MR2069117 (2005f:11112) 11G05

Jeon, Daeyeol (KR-KIAS); **Kim, Chang Heon**; **Schweizer, Andreas** (KR-KIAS)

On the torsion of elliptic curves over cubic number fields.

Acta Arith. **113** (2004), *no. 3,* 291–301.

In this paper, the authors prove that as K varies over all cubic number fields and E varies over all elliptic curves over K, the group structures which appear for infinitely many j-invariants as the torsion subgroup of $E(K)$ are precisely $\mathbf{Z}/N\mathbf{Z}$ for $N = 1, \ldots, 16, 18, 20$ and $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z}$ for $N = 1, \ldots, 7$. It is not known which other finite abelian groups might appear inside the Mordell l-Weil group of some elliptic curve over a cubic number field, though by L. Merel's uniform boundedness theorem [Invent. Math. **124** (1996), no. 1-3, 437–449; MR1369424 (96i:11057)] there are only finitely many possibilities (and there are explicit upper bounds due to Parent). For elliptic curves over $\mathbf{Q}$ and over quadratic fields, every group which occurs as the torsion subgroup of some $E(K)$ occurs for infinitely many j-invariants. So one might suspect, by analogy, that the above list exhausts all (or at least nearly all) possible torsion structures over cubic fields.

A sketch of the proof of the main result is as follows. Using the Weil pairing, one sees that if E is an elliptic curve over a cubic number field K, then the torsion subgroup of $E(K)$ is either cyclic or of the form $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z}$. Moreover, to say that as K varies over all cubic number fields there are infinitely many elliptic curves E/K having a K-rational N-torsion point (resp. having a copy of $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z}$ inside $E(K)$) is equivalent to saying that the modular curve $X_1(N)$ (resp. $X_1(2N, 2)$) has infinitely many cubic points. Using a deep theorem of Faltings, together with results of G. Frey [Israel J. Math. **85** (1994), no. 1-3, 79–83; MR1264340 (94m:11072)] and O. Debarre and R. Fahlaoui [Compositio Math. **88** (1993), no. 3, 235–249; MR1241949 (94h:14028)], the determination of which curves have infinitely many cubic points is reduced to the question of which of the curves are trigonal. The trigonality question is then resolved by methods similar to those used by Y. Hasegawa and M. Shimura [Acta Arith. **88** (1999), no. 2, 129–140; MR1700245 (2000d:11080)].

Reviewed by *Matthew H. Baker*

References

1. D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices 1996, no. 20, 1005–1011. MR1422373 (98b:11063)
2. M. H. Baker, E. González-Jiménez, J. González and B. Poonen, *Finiteness results for modular curves of genus at least* 2, e-print arXiv: math.NT/0211394, preprint. cf. MR 2006i:11065
3. J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992. MR1201151 (93m:11053)
4. O. Debarre and R. Fahlaoui, *Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves*, Compositio Math. 88 (1993), 235–249. MR1241949 (94h:14028)
5. G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. 85 (1994), 79–83.

MR1264340 (94m:11072)
6. R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, 1977. MR0463157 (57 #3116)
7. Y. Hasegawa and M. Shimura, *Trigonal modular curves*, Acta Arith. 88 (1999), 129–140. MR1700245 (2000d:11080)
8. N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. 15 (1991), 413–423. MR1138196 (93b:14037)
9. D. Jeon and C. H. Kim, *Bielliptic modular curves* $X_1(N)$, Acta Arith. 112 (2004), 75–86. MR2040593 (2005a:11085)
10. S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields* (with an appendix by A. Granville), in: Columbia University Number Theory Seminar (New York, 1992), Astérisque 228 (1995), 81–100. MR1330929 (96c:11058)
11. D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), 193–237. MR0434947 (55 #7910)
12. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186. MR0488287 (80c:14015)
13. L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449. MR1369424 (96i:11057)
14. F. Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 96 (1984), 139–165. MR0771075 (86m:11039)
15. K. V. Nguyen and M.-H. Saito, *d-gonality of modular curves and bounding torsions*, e-print arXiv: math.AG/9603024, preprint. cf. MR 2004k:11097
16. P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116. MR1665681 (99k:11080)
17. P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) 50 (2000), 723–749. MR1779891 (2001i:11067)
18. P. Parent, *No* 17*-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux, to appear. cf. MR 2001i:11067
19. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986. MR0817210 (87g:11070)
20. W. A. Stein, http://modular.fas.harvard.edu
21. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993. MR1251961 (94k:14016)

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