Astérisque

S. KAMIENNY
B. MAZUR

Rational torsion of prime order in elliptic curves over number fields

Astérisque, tome 228 (1995), p. 81-98
<http://www.numdam.org/item?id=AST_1995__228__81_0>

Rational Torsion of Prime Order in Elliptic Curves over Number Fields

S. Kamienny and B. Mazur
(with an appendix by A. Granville)

Definition. *Let d be a positive integer. A prime number p will be called a* **torsion prime for degree** *d if there is a number field k of degree d, an elliptic curve E defined over k, and a k-rational point P of E, of order p.*

Denote by $S(d)$ the set of torsion primes of degree $\leq d$. It has long been conjectured that $S(d)$ is finite for every d.

Prior to this note, these facts related to the above conjecture were known:

- $S(1) = \{2, 3, 5, 7\}$ $[M1, 2]$
- $S(2) = \{2, 3, 5, 7, 11, 13\}$ $[K1, 2, 5]$
- $S(3)$ is of density < 1 $[M4]$
- $S(d)$ is of density < 1 for all d, and is finite for $d \leq 8$ [Kamienny, unpublished]

The object of this paper is to push ahead slightly, by proving

Theorem. *For any d, the set $S(d)$ is of (natural) density zero.*

Our proof, which will also show that $S(d)$ is finite for $d \leq 8$, has two parts.

Firstly, we use the theory of the "Eisenstein ideal" (specifically: we use results of $[M2], [K5]$, we extend the technique of $[M4]$ and we apply this technique together with a criterion due to the first author $[K4]$) to show that the set $S(d)$ is contained in the union of an explicit finite set and an explicit finite collection of what we shall call *fugitive sets*[1] of prime numbers.

Secondly, we invoke the fact that *fugitive sets* in general are rather "thin" sets of prime numbers: they are of density zero,[2] hence the above Theorem.

---

[1] **"fugitive" because they seem to escape our methods**

[2] **we are thankful to Hendrik Lenstra for providing us with a neat elementary proof of this**

We include an appendix, provided for us by Andrew Granville which gives a slight improvement on *density zero*. Specifically, Granville shows that for any fugitive set of primes, the number of its members $< x$ is less than

$$O\{(x/\log x)\cdot(\log\log\log x/\log\log x)\}.$$

As Kumar Murty pointed out to us, one may also improve this bound ever so slightly[3] if we make use of the Riemann Hypothesis. In any event we expect that the actual size of fugitive sets is a good deal smaller than the above bound, and in particular, the number of primes $< x$ in a fugitive set "should be" less than $O(\log\log x)$.

Our theorem is "effective" in the sense that for any d we do make explicit the finite set of fugitive sets whose union contains $S(d)$, and each of these fugitive sets is recursive (and even more to the point: we can easily determine, by computer, the prime numbers less than, say, 5000, contained in any one of them). These bounds, for all their explicitness, may be of small comfort in that even in the cases where $S(d)$ will be proved below to be finite, e.g., for $d = 3$ where we *expect* that $S(3) \subset \{2, 3, 5, 7, 11, 13, 17, 19\}$, it would simply be too embarrassing to parade the actual astronomical finite bound that the proof gives; and in the case of $S(9) - 9$ being the smallest "d" for which we cannot yet show finiteness – our proof (without further diligence) imbeds $S(9)$ into the union of roughly 480 billion fugitive sets!

For some reflections on the manner in which one might (at present, only conjecturally) determine $S(d)$ in terms of the nature of the action of the Hecke algebra on cuspforms of degree 2 on $\Gamma_1(p)$, see §5 below.

Both authors are appreciative of the NSF, and the first author of the Sloan Foundation, the second author of the Miller Institute at Berkeley, for support while working on this article. We are also most thankful to Ken Ribet for his continued encouragement and advice in the various stages of our work.

§1. Further questions of boundedness.

Let $\Phi(d)$ denote the set of isomorphy types of finite abelian groups occurring as the full groups of torsion in the Mordell-Weil groups of elliptic curves

[3]But not much – to $O\{(x/\log x)\cdot(\log\log x/\log x)\}$

over number fields of absolute degree $\leq d$. Let $N(d)$ (which might be $+\infty$) denote the least common multiple of all the exponents of the groups occurring in $\Phi(d)$. Since any group occurring in $\Phi(d)$ is a quotient group of the product of two cyclic groups of order $N(d)$, one has that $N(d)$ is finite if and only if $\Phi(d)$ is of finite cardinality. At present writing, one only has a *complete* determination of $\Phi(d)$ in the case of $d = 1$ and 2:
$\Phi(1) = \{\mathbf{Z}/m\mathbf{Z}$, with $m \leq 10$, or $m = 12$; and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\nu\mathbf{Z}$ with $\nu \leq 4\}$
(cf. [M 1,2]).
$\Phi(2) = \{\mathbf{Z}/m\mathbf{Z}$, with $m \leq 16$, or $m = 18$; $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mu\mathbf{Z}$ with $\nu \leq 6$; $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}\mu\mathbf{Z}$ with $\mu \leq 2$; and $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}\}$
(This follows from the work in [K 3,5] and [K-M]; see [Mo], [M-S-Z 1,2] and [R] for further results and specific determination of torsion structures in the Mordell-Weil groups of elliptic curves over quadratic fields.)

What is presently known about the general relationship between boundedness of $S(d)$ and boundedness of $\Phi(d)$ is given in the following:

Proposition. *$S(d)$ is finite if and only if $\Phi(d)$ is finite.*

One should note, however, that even if $S(d)$ is given explicitly, the proposition will *not* provide an effective determination of $\Phi(d)$.

Proof of the Proposition. Clearly, if $\Phi(d)$ is finite, then so is $S(d)$. Suppose, then, that $S(d)$ is finite.

The set $\Phi(d)$ will be shown to be finite provided that we can bound, for each $p \in S(d)$, the maximal power of p which can occur as the order of a rational torsion point on any elliptic curve over *any number field of absolute degree* $\leq d$. This is a problem somewhat in the spirit of the result of Manin, which used methods originating with Demjanenko; cf. [Man], [S 1], and which bounds, for a fixed prime number p and number field k, the maximal power of p which can occur as the order of a rational torsion point on any elliptic curve over k. But here we must do this uniformly for all number fields k of degree $\leq d$.

Let us test, first, for a given positive integer N, whether p^N can occur as a torsion point in the Modell-Weil groups of *an infinity* of elliptic curves (with distinct elliptic modular invariants j) over number fields of absolute degree $\leq d$. Equivalently, we are asking whether $X_{/\mathbf{Q}}^{(d)}$, the d-fold symmetric power of the modular curve $X_1(p^N)_{/\mathbf{Q}}$, has an infinity of $\mathbf{Q}$-rational points. Using the results of Faltings [Fa], Frey has shown (in [Fr]) that a sufficient

criterion that the d-fold symmetric power of a curve C, defined over a number field K, have only a finite number of K-rational points is that the curve C does not admit a K-rational covering of $\mathbf{P}^1_{/K}$ of degree $\leq 2d$. Consider, for a small prime number ℓ different from p, the reduction of the modular curve mod ℓ, i.e., $X_1(p^N)_{\mathbf{F}_\ell}$, which is an irreducible (smooth) curve over $\mathbf{F}_\ell$. If $C = C(N, \ell)$ denotes the cardinality of its set of $\mathbf{F}_\ell$-rational points, then, following a strategy used in a similar context by Ogg (compare [O 1]), the minimal degree of any $\mathbb{Q}$-rational mapping of $X_1(p^N)_{/\mathbb{Q}}$ to $\mathbf{P}^1_{/\mathbb{Q}}$ is $\geq C/(\ell+1)$. To conclude that $X^{(d)}$ has only a finite number of $\mathbb{Q}$-rational points, we need only find an N and an ℓ such that $C(N, \ell)/(\ell+1) > 2d$. Taking $\ell = 2$ or 3 (and different from p), and noting that there are at least $p^{N-1}(p-1)/2$ $\mathbf{F}_\ell$-rational cusps on $X_1(p^N)_{/\mathbf{F}_\ell}$, we see that we can guarantee finiteness of the number of $\mathbb{Q}$-rational points on $X^{(d)}$ by choosing an $N > \log_p(12d)/(p-1)) + 1$.

Fix an N as above. Now each $\mathbb{Q}$-rational point on $X^{(d)}$ will give rise to (possibly more than one, but) at most a finite number of distinct elliptic curves E_{j/k_j} defined over number fields k_j of absolute degree $\leq d$. The totality (corresponding to *all* the $\mathbb{Q}$-rational points of $X^{(d)}$) of such elliptic curves E_{j/k_j} give, after possible base extension, *all* isomorphism classes of elliptic curves defined over number fields k of degree $\leq d$ whose Mordell-Weil groups contain points of order p^N.

One now makes use of the following lemma whose proof (which we omit) is an easy exercise, using, for example, the results of Serre [S 2] on the natural action of the Galois group of a number field k on the group of p-power torsion points of an elliptic curve defined over k:

Lemma. *Let E be an elliptic curve defined over a number field K. Let D be a positive integer. There is a finite upper bound $B = B(E_{/K}, D)$ for the order of the torsion subgroup in $E(L)$ where L/K ranges over all field extensions of K of degree $\leq D$.* □

Now, for each of the elliptic curves E_{j/k_j} listed above, let p^{N_j} denote the maximal power of p which occurs as the order of a k-rational torsion point of E_j considered over k, where k ranges over all field extensions of k_j of degree $\leq d$. That there is an integer N_j with the above property for each j, is guaranteed by the above lemma. Now put $M = \max_j(N_j)$; we have that p^M

is the maximal power of p which can occur as the order of a rational torsion point on any elliptic curve over *any number field of absolute degree* $\leq d$. □

We end this section with some speculations concerning related questions of boundedness.

Boundedness of isogenies. As for isogenies of elliptic curves over $\mathbb{Q}$, one has an explicit classification (see [Ma 3] and for explicit parametrizations in the genus zero cases, see [Ku]).

There is also the following result proved in [Fr], using the work of [Fa], concerning prime numbers p for which there are an *infinity* of isogenies of degree p of elliptic curves over number fields of absolute degree d. If d is a positive integer, and p is a prime number let $J(p,d)$ denote the set of j-invariants of elliptic curves E defined over number fields k of absolute degree d and possessing a k-rational cyclic subgroup of order p. The Corollary to Proposition 3 of [Fr] asserts, in effect, that *if* $J(p,d)$ *is infinite, then* $p \leq 240 \cdot d$.

One must be careful in framing "boundedness" questions concerning isogenies of elliptic curves over number fields because *any* elliptic curve with complex multiplication, considered over *any* number field k containing its field of complex multiplication will possess k-rational isogenies of degree p for *all* prime numbers p which split in the field of complex multiplication. It is tempting, though, to formulate boundedness questions which avoid this source of isogeny. Is there, for fixed positive integer d, an upper bound to the set of prime numbers p which can occur as degrees of isogenies of elliptic curves *without complex multiplication* rational over number fields of absolute degree $\leq d$?

Rational points on abelian varieties over $\mathbb{Q}$ of fixed dimension:. Let $T(d)$ denote the set of prime numbers p for which there exists an abelian variety A of dimension $\leq d$ defined over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational torsion point of order p. It is immediate, from the properties of the "Weil trace", that $S(d)$ is contained in $T(d)$. Since $J_1(13)_{/\mathbb{Q}}$ is an abelian variety of dimension two containing a point of order 19, one sees (since $S(2)$ is known explicitly) that $S(2)$ is *properly* contained in $T(2)$. Is $T(d)$ finite for each d?

§2. "Fugitive sets" of primes

First, for every prime number p, we choose an isomorphism, which we

call "log":

$$(\mathbf{Z}/p\mathbf{Z})^* \xrightarrow[\cong]{\log} \mathbf{Z}/(p-1)\mathbf{Z};$$

our definition of "fugitive set" will be independent of this choice.

Now fix the following data:

(1) a natural number ν,

(2) a set $\{q_1, \ldots, q_\nu\}$ consisting of ν prime numbers; these q_i we will call the "**log-primes**",

(3) a homogeneous form $F(X_1, \ldots, X_\nu)$ of some degree r, with rational integral coefficients. We assume F nontrivial.

Definition. *A prime number p will be called* **fugitive** *for the above data if p is not one of the log-primes q_i and the equation*

$$F(\log q_1, \log q_2, \ldots, \log q_\nu) = 0$$

holds in the ring $\mathbf{Z}/(p-1)\mathbf{Z}$.

The set of all fugitive primes for a given choice of homogeneous form F in logs of primes $\{q_1, \ldots, q_\nu\}$ will be referred to as the **fugitive set** of primes *attached to the relation* "$F(\log q_1, \log q_2, \ldots, \log q_\nu) = 0$". Of special interest to us will be the degree r of the homogeneous form involved, and a **fugitive set of degree** r refers to a fugitive set attached to a homogeneous form of degree r.

Example: (1). Fugitive sets of degree 1 are finite. For, if p is a fugitive prime for a nontrivial form of degree 1,

$$F(\log q_1, \ldots, \log q_\nu) = \sum a_j \cdot \log q_j,$$

then p is a divisor of (the numerator of) $\prod q_j^{a_j} - 1$, this being a nonvanishing rational number since not all the a_i's are zero.

(2) Given any homogeneous form in log-primes, e.g.,

$$"(\log 2)^2 - (\log 3)^2 = 0",$$

it is quite easy to program a computer to determine its "small" fugitive primes (and for the above homogeneous form in log-primes, the first two fugitive primes are 5, 5333).

§3. The Hecke algebra and the Eisenstein Ideal

Let p be a prime number, and $J = J_0(p)$, the jacobian of the modular curve $X_0(p)$. Let $\mathbf{T}$ denote the image of the Hecke algebra in $\mathrm{End}(J)$, or equivalently, in the endomorphism ring of the space of cuspforms of weight 2 over $\Gamma_0(p)$. Specifically, $\mathbf{T}$ is generated as a $\mathbf{Z}$-algebra in $\mathrm{End}(J)$ by the operators T_ℓ for every prime number $\ell \neq p$, and by the Atkin involution w_p. We call $\mathbf{T}$ "*the Hecke algebra*" and if we wish to exhibit its dependence on p, we denote it $\mathbf{T}(p)$.

For each prime number $\ell \neq p$, put $\eta_\ell := 1+\ell-T_\ell$, and let $\eta_p := 1+w_p$. It is also convenient to define η_m, for all indices $m \in \mathbf{N}$, extending the definition of η_ℓ for prime indices ℓ by the multiplicative rules: $\eta_1 = 1$, and $\eta_{a\cdot b} = \eta_a \cdot \eta_b$ for $a, b \in \mathbf{N}$. It will be important for us to note that for any fixed positive integer d, there is a $d \times d$ triangular matrix M_d in $\mathrm{GL}_d(\mathbf{Z})$ (*independent of* p) having the property that for any prime number $p > d$, the application of M_d to the column vector

$$(\eta_1, \eta_2, \eta_3, \ldots, \eta_d)$$

in $\mathbf{T}(p)^d$ yields the column vector of Hecke operators in $\mathbf{T}(p)^d$

$$(T_1, T_2, T_3, \ldots, T_d).$$

By the *Eisenstein ideal* (see [M 2]) we mean the ideal $I \subset \mathbf{T}$ generated by the elements η_ℓ for all prime numbers ℓ (or equivalently, by η_m for all integers $m \geq 2$).

In [M 2] it is proven that $\mathbf{T}/I$ is canonically isomorphic to $\mathbf{Z}/n\mathbf{Z}$, where $n =$ the numerator of $(p-1)/12$, and that the ideal I is locally principal in $\mathbf{T}$. Moreover, the "*winding homomorphism*" (cf. [M 2] Prop. 18.6) gives a canonical isomorhpism between I/I^2 and the (unique, cyclic) quotient group of $(\mathbf{Z}/p\mathbf{Z})^*$ of order n.

We recall the description of the "winding homomorphism". We may assume that $p > 2$. Let e be the greatest common divisor of 12 and $p-1$, so that $p - 1 = e\cdot n$, and e is an even divisor of 12. Let $\mathcal{E} \subset (\mathbf{Z}/p\mathbf{Z})^*$ denote the (unique, cyclic) subgroup of order e.

Proposition. *There is an isomorphism of cyclic subgroups of order* n,

$$w : I/I^2 \xrightarrow{\cong} (\mathbf{Z}/p\mathbf{Z})^*/\mathcal{E}$$

uniquely specified by the property that w *sends* η_ℓ *to the image of* $\ell^{(\ell-1)/2}$ *in* $(\mathbf{Z}/p\mathbf{Z})^*$ *module* $\mathcal{E}$, *for every prime number* $\ell \neq p$.

Remark. this is [M 2] Prop. 18.6. At first view, the above statement seems a bit strange for $\ell = 2$, since $\ell^{(\ell-1)/2} = 2^{1/2}$. But note that there are two possibilities: either n is odd (in which case the expression makes sense, since the square-root operation in an odd, multiplicatively-written, cyclic group is well-defined) or else n is even, i.e., $p \equiv 1 \bmod 8$ (in which case 2 is a quadratic residue modulo p; if $\pm\alpha \in (\mathbf{Z}/p\mathbf{Z})^*$ are the two square-roots of 2 modulo p, then since $\{\pm 1\}$ modulo p lies in $\mathcal{E}$, $\pm\alpha$ determines a unique congruence class in $(\mathbf{Z}/p\mathbf{Z})^*$ modulo $\mathcal{E}$ and this gives a unique meaning to "$2^{1/2}$").

Since the mapping $12\cdot\log : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}/(p-1)\mathbf{Z}$ factors through the quotient group $(\mathbf{Z}/p\mathbf{Z})^*/\mathcal{E}$, we get, from the above Proposition the existence of a unique homomorphism $\varphi : I/I^2 \to \mathbf{Z}/(p-1)\mathbf{Z}$ fitting into a commutative triangle

$$\begin{array}{ccc} & & (\mathbf{Z}/p\mathbf{Z})^*/\mathcal{E} \\ & & \Big\downarrow \text{“}12\cdot\log\text{”} \\ I/I^2 & \xrightarrow[\varphi]{} & \mathbf{Z}/(p-1)\mathbf{Z} \end{array}$$

where w

where $\varphi(\eta_\ell) = 6\cdot(\ell-1)\cdot\log\ell$ (modulo $p-1$) for all prime numbers $\ell \neq p$.

A feature of this homomorphism, which is quite important for us, is that the expression $6\cdot(\ell-1)\cdot\log\ell$ makes "no" reference to p (with the exception of the appearance of the "log"-term, and the fact that it will be interpreted only modulo $p-1$).

The ring $\mathbf{T}$ is a commutative ring, free of finite rank as a $\mathbf{Z}$-module with the property that $\mathbf{T}\otimes\mathbf{Q}$ is a direct product of totally real fields. The completion of $\mathbf{T}$ with respect to the Eisenstein ideal,

$$\mathbf{T}_I := \varprojlim_{\nu} \mathbf{T}/I^\nu,$$

is a complete semi-local ring of Krull dimension 1 in which the ideal $I\cdot\mathbf{T}_I \subset \mathbf{T}_I$ is principal, and, moreover, the successive quotients, $I^r\cdot\mathbf{T}_I/I^{r+1}\cdot\mathbf{T}_I \cong I^r/I^{r+1}$, are cyclic groups of order n, for all $r \geq 1$. To lighten the notation below, we shall identify $I^r\cdot\mathbf{T}_I/I^{r+1}\cdot\mathbf{T}_I$ with I^r/I^{r+1}, and if we wish to indicate the dependence of $\mathbf{T}_I$ on p, we may refer to it as $\mathbf{T}_I(p)$. If $\tau \in \mathbf{T}$, let $\tilde{\tau}$ denote the image of τ in $\mathbf{T}_I$.

If we denote by $\tilde{\mathbf{T}}$ the image of the Hecke algebra $\mathbf{T}$ in $\mathbf{T}_I$, and by $\tilde{J}$ the *Eisenstein quotient* of the abelian variety J (see [M 2]) then the canonical action of $\mathbf{T}$ on J induces a faithful action of $\tilde{\mathbf{T}}$ on $\tilde{J}$.

Definition. *For any positive number r, let the* $\mathbf{r-th}$ **winding isomorphism**

$$\varphi_r : I^r/I^{r+1} \longrightarrow \mathbf{Z}/(p-1)\cdot\mathbf{Z}$$

denote the homomorphism given as the composition of these homomorphisms of
$\mathbf{Z}/(p-1)\cdot\mathbf{Z}$*-modules, each of which will be explained below:*

$$I^r/I^{r+1} \underset{\iota^{-1}}{\overset{\cong}{\longrightarrow}} (I/I^2)^{\otimes r} \overset{(\varphi)^{\otimes r}}{\longrightarrow} (\mathbf{Z}/(p-1)\cdot\mathbf{Z})^{\otimes r} \longrightarrow \mathbf{Z}/(p-1)\cdot\mathbf{Z}. \qquad (1)$$

The tensor powers are simply over $\mathbf{Z}$. The mapping

$$\iota : (I/I^2)^{\otimes r} \longrightarrow I^r/I^{r+1}$$

is given by the rule that an element of $(I/I^2)^{\otimes r}$ of the form $\bar{\alpha}_1 \otimes \bar{\alpha}_2 \otimes \ldots \otimes \bar{\alpha}_r$ be sent to the image of $\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_r \in I^r$ mod I^{r+1} (where the $\bar{\alpha}_j$ are the images of elements $\alpha_j \in I$). Then ι is well-defined; it is surjective; it is an isomorphism since both domain and range are (cyclic) groups of the same order. The middle mapping in (1) is as labelled, and the last mapping of (1) is multiplication in the ring $\mathbf{Z}/(p-1)\cdot\mathbf{Z}$.

§4. Linear relations in Hecke operators

For a fixed d-tuple of integers, $a_1, a_2, \ldots, a_d$, not all zero, let

$$\mathcal{N}(a_1, , a_2, \ldots, a_d)$$

denote the set of prime numbers $p > d$ for which the image of the linear combination $a_1\cdot 1 + a_2\cdot T_2 + \ldots + a_d\cdot T_d$ vanishes in $\mathbf{T}_I(p)$.

Proposition 1. *For a fixed d-tuple of integers, $a_1, a_2, \ldots, a_d$, not all zero, the set $\mathcal{N}(a_1, \ldots, a_d)$ is (either finite, or else it is) contained in a fugitive set (attached to an explicit homogeneous form in log-primes).*

Proof.

First, viewing $(a_1, \ldots, a_d)$ as a row-vector of length d, let $(b_1, \ldots, b_c)$ denote the (nontrivial) row-vector $(a_1, \ldots, a_d) \cdot M_d$, where the $d \times d$ matrix $M_d \in GL_d(\mathbf{Z})$ is as in §3. We then have that for $p > d$, the image of the linear combination

$$a_1 \cdot 1 + a_2 \cdot T_2 + \ldots + a_d \cdot T_d$$

vanishes in $\mathbf{T}_I(p)$ if and only if the image of the linear combination

$$b_1 \cdot \eta_1 + b_2 \cdot \eta_2 + \ldots + b_d \cdot \eta_d$$

vanishes in $\mathbf{T}_I(p)$, and it will be more convenient for us to deal with the η's rather than the classical T's.

By the **weight** $w(m)$ of a positive number m, we shall mean the number of prime factors (counting multiplicity) in its prime factorization (e.g., $w(1) = 0, w(12) = 3$, etc.). For an integer $m > 1$, consider its prime decomposition, $m = p_1 \cdot p_2 \cdot \ldots \cdot p_w$, where $w = w(m)$. Recall that η_m is the element in the Hecke algebra $\mathbf{T}$ given as the product $\eta_m = \eta_{p_1} \cdot \ldots \cdot \eta_{p_w}$, and therefore η_m lies in I^w, the w-th power of the Eisenstein ideal.

Suppose, then, we have a prime $p > d$ for which the relation

$$b_1 \cdot 1 + b_2 \cdot \tilde{\eta}_2 + \ldots + b_d \cdot \tilde{\eta}_d = 0$$

holds in $\mathbf{T}_1(p)$ for the rational integers b_i, or equivalently, that

$$b_1 \cdot 1 + b_2 \cdot \eta_2 + \ldots + b_d \cdot \eta_d \equiv 0 \qquad \mod I^{r+1}$$

holds in $\mathbf{T}(p)$ for all integers $r \geq 0$.

Note that from the above relation, we have $b_1 \in I$, and hence b_1 is a multiple of $n =$ numerator $(p-1)/12$. Therefore, if b_1 is nonzero it follows that $p \leq 12 \cdot |b_1| + 1$, and consequently the set $\mathcal{N}(a_1, \ldots, a_d)$ is finite.

So we may assume that $b_1 = 0$, i.e., that our relation is of the form

$$\sum_{j=2}^{d} b_j \tilde{\eta}_j = 0. \tag{2}$$

For positive numbers w, define:

$$H_w := \sum_{\substack{j=2,\ldots,d \\ w(j)=w}} b_j \eta_j \ ,$$

that is, H_w is the contribution to the left-hand side of (2) coming from summands whose index j has weight w. Note that $H^w \in I^w$. Let r be the lowest weight for which there is an integer j in the range $2 \leq j \leq d$, with $w(j) = r$ and such that the integer b_j is nonzero.

Relation (2) then can be written

$$\tilde{H}_r + \tilde{H}_{r+1} + \tilde{H}_{r+2} + \ldots = 0 \quad \text{in} \quad \mathbf{T}_1(p). \tag{3}$$

In the above formula, each summand lies in I^r and all but the first lie in I^{r+1}. We have, then, that the image of H_r vanishes in I^r/I^{r+1}, and consequently, applying the r-th winding homomorphism of §3 above, we have that $\varphi_r(H_r) = 0$.

All that remains is to write out this relation. For any positive integer j and prime number q, let $v_q(j)$ denote the maximal exponent v such that q^v divides j. We may write:

$$\eta_j = \prod_{q|j} (\eta_q)^{v_q(j)}$$

and if j is of weight r, then the right-hand side is a monomial in the η_q's of degree r.

So:

$$\begin{aligned} \varphi_r(H_r) &= \sum_{\substack{j=2,\ldots,d \\ w(j)=r}} b_j \cdot \varphi_r(\eta_j) = \sum_{\substack{j=2,\ldots,d \\ w(j)=r}} b_j \cdot \varphi_r\Big(\prod_{q|j} (\eta_q)^{v_q(j)}\Big) \\ &= \sum_{\substack{j=2,\ldots,d \\ w(j)=r}} b_j \cdot \Big\{\prod_{q|j} (6(q-1))^{v_q(j)}\Big\} \cdot \prod_{q|j} (\log q)^{v_q(j)}. \end{aligned}$$

Now, for $j = 2, \ldots, d$ of weight r, put

$$B_j := b_j \cdot \Big\{\prod_{q|j} (6(q-1))^{v_q(j)}\Big\} \in \mathbf{Z}$$

and let $\mathcal{Q}$ stand for the set of prime numbers q which actually divide some integer $j = 2, \ldots, d$ of weight r, for which b_j is nonzero. We take $\mathcal{Q}$ as an index

set for a system of variables X_q, $q \in \mathcal{Q}$, and define the *nontrivial* homogeneous form F of degree r in the variables X_q by the rule:

$$F(\ldots, X_q, \ldots) := \sum_{\substack{j=2,\ldots,d \\ w(j)=r}} B_j \cdot \prod_{q|j} (X_q)^{v_q(j)}.$$

We then have that $F(\ldots, \log q, \ldots) = 0$ in $\mathbf{Z}/(p-1)\cdot\mathbf{Z}$, i.e., that p is a fugitive prime number for the above homogeneous log-prime relation of degree r. □

Remark. In working with specific numerical cases, it is sometimes useful to refine the procedure given in the above demonstration, to get somewhat stronger consequences. Specifically, when one gets to the relation given by formula (2), it is advisable to consider the greatest common divisor m of the integers j for which b_j is nonzero. Then, since $\Sigma b_j \cdot \eta_j = \eta_m \cdot \sum b_j \cdot \eta_{(j/m)}$, and since multiplication by η_m yields an isogeny of J (as can be seen from the standard estimates on the eigenvalues of the Hecke operators), it follows that if the image of $\Sigma b_j \cdot \eta_j$ is 0, then the image of $\Sigma b_j \cdot \eta_{j/m)}$ is also 0 in $\mathbf{T}_I(p)$. Continuing through the proof with the "finer relation" (if $m > 1$) will yield that p is in the fugitive set of a homogeneous form in log-primes of *lower degree.* This refinement is a particular help when it reduces the homogeneous form to one of degree 1 (in which case the fugitive set is *finite*, by Example (1) of §2).

Our next step is to consider the more encompassing set, $\mathcal{N}_d$, of prime numbers p for which there is *some* nontrivial linear combination $a_1 \cdot 1 + a_2 \cdot T_2 + \ldots + a_d \cdot T_d$ which vanishes in $\mathbf{T}_I(p)$.

Proposition 2. *The set $\mathcal{N}_d$ is contained in a finite union of fugitive sets (attached to an explicit finite set of homogeneous forms in log-primes).*

Proof.

For positive numbers $r \leq d$, let $\mathcal{N}(r, d)$ denote the set of prime numbers p for which (**i**) there is a linear combination

$$a_1 \cdot 1 + a_2 \cdot T_2 + \ldots + a_d \cdot T_d$$

whose image vanishes in $\mathbf{T}_I(p)$, with (**ii**) precisely $r - 1$ of the integers $a_1, a_2, \ldots, a_{d-1}$ not zero, and (**iii**) $a_d \neq 0$.

Let $\mathcal{N}_0(r,d)$ denote the "new primes" in $\mathcal{N}(r,d)$, i.e., those that have not appeared in an $\mathcal{N}(r',d')$ for smaller r' and/or d'. It suffices to show that the sets $\mathcal{N}_0(r,d)$ are each contained in a finite union of fugitive sets (attached to a finite set of explicit log-prime relations), for each pair (r,d).

Now, let $p \in \mathcal{N}_0(r,d)$ and we shall analyze a linear Hecke relation,

$$a_1 \cdot 1 + a_2 \cdot T_2 + \ldots + a_d \cdot T_d = 0$$

in $\mathbf{T}_I(p)$, satisfying (i) – (iii). We may suppose that the gcd of the a_i's is 1. Let $\mathcal{R} \subset [1,\ldots,d]$ be the set of r indices $i \in [1,\ldots,d]$ such that $a_i \neq 0$.

Proposition 2 follows immediately from Proposition 1, together with the following lemma.

Lemma. *There is a bound*[4] $B(d)$, *such that* $|a_j| \leq B(d)$ *for all* $j \in \mathcal{R}$.

Fix any $j \in \mathcal{R}$; denote $\mathcal{R} - \{j\}$ by $\mathcal{R}'$. For each $k \in \mathcal{R}'$ fix a differential 1-form f_k on the Eisenstein quotient $\tilde{J}$ (recall this terminology from §3 above, and from [M 2]), (e.g., we can, and do, choose the f_k's to correspond to newforms of weight 2 parametrized by $\tilde{J}$) giving us a choice of $r-1$ differential forms. We may even find such a choice with the property that if $c_m(f)$ denotes the m-th coefficient of the Fourier expansion of a form f, then the $(r-1) \times (r-1)$ matrix $C = (c_i(f_k))$ for $i,k \in \mathcal{R}'$ has nonzero determinant. The reason why we can do this is that if we *fail* to find such a choice of $r-1$ differential 1-forms, there would necessarily be some nontrivial linear relation which holds among the Fourier coefficients with indices drawn from the set $\mathcal{R}'$ of cardinality $r-1$, this linear relation being valid for all differential forms on $\tilde{J}$, violating the hypothesis that p is "new", i.e., is not in $\mathcal{N}(r-1,d)$, or $\mathcal{N}(r-1,d-1)$. Let $\mathcal{O}$ denote the ring of integers in a number field large enough to contain the $c_i(f_k)$; then $\delta := \det(C)$ lies in $\mathcal{O}$. There is a bound $B = B(d)$, depending only on d such that under every imbedding of $\mathcal{O}$ in $\mathbf{C}$, δ maps to an element of absolute value $< B$, the bound being calculated directly from the Ramanujan-Peterson bound on the m-th coefficient of any (normalized) newform f of weight 2: $|c_m(f)| \leq d(m) \cdot m^{1/2}$ where $d(m)$ is the number of divisors of the integer m. If $\mathcal{O}$ is of degree N over $\mathbf{Z}$, and if $\nu : \mathcal{O} \to \mathbf{Z}$ denotes its norm mapping, then $\nu(\delta) \leq B(d)^N$.

[4]For any $\epsilon > 0$, and $d \underset{\epsilon}{\gg} 0$, $B(d)$ can be taken to be $(d!)^{3/2+\epsilon}$.

Now consider the relations (for $k = 1, \ldots, r-1$)

$$\sum_{i \in \mathcal{R}'} a_i c_i(f_k) = -a_j c_j(f_k). \qquad (*)$$

Denote by V the free, $\mathcal{O}$-module of rank $r-1$ given by $(r-1)$-tuples of elements $(v_i; i \in \mathcal{R}')$ with $v_i \in \mathcal{O}$.

Put $\alpha = (a_i; i \in \mathcal{R}')$ and $\gamma = (c_j(f_k); k \in \mathcal{R}')$.

The matrix C may be viewed as an $\mathcal{O}$-linear mapping $C : V \to V$ by matrix multiplication with elements of V on the right, i.e., $C(v) := v \cdot C$.

Then the system of linear relations given in (*) can be written as:

$$C(\alpha) = -a_j \cdot \gamma.$$

Reducing C modulo the nonzero integer a_j, we get an $\mathcal{O}/a_j \cdot \mathcal{O}$ homomorphism, $\bar{C} : V/a_j \cdot V \to V/a_j \cdot V$, we see, first, that the image $\bar{\alpha}$ of α in $V/a_j \cdot V$ may be taken as a basis element of $V/a_j \cdot V$, viewed as free $\mathcal{O}/a_j \cdot \mathcal{O}$-module of rank $r-1$. This is because the integers $a_1, \ldots, a_d$ were assume to have gcd equal to 1. By the above relation, we have $\bar{C}(\bar{\alpha}) = 0$. Therefore, the reduction of $\delta = \det C \bmod \mathcal{O}/a_j \cdot \mathcal{O}$, call it $\bar{\delta}$, vanishes in $\mathcal{O}/a_j \cdot \mathcal{O}$. Consequently, there is an element $\tau \in \mathcal{O}$ such that $\delta = a_j \cdot \tau$. Since δ is nonzero, so is τ. So $|\nu(\tau)| \geq 1$, and $\nu(\delta) = (a_j)^N \cdot \nu(\tau)$, and therefore $|a_j|^N \leq B(d)^N$; i.e., $|a_j| \leq B(d)$. □

Corollary. *For any positive integer d, the set $S(d)$ of torsion primes for degree d is contained in the union of an explicit finite set and a finite union of fugitive sets (attached to an explicit finite set of homogeneous forms in log-primes).*

Remark. As mentioned in our introduction, our Main Theorem follows from this Corollary together with the density zero result proven in the appendix.

Proof of Corollary. For a fixed positive integer d, from Propositions 1,2 above we see that except for a set of prime numbers p contained in a finite union of fugitive sets (and a finite set), the images of the Hecke operators $T_1 = 1, T_2, \ldots, T_d$ are linearly independent in $\mathbf{T}_I(p)$. It follows from Corollary 3.4 of [K 4] that such prime numbers p are not torsion primes of degree d. We will discuss this last reference in greater detail in §5 below.

Concluding Remarks. As mentioned in the introduction, $S(1)$ and $S(2)$ had been previously determined. The first author had also previously obtained *finiteness* of $S(d)$ for $d = 3, 4, 5, 6, 7$ and 8. Finiteness for $d \leq 8$ can be seen from the fact that the only monomials of degree > 1 in log-primes that intervene in our bounds for $S(d)$ for $d \leq 8$ are $(\eta_2)^2, \eta_2\eta_3$, and $(\eta_2)^3$, and therefore η_2 is a multiplicative factor in any relation of degree $r \geq 2$ that will occur in formula (2) above (if $d \leq 8$). Using the remark after Proposition 1, one sees then that if $d \leq 8$, $S(d)$ is contained in the union of a finite set, and a finite union of fugitive sets of degree 1. Invoking, then, Example (1) of §2, $S(d)$ is finite for $d \leq 8$.

The case $d = 9$ is the first case where our present methods *do not* obtain finiteness – $S(9)$ is contained in the union of a finite set together with the fugitive sets of degree two coming from homogeneous forms in log-primes of the type

$$A\cdot(\log 2)^2 + B\cdot(\log 2)(\log 3) + C\cdot(\log 3)^2 = 0$$

for $|A|, |B|, |C| \leq 2956, 3786, 4848$, respectively.

§5. Remarks on a generalization of Ogg's conjecture.

Ogg's conjecture [O 2] , prived in [M 1], asserts that there is an elliptic curve defined over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational point of order N if and only if the modular curve $X_1(N)$ is of genus 0. Recently, the first author of this note has formulated a "rough suggestion" in the spirit of Ogg's conjecture to determine the set $S(d)$ (see [K 3]). We would like to end this note by formulating another rough suggestion inspired by the sufficient criterion proved in [K 4] for p to lie in the complement of $S(d)$.

Recall that the group $(\mathbb{Z}/p)^*$ acts on the modular curve $X_1(p)$ via the "diamond operators": if r is an integer not divisible by p, then the **diamond operator** $\langle r\rangle : X_1(p) \to X_1(p)$ is the automorphism which is induced by the automorphism on the moduli problem obtained by sending the pair $(\mathcal{E}, \alpha : \mu_p \to \mathcal{E})$ (where $\mathcal{E}$ is an elliptic curve, and α an injective homomorphism) to the pair $(\mathcal{E}, r\cdot\alpha : \mu_p \to \mathcal{E})$. The diamond operator action then induces an action of the algebra $R = \mathbb{Z}[\mathbb{Z}/p^*]$ on $J_1(p)$, the jacobian of the modular curve $X_1(p)$.

As an approximation to the Hecke algebra of $X_1(p)$ let us form $\mathcal{T}$, the subring in the endomorphism ring of the abelian variety $J_1(p)$ generated by

R and the Hecke operators T_ℓ for all $\ell \neq p$. As our approximation to the *Eisenstein ideal* let us consider the ideal $\mathcal{I}$ defined as the ideal in $\mathcal{T}$ generated by the elements $1 = \ell \cdot \langle \ell \rangle - T_\ell$ in $\mathcal{T}$, for all prime numbers $\ell \neq p$. Let $\mathcal{T}_\mathcal{I}$ denote the completion of the (commutative) ring $\mathcal{T}$ with respect to the ideal $\mathcal{I}$. As before, if we wish to indicate dependence on p, we will denote R as $R(p)$, and $\mathcal{T}_\mathcal{I}$ as $\mathcal{T}_\mathcal{I}(p)$.

Now fix a positive integer d, and (ignoring prime numbers $p \leq d$) consider the set $\mathcal{S}(d)$ consisting in all prime numbers $p > d$ for which *the images of the Hecke operators* $T_1, T_2, \ldots, T_d$ in the $R(p)$-algebra $\mathcal{T}_\mathcal{I}(p)$ *are* $R(p)$*-linearly dependent.*

Question. *For prime numbers $p > d$ is it the case that p is in $\mathcal{S}(d)$ if and only if p is in $S(d)$?*

For $d = 1$ this is indeed the case, and its assertion is precisely Ogg's conjecture. For $d = 2$, this is shown in [K 5]. For general d we cannot, at present, show inclusion in either direction.

§6. References.

[F 1] Faltings, G.: Diophantine approximation on abelian varieties. Ann. Math. **133** (1991) 549-576

[Fa 2] Faltings, G.: The general case of S. Lang's conjecture. Preprint. Princeton U. 1992

[Fr] Frey, G.: Curves with infinitely many points of fixed degree. Preprint 1992. Institut für Experimentelle Mathematik

[K 1] Kamienny, S.: Torsion points on Elliptic Curves over all quadratic fields, Duke Math. J **53** (1986) 157-162

[K 2] Kamienny, S.: Torsion points on Elliptic Curves over all quadratic fields II, Bull. Soc. Math. de France. **114** (1986) 119-122

[K 3] Kamienny, S.: Torsion points on elliptic curves. *Proceedings of the Conference on Number Theory, March 12-15, 1991*, GH Essen Preprint Series (G. Frey, ed.) (1991).

[K 4] Kamienny, S.: Torsion points on elliptic curves over fields of higher degree. *Int. Math. Research Notices* no. **6**, at the end of Duke Math. J. **66** no. 3 (1992) 129-133

[K 5] Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Inv. Math. **109** (1992) 221-229

[K-M] Kenku, M., Momose, F.: Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **109** (1988) 125-149

[Ku] Kubert, D.: Universal bounds on torsion of elliptic curves, Proc. London Math. Soc. (3) **33** (1976) 193-237

[Man] Manin, Y.: A uniform bound for p-torsion in elliptic curves. Izv. Akad. Nauk. CCCP **33** (1969) 459-465

[M 1] Mazur, B.: Rational points on modular curves, in *Modular Functions of one Variable V* Lecture Notes in Math. **601** (1977) 107-148 (Springer-Verlag)

[M 2] Mazur, B.: Modular curves and the Eistenstein ideal, Publ. Math.

IHES **47** (1978) 33-186

[**M 3**] Mazur, B.: Rational isogenies of prime degree, Inv. Math. **44** (1978) 129-162

[**M 4**] Mazur, B.: Kamienny's recent work on torsion in the Mordell-Weil group of elliptic curves over quadratic number fields, Quebec-Vermont Number Theory Seminar Proceedings 1990-1991 pp. 1-7

[**M-T**] Mazur, B., Tate, J.: Points of order 13 on elliptic curves, Inv. Math. **22** (1973) 41-49

[**Mo**] Momose, F.: p-torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **96** (1984) 139-165

[**M-S-Z 1**] Müller, H., Ströher, H., Zimmer, H.: Complete determination of all torsion groups of elliptic curves with integral absolute invariant over quadratic and pure cubic fields, *Number Theory* (J.-M. De Koninck and C. Leveque, eds.) Walter de Gruyer, Berlin-New York, 1989, pp. 671-698

[**M-S-Z 2**] Müller, H., Ströher, H., Zimmer, H.: Torsion groups of elliptic curves with integral absolute invariant over quadratic fields, J. Reine Angew. Math. **397** (1989) 100-161

[**O 1**] Ogg, A.: Diophantine equations and modular forms, Bull. A.M.S. **81** (1975) 14-27

[**R**] Reichert, M.A.: Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, Math. Comp. **46** (1986) 637-658

[**S 1**] Serre, J.-P.: p-torsion des courbes elliptiques [d'après Y. Manin] pp. 281-294 in *Séminaire Bourbaki* 1969/70 exp. 380 Lecture Notes in Math **180** (1971) Springer-Verlag

[**S 2**] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. **15** (1972) 259-331

Barry Mazur
Department of Mathematics
Harvard University
Cambridge, MA 02138

Sheldon Kamienny
Department of Mathematics
University of Southern California
Los Angeles, CA 90089