) 401
 SylvesterMatrix (Sylvestermatrix) 241, 255
 SymmetricPolynomialMod (symmetrische Modulofunktion) 279
 Taylor (Taylorpolynom) 325
 Teilmengen (Teilmengen einer Menge) 48
 TextToNumber (Konversion eines Texts in eine Zahl) 143
 Vandermonde (Vandermonde-Matrix) 11
 Variable (Variable einer Potenzreihe) 374
 Verbalisiere (zu Nummer gehöriger Buchstabe) 131
 Verschlüssele (RSA-Verschlüsselung) 144
 ZassenhausSchranke (Zassenhaus-schranke) 280

Stichwortverzeichnis

- Abbruch einer Kontrollstruktur (Return) 104
- Abbruch einer Rechnung in *Mathematica* 77
- Abbruchbedingung 6, 33
- Abbruchordnung einer Potenzreihe (O) 321
- abgebrochene Reihen 321
- Ablaufprotokoll (Trace) 33, 57
- Ableitung 193, 443
 - einer Funktion (', Derivative) 35, 47, 335
 - eines Ausdrucks (D) 19, 40, 47
- Ableitungsregeln 40
- Abrunden (Floor) 65
- Absolutbetrag (Abs) 128, 305
- Absolutglied 317
- Addition 53
 - +, Plus 3, 27
 - Übertrag 53
- Additionstafel Z_p (AddZ) 92
- Additionstheorem, trigonometrisches 307
- Adjunktion 156, 213
- Äquivalenzklasse 67, 87, 205, 298
- Äquivalenzrelation 67, 87, 298
- äußeres Produkt (Outer) 186, 189
- Airyfunktionen (AiryAi, AiryBi) 339, 380
- algebraische Funktion 340, 359
 - Grad 359
 - Graph 359
 - Zweig 359, 363
- algebraische Körpererweiterung 223, 247
- algebraische Vereinfachung (RootReduce)
 - 15, 214, 221, 226, 253
- algebraische Zahl 218
 - Grad 218
 - Minimalpolynom 218
 - über einem Körper 218
- algebraischer Erweiterungskörper 207
 - Automatic 466
 - Extension 10, 466
- algorithmisches Rechnen 51
- Algorithmus
 - deterministischer 116
 - Divide-and-Conquer 39, 55, 58, 100, 159, 160, 168, 313, 368
 - effizienter 38, 77, 95, 107
 - erweiterter Euklidischer 68, 70
 - für Polynome 182
 - Euklidischer 68
 - für Polynome 181
 - exponentieller 77, 95, 107
 - Fasenmyer 395
 - Gaußscher 243
 - Gosper (Gosper) 406, 409
 - Karatsuba 58, 159, 160
 - polynomialer 116
 - probabilistischer 115
 - Schönhage-Strassen 199
- allgemeine hypergeometrische Reihe (HypergeometricPFQ) 350, 351
- Alphabet 121
- Analysis 19
- Anfang einer Zeichenkette (StringTake) 137
- Anfangsbedingung 33
- Anfangswertproblem, Taylorapproximation (DSolveTaylor) 383
- Anhängen an eine Liste
 - Append 46, 48
 - vorn (Prepend) 46, 48
- Anhängen führender Nullen (PadLeft) 160
- Anhängen und Zuweisen
 - AppendTo 70
 - vorn (PrependTo) 128
- Anhängen von Nullen (PadRight) 166, 170, 241
- Anweisungstrennung (;) 31
- Anwendung einer Funktion auf die Teile eines Ausdrucks (Map) 48
- Anzahl (Count) 30
- Anzahl irreduzibler Polynome (AnzahlIrreduzibel) 255
- arabisches Zahlssystem 51
- Argument eines Ausdrucks 27
- Argumentanzahl (Length) 52

- Argumentfolge (Sequence) 189, 262, 264
- Argumenttrennung (,) 31
- Arithmetik, rational exakt 4
- arithmetische Menge 87
- Arkussinusfunktion (ArcSin) 42
- Arkustangens über einem Körper 469
- Arkustangensfunktion (ArcTan) 20, 42, 469, 476
- ASCII-Nummer eines Zeichens (ToCharacterCode) 123
- ASCII-Zeichensatz 122
- assoziativ (Flat) 41
- assoziierte Zahlen 67
- asymmetrisches Verschlüsselungsverfahren 140
- asymptotische Äquivalenz 159
- asymptotische Reihe 318
- Attribut einer Funktion
 - Flat 41
 - Listable 463
 - Orderless 41
- Aufrunden (Ceiling) 281
- Ausblenden einer graphischen Darstellung
 - (DisplayFunction \rightarrow Identity) 257
- ausdividieren 176
- Ausdruck 27
 - Argument 27
 - Kopf 27
- Ausgabe (% , Out) 4, 44
- Ausgabeunterdrückung (;) 44
- Ausmultiplizieren
 - Expand 9, 45, 158, 297, 300, 303
 - ExpandAll 407
- ausmultipliziertes Polynom 155
- Auswahl (Select) 29
- Auswertung
 - erzwingen (Evaluate) 470
 - verhindern (Hold) 43
- Auswertung über \mathbb{C} (ComplexExpand) 8, 471
- Auswertung in *Mathematica* 298
- automatische Vereinfachung 27, 314
- Axiom* 21, 321
- B*-adische Zahldarstellung 51
- BaseForm, \wedge 52
- BasicInput Palette 3
- Basis des Zahlensystems 51
- Basis eines Vektorraums 215, 336
- bedingte Verkettung (NestWhile) 32
- bedingte Verkettungsliste (NestWhileList) 32
- Bedingung (/ ; , Condition) 6
- Benutzerauthentifikation 140
- berechenbare Funktion 299
- Berechnung abgebrochener Potenzreihen
 - (Series) 19, 326
- Berlekamp-Algorithmus 267
 - AnzahlFaktoren 273
 - Berlekamp 269
 - Teil II 272
- Bernoulli-Algorithmus zur rationalen Integration 441
- Bernoullische Zahlen (BernoulliB) 328, 378
- Besselfunktionen 435
- bestimmte Summation 387
- Betrag (Abs) 128, 305
- Bézoutkoeffizienten 70, 182, 184
- Bildschirm 121
- binäres Zahlssystem 51
- Binomialkoeffizient (Binomial) 99, 135, 159, 344, 389
- Binomialverteilung 135
- binomische Formel 99, 159, 318, 388, 428
- Bit 122
- Bitlänge 122
- Blockcode 125
- Blocklänge 125
- Buchstabe 121
 - zu Nummer gehöriger (Verbalisiere) 131
- Buchstabenhäufigkeit 126
- Buchstabennummer (Digitalisiere) 131
- Byte 122
- Caesarcode 125, 137
 - CaesarE 137
 - CaesarV 137

- Cardanische Formeln 13
- Carmichaelzahl 108
 - FastNextCarmichael 110
 - NextCarmichael 108
- casus irreducibilis 13
- Cauchyprodukt 155, 437
- Ceiling-Funktion (Ceiling) 281
- Charakteristik 91
- Chebyshevpolynome (ChebyshevT) 254
- chiffrieren 136
- chinesischer Restsatz
 - ChineseRemainder 97
 - CR 98
 - für Polynome (PolynomialCR) 210, 211
- Chu-Vandermonde-Identität 430, 437, 438
- Clausensche Formel 437
- Clausensche hypergeometrische Reihe 350
- Code 121
 - baum 128
 - Block- 125
 - Huffman- 127
 - Präfix- 125
 - wort 124
- Codierung 121
- Codierungstheorie 121
- Computerbildschirm 121
- Computerdatei 121
- Computerfestplatte 121
- Computertastatur 121
- Cosinusfunktion (Cos) 7, 42, 297

- dechiffrieren 136
- Decodierung 124
- definite Summe, Differentialgleichung
 - (FasenmyerDE) 434, 435
- definite Summe, Rekursionsgleichung
 - (FasenmyerRE) 393, 435
- Deklaration von Variablen 4
- Δ -Operator (Delta) 400
- Derive 21, 214
- Designfehler in *Mathematica* 314
- Determinante (Det) 11
- deterministischer Algorithmus 116
- Dezimaldarstellung 51
 - periodische (RealDigits, FromDigits) 84
- Dezimalpunkt (.) 3
- Dezimalrauschen 343
- Dezimalsystem 52
- Dezimalwert (N) 3
- Dezimalzahl (Real) 27
 - Unterdrücken (Chop) 165
- Differentialalgebra 445
- Differential-Erweiterungskörper 447
- Differentialgleichung
 - einer algebraischen Funktion (Algebraic-DE) 362, 382
 - einer definiten Summe (FasenmyerDE) 434, 435
 - einer Potenz (PowerDE) 379
 - einer Summe (SumDE) 338
 - eines Produkts (ProductDE) 339, 378
 - erster Ordnung 331, 333, 340
 - explizite 361, 366
 - holonome (holonomicDE, Holonomic-DE) 332, 334, 338
 - homogene 332
 - hypergeometrische (hypDE) 381
 - k -freie (kfreieDE) 434
 - Kompatibilität 341
 - lineare 332
 - Lösung (DSolve) 339, 379, 435
 - Taylorapproximation (DSolveTaylor) 383
- Differentialgleichung zu Rekursion
 - DEtoRE 348, 381
 - detore 381
- Differentialkörper 193, 443
- Differentialoperator 344, 397, 443
- Differentiation
 - D 19, 40, 47
 - Diff 40, 47
- Differentiationsregeln 40
- Differenzenoperator 397
- Differenzenrechnung 396, 397
- Diffie-Hellman-Schlüsselvereinbarung 141
- digitale Signatur 140
- digitalisierte Musik 121

- Dimension eines Vektorraums 215, 272, 336
- diskrete Fouriertransformation 163
 - Fourier 165
 - inverse (InverseFourier) 165, 166
- diskrete Stammfunktion 397, 398
 - DiskreteStammfunktion 431, 436
 - Summation 401
- diskreter Logarithmus 104
 - DiskreterLogarithmus 104
 - ModularLog 118
- Diskriminante eines Polynoms 256
- Dispersion 255, 406
- Dispersionsmenge 415, 416
 - DispersionsMenge 418, 436
- distributive Darstellung von Polynomen mehrerer Variablen 157
- distributive kanonische Form 303
- Divide-and-Conquer-Algorithmus
 - FFT 168
 - Fibonaccizahlen 39
 - Hensel-Lifting 282
 - Karatsuba 58, 159, 160
 - Langzahlmultiplikation 55, 368
 - modulare Potenz 100
 - trigonometrische Expansion 313
- dividierte Differenzen 200
- Division (/ , Divide) 3, 27
- Division mit Rest
 - für ganze Zahlen
 - Mod 65
 - Quotient 65
 - für Polynome 174
 - PolynomialQuotient 175
 - PolynomialRemainder 175, 182, 209, 307
- Divisionsalgorithmus 64
 - Quotient 65
- Divisionsrest (Mod) 65, 88, 279
- Dixon-Identität 437, 438
- Dougall-Identität 437, 438
- dreidimensionale Graphik (Plot3D) 17
- Dreiecksform eines linearen Gleichungssystems 243
- dreiwertige Logik 31
- Druckbefehl (Print) 138, 412
- durchführbares kryptographisches Verfahren 141
- dynamische Speicherverwaltung 4
- EAN-Prüfziffer 130, 148
 - EANPrüfziffer 148
- eckige Klammern 3, 154
- effizienter Algorithmus 38, 77, 95, 107
- effizientes Rechnen 51
- effizientes Verschlüsselungsverfahren 140
- Eigenfunktionen 398
- Eindeutigkeit der Primfaktorzerlegung 73
 - in Polynomringen 185
 - in Polynomringen mit mehreren Variablen 202
- einfache Körpererweiterung 213
- einfache Nullstelle 185
- Eingabe (In) 44
- Eingabeformat (InputForm) 27, 300
- Einheit 67
- Einheitengruppe 81
- Einheitsmatrix (IdentityMatrix) 273
- Einheitswurzel, primitive 163
- Einmaleins 53
- Einscannen 130
- Einsetzen
 - /. , ReplaceAll 12
 - rekursives (//. , ReplaceRepeated) 44, 70
- Einsetzungshomomorphismus 199
- Einspolynom 154
- Einsteinsche Formel 24
- Einwegfunktion 141
- Eisensteinsches Irreduzibilitätskriterium (Eisenstein) 201
- Element einer Liste ([[]], Part) 15, 34
- elementarsymmetrische Polynome 217, 278
- Elimination von Variablen (Eliminate) 337
- Ellipse 16
- elliptische Kurve 116, 146
- E-Mail 121
- Empfänger 121
- Ende einer Zeichenkette (StringDrop) 137

- endliche Körpererweiterung 214
- endlicher Körper 227
 - Format (ElementToPolynomial, FunctionOfCode, SetFieldFormat) 228, 229
 - irreduzibles Polynom (FieldIrreducible, IrreduciblePolynomial) 229
- endlicher Träger 420
- Endlosschleife 33
- Entfernen einer Variablen/Funktion (Remove) 334
- Entschachtelung von Wurzelausdrücken 222
- Entschlüsselung 136
 - mit Caesarcode (CaesarV) 137
 - mit RSA (Entschlüssele) 142, 144
- Eratosthenes 84
- Ersetzen (->, →, Rule) 9, 12
- Ersetzen des Kopfs (Apply) 31, 110, 132, 189, 262
- Ersetzen in einer Zeichenkette (StringReplace) 134
- erstes Element einer Liste (First) 46, 48
- Erwartungswert 136
- erweiterte Hilfestellung (??) 41, 463
- erweiterter ASCII-Zeichensatz 122
- erweiterter Euklidischer Algorithmus 68, 70
 - ExtendedGCD 71, 92
 - extendedgcd 70, 182
 - für Polynome 182
 - PolynomialExtendedGCD 184, 200, 211, 479
- erweitertes Muster (., Optional) 40
- Erweiterungskörper 447
- erzeugende Funktion 45, 318, 328
- erzeugendes Element 102
 - MinErzeuger 103
- Erzeugung einer Liste (Table) 10, 31, 34
- Erzeugung eines primitiven Polynoms (PrimitiverTeil) 262
- Erzwingen der Auswertung (Evaluate) 470
- Euklidische Länge 68
- Euklidische Norm 199
- Euklidischer Algorithmus 68
 - erweiterter 70
 - für Polynome 181
 - für Polynome, erweiterter 182
- Eulersche Gammafunktion (Gamma) 375
- Evaluierung in *Mathematica* 298
- exakte Arithmetik 4
- expandiertes Polynom 155
- explizite Differentialgleichung erster Ordnung 361, 366
- exp-log-Funktionen 441
- Exponent der Primfaktorzerlegung (IntegerExponent) 112
- Exponentialfunktion (Exp) 8, 27
- exponentielle erzeugende Funktion 328
- exponentielle Komplexität 77, 95
- expression swell 251, 265
- factorial, shifted 345, 349
- Fälle (Cases) 29
- Faktoren eines Polynoms modulo p (Faktoren) 186, 265
- Faktorielle, fallende 399
- Faktorielle, steigende 399
- faktorieller Ring 199, 310
- faktorisierbare Zahl 73
- Faktorisierung
 - Berlekamp-Algorithmus 267, 272
 - ganzer Zahlen
 - FactorInteger 5, 75, 154
 - factorinteger 76, 77, 84
 - quadratfrei 193
 - von Polynomen
 - über \mathbb{R} 442
 - über \mathbb{Z} 188
 - über \mathbb{Z} (Kronecker) 201
 - über \mathbb{Z}_p (Faktoren) 186
- Faktorisierungsweltrekord 78, 142
- Faktorring 199, 310
- Faktorzerlegung
 - ganzer Zahlen 73
 - von Polynomen 185
- Fakultät
 - !, Factorial 4
 - Fak1 32

- Fak2 32
- Fak3 32
- Fak4 33
- Fak5 34
- Fak6 34
- Fak7 34
- fallende Faktorielle 399
 - FallendeFaktorielle 401
 - fallendeFaktorielle 400
- Fallunterscheidung (/ ; , Condition) 6
- Fallunterscheidung (Which) 31
- falsch (False) 6
- Farbenwert (RGBColor) 17
- Farbfunktion (Hue) 18
- Fasenmyer-Algorithmus 395
- Fehlerfunktion 356
- Fehlermeldung
 - : , MessageName 112
 - Message 112
 - Variable (` 1 `) 112
- Fermat, kleiner Satz von 99
- Fermatsche Pseudoprimzahl 108
- Fermatsche Zahl 83, 118
- Fermatscher Zeuge 108
- Fermattest 108
- Festplatte 121
- FFT 163
 - FFT, IFFT 170
- Fibonaccizahlen und -polynome 36, 45
 - Fib1 36
 - Fib2 37
 - Fibonacci 38, 45
- Fixpunkt 150
- Fixpunktiteration (FixedPoint) 32, 35, 368
- Fixpunktiterationsliste (FixedPointList) 32, 257, 368
- Fixpunktverfahren, graphische Darstellung
 - FixedPointGraph 257
 - FixedPointRestGraph 257
- Flachmachen von Listen (Flatten) 29, 57, 95
- Floor-Funktion (Floor) 65
- Folge (Sequence) 189, 262, 264
- for-Schleife (For) 32
- formale
 - Laurentreihen 322
 - Potenzreihen 317
 - FPS 330, 380, 435
 - Puiseuxreihen 323
- Format endlicher Körper (ElementToPolynomial, FunctionOfCode, SetFieldFormat) 228, 229
- Fouriertransformation 163
 - FFT, IFFT 170
 - Fourier 165
 - InverseFourier 166
- Fragemuster (_ ?) 29
- führender Koeffizient eines Polynoms 154
 - lcoeff 255
- führender Term eines Polynoms 155
- Fundamentalsatz der Algebra 216
- Fundamentalsatz der Zahlentheorie 74
- Funktion
 - algebraische 340
 - reine 29
 - vom hypergeometrischen Typ 355
- Funktionsaufruf ([]) 3
- Galoisfeld ($GF(q)$, F_q) 91, 136, 227
 - $GF(9)$ 118
- Gammafunktion (Gamma) 339, 375
- ganze Zahl (Integer) 27
- ganze Zahl? (IntegerQ) 29
- Ganzzahlarithmetik 51
- ganzzahlige Division (Quotient) 65
- ganzzahlige Potenz (power) 117
- ganzzahliger Anteil (Floor) 65
- ganzzahliger Quotient 64
- Gaußsche ganze Zahlen 153
 - GaussianIntegers 10, 154
- Gaußsche hypergeometrische Reihe (Hypergeometric2F1) 350, 351
- Gaußscher Algorithmus 243
- Gaußsches Lemma 264
- Geheimtext 136
- gemeinsamer Teiler, größter 67
- general number field sieve 78
- generischer Fall 246

- gerade? (EvenQ) 39
- gerader Anteil einer Funktion 332
- gestörter Kanal 121
- Gitterreduktionsverfahren, LLL 291
- Gleichheit
 - `==`, Equal 12, 43, 183, 298
 - syntaktische (`===`, SameQ) 183, 298
- Gleichungslösen (Solve) 12, 92, 132, 245, 249
- Gleichungslösen, numerisches (NSolve) 13
- Gleichungssystem 12
 - Dreiecksform eines linearen 243
 - Lösungsmenge eines linearen 243
 - Lösungsmenge eines polynomialen 246
 - Rücksubstitution 244
- Gleichwertigkeit, mathematische 298
- globale Variable 71, 366
- Gosper-Algorithmus (Gosper) 406, 409
- Gospersummierbarkeit 404
- Grad
 - einer algebraischen Funktion 359
 - einer algebraischen Zahl 218
 - einer endlichen Körpererweiterung 214
 - einer holonomen Funktion 332
 - eines Polynoms 154
 - Exponent 241
 - Grad 47
- Gradsatz 252
- Gradschranke 411
 - GradSchranke 412
- Graph einer algebraischen Funktion 359
- Graphikroutine (Graphics) 257
 - Line 257
 - Thickness 257
- graphische Darstellung 17
 - Ausblenden (DisplayFunction \rightarrow Identity) 257
 - ContourPlot 18
 - des Fixpunktverfahrens
 - FixedPointGraph 257
 - FixedPointRestGraph 257
 - ImplicitPlot 15
 - Plot 17
 - Plot3D 17
- Grenzwert (Limit) 19, 159, 325, 436
- Gröbnerbasis 251
- größer gleich (\geq , $>=$) 70
- größte bekannte Primzahl 22
- größter gemeinsamer Teiler 67
 - GCD 82, 262
 - von Polynomen (PolynomialGCD) 181
- Häufigkeitsverteilung 126
- harmonische Zahlen 400
- Hashfunktion 141
- hebbare Singularität 325
- Hensel-Lifting (HenselLifting) 282, 286
- Hermite-Reduktion 478
- Hermitepolynome (HermiteH) 353
- Hexadezimalsystem 51
- Hilbertmatrix (Hilbertmatrix) 10
- Hilfestellung
 - ? 37
 - erweiterte (??) 41, 463
- Höhenliniendiagramm 18
 - ContourPlot 18
- Hofstadter-Determinante 313
- holonome/r
 - Differentialgleichung 332
 - HolonomicDE 338
 - einer algebraischen Funktion (AlgebraicDE) 362, 382
 - Folge 343
 - Folgenring 344
 - Funktion 332
 - Funktionsring 336
 - Grad 332
 - Rekursionsgleichung 343
 - HolonomicRE 344
- homogene Differentialgleichung 332
- homogene Rekursionsgleichung 343
- Hornerverfahren (Horner) 83
- Huffman-Code 127
 - Huffman, HuffmanList 128
- Hyperbel 16
- hyperbolische Funktionen 20
- hyperbolische Tangensfunktion, inverse (ArcTanh) 297, 342

- hyperexponentielle Funktion 434, 441
- hypergeometrische/r
 - Differentialgleichung (`hypDE`) 381
 - Funktion 350
 - Reihe 349, 350
 - Clausensche 350
 - Gaußsche 350
 - `Hypergeometric1F1` 351
 - `Hypergeometric2F1` 351
 - `HypergeometricPFQ` 351
 - Kummersche 350
 - obere Parameter 350
 - Umwandlung (`SumToHypergeometric`) 352, 380, 435
 - unevaluiert (`hypergeometricPFQ`) 352
 - untere Parameter 350
 - Term 350
 - `HyperTerm` 380
 - `hyperTerm` 380
 - Typ 355
- Ideal 251
- Identifikationsproblem 300
- identische Ausdrücke 298
- Identitätssatz für Polynome 177
- implizite Funktion 364
- impliziter Plot (`ImplicitPlot`) 15
- Informationsrate 135
- Inhalt eines Polynoms 188, 261
 - `Content` 201
- Initialisierung des RSA-Verfahrens (`InitialisiererRSA`) 144
- Integral 443
 - `Integrate` 19, 28, 309, 451
- Integraloperator 397
- Integrationsvariable 445
- Integritätsbereich 153
- Integritätsring 153
- intermediate expression swell 183, 251, 265
- interne Darstellung (`FullForm`) 27
- interne Darstellung von Potenzreihen (`SeriesData`) 324, 374
- Interpolation 96
- Interpolationspolynom 178
 - `InterpolatingPolynomial` 180, 190
 - Lagrangesches (Lagrange) 179, 180
 - Newtonsches 178, 180, 200
- inverse diskrete Fouriertransformation 165
- inverse hyperbolische Sinusfunktion (`ArcSinh`) 314
- inverse hyperbolische Tangensfunktion (`ArcTanh`) 297, 342
- inverse Matrix (`Inverse`) 10
- inverse Tangensfunktion (`ArcTan`) 20, 469, 476
- Inverses, modulares 91
- Inversion einer Reihe 320
 - `InverseSeries` 324, 374, 375
 - `inverseSeries` 375
- Irrationalitätsbeweis 202
- Irreduzibilitätskriterium von Eisenstein (Eisenstein) 201
- irreduzible Zahl 73
- irreduzibles Polynom
 - in $\mathbb{Z}[x]$ 201
 - in $\mathbb{Z}_p[x]$ (`FieldIrreducible`, `IrreduciblePolynomial`) 229
- ISBN-Prüfziffer 130, 147
 - `ISBNPrüfziffer` 147
- Iteration (`Fold`) 32, 34
- Iteration (`Nest`) 32, 34
- Iterationsliste
 - `ComposeList` 32
 - `FixedPointList` 32, 257, 368
 - `FoldList` 32
 - `NestList` 32, 241, 325
 - `Range` 34
- iteratives Programm 33
- Iterator (`{k, k1, k2}`) 31
- Kanal, gestörter 121
- kanonische Form 299
 - distributive 303
 - für Polynome (`Expand`) 300
 - für trigonometrische Polynome (`TrigReduce`) 307
- kanonische Funktion 299

- Karatsuba-Algorithmus 58
 - für Polynome 159
- Kern einer Matrix 272
 - NullSpace 245, 273
- Kern von *Mathematica* 63
- Kettenbruch 46
 - ContinuedFraction, FromContinuedFraction 82
- Kettenregel 42, 445, 447, 469
- k -freie Differentialgleichung (kfreieDE) 434
- k -freie Rekursionsgleichung (kfreieRE) 387, 390
- kinetische Energie 24
- Klammerung mathematischer Ausdrücke
 - (()) 39
- Klartext 136
- Klasseneinteilung 87
- kleiner Satz von Fermat 99
- kleines Einmaleins 53
- kleines Einspluseins 53
- kleinster Erzeuger 103
- kleinstes gemeinsames Vielfaches 67
 - LCM 110, 262
- Koeffizient eines Polynoms 154
 - Coefficient 70, 156
- Koeffizientenliste eines Polynoms 156
 - CoefficientList 156, 160, 214
- Körper 67, 90
 - der rationalen Funktionen 198
- Körpererweiterung
 - algebraische 223, 247
 - einfache 213
 - endliche 214
 - Grad 214
 - logarithmische 447
 - transzendente 156
- kommutativ (Orderless) 41
- Kompatibilität von Differentialgleichungen 341
- Kompatibilität von Rekursionsgleichungen 382
- kompilierende Programmiersprache 101
- komplexe Einheit (i , i) 27
- komplexe Ganzzahlen (GaussianIntegers) 10, 154
- komplexe Zahl (Complex) 8, 27
- Komplexität
 - eines Algorithmus 36, 56
 - exponentielle 77, 95
 - polynomiale 116
- Komplexitätstheorie 116
- Komposition von Potenzreihen 320
 - ComposeSeries 324, 375
- Komprimierung von Dateien 121
- Kondition einer Matrix 10
- Kongruenz modulo p 87
- Kongruenz modulo $p(x)$ 205
- konstante Potenzreihen 317
- Konstantenkörper 443, 444
- Konstantenregel 444
- konstantes Polynom 155
- Konstruktion des regelmäßigen 17-Ecks 253
- Konvergenzradius 318, 324
- Konversion
 - einer Zahl in ASCII-Nummern (NumberToList) 143
 - einer Zahl in einen Text (NumberToText) 143
 - eines Texts in eine Zahl (TextToNumber) 143
 - nach ASCII (ToCharacterCode) 123
 - von ASCII (FromCharacterCode) 123
 - von ASCII-Nummern in Zahl (ListToNumber) 143
- Kopf eines Ausdrucks (Head) 27
- Kosinusfunktion (Cos) 7, 42, 297
- Kreis 16
- Kreiszahl π 3
- Kronecker-Algorithmus zur Polynomfaktorisierung 188, 201
 - Kronecker 201
- Kryptoanalyse 137
- Kryptogramm 136
- Kryptographie 137
- kryptographisches Protokoll 142
- Kryptologie 137
- Kürzen rationaler Zahlen 4, 28
- Kürzungsregel 117
- Kummer-Identität 437, 438

- Kummersche hypergeometrische Reihe
 (Hypergeometric1F1) 350, 351
- Länge eines Worts 121
- Länge einer Liste (Length) 52
- Lagrange, Satz von 116
- Lagrangesches Interpolationspolynom 179
- Laguerrepolynome (LaguerreL) 380, 426, 435
- Lambertsche W -Funktion (ProductLog) 367
- Langzahladdition (Add) 81
- Langzahlarithmetik 51
 - Addition 53
 - Multiplikation 53
 - Schulgorithmen 53, 64
 - Subtraktion 53
- Langzahlmultiplikation
 - Karatsuba 60
 - Multiply 56
- Laufzeit eines Algorithmus 36, 56
- Laurentreihe, formale 322
- lazy evaluation 373
- leeres Ergebnis (Null) 31, 138
- leeres Wort 121
- Legendrepolynome (LegendreP) 426, 435
- letzte Ausgabe (% Out) 4, 44
- lexikographische Ordnung 303
- Lifting 264
 - Hensel- 282
- lineare Algebra 10
- lineare Differentialgleichung 332
- lineare Rekursionsgleichung 343
- lineares Gleichungssystem
 - Dreiecksform 243
 - Lösungsmenge 243
 - Rücksubstitution 244
- Linearität der Differentiation 41, 193, 444
- Liste ({}, List) 5, 27
- Liste ohne erstes Element (Rest) 46, 48
- Liste ohne Klammern (Sequence) 189, 262, 264
- Listenelement ([[]]) 15, 34
- Listenerzeugung (Table) 10, 31, 34
- Listenzerlegung (Partition) 84, 123, 189
- LLL-Gitterreduktionsverfahren 291
- Lochkarte 121
- Löschen des Überschreibschutzes (Unprotect) 241
- Löschen einer Variablen/Funktion (Clear, Remove) 8, 44, 56, 334
- Löschen eines Teilausdrucks (DeleteCases) 30
- Lösen
 - linearer Gleichungssysteme (LinearSolve, Solve) 245
 - polynomialer Gleichungssysteme (Solve) 249
 - von Differentialgleichungen (DSolve) 339, 379, 435
 - von Gleichungen (Solve) 12, 92, 132, 245, 249
 - von Gleichungen, numerisches (NSolve) 13
- Lösungsmenge
 - eines linearen Gleichungssystems 243
 - eines polynomialen Gleichungssystems 246
- logarithmische Körpererweiterung 447
- logarithmischer Teil eines rationalen Integrals 450
- logarithmisches Element über einem Körper 447
- Logarithmus
 - diskreter 104
 - modularer 104
- Logarithmusfunktion (Log) 28, 42, 44, 314, 342, 447, 476
- logisches „nicht“ (Not, !) 70, 128
- logisches „und“ (&&, And) 33
- logistische Iteration 256
- lokale Variable 32, 34, 71, 366
- Lucas-Test 6
- Macsyma* 21, 301
- Maple* 21, 300, 327
 - Worksheet VII
- Mathematica*-Notebook VII
- mathematische Gleichwertigkeit 298

- Matrix
 - Determinante 10
 - Inverse (Inverse) 10
 - Kondition 10
- Matrizendarstellung (MatrixForm) 5, 57, 92
- Matrizenpotenz (MatrixPower) 44
- Maximum (Max) 47
- maxint (Pascal) 4
- mehrdimensionales Monom 303
- mehrfache Nullstelle 185
- Mengenkomplement (Complement) 186
- Mersennesche Zahlen 22
- m -fach symmetrische Reihe 356
- Miller-Rabin-Test 6, 111
 - RabinMillerPrime 112
- minimaler Erzeuger (MinErzeuger) 103
- Minimalpolynom einer algebraischen Zahl 218
 - via Resultanten 240
- Modul 87
- Modul (Module) 32
- modulare Logarithmusfunktion (MultiplicativeOrder) 103, 106, 118
- modulare Potenz
 - PowerMod 92, 100
 - powermod 100, 117
 - eines Polynoms (PolynomialPowerMod) 252
- modulare Quadratwurzel 93
 - ModularSqrt 95
- modularer Logarithmus 104
 - ModularLog 118
- modulares Inverses 91
 - eines Polynoms (PolynomialModInverse) 252
- modulares Rechnen (Modulus) 9, 92, 95, 132
 - mit Polynomen (PolynomialMod) 209, 229
- monisches Polynom 155
 - makemonic 463
- Monom, mehrdimensionales 303
- Monomordnung 303
 - lexikographische 303
- Morley, Satz von 312
- Morsealphabet 123, 126
- Multiindex 303
- Multiplikation 53
 - *, Times 7, 27, 31, 339
 - von Langzahlen (Karatsuba) 60
 - von Polynomen (ListKaratsuba, PolynomialKaratsuba) 160
- Multiplikationstafel 90, 228
 - \mathbb{Z}_p (MultZ, MultZ0) 92
- multiplikative Ordnung
 - eines Elements einer Gruppe 117
 - eines Elements in \mathbb{Z}_p^* 102
 - MultiplicativeOrder 103, 234
- MuPAD 21
 - Notebook VII
- Musik-CD 121
- Muster (_, Blank) 6, 29
- Mustererkennung 28
- N (numerischer Wert) 3
- nachgewiesene Primzahl (ProvablePrimeQ) 116
- Nachrichtenintegrität 140
- nächste Primzahl (NextPrime) 6, 76, 98, 200
- nächstgrößere ganze Zahl (Ceiling) 281
- natürliche Grenzen 353
- Nenner einer rationalen Funktion (Denominator) 262
- Newtonsches Interpolationspolynom 180, 200
- Newtonverfahren 368
 - NewtonListe 368
 - NewtonVerfahren 368
 - numerisches (NewtonVerfahren) 35
 - quadratische Konvergenz 368
- nicht (Not, !) 70, 128
- Norm, Euklidische 199
- Normalform 299
 - für holonome Folgen 345
 - für holonome Funktionen 341
 - für Polynome (Expand) 300
 - für trigonometrische Polynome (TrigReduce) 307

- rationale (Together) 9, 198, 297, 304
- Normalfunktion 299
- normiertes Polynom 155
 - makemonic 463
- n -te Primzahl (Prime) 114, 200, 285
- Nullpolynom 154
- Nullreihe 317
- Nullstelle
 - eines Polynoms 156
 - Root 15, 217, 226, 249
 - einfache 185
 - in \mathbb{Z}_p (Nullstellen) 291
 - mehrfache 185
 - Ordnung 185
- Nullteiler 91
- number field sieve 78
- numerischer Wert (N) 3
- numerisches Lösen von Gleichungen
 - (NSolve) 13
- o. B. d. A. (ohne Beschränkung der Allgemeinheit) 65
- obere Parameter der hypergeometrischen
 - Reihe 350
- öffentlicher Schlüssel 140
- Oktalsystem 51
- Optionen (Options) 17
- Ordnung
 - der Nullstelle eines Polynoms 185
 - einer Differentialgleichung (DEOrder) 47
 - einer Potenzreihe 317
 - einer Rekursionsgleichung 343
 - eines Elements einer Gruppe 117
 - eines Elements in \mathbb{Z}_p^* 102
 - lexikographische 303
 - MultiplicativeOrder 103, 234
- Paletten in *Mathematica* 3
- Parität 130
- Partialbruchzerlegung (Apart) 311, 448, 479
 - bzgl. einer partiellen Faktorisierung 312, 458
 - reelle 442, 449
 - vollständige 456
- partielle Ableitung
 - einer Funktion (', Derivative) 35, 47, 335
 - eines Ausdrucks (D) 19, 40, 47
- partielle Integration 444
- partielle Summation 403
- Pascalsches Dreieck 346, 376, 388
- periodische Dezimaldarstellung (RealDigits, FromDigits) 84
- Periodizität der modularen Potenz 101
- Pfaff-Saalschütz-Identität 437, 438
- Plot
 - ContourPlot 18
 - ImplicitPlot 15
 - Optionen
 - AspectRatio 35
 - PlotPoints 18
 - PlotRange 17
 - PlotStyle 17
 - Plot 17
 - Plot3D 17
- Pochhammer-Symbol (Pochhammer) 345, 349
- Polynom
 - ausmultipliziertes 155
 - distributive Darstellung 157
 - division 173
 - PolynomialQuotient 175, 182, 186
 - Rest (PolynomialRemainder) 175, 182, 186, 209, 307
 - Divisionsrest 174
 - elementarsymmetrisches 217, 278
 - expandiertes 155
 - faktorisierung
 - Factor 9, 187, 192
 - Berlekamp-Algorithmus 267
 - Kronecker-Algorithmus 201
 - über \mathbb{Z} 188
 - über \mathbb{Z} (Kronecker) 201
 - über \mathbb{Z}_p (Faktoren) 186
 - führender Koeffizient 154
 - führender Term 155
 - Grad 154
 - Exponent 241

- Grad 47
- Identitätssatz 177
- interpolation 178
- Karatsuba-Algorithmus 159
- Koeffizient 154
 - Coefficient 70, 156
- Koeffizientenliste 156
 - CoefficientList 156, 160, 214
- konstantes 155
- mehrerer Variablen 157
- modulare Potenz (PolynomialPower-Mod) 252
- modulares Inverses (PolynomialMod-Inverse) 252
- modulares Rechnen (PolynomialMod) 209, 229
- monisches 155
- Multiplikation (ListKaratsuba, PolynomialKaratsuba) 160
- normiertes 155
- Nullstelle 156
 - Root 15, 217, 226, 249
 - Ordnung 185
- primitives 261
 - PrimitiverTeil 262
- quadratfrei 192
- quadratfreie Faktorisierung 193
- quotient 174
- rationale Nullstellen (RationaleNullstellen) 291
- rekursive Darstellung 157
- ring ($R[x]$) 154
- Standarddarstellung 154
- Swinnerton-Dyer 293
- Wert 156
- zyklotomisches 292
- polynomialer Algorithmus 116
- polynomiales Gleichungssystem
 - Lösungsmenge 246
 - Solve 15, 249
- Polynomlösung der Gosperrekursion (REtoPol) 414, 436
- Position (Position) 29, 95, 186, 191
- Postfixform (//) 5
- Potenz ($^$, Power) 4, 27
- Potenz einer Matrix (MatrixPower) 44
- Potenzalgorithmus für Differentialgleichungen (PowerDE) 379
- Potenzmenge (Potenzmenge) 47
- Potenzregel 40, 444
- Potenzreihen
 - Abbruchordnung
 - Abbruchordnung 374
 - O 321
 - Abfrage (PowerSeriesQ) 374
 - abgebrochene 321
 - Absolutglied 317
 - asymptotische 318
 - Berechnung abgebrochener (Series) 19, 326
 - formale 317
 - FPS 330, 380, 435
 - interne Darstellung (SeriesData) 324, 374
 - Inversion 320
 - InverseSeries 324, 374, 375
 - inverseSeries 375
 - Kehrwert (Kehrwert) 374
 - Komposition 320
 - ComposeSeries 324, 375
 - konstante 317
 - Laurentreihe 322
 - Nullreihe 317
 - Ordnung 317
 - Ordnung 374
 - Puiseuxreihe 323
 - Quadratwurzel (SeriesSqrt) 375
 - ring 317
 - Umformung in ein Polynom (Normal) 323
 - Variable (Variable) 374
- Präfixcode 125
- prim? (PrimeQ) 6, 76, 77, 154
- Primdispersion (PrimDispersion) 417
- primitive n -te Einheitswurzel 163
- primitiver Teil 262
- primitives Element 102
- primitives Polynom 261
 - PrimitiverTeil 262

- Primzahl 6, 73
 - nachgewiesene (`ProvablePrimeQ`) 116
 - Nummer n (`Prime`) 114, 200, 285
 - Pseudo- 6, 108, 111
- Primzahlsieb (Eratosthenes) 84
- Primzahlweltrekord 22
- Primzahlzwillinge 23
- private key 140
- privater Schlüssel 140
- probabilistischer Algorithmus 115
- Probedivision 76
- ProductLog-Funktion (`ProductLog`) 367
- Produkt (`Product`) 15, 28, 31
- Produktalgorithmus für
 - Differentialgleichungen (`ProductDE`) 339, Quelle 121
378
 - Rekursionsgleichungen (`ProductRE`) 344
- Produktregel 41, 193, 443
- Programm 32
 - iteratives 33
 - rekursives 6, 33
- Programmgruppe (`Module`) 32
- Programmieren in Computeralgebrasystemen 27
- Programmieren mit *Mathematica* 6
- Programmiersprache, kompilierende 101
- Protokoll, kryptographisches 142
- Prüfbit 130
- Prüfzeichen 130
- Prüfziffer 130
 - EAN (`EANPrüfziffer`) 148
 - ISBN (`ISBNPrüfziffer`) 147
- Pseudocode VII
- Pseudodivision 199
- Pseudoprimzahl 6
 - Fermatsche 108
 - strenge 111
- public key 140
- Public-Key-Verfahren 140
- Puiseuxreihe, formale 323
- pythagoreische Identität 305, 342
- quadratfreie Faktorisierung eines Polynoms 193
 - `FactorSquareFree` 196, 275, 478
 - `FactorSquareFreeList` 478
 - QuadratfreieFaktorisierung 202
- quadratfreie ganze Zahl 110
- quadratfreier Teil eines Polynoms 196
 - `QuadratfreierTeil` 202
- quadratisches Polynom 192
- quadratische Konvergenz des Newtonverfahrens 368
- quadratischer Rest 93
- Quadratwurzel
 - modulare 93
 - `ModularSqrt` 95
 - `Sqrt` 7
- Quotient, ganzzahliger 64
- Quotientenmenge 298
- Quotientenregel 444
- Quotientenring 116
- Rabin-Miller-Test 111
 - `RabinMillerPrime` 112
- rational exakte Arithmetik 4, 79
- rationale Funktion 198
 - Nenner (Denominator) 262
 - Standarddarstellung 198
 - Zähler (Numerator) 334
- rationale Normalform (`Together`) 9, 198, 297, 304
- rationale Nullstellen eines Polynoms (`RationaleNullstellen`) 291
- rationale Zahl (`Rational`) 27
- rationaler Teil eines rationalen Integrals 450
- rationales Zertifikat 427
- Realteil (`Re`) 8
- Rechenzeitmessung (`Timing`) 36, 44
- Reduce* 21, 304
- redundante Information 130
- reduzibel 73
- Reed-Solomon-Code 131
 - `ReedSolomon` 132, 150, 255
 - Umkehrung (`InverseReedSolomon`) 134, 150, 255
- reelle Faktorisierung 442

- reelle Partialbruchzerlegung 442
- regelmäßiges 17-Eck 253
- reine Funktion
 - &, Function 29, 30, 34
 - Variable (#, Slot) 29
 - Variablen (#1, #2) 34
- Rekursion zu Differentialgleichung
 - REtoDE 348, 382
 - retode 382
- Rekursionsgleichung
 - des Pascalschen Dreiecks 388
 - einer definiten Summe (FasenmyerRE) 393, 435
 - einer Summe (SumRE) 344
 - eines Produkts (ProductRE) 344
 - holonome 343
 - HolonomicRE 344
 - homogene 343
 - k-freie (kfreieRE) 387, 390
 - Kompatibilität 382
 - lineare 343
 - Ordnung 343
- Rekursionstiefe (\$RecursionLimit) 37, 44
- rekursive Darstellung von Polynomen mehrerer Variablen 157
- rekursive Multiplikation 55
- rekursives Programm 6, 33
- relativ prim 67
- Rememberprogrammierung 36, 37
- Residuum 457
- Rest bei der ganzzahligen Division (Mod) 64, 65
- Rest bei der Polynomdivision (PolynomialRemainder) 175, 182, 186, 209, 307
- Restklasse 87, 205
- Restklassenpolynomring 205
- Resultante 237
 - Resultant 239, 459
 - resultant 239
- Resultat eines Moduls 32
- Ring
 - der formalen Potenzreihen 317
 - der ganzen Zahlen (\mathbb{Z}) 67
 - Einheit 67
 - holonomer Folgen 344
 - holonomer Funktionen 336
- Ringoperationen 160
- Rioboo-Algorithmus (LogToArcTan) 476
- Risch-Algorithmus 441
- Robertson-Vermutung 23
- römisches Zahlensystem 51
- Rot-Grün-Blau-Farbenwert (RGBColor) 17
- Rothstein-Träger-Algorithmus (Rothstein-Träger) 465
- RSA-Entschlüsselung (Entschlüssele) 144
- RSA-Verfahren 142
- RSA-Verschlüsselung (Verschlüssele) 144
- Rücksubstitution 244
- Rückwärtsdifferenzenoperator 397
- Runden reeller Zahlen (Round) 45
- Saalschütz-Identität 437, 438
- Sammeln nach Potenzen einer Variablen (Collect) 158, 302
- Sattelpunkt 17
- Satz von Fermat 99
- Satz von Lagrange 116
- Satz von Vieta 217
- Scannen 130
- Schleife 31
- Schlüssel 137
 - öffentlicher 140
 - privater 140
 - übergabe 140
 - vereinbarung von Diffie-Hellman 141
- schnelle Fouriertransformation 163
 - FFT, IFFT 170
- schnelle Multiplikation
 - Karatsuba 60
 - von Polynomen (ListKaratsuba, PolynomialKaratsuba) 160
- Schönhage-Strassen-Algorithmus 199
- secure shell 137
- Segment 87
- Seiteneffekt 32, 71, 113
- Sekansfunktion (Sec) 314
- Sender 121

- shifted factorial 345, 349
- Shiftoperator 344
- Sicherheit eines Verschlüsselungsverfahrens 140
- Sieb des Eratosthenes 84
- Singularität, hebbare 325
- Sinusfunktion (`Sin`) 7, 8, 28, 42, 297
- Skalarprodukt 463
 - `.`, Dot 465
- Sortieren (`Sort`) 73, 128
- Speicherplatz 4
- Speicherzugriff 54
- spezielle Relativitätstheorie 24
- splitting field 215
- Stammfunktion 396, 443
 - diskrete 397
 - `Summation` 401
 - stetige 473
- Standarddarstellung 213
 - einer rationalen Funktion 198
 - eines Polynoms 154
- Standardform einer *Mathematica*-Funktion 5
- steigende Faktorielle 399
- stetige Stammfunktion 473
- Steuerzeichen 123
- Stirlingsche Formel 159, 436
- Strassen-Schönhage-Algorithmus 199
- strenge Pseudoprimalzahl 111
- Strichcode 130
- Strings und lazy evaluation 373
- Stützstellen bei der Polynom-Approximation 178
- Substitution
 - `->`, `->`, Rule 9, 12
 - `/.`, `ReplaceAll` 12
 - rekursive (`//.`, `ReplaceRepeated`) 44, 70
 - verzögerte (`:>`, `RuleDelayed`) 43, 225
- Subtraktion (`-`, `Subtract`) 4, 28
- `Summation`, partielle 403
- Summe (`Sum`) 4, 28
 - unbestimmte 398
- Summe über die Nullstellen eines Polynoms (`RootSum`) 458
- Summenalgorithmus für
 - Differentialgleichungen (`SumDE`) 338
 - Rekursionsgleichungen (`SumRE`) 344
- Summenregel 41, 443
- Swinerton-Dyer-Polynom 293
- Sylvestermatrix 236
 - `SylvesterMatrix` 241, 255
- Symbol (`Symbol`) 27
- Symmetriezahl 355
- symmetrische Modulofunktion (`SymmetricPolynomialMod`) 279
- symmetrische Reihe 356
- symmetrisches Verschlüsselungsverfahren 139
- syntaktische Gleichheit (`===`, `SameQ`) 183, 298
- Tangensfunktion (`Tan`) 17, 297
- Taschenrechner 3
- Tastatur 121
- Taylorapproximation eines Anfangswertproblems (`DSolveTaylor`) 383
- Taylorpolynom 324
 - `FastImplicitTaylor` 372
 - `ImplicitTaylor` 365
 - `ImplicitTaylor2` 370
 - `ImplicitTaylor3` 371
 - `Series` 19, 326
 - `Taylor` 325, 358
- Teil einer Liste (`Take`) 160
- Teilbarkeit 67
- Teiler 67
 - `divisors` 189
 - `Divisors` 154, 189
 - gemeinsamer 67
 - größter gemeinsamer 67
- teilerfremd 67
- Teillöschung einer Liste (`DeleteCases`) 30
- Teilmengen einer Menge (`Teilmengen`) 48
- Teleskopsumme 397
- Termordnung 303
- Testen einer ISBN-Nummer (`CheckISBN-Prüfziffer`) 147
- Träger, endlicher 420

- Transponieren von Matrizen (Transpose) 110, 190
- transzendente Funktionen 7
- transzendente Ringerweiterung 156
- transzendenter Teil eines rationalen Integrals 450
- transzendentes Element 156
- Trennung von Anweisungen (;) 31
- Trennung von Argumenten (,) 31
- trigonometrische Additionstheoreme 307
- trigonometrische Vereinfachung
 - TrigExpand 254, 307
 - TrigFactor 307, 310, 314
 - TrigFactorList 307
 - TrigReduce 307, 309
 - TrigToExp 307
- Tschebyshevpolynome (ChebyshevT) 254
- Typ einer Variablen 4
- Übertrag bei der Addition 53
- Übertragung von Nachrichten 121
- Übertragungskanal 121
 - gestörter 121
- UFD 199, 310
- Umformung in ein Polynom (Normal) 323
- Umkehrfunktion 20, 320
- Umkehrung des Reed-Solomon-Codes (InverseReedSolomon) 134, 150, 255
- Umkehrung einer Liste
 - Reverse 47, 160, 241
 - reverse 47
- Umwandlung in hypergeometrische Notation (SumToHypergeometric) 352, 380, 435
- Unabhängigkeit (FreeQ) 40, 181
- unbestimmte Summe 398
- und (&&, And) 33
- unendlich (∞ , Infinity) 37
- unevaluierte Ausdrücke in *Mathematica* 298
- unevaluierte hypergeometrische Reihe (hypergeometricPFQ) 352
- ungerade? (OddQ) 39
- ungerader Anteil einer Funktion 332
- unique factorization domain 199, 310
- Unterdrückung der Ausgabe (;) 44
- Unterdrücken kleiner Dezimalzahlen (Chop) 165
- untere Parameter der hypergeometrischen Reihe 350
- Unterstrich (_, Blank) 6, 29
- Vandermonde-Identität 430, 437, 438
- Vandermonde-Matrix (Vandermonde) 11
- Vandermondesumme 376
- Variablen
 - _, Blank 6, 29
 - Deklaration 4
 - einer reinen Funktion
 - #1, #2 34
 - #, Slot 29
 - eines Ausdrucks (Variables) 306
 - für Fehlermeldung ('1 ') 112
 - global 71, 366
 - lokal 32, 34, 71, 366
 - typ 4
- Vektorraum 215, 336
- verallgemeinerte hypergeometrische Reihe (HypergeometricPFQ) 351
- Verbinden einer Zeichenkette (StringJoin, <>) 137
- Verbinden von Listen (Join) 160, 241, 452
- Verbosemodus (specfunprint) 330
 - abstellen (specfunprintoff) 331
- Vereinfachung 21
 - automatische 27, 314
 - Expand 9, 45, 158, 297, 300, 303
 - ExpandAll 407
 - Factor 9, 187, 192
 - FullSimplify 7, 214, 297, 310, 342
 - hypergeometrischer Terme (Simplify-Combinatorial) 423, 436
 - RootReduce 15, 214, 221, 226, 253
 - Simplify 7, 297, 310, 314
 - spezieller Funktionen (Function-Expand) 389, 436
 - Together 9, 198, 297, 304
 - trigonometrische
 - TrigExpand 254, 307
 - TrigFactor 307, 310, 314

- TrigFactorList 307
- TrigReduce 307, 309
- TrigToExp 307
- Vereinfachungsfunktion 299
- Vereinfachungsoption (Integers) 377
- Vereinigung (Union) 48, 74
- Verhindern der Auswertung (Hold) 43
- verkettete Wurzel 46
- Verkettung (Nest) 32, 34
- Verkettungsliste (NestList) 32, 241, 325
- Verschlüsselung 136
 - mit Caesarcode (CaesarV) 137
 - mit RSA (Verschlüssele) 142, 144
- Verschlüsselungsverfahren
 - asymmetrisches 140
 - effizientes 140
 - Sicherheit 140
 - symmetrisches 139
- Verträglichkeit einer Äquivalenzrelation 299
- verzögerte Zuweisung (:=, SetDelayed) 6, 30
- verzögertes Ersetzen (:>, RuleDelayed) 43, 225
- Vielfaches 67
- Vieta, Satz von 217
- vollständige Lösungsmenge eines linearen Gleichungssystems 243
- Vorwärtsdifferenzenoperator 397
- Vorwärtsshiftoperator 344
- wahr (True) 6
- Wahrscheinlichkeitsmaß 126
- Weltrekord beim Faktorisieren 78, 142
- Weltrekordprimzahl 22
- wenn, dann (If) 30, 298
- Wert eines Polynoms 156
- while-Schleife (While) 32, 70
- wohldefiniert 89
- Wohlordnung 303
- word (Speichereinheit) 52
- Wort 121
 - Länge 121
 - leeres 121
- Wurzel, verkettete 46
- WZ-Methode 427
 - Zertifikat (WZCertificate) 431
- Zähler einer rationalen Funktion (Numerator) 334
- Zählschleife (Do) 31
- Zahldarstellung (BaseForm, ^^) 52
- Zahlkonversion
 - digitstonumber 46
 - numbertodigits 46
- Zahlsystem 51
 - arabisches 51
 - B-adisches 51
 - Basis 51
 - binäres 51
 - Dezimal- 52
 - Hexadezimal- 51
 - Oktal- 51
 - römisches 51
 - Ziffer 51
- Zassenhausschranke (Zassenhaus-Schranke) 280
- Zeichen 121
- Zeichen aus ASCII-Code (FromCharacterCode) 123
- Zeichenkette 121
 - Anfang (StringTake) 137
 - Ende (StringDrop) 137
 - Ersetzen (StringReplace) 134
 - Länge 121
 - Verbinden (StringJoin, <>) 137
- Zeilberger-Algorithmus
 - SumRekursion 423
 - Zb 425
- Zeitmessung (Timing) 36, 44
- Zelle in *Mathematica* 56
- Zerfallungskörper 215, 456
- zerlegbare Zahl 73
- Zerlegung einer Liste (Partition) 84, 123, 170, 189
- Zerlegung eines rationalen Integrals (RationaleZerlegung) 453, 479
- Zertifikat der WZ-Methode (WZCertificate) 431

- Zertifikat, rationales 427
- Zeuge
 - für die Zerlegbarkeit einer ganzen Zahl 112
 - Fermatscher 108
- Ziffern im Zahlssystem 51
- Ziffernfolge (`IntegerDigits`) 52
- ZPE-Ring 199, 310
- Zufallszahl (`Random`) 29, 62
- Zugriff auf Speicher 54
- zusammengesetzte Zahl 67
- Zuweisung
 - =, `Set` 7
 - verzögerte (`:=`, `SetDelayed`) 6, 30
- zweidimensionale Graphik (`Plot`) 17
- 2-fehlerkorrigierender Code 136, 150
- Zweig einer algebraischen Funktion 359, 363
- zyklische Gruppe 251
- zyklische Vertauschung einer Liste (`RotateRight`) 241
- zyklotomische Polynome (`Cyclotomic`) 292, 293