“Galois Actions and Geometry”: Almost rational torsion points on abelian varieties

Kenneth A. Ribet
University of California, Berkeley
and MSRI

October 13, 1999

The Manin–Mumford Conjecture

Start with a curve X (nonsingular, irreducible,. . .) over $\mathbf{C}$. Let J be the Jacobian of X — a g-dimensional abelian variety, where g is the genus of X.

Fix $x_0 \in X$. The Albanese map $\iota \colon X \to J$ arising from x_0 is defined by

$$x \mapsto \text{class of } (x) - (x_0).$$

If $g \neq 0$, ι is an embedding.

Suppose now that g is at least 2. Let J_{tors} be the torsion subgroup of J and consider

$$X_{\mathrm{tors}} := \iota(X) \cap J_{\mathrm{tors}}.$$

The *Manin–Mumford Conjecture* states that X_{tors} is a finite set.

This conjecture was the subject of Serge Lang's "Division points on curves," *Ann. Mat. Pura Appl.* **70**, 229–234 (1965).

Lang reduced the conjecture to a second (arithmetic) conjecture about abelian varieties over number fields. Given A/K, we view the action of $G := \mathrm{Gal}(\overline{K}/K)$ on A_{tors} as a continuous homomorphism

$$\rho\colon G \to \mathrm{Aut}(A_{\mathrm{tors}}) \approx \mathbf{GL}(2g, \hat{\mathbf{Z}}),$$

where g is the dimension of A.

Lang's arithmetic conjecture states that the image of ρ contains an open subgroup of the group $\hat{\mathbf{Z}}^*$ of scalar matrices (homotheties) in $\mathbf{GL}(2g, \hat{\mathbf{Z}})$.

Lang's conjecture is still an open problem. However, J-P. Serre presented a partial result in his 1985–1986 course at the Collège de France: there is an integer $e \geq 1$ so that the image of ρ contains the subgroup $(\hat{\mathbf{Z}}^*)^e$ of eth powers in the homothety group $\hat{\mathbf{Z}}^*$.

Meanwhile, the Manin–Mumford conjecture was proved by M. Raynaud in 1982 ("Courbes sur une variété abélienne et points de torsion," Invent. Math. **71** (1983), 207–233). Another proof was given by R. Coleman a few years later ("Ramified torsion points on curves," Duke Math. J. **54** (1987), 615–640).

I will explain how Serre's result may be used to give a proof of the conjecture that is different in spirit from Raynaud's proof and Coleman's proof.

For this, we view the curve X and the point x_0 as being defined over a finitely generated subfield K of $\mathbf{C}$. To fix ideas, we suppose that K is a number field, so that we can apply Serre's result. (That result is true in the general case by specialization.) We have $\iota\colon X \hookrightarrow J$, and we wish to prove that there are only finitely many torsion points of J that lie on X.

We neglect the set of hyperelliptic branch points on X if there are any; these are finite in number. We use the following principle, which I learned from M. Baker and A. Tamagawa: Suppose that $x \in X$ is *not* a hyperelliptic branch point, and let x' and x'' be points on X. If we have $2x = x' + x''$ on J, then $x' = x = x''$. Indeed, if $2x = x'+x''$, then the divisor $2(x) - (x') - (x'')$ on X is principal; it must be identically 0 in view of the hypothesis.

Especially, suppose that x is a torsion point on X that is not a hyperelliptic branch point of X. Then x lies in $X(\overline{K})$ and we can consider the conjugates of x by elements of $\mathrm{Gal}(\overline{K}/K)$. We find: *For* $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$*, the equation* $2x = \sigma x + \tau x$ *implies* $\sigma x = x = \tau x$. Equivalently: the set

$$\{\, \sigma x - x \,|\, \sigma \in \mathrm{Gal}(\overline{K}/K) \,\}$$

contains no non-zero point of J along with the negative of that point.

This circumstance suggests that we introduce the following concept:

Let A be an abelian variety over K and let P be a point of A over $\overline{K}$. Say that P is *almost rational* if the equation $2P = \sigma P + \tau P$ implies that σP and τP are both equal to P.

This is a somewhat weird condition that takes getting used to!

Suppose that P is almost rational. Then:

- No difference $\sigma P - P$ can be of order 2.
- If $(\sigma - 1)^2 P = 0$, then σ fixes P.
- Let v be a prime of K at which A has semistable reduction. Assume that P is an almost-rational *torsion* point whose order is prime to v. Then P is unramified at v (in view of SGA7I Ex. IX and the second item)!

Theorem 1. *The set of almost-rational torsion points on A is finite.*

To apply this theorem to the M–M conjecture, take $A =$ the Jacobian of X. The torsion points on X are either hyperelliptic branch points or almost-rational torsion points. There are only finitely many of each type, QED.

The theorem, on the other hand, is an easy consequence of Serre's homothety theorem:

Choose e such that the image of $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(A_{\mathrm{tors}})$ contains all eth powers of scalars. For $m > C(e)$ (a constant depending on e), there are $r, s \in ((\mathbf{Z}/m\mathbf{Z})^*)^e$ with $s + t = 2$, $(s, t) \neq (1, 1)$.

If P is an almost-rational torsion point of order m, we will prove that $m \leq C(e)$. If not, pick s and t as "above" and choose $\sigma \rightsquigarrow s$, $\tau \rightsquigarrow t$. We must have $sP = P$. Since P has order m and $s-1$ is non-zero in $\mathbf{Z}/m\mathbf{Z}$, this is impossible.

In the *Annuaire* of the Collége de France, Serre reports that his theorem is “d’ailleurs suffisant pour les applications que Lang avait en vue”. In fact, Lang’s proof of “Lang conjecture $\implies$ M–M conjecture” shows by a different route that Serre’s theorem implies M–M.

Some time ago, Robert Coleman proposed that the set of torsion points on X should be worthy of explicit study if X and the base point x_0 are of special interest. There is a significant literature in this direction. For example, Coleman, Tamagawa and Tzermias proved that if X is a Fermat curve ($x^n + y^n = z^n$) of genus > 1 and if x_0 is one of the cusps of X ($=$ points where one coordinate vanishes), then the set of torsion points on X is the set of cusps of X.

The “guess”

It is natural to consider modular curves in place of Fermat curves.

Let N be a prime so that the modular curve $X = X_0(N)$ has genus $g > 1$. (Thus $N \geq 23$.) Let x_0 be the standard cusp “∞” of X. The two cusps x_0 and 0 of X map to torsion points of $J = J_0(N)$ under the Albanese embedding attached to $\infty = x_0$. Are there other torsion points on X?

According to Ogg, there are eight values of N for which $X_0(N)$ is hyperelliptic: 37, 23, 29, 31, 41, 47, 59 and 71. In the latter seven cases, the hyperelliptic branch points of X are torsion points (i.e., map to torsion points on J); if $N = 37$, the six hyperelliptic branch points have infinite order on J.

The *guess*, a.k.a. the Coleman-Kaskel-Ribet *conjecture*, states that 0 and ∞ are the only torsion points on X that are not hyperelliptic branch points.

This conjecture was proved by M. Baker and by A. Tamagawa (independently) last spring. I'll now describe the proof in the language of almost-rational torsion points.

Our proof is close to that of Tamagawa but rather different from Baker's original arguments. In "Torsion points on modular curves," Invent. Math. (to appear), Baker presents his first proof and then this variant:

Let P be a torsion point on X that is not a hyperelliptic branch point. Thus P is an almost-rational torsion point on J. To show: that P is a cusp.

To postpone a technicality, we suppose first that the order of P is prime to N. As we saw before, SGA7I implies that P is unramified at N: the discriminant of the field $\mathbf{Q}(P)$ (which is not necessarily a Galois extension of $\mathbf{Q}$ a priori) is prime to N. This is somewhat surprising: such extensions normally have the right to be ramified at primes of bad reduction.

Fact. *The point P is killed by the Eisenstein ideal.*

Background: In his 1977 “Eisenstein ideal” article (Publ. Math. IHES **47**), Barry Mazur made a close study of the torsion points on $J = J_0(N)$, where N is a prime number. The difference of cusps $(\infty) - (0)$ is a rational point on J of order $n = \mathrm{num}((N-1)/12)$; it generates the *cuspidal group* $C \subset J$.

The *Shimura subgroup* of J is the kernel Σ of the natural map $J = J_0(N) \longrightarrow J_1(N)$. While Σ is again cyclic of order n, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on Σ is cyclotomic (so $\Sigma \approx \mu_n$).

The *Hecke ring* attached to J is the subring $\mathbb{T}$ of $\mathrm{End}_{\mathbf{Q}}\, J$ generated by the Hecke operators T_m $(m \geq 1)$. This ring stabilizes C, and in fact we have $T_p = 1+p$ on C for each prime $p \neq N$.

The *Eisenstein ideal* is the kernel I of the resulting surjective map

$$\mathbb{T} \longrightarrow \mathrm{End}(C) = \mathbf{Z}/n\mathbf{Z}.$$

It is generated by the differences $T_p - (1+p)$ and contains $T_N - 1$ as well. We have $\mathbb{T}/I \approx \mathbf{Z}/n\mathbf{Z}$.

Let $J[I]$ be the group of torsion points of J that are killed by all elements of I. Then $J[I]$ contains C, and $J[I]$ contains Σ as well. Mazur showed that $J[I]$ is free of rank 2 over $\mathbb{T}/I = \mathbf{Z}/n\mathbf{Z}$.

If n is odd, $J[I]$ is the direct sum of its two subgroups C and Σ. When n is even, $J[I]$ is harder to describe because C and Σ intersect in the group $C[2] = \Sigma[2]$ of order 2. The precise structure of $J[I]$ as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module was determined by János Csirik last year.

The following result explains the “fact” that was presented before.

Theorem 2. *The group $J[I]$ consists precisely of those torsion points of J that are unramified at N.*

One direction is easy: it is not hard to see that the points in $J[I]$ are unramified at N.

The hard direction is an application of my "level-lowering" theorem for irreducible mod p representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from $J_0(N)$. Level-lowering implies that such representations are ramified at N. It follows that unramified torsion points are killed by a *power* of I. Borrowing techniques from Mazur, one then shows that they are killed by I.

For most primes N, it is now easy to conclude by showing that points on X that lie in $J[I]$ can only be cusps.

Indeed, let X^+ be the quotient of X by its Atkin–Lehner involution w, and consider the diagram

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d] & J \arrow[d] \\
X^+ \arrow[r] & J^+
\end{tikzcd}$$

in which J^+ is the Jacobian of X^+, the left-hand vertical map is the quotient, the horizontal maps are Albanese maps, and the right-hand vertical map is induced by Albanese functoriality. (As base point on X^+, we use the unique cusp of X^+.)

It's an easy fact that $J[I]$ maps to 0 in J^+. Hence if $P \in X$ is killed by I, it maps to 0 on J^+. When the Albanese map $X^+ \to J^+$ is injective, P is forced to map to the unique cusp on X^+ and thus P must be a cusp of X!

Another argument is required when X^+ has genus 0, i.e., when N is one of 23, 29, 31, 41, 47, 59 and 71. Observe that none of these primes is congruent to 1 mod 9.

To complete the proof, we have to look more closely at the set $J[I]_{\mathrm{a.r.t.}}$ of those almost-rational torsion points of J that lie in $J[I]$. Using Csirik's results, one proves:

$$J[I]_{\mathrm{a.r.t.}} = C \oplus \Sigma[3].$$

The group $\Sigma[3]$ is cyclic of order 3 when $N \equiv 1$ mod 9 and trivial otherwise. Thus if $N \in \{ 23, 29, 31, 41, 47, 59, 71 \}$, we have $P \in C$. It is easy to conclude once one knows that $X \cap C = \{ 0, \infty \}$.

The proof that I have sketched becomes complete once one proves that all almost-rational torsion points of J have order prime to N.

Suppose that P is an almost-rational torsion point on J, and let M be the sub-$\mathbb{T}$-module of $J(\overline{\mathbf{Q}})$ generated by P and its conjugates. Thus M is a finite group of torsion points of J on which $\mathbb{T}$ and $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ operate.

If the order of P is divisible by N, there is more work to do. Let $\mathcal{I}$ be an inertia group for N in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The argument involving SGA7I and $(\sigma - 1)^2$ proves that the kernel of the N-adic cyclotomic character $\mathcal{I} \to \mathbf{Z}_N^*$ acts trivially on M. In particular, the action of $\mathcal{I}$ on M is abelian:

Assume now that P has order divisible by N. Then M has order divisible by N, so that there is a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ that divides N for which $M[\mathfrak{m}] \neq 0$. Because $\mathfrak{m}$ is prime to $N-1$, $J[\mathfrak{m}]$ is an irreducible 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over the field $\mathbb{T}/\mathfrak{m}$. Thus M contains $J[\mathfrak{m}]$. Accordingly, the action of $\mathcal{I}$ on $J[\mathfrak{m}]$ is abelian.

A contradiction arises because the action of $\mathcal{I}$ on $J[\mathfrak{m}]$ is non-abelian when $\mathfrak{m}|N$. To see this, let Δ be the abelian quotient of $\mathcal{I}$ that is cut out by $J[\mathfrak{m}]$. The mod N cyclotomic character factors through Δ because $J[\mathfrak{m}]$ fits into an exact sequence

$$0 \to J[\mathfrak{m}]^{\mathrm{t}} \to J[\mathfrak{m}] \to Q \to 0,$$

where $\mathcal{I}$ acts via the cyclotomic character on the "toric" part $J[\mathfrak{m}]^{\mathrm{t}}$ of $J[\mathfrak{m}]$ and acts trivially on Q. The modules $J[\mathfrak{m}]^{\mathrm{t}}$ and Q are 1-dimensional over $\mathbb{T}/\mathfrak{m}$.

We will show that this sequence of $\mathcal{I}$-modules *splits*, which is impossible for various reasons. (E.g., it implies that $J[\mathfrak{m}]$ is *finite* at N in Serre's sense, in contradiction with level-lowering principles). The class of the extension lives in $H^1(\Delta, \mathrm{Hom}(Q, J[\mathfrak{m}]^{\mathrm{t}}))$. The action of Δ on $\mathrm{Hom}(Q, J[\mathfrak{m}]^{\mathrm{t}}$ is given by the inverse of the mod N cyclotomic character. This is a non-trivial character because N must be odd. (Note that $J_0(2) = 0$.) The vanishing of the cohomology group follows by Sah's Theorem.

Closing comments

When A is an abelian variety over a number field K, the set of almost rational torsion points of A constitute a canonical subset of the set of all torsion points of A. Can one identify this set for semistable abelian varieties over $\mathbf{Q}$? For Jacobians of modular curves?