RESEARCH ANNOUNCEMENTS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 23, Number 2, October 1990

TORSION POINTS ON ELLIPTIC CURVES

S. KAMIENNY

1. Statement of the problem

The study of elliptic curves has long occupied a central place in number theory. We recall that an elliptic curve is an abelian variety of dimension one, or equivalently, an irreducible nonsingular projective algebraic curve of genus one, equipped with a distinguished point O, which is the origin for the group law (see [10] or [11] for a general survey of the subject). Let E be an elliptic curve defined over a number field K. The Mordell–Weil theorem states that the group $E(K)$ of K-rational points of E is a finitely generated abelian group. One of the classical conjectures in the theory of elliptic curves is the Uniform Boundedness Conjecture that there is a positive integer B_K (depending on K) such that if E is any elliptic curve over K, then the order of the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is less than B_K. A stronger form of this conjecture asserts that B_K depends not on K, but only on $d = [K\colon \mathbf{Q}]$ (i.e., the same bound B works for every number field whose degree over $\mathbf{Q}$ is d).

2. Known results

In 1969 Manin [5] proved a local version of this conjecture. He showed that for each prime p, and each number field K, there is

Received by the editors April 5, 1990 and, in revised form, June 28, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 11G18, 11F11, 14K07, 14H25.

Partially supported by an NSA grant.

a positive integer $B_{K,p}$ such that if E is an elliptic curve over K possessing a K-rational point of order p^n then $n < B_{K,p}$.

In 1976 Mazur [6] proved the global Uniform Boundedness Conjecture for the field $\mathbf{Q}$ of rational numbers (with $B_{\mathbf{Q}} = 16$). More precisely, he proved a beautiful conjecture of Ogg [9] that for any elliptic curve E over $\mathbf{Q}$, the group $E(\mathbf{Q})_{\text{tors}}$ is one of the following:

$$\begin{array}{ll} \mathbf{Z}/m\mathbf{Z} & \text{with } m \leq 10 \text{ or } m = 12 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\nu\mathbf{Z} & \text{with } \nu \leq 4. \end{array}$$

Aside from these two results, there is one partial result for elliptic curves over totally real number fields. In [1] it is shown, for a certain large class S of elliptic curves over the totally real field F, that there is a positive integer B_F such that if $E \in S$ then the order of $E(F)_{\text{tors}}$ is less than B_F. The constant B_F involves the order of $K_2(\mathscr{O})$, where $\mathscr{O}$ is the ring of integers of F, and $K_2(\mathscr{O})$ is the second algebraic K-group (see [8] for the definition of K_2).

3. New results

Recently we have given a proof of the strong form of the Uniform Boundedness Conjecture for quadratic fields. More precisely, we have the following.

Theorem 1. *There is a positive integer B such that if K is any quadratic number field, and E is any elliptic curve over K, then the order of $E(K)_{\text{tors}}$ is less than B. Moreover, the only primes possibly dividing the order of $E(K)_{\text{tors}}$ are* 2, 3, 5, 7, 11, *and* 13.

All of the primes in the above list actually do occur as the order of a rational torsion point on some elliptic curve over some quadratic field. The proof that this is the complete list of possible prime divisors of the order of $E(K)_{\text{tors}}$ uses the results of [3] and [4].

More generally, let d be a positive integer, and N a prime which is relatively large with respect to d. In recent work we have found a criterion which insures that there are no elliptic curves, defined over any field K of degree d, possessing a K-rational point of order N. The criterion involves the first d q-coefficients of the q-expansions of certain weight-two cusp forms on $\Gamma_0(N)$ (or $\Gamma_1(N)$). Our proof of this criterion rests upon a study of the geometry of the image of the cuspidal section ∞, diagonally embedded in the symmetric powers of the modular curves.

The proof of Theorem 1 is obtained by verifying that our criterion is satisfied when $d = 2$, and N is sufficiently large. We are in the process of explicitly calculating the minimal bound B (of Theorem 1) by carrying out our procedure working with $\Gamma_0(N^k)$ instead of $\Gamma_0(N)$ (this gives us a way of making Manin's results [5] explicit).

Research on the degree $d > 2$ case is still in progress. We hope to obtain a proof of the general conjecture by these methods. Our techniques should also be applicable in other situations and, in particular, may yield information about isogenies of elliptic curves over fields of degree d.

References

1. S. Kamienny, *On torsion subgroups of elliptic curves over totally real fields*, Invent. Math. **83** (1986), 545–551.
2. ——, *Torsion points on elliptic curves and q-coefficients of modular forms* (in preparation).
3. ——, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), 157–162.
4. ——, *Torsion points on elliptic curves over all quadratic fields* II, Bull. Soc. Math. France **114** (1986), 119–122.
5. Y. Manin, *A uniform bound for p-torsion in elliptic curves*, Izv. Akad. Nauk. CCCP **33** (1969), 459–465.
6. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1978), 33–186.
7. ——, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
8. J. Milnor, *Introduction to algebraic K-theory*, Annals of Math., study 72, Princeton University Press, 1971.
9. A. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111.
10. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag Graduate Texts in Mathematics, 1986.

11 J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

Department of Mathematics, University of Arizona, Tucson, AZ 85721

E-mail: SQK@MATH.ARIZONA.EDU