

# List of Publications

M. Pohst

Fachbereich 3 Mathematik, MA 8 - 1  
Technische Universität Berlin  
Straße des 17. Juni 136  
10623 Berlin

October 14, 2009

# Schriftenverzeichnis

- [1] *Mehrklassige Geschlechter von Einheitsformen in total reellen algebraischen Zahlkörpern*, J. Reine Angew. Math. **262/263** (1973), 420–435.
- [2] *Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper*, J. Reine Angew. Math. **278/279** (1975), 278–300.
- [3] *Berechnung unabhängiger Einheiten und Klassenzahlen in total reellen biquadratischen Zahlkörpern*, Computing **14** (1975), 67–78.
- [4] *Über biquadratische Zahlkörper gleicher Diskriminante*, Abh. Math. Sem. Univ. Hamb. **43** (1975), 192–197.
- [5] *Invarianten des total reellen Körpers siebten Grades mit Minimaldiskriminante*, Acta Arithmetica **30** (1976), 199–207.
- [6] *A program for determining fundamental units*, in Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation, 235–240.
- [7] *The minimum discriminant of seventh degree totally real algebraic number fields*, in Number Theory and Algebra ed. by H. Zassenhaus, Academic Press 1977, 235–240.
- [8] (mit W. Plesken) *On maximal finite irreducible subgroups of  $GL(n, \mathcal{Z})$ , I. The five and seven dimensional case*, Math. Comp. **31** (1977), 536–551.
- [9] (mit W. Plesken) *On maximal finite irreducible subgroups of  $GL(n, \mathcal{Z})$ , II. The six dimensional case*, Math. Comp. **31** (1977), 552–573.
- [10] (mit H. Zassenhaus) *An effective number geometric method of computing the fundamental units of an algebraic number field*, Math. Comp. **31** (1977), 754–770.

- [11] *Regulatorabschätzungen für total reelle algebraische Zahlkörper*, J. Number Theory **9** (1977), 459–492.
- [12] *Eine Regulatorabschätzung*, Abh. Math. Sem. Univ. Hamb. **47** (1978), 95–106.
- [13] (mit H. Zassenhaus) *On unit computation in real quadratic fields*, in Symbolic and Algebraic Computation, Springer Lect. Notes in Comp. Sc. **72** (1979), 140–152.
- [14] (mit W. Plesken) *On maximal finite irreducible subgroups of  $GL(n, \mathbb{Z})$ , III. The nine dimensional case*, Math. Comp. **34** (1980), 245–258.
- [15] (mit W. Plesken) *On maximal finite irreducible subgroups of  $GL(n, \mathbb{Z})$ , IV. Remarks on even dimensions with applications to  $n=8$* , Math. Comp. **34** (1980), 259–275.
- [16] (mit W. Plesken) *On maximal finite irreducible subgroups of  $GL(n, \mathbb{Z})$ , V. The eight dimensional case and a complete description of dimensions less than ten*, Math. Comp. **34** (1980), 277–301.
- [17] *On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications*, ACM SIGSAM Bulletin **15** (1981), 37–44.
- [18] (mit D. Y. Y. Yun) *On solving systems of algebraic equations via ideal bases and elimination theory*, in Proc. 1981 ACM Symposium on Symbolic and Algebraic Computation, 206–211.
- [19] *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.
- [20] (mit H. Zassenhaus) *On effective computation of fundamental units I*, Math. Comp. **38** (1982), 275–291.
- [21] (mit P. Weiler und H. Zassenhaus) *On effective computation of fundamental units II*, Math. Comp. **38** (1982), 293–329.
- [22] *On the determination of algebraic number fields of given discriminant*, in Computer Algebra, Springer Lect. Notes in Comp. Sc. **144** (1982), 71–76.

- [23] *Computation of integral solutions of a special type of systems of quadratic equations*, in Computer Algebra, Springer Lect. Notes in Comp. Sc. **162** (1983), 203–213.
- [24] (mit U. Fincke) *A procedure for determining algebraic integers of given norm*, in Computer Algebra, Springer Lect. Notes in Comp. Sc. **162** (1983), 194–202.
- [25] (mit U. Fincke) *On reduction algorithms in non linear mathematical programming*, in DGOR Operations Research Proc. **83**, Springer Verlag 1983, 289–295.
- [26] *On constructive methods in algebraic number theory*, in Coll. Math. Soc. János Bolyai **34**, Topics in Classical Number Theory, Elsevier North Holland 1984, 1251–1263.
- [27] (mit U. Fincke) *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.
- [28] (mit W. Plesken) *Constructing integral lattices with prescribed minimum I*, Math. Comp. **45** (1985), 209–221 und S5–S16.
- [29] (mit U. Fincke) *A new method of computing fundamental units in algebraic number fields*, Proc. EUROCAL'85, Springer Lect. Notes in Comp. Sc. **204** (1985), 470–478.
- [30] (mit H. Zassenhaus) *Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper*, J. Reine Angew. Math. **361** (1985), 50–72.
- [31] *Über zahlengeometrische Methoden in der Konstruktiven Algebraischen Zahlentheorie*, Bericht Nr. **270** (1986), Math.–Stat. Sekt., Forsch.ges. Joanneum, Graz, 23 pp..
- [32] *On computing isomorphisms of equation orders*, Math. Comp. **48** (1987), 309–314.
- [33] *A modification of the LLL–algorithm*, J. Symbolic Computation **4** (1987), 123–127.
- [34] *Zur Faktorisierung großer Zahlen*, Der math. u. naturwiss. Unterricht, Jahrgang **41** (1988), 335–339.

- [35] *Three principal tasks of computational algebraic number theory*, in Number Theory and Applications, ed. by R. A. Mollin, NATO ASI, Ser. C: Math'l and Physic'l Sciences, vol. **265**, Kluwer Acad. Publ. 1989, 279–324.
- [36] (mit J. Buchmann) *On the complexity of computing class groups of algebraic number fields*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-6, Springer Lect. Notes in Comp. Sc. **357** (1989), 122–131.
- [37] (mit J. Buchmann) *Computing a lattice basis from a system of generators*, in Proc. EUROCAL'87, Springer Lect. Notes in Comp. Sc. **378** (1989), 54–63.
- [38] (mit J. Buchmann und J. von Schmettow) *On the computation of unit groups and class groups of totally real quartic fields*, Math. Comp. **53** (1989), 387–397.
- [39] (mit J. Martinet und F. Diaz y Diaz) *The Minimum Discriminant of Totally Real Octic Fields*, J. Number Theory **36** (1990), 145–159.
- [40] (mit U. Halbritter) *On the computation of the Values of the Zeta Functions of Totally Real Cubic Fields*, J. Number Theory **36** (1990), 266–288.
- [41] (mit I. Gaál und A. Pethö) *On the Resolution of Index Form Equations in Biquadratic Number Fields I*, J. Number Theory **38** (1991), 18–34.
- [42] (mit I. Gaál und A. Pethö) *On the Resolution of Index Form Equations in Biquadratic Number Fields II*, J. Number Theory **38** (1991), 35–51.
- [43] *A note on index divisors*, in Computational Number Theory, ed. by A. Pethö, M. E. Pohst, H. C. Williams, H. G. Zimmer, Walter de Gruyter 1991, 173–182.
- [44] (mit W. Bosma) *Computations with finitely generated modules over Dedekind rings*, in Proc. ISSAC'91 ed. by M. Watt, ACM Press, New York 1991, 151–156.
- [45] (mit I. Gaál und A. Pethö) *On the resolution of index form equations*, in Proc. ISSAC'91 ed. by M. Watt, ACM Press, New York 1991, 185–186.

- [46] (mit I. Gaál und A. Pethö) *On the indices of biquadratic number fields with Galois group  $V_4$* , Arch. Math. **57** (1991), 357–361.
- [47] *Some aspects of computational algebraic number theory*, in Proc. of the Int. Conf. on Algebra honoring A. Malcev, ed. by L. A. Bokut, Yu. L. Ershov, O. H. Kegel, and A. I. Kostrikin, Contemporary Mathematics 131 (1992), 461–474.
- [48] (mit D. Ford), *The totally real  $A_5$  extension of degree 6 with minimum discriminant*, Exper. Math. **1** (1992), 231–235.
- [49] (mit J. von Schmettow) *On the computation of unit groups and class groups of totally complex quartic fields*, Math. Comp. **60** (1993), 793–800.
- [50] (mit W. Plesken), *Constructing integral lattices with prescribed minimum II*, Math. Comp. **60** (1993), 817–825.
- [51] (mit J. Buchmann und D. Ford) *Enumeration of Quartic Fields of Small Discriminant*, Math. Comp. **61** (1993), 873–879.
- [52] (mit D. Ford), *The totally real  $A_6$  extension of degree 6 with minimum discriminant*, Exper. Math. **2** (1993), 231–232.
- [53] (mit I. Gaál und A. Pethö) *On the resolution of index form equations in quartic number fields*, J. Symb. Comp. **16** (1993), 563–584.
- [54] *In Memoriam: Hans Zassenhaus*, J. Number Theory **47** (1994), 1–12.
- [55] *On computing fundamental units*, J. Number Theory **47** (1994), 93–105.
- [56] (mit J. Buchmann und J. von Schmettow) *On Unit Groups and Class Groups of Quartic Fields of Signature  $(2,1)$* , Math. Comp. **62** (1994), 387–390.
- [57] (mit A. Schwarz und F. Diaz y Diaz), *A Table of Quintic Fields*, Math. Comp. **63** (1994), 361–376.
- [58] (mit J. Buchmann und M. Jüntgen), *A Practical Version of the Generalized Lagrange Algorithm*, Exper. Math. **3** (1994), 199–207.
- [59] (mit I. Gaál und A. Pethö) *On the Resolution of Index Form Equations in Dihedral Quartic Number Fields*, Exper. Math. **3** (1994), 245–254.

- [60] (mit M. Daberkow) *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields*, in Proc. ISSAC'95 ed. by A. H. M. Levelt, ACM Press, New York 1995, 68–76.
- [61] (mit I. Gaál und A. Pethö) *On the Resolution of Index Form Equations in Biquadratic Number Fields III*, J. Number Theory **53** (1995), 100–114.
- [62] (mit I. Gaál und A. Pethö) *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, J. Number Theory **57** (1996), 90–104.
- [63] (mit M. Daberkow) *On integral bases in relative quadratic extensions*, Math. Comp. **65** (1996), 319–329.
- [64] *Computational aspects of Kummer theory*, in Algorithmic Number Theory ed. by H. Cohen, Springer Lect. Notes in Comp. Sc. **1122** (1996), 259–272.
- [65] (mit M. Daberkow) *On computing Hilbert class fields of prime degree*, in Algorithmic Number Theory ed. by H. Cohen, Springer Lect. Notes in Comp. Sc. **1122** (1996), 67–74.
- [66] (mit C. Fieker) *On lattices over number fields*, in Algorithmic Number Theory ed. by H. Cohen, Springer Lect. Notes in Comp. Sc. **1122** (1996), 133–139.
- [67] (mit M. Schörnig) *On computing invariants of function fields*, in Algorithmic Number Theory ed. by H. Cohen, Springer Lect. Notes in Comp. Sc. **1122** (1996), 273–282.
- [68] *Computing Invariants of Algebraic Number Fields*, in Group Theory, Algebra, and Number Theory ed. by H. G. Zimmer, de Gruyter 1996, 53–73.
- [69] (mit I. Gaál) *On the Resolution of Index Form Equations in Sextic Fields with an Imaginary Quadratic Subfield*, J. Symb. Comp. **22** (1996), 425–434.
- [70] (mit C. Fieker und A. Jurk) *On solving relative norm equations in algebraic number fields*, Math. Comp. **66** (1997), 399–410.

- [71] (mit J. Klüners) *On computing subfields*, J. Symb. Comp. **24** (1997), 385–397.
- [72] (mit M. Daberkow, C. Fieker, J. Klüners, K. Roegner, M. Schörnig, and K. Wildanger) *KANT V4*, J. Symb. Comp. **24** (1997), 267–283.
- [73] *On validated computing in algebraic number fields*, J. Symb. Comp. **24** (1997), 657–665.
- [74] (mit I. Gaál) *Power integral bases in a parametric family of totally real cyclic quintics*, Math. Comp. **66** (1997), 1689–1696.
- [75] (mit K. Wildanger) *A table of unit groups and class groups of quintic fields and a regulator bound*, Math. Comp. **67** (1998), 361–367.
- [76] (mit M. Daberkow) *On the Computation of Hilbert Class Fields*, J. Number Theory **69** (1998), 213–230.
- [77] (mit D. Ford, M. Daberkow und N. Haddad) *The  $S_5$  Extensions of degree 6 with minimum discriminant*, Exper. Math. **7** (1998), 121–124.
- [78] *From class groups to class fields*, pp. 103–119 in “Algorithmic Algebra and Number Theory”, eds. B.H. Matzat, G.-M. Greuel, G. Hiss, Springer–Verlag Berlin Heidelberg 1999.
- [79] *On Legendre’s equation over number fields*, Publ. Math. Debrecen **56** (2000), 535–546.
- [80] (mit I. Gaál) *Computing Power Integral Bases in Quartic Relative Extensions*, J. Number Theory **85** (2000), 201–219.
- [81] (mit U. Halbritter) *On lattice bases with special properties*, J. de Théorie des Nombres de Bordeaux **12** (2000), 437–453.
- [82] (mit I. Gaál) *On the resolution of relative Thue equations*, Math. Comp. **71** (2002), 429–440.
- [83] (mit I. Gaál und P. Olajos) *Power integer bases in orders of composite fields*, Exper. Math. **11** (2002), 87–90.
- [84] (mit F. Heß und S. Pauli) *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), 1531–1548.

- [85] (mit F. Lerevost and A. Schöpp) *Familles de polynômes liées aux courbes modulaires  $X_1(l)$  unicursales et points rationels non-triviaux de courbes elliptiques quotient*, Acta Arithmetica **110** (2003), 401–410.
- [86] (mit F. Lerevost and A. Schöpp) *Rational torsion of  $J_0(N)$  for hyper-elliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5,7 or 10*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 193–203.
- [87] *Factoring polynomials over global fields I*, J. Symb. Comp. **39** (2005), 617–630.
- [88] (mit F. Diaz y Diaz, J.-F. Jaulent, S. Pauli und F. Soriano) *Computing logarithmic class groups of number fields*, Exper. Math. **14** (2005), 65–74.
- [89] (mit D. Schielzeth) *On Real Quadratic Number Fields Suitable for Cryptography*, Exper. Math. **14** (2005), 189–197.
- [90] (mit J. Mendez) *Factoring polynomials over global fields II*, J. Symb. Comp. **40** (2005), 1325–1339.
- [91] (mit M. Wagner) *On the computation of Hermite-Humbert constants for real quadratic number fields*, J. de Théorie des Nombres de Bordeaux **17** (2005), 905–920.
- [92] (mit I. Gaál) *Diophantine equations over global function fields I: The Thue equation*, J. Number Theory **119** (2006), 49–65.
- [93] (mit I. Gaál) *Diophantine Equations over Global Function Fields II: R-Integral Solutions of Thue Equations*, Exper. Math. **15** (2006), 1–6.
- [94] (mit C. Fieker) *Dependency of units in number fields*, Math. Comp. **75** (2006), 1507–1518.
- [95] (mit F. Lerevost and A. Schöpp) *Units in some parametric families of quartic fields*, Acta Arithmetica **127** (2007), 205–216.
- [96] (mit I. Gaál) *Solving resultant form equations over number fields*, Math. Comp. **77** (2008), 2447–2453.
- [97] (mit C. Fieker) *A lower regulator bound for number fields*, J. Number Theory **128** (2008), 2767–2775.

- [98] (mit I. Gaál) *Diophantine Equations over Global Function Fields III: An application to resultant form equations*, *Functiones et Approximatio* **XXXIX.1** (2008), 97–102.
- [99] (mit I. Gaál) *A note on the number of solutions of resultant equations*, *JP Journal of Algebra, Number Theory and Applications* **12** (2008), 185–189.
- [100] (mit J.-F. Jaulent, S. Pauli, F. Soriano) *Computation of 2-groups of positive classes of exceptional number fields*, *J. de Théorie des Nombres de Bordeaux* **20** (2008), 715–732.
- [101] (mit N. Bernard, F. Lèprevost) *Jacobians of genus 2 curves with a rational point of order 11*, *Exp. Math.* **18** (2009), 65–70.
- [102] (mit J.-F. Jaulent, S. Pauli, F. Soriano) *Computation of 2-groups of narrow logarithmic divisor classes of number fields*, *J. Symb. Comp.* **44** (2009), 852–863.
- [103] (mit M. Wagner) *On the computation of Hermite-Humbert constants: The algorithm of Cohn revisited*, *J. Algebra* **322** (2009), 936–947.
- [104] (mit I. Gaál) *Diophantine Equations over Global Function Fields V: Resultant equations in two unknown polynomials*, *Int. J. Pure and Appl. Math.* **53** (2009), 307–317.
- [105] (mit I. Gaál) *Diophantine Equations over Global Function Fields IV: S-unit equations in three variables. An application to norm form equations*, to appear in *J. Number Theory*.
- [106] (mit I. Gaál) *On solving norm equations in global function fields*, to appear in *J. Math. Cryptology*.
- [107] (mit F. Lèprevost, O. Uzunkol) *On the computation of class polynomials with “Thetanullwerte” and its applications to the unit group computation*, submitted.
- [108] (mit I. Gaál) *Diophantine equations of type  $F(x, y) = G(x, y)$  over function fields*, manuscript.

# Bücher

1. (als Herausgeber) *Algorithmic Methods in Algebra and Number Theory*, Academic Press 1988.
2. (mit H. Zassenhaus) *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press 1989.  
First Paperback edition 1997 (contains additional chapter on recent developments).
3. (als Herausgeber mit A. Pethö, H. C. Williams und H. G. Zimmer) *Computational Number Theory*, Walter de Gruyter 1991.
4. *Computational Algebraic Number Theory*, DMV Seminar 21, Birkhäuser Verlag 1993.
5. (als Herausgeber) A. Pethö, *Algebraische Algorithmen*, Vieweg Verlag, 1999.
6. (als Herausgeber gemeinsam mit F. Hess, S. Pauli) *Algorithmic Number Theory*, Proc. ANTS-VII, Springer Verlag, LNCS 4076, 2006.