

# List of publications

H.W. Lenstra, Jr. List of publications October 20, 2008

## 1969

- a. *A transfinite generalization of a combinatorial problem on abelian groups* (with P. van Emde Boas), Report WN-29, Mathematisch Centrum, Amsterdam.

## 1972

- a. *Rational functions invariant under a finite abelian group*, Report 72-02, Mathematisch Instituut, Universiteit van Amsterdam.
- b. *Two theorems on perfect codes*, Discrete Math. **3**, 125–132.

## 1973

- a. *Simple abelian varieties having a prescribed formal isogeny type* (with F. Oort), Report 73-02, Mathematisch Instituut, Universiteit van Amsterdam.
- b. *Multiplicative division algorithms on the integers* (with A. E. Brouwer), Report 54/73, Mathematisch Centrum, Amsterdam.
- c. *The acyclic subgraph problem*, Report BW 26/73, Mathematisch Centrum, Amsterdam.
- d. *Bases for Boolean rings* (with P. van Emde Boas), Report 73-05, Mathematisch Instituut, Universiteit van Amsterdam.

## 1974

- a. *Euclid's algorithm in cyclotomic fields*, Report 74-01, Mathematisch Instituut, Universiteit van Amsterdam.
- b. *Eindige lichamen*, ch. IV in: *Algebraïsche vergelijkingen*, Vakantiecursus 1974, VC 28/74, Mathematisch Centrum, Amsterdam.
- c. *Rational functions invariant under a finite abelian group*, Invent. Math. **25**, 299—325.
- d. *Simple abelian varieties having a prescribed formal isogeny type* (with F. Oort), J. Pure Appl. Algebra **4**, 4–53.
- e. *A sharpened version of the Aanderaa-Rosenberg conjecture* (with M.R. Best and P. van Emde Boas), Report 30/74, Mathematisch Centrum, Amsterdam.

## 1975

- a. *Necessary conditions for the existence of perfect Lee codes*, Report ZN 59/75, Mathematisch Centrum, Amsterdam.

- b. *Lectures on Euclidean rings*, Fakultät für Mathematik, Universität Bielefeld.
- c. *Abelian extensions of arbitrary fields* (with W. Kuyk), Math. Ann. **216**, 99–104.
- d. *Euclid's algorithm in cyclotomic fields*, J. London Math. Soc. **10**, 457–465.
- e. *Linear independence of cosecant values* (with H. Jager), Nieuw Arch. Wisk. (3) **23**, 131–144.
- f. *Arithmetische codes*, ch. VIII in: *Inleiding in de coderingstheorie*, ZC 87/75, Mathematisch Centrum, Amsterdam.

## 1976

- a. *Euclidean number fields of large degree*, Report 76-09, Mathematisch Instituut, Universiteit van Amsterdam.
- b.  *$K_2$  of a global field consists of symbols*, pp. 69–73 in: M.R. Stein (ed.), *Algebraic K-theory, Proceedings of the conference held at Northwestern University*, Lecture Notes in Mathematics **551**, Springer-Verlag, Heidelberg.
- c. *Arithmetische codes*, ch. 10 in: J.H. van Lint (ed.), *Inleiding in de coderingstheorie*, MC Syllabus 31, Mathematisch Centrum, Amsterdam.

## 1977

- a. *On Artin's conjecture and Euclid's algorithm in global fields*, Report 77-03, Mathematisch Instituut, Universiteit van Amsterdam.
- b. *Euclidean number fields of large degree*, Invent. Math. **38**, 237–254.
- c. *Euclidische getallenlichamen* (Ph.D. thesis), Mathematisch Centrum, Amsterdam.
- d. *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42**, 201–224.
- e. *On the algebraic closure of two*, Proc. Kon. Ned. Akad. Wet. series A **80**, 389–396.

## 1978

- a. *Nim multiplication*, I.H. E. S., Bures-sur-Yvette.
- b. *Euclidean ideal classes*, I.H. E. S., Bures-sur-Yvette.
- c. *Artin's conjecture on primes with prescribed primitive roots*, Sémin. Delange-Pisot-Poitou **18** no. 14.
- d. *Perfect arithmetic codes*, Sémin. Delange-Pisot-Poitou **19** no. 15.
- e. *Quelques exemples d'anneaux euclidiens*, C.R. Acad. Sc. Paris Sér. I Math. **286**, 683–685.

## 1979

- a. *Euclidean number fields I*, Math. Intelligencer **2** (1), 6–15.
- b. *Nim multiplication*, Sémin. théorie des nombres, Bordeaux, 1977/78, no. 11.

- c. *Euclidean ideal classes*, Astérisque **61**, 121–131.
- d. *Vanishing sums of roots of unity*, pp. 249–268 in: P.C. Baayen, D. van Dulst and J. Oosterhoff (eds), *Proceedings bicentennial congress Wiskundig Genootschap*, Math. Centre Tracts **100 /101**, Mathematisch Centrum, Amsterdam.
- e. *Miller's primality test*, Inform. Process. Lett. **8**, 86–88.

## 1980

- a. *Grothendieck groups of abelian group rings*, Report 80-04, Mathematisch Instituut, Universiteit van Amsterdam.
- b. *On the calculation of regulators and class numbers of quadratic fields*, Report 80-08, Mathematisch Instituut, Universiteit van Amsterdam.
- c. *Primality testing*, pp. 41–60 in: *Studieweek getaltheorie en computers*, Mathematisch Centrum, Amsterdam.
- d. *Rational functions invariant under a cyclic group*, pp. 91–99 in: P. Ribenboim (ed.), *Proceedings of the Queen's number theory conference, 1979*, Queen's papers in pure and applied mathematics **54**, Kingston.
- e. *Euclidean number fields 2*, Math. Intelligencer **2** (2), 73–77.
- f. *Euclidean number fields 3*, Math. Intelligencer **2** (2), 99–103.

## 1981

- a. *Grothendieck groups of abelian group rings*, J. Pure Appl. Algebra **20**, 173–193.
- b. *Primality testing algorithms*, Séminaire Bourbaki **33** exp. no. 576, pp. 243–257 in Lecture Notes in Mathematics **901**, Springer-Verlag, Heidelberg.
- c. *Primality testing with Frobenius symbols*, C.-R. des Journées de théorie analytique et élémentaire des nombres, Reims.
- d. *Integer programming with a fixed number of variables*, Report 81-03, Mathematisch Instituut, Universiteit van Amsterdam.

## 1982

- a. *On a question of Colliot-Thélène*, pp. 143–147 in: M.-J. Bertin (ed.), *Séminaire de théorie des nombres Paris 1980-1981*, Progress in Mathematics **22**, Birkhäuser, Boston.
- b. *Primaliteit en factorisatie*, pp. 69–81 in: P.M.B. Vitányi, J. van Leeuwen and P. van Emde Boas (eds), *Colloquium complexiteit en algoritmen, deel 2*, MC syllabus 48.2, Mathematisch Centrum, Amsterdam.
- c. *On the calculation of regulators and class numbers of quadratic fields*, pp. 123–150 in: J. Armitage (ed.), *Journées Arithmétiques 1980*, London Math. Soc. Lecture Note Ser. **56**, Cambridge University Press, Cambridge.
- d. *Factoring polynomials with rational coefficients* (with A.K. Lenstra and L. Lovász), Report 82-06, Mathematisch Instituut, Universiteit van Amsterdam; Report IW 195/82, Mathematisch Centrum, Amsterdam.

- e. *Primality testing with Artin symbols*, pp. 341–347 in: N. Koblitz (ed.), *Number theory related to Fermat's last theorem*, Progress in Mathematics **26**, Birkhäuser, Boston.
- f. *Factoring polynomials with rational coefficients* (with A.K. Lenstra and L. Lovász), Math. Ann. 261, 515–534.
- g. *Primality testing and Jacobi sums* (with H. Cohen), Report 82-18, Mathematisch Instituut, Universiteit van Amsterdam.
- h. *Arithmetic codes*, ch. 10 in: J.H. van Lint, *Introduction to coding theory*, Graduate Texts in Mathematics **86**, Springer-Verlag, New York.
- i. *Reduced bases for lattices and factorization of polynomials*, Sémin. théorie des nombres, Bordeaux, 1981/82, no. 35.

### 1983

- a. *Computational methods in number theory* (edited with R. Tijdeman), Math. Centre Tracts **154/155**, Mathematisch Centrum, Amsterdam; second edition, 1984.
- b. *Introduction*, pp. 1–6 in 1983a.
- c. *Primality testing*, pp. 55–77 in 1983a.
- d. *Primality and factorization*, pp. 13–15 in: E.C. van der Meulen (ed.), *Proceedings of the fourth symposium on information theory in the Benelux*, Leuven.
- e. *Snelle priemgetaltests*, Wiskunde en onderwijs **9**, 171–178.
- f. *Fast prime number tests*, Nieuw Arch. Wisk. (4) **1**, 133–144.
- g. *Divisors in residue classes*, Report 83-03, Mathematisch Instituut, Universiteit van Amsterdam.
- h. *Abelian varieties having very bad reduction* (with F. Oort), Report 315, Mathematisch Instituut, Rijksuniversiteit Utrecht.
- i. *Integer programming with a fixed number of variables*, Math. Oper. Res. **8**, 538–548.

### 1984

- a. *Primality testing and Jacobi sums* (with H. Cohen), Math. Comp. **42**, 297–330.
- b. *Divisors in residue classes*, Math. Comp. **42**, 331–340.
- c. *A Monte Carlo factoring algorithm with linear storage* (with C. P. Schnorr), Math. Comp. **43**, 289–311.
- d. *Heuristics on class groups* (with H. Cohen), pp. 26–36 in: *Number theory*, New York 1982, Lecture Notes in Mathematics **1052**, Springer-Verlag, Heidelberg.
- e. *Heuristics on class groups of number fields* (with H. Cohen), pp. 33–62 in: H. Jager (ed.), *Number theory, Noordwijkerhout 1983*, Lecture Notes in Mathematics **1068**, Springer-Verlag, Heidelberg.
- f. *Integer programming and cryptography*, Math. Intelligencer **6** (3), 14–19.
- g. *Galois theory and primality testing*, Report 84-30, Mathematisch Instituut, Universiteit van Amsterdam.

## 1985

- a. *Abelian varieties having purely additive reduction* (with F. Oort), J. Pure Appl. Algebra **36**, 281–298.
- b. *Galois theory for schemes* (lecture notes), Mathematisch Instituut, Universiteit van Amsterdam.
- c. *A normal basis theorem for infinite Galois extensions*, Proc. Kon. Ned. Akad. Wet. series A **88**, 221–228.
- d. *Galois theory and primality testing*, pp. 169–189 in: I. Reiner, K. Roggenkamp (eds), Orders and their applications, Lecture Notes in Mathematics **1142**, Springer-Verlag, Heidelberg.
- e. *Tests rapides de nombres premiers*, Mathématique et Pédagogie **52**, 57–64.

## 1986

- a. *Finding irreducible polynomials over finite fields* (with L.M. Adleman), Proc. 18th Annual ACM Symp. on Theory of Computing (STOC), Berkeley, May 28–30, 350–355.
- b. *Primality testing*, pp. 269–287 in: J.W. de Bakker, M. Hazewinkel, J.K. Lenstra (eds), *Mathematics and computer science*, Proceedings of the CWI symposium, November 1983, CWI Monograph **1**, North-Holland, Amsterdam.
- c. *Factoring integers with elliptic curves*, Report 86-18, Mathematisch Instituut, Universiteit van Amsterdam.
- d. *Elliptic curves and number-theoretic algorithms*, Report 86-19, Mathematisch Instituut, Universiteit van Amsterdam.
- e. *Efficient algorithms in number theory* (abstract), International Congress of Mathematicians, Berkeley.
- f. *Codes from algebraic number fields*, pp. 95–104 in: M. Hazewinkel, J.K. Lenstra, L.G.L.T. Meertens (eds), *Mathematics and computer science II*, Fundamental contributions in the Netherlands since 1945, CWI Monograph **4**, North-Holland, Amsterdam.
- g. *Euclid's algorithm in large Dedekind domains*, Report 86-25, Mathematisch Instituut, Universiteit van Amsterdam.

## 1987

- a. *Primitive normal bases for finite fields* (with R. J. Schoof), Math. Comp. **48**, 217–231.
- b. *Algorithms in number theory* (with A.K. Lenstra), Technical Report 87-008, Department of Computer Science, The University of Chicago.
- c. *Factoring integers with elliptic curves*, Ann. of Math. **126**, 649–673.

## 1988

- a. *Elliptic curves and number-theoretic algorithms*, pp. 99–120 in: Proceedings of the International Congress of Mathematicians, Berkeley, 1986, American Mathematical Society, Providence.
- b. *Euclid's algorithm in large Dedekind domains*, J. Indian Math. Soc. **50** (1986), 41–47.

### 1989

- a. *Subgroups close to normal subgroups* (with G. Bergman), J. Algebra **127**, 80–97.
- b. *Über das Fortsetzen von Bewertungen in vollständigen Körpern* (with P. Stevenhagen), Arch. Math. (Basel) **53**, 547–552.

### 1990

- a. *Automorphisms of finite fields*, J. Number Theory **34**, 33–40.
- b. *Groups with finitely many non-normal subgroups* (with N. S. Hekster), Arch. Math. (Basel) **54**, 225–231.
- c. *Algorithms for finite fields*, pp. 76–85 in: J.H. Loxton (ed.), *Number theory and cryptography*, London Math. Soc. Lecture Note Ser. **154**, Cambridge University Press, Cambridge.
- d. *The number field sieve* (extended abstract) (with A.K. Lenstra, M. S. Manasse, and J.M. Pollard), Proc. 22nd Annual ACM Symp. on Theory of Computing (STOC), Baltimore, May 14–16, 564–572.
- e. *Forms in odd degree extensions and self-dual normal bases* (with E. Bayer-Fluckiger), Amer. J. Math. **112**, 359–373.
- f. *Algorithms in number theory* (with A.K. Lenstra), pp. 673–715 in: J. van Leeuwen (ed.), *Handbook of theoretical computer science*, Vol. A, *Algorithms and complexity*, Elsevier, Amsterdam and The MIT Press, Cambridge, Massachusetts.
- g. *Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice* (with J.C. Lagarias and C. P. Schnorr), Combinatorica **10**, 343–358.
- h. *Applied number theory*, pp. 5–14 in: Number Theory, Proceedings of a Symposium, May 4, 1989, National Research Council, Washington, D.C.

### 1991

- a. *Perfect squares don't exist*, Math. Intelligencer **13** (1), 40.
- b. *Finding isomorphisms between finite fields*, Math. Comp. **56**, 329–347.
- c. *Quotients of group rings arising from two-dimensional representations* (with N. Boston and K.A. Ribet), C. R. Acad. Sci. Paris Sér. I Math. **312**, 323–328.
- d. *Primes of degree one and algebraic cases of Chebotarev's theorem* (with P. Stevenhagen), Enseign. Math. (2) **37**, 17–30.
- e. *On the Chor-Rivest knapsack cryptosystem*, J. Cryptology **3**, 149–155.

### 1992

- a. [Algorithms in algebraic number theory](#), Bull. Amer. Math. Soc. **26**, 211–244.
- b. [The number field sieve \(NFS\)](#), Sec. 5.1.3, pp. 40–44 in: Th. Beth, M. Frisch, G. J. Simmons (eds), *Public-key cryptography: state of the art and future directions*, Lecture Notes in Comput. Sci. **578**, Springer-Verlag, Berlin.
- c. [A rigorous time bound for factoring integers](#) (with C. Pomerance), J. Amer. Math. Soc. **5**, 483–516. 5
- d. [On the inverse Fermat equation](#), Discrete Math. **106/107**, 329–331.
- e. [Optimal normal bases](#) (with Shuhong Gao), Designs, Codes and Cryptography **2**, 315– 323.
- f. [Numerieke aspecten van de vergelijking van Cantor](#), 5 pp., in: P. van Emde Boas et al. (eds), "Is er nog nieuws?" aangeboden aan Prof. Dr Th. J. Dekker, Amsterdam.

### 1993

- a. [The Tate conjecture for almost ordinary Abelian varieties over finite fields](#) (with Yu.G. Zarhin), pp. 179–194 in: F.Q. Gouvêa, N. Yui (eds), *Advances in number theory, The Proceedings of the Third Conference of the Canadian Number Theory Association, 1991*, Oxford University Press.
- b. [The development of the number field sieve](#) (edited with A.K. Lenstra), Lecture Notes in Mathematics **1554**, Springer-Verlag, Heidelberg.
- c. [The number field sieve: an annotated bibliography](#), pp. 1–3 in 1993b.
- d. [The number field sieve](#) (with A.K. Lenstra, M. S. Manasse, and J.M. Pollard), pp. 11–42 in 1993b.
- e. [Factoring integers with the number field sieve](#) (with J. P. Buhler and C. Pomerance), pp. 50–94 in 1993b.
- f. [The factorization of the ninth Fermat number](#) (with A.K. Lenstra, M. S. Manasse, and J.M. Pollard), Math. Comp. **61**, 319–349; *Addendum*, *ibid.* **64** (1995), 1357.
- g. [Continued fractions and linear recurrences](#) (with J.O. Shallit), Math. Comp. **61**, 351– 355.
- h. [Generating units modulo an odd integer by addition and subtraction](#), Acta Arith. **64**, 383–388.
- i. [A hyperelliptic smoothness test, I](#) (with J. Pila and C. Pomerance), Philos. Trans. Roy. Soc. London Ser. A **345**, 397–408.

### 1994

- a. [Sharp characters with only one rational value](#) (with D. Alvis, M. Kiyota, and S. Nozawa), Comm. in Algebra **22**, 95–115.
- b. [Finite complete intersection algebras](#) (with B. de Smit), Report 9453/B, Econometric Institute, Erasmus University Rotterdam.
- c. [Chebotarëv and his density theorem](#) (with P. Stevenhagen), Report 94-25, Faculteit Wiskunde en Informatica, Universiteit van Amsterdam.

## 1995

- a. *Approximating rings of integers in number fields* (with J.A. Buchmann), *Journal de Théorie des Nombres de Bordeaux* **6**, 221–260.
- b. *Complete intersections and Gorenstein rings*, pp. 99–109 in: J. Coates, S.T. Yau (eds), *Elliptic curves, modular forms, and Fermat's last theorem*, International Press, Boston.
- c. *Complete systems of two addition laws for elliptic curves* (with W. Bosma), *J. Number Theory* **53**, 229–240.
- d. *Het ontbinden van grote getallen in priemfactoren*, *Nieuwe Wiskrant* **15**, 7–15.
- e. *Does the set of points of an elliptic curve determine the group?* (with J. Pila), in: W. Bosma, A. van der Poorten (eds), *Computational algebra and number theory, Sydney 1992*, Kluwer, Dordrecht, pp. 111–118.
- f. *Rekenen met priemgetallen*, *Wiskunde en Onderwijs* **21**, 452–468.
- g. *Computing Jacobi symbols in algebraic number fields*, *Nieuw Arch. Wisk.* **13**, 421–426.

## 1996

- a. *My butter, garçon* (with E.W. Howe and D. P. Moulton), p. 28 in: A. van der Poorten, *Notes on Fermat's Last Theorem*, Wiley, New York; *reprinted* on p. 306 of: S. Singh, *Fermat's last theorem*, Fourth Estate, London, 1997.
- b. *Abelian subvarieties* (with F. Oort and Yu.G. Zarhin), *J. Algebra* **180**, 513–516.
- c. *Complex multiplication structure of elliptic curves*, *J. Number Theory* **56**, 227–241.
- d. *Chebotarëv and his density theorem* (with P. Stevenhagen), *Math. Intelligencer* **18** (2), 26–37.
- e. *Wiskunde en onbegrip*, *Nieuw Arch. Wisk.* **14**, 33–43.
- f. *A family of exceptional polynomials in characteristic three* (with M. Zieve), pp. 209–218 in: S.D. Cohen, H.G. Niederreiter (eds), *Finite fields and applications*, Cambridge University Press, Cambridge.

## 1997

- a. *Explicit construction of universal deformation rings* (with B. de Smit), pp. 313–326 in: G. Cornell, J.H. Silverman, G. Stevens (eds), *Modular forms and Fermat's last theorem*, Springer, New York.
- b. *Class field theory and the first case of Fermat's last theorem* (with P. Stevenhagen), pp. 499–503 in: G. Cornell, J.H. Silverman, G. Stevens (eds), *Modular forms and Fermat's last theorem*, Springer, New York.
- c. *Finite complete intersection algebras and the completeness radical* (with B. de Smit), *J. Algebra* **196**, 520–531.



## 1998

- a. *Andries en zijn kameraden* (edited with Ruud Koning, Jan Karel Lenstra, and Tom Wansbeek), Amsterdam, 26 maart 1998.
- b. *Het wijnmengersprobleem van Diophantus*, pp. 36–41 in 1998a.
- c. *Linearly equivalent actions of solvable groups* (with B. de Smit), 16 pages, Report W98–19, Mathematical Institute, University of Leiden.

## 1999

- a. *Finding small degree factors of lacunary polynomials*, pp. 267–276 in: K. Gyory, H. Iwaniec, J. Urbanowicz (eds), *Number theory in progress*, De Gruyter, Berlin.
- b. *On the factorization of lacunary polynomials*, pp. 277–291 in: K. Gyory, H. Iwaniec, J. Urbanowicz (eds), *Number theory in progress*, De Gruyter, Berlin.
- c. *Archimedes, The cattle problem* (with S. J. P. Hillion), Mercator Pers, Santpoort.
- d. *Rationale punten op algebraïsche oppervlakken*, *Nieuw Arch. Wisk.* **17**, 475–481.

## 2000

- a. *Artin reciprocity and Mersenne primes* (with P. Stevenhagen), *Nieuw Arch. Wisk.* (5) **1**, 44–54.
- b. *Linearly equivalent actions of solvable groups* (with B. de Smit), *J. Algebra* **228**, 270–285.

## 2001

- a. *Factoring polynomials over special finite fields* (with E. Bach and J. von zur Gathen), *Finite fields and their applications* **7**, 5–28.
- b. *Aeternitatem cogita*, *Nieuw Arch. Wisk.* (5) **2**, 23–28.
- c. *Aeternitatem cogita*, Universiteit Leiden, 20 pp., September 2001.
- d. *Het leukste van wiskunde is een bewijs*, *Natuur & Techniek* **69** (10), 66–72.
- e. *Aeternitatem cogita*, *Nieuwe Wiskrant* **21** (1), 34–41.
- f. *Flags and lattice basis reduction*, pp. 37–51 in: C. Casacuberta et al. (eds), *European congress of mathematics, Barcelona, July 10-14, 2000*, vol. I, Birkhäuser Verlag, Basel.

## 2002

- a. *Solving the Pell equation*, *Notices Amer. Math. Soc.* **49**, 182–192.
- b. *A hyperelliptic smoothness test II* (with J. Pila and C. Pomerance), *Proc. London Mathematical Soc.* (3) **84**, 2361–2401.

- c. *On a problem of Garcia, Stichtenoth, and Thomas*, Finite fields and their applications **8**, 166–170.
- d. *On hats and other covers* (with G. Seroussi), ISIT 2002, Lausanne, Switzerland.

### 2003

- a. *The mathematical structure of Escher's Print Gallery* (with B. de Smit), Notices Amer. Math. Soc. **50**, 446–451.

### 2004

- a. *La struttura matematica della Galleria di stampe di Escher* (with B. de Smit), pp. 217–226 in: M. Emmer (ed.), *Matematica e cultura 2004*, Springer-Verlag, Milano.
- b. *Escher en het Droste-effect*, pp. 21–30 in: Natuurkundige Voordrachten Nieuwe Reeks **82**, Diligentia, 's-Gravenhage.

### 2005

- a. *Over de fabricage van priemgetallen*, Verslag van de gewone vergadering van de Afdeling Natuurkunde, deel 114, nr. 1, 9–13, Koninklijke Nederlandse Akademie van Wetenschappen.
- b. *Profinite Fibonacci numbers*, Nieuw Arch. Wisk. (5) **6**, 297–300.
- c. *Escher en het droste-effect*, pp. 131–144 in: B. Mols (ed.), *Het raadsel van informatie*, Boom, Amsterdam.

### 2006

- a. *Profinite Fibonacci numbers*, Newsletter of the European Mathematical Society **61** (September 2006), 15–19.

### 2007

- a. *Commentary on H: Divisibility and congruences*, in: Andrzej Schinzel, *Selected papers*, European Mathematical Society, Zürich, 2007, vol. II, 901–902.
- b. *Detecting perfect powers by factoring into coprimes* (with D. J. Bernstein and J. Pila), Math. Comp. **76**, 385–388.
- c. *Het hoofd en de boekenkast* (3 pages), published in a collection of essays dedicated to Jan Karel Lenstra on the occasion of his sixtieth birthday.

### 2008

- a. *Solving the Pell equation*, pp. 1–23 in: J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, Mathematical Sciences Research Institute Publications, Cambridge University Press.
- b. *Lattices*, pp. 127–181 in: J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, Mathematical Sciences Research Institute Publications, Cambridge University Press.

**2009**

- a. *Ode aan het getal 43*, Nieuw Arch. Wisk. (5) **10**, 240–244.

**2010**

- a. *Irreducible cubics modulo five*, Amer. Math. Monthly **117**, 817–821.

*Elliptic curves and factorization algorithms* (?), Report 87-2, Mathematisch Instituut, Universiteit van Amsterdam.

*De kleinste algoritme van enkele euclidische ringen* 1973? , Universiteit van Amsterdam.