

CURRICULUM VITAE

of Peter Stevenhagen

Born: March 12, 1963 in Haarlem, the Netherlands.

Civil status: daughters Susanne (1999), Eva (2002) en Louise (2003) with Armelle Rouyère, born July 6, 1965 in Clermont (Oise, France).

ADRESSES

Mathematisch Instituut – Universiteit Leiden

Postbus 9512

2300 RA Leiden, the Netherlands

Phone + 31 71 527 7125

E-mail: psh@math.leidenuniv.nl

Herengracht 277

1016 BK Amsterdam

Phone + 31 20 6204588

POSITIONS

2000– : full professor in mathematics, Universiteit Leiden;

2005–06: visiting professor, University of California at San Diego;

1997–99: associate professor, Universiteit van Amsterdam;

1991–96: assistant professor, Universiteit van Amsterdam;

1990–92: *chargé de recherche* (CNRS), Université de Franche-Comté, Besançon, France;

1989–90: stipend of the Dutch Organisation for Scientific Research (NWO) for a one-year stay at the University of California, Berkeley;

1987–88: teaching assistant, University of California, Berkeley.

1986: instructor, University of Chicago;

1986: part-time teacher (1st degree) in physics, Gymnasium Felisenum, Velsen;

1985–1989: PhD student and lecturer at the Universiteit van Amsterdam;

1982–85: teaching assistant in mathematics, Universiteit van Amsterdam.

EDUCATION

1989: ‘doctoraat’ in mathematics, Universiteit van Amsterdam.

Thesis: *Ray class groups and governing fields*; advisor: H. W. Lenstra, Jr.

1988: PhD in Mathematics, University of California, Berkeley;

1985: doctoraalexamen in mathematics (cum laude), Universiteit van Amsterdam.

Minor thesis: *Generalized unramified class field theory*; secondary topic: Russian language and literature;

1982: kandidaatsexamen in mathematics and physics (cum laude), Universiteit van Amsterdam;

1980: exam of the ‘gymnasium’ (10 subjects), Gymnasium Felisenum, Velsen;

LANGUAGES

Dutch, French, English, German, Russian

HONORS

- 2004: best teacher in mathematics, Faculty of Science
- member, special semester on Algorithmic Number Theory, Mathematical Sciences Research Institute, Berkeley (2000);
- 1989–90: NWO travel stipend (12 months)
- 1987: Regent's Fellowship of the University of California, Berkeley;
- 1984: prize at the International Student Competition in Mathematics, Belgrade;
- 1980: member of the Dutch team at the International Mathematical Olympiad in Luxemburg;

REFEREED PUBLICATIONS

1. *On Aurifeuillian factorizations*, Indag. Math. **90**(4), 451–468 (1987). MR 89a:11015
2. *Unramified class field theory for orders*, Trans. Amer. Math. Soc. **311**(2), 483–500 (1989). MR 90b:11119
3. (with H. W. Lenstra, Jr.) *Über das Fortsetzen von Bewertungen in vollständigen Körpern*, Archiv für Mathematik **53**, 547–552 (1989). MR 90j:12018
4. *Ray class groups and governing fields*, Academisch proefschrift (1989). Appeared as: Publ. Math. Fac. Sci. Besançon, année 1989/90, 1–94. MR 91j:11095
5. (with H. W. Lenstra, Jr.) *Primes of degree one and algebraic cases of Čebotarev's theorem*, Ens. Math. **37**, 17–30 (1991). MR 92f:11162
6. *On the 2-power divisibility of certain quadratic class numbers*, J. of Number Theory **43** (1), 1–19 (1993). MR 94b:11113
7. *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (2), 121–136 (1993). MR 94k:11120
8. *Extensions of homomorphisms and the structure of ray class groups*, J. of Algebra **163** (3), 832–860 (1994). MR95c:11130
9. *Class number parity for the p -th cyclotomic field*, Math. Comp. **63** no. 208, 773–784 (1994). MR95a:11099
10. *A density conjecture for the negative Pell equation*, in: Computational Algebra and Number Theory, 187–200, Mathematics and Its Applications 325, Kluwer Academic Publishers, Dordrecht, 1995. MR96g:11137
11. *Rédei-matrices and applications*, in: Number Theory Paris 1992–93, 245–259, London Math. Soc. Lecture Notes 215, Cambridge University Press, 1995. MR97b:11132
12. *Frobenius distributions for real quadratic orders*, J. Théorie des Nombres Bordeaux **7** (1), 121–132 (1995). MR97g:11118
13. *Lattices and quadratic forms*, in: Summer course 1995: conic sections and quadratic forms (Dutch), CWI Syllabus 40, 94–109 (1995). MR96k:11046

14. (with W. Bosma) *Density computations for real quadratic units*, Math. Comp. **65** no. 215, 1327–1337 (1996). MR96j:11171
15. (with H. W. Lenstra, Jr.) *Chebotarev and his density theorem*, Math. Intelligencer **18** (2), 11 pp. (1996). MR97e:11144
16. *On a problem of Eisenstein*, Acta Arith. **74**(3), 259–268 (1996). MR97b:11138
17. (with W. Bosma) *On the computation of quadratic 2-class groups*, J. Théorie des Nombres Bordeaux **8** (1996), no. 2, 283–313. MR98e:11129
18. (with H. W. Lenstra, Jr.) *Class field theory and the first case of Fermat’s Last Theorem*, in: Modular Forms and Fermat’s Last Theorem (Cornell, Silverman, Stevens, Eds), Springer-Verlag (1997). MRMR1638492
19. (with P. Moree) *Prime divisors of Lucas sequences*, Acta Arith. **82**(4), 403–410 (1997). MR98i:11098
20. (with A. C. P. Gee) *Generating class fields using Shimura reciprocity*, in: Algorithmic Number Theory (J. P. Buhler, ed.), 441–453, LNCS 1423, Springer Verlag (1998). MR2000m:11112
21. *Prime numbers*, in: Summer course 1999: unproven conjectures (Dutch), CWI Syllabus **45**, 17–29 (1999). MR2001f:11013
22. (with H. W. Lenstra, Jr.) *Artin reciprocity and Mersenne primes*, Nieuw Arch. Wiskd. (5) **1** (2000), no. 1, 44–54. MR2001h:11006
23. (with P. Moree) *A two-variable Artin conjecture*, J. Number Theory **85** (2000), no. 2, 291–304. MR2001k:11188
24. (with P. Moree) *Prime divisors of the Lagarias sequence*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 241–251. MR2002c:11016
25. *Hilbert’s 12th problem, complex multiplication and Shimura reciprocity*, in: Class Field Theory - Its centenary and Prospect, 161–176, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, (2001). MR2002i:11110
26. *The correction factor in Artin’s primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 383–391. MR2019022
27. *Triangles, squares, oranges and cuboids*, in: Mathematical Adventures for Students and Amateurs, D. F. Hayes & T. Shubin (eds.), MAA Spectrum Series, 51–63 (2004)
28. (with D. A. Cox and J. McKay) *Principal moduli and class fields*, Bull. London Math. Soc. **36** (2004), no. 1, 3–12. MR2011972
29. (with R. Bröker) *Elliptic curves with a given number of points*, in: Algorithmic Number Theory (D. Buell, ed.), 117–131, LNCS 3076, Springer Verlag (2004). MR
30. *The number field sieve*, in: Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press. MR.

31. (with R. Bröker) *Efficient CM-constructions of elliptic curves over finite fields*, Math. Comp. (to appear)
32. *The arithmetic of number fields*, in: Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press. 50pp. MR.

IN PREPARATION

33. *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Cambridge University Press, editors J. P. Buhler en P. Stevenhagen.
34. (with H. Cohen) *Computational class field theory*, preprint
35. (with H. W. Lenstra, Jr. and P. Moree) *Character sums for primitive root densities*, preprint
36. *Prime densities for second order torsion sequences*, preprint
37. (with R. Bröker) *Constructing elliptic curves of prime order*, in preparation

POPULARIZING

38. *Fermats laatste stelling en de ontwikkeling van de getaltheorie*, in: ‘De Laatste Stelling van Fermat’, syllabus Nationale Fermatdag, 3–13 (1993).
39. *De wiskunde van de overkant*, Afliding **6**, 12–14 (1996)
40. *Driehoeksgetallen en kwadraten*, Pythagoras **5**, 4–7 (1997).
41. (met W. Bosma) *Priemgetallen*, serie in Pythagoras, jaargang 1997-1998.
42. Review of *Quadratics* by R.A. Mollin, Bull. Amer. Math. Soc. **35** (4), 333–338. (1998)
43. *Een Europees visitekaartje*, Nieuw Arch. Wiskd. (5) 1, no. 2, 162–164 (2000)
44. *Het Wiskundig Genootschap*, Notices of the South African Mathematical Society **31**, no. 2, 36–40 (2000).
45. *Rekenen en getaltheorie*, oratie, Universiteit Leiden (2001).
46. *Meetkunde en getaltheorie in de laatste stelling van Fermat*, in: Speeltuin van de wiskunde, 93–104, Veen Magazines (2003).
47. *Homeland Security*, Nieuw Arch. Wiskd. (5) 6, no. 4 (2005)

TALKS

Sinds 1985 more than 150 invited talks on conferences and seminars all over the world. Usually in English, incidentally in French or German. Most of the time for experts or for a broad mathematical audience, sometimes for high school students, teachers or non-mathematicians.

TEACHING

Numerous courses at the Universiteit van Amsterdam (1982–1999), University of Chicago (1986), University of California (1987–1988), Université de Franche-Comté (1989–1991) and, as of 2000, at the Universiteit Leiden. Courses and seminar talks at UC San Diego (2005-06).

Undergraduate courses in analysis and (linear) algebra, big calculus courses, many advanced courses in number theory (algebraic number theory, class field theory, Iwasawa theory, complex multiplication) and related topics (elliptic curves, Riemann surfaces). Graduate seminars in number theory. Just once: *Scientific Russian* (Universiteit van Amsterdam, 1991).

Responsible for the Leiden courses Algebra 1, Algebra 2 en Algebra 3.

Coordinator of the Stieltjes Onderwijsweken, organiser of the weeks on *Riemann surfaces* (2000), *Algorithms in number theory* (2001), *Explicit algebraic number theory* (2002). See www.stieltjes.org/stieltjesweken.html.

Invited instructor for the Oberwolfach Seminar *Explicit Algebraic Number Theory* (2002).

Instructor for the 2004 national master course *Algebraic number theory*.

Invited instructor for the special course *Number theory in cryptography*, Bogota, Colombia (2006).

Supervisor of the master theses of the later PhD students A. Herczog (KUN), A. van der Waall (UU), M. Mackaaij (Univ. Algarve), J. Scholten (RUG), W. Oudshoorn (RUG), A. Gee (UvA), J. Roskam (UL), J. Daems (UL).

PHD STUDENTS

- A. C. P. Gee (UvA, 2001)
- J. Roskam (UL, 2003)
- R. Bröker (UL, 2006)
- W.J. Palenstijn (UL, expected 2008)
- M. Streng (UL, expected 2010).

MEMBERSHIP OF EDITORIAL BOARDS

- Contributions to Discrete Mathematics
- Japan Journal of Industrial and Applied Mathematics (guest associate editor for the special issue on Algorithmic Number Theory, Vol.24, No.3)

ORGANISATION OF CONFERENCES AND WORKSHOPS

- Initiator (in 1993) and organizer of the biweekly *Intercity number theory seminar*. The national platform for research in number theory in the Netherlands, and one of the oldest still running math seminars in the country.

- Organizer (with H. W. Lenstra) of the ‘Centenary Celebrations’ at the Universiteit van Amsterdam; in 1994 the *Chebotarev Density Celebration*, in 1998 the *Artin Reciprocity Celebration*. Invited speakers: Serre, Zagier, Tate, Tits.
- Chair of the Algorithmic Number Theory Symposium ANTS IV in Leiden (2000).
- Organizer of the Lorentz-workshops *L-functions from algebraic geometry* (2001), *Abelian number theory and geometry* (2001), *Explicit algebraic number theory* (2002).
- Co-organizer of the workshop *Explicit Methods in Number Theory*, Pacific Institute for the Mathematical Sciences, Banff, Canada (2004).
- Organizer of the Special Session on *Field extensions and algorithms* at the Annual Mathematical Meeting of the American Mathematical Society in San Antonio, Texas (2006).
- Programme Committee member of the Algorithmic Number Theory Symposium ANTS VII in Berlin (2006).

EXTERNAL FUNDING

- Amsterdam representative and co-author of the NWO Groot Project *getaltheorie* (1995–2000, 800kf).
- budget ANTS IV (50 kf excluding the Ludolph van Ceulen tombstone in the Leiden Pieterskerk) from various sponsors.
- stipend for *Vierkant voor Wiskunde* from the Gratama Stichting (2001, 50kf)
- NWO-grant ‘Leraar in Onderzoek’ for the project *Algorithmen in de klassenlichamentheorie*
- PhD position (with Bart de Smit) for the NWO project *Radicals in arithmetic* (2004–2008, 230kE)
- Leiden coordinator of the Erasmus Mundus ALGANT master program (joint program with the universities of Bordeaux, Padova and Paris-Orsay)
- one of the four authors of the DIAMANT cluster proposal (2005–2009, 3000kE).
- NWO-grant ‘Leraar in Onderzoek’ for the project *Reken mee met ABC*

ADMINISTRATION

- member of the board of the KdV Instituut voor Wiskunde at the Universiteit van Amsterdam (1991–1993).
- Head of the *UvA Number Theory* group (1995–2000)
Two-year postdocs in the group: W. Bosma (1996–1997), B. de Smit (1996–1997).
One-year postdocs: P. Moree, V. Talamanca.
PhD students: A. C. P. Gee (thesis defense: UvA, 2001), J. Roskam (thesis defense: Leiden, 2003).
- coordinator graduate studies in mathematics at the Universiteit van Amsterdam (1996–1999).
- member of the board of the Dutch Mathematical Society (1999–2002)
- secretary for education of the Thomas Stieltjes Instituut (1998–)

- member of the VSNU-kamer (Association of Dutch universities) for mathematics for the Universiteit Leiden (2001–)
- jury member of the NWO committee for VIDI-grants (2003, 2005)
- member for the Universiteit Leiden of the Regieorgaan Landelijke Masteropleidingen Wiskunde (2004–)
- director of education of the Mathematisch Instituut, Leiden (2001–)
- adjoint to the Board of the DIAMANT cluster (2005–)
- lid Nationale Strategievergadering Wiskunde (2006–07)