Inventiones math. 44, 129 – 162 (1978)

Inventiones mathematicae

Rational Isogenies of Prime Degree

B. Mazur
(with an appendix by D. Goldfeld)

Department of Mathematics, Harvard University, One Oxford Street, Cambridge, MA 02138, USA

Let N be a positive integer. Examples of elliptic curves over $\mathbf{Q}$ possessing rational cyclic N-isogenies are known for the following values of N:

N	g	v	N	g	v	N	g	v
$\leqq 10$	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

In this table, g is the genus of $X_0(N)$, and v the number of noncuspidal rational points of $X_0(N)$ (which is, in effect, the number of rational N-isogenies classified up to "twist"). For an excellent readable account of isogenies and their related diophantine problems, see Ogg's [25, 26]. The first column of the table corresponds to the genus 0 cases; for each of these values of N rational parametrizations of $X_0(N)$ are known [10]. For each integer N, and each order $R \subset \mathbf{Q}(\sqrt{-N})$ such that R contains $\sqrt{-N}$ and has class number one, there is a $\mathbf{Q}$-rational N-isogeny. This accounts for one noncuspidal rational point on $X_0(N)$ for $N = 11, 19, 27, 43, 67, 163$ and for the two noncuspidal rational points on $X_0(14)$. For a discussion of the cases: $N = 11, 15, 17, 21$ see ([43], pp. 78–80) and for the peculiar $N = 37$, see ([22], § 5).

The object of this paper is to show that when N is a prime number there are no $\mathbf{Q}$-rational N-isogenies beyond those exhibited in the above table.

To prove this (in the light of known results concerning $X_0(N)(\mathbf{Q})$ for the twelve prime numbers N appearing in the table [19]) it suffices to show:

Theorem 1. *Let N be a prime number such that some elliptic curve over $\mathbf{Q}$ admits a $\mathbf{Q}$-rational N-isogeny. Then*

$N=2, 3, 5, 7, 13$ (the genus 0 cases) *or*

$N=11, 17, 19, 37, 43, 67,$ *or* 163[1]

(Theorem 7.1 below).

One consequence of Theorem 1 is the classification of elliptic curves over $\mathbf{Q}$ with nontrivial torsion in their Mordell-Weil groups:

Theorem 2 (Conjecture of Ogg). *Let Φ be the torsion subgroup of the Mordell-Weil group of an elliptic curve over $\mathbf{Q}$. Then Φ is isomorphic to one of the following fifteen groups:*

$$\mathbf{Z}/m\mathbf{Z} \qquad 1 \leqq m \leqq 10 \quad \text{or} \quad m=12,$$
$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2v\mathbf{Z} \quad 1 \leqq v \leqq 4$$

(Theorem 4.1 below).

All of the fifteen related moduli problems are of genus 0 with known parametrizations ([13], p. 217) and we may obtain (infinite) rationally parametrized families of elliptic curves over $\mathbf{Q}$ whose Mordell-Weil group contains any one of the above groups.

The proof of Theorem 2 in this paper is significantly different from the first proof *I* found for it ([18]; [19] III 5.1); and it is easier. It is obtained in the course of the proof of Theorem 1 (§ 4).

The question of classification of isogenies may be viewed as part of the broader question of analyzing, for an elliptic curve $E_{/K}$ (with K a number field) the representation ρ_N of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ obtained by the natural action on $E[N]$, the group of N-division points ([32]).

A consequence of Theorem 1 (and a result of Serre) is the following:

Theorem 3. *If $E_{/\mathbf{Q}}$ is an elliptic curve, and N is a prime number, one has the following three possibilities:*

(i) $\rho_N: \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ *is surjective.*

(ii) *The image of ρ_N is contained in the normalizer of a Cartan subgroup of* $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

(iii) $N \leqq 19$ *or* $N=37, 43, 67,$ *or* 163.

Proof. By the classification of maximal proper subgroups in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ ([19]), if the image of ρ_N is not surjective, it is either contained in the normalizer of a Cartan subgroup (case (ii) or it is contained in a Borel subgroup (which by Theorem 1 implies that we are in case (iii)) or its image in $\mathrm{PGL}(\mathbf{Z}/N\mathbf{Z})$ is contained in an "exceptional subgroup". But Serre has shown (see discussion in [19] introduction) that the modular curve associated to an "exceptional subgroup" has no N-adic rational points (and consequently this case cannot occur) if $N \geqq 17$.

A consequence (communicated to me by Serre) of Theorem 2 and Proposition 21 of [32] is the following:

---

[1] The proof we give shows that either $N \leqq 17$, or $N=37$, or $\mathbf{Q}(\sqrt{-N})$ has class number one

Theorem 4. *Let $E_{/\mathbf{Q}}$ be a semi-stable elliptic curve, and N a prime number. Then the image of ρ_N is $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ if $N \geqq 11$.*

The question of isogenies for composite N, rational over $\mathbf{Q}$, is not yet completely settled. Here is how the matter stands. Say that an integer N is *minimal of positive genus* if the genus of $X_0(N)$ is >0, but the genus of $X_0(d)$ is 0, for all proper divisors d of N.

One will clearly have settled the question of isogenies for all N if

(a) one determines $X_0(N)(\mathbf{Q})$ for all N which are minimal of positive genus, and

(b) for every elliptic curve $E_{/\mathbf{Q}}$ possessing a rational N-isogeny, with N minimal of positive genus, one determines the "graph of rational isogenies" of E.

Concerning (a), Theorem 1 provides the answer for prime numbers N and therefore it remains to consider composite numbers N which are minimal of positive genus. These are given by the following list:

13^2, $13 \cdot 7$, $13 \cdot 5$, $13 \cdot 3$, $13 \cdot 2$, 7^2, $7 \cdot 5$, $7 \cdot 3$, $7 \cdot 2$, 5^3, $5 \cdot 3$, $5 \cdot 2^2$, $5^2 \cdot 2$, 3^3, $3^2 \cdot 2^2$, $3 \cdot 2^3$, and 2^5.

Since $X_0(N)(\mathbf{Q})$ is known when $X_0(N)$ is of genus 1 ([14]) and there are no $\mathbf{Q}$-rational N-isogenies if $N = 35$, 50 ([13], IV.3) or $N = 26$ ([24]), the cases which have yet to be treated are these: $N = 13^2$, $13 \cdot 7$, $13 \cdot 5$, $13 \cdot 3$ and 5^3. For the first four of these five values of N it is known that $X_0(N)(\mathbf{Q})$ is finite ([4]); indeed $N = 125$ is the only value of N such that $X_0(N)$ is of positive genus, and $X_0(N)(\mathbf{Q})$ is not known to be finite.

Concerning (b), it is an easy matter to determine (by "pure thought") the "graph of rational isogenies" for each elliptic curve supporting an isogeny of degree N (where $g = \text{genus } X_0(N) > 0$) as recorded in the table above. One finds no "unrecorded" isogenies in this manner. Thus the table would be complete (for all integers N) if there were no noncuspidal rational points on $X_0(N)$ for $N = 13^2$, $13 \cdot 7$, $13 \cdot 5$, $13 \cdot 3$, or 5^3.

The following application of Theorem 1 was pointed out to me by Serre:

Theorem 5. *There is a constant C such that every elliptic curve $E_{/\mathbf{Q}}$ is isogenous* (over $\mathbf{Q}$) *to at most C* (mutually nonisomorphic) *elliptic curves.*

Proof. By Manin's theorem ([16, 33]) or by ([4]), for any prime number p there is a constant C_p such that any elliptic curve over $\mathbf{Q}$ is isogenous (over $\mathbf{Q}$) to at most C_p (isomorphically distinct) elliptic curves, via isogenies of degree a power of p (C_p is an upper bound for the number of vertices of the "tree of rational p-power isogenies" of any elliptic curve over $\mathbf{Q}$). But by Theorem 1, C_p may be taken to be 1 for all but the finitely many exceptional primes p ($p \leqq 19$, or $p = 37$, 43, 67, 163). We may take C to be $\prod_p C_p$.

Remark. For the exceptional primes p the smallest possible C_p is:

p	2	3	5	7	11	13	17	19	37	43	67	163
C_p	8	4	?	2	2	?	2	2	2	2	2	2

Can one take $C=8$? In the tables of [43] one finds a number of elliptic curves whose graph of rational isogenies has 8 vertices.

The method of proof of Theorem 1 enables one (with the help of a result of Goldfeld: see Appendix) to obtain a partial result for quadratic imaginary fields.

Theorem 6. *Let K be a quadratic imaginary field. There is a finite set of* (rational) *prime numbers $\mathcal{N}(K)$ such that if N is a rational prime which remains prime in K and $N \notin \mathcal{N}(K)$, then there are no K-rational N-isogenies of elliptic curves over K.*

(Proposition 8.1 below.)

In contrast to the above theorem, there are quadratic imaginary fields K "possessing K-rational N-isogenies" for *infinitely many* primes N which split in K. One might expect, however, that all but a finite number of these are N-isogenies "obtained by complex multiplication". For a more detailed discussion, see [18].

In the course of the proof of Theorem 1 we obtain a partial result concerning the rational number c associated to a strong Weil curve ([39, 24], § 2). Recall that if $X_0(N) \xrightarrow{\pi} E$ is a (strong) Weil parametrization of an elliptic curve E, and if ω is a Néron differential for E we may write the q-expansion for $\pi^*\omega$ in the form $c \cdot (q^1 + a_2 q^2 + \cdots)$ where c is a nonzero rational number which we "normalize" to be positive. Manin conjectured that $c=1$. Although we cannot show this, we prove that when N is square-free, c is a power of 2.

The method of proof of Theorem 1 is as follows.

Step 1. Let N be a prime number. We begin with a geometric analysis of the projection f: $X_0(N)^{\text{smooth}}_{/\mathbf{Z}} \to \tilde{J}_{/\mathbf{Z}}$ where $\tilde{J}_{/\mathbf{Z}}$ is the Néron model of the Eisenstein quotient of the jacobian of $X_0(N)$.

We show that f is a formal immersion along the cuspidal section ∞ at least away from characteristic 2. We show this when $p \neq N$, by noting that if f were not a formal immersion at ∞ (in characteristic p), then for every differential form ω on $\tilde{J}_{/\mathbf{F}_p}$, the modular form $f^*\omega$ would have q-expansion $a_1 q^1 + a_2 q^2 + \cdots$ where $a_1 = 0 \in \mathbf{F}_p$. Taking a suitable nonzero eigenvector ω for all the Hecke operators $T_l (l \neq N)$ and U_N the standard recursive relations express the n-th Fourier coefficient a_n of ω as a multiple of a_1, giving us a contradiction, once we make use of a result of Raynaud (Proposition 1.2 below) concerning the specialization of abelian subvarieties of an abelian variety in characteristic p. For $p=N$, we obtain the same result by phrasing the above argument appropriately using Grothendieck duality, or the reader may skirt the issue of $p=N$ and pass to the "alternate route" described at the end of § 5 below.

Step 2. We are now prompted by a simple scheme-theoretic picture (the diagram in the proof of Corollary 4.3). We use Step 1 together with the theorem ([19] III 3.1) which asserts that the Mordell-Weil group of the Eisenstein quotient $\tilde{J}$ is finite,[2] and a specialization lemma (§ 1(c)) to deduce that an elliptic curve $E_{/\mathbf{Q}}$ possessing a rational N-isogeny has potentially good reduction at all primes $p \neq 2$.

[2] This does not involve the more delicate results of [19]. See a sketch of its proof in [21]

Step 3. By Step 2, E has potentially good reduction at N. After a suitable base change we may arrange it to have good reduction, and then apply the theory of Raynaud ([31]) which puts strong constraints on the inertia characters of a Galois representation coming from a finite flat group scheme. This, plus some geometry of the modular curve, enables one to describe the "isogeny character" (that is: the one-dimensional $\mathbf{F}_N$-representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ coming from the natural action on the cyclic subgroup $C_N \subset E$ which gives the N-isogeny) (§ 5).

Step 4. Having the isogeny character firmly in hand, the Riemann hypothesis for the reduction of E to characteristic p $(p \neq 2, N)$ provides us with stringent numerical congruences that N must satisfy. For sufficiently large N these congruences force $\mathbf{Q}(\sqrt{-N})$ to have class number 1, and at this point we invoke the theorem of Heegner-Baker-Stark ([3, 37, 38]) to conclude the proof.

A question. Fix $E_{/\mathbf{Q}}$ an elliptic curve and N an integer >0. Regard $V = E[N]$ as a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ module with symplectic form given by the e_N-pairing.

Consider the problem of determining *all* elliptic curves $E'_{/\mathbf{Q}}$ with sympletic $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-isomorphisms $E'[N] \approx V$.

This can be reduced to (or rephrased as) the problem of determining all $\mathbf{Q}$-rational points of a certain twisted form $X(V)$ of the modular curve $X(N)$ (associated to the principal congruence subgroup of level N).

When $N \leqq 5$ the genus of $X(N)$, and hence of $X(V)$ is 0; one then obtains an infinite parametrized family of elliptic curves $E'_{/\mathbf{Q}}$ with symplectic $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-isomorphisms $E'[N] \cong E[N]$. When $N = 6$, the genus is 1 and it might be interesting to consider this case in some detail. For $N \geqq 7$ one is faced with a diophantine problem for a curve of genus $\geqq 3$. Are there examples of elliptic curves $E_{/\mathbf{Q}}$, $E'_{/\mathbf{Q}}$ which are not isogenous over $\mathbf{Q}$ such that $E[N] \cong E'[N]$ (as $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ modules) for some $N \geqq 7$?

Notation

If K is a field, $\bar{K}$ denotes an algebraic closure. If K is a local or global field, $\mathcal{O}(K)$ is its ring of integers, and $U(K)$ the group of units in $\mathcal{O}(K)$. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}(K)$, then its residue field is denoted $k_{\mathfrak{p}}$ — or $k(\mathfrak{p})$, if it occurs as a subscript.

If Y is a scheme over a base S and $T \to S$ any base change, $Y_{/T}$ denotes the pullback of Y to T. If $T = \mathrm{Spec}\, A$, we may also denote this scheme by $Y_{/A}$. By $Y(T)$ we mean the T-rational points of the S-scheme Y, and again, if $T = \mathrm{Spec}\, A$, we may also denote this set by $Y(A)$.

If $A_{/T}$ is a group scheme and N an integer, $A[N]_{/T}$ is the kernel of multiplication by N in A, viewed as group scheme over T.

If E is an elliptic curve, a cyclic subgroup of order N in E will often be denoted C_N, and the pair (C_N, E) will be referred to as an *N-isogeny* (because this data amounts to the same as giving a homomorphism of elliptic curves $E \xrightarrow{\varphi} E'$ where $\ker \varphi$ is cyclic of order N); we denote by $j(C_N, E)$ the point in $X_0(N)$ to which it gives rise.

Contents

§ 1. Specialization of Abelian Subvarieties in Characteristic p

In this section we collect a number of results concerning specialization and flat group schemes which will be used in the sequel. Among these is Proposition 1.2 below (the reason for the title of this section); this is a result of Raynaud, communicated to me by Serre. It will undoubtedly be useful in other contexts. Let $K/\mathbf{Q}_p$ be a finite extension, and $\mathcal{O}=\mathcal{O}(K)$, its ring of integers.

a) Quasi-Finite Group Schemes

Lemma 1.1. *Let G be a quasi-finite flat group scheme of finite type over $\mathcal{O}$. There is a canonical exact sequence*

$$0\to FG\to G\to EG\to 0 \tag{1.1}$$

of quasi-finite flat group schemes over $\mathcal{O}$ such that FG is a finite flat group scheme over $\mathcal{O}$, and EG is an étale quasi-finite group scheme whose closed fiber is trivial.

Proof. If Y is a separated quasi-finite flat (finite type) scheme over $\mathcal{O}$, Y decomposes canonically as $Y=FY\coprod Y'$ where FY is a finite flat $\mathcal{O}$-scheme, and the closed fiber of Y' is empty. This is true since $\mathcal{O}$ is henselian ([45] SGA 7, Exp IX 2.2.3.1), and the proof of the lemma is straightforward from this, taking $Y=G$, $FY=FG$.

b) Semi-Stable Néron Models

If $A_{/K}$ is an abelian variety, in this section (and this section only) let $A_{/\mathcal{O}}$ denote the *connected component* of the Néron model of $A_{/K}$ over the base $\mathcal{O}$.

Thus $A_{/\mathcal{O}}$ is the open subgroup scheme of the Néron model, whose closed fiber A_0 is the connected component containing the identity of the closed fiber of the Néron model over the residue field k. Suppose that $A_{/K}$ has semi-stable reduction. Then A_0 is an extension of an abelian variety by a multiplicative type group (a torus). Let $m>1$ be an integer and let $A[m]_{/\mathcal{O}}$ denote the subgroup scheme kernel of multiplication by m in $A_{/\mathcal{O}}$. Then $A[m]_{/\mathcal{O}}$ is a quasi-finite flat

separated group scheme over $\mathcal{O}$ by ([45] SGA 7, Exp IX, Lemme 2.2.1). We have a filtration of $A[m]_{/\mathcal{O}}$ as follows:

$$0 \subset A[m]^t \subset A[m]^0 \subset FA[m] \subset A[m] \tag{1.2}$$

where $FA[m]$ is the finite flat subgroup scheme coming from Lemma 1.1, $A[m]^0$ is its connected component (over $\mathcal{O}$), and $A[m]^t$ is the "toric part" of $A[m]^0$ (the maximal multiplicative type subgroup scheme).

c) Specialization Results

Suppose that the ramification index $e(K/\mathbf{Q}_p)$ is $<p-1$ (e.g., when $K=\mathbf{Q}_p$, we suppose that $p\neq 2$). We have the following proposition of Raynaud ([31]).

Proposition 1.1. *Let $e(K/\mathbf{Q}_p)$ be $<p-1$. Let $H \xrightarrow{f} G$ be a morphism of finite flat group schemes over $\mathcal{O}$. If $f_{/K}$: $H_{/K} \to G_{/K}$ is an injection on the associated Galois modules, then $f_{/\mathcal{O}}$ is a closed immersion. If $f_{/K}$ is an isomorphism, then so is $f_{/\mathcal{O}}$.*

This proposition is a generalization of the following:

Specialization Lemma: Let $e(K/\mathbf{Q}_p)$ be $<p-1$. Let $G_{/\mathcal{O}}$ be a finite flat group scheme, and $x \in G(\mathcal{O})$, a section. Then the order of x equals the order of the specialization of x to k (denoted $x_{/k}$) *in $G(k)$.*

Remarks. One may obtain the above lemma from Proposition 1.1, by taking H to be the constant group scheme $\mathbf{Z}/r\mathbf{Z}$ where r is the order of x in $G(\mathcal{O})$, and the map f: $H \to G$ is the one which sends 1 to x. The specialization lemma also follows from the classification theory of Oort-Tate ([27], Theorem 2). If the group scheme G is contained in an abelian variety (which is the case in all our applications) the specialization lemma is more elementary still, and follows from a calculation in formal Lie groups.

d) Specialization of Abelian Subvarieties

Proposition 1.2 (Raynaud). *Let $e(K/\mathbf{Q}_p)$ be $<p-1$. Let*

$$0 \to A_{/K} \to B_{/K} \to C_{/K} \to 0 \tag{1.3}$$

be an exact sequence of abelian varieties, such that B has good reduction (i.e., the Néron model of B over $\mathcal{O}$ is an abelian scheme). *Then A and C also have good reduction, and the induced sequence of abelian schemes*

$$0 \to A_{/\mathcal{O}} \xrightarrow{f} B_{/\mathcal{O}} \xrightarrow{g} C_{/\mathcal{O}} \to 0 \tag{1.4}$$

is exact (i.e., f is a closed immersion, and g induces an isomorphism from the quotient of B by the image of A onto C).

Proof. The abelian varieties A and C have good reduction by ([45] SGA 7, IX 2.2.9(v)). We proceed by a series of steps.

1. The Morphism f is Finite. For let $f'_{/K}: B_{/K} \to A_{/K}$ be a quasi-inverse to $f_{/K}$. That is, for some integer r, $f'f = r \cdot 1_A$ (multiplication by r in the abelian variety A). Using the Néron property, one sees that $f'_{/K}$ is the restriction to K of a unique morphism $f'_{/\mathcal{O}}: B_{/\mathcal{O}} \to A_{/\mathcal{O}}$ such that $f'f$ is multiplication by r in $A_{/\mathcal{O}}$. Since $r \cdot 1_A$ is a finite morphism, and f' is separated, [44] EGA II 6.15(v) applies giving that f is a finite morphism.

2. The Restriction of f to the Closed Fiber is a Closed Immersion. For, if not, there would be a prime number l and a nontrivial subgroup scheme killed by l in the kernel of $f_0 = f_{/k}$. But since f: $A[l]_{/\mathcal{O}} \to B[l]_{/\mathcal{O}}$ is an injection on the associated Galois modules, Proposition 1.1 applies and gives that f_0 is a closed immersion on $A[l]_{/k}$.

3. The Morphism f is a Closed Immersion. Apply [44] EGA IV, Corollary 18.22.6c. Identify A with its image under f.

4. The Morphism g Induces an Isomorphism of B/A Onto C. We form the indicated quotient in, say, the category of algebraic spaces using Corollary 7.3 of ([2]). This quotient is indeed a (projective) abelian scheme using ([28] VI 2.5) and ([30] Th. 1 iv). The induced morphism $\bar{g}$: $B/A \to C$ is an isomorphism when restricted to generic fibers, and is then easily seen to be an isomorphism over $\mathcal{O}$, using the universal property of Néron models. q.e.d.

We shall prove a weakened version of the above proposition in the case of semi-stable reduction.

Proposition 1.3. *Let $e(K/\mathbf{Q}_p)$ be $< p-1$. Let*

$$0 \to A_{/K} \to B_{/K} \to C_{/K} \to 0 \tag{1.5}$$

be an exact sequence of abelian varieties such that B has semi-stable reduction. Then A and C also have semi-stable reduction, and for m any power of p, the induced sequence of finite flat group schemes over $\mathcal{O}$

$$0 \to A[m]^0_{/\mathcal{O}} \xrightarrow{f^0} B[m]^0_{/\mathcal{O}} \xrightarrow{g^0} C[m]^0_{/\mathcal{O}} \to 0 \tag{1.6}$$

is an exact sequence of finite flat group schemes.

Proof. Note that the notation in (1.6) is as in (1.2) of (b) above. The abelian varieties A and C have semi-stable reduction by ([45] SGA 7 IX 3.5(iv)). Since $f^0_{/K}$ is injective, Proposition 1.1 applies, giving that f^0 is a closed immersion. To establish exactness of (1.6), it suffices to establish its exactness when restricted to K (using Prop. 1.1 again), and therefore we need only check that

$$A[m]_{/K} \cap B[m]^0_{/K} = A[m]^0_{/K}.$$

Note that $A[m]^0_{/K}$ is contained in $A[m]_{/K} \cap B[m]^0_{/K}$ and the cokernel extends to a connected finite flat group scheme over $\mathcal{O}$. Using Proposition 1.1 we will have proved that this cokernel is zero if we show that it *also* extends to an étale finite flat group scheme over $\mathcal{O}$. Indeed, we shall show that $(A[m]/A[m]^0)_{/K}$

extends to an étale finite flat group scheme over $\mathcal{O}$. Consider the diagram (1.2) for $A_{/K}$ and the dual abelian variety $A'_{/K}$:

$$0 \subset A[m]^t \subset A[m]^0 \subset A[m],$$
$$0 \subset A'[m]^t \subset A'[m]^0 \subset A'[m].$$

The Galois modules $A[m]_{/K}$ and $A'[m]_{/K}$ are in Cartier duality. Using Proposition 1.1 it follows that $A'[m]^t_{/K}$ is orthogonal to $A[m]^0_{/K}$ with respect to this duality. To check that $(A[m]/A[m]^0)_{/K}$ extends to an étale group scheme over $\mathcal{O}$ it suffices to check, then, that its order is equal to the order of the group $A'[m]^t$. But this is easily seen as follows: If A_0 is an extension of an abelian variety A_0^{ab} by a torus of dimension τ, write $\tau = \tau(A_0)$, and consider G, the p-divisible group over k associated to A_0^{ab}. Write $\mu(A_0) =$ height of the multiplicative type part of G, $\varepsilon(A_0) =$ height of the étale part of G, and $\alpha(A_0) =$ height of the "local-local" part. Since A is isogenous to A' and A_0 to A'_0,[3] we have:

$$\tau(A_0) = \tau(A'_0); \quad \mu(A_0) = \mu(A'_0) = \varepsilon(A_0) = \varepsilon(A'_0); \; \alpha(A_0) = \alpha(A'_0).$$

Moreover,

$$2 \cdot \dim(A_{/K}) = 2 \cdot \tau(A_0) + \mu(A_0) + \alpha(A_0) + \varepsilon(A_0).$$

Now the operation $[m]$ (passage to scheme-theoretic kernel of multiplication by m) commutes with passage to the closed fiber, and so

$$l(A'[m]^t) = \tau(A_0) + \mu(A_0),$$
$$l(A[m]^0) = \tau(A_0) + \mu(A_0) + \alpha(A_0)$$

where $l(H) = \log_m$ (order of H).

The required equality then follows.

If S is any base scheme and $G_{/S}$ a smooth group scheme, let $\mathrm{Tan}(G_{/S})$ and $\mathrm{Cot}(G_{/S})$ denote the (free, finite rank, $\mathcal{O}_S$-modules which are, respectively, the tangent space and cotangent space of $G_{/S}$ along the zero-section.

Corollary 1.1. *Let $e(K/\mathbf{Q}_p)$ be $< p-1$. Let*

$$0 \to A_{/K} \to B_{/K} \to C_{/K} \to 0$$

be an exact sequence of abelian varieties such that B has semi-stable reduction. Let

$$A_{/\mathcal{O}} \to B_{/\mathcal{O}} \to C_{/\mathcal{O}}$$

be the induced sequence of connected components of Néron models. We have the exact *sequences of free $\mathcal{O}$-modules:*

$$0 \to \mathrm{Tan}(A_{/\mathcal{O}}) \to \mathrm{Tan}(B_{/\mathcal{O}}) \to \mathrm{Tan}(C_{/\mathcal{O}}) \to 0$$

and

$$0 \to \mathrm{Cot}(C_{/\mathcal{O}}) \to \mathrm{Cot}(B_{/\mathcal{O}}) \to \mathrm{Cot}(A_{/\mathcal{O}}) \to 0.$$

[3] Notation as in the beginning of paragraph (b)

e) The Condition $e<p-1$.

This condition is definitely needed for both propositions and the corollary (even if B has good reduction), as the following example of Serre shows. Let E and E' be two elliptic curves with good reduction over $\mathcal{O}=\mathbf{Z}_2$ such that E contains the étale finite subgroup $\mathbf{Z}/2$ and E' contains a subgroup isomorphic to $\mu_{2/\mathcal{O}}$ (i.e., $E_{/\mathbf{Q}_2}$ contains a rational point P of order 2 which does not specialize to 0 in characteristic 2, while $E'_{/\mathbf{Q}_2}$ contains a rational point P' of order 2 which does specialize to 0 in characteristic 2). Consider the "diagonal" subgroup Δ of $Z/2\times\mu_2\subset E\times E'$ (the subgroup isomorphic to $\mathbf{Z}/2$ generated by the point (P,P')). Take $A=E$, $B=E\times E'/\Delta$ and $C=E'/\mu_2$, and take the morphisms to be the evident ones.

In this case f: $A\to B$ is *not* a closed immersion; if $A'_{/\mathbf{Z}_2}$ is the scheme-theoretic closure of $A_{/\mathbf{Q}_2}$ in $B_{/\mathbf{Z}_2}$, then A' is not smooth, (indeed, A is the *normalization* of A'; the morphism $A_0\to A'_0$ is an étale isogeny of degree 2) and the maps $\mathrm{Tan}(B_{/\mathbf{F}_2})\to\mathrm{Tan}(C_{/\mathbf{F}_2})$ and $\mathrm{Cot}(C_{/\mathbf{F}_2})\to\mathrm{Cot}(B_{/\mathbf{F}_2})$ are zero.

§ 2. Modular Curves

Let N be an arbitrary positive integer. Let m be the largest perfect square dividing N, and $S''=\mathrm{Spec}\,\mathbf{Z}[1/m]$. Let $X_0(N)_{/S''}$ denote the minimal regular model of $X_0(N)_{/\mathbf{Q}}$ (over the base S''). The results of [8] provide much information concerning the singular fibres of $X_0(N)_{/S''}$. (See also [19], Appendix, for N square-free and prime to 6.)

Let $J_{/\mathbf{Z}}=J_0(N)_{/\mathbf{Z}}$ denote the Néron model (over $\mathbf{Z}$) of the jacobian of $X_0(N)_{/\mathbf{Q}}$.

a) Degeneracy Operators

For every triple (d,N',N) where $d\cdot N'$ divides N, one has a morphism B_d: $X_0(N)\to X_0(N')$ (a "degeneracy operator") defined over $\mathbf{Q}$. It is defined on pairs (C_N, E) representing elliptic curves E with a cyclic subgroup, C_N of order N, by the following rule: Let $C_d\subset C_N$ denote the unique cyclic subgroup of order d. Set $E'=E/C_d$, $C_{N'}\subset C_N/C_d$ the unique cyclic subgroup of order N'. Then $B_d(C_N,E)=(C_{N'},E')$. On the upper half plane, B_d is induced by the map $z\mapsto dz$ i.e., $q\mapsto q^d$. (Compare [39, 1].)

The morphism B_d induce morphisms

$(B_d)^*$: $J_0(N')\to J_0(N)$,

$(B_d)_*$: $J_0(N)\to J_0(N')$.

b) The New Part of the Jacobian

We let $J_0(N)_{\mathrm{old}/\mathbf{Q}}\hookrightarrow J_0(N)_{/\mathbf{Q}}$ be the abelian subvariety (over $\mathbf{Q}$) generated by the images of the morphisms $(B_d)^*$ where (d,N',N) ranges through all triples of integers such that $d\cdot N'$ divides N, and $N'<N$. (Compare [39] § 4.)

Remark. Define the abelian variety $J_0(N)^{\text{old}}$ as the *quotient* of $J_0(N)$ by the connected component of the algebraic subgroup $\cap \ker(B_d)_*$; then one can check that the natural map $J_0(N)_{\text{old}} \to J_0(N)^{\text{old}}$ is an isogeny. It would be interesting to know something about the degree of this isogeny.

Define $J_0(N)^{\text{new}}_{/\mathbf{Q}}$ to be the quotient abelian variety, making the sequence

$$0 \to J_0(N)_{\text{old}/\mathbf{Q}} \to J_0(N)_{/\mathbf{Q}} \to J_0(N)^{\text{new}}_{/\mathbf{Q}} \to 0 \tag{2.1}$$

exact. Set $J^{\text{new}}_{/\mathbf{Z}} = J_0(N)^{\text{new}}_{/\mathbf{Z}} =$ the Néron model of $J_0(N)^{\text{new}}_{/\mathbf{Q}}$.

c) The Hecke Algebra

The Hecke operators T_l $(l \nmid N)$ and U_p $(p \mid N)$ may be viewed as endomorphisms of $J_0(N)_{/\mathbf{Q}}$ and they all leave J_{old} stable, and therefore may be viewed as endomorphisms of the exact sequence (2.1). The operators U_p (if $p^2 \mid N$) bring J into J_{old} and therefore induce the trivial endomorphism on J^{new} (compare [39] Thm. 3). The operators U_p (if $p \| N$) are equal to $-w_p$ on J^{new}, where w_p is the involution (as in [1] or [39]). Let $\mathbf{T}$ (*the* "Hecke algebra") denote the subring of the endomorphism ring $\text{End}_{\mathbf{Q}}(J^{\text{new}})$ generated by the T_l $(l \nmid N)$ and by the U_p $(p \mid N)$. Equivalently, it is the subring generated by the T_l $(l \nmid N)$ and by the w_p $(p \| N)$. If $M_{\mathbf{Q}} = \text{Cot}(J_{/\mathbf{Q}})$ and $M^{\text{new}}_{\mathbf{Q}} = \text{Cot}(J^{\text{new}}_{/\mathbf{Q}})$ then $M_{\mathbf{C}} = M_{\mathbf{Q}} \otimes \mathbf{C}$ may be identified with the space of cusp forms for $\Gamma_0(N)$, of weight 2, while $M^{\text{new}}_{\mathbf{Q}} \otimes \mathbf{C} \subseteq M_{\mathbf{C}}$ is the subspace of newforms.

The following proposition is well known. Its proof is due to Ribet, based on an idea of Shimura and Casselman.

Proposition 2.1. *Let N be an arbitrary integer > 1. Set $A = J_0(N)^{\text{new}}_{/\mathbf{Q}}$, and $E = \text{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$.*

Then E is generated as a $\mathbf{Q}$-algebra by the Hecke operators T_l $(l \nmid N)$.

Proof. Let E' be the $\mathbf{Q}$-subalgebra generated by the Hecke operators T_l $(l \nmid N)$. We first show that E' is in the center of E. For, let f be a $\mathbf{Q}$-endomorphism of A. Since f commutes with the Frobenius endomorphism of the reduction of A at l, f commutes with T_l acting on the reduction of A at l, by the Eichler-Shimura relations. It follows that f commutes with T_l acting on A.

Now suppose A is $\mathbf{Q}$-isogenous to $A_1 \times A_2 \times \cdots \times A_r$ where the A_i are $\mathbf{Q}$-simple abelian varieties (over $\mathbf{Q}$). We have corresponding factorizations of the $\mathbf{Q}$-algebras

$$E \cong E_1 \times E_2 \times \cdots \times E_r,$$

$$E' \cong E'_1 \times E'_2 \times \cdots \times E'_r$$

where $E_i = \text{End}_{\mathbf{Q}}(A_i) \otimes \mathbf{Q}$, and E'_i is the image of E' in E_i.

Since A_i is $\mathbf{Q}$-simple, E_i is a division algebra. By [1], E'_i is a totally real number field such that $\dim A_i = [E'_i : \mathbf{Q}]$. To prove our proposition, it suffices to show that E'_i is a maximal commutative subfield in E_i (all i), for then $E'_i = E_i$. But $\text{End}_{\mathbf{Q}}(A_i) \otimes \mathbf{Q}$ cannot contain a (commutative) subfield F of degree $> \dim A_i$, as can be seen by considering the induced action of F on the Lie algebra of $A_{i/\mathbf{Q}}$.

d) Optimal Quotients

By an *optimal quotient* of $J_0(N)^{\text{new}}$ we shall mean an abelian variety quotient $J_0(N)^{\text{new}} \xrightarrow{\pi} A$ (*over* $\mathbf{Q}$) such that the kernel of π is a connected subgroup scheme (an abelian subvariety). It is evident that if $J_0(N)^{\text{new}} \xrightarrow{\pi'} A'$ is any quotient over $\mathbf{Q}$, there is a unique optimal quotient making

$$\begin{array}{ccc} J_0(N)^{\text{new}} & \xrightarrow{\pi} & A \\ & {\scriptstyle \pi'} \searrow \quad \swarrow {\scriptstyle \varphi} & \\ & A' & \end{array}$$

commutative, where φ is an isogeny. If $J_0(N)^{\text{new}} \xrightarrow{\pi} A$ is an optimal quotient, it follows from prop. 2.1 that $\ker \pi$ is stable under the action of $\mathbf{T}$. Therefore there is an induced action of $\mathbf{T}$ on A.

e) Cotangent Spaces and Relative Differentials

By the description of the coarse moduli scheme $M_{\Gamma_0(N)}$ given in [8] VI 6.9 it is clear that $X = X_0(N)_{/S''}$ is Cohen-Macaulay, purely of relative dimension 1, and therefore the duality theory of Grothendieck, as sketched in [8] II.2 applies. In particular, the relative dualizing complex of sheaves (2.1) *is* the sheaf of regular differentials $\Omega_{X_{/S''}}$[4]. Moreover, its sections over the "bad" fibres (of characteristics dividing N) admit a simple description ([8] II 6.9).

The natural morphism $\mathscr{P}ic^0(X_{/S''}) \to J_{/S''}$ identifies $\mathscr{P}ic^0(X_{/S''})$ with $J^0_{/S''}$, the "connected component of the Néron model" ([19] Appendix, Thm. 1.3; or [29]; or compare discussion in [7] after Thm. 2.5). Passing to tangent spaces along the zero-section over S' we obtain an isomorphism

$$i\colon\ H^1(X_{/S''}, \mathcal{O}_X) \xrightarrow{\approx} \mathrm{Tan}(J_{/S''}).$$

We now view $\mathrm{Cot}(J_{/S''})$ as the $\mathcal{O}_{S''}$-dual of $\mathrm{Tan}(J_{/S''})$ via the natural pairing, and $H^0(X_{/S''}, \Omega)$ as the $\mathcal{O}_{S''}$-dual of $H^1(X_{/S''}, \mathcal{O}_X)$ via Grothendieck duality. The mapping i then induces an isomorphism

$$\Theta\colon\ \mathrm{Cot}(J_{/S''}) \xrightarrow{\approx} H^0(X_{/S''}, \Omega).$$

Recall that the Tate curve ([8] VII Th. 2.1 or [12] A 1.2) over $\mathbf{Z}[1/m]\,[[q]]$ gives rise to a morphism

$$\tau\colon\ \mathrm{Spec}\,\mathbf{Z}[1/m]\,[[q]] \to X^{\text{smooth}}_{/S''} \qquad \text{(the smooth locus of } X \to S'').$$

The morphism τ identifies the formal completion of $X^{\text{smooth}}_{/S''}$ along the cuspidal section $\infty_{/S''}$ with

$$\mathrm{Spec}\,\mathbf{Z}[1/m]\,[[q]] = S''[[q]].$$

[4] Deligne and Rapoport denote this $\omega_{X/S''}$

By restricting a section of $H^0(X_{/S''}, \Omega)$ to the cotangent bundle of $\infty_{/S''}$ in $X_{/S''}$, we obtain a diagram

$$\begin{array}{ccccc} H^0 X_{/S''}, \Omega) & \xrightarrow{q\text{-exp}} & \mathbf{Z}[1/m]\,[[q]] & \sum a_i q^i \\ \downarrow{\scriptstyle v} & & \downarrow & \downarrow \\ \mathrm{Cot}_\infty(X_{/S''}) & \xrightarrow[\approx]{} & \mathbf{Z}[1/m] & a_1 \end{array}$$

where "q-exp" is the morphism induced by τ, and $\mathrm{Cot}_\infty(X_{/S''})$ is the cotangent space of X along the section $\infty_{/S''}$.

Lemma 2.1. *The triangle*

$$\begin{array}{ccc} \mathrm{Cot}(J_{/S''}) & \xrightarrow{\Theta} & H^0(X_{/S''}, \Omega) \\ & {\scriptstyle\mu}\searrow \quad \swarrow{\scriptstyle v} & \\ & \mathrm{Cot}_\infty(X_{/S''}) & \end{array}$$

is commutative up to sign, where μ is the natural restriction mapping on cotangent spaces induced from the standard morphism $X \to J$ (normalized so that $\infty \mapsto 0$).

Proof. The reader will first note that this is not evident.[5] Since the $\mathcal{O}_{S''}$-modules involved are torsion-free it suffices to check the compatibility with the base S'' replaced by Spec **C**, and Grothendieck duality replaced by Serre duality. To be sure, the proposition to be checked is valid for *any* smooth curve $X_{/\mathrm{Spec}\,\mathbf{C}}$. Let g be the genus of X, supposed > 0. Choose g distinct points $\infty = x_1, x_2, \ldots, x_g$ such that the invertible sheaf $\mathcal{O}_X(D)$ has vanishing H^1, where D is the divisor $x_1 + x_2 + \cdots + x_g$. By forming the cohomology of the evident exact sequence one deduces an isomorphism

$$\bigoplus_{i=1}^{g} \mathrm{Tan}_{x_i} X \xrightarrow{\approx} H^1(X, \mathcal{O}_X).$$

Combining the two isomorphisms above, one obtains an isomorphism

$$H^1(X, \mathcal{O}_X) \xrightarrow{\approx} \mathrm{Tan}\, J$$

and this can be checked to be the isomorphism $i_{/\mathrm{Spec}\,\mathbf{C}}$ (up to sign). Our compatibility formula then follows from well known formulas (e.g., compare the formula displayed in the middle of page 26 of [34] II § 8 with the discussion of (*loc. cit.*) § 10) which express the duality mapping as a sum of residues.

---

[5] It is curious that there is yet a "third" way of going from the cotangent space of the jacobian of a (pointed) curve to the cotangent space of the curve (at its base point). This is via extensions deduced from the generalized jacobian (see [34] VII § 19 *Remarque* p. 190). After a nontrivial demonstration this is seen (*loc. cit.*) to be equal to μ (or to $v \cdot \Theta$) up to sign

§ 3. The Geometry of the Cuspidal Sections

In this section we let $J_{/\mathbf{Q}} \to A_{/\mathbf{Q}}$ be any (nontrivial) optimal quotient of the new part of the jacobian of $X = X_0(N)$ and let $J_{/\mathbf{Z}} \to A_{/\mathbf{Z}}$ denote the induced morphism on Néron models. Let f: $X_{/S''}^{\text{smooth}} \to A_{/S''}$ be the composition of the above projection with the natural injection of $X_{/S''}^{\text{smooth}}$ into $J_{/S''}$ where $S'' = \operatorname{Spec} \mathbf{Z}[1/m]$ and m is the largest square dividing N.

We intend to study the geometry of the mapping f in a formal neighborhood of the section $\infty_{/S''}$. If f: $X \to Y$ is a morphism of finite type between noetherian schemes, we shall say that f is a *formal immersion* at a point x if the induced map on the completions of local rings $\hat{\mathcal{O}}_{Y, f(x)} \to \hat{\mathcal{O}}_{X,x}$ is surjective. This is equivalent to asking that the map induce an isomorphism between residue fields of x and $f(x)$, and that f be formally unramified at x ([44] EGA IV 17.4.4). Recall further that to check that f is formally unramified one has the "differential criterion" (EGA IV 17.4).

Proposition 3.1. *If A is a nontrivial optimal quotient of the new part of J, then the morphism*

$$f\colon X_{/S''}^{\text{smooth}} \to A_{/S''}$$

is a formal immersion along the section ∞ away from characteristic 2.

Proof. Let R be a field of characteristic $p \nmid 2$. Consider the diagram

$$\begin{array}{ccccccc} \operatorname{Cot}(A) & \to & \operatorname{Cot}(J) & \xrightarrow[\approx]{\Theta} & H^0(X_{/R}, \Omega) & \xrightarrow{q\text{-exp}} & R[[q]] \\ & & & & \downarrow & & \downarrow \\ & & & & \operatorname{Cot}(X_{/R}) & \xrightarrow{\cong} & R \end{array} \qquad \begin{array}{c} \sum_1^\infty a_i q^i \\ \downarrow \\ a_1 \end{array} \tag{3.1}$$

Note that the first morphism is an inclusion by Corollary 1.1. The isomorphism Θ is as in § 2(e).

Since $\operatorname{Cot}(A)$ is stable under the operators T_l and U_p, (§ 2(d)), we view it as a module over $\mathbf{T} \otimes R$. Since A is nontrivial, so is $\operatorname{Cot}(A)$, and consequently, there is a maximal ideal $\mathfrak{p} \subseteq \mathbf{T} \otimes R$ which lies in the support of the $\mathbf{T} \otimes R$ module $\operatorname{Cot}(A)$. If $k = (\mathbf{T} \otimes R)/\mathfrak{p}$ is the residue field, then k is a finite extension field of R. It is convenient to extend R to a field R' large enough so that there is an R-homomorphism of k to R'. Fixing such an R-homomorphism, the maximal ideal $\mathfrak{p}' = \ker(\mathbf{T} \otimes R' \to R')$ is in the support of the module $\operatorname{Cot}(A_{/R'})$. Dropping the $'$ from the notation, we may assume that there is a prime $\mathfrak{p}$ in $\operatorname{Supp} \operatorname{Cot}(A_{/R})$ whose residue field is R. By ([5] IV § 1.3 Cor. 1 to Prop. 7) there is a nonzero element $\omega \in \operatorname{Cot}(A_{/R})$ annihilated by $\mathfrak{p}$. Such an element is an eigenvector for T_l and U_p with eigenvalues lying in R. Consider, now, the diagram (3.1). If $\omega(q) \in R[[q]]$ denotes the q-expansion of ω, we have that

$$\omega(q) = a_1 q^1 + a_2 q^2 + \cdots$$

is *not* identically zero. If $p (= \operatorname{char} R)$ does not divide N, this comes from the q-expansion principle, together with the asserted injectivities of the above diagram. If

p does divide N, (and by our assumption we must have $p \| N$), then $X_{/R}$ breaks up into a union of two irreducible components, and the q-expansion principle merely insures that Θ is zero on the irreducible component containing ∞. However, ω is an eigenvector for the involution w_N, which permutes the two irreducible components, and therefore ω must be 0 on all of $X_{/R}$.

Now recall the standard recursive relations on the q-expansion coefficients in terms of the eigenvalues of the operators T_l and U_N. Explicitly, let

$$T_l \omega = c_l \cdot \omega,$$
$$U_N \omega = c_N \cdot \omega.$$

Then

$$a_{l.m} = c_l \cdot a_m + l \cdot a_{m/l},$$
$$a_{N.m} = c_N \cdot a_m.$$

These are the "classical" formulae of [1]. For a derivation of the first of these formulae in an algebraic context (over an arbitrary base R) see [12] 1.11.1. The second formula is obtained in the same way.

It follows that, if $a_1 = 0$, each of the coefficients a_m is 0, contradicting the nontriviality of ω. Thus $a_1 \neq 0$, and consequently f: $\mathrm{Cot}(A_{/R}) \to \mathrm{Cot}(X_{/R})$ is nonzero. q.e.d.

The same idea may be applied to the morphism $X_{\mathrm{split}}(p) \to J_0(p)^-$ of [19] III § 6, as shall be now explained. Recall that $X_{\mathrm{split}}(p)$ is the modular curve associated to the normalizer of the split Cartan subgroup in $\mathrm{GL}_2(\mathbf{F}_p)$. One checks easily that $X_{\mathrm{split}}(p) \cong X_0(p^2)/w_{p^2}$. Further, one has the two degeneracy maps $X_0(p^2) \underset{B_1}{\overset{B_p}{\rightrightarrows}} X_0(p)$, and the commutativity relations $w_p \cdot B_1 = w_{p^2} B_p$ and $w_p \cdot B_p = w_{p^2} \cdot B_1$. Let g: $X_0(p^2) \to J_0(p)$ be the map which associates to x the divisor class of $B_1(x) - B_p(x)$. One has the commutativity relation $-w_p \cdot g = g \cdot w_{p^2}$. Thus, if $J_0(p)^- = J_0(p)/(1 + w_p) \cdot J_0(p)$, we obtain a commutative diagram

$$\begin{array}{ccc} X_0(p^2) & \longrightarrow & J_0(p) \\ \downarrow & & \downarrow \\ X_{\mathrm{split}}(p) & \longrightarrow & J_0(p)^-. \end{array}$$

Let $J_0(p)^- \to A$ be any optimal quotient, and consider the composition mapping h: $X_0(p^2) \to A$. It extends to a morphism h: $X_0(p^2)_{/S'} \to A_{/S'}$ of smooth schemes.

Proposition 3.2. *The morphism h is a formal immersion along the section $\infty_{/S}$, in characteristics different from 2 and p.*

Proof. The argument is similar to the preceding. Since we have already seen that for a field of characteristic different from 2 the induced morphism $\mathrm{Cot}(A_{/R}) \to \mathrm{Cot}(J_0(p)_{/R})$ is injective, we may consider a nonzero element ω of $\mathrm{Cot}(J_0(p)_{/R})$ contained in $\mathrm{Cot}(A_{/R})$ which is an eigenvector for all the T_l and U_p (R

being suitably enlarged, if necessary, as in the proof of Proposition 3.1), and we must prove that the induced cotangent vector $\mathrm{Cot}(g)(\omega) \in \mathrm{Cot}(X_0(p^2)_{/R})$ is nonzero. But, as in the previous argument, if the q-expansion of ω is $a_1 q^1 + a_2 q^2 + \cdots$ then $a_1 \neq 0$ (using that ω is a simultaneous eigenvector). Moreover, since $g = B_1 - B_p$, the q-expansion of $g^* \omega$ is $\sum a_i q^i - \sum a_i q^{pi} = a_1 q^1 +$ higher order terms. Again, as in the previous argument, under the natural identification of $\mathrm{Cot}(X_0(p^2)_{/R})$ with R, a parabolic form is sent to the leading term of its q-expansion. Consequently $\mathrm{Cot}(g)(\omega) \neq 0$.

§ 4. First Applications of Proposition 3.1

a) *The Constant "c" of a Strong Weil Curve*

Let $E_{/\mathbf{Q}}$ be a strong Weil curve in the sense of [22]. That is, if N is its analytic conductor ([39, 22] 2.1) we are given a morphism $\pi: X_0(N) \to E$ over $\mathbf{Q}$ expressing the elliptic curve $E_{/\mathbf{Q}}$ as an optimal quotient of the new part of the jacobian of $X_0(N)$. Moreover, π is normalized so that $\pi(\infty)$ is the origin. If ω is a Néron differential for $E_{/\mathbf{Q}}$ (i.e., an invariant differential on the Néron model $E_{/\mathbf{Z}}$ which does not vanish on any fibre) then we may write the q-expansion of $\pi^*(\omega)$ in the form

$$c(q^1 + a_2 q^2 + \cdots)$$

where $c \in \mathbf{Q}^*$. By adjusting the sign of ω we may suppose that $c > 0$.

Manin has conjectured that $c = 1$. We prove:

Corollary 4.1. *The rational number c is a unit in $\mathbf{Z}[1/2 \cdot m]$ where m is the largest square dividing N.*

Proof. This is an immediate corollary of Proposition 3.1.

Corollary 4.2. *If E is a strong Weil curve of square-free conductor, then $c(E)$ is a power of 2.*

b) *Potentially Good Reduction for Elliptic Curves Supporting Isogenies*

Corollary 4.3. *Let K be a number field, and N a square-free number. Let $\mathfrak{p}$ be a prime of K, of characteristic p* (possibly dividing N) *such that the ramification index at $\mathfrak{p}$ satisfies the inequality*

$$e_{\mathfrak{p}}(K/\mathbf{Q}) < p - 1.$$

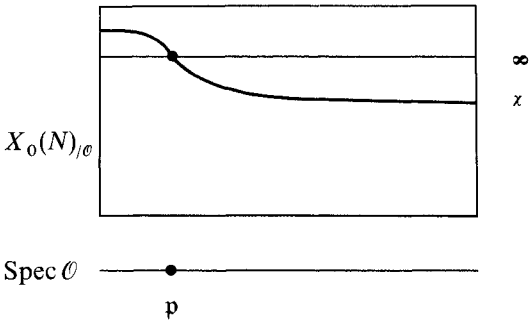
Let $E_{/K}$ be an elliptic curve possessing a K-rational cyclic subgroup C_N of order N. Let $x = j(C_N, E) \in X_0(N)(K)$. Suppose there exists an optimal quotient $f: J_0(N)^{\mathrm{new}} \to A$ such that $f(x)$ is of finite order in $A(K)$. (This is necessarily true if the Mordell-Weil group $A(K)$ is finite.) *Then E has potentially good reduction at $\mathfrak{p}$.*

Proof. Suppose that E has potentially multiplicative reduction at $\mathfrak{p}$. The point x then specializes to one of the cusps at $\mathfrak{p}$. Since N is square-free, the group of involutions $W = \{w_d \mid 1 \leqq d \mid N\}$ operates transitively on the cusps. Applying an involution w_d to x, if necessary, we may suppose that $x_{/k(\mathfrak{p})} = \infty_{/k(\mathfrak{p})}$. Let $f_{/\mathbf{Z}}$:

$X_0(N)_{/\mathbf{Z}} \to A_{/\mathbf{Z}}$ be the map to the optimal quotient occurring in the assertion of our corollary. Since $1 \leqq e < p-1$, we have that $p \neq 2$, and therefore by Proposition 3.1, f is a formal immersion at $\infty_{/k(\mathfrak{p})}$.

Since $f(x)$ is assumed to be of finite order, and $e < p-1$, the specialization lemma (§ 1(d)) applies, and shows that $f(x)$ vanishes, since it specializes to 0 at $\mathfrak{p}$ in characteristic p.

We have, therefore, the following state of affairs: the two $\mathcal{O}$-sections of $X_0(N)$, $x_{/\mathcal{O}}$ and $\infty_{/\mathcal{O}}$, "cross" at $\mathfrak{p}$, and map to the same section of A under $f_{/\mathcal{O}}$ (the zero-section). But this contradicts the fact that f is a formal immersion at $\infty_{/k(\mathfrak{p})}$.



Since this is a key point, we spell out the elementary proof that the above diagram contradicts the fact that f is a formal immersion at $\infty_{/k(\mathfrak{p})}$:

If $\hat{\mathcal{O}}_{\mathfrak{p}}[[q]]$ is the formal completion of $X_0(N)$ at $\infty_{/k(\mathfrak{p})}$ then the ∞-section "is" the homomorphism

$$\hat{\mathcal{O}}_{\mathfrak{p}}[[q]] \to \hat{\mathcal{O}}_{\mathfrak{p}} \quad (q \mapsto 0)$$

while the section $x_{/\hat{\mathcal{O}}_p}$ "is" the homomorphism

$$\hat{\mathcal{O}}_{\mathfrak{p}}[[q]] \to \hat{\mathcal{O}}_{\mathfrak{p}} \quad (q \mapsto q_0)$$

for some nonzero q_0. If $\mathscr{A}$ is the formal completion of $0_{/k(\mathfrak{p})}$ in $A_{/\mathcal{O}'}$ then since f is a formal immersion at $\infty_{/k(\mathfrak{p})'}$, f induces a *surjection* $\mathscr{A} \to \hat{\mathcal{O}}_{\mathfrak{p}}[[q]]$ which is incompatible with the assertion that the two homomorphisms $\mathscr{A} \to \hat{\mathcal{O}}_{\mathfrak{p}}$ induced by $q \mapsto 0$ and $q \mapsto q_0 \neq 0$ coincide. q.e.d.

From this point on, N will designate a rational *prime* number.

Corollary 4.4. *Let $K = \mathbf{Q}$, and $N = 11$ or $N =$ a prime number $\geqq 17$. Then any elliptic curve over $\mathbf{Q}$ which possesses a $\mathbf{Q}$-rational N-isogeny has potentially good reduction at all primes $p \neq 2$.*

Proof. Apply Corollary 4.3 with $A = \tilde{J}$, the Eisenstein quotient of $J_0(N)$ which has finite Mordell-Weil group by ([19] III 3.1).

c) Bounds on Rational Torsion

An immediate application of the above corollary is the following theorem which classifies all possible torsion groups of Mordell-Weil groups of elliptic curves

defined over $\mathbf{Q}$. The first proof *I* had for this theorem ([18, 19] III § 5) also used the theorem of finiteness of the Mordell-Weil group of the Eisenstein quotient of $J_0(N)$, but otherwise proceeded along significantly different lines.

Theorem 4.1 *(Conjecture of Ogg). Let Φ be the torsion subgroup of the Mordell-Weil group of some elliptic curve defined over $\mathbf{Q}$. Then Φ is isomorphic to one of the following fifteen groups:*

$$\mathbf{Z}/m\mathbf{Z} \qquad m=1,\ldots,10 \quad \text{or} \quad m=12$$
$$\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2v\mathbf{Z} \qquad v=1,\ldots,4.$$

Remark. All fifteen of the above groups do occur. Indeed the associated moduli problems are of genus 0, and there are known rational parametrizations of (infinite) families of elliptic curves whose Mordell-Weil groups (over $\mathbf{Q}$) contain each of the above groups. For a more complete discussion see [26, 18], and [13]. By known previous results (see [13], Main result 1) to prove the above theorem it suffices to show that a rational torsion point x of an elliptic curve $E_{/\mathbf{Q}}$ cannot have a prime order N, where $N \geqq 23$. We shall in fact show that such a torsion point cannot have a prime order N, where $N=11$ or $N \geqq 17$.

Proof. Suppose there is such an $(x, E_{/\mathbf{Q}})$. Let $C_N = \langle x \rangle$ be the subgroup of E generated by x. It follows by the previous corollary that E has potentially good reduction at all primes $p \neq 2$. In particular, E has potentially good reduction at $p=3$. Since the specialization of $x_{/\mathbf{Z}}$ to the Néron fibre $E_{/\mathbf{F}_3}$ cannot be zero, by the specialization lemma, the Néron fibre $E_{/\mathbf{F}_3}$ possesses a point of order N. It follows that $E_{/\mathbf{F}_3}$ cannot be of additive type. For, if it were, by the tables of ([40] § 6) the group of connected components is of order $\leqq 4$, and therefore $x_{/\mathbf{F}_3}$ would be contained in the connected component of $E_{/\mathbf{F}_3}$ which is isomorphic to $\mathbf{G}_a$: a contradiction since $N>3$. Therefore $E_{/\mathbf{F}_3}$ is an elliptic curve. This easily implies that the order of the group $E(\mathbf{F}_3)$ is $\leqq 7$, which is a contradiction since $N>7$.

We may apply the results of [18] to obtain a partial analogue of Corollary (4.4) for quadratic imaginary number fields.

Corollary 4.5. *Let K be a quadratic imaginary number field. There is a finite set of rational primes $\mathcal{N}_1(K)$ such that, if N is a rational prime not in $\mathcal{N}_1(K)$ which remains prime in K, and $E_{/K}$ is an elliptic curve possessing a K-rational N-isogeny, then E has potentially good reduction at all primes $\mathfrak{p}$ of K such that* $\operatorname{char} k(\mathfrak{p}) \geqq 5$ (and also at primes $\mathfrak{p}$ such that $\operatorname{char} k(\mathfrak{p})=3$, provided that 3 is unramified in K).

Proof. This is an immediate application of Corollary (4.3) and [18].

Corollary 4.6. *Let K be an imaginary quadratic field. There is a finite set of primes $\mathcal{N}'(K)$ such that, if N is a rational prime not in $\mathcal{N}'(K)$ which remains prime in K, then no elliptic curve $E_{/K}$ possesses a K-rational torsion point of order N.*

Proof. The proof is based on the previous corollary and proceeds along exactly the same lines as the proof of Theorem 4.1.

Note that one can take $\mathcal{N}'(K) = \mathcal{N}_1(K) \cup \{\text{all prime numbers} \leqq 31\}$, and therefore it is feasible to exhibit $\mathcal{N}'(K)$ for any given quadratic imaginary number field K. In § 7 we shall prove a "stronger" result (Prop. 8.1 for K-rational N-

isogenies). However, the set of primes $\mathcal{N}(K)$ that must be excluded in Proposition 8.1 is not effectively determined.

d) Construction of Points of Infinite Order in all Factors of $J_0(N)$ Over Suitable Number Fields

We shall indicate how Corollary 4.4 can be used to provide points of infinite order.

Let $E_{/\mathbf{Q}}$ be an elliptic curve with multiplicative reduction at 3. Let $E^0_{/\mathbf{Z}_3}$ be the connected component of its Néron model over $\mathbf{Z}_3$. Fix $\bar{\mathbf{Q}}_3$, an algebraic closure of $\mathbf{Q}_3$. Let N be a prime number >3. Let $C_N \subset E^0[N](\bar{\mathbf{Q}}_3)$. Then C_N is a cyclic subgroup of order N in $E[N](\bar{\mathbf{Q}}_3)$, stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}_3/\mathbf{Q}_3)$. Choose an imbedding of $\bar{\mathbf{Q}}$ in $\bar{\mathbf{Q}}_3$. By means of this imbedding we may identify $E[N](\bar{\mathbf{Q}})$ with $E[N](\bar{\mathbf{Q}}_3)$, and C_N with a subgroup of $E[N](\bar{\mathbf{Q}})$. Let $K^N \subset \bar{\mathbf{Q}}$ denote the field of rationality of the subgroup C_N. That is, $\mathrm{Gal}(\bar{\mathbf{Q}}/K_N) = \{g \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) | g \cdot C_N = C_N\}$. Then the prime $\mathfrak{p}$ of K^N determined by the above imbedding of $\bar{\mathbf{Q}}$ in $\bar{\mathbf{Q}}_3$ is of degree one over $\mathbf{Q}$, and, in particular, is absolutely unramified. The point $e_N = j(C_N, E)$ is in $X_0(N)(K^N)$.

Corollary 4.7. *With the notation of the discussion above, the point e_N projects to a point of infinite order in every nontrivial optimal quotient A of $J_0(N)$.*

Proof. By the above discussion, $e_{\mathfrak{p}}(K^N/\mathbf{Q}) = 1 < 3-1$. If there were a nontrivial optimal quotient A of $J_0(N)$ such that e_N mapped to an element of finite order in $A(K^N)$, then Corollary 4.3 would apply, giving us that E has potentially good reduction at $\mathfrak{p}$ which it does not, by our original choice.

e) Potentially Good Reduction for Elliptic Curves Representing Points in $X_{\mathrm{split}}(N)$

Let N be a prime number such that $N = 11$ or $N \geqq 17$. Let $E_{/\mathbf{Q}}$ be an elliptic curve such that the image of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ in $\mathrm{GL}_2(\mathbf{F}_N) = \mathrm{GL}(E[N])$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_N)$. Thus $E_{/\mathbf{Q}}$ represents a non-cuspidal point $x \in X_{\mathrm{split}}(N)(\mathbf{Q})$.

Corollary 4.8. *Under the above assumption, E has potentially good reduction at all primes $p \neq 2$, N such that $p \not\equiv \pm 1 \bmod N$. In particular, E has potentially good reduction for all primes p such that $2 < p < N-1$.*

Proof. The cusps of $X_{\mathrm{split}}(N)$ are as follows: there is a unique rational cusp ∞_{split} (the image of ∞ or $\mathbf{0}$ in $X_0(N^2)$); the remaining $(N-1)/2$ cusps are rational over the maximal real subfield

$$\mathbf{Q}(\zeta_N + \zeta_N^{-1}) = \mathbf{Q}(\zeta_N)^+$$

in $\mathbf{Q}(\zeta_N)$ (ζ_N a primitive N-th root of 1) and are all conjugate over $\mathbf{Q}$. A prime $\mathfrak{p}$ in $\mathbf{Q}(\zeta_N)$ of characteristic $p \neq N$ has residue field isomorphic to $\mathbf{F}_p$ if and only if $p \equiv \pm 1 \bmod N$. Therefore, if $\mathfrak{p}$ is of characteristic $p \not\equiv \pm 1 \bmod N$ ($p \neq N$) and $x_{/k(\mathfrak{p})}$ is a

cusp, we have $x_{/k(\mathfrak{p})} = \infty_{\text{split}/k(\mathfrak{p})}$. We shall now apply Proposition 3.2 following the general lines of the proof of Corollary 4.3.

Take $A = \tilde{J}$, the Eisenstein quotient; it is a quotient of $J_0(N)^-$ ([19] II 17.10). Consider the commutative diagram

$$\begin{array}{ccc} X_0(N^2) & \xrightarrow{g} & J_0(N)^- \\ \downarrow & \overset{h}{\searrow} & \downarrow \\ X_{\text{split}}(N) & \xrightarrow[f]{} & A \end{array}$$

where g is as in the discussion preceding Proposition 3.2, and the vertical maps are the natural ones. The map h: $X_0(N^2) \to A$ is a formal immersion at $\infty_{/\mathbf{F}_p}$ by Proposition 3.2. Thus the induced map f: $X_{\text{split}}(N) \to A$ is also a formal immersion at $\infty_{\text{split}/\mathbf{F}_p}$.

Since $A(\mathbf{Q})$ is a finite group by ([19] III 3.1), the section $f(x)$ is of finite order. Since it specializes to zero at $p > 2$, by the specialization lemma (§ 1(d)) we have $f(x) = 0$. But the same argument as in Corollary 4.3 (see diagram there) shows this to be in contradiction with the fact that f is a formal immersion at $\infty_{\text{split}/\mathbf{F}_p}$.

§ 5. The Isogeny Character

Let K be a number field, and (C_N, E) an N-isogeny defined over K. Consider the character

$$r\colon \operatorname{Gal}(\bar{K}/K)^{\text{ab}} \to \operatorname{Aut}(C_N) = (\mathbf{Z}/N\mathbf{Z})^*$$

defined by the natural action of Galois on the cyclic subgroup C_N.

Lemma 5.1. *Suppose that (C_N, E) is an N-isogeny defined over a number field K such that N remains prime in K. Then $\operatorname{Aut}_{\mathbf{C}}(C_N, E) = \{\pm 1\}$. That is, there are no exceptional automorphisms of the pair (C_N, E).*

Proof. There are three possibilities: $\operatorname{Aut}(C_N, E) = \mu_{2\gamma}$ (2γ-th roots of 1) where $\gamma = 1$, 2, or 3. Let g be a generator of $\operatorname{Aut}_{\mathbf{C}}(C_N, E)$. Since g leaves C_N stable, an elementary argument shows that g is defined over K. (If $\sigma \in \operatorname{Gal}(\bar{K}/K)$, one sees that g and g^σ induce the same automorphism of C_N; hence they must be equal since $N \neq 2, 3$.)

The action on the tangent space of $E_{/K}$ induces an injection of $\mathbf{Q}(g)$ (the subfield of $\operatorname{End}(E) \otimes \mathbf{Q}$ generated by g) into K. But if $\gamma = 2$ or 3, since g leaves C_N stable, the rational prime N splits in the quadratic field $\mathbf{Q}(g)$, and therefore cannot remain prime in K.

From here on, *suppose that N remains prime in K.* If U refers to the units of the ring of integers of a local field, and K_N is the completion of K at the prime N we have the commutative diagram

$$\begin{array}{ccccc} U(K_N) & \longrightarrow & \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}} & \xrightarrow{r} & \mathbf{F}_N^* \\ \Big\downarrow{\scriptstyle \mathrm{norm}} & & \Big\downarrow & & \\ U(\mathbf{Q}_N) & \longrightarrow & \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})^{\mathrm{ab}} & & \end{array}$$

where the left horizontal arrow comes from class field theory, and the vertical arrows are surjective. Since any continuous homomorphism $U(K_N) \to \mathbf{F}_N^*$ factors through $U(\mathbf{Q}_N)$, and may continuous homomorphism $U(\mathbf{Q}_N) \to \mathbf{F}_N^*$ is a power of the cyclotomic character, we have:

Lemma 5.2. *There is a unique k in $\mathbf{Z}/(N-1)\mathbf{Z}$ such that*

$$r = \alpha \cdot \chi^k$$

where χ: $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_N^*$ is the cyclotomic character, and α is unramified at N.

For the remainder of this paper, we will adhere to the following notational conventions:

$N \geqq 5$, a prime number,

$m = (N-1)/2$,

n = numerator of $\left(\dfrac{N-1}{12}\right)$,

$t = m/n$,

and here is a table to aid the reader in keeping track of these numbers:

N mod 12	m mod 6	t	
-1	-1	1	
5	2	2	(5.1)
7	3	3	
1	0	6	

Lemma 5.3. *Let α be as in Lemma 5.2. Then α^{2t} is an unramified character of $\mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$. If $K = \mathbf{Q}$ (or, more generally, if K has class number one) then the order of α divides $2t$* (which divides 12).

Proof. We use the cyclic Galois extensions with indicated orders:

$$X_1(N) \xrightarrow{t} X_2(N) \xrightarrow{n} X_0(N), \qquad X_1(N) \xrightarrow{m} X_0(N) \tag{5.2}$$

which are finite flat (Galois) morphisms over $S' = \mathrm{Spec}\,\mathbf{Z}[1/N]$. Moreover ([19] II Cor. 2.3) $X_2(N)_{/S'} \xrightarrow{\pi} X_0(N)_{/S'}$ is a finite étale morphism with Galois group equal to W_n, the unique quotient group of $(\mathbf{Z}/N\mathbf{Z})^*$ of order n.

If $x=j(C_N, E)\in X_0(N)(K)$, then the diagram makes it plain that there is an abelian field extension K'/K whose Galois group is cyclic, of order dividing m, such that if $\mathfrak{p}$ is a prime of K of characteristic different from N, then the ramification index $e_{\mathfrak{p}}(K'/K)$ divides t, and finally, there is a K'-rational point $x'\in X_1(N)(K')$ projecting to $x\in X_0(N)(K)$.

If $(C'_N, E')_{/K'}$ represents the point x', then the *isogeny character* of $(C'_N, E')_{/K'}$ is trivial (since it represents a point on X_1) and the two N-isogenies $(C'_N, E')_{/K'}$ and $(C_N, E)_{/K'}$ are twists of one another by a 1-cocycle representing a class in $H^1(\mathrm{Gal}(\bar{K}'/K'), \mathscr{A}ut(C_N, E))$. By Lemma 5.1 it follows that their isogeny characters differ by a quadratic character. Thus r restricted to $\mathrm{Gal}(\bar{K}'/K')$ is of order dividing $2t$; hence r^{2t} is unramified except in characteristic N, and therefore so is α^{2t}.

Proposition 5.1. *If E has potentially good reduction in characteristic N, the isogeny character r may be written in the form*

$$r=\alpha\cdot\chi^k \tag{5.3}$$

where α^{2t} is unramified everywhere, and where the integer k takes on only these values modulo m:

$k\equiv 0$, *or* $1 \mod m$,

$k\equiv 1/2 \mod m$ (only possible if $m\not\equiv 0 \bmod 2$),

$k\equiv 1/3$ *or* $2/3 \mod m$ (only possible if $m\not\equiv 0 \bmod 3$).[6]

Proof. Begin with a decomposition $r=\alpha\cdot\chi^k$ as in Lemma 5.2. Thus α is unramified at N. Since E has potentially good reduction at N there is a finite extension field L of K_N such that $E_{/\mathscr{O}(L)}$ has good reduction. That is, the Néron model $E_{/\mathscr{O}(L)}$ is an abelian scheme. By ([35] or more conveniently displayed in [32] $5.6a_1$) we may suppose that e, the absolute ramification index of L, is of the form $e=2e_0$ where $e_0=2$ or 3. The kernel of multiplication by N in $E_{/\mathscr{O}(L)}$ is a finite flat group scheme $E[N]_{/\mathscr{O}(L)}$ of order N^2. If θ is the fundamental character over L of level 1 (terminology as in [32] § 1) we have the relation $\chi=\theta^e$ by ([32] Prop. 8) as characters on the inertia subgroup $I\subset\mathrm{Gal}(\bar{L}/L)$. Consequently we have the equation $r=\theta^a$ where $a=2e_0k$ (again, as characters on the inertia subgroup I). If c and $d>0$ are integers, let $\langle c\rangle_d$ stand for the unique integer congruent to $c \bmod d$, in the range: $0\leqq\langle c\rangle_d<d$.

By Raynaud's theorem [31] applied to $E[N]_{/\mathscr{O}(L)}$ we have:

$$0\leqq\langle a\rangle_{N-1}\leqq e$$

or equivalently

$$0\leqq\langle e_0\cdot k\rangle_m\leqq e_0.$$

---

[6] This proposition might be compared with Theorem 10 of ([19]: introduction) which asserts that a rational point $x\in X_0(N)(\mathbf{Q})$ may specialize to one of a set of five particular connected components of the Néron fibre in characteristic N. Indeed, after Theorem 7.1 it is clear that the value $k \bmod m$ of the isogeny character r of (C_N, E) determines, and is determined by, the connected component of the Néron fibre in characteristic N containing the specialization of x. It would be of interest to establish a more general relationship of this type, valid for rational points over finite extensions of $\mathbf{Q}_N$, by local arguments

Let us first suppose that we have strict inequalities in the above. If $e_0 = 2$, then we have $2k \equiv 1$ modulo m which implies that $m \not\equiv 0 \bmod 2$ and $k \equiv 1/2 \bmod m$. If $e_0 = 3$, then $3k \equiv 1$ or $2 \bmod m$, which implies that $m \not\equiv 0 \bmod 3$, and $k \equiv 1/3$ or $2/3 \bmod m$. In this case the given decomposition $r = \alpha \cdot \chi^k$ satisfies the requirements of the conclusion of prop. 5.1.

Now suppose that an equality occurs. Without loss of generality we may suppose that $e_0 \cdot k \equiv 0 \bmod m$ (for otherwise replace the point $x \in X_0(N)$ by $w(x)$, k by $1-k, \ldots$). Since e_0 is either 2 or 3 a glance at the table (5.1) shows that g.c.d. (e_0, m) divides t. Consequently χ^k is of order dividing $2t$. We may achieve the assertion of the proposition, therefore, by taking $\alpha = r$ and $k = 0$.

An Alternate Route

To apply Proposition 5.1 we must know that E has potentially good reduction at N. This can be obtained by applying Proposition 3.1 *in characteristic N*. This, in turn, requires an appeal to some delicate geometry in characteristic N (e.g., Prop. 1.2 and the discussion of § 2(e) using Grothendieck duality). When $K = \mathbf{Q}$ one can avoid these considerations and obtain the conclusions of Proposition 5.1 (and therefore also a proof of Theorem 7.1), by the following alternate argument. Suppose $(C_N, E)_l$ is an N-isogeny (N prime, $\neq 2, 3, 5, 7$ and 13). Let $\tilde{x}$ be the image of $x = j(C_N, E)$ in $\tilde{J}$, the Eisenstein quotient of J. Since $\tilde{J}(\mathbf{Q})$ is finite, the point $\tilde{x}$ is of finite order. If $\tilde{x}$ is nonzero, by the specialization lemma, $\tilde{x}$ does not specialize to zero in any characteristic $\neq 2$. It follows that x cannot specialize to ∞ in any characteristic $\neq 2$. Applying this argument both to x and wx we see that without loss of generality we may suppose either that E has potentially good reduction in all characteristic $\neq 2$ (including N), or $\tilde{x} = 0$ in $\tilde{J}(\mathbf{Q})$. In the first case, Proposition 5.1 applies as above.

We now *suppose* $\tilde{x} = 0$, and use ([19] III Cor. 1.4) to deduce that x specializes to the irreducible component containing ∞ in $X_0(N)_{/\mathbf{F}_N}^{\text{smooth}}$. We shall extend the diagram (5.3) of schemes over $S' = \operatorname{Spec} \mathbf{Z}[1/N]$ to a diagram of algebraic spaces over S:

Lemma 5.4. *If $\mathscr{X}_0(N)_{/S}$ denotes the coarse moduli space over* $\operatorname{Spec} \mathbf{Z} = S$ *associated to the problem of classifying elliptic curves together with* étale *finite subgroup schemes of order N, and $\mathscr{X}_1(N)_{/S}$ denotes the* (coarse) *moduli space associated to the problem of classifying elliptic curves together with an isomorphism between the* constant *group scheme $\mathbf{Z}/N\mathbf{Z}$ and an étale finite subgroup scheme in E, then there is a diagram of smooth algebraic spaces and finite flat morphisms over S*

$$\mathscr{X}_1(N) \longrightarrow \mathscr{X}_2(N) \xrightarrow{\pi} \mathscr{X}_0(N)$$

where $\mathscr{X}_i(N)_{/S'} = X_i(N)_{/S'}$ ($i = 1$, 2, and 0). Moreover, the morphism

$$\mathscr{X}_2(N)_{/S} \xrightarrow{\pi} \mathscr{X}_0(N)_{/S}$$

is a finite étale (Galois) *morphism, with Galois group equal to W_n* (= the quotient of $(\mathbf{Z}/N\mathbf{Z})^*$ of order n).

Proof of Lemma 5.4. We quote Deligne-Rapoport [8]. Note that $\mathscr{X}_1(N)$ is just the algebraic stack $\mathscr{V}$ ([8] V 2.2; their p is our N) and $\mathscr{X}_0(N)$ is the coarse moduli scheme associated to the algebraic stack $\mathfrak{B}'_p$. For a general discussion of algebraic stacks, see [7], § 4.

The stack $\mathscr{V}$ is a finite étale covering of $\mathfrak{B}'_p$ with Galois group $(\mathbf{Z}/N)^*$. Division by the subgroup of order $2t$ in $(\mathbf{Z}/N)^*$ yields an intermediate stack $\mathscr{W}$, and we take the coarse moduli space of this intermediate stack to be $\mathscr{X}_2(N)_{/S}$.

Making use of ([8] I 8.2.1) we can determine the strict henselizations of the local rings of $\mathscr{W}$ and of $\mathscr{X}_2(N)$. The essential point is that the automorphism group of any geometric point z of $\mathscr{W}$ is equal to the automorphism group of the image of z in the stack $\mathfrak{B}'_p$, giving that π is unramified.

Since x specializes to the irreducible component containing ∞ in $X_0(N)^{\text{smooth}}_{/\mathbf{F}_N}$, one obtains that the closure of x in $\mathscr{X}_0(N)_{/S}$ is a section over $S=\operatorname{Spec}\mathbf{Z}$. Since $\mathscr{X}_2(N)_{/S} \to \mathscr{X}_0(N)_{/S}$ is a finite (cyclic) étale morphism, and since $\mathbf{Q}$ has no nontrivial everywhere unramified (finite cyclic) extensions, x lifts to an S-valued section of $\mathscr{X}_2(N)_{/S}$.

It follows that $x_{/\mathbf{Q}}$ lifts to a K-valued point of $X_1(N)$ where $K/\mathbf{Q}$ is a cyclic field extension of degree dividing t. Since $\mathscr{A}ut(C_N, E)=\{\pm 1\}$, it follows that the isogeny character r: $\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\to(\mathbf{Z}/N\mathbf{Z})^*$ is of order $2t$. Therefore we can take $k=0$, $r=\alpha$ for (5.3), and obtain the conclusion of Proposition 5.1.

§ 6. Congruences Implied by the Existence of an N-Isogeny

Now let K be a number field, N a rational prime which remains prime in K, and $\mathfrak{p}$ a prime of K of characteristic $\neq N$.

Let a K-rational N-isogeny (C_N, E) be given such that

E has potentially good reduction at $\mathfrak{p}$ and at N. (6.1)

Write the isogeny character of (C_N, E) in the form given by Proposition 5.1 above: $r=\alpha\cdot\chi^k$ and consider the restriction $\alpha_{\mathfrak{p}}$ of α to a decomposition group $\operatorname{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ at $\mathfrak{p}$. By local class field theory we have a factorization

$$\operatorname{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})^{\text{ab}} \cong U(K_{\mathfrak{p}}) \times \hat{\mathbf{Z}} \tag{6.2}$$

dependent upon a choice of uniformizing parameter for $\mathfrak{p}$.

We may consider the corresponding factorization $\alpha_{\mathfrak{p}}=\gamma_{\mathfrak{p}}\cdot b_{\mathfrak{p}}$, where $\gamma_{\mathfrak{p}}$ factors through the projection to $U(K_{\mathfrak{p}})$ in the factorization above, and $b_{\mathfrak{p}}$ is an unramified character. By Proposition 5.1, $\gamma_{\mathfrak{p}}$ has order dividing $2t$, and by construction, if $L\subset\bar{K}_{\mathfrak{p}}$ is the splitting field for the character $\gamma_{\mathfrak{p}}$, then $L/K_{\mathfrak{p}}$ is totally ramified.

Let P be the unique prime of $\mathcal{O}(L)$. We shall first prove that, under our hypotheses, *$E_{/L}$ has good reduction at P*. That is, the Néron model $E_{/\mathcal{O}(L)}$ is an abelian scheme. The reason for this is the following: The isogeny character for $(C_N, E)_{/L}$ is $b_{\mathfrak{p}}\cdot\chi^k$, which is unramified. Since formation of Néron model commutes with étale base change, it suffices to show that $E_{/\mathcal{O}(M)}$ is an abelian scheme, where $M\subset\bar{K}$ is the splitting field of the isogeny character r. But since E has potentially good reduction, either $E_{/\mathcal{O}(M)}$ is an abelian scheme, or its closed fibre is of additive type. But the latter

case is excluded since E possesses a rational point of order N (which is >4) over M, and the residue characteristic is different from N (the group of connected components of a Néron fibre of additive type is of order $\leqq 4$ by [40] § 6 Table).

Since L/K is totally ramified, we have $\mathcal{O}(L)/P = k_P \cong k_\mathfrak{p} = \mathcal{O}(K_\mathfrak{p})/\mathfrak{p}$. Denote by $E_{/k(\mathfrak{p})}$ the fibre of the Néron model $E_{/\mathcal{O}(L)}$ modulo P. By the above discussion, $E_{/k(\mathfrak{p})}$ is an elliptic curve, possessing an N-isogeny rational over $k_\mathfrak{p}$ with isogeny character equal to $b_\mathfrak{p} \cdot \chi^k$.

Notation. Let q_0 be a power of a rational prime p. Let q be a power of q_0. Let $a(\mathbf{F}_q/\mathbf{F}_{q_0})$ denote *any* integer which is the trace of Frobenius over the field $\mathbf{F}_q$ of some elliptic curve which can be defined over $\mathbf{F}_{q_0}$. If $q = q_0$, write $a(\mathbf{F}_q) = a(\mathbf{F}_q/\mathbf{F}_q)$. Note that $a(\mathbf{F}_q)^2 \leqq 4q$ by the "Riemann Hypothesis".

Example. (As can be verified by hand-calculation.)

$$\begin{aligned} &a(\mathbf{F}_{2^{12}}/\mathbf{F}_2) = +128,\ -128, \text{ or } -47 \\ &a(\mathbf{F}_{3^{12}}/\mathbf{F}_3) = +658,\ -1358, \text{ or } +1458. \end{aligned} \tag{6.3}$$

Now let $\sigma_\mathfrak{p} \in \mathrm{Gal}(\bar{k}_\mathfrak{p}/k_\mathfrak{p})$ be the Frobenius automorphism, and set $q_0 = N\mathfrak{p} = \mathrm{card}(k_\mathfrak{p})$.

Proposition 6.3. *With the notation and assumptions* (6.1) *above, we have:*

(1) $b_\mathfrak{p}(\sigma_\mathfrak{p}) \cdot q_0^k + b_\mathfrak{p}^{-1}(\sigma_\mathfrak{p}) \cdot q_0^{1-k}$ *is congruent* mod N *to one of the* $a(\mathbf{F}_{q_0})$,

(2) $q^k + q^{1-k}$ *is congruent to one of the* $a(\mathbf{F}_q/\mathbf{F}_{q_0})$ mod N,

where $q = q_0^v$ *and* v *is the order of the character* $b_\mathfrak{p}$.

Proof. Equation (1) is obtained by computing the trace of Frobenius of $E_{/k(\mathfrak{p})}$, while Equation (2) comes from computing the trace of Frobenius of E raised to the extension field of $k_\mathfrak{p}$ of degree v.

Corollary 6.1. *With the notation and assumptions* (6.1) *as above, suppose that* $K = \mathbf{Q}$. *Then*

(1) $b_\mathfrak{p}(\sigma_\mathfrak{p}) \cdot p^k + b_\mathfrak{p}^{-1}(\sigma_\mathfrak{p}) \cdot p^{1-k}$ *is congruent to one of the* $a(\mathbf{F}_p)$ mod N,

(2) $p^{12 \cdot k} + p^{12 - 12k}$ *is congruent to one of the* $a(\mathbf{F}_{p^{12}}/\mathbf{F}_p)$ mod N.

Proof. When $K = \mathbf{Q}$, Proposition 5.1 gives us that $b_\mathfrak{p}$ has order dividing $2t$, which in turn divides 12.

§ 7. Rational Isogenies of Prime Degree

Theorem 7.1. *Let* N *be a prime number such that the genus of* $X_0(N)$ *is* >0 (i.e., $N = 11$ or $N \geqq 17$). *Then there are no elliptic curves over* $\mathbf{Q}$ *possessing* $\mathbf{Q}$*-rational* N*-isogenies except when* $N = 11, 17, 19, 37, 43, 67,$ *or* 163. *Equivalently, there are no noncuspidal* $\mathbf{Q}$*-rational points on* $X_0(N)$ *except for the above values of* N. *In the above cases a complete list of the* $\mathbf{Q}$*-rational noncuspidal points of* $X_0(N)$ *is given in the table at the beginning of the introduction.*

Proof of Theorem 7.1. We suppose that $N=11$ or $N\geqq 17$, and $(C_N, E)_{/\mathbf{Q}}$ is an N-isogeny. Corollary 4.4 insures us that E has potentially good reduction at all primes $p>2$ and therefore the hypothesis of Proposition 5.1 is satisfied for $K=\mathbf{Q}$, $p>2$. Let $r=\alpha\cdot\chi^k$ be its isogeny character, as in Proposition 5.1.

Note that the canonical involution w on $X_0(N)$ interchanges k and $1-k$ and therefore we need only consider the three cases: $k\equiv 0$, $1/3$, and $1/2$ modulo m. By twisting appropriately by quadratic characters, we suppose that $k\equiv 0 \bmod N-1$, $3k\equiv 1 \bmod N-1$ and $2k\equiv 1+m \bmod N-1$ in the three respective cases above.

$k\equiv 0$: Apply Proposition 6.3 with $p=3$. Formula (2) and Example (6.3) give

$$1+3^{12}\equiv 658,\ -1358,\text{ or }+1458 \bmod N$$

and the only primes N for which this congruence is satisfied are:

$$N=2,\ 3,\ 5,\ 7,\ 13,\ 19,\ 37,\text{ and } 97.$$

The case $N=37$ does occur, while $N=19$ and 97 do not.[7] Besides citing [19] the most efficient way to eliminate the cases $N=19$, and 97, is to repeat the above argument using Proposition 6.3 taking $p=5$. When $p\geqq 5$, it is no longer practical to do the required arithmetic by hand. I am grateful to Neal Koblitz who did this (for all $p\leqq 23$) on a computer. In particular, he found that the only primes N dividing $1+5^{12}-a(\mathbf{F}_{5^{12}}/\mathbf{F}_5)$ are

$$N=2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 31,\ 37,\ 61,\ 157,\text{ and } 229$$

and thus 19 and 97 cannot occur when $k\equiv 0 \bmod m$.

$k\equiv 1/3$. Again we take $p=3$ and apply formula (2) of Proposition 6.3, and Example (6.3). We get the congruences

$$3^4+3^8\equiv 658,\ -1358,\text{ or }+1458 \bmod N$$

and the only primes N for which this congruence is satisfied are:

$$N=2,\ 3,\ 5,\ 11,\text{ and } 17.$$

Both cases $N=11$ and 17 do occur.

$k=1/2$. Here we may suppose that $2k\equiv 1+m \bmod N-1$, $t=1$ or 3, and $N\equiv -1 \bmod 4$.

Claim. If the above case occurs then for all odd primes $p<N/4$ we have $\left(\frac{p}{N}\right)=-1$.

Proof. Suppose $2<p<N/4$ and $\left(\frac{p}{N}\right)=+1$, i.e., $p^m\equiv +1 \bmod N$. Then $p^{1-k}\equiv p^k \bmod N$ and $p^{2k}\equiv p \bmod N$. Apply formula (1) of Proposition 6.3 to p and (noting that either $b_p(\sigma_p)$ or $-b_p(\sigma_p)$ is a 3-rd root of 1) we have:

$$p^k(\Theta+\Theta^{-1})\equiv a(\mathbf{F}_p) \bmod N$$

[7] Which follows from [19] Table in introduction

where Θ is a 3-rd root of 1. If Θ is a primitive 3-rd root of 1, then

$$-p^k \equiv a(\mathbf{F}_p) \bmod N$$

and squaring gives $a(\mathbf{F}_p)^2 = p$ (using the "Riemann hypothesis") which is absurd, for $a(\mathbf{F}_p)$ must be a rational integer. If $\Theta = 1$, then

$$4p \equiv a(\mathbf{F}_p)^2 \bmod N$$

and the Riemann hypothesis gives us that $a(\mathbf{F}_p)^2 = 4p$ again implying an irrational value for $a(\mathbf{F}_p)$.

To conclude our theorem, we shall now prove that the above *claim* implies that $\mathbf{Q}(\sqrt{-N})$ has class number 1 and hence (by Baker-Stark-Heegner [3, 37, 38]) we have $N = 11$, 19, 43, 67, or 163 (ignoring the genus 0 cases).

Since $N \equiv -1 \bmod 4$, quadratic reciprocity applied to (7.1) implies that for $2 < p < N/4$, p remains prime in $\mathbf{Q}(\sqrt{-N})$.

Thus all ideals I of odd norm $< N/4$ are principal in the ring of integers of $\mathbf{Q}(\sqrt{-N})$. To be sure, if we had the stronger assertion that *all* ideals of norm $< N/4$ were principal, then $\mathbf{Q}(\sqrt{-N})$ would have class number 1 by Minkowski's theorem: the absolute value of the discriminant of $\mathbf{Q}(\sqrt{-N})$ is N; the Minkowski constant is $2/\pi$; and $2/\pi \cdot \sqrt{N} < N/4$ for $N \geqq 11$. We shall prove this stronger assertion. If 2 does not split in $\mathbf{Q}(\sqrt{-N})$, there is nothing to prove. Suppose, then, that 2 does split, in which case $N \equiv -1$ or 7 mod 16. We must show that one (and hence both) of the primes of norm 2 are principal. If $N \equiv -1 \bmod 16$, consider the element $\alpha = (3 + \sqrt{-N})/2$. One sees that the norm of α is twice an odd number; hence $(\alpha) = \mathfrak{p} \cdot I$ where $\mathfrak{p}$ is one of the primes of norm 2, and I is an "odd" ideal, with norm $(9+N)/8$. Since $N \geqq 11$, the norm of I is less than $N/4$, and therefore I is principal. Consequently so is $\mathfrak{p}$. If $N \equiv 7 \bmod 16$, take the element $\alpha = (1 + \sqrt{-N})/2$, and repeat the above argument.

§ 8. N-Isogenies Over Quadratic Imaginary Fields in which N Remains Prime

Proposition 8.1. *Let K be a quadratic imaginary field. There is a finite set of primes $\mathcal{N}(K)$ such that, if N is a rational prime which remains prime in K and $N \notin \mathcal{N}(K)$, then there is no elliptic curve defined over K possessing a K-rational N-isogeny.*

Proof. Firstly it was shown in [18] that there is a finite set of primes $\mathcal{N}_1(K)$ such that if N is a rational prime which remains prime in K and $N \notin \mathcal{N}_1(K)$, then there is a nontrivial optimal quotient A of $J_0(N)$ such that $A(K)$ is finite. It follows from Corollary 4.5 that any elliptic curve $E_{/K}$ possessing a K-rational N-isogeny (N remaining prime in K, and $N \notin \mathcal{N}_1(K)$) has potentially good reduction at all primes $\mathfrak{p}$ of K of characteristic $\geqq 3$ if 3 is unramified in K, and at all primes of characteristic $\geqq 5$ in general.

Fix $(C_N, E)_{/K}$ with N as in the assertion of the proposition. Let h denote the class number of K, and consider the isogeny character $r = \alpha \cdot \chi^k$, as in Proposition 5.1. Consider the two cases:

$k \not\equiv 1/2 \bmod m$: This is the easy case. Choose $\mathfrak{p}$ a prime of K of characteristic 3 (if 3 is unramified in K) or 5 (if 3 is ramified). Set $q_0 = N\mathfrak{p}$ and $q = q_0^{12h}$.

Proposition 6.3, formula (2), then gives the congruence

$$1+q \equiv a(\mathbf{F}_q/\mathbf{F}_{q_0}) \bmod N \qquad (\text{if } k \equiv 0 \bmod N-1),$$
$$q_0^{4h}+q_0^{8h} \equiv a(\mathbf{F}_q/\mathbf{F}_{q_0}) \bmod N \quad (\text{if } 3k \equiv 1 \bmod N-1).$$

Let $\mathcal{N}_2(K)$ denote the set of rational primes dividing one of the numbers

$$\begin{matrix} 1+q-a(\mathbf{F}_q/\mathbf{F}_{q_0}) \\ q_0^{4h}+q_0^{8h}-a(\mathbf{F}_q/\mathbf{F}_{q_0}) \end{matrix} \tag{8.1}$$

for the above choice of q_0 and q, where $a(\mathbf{F}_q/\mathbf{F}_{q_0})$ ranges as above through all integers which are the trace of Frobenius over $\mathbf{F}_q$ of some elliptic curve definable over $\mathbf{F}_{q_0}$. By the "Riemann hypothesis" (8.1) is a finite set of *nonzero* integers. Hence $\mathcal{N}_2(K)$ is finite, and by Proposition 5.1 and 6.3, N belongs to $\mathcal{N}_2(K)$, if $k \not\equiv 1/2 \bmod m$.

$k \equiv 1/2 \bmod m$: (Hence $N \equiv -1 \bmod 4$; $2k \equiv 1+m \bmod N-1$; $2t = 2$ or 6.)

With the notation of Proposition 6.3 we have

$$\chi^k(\sigma_\mathfrak{p}) \cdot \left(b_\mathfrak{p}(\sigma_\mathfrak{p}) + \binom{N\mathfrak{p}}{N} \cdot b_\mathfrak{p}^{-1}(\sigma_\mathfrak{p})\right) \equiv a(k_\mathfrak{p}) \bmod N \tag{8.2}$$

where $\mathfrak{p}$ is any prime of K of characteristic p, with $3 < p < N$. We may also take $p = 3$ if 3 doesn't ramify in K. Recall that the character $b_\mathfrak{p}$ depends upon the splitting (6.2) and therefore on the prime $\mathfrak{p}$. It is of order dividing $6 \cdot h$.

Fix c, a positive number such that the ideal class group of K is generated by classes which are represented by prime ideals $\mathfrak{p}$ of residual characteristic $\geqq 5$ such that $N\mathfrak{p} < c$.

Let $M \subset \bar{\mathbf{Q}}$ be the number field generated by all $12 \cdot h$-th roots of unity, and by $\sqrt[]{N\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ with $N\mathfrak{p} < c$.

Consider the finite set $\mathcal{S}$ consisting of pairs of algebraic integers of the form

$$(\sqrt[]{N\mathfrak{p}}, \Theta)$$

where:

(i) Θ is a $12 \cdot h$-th root of unity.

(ii) $\mathfrak{p}$ is a prime of K of residual characteristic $\geqq 5$, and $N\mathfrak{p} < c$.

(iii) $\sqrt[]{N\mathfrak{p}} \cdot \Theta$ is not an eigenvalue of Frobenius of any elliptic curve defined over $k_\mathfrak{p}$.

Let $\mathcal{N}_3(K)$ denote the (finite) set of rational primes N which divide any one of the integers

$$N_{M/\mathbf{Q}}(\sqrt[]{N\mathfrak{p}} \cdot (\Theta + \Theta^{-1}) - a(k_\mathfrak{p})), \tag{8.3}$$

where $N_{M/\mathbf{Q}}$ is the norm from M to $\mathbf{Q}$, $(\sqrt[]{N\mathfrak{p}}, \Theta) \in \mathcal{S}$, and $a(k_\mathfrak{p})$ satisfies our notational convention (i.e. $a(k_\mathfrak{p})$ ranges through all integers which are the trace of Frobenius of some elliptic curve defined over $k_\mathfrak{p}$).

The set (8.3) is a finite set of nonzero integers by (iii) and the "Riemann hypothesis".

Now suppose $N \notin \mathcal{N}_3(K)$. Let $\beta(\mathfrak{p})$ denote the order of the element $b_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ in the multiplicative group $\mathbf{F}_N^*$. Let $B(\mathfrak{p})$ be a primitive $\beta(\mathfrak{p})$-th root of 1 in M. Let $N\mathfrak{p}^* = \left(\frac{N\mathfrak{p}}{N}\right) \cdot N\mathfrak{p}$ and choose a square root of $\left(\frac{N\mathfrak{p}}{N}\right)$ in M. We then have a definite choice of square root of $N\mathfrak{p}^*$:

$$\sqrt{N\mathfrak{p}^*} = \sqrt{\left(\frac{N\mathfrak{p}}{N}\right)} \cdot \sqrt{N\mathfrak{p}}.$$

Let $L = \mathbf{Q}(B(\mathfrak{p}), \sqrt{N\mathfrak{p}^*}) \subset M$, and $\mathcal{O} = \mathcal{O}(L)$. There is a homomorphism

$$\psi\colon \mathbf{Z}[B(\mathfrak{p}), \sqrt{N\mathfrak{p}^*}] \to \mathbf{F}_N$$

which sends $B(\mathfrak{p})$ to $b_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ and $\sqrt{N\mathfrak{p}^*}$ to $\pm \chi^k(\sigma_{\mathfrak{p}})$. We may change our compatible choices of square roots $\left(\text{of } \left(\frac{N\mathfrak{p}}{N}\right) \text{ and } N\mathfrak{p}^*\right)$, if necessary, so that ψ sends $\sqrt{N\mathfrak{p}^*}$ to $\chi^k(\sigma_{\mathfrak{p}})$.

Since N is prime to $2 \cdot N\mathfrak{p}$, an elementary argument shows that the N-adic completions of $\mathcal{O}$ and $\mathbf{Z}[B(\mathfrak{p}), \sqrt{N\mathfrak{p}^*}]$ are equal, and therefore ψ extends to a homomorphism $\psi\colon \mathcal{O} \to \mathbf{F}_N$.

Suppose $\mathfrak{p}$ *has residual characteristic* $\geqq 5$, and $N\mathfrak{p} < c$.

Let $\Theta = \Theta(\mathfrak{p}) = \sqrt{\left(\frac{N\mathfrak{p}}{N}\right)} \cdot B(\mathfrak{p})$. Then Θ is a $12 \cdot h$-th root of 1,

and

$$\sqrt{N\mathfrak{p}^*} \cdot \left(B(\mathfrak{p}) + \left(\frac{N\mathfrak{p}}{N}\right) \cdot B(\mathfrak{p})^{-1}\right) = \sqrt{N\mathfrak{p}} \cdot (\Theta + \Theta^{-1}).$$

By (8.2), for a suitable $a(k_{\mathfrak{p}})$ we have:

$$\psi\left(\sqrt{N\mathfrak{p}^*} \cdot \left(B(\mathfrak{p}) + \left(\frac{N\mathfrak{p}}{N}\right) \cdot B(\mathfrak{p})^{-1}\right) - a(k_{\mathfrak{p}})\right) = 0.$$

It follows that N divides the norm

$$N_{M/\mathbf{Q}}\left(\sqrt{N\mathfrak{p}^*} \cdot \left(B(\mathfrak{p}) + \left(\frac{N\mathfrak{p}}{N}\right) \cdot B(\mathfrak{p})^{-1}\right) - a(k_{\mathfrak{p}})\right)$$

but since $N \notin \mathcal{N}_3(K)$, we then must have that $\sqrt{N\mathfrak{p}} \cdot \Theta$ does not satisfy condition (iii), or,

$$\sqrt{N\mathfrak{p}} \cdot (\Theta + \Theta^{-1}) = a(k_{\mathfrak{p}}),$$

for a suitable $a(k_{\mathfrak{p}})$.

This equation implies (by elementary calculation, separating the cases $N\mathfrak{p} = p$ and $N\mathfrak{p} = p^2$) that Θ has only these possible orders: 1, 2, 3, 4, or 6. It follows that $\alpha(\sigma_{\mathfrak{p}})^{12} = 1$ for all $\mathfrak{p}$ of residual characteristic $\geqq 5$, and such that $N\mathfrak{p} < c$.

Since α^{12} is an unramified character (Prop. 5.3), by choice of the number c, we have $\alpha^{12}=1$. In particular, $\Theta=\Theta(\mathfrak{p})$ has order dividing 12 for all $\mathfrak{p}$ of residual characteristic $\geqq 5$ and such that $N\mathfrak{p}<N$. But since $N\equiv -1 \bmod 4$, the possible orders of $B(\mathfrak{p})$ are: 1, 2, 3, or 6.

Lemma 8.1. *If $(C_N, E)_{/K}$ is an N-isogeny with $N\notin \mathcal{N}_1(K)\cup\mathcal{N}_2(K)\cup\mathcal{N}_3(K)$, then for all rational primes p which split or ramify in K, such that $3<p<N/4$, we have $\left(\frac{p}{N}\right)=-1$.*

Proof. Suppose that $\mathfrak{p}$ is a prime of K such that $N\mathfrak{p}=p$ and $\left(\frac{p}{N}\right)=+1$, where $3<p<N/4$.

Then by formula (8.2) we have

$$a(\mathbf{F}_p)^2\equiv p(b^2+b^{-2}+2) \bmod N$$

where $b=b_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ is an element in $\mathbf{F}_N^*$ of order 1, 2, 3, or 6. Thus

$$a(\mathbf{F}_p)^2\equiv 4\cdot p \bmod N \quad \text{if order } (b)=1 \text{ or } 2,$$
$$\equiv 3\cdot p \bmod N \quad \text{if order } (b)=3 \text{ or } 6.$$

Using the "Riemann hypothesis" one sees that the above congruences imply:

$$a(\mathbf{F}_p)^2=4\cdot p \quad \text{if order } (b)=1 \text{ or } 2,$$
$$=3\cdot p \quad \text{if order } (b)=3 \text{ or } 6.$$

But neither equality is possible since $a(\mathbf{F}_p)$ is a rational integer and $p>3$.

Let $\mathcal{N}_4(K)$ be the set of prime numbers N such that $\left(\frac{p}{N}\right)=-1$ for all primes p such that $3<p<N/4$ and p either splits or ramifies in K. By Goldfeld's theorem (see Appendix) $\mathcal{N}_4(K)$ is a finite set.

By the above discussion it is clear that Proposition 8.1 is proved where $\mathcal{N}(K)$ is the finite set of primes $\mathcal{N}_1(K)\cup\mathcal{N}_2(K)\cup\mathcal{N}_3(K)\cup\mathcal{N}_4(K)$.

Appendix. *An Analogue of the Class Number One Problem*

By D. Goldfeld

1. Let K be an algebraic number field of finite degree over $\mathbf{Q}$ with discriminant k, and let S be a finite set of rational primes. Define $\mathcal{N}(K, S)$ to be the set of rational integers N satisfying the conditions:

$-N$ is a discriminant of a quadratic field and for all primes $l\notin S$, $l<|N|/4$, if l splits completely in K, then l doesn't split in $\mathbf{Q}(\sqrt{-N})$.

In the case that K is equal to $\mathbf{Q}$ or a quadratic field, we shall show that $\mathcal{N}(K, S)$ is a finite set. The method of proof, however, is ineffective and all that can be deduced is the existence of a large constant $C(K, S)$ depending only on K and S such that

$$N \in \mathcal{N}(K,S) \Rightarrow |N| < C(K,S), \quad (\text{degree } K \leqq 2)$$

with at most one possible exception. The exceptional N can occur only if the Dedekind zeta function of either $\mathbf{Q}(\sqrt{-N})$ or $\mathbf{Q}(\sqrt{-kN})$ has a Siegel zero; i.e., a real zero near to one.

Remark. For $|k| \leqq 10$, $S=\{2,3\}$, $c(K,S)$ may be taken to be e^{100}. However, we are grateful to Joe Buhler for making some computations which suggest that this constant can be much improved. Extracting from his print-out, we have made the following table:

key: $S=\{2,3\}$; $K=\mathbf{Q}(\sqrt{k})$;
p = largest prime $\leqq 32{,}768$ in $\mathcal{N}(K,S)$.

k	−1	−2	−3	−7	−11	−19	−43	−67	−163
p	193	163	163	163	163	163	163	163	239

It does not seem possible at present to establish the finiteness of $\mathcal{N}(K,S)$ if the degree of K is greater than two, although various well-known hypotheses do suggest that this is in fact the case. In particular, the truth of the generalized Riemann hypothesis for algebraic number fields would imply an effective version of Theorem A for all K, while the weaker Lindelöf hypothesis would give a similar but ineffective result.

2. In the sequel we take $K=\mathbf{Q}(\sqrt{k})$ to be a quadratic field, and for $-N \neq k$ put $F=\mathbf{Q}(\sqrt{k}, \sqrt{-N})$ and let

$$\zeta_F(s)=\zeta(s)\, L(s,\chi_k)\, L(s,\chi_N)\, L(s,\chi_k\chi_N)$$

be the Dedekind zeta function of the biquadratic field F. Here χ_k and χ_N are primitive quadratic characters of $\mathbf{Z}/k\mathbf{Z}$ and $\mathbf{Z}/N\mathbf{Z}$, respectively, while

$$\zeta(s)=\sum_{n=1}^{\infty} n^{-s}, \qquad L(s,\chi)=\sum_{n=1}^{\infty} \chi(n)\, n^{-s}$$

are the usual Riemann zeta function and Dirichlet L-function.

Now, define

$$f(s)=\zeta_F(s)\prod_{p\in S}(1-p^{-s})(1-\chi_k(p)\,p^{-s})(1-\chi_N(p)\,p^{-s})(1-\chi_k\chi_N(p)\,p^{-s}) = \sum_{n=1}^{\infty} A_n n^{-s}$$

$$g(s)=\zeta(2s)^2\prod_{p\in S}(1-p^{-2s})^2 = \sum_{n=1}^{\infty} B_n n^{-s}.$$

Lemma A. *If $N \in \mathcal{N}(K,S)$, then $A_n = B_n$ for all $n < |N|/4$.*

Proof. $f(s)$ has the Euler product

$$f(s)=\prod_{l\notin S}(1-l^{-s})^{-1}(1-\chi_k(l)\,l^{-s})^{-1}(1-\chi_N(l)\,l^{-s})^{-1}(1-\chi_k\chi_N(l)\,l^{-s})^{-1}.$$

But for $l \notin S$ and $l < |N|/4$ either $\chi_k(l) = -1$ or $\chi_N(l) = -1$, so the Euler factor for l must be of the form

$$(1 - l^{-2s})^{-2}$$

which is precisely the l-th Euler factor for $g(s)$. q.e.d.

Theorem A. *If k is a quadratic field, then there exists an effectively computable constant $C(K, S)$ depending only on K and S such that $N \in \mathcal{N}(K, S)$ implies that $|N| < C(K, S)$ with at most one possible exception.*

Proof. We use an idea of Linnik-Vinogradov [15]. Assume the theorem is false. Then by Lemma A there will be at least two discriminants $|N| \geqq C(K, S)$ for which

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} f(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} g(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds \tag{1}$$

since

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{s(s+1)\ldots(s+r)}\, ds = 0$$

for $0 < x < 1$ and any positive integer r. To ensure the absolute convergence of all the relevant integrals, we can simply take $r \geqq 5$.

Shifting the line of integration to $\mathrm{Re}(s) = -\frac{1}{4}$ and noting that $g(s)$ has a double pole at $s = \frac{1}{2}$, it follows that

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} g(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds = c_1 \sqrt{|N|} + c_2 \sqrt{|N|} \log |N| + \frac{g(0)}{n!}$$

$$+ \frac{1}{2\pi i} \int_{-\frac{1}{4}-i\infty}^{-\frac{1}{4}+i\infty} g(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds = \sqrt{|N|}\,(c_1 + c_2 \log |N|) + c_3 + O(|N|^{-\frac{1}{4}}) \tag{2}$$

for effectively computable constants c_1, c_2, c_3 depending only on S and r.

On the other hand,

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} f(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds$$

$$= \frac{|N|}{4(r+1)!} \Lambda \cdot \mathscr{P} + \frac{1}{2\pi i} \int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty} f(s) \frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\, ds \tag{3}$$

where

$$\Lambda = L(1, \chi_k)\, L(1, \chi_N)\, L(1, \chi_k \chi_N),$$

$$\mathscr{P} = \prod_{p \in S} \left(1 - \frac{1}{p}\right) \left(1 - \frac{\chi_k(p)}{p}\right) \left(1 - \frac{\chi_N(p)}{p}\right) \left(1 - \frac{\chi_k \chi_N(p)}{p}\right).$$

By the Siegel-Tatuzawa Theorem (see [35, 11, 42])

$$\Lambda > c_4 |N|^{-\varepsilon} \qquad (\varepsilon > 0) \tag{4}$$

except for at most one exceptional N. Here c_4 is an effectively computable constant depending on k and ε. Also, using Burgess' bounds [6] (obtained by using the known Riemann hypothesis for hypoelliptic curves over finite fields)

$$|L(\tfrac{1}{2}+it,\chi)| \ll q^{\frac{3}{16}+\varepsilon}|\tfrac{1}{2}+it| \quad (\chi \bmod q)$$

it is easily seen that

$$|f(\tfrac{1}{2}+it)| < c_5|N|^{\frac{3}{8}+\varepsilon}|\tfrac{1}{2}+it|^4 \tag{5}$$

where c_5 can be effectively computed and depends only on k and ε. It follows from (3), (4) and (5) that

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} f(s)\frac{(|N|/4)^s}{s(s+1)\ldots(s+r)}\,ds > c_6|N|^{1-\varepsilon}+O(|N|^{\frac{7}{8}+\varepsilon}).$$

Since this contradicts (1) and (2) for $\varepsilon < \frac{1}{16}$ and sufficiently large N the Theorem is proved. q.e.d.

References

1. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. **185**, 134–160 (1970)
2. Artin, M.: The implicit function theorem in algebraic geometry. Algebraic Geometry: Papers presented at the Bombay Colloquium 1968, 13–34, Oxford University Press 1969
3. Baker, A.: On the class number of imaginary quadratic fields. Bull Amer. Math. Soc. **77**, 678–684 (1971)
4. Berkovic, B.G.: Rational points on the jacobians of modular curves (in Russian). Mat. Sbornik T. **101 (143)**, No. 4 (12), 542–567 (1976)
5. Bourbaki, N.: Commutative algebra. Paris: Hermann 1972
6. Burgess, D.A.: On character sums and L-series II. Proc. London Math. Soc. (3) **13**, 524–536 (1963)
7. Deligne, P., Mumford, D.: The irreducibility of the space curves of given genus. Publ. Math. I.H.E.S. **36**, 75–109 (1969)
8. Deligne, P., Rapoprt, 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
9. Dickson, L.E.: Linear groups with an exposition of the Galois field theory. Leipzig: Teubner 1901
10. Fricke, R.: Die elliptischen Funktionen und ihre Anwendungen. I. Leipzig-Berlin: Teubner 1922
11. Goldfeld, D.M.: A simple proof of Siegel's theorem, Proc. Nat. Acad. Sci. USA **71**, 1055–1055 (1974)
12. Katz, N.M.: p-adic properties of modular schemes and modular forms. Vol. III of the Proceedings of the International Summer School on modular functions, Antwerp (1972). Lecture Notes in Mathematics 350, 68–190. Berlin-Heidelberg-New York: Springer 1973
13. Kubert, D.: Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. (3) **33**, 193–237 (1976)
14. Ligozat, G.: Courbes Modulaires de genre 1. Bull. Soc. Math. France, Mémoire **43**, 1–80 (1975)
15. Linnik, J.V., Vinogradov, A.I.: Hypoelliptic curves and the least prime quadratic residue. [in Russian] Dokl. Akad. Nauk CCCP **168**, 259–261 (1966). [Eng. transl.: Soviet Math. Dokl. **7**, 612–614 (1966)]
16. Manin, Y.: A uniform bound for p-torsion in elliptic curves [in Russian]. Izv. Akad. Nauk CCCP **33**, 459–465 (1969)
17. Manin, Y.: Parabolic points and zeta functions of modular curves [in Russian]. Izv. Akad. Nauk CCCP **36**, 19–65 (1972). [English transl.: Math. USSR Izv. **6**, 19–64 (1972)]

18. Mazur, B.: Rational points on modular curves. Proceedings of a conference on modular functions held in Bonn 1976. Lecture Notes in Math., 601, Berlin-Heidelberg-New York: Springer 1977
19. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. I.H.E.S. **47** (1977)
20. Mazur, B.: p-adic analytic number theory of elliptic curves and abelian varieties over $\mathbf{Q}$. Proc. of International Congress of Mathematicians at Vancouver, 1974, Vol. I, 369–377, Canadian Math. Soc. (1975)
21. 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
22. Mazur, B., Swinnerton-Dyer, H.P.F.: Arithmetic of Weil curves. Inventiones math. **25**, 1–61 (1974)
23. Mazur, B., Tate, J.: Points of order 13 on elliptic curves. Inventiones math. **22**, 41–49 (1973)
24. Mazur, B., Vélu, J.: Courbes de Weil de conducteur 26. C.R. Acad. Sc. Paris **275**, Série A, 743–745
25. Ogg, A.: Rational points on certain elliptic modular curves. Proc. Symp. Pure Math. **24**, 221–231 (1973), AMS, Providence
26. Ogg, A.: Diophantine equations and modular forms. Bull. Soc. Math. France **102**, 449–462 (1974)
27. Oort, F., Tate, J.: Group schemes of prime order. Ann. Scient. Éc. Norm. Sup., série **4**, **3**, 1–21 (1970)
28. Raynaud, M.: Faisceaux amples sur les schémas en groupes et les espaces homogènes. Lecture Notes in Mathematics **119**, Berlin-Heidelberg-New York: Springer 1970
29. Raynaud, M.: Spécialisation du foncteur de Picard, Publ. Math. I.H.E.S. **38**, 27–76 (1970)
30. Raynaud, M.: Passage au quotient par une relation d'équivalence plate. Proceedings of a conference on Local Fields, NUFFIC Summer School held at Driebergen in 1966, 133–157, Berlin-Heidelberg-New York: Springer 1967
31. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$, Bull. Soc. Math. France, **102**, 241–280 (1974)
32. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. **15**, 259–331 (1972)
33. Serre, J.-P.: p-torsion des courbes elliptiques (d'après Y. Manin). Séminaire Bourbaki ^{no} 380. Lecture Notes in Mathematics, 180, Berlin-Heidelberg-New York: Springer 1971
34. Serre, J.-P.: Groupes algébriques et corps de classes. Paris: Hermann 1959
35. Serre, J.-P., Tate, J.: Good reduction of abelian varieties, Ann. of Math. **88**, 492–517 (1968)
36. Siegel, C.L.: Über die Classenzahl quadratischer Zahlkörper. Acta Arith. **1**, 83–86 (1935). Also in Gesammelte Abhandlungen I, 406–409, Berlin-Heidelberg-New York: Springer 1966
37. Stark, H.M.: On complex quadratic fields with class-number equal to one. Trans. Amer. Math. Soc. **122**, 112–119 (1966)
38. Stark, H.M.: A complete determination of the complex quadratic fields of class-number one. Mich. Math. J. **14**, 1–27 (1967)
39. Swinnerton-Dyer, H.P.F., Birch, B.J.: Elliptic curves and modular functions. Modular functions of one variable IV (Proc. of the Int. Summer School, University of Antwerp, RUCA, 1972). Lecture Notes in Mathematics, 476, 2–31, Berlin-Heidelberg-New York: Springer 1975
40. Tate, J.: Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil, 33–53, Modular functions of one variable IV (Proc. of the Int. Summer School, University of Antwerp, RUCA, 1972). Lecture Notes in Mathematics, 476, Berlin-Heidelberg-New York: Springer 1975
41. Tate, J.: Classes d'isogénies des variétés abéliennes sur un corps fini (d'après T. Honda), Séminaire Bourbaki no. 352. Lecture Notes in Mathematics. 179 Berlin-Heidelberg-New York: Springer 1971
42. Tatuzawa, T.: On a theorem of Siegel. Japanese J. of math. **21**, 163–178 (1951)
43. Modular functions of one variable IV. (Ed. by B.J. Birch and W. Kuyk). Lecture Notes in Mathematics. 476 Berlin-Heidelberg-New York: Springer 1975
44. [EGA] Éléments de géométrie algébrique (par A. Grothendieck, rédigés avec la collaboration de J. Dieudonné) II. Étude globale élémentaire de quelques classes de morphismes. Publ. Math. I.H.E.S. **8** (1961). IV Étude locale des schémas et des morphismes de schémas. Publ. Math. I.H.E.S. **32** (1967)
45. [SGA 7 II] Groupes de Monodromie en Géométrie Algébrique (dirigé par A. Grothendieck avec la collaboration de M. Raynaud et D.S. Rim). Lecture Notes in Mathematics 288, Berlin-Heidelberg-New York: Springer 1972

Received July 11, 1977