Annex 2: Curriculum vitae and publication list

Biographical details
Full name: Hendrik Willem Lenstra.
Titles: Prof. Dr.
Date of birth: April 16, 1949.
University and Faculty: Universiteit Leiden, Faculteit der Wiskunde en Natuurwetenschappen.
Work address and telephone number: Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 CA Leiden, tel. 071-527-7127.

Training
Particulars of doctorate: 1977, "Euclidische getallenlichamen", supervisor F. Oort.

Career
Past and present positions: full professor, Universiteit van Amsterdam (1978–1986); full professor, University of California at Berkeley (1987–2003); full professor, Universiteit Leiden (1998–. . .).
Memberships, prizes awarded, lecture invitations received (selection): Koninklijk Wiskundig Genootschap, American Mathematical Society, Koninklijke Nederlandse Akademie van Wetenschappen (since 1984), American Academy of Arts and Sciences (since 1996), Hollandsche Maatschappij der Wetenschappen (since 2001), Academia Europaea (since 2005), Fulkerson Prize (American Mathematical Society & Mathematical Programming Society, 1985), Distinguished visiting professorship (Institute for Advanced Study, Princeton, 1990/1991), Honorary doctorate (Université de Franche Comté, Besançon, 1995), Spinoza award (1999), Séminaire Bourbaki (1981), Porcelli lectures (LSU, Baton Rouge, 1985), Plenary lecture (International Congress of Mathematicians, Berkeley, 1986), Plenary lecture (Joint Mathematics Meeting, 1988), Progress in mathematics lecture (American Mathematical Society, 1991), Distinguished lecturer (University of Waterloo, 1992), Main speaker (First Annual Meeting of the Saudi Association for Mathematical Sciences, Riyadh, Saudi Arabia, 1994), Kloosterman professor (Leiden, 1995), Bernoulli lecturer (Groningen, 1995), First EMS lecturer (Besançon, 1995), Division speaker (Reed College, 1997), Beeger lecture (Enschede, 1998), Cryptographie et théorie des nombres (Académie des sciences, Paris, 1999), Plenary lecture (Third European Congress of Mathematicians, Barcelona, 2000), Hewlett Packard/MSRI visiting research professor (2000/2001), Invited address (Joint Mathematics Meetings, 2002), Mahler lecturer (Australia, 2003), Colloquium lecturer (American Mathematical Society, 2006).

Administrative and management activities
Department chair, Mathematisch Instituut, Universiteit van Amsterdam, Fall 1986. Former member of many committees of the American Mathematical Society. Former member of

many committees in the Department of Mathematics, University of California, Berkeley. Former member of the Comité scientifique de l'I. H. E. S. Former member of a number of KNAW committees. Member of the Commissie Persoonlijke Archieven van Wiskundigen of the Koninklijk Wiskundig Genootschap. Organizer and coorganizer of numerous scientific meetings. Non-organizer of the *Lenstra Treurfeest*, Berkeley, 2003. Editor or former editor of several journals and a book series.

Awards and Honours
See above.

Ph.D. students
H. Zantema (Universiteit van Amsterdam, "Integer valued polynomials in algebraic number theory", 1983, Dutch, employed in the Technische Universiteit Eindhoven),
F. J. van der Linden (Universiteit van Amsterdam, "Euclidean rings with two infinite primes", 1984, Dutch, employed in industry),
R. J. Schoof (Universiteit van Amsterdam, "Elliptic curves and class groups", 1985, Dutch, professor in the Università di Roma),
N. S. Hekster (Universiteit van Amsterdam, "Isoclinism, isologism and representations of finite groups", 1986, Dutch, employed in industry),
P. Stevenhagen (University of California, "Class groups and governing fields", 1988, and: Universiteit van Amsterdam, "Ray class groups and governing fields", 1989, Dutch, professor in the Universiteit Leiden),
W. Bosma (Universiteit van Amsterdam, "Primality proving with cyclotomy", 1990, Dutch, employed in the Radboud Universiteit Nijmegen),
M. P. M. van der Hulst (Universiteit van Amsterdam, "Primality proving with cyclotomy", 1990, Dutch, employed in industry),
O. Schirokauer (University of California, "On pro-finite groups and on discrete logarithms", 1992, American, professor in Oberlin College, U.S.A.),
E. Schaefer (University of California, "Class groups and Selmer groups", 1992, American, professor in Santa Clara University, U.S.A.),
G. Ge (University of California, "Algorithms related to multiplicative representations of algebraic numbers", 1993, Chinese),
B. de Smit (University of California, "Class group relations and Galois module structure", 1993, Dutch, employed in the Universiteit Leiden),
E. Howe (University of California, "Elliptic curves and ordinary abelian varieties over finite fields", 1993, American, employed in the Center for Communications Research, U.S.A.),
S. W. Yiu (University of California, "Computing L-series and the rank of semistable elliptic curves over $\mathbf{Q}$", 1993, Chinese),
D. J. Bernstein (University of California, "Detecting perfect powers in essentially linear

time, and other studies in computational number theory", 1995, American, professor in the University of Illinois, U.S.A.),

C. C. Powell (University of California, "Two problems from elementary number theory involving the Euler phi-function", 1995, American),

D. P. Moulton (University of California, "Number theory and groups", 1995, American, employed in the Institute for Defense Analyses, U.S.A.),

C. F. Cotner (University of California, "The nesting depth of radical expressions", 1995, American),

S. J. P. Hillion (University of California, "Dimensions of spaces of modular forms", 1996, English),

M. E. Zieve (University of California, "Cycles of polynomial mappings", 1996, American, employed in the Institute for Defense Analyses, U.S.A.),

D. R. Kohel (University of California, "Endomorphism rings of elliptic curves over finite fields", 1996, employed in the University of Sydney, Australia),

Hui Zhu (University of California, "Supersingular abelian varieties over finite fields", 1997, Chinese, Professor in SUNY Buffalo, U.S.A.),

D. C. Terr (University of California, "The distribution of shapes of cubic orders", 1997, American, employed in industry),

L. S. Khadjavi (University of California, "An effective version of Belyi's theorem", 1999, American, professor in Loyola Marymount University, U.S.A.),

J. M. Borger (University of California, "On conductors over discrete valuation rings with general residue fields", 2000, American, professor in the Australian National University, Canberra, Australia),

D. S. Romano (University of California, "Galois groups of strongly Eisenstein polynomials", 2000, American),

W. A. Stein (University of California, "Explicit approaches to modular abelian varieties", 2000, American, professor in the University of Washington, U.S.A.),

J. J. Flynn (University of California, "Near-exceptionality over finite fields", 2001, Irish),

W. A. Whitney (University of California, "Functorial Cohen rings", 2002, American),

J. C. Elliott (University of California, "Witt-Burnside rings", 2003, American, professor in California State University, Channel Islands, U.S.A.),

R. P. Groenewegen (Universiteit Leiden, "Vector bundles and geometry of numbers", 2003, Dutch, employed in industry),

R. Carls (Rijksuniversiteit Groningen, "A generalized arithmetic geometric mean", 2004, German, postdoc in Sydney),

R. M. van Luijk (University of California, "Rational points on $K3$ surfaces", 2005, Dutch, postdoc in Colombia and in Vancouver),

J. M. Voight (University of California, "Quadratic forms and quaternion algebras: algorithms and arithmetic", 2005, American, postdoc in Minnesota, U.S.A.),
C. E. van de Woestijne (Universiteit Leiden, "Deterministic equation solving over finite fields", 2006, Dutch, postdoc in Graz, Austria).

Postdoctoral fellows
The candidate never supervised postdoctoral fellows. In mathematics, postdoctoral fellows are treated as colleagues and are not supervised. For this reason, there are no records from the period that the candidate was a professor in Berkeley. Since 1998, the following postdoctoral fellows have been working in the research group of the candidate in Leiden.
P. Moree (1999, Dutch),
M. Zieve (2000, American),
M. Girard (2001-2002, French),
W. B. Hart (2004-2005, Australian),
C. L. J. Ritzenthaler (2004, French).

Publications
Factoring polynomials with rational coefficients (with A. K. Lenstra and L. Lovász), Math. Ann. **261** (1982), 515–534.
Integer programming with a fixed number of variables, Math. Oper. Res. **8** (1983), 538–548.
Factoring integers with elliptic curves, Ann. of Math. **126** (1987), 649–673.
Algorithms in algebraic number theory, Bull. Amer. Math. Soc. **26** (1992), 211–244.
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, 2001.
Solving the Pell equation, Notices Amer. Math. Soc. **49** (2002), 182–192.
A hyperelliptic smoothness test II (with J. Pila and C. Pomerance), Proc. London Mathematical Soc. (3) **84** (2002), 2361–2401.
On a problem of Garcia, Stichtenoth, and Thomas, Finite fields and their applications **8**, 166–170.
The mathematical structure of Escher's Print Gallery (with B. de Smit), Notices Amer. Math. Soc. **50** (2003), 446–451.
Lattices, to appear in: J. P. Buhler, P. Stevenhagen (eds), *Surveys in algorithmic number theory*, Cambridge University Press, 2006.