

David R. Kohel

School of Mathematics and Statistics
University of Sydney, F07
NSW 2006 Australia

DOB: 27 February 1966
Residency: Australia
Citizenship: U.S.A.

kohel@maths.usyd.edu.au
<http://www.maths.usyd.edu.au/u/kohel>

Tel : 61-2-9351-3279
Fax : 61-2-9351-4534

Education

Academic Degrees

- Ph.D, Mathematics, U. C. Berkeley, December 1996.
Thesis: *Endomorphism rings of elliptic curves over finite fields.*
Advisor: Hendrik W. Lenstra, Jr.
- B.S., Mathematics, Texas A&M University (Summa Cum Laude), May 1989.
- B.S., Biochemistry, Texas A&M University (Summa Cum Laude), May 1989.

Academic Employment

University of Sydney

- Senior Lecturer, Number Theory Group, 2005–present.
- Lecturer in Cryptography, Computational Algebra Group, 2002–2005.
- Senior Research Associate, Computational Algebra Group, 2001–2002.

Mathematical Sciences Research Institute

- Postdoctoral Fellow, Fall 2000.

University of Sydney

- Senior Research Associate, Computational Algebra Group, 1999–2000.

National University of Singapore

- Postdoctoral Fellow, 1997–1999.

Professional Activities

Preprints

- Efficient scalar multiplication by isogeny decompositions, with C. Doche and T. Icart, 2005.
- Efficiently computable endomorphisms for hyperelliptic curves, with B. Smith, 2005.
- The p -adic CM method in genus 2, with P. Gaudry, T. Houtmann, C. Ritzenhaler, and A. Weng, <http://arxiv.org/abs/math.NT/0503148>, 2005.
- The Weierstrass subgroup of a curve has maximal rank, with M. Girard and C. Ritzenhaler, <http://arxiv.org/abs/math.NT/0504130>, 2005.
- Constructive and destructive facets of torus-based cryptography, 2004.

Publications

- The AGM- $X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting, in *Advances in Cryptology – Asiacrypt 2003*, 124–136, *Lecture Notes in Comput. Sci.*, **2894**, Springer, Berlin, 2003.
- Fundamental domains for Shimura curves, with H. Verrill, *J. Théorie de Nombres Bordeaux*, **15** (2003), no. 1, 205–222.
- *Algorithmic number theory (Sydney, 2002)*, C. Fieker and D. Kohel, eds., *Lecture Notes in Comput. Sci.*, **2369**, Springer, Berlin, 2002.
- Hecke module structure of quaternions, *Class Field Theory—Its Centenary and Prospect (Tokyo, 1998)*, 177–195, *Advanced Studies in Pure Math.*, **30**, Tokyo, 2001.
- Rational groups of elliptic curves suitable for cryptography, *Cryptography and Computational Number Theory (Singapore, 1999)*, 69–80, *Progr. Comput. Sci. Appl. Logic*, **20**, Birkhäuser, 2001.
- Counting the number of points on affine diagonal curves, with C. Ding and S. Ling, *Cryptography and Computational Number Theory (Singapore, 1999)*, 15–24, *Progr. Comput. Sci. Appl. Logic*, **20**, Birkhäuser, 2001.
- On exponential sums and group generators for elliptic curves over finite fields, with I. Shparlinski, *Algorithmic number theory (Leiden, 2000)*, 395–404, *Lecture Notes in Comput. Sci.* **1838**, Springer, Berlin, 2000.
- Component groups of quotients of $J_0(N)$, with W. Stein, *Algorithmic number theory (Leiden, 2000)*, 405–412, *Lecture Notes in Comput. Sci.* **1838**, Springer, Berlin, 2000.
- Split group codes, with S. Ling and C. Ding. *IEEE Trans. on Inform. Theory* **46**, no. 2, (2000), 280–284.
- Elementary 2-group character codes, with S. Ling and C. Ding. *IEEE Trans. on Inform. Theory* **46**, no. 1, (2000), 485–496.
- Secret-sharing with a class of ternary codes, with S. Ling and C. Ding. *Theoret. Comput. Sci.* **246** (2000), no. 1-2, 285–298.
- Explicit sequence expansions, with S. Ling and C. Xing, *Sequences and their applications (Singapore 1998)*, 308–317, C. Ding, T. Helleseth, and H. Niederreiter, eds., *Discrete Math. and Theor. Comp. Sci.* Springer-Verlag, 1999.
- *Endomorphism rings of elliptic curves over finite fields*. Ph.D. Thesis, University of California, Berkeley, 1996.

Magma Computational Algebra Development

From 1999–2002 I contributed to computational algebra design, code, and documentation for the MAGMA computational algebra system. This included a computational model for schemes (with G. Brown); algorithms for curves of low genus, particular conics, elliptic and hyperelliptic curves; isogeny structures for elliptic curves, modular curves and parametrized isogenies; SEA and p -adic point counting algorithm AGM- $X_0(N)$; binary quadratic forms and class groups of nonmaximal quadratic orders; spinor genera and genera of integral lattices; quaternion algebras and associated Brandt modules; modules of supersingular points (with W. Stein); congruence subgroups of $SL_2(\mathbf{Z})$ and quaternion unit groups, their actions on upper half complex plane, and invariants of Shimura curves (with H. Verrill); Witt rings.

Grant, Journal, and Thesis Refereeing

- Australia Research Council (Intreader) since 2003.
- Royal Grant Council, Hong Kong, 2004.
- Ph.D. Thesis Committee, Mireille Fouquet, École Polytechnique (LIX), 2001.
- Referee for journals and conferences, including *IEEE Transactions on Information Theory*, *Mathematics of Computation*, *Finite Fields and Applications*, *Experimental Mathematics*, *Journal of Complexity*, *Handbook of Information Security*, and *Algorithmic Number Theory Symposium (ANTS) IV (Leiden) and VI (Vermont)* (ANTS V being organised by Cannon, Fieker and Kohel in Sydney).

Australia Research Council Grants

- *Abelian Varieties in Cryptography*, David Kohel and Christophe Doche (Department of Computing, Macquarie), Chief Investigators, submitted 2005 for consideration of funding for 2006-2010. The research is intended to investigate effective and efficient algorithms for elliptic curves, Jacobians, and abelian varieties for use in cryptography.
- *p-Adic Methods in Arithmetic Geometry*, David Kohel, Chief Investigator, 2004-2006. The programme of research to be undertaken in this project concerns the effective determination of the orders of certain groups, the Jacobian of an algebraic curve, which can be used for cryptography.
- *Effective Methods in Class Field Theory*, John Cannon and Michael Pohst (KANT, Berlin), Chief Investigators, 2001-2003. In this application, I designed a programme of research for extending effective class field theory algorithms to function fields, extending work of the KANT group in collaboration with the Computational Algebra Group in Sydney. The author and Claus Fieker were beneficiaries of the postdoc position created.

University of Sydney Teaching

Ph.D. Students

- Steve Ward, 2005–present.
- David Gruenewald, 2004–present.
- Ben Smith, 2002–2005 (expected completion).

International Exchange Students

- Thomas Icart, *Cryptologie : multiplication scalaire sur les courbes elliptiques*, Stage internship, École Polytechnique, 2005.
- Alex Unger (Leipzig), honours reading course on elliptic curves, 2005.

Honours Students

- David Gruenewald, *An introduction to modular forms*, Honours Thesis, 2003.
- Gordon Childs, *Counting points on hyperelliptic curves over finite fields*, Honours Thesis, 2001.
- Quy Tuan Nguyen, *Binary quadratic forms*, Honours Thesis, 2000.

Summer Scholars

- Peter McNamara (elliptic curves), 2004.
- Quy Tuan Nguyen (quadratic forms), 2000.

Curriculum Design and Teaching

- *Commutative Algebra*, Sem. 1, 2005, Honours course on commutative algebra following first four chapters of Atiyah–Macdonald.
- MATH 3024, *Elementary Cryptography and Protocols (Ordinary)*, Sem. 1, 2001–2004. This unit was newly introduced in 2001. It presents students with the foundational principles of cryptography and cryptanalysis. I developed lecture and tutorials materials, including a cryptography teaching package in the computational algebra system Magma for hands-on exercises.
- MATH 3925, *Public Key Cryptography (Advanced)*, Sem. 2, 2002–2004. This unit covers the mathematical foundations for construction and cryptanalysis of common public key cryptosystems. This was first taught in 2001 as an extension of a prior unit computational algebra. I redesigned the unit in 2002, incorporating recent results in cryptography and updating the curriculum to cover aspects of elliptic curve cryptography.
- MATH 1003, *Integral Calculus and Modelling (Ordinary)*, Sem. 2, 2003–2004. This is a first year calculus class consisting of 1100–1200 students distributed into four lecture streams of 300–400 students. Lectures are coordinated between the four lecturers and some 40 tutorials.
- *Elliptic Curves and Cryptography*, 2003 & 2004. Supplementary lectures for the Talented Student Programme.

Administration

- Organizer, *ECHIDNA II*, University of Sydney, 12–14 January 2005.
- Organizer, *Algorithmic Number Theory Symposium V*, with J. Cannon and C. Fieker, University of Sydney, 7–12 July 2002,
- Editor, *Algorithmic number theory (Sydney, 2002)*, Proceedings of Algorithmic Number Theory Symposium V, with C. Fieker, *Lecture Notes in Computer Science* **2369**, Springer, Berlin, 2002.
- Organizer, *Elliptic Curves and Higher Dimensional Analogues (ECHIDNA)*, University of Sydney, 15–19 July 2002.
- Organizer, *Number Theory Seminar*, School of Mathematics and Statistics, University of Sydney, 2003–present.
- Organizer, *Computational Algebra Seminar*, School of Mathematics and Statistics, University of Sydney, 2001–2002.
- Supervision of programmers and development design in number theory and arithmetic geometry, Computational Algebra Group, University of Sydney, 1999–2002.

Mathematical Talks and Conferences

- Explicit methods in number theory, Oberwolfach, 17–23 July 2005.
- *An ℓ -adic CM method for genus 2*, XXIV^{èmes} Journées Arithmétiques, Marseille, 4–8 July 2005.
- *Introduction to Magma and Applications*, African Institute for the Mathematical Sciences, South Africa, 2 February 2005.
- *Constructing CM invariants of genus 2 curves, Workshop on Arithmetic Geometry, Related Areas, and Applications*, University of Stellenbosch, 1 February 2005.

- *Igusa class invariants via p -adic lifting*, ECHIDNA II, 12–14 January 2005.
- *Igusa class invariants and the AGM*, Magma Workshop, Georg-August-Universität, Göttingen, 11–15 December 2004.
- *Constructive CM by p -adic lifting*, *Effective Methods in Arithmetic Geometry*, Institut Henri Poincaré, 6–10 December 2004.
- *Weierstrass points and the groups they generate*, Texas A&M University, 19 November 2004.
- *Constructing CM invariants of genus 2 curves*, Banff, 13–18 November 2004.
- *The AGM- $X_0(N)$ algorithm: Heegner point lifting with applications* Schloss Dagstuhl, *Algorithms and Number Theory*, 16–21 May 2004.
- *The AGM- $X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Asiacrypt 2003 (Taipei), 1 December 2003.
- *The AGM- $X_0(N)$ point counting algorithm.*, Hong Kong University of Science and Technology, 28 November 2003.
- *Elliptic curve point counting using $X_0(N)$* . Explicit methods in number theory, Oberwolfach, 20–26 July 2003.
- *Effective Brauer group computations over global fields*. XXIIIèmes Journées Arithmétiques, Graz, 6–12 July 2003.
- *Galois module structure and ranks for Weierstrass subgroups*, Workshop on Computational Arithmetic Geometry, University of Sydney, 18–20 June 2003.
- *p -Adic lifts of Heegner points on $X_0(N)$* , Leiden University, 13 January 2003.
- *p -Adic lifts of Heegner points on $X_0(N)$* , Séminaire de Théorie des Nombres, Algorithmique et Cryptographie, University of Toulouse II, 18 December 2002.
- *Canonical p -adic lifts on $X_0(N)$* Università di Roma 2, 13 December 2002.
- *p -Adic point counting algorithms for elliptic curves* Algebraic Geometry Seminar, University of Sydney, 22 November 2002.
- *CM points on $X_0(N)$ via p -adic lifts*, Elliptic Curves and Higher Dimensional Analogues (ECHIDNA, Workshop in Arithmetic Geometry and Applications), 15–19 July 2002.
- *Applications of class invariants on modular curves*. Computational Algebra Seminar, University of Sydney, 24 January 2002.
- *Fundamental domains for Shimura curves*. Computational Algebra Seminar, University of Sydney, 29 November 2001.
- *Computational aspects of Shimura curves*. Explicit methods in number theory, Oberwolfach, 23–27 July 2001.
- *Fundamental domains for Shimura curves*. XXIIèmes Journées Arithmétiques, Lille, 2–6 July 2001.
- *Shimura curve invariants*. Workshop on Arithmetic Geometry, Mathematical Sciences Research Institute, 11–15 December 2000.
- *On Satoh's algorithm*. Computer algebra seminar, Nijmegen University, 30 November 2000.
- *Endomorphism ring structure of elliptic curves*. Number theory seminar, University of Texas, 20 November 2000.
- *Endomorphism ring structure of elliptic curves*. Number theory seminar, Mathematical Sciences Research Institute, 8 November 2000.

- *The Magma Language and Vistas*. Mathematical Sciences Research Institute, Computer Education Seminar, 6 October 2000.
- *On exponential sums and group generators for elliptic curves over finite fields*. with Igor Shparlinski. Algorithmic Number Theory Symposium IV (Leiden), 2–7 July 2000.
- *Component groups of quotients of $J_0(N)$* . with William Stein (presenting). Algorithmic Number Theory Symposium IV (Leiden), 2–7 July 2000.
- *Component groups of Shimura curves*. Workshop on Number Theory, Lorentz Center, Leiden, 26–30 June 2000.
- *Rational groups of elliptic curves suitable for cryptography*. Number Theory and Cryptography Conference. National University of Singapore, 22–26 November 1999.
- *Quaternion algebras and invariants of Shimura curves*. Algebra seminar, University of Sydney, 1 October 1999.
- Elliptic Curves, Modular Forms, and Galois Representations Workshop, Università di Roma 3, 19–23 July 1999.
- XXIèmes Journées Arithmétiques Università Lateranense, Vatican City, 12–16 July 1999.
- *An overview of algebraic geometric coding theory*. Colloquium talk, University of Philippines, 11 March 1999.
- *On representation numbers of certain ternary quadratic forms*. 2nd KIAS Number Theory Conference. Korean Institute for Advanced Studies, 16–18 December 1998.
- *Explicit sequence expansions*. with S. Ling (presenting) and C. Xing. International Conference on Sequences and their Applications. National University of Singapore. 14–17 December 1998.
- Algorithmic Number Theory Symposium (ANTS III). Reed College, Portland. 21–25 June 1998.
- *Hecke module structure of quaternions*. Class Field Theory Conference – its Centenary and Prospect. Waseda University, Tokyo. 3–12 June 1998.
- Number Theory and Topology. In honor of Barry Mazur’s 60th birthday. Harvard University, Boston. 27–30 May 1998.
- *Computing the zeta function of diagonal varieties over finite fields*. Algebra seminar, University of Sydney, 22 May 1998.
- *Computing modular curves via quaternions*. Fourth CANT Conference: Number Theory and Cryptography. University of Sydney, 3–5 Dec. 1997.
- *Coding theory: algebraic geometry of linear algebra*. National University of Singapore, 16 April 1997.
- *Sumas de tres cuadrados y otras formas cuadráticas*. Instituto de Matemáticas, UNAM, Morelia, 20 February 1997.
- *On sums of squares*. Number theory seminar, University of California at Berkeley, 12 February 1997.
- Elliptic curves and modular forms, National Academy of Sciences Washington, D.C., 15–17 March 1996.
- *Computation of the endomorphism ring of elliptic curves over finite fields*. University of Santa Clara, 3 October 1995.
- Computational perspectives on number theory. In honor of A. O. L. Atkin. University of Illinois at Chicago, 14–16 September 1995.

- XIXièmes Journées Arithmétiques. Barcelona, Spain, 16–20 July 1995.
- Arithmetic and geometry of abelian varieties. In honor of Frans Oort. University of Utrecht, The Netherlands, 5–9 June 1995.
- *On the category of supersingular elliptic curves: computational aspects*. Computational number theory. Oberwolfach, 28 May–3 June 1995.
- *On the category of supersingular elliptic curves*. Algebra seminar, University of Leiden, The Netherlands, 19 May 1995.
- Graduate student number theory seminar. Joint organizer with Steven Hillion, Spring–Fall 1995. Talks:
 - *The arithmetic of quaternion algebras*.
 - *Calculating the endomorphism ring of an ordinary elliptic curve*.
- Joint mathematics meetings of the AMS & MAA, San Francisco, California, 4–7 January 1995.
- “Dessins d’Enfants” Workshop: Moduli spaces and aspects of Galois theory. University of California at Berkeley and MSRI, 23–25 April 1994.
- Arithmetic geometry with an emphasis in Iwasawa theory. Arizona State University, 15–18 March 1993.

