RATIONAL POINTS ON MODULAR CURVES

by B. Mazur

RATIONAL POINTS ON MODULAR CURVES

§1. Introduction

In the course of preparing my lectures for this conference, I found a proof of the following theorem, conjectured by Ogg (conjecture 1 [17b]):

THEOREM 1. *Let Φ be the torsion subgroup of the Mordell-Weil group of an elliptic curve E, over $\mathbb{Q}$. Then Φ is isomorphic to one of the following* 15 *groups:*

$$\mathbb{Z}/m\cdot\mathbb{Z} \qquad \text{for} \quad m \leq 10 \quad \text{or} \quad m = 12$$

$$\mathbb{Z}/2\cdot\mathbb{Z} \times \mathbb{Z}/2\nu\cdot\mathbb{Z} \qquad \text{for} \quad \nu \leq 4 \ .$$

This proof will be presented here (see also [14a]).

The above 15 groups do indeed occur, for their "associated" moduli problems are of genus 0 with known rational parametrizations. [1)]

Theorem 1 fits into a broader conjecture, attributed by Cassels ([3] p. 264 ; cf. also bibliography) to the "folklore":

---

1) The equations are collected in ([10], Table 3, page 217), and were known for the most part to Fricke. It is amusing to consider, however, that, in disguised form, some of these parametrizations may have been known far earlier than that. Griffiths pointed out to me that the data of the classical Poncelet theorem (an n-gon inscribed in one conic and circumscribed about another) provides one with an elliptic curve and a point of order n on that elliptic curve. (As was known, in effect, to Jacobi. See [7] §1 d.)

But judging from the hints given in [6], the mathematician Nicolaus Fuss (1755-1826 ; a friend and student of Euler) may have found rational parametrizations of Poncelet quadrilaterals, pentagons, hexagons, heptagons and octagons (Nova Acta Petropol. XIII 1798, which I have not been able to track down).

Conjecture A

If K is a number field, there is a positive integer $B(K)$ such that for elliptic curve E over K, the torsion subgroup of $E(K)$ (the Mordell-Weil group of E over K) is of order $\leq B(K)$.

Theorem 1 also fits into a general program:

B. Given a number field K and a subgroup H of $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $Gal(\bar{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

Concerning conjecture A one has very little general information except for the case $K = \mathbb{Q}$. For no $K \neq \mathbb{Q}$ is the conjecture proved, nor does one even possess any serious lower bounds for $B(K)$.

One has, however, partial information of two sorts. Firstly, for a given number field K, and prime number p, there is a finite power of p, $q = p^{e(p,K)}$ such that no elliptic curve defined over K possesses a K - rational point of order (divisible by) q. This follows from a more general theorem of Manin (using the theory of heights and methods of Demjanenko [13] [22b]). The exponents $e(p,K)$ have recently been made effective by Berkovic [1] (using the descent techniques of [14a]).

Secondly, there is an extremely intriguing technique of associating to a K - rational torsion point on any elliptic curve over K (which is required to be 'rigidified' over K by extra data) K - rational points of some specific algebraic

curve V of genus > 1 over K. In this way one obtains uniform bounds for the order of the torsion parts of the Mordell-Weil groups of those elliptic curves over (certain fields) K which possess the requisite rigidification over K, provided $V(K)$ is finite (more precisely: the bound is in terms of the cardinality of $V(K)$). [1)]

These techniques occur in the work of Demjanenko [5] in which further claims are made which are, it seems, unjustified. See [10] for a rigorous development and broadening of these methods. For a relationship between the problem of existence of rational $2N$-torsion in elliptic curves over K and K-rational points on the Fermat curve $X^N + Y^N = 1$ see [11]. The paper of Kubert [10] should be consulted for its close study and ingenious use of these (and other) methods to obtain a number of specific applications.

Concerning the general program (B), a theorem of Serre [22a] assures us that, if we ignore elliptic curves of complex multiplication, we may take H to be a subgroup of finite index in $GL_2 \hat{\mathbb{Z}}$. As we shall see below, a diverse range of diophantine questions are embraced by program (B) (See [14a]). Included, in particular, is the problem of classifying elliptic curves over K possessing a K-rational N-isogeny (N a given integer > 1), or equivalently, a K-rational cyclic subgroup of order N. This problem, moreover, is also

---

1) This is reminiscent of a method introduced by Hellegouarch [8] where he related the existence of a $\mathbb{Q}$-rational point of order p^h (p a prime number > 13, $h > 1$) to the existence of systems of $(p^h - 1)/2$ rational points of an appropriate (generalized) Fermat variety: $\sum_{j=1}^{N} X_j^{p^{h-1}} = 0$ where N is an integer independent of p and h.

equivalent to the problem of determining the K - rational points of the modular curve $X_0(N)$. Although our knowledge of isogenies is not as sharp as that of rational torsion, the theory of the Eisenstein ideal provides much information when $K = \mathbb{Q}$.[1] [Ogg and I expect to find no $\mathbb{Q}$ - rational N - isogenies when $N > 163$.] For $K \neq \mathbb{Q}$, again, very little is known. To be sure, elliptic curves possessing complex multiplication must be treated specially when studying isogenies: if $E_{/K}$ is such an elliptic curve, for any rational prime N which splits in $R = \mathrm{End}_K(E)$ ($N = \pi \cdot \pi'$ with neither π nor π' units in R) multiplication by π in E provides us with a K - rational N - isogeny.[2]

Let us say, provisionally, that an isogeny is large if it is an N - isogeny for an integer N such that genus $X_0(N) \geq 2$ (equivalently: $N > 21$ and $N \neq 24, 25, 27, 32, 36, 49$). It is tempting to ask

Question C: Is it true that for a given number field K, there are only a finite number of values $j_1, j_2, \cdots, j_{C(K)}$ such that if $E_{/K}$ is an elliptic curve possessing a large K - rational isogeny, then the elliptic modular invariant $j(E) = j_m$ for some $m \leq C(K)$?

It would be interesting to make empirical investigations in this area. At the moment, one lacks sufficient experience to make any conjectures for $K \neq \mathbb{Q}$.

---

1) Surveys of some of the results of this theory occur in [14b], [16], [17b] and the complete details will appear in [14a]. See also §4 below.

2) If N does not split in the complex quadratic field $K = \mathbb{Q}(\sqrt{-d})$, see §4 cor. 2 below.

Notational conventions: If X is a scheme over a base S and $T \to S$ a morphism of schemes, we shall indicate the pullback of X to T $(X \times_S T)$ by $X_{/T}$. If $T = \operatorname{Spec} A$, we may also write $X_{/A}$. The T-valued points of X we denote $X(T)$, and again if $X = \operatorname{Spec} A$ we may also denote it $X(A)$. If X is a scheme over the field of complex numbers $\mathbb{C}$, then $X_{\mathbb{C}}$ denotes the underlying analytic space.

§2. Modular curves

Let $\mathbb{H}$ be the upper half-plane regarded as homogeneous space under $PSL_2\,\mathbb{R}$ by the usual action $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right): z \mapsto \frac{az+b}{cz+d}$. To a point $z \in \mathbb{H}$ we may associate a lattice $\wedge_z = \mathbb{Z} + z \cdot \mathbb{Z} \subset \mathbb{C}$ and an elliptic curve $E_z = \mathbb{C}/\wedge_z$. The lattice does not change under modification of z by any element of $\Gamma(1) = PSL_2\,\mathbb{Z}$ and one has the one-to-one correspondences

$$\left\{\begin{array}{c}\text{elliptic curves}\\ \text{over } \mathbb{C}\text{, up to}\\ \text{isomorphism}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{lattices in } \mathbb{C}\\ \text{up to}\\ \text{homothety}\end{array}\right\} \longleftrightarrow \Gamma(1)\backslash\mathbb{H} \xrightarrow[\approx]{j} \mathbb{C}$$

where the analytic isomorphism j is the elliptic modular invariant.

Let E be an elliptic curve defined over a field K and N an integer ≥ 1. Let $E[N]$ denote the kernel in E of multiplication by N. If N is prime to the characteristic of K, we view $E[N]$ as $Gal(\overline{K}/K)$ - module. It is a free $\mathbb{Z}/N$ module of rank 2 and the classical e_N - pairing provides us with a canonical isomorphism

$$\wedge^2 E[N] \xrightarrow{\approx} \mu_N \quad (= Gal(\overline{K}/K)\text{ - module of } N\text{-th roots of } 1)\,.\ ^{1)}$$

Thus the determinant of the representation of $Gal(\overline{K}/K)$ on $E[N]$ (viewed as a 2 - dimensional representation over $\mathbb{Z}/N$) is equal to the standard character

---

1) There are, indeed, two canonical isomorphisms, which differ by sign. A convention we make below will stipulate which of these two we are choosing but this choice is irrelevant for our considerations.

$\chi : \mathrm{Gal}(\overline{K}/K) \longrightarrow (\mathbb{Z}/N)^*$ defined by the rule $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ where $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $\zeta \in \mu_N(\overline{K})$. In particular, note that the image of the determinant, $\det(\mathrm{Gal}(\overline{K}/K))$, is equal to $(\mathbb{Z}/N)^*$.

Any isomorphism $E[N] \xrightarrow{\alpha_N} \mathbb{Z}/N \times \mathbb{Z}/N$ is called a <u>level N - structure</u>. To a level N structure α_N we may associate an N-th root of 1, $\zeta(\alpha_N) = \alpha_N^{-1}(1,0) \wedge \alpha_N^{-1}(0,1) \in \mu_N(\overline{K})$ where the wedge denotes the e_N - pairing.

If E is defined over $\mathbb{C}$, we shall say that α_N is a <u>canonical</u> level N structure provided $\zeta(\alpha_N) = \exp(2\pi i/N)$.

If $z \in \mathbb{H}$, the level N structure $\alpha_N : E_z[N] \xrightarrow{\approx} \mathbb{Z}/N \times \mathbb{Z}/N$ obtained by sending $a/N + z \cdot b/N$ in $E_z[N] = \frac{1}{N}\wedge_z/\wedge_z$ to (a,b) in $\mathbb{Z}/N \times \mathbb{Z}/N$ is seen to be canonical (which pins down our choice of sign for the e_N - pairing).

If (E, α_N) is any pair consisting of an elliptic curve $E_{/\mathbb{C}}$ and a canonical level N structure $\alpha_N : E[N] \xrightarrow{\approx} \mathbb{Z}/N \times \mathbb{Z}/N$ then (E, α_N) is isomorphic to a pair (E_z, α_N) and the set of z for which this is true forms a single orbit under

$$\Gamma(N) = \left\{ g \in \Gamma(1) \mid g \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ modulo } N \right\}$$

(<u>the principal congruence subgroup of level N</u>). One compactifies the open Riemann surface $\Gamma(N)\backslash\mathbb{H}$ (of iso. classes of elliptic curves over $\mathbb{C}$ with "canonical" level N structures) by adjunction of a finite set of points (cusps) which

may be identified with $\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q})$ to obtain the compact algebraic curve $X(N)_{/\mathbb{C}}$ (the modular curve of level N):

$$X(N)_{\mathbb{C}} = \Gamma(N)\backslash\mathbb{H} \amalg \Gamma(N)\backslash P^1(\mathbb{Q}) \quad .$$

See ([4] II) for an interpretation of the cusps of $X(N)$ in terms of degenerate forms of elliptic curves ($\mathbb{C}^* \times \mathbb{Z}/N$) with canonical level N structure. The curve $X(N)$ is a Galois covering of $X(1) = \mathbb{C} \cup \infty$ (via the elliptic modular function j), with Galois group $\Gamma(1)/\Gamma(N)$ ($\cong PSL_2\mathbb{Z}/N\mathbb{Z}$, if N is a prime). If $H \subset GL_2\ \mathbb{Z}/N\mathbb{Z}$, set $H_o = H \cap SL_2\ \mathbb{Z}/N\mathbb{Z}$, and let X_H denote the intermediate covering $H_o\backslash X(N)$. A non-cuspidal point of X_H is given either by a $\mathbb{C}$ - isomorphism class of pairs consisting in an elliptic curve E and an H - orbit of level N structures on E, or equivalently, an H_o - orbit of canonical level N structures. As a curve over $\mathbb{C}$, X_H is dependent only on the subgroup H_o; however X_H admits a natural structure over the field $\mathbb{Q}(\exp(2\pi i/N))^{\det H}$, the fixed field under the action of $\det H \subset (\mathbb{Z}/N)^* = Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, where $\det H$ denotes the image of the determinant. (See [4] IV 3.20.4)

In particular, if $\det H = (\mathbb{Z}/N)^*$, then X_H is defined over $\mathbb{Q}$.

If $H = \{\left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right) \in GL_2\ \mathbb{Z}/N\}$, the standard notation for X_H is $X_1(N)$ and its non-cuspidal points correspond to elliptic curves with a chosen point of order N.

If $H = \{\left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right) \in GL_2\ \mathbb{Z}/N\}$, the standard notation for X_H is $X_0(N)$ and its non-cuspidal points classify N - isogenies.

More systematically, if $N \geq 5$ is a prime number, any proper subgroup

$H \subset GL_2\ \mathbb{Z}/N$ is conjugate to a subgroup of one of the entries of the following table, in which $\mathcal{S}_n$ denotes the symmetric group on n letters, $\mathcal{A}_n$ the alternating group and $\mathbb{Q}(\chi_N)$ denotes the quadratic subfield of $\mathbb{Q}(e^{2\pi i/N})$.

(N = prime ≥ 5)

H	Notation for X_N	Field of definition
(a) The Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$	$X_0(N)$	$\mathbb{Q}$
(b) The normalizer of a split Cartan $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \cup \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$	$X_{split}(N)$	$\mathbb{Q}$
(c) The normalizer of a nonsplit Cartan subgroup $\mathbb{F}^*_{N^2} \subset GL_2\ \mathbb{Z}/N$	$X_{nonsplit}(N)$	$\mathbb{Q}$
(d) The inverse image in $GL_2\ \mathbb{Z}/N$ of $\mathcal{S}_4 \subset PGL_2\ \mathbb{Z}/N$	$X_{\mathcal{S}_4}(N)$	$\mathbb{Q}$ if $N \equiv \pm 3 \bmod 8$ $\mathbb{Q}(\chi_N)$ if $N \not\equiv \pm 3 \bmod 8$.
(e) The inverse image in $GL_2\ \mathbb{Z}/N$ of $\mathcal{A}_5 \subset PGL_2\ \mathbb{Z}/N$ (possible only if $N \equiv \pm 1 \bmod 5$)	$X_{\mathcal{A}_5}(N)$	$\mathbb{Q}(\chi_N)$
(f) The inverse image in $GL_2\ \mathbb{Z}/N$ of $\mathcal{A}_4 \subset PGL_2\ \mathbb{Z}/N$	$X_{\mathcal{A}_4}(N)$	$\mathbb{Q}(\chi_N)$

Remarks:

1. The normalizer of Cartan subgroups.

If $N \geq 5$ is a prime number, one has these formulae for the genus of $X_{split}(N)$ and $X_{nonsplit}(N)$ respectively:

$$g_{split}(N) = \frac{11 + (N - 8) \cdot N - 4\left(\frac{-3}{N}\right)}{24}$$

$$g_{nonsplit}(N) = \frac{23 + (N - 10) \cdot N + 6\left(\frac{-1}{N}\right) + 4\left(\frac{-3}{N}\right)}{24} \quad .$$

where $\left(\frac{-}{N}\right)$ denotes the Legendre symbol.

It is immediate that $X_{split}(N)$ corresponds to the problem of classifying elliptic curves endowed with an unordered pair of independent N - isogenies, and $X_{nonsplit}(N)$ corresponds to the problem of classifying an elliptic curve together with a chosen subfield of order N^2 in the endomorphism ring of $E[N]$ (equivalently: an $\mathbb{F}_{N^2}$ - vector space structure on $E[N]$ determined up to the conjugation in $\mathbb{F}_{N^2}$).

One sees easily that the curve $X_{split}(N)$ is isomorphic (over $\mathbb{Q}$) to $X_0(N^2)/w$ where w is the canonical involution (induced from $z \mapsto -1/N^2 z$ in $\mathbb{H}$). In contrast, the family of curves $X_{nonsplit}(N)$ does not seem to be directly related to any of the more "familiar" modular curves.

2. N - adic points of the modular curves associated to exceptional subgroups.

Serre has proved the following local result for elliptic curves (which Ribet and I have checked remains valid for abelian varieties of arbitrary dimension):

Let K be a finite extension of $\mathbb{Q}_N$ of ramification index e. Let E be an elliptic curve over K with a semi-stable Néron model over the ring of integers $\mathfrak{o}_K$. Let $r : \mathrm{Gal}(\overline{K}/K) \to \mathrm{PGL}(E[N])$ denote the projective representation associated to the action of Galois on N - division points of E. Then: if $2e < N - 1$, the image of the inertia subgroup under r contains an element of $\geq (N - 1)/e$.

Using this local result, one obtains a bound $c(K)$ such that X_H possesses no K - rational points, when H is an exceptional subgroup of $GL_2\ \mathbb{Z}/N$ and $N > c(K)$. In particular, Serre has shown that $X_{\mathcal{A}_4}(N)$ possesses no points rational over $\mathbb{Q}_N$ if $N > 13$.

3. 'Expected' rational points on X_H. [1]

Let N be a prime number and E be an elliptic curve with complex multiplication over $\mathbb{C}$. Let $R = \mathrm{End}_{\mathbb{C}} E$. It is well known that $E[N]$ is a free $R/N \cdot R$ - module of rank 1. [2] Since $R/N \cdot R$ is an $\mathbb{F}_N$ - algebra of dimension 2, there are 3 possibilities:

---

1) These are closely related to the Heegner points studied by Birch and Stephens. Compare also [14a] Ch. III §2.

2) This follows e.g. from ([12] Ch. 8, §1 Cor. 1).

(a) $R/N \cdot R$ has a nontrivial radical. In this case $R/N \cdot R = \mathbb{F}_N[\varepsilon]$, where ε is a nontrivial element in the radical, necessarily of square zero.

(b) $R/N \cdot R$ is a product of two fields (each $\approx \mathbb{F}_N$). In this case we have the equation $1 = \varepsilon_1 + \varepsilon_2$ in $R/N \cdot R$ where ε_1, ε_2 are a pair of orthogonal idempotents.

(c) $R/N \cdot R$ is a field.

In case (a), the kernel of ε in $E[N]$ is a subgroup of order N, and the pair $(E, \ker \varepsilon)$ determines a point $a_E \in X_0(N)$.

In case (b), the kernels of ε_1 and ε_2 in $E[N]$ provide an unordered pair of independent cyclic subgroups of order N, and thereby determines a point $a_E \in X_{split}(N)$.

In case (c) we obtain a point $a_E \in X_{nonsplit}(N)$.

Consequently, for each elliptic curve with complex multiplication E, we obtain a (noncuspidal) point $a_E = a_E(N) \in X_0(N) \amalg X_{split}(N) \amalg X_{nonsplit}(N)$ which, by the theory of complex multiplication (e.g. [12] part two Chapter 10), is defined over a subfield of index two in the ray class field of $R \otimes \mathbb{Q}$, with conductor equal to the conductor of R.

Since there are 13 complex quadratic orders R with class number 1, for each N we obtain 13 $\mathbb{Q}$-rational points $a_E(N)$ in $X_0(N) \amalg X_{split}(N) \amalg X_{nonsplit}(N)$ (the "expected" rational points).

For $R = \mathbb{Z}[\frac{1+\sqrt{-N}}{2}]$, $E = \mathbb{C}/R$, and $N = 11, 19, 43, 67, 163$, the point

$a_E(N)$ lands in $X_0(N)$. For all other cases $(N \geq 11)$ the "expected" rational points distribute themselves among X_{split} and $X_{nonsplit}$.

4. The status of knowledge of $\mathbb{Q}$ - rational points of the modular curves.

If N is prime, and $H \subset GL_2\ \mathbb{Z}/N$ is an entry of the above table, such that $g_H > 0$, and X_H is defined over $\mathbb{Q}$, the following facts are known:

(a) $X_H = X_0(N)$ has only a finite number of $\mathbb{Q}$ - rational points. If ν denotes the number of noncuspidal rational points on $X_0(N)$, then ν is known for all $N < 250$ except $N = 151$ and 227 and $\nu = 0$ in this range except for the following values of N:

N	11	17	19	37	43	67	(151)	163	(227)
ν	3	2	1	2	1	1	?	1	?

(besides the techniques of [14a], this tabulation makes use of calculations and results due to Atkin, Brumer and Kramer, Ogg, Parry, Tingley and Wada. See [14a]).

(b) $X_H = X_{split}(N)$ has only a finite number of $\mathbb{Q}$ - rational points if $N \neq 13$. Since $X_{split}(13)$ is of genus 3, one expects that it, too, has only a finite number of rational points. ([14a] Ch. III §6).

(c) For $X_H = X_{nonsplit}(N)$ nothing is known.

(d) By remark 3, $X_{\mathscr{I}_4}(N)$ has no rational points for $N > 13$. Serre, however, has constructed a rational point on $X_{\mathscr{I}_4}(11)$ and on $X_{\mathscr{I}_4}(13)$ using

elliptic curves with complex multiplication by $\sqrt{-3}$.

To be sure, the last two entries in the table are not defined over $\mathbb{Q}$, and therefore can have no $\mathbb{Q}$ - rational points.

§3. A proof of Theorem 1

Theorem 1 implies that if $m < \infty$ is the order of a $\mathbb{Q}$ - rational torsion point of an elliptic curve over $\mathbb{Q}$, then $m \leq 10$ or $m = 12$. This statement is equivalent to:

THEOREM 2. *If the genus of* $X_1(m)$ *is* > 0 (*i.e.* $m = 11$ *or* $m > 13$), *then the only* $\mathbb{Q}$ - *rational points on* $X_1(m)$ *are the* $\mathbb{Q}$ - *rational cusps.*

Kubert ([10] IV. 1.2) has shown that to prove Theorem 1, it suffices to prove Theorem 2 for m a prime number ≥ 23; this is what we shall do below.

The proof we shall give for Theorem 2 will in fact be valid for $m = N$, a prime number such that either $N = 11$, or $N \geq 17$ (i.e. such that the genus of $X_0(N)$ is > 0). Since it may be of interest, at least for clarity of presentation, to make essential ingredients of the proof explicit at the outset, we shall do this by axiomatizing what is needed.

We shall prove:

PROPOSITION: *Let* (K, N) *be a pair consisting in a number field* K *and a prime number* N, *which satisfies Axioms* 1, 2, *and* 3 *below.*

Then the only K - *rational points of* $X_1(N)$ *are the* K - *rational cusps.* [1)]

---

1) At present, I have no example of a number field K different from $\mathbb{Q}$ and a prime number N such that (K, N) satisfies these axioms. But compare the next footnote with §4 Cor. 1.

Our first axiom is simply a bound:

Axiom 1: Let $d = [K:\mathbb{Q}]$. Then $N > 1 + 3^d + 2 \cdot 3^{d/2}$.

Axiom 2: There is a nonconstant map (over $\mathbb{Q}$)

$$f : X_0(N) \to A$$

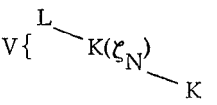
where A is an abelian variety, such that:

(i) if 0 and ∞ are the cusps of $X_0(N)$, then $f(0) \neq f(\infty)$.

(ii) The Mordell-Weil group $A(K)$ is finite.

Remark: If $K = \mathbb{Q}$, then Axiom 2 is satisfied when A is taken to be the Eisenstein quotient of J = the jacobian of $X_0(N)$ provided $N = 11$ or $N \geq 17$. (cf. [14a] theorem 4 of introduction and §4 below).

For our third axiom, we need a definition. Let L/K be a Galois extension such that ζ_N (a primitive N-th root of 1) lies in L and such that $V = \mathrm{Gal}(L/K(\zeta_N))$ is an abelian group killed by N.



Suppose that the natural action of $\mathrm{Gal}(K(\zeta_N)/K)$ on V (via conjugation through $\mathrm{Gal}(L/K)$) is given by multiplication by the j-th power of the standard character χ. That is

$$\tau \cdot v = \chi(\tau)^j \cdot v$$

where we recall that the standard character $\chi : \mathrm{Gal}(K(\zeta_N)/K) \to (\mathbb{Z}/N)^*$

is defined by the rule: $\zeta_N^{\chi(\tau)} = \tau \cdot \zeta_N$, for $\tau \in \mathrm{Gal}(K(\zeta_N)/K)$.

Here j may be taken to be an integer modulo $N - 1$.

If the above is the case, let us refer to L as a χ^j - extension of $K(\zeta_N)$.

Axiom 3: There are no nontrivial everywhere unramified χ^{-1} - extensions of $K(\zeta_N)$.

Remark: When $K = \mathbb{Q}$, Axiom 3 is indeed valid, and follows from a theorem of Herbrand, which is a sharpened version of Kummer's famous criterion. Explicitly, if B_{2k} denotes the $2k$-th Bernoulli number $(B_2 = \frac{1}{6}, B_3 = 0, B_4 = \frac{1}{30}, \cdots)$ and $2 \leq 2k < N - 1$, write $j = 1 - 2k \bmod N - 1$. Then:

THEOREM (Herbrand-Kummer): If B_{2k} is a N - adic unit, then there are no nontrivial everywhere unramified χ^j - extensions of $\mathbb{Q}(\zeta_N)$.

In particular, since $B_2 = 1/6$, Axiom 3 follows for $K = \mathbb{Q}$.

Further remarks: Ribet has recently shown [20b] that, under the same conditions as above, B_{2k} is an N - adic unit if and only if there are no nontrivial everywhere unramified χ^j - extensions, of $\mathbb{Q}(\zeta_N)$.

Gilles Robert [21] has developed machinery for the study of unramified χ^j - extensions of $K(\zeta_N)$ where K is a quadratic imaginary field. In particular he has a generalization of the Kummer criterion to this case, where the Bernoulli numbers are replaced by certain determinants of certain "Hurwitz numbers".

However, the (conjectured) analogue of Herbrand's "sharpening" is not yet known. [1]

We may now proceed with the proof of the above proposition. For the remainder of the proof we shall let $E_{/K}$ denote an elliptic curve with a K - rational torsion point of order N (equivalently: a Galois sub-module isomorphic to the constant $Gal(\overline{K}/K)$ - module $\mathbb{Z}/N$) and we shall study the properties of such a curve E, supposing that (K,N) satisfies our axioms. In the end we shall conclude that E cannot exist.

The e_N - pairing provides a self-duality of $E[N]$ into μ_N, and therefore our K - rational point of order N gives us an exact sequence of $Gal(\overline{K}/K)$ modules:

$$(*) \qquad 0 \longrightarrow \mathbb{Z}/N \longrightarrow E[N] \longrightarrow \mu_N \longrightarrow 0$$

Choosing a $\mathbb{Z}/N$ - basis of $E[N](\overline{K})$ compatible with this exact sequence (i.e. such that the first member is a nontrivial K - rational point) enables us to view the 2 - dimensional $Gal(\overline{K}/K)$ - representation over $\mathbb{Z}/N$ (the action of $Gal(\overline{K}/K)$ on $E[N](\overline{K})$) as a representation $\rho : Gal(\overline{K}/K) \longrightarrow GL_2\ \mathbb{Z}/N$ of the form $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$, where χ is the standard character. Let L/K be the field extension generated by the N - division points of E (i.e. the 'splitting field' of the representation ρ). It is evident that L/K is Galois. The field L contains $K(\zeta_N)$, and from the exact sequence $(*)$ one gets a natural injection

---

[1] It might nevertheless be of interest to have lists of (K,N) where K is a quadratic imaginary field, and N is a rational prime, ≥ 5 remaining prime in K, such that N is a regular prime in K in the terminology of [21]. These (K,N) would indeed satisfy Axiom 3. ([21] Cor. 2).

$$(**) \qquad \mathrm{Gal}(L/K(\zeta_N)) \hookrightarrow \mathrm{Hom}(\mu_N(\bar{K}), \mathbb{Z}/N) \quad (= \mu_N^{-1}(\bar{K})) \quad .$$

To be sure, this shows that $\mathrm{Gal}(L/K(\zeta_N))$ is an abelian group killed by N. But a simple calculation shows, further, that the natural action of $\mathrm{Gal}(K(\zeta_N)/K)$ on $\mathrm{Gal}(L/K(\zeta_N))$ is by multiplication by the character χ^{-1}. As Serre pointed out, this calculation is particularly transparent if one views $\mathrm{Gal}(L/K(\zeta_N))$ as a subgroup of $\mu^{-1}(\bar{K})$ using $(**)$ above.

Thus: $L/K(\zeta_N)$ is a χ^{-1} - extension .

We shall prove the following

MAIN LEMMA: (a) $L/K(\zeta_N)$ is everywhere unramified.

(b) E is not an elliptic curve of complex multiplication.

Proof of the proposition, granted the main lemma:

Since the χ^{-1} - extension $L/K(\zeta_N)$ is everywhere unramified, by Axiom 3 , it is trivial. It follows that the exact sequence $(*)$ splits, giving a $\mathrm{Gal}(\bar{K}/K)$ - isomorphism $E[N] = \mathbb{Z}/N \times \mu_N$. That is, we may view the $\mathrm{Gal}(\bar{K}/K)$ module $\mathbb{Z}/N \times \mu_N$ as contained in $E_{/K}$. We may pass to the quotient $E' = E/\mu_N$ which is, again, an elliptic curve over K , and the image of the sub-Galois module $\mathbb{Z}/N \subset E$ in E' is, again, a sub-Galois module isomorphic to $\mathbb{Z}/N$. Since $\mathbb{Z}/N \subset E'$ satisfies all the hypotheses that $\mathbb{Z}/N \subset E$ does, the main lemma is applicable to it also. Proceeding as above, we get a sequence of elliptic curves over K

$$\begin{array}{ccccccccc} E & \to & E' & \to & E'' & \to \cdots \to & E^{(j)} & \to \cdots \\ \cup & & \cup & & \cup & & \cup & \\ \mathbb{Z}/N & & \mathbb{Z}/N & & \mathbb{Z}/N & & \mathbb{Z}/N & \end{array}$$

each obtained from the next by an N - isogeny , and such that the original subgroup $\mathbb{Z}/N \subset E$ maps isomorphically into every $E^{(j)}$.

Since all the curves $E^{(j)}$ will have good reduction outside a fixed finite set of closed points of S = the spectrum of the ring of integers in K , it follows from Shafarevic's theorem ([22c] Ch. IV 1.4) that among the set of $E^{(j)}$'s there can be only a finite number of K - isomorphism classes of elliptic curves represented. Consequently, for some indices $j > j'$ we must have $E^{(j)} \cong E^{(j')}$. But $E^{(j)}$ maps to $E^{(j')}$ by a nonscalar isogeny. Therefore $E^{(j)}$, and hence E , is an elliptic curve of complex multiplication. But this contradicts part (b) of the main lemma.

Remarks: 1. The above argument, using part (a) of the main lemma, shows that E has a complex multiplication defined over K , which is impossible when $K = \mathbb{Q}$. So, in that case, one has a contradiction from part (a) alone.

2. Although Part (a) is an assertion which is 'local' for every prime of K , the essential step (2 below) in the proof of the main lemma is global.

Step 1: (The Néron model of $E_{/K}$)

Let S be the spectrum of the ring of integers in K , and $E_{/S}$ the Néron model of $E_{/K}$. By the universal property of Néron models the morphism

$\mathbb{Z}/N_{/K} \to E_{/K}$ extends to a morphism $\mathbb{Z}/N_{/S} \to E_{/S}$ which maps to the Zariski closure in $E_{/S}$ of $\mathbb{Z}/N_{/K} \subset E_{/K}$ (the 'group scheme extension' of $\mathbb{Z}/N_{/K}$ ([19] §2 ; [14a] Ch. 1 (c).) This group scheme extension $G_{/S}$ is a (separated) quasi-finite group scheme over S whose generic fibre is $\mathbb{Z}/N$. Since, however, it admits a map from $\mathbb{Z}/N_{/S}$ which is an isomorphism on the generic fiber, it follows that $G_{/S}$ is a finite flat group scheme (of order N). Since, by Axiom 1, $N > d+1$, for each closed point $s \in S$, the absolute ramification index e_s (over Spec $\mathbb{Z}$) is $< N-1$, and consequently, by a theorem of Raynaud ([19] 3.3.6) $G_{/S} \cong \mathbb{Z}/N_{/S}$.

Therefore we shall identify $G_{/S}$ with $\mathbb{Z}/N_{/S}$, and we obtain, therefore, for each closed point $s \in S$ the subgroups $\mathbb{Z}/N_{/s} \subset E_{/s}$ in the Néron fibre over s (the 'specializations').

LEMMA 1: $E_{/S}$ is semi-stable. That is, for each $s \in S$, $E_{/s}$ is either an elliptic curve, or its connected component $(E_{/s})^o$ is of multiplicative type.

Proof: Suppose that $(E_{/s})^o$ is an additive group. Then the index of $(E_{/s})^o$ in $E_{/s}$ is ≤ 4 ([24 §6 Table p. 46). It follows that $\mathbb{Z}/N_{/s} \subset (E_{/s})^o$. Let $k(s)$ denote the residue field of s. Since the additive group over $k(s)$ is killed by multiplication by the characteristic of $k(s)$ (= "char s") it follows that char $s = N$. Now let K_s denote the completion of K at s, and note that there is a field extension K'_s/K_s whose relative ramification index is ≤ 6, and such that $E_{/K'_s}$ possess a semi-stable Néron model $\mathcal{E}/_{\mathcal{O}'_s}$ where $\mathcal{O}'_s$ is the ring of integers in

K'_s [23]. [1] If $E_{/\mathcal{O}'_s}$ denotes the pullback of $E_{/S}$ to $\mathcal{O}'_s$, we have a morphism

$$E_{/\mathcal{O}'_s} \xrightarrow{\varphi} \mathcal{E}_{/\mathcal{O}'_s}$$

which is an isomorphism on generic fibres, using the Universal Néron Property of $\mathcal{E}_{/\mathcal{O}'_s}$. The mapping φ is zero on the connected component of the special fibre of $E_{/\mathcal{O}'_s}$ since there are no non-zero morphisms from an additive to a multiplicative type group over a field. Consequently, the mapping φ restricted to the special fibre of $\mathbb{Z}/N_{/\mathcal{O}'_s}$ is zero. As in the discussion before the present lemma, one sees that if $\mathcal{C}_{/\mathcal{O}'_s}$ is the 'group scheme extension' in $\mathcal{E}_{/\mathcal{O}'_s}$ of $\mathbb{Z}/N_{/K'_s}$ then there is a morphism from $\mathbb{Z}/N_{/\mathcal{O}'_s}$ to $\mathcal{C}_{/\mathcal{O}'_s}$ which is an isomorphism on generic fibres, and which is zero on special fibres.

Using Raynaud's Cor. 3.3.6 [19], again, one sees that this is impossible, since the absolute ramification index of K'_s is $\leq 6d$ and $N - 1 > 6d$ by Axiom 1.

LEMMA 2: If $s \in S$ is a point of characteristic 2 or 3, then E has bad (hence multiplicative) reduction over s, and $\mathbb{Z}/N_{/s} \not\subset (E_s)^o$. (Recall that ^{o} denotes connected component).

---

[1] Proof: apply §2 Corollary 3 of [23] with $m = 3$ and 4, noting that $N = \text{char } s$ is different from 2 and 3.

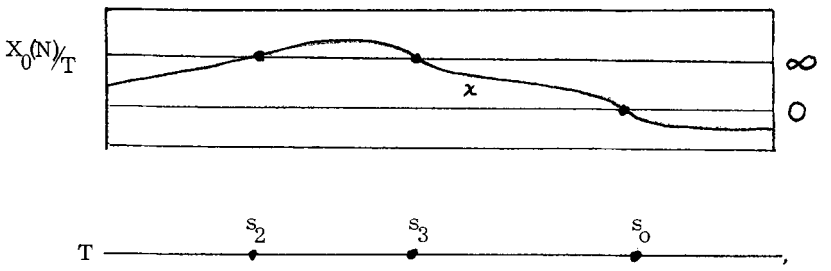
Proof: Let $d = [K : \mathbb{Q}]$. If s has characteristic ℓ then the cardinality of $k(s)$ is $\leq \ell^d$. If E_s has good reduction at s, it has at most $1 + \ell^d + 2 \cdot \ell^{d/2}$ points by the "Riemann hypothesis". Since $\mathbb{Z}/N \subset E_s$ this contradicts Axiom 1 if $\ell = 2$ or 3. Thus E has multiplicative type reduction at the point s. Then over the quadratic extension $\widetilde{k(s)}$ of $k(s)$, we have an isomorphism $(E_{/\widetilde{k(s)}})^0 \cong \mathbb{G}_{m/\widetilde{k(s)}}$ ([22c] IV A. 1. 1) and therefore N must divide the cardinality of $\widetilde{k(s)}$. If $\mathrm{card}(\widetilde{k(s)}) = \ell^{2r}$ with $r \leq d$, then N divides $\ell^{2r} - 1 = (\ell^r - 1)(\ell^r + 1)$ which again violates Axiom 1, since N is prime.

Remark: We have established part (b) of the main lemma, since if E were a complex multiplication elliptic curve, its Néron model could not have multiplicative type reduction at any point $s \in S$.

Step 2: (The Global Step).

LEMMA 3: If $s \in S$ is any point of bad reduction for $E_{/S}$ then the 'specialization' $\mathbb{Z}/N_{/s}$ is not contained in the connected component of the identity $(E_{/s})^0$.

Proof: Let s_o be a point of bad reduction such that $\mathbb{Z}/N_{/s_o} \subset (E_{/s_o})^0$. By Lemma 1, $\mathrm{char}\ s_o \neq N$, and by Lemma 2, $\mathrm{char}\ s_o \neq 2, 3$. Let $T = \mathrm{Spec}\ \mathcal{O}[1/N]$ where $\mathcal{O}$ is the ring of integers in K, and let $X_0(N)_{/T}$ be the modular curve over the indicated base. It is a smooth scheme over T. Let $\underline{0}_{/T}$, $\underline{\infty}_{/T}$ denote the cuspidal sections of $X_0(N)_{/T}$ and let x denote the T-valued point of $X_0(N)$ determined by our couple $(\mathbb{Z}/N_{/T} \subset E_{/T})$. It is illuminating to draw a scheme-theoretic diagram:



Here s_2 is any point of T of characteristic 2 and s_3 is any point of characteristic 3. Such points exist. We are justified in drawing the intersections $x_{/s_2} = \underline{\infty}_{/s_2}$ and $x_{/s_3} = \underline{\infty}_{/s_3}$ because, by ([4] VI §5) the modular interpretation of $\underline{\infty}_{/s}$ is the 'generalized elliptic curve' $(\mathbb{Z}/N \subset \mathbb{G}_m \times \mathbb{Z}/N)$ (i.e. the cyclic subgroup of order N which gives the $\Gamma_0(N)$ - structure is not contained in the connected component of the identity) while the interpretation of $\underline{0}_{/s}$ is the 'generalized elliptic curve' $(\mu_N \subset \mathbb{G}_m \times \mathbb{Z}/N)$ (i.e. the cyclic subgroup of order N which give the $\Gamma_0(N)$ - structure is contained in the connected component containing the identity).

Let us consider, now, any abelian variety quotient $B_{/\mathbb{Q}}$ of the jacobian J of $X_0(N)_{/\mathbb{Q}}$. We assume therefore the existence of a homomorphism $J \to B$ defined over $\mathbb{Q}$. Since J has 'good reduction' over Spec $\mathbb{Z}[1/N]$, by the Criterion of Néron-Ogg-Shafarevic (cf. [23] §1), the Néron model of B over Spec $\mathbb{Z}[1/N]$ is an abelian scheme, and consequently so is its pullback $B_{/T}$. We have a morphism $X_0(N)_{/T} \xrightarrow{f} B_{/T}$ which sends $\underline{\infty}_{/T}$ to the zero-section. This morphism is simply the composition of the natural morphisms $X_0(N)_{/T} \xrightarrow{\alpha} J_{/T} \longrightarrow B_{/T}$ where α sends a section z to the divisor class of $z - \underline{\infty}$.

Claim: The image of the T - section x under f is either 0 or of infinite order in B(T).

The proof of the above claim is as follows: If f(x) were of finite order m, since $\gamma(x)_{/S_2} = 0$, m is a power of 2 (= char s_2); but since $\gamma(x)_{/S_3} = 0$, m is a power of 3 (= char s_3).

We are now ready to invoke Axiom 3. Applying the above Claim to the abelian variety B = A of Axiom 3, we deduce that f(x) = 0. Consequently $f(\underline{0}_{/S_o}) = 0$ (in $B_{/S_o}$). But since f is defined over the base S' = Spec $\mathbb{Z}[1/N]$ and $\underline{0} - \underline{\infty}$ is an S' - section of finite order $\neq 0$, one obtains by Oort-Tate [18] or by Raynaud ([19] 3.3.6) that $f(\underline{0}_{/S'}) \neq 0$ for any point $s' \in S'$ of characteristic $\neq 2$. Taking s' to be the image of s_o in S', we arrive at a contradiction, and we conclude the assertion of Lemma 3.

Step 3: ($L/K(\zeta_N)$ is unramified)

Proof: We shall prove the above assertion for all closed points $s \in S$:

(a) If E has good reduction at s, and char $s \neq N$ then E[N] is an étale finite flat group scheme in a Zariski open set about s. In particular, L/K is unramified 'above' the point $s \in S$.

(b) If E has good reduction at s, and char s = N then E[N] is a finite flat group scheme over S_s, the completion of S at the point s. Applying the connected component of the identity functor (denoted ^{0}) to the exact sequence of finite flat group schemes over S_s: $0 \to \mathbb{Z}/N \to E[N] \to \mu_N \to 0$, one sees that

$E[N]^0 = \mu_N$, giving us a canonical splitting: $E[N] = \mathbb{Z}/N \times \mu_N$ which shows, again, that $L/K(\zeta_N)$ is unramified 'above' the point $s \in S$.

(c) If E has bad (hence multiplicative) reduction at s, we shall work, as in (b), over the base S_s. The quasi-finite group scheme $E[N]_{/S_s}$ (= kernel of multiplication by N in the group scheme $E_{/S_s}$) fits into a short exact sequence of quasi-finite group schemes over S_s : $0 \to \mathbb{Z}/N \to E[N] \to G \to 0$ where the generic fibre of G is isomorphic to μ_N. The point of Lemma 3 in Step 2 is to insure that the special fibre of G is non-zero. Explicitly, since $\mathbb{Z}/N_{/s} \not\subset (E_{/s})^0$, we have that the kernel of N in the multiplicative group $(E_{/s})^0$ maps injectively to $G_{/s}$. It follows that G, and hence $E[N]$ is a finite flat group scheme over S_s. If char $s \neq N$ then $E[N]$ is an étale finite flat group scheme, and one concludes as in (a) above. If char $s = N$, then let us note that $G = \mu_N$ over S_s. (Here are two possible arguments for this: By Axiom 1, the absolute ramification index of K_s is $< N - 1$, and therefore a finite flat group scheme over S_s of order N is determined by its generic fibre ([19] 3.3.6). Or, one can show directly that $E[N]$, being a finite flat group scheme must be self (Cartier) dual, using an autoduality formula for Néron models and 'Néron-connected' models. [15] Ch. I 5.1).

We thus have a short exact sequence of finite flat group schemes as in (b) above, and we conclude the argument similarly.

§4. Eisenstein quotients.

Our presentation of the proof of Theorem 1 would be incomplete without some account of the proof that the pair $(\mathbb{Q}, N)$ satisfies Axiom 2 when $N = 11$ or $N \geq 17$ (i.e. when the genus of $X_0(N)$ is > 0). Two different proofs of this are given in [14a]. (Let us call these the easy and hard proofs. The 'easy' proof is also sketched in [16]. It is given in [14a] in Ch. III §3). Both proofs rely on an argument of 'geometric descent' using the 'Eisenstein ideal' in the Hecke algebra of endomorphisms of J the jacobian of $X_0(N)$. The easy proof is an 'infinite descent' (a more appropriate title would be: an 'indefinite descent') which uses surprisingly little information concerning the Eisenstein ideal. The hard proof uses the detailed study of the Eisenstein ideal given in Ch. II of [14a]. It is a 'first descent' and yields more precise information concerning the Shafarevic-Tate group.

Rather than repeat either of these proofs here, we shall adapt the hard proof so as to make it yield information in the case where K is a quadratic imaginary field. In particular, we shall prove that (K, N) satisfies Axiom 2 (ii) (i.e. the Eisenstein quotient of J has a nontrivial factor with finite Mordell-Weil group over K) provided K is a quadratic imaginary field in which N does not split, and $N \geq N(K)$ where $N(K)$ is an explicit constant, dependent upon K (Cor. 2 below). The easy proof would not suffice for this application. The reader should easily be able to reconstitute the hard proof for $K = \mathbb{Q}$ from the facts concerning the Eisenstein ideal collected below, and the proof given.

We shall try to introduce the reader to the relevant parts of the theory of the

Eisenstein ideal by presenting the needed definitions interspersed with results quoted from [14a] (collected in the facts numbered 1 - 6 below). Having accumulated what we need, it will be a relatively simple matter to 'perform the required descent'.

To begin, N will denote a fixed prime number such that genus $(X_0(N)) > 0$ (i.e. $N = 11$ or $N \geq 17$). Let J be the jacobian of $X_0(N)$ over $\mathbb{Q}$, and $J_{/\mathbb{Z}}$ its Néron model over $\mathbb{Z}$.

$\mathbb{T}$: The Hecke algebra is the subalgebra of the endomorphism ring $\mathrm{End}_{\mathbb{C}} J$ generated by the Hecke operators T_ℓ (ℓ running through all rational prime numbers $\neq N$) and by w (the canonical involution induced from $z \mapsto -1/Nz$ on the upper half plane $\mathbb{H}$).

Fact 1: $\mathbb{T} = \mathrm{End}_{\mathbb{C}} J$ ([14a] Ch. II 9.5).

I: The Eisenstein ideal is the ideal in $\mathbb{T}$ generated by the elements

$$\eta_\ell = 1 + \ell - T_\ell \qquad (\ell \neq N)$$

and by $1 + w$.

Fact 2: By ([14a] Ch. II 9.7) one has $\mathbb{T}/I = \mathbb{Z}/n\mathbb{Z}$ where n = numerator $(\frac{N-1}{12})$. Let us reserve the letter p to denote a rational prime number dividing n. The prime ideals of $\mathbb{T}$ which are in the support of I (called the Eisenstein primes) are in one-one correspondence with the prime divisors p of n.

Let P be the (Eisenstein) prime generated by I and p. Then $\mathbb{T}/P = \mathbb{Z}/p$.

Fact 3: The Eisenstein ideal is locally principal in $\mathbb{T}$ ([14a] Ch. II 18.10). Explicitly we have the following criterion which furnishes us amply with local generators of I at an Eisenstein prime $P = (I, p)$:

Let (p, ℓ) be a pair of rational primes $\neq (2,2)$ such that p divides n. Then the element $\eta_\ell = 1 + \ell - T_\ell$ is a generator of the ideal I locally at $P = (I, p)$ if and only if:

(i) ℓ is not a p-th power mod N

(ii) $\frac{\ell - 1}{2} \not\equiv 0 \mod p$.

In the exceptional case $(p, \ell) = (2,2)$ we have that η_2 is a local generator of I at $P = (I, 2)$ if and only if 2 is not a quartic residue modulo N.

C: the cuspidal subgroup. If c is the class of the divisor of degree zero $0 - \infty$ in $J(\mathbb{Q})$, then ([17a], [14a] Ch. II 11.1) n = order (c). The cuspidal subgroup C is the subgroup of $J(\mathbb{Q})$ generated by c. We use the notation $C_{/\mathbb{Z}}$ to indicate the finite flat subgroup scheme over $\mathbb{Z}$ generated by C in $J_{/\mathbb{Z}}$. By ([14a] Ch. II 11.1) C is annihilated by the Eisenstein ideal.

$J[I]_{/\mathbb{Q}}$: the kernel of the ideal I in the jacobian $J_{/\mathbb{Q}}$. This is, by definition, the intersection of the kernels in $J_{/\mathbb{Q}}$ of all (or of a generating system of) elements in I.

Fact 4: By ([14a] Ch. II 16.4 and 17.9) $J[I]_{/\mathbb{Q}}$ is of order n^2. By ([14a] Ch. II 1.7) there is a Galois submodule $\Sigma \subset J[I]_{/\mathbb{Q}}$ (called the Shimura subgroup) such that Σ is isomorphic (as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module) to μ_n. If n is

odd (i.e. $N \not\equiv 1 \mod 8$) then $J[I] = C \oplus \Sigma$. If, however, n is even, then $C \cap \Sigma$ is a sub-Galois module of order 2 and thus $C + \Sigma$ is of index two in $J[I]$. Only in certain cases (i.e. $N \equiv 9 \mod 16$) have we given an explicit construction of the 'remaining piece' in $J[I]$.

Fact 5: (The fibre of Néron in characteristic N)

The 'bad' Néron fiber $J_{/\mathbb{F}_N}$ has the following structure:

$$J_{/\mathbb{F}_N} = (J_{/\mathbb{F}_N})^o \times \overline{C}$$

where $\overline{C}$ is a cyclic group of order n, which may be viewed as the specialization to $\mathbb{F}_N$ of the cuspidal group C, and $(J_{/\overline{\mathbb{F}}_N})^o$ is a multiplication type group. ([14a] Appendix).

Fact 6: (Quotients of J) An abelian variety quotient of J, $J_{/\mathbb{Q}} \xrightarrow{f} B_{/\mathbb{Q}}$ will be called an optimal quotient if the kernel of f is an abelian subvariety of J (i.e. if it is connected). Clearly every quotient is isogenous to a unique optimal quotient. The $\mathbb{Q}$-simple quotients of J are $\mathbb{C}$-simple [20a].

The Hecke algebra $\mathbb{T}$ has the property that $\mathbb{T} \otimes \mathbb{Q} = \prod_j k_j$ (***) where k_j are (totally real) algebraic number fields. One has the following natural one-one correspondences:

$$\left\{\begin{matrix}\text{simple optimal}\\ \text{quotients of } J\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{factors } k_j\\ \text{in (***)}\end{matrix}\right\} = \left\{\begin{matrix}\text{irreducible}\\ \text{components in Spec } \mathbb{T}\end{matrix}\right\}$$

$$= \left\{\begin{matrix}\text{minimal prime ideals}\\ \text{of } \mathbb{T}\end{matrix}\right\}$$

If $\mathfrak{a}$ is any ideal in $\mathbb{T}$ let $\gamma_{\mathfrak{a}} \subset \mathbb{T}$ be the ideal $\gamma = \bigcap_{r=1}^{\infty} \mathfrak{a}^r$ and $J^{(\mathfrak{a})}$ the optimal quotient of J obtained by passing to the quotient of J by the abelian subvariety $\gamma_{\mathfrak{a}} \circ J \subset J$. Geometrically, we may view $J^{(\mathfrak{a})}$ as that optimal quotient of J, which under the one-one correspondence above corresponds to the set of all those irreducible components of Spec $\mathbb{T}$ which meet the support of $\mathfrak{a}$.

$\tilde{J}$: The Eisenstein quotient; it is the optimal quotient $J^{(I)}$ where I is the Eisenstein ideal.

$\tilde{J}^{(p)}$: The p - Eisenstein quotient, $J^{(P)}$, where $P = (I, p)$.

One has that the Eisenstein quotient is that optimal quotient of J comprising all the simple quotients of $\tilde{J}^{(p)}$, $p|n$.

For a detailed study of these quotients and numerical data for $N < 250$ see [14a].

ℓ_P, ℓ_p : If W is a finite T - module, $\ell_P(W)$ is the P - length of W. If W is a finite abelian group then $\ell_p(W)$ denotes its p - length (i.e. $\log_p$ of the order of the p - Sylow subgroup of W).

$H^i(S, \mathfrak{F})$: will denote cohomology for the fppf site ([26] exp. IV 6.3) over a scheme S, where $\mathfrak{F}$ is an abelian fppf - sheaf. The reader will note that the only fppf sheaves we use explicitly are flat group schemes over S (although Φ, which occurs below, is an étale nonseparated group scheme). Moreover, the only

dimensions i we consider are: $H^0(S, \mathbb{F})$ = group of S - valued sections of $\mathbb{F}$, and $H^1(S, \mathbb{F})$.

Conventions: Fix p a prime divisor of n, and $\eta = \eta_\ell$ a local generator of I at $P = (I, p)$ (See fact 3). One sees by an elementary argument that η is an isogeny of J (cf. [14a] Ch. II. proof of 16.10).

Let $\Delta \subset \operatorname{Spec} \mathbb{T}$ be the closed subscheme (the finite set of closed points) whcih is the complement of the point P in the support of the ideal (η). We shall work consistently modulo Δ. That is, we shall ignore finite $\mathbb{T}$ - modules supported on Δ.

Let K be a quadratic imaginary field and S the spectrum of the ring of integers in K.

Consider the exact sequence of abelian fppf sheaves over S:

(the "descent sequence"): $0 \longrightarrow J[\eta] \longrightarrow J \xrightarrow{\eta} J \longrightarrow \Phi \longrightarrow 0$.

Here $J[\eta]$ is the kernel of η in $J_{/S}$. It is a quasi-finite (separated) flat group scheme. The cokernel of η, Φ, is a 'skyscraper sheaf' concentrated at the points s of S of characteristic N. Its stalk at any such point is isomorphic to $\overline{C}$ (fact 5).

Now let p^α denote the maximal power of p dividing n. Thus, $\ell_p(C) = \ell_p(C) = \alpha$. If $p \neq 2$, $J[\eta] \cong \mathbb{Z}/p^\alpha \oplus \mu_{p^\alpha}$ modulo Δ (fact 4).

Let h(K) denote the class number of K and $\beta = \ell_p(h(K))$. We make the further hypothesis that $\alpha \geq \beta$ which will be strengthened later.

The Mordell-Weil group of J over K is the finitely generated group $H^0(S,J) = J(S) = J(K)$, which we view as a $\mathbb{T}$ - module (indeed: as a coherent sheaf over Spec $\mathbb{T}$). Let $M = J(K)/\underline{\text{torsion}}$.

Set $\nu = 0$ if N does not split in K, (i.e. ramifies or stays prime), and $\nu = 1$ if N splits in K.

The descent estimate:

$$\ell_p(M/\eta \cdot M) \leq 2\beta + \nu \cdot \alpha \qquad \text{if } p \neq 2, \text{ and}$$

$$\ell_p(M/\eta \cdot M) \leq 2\beta + \nu \cdot \alpha + (1 + g + \nu) \qquad \text{if } p = 2,$$

where g is the 2-length of the subgroup of points of order two in the ideal class group of K.

Proof: We indicate the proof in some detail when $p \neq 2$. When $p = 2$, we 'lose' the quantity $(1 + g + \nu)$ in our estimate since we lack a complete description of the P - primary component of $J[I]$ and possess a description only 'up to a group of order two'. [1]

Suppose, then, $p \neq 2$.

Note that $\ell_p(W)$ depends only on W modulo Δ. The estimate is established by first obtaining a bound for the P - length of $J(K)/\eta \cdot J(K)$, by estimating the P - lengths of terms occuring in the long (fppf) - cohomological exacts sequences arising from the "descent sequence". For this calculation one

---

1) To complete the argument for $p = 2$ when $K = \mathbb{Q}(\sqrt{-1})$ one must make use of the explicit Galois module structure of the points of order 2 in $J[I]$ ([14a] Ch. II §12).

must know that:

(a) $\ell_p(H^1(S, \mathbb{Z}/p^\alpha)) = \beta$,

for (since $\alpha \geq \beta$) $H^1(S, \mathbb{Z}/p^\alpha)$ is isomorphic to the dual of the p - primary component of the Hilbert Class Field of K .

(b) $\ell_p(H^1(S, \mu_{p^\alpha})) = \beta$ if $(p, K) \neq (3, \mathbb{Q}(\sqrt{-3}))$

$= \beta + 1$ if $(p, K) = (3, \mathbb{Q}(\sqrt{-3}))$.

Proof: By Kummer theory for μ_{p^α}, we have the short exact sequence:

$$0 \longrightarrow S^*/S^{*p^\alpha} \longrightarrow H^1(S, \mu_{p^\alpha}) \longrightarrow H^1(S, \mathbb{G}_m)[p^\alpha] \longrightarrow 0$$

where S^* denotes $\mathbb{G}_m(S)$ = Global units in K , and $[p^\alpha]$ means, as usual, the kernel of multiplication by p^α.

If we recall that $H^1(S, \mathbb{G}_m)$ is the ideal class group of K , and, again, that $\alpha \geq \beta$, we obtain (b) .

(c) $H^0(S, \Phi) = \overline{C}$ if N does not split in K .

$= \overline{C} \oplus \overline{C}$ if N does split in K .

$\ell_p(H^0(S, \Phi)) = (1 + \nu) \cdot \alpha$.

From the "descent sequence" and (a) , (b) , and (c) one may deduce that $\ell_p(J(K)/\eta \cdot J(K))$ is $\leq (1 + \nu)\alpha + 2\beta + \epsilon$ where $\epsilon = 1$ if $(p, K) = (3, \mathbb{Q}(\sqrt{-3}))$ and $\epsilon = 0$ otherwise. By applying the snake-lemma to the endomorphism η operating on the short exact sequence $0 \to \underline{\text{torsion}} \to J(K) \to M \to 0$, one obtains the "descent

estimate" above.

If $\mathfrak{P} \subset \mathbb{T}$ is a prime ideal, let the subscript $(\mathfrak{P})$ denote localization at $\mathfrak{P}$.

PROPOSITION: Suppose

$$\alpha > 2\beta \quad \text{if} \quad p \neq 2$$

$$\alpha > 2\beta + (1 + g + \nu) \quad \text{if} \quad p = 2 \ .$$

Then there is a minimal prime ideal $\mathfrak{P} \subset P \subset \mathbb{T}$ such that the $\mathbb{T}_{(\mathfrak{P})}$ - rank of $M_{(\mathfrak{P})}$ is 0 if N does not split in K, and is ≤ 1 if N splits in K.

Proof: Comparing our hypotheses wtih the descent estimates we see that we have $(1+\nu)\alpha = (1+\nu)\ell_p(\mathbb{T}/\eta \cdot \mathbb{T}) > \ell_p(M/\eta \cdot M)$. Consequently,

$$(1+\nu) \cdot \ell_p(\mathbb{T}_{(P)}/\eta \cdot \mathbb{T}_{(P)}) > \ell_p(M_{(P)}/\eta \cdot M_{(P)}) \ .$$

Claim: $M_{(P)}$ does not contain a free $\mathbb{T}_{(P)}$ - module of rank $1+\nu$.

Proof: If $F \subset M_{(P)}$ is such a $\mathbb{T}_{(P)}$ - module, and Q is the quotient of $M_{(P)}$ by F, apply the snake-lemma to the endomorphism η operating on the exact sequence $0 \to F \to M_{(P)} \to Q \to 0$ and one quickly deduces a contradiction to the inequality displayed above.

Our proposition then follows from the claim, for if R is a commutative noetherian local subring of $R \otimes \mathbb{Q}$ = a product of fields, and if W is an R - module of finite type, then W contains a free R - module of rank r if

and only if $W_{(\mathfrak{P})}$ is free of rank $\geq r$ over $R_{(\mathfrak{P})}$ for every minimal prime $\mathfrak{P}$ in R.

COROLLARY 1: If the inequalities of the previous proposition hold, and if, further, N does not split in K, then there is an (optimal) abelian variety quotient $J^{(p)} \to A$ defined over $\mathbb{Q}$, such that $A(K)$ is finite.

Proof: This follows directly from the proposition (cf. [14a] Ch. III 3.5).

Remarks: 1. If $p \neq 2$, and in the frequently encountered case $\beta = 0$, the above argument can be made to show that $J^{(p)}$ itself has a finite Mordell-Weil group over K. One has no reason to believe that this will continue to be true when $\beta > 0$.

Nevertheless it seems difficult to get examples where $J^{(p)}$ is not simple. The only example of this when $N < 250$ is for $p = 2$, $N = 113$ (See the table in the introduction of [14a]). If one admits certain standard conjectures (of Weil, and Hardy-Littlewood. [14a] Ch. III §7) one sees, however, that $J^{(2)}$ is not simple for an infinite number of values of N.

2. It seems likely that, if N does split in K, the $\mathbb{T}_{(\mathfrak{P})}$ rank of $M_{(\mathfrak{P})}$ is ≥ 1 for every minimal prime $\mathfrak{P} \subset \mathbb{P}$. [1)]

1) If $x \in X_0(N)$ is represented by an elliptic curve with complex multiplication by the ring of integers in K, with N-isogeny given by one of its complex multiplications, there is some evidence to support the hope that the trace to K of the class $x - \infty$ in J generates a $\mathbb{T}_{(\mathfrak{P})}$-vectorspace of dimension one in $M_{(\mathfrak{P})}$ for every minimal prime $\mathfrak{P} \subseteq \mathbb{T}$.

As a consequence of the proposition one would then have the existence of a minimal prime $\mathfrak{P}$ such that the $\mathbb{T}_{(\mathfrak{P})}$ - rank of $M_{(\mathfrak{P})}$ is precisely 1.

3. For a fixed quadratic imaginary number field K, the inequalities required by the proposition will hold for some prime divisor p of $n = \text{num}(\frac{N-1}{12})$ for all but a finite number of values of N. (e.g. $N > 48 \cdot h(K)^3 + 1$ will certainly insure the existence of such a p.)

COROLLARY 2: If $N > 48 \cdot h(K)^3 + 1$, and N does not split in the quadratic imaginary field K, then $X_0(N)(K)$ is finite.

Proof: In this case Cor. 1 applies, giving a nonconstant map $X_0(N) \xrightarrow{f} A$ (defined over $\mathbb{Q}$) where A is an abelian variety such that $A(K)$ is finite. Since $X_0(N)$ is of dimension one, the fibers of the mapping f are finite. Therefore $X_0(N)(K)$ is also finite.

4. (Examples of isogenies over quadratic imaginary fields.)
Consider only prime numbers N such that genus $X_0(N) > 1$. Let $X^+ = X_0(N)^+$ denote the quotient of $X = X_0(N)$ by the canonical involution w. Since N is prime, it is known that the real locus $X(\mathbb{R})$ consists in a single circle, and if $X^+(\mathbb{R})^0$ is the connected components in $X^+(\mathbb{R})$ containing the image of the cusps, then the natural projection sends $X(\mathbb{R})$ to a proper arc in $X^+(\mathbb{R})^0$ (since w has a fixed point in $X(\mathbb{R})$). Call the complement of this image the imaginary arc in $X^+(\mathbb{R})^0$. Any $\mathbb{Q}$ - rational point of X^+ in this imaginary arc will provide (by passing to the inverse image in X) an N - isogeny, rational over some quadratic

imaginary field. When are there an infinite number of $\mathbb{Q}$ - rational points of X^+ lying in the imaginary arc? This will certainly be the case when X^+ is of genus 0 ($N = 23, 29, 31, 41, 47, 59,$ and 71). This will also be the case when X^+ is of genus 1 ($N = 37, 43, 53, 61, 79, 83, 89, 101,$ and 131). For, if J^+ is the jacobian of X^+, it is proved in [14a] (introduction. Theorem 3) that if the genus of X^+ is >0, then the Mordell-Weil group of J^+ is a free abelian group of positive rank. Thus, in particular, when X^+ is an elliptic curve, its Mordell-Weil group is infinite [1] and therefore its intersection with the circle group $X^+(\mathbb{R})^o$ (which is at most of index 2 in $X^+(\mathbb{R})$) must likewise be infinite, hence dense.

It would be interesting to obtain N - isogenies (prime N) over quadratic imaginary fields which do not arise from the above process nor from complex multiplication. In this connection one might mention that there are four values of N known ($N = 389, 419, 479$ and 491) such that $X_0(N)$ has only a finite number of cubic points. That is, the totality of rational points of $X_0(N)$ in all cubic fields is a finite set ([14a] Ch. III 4.6 , using data provided by Atkin on New Year's eve 1975). Does this persist for larger values of N ?

---

[1] Brumer and Kramer have shown it to be infinite cyclic.

BIBLIOGRAPHY

1. Berkovic, V.: On rational points on the jacobians of modular curves [in Russian]. To appear.

2. Brylinski, J.-L.: Torsion des courbes elliptiques (d'après Demjanenko). D. E. A. de Mathématique Pure presented at the Faculté des Sciences de Paris-Sud (1973).

3. Cassels, J. W. S.: Diophantine equations with special reference to elliptic curves. J. London Math. Soc. 41 (193-291) (1966).

4. Deligne, P., Rapoport, M.: Schémas de modules des courbes elliptiques. Vol. II of the Proceedings of the International Summer School on Modular Functions, Antwerp (1972). Lecture Notes in Mathematics 349. Berlin-Heidelberg-New York: Springer 1973.

5. Demjanenko, V. A.: Torsion of elliptic curves [in Russian], Izv. Akad. Nauk. CCCP, 35, 280-307 (1971) [MR 44, 2755].

6. Dörrie, H.: 100 great problems of elementary mathematics; their history and solution. Dover, New York 1965.

7. Griffiths, P.: Variations on a theme of Abel. Inventiones Math. 35 321-390 (1976).

8. Hellegouarch, Y.: Courbes elliptiques et équation de Fermat. Thèse d'Etat. Faculté des Sciences de Besançon (1972). See also the series of notes in the Comptes-Rendus de l'Académie des Sciences de Paris. 260 5989-5992, 6256-6258 (1965); 273 540-543, 1194-1196 (1971).

9. Herbrand, J.: Sur les classes des corps circulaires. Journal de Math. Pures et Appliquées. 9^{e} série II, 417-441 (1932).

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

11. Kubert, D., Lang, S.: Units in the modular function field. I, II, III Math. Ann. 218, 67-96, 175-189, 273-285 (1975).

12. Lang, S.: Elliptic Functions. Addison Wesley, Reading 1974.

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

14a. Mazur, B.: Modular curves and the Eisenstein Ideal. To appear: Publ. Math. I.H.E.S.

14b. Mazur, B.: p - adic analytic number theory of elliptic curves and abelian varieties over $\mathbb{Q}$. Proc. of International Congress of Mathematicians at Vancouver, 1974, vol. I, 369-377, Canadian Math. Soc. (1975).

15. Mazur, B., Messing, W.: Universal extensions and one dimensional crystalline cohomology. Lecture Notes in Mathematics. 370. Berlin-Heidelberg-New York: Springer 1974.

16. Mazur, B., Serre, J.-P.: Points rationnels des courbes modulaires $X_0(N)$. Séminaire Bourbaki no. 469. Lecture Notes in Mathematics. 514 Berlin-Heidelberg-New York: Springer 1976.

17a. Ogg, A.: Rational points on certain elliptic modular curves. Proc. Symp. Pure Math. 24 221-231 (1973) AMS, Providence.

17b. Ogg, A.: Diophantine equations and modular forms. Bull. AMS 81 14-27 (1975).

18. Oort, F., Tate, J.: Group schemes of prime order. Ann. Scient. Ec. Norm. Sup. série 4, 3, 1-21 (1970).

19. Raynaud, M.: Schémas en groupes de type $(p,\cdots,p)$. Bull. Soc. Math. France. 102 fasc. 3, 241-280 (1974).

20a. Ribet, K.: Endomorphisms of semi-stable abelian varieties over number fields. Ann. of Math. 101 no. 3. 555-562 (1975).

20b. Ribet, K.: A modular construction of unramified p - extension of $\mathbb{Q}(\mu_p)$. Inventiones Math. 34, 151-162 (1976).

21. Robert, G.: Nombres de Hurwitz et regularité des idéaux premiers d'un corps quadratique imaginaire. Séminaire Delange-Pisot-Poitou. Exposé given April 28, 1975.

22a. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. 15, 259-331 (1972).

22b. Serre, J.-P.: p - torsion des courbes elliptiques (d'après Y. Manin) Séminaire Bourbaki 69/70 no. 380. Lecture Notes in Mathematics. 180. Berlin-Heidelberg-New York: Springer 1971.

22c. Serre, J.-P.: Abelian ℓ - adic representations and elliptic curves. Lectures at McGill University. New York-Amsterdam: W. A. Benjamin Inc., 1968.

23. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. of Math. 88, 492-517 (1968).

24. Tate, J.: Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil. 33-52. Modular Functions of one variable IV. Proceedings of the International Summer School, Antwerp RUCA. Lecture Notes in Mathematics 476. Berlin-Heidelberg-New York: Springer 1975.

25. SGA 3: Schémas en groupes I. Lecture Notes in Mathematics. 151. Berlin-Heidelberg-New York: Springer 1970.

B.Mazur
Harvard University
Department of Mathematics
Science Center
One Oxford Street
Cambridge, Mass. 02138