

Curriculum Vitae

William Bruce Hart

Birthdate 11th Dec. 1975

Address Mathematics Institute, Warwick University, Coventry, CV4 7AL UK.

Phone +44 (0)24 7615 0041

Email W.B.Hart@warwick.ac.uk

Research Interests

I currently have three main areas of research interest:

- **Algorithmic Number Theory and Arithmetic Geometry:** I maintain the FLINT number theory library, BSDNT, a library for multiple precision arithmetic and MPIR, a fork of the GNU MP project. I am also researching factoring algorithms, including the number field sieve and parallel computation.
- **Modular Forms and Stark Conjectures:** I am researching Hilbert, classical modular forms, Stark conjectures, special values of L -series and explicit class field theory.
- **Iwasawa Theory:** I am interested in Iwasawa theory (GL_2 and CM field main conjectures) and related mathematics, algebraic K -theory, complex and p -adic L -series.

Academic

Oct 2008–present University of Warwick - EPSRC Career Acceleration Fellow

Oct 2006–Oct 2008 University of Warwick - Research Fellow

Aug 2005–Aug 2006 University of Illinois at Urbana-Champaign - Visiting Assistant Professor

Mar 2004–Jul 2005 Leiden University - Postdoc at invitation of Peter Stevenhagen

Jul 2001–Feb 2004 Macquarie University - *Evaluation of the Dedekind Eta Function* (PhD.)

2000 University of Tasmania - First Class Honours 86/100 (BSc. Hons.)

1995-98 University of Tasmania - Bachelor of Science (BSc.)

Selected Awards

2003 B.H. Neumann Award (best student seminar Aust. Math. Soc) See

<http://www.austms.org.au/AMSInfo/BHN/pastwinners.html>

1993 Silver Medal Int. Math. Olympiad, Istanbul (44th place overall) See

<http://www.srcf.ucam.org/jsm28/imo-scores/1993/scores-code.html>

Scholarships/Grants

2008-2013 EPSRC Career Acceleration Fellowship (approx. £740,000) for research into algorithms in Number Theory.

2009 Obtained 5000 USD from Microsoft Research, with William Stein for Jason Moxham (a Southampton based independent researcher) to work on an MS Windows port of the Pari/GP algebraic number theory project.

2012 Warwick Undergraduate Research Scholarship Scheme - Obtained £1000 funding for an undergraduate to work on algorithms in Number Theory

2010 Obtained £1000 from Imperial College for an undergraduate to work on algorithms in Number Theory over the summer

2010 Warwick Undergraduate Research Scholarship Scheme - Obtained £1000 funding for an undergraduate to work on algorithms in Number Theory

2008 Warwick Undergraduate Research Scholarship Scheme - Obtained £2000 for two undergraduates to work on algorithms in Number Theory

2008 Nuffield Foundation Bursary - Obtained £1440 for an undergraduate to do a summer project in algorithmic Number Theory

2007 Warwick Undergraduate Research Scholarship Scheme - Obtained £2000 for two undergraduates to work on algorithms in Number Theory

2007 Nuffield Foundation Bursary - Obtained £1440 for an undergraduate to do a summer project in algorithmic Number Theory

2001-2004 Macquarie University Research Area and Centre of Excellence Award

2002 Postgraduate Research Fund (PGRF) Grant - Funded an overseas collaboration and partially funded a conference trip.

1995-98 University of Tasmania Scholarship

Teaching Related Experience

2010 Taught third year Algebraic Number Theory, Warwick University.

2009-present Enrolled in course *Professional Certificate in Academic and Professional Practice*.

2009 Mini graduate course on Toom algorithms, the quadratic sieve and the number field sieve, University of Washington.

2008 Taught third year Algebraic Number Theory, Warwick University

2007 Taught third year Algebraic Number Theory, Warwick University

2005-2006 Visiting Assistant Professor (full teaching responsibilities, including a graduate course)

2003 (2nd Semester) Lecturer Multivariable Calculus, Macquarie Uni.

2001-2003 Classroom Mathematics Tutor, Macquarie Uni.

2003 One-on-one Mathematics Tutor, Numeracy Centre, Macquarie Uni.

Selected Talks

2010 Plenary talk: *The generalised Fast Fourier Transform*, The Lorentz Institute, Leiden, The Netherlands

2010 Invited talk: *Massive computations with the FFT* – Computer Methods for L-functions and Automorphic Forms, Centre de Recherché Mathématiques, Montreal, Canada

2010 *Congruent number theta coefficients to 10^{12}* – Algorithmic Number Theory Symposium, Nancy, France

2009 Invited Talk: *FLINT : Fast Library for Number Theory* – Sage Days 15, University of Washington

2009 Invited Talk: *MPIR : Multiple Precision Integers and Rationals* – Sage Days 15, University of Washington

2007 Invited Talk: *Parallel computation in number theory* – Interactive Parallel Computation in Support of Research in Algebra, Geometry and Number Theory, MSRI, Berkeley

2003 Award: I won the B.H. Neumann award for the best postgraduate talk at the annual Australian Mathematical Society general meeting embedded at ICIAM in Sydney

2011 *The van Hoeij–Novocin approach to univariate polynomial factorisation* – Number Theory Seminar, University of Exeter

2009 *FLINT: Fast Library for Number Theory* – Ecole Normale Supérieure de Lyon to the Laboratoire de l'Informatique du Parallélisme, France

2009 *FLINT: Fast Library for Number Theory* – Algorithms and Number Theory, Dagstuhl, Germany

2009 *Fast polynomial arithmetic* – Ecole Polytechnique, Paris, France

2009 *MPIR: Multiple Precision Integers and Rationals* – Magma Group, Sydney, Australia
2008 *Curves of genus one* – Number Theory Seminar, Oxford
2008 *Curves of genus one* – Jobs Talk, University of Exeter
2008 *Curves of genus one* – Tenure Track Jobs Talk, University of Washington
2007 *On short division; FLINT: a status report* – Computational Arithmetic Geometry, Clay Mathematics Institute
2007 *A new C library for number theory* – Number Theory Fest, University of Illinois at Urbana-Champaign
2007 *FLINT: A new C library for number theory* – Bristol University, United Kingdom
2006 *A New Identity for the Dedekind Eta Function* – University of Illinois at Urbana-Champaign
2006 *Elliptic Units* – University of Illinois at Urbana-Champaign
2005 *Extending Weber's Explicit Class Field Theory* – Macquarie University, Sydney, Australia
2005 *Computing Modular Equations* – Nottingham University, UK
2005 *Schläfli-type Modular Equations for Generalized Weber Functions* – Singapore National University
2004 *What is the non-commutative Iwasawa main conjecture?* – Intercity Number Theory Seminar, Leiden, The Netherlands
2004 *Generalized η -function modular equations* – Algorithms and Number Theory, Dagstuhl, Germany
2004 *Schläfli Modular Equations for generalized Weber functions* – Exeter University, UK
2004 *Evaluation of eta quotients* – Intercity Number Theory Seminar, Leiden, The Netherlands
2003 *Modular Equations for Weber-type Functions of Higher Signature* – Computational Arithmetic Geometry, Sydney University, Australia

Selected Conferences

London, UK 2011, EPSRC Cybersecurity Showcase
 Exeter, UK 2011, LMS Regional Meeting and workshop on Iwasawa Theory
 Kassel, Germany 2011, Computer Algebra in Scientific Computing
 Durham, UK 2011, Automorphic Forms and Galois Representations
 Cambridge, UK 2011, Conference on the Birch and Swinnerton-Dyer Conjecture
 Nancy, France 2010, Algorithmic Number Theory, 9th International Symposium
 CRM, Montreal 2010, Computer methods for L-functions and automorphic forms
 Lorentz Institute, Leiden 2010, Number Theory and Computer Algebra
 Dagstuhl, Germany 2009, Algorithms and Number Theory
 University of Washington 2009, Sage Days 15 (I was an organiser)
 Key West Florida 2009, Workshop on L-functions and Modular Forms III
 LORIA Nancy, France 2008, Sage Days 10
 University of Washington 2008, Graduate Modular Forms and L-functions workshop
 University of Washington 2008, L-functions and Modular Forms II
 University of Washington 2008, Sage Developer Days 1
 University of Bristol 2007, Cryptology, Number Theory and Arithmetic Geometry
 MSRI Berkeley 2007, Interactive Parallel Computation in Support of Research in Algebra, Geometry and Number Theory
 Clay Mathematics Institute Boston 2007, Computational Arithmetic Geometry
 University of Illinois at Urbana-Champaign 2007, Number Theory Fest
 Lorentz Centre Netherlands 2007, Solvability of Diophantine Equations
 Besançon France 2004, Iwasawa 2004

Dagstuhl Germany 2004, Algorithms and Number Theory
Sydney Convention Centre 2003, ICIAM (Aust MS embedded meeting)
Sydney University 2003, Computational Arithmetic Geometry
Sydney University 2002, Echidna and Algorithmic Number Theory Seminar (ANTS) V
Oberwolfach Germany 2002, Explicit Algebraic Number Theory
Johns Hopkins, Baltimore 2002, Conference on the Stark Conjectures

PhD Students and Postdocs

Marco Streng (postdoc) Oct 2010 - Oct 2012

Thomas Ward (postdoc) Oct 2012 - present

Academic Visits and Visitors

Ecole Normale Superior, Lyon, France, 23 - 27 Nov 2010 - invited by Andy Novocin

University of Washington 1 Apr - 21 May 2009, Visiting Scholar - invited by William Stein

Ecole Polytechnique, France, 23 - 24 Mar 2009 - invited by Grégoire Lecerf

Hosted Andy Novocin from University of Montpellier, 12 - 26 Dec 2009

Press coverage

The American Institute of Mathematics wrote a press release entitled “A trillion triangles”. It was picked up by almost every major science reporting outlet. Warwick University simultaneously produced a press release which was picked up by numerous UK and international media outlets. See:

<http://www.aimath.org/news/congruentnumbers/>

Professional Memberships

2001-Present Australian Mathematical Society

2010-Present Member of EPSRC Peer Review College

Thesis

[1] *Evaluation of the Dedekind Eta Function*, Ph.D. Thesis, 2004. Macquarie University, Sydney, 144 pp.

Refereed Papers

[2] *Modular equations and eta evaluations*, Aust. Math. Soc. Gazette, Vol. 31 No. 1, Mar 2004, pp. 43–47.

[3] *Schläfli modular equations for generalized Weber functions*, Ramanujan Journal, (15), 2008, pp. 435–468.

[4] *A new class of modular equation for Weber functions*, International Journal of Number Theory 2007, vol 3, (1) pp. 141–157.

[5] *Evaluation of the Dedekind Eta Function*, (with Robin Chapman), Canad. Math. Bull. Vol. 49 (1), 2006, pp. 21–35.

[6] *An identity for the Dedekind eta-function involving two independent complex variables*, (with Bruce Berndt), Bull. London Math. Soc. 2007, vol 39 (2), pp. 345–347.

[7] *Algorithm 898: Efficient Multiplication of Dense Matrices over $GF(2)$* , (with Martin Albrecht and Gregory Bard), Transactions on Mathematical Software, vol 37, (1), Jan 2010. pp 9:1–9:14.

- [8] *A new class of theta function identities in two variables*, (with Robin Chapman and Pee Choon Toh), Journal of Combinatorics and Number Theory, vol 2, issue 3, 2010, pp. 201–208.
- [9] *Congruent number theta coefficients to 10^{12}* , (with Gonzalo Tornaria and Mark Watkins), Guillaume Hanrot, François-Morain, Emmanuel Thomé (Eds.): Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings. Lecture Notes in Computer Science 6197 Springer 2010. pp. 186-200.
- [10] *Fast Library for Number Theory: an introduction*, Mathematical Software - ICMS 2010 Third International Congress on Mathematical Software, Kobe, Japan, September 13-17, 2010, Proceedings Series: Lecture Notes in Computer Science, Vol. 6327, pp 88–91.
- [11] *Practical polynomial factoring in polynomial time*, (with Andy Novocin and Mark van Hoeij), Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, San Jose, CA, June 8–11, ACM New York, 2011, pp 163–170.
- [12] *Practical divide-and-conquer algorithms for polynomial arithmetic*, (with Andy Novocin), Proceedings 13th International Workshop, CASC 2011, Kassel, Germany, September 2011, Lecture Notes in Computer Science, Vol. 6885, pp 200–214.
- [13] *A one line factoring algorithm*, Journal of the Australian Mathematical Society, vol. 92, (1), 2012, pp 61–69.

Software Projects

- [14] *FLINT 1.6 : Fast Library for Number Theory*, (2007-2010), I am the lead developer. FLINT 1 is around 120,000 lines of code (approx. half written by me), has had substantial contribution from numerous researchers across the world and is used extensively in the Sage Computer Algebra System. Documentation is 184 pp.
- [15] *FLINT 2.3 : Fast Library for Number Theory*, (2011-present), I am the lead developer. FLINT 2 is around 150,000 lines of code (approx. one third written by me), has had substantial contribution from numerous researchers across the world and is used extensively in the Sage Computer Algebra System. Documentation is 284 pp.
- [16] *MPIR : Multiple Precision Integers and Rationals*, (2008-present), I am the lead developer. MPIR is used extensively in the Sage Computer Algebra System. It is a fork of the GNU MP project and I have contributed around 6,000 lines of code to the fork.

Preprints / In Preparation

- [17] *On the complexity of polynomial factorisation*, (with Andy Novocin and Mark van Hoeij), 13 pp.
- [18] *A generalized theta identity in two \mathcal{H}_g variables*, (with Marco Streng), 5 pp.
- [19] *Class invariants from a new kind of Weber-like modular equation*, 21 pp.
- [20] *An L^2 Hermite Normal Form Algorithm*
- [21] *An FFT-based splitting technique for polynomial multiplication*
- [22] *Cesium: a new programming language for mathematics*

Software in preparation

- [23] *BSDNT*, (2010-present), I am the lead developer. BSDNT is a new library for fast arithmetic and number theory. I have contributed around 3,000 lines of code.
- [24] *Cesium*, (2011-present), I am the sole developer. Cesium is a new programming language designed for mathematicians.
- [25] *Comb*, (2012-present), I am the sole developer. Comb is a parser combinator library written in C which allows run time manipulation of the grammar at the statement and expression level and allows error reporting.

Other Papers: Unpublished Expositions

- [26] *Notes on the GL_2 Main Conjecture a la Coates, Fukaya, Kato, Sujatha and Venjakob*, (2004), 15 pp.
- [27] *Complex multiplication and explicit class field theory*, (2012), 9 pp.