Curriculum of René Schoof (version September 2012).

2ª Università di Roma "Tor Vergata"
Dipartimento di Matematica
I-00133 ROMA, Italy

May 8, 1955	Born in Den Helder, The Netherlands.
1974–1979	Study in pure mathematics, University of Amsterdam. Doctoraalscriptie with Prof. H.W. Lenstra jr.
1976–1983	Assistent, Universities of Amsterdam and Leiden.
1983–1984	Visiting Lecturer, University of Maryland.
1984–1985	Scientific assistent, University of Amsterdam.
May 1985	Ph.D. Thesis. Advisor: Prof. H.W. Lenstra jr.
1985–1987	Visitor of MSRI at Berkeley.
1986–1987	Lecturer, University of California at Berkeley.
1987–1988	Visiting Professor at the University of Pisa. CNR Fellowship at the University of Pisa.
1988–1990	*Huygens & Huygens* fellow at the University of Utrecht.
1990–1994	Professore straordinario, Università di Trento, Italy.
1999–2000	Visiting Professor at Harvard University.
Fall 2000	Visiting Professor at the University of California at Berkeley and MSRI.
Spring 2006	Visitor at MSRI, Berkeley.
Spring 2012	Two months visitor at Harvard University.
1994–...	Professore ordinario, Università di Roma II, "Tor Vergata" Italy.

1987–2004	Editor of the AMS journal *Mathematics of Computation.*
1996–2004	Editor of *Revista de Matemática de la Universidad Complutense.*
1998–2004	Editor of *Journal de Théorie de Nombres de Bordeaux*
2011–...	Editor of *Rendiconti del Circolo Matematico di Palermo*
1988–2004	Reviewer for Zentralblatt für Mathematik.
1987–...	Reviewer of several NSF–proposals.
1994–2002	Program committee member of the biannual ANTS conference.
July 1999	Organizer (with F. Pappalardi and V. Talamanca) of the "XXI Journées Arithmétiques" and editor of its proceedings: *Journal de Théorie de Nombres de Bordeaux* **13**, (2001).
April 2004	Organizer (with G. van der Geer and B. Moonen) of the Texel meeting and editor of its proceedings: *Number Fields and Function Fields: Two Parallel Worlds*, Progress in Mathematics, Birkhäuser 2005.
Fall 2004	Member of scientific committee of the "XXIV Journées Arithmétiques".
May 2005	Organizer (with B. Conrad and F. Andreatta) of the Oberwolfach Seminar on group schemes and p-divisible groups.
July 2005	Organizer of the summer school "Number fields and curves over finite fields", Anogia Crete.
1998–...	Supervisor of 20 PhD theses.

1983–...	Several visits of at least one month: the Max Planck Institut in Bonn, the Tata Institute for Fundamental Research in Bombay,

de Universiteit van Amsterdam, de Universiteit van Utrecht, the University of Maryland at College Park, the University of California at Berkeley and the MSRI in Berkeley, CICMA at Concordia University in Montreal, l'Université de Paris VII, Université Laval in Quebec, Tokyo Metropolitan University, and l'Université de Franche-Comté at Besançon, IMPA Rio de Janeiro, University of California at San Diego.

1985–... Referee of several papers for *Mathematics of Computation, Annals of Mathematics, Inventiones Mathematicae, Mathematische Annalen, Acta Arithmetica, Annales Fourier, Proceedings of the AMS, Journal of Number Theory, Compositio Mathematicae, Journal für die reine und angewandte Mathematik, Journal of Pure and applied Algebra, Abhandlungen Hamburg, J. Experimental Mathematics, Journal of Complexity Theory, IEEE Transactions of Information Theory, ...*

List of publications of René Schoof (September 2012).

2ª Università di Roma "Tor Vergata"
Dipartimento di Matematica
I-00133 ROMA
Italy

1982

- *Quadratic fields and factorization*, pp. 235–286 in: H.W. Lenstra jr. and R. Tijdeman (eds.): "Computational Methods in Number Theory", MC-Tracts 154/155, Amsterdam 1982.

1983

- *Class groups of complex quadratic fields*, Math. Comp. **41**, (1983), 295–302.

1984

- (with J. van der Craats) *On the normal subgroups of Rubik groups*, Nieuw archief voor wiskunde **2**, (1984), 267–280.

1985

- *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44**, (1985), 483–494.
- *Elliptic curves and class groups*, Thesis, Universiteit van Amsterdam, 1985.

1986

- *Infinite class field towers of quadratic fields*, J. für die reine und angewandte Mathematik **372**, (1986), 209–220.
- (with H.W. Lenstra jr.) *Primitive normal bases for finite fields*, Math. Comp. **48**, (1986), 217–231.

1987

- *Nonsingular plane cubic curves over finite fields*, J. of Combinatorial Theory, series A, **46**, (1987), 183–211.

1988

- *Cohomology of class groups of cyclotomic fields; an application to Morse-Smale diffeomorphisms*, J. of Pure and Applied Algebra **53**, (1988), 125–137.
- *Fattorizzazione e criptosistemi a chiave pubblica*, Didattica delle scienze **137**, (1988), 48–54.
- (with L.C. Washington) *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50**, (1988), 543–556.

1990

- *The structure of minus class groups of abelian number fields*, pp. 185–204 in: C. Goldstein (ed.), "Séminaire de Théorie de Nombres, Paris 1988–1990", Progress in Math. **91**, Birkhäuser 1990.
- *Algebraic curves and coding theory*, Preprint 336, 38 pages. Università di Trento 1990.

1991

- *The exponents of the groups of points on the reductions of an elliptic curve*, pp. 325–336 in: G. Van der Geer, "Arithmetic Algebraic Geometry", Progress in Math. **89** , Birkhäuser, New York 1991.
- (with M. van der Vlugt) *Hecke operators and the weight distributions of certain codes*, Journal of Combinatorial Theory A, **57**, (1991), 163–186.

1992

- *Algebraic curves over* $\mathbf{F}_2$ *with many rational points*, Journal of Number Theory **41** (1992), 6–14.
- (with G. van der Geer and M. van der Vlugt) *Weight formulas for ternary Melas codes*, Math. Comp. **58**, (1992), 781–792.

1995

- *Counting points on elliptic curves over finite fields*, in: "Les 18ièmes Journées Arithmétiques, Bordeaux 1993", J. Théorie de Nombres Bordeaux **7** (1995), 219–254.
- *Families of curves and weight distributions of codes*, Bull. AMS. **32** (1995), 171–183.
- *Fermat's Last Theorem*, pp. 193–211 in: "Überblicke der Mathematik", Vieweg-Verlag 1995.
- (with J.S. Kraft) *Computing Iwasawa invariants of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.
- *Wiles's proof of the Taniyama-Weil conjecture for semi-stable elliptic curves over* $\mathbf{Q}$, Gazette de Mathématiques **66** (1995), 7–24.

1996

- (with N. Schappacher) *Beppo Levi and the arithmetic of elliptic curves*, The Mathematical Intelligencer **18** (1996), 57–69.

1997

– (with C. Corrales Rodrigáñez) *The support problem and its elliptic analogue*, Journal of Number Theory **64** (1997), 276–290.

– (with B. de Smit and K. Rubin) *Criteria for complete intersections*, pp. 343–355 in: G. Cornell, J. Silverman, G. Stevens (eds.), "Modular Forms and Fermat's Last Theorem", Springer Verlag, New York 1997.

1998

– *Minus class groups of cyclotomic fields of prime conductor*, Math. Comp **67** (1998), 1225–1245.

1999

– *Algebraic number theory*, pp. 23–32 in: C. Andradas and C. Corrales Rodrigáñez (eds.): "400 años de matemáticas en torno al último teorema de Fermat", Editorial de la Universidad Complutense de Madrid, 1999.

2000

– (with G. van der Geer) *Effectivity of Arakelov divisors and the analogue of the theta divisor of a number field*, Selecta Math., New Ser. **6** (2000), 377–398. (preprint 9802121 at: http://xxx.lanl.gov/list/math.AG/9802).

2001

– *Finite flat group schemes over Artin rings*, Compositio Math. **128** (2001), 1–15.

– *Abelian varieties with good reduction everywhere over* $\mathbf{Q}(\sqrt{6})$, p. 287–306 in "Class Field Theory – Its Centenary and Prospect" (ed. by K. Miyake), Advanced Studies in Pure Mathematics, Math. Soc. Japan, Tokyo 2001.

– *Abelian varieties over the field of the 20th roots of unity with good reduction everywhere*, p. 291–296 in Ciliberto, C. et al., Proceedings of the NATO advanced research workshop "Applications of Algebraic Geometry to Coding Theory, Physics and Computation",Kluwer, Dordrecht 2001.

2002

– (with J.-C. Lario) *Computations with Hecke rings and deformation rings*, J. of Experimental Math. **11** (2002), 303–312.

– *Wiles's proof of the Taniyama-Weil conjecture for semi-stable elliptic curves over* $\mathbf{Q}$, Reprinted in Kantor, J.M. (ed): Où sont les Mathématiques?, Société Math. de France, Vuibert, Paris 2002, 305–326.

2003

– *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Annalen. **325** (2003), 413–48.

– *Class groups of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), 913–937.

2004

– (with E. Bayer-Fluckiger, M. Monsurrò, R. Parimala) *Trace forms of G-Galois algebras in virtual cohomological dimension 1 and 2*, Pacific J. of Math., **217** (2004), 29–43.

2005

– *Abelian varieties over* **Q** *with bad reduction in one prime only*, Compositio Math. **141** (2005), 847–868.

2006

– (with M. Larsen) *A refined counter-example to the support conjecture for abelian varieties*, J. of Number Theory. **116** (2006), 396–398.

2008

– *Four primality testing algorithms*, in Buhler, J.P. and Stevenhagen, P. Eds.: *Surveys in Algorithmic Number Theory*, MSRI Publications **44** Cambridge University Press, Cambridge 2008. 101–126.

– *Computing Arakelov class groups*, in Buhler, J.P. and Stevenhagen, P. Eds.: *Surveys in Algorithmic Number Theory*, MSRI Publications **44** Cambridge University Press, Cambridge 2008. 447–495

– *Catalan's Conjecture*, Universitext, Springer-Verlag, ISBN 978-184800-184-8, London 2008.

2010

– (with L.C. Washington) *Visibility of ideal classes* , Journal of Number Theory **130** (2010), 2715–2731..

2011

– *Semistable abelian varieties with good reduction outside* 15, Manuscripta Mathematica **139** (2012), 49–70.

2012

– (with N. Tzanakis) *Integral points of a modular curve of level* 11, Acta Arithmetica **152** (2012), 39–49.

– *On the modular curve* $X_0(23)$, in "*Geometry and Arithmetic*, EMS Publishing House, Zürich 2012, 317–345.

2014

– (with V. Dose, J. Fernandez, J. Gonzalez) *The automorphism group of the non-split Cartan modular curve of level* 11, Journal of Algebra **417** (2014), 95–102.

2015

– *The discrete logarithm problem*, in Eds. Nash, J. and Rassias, M.: "Open problems in mathematics, Springer Verlag.