References

[1] Miho Aoki and Takashi Fukuda. An algorithm for computing p-class groups of abelian number fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 56–71. Springer-Verlag, Berlin-Heidelberg, 2006.

[2] Werner Bley and Robert Boltje. Computation of locally free class groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 72–86. Springer-Verlag, Berlin-Heidelberg, 2006.

[3] Nigel Boston and Harris Nover. Computing pro-p galois groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 1–10. Springer-Verlag, Berlin-Heidelberg, 2006.

[4] Johannes Buchmann and Christoph Ludwig. Practical lattice basis sampling reduction. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 222–237. Springer-Verlag, Berlin-Heidelberg, 2006.

[5] John Cremona. The elliptic curve database for conductors to 130000. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 11–29. Springer-Verlag, Berlin-Heidelberg, 2006.

[6] John Cremona and Samir Siksek. Computing a lower bound for the canonical height on elliptic curves over Q. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 275–286. Springer-Verlag, Berlin-Heidelberg, 2006.

[7] Isabelle Déchène. Arithmetic of generalized jacobians. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 421–435. Springer-Verlag, Berlin-Heidelberg, 2006.

[8] Alexander W. Dent and Steven D. Galbraith. Hidden pairings and trapdoor ddh groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 436–451. Springer-Verlag, Berlin-Heidelberg, 2006.

[9] Jean-Marc Deshouillers, François Hennecart, and Bernard Landreau. On the density of sums of three cubes. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 141–155. Springer-Verlag, Berlin-Heidelberg, 2006.

[10] Claus Diem. An index calculus algorithm for plane curves of small degree. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 543–557. Springer-Verlag, Berlin-Heidelberg, 2006.

[11] Bas Edixhoven. On the computation of the coefficients of a modular form. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 30–39. Springer-Verlag, Berlin-Heidelberg, 2006.

[12] Noam D. Elkies. Points of low height on elliptic curves and surfaces — i: Elliptic surfaces over P^1 with small d. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 287–301. Springer-Verlag, Berlin-Heidelberg, 2006.

[13] Noam D. Elkies. Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 302–316. Springer-Verlag, Berlin-Heidelberg, 2006.

[14] Andreas-Stephan Elsenhans and Jörg Jahnel. The asymptotics of points of bounded height on diagonal cubic and quartic threefolds. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 317–332. Springer-Verlag, Berlin-Heidelberg, 2006.

[15] Tom Fisher. Testing equivalence of ternary cubics. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 333–345. Springer-Verlag, Berlin-Heidelberg, 2006.

[16] Étienne Fouvry and Jürgen Klüners. Cohen-lenstra heuristics of quadratic number fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 40–55. Springer-Verlag, Berlin-Heidelberg, 2006.

[17] David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 452–465. Springer-Verlag, Berlin-Heidelberg, 2006.

[18] Gerhard Frey and Tanja Lange. Fast bilinear maps from the tate-lichtenbaum pairing on hyperelliptic curves. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 466–479. Springer-Verlag, Berlin-Heidelberg, 2006.

[19] Martine Girard and David R. Kohel. Classification of genus 3 curves in special strata of the moduli space. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 346–360. Springer-Verlag, Berlin-Heidelberg, 2006.

[20] R. Granger, D. Page, and N.P. Smart. High security pairing-based cryptography revisited. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 480–494. Springer-Verlag, Berlin-Heidelberg, 2006.

[21] Matthew Greenberg. Heegner point computations via numerical p-adic integration. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 361–376. Springer-Verlag, Berlin-Heidelberg, 2006.

[22] Ming-Deh Huang and Wayne Raskind. Signature calculus and discrete logarithm problems. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 558–572. Springer-Verlag, Berlin-Heidelberg, 2006.

[23] Jr. Jacobson, Michael J., Shantha Ramachandran, and Hugh Williams. Numerical results on class groups of imaginary quadratic fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 87–101. Springer-Verlag, Berlin-Heidelberg, 2006.

[24] Masanari Kida. Cyclic polynomials arising from kummer theory of norm algebraic tori. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic*

Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006), volume 4076 of *LNCS*, pages 102–113. Springer-Verlag, Berlin-Heidelberg, 2006.

[25] David R. Kohel and Benjamin A. Smith. Efficiently computable endomorphisms for hyperelliptic curves. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 495–509. Springer-Verlag, Berlin-Heidelberg, 2006.

[26] Tadej Kotnik and Herman te Riele. The mertens conjecture revisited. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 156–167. Springer-Verlag, Berlin-Heidelberg, 2006.

[27] Gunter Malle. The totally real primitive number fields of discriminant at most 10^9. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 114–123. Springer-Verlag, Berlin-Heidelberg, 2006.

[28] Phil Martin and Mark Watkins. Symmetric powers of elliptic curve l-functions. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 377–392. Springer-Verlag, Berlin-Heidelberg, 2006.

[29] Stephen D. Miller and Ramarathnam Venkatesan. Spectral analysis of pollard rho collisions. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 573–581. Springer-Verlag, Berlin-Heidelberg, 2006.

[30] Ilya Mironov, Anton Mityagin, and Kobbi Nissim. Hard instances of the constrained discrete logarithm problem. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin,*

Germany, July 23-28, 2006), volume 4076 of *LNCS*, pages 582–598. Springer-Verlag, Berlin-Heidelberg, 2006.

[31] Phong Q. Nguyen and Damien Stehlé. Lll on the average. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 238–256. Springer-Verlag, Berlin-Heidelberg, 2006.

[32] Scott T. Parsell and Jonathan P. Sorenson. Fast bounds on the distribution of smooth numbers. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 168–181. Springer-Verlag, Berlin-Heidelberg, 2006.

[33] Parthasarathy Ramachandran. Use of extended euclidean algorithm in solving a system of linear diophantine equations with bounded variables. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 182–192. Springer-Verlag, Berlin-Heidelberg, 2006.

[34] Guénaël Renault and Kazuhiro Yokoyama. A modular method for computing the splitting field of a polynomial. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 124–140. Springer-Verlag, Berlin-Heidelberg, 2006.

[35] Andrew Shallue and Christiaan E. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 510–524. Springer-Verlag, Berlin-Heidelberg, 2006.

[36] Jonathan P. Sorenson. The pseudosquares prime sieve. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006*

(Berlin, Germany, July 23-28, 2006), volume 4076 of *LNCS*, pages 193–207. Springer-Verlag, Berlin-Heidelberg, 2006.

[37] Damien Stehlé. On the randomness of bits generated by sufficiently smooth functions. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 257–274. Springer-Verlag, Berlin-Heidelberg, 2006.

[38] Alfred J. van der Poorten. Determined sequences, continued fractions, and hyperelliptic curves. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 393–405. Springer-Verlag, Berlin-Heidelberg, 2006.

[39] John Voight. Computing cm points on shimura curves arising from cocompact arithmetic triangle groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 406–420. Springer-Verlag, Berlin-Heidelberg, 2006.

[40] Kjell Wooding and Hugh C. Williams. Doubly-focused enumeration of pseudosquares and pseudocubes. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 208–221. Springer-Verlag, Berlin-Heidelberg, 2006.

[41] Paul Zimmermann and Bruce Dodson. 20 years of ecm. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory, ANTS'2006 (Berlin, Germany, July 23-28, 2006)*, volume 4076 of *LNCS*, pages 525–542. Springer-Verlag, Berlin-Heidelberg, 2006.