MR1369424 (96i:11057) 11G05 (11L05)

Merel, Loïc (F-PARIS6-DP)

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

Invent. Math. **124** (1996), *no. 1-3,* 437–449.

FEATURED REVIEW.

In this article, the author proves the celebrated strong uniform boundedness conjecture (UBC) of B. Mazur and S. Kamienny: If E is an elliptic curve over a number field K, the order of the torsion subgroup of $E(K)$ is bounded by a constant which depends only on the degree of K over $\mathbf{Q}$.

This settles a long-standing open question that originated in 1977 with the publication of Mazur's landmark paper [Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978); MR0488287 (80c:14015)]. In that work, Mazur studied the rational points of the modular curve $X_0(N)$ and the Mordell-Weil group of its Jacobian $J_0(N)$, when N is prime. He was able to deduce the UBC for $K = \mathbf{Q}$, with a precise and sharp uniform bound on $E(\mathbf{Q})_{\mathrm{tors}}$ which appears to have been first conjectured by Beppo Levi at the turn of this century, and was later rediscovered by Ogg.

Central to Mazur's strategy was the result that, when $N = 11$ or $N \geq 17$ is prime, the abelian variety $J_0(N)$ has a quotient $\tilde{J}$—the so-called Eisenstein quotient—such that (1) the Mordell-Weil group $\tilde{J}(\mathbf{Q})$ is finite, and (2) the natural map from the cuspidal group of $J_0(N)$ to $\tilde{J}$ is injective. Mazur's proof of the finiteness of $\tilde{J}(\mathbf{Q})$ exploited the fact that for the primes l dividing the numerator of $(N-1)/12$, the mod l representation associated to $\tilde{J}$ is reducible, and hence has abelian or solvable image. The finiteness of $\tilde{J}(\mathbf{Q})$ was then proved by means of an l-descent, where the estimates for the relevant Galois cohomology groups could be carried out with the tools of class field theory.

By a delicate argument involving the geometry of the modular curve $X_0(N)$ (and in particular its cusps), the properties (1) and (2) of $\tilde{J}$ were used to show that if E is any elliptic curve having a rational point of order N with $N = 11$ or $N \geq 17$, then the Galois module E_N splits as a product $E_N \simeq \mathbf{Z}/N\mathbf{Z} \times \mu_N$ of Galois modules. From this, Mazur concluded directly that no such curve could exist (for it would be equipped with rational cyclic N^k-isogenies, for all $k \geq 0$).

In a subsequent work [Invent. Math. **44** (1978), no. 2, 129–162; MR0482230 (80h:14022)], Mazur introduced an important simplification of his earlier arguments. He showed that the natural map $X_0(N) \to \tilde{J}$ is a formal immersion at the cusp $i\infty$, over all primes $l \neq 2$. This directly implies that an elliptic curve with a rational point (or even, a rational subgroup) of order N with $N = 11$ or $N \geq 17$ has potentially good reduction at all primes $l \neq 2$. The bound on the torsion subgroup of $E(\mathbf{Q})$ established in his earlier paper on the Eisenstein ideal follows directly, and with less effort, by using the fact that the prime-to-l part of the torsion subgroup of $E(\mathbf{Q})$ injects into the points of E modulo l. As a result of this strengthening of his earlier methods, Mazur could also show that an elliptic curve over $\mathbf{Q}$ cannot have a rational cyclic subgroup of order N when $N > 163$. The finiteness of the Eisenstein quotient $\tilde{J}$ still played an essential role in this work.

Mazur's work gave evidence for the folklore conjecture that the order of the torsion subgroup of $E(K)$, when E/K is an elliptic curve over a number field K, is bounded by a constant depending only on K and not on E. But rather little progress was made on this conjecture in the intervening decade.

A major breakthrough came in 1992 with the article of Kamienny [Invent. Math. **109** (1992), no. 2, 221–229; MR1172689 (93h:11054)]. This article established the UBC for all quadratic fields K; moreover, the bound on the torsion subgroup of $E(K)$ obtained by Kamienny was absolute, supporting the intuition that a good bound might involve only the degree of K over $\mathbf{Q}$, and not other invariants of K: indeed the subtleties in Kamienny's argument seemed to be more geometric than arithmetic.

Kamienny's first idea was to observe that a curve over a quadratic field K with a K-rational point of order N gives rise to a rational point on the symmetric square variety $X_0(N)^{(2)}$, and to try to understand these rational points directly. He showed that the UBC would follow if one could show that the map $X_0(N)^{(2)} \to \tilde{J}$ induced by the natural map $X_0(N)^{(2)} \to J_0(N)$ is a formal immersion at the pair $\{i\infty, i\infty\}$. He then managed to give an explicit criterion, in terms of the first two Fourier coefficients of modular forms, for this map to be a formal immersion. By checking this criterion, he could prove that there is no elliptic curve over a quadratic field with a rational point of order N, if $N > 13$ is prime.

In addition to representing the first serious progress on the UBC since Mazur's work, Kamienny's strategy suggested a method of attacking the UBC for general number fields of degree d: it was now enough to prove that the map $X_0(N)^{(d)} \to \tilde{J}$ is a formal immersion for N large enough, a condition which translates into a linear independence condition on the first d Hecke operators in the image of the Hecke algebra in $\mathrm{End}(\tilde{J})$. By establishing Kamienny's criterion with $d \leq 8$, Kamienny and Mazur proved the UBC in those degrees [Astérisque No. 228 (1995), 3, 81–100; MR1330929 (96c:11058)]. Replacing the formal immersion condition by a weaker one, which he called formal finiteness, D. Abramovich [Astérisque No. 228 (1995), 3, 5–17; MR1330925 (96c:11059)] pushed the method further, and deduced the UBC for $d \leq 14$.

Shortly afterwards, the paper of Merel under review established the UBC for all degrees, settling the question completely. The author's opening gambit is to replace the Eisenstein quotient $\tilde{J}$ by a larger quotient of $J_0(N)$, which he calls the winding quotient (quotient d'enroulement). Let $e = \{0, \infty\}$ be the image of the path joining the cusps 0 and $i\infty$ in the (rational) homology of the modular curve $X_0(N)$, and let $I_e \subset \mathbf{T}$ be the ideal in the Hecke algebra which annihilates e. Then J_e is defined to be $J_0(N)/I_e J_0(N)$. The main point is that J_e is the largest abelian variety quotient of $J_0(N)$ such that the Hasse-Weil L-function $L(J_e, s)$ does not vanish at $s = 1$. The finiteness of $J_e(\mathbf{Q})$ follows from the Birch and Swinnerton-Dyer conjecture, but was not known unconditionally at the time of Mazur's Eisenstein ideal paper. Since then, however, a great deal of progress on the Birch and Swinnerton-Dyer conjecture has been accomplished thanks to the work of Gross-Zagier and V. A. Kolyvagin and D. Yu. Logachëv [Algebra i Analiz **1** (1989), no. 5, 171–196; MR1036843 (91c:11032); V. A. Kolyvagin, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671; MR0954295 (89m:11056)]. In particular, it is known that the Mordell-Weil group of J_e is finite, so that one can replace $\tilde{J}$ by J_e in Kamienny's conjecture. The crucial role played until then by Mazur's Eisenstein descent is now played by the descent of Kolyvagin.

The author then establishes Kamienny's criterion on linear independence of the d first Hecke operators in the larger quotient $\mathbf{T}_e = \mathbf{T}/I_e$ of the Hecke algebra acting on J_e. He notes that it is enough to show that the modular symbols $T_1 e, \cdots, T_d e$ are linearly independent in $H_1(X_0(N), \mathbf{Q})$. This linear independence is proved by an intricate calculation with modular symbols which is in itself a brilliant tour de force. More precisely, the author exhibits (when the prime N is large enough) elements $x_k \in H_1(X_0(N), \mathbf{Q})$ such that $x_k \cdot T_k e \neq 0$ but $x_k \cdot T_i e = 0$ for all $1 \leq i < k$. (Here the product is the usual intersection product.) The construction of x_k is reduced to a nontrivial lemma of analytic number theory: if A and B are intervals in $\{1, \cdots, p\}$ of size p/a and p/b respectively, and p is sufficiently large relative to ab, then there is a $k \in A$ such that the least positive residue of $-1/k$ mod p belongs to B. This lemma, which plays a central role in the proof, is established using Fourier analysis on $\mathbf{Z}/p\mathbf{Z}$ and a bound on Kloosterman sums due to Weil (itself a consequence of the Riemann hypothesis for varieties over finite fields).

Written in an elegant and concise style, Merel's article is the last movement in a beautiful symphony of ideas. It also contains a wealth of insights whose importance may well transcend the application to the uniform boundedness conjecture.

Reviewed by *Henri Darmon*