MR1172689 (93h:11054) 11G05 (11F30 11G18 14H52)
Kamienny, S. (1-SCA)
Torsion points on elliptic curves and q-coefficients of modular forms.
Invent. Math. **109** (1992), *no. 2,* 221–229.

This excellent paper makes a major contribution to the following well-known uniform boundedness conjecture: For every positive integer n there is a bound $B_n > 0$ such that if K is any number field of degree n over $\mathbf{Q}$ and E is any elliptic curve defined over K then the number of K-rational torsion points on E is less than B_n. The main theorem of the paper establishes the validity of this conjecture when $n = 2$. Moreover, it is proved (for $n = 2$) that the order of the torsion subgroup $E(K)_{\rm tor}$ is not divisible by any prime $p > 13$. This is a significant extension of a theorem of B. C. Mazur [Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978); MR0488287 (80c:14015)] which gives a complete list of isomorphism classes of torsion subgroups of elliptic curves over $\mathbf{Q}$.

The present author's method extends ideas of Mazur. Let N be a prime with $N > 61$ and $N \neq 71$ and let $X^{(2)}_{/S}$ be the symmetric square of the modular curve $X = X_0(N)_{/S}$ viewed as a smooth scheme over $S = \operatorname{Spec}(\mathbf{Z}[1/N])$. Let $J = J_0(N)$ be the Jacobian variety of X and $h\colon X^{(2)} \to J$ be the morphism defined by $(x, y) \mapsto (x + y - 2\infty)$, where ∞ is the infinity cusp on X. Let $f\colon X^{(2)} \to \widetilde{J}$ be the composition of h with Mazur's Eisenstein quotient $J \to \widetilde{J}$ [B. C. Mazur, op. cit.]. The key new observation in the paper under review is that f is a formal immersion along (∞, ∞) away from characteristics 2, 3, and 5. The proof of this fact reduces to a property of modular forms: For each prime $p \neq 2, 3, 5$ there exists a pair of weight-two cusp forms, F, G, attached to $\widetilde{J}$ whose Fourier coefficients $a_n(F)$, $a_n(G)$, $n \geq 1$, are integral and such that the vectors $(a_1(F), a_2(F))$, $(a_1(G), a_2(G))$ are linearly independent modulo p. To prove that there is no K-rational point of order N on any elliptic curve $E_{/K}$, the author then shows how such a point would give rise to an S-section (x, x^σ) of $X^{(2)}_{/S}$ which is distinct from (∞, ∞) while intersecting (∞, ∞) above 7 and having the same image in $\widetilde{J}(S)$ under f. This would contradict the fact that f is an immersion along (∞, ∞) in characteristic 7. Completing the proof of the uniform boundedness conjecture for $n = 2$ now reduces to a case-by-case examination of each of the primes $N \leq 61$ and $N = 67$, much of which had already been done in earlier works of the author.

The paper begins with a useful survey of previous work on this topic and closes with remarks concerning generalizations of the techniques to number fields of higher degree.

Reviewed by *Glenn Stevens*