

MR1665681 (99k:11080) 11G05

Parent, Pierre (F-RENNB-IM)

Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. (French. French summary) [Effective bounds for the torsion of elliptic curves over number fields]

J. Reine Angew. Math. **506** (1999), 85–116.

Let K be a number field of degree d over \mathbf{Q} and E an elliptic curve defined over K . The torsion subgroup $E(K)_t$ of the Mordell-Weil group of E is finite, and L. Merel [*Invent. Math.* **124** (1996), no. 1-3, 437–449; [MR1369424 \(96i:11057\)](#)] proved that there exists a constant $B(d)$ depending only on d such that $|E(K)_t| < B(d)$.

The main result of this paper is that if the order of $P \in E(K)_t$ is p^n for some prime $p \geq 5$, then $p^n \leq 65(3^d - 1)(2d)^6$. Similar explicit bounds are also obtained for $p = 2$ and 3 . Since the primes p that may appear as orders of elements in $E(K)_t$ must satisfy $p \leq (1 + 3^{d/2})^2$ (this is a result of Merel and J. Oesterlé), the author's result is enough to establish an explicit bound for $|E(K)_t| < B(d)$.

The proof follows the lines of Merel's proof [op. cit.], making use of the “quotient d'enroulement” J_0^e of the Jacobian $J_0(p^n)$, and of the criterion of Kamienny to reduce the bound to a question of linear independence among certain modular symbols constructed with the help of the Hecke algebra.

Reviewed by [Andrea Mori](#)

References

1. A.O.L. Atkin, J. Lehner, Hecke Operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160. [MR0268123 \(42 #3022\)](#)
2. D. Bump, S. Friedberg, J. Hoffstein, Nonvanishing theorems for L -functions of modular forms and their derivatives, *Invent. Math.* **102** (1990), 543–618. [MR1074487 \(92a:11058\)](#)
3. Robert F. Coleman, Bas Edixhoven, On the semi-simplicity of the U_p -operator on modular forms, *Math. Ann.*, à paraître. [MR1600034 \(99b:11043\)](#)
4. Fred Diamond, John Im, Modular forms and modular curves, *Canad. Math. Soc. Conf. Proc.*, à paraître. [MR1357209 \(97g:11044\)](#)
5. B. Edixhoven, Rational torsion points on elliptic curves over number fields, *Sém. Bourbaki* **782** (1993), *Astérisque* **227** (1995), 209–227. [MR1321648 \(96c:11056\)](#)
6. A. Grothendieck, *Éléments de géométrie algébrique IV (Étude locale des morphismes de schémas)*, *Publ. math. I.H.E.S.* **28** (1965). [MR0199181 \(33 #7330\)](#)
7. Grothendieck *et al.*, *Séminaire de géométrie algébrique du Bois-Marie 7-I (Groupes de monodromie en géométrie algébrique)*, *Springer Lect. Notes Math.* **288** (1972). [MR0354656 \(50 #7134\)](#)
8. R. Hartshorne, *Algebraic Geometry*, *Grad. Texts Math.* **52**, Springer-Verlag (1983). [MR0463157 \(57 #3116\)](#)

9. S. Kamienny, Torsion points on elliptic curves and q -coefficients of modular forms, *Invent. Math.* **109** (1992), 221–229. [MR1172689 \(93h:11054\)](#)
10. S. Kamienny, Torsion points on elliptic curves over fields of higher degree, *Intern. Math. Res. Notices* **6** (1992). [MR1167117 \(93e:11072\)](#)
11. S. Kamienny, B. Mazur, Rational torsion of prime order in elliptic curves over number fields, *Astérisque*, à paraître. [MR1330929 \(96c:11058\)](#)
12. N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, *Ann. Math. Stud.* **108**, Princeton University Press (1985). [MR0772569 \(86i:11024\)](#)
13. V.A. Kolyvgin, D. Yu. Logachev, Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties, *Leningrad Math. J.* **1**, nr. **5** (1990). [MR1036843 \(91c:11032\)](#)
14. Manin, A Uniform Bound for p -torsion of Elliptic Curves, *Izv. Akad. Nau. CCCP* **33** (1969). [MR0272786 \(42 #7667\)](#)
15. Y. Manin, Parabolic points and zeta function of modular curves, *Math. USSR Izv.* **6** (1972), 19–64. [MR0314846 \(47 #3396\)](#)
16. B. Mazur, Modular curves and the Eisenstein ideal, *Publ. math. I.H.E.S.* **47** (1977), 33–186. [MR0488287 \(80c:14015\)](#)
17. B. Mazur, Rational Isogenies of Prime Degree, *Invent. Math.* **44** (1978), 129–162. [MR0482230 \(80h:14022\)](#)
18. Loïc Merel, *Sur quelques aspects géométriques et arithmétiques de la théorie des symboles modulaires*, Thèse de doctorat de l'université de Paris VII (1993).
19. Loïc Merel, Universal Fourier expansions of modular forms, in: *On Artin's conjecture for odd 2-dimensional representations*, *Springer Lect. Notes Math.* **1585** (1994), 59–94. [MR1322319 \(96h:11032\)](#)
20. Loïc Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), 437–449. [MR1369424 \(96i:11057\)](#)
21. David Mumford, *Abelian Varieties*, Oxford University Press, 1970. [MR0282985 \(44 #219\)](#)
22. M. R. Murty, V.K. Murty, Mean values of derivatives of modular L -series, *Ann. Math.* **133** (1991), 447–475. [MR1109350 \(92e:11050\)](#)
23. Joseph Oesterlé, *Torsion des courbes elliptiques sur les corps de nombres*, à paraître.
24. J. Oesterlé, *Un lemme de théorie analytique des nombres*, à paraître.
25. P. Parent, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, *prépubl. IRMAR (université de Rennes)* **95-33** (1995).
26. Jean-Pierre Serre, *Groupes algébriques et corps de classes*, Hermann, 1959. [MR0103191 \(21 #1973\)](#)
27. Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971. [MR0314766 \(47 #3318\)](#)

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