Proceedings of the International Congress of Mathematicians
Vancouver, 1974

# $p$-Adic Analytic Number Theory of Elliptic Curves and Abelian Varieties over $\boldsymbol{Q}$

B. Mazur

The "$p$-adic analytic number theory" alluded to in the title of my article is in a very beginning state: [4], [6], [2]. In different contexts, and from different points of view, p-adic analytic number theory has been the subject of much recent work: "the $p$-adic analytic number theory of totally real number fields" has been developed by Serre [10], using work of Siegel, and more recently by Katz, and Deligne-Ribet; "of quadratic imaginary number fields": by Katz, and Manin; "of modular forms of weight $k \geqq 2$ for the full modular group": by Manin [3]; "of Eichler cohomology classes associated to certain arithmetic groups": being presently worked on by V. Miller.

One exciting aspect of this emerging theory is its sheer difficulty: for example, no matter which elliptic curve $E/\boldsymbol{Q}$ you choose (e.g., $y^2 + y = x^3 + x^2$), its $p$-adic analytic number theory is hard to get to know intimately for *most* primes $p$, either conceptually or computationally.

Nevertheless, for the jacobian of the modular curve $X_0(N)/\boldsymbol{Q}$, there are certain special primes[1] where things are under better control, and for which a more precise picture is beginning to come into view.

One obtains a number of by-products of this picture which are of independent diophantine interest. Notably, as we shall discuss below, one can prove Mordell's conjecture for the curves $X_0(N)$ for prime $N$ over $\boldsymbol{Q}$. For general prime numbers $N$ the "Mordell conjecture" is proven in a bleakly indeterminate form; Ogg and I have been working with (and sharpening) the result, however, and have obtained an actu-

[1] These special primes are not *rational* primes, but rather certain prime ideals in the Hecke algebra, called *Eisenstein primes.*

al determination of the $\boldsymbol{Q}$-rational points of $X_0(N)$ in a great number of cases (see §5).

In this article I shall try to describe some results and (terribly briefly) some methods in the theory of these special (*Eisenstein*) primes, emphasizing questions of diophantine interest. Full results and details will be given in [5].

**1. Arthmetic of elliptic curves over $\boldsymbol{Q}$.** Let $E$ be an elliptic curve defined over $\boldsymbol{Q}$. The following extremely conjectural formula has been a focal point for research concerning the arithmetic of $E/\boldsymbol{Q}$ for about ten years, and will probably continue to be so for some years to come. We shall state this conjectural formula baldly and then we shall recall, rather than define, the terms which intervene:

CONJECTURE OF BIRCH AND SWINNERTON-DYER.

$$|Ш|\cdot R = |M_{\text{tors}}|^2 \cdot \operatorname{Lim}_{s \to 1} \frac{L^*(E,s)}{(s-1)^r} \cdot \prod c_l^{-1}, \qquad l\text{: primes of bad reduction for } E,$$

where $M$ is the *Mordell-Weil* group of $E$: the group $E_{\boldsymbol{Q}}$ of points of $E$ rational over $\boldsymbol{Q}$. This group is a finitely generated abelian group, as proved by Mordell. The finite subgroup $M_{\text{tors}}$ of torsion elements in $M$ is easily computed in any given case. The rank $r$ of the torsion-free quotient of $M$ is not at all easily computable, even in special cases. One may obtain *upper* bounds for $r$ by a difficult, but mechanical, procedure.

$R$ is the regulator of $E/\boldsymbol{Q}$: It is the real number (probably transcendental) which is the discriminant of image$(M) \subset M \otimes \boldsymbol{R}$ computed by means of the inner product structure on $M \otimes \boldsymbol{R}$ coming from the 'canonical height' [12]. Intuitively, it is a measure of the size of the rational coordinates of a basis of the torsion-free part of $M$.

$c_l$ is the number of components of multiplicity one, rational over $\boldsymbol{F}_l$ on the special fiber of Néron's minimal model for $E$ at $l$.

Ш is the *Shafarevitch-Tate group* of $E/\boldsymbol{Q}$: It is often "yoked" to the Mordell-Weil group in the sense that when one tries to obtain information about $M$, it is sometimes the case that one must first deal with Ш, or at least some $p$-primary component of Ш. The group Ш is known to be a torsion group, and is conjectured to be finite. In no case, however, is Ш known to be finite.

$L^*(E, s)$ is the *Hasse-Weil L* series of $E/\boldsymbol{Q}$. See [12] for its appropriate normalization.[2] It is defined as an infinite (Euler) product, and is a Dirichlet series which may be seen to be convergent in the half-plane $\operatorname{Re}(s) > 3/2$. This domain of convergence is totally inadequate for the role played by $L^*(E, s)$ in our above formula. It is conjectured that $L^*(E,s)$ extends to an entire function. This conjecture has been proved in the important (and possibly general) case where $E/\boldsymbol{Q}$ is parametrized by modular forms. We shall make precis ewhat is meant by "parametrized by modular forms", below.

[2] We have allowed *our* normalization to absorb the "real period of the Néron differential", a factor about which we have little to say in this article. Compare our formula with the formula of Conjecture 4(b) of [12].

Note that the conjectured formula implies:

*Weak version of the conjecture.* The rank of (the torsion-free part of) $M$ is the order of zero of $L^*(E, s)$ at $s = 1$.

**2. $p$-adic analytic analogues.** In a recent paper [**6**] Swinnerton-Dyer and I have defined a $p$-adic analytic power series $L_p(E, s) \in \boldsymbol{Z}_p[[s]]$ for any $E/\boldsymbol{Q}$ which is, again, parametrized by modular functions, and any prime $p$ of good, nonsupersingular reduction for $E$.[3] We regard $L_p(E, s)$ as something in the spirit of an *analytic continuation* of $L^*(E, s)$, suitably normalized, *onto the p-adic disc.* In many respects it behaves just like the Hasse-Weil $L$-series of $E/\boldsymbol{Q}$, and we have computational and some theoretical reasons to expect that

CONJECTURE. $L_p(E, s)$ and $L^*(E, s)$ have the same order of zero at $s = 1$.

All one can show at present [**6**] is that $L_p(E, s)$ (when defined) vanishes at $s = 1$ if and only if $L^*(E, s)$ vanishes at $s = 1$. In fact one has a precise formula relating their values.

The $p$-adic $L$-series extends to an analytic function on a disc somewhat larger than the unit disc (call it the *extended* disc) and it is interesting to consider:

(a) the precise power of $p$ which divides $L_p(E, s)$ in $\boldsymbol{Z}_p[[s]]$,

(b) the zeroes (counted with multiplicity) of $L_p(E, s)$ in the extended disc.

Evidence is accumulating which suggests that one may hope for a certain *arithmetical* interpretation of the information contained in (a), (b) which is analogous to the theory of Iwasawa and Kubota-Leopoldt. See [**4**], [**6**].

At the moment, nothing is known about $p$-adic analogues of the regulator $R$. At first it might be reasonable to try to set up such a theory in the case where $E/\boldsymbol{Q}$ has complex multiplication (especially in the light of some recent results of Katz [**1**]).

**3. The modular curves.** For any integer $N \geqq 1$, there is a smooth projective curve defined over $\boldsymbol{Q}$ and usually denoted $X_0(N)$ [**11**]. As a Riemann surface, one has $X_0(N)_{\boldsymbol{C}} = U/\Gamma_0(N) \cup$ cusps where $U$ is the upper half-plane, $\Gamma_0(N) \subset \mathrm{Sl}_2(\boldsymbol{Z})$ is the subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $c \equiv 0 \bmod N$, and $X_0(N)_{\boldsymbol{C}}$ is the compact Riemann surface obtained by adjoining to the quotient $U/\Gamma_0(N) = Y_0(N)$ the *finite* set of cusps.

The structure of $X_0(N)$ *over* $\boldsymbol{Q}$ is related to an important diophantine problem in the theory of elliptic curves over number fields. Namely, if $K$ is a number field in $\boldsymbol{C}$, to any pair $[C_N \subset \underline{E}]$ consisting in an elliptic curve $\underline{E}$ defined over $K$ and a cyclic subgroup $C_N$ of order $N$, rationally defined over $K$ one may associate a noncuspidal point of $X_0(N)$, defined over $K$,

$$[C_N \subset \underline{E}] \mapsto e \in Y_0(N)_K.$$

Moreover, any point of $Y_0(N)_K$ may be obtained in this way,[4] and two pairs $[C_N \subset \underline{E}]$, $[C'_N \subset \underline{E}']$ correspond to the same point of $Y_0(N)_K$ if and only if they are isomorphic over $\boldsymbol{C}$.

[3] At this Congress I learned that Amice and Vélu have a generalization of this theory for the supersingular primes $p$ as well.

[4] See [13] and a forthcoming book of A. Ogg which will treat these issues thoroughly.

We may now explain the requirement that $E/\boldsymbol{Q}$ be *parametrized by modular forms*, made twice before, namely: For some $N$ we require that there be a surjective map $X_0(N) \to E$ defined over $\boldsymbol{Q}$.

For the rest of our constructions, we shall be (implicitly and explicitly) studying *quotients of the jacobian of* $X_0(N)$. Fix $N$ a *prime number*. We make this restriction since our nontrivial results have only been proved for $N$ prime, and it enables us to avoid discussing the technical matter of primitive (or *new*) forms. Let $J$ be the jacobian of $X_0(N)$, regarded as abelian variety over $\boldsymbol{Q}$.

By the *Hecke algebra* $\underline{T} \subset$ End $J$ we shall mean the ring of endomorphisms of $J$ generated by the Hecke operators $T_l$ for prime numbers $l \neq N$, and by the canonical involution $w$ (which, on $U$ is $z \mapsto -1/Nz$). The Hecke algebra $\underline{T}$ is a free module over $\boldsymbol{Z}$ of rank equal to dim $J$, and is a subalgebra of finite index in a finite product of Dedekind domains, each factor being the ring of integers in some totally real number field.

If $P \subset \underline{T}$ is a maximal ideal, let $\underline{T}_P$ denote the completion of $\underline{T}$ at $P$. Let $\underline{a} \subset \underline{T}$ denote the kernel of $\underline{T} \to \underline{T}_P$. Let $\underline{a} \cdot J \subset J$ denote the subabelian variety generated by the images of $J$ under elements in $\underline{a}$.

Form $J/\underline{a} \cdot J = J^{(P)}$ which may again be regarded as an abelian variety defined over $\boldsymbol{Q}$, and which we call the *factor associated to P*. The construction of $p$-adic $L$-series alluded to above is not restricted to the case of elliptic curves parametrized by modular forms but rather, with a certain twist, makes sense for arbitrary factors of $J$. For example, let $P \subset \underline{T}$ be any maximal ideal lying over the rational prime $p$. Suppose that *the Hecke operator* $T_p$ *does not lie in P*. Then the construction of [**6**] provides a ($p$-adic) analytic power series $L_P(J, s)$. The "twist" consists in that this power series does *not* naturally lie in $\underline{T}_P[[s]]$, but rather in $\underline{T}_P[[s]] \otimes_{\underline{T}_P} H_P^+$ where $H_P^+$ is the following $\underline{T}_P$-module. Let $H = H_1(J_{\boldsymbol{C}}, \boldsymbol{Z})$, the classical 1-dimensional singular homology group of the complex torus $J_{\boldsymbol{C}}$. Let $\mathfrak{S}$ denote complex conjugation, and $H \to H^+$ the quotient by the minus-eigenspace of $\mathfrak{S}$. Set $H_P^+ = H^+ \otimes_{\underline{T}} \underline{T}_P$.

In *good* cases, $H_P^+$ is a free $\underline{T}_P$-module of rank one.

**4. Eisenstein primes.** We are now ready to describe prime ideals in the Hecke algebra which seem to play an effective part in the study of certain arithmetic questions.

We repeat that $N$ is assumed to be prime. By the *Eisenstein ideal* $I \subset \underline{T}$ we mean the ideal generated by the elements $1 + l - T_l$ for all primes $l \neq N$, and by $1 + w$.

Let $\nu$ denote the numerator of $(N - 1)/12$. Let $p$ be a prime number *dividing* $\nu$, and let $p^\alpha$ denote the precise power of $p$ which divides $\nu$. By the *Eisenstein prime* $P \subset \underline{T}$ *over* $p$ we mean the ideal $P = (I, p)$. Using the fact that $p$ divides $\nu$ one can prove that $\underline{T}/P = \boldsymbol{Z}/p$, and in particular that $P \neq \underline{T}$.

We can now state our results. The first main result may be loosely paraphrased as follows: "*The Birch Swinnerton-Dyer conjecture is valid locally at an Eisenstein prime*". We actually have something stronger in mind: "locally with respect to an Eisenstein prime" each of the relevant factors of the conjectural ($P$-adic) Birch

Swinnerton-Dyer formula may be evaluated. Explicitly, we describe the evaluation of the arithmetically interesting factors:

THEOREM A. *Let $N$ be a prime, and suppose $p$ is an odd prime dividing $\nu$. Let $P$ be the Eisenstein prime over $p$.*

1. *(Nonvanishing of the L-series) $H_P^+$ is free of rank* 1 *over $\underline{T}_P$ and $L_P(J, 1) \cdot \underline{T}_P$ is of finite index in $H_P^+$.*[5]

2. *(Finiteness of Mordell-Weil) $J^{(P)}$ has only a finite number of rational points over* $\boldsymbol{Q}$. *(This result remains valid if $p = 2$, at least in the case where* $N \equiv 1$ mod 16.)

3. *(Torsion part of Mordell-Weil) The P-primary component of the Mordel-Weil group of $J^{(P)}$ is cyclic of order $p^\alpha$.*

4. *(Shafarevitch-Tate) The P-primary component of the Shafarevitch-Tate group of $J^{(P)}/\boldsymbol{Q}$ is zero.*

REMARKS. 1. *What is the dimension of $J^{(P)}$?* By part 3 of the above theorem, $J^{(P)}$ has a point of order $p^\alpha$. Using the Riemann hypothesis applied to $J^{(P)}$ over $\boldsymbol{F}_2$ one may conclude that dim $J^{(P)} \geqq \log_6 p^\alpha$. Actual computation ($N < 250$) finds the $J^{(P)}$'s to be of significantly larger dimension than this. Indeed, factors associated to Eisenstein primes usually account for all or almost all of the minus-eigenspace of the involution $w$ on $J$.

A consequence of some of the theory developed in [5] is the following: If $\alpha = 1$, then $J^{(P)}$ is an absolutely irreducible abelian variety. By appropriate choice of $N$ and $p$, using the Dirichlet theorem on primes in arithmetic progressions, one may then deduce (using part 2 of Theorem A):

THEOREM B. *There are absolutely irreducible abelian varieties of arbitrarily high dimensions defined over $\boldsymbol{Q}$, with finite Mordell-Well group.*

We state this theorem explicitly because at present we know of no other means of obtaining such examples.

2. *Torsion in the Mordell-Weil group of $J$.* If $N$ is a prime, then the divisor class of the difference $(0) - (i\infty)$ of the two cusps on $X_0(N)$ is a point of $J$, rational over $\boldsymbol{Q}$, and of order precisely $\nu =$ numerator $(N - 1)/12$, as has been shown by Ogg. Ogg conjectured that this point generates *all* the torsion in the Mordell-Weil group of $J$ over $\boldsymbol{Q}$. In the course of proving part 3 of Theorem A, we have shown the following:

THEOREM C. *The torsion subgroup of the Mordell-Weil group of $J$ is generated by* $(0) - (i\infty)$ *if* $N \equiv -1$ (4) *or* $N \equiv 1$ (16). *In all cases, the quotient of $M_{\text{tors}}$ by the subgroup generated by* $(0) - (i\infty)$ *is a* 2-*group.*

3. *Finiteness of Mordell-Weil of $J^{(P)}$ over larger fields?* From the explicit calculation of the $P$-adic $L$-series given in part 1 of Theorem A and from general conjec-

[5] A more precise formula, which depends, of course, on the normalization chosen for $L_P(J, 1)$, will be given in [5]. Curiously, the size of this index seems to depend on whether $p$ is a $p$th power modulo $N$.

tures (relating the so-called *analytically defined* characteristic polynomials to the *algebraically defined* ones; cf. [6]), one is led to ask a question, which may be attackable, and may have an affirmative answer, at least when $p$ is not a $p$th power mod $N$.

*Question.* Let $\boldsymbol{Q}^{(p)}/\boldsymbol{Q}$ be the unique Galois extension with Galois group isomorphic to $\boldsymbol{Z}_p$. Does $J^{(P)}$ have only a finite number of rational points over $\boldsymbol{Q}^{(p)}$?[6]

4. *The proper context of Eisenstein primes.* Wherever there are Eisenstein series in the theory of modular forms, there seems to be the analogue of Eisenstein primes in the relevant Hecke algebra. The next task of our theory should be to make a systematic connection between these two notions. Among other things, this should encompass a study of the jacobian of $X_0(N)$ where $N$ is no longer necessarily prime.[7] Especially intriguing, however, is the prospect of studying other quotient curves of the modular curve $X(N)$, and modular forms of weight higher than 2.

**5. The Mordell conjecture for $X_0(N)$ over $\boldsymbol{Q}$.** Here $N$ remains a prime number.

THEOREM D. *Let $X_0(N)$ have genus greater than zero. Then $X_0(N)$ has no more than a finite number of rational points over $\boldsymbol{Q}$.*[8]

One is after something *much finer* than this, though.

PROOF BASED ON THE RESULTS OF §4. One checks, with no trouble, that the genus of $X_0(N)$ is greater than zero if and only if $\nu > 1$. Also, either there is an *odd* prime $p$ dividing $\nu$, or $p = 2$ divides $\nu$ and $N \equiv 1 \bmod 16$. Thus, by part 2 of Theorem A applied to such a $p$, there is always some Eisenstein prime $P$ such that $J^{(P)}$ has a finite number of rational points over $\boldsymbol{Q}$. Now consider

(∗)

$$\begin{tikzcd} X_0(N) \arrow[rr] \arrow[dr, "\beta"'] & & J \arrow[dl] \\ & J^{(P)} & \end{tikzcd}$$

and since $X_0(N)$ generates $J$ as a group and the factor $J^{(P)}$ is of positive dimension, it follows that $\beta$ must be nonconstant, and therefore a finite map of the curve $X_0(N)$ onto its image. Theorem D then follows.

In *actually* determining the rational points of $X_0(N)$ for some value of $N$, the fun only *begins* with diagram (∗). For example, if $N \not\equiv 9 \bmod 16$ or if $p \neq 2$ one can produce a certain set $\Delta$ of points in $J^{(P)}$ which is of cardinality 2,3,4, or 5 depending on the congruence class of $N$ modulo 12 ($N \equiv 1, 5, 7$, or $11 \bmod 12$ resp.) such that if $x$ is a rational point of $X_0(N)$, then $\beta(x) \in \Delta$.

Using this, geometric analysis of $\beta$ (cf. [8], [9]), and work of Brumer and Kramer on certain elliptic curve factors of $J$ which are *not* associated to Eisenstein primes, Ogg and I have calculated the set of rational points of $X_0(N)$ for all primes $N < 250$ *except for* $N = 53, 113, 137, 151, 227$ (in the first three of these unresolved cases the method gives that there are either two noncuspidal rational points on $X_0(N)$

[6] Cf. [4] where the first nontrivial case $N = 11$ is worked out.

[7] There seem to be conceptual as well as technical barriers to this, at present.

[8] We give no upper bound for the number of these rational points in general.

or there are none). Based on this numerical work, Ogg has made a conjecture, which we describe below.

Suppose that $N$ is any positive integer, no longer necessarily prime. The cases where the genus of $X_0(N)$ is zero are well known; so are the 12 cases where $X_0(N)$ is of genus one, and in these cases, all rational points of $X_0(N)$ are known. Therefore let us suppose that the genus of $X_0(N)$ is greater than one. The following curious list of noncuspidal rational points is also known:

$N = 43, 67, 163$: $X_0(N)$ has a (single) noncuspidal rational point "coming from a quadratic imaginary field of class number one".

$N = 37$: $X_0(37)$ has two noncuspidal rational points interchanged by the canonical involution $w$.

CONJECTURE. The above list gives all noncuspidal rational points on all $X_0(N)$ of genus greater than one.

The case $N = 37$ was studied at great length by Swinnerton-Dyer and myself [**6**]. The extra lever one has in this case is the following: $X_0(37)$ is a hyperelliptic curve whose hyperelliptic involution $u$ is different from $w$. Ogg has recently proved that among the $X_0(N)$'s, $X_0(37)$ is the *only* curve with the above property. Note that the image under $u$ of the two cusps (0) and $(i\infty)$ are rational points of $X_0(37)$. Swinnerton-Dyer and I were able to show (from general principles) that these two rational points are *different* from the cusps, thereby establishing these points as candidates for the above list.

**6. Indications of the method of proof.** There are three main stages in the proof of Theorem A.

1. Proof that $H_P^+$ is free of rank 1 over $\underline{T}_P$. This uses the theory of modular forms in characteristic $p$.

2. Proof that $I_P$ (the ideal generated by the Eisenstein ideal $I$ in $\underline{T}_P$) is a *principal* ideal in $\underline{T}_P$. One does this by defining a $\underline{T}_P$-homomorphism $I_P \to H_P^+$ and shows, using the theory of the *modular symbol*, that this homomorphism is an isomorphism.

3. The "geometric" descent. One takes an element $\alpha$ in $I$ which is a local generator of $I_P$, and uses the endomorphism $\alpha$ of $J$ to perform a "descent" as explained in [**4**] and [**7**].

By far the longest and most involved stage is the first. I shall try, in a few brief paragraphs, to convey the flavor of the arguments that enter into it. We keep to $p \neq 2$, as hypothesized in Theorem A. At one point (which we shall gloss over) in the argument, one must do some extra work when $p = 3$.

To prove that $H_P^+$ is free of rank one over $\underline{T}_P$, it suffices to prove that $H_P$ is free of rank two over $\underline{T}_P$. We identify the $\underline{T}_P$-module $H_P$ with the $\bar{\boldsymbol{Q}}$-rational points of the "$P$-primary" factor of $\text{Tate}_pJ$. By $\text{Tate}_pJ$ we mean the pro-$p$ Barsotti-Tate group associated to the abelian scheme $J$ over Spec $\boldsymbol{Z}[1/N]$. Refer to this "$P$-primary" factor as $\text{Tate}_PJ$. Let $\text{Tate}_PJ[1]$ denote the cokernel of "multiplication by $p$". That is, it is the "first truncation" of the pro-$p$ Barsotti-Tate group, and we regard $\text{Tate}_PJ[1]$ as a finite flat group scheme killed by $p$ over Spec $\boldsymbol{Z}[1/N]$, which is self-dual under Cartier duality. Let $V$ denote the group of $\bar{\boldsymbol{Q}}$-rational points of this finite flat group scheme. We regard $V$ as a $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module and as $\underline{T}_P$-module. Consider the $P$-adic filtration on $V$ and form the associated graded $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module $\mathrm{gr}_P V$. Any element $x$ of $\mathrm{gr}_P V$ is killed by $P$, and therefore

$$(**) \qquad T_l \cdot x = (1 + l) \cdot x, \qquad l \neq N, \qquad w \cdot x = -x.$$

By the Eichler-Shimura relations, and Cartier self-duality of $V$, one obtains from $(**)$ that the eigenvalues of $l$-Frobenius ($l \neq N$) acting on $\mathrm{gr}_P V$ are 1 and $l$ with the same multiplicity $m$. By the Čebotarev density theorem and standard representation theory, one obtains that the semisimplification of the representation of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on $V$ is isomorphic to $(\boldsymbol{Z}/p)^m \oplus (\boldsymbol{\mu}_p)^m$, where $\boldsymbol{Z}/p$ means the $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module with trivial action, and $\boldsymbol{\mu}_p$ means the $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module of $p$th roots of unity.

Using standard techniques in the theory of finite flat group schemes, and using the Oort-Tate classification theorem of finite flat group schemes of order $p$, one then learns that there is a filtration of the finite flat group scheme $\mathrm{Tate}_P J[1]$ by subgroup schemes, finite and flat over Spec $\boldsymbol{Z}[1/N]$ whose associated graded finite flat group scheme over $\boldsymbol{Z}[1/N]$ is $(\boldsymbol{Z}/p)^m \oplus (\boldsymbol{\mu}_p)^m$ where $\boldsymbol{Z}/p$ and $\boldsymbol{\mu}_p$ now refer to the group schemes over Spec $\boldsymbol{Z}[1/N]$. We are now ready to reduce the Barsotti-Tate group $\mathrm{Tate}_P J$ *to characteristic p*.

One thing we discover from our group scheme filtration of $\mathrm{Tate}_P J[1]$ is that $\mathrm{Tate}_P J$ is an "ordinary" Barsotti-Tate group. Over $\boldsymbol{F}_p$ we may write it as

$$\mathrm{Tate}_P J/\boldsymbol{F}_p = \textit{multiplicative part} \times \textit{étale part}$$

where each part is a $\underline{T}_P$-module and is dual to the other part. To establish the assertion of stage 1, it suffices to show that the $\bar{\boldsymbol{F}}_p$-rational points of the *étale part* form a free $\underline{T}_P$-module of rank one. After much difficult work,[9] one finds that the key to this is to show that the étale part of the kernel of $P$ in $J/\bar{\boldsymbol{F}}_p$ is a group scheme of order precisely $p$. Let this étale group scheme be denoted $C$. There is a *general* geometric construction which gives us an imbedding

$$C(k) \otimes_{\boldsymbol{F}_p} k \xrightarrow{c} H^0(X_0(N)/k, \Omega^1_{X_0(N)/k})$$

for any extension field $k/\boldsymbol{F}_p$. Moreover, by naturality, $c$ maps the domain to the kernel of $P$ in the range. Consider an element $f$ in the kernel of $P$ in the range of the above map. We regard $f$ as a modular form, parabolic, of weight 2 under $\Gamma_0(N)$, which is an eigenvector for the Hecke operators $T_l$ with eigenvalue $(1 + l)$, $l \neq N$, and an eigenvector for $w$ with eigenvalue $-1$. With some work, one discovers that mod $p$, up to scalar multiplication, $f$ has the same $q$-expansion as the Eisenstein series of weight 2 for $\Gamma_0(N)$. By the $q$-expansion principle $f$ must be (mod $p$) a scalar multiple of the Eisenstein series. In other words $C(k)$ is an $\boldsymbol{F}_p$-vector space of dimension $\leqq 1$; it is seen to be of dimension precisely one by explicit construction.

[9] Added in proof. It was only after the Congress that I realized how difficult this point is. In working it out, however, some new things emerge. Firstly, Theorem D may now be proved in a more elementary way. Secondly, some of the results may be significantly sharpened. Cf. [5] and the Bourbaki seminar report (*Points rationnels des modulaires $X_0(N)$*, n° 469, Juin 1975) by J.-P. Serre and myself.

## References

**1.** N. Katz, *Letter to S. Lichtenbaum*, June 1974.

**2.** Ju. I. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk **26** (1971), no. 6 (162), 7–71 = Russian Math. Surveys **26** (1971), no. 6, 7–78.

**3.** ———, *The values of p-adic Hecke series at integer points of the critical strip*, Mat. Sb. **93** **(135)** (1974), 621–626 = Math. USSR Sb. **22** (1974) (to appear).

**4.** B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

**5.** ———, *Modular curves and the Eisenstein ideal* (in preparation).

**6.** B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent Math. **25** (1974), 1–16.

**7.** B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973), 41–49.

**8.** A. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27.

**9.** ———, *Hyperelliptic modular curves* (to appear).

**10.** J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular Functions on one Variable, III, Proc. Internat. Summer School, Univ. of Antwerp, RUCA, Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin and New York, 1973, pp. 191–268. MR **48** #2080.

**11.** Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, no. 1, Publ. Math. Soc. Japan, no. 11, Iwannami Shoten, Tokyo; Princeton Univ. Press, Princeton, N.J., 1971. MR **47** #3318.

**12.** J. Tate, *Arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

**13.** P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions on one Variable, II, Proc. Internat. Summer School, Univ. of Antwerp, RUCA, Lecture Notes in Math., vol. 349, Springer-Verlag, Berlin and New York, 1973, pp. 143–317.

HARVARD UNIVERSITY
CAMBRIDGE, MASSACHUSETTS 02138, U.S.A.