Séminaire BOURBAKI Mars 1994
46ème année, 1993-94, n° 782

RATIONAL TORSION POINTS ON ELLIPTIC CURVES OVER NUMBER FIELDS
[after Kamienny and Mazur]

by **Bas EDIXHOVEN**

1. INTRODUCTION

Let E be an elliptic curve over a number field K. In other words, K is a finite field extension of $\mathbf{Q}$ and E is a non-singular algebraic curve in the projective plane $\mathbf{P}^2_K$ over K given by an equation of the form $y^2z = x^3 + axz^2 + bz^3$, with a, b in K such that $4a^3 + 27b^2 \neq 0$. For each field extension L of K, we denote by $E(L)$ the set of L-rational points of E; the point $(0, 1, 0)$ in $E(K)$ will be denoted by 0_E. It is well known that the sets $E(L)$ have a unique stucture of abelian group with 0_E as origin, such that $P_1 + P_2 + P_3 = 0_E$ whenever P_1, P_2 and P_3 are the three intersection points (counted with multiplicity) of E with a straight line. For example, $E(\mathbf{C})$ is isomorphic to a group of the form $\mathbf{C}/\Lambda$ with Λ a lattice in $\mathbf{C}$. This already shows that the torsion subgroup $E(\mathbf{C})_{\mathrm{tors}}$ of $E(\mathbf{C})$ is isomorphic to $\mathbf{Q}/\mathbf{Z} \times \mathbf{Q}/\mathbf{Z}$.

The theorem of Mordell-Weil states that $E(K)$ is finitely generated, hence isomorphic to $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \mathbf{Z}^r$ with $n_1|n_2$, $n_1 > 0$, $n_2 > 0$ and $r \geq 0$. The pair (n_1, n_2) is the isomorphism type of $E(K)_{\mathrm{tors}}$; the integer r is called the rank of $E(K)$.

1.1. Conjecture. *For every integer $d \geq 1$ there exists an integer B_d such that for every number field K of degree d (over $\mathbf{Q}$) and every elliptic curve E over K one has: $|E(K)_{\mathrm{tors}}| < B_d$.*

This conjecture is known as the strong uniform boundedness conjecture, the word "strong" meaning that the bound is uniform in all number fields of degree d.

Let us introduce some notation. For $d \geq 1$ we define $\Phi(d)$ to be the set of isomorphism types of the groups $E(K)_{\mathrm{tors}}$ with E an elliptic curve over a number field K with $[K : \mathbf{Q}] = d$. We define $S(d)$ to be the set of primes p for which there exists an elliptic curve E over a number field K with $[K : \mathbf{Q}] = d$ and $|E(K)_{\mathrm{tors}}|$ divisible by p. With this terminology, Conjecture 1.1 is clearly equivalent to the statement that for all d, $\Phi(d)$ is a finite set. The results obtained by Kamienny and Mazur can now be stated as follows.

1.2. Theorem. [1]

1. *For $d \leq 8$ the set $\Phi(d)$ is finite (Kamienny [8], see also [9]).*
2. *The sets $S(d)$ have density zero for all d ([9]).*
3. *$\Phi(d)$ is finite if and only if $S(d)$ is finite ([9]).*

Furthermore, the sets $S(1)$, $S(2)$, $\Phi(1)$ and $\Phi(2)$ are known:

$$\begin{aligned}
\Phi(1) &= \{(1,m) \,|\, 1 \leq m \leq 10\} \cup \{(1,12)\} \cup \{(2,2m) \,|\, 1 \leq m \leq 4\} \\
\Phi(2) &= \{(1,m) \,|\, 1 \leq m \leq 16\} \cup \{(1,18)\} \cup \{(2,2m) \,|\, 1 \leq m \leq 6\} \cup \\
&\quad\ \{(3,3m) \,|\, 1 \leq m \leq 2\} \cup \{(4,4)\}
\end{aligned}$$

The set $\Phi(1)$ was determined by Mazur [17] in 1976, see also [18], using results of Kubert [13]. This result was at that time known as a conjecture of Ogg ([22]), but in fact it had already been conjectured by B. Levi ([15]) in 1908 (see a forthcoming article by Schappacher and Schoof). The determination of $\Phi(2)$ uses work of Kamienny, Kenku and Momose (see [11]). Part 3 of Theorem 1.2 is an easy consequence of a result of Frey (1992), which in turn is an easy consequence of a theorem of Faltings (see §6). A "local" version of the uniform boundedness conjecture was proved by Manin in 1969: he showed that for any number field K and any prime p there exists an integer $e \geq 0$ such that no elliptic curve over K has a rational point of order p^e (see [16] and [23]).

[1] See §7 for more recent results. In particular, Conjecture 1.1 is now a theorem of Merel.

2. RELATION WITH OTHER CONJECTURES

It is easily seen that the ABC-conjecture for a number field K implies a uniform bound for $|E(K)_{\mathrm{tors}}|$ (see [4]). The same is true for the height conjecture for elliptic curves over K (see [4]). Instead of considering elliptic curves over number fields of degree d, one might consider abelian varieties over $\mathbf{Q}$ of dimension d. Restriction of scalars à la Weil shows that Conjecture 1.1 is a consequence of:

2.1. Conjecture. *For every $d \geq 0$ there exists an integer B'_d with the property that $|A(\mathbf{Q})_{\mathrm{tors}}| < B'_d$ for all d-dimensional abelian varieties over $\mathbf{Q}$.*

It seems almost nothing is known about this conjecture, see [24] and references therein.

3. MAZUR'S METHOD FOR THE NUMBER FIELD Q

Let E be an elliptic curve over a number field K and $P \in E(K)$ a point of prime order N. Let $\mathcal{O}_K$ be the ring of integers of K and let $\mathbf{F}_q$ (q some prime power) be a residue field of $\mathcal{O}_K$. Let $\widetilde{E}$ be the fibre over $\mathbf{F}_q$ of the Néron model of E, and let $\widetilde{P}$ in $\widetilde{E}(\mathbf{F}_q)$ be the reduction of P. Suppose that N does not divide q. Then elementary theory of group schemes shows that $\widetilde{P}$ has order N. Now $\widetilde{E}$ is of one of the following three types:

good reduction: $\widetilde{E}$ is an elliptic curve over $\mathbf{F}_q$, hence $|\widetilde{E}(\mathbf{F}_q)| \leq (q^{1/2}+1)^2$, so $N \leq (q^{1/2}+1)^2$;

additive reduction: there is an exact sequence $0 \to \mathbf{G}_{\mathrm{a},\mathbf{F}_q} \to \widetilde{E} \to \Phi \to 0$ with $|\Phi(\mathbf{F}_q)| \leq 4$; since $\mathbf{G}_{\mathrm{a},\mathbf{F}_q}(\mathbf{F}_q) \cong \mathbf{F}_q$, one has $N \leq 3$;

multiplicative reduction: there is an exact sequence $0 \to T \to \widetilde{E} \to \Phi \to 0$ with $T = \mathbf{G}_{\mathrm{m},\mathbf{F}_q}$ or $T = \widetilde{\mathbf{G}_{\mathrm{m},\mathbf{F}_q}}$ (the unique non-trivial twist) and $\Phi(\mathbf{F}_q) = \mathbf{Z}/n\mathbf{Z}$ for some n, so in this case one has $N|(q-1)$ or $N|(q+1)$ or $N|n$.

We conclude that in order to prove that $S(1) \subset \{2,3,5,7,13\}$, it suffices to prove that an elliptic curve over $\mathbf{Q}$ with a point of prime order $N \notin \{2,3,5,7,13\}$ does not have multiplicative reduction at 3.

So let us suppose that we have $P \in E(\mathbf{Q})$ of prime order N with N not in $\{2,3,5,7,13\}$. Our goal is now to show that E does not have multiplicative reduction at 3 (actually, with a bit more work one can show that E has potentially good reduction at all $p \geq 3$). The idea of the proof is to interpret (E,P) as a $\mathbf{Q}$-rational point of some moduli space, and to study the reduction of that point modulo 3.

Let $X_0(N)$ be the coarse moduli space of generalized elliptic curves equipped with a subgroup scheme of rank N which meets all irreducible components in all geometric fibres ([2], [10]). It is known that $X_0(N)$ is a projective curve over $\mathrm{Spec}(\mathbf{Z})$, smooth over $\mathbf{Z}[1/N]$. Its fibre $X_0(N)_{\mathbf{F}_N}$ over $\mathbf{F}_N$ has two irreducible components which are both smooth, of genus zero and which intersect transversally in the so-called supersingular points. The genus of $X_0(N)$ is roughly $N/12$ and the condition $N \notin \{2,3,5,7,13\}$ means precisely that $X_0(N)$ has positive genus. By construction, a pair $(E/S, G)$ with E an elliptic curve over a scheme S and G a subgroup scheme of rank N of E gives an S-valued point of $X_0(N)$. Points of $X_0(N)$ with values in an algebraically closed field k correspond to isomorphism classes of objects $(E/k, G)$. The Riemann surface $X_0(N)(\mathbf{C})$ can be obtained by adding two points (called the cusps 0 and ∞) to $\Gamma_0(N)\backslash\mathbf{H}$ (the quotient of the upper half plane by the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbf{Z})$). The cusp ∞ corresponds to a projective line with its points 0 and ∞ identified, equipped with its subgroup μ_N. The cusp 0 corresponds to an N-gon of projective lines, equipped with a subgroup $\mathbf{Z}/N\mathbf{Z}$ meeting all N projective lines. In fact 0 and ∞ give $\mathbf{Z}$-valued points of $X_0(N)$; the complement of 0 and ∞ is the moduli space for elliptic curves with a subgroup scheme of rank N.

Let $J_0(N)$ be the Néron model over $\mathbf{Z}$ of the jacobian of $X_0(N)_{\mathbf{Q}}$. Its restriction to $\mathbf{Z}[1/N]$ is an abelian scheme whose fibres have dimension equal to the genus of $X_0(N)$. The points of $J_0(N)$ with values in a field k of characteristic different from N correspond to divisor classes of degree zero on $X_0(N)_k$, modulo principal divisors. The fibre over $\mathbf{F}_N$ of $J_0(N)$ sits in an exact sequence

$$0 \to \text{torus} \to J_0(N)_{\mathbf{F}_N} \to \mathbf{Z}/n\mathbf{Z} \to 0, \qquad n = \mathrm{num}\left(\frac{N-1}{12}\right)$$

with the group $\mathbf{Z}/n\mathbf{Z}$ generated by the reduction mod N of the point c in $J_0(N)(\mathbf{Q})$ of order n given by the divisor class $c = (0) - (\infty)$.

Let $\mathbf{T}$ be the endomorphism ring of $J_0(N)$; it is generated by the Hecke operators T_p ($p \neq N$ prime) and the Atkin-Lehner involution w_N. It will be convenient to work with the Hecke operators T_m for all $m \geq 1$; these are defined as follows: $T_N = -w_N$ and one formally has the Euler product:

$$\left(1 - T_N N^{-s}\right)^{-1} \prod_{l \neq N} \left(1 - T_l l^{-s} + l^{1-2s}\right)^{-1} = \sum_{m \geq 1} T_m m^{-s}$$

If one interprets $\mathrm{H}^0(J_0(N)_{\mathbf{C}}, \Omega^1) = \mathrm{H}^0(X_0(N)_{\mathbf{C}}, \Omega^1)$ as the space of cuspidal modular forms of weight two on $\Gamma_0(N)$ and uses q-expansions, these operators are given by the usual formulas. This implies that the coefficient of q^m of an eigenform with eigenvalue a_m for T_m, equals a_m times the coefficient of q. The ring $\mathbf{T}$ is commutative, reduced, free of rank $\dim(J_0(N)_{\mathbf{Q}})$ as $\mathbf{Z}$-module. The $\mathbf{Q}$-algebra $\mathbf{Q} \otimes \mathbf{T}$ is a product of totally real fields and $\mathrm{Spec}(\mathbf{T})$ is connected. For each prime number $p \neq N$ one has the Eichler-Shimura identity in $\mathrm{End}_{\mathbf{F}_p}(J_0(N)_{\mathbf{F}_p})$:

$$T_p = \mathrm{Frob}_p + \mathrm{Ver}_p, \qquad \text{where } \mathrm{Frob}_p \mathrm{Ver}_p = \mathrm{Ver}_p \mathrm{Frob}_p = p$$

Weil's theorem on the eigenvalues of Frobenius endomorphisms of abelian varieties then implies that for any homomorphism $\phi\colon \mathbf{T} \to \mathbf{C}$ and for any prime $p \neq N$, one has $|\phi(T_p)| \leq 2p^{1/2}$.

The action of $\mathbf{T}$ on c is as follows: $T_p(c) = (p+1)c$ for all primes $p \neq N$, and $w_N(c) = -c$. Let $I \subset \mathbf{T}$ be the annihilator of c. It follows that $\mathbf{T}/I = \mathbf{Z}/n\mathbf{Z}$ and that I is generated by the $T_p - p - 1$ ($p \neq N$ prime), $w_N + 1$ and n (actually one doesn't need n). The ideal $I \subset \mathbf{T}$ is called the Eisenstein ideal because it corresponds to congruences between cuspidal forms and non-cuspidal forms on $\Gamma_0(N)$ of weight two ([17], page 37).

Let $\mathbf{T}_I := \varprojlim \mathbf{T}/I^m$ be the I-adic completion of $\mathbf{T}$. The ideal γ_I of $\mathbf{T}$ is then defined to be the kernel of the map $\mathbf{T} \to \mathbf{T}_I$. In other words, γ_I is the intersection of the minimal prime ideals $\mathbf{p}$ of $\mathbf{T}$ with $\mathbf{p} + I \neq \mathbf{T}$. Phrased differently: $\mathrm{Spec}(\mathbf{T}/\gamma_I)$ is the union of the irreducible components of $\mathrm{Spec}(\mathbf{T})$ that have non-empty intersection with $\mathrm{Spec}(\mathbf{T}/I)$.

Let $\gamma_I J_0(N)_{\mathbf{Q}}$ be the abelian subvariety of $J_0(N)_{\mathbf{Q}}$ generated by the $tJ_0(N)_{\mathbf{Q}}$, $t \in \gamma_I$. The Eisenstein quotient $J_{\mathbf{Q}}$ is then defined by: $J_{\mathbf{Q}} := J_0(N)_{\mathbf{Q}}/\gamma_I J_0(N)_{\mathbf{Q}}$. Let J be its Néron model over $\mathbf{Z}$. By construction, $\mathbf{T}/\gamma_I$ acts faithfully on J. The following theorem is one of the main results of [17] (see also [19]).

3.1. Theorem (Mazur). *The group $J(\mathbf{Q})$ is torsion, and in fact, $J(\mathbf{Q})$ is generated by c, hence cyclic of order n.*

Let $X_0(N)^{\mathrm{sm}} \subset X_0(N)$ be the biggest open part which is smooth over $\mathbf{Z}$ (i.e., $X_0(N)^{\mathrm{sm}}$ is the complement of the set of double points in characteristic N). The points 0 and ∞ in $X_0(N)(\mathbf{Z})$ are in fact in $X_0(N)^{\mathrm{sm}}(\mathbf{Z})$. Let $X_0(N)^{\mathrm{sm}} \to J_0(N)$ be the usual embedding of a curve in its jacobian, normalized by the condition that ∞ is sent to 0. By composition with the canonical map $J_0(N) \to J$ we get a morphism $f\colon X_0(N)^{\mathrm{sm}} \to J$.

3.2. Theorem (Mazur). *(See [18].) The morphism f is a formal immersion at ∞, away from characteristic 2. In other words, the cotangent space $\mathrm{Cot}_0(J_{\mathbf{Z}[1/2]})$ of $J_{\mathbf{Z}[1/2]}$ at 0 maps surjectively to $\mathrm{Cot}_\infty(X_0(N)_{\mathbf{Z}[1/2]})$, or equivalently, for each prime $p \neq 2$ the map from $\mathrm{Cot}_0(J_{\mathbf{F}_p})$ to $\mathrm{Cot}_\infty(X_0(N)_{\mathbf{F}_p})$ is non-zero.*

Proof. The hypothesis that p is not equal to 2 implies that $\mathrm{Cot}_0(J_{\mathbf{F}_p})$ maps injectively to $\mathrm{Cot}_0(J_0(N)_{\mathbf{F}_p})$. Because $J_0(N)$ is a (commutative) group scheme, we have a canonical isomorphism $\Omega^1_{J_0(N)/\mathbf{Z}} \cong \pi^*\mathrm{Cot}_0(J_0(N))$ ($\pi\colon J_0(N) \to \mathrm{Spec}(\mathbf{Z})$), inducing $\mathrm{Cot}_0(J_0(N)) \cong \mathrm{H}^0(J_0(N), \Omega^1_{J_0(N)/\mathbf{Z}})$. Composing with the pullback of differential forms along f gives an isomorphism:

$$\mathrm{Cot}_0(J_0(N)) \cong \mathrm{H}^0(J_0(N), \Omega^1_{J_0(N)/\mathbf{Z}}) \xrightarrow{\sim} \mathrm{H}^0(X_0(N)^{\mathrm{sm}}, \Omega^1_{X_0(N)/\mathbf{Z}}) = S(N,2)$$

where $S(N,2)$ is the $\mathbf{Z}$-module of cusp forms over $\mathbf{Z}$ of weight two on $\Gamma_0(N)$. With this identification, the map $\mathrm{Cot}_0(J_0(N)) \to \mathrm{Cot}_\infty(X_0(N))$ corresponds to evaluating at ∞. The Tate curve over $\mathbf{Z}((q))$ shows that dq is a $\mathbf{Z}$-basis of $\mathrm{Cot}_\infty(X_0(N))$; the q here can be interpreted as the function $z \mapsto \exp(2\pi i z)$ on the upper half plane $\mathbf{H}$. So finally we see that the map on cotangent spaces corresponds to the map:

$$S(N,2) \to \mathbf{Z}, \qquad \left(\sum_{m\geq 1} a_m q^m\right)(dq)/q \mapsto a_1$$

Let $p > 2$ and let $\omega \neq 0$ be an eigenvector for $\mathbf{T}$ in $\mathrm{Cot}_0(J_{\overline{\mathbf{F}}_p})$. Since $p > 2$, ω has non-zero image in $S(N,2)_{\mathbf{F}_p}$; this image is an eigenvector for $\mathbf{T}$, hence it has $a_1 \neq 0$. □

With all this, we can finish Mazur's proof that the elliptic curve E does not have multiplicative reduction at 3. So suppose that E has multiplicative reduction at 3. Since $N \geq 11 > 3{+}1$, $\widetilde{P}$ in $\widetilde{E}(\mathbf{F}_3)$ has non-zero image in $\Phi(\mathbf{F}_3)$. This means that the $\mathbf{Q}$-rational point $(E/\mathbf{Q}, \langle P\rangle)$ of $X_0(N)$ specializes to the cusp 0 modulo 3. Let x be the $\mathbf{Q}$-rational point corresponding to $(E/\langle P\rangle, E[N]/\langle P\rangle)$; then x specializes to ∞ modulo 3. We consider $f(x) \in J(\mathbf{Q})$. By Thm. 3.1, $f(x)$ is torsion. By Thm. 3.2, $f(x)$ is not zero (this can be seen in the completion of $X_0(N)$ along ∞). But this is in contradiction with the following lemma, whose proof is an elementary calculation with formal groups.

3.3. Lemma. *Let R be a discrete valuation ring of characteristic* 0 *and with residue field k of characteristic p. Let G be a smooth group scheme over R. Let $x \in G(R)$ be torsion. Suppose that the valuation of p is strictly less than $p-1$. Then the specialization x_k has the same order as x.*

4. KAMIENNY'S GENERALIZATION OF MAZUR'S METHOD

Let $d \geq 1$, K a number field of degree d, E an elliptic curve over K and $P \in E(K)$ a point of prime order N. Let $y \in X_0(N)(K)$ be the point corresponding to $(E/\langle P\rangle, E[N]/\langle P\rangle)$. The idea is now to look at the $\mathbf{Q}$-rational point $x := \sum_\sigma \sigma(y)$, with $\sigma\colon K \to \mathbf{C}$, of the dth symmetric power $X_0(N)^{(d)}$ of $X_0(N)$. By definition, $X_0(N)^{(d)}$ is the quotient by the symmetric group S_d acting on the dth power $X_0(N)^d$. Hence $X_0(N)^{(d)}$ is proper over $\mathbf{Z}$, smooth of relative dimension d over $\mathbf{Z}[1/N]$. To give a k-valued point of $X_0(N)^{(d)}$, where k is a perfect field, is the same as giving an effective divisor of degree d on $X_0(N)_k$.

Let $f_d\colon X_0(N)^{(d)}_{\mathbf{Z}[1/N]} \to J_{\mathbf{Z}[1/N]}$ be the usual map from the symmetric product of a curve to its jacobian, normalized by the condition that $d{\cdot}\infty$ is sent to 0. We apply Mazur's method to x and f_d.

Suppose $p > 2$ is a prime such that $N > (p^{d/2}+1)^2$. Then at each residue field of $\mathcal{O}_K$ of characteristic p, E has multiplicative reduction, and $\widetilde{P}$ has non-zero image in Φ; in other words, all specializations to characteristic p of the K-valued point y of $X_0(N)$ are ∞. This means that x specializes to $d{\cdot}\infty$ modulo p. If moreover f_d is a formal immersion at the point $d{\cdot}\infty$ modulo p, then we obtain a contradiction as before: $f_d(x)$ is torsion, $f_d(x)$ is not zero and $f_d(x)$ specializes to 0 modulo p. These arguments prove the following proposition.

4.1. Proposition. *Let $d \geq 1$, $N \in S(d)$ and suppose that f_d is a formal immersion at $d{\cdot}\infty$ modulo a prime $p > 2$. Then $N \leq (p^{d/2} + 1)^2$.* □

Recall that $X_0(N)$ has a formal local coordinate q at ∞. Hence $X_0(N)^d$ has formal local coordinates $q_1, \ldots, q_d$ at $(\infty, \ldots, \infty)$. The elementary symmetric functions $\sigma_1 = q_1 + \cdots + q_d, \ldots, \sigma_d = q_1 \cdots q_d$ are then formal local coordinates of $X_0(N)^{(d)}$ at $d{\cdot}\infty$, so $d\sigma_1, \ldots, d\sigma_d$ is a $\mathbf{Z}$-basis for $\mathrm{Cot}_{d\cdot\infty}(X_0(N)^{(d)})$.

4.2. Lemma. *Let ω be in $\mathrm{Cot}_0(J)$, or, equivalently, in $\mathrm{H}^0(J, \Omega^1_{J/\mathbf{Z}})$. Then $f_1^*(\omega)$ is a differential form on $X_0(N)_{\mathbf{Z}[1/N]}$, say with q-expansion $(\sum_{m\geq 1} a_m q^m)(dq)/q$. We have:*

$$f_d^*(\omega) = a_1 d\sigma_1 - a_2 d\sigma_2 + \cdots + (-1)^{d+1} a_d d\sigma_d \qquad \textit{in } \mathrm{Cot}_{d\cdot\infty}(X_0(N)^{(d)}_{\mathbf{Z}[1/N]}).$$

Proof. Let $g\colon X_0(N)^d \to X_0(N)^{(d)}$ be the canonical map. For $m \geq 1$ define $s_m = q_1^m + \cdots + q_d^m$. Then

$$g^* f_d^*(\omega) = \sum_{i=1}^{d} \sum_{m\geq 1} a_m q_i^m \, (dq_i)/q_i = \sum_{m\geq 1} a_m m^{-1} ds_m$$

From Newton's identities

$$s_m - \sigma_1 s_{m-1} + \cdots + (-1)^{m-1}\sigma_{m-1} s_1 + (-1)^m m \sigma_m = 0$$

one sees that

$$m^{-1} ds_m = (-1)^m d\sigma_m \qquad \text{in } \mathrm{Cot}_{d\cdot\infty}(X_0(N)^{(d)}).$$

This finishes the proof. □

4.3. Theorem (Kamienny's criterion). *Let $d \geq 2$ and $N \in S(d)$. Suppose that the images $T_1', \ldots, T_d'$ in $\mathbf{T}/\gamma_I$ of $T_1, \ldots, T_d \in \mathbf{T}$ are linearly independent. Then $N \leq 2^{d+1}(d!)^{5d/2}$.*

Proof. By the q-expansion principle, $\mathrm{Tan}_0(J_0(N))$ is a locally free $\mathbf{T}$-module of rank 1. Since $\mathbf{Q}\otimes\mathbf{T}$ is a product of fields, $\mathbf{Q}\otimes S(N,2)$ is a free $\mathbf{Q}\otimes\mathbf{T}$-module of rank 1. It follows that $\mathbf{Q}\otimes S(N,2)[\gamma_I]$ (forms annihilated by γ_I) is a free module of rank 1 over $\mathbf{Q}\otimes(\mathbf{T}/\gamma_I)$. Let $\omega_1,\ldots,\omega_r$ be a basis of $\overline{\mathbf{Q}}\otimes S(N,2)[\gamma_I]$ consisting of normalized eigenforms for $\mathbf{T}$, and write $\omega_i=\sum_{m\geq 1}a_{i,m}q^m(dq)/q$ (normalized means that $a_{i,1}=1$ for all i). Let $R\subset\overline{\mathbf{Q}}$ be the ring generated by the $a_{i,m}$. Then, as a $\mathbf{Z}$-module, R is free of some rank t, say. The hypothesis that $T_1',\ldots,T_d'$ are linearly independent means that the $(a_{i,1},\ldots,a_{i,d})$, $1\leq i\leq r$, generate the $\overline{\mathbf{Q}}$-vector space $\overline{\mathbf{Q}}^d$. Note that Lemma 4.2 implies that $f_d\colon X_0(N)^{(d)}_{\mathbf{Q}}\to J_{\mathbf{Q}}$ is a formal immersion at $d{\cdot}\infty$.

Exactness properties of Néron models show that the torsion of the quotient $\mathrm{Cot}_0(J_0(N))/\mathrm{Cot}_0(J)$ is killed by 2 (compare [18], Cor. 1.1). Hence $\omega_1,\ldots,\omega_r$ can be viewed as elements of $R[1/2]\otimes\mathrm{Cot}_0(J)$.

After renumbering, we may suppose that $\Delta:=\det(a_{i,m})_{1\leq i,m\leq d}$ is non-zero. Recall that for all embeddings $R\to\mathbf{C}$ and all prime numbers $l\neq N$ one has $|a_{i,l}|\leq 2l^{1/2}$, and that $a_{i,N}=\pm1$. For arbitrary m one has $|a_{i,m}|\leq\sigma_0(m)m^{1/2}$, where $\sigma_0(m)$ is the number of positive divisors of m. Hence for the norm of Δ one has:

$$|N(\Delta)|\leq\Big(d!\cdot(d!)^{1/2}\sigma_0(2)\cdots\sigma_0(d)\Big)^t\leq(d!)^{5t/2}$$

Suppose now that $p>2$ is a prime such that f_d is not a formal immersion at ∞ modulo p. Then p divides the index of $f_d^*\mathrm{Cot}_0(J)$ in $\mathrm{Cot}_{d\cdot\infty}(X_0(N)^{(d)})$. It follows that there is an $\alpha\in R$ such that $\Delta=p\alpha$, hence also $|N(\Delta)|=p^t|N(\alpha)|\geq p^t$. We conclude that $p\leq(d!)^{5/2}$.

Let p be a prime between $(d!)^{5/2}$ and $2(d!)^{5/2}$; then f_d is a formal immersion at ∞ modulo p. Prop. 4.1 implies that $N\leq(p^{d/2}+1)^2\leq 2^{d+1}(d!)^{5d/2}$. $\square$

We end this section with some remarks. First of all, the difficulty with Kamienny's criterion is that one needs to know whether $T_1',\ldots,T_d'$ are linearly independent or not. The question of linear dependence of $T_1,\ldots,T_d$ in $\mathbf{T}$ itself is easily settled: let $g:=\dim(J_0(N)_{\mathbf{Q}})$, then $T_1,\ldots,T_g$ are linearly independent in $\mathbf{T}$. To prove this (optimal) result, one remarks that it is equivalent to ∞ not being a Weierstrass point on $X_0(N)_{\mathbf{Q}}$. Reduction modulo N shows that ∞ is not a Weierstrass point (one finds a Vandermonde determinant, see also [14]).

Secondly, let us consider the case $d = 2$. We want to know the primes N for which T_1' and T_2' are linearly independent. Since T_1' is the identity, the question is whether T_2' acts as a scalar on J or not, so suppose that T_2' acts as a scalar. Weil's bound implies that $T_2' \in \{-2, -1, 0, 1, 2\}$. But on the other hand we have $T_2' = 2{+}1$ modulo n (consider the image of T_2' in $\mathbf{T}/I = \mathbf{Z}/n\mathbf{Z}$). It follows that $(N-1)/12 \leq \mathrm{num}((N-1)/12) = n \leq 5$, hence that $N \leq 61$. So Conjecture 1.1 is now proved for $d = 2$. The bounds given in Theorem 4.3 can be improved in this case: the proof shows that for $N > 61$ the map $f_2\colon X_0(N)^{(2)} \to J$ is a formal immersion at ∞ modulo 7, so that $N \in S(2)$ implies $N \leq ((7^2)^{1/2} + 1)^2 = 64$. To go further, one has to do explicit calculations for the $N \leq 61$. For example, by calculating the characteristic polynomial of T_2 acting on the space of weight two cusp forms on $\Gamma_0(N)$ one sees that T_2' does not acts as a scalar modulo 5 for $N = 43$, 53 and 61, which means that these three N are not in $S(2)$.

5. WINDING HOMOMORPHISMS AND FUGITIVE SETS

In order to prove that the sets $S(d)$ are finite for $d \leq 8$ and, for all d, have density zero, it suffices, in view of Theorem 4.3, to prove that the set of primes N such that $T_1', \ldots, T_d'$ are linearly dependent is finite for $d \leq 8$ and has density zero for all d. The following lemma shows that to check whether $T_1', \ldots, T_d'$ are linearly independent or not (for a given N), it suffices to check a finite set of relations; this set of relations is independent of N.

5.1. Lemma. *Let $d \geq 1$, let N be a prime and suppose that $T_1', \ldots, T_d'$ are linearly dependent. Consider a non-trivial relation*

$$a_1 T_1' + \cdots + a_d T_d' = 0, \qquad a_1, \ldots, a_d \text{ in } \mathbf{Z}$$

which is minimal in the following sense: there is no non-trivial relation among $T_1', \ldots, T_d'$ with more coefficients equal to zero, and $a_1, \ldots, a_d$ have greatest common divisor equal to 1. Then $|a_i| \leq ((d-1)!)^{5/2}$ for all i.

Proof. Let $a_{i_1}, \ldots, a_{i_{r+1}}$ be the a_i which are non-zero. We rewrite the equation as:

$$-a_{i_{r+1}} T'_{i_{r+1}} = a_{i_1} T'_{i_1} + \cdots + a_{i_r} T'_{i_r}$$

Recall that $\mathbf{Q}\otimes\mathbf{T}$ is a product of totally real fields. Hence $\mathbf{R}\otimes\mathbf{T}/\gamma_I$ is canonically isomorphic (as $\mathbf{R}$-algebra) to $\mathbf{R}^e$, where $e = \dim(J_{\mathbf{Q}})$. This gives an embedding $\mathbf{T}/\gamma_I \hookrightarrow \mathbf{R}^e$; let $v_i = (v_{i,1}, \ldots, v_{i,e})$ denote the image of T'_i. Then, by Weil's bound, we have $|v_{i,j}| \leq i^{3/2}$ for all i and j. Since $T'_{i_1}, \ldots, T'_{i,r}$ are linearly independent, there exist $j_1, \ldots, j_r$ in $\{1, \ldots, e\}$ such that $\Delta := \det(v_{i_k,j_l})_{1\leq k,l\leq r}$ is not zero. Let R be the subring of $\mathbf{R}$ generated by all $v_{i,j}$. Then, as a $\mathbf{Z}$-module, R is free of some rank t, say. Let $\overline{R}$ denote $R/a_{i_{r+1}}R$. Then in $\overline{R}^e$ we have the relation:

$$0 = \overline{a}_{i_1}\overline{v}_{i_1} + \cdots + \overline{a}_{i_r}\overline{v}_{i_r}$$

and $\overline{a}_{i_1}\overline{R} + \cdots + \overline{a}_{i_r}\overline{R} = \overline{R}$ since $a_{i_1}, \ldots, a_{i_{r+1}}$ have greatest common divisor equal to 1. It follows that $v_{i_1} \wedge \cdots \wedge v_{i_r}$ has image 0 in $\bigwedge^r(\overline{R}^e)$, hence Δ has image zero in $\overline{R}$ (it is one of the "coordinates" of $v_{i_1} \wedge \cdots \wedge v_{i_r}$). Hence we have $\Delta = a_{i_{r+1}}\Delta'$ for some Δ' in R. It follows that $|N(\Delta)| \geq |a_{i_{r+1}}|^t$. As in the proof of Theorem 4.3 one shows that $|N(\Delta)| \leq ((d-1)!)^{5t/2}$, hence the result. $\square$

Remark. Applying Siegel's lemma (which gives an upper bound for the smallest non-trivial solution of a system of linear equations with coefficients in $\mathbf{Z}$) one gets more or less the same estimate.

Recall that, by definition, $\mathbf{T}/\gamma_I$ is the image of $\mathbf{T}$ in its completion $\mathbf{T}_I$. Hence, for $a_1, \ldots, a_d$ in $\mathbf{Z}$, one has $a_1T'_1 + \cdots + a_dT'_d = 0$ if and only if $a_1T_1 + \cdots + a_dT_d$ is in I^m for all m. The finiteness of $S(2)$ was obtained by studying the image of a relation among T_1 and T_2 in $\mathbf{T}/I$. We will now generalize this method and study an arbitrary relation using the filtration $\mathbf{T} \supset I \supset I^2 \supset \cdots$. To do this, it will be convenient not to work with the T_i, but with the η_i in $\mathbf{T}$ defined as follows:

$$\eta_l := T_l - l - 1 \quad \text{for } l \neq N \text{ prime}, \qquad \eta_N := T_N - 1, \qquad \eta_1 := 1, \qquad \eta_{ab} := \eta_a\eta_b.$$

The T_m can be written as linear combinations of the η_k:

$$T_m = \eta_m + \sum_{k<m} c_{m,k}\eta_k,$$

with $c_{m,k}$ in $\mathbf{Z}$. It is important to note that the $c_{m,k}$ with $m < N$ do not depend on N. For all m, let η'_m be the image of η_m in $\mathbf{T}/\gamma_I$. For $m \geq 1$, let $v(m)$ denote the number of factors in a prime factorization of m: if $m = l_1 \cdots l_r$ with the l_i prime, then $v(m) = r$. Note that by definition, we have $\eta_l \in I$ for all primes l, hence for all $m \geq 1$ we have $\eta_m \in I^{v(m)}$.

Suppose now that we have $d \geq 1$ and a prime $N > d$ such that $T'_1 \ldots, T'_d$ are linearly dependent. Then Lemma 5.1 gives a non-trivial relation $b_1\eta'_1 + \cdots + b_d\eta'_d = 0$, with $|b_i| < C(d)$ for all i, where $C(d)$ is an integer depending only on d. We want to show that, for $d \leq 8$, N is bounded, and that in general N lies in a set of primes which has density zero.

Before treating the general case, let us deal with $d \leq 8$, or, what amounts to the same, with $d = 8$. Then we have $b_1, \ldots, b_8$ in $\mathbf{Z}$, $|b_i| \leq C(8)$ for all i, such that the element

$$x := b_1\eta_1 + (b_2\eta_2 + b_3\eta_3 + b_5\eta_5 + b_7\eta_7) + (b_4\eta_2^2 + b_6\eta_2\eta_3) + b_8\eta_2^3$$

of $\mathbf{T}$ is in I^m for all $m \geq 0$. Note that in this expression for x the second term is in I, the third is in I^2 and the fourth is in I^3. Suppose first that $b_1 \neq 0$. Since $b_1 = b_1\eta_1 \in I \cap \mathbf{Z} = n\mathbf{Z}$, one then has $(N-1)/12 \leq n \leq |b_1| \leq C(8)$, hence $N \leq 12C(8)+1$. So we may suppose that $b_1 = 0$. Then $x \in I$, so it will be useful to consider the image of x in I/I^2; this is where Mazur's winding homomorphism comes in.

5.2. Theorem ([17], §18). *Write $N-1 = en$, hence $e = \gcd(N-1, 12)$. Let $\mathbf{F}_N^*[e]$ be the kernel of the eth power endomorphism of $\mathbf{F}_N^*$. There is a unique isomorphism of groups (the winding homomorphism)*

$$w\colon I/I^2 \longrightarrow \mathbf{F}_N^*/\mathbf{F}_N^*[e]$$

which sends η_l to $l^{(l-1)/2}$ for all primes $l \neq N$.

Let $\phi\colon I/I^2 \to \mathbf{F}_N^*$ be the homomorphism defined by $\phi(y) = w(y)^{12}$. Then for all primes $l \neq N$, $\phi(\eta_l) = l^{6(l-1)}$.

Now suppose that b_2, b_3, b_5 and b_7 are not all zero. Then we have:

$$1 = \phi(x) = \left(2^{b_2}3^{2b_3}5^{4b_5}7^{6b_7}\right)^6 \quad \text{in } \mathbf{F}_N^*$$

It follows that N divides the numerator of $(2^{b_2}3^{2b_3}5^{4b_5}7^{6b_7})^6 - 1$, hence N is at most $\exp(127{\cdot}C(8))$. So we may now suppose that b_2, b_3, b_5 and b_7 are zero. Then we have $\eta_2'(b_4\eta_2' + b_6\eta_3' + b_8\eta_4') = 0$. Since η_2' is an isogeny from J to itself (this follows from Weil's bound), we must also have:

$$y := (b_4\eta_2 + b_6\eta_3) + b_8\eta_2^2 \in I^m \quad \text{for all } m \geq 0$$

If b_4 and b_6 are not both zero, we find $N \leq \exp(18{\cdot}C(8))$. If b_4 and b_6 are both zero, then we find $\eta_2' = 0$, which implies that $J = 0$ and hence $N \leq 13$. This finishes the proof that the sets $S(d)$ with $d \leq 8$ are finite. Note, by the way, that the reason the proof works, is that we obtained linear relations among the images of the η_l in I/I^2. This method breaks down for $d = 9$, since then one has to deal with $b_4\eta_2^2 + b_6\eta_2\eta_3 + b_9\eta_3^2$.

In the general case (i.e., d arbitrary) let m be minimal such that not all b_i with $v(i) = m$ are zero. We define $x := \sum_{v(i)=m} b_i\eta_i$; then $x \in I^{m+1}$. We choose an isomorphism of groups $\log\colon \mathbf{F}_N^* \to \mathbf{Z}/(N{-}1)\mathbf{Z}$. The fact (see [17], Thm. 18.10) that $I \subset \mathbf{T}$ is locally principal, implies that we have a homomorphism of groups:

$$\phi_m\colon I^m/I^{m+1} \xrightarrow{\sim} (I/I^2)^{\otimes m} \xrightarrow{\phi^{\otimes m}} (\mathbf{F}_N^*)^{\otimes m} \xrightarrow{\log^{\otimes m}} (\mathbf{Z}/(N{-}1)\mathbf{Z})^{\otimes m} \xrightarrow{\sim} \mathbf{Z}/(N{-}1)\mathbf{Z}$$

(The tensor products are over $\mathbf{Z}$.) We have $\phi_m(x) = 0$. To see what this means, let us first consider $\phi_m(b_i\eta_i)$, where $i = l_1^{e_1}\cdots l_r^{e_r}$ with the l_j prime. One computes that

$$\phi_m(b_i\eta_i) = B_i(\log l_1)^{e_1}\cdots(\log l_r)^{e_r}, \qquad \text{with} \quad B_i = b_i(6(l_1-1))^{e_1}\cdots(6(l_r-1))^{e_r}$$

where we view B_i as an integer. Note that B_i does not depend on N, that B_i does not depend on the choice of $\log\colon \mathbf{F}_N^* \to \mathbf{Z}/(N{-}1)\mathbf{Z}$ and that not all B_i are zero. Let F be the homogenous polynomial of degree m, with coefficients in $\mathbf{Z}$, in the variables X_l, $l \leq d$ prime, whose monomials are the $B_iX_{l_1}^{e_1}\cdots X_{l_r}^{e_r}$, with $v(i) = m$ and $1 \leq i \leq d$. Then the relation $0 = \phi_m(x) = \sum_i b_i\phi_m(\eta_i)$ can be rewritten as $F(\log 2, \log 3, \ldots) = 0$ in $\mathbf{Z}/(N{-}1)\mathbf{Z}$. The set of primes N with the property that $F(\log 2, \log 3, \ldots) = 0$ in $\mathbf{Z}/(N{-}1)\mathbf{Z}$ is called the fugitive set associated to F (note that this does not depend on the choice of the logarithms on the $\mathbf{F}_N^*$). We conclude that the set of primes N such that $T_1', \ldots, T_d'$ are linearly dependent, is contained in a finite union of such fugitive sets. H.W. Lenstra has given an elementary argument, using Cebotarev's theorem, that fugitive sets have density zero. In an appendix to [9], A. Granville improves this result as follows: for $x \in \mathbf{R}$ sufficiently large, the number of primes $N \leq x$ in a fixed fugitive set is bounded by a constant times $(x/\log(x))(\log\log\log(x))/(\log\log(x))$. K. Murty has shown that under the generalized Riemann hypothesis, Granville's bound can be improved to $O((x/\log(x))\log\log(x)/\log(x))$. One expects that the actual size of a fugitive set is $O(\log\log(x))$.

6. AN APPLICATION OF A THEOREM OF FALTINGS

In this section we prove that $S(d)$ is finite if and only if $\Phi(d)$ is finite. We begin by recalling a result of Frey [6].

6.1. Proposition (Frey). *Let K be a number field, $d \geq 0$ an integer and C a smooth projective geometrically irreducible curve over K with $C(K)$ non-empty. Suppose that every non-constant morphism from C to $\mathbf{P}^1_K$ has degree $> 2d$. Then $C^{(d)}(K)$ is finite.*

Proof. Consider the morphism $C^{(d)} \to \mathrm{Pic}^d_C$ which sends an effective divisor D of degree d to the line bundle $\mathcal{O}_C(D)$ of degree d. This map induces an injection on K-rational points, since if $D_1 \neq D_2$ are effective divisors of degree d on C such that $D_1 - D_2$ is a principal divisor (f), then f is a finite morphism of degree $\leq d$ to $\mathbf{P}^1_K$. Let X be the image of $C^{(d)}$ in Pic^d_C. It suffices to show that $X(K)$ is finite. Suppose that $X(K)$ is not finite. Then, by Faltings's theorem [3, Thm. 4.2], there exists a non-zero abelian subvariety B of Pic^0_C with $B(K)$ Zariski-dense in B, and a point P_0 in $X(K)$ such that $P_0 + B \subset X$. For b in $B(K)$, let $P_b := b + P_0 \in X(K)$; let D_b denote the effective divisor on C corresponding to P_b (here we use that $C^{(d)}(K) \to X(K)$ is a bijection). Then for all $b \in B(K)$ the divisors $D_b + D_{-b}$ and $2D_0$ are linearly equivalent. Note that the equality $D_b + D_{-b} = 2D_0$ can happen only for finitely many b, so there exists a b and a non-constant rational function f on C such that $D_b + D_{-b} - 2D_0 = (f)$. But such a f is a morphism from C to $\mathbf{P}^1_K$ of degree at most $2d$. $\square$

6.2. Corollary (Frey, [6]). *Let $d \geq 0$ and $e \geq 0$ be integers, let N be prime and suppose that $N^e \geq 120d$. Then there are, up to isomorphism, only finitely* *many elliptic curves E over $\overline{\mathbf{Q}}$ which have a cyclic isogeny of degree N^e that can be defined over a number field K of degree at most d.*

Proof. Let $f\colon X_0(N^e) \to \mathbf{P}^1_{\mathbf{Q}}$ be a finite morphism. Take $l \in \{2,3\}$, $l \neq N$. Since $X_0(N^e)$ has good reduction at l, the line bundle $f^*\mathcal{O}(1)$ has a unique extension to $X_0(N^e)_{\mathbf{Z}_l}$ and induces a finite morphism $f_l\colon X_0(N)_{\mathbf{F}_l} \to \mathbf{P}^1_{\mathbf{F}_l}$ of degree at most $\deg(f)$. An easy computation shows that $X_0(N^e)(\mathbf{F}_{l^2}) \geq (N{+}1)N^{e-1}/e_l$, where $e_2 = 12$ and $e_3 = 6$ (consider the supersingular points). Hence

$$\deg(f) \geq \deg(f_l) > N^e/(e_l(l^2{+}1) \geq 120d/60 = 2d \qquad \square$$

6.3. Corollary ([9]). *Let $d \geq 1$. If $S(d)$ is finite then $\Phi(d)$ is finite.*

Proof. Instead of giving a proof using Cor. 6.2, we give a proof using a variant of that corollary for the curves $X_1(N^e)$. An advantage of this is that the curves $X_1(N^e)_{\mathbf{Q}}$ are fine moduli spaces for $N^e > 4$.

Let $d \geq 1$ and suppose that $S(d)$ is finite. Since $S(d)$ is finite, it suffices to give, for each N in $S(d)$, an integer $r \geq 0$ such that no elliptic curve over a field of degree d has a rational point of order N^r. So let N be in $S(d)$ and $e \geq 0$. An elliptic curve E over a field K of degree d, together with a rational point P of order N^e, gives a K-valued point of the modular curve $X_1(N^e)$, hence a $\mathbf{Q}$-valued point of the symmetric product $X_1(N^e)^{(d)}$. The curve $X_1(N^e)$ is projective and smooth over $\mathbf{Z}[1/N]$, and has geometrically irreducible fibres. For any field k not of characteristic N, $X_1(N^e)_k$ has at least $(N{-}1)N^{e-1}/2$ rational points (coming from the cusps). It follows that any finite morphism from $X_1(N^e)_{\mathbf{Q}}$ to $\mathbf{P}^1_{\mathbf{Q}}$ has degree at least $(N{-}1)N^{e-1}/8$. Suppose that $e > 1 + \log_N(16d/(N{-}1))$. Then, by Prop. 6.1, $X_1(N^e)^{(d)}(\mathbf{Q})$ is finite. Let $x_1, \ldots, x_m$ be the non-cuspidal closed points of the scheme $X_1(N^e)_{\mathbf{Q}}$ that have non-zero multiplicity in at least one of the finitely many effective divisors on $X_1(N^e)_{\mathbf{Q}}$ corresponding to the elements of $X_1(N^e)^{(d)}(\mathbf{Q})$. Let K_i be the residue field of $X_1(N^e)$ at x_i; then K_i is a field of degree $\leq d$. Note that $N^e > 4$, so $X_1(N^e)_{\mathbf{Q}}$ is a fine moduli space. Hence over each K_i we have an elliptic curve E_i together with a point P_i in $E_i(K_i)$ of order N^e. By construction, these $(E_i/K_i, P_i)$ have the property that all $(E/K, P)$ with E an elliptic curve over K, K of degree d and $P \in E(K)$ of order N^e, can be obtained by extension of scalars from one of the $(E_i/K_i, P_i)$. For each i, choose a residue field k_i of the ring of integers $\mathcal{O}_i$ of K_i such that k_i has characteristic different from N and E_i has good reduction at k_i. Now if $(E/K, P)$ is obtained by extension of scalars from $(E_i/K_i, P_i)$, then $\mathcal{O}_K$ has a residue field k which is an extension of degree at most d of k_i such that E has good reduction at k. Let $\widetilde{E}/k$ be the reduction. Then $|\widetilde{E}(k)| \leq (|k_i|^{d/2}+1)^2$. Now take $r \geq e$ such that for all i one has $N^r > (|k_i|^{d/2}+1)^2$. □

7. BEYOND KAMIENNY AND MAZUR

D. Abramovich [1] has remarked that the hypothesis in Prop. 4.1 that f_d is a formal immersion at $d{\cdot}\infty$ modulo a prime $p > 2$ can be weakened. In fact, all one needs is that $f_d(x) \neq 0$ for all x in $X_0(N)^{(d)}(\mathbf{Q})$ that specialize to $d{\cdot}\infty$ modulo p. Using this remark Abramovich has proved finiteness of $S(d)$ for all $d \leq 14$. For d equal to 13 and 14 his proof uses computer computations.

Very recently (February 11), L. Merel has announced a proof of the finiteness of $S(d)$ for all d. His method is to replace the Eisenstein quotient J of $J_0(N)$ by a bigger quotient J_{w}. This quotient, which he calls the winding quotient, is defined as follows. Integration over $\{it \mid t \in \mathbf{R}_{>0}\} \subset \mathbf{H}$ defines a $\mathbf{C}$-linear form on $\mathrm{H}^0(X_0(N)(\mathbf{C}), \Omega)$. It is known that this form corresponds to an element e in $\mathrm{H}_1(X_0(N)(\mathbf{C}), \mathbf{Q})$. Let $a \subset \mathbf{T}$ be the annihilator of e, then $J_{\mathrm{w},\mathbf{Q}} = J_0(N)_{\mathbf{Q}}/aJ_0(N)_{\mathbf{Q}}$. A result of Kolyvagin and Logachev [12], supplemented by work of Bump, Friedberg and Hoffstein [7], or by work of Murty and Murty [21], shows that $J_{\mathrm{w}}(\mathbf{Q})$ is finite. The condition for $f_d\colon X_0(N)^{(d)}_{\mathbf{Q}} \to J_{\mathrm{w},\mathbf{Q}}$ to be a formal immersion at $d{\cdot}\infty$ is that $T_1e, \ldots, T_de$ are linearly independent in the free $\mathbf{Z}$-module $\mathbf{T}{\cdot}e \subset \mathrm{H}_1(X_0(N)(\mathbf{C}), \mathbf{Q})$. For N sufficiently large with respect to d (to be precise, $N/(\log N)^4$ should be greater than $400d^4$ and greater than d^8), Merel shows this linear independence using the theory of modular symbols.

The text that follows has been added at the time the final version of this text was written (August 1994). Shortly after this exposé, Oesterlé has improved Merel's result: he shows that $N \in S(d)$ implies $N \leq (3^{d/2}+1)^2$. His proof, which follows Merel's proof, shows that for N prime such that $N/(\log N)^4 > (2d)^8$, the images in $(\mathbf{T}{\cdot}e) \otimes \mathbf{F}_3$ of $T_1e, \ldots, T_de$ are $\mathbf{F}_3$-linearly independent, and from that he deduces that the map f_d of §4 (with the Eisenstein quotient replaced by the winding quotient) is a formal immersion at $d{\cdot}\infty$ modulo 3. The proof is then finished by Prop. 4.1 and some extra work for the primes $N < 37$.

Merel's work will appear in [20].

REFERENCES

[1] D. Abramovich. *Formal finiteness and the uniform boundedness conjecture, a footnote to a paper of Kamienny and Mazur.* Preprint March 1993. To appear in an Astérisque volume.

[2] P. Deligne, M. Rapoport. *Les schémas de modules des courbes elliptiques.* In Modular Functions of One Variable II. Springer Lecture Notes in Mathematics 349 (1973).

[3] G. Faltings. *The general case of S. Lang's conjecture.* To appear in "The Barsotti symposium in algebraic geometry", W. Messing and V. Christante, eds. Acad. Press, Cambridge, Mass.

[4] G. Frey. *Links between solutions of $A - B = C$ and elliptic curves.* Number theory, Ulm 1987. Lecture Notes in Mathematics 1380.

[5] G. Frey. *A remark on isogenies of elliptic curves defined over quadratic fields.* Compos. Math. 58, 133-134 (1986).

[6] G. Frey. *Curves with infinitely many points of fixed degree.* Preprint, Institut für Experimentelle Mathematik (1992).

[7] D. Bump, S. Friedberg and J. Hoffstein. *Nonvanishing theorems for L-functions of modular forms and their derivatives.* Invent. Math. 102, 543–618 (1990).

[8] S. Kamienny. *Torsion points on elliptic curves and winding homomorphisms.* MSRI preprint, December 1993.

[9] S. Kamienny, B. Mazur. *Rational torsion of prime order in elliptic curves over number fields.* To appear in an Astérisque volume.

[10] N.M. Katz, B. Mazur. *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies 108, Princeton University Press (1985).

[11] M. Kenku, F. Momose. *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Mathematical Journal 109, 125–149 (1988).

[12] V.A. Kolyvagin, D. Logachev. *Finiteness of the Shafarevich-Tate group and group of rational points for some modular abelian varieties.* Leningrad Math. J. 1, 1229–1253 (1990).

[13] D. Kubert. *Universal bounds on the torsion of elliptic curves.* Proceedings London Math. Soc. (3) 33, 193–237 (1976).

[14] J. Lehner, M. Newman. *Weierstrass points of* $\Gamma_0(N)$. Annals of Mathematics 79, No. 2, 360–368 (1963).

[15] B. Levi. *Sull'equazione indeterminata del* 3^o *ordine.* Atti del IV congresso internazionale dei matematici, Roma, 6–11 Aprile 1908, G. Castelnuovo editor.

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

[17] B. Mazur. *Modular curves and the Eisenstein ideal.* Publications Mathématiques de l'IHES 47, 33–186 (1977).

[18] B. Mazur. *Rational isogenies of prime degree.* Invent. Math. 44, 129–162 (1978).

[19] B. Mazur and J-P. Serre. *Points rationnels des courbes modulaires* $X_0(N)$. Séminaire Bourbaki exp. 469 (1974–1975). Lecture Notes in Mathematics 514, 238–255 (1976).

[20] L. Merel. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* To appear.

[21] M.R. Murty and V.K. Murty. *Mean values of derivatives of modular* L*-series.* Ann. Math. 133, 447–475 (1991).

[22] A. Ogg. *Rational points of finite order on elliptic curves.* Invent. Math. 12, 105–111 (1971).

[23] J-P. Serre. *p-torsion des courbes elliptiques (d'après Y. Manin).* Séminaire Bourbaki exp. 380 (1969–1970). Lecture Notes in Mathematics 180, 281–294 (1971).

[24] A. Silverberg. *Points of finite order on abelian varieties.* Contemporary Mathematics 133, 175–193 (1992).

Bas EDIXHOVEN

Institut Mathématique
URA 305 du CNRS
Campus de Beaulieu
F-35042 Rennes cedex
France