Astérisque

DAN ABRAMOVICH

Formal finiteness and the torsion conjecture on elliptic curves

Astérisque, tome 228 (1995), p. 5-17

<http://www.numdam.org/item?id=AST_1995__228__5_0>

FORMAL FINITENESS AND THE TORSION CONJECTURE ON ELLIPTIC CURVES,
a footnote to a paper of Kamienny and Mazur.

by

DAN ABRAMOVICH

In their paper [KaMa-92], Kamienny and Mazur discuss *torsion primes of degree d*. A prime number N is defined to be a torsion prime of degree d if there is a number field K of degree d over $\mathbb{Q}$, and a pair (E, P) consisting of an elliptic curve E over K and a K-rational N-torsion point P.

One denotes by $S(d)$ the collection of all torsion primes of degree d. The well known *strong uniform boundedness conjecture* states that for every d, the set $S(d)$ is finite. The main results of [KaMa-92] summarize as follows: for all d, $S(d)$ is of density zero, and for $d \leq 8$, $S(d)$ is finite. It should be mentioned that the original conjecture is not restricted to prime levels, but in [KaMa-92] it is shown that prime levels are sufficient.

The goal of this note is to present a slight modification of the methods of Kamienny and Mazur (developped in [Maz-77], [Kam-92b], [Kam-92a], [KaMa-92]). We will pose a weakened version of Kamienny's formal immersion conjecture, which we call the *formal finiteness conjecture*. This allows to reduce the verification of the strong uniform boundedness conjecture for a given degree d to an explicit computation (theorem 2, see also remark at the end of the paper). In particular, we will show that $S(d)$ is finite for $d \leq 12$ (theorem 3). A simple computer program should verify the conjecture for the next few degrees (I have checked this for degrees 13 and 14 using Mathematica).

ACKNOWLEDGEMENTS. It is a pleasure to thank Sheldon Kamienny and Barry Mazur, whose work inspired this note and who had the patience to hear my ideas at their infancy. Thanks to S. David, A. Silverberg and J. F. Voloch,

and to the participants of Coleman's seminar at Berkeley, who had commented on the paper. Thanks to Arthur Ogus for pointing to a mistake in an earlier version. I am also thankful to Noam Elkies, who initiated me into the mysteries of modular curves. This work was partially supported by NSF grant DMS 92 07285.

0.1. Notation. We follow [Maz-77] for the basics.

Let N be a prime and let $X_1(N)$ be the modular curve parametrizing pairs (E,P) consisting of an elliptic curve together with an N-torsion point, completed by adding the cusps. For our purposes here, $X_1(N)$ is a smooth projective curve over $S' = \operatorname{Spec} \mathbb{Z}[1/N]$. A pair (E,P) defined over a field K corresponds to a point $x_{(E,P)}$ in $X_1(N)(K)$. The set $\{x^{\sigma}_{(E,P)}\}_{\sigma \in T}$, where $T = Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/K)$, is Galois stable, and therefore corresponds to a $\mathbb{Q}$-rational point on $Y_1 = X_1(N)^{(d)}$, the symmetric power of degree $d = [K : \mathbb{Q}]$ of $X_1(N)$.

Let $X_0(N)$ be the modular curve parametrizing pairs (E,C) consisting of an elliptic curve and a cyclic subgroup of order N, again completed, by adding the cusps x_∞ and x_0, and viewed as a smooth curve over S'. We have the natural morphism $X_1(N) \to X_0(N)$, mapping the point (E,P) to (E,C), where C is the group generated by P. This induces a morphism $\pi : Y_1 \to Y = X_0(N)^{(d)}$.

Let $J_0(N)$ be the jacobian of $X_0(N)$. Let T_l be the Hecke operators, $l \neq N, l$ prime, and let w be the Atkin - Lehner involution. These operators act on $J_0(N)$, and thus on the space of differential forms on it. We denote by T the $\mathbb{Z}$-algebra generated by T_l and w. We define $\eta_l = T_l - (l+1)$ and $\eta_N = 1 + w$. We extend the definition to all natural numbers by $\eta_1 = id$; $\eta_n = \prod \eta_{l_i}^{\nu_i}$ for $n = \prod l_i^{\nu_i}$. We denote by $I \subset T$ the *Eisenstein ideal*, generated by the operators $\eta_n, n > 1$, and by J_I the *Eisenstein quotient* of $J_0(N)$ as in [Maz-77]. We compose the natural morphism $Y \to J_0(N)$ with the quotient morphism and denote the result by $f : Y \to J_I$. We denote by T_I the I-adic completion of T. The image of T in T_I acts on J_I. Note that in all the above constructions we should have the index N, but we suppressed it, hoping that this will not cause confusion.

Let $y \in Y$ denote the point $\{x_\infty, \dots, x_\infty\}$. Let $Y_m = \operatorname{Spec} \mathcal{O}_Y/\mathfrak{m}_y^{m+1}$ denote the m-th order infinitesimal neighborhood of y in Y. We can view y and Y_m as schemes over S'.

1. Controlling a morphism

We introduce here a simple geometric ingredient which we add to the work of Kamienny and Mazur. The discussion is rather specific to our case, but the

reader will enjoy generalizing it to the favorite situation.

1.1. The local picture. Let $f : Y \to J$ be a morphism between two schemes of finite type over some integral noetherian scheme S. For our applications, S will be either the spectrum of a field or the spectrum of a localization of a number ring. Let $y \in Y(S)$ and $0 = f(y)$. We view y as a closed subscheme of Y mapping isomorphically to S, and similarly for 0 in J. We denote $Z_f(y) = (f^{-1}(0))_y$, the localization along y of the scheme theoretic inverse image of 0.

Definition 1. (1) *The morphism $f : Y \to J$ is said to be* controlled *at y over S if the scheme $Z_f(y)$ is supported along y.*

(2) *The morphism is called* flatly controlled *at y over S if $Z_f(y)$ is supported along y and flat over S.*

(3) *We denote by $S_{fc}(f)$ the maximal open subscheme of S over which f is flatly controlled.*

The existence of $S_{fc}(f)$ is an easy exercise.

These definitions become useful through the following proposition:

Proposition 1. *Let $f : Y \to J$ be a morphism which is controlled at y. Let $x \in Y(S), x \neq y$ such that $f(x) = 0$. Then $x \cap y = \emptyset$.*

Proof. Otherwise the scheme $Z_f(y)$ contains the generic point of x, which is not supported at y. □

The flatness requirement in (2) is a technical convenience which will be used later. Note that over $S_{fc}(f)$, the morphism f is finite in a formal neighborhood of y, which explains the title of this note.

1.2. The main example. Let Y be the d-fold symmetric power of $X_0(N)$. Let $J = J_I$ be the Eisenstein quotient, and let $f : Y \to J$ be the Abel Jacobi map, normalized by sending y to the origin 0. Let $x_{(E,P)}$ be a point on $X_1(N)$ defined over a number field of degree d over $\mathbb{Q}$. Let $x \in Y$ be the image of the point associated to the Galois orbit of $x_{(E,P)}$. Kamienny has shown in [Kam-92a], lemma 3.2 that $f(x) = 0$, and that x meets y over any prime p such that $N > (1 + p^{d/2})^2$.

Kamienny's idea in proving this is as follows: the curve E has an N-torsion rational point over some number field K, therefore its Néron model has N different points over the ring of integers. The reduction modulo a prime over p has many (at least N) different rational points over the residue field. One checks through Tate's list of possible reductions of the Neŕon model, and one verifies that the only cases which do not violate Weil's estimate on the number of points are reductions of type x_∞. This shows that x meets y over p. Now,

since $f(x)$ and $f(y)$ are both rational points on a finite group scheme, and $p > 2$, we have that $f(x) = f(y)$.

The proposition above immediately gives us the following:

Corollary 1. *If $S_{fc}(f)$ contains a prime p such that $N > (1 + p^{d/2})^2$, then for every number field K of degree d over $\mathbb{Q}$, every K-rational point on $X_1(N)$ is a cusp.*

This brings up the question: how to verify $p \in S_{fc}(f)$?

1.3. The infinitesimal picture. We first answer "half" of the question above, by giving a criterion for controlling the morphism which requires a finite amount of data.

Let $f : Y \to J$ be a morphism over S as above, and let m be an integer. We denote $Y_m = \operatorname{Spec} \mathcal{O}_Y/\mathfrak{m}_y^{m+1}$, the m-th order infinitesimal neighborhood of y in Y. Similarly, we denote: $J_1 = \operatorname{Spec} \mathcal{O}_J/\mathfrak{m}_0^2$. Let $Z_m = f^{-1}(0) \cap Y_m$.

Proposition 2. *Assume that $Z_m \subset Y_{m-1}$. Then f is controlled.*

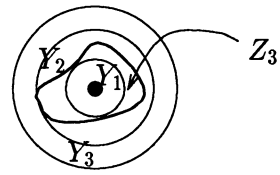

FIGURE 1. Nakayama's lemma: if $Z_3 \subset Y_2$ then Z_3 cannot be the restriction to Y_3 of a bigger scheme supported at y.

Proof (see figure 1): We translate the inclusion into an inclusion of ideal sheaves in Y. We have

$$\mathcal{I}_{f^{-1}(0)} + \mathcal{I}_{Y_m} \supset \mathcal{I}_{Y_{m-1}},$$

therefore, locally at any point of y, a certain set of elements of $\mathcal{I}_{f^{-1}(0)}$ generates $\mathcal{I}_{Y_{m-1}}/\mathcal{I}_{Y_m}$. By Nakayama's lemma, these elements generate $\mathcal{I}_{Y_{m-1}}$ locally at any point of y, that is, $(f^{-1}(0))_y \subset Y_{m-1}$. □

Notice that, assuming Z_m is flat, the condition $Z_m \subset Y_{m-1}$ in the proposition needs only be checked over the generic point of S. This is helpful in explicit computations.

We can now apply this to our main example. We obtain the following generalization of corollary 3.4 of [Kam-92a]:

Theorem 1. *Notation as in* 1.2. *Let N be a prime. Assume we are given m such that over some open subscheme $S'' \subset S'$ we have that Z_m is flat, and $(Z_m)_{\mathbb{Q}} \subset (Y_{m-1})_{\mathbb{Q}}$. Assume we have a prime $p \in S''$ such that $N > (1+p^{d/2})^2$. Then for every number field K of degree d over $\mathbb{Q}$, every K-rational point of $X_1(N)$ is a cusp (see figure 2).*

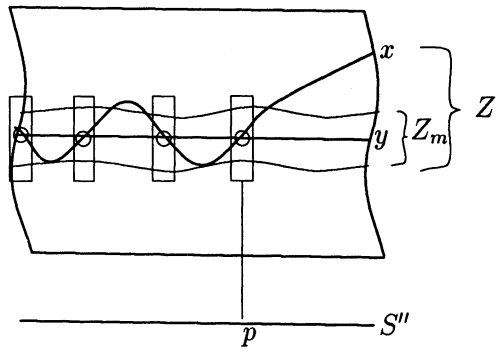

FIGURE 2. The inverse image of the point $f(y)$ in Y. By Kamienny's argument x meets y at p, which forces the fiber of Z_m at p to jump in degree.

This motivates the following definition:

Definition 2. *The morphism $f : Y \to J$ is said to be* controlled at order m *at y if $Z_m \subset Y_{m-1}$.*

In terms of this definition, if f is controlled at order m then f is controlled at y. On the other hand, it is clear that any flatly controlled morphism is controlled at some order m, bounded by $deg(f^{-1}(0))_y + 1$.

Since we will eventually restrict our attention to modular curves, we will need to use modular forms; specifically, we will use differential 1-forms on J. Intuitively, we can view our scheme Z_m as lying in the foliation induced by the 1-forms pulled back from J. In characteristic 0, we would simply integrate these forms and obtain functions, thus returning to the formulation above. Since we will use schemes of mixed characteristic, we need to be a bit careful.

Let f_m be the restriction of f to Y_m.

Proposition 3. *Let $\mathcal{C}$ be a collection of 1-forms on J, and assume that for any $\omega \in \mathcal{C}$ we have $P_\omega \in \mathcal{O}_{Y_m}$, $P_\omega(y) = 0$ such that $dP_\omega = f_m^*\omega$. Assume that m is smaller than the residue characteristic of any point in S. Then*

(1) *$Z_m \subset Spec\ \mathcal{O}_{Y_m}/(P_\omega, \omega \in \mathcal{C})$.*

(2) *If $\mathcal{C}$ generates the cotangent space of J at 0 then*

$$Z_m = Spec\ \mathcal{O}_{Y_m}/(P_\omega, \omega \in \mathcal{C})$$

Proof. Each element ω of $\mathcal{C}$ restricts to an element of $\mathfrak{m}_y/\mathfrak{m}_y^2$, which we identify as an element $\bar{\omega} \in \mathcal{O}_{J_1}$ vanishing at 0. We have $Z_m \subset Y'_m = f_m^{-1}J_1$, where $\bar{\omega}$ vanishes on Z_m. But since $dP_\omega = f_m^*\omega$, we have that $P_{|Y'_m} = (f_{m|Y'_m})^*\bar{\omega}$. □

This means that given a collection of differential forms on J, we can verify that the morphism f is controlled at order m, over points of residue characteristic higher than m.

For our modular curves, this gives a computable condition assuring the non-existence of non-trivial points.

2. Flatness of Z_m

Fix integers d, m and N. From now on, Y will denote the d-fold symmetric power of $X_0(N)$ and $J = J_I$, the Eisenstein quotient.

2.1. Newton's formulas. To study the flatness of our schemes Z_m we will need to bound the coefficients of the pull-back of modular forms to Y_m, and it is useful to present the pull-back homomorphism explicitly.

Let $\omega = \Sigma_{i\geq 1} a_i(\omega)q^i dq/q$ be a 1-form on the Eisenstein quotient, written in its q-expansion as a 1-form on $X_0(N)$. The argument of [Kam-92a] shows that, over $\mathbb{Q}$, $f^*\omega = \Sigma a_i(\omega)d\tau_i/i$, where $\tau_i = \Sigma_{j=1}^d q_j^i$ as a symmetric function. In order to do this over the integers, we invert the primes up to $D = md$, and restrict attention to Y_m. Here the first D coefficients of the form $\Sigma a_i q^i dq/q$ pull back to: $\Sigma_{i=1}^D a_i d\tau_i/i = d(\Sigma_{i=1}^D a_i\tau_i/i)$.

Using Newton's formulas:

$$\tau_n = \sum_{j=1}^{d}(-1)^{j-1}\sigma_j\tau_{n-j} \quad n > d$$

$$\tau_n = \sum_{j=1}^{n-1}(-1)^{j-1}\sigma_j\tau_{n-j} + (-1)^n n\sigma_n \quad n \leq d$$

which are sometimes written concisely as

$$-\frac{d}{dt}\log\left(1 + \sum_{j=1}^{d}\sigma_i(-t)^i\right) = \sum_{i=1}^{\infty}\tau_i t^{i-1}$$

we can rewrite the functions obtained above as power series with zero constant coefficient in σ_i, $\quad 1 \leq i \leq d$ (or in τ_i, $\quad 1 \leq i \leq d$). Since all the first D terms

are known, and $D = md$, we have precisely the terms of order up to m in these power series. Therefore $f^*\omega = dP_\omega$, where $P_\omega = \sum_{i=1}^{D} a_i\tau_i/i$ on Y_m.

2.2. A bound on the non-flat primes. Let

$$\mathcal{A}_m = \mathcal{O}_{S'}[\sigma_1, \ldots, \sigma_d]/(\sigma_1, \ldots, \sigma_d)^{m+1}.$$

We have the explicit presentation $Y_m = \text{Spec } \mathcal{A}_m$ and

$$Z_m = \text{Spec } \mathcal{A}_m/(\{P_\omega\}).$$

Proposition 4. *The scheme Z_m is flat over $S'' =$ Spec $\mathbb{Z}[1/(B(m,d)!N)]$, for some $B(m,d)$ independent of N.*

Proof. Let $\mathcal{C}$ be a $\mathbb{Z}$-basis for the space of 1-forms on J_I. We obtain a resolution:

$$\mathcal{O}_{Y_m}^{\mathcal{C}} \to \mathcal{O}_{Y_m} \to \mathcal{O}_{Z_m} \to 0$$

which we can push down to S'' and obtain:

$$\mathcal{O}_{S''}^{r} \xrightarrow{g} \mathcal{O}_{S''}^{k} \to \mathcal{F} \to 0,$$

where $\mathcal{F} = \pi_*\mathcal{O}_{Z_m}$, for some r and k. The morphism g is given by a matrix A with coefficients in $H^0(S'', \mathcal{O}_{S''})$. The torsion in $\mathcal{F}$ is given by the elementary divisors of A (see Jacobson [BA]), or, scheme theoretically, the support of this torsion is defined as the zero set of all the minors of A of size Rank A. Now assume that a prime p is in the support of the torsion in $\mathcal{F}$. Then p divides all the appropriate minors of A. As in the proof of Corollary 3.4 in [Kam-92a], let R be the ring generated by the coefficients of the eigenforms for the Hecke algebra acting on 1-forms from the Eisenstein quotient. By the base change property, p will divide the minors of the matrix formed by using the eigenforms for the basis $\mathcal{C}$. But, just as in [Kam-92a], the coefficients of order m of the pulled back eigenforms are bounded by some B_0: this is obtained by combining the classical bound $a_n < d_n n^{1/2}$ with Newton's formulas. By looking at the norms, we find that the prime number p is now bounded by $B(m,d) = (r)!B_0^r$, where r is a multinomial function of d and m which grows at most like $(d+m)^{(d+m)}$. □

It has been noted by S. David that we will only use one prime p at which Z_m is flat, and we could get a much lower bound for the size of the minimal prime which does not divide the determinants.

As mentioned before, it is now enough to control f over $\mathbb{Q}$, since then f will automatically be flatly controlled over S''.

3. Fugitivity relations on Hecke operators and on q-coefficients

3.1. Fugitivity relations. Kamienny and Mazur study the implications of linear relations among the Hecke operators η_i, $1 \leq i \leq d$ (they are interested, in particular, in the cases when no relations can occur outside a finite set of levels N). We will look at classes of relations which escape their techniques, which, following their path, we call *fugitivity relations.*

It is important to make this study uniform, as much as possible, over large N. There are two main ingredients in this uniformity: uniform bounds on modular forms, and an almost uniform description of a piece of the Eisenstein ideal, using Mazur's *winding homomorphisms.* Here we regard this almost as a "black box", as a fuller discussion is found in [KaMa-92].

Let D be an integer (it will be a multiple of the degree d we study) and consider the linear equation $\sum_{i=1}^{D} A_i \eta_i = 0$ where A_i are integers. The *weight* of this equation is defined to be

$$w = \min\{n : \exists i = \prod_{j=1}^{n} l_j; \quad l_j \text{ prime}, A_i \neq 0\},$$

that is, the least length of factorization of a number i appearing as an index. We say that the equation is *appropriately bounded* if $A_i \leq B(D)$, where $B(D)$ is the bound obtained as in [KaMa-92] on reduced relations among η_i, similarly to the flatness bound in the previous section.

Definition 3. *A system of equations* $\sum_{j=1}^{D} A_{i,j}\eta_j = 0 \quad j = 1, \ldots, k$ *is called a set of* fugitivity relations of degree D *if*

(1) *all equations are appropriately bounded;*
(2) *all equations have weight at least 2, and*
(3) *whenever* $mC \leq D$, *the equation* $\sum_{j=1}^{C} A_{i,j}\eta_j = 0$ *is in the span of the given equations if and only if* $\sum_{j=1}^{C} A_{i,j}\eta_{mj} = 0$ *is in the span of the given equations.*

A set of fugitivity relations is said to be *realized* if there are *infinitely many* prime levels N for which the linear relations among the actions of the operators η_i on the 1-forms from the Eisenstein quotient are generated by the given set. Kamienny and Mazur showed in effect that any system of relations which holds for infinitely many prime levels N is generated by equations satisfying (1)-(3). In short, condition (1) comes from bounds on q-coefficients of eigenforms, condition (3) comes from the fact that the matrix of $\eta_l, l \neq N$ acting on modular forms is invertible, and condition (2) comes from the winding homomorphisms, giving an equation in "log-primes" for every fugitivity equation. Details can be found in [KaMa-92].

3.2. Passage to q-coefficients. Let V be the space of rational 1-forms on the Eisenstein quotient, and let $a_i : V \to \mathbb{Q}$ be the q-coefficients:

$$\omega = \sum_{i \geq 1} a_i(\omega) q^i dq/q.$$

We need to translate fugitivity relations into relations among a_i. First, we use the definition of η_i and write everything in terms of T_i. Now, after extending the field, we can diagonalize the action of T_i on V simultaneously. Let c_i be the eigenvalue vector, that is, the diagonal elements of T_i. We use the formula for the q-coefficients of an eigenform:

$$a_{lm} = c_l a_m - l a_{m/l}$$

(with the agreement that $a_{m/l} = 0$ if $l \not| m$) and translate our fugitivity relation to a relation among q-coefficients of 1-forms on the Eisenstein quotient. We write this relation as $\sum B_{i,j} a_i = 0 \quad j = 1, \ldots, k$, and call these equation *the set of fugitivity relations on q coefficients.*

An example for $d \leq 12$ is shown in the sequel.

4. The formal finiteness conjecture

Assume we are given a realized set of fugitivity relations. Let W be the solution space over $\mathbb{Q}$ of $\sum B_{i,j} a_i = 0 \quad j = 1, \ldots, k$. Then for infinitely many prime levels, and for each rational element (a_i) of W, there is a rational 1-form on the Eisenstein quotient whose first D q-coefficients are precisely a_i. These forms can be pulled back to $(Y_m)_{\mathbb{Q}}$ and integrated, giving a collection of functions $\{P_n\}$ and thus define the scheme $(Z_m)_{\mathbb{Q}}$.

Definition 4. *We say that the set of fugitivity relations is* controlled *if* $(Z_m)_{\mathbb{Q}} \subset (Y_{m-1})_{\mathbb{Q}}$, *that is, if* $(\sigma_1, \ldots, \sigma_d)^m \subset (\{P_n\})$ *over* $\mathbb{Q}$.

This is equivalent to saying that $f_{\mathbb{Q}}$ is controlled at order m, for *all* the relevant levels N.

FORMAL FINITENESS CONJECTURE. *For every d there is an integer m such that every realized set of fugitivity relations of degree $D = dm$ is controlled.*

We obtain the following theorem:

Theorem 2. *Let d be an integer, and assume that there is an integer m such that every realized set of fugitivity relations of degree $D = md$ is controlled. Then $S(d)$ is finite. In particular, the formal finiteness conjecture implies the strong uniform boundedness conjecture.*

Remark. In [Kam-92b] (proof of Theorem 3.4 for $N = 37$) Kamienny shows how to refine his proof by working directly on the jacobian of $X_1(N)$, defining an Eisenstein quotient and studying the action of the Hecke operators. The reader can easily verify that the methods presented here can also be generalized in that way. However, in order to get general results, one would need a nice description of certain Hecke operators in the Hecke algebra for $X_1(N)$, in a similar way to the "winding homomorphism" description of η_l in terms of $\log l$ in I/I^2. In another direction, one would like to be able to describe η_l in I/I^3 in a useful way, maybe using some higher order winding homomorphisms.

5. **Example:** $d \leq 12$

Theorem 3. *$S(d)$ is finite for $d \leq 12$*

Proof. The theorem follows from theorem 2, once we show that

- for $d \leq 11$, every set of fugitivity relations of degree $D = 2d$ is controlled.
- for $d = 12$, every set of fugitivity relations of degree $D = 4d$ is controlled.

If $d \leq 12$, it follows from the definition that there is at most one fugitivity relation:

$$A_4\eta_4 + A_6\eta_6 + A_8\eta_8 + A_9\eta_9 + A_{10}\eta_{10} + A_{12}\eta_{12} = 0 \tag{1}$$

outside a finite set of levels N. At first thought, it might seem that we need to list all the possible fugitivity relations of degree md. Luckily we will need only facts such as that η_{13}, η_{17}, η_{19} and η_{23} do not appear in any relation of degree 24.

The relation above translates to the equation:

$$\begin{aligned} A_4(c_2-3)^2 + A_6(c_2-3)(c_3-4) + A_8(c_2-3)^3 + A_9(c_3-4)^2 \\ +A_{10}(c_2-3)(c_5-6) + A_{12}(c_2-3)^2(c_3-4) = 0 \end{aligned} \tag{2}$$

Using the formula for the q-coefficients of eigenforms we obtain:

$$\begin{array}{llll} a_2 = c_2a_1; & a_3 = c_3a_1; & a_6 = c_2c_3a_1; \\ a_4 = (c_2^2-2)a_1; & a_9 = (c_3^2-3)a_1; & a_{10} = c_2c_5a_1; \\ a_8 = (c_2^3-4c_2)a_1; & & a_{12} = (c_2^2-2)c_3a_1; \\ a_l = c_la_1 & \text{for } l = 11,13,17,19. & \end{array} \tag{3}$$

Substituting into the relation, we obtain

$$\begin{array}{c} A_4(a_4-6a_2+11a_1)+A_6(a_6-3a_3-4a_2+12a_1) \\ +A_8(a_8-9a_4+31a_2-45a_1) \\ +A_9(a_9-8a_3+19a_1)+A_{10}(a_{10}-3a_5-6a_2+18a_1) \\ +A_{12}(a_{12}-6a_6+11a_3-4a_4+24a_2-44a_1)=0 \end{array} \tag{4}$$

We may assume that $A_9 \neq 0$, otherwise all the indices were divisible by 2 and we would obtain a contradiction to the definition of a fugitivity relation. We can now choose as some of the generators of the solution space:

$$\omega_1 = -A_9 dq + (11A_4 + 12A_6 - 45A_8 + 19A_9 + 18A_{10} - 44A_{12}) d(q^9)/9 + h.o.t.$$

$$\omega_2 = -A_9 d(q^2)/2 + (-6A_4 - 4A_6 + 31A_8 - 6A_{10} + 24A_{12}) d(q^9)/9 + h.o.t$$

$$\omega_3 = -A_9 d(q^3)/3 + (-3A_6 - 8A_9 + 11A_{12}) d(q^9)/9 + h.o.t$$

$$\omega_4 = -A_9 d(q^4)/4 + (A_4 - 9A_8 - 4A_{12}) d(q^9)/9 + h.o.t$$

$$\omega_5 = -A_9 d(q^5)/5 - 3A_{10} d(q^9)/9 + h.o.t$$

$$\omega_6 = -A_9 d(q^6)/6 + (A_6 - 6A_{12}) d(q^9)/9 + h.o.t$$

$$\omega_7 = d(q^7) + h.o.t; \quad \omega_8 = -A_9 d(q^8)/8 + A_8 d(q^9)/9 + h.o.t$$

$$\omega_{10} = A_{10} d(q^9)/9 - A_9 d(q^{10})/10 + h.o.t; \quad \omega_{11} = d(q^{11}) + h.o.t$$

$$\omega_{12} = A_{12} d(q^9)/9 - A_9 d(q^{12})/12 + h.o.t.$$

The above "h.o.t" stand for terms of order 13 or more, and

$$\omega_{13} = d(q^{13}) + h.o.t.; \quad \omega_{17} = d(q^{17}) + h.o.t.; \quad \omega_{19} = d(q^{19}) + h.o.t.$$

Here "h.o.t" stand for terms of order 25 or more.

For $d = 12$ we will actually need a little bit more:

$$\omega_{11} = d(q^{11})/11 + 3d(q^{22})/22 + \text{ terms of order 33}$$

$$\omega_{23} = d(q^{23})/23 + \text{ terms of order 46}$$

$$\omega_{37} = d(q^{37})/37 + \text{ terms of order 74}$$

Now we pull back the integrals of these generators to Y_2, writing them in terms of the symmetric functions. These pullbacks vanish on Z_2. Let $h_m = f_{m|Z_m} : Z_m \to J_I$ be the morphism along which we pull back. In particular we obtain:

$$0 = h_2^* \int \omega_{19} = h_2^* \tau_{19} = h_2^* (\sigma_7 \tau_{12} - \sigma_8 \tau_{11} + \sigma_9 \tau_{10} - \sigma_{10} \tau_9 + \sigma_{11} \tau_8 - \sigma_{12} \tau_7)$$

where we already cancelled the cubic terms. But by the vanishing of ω_{11} and ω_7, we see that $\sigma_{11}, \tau_{11}, \sigma_7$ and τ_7 are in the square of the maximal ideal of Z_m, therefore

$$0 = h_2^* (\sigma_9 \tau_{10} - \sigma_{10} \tau_9)$$

Using Newton's formulas again, cancelling out terms of degree 3, we obtain

$$0 = h_2^*(\tau_9\tau_{10}).$$

Using ω_{10} we can replace τ_{10} by a multiple of τ_9, up to 2nd order, and we obtain: $h_2^*(A_{10}\tau_9^2) = 0$. So either $A_{10} = 0$ or τ_9^2 vanishes on Z_2. In the latter case, the vanishing of ω_i implies that all $\tau_i\tau_j, i, j \leq 11$ vanish on Z_2, which means that $Z_2 \subset Y_1$, that is, the relation is controlled. Otherwise we must have $A_{10} = 0$. This gives, in particular, that τ_{10} and τ_5 are in the square of the maximal ideal on Z_m.

Using now τ_{17} instead of τ_{19}, we obtain that we must have $A_8 = 0$, unless the relation is controlled, and therefore τ_8 is in the square of the maximal ideal. Repeating with 13, we obtain that

$$h_2^*(\tau_1\tau_{12} + 3\tau_4\tau_9) = 0. \tag{5}$$

Assume for a minute that we know that $A_{12} = 0$ (e.g., if $d < 12$). Then we obtain $A_4 = 0$. At this point the fugitivity relation involves only terms divisible by 3: $A_6\eta_6 + A_9\eta_9 = 0$. Therefore we must have $A_6\eta_2 + A_9\eta_3 = 0$, which contradicts requirement (2) in the definition of a fugitivity relation. Therefore our relation is controlled. Thus we need to show $A_{12} = 0$, and we assume by contradiction that it is not, and in particular τ_{12} is not in the square of the maximal ideal.

A simple calculation using $0 = h_4^*\tau_{37}$ gives

$$0 = h_4^*(\tau_{12}^2(36\tau_1\tau_{12} + 49\tau_4\tau_9)).$$

Combining this with (5) we obtain: $0 = h_4^*(\tau_1\tau_{12}^3)$ and $0 = h_4^*(\tau_4\tau_9\tau_{12}^2)$. Since A_{12} is assumed nonzero, we obtain that τ_4 and τ_1 are in the square of the maximal ideal, that is $A_4 - 4A_{12} = 0$, and $11A_4 + 12A_6 + 19A_9 - 44A_{12} = 0$, which gives $12A_6 + 19A_9 = 0$. If we now utilize $0 = h_3^*\tau_{23}$ we obtain (after another simple calculation) that $0 = h_3^*(\tau_2\tau_9\tau_{12})$. This gives that τ_2 must be in the square of the maximal ideal, which gives $-6A_4 - 4A_6 + 24A_{12} = 0$. Combining, we obtain $A_9 = 0$, which is a contradiction.

5.1. Remark. In the course of the proof, we used several times the fact that the condition on the weight of a relation implies that we can always find formal 1-forms with leading term $d(q^p)/p$ for $p =$ either 1 or any prime number. In fact, such formal 1-forms can be explicitely written as follows: for $p = 1$ we take Mazur's power series

$$\delta(q) = \sum_{i\geq 1} \sigma(i)d(q^i)/i,$$

where $\sigma(i)$ is the sum of all divisors of i, and for $p > 1$ one takes a power series δ_p such that

$$\eta_p \delta_p = \delta; \quad \eta_l \delta_p = 0, l \neq p.$$

It is interesting to know whether these elements always suffice to control all fugitivity relations. In very explicit terms, for given degree d, let

$$P_p(q_1, \ldots, q_d) = \sum_{i=1}^{d} \int \delta_p(q_i).$$

Let $B_d = \mathbb{Q}[[q_1, \ldots, q_d]]/(\{P_p\})$. If B_d is artinian then the torsion conjecture holds for degree d. Notice that the power series P_p seem to be thoroughly independent, and there are infinitely many of them. How could the quotient ring fail to be artinian?!

REFERENCES

[BA] Jacobson, N.: Basic Algebra I. W.H. Freeman and Co., New York, 1985.

[Kam-92a] Kamienny, S.: *Torsion points on elliptic curves over fields of higher degree.* Duke I.M.R.N 1992 no. 6, 129-133.

[Kam-92b] Kamienny, S.: *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. **109** (1992), 221-229.

[KaMa-92] Kamienny, S. and Mazur, B.: *Rational torsion of prime order in elliptic curves over number fields*, this volume.

[Maz-77] Mazur, B.: *Modular curves and the Eisenstein ideal.* I.H.E.S. publ. Math. No. 47 (1977), 33-186.

DAN ABRAMOVICH
Department of Mathematics, M.I.T
Cambridge, MA. 02139, U.S.A.
e-mail: abrmovic@math.mit.edu