MR2728489 (2012c:11120) 11G05 (11G07 14H52)
Cremona, John E. (4-WARW-MI);
Fisher, Tom A. [Fisher, Thomas Anthony] (4-CAMB-PSM); **Stoll, Michael** (D-BAYR-IM)
Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves. (English summary)
Algebra Number Theory **4** (2010), *no. 6,* 763–820.1944-7833

Let E be an elliptic curve defined over a number field K. An n-covering of E is a principal homogeneous space C for E together with a map $\pi\colon C \to E$ which can be factored as $\pi \simeq [n] \circ \psi$, where $\psi\colon C \to E$ is an isomorphism defined over an algebraic closure of K, and $[n]$ is the multiplication-by-n map on E. The n-Selmer group $\mathrm{Sel}^{(n)}(K, E)$ parametrizes the everywhere locally soluble n-coverings of E up to isomorphism. If C is an element of $\mathrm{Sel}^{(n)}(K, E)$, then C has a degree-n model in the $(n-1)$-dimensional projective space. For such a C and for $n = 2, 3, 4$, the authors show there is a model with integral coefficients and the same discriminant as a global minimal model, and they give algorithms for computing these minimal models over local fields. They also establish a strong minimisation theorem, i.e., if an n-covering of E defined over a local field and represented by a degree-n model is soluble over the maximal unramified extension, then it has a model with integral coefficients and the same discriminant as a minimal Weierstrass equation for E. In the later sections, the authors also discuss reduction results over the rationals for n-covers, i.e., they produce explicit equations where the size of the coefficients is small and again they give explicit algorithms for $n = 2, 3, 4$.

Reviewed by *Conjeeveram S. Rajan*

References

1. S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, ”Jacobians of genus one curves”, *J. Number Theory* **90:**2 (2001), 304–315. MR 2002g:14040 Zbl 1066.14035 MR1858080 (2002g:14040)
2. M. Artin, F. Rodriguez-Villegas, and J. Tate, ”On the Jacobians of plane cubics”, *Adv. Math.* **198:**1 (2005), 366–382. MR 2006h:14043 Zbl 1092.14054 MR2183258 (2006h:14043)
3. B. J. Birch and H. P. F. Swinnerton-Dyer, ”Notes on elliptic curves. I”, *J. Reine Angew. Math.* **212** (1963), 7–25. MR 26 #3669 Zbl 0118.27601 MR0146143 (26 #3669)
4. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Math. (3) **21,** Springer, Berlin, 1990. MR 91i:14034 MR1045822 (91i:14034)
5. W. Bosma, J. Cannon, and C. Playoust, ”The Magma algebra system, I: The user language”, *J. Symbolic Comput.* **24:**3–4 (1997), 235–265. MR 1484478 MR1484478
6. I. Connell, ”Elliptic curve handbook”, on-line notes, McGill University, 1996, available at http://www.math.mcgill.ca/connell/public/ECH1/.
7. J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR 99e:11068 Zbl 0872.14041 MR1628193 (99e:11068)
8. J. E. Cremona, ”Reduction of binary cubic and quartic forms”, *LMS J. Comput. Math.* **2** (1999),

64–94. MR 2000f:11040 MR1693411 (2000f:11040)

9. J. E. Cremona, Elliptic curve data, available at http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/I
10. J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, "Explicit n-descent on elliptic curves, I: Algebra", *J. Reine Angew. Math.* **615** (2008), 121–155. MR 2009g:11067 MR2384334 (2009g:11067)
11. J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, "Explicit n-descent on elliptic curves, II: Geometry", *J. Reine Angew. Math.* **632** (2009), 63–84. MR 2544143 MR2544143 (2011d:11128)
12. J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, "Explicit n-descent on elliptic curves, III: Algorithms", in preparation.
13. P. Deligne, "Courbes elliptiques: formulaire d'après J. Tate", pp. 53–73 in *Modular functions of one variable, IV* (Antwerp, 1972), edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476,** Springer, Berlin, 1975. MR 52 #8135 MR0387292 (52 #8135)
14. Z. Djabri and N. P. Smart, "A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve", pp. 502–513 in *Algorithmic number theory* (Portland, OR, 1998), edited by J. Buhler, Lecture Notes in Comput. Sci. **1423,** Springer, Berlin, 1998. MR 2001f:11086 Zbl 0915.11034 MR1726097 (2001f:11086)
15. I. Dolgachev, *Lectures on invariant theory,* London Mathematical Society Lecture Note Series **296,** Cambridge University Press, Cambridge, 2003. MR 2004g:14051 Zbl 1023.13006 MR2004511 (2004g:14051)
16. A. Dujella, "High rank elliptic curves with prescribed torsion", online table, available at http://web.math.hr/∼duje/tors/tors.html.
17. T. Fisher, "The Hessian of a genus one curve", preprint, 2006.
18. T. Fisher, "Testing equivalence of ternary cubics", pp. 333–345 in *Algorithmic number theory,* edited by F. Hess et al., Lecture Notes in Comput. Sci. **4076,** Springer, Berlin, 2006. MR 2007j:11074 Zbl 1143.11325 MR2282934 (2007j:11074)
19. T. Fisher, "A new approach to minimising binary quartics and ternary cubics", *Math. Res. Lett.* **14:**4 (2007), 597–613. MR 2008k:11058 Zbl 1142.11038 MR2335986 (2008k:11058)
20. T. Fisher, "The invariants of a genus one curve", *Proc. Lond. Math. Soc.* (3) **97:**3 (2008), 753–782. MR 2009j:11087 Zbl 05365466 MR2448246 (2009j:11087)
21. T. Fisher, "Some improvements to 4-descent on an elliptic curve", pp. 125–138 in *Algorithmic number theory,* edited by A. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011,** Springer, Berlin, 2008. MR 2009m:11078 Zbl 05279282 MR2467841 (2009m:11078)
22. T. A. Fisher, "Finding rational points on elliptic curves using 6-descent and 12-descent", *J. Algebra* **320:**2 (2008), 853–884. MR 2009g:11068 Zbl 1149.14025 MR2422319 (2009g:11068)
23. T. A. Fisher, "Elements of order 3 in the Tate-Shafarevich group", online table, available at http://www.dpmms.cam.ac.uk/∼taf1000/g1data/order3.html.
24. J. Gebel, A. Pethő, and H. G. Zimmer, "On Mordell's equation", *Compositio Math.* **110:**3 (1998), 335–367. MR 98m:11049 Zbl 0899.11013 MR1602064 (98m:11049)
25. D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993. Translated by Reinhard C. Laubenbacher from handwritten course notes, taken by Sophus

Marxsen. MR 97j:01049 Zbl 0801.13001 MR1266168 (97j:01049)
26. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry*, vol. II, Cambridge University Press, Cambridge, 1952. MR 95d:14002b Zbl 0048.14502 MR1288306 (95d:14002b)
27. K. Hulek, *Projective geometry of elliptic curves*, Astérisque **137,** Société Mathématique de France, Paris, 1986. MR 88c:14046 Zbl 0602.14024 MR0845383 (88c:14046)
28. N. Jacobson, *Basic algebra, I,* 2nd ed., W. H. Freeman and Company, New York, 1985. MR 86d:00001 Zbl 0557.16001 MR0780184 (86d:00001)
29. G. Julia, ”Étude sur les formes binaires non quadratiques à indeterminées réelles ou complexes”, *Mem. Acad. Sci. l'Inst. France* **55** (1917), 1–293.
30. J. Kollár, ”Polynomials with integral coefficients, equivalent to a given polynomial”, *Electron. Res. Announc. Amer. Math. Soc.* **3** (1997), 17–27. MR 98g:11076 Zbl 0867.11047 MR1445631 (98g:11076)
31. A. Kraus, ”Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique”, *Acta Arith.* **54:**1 (1989), 75–80. MR 90j:11045 Zbl 0628.14024 MR1024419 (90j:11045)
32. M. Laska, ”An algorithm for finding a minimal Weierstrass equation for an elliptic curve”, *Math. Comp.* **38:**157 (1982), 257–260. MR 84e:14033 Zbl 0493.14016 MR0637305 (84e:14033)
33. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, ”Factoring polynomials with rational coefficients”, *Math. Ann.* **261:**4 (1982), 515–534. MR 84a:12002 Zbl 0488.12001 MR0682664 (84a:12002)
34. Q. Liu, ”Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète”, *Trans. Amer. Math. Soc.* **348:**11 (1996), 4577–4610. MR 97h:11062 Zbl 0926.11043 MR1363944 (97h:11062)
35. J. R. Merriman, S. Siksek, and N. P. Smart, ”Explicit 4-descents on an elliptic curve”, *Acta Arith.* **77:**4 (1996), 385–404. MR 97j:11027 Zbl 0873.11036 MR1414518 (97j:11027)
36. J. S. Milne, ”Lectures on étale cohomology”, v. 2.10, 2008, available at http://www.jmilne.org/math/Co
37. B. Poonen, ”An explicit algebraic family of genus-one curves violating the Hasse principle”, *J. Théor. Nombres Bordeaux* **13:**1 (2001), 263–274. MR 2002e:14036 Zbl 1046.11038 MR1838086 (2002e:14036)
38. M. Raynaud, *Anneaux locaux henséliens,* Lecture Notes in Math. **169,** Springer, Berlin, 1970. MR 43 #3252 Zbl 0203.05102 MR0277519 (43 #3252)
39. M. Sadek, *Models of genus one curves*, Ph.D. thesis, University of Cambridge, 2009.
40. E. F. Schaefer and M. Stoll, ”How to do a p-descent on an elliptic curve”, *Trans. Amer. Math. Soc.* **356:**3 (2004), 1209–1231. MR 2004g:11045 Zbl 1119.11029 MR2021618 (2004g:11045)
41. J.-P. Serre, *Local fields,* Graduate Texts in Mathematics **67,** Springer, New York, 1979. MR 82e:12016 Zbl 0423.12016 MR0554237 (82e:12016)
42. S. Siksek, *Descent on curves of genus one,* Ph.D. thesis, University of Exeter, 1995, available at http://www.warwick.ac.uk/staff/S.Siksek/papers/phdnew.pdf.
43. J. H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics **106,** Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026 MR0817210 (87g:11070)
44. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in

Mathematics **151,** Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015 MR1312368 (96b:11074)
45. A. Skorobogatov, *Torsors and rational points,* Cambridge Tracts in Mathematics **144,** Cambridge University Press, Cambridge, 2001. MR 2002d:14032 Zbl 0972.14015 MR1845760 (2002d:14032)
46. W. A. Stein and M. Watkins, ”A database of elliptic curves: first report”, pp. 267–275 in *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. **2369,** Springer, Berlin, 2002. MR 2005h:11113 Zbl 1058.11036 MR2041090 (2005h:11113)
47. M. Stoll, Posting to NMBRTHRY mailing list, 2002, available at http://tinyurl.com/2bgpxfd.
48. M. Stoll and J. E. Cremona, ”Minimal models for 2-coverings of elliptic curves”, *LMS J. Comput. Math.* **5** (2002), 220–243. MR 2003j:11062 Zbl 1067.11031 MR1951757 (2003j:11062)
49. M. Stoll and J. E. Cremona, ”On the reduction theory of binary forms”, *J. Reine Angew. Math.* **565** (2003), 79–99. MR 2005e:11091 Zbl 1153.11317 MR2024647 (2005e:11091)
50. J. Tate, ”Algorithm for determining the type of a singular fiber in an elliptic pencil”, pp. 33–52 in *Modular functions of one variable, IV* (Antwerp, 1972), edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476,** Springer, Berlin, 1975. MR 52 #13850 MR0393039 (52 #13850)
51. A. Weil, ”Remarques sur un mémoire d’Hermite”, *Arch. Math.* (*Basel*) **5** (1954), 197–202. MR 15,896d Zbl 0056.03402 MR0061857 (15,896d)
52. A. Weil, ”Euler and the Jacobians of elliptic curves”, pp. 353–359 in *Arithmetic and geometry, I*, edited by M. Artin and J. Tate, Progr. Math. **35,** Birkhäuser, Boston, MA, 1983. MR 85d:14060 Zbl 0554.01014 MR0717601 (85d:14060)
53. T. Womack, *Explicit descent on elliptic curves,* Ph.D. thesis, University of Nottingham, 2003, available at http://www.warwick.ac.uk/staff/J.E.Cremona/theses/.

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.