

References

- [1] Saurabh Agarwal and Gudmund Skovberg Frandsen. Binary gcd like algorithms for some complex quadratic rings. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 57–71. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [2] V. Arvind and Piyush P. Kurur. On the complexity of computing units in a number field. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 72–86. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [3] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel. Implementing the arithmetic of $c_{3,4}$ curves. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 87–101. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [4] P. Berrizbeitia, S. Müller, and H.C. Williams. Pseudocubes and primality testing. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 102–116. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [5] Reinier Bröker and Peter Stevenhagen. Elliptic curves with a given number of points. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 117–131. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [6] N. Bruin and E.V. Flynn. Rational divisors in rational divisor classes. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA,*

- June 13-18, 2004), volume 3076 of *LNCS*, pages 132–139. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [7] Frank Calegari and William A. Stein. Conjectures about discriminants of hecke algebras of prime level. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 140–152. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [8] Sylvain Duquesne. Montgomery scalar multiplication for genus 2 curves. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 153–168. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [9] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery. Improved weil and tate pairings for elliptic and hyperelliptic curves. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 169–183. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [10] Noam D. Elkies and Nicholas F. Rogers. Elliptic curves $x^3 + y^3 = k$ of high rank. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 184–193. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [11] Noam D. Elkies and Mark Watkins. Elliptic curves of large rank and small conductor. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 42–56. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.

- [12] J. Franke, T. Kleinjung, F. Morain, and T. Wirth. Proving the primality of very large numbers with fastecpp. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 194–207. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [13] Pierrick Gaudry and Éric Schost. A low-memory parallel version of matsuo, chao, and tsujii's algorithm. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 208–222. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [14] R. Granger, A.J. Holt, D. Page, N.P. Smart, and F. Vercauteren. Function field sieve in characteristic three. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 223–234. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [15] R. Granger, D. Page, and M. Stam. A comparison of ceilidh and xtr. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 235–249. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [16] Jordi Guàrdia, Eugenia Torres, and Montserrat Vela. Stable models of elliptic curves, ring class fields, and complex multiplication. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 250–262. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [17] F. Hess. An algorithm for computing isomorphisms of algebraic function fields. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington,*

- VT, USA, June 13-18, 2004), volume 3076 of *LNCS*, pages 263–271. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [18] Nick Howgrave-Graham and Mike Szydło. A method to solve cyclotomic norm equations $f * \bar{f}$. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 272–279. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [19] Jr. Jacobson, M.J., H.C. Williams, and K. Wooding. Imaginary cyclic quartic fields with large minus class numbers. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 280–292. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [20] John W. Jones and David P. Roberts. Nonic 3-adic fields. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 293–308. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [21] Kiran S. Kedlaya. Computing zeta functions via p -adic cohomology. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 1–17. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [22] Tanja Lange. Montgomery addition for genus two curves. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 309–317. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [23] Stéphane R. Louboutin. Numerical evaluation at negative integers of the dedekind zeta functions of totally real cubic number fields. In

- Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 318–326. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [24] James McKee and Chris Smyth. Salem numbers of trace -2 and traces of totally positive algebraic integers. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 327–337. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [25] Phong Q. Nguyen and Damien Stehlé. Low-dimensional lattice basis reduction revisited. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 338–357. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [26] Corina E. Pătraşcu and Mihai Pătraşcu. Computing order statistics in the farey sequence. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 358–366. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [27] Sebastian Pauli and Florence Soriano-Gafiuk. The discrete logarithm in logarithmic l -class groups and its applications in k -theory. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 367–378. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [28] Christophe Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington,*

- VT, USA, June 13-18, 2004), volume 3076 of *LNCS*, pages 379–394. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [29] K. Rubin and A. Silverberg. Using primitive subgroups to do more with fewer bits. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 18–41. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [30] R. Scheidler. Algorithmic aspects of cubic function fields. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 395–410. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [31] Damien Stehlé and Paul Zimmermann. A binary recursive gcd algorithm. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 411–425. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [32] Brett A. Tangedal. Lagrange resolvents constructed from stark units. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 426–441. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.
- [33] Aaram Yun, Jaeheon Kim, and Dong Hoon Lee. Cryptanalysis of a divisor class group based public-key cryptosystem. In Duncan Buell, editor, *Proceedings of the 6th International Symposium on Algorithmic Number Theory, ANTS'2004 (Burlington, VT, USA, June 13-18, 2004)*, volume 3076 of *LNCS*, pages 442–450. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2004.