References

[1] Roland Auer and Jaap Top. Some genus 3 curves with many points. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 163–171. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[2] Manjul Bhargava. Gauss composition and generalizations. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 1–8. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[3] Wieb Bosma and Bart de Smit. On arithmetically equivalent number fields of small degree. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 67–79. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[4] Nils Bruin and Noam D. Elkies. Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with galois groups of order 168 and $8 \cdot 168$. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 172–188. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[5] John Coates. Elliptic curves — the crossroads of theory and computation. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 9–19. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[6] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. A survey of discriminant counting. In Claus Fieker and David R. Kohel, editors,

Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002), volume 2369 of *LNCS*, pages 80–94. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[7] Jean-Marc Couveignes and Thierry Henocq. Action of modular correspondences around cm points. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 234–243. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[8] Jan Denef and Frederik Vercauteren. An extension of kedlaya's algorithm to artin-schreier curves in characteristic 2. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 308–323. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[9] Peter Ebinger and Edlyn Teske. Factoring $n = pq^2$ with the elliptic curve method. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 475–490. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[10] Noam D. Elkies. Curves $dy^2 = x^3 - x$ of odd analytic rank. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 244–251. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[11] Andreas Enge and François Morain. Comparing invariants for class fields of imaginary quadratic fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 252–266. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[12] Graham Everest, Peter Rogers, and Thomas Ward. A higher-rank mersenne problem. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 95–107. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[13] Mireille Fouquet and François Morain. Isogeny volcanoes and the sea algorithm. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 276–291. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[14] Takashi Fukuda and Keiichi Komatsu. An application of siegel modular functions to kronecker's limit formula. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 108–119. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[15] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the tate pairing. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 324–337. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[16] Enrique González-Jiménez, Josep González, and Jordi Guàrdia. Computations on modular jacobian surfaces. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 189–197. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[17] Florian Hess. An algorithm for computing weierstrass points. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002*

(Sydney, Australia, July 7-12, 2002), volume 2369 of *LNCS*, pages 357–371. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[18] Joshua Holden. Fixed points and two-cycles of the discrete logarithm. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 405–415. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[19] Jeremy Horwitz and Ramarathnam Venkatesan. Random cayley digraphs and the discrete logarithm. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 416–430. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[20] Jr. Jacobson, Michael J. and Alfred J. van der Poorten. Computational aspects of nucomp. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 120–133. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[21] Antoine Joux. The weil and tate pairings as building blocks for public key cryptosystems. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 20–32. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[22] Antoine Joux and Reynald Lercier. The function field sieve is quite special. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 431–445. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[23] Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park, Jae Heon Kim, and Sang Geun Hahn. Fast elliptic curve point counting using gaussian normal basis. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 292–307. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[24] Andrew Kresch and Yuri Tschinkel. Integral points on punctured abelian surfaces. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 198–204. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[25] Paul Leyland, Arjen Lenstra, Bruce Dodson, Alec Muffett, and Sam Wagstaff. Mpqs with three large primes. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 446–460. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[26] Wen-Ching W. Li, Hiren Maharaj, Henning Stichtenoth, and Noam D. Elkies. New optimal tame towers of function fields over small finite fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 372–389. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[27] Stéphane R. Louboutin. Efficient computation of class numbers of real abelian number fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 134–147. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[28] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over fi-

nite fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 461–474. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[29] Carl Pomerance and Igor E. Shparlinski. Smooth orders and cryptographic applications. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 338–348. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[30] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of hilbert's tenth problem over rings of algebraic integers. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 33–42. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[31] J. Maurice Rojas. Additive complexity and roots of polynomials over number fields and p-adic fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 506–515. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[32] Takakazu Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 43–66. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[33] Tony Shaska. Genus 2 curves with (3, 3)-split jacobian and large automorphism group. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369

of *LNCS*, pages 205–218. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[34] Igor E. Shparlinski and Ron Steinfeld. Chinese remaindering for algebraic numbers in a hidden field. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 349–356. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[35] Allan Steel. A new scheme for computing with algebraically closed fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 491–505. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[36] William A. Stein and Mark Watkins. A database of elliptic curves — first report. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 267–275. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[37] Alfred J. van der Poorten and Xuan Chuong Tran. Periodic continued fractions in elliptic function fields. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 390–404. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[38] Helena A. Verrill. Transportable modular symbols and the intersection pairing. In Claus Fieker and David R. Kohel, editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 219–233. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[39] Ulrich Vollmer. An accelerated buchmann algorithm for regulator computation in real quadratic fields. In Claus Fieker and David R. Kohel,

editors, *Proceedings of the 5th International Symposium on Algorithmic Number Theory, ANTS'2002 (Sydney, Australia, July 7-12, 2002)*, volume 2369 of *LNCS*, pages 148–162. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.