The Manin Constant, Congruence Primes, and the Modular Degree

Amod Agashe Kenneth Ribet William Stein

January 16, 2005

Abstract

We obtain relations between the modular degree and congruence modulus of elliptic curves, and answer a question raised in a paper of Frey and Müller about whether or not the congruence number and modular degree of elliptic curves are always equal; they are not, but we give a conjectural relation between them. We also prove results and make conjectures about Manin constants of quotients of $J_1(N)$ of arbitrary dimension. For optimal elliptic curve, we prove that if 2 exactly divides N and the congruence number of E is odd, then the Manin constant of E is also odd.

1 Introduction

Let N be a positive integer and E be an optimal elliptic curve quotient of $J_0(N)$, where optimal means that $\ker(J_0(N) \to E)$ is connected. The Manin constant of E is an invariant associated to E that plays a role in the Birch and Swinnerton-Dyer conjecture (see Section 3.2.1). Manin conjectured that it is always equal to 1. In Section 2.1, we recall the definition of the Manin constant of an optimal elliptic curve quotient E of $J_0(N)$ and summarize previous results about it. We extend the techniques of Abbes and Ullmo [AU96] to show that if p is a prime such that p^2 does not divide N and p does not divide the congruence number of E, then p does not divide the Manin constant of E either. In light of what is known before, the only new information is that if 2 exactly divides N and the congruence number of E is odd, then the Manin constant of E is also odd.

In Section 2.2, we discuss the relation between the congruence number r_E associated to E and the modular degree m_E of E. It is known that $m_E \mid r_E$. Frey and Müller [FM99, Ques. 4.4] asked whether $r_E = m_E$; we give examples where $r_E \neq m_E$. These computations suggested that if p is a prime such that p^2 does not divide N, then p does not divide r_E/m_E, and we were able to prove this statement. We have not yet proved the more general conjecture that $\mathrm{ord}_p(r_E/m_E) \leq \frac{1}{2}\,\mathrm{ord}_p(N)$.

In Section 3, we consider optimal quotients of $J_1(N)$ and $J_0(N)$ of arbitrary dimension associated to ideals of the Hecke algebra. We generalize the notions of the congruence number, the modular degree and the Manin constant to such quotients, and give generalizations of some of the results from Section 2. We also make the conjecture that the generalized Manin constant is 1 for newform quotients of $J_0(N)$, which we support with data.

Finally, in Sections 4 and 5, we prove some of the results mentioned in the preceeding sections.

Acknowledgment. The authors are grateful to A. Abbes, R. Coleman, B. Conrad, E. de Shalit, B. Edixhoven, L. Merel, and R. Taylor for several discussions and advice regarding this paper. They would also like to thank J. Cremona for explaining his computations involving the Manin constant.

2 Optimal Elliptic Curve Quotients

Let N be a positive integer and let $X_0(N)$ be the modular curve over $\mathbf{Q}$ that classifies isomorphism classes of elliptic curves with a cyclic subgroup of order N. The Hecke algebra $\mathbf{T}$ of level N is the subring of the ring of endomorphisms of $J_0(N) = \mathrm{Jac}(X_0(N))$ generated by the Hecke operators T_n for all $n \geq 1$. Let f be a newform of weight 2 for $\Gamma_0(N)$ with integer Fourier coefficients, and let I_f be the annihilator of f under the action of $\mathbf{T}$. Note that I_f is also the kernel of the natural ring homomorphiam $\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots]$ that sends T_n to a_n. Then the quotient $E = J_0(N)/I_f J_0(N)$ is an elliptic curve over $\mathbf{Q}$. We call E the *optimal quotient* associated to f. Composing the embedding $X_0(N) \hookrightarrow J_0(N)$ that sends ∞ to 0 with the quotient map $J_0(N) \to E$, we obtain a surjective morphism of curves $\phi_E : X_0(N) \to E$.

Definition 2.1 (Modular Degree). The *modular degree* m_E of E is the degree of ϕ_E.

2.1 The Manin Constant

Let $E_{\mathbf{Z}}$ denote the Néron model of E over $\mathbf{Z}$ (see, e.g., [Sil92, App. C, §15], [Sil94] and [BLR90]). Let ω be a generator for the rank one $\mathbf{Z}$-module of invariant differential one forms on $E_{\mathbf{Z}}$. The pullback of ω to $X_0(N)$ is a differential $\phi_E^*\omega$ on $X_0(N)$. The newform f defines another differential $2\pi i f(z)dz$

on $X_0(N)$. Note that $f(q)dq/q = 2\pi i f(z)dz$, which explains the factor of $2\pi i$. Because the action of Hecke operators is compatible with the map $X_0(N) \to E$, the results of [AL70] imply that $\phi_E^* \omega = c \cdot 2\pi i f(z)dz$ for some $c \in \mathbf{Q}^*$ (see also [Man72, §5]).

Definition 2.2 (Manin Constant). The *Manin constant* c_E of E is the absolute value of c, where c is as above.

Note that c_E depends on E. The Manin constant plays a role in the Birch and Swinnerton-Dyer conjecture (see Section 3.2.1), and its integrality is important to Cremona's computations of elliptic curves (see [Cre97, pg. 45]).

The following conjecture is implicit in Manin's discussion of "Weil curves" in [Man72, §5].

Conjecture 2.3 (Manin). $c_E = 1$.

Significant progress has been made towards this conjecture. In the following, p denotes a prime and N denotes the conductor of E.

Theorem 2.4 (Edixhoven [Edi91, Prop. 2]). *c_E is an integer.*

Edixhoven proved this theorem using an integral q-expansion map, whose existence and properties he deduced from results in [KM85]. We generalize this theorem to quotients of arbitrary dimension in Section 3.2.3, using a very similar proof.

Theorem 2.5 (Mazur, [Maz78, Cor. 4.1]). *If $p \mid c_E$, then $p^2 \mid 4N$.*

Mazur proved this theorem by applying nontrivial theorems of Raynaud about exactness of sequences of differentials, then using the "q-expansion principle" in characteristic p and a trick involving the Atkin-Lehner involution. We generalize this result in Section 3.2.3, essentially by following Mazur's proof.

The following two results refine the above results at $p = 2$.

Theorem 2.6 (Raynaud [AU96, Prop. 3.1]). *If $4 \mid c_E$, then $4 \mid N$.*

Theorem 2.7 (Abbes-Ullmo [AU96, Thm. A]). *If $p \mid c_E$, then $p \mid N$.*

We generalize Theorem 2.6 in Section 3.2.3. However, it is not clear if one can generalize Theorem 2.7 to dimension greater than 1; for the obstruction, see Remark 5.3. It would be fantastic if the theorem could be generalized, since it would imply that for quotients A_f of $J_0(N)$, with N odd and square free, that the Manin constant is 1, which would be useful for computations regarding the Birch and Swinnerton-Dyer conjecture.

B. Edixhoven also has unpublished results (see [Edi89]) which assert that the only primes that can divide c_E are 2, 3, 5, and 7; he also gives bounds that are independent of E on the valuations of c_E at 2, 3, 5, and 7. His arguments rely on construction of certain stable integral models for $X_0(p^2)$.

Cremona verified computationally that the Manin constant is 1 for every elliptic curve of conductor up to at least 6000. Cremona computes lattice invariants c_4 and c_6 from a rational newform f, and verifies in each case that c_4 and c_6 are the invariants of a minimal Weierstrass equation, to conclude that the Manin constant for the corresponding elliptic curve is 1.

Definition 2.8 (Congruence Number). The *congruence number* r_E of E is the largest integer r such that there exists a cusp form g that has integer Fourier coefficients, is orthogonal to f with respect to the Petersson inner product, and satisfies $g \equiv f \pmod{r}$. The *congruence primes* of E are the primes that divide r_E.

To the above list we add the following theorem. Our proof builds on the techniques of [AU96].

Theorem 2.9. *If $p \mid c_E$ then $p^2 \mid N$ or $p \mid r_E$.*

This theorem is a special case of Theorem 3.19 below, which we prove in Section 5. In view of Theorem 2.5, our only new contribution for elliptic curves is that if r_E is odd and $\mathrm{ord}_2(N) = 1$, then c_E is odd.

The hypothesis that r_E is odd and $\mathrm{ord}_2(N) = 1$ is very stringent—of the 17922 optimal elliptic curve quotients of conductor ≤ 5300, a mere 17 of them satisfy the hypothesis. These 17 curves are given in Table 1, where the notation is as in [Cre97]. We computed this table as follows. We use the fact that Cremona has computed the modular degree m_E for each curve of conductor up to 5300 (in fact he has gone much further). First we consider all curves in Cremona's tables with odd modular degree and $\mathrm{ord}_2(N) = 1$. As discussed at the beginning of Section 2.2, $\mathrm{ord}_2(r_E) = \mathrm{ord}_2(m_E)$ for each such curve, so r_E is odd as well. Note that the number r_E seems difficult to compute directly, which is why we use m_E and the divisibility $r_E \mid m_E$ of Theorem 2.10 below. Our Theorem 2.9 then implies that c_E is odd for each E in Table 1, as is verfied by Cremona's computation that $c_E = 1$ for all these curves. For example, for the elliptic curve E of conductor $2 \cdot 23$, Theorems 2.4–2.7 only imply that $\mathrm{ord}_2(c_E) \leq 1$, but Theorem 2.9 implies that $\mathrm{ord}_2(c_E) = 0$.

Table 1: Theorem 2.9 Applies to These Curves

N	isogeny class	r_E
$2 \cdot 7$	A	1
$2 \cdot 23$	A	5
$2 \cdot 71$	C	3^2
$2 \cdot 103$	A	$3 \cdot 5$
$2 \cdot 151$	C	3^3
$2 \cdot 199$	A	$5 \cdot 11$
$2 \cdot 487$	C	$3^3 \cdot 7$
$2 \cdot 503$	B	$3^2 \cdot 7$
$2 \cdot 727$	A	3^6
$2 \cdot 823$	A	$5 \cdot 109$
$2 \cdot 967$	A	$7 \cdot 139$
$2 \cdot 1303$	A	$7 \cdot 113$
$2 \cdot 1319$	B	$3^2 \cdot 5 \cdot 7$
$2 \cdot 1559$	B	$3^2 \cdot 5^2 \cdot 13$
$2 \cdot 1607$	B	$3 \cdot 5^3$
$2 \cdot 1879$	D	$5 \cdot 7 \cdot 23$
$2 \cdot 2039$	A	$3 \cdot 5 \cdot 47$

2.2 Congruence Primes and the Modular Degree

The congruence number r_E and the modular degree m_E, defined earlier, are quantities of great interest. Congruence primes have been studied by Doi, Hida, Ribet, Mazur and others (e.g., see [Rib83, §1]), and played an important role in Wiles's work [Wil95] on Fermat's last theorem. Furthermore, Frey and Mai-Murty have observed that an appropriate asymptotic bound on the modular degree is equivalent to the *abc*-conjecture (see [Fre97, p.544] and [Mur99, p.180]).

To start with, we have the following relation between the congruence number and the modular degree.

Theorem 2.10. *Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, with modular degree m_E and congruence modulus r_E. Then $m_E \mid r_E$ and if $\mathrm{ord}_p(N) \leq 1$ then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$.*

The divisibility $m_E \mid r_E$ was first discussed in [Zag85, Th. 3], where it is attributed to Ribet; however the divisibility was mistakenly written in the opposite direction. For some other expositions of the proof, see [AU96, Lem 3.2] and [CK03]. We generalize this divisibility in Proposition 3.9. We prove the second part of Theorem 2.10, i.e., that if $\mathrm{ord}_p(N) = 1$ then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$, in Section 2.3 below. Note that [AU96, Prop. 3.3 and Prop. 3.4] implies the weaker statement that if $p \nmid N$ then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$, since Prop. 3.3 implies

$$\mathrm{ord}_p(r_E) - \mathrm{ord}_p(m_E) = \mathrm{ord}_p(\#\mathcal{C}) - \mathrm{ord}_p(c_E) - \mathrm{ord}_p(\#\mathcal{D}),$$

and by Prop. 3.4 $\mathrm{ord}_p(\#\mathcal{C}) = 0$.

Frey and Müller [FM99, Ques. 4.4] asked whether $r_E = m_E$ in general. After implementing an algorithm to compute r_E in MAGMA, we quickly found that the answer is no. The first countexamples occur at levels

$$54, 64, 72, 80, 88, 92, 96, 99, 108, 112, 120, 124, 126, 128, 135, 144.$$

For example, the elliptic curve 54B1 of [Cre97], with equation $y^2+xy+y = x^3-x^2+x-1$, has $r_E = 6$ and $m_E = 2$. To see explicitly that $3 \mid r_E$, observe that the newform corresponding to E is $f = q+q^2+q^4-3q^5-q^7+\cdots$ and the newform corresponding to $X_0(27)$ if $g = q-2q^4-q^7+\cdots$, so $g(q)+g(q^2)$ is congruent to f modulo 3. To prove this congruence, we checked it for 18 Fourier coefficients, where the precision 18 was determined using [Stu87]. In accord with Theorem 2.10, since $\mathrm{ord}_3(r_E) \neq \mathrm{ord}_3(c_E)$, we have $\mathrm{ord}_3(54) \geq 2$.

In our computations, there appears to be no absolute bound on the p that occur (e.g., p does *not* appear to just be 2, 3, 5, or 7). We propose the following replacement for Question 4.4 of [FM99]:

Conjecture 2.11. *Let E be an optimal elliptic curve of conductor N and p be any prime. Then*

$$\mathrm{ord}_p\left(\frac{r_E}{m_E}\right) \leq \frac{1}{2}\,\mathrm{ord}_p(N).$$

In particular, for $p \geq 5$, the conjecture simply asserts that

$$\mathrm{ord}_p\left(\frac{r_E}{m_E}\right) \leq 1,$$

because $\mathrm{ord}_p(N) \leq 2$ for any $p \geq 5$. As evidence, we verified Conjecture 2.11 for every optimal elliptic curve quotient of $J_0(N)$, with $N \leq 539$.

2.3 Proof of Theorem 2.10

In this section we prove Theorem 2.10.

Let p be a prime number, and let N be a positive integer prime to p, and let $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots]$ be the subring of $\mathrm{End}(J_0(pN))$ generated by the Hecke operators T_n for all $n \geq 1$. Let $\mathbf{T}''$ be the saturation of $\mathbf{T}$ in $\mathrm{End}(J_0(pN))$, so

$$\mathbf{T}'' = (\mathbf{T} \otimes \mathbf{Q}) \cap \mathrm{End}(J_0(pN)),$$

where the intersection is taken inside $\mathrm{End}(J_0(pN)) \otimes \mathbf{Q}$. (We use the notation $\mathbf{T}''$ because we will introduce a ring $\mathbf{T}'$ intermediate between $\mathbf{T}$ and $\mathbf{T}''$ near

the end of the proof. [1]) The quotient $\mathbf{T}''/\mathbf{T}$ is a finitely generated abelian 1
group because both $\mathbf{T}$ and $\mathrm{End}(J_0(pN))$ are finitely generated over $\mathbf{Z}$.

Suppose for the moment that $N = 1$, so $p = Np$. In [Maz77], Mazur proves that $\mathbf{T} = \mathbf{T}''$. He combines this result with the equality

$$\mathbf{T} \otimes \mathbf{Q} = \mathrm{End}(J_0(p)) \otimes \mathbf{Q}$$

of [Rib75] or [Rib81], to deduce that $\mathbf{T} = \mathrm{End}(J_0(p))$.

2.3.1 Multiplicity One

Mazur's argument (see [Maz77, pg. 95]) is quite general; it relies on a multiplicity 1 statement for spaces of differentials in positive characteristic (see [Maz77, Prop. 9.3, pg. 94]). His method shows in the general case (where N is no longer constrained to be 1) that $\mathrm{Supp}_{\mathbf{T}}(\mathbf{T}''/\mathbf{T})$ contains no maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ for which his space $\mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ has dimension ≤ 1. (Here ℓ is the residue characteristic of $\mathfrak{m}$.) In other words, multiplicity one for $\mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ implies that $\mathbf{T}$ and $\mathbf{T}''$ agree at $\mathfrak{m}$. We record this fact as a lemma.

Lemma 2.12. *Suppose $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ of residue characteristic ℓ and that*

$$\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}] \leq 1.$$

Then $\mathfrak{m}$ is not in the support of $\mathbf{T}/\mathbf{T}''$.

There is quite a bit of literature on the question of multiplicity 1 for $\mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$. The easiest case is that ℓ is prime to the level pN.

Lemma 2.13. *Suppose $\ell \nmid pN$. Then ℓ does not divide $\#(\mathbf{T}/\mathbf{T}'')$.*

Proof. The standard q-expansion argument of [Maz77][2] proves that 2

$$\dim_{\mathbf{T}/\mathfrak{m}} \mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}] \leq 1$$

for all $\mathfrak{m} \mid \ell$. Now apply Lemma 2.12 [3] □ 3

[1] EDIT: Actually we don't. It only appears in a remark after the proof. Can we change to $\mathbf{T}'$ and call the $\mathbf{T}'$ in the remark something else? -WAS

[2] EDIT: which section? -WAS

[3] EDIT: Is there a problem if $\ell = 2$? How do Lloyd Kilford's examples fit into this, where I guess $N = 1$ and $\ell = 2$ and multiplicity one in $J_0(p)$ fails. Is it still OK in Mazur's differentials? -WAS

In the context of Mazur's paper, where $p = Np$, we see from Lemma 2.13 that $\mathbf{T}$ and $\mathbf{T}''$ agree away from p. At p, we can still use the q-expansion principle because of the arguments in [Maz77, Ch.II §4]. Thus in this case $\mathbf{T} = \mathbf{T}''$, as we asserted above.

The question of multiplicity 1 at p for $\mathrm{H}^0(X_0(pN)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ is discussed in [MR91], where the authors establish multiplicity 1 for maximal ideals $\mathfrak{m} \mid p$ for which the associated mod p Galois representation is irreducible and *not* p-old. (A representation is p-old if it arises already from the space of weight-two cusp forms of level N.)

Lemma 2.14 (Wiles). *If* $\mathfrak{m}$ *is an ordinary prime of* $\mathbf{T}$ *of characteristic* ℓ *and* $\mathrm{ord}_\ell(Np) = 1$*, then* $\mathfrak{m}$ *is not in the support of* $\mathbf{T}''/\mathbf{T}$*.*

Proof. This follows from [Wil95, Lem. 2.2, pg. 485], which proves, under a suitable hypothesis, that $\mathrm{H}^0(X_0(pN)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}]$ is 1-dimensional if $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ that divides p. The "suitable hypothesis" is that $\mathfrak{m}$ is ordinary, in the sense that $T_p \not\in \mathfrak{m}$. (Note that T_p is often denoted U_p in this context.) It follows from Wiles's lemma that $\mathbf{T}'' = \mathbf{T}$ locally at $\mathfrak{m}$ whenever $\mathfrak{m}$ is an ordinary prime whose residue characteristic divides the level (which is Np here) exactly once.

We make a few further comments about this lemma.

1. Wiles considers $X_1(N, p)$ instead of $X_0(pN)$, which means that he is using $\Gamma_1(N)$-structure instead of $\Gamma_0(N)$-structure. This surely has no relevance to the issue at hand.

2. Wiles assumes (on page 480) that p is an odd prime, but again this assumption does not seem to be relevant to our question.

3. The condition that $\mathfrak{m}$ is ordinary does not appear explicitly in the statement of the lemma; one could describe it as a reigning assumption in the context of his discussion.

4. We see by example that Wiles's "ordinary" assumption is less stringent than the assumption in [MR91]; note that [MR91] rule out cases where $\mathfrak{m}$ is both old and new at p, whereas Wiles is happy to include such cases. (On the other hand, Wiles's assumption is certainly nonempty, since it rules out maximal ideals $\mathfrak{m}$ that arise from non-ordinary forms of level N.) Here is an example with $p = 2$ and $N = 11$: There is a unique newform $f = \sum a_n q^n$ of level 11, and $\mathbf{T} = \mathbf{Z}[T_2] \subset \mathrm{End}(J_0(22))$, where $T_2^2 - a_2 T_2 + 2 = 0$. Since $a_2 = -2$, we have $\mathbf{T} \cong \mathbf{Z}[\sqrt{-1}]$. We can choose the square root of -1 to be

$T_2 + 1$. Then T_2 is a generator of the unique maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ with residue characteristic 2.

□

We now summarize the conclusions we can make from the lemmas so far. Wiles's lemma and the standard q-expansion argument (Lemma 2.13 and Lemma 2.14) imply that $\mathbf{T}$ and $\mathbf{T}''$ agree locally at each rational prime that is prime to the level pN, and also at each maximal ideal $\mathfrak{m}$ dividing p that is ordinary, in the sense that $T_p \notin \mathfrak{m}$. A more palatable description of the situation involves considering the Hecke algebra $\mathbf{T}$ and its saturation $\mathbf{T}''$ at a level $M \geq 1$. Then $\mathbf{T} = \mathbf{T}''$ locally at each maximal ideal $\mathfrak{m}$ that is either prime to M or that satisfies the following supplemental hypothesis: the residue characteristic of $\mathfrak{m}$ divides M only to the first power and $\mathfrak{m}$ is ordinary. In Mazur's original context, the level M is prime. Moreover, we have $T_M^2 = 1$ because there are no forms of level 1. Accordingly, each $\mathfrak{m}$ dividing M is ordinary, and we recover Mazur's equality $\mathbf{T} = \mathbf{T}''$ in this special case.

2.3.2 Degrees and Congruences

Let $e \in \mathbf{T} \otimes \mathbf{Q}$ be an idempotent, and let $A \subset J_0(pN)$ be the abelian variety image of e, i.e., the image of the homomorphism $ne \in \mathbf{T}$, where the integer $n \geq 1$ is a multiple of the denominator of e. Let B be the image of the complementary idempotent $1 - e$. Then $J_0(pN) = A + B$, and $A \cap B$ is a finite group whose exponent divides the denominator of e. For $t \in \mathbf{T}$, let t_A be the restriction of t to A, and let t_B be the image of t in $\mathrm{End}(B)$. Let $\mathbf{T}_A$ be the subgroup[4] of $\mathrm{End}(A)$ consisting of the various t_A, and define $\mathbf{T}_B$ 4
similarly. By combining these restriction maps we obtain an injection

$$j : \mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B$$

with finite cokernel. Because j is an injection, we refer to the maps $\pi_A : \mathbf{T} \to \mathbf{T}_A$ and $\pi_B : \mathbf{T} \to \mathbf{T}_B$, given by $t \mapsto t_A$ and $t \mapsto t_B$, respectively, as "projections".

Definition 2.15 (Congruence Ideal). The *congruence ideal* associated with the projector e is

$$I = \pi_A(\ker(\pi_B)) \subset \mathbf{T}_A.$$

[4] EDIT: I changed this from subring to subgroup, since the identity element is different, and we only use the group structure. -WAS

Viewing $\mathbf{T}_A$ as $\mathbf{T}_A \times \{0\}$, we may view $\mathbf{T}_A$ as a subgroup of $\mathbf{T} \otimes \mathbf{Q}$. Also, we may view $\mathbf{T}$ as embedded in $\mathbf{T}_A \times \mathbf{T}_B$.

Lemma 2.16. *We have $I = \mathbf{T}_A \cap \mathbf{T}$.*

A larger ideal of $\mathbf{T}_A$ is

$$J = \mathrm{Ann}_{\mathbf{T}_A}(A \cap B);$$

it consists of restrictions to A of Hecke operators that vanish on $A \cap B$.

Lemma 2.17. *We have $I \subset J$.*

Proof. The image in $\mathbf{T}_A$ of an operator that vanishes on B also vanishes on $A \cap B$. □

Lemma 2.18. *We have $J = \mathbf{T}_A \cap \mathrm{End}(J_0(pN)) = \mathbf{T}_A \cap \mathbf{T}''$.*

Proof. This is elementary; it is an analogue of Lemma 2.16. □

Proposition 2.19. *There is a natural inclusion*

$$J/I \hookrightarrow \mathbf{T}''/\mathbf{T}$$

of $\mathbf{T}$-modules.

Proof. Consider the map $\mathbf{T} \to \mathbf{T} \otimes \mathbf{Q}$ given by $t \mapsto te$. This homomorphism factors through $\mathbf{T}_A$ and yields an injection $\iota_A : \mathbf{T}_A \hookrightarrow \mathbf{T}\otimes\mathbf{Q}$. Symmetrically, we also obtain $\iota_B : \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. The map $(t_A, t_B) \mapsto \iota_A(t_A) + \iota_B(t_B)$ is an injection $\mathbf{T}_A \times \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. The composite of this map with the inclusion $j : \mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B$ defined above is the natural map $\mathbf{T} \hookrightarrow \mathbf{T} \otimes \mathbf{Q}$. We thus have a sequence of inclusions

$$\mathbf{T} \hookrightarrow \mathbf{T}_A \times \mathbf{T}_B \hookrightarrow \mathbf{T} \otimes \mathbf{Q} \subset \mathrm{End}(J_0(pN)) \otimes \mathbf{Q}.$$

By Lemma 2.16 and Lemma 2.18, we have $I = \mathbf{T}_A \cap \mathbf{T}$ and $J = \mathbf{T}_A \cap \mathbf{T}''$. Thus $I = J \cap \mathbf{T}$, where the intersection is taken inside $\mathbf{T}''$. Thus

$$J/I = J/(J \cap \mathbf{T}) \cong (J + \mathbf{T})/\mathbf{T} \hookrightarrow \mathbf{T}''/\mathbf{T}.$$

□

Corollary 2.20. *If $\mathfrak{m}$ is a maximal ideal not in $\mathrm{Supp}_{\mathbf{T}}(\mathbf{T}''/\mathbf{T})$, then $\mathfrak{m}$ is not in the support of J/I, i.e., if $\mathbf{T}$ and $\mathbf{T}''$ agree locally at $\mathfrak{m}$, then I and J also agree locally at $\mathfrak{m}$.*

Note that the Hecke algebra $\mathbf{T}$ acts on J/I through its quotient $\mathbf{T}_A$, since the action of $\mathbf{T}$ on I and on J factors through this quotient.

Now we specialize to the case where A is ordinary at p, in the sense that the image of T_p in $\mathbf{T}_A$, which we denote $T_{p,A}$, is invertible modulo every maximal ideal of $\mathbf{T}_A$ that divides p. This case occurs when A is a subvariety of the p-new subvariety of $J_0(pN)$, since the square of $T_{p,A}$ is the identity. If $\mathfrak{m} \mid p$ is a maximal ideal of $\mathbf{T}$ that arises by pullback from a maximal ideal of $\mathbf{T}_A$, then $\mathfrak{m}$ is ordinary in the sense used above. When A is ordinary at p, it follows from Lemma 2.14 and Proposition 2.19 that $I = J$ locally at p. The reason is simple: regarding I and J as $\mathbf{T}_A$-modules, we realize that we need to test that $I = J$ at maximal ideals of $\mathbf{T}_A$ that divide p. These ideals correspond to maximal ideals $\mathfrak{m} \mid p$ of $\mathbf{T}$ that are automatically ordinary, so we have $I = J$ locally at $\mathfrak{m}$ because of Lemma 2.14. By Lemma 2.13, we have $\mathbf{T} = \mathbf{T}''$ locally at primes away from the level Np. Thus we conclude that $I = J$ locally at all primes $\ell \nmid Np$ and also at p, a prime that divides the level Np exactly once.

Suppose, finally, that A is the elliptic curve associated with a newform f of level pN. We then have $\mathbf{T}_A = \mathbf{Z}$. The ideal $I \subset \mathbf{Z}$ measures congruences between f and the space of forms in $S_2(\Gamma_0(pN))$ that are orthogonal to the space generated by f. Also, $A \cap B$ is the kernel in A of the map "multiplication by the modular degree". In this case, the inclusion $I \subset J$ corresponds to the divisibility

$$m_E \mid r_E.$$

We have proved the the congruence number and the modular degree agree both at p and at primes not dividing Np, which completes our proof of Theorem 2.10.

Remark 2.21. The ring

$$\mathbf{T}' = \mathrm{End}(J_0(pN)) \cap (\mathbf{T}_A \times \mathbf{T}_B)$$

is often of interest, where the intersection is taken in $\mathrm{End}(J_0(pN)) \otimes \mathbf{Q}$. We proved above that there is a natural inclusion $J/I \hookrightarrow \mathbf{T}''/\mathbf{T}$. It is elementary that this inclusion yields an isomorphism

$$J/I \xrightarrow{\sim} \mathbf{T}'/\mathbf{T}.$$

Indeed, if (t_A, u_B) is an endomorphism of $J_0(pN)$, where $t, u \in \mathbf{T}$, then $(t_A, u_B) - u = (t_A, 0)$ is an element of J. The ideals I and J are equal to the extent that the rings $\mathbf{T}$ and $\mathbf{T}'$ coincide. Even when $\mathbf{T}''$ is bigger than $\mathbf{T}$, its subring $\mathbf{T}'$ may be not far from $\mathbf{T}$.

3 Quotients of Arbitrary Dimension

Let N denote a positive integer greater than 4, and let Γ denote either $\Gamma_0(N)$ or $\Gamma_1(N)$. Let X be the modular curve over $\mathbf{Q}$ associated to Γ and let J be the Jacobian of X. Thus, if $\Gamma = \Gamma_0(N)$, then $X = X_0(N)$ and $J = J_0(N)$, and if $\Gamma = \Gamma_1(N)$, then $X = X_1(N)$ and $J = J_1(N)$. Let I be a saturated ideal of the corresponding Hecke algebra $\mathbf{T}$ (i.e., such that $\mathbf{T}/I$ is torsion free). Let $A = J/IJ$ be the optimal quotient of J associated to I (this quotient is optimal, because IJ is an abelian subvariety, hence connected).

In particular, if f is a newform on Γ, and I_f is the annihilator of f in $\mathbf{T}$, then the quotient abelian variety J/I_fJ is called the *newform (optimal) quotient* associated to f, and we denote it by A_f. It has dimension equal to the degree of the field generated by the Fourier coefficients of f.

Let J_{old} denote the abelian subvariety of J generated by the degeneracy maps from levels dividing N (e.g., see [Maz78, §2(b)]) and let J^{new} denote the quotient of J by J_{old}. We call J^{new} the new quotient of J.

In Section 3.1, we generalize the notions of the congruence number and the modular degree (as in Section 2) to quotients A as above, and state a generalization of the result that the modular degree divides the congruence number. In Section 3.2, we generalize the notion of the Manin constant to quotients A as above and prove its integrality. We also give generalizations of some of the results from Section 2 to quotients A that factor through the new part of J when $\Gamma = \Gamma_0(N)$, and make the conjecture that the generalized Manin constant is 1 for newform quotients.

If B is an abelian variety over $\mathbf{Q}$ and n is a positive integer, let $B_{\mathbf{Z}[1/n]}$ denote the Néron model of B over $\mathbf{Z}[1/n]$. If R is a subring of $\mathbf{C}$, let $S_2(R)$ denote the $\mathbf{T}$-submodule of $S_2(\Gamma, \mathbf{C})$ consisting of modular forms whose Fourier expansions (at the cusp ∞) have coefficients in R. Note that $S_2(\mathbf{C}) \cong S_2(\mathbf{Z}) \otimes \mathbf{C}$. If B is an abelian variety, let $B^\vee$ denote the dual abelian variety of B. If G is a finite group, then by the *exponent* of G, we mean the smallest positive integer n such that every element of G has order dividing n.

3.1 Generalizations of the congruence number and the modular degree

Let ϕ_2 denote the quotient map $J \to A$. There is a canonical principal polarization $\theta : J \cong J^\vee$ arising from the theta divisor (e.g., see [Mil86, Thm. 6.6]). Dualizing ϕ_2, we obtain a map $\phi_2^\vee : A^\vee \to J^\vee$, which we compose with $\theta^{-1} : J^\vee \cong J$ to get a map $\phi_1 : A^\vee \to J$.

Since ϕ_2 is a surjection, by [Lan83, §VI.3, Prop 3], $\ker(\phi_2^\vee)$ is finite. Since $\ker(\phi_2)$ is connected (it is IJ, by hypothesis), $\ker(\phi_2^\vee)$ is in fact trivial, and thus $\phi_2^\vee$ (and hence ϕ_1) is an injection. Consider the composite

$$\phi : A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A.$$

Proposition 3.1. *The map ϕ is an isogeny, and moreover, it is a polarization.*

Proof. Let i be the injection $\phi_2^\vee : A^\vee \to J^\vee$, and let Θ denote the theta divisor. By unwinding the definition of the polarization attached to an ample divisor, we see that the map ϕ is induced by the pullback $i^*(\Theta)$ of the theta divisor. The theta divisor is effective, and hence so is $i^*(\Theta)$. By [Mum70, §6, Application 1, p. 60], $\ker\phi$ is finite. Since the dimensions of A and $A^\vee$ are the same, ϕ is an isogeny. Moreover, since Θ is ample, some power of it is very ample. Then the pullback of this very ample power by i is again very ample, and hence a power of $i^*(\Theta)$ is very ample, so $i^*(\Theta)$ is ample (by [Har77, II.7.6]). This shows that ϕ is a polarization. □

Definition 3.2. The *modular exponent* of A is the exponent of the kernel of the isogeny ϕ, and the *modular number* of A is the degree of ϕ.

We denote the modular exponent of A by $\tilde{n}_A$ and the modular number by n_A. Note that when A is an elliptic curve, the modular exponent is equal to the modular degree of A, while the modular number is the square of the usual modular degree (see, e.g., [AU96, p. 278]).

Let $W(I) = S_2(\mathbf{Z})[I]^\perp$ denote the orthogonal complement of $S_2(\mathbf{Z})[I]$ in $S_2(\mathbf{Z})$ with respect to the Petersson inner product.

Definition 3.3. The exponent of the quotient group

$$\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I] + W(I)} \tag{1}$$

is called the *congruence exponent* $\tilde{r}_A$ of A and its order is called the *congruence number* r_A of A.

Note that this definition of r_A coincides with the definition in Section 2.2, where A was an elliptic curve (see [AU96, p. 276]).

The rest of the section is devoted to proving Proposition 3.9 below, which asserts that if f is a newform, then $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$. The reader who is primarily interested in the generalization of the Manin constant may go directly to Section 3.2.

Remark 3.4. Note that in general the polarization of J induced by the theta divisor need not be Hecke equivariant. If T is a Hecke operator on J, then on $J^\vee$ it acts as $W_N T W_N$, where W_N is the Atkin-Lehner involution (e.g., see [DI95, Remark 10.2.2]). However, on J^{new}, the action of the Hecke operators commutes with that of W_N. If the quotient map $J \to A$ factors through J^{new}, then the Hecke action on $A^\vee$ induced by the embedding $A^\vee \to J^\vee$ and the action on $A^\vee$ induced by $\phi_1 : A^\vee \to J$ are the same. Hence for such quotients we may identify $A^\vee$ with $\phi_1(A^\vee)$ as modules over $\mathbf{T}$.

For the rest of this section, $I = I_f$ is the annihilator of a newform f. Let $A = A_f$ and $B = I_f J$, so that $A^\vee + B = J$, and $J/B \cong A$.

Lemma 3.5. $\mathrm{Hom}(A^\vee, B) = 0$.

Proof. If there were a nonzero element of $\mathrm{Hom}(A^\vee, B)$, then for all ℓ, the Tate module $\mathrm{Tate}_\ell(A^\vee) = \mathbf{Q} \otimes \varprojlim_n A^\vee[\ell^n]$ would be a factor of $\mathrm{Tate}_\ell(B)$. One could then extract almost all prime-indexed coefficients of the corresponding eigenforms from the Tate modules, which would violate multiplicity one (see [Li75, Cor. 3, pg. 300]). □

Let $\mathbf{T}_1$ be the image of $\mathbf{T}$ acting on $A^\vee$, and similiarly let $\mathbf{T}_2$ be the image of $\mathbf{T}$ in $\mathrm{End}(B)$.

We have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{T} \arrow[r] \arrow[d] & \mathbf{T}_1 \oplus \mathbf{T}_2 \arrow[r] \arrow[d] & \dfrac{\mathbf{T}_1 \oplus \mathbf{T}_2}{\mathbf{T}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{End}(J) \arrow[r] & \mathrm{End}(A^\vee) \oplus \mathrm{End}(B) \arrow[r] & \dfrac{\mathrm{End}(A^\vee) \oplus \mathrm{End}(B)}{\mathrm{End}(J)} \arrow[r] & 0.
\end{tikzcd} \tag{2}$$

Let

$$e = (1, 0) \in \mathbf{T}_1 \oplus \mathbf{T}_2,$$

and let e_1 and e_2 denote the images of e in the groups $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ and $(\mathrm{End}(A^\vee) \oplus \mathrm{End}(B))/\mathrm{End}(J)$, respectively. It follows from Lemma 3.5 that the two quotient groups on the right hand side of (2) are finite, so e_1 and e_2 have finite order. Note that the order of e_2 is a divisor of the order of e_1, which is the crucial ingredient in the proof of Proposition 3.9 below.

The *denominator* of any $\varphi \in \mathrm{End}(J) \otimes \mathbf{Q}$ is the smallest positive integer n such that $n\varphi \in \mathrm{End}(J)$. Explicitly, the denominator of φ is the least common multiples of the denominators of the entries of any matrix that represents the action of φ on the lattice $\mathrm{H}_1(J, \mathbf{Z})$.

Let $\pi_{A^\vee}, \pi_B \in \mathrm{End}(J) \otimes \mathbf{Q}$ be projection onto $A^\vee$ and B, respectively. Note that the denominator of $\pi_{A^\vee}$ equals the denominator of π_B, since $\pi_{A^\vee} + \pi_B = 1_J$, so that $\pi_B = 1_J - \pi_{A^\vee}$.

Lemma 3.6. *The element $e_2 \in (\mathrm{End}(A^\vee) \oplus \mathrm{End}(B))/\mathrm{End}(J)$ defined above has order $\tilde{n}_A$.*

Proof. Let n be the order of e_2, so n is the denominator of $\pi_{A^\vee}$, which, as mentioned above, is also the denominator of π_B. We want to show that n is equal to $\tilde{n}_A$, the exponent of $A^\vee \cap B$.

Let $i_{A^\vee}$ and i_B be the embeddings of $A^\vee$ and B into J, respectively. Then

$$\varphi = (n\pi_{A^\vee}, n\pi_B) \in \mathrm{Hom}(J, A^\vee \times B)$$

and $\varphi \circ (i_{A^\vee} + i_B) = [n]_{A^\vee \times B}$. We have an exact sequence

$$0 \to A^\vee \cap B \xrightarrow{x \mapsto (x, -x)} A^\vee \times B \xrightarrow{i_{A^\vee} + i_B} J \to 0.$$

Let Δ be the image of $A^\vee \cap B$. Then by exactness,

$$[n]\Delta = (\varphi \circ (i_{A^\vee} + i_B))(\Delta) = \varphi \circ ((i_{A^\vee} + i_B)(\Delta)) = \varphi(\{0\}) = \{0\},$$

so n is a multiple of the exponent $\tilde{n}_A$ of $A^\vee \cap B$.

To show the opposite divisibility, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A^\vee \cap B \arrow[r, "x \mapsto (x,-x)"] \arrow[d, "{[\tilde{n}_A]}"] & A^\vee \times B \arrow[r] \arrow[d, "{([\tilde{n}_A],0)}"] & J \arrow[r] \arrow[d, dotted, "\psi"] & 0 \\
0 \arrow[r] & A^\vee \cap B \arrow[r, "x \mapsto (x,-x)"] & A^\vee \times B \arrow[r] & J \arrow[r] & 0,
\end{tikzcd}$$

where the middle vertical map is $(a, b) \mapsto (\tilde{n}_A a, 0)$ and the map ψ exists because $[\tilde{n}_A](A^\vee \cap B) = 0$. But $\psi = \tilde{n}_A \pi_{A^\vee}$ in $\mathrm{End}(J) \otimes \mathbf{Q}$. This shows that $\tilde{n}_A \pi_{A^\vee} \in \mathrm{End}(J)$, i.e., that $\tilde{n}_A$ is a multiple of the denominator n of $\pi_{A^\vee}$.

□

Lemma 3.7. *The group $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ is isomorphic to the quotient (1) in Definition 3.3, so $r_A = \#((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T})$ and $\tilde{r}_A$ is the exponent of $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$. More precisely, $\mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z})$ is isomorphic as a $\mathbf{T}$-module to the quotient (1).*

Proof. Apply the $\mathrm{Hom}(-,\mathbf{Z})$ functor to the first row of (2) to obtain a three-term exact sequence

$$0 \to \mathrm{Hom}(\mathbf{T}_1 \oplus \mathbf{T}_2, \mathbf{Z}) \to \mathrm{Hom}(\mathbf{T}, \mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z}) \to 0. \quad (3)$$

The term $\mathrm{Ext}^1(\mathbf{T}_1 \oplus \mathbf{T}_2, \mathbf{Z})$ is 0 is because $\mathrm{Ext}^1(M, \mathbf{Z}) = 0$ for any finitely generated free abelian group. Also, $\mathrm{Hom}((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z}) = 0$ since $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ is torsion. There is a $\mathbf{T}$-equivariant bilinear pairing $\mathbf{T} \times S_2(\mathbf{Z}) \to \mathbf{Z}$ given by $(t, g) \mapsto a_1(t(g))$, which is perfect by [AU96, Lemma 2.1] (see also [Rib83, Theorem 2.2]). Using this pairing, we transform (3) into an exact sequence

$$0 \to S_2(\mathbf{Z})[I] \oplus W(I) \to S_2(\mathbf{Z}) \to \mathrm{Ext}^1((\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}, \mathbf{Z}) \to 0$$

of $\mathbf{T}$ modules. Here we use that $\mathrm{Hom}(\mathbf{T}_2, \mathbf{Z})$ is the unique saturated Hecke-stable complement of $S_2(\mathbf{Z})[I]$ in $S_2(\mathbf{Z})$, hence must equal $S_2(\mathbf{Z})[I]^\perp = W(I)$. Finally note that if G is any finite abelian group, then $\mathrm{Ext}^1(G, \mathbf{Z}) \approx G$ as groups, to get the desired result. □

Lemma 3.8. *The element $e_1 \in (\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ has order $\tilde{r}_A$.*

Proof. By Lemma 3.7, the lemma is equivalent to the assertion that the order r of e_1 equals the exponent of $M = (\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$. Since e_1 is an element of M, the exponent of M is divisible by r.

To obtain the reverse divisibility, consider an element x of M. Let $(a, b) \in \mathbf{T}_1 \oplus \mathbf{T}_2$ be such that its image in M is x. By definition of e_1 and r, we have $(r, 0) \in \mathbf{T}$, and since $1 = (1, 1) \in \mathbf{T}$, we also have $(0, r) \in \mathbf{T}$. Thus $(\mathbf{T}r, 0)$ and $(0, \mathbf{T}r)$ are both subsets of $\mathbf{T}$ (i.e., in the image of $\mathbf{T}$ under the map $\mathbf{T} \to \mathbf{T}_1 \oplus \mathbf{T}_2$), so $r(a, b) = (ra, rb) = (ra, 0) + (0, rb) \in \mathbf{T}$. This implies that the order of x divides r. Since this is true for every $x \in M$, we conclude that the exponent of M divides r. □

Proposition 3.9. *If $f \in S_2(\mathbf{C})$ is a newform, then $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$.*

Proof. Since e_2 is the image of e_1 under the right-most vertical homomorphism in (2), the order of e_2 divides the order of e_1. Now apply Lemmas 3.6 and 3.8. □

Remark 3.10. When A_f is an elliptic curve, Proposition 3.9 implies Ribet's theorem, that the modular degree divides the congruence number, i.e., $\sqrt{n_{A_f}} \mid r_{A_f}$. In contrast, when $\dim(A_f) > 1$, the divisibility $n_{A_f} \mid {r_{A_f}}^2$ need not hold. For example, there is a newform of degree 24 in $S_2(\Gamma_0(431))$, where 431 is prime, such that $n_{A_f} = (2^{11} \cdot 6947)^2$, but $r_{A_f} = 2^{10} \cdot 6947$. Note that mod 2 multiplicity one fails for $J_0(431)$ (see [Kil02]).

The following MAGMA session illustrates how to verify the above assertion about n_{A_f} and r_{A_f}. The commands were implemented by the second author, and are parts of MAGMA V2.10 or greater.

```
> A := ModularSymbols("431F");
> Factorization(ModularDegree(A));
[ <2, 11>, <6947, 1> ]
> Factorization(CongruenceModulus(A));
[ <2, 10>, <6947, 1> ]
```

3.2 Generalization of the Manin Constant

In section 3.2.1, we generalize the notion of the Manin constant to quotients associated to saturated ideals of the Hecke algebra. In Section 3.2.2, we prove that this generalized Manin constant is an integer. Finally, in Section 3.2.3, we give the generalizations of some of the results from Section 2 to quotients of the new part of $J_0(N)$, and make the conjecture that the generalized Manin constant is 1 for newform quotients of $J_0(N)$.

We continue to use the notation introduced at the beginning of Section 3.

3.2.1 Motivation and Definition

On a Néron model, the global differentials are the same as the group of invariant differentials. Hence the group $H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})$ is free of rank d, where $d = \dim(A)$ and $\Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}}$ is the sheaf of differentials on the Néron model $A_{\mathbf{Z}}$ of A. Let D be a generator of $\bigwedge^d H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})$.

The *real volume* Ω_A of A is the volume of $A(\mathbf{R})$ with respect to the measure given by D. This quantity is of interest because it appears in the Birch and Swinnerton-Dyer conjecture, which expresses the ratio $L(A,1)/\Omega_A$ in terms of certain arithmetic invariants of A (see [Lan91, Chap. III, §5] and [AS03]). Let $g_1, \ldots, g_d$ be a $\mathbf{Z}$-basis of $S_2(\mathbf{Z})[I]$, and for $j = 1, \ldots, d$, let

$$\omega'_j = 2\pi i g_j(z)dz \in H^0(X, \Omega_{X/\mathbf{Q}}) = H^0(J, \Omega_{J/\mathbf{Q}})$$

(where we use the standard map $X \to J$ that sends the cusp ∞ to 0). As before, let ϕ_2 denote the quotient map $J \to A$. Then ϕ_2^* induces an isomorphism $H^0(A, \Omega_{A/\mathbf{Q}}) \to \bigoplus_j \mathbf{Q} w'_j$. For $j = 1, \ldots, d$, let $\omega_j = (\phi_2^*)^{-1}\omega'_j$.

In calculations (see [AS03]), or while proving formulas regarding the ratio mentioned above (see [Aga99, §2]), instead of working with Ω_A, it is easier to work with the volume Ω'_A of $A(\mathbf{R})$ with respect to the measure given by $\wedge_j \omega_j$. There exists $c \in \mathbf{Q}^*$ such that $D = c \cdot \wedge_j \omega_j$. The absolute value of c depends only on I, and is independent of other choices made above.

Definition 3.11. Let A be an optimal quotient of J attached to an ideal I of the Hecke algebra, as above. The *Manin constant* c_A of the optimal quotient A is the absolute value of the constant c defined above.

If A has dimension one, then c_A is the usual Manin constant. The constant c as defined above was considered earlier by Gross [Gro82, (2.5) on p. 222] and Lang [Lan91, III.5, p.95], although they did not explicitly state its relation to the usual Manin constant (for elliptic curves). The constant c_A was defined for a particular quotient A in [Aga99], where it was called the generalized Manin constant. In [CES03] it is called the Manin index.

If one works with the easier-to-compute volume Ω'_A instead of Ω_A, it is necessary to obtain information about c_A in order to make conclusions regarding the Birch and Swinnerton-Dyer conjecture, as the two volumes differ by the factor c_A. This is our main motivation for studying the Manin constant. Cremona's method for proving that $c_A = 1$ for a specific elliptic curve, i.e., computing c_4 and c_6 and checking that they are invariants of a minimal Weierstrass model, is of little use when A has dimension greater than one, since there is no simple analogue of the minimal Weierstrass model for A.

3.2.2 Integrality

In this section we prove that the Manin constant is an integer (see also [CES03, §6.1.2] for a similar argument). The reader who is primarily interested in other results about the (generalized) Manin constant may jump to the paragraph before Theorem 3.17.

The proof is a generalization of that of [Edi91, Prop. 2]. The idea of the proof is to construct an injective map on $H^0(A, \Omega^1_{A/\mathbf{Q}})$ using "q-expansions", then show that the image of $H^0(A_\mathbf{Z}, \Omega^1_{A_\mathbf{Z}/\mathbf{Z}})$ under this map is contained in the image of $\oplus_j \mathbf{Z}\omega_j$. We continue to use the notation of Section 3.2.1. Recall that $N > 4$, which is harmless since $J_1(N)$ has dimension 0 for $N \leq 10$.

Using the standard immersion $X \hookrightarrow J$ (which sends the cusp ∞ to 0), we have maps

$$X \hookrightarrow J \to A. \tag{4}$$

If $X = X_1(N)$, then we thus get a map $X_1(N) \to A$. If $X = X_0(N)$, then composing with the standard map $X_1(N) \to X_0(N)$ we get a map $X_1(N) \to A$. In either case, denote the resulting map $X_1(N) \to A$ by ϕ_A.

Consider the model $\mathcal{X}_\mu(N)$ over $\mathbf{Z}$ for $X_1(N)$ obtained by considering generalized elliptic curves E with immersions $\mu_N \hookrightarrow E^{\mathrm{reg}}$ as in [Kat76] (see also [DI95, §9.3.6, p. 80]). Since $\mathcal{X}_\mu(N)$ is smooth over $\mathbf{Z}$ (by [Kat76, §II.2.5]), by the Néron mapping property, there is a map

$$\mathcal{X}_\mu(N) \to A_{\mathbf{Z}},$$

which we again denote by ϕ_A.

The Tate curve E_q over $\mathbf{Z}[[q]]$ with the canonical immersion of μ_N gives a map (see, e.g., [DI95, p. 112])

$$\tau : \operatorname{Spec} \mathbf{Z}[[q]] \to \mathcal{X}_\mu(N). \tag{5}$$

Pulling back differentials, we get a map

$$H^0\left(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}}\right) \longrightarrow H^0\left(\operatorname{Spec} \mathbf{Z}[[q]], \Omega^1_{\mathbf{Z}[[q]]/\mathbf{Z}}\right).$$

Now $H^0(\operatorname{Spec} \mathbf{Z}[[q]], \Omega^1_{\mathbf{Z}[[q]]/\mathbf{Z}})$ is free of rank one over $\mathbf{Z}[[q]]$ with generator dq, so we get a map

$$H^0\left(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}}\right) \longrightarrow \mathbf{Z}[[q]].$$

Let q-exp denote the composite

$$H^0\left(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}}\right) \longrightarrow \mathbf{Z}[[q]] \xrightarrow{q\cdot} \mathbf{Z}[[q]],$$

where the second map is multiplication by q.

Next, we need to relate q-exp to the usual Fourier-expansion over $\mathbf{C}$. Now $\mathcal{X}_\mu(N) \otimes \mathbf{C} \cong X_1(N)_{\mathbf{C}}$. The Tate curve over $\mathbf{C}$ (see [DR73, VII.4.2]) gives a map

$$\tau_{\mathbf{C}} : \operatorname{Spec} \mathbf{C}[[q]] \to X_1(N)_{\mathbf{C}},$$

which is the base extension of (5) and which identifies q with the local parameter $e^{2\pi i z}$ on $X_1(N)_{\mathbf{C}}$ at the cusp ∞. As above, pulling back differentials, we get a map

$$H^0\left(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}}\right) \longrightarrow \mathbf{C}[[q]].$$

Let F-exp denote the composite

$$H^0\left(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}}\right) \longrightarrow \mathbf{C}[[q]] \xrightarrow{q\cdot} \mathbf{C}[[q]],$$

where the second map is multiplication by q.

From the discussion above, we obtain a commutative diagram

$$\begin{tikzcd}
H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}}) \arrow[r, "\phi_A^*"] \arrow[d] & H^0(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}}) \arrow[r, "q\text{-exp}"] \arrow[d] & \mathbf{Z}[[q]] \arrow[d] \\
H^0(A_{\mathbf{C}}, \Omega^1_{A_{\mathbf{C}}/\mathbf{C}}) \arrow[r, "\phi_A^* \otimes \mathbf{C}"] & H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}}) \arrow[r, "F\text{-exp}"] & \mathbf{C}[[q]]
\end{tikzcd}$$

in which the first and last vertical maps are clearly injections.

The relation of F-exp to the Fourier expansion of cusp forms is given by the following lemma. Let ψ denote the isomorphism $S_2(\Gamma_1(N), \mathbf{C}) \overset{\cong}{\to} H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}})$ given by $f(z) \mapsto 2\pi i f(z) dz$.

Lemma 3.12. *Let $f \in S_2(\Gamma_1(N), \mathbf{C})$, and let $\{a_n\}$ be the coefficients of the Fourier expansion of f. Then F-exp$(\psi(f)) = \sum_n a_n q^n$.*

Proof. If $f \in S_2(\Gamma_1(N), \mathbf{C})$, and its Fourier series is $\sum_n a_n e^{2\pi i z n}$, then $\psi(f) = 2\pi i \sum_n a_n e^{2\pi i z n} dz$. Since $\tau_{\mathbf{C}}$ identifies q with the local parameter $e^{2\pi i z}$, we see that the pullback of $\psi(f)$ via $\tau_{\mathbf{C}}$ to $H^0(\operatorname{Spec} \mathbf{C}[[q]], \Omega^1_{\mathbf{C}[[q]]/\mathbf{C}})$ is $\sum_n a_n q^{n-1} dq$. So F-exp$(\psi(f)) = \sum_n a_n q^n$. □

Lemma 3.13. *The group q-exp$\left(\phi_A^*\left(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})\right)\right)$ is a subgroup of F-exp$(\psi(S_2(\Gamma_1(N), \mathbf{Z})[I]))$.*

Proof. If $x \in H^0(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}})$ maps to $y \in H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}})$, then by the commutativity of the right half of the commutative diagram above and by Lemma 3.12, the Fourier expansion of $\psi^{-1}(y) \in S_2(\Gamma_1(N), \mathbf{C})$ is the same as q-exp(x), i.e., has integral Fourier coefficients; hence $\psi^{-1}(y) \in S_2(\Gamma_1(N), \mathbf{Z})$. This gives an injection

$$q\text{-exp}\left(H^0(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}})\right) \hookrightarrow F\text{-exp}(\psi(S_2(\Gamma_1(N), \mathbf{Z}))).$$

Now the lemma follows from the fact that $\phi_A^*(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}}))[I] = 0$. □

Proposition 3.14. *We have $H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}}) \subseteq \oplus_j \mathbf{Z}\omega_j$, considered as subgroups of $H^0(A, \Omega^1_{A/\mathbf{Q}})$.*

Proof. Let ϕ denote the composite

$$H^0(A_{\mathbf{C}}, \Omega^1_{A_{\mathbf{C}}/\mathbf{C}}) \overset{\phi_A^* \otimes \mathbf{C}}{\longrightarrow} H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}}) \overset{F\text{-exp}}{\longrightarrow} \mathbf{C}[[q]].$$

Now ϕ_A^* is injective: if $X = X_1(N)$, this follows by considering pullbacks along the sequence of maps in (4); if $X = X_0(N)$, then a similar argument works, noting that the pullback of differentials along $X_1(N) \to X_0(N)$ is injective. Also, F-exp is injective since the Fourier expansion map is injective. Thus ϕ is injective.

By Lemma 3.13 and the commutativity of the diagram preceeding it, $\phi(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})) \subseteq \phi(\oplus_j \mathbf{Z}\omega_j)$. As ϕ is injective, $H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}}) \subseteq \bigoplus_j \mathbf{Z}\omega_j$. □

As a corollary, we get the following generalization of Thm. 2.4 of Edixhoven:

Theorem 3.15. *The Manin constant c_A is an integer.*

Note that the quotient

$$\frac{\oplus_j \mathbf{Z}\omega_j}{H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}})} \cong \frac{\psi(S_2(\Gamma_1(N), \mathbf{Z}))}{\phi_A^*(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}}))} \cong \frac{F\text{-exp}(\psi(S_2(\Gamma_1(N), \mathbf{Z})[I]))}{q\text{-exp}\left(\phi_A^*\left(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}})\right)\right)}$$

is in fact a module over $\mathbf{T}$, and hence one may in general be interested in its module structure, as opposed to just the Manin constant, which is its order. However, we shall not go into such questions in this paper.

Remark 3.16. Note that the reason we used the model $\mathcal{X}_\mu(N)$ above was that we needed a smooth model over $\mathbf{Z}$ (so that we can use the Néron mapping property) on whose differentials we could define a q-expansion map over $\mathbf{Z}$ that agreed with the usual one over $\mathbf{C}$. When A is a quotient of $J_0(N)$, (i.e., when $J = J_0(N)$), we could have used a model for $X_0(N)$ itself in the proof above, as we describe now.

By [KM85, 6.6.1], the moduli problem $[\Gamma_0(N)]$ ([KM85, 3.4]) is relatively representable and finite. The moduli problem $[\Gamma_0(N)]$ is also regular (by [KM85, 6.6.1] again), and hence normal, and so the associated coarse moduli scheme $M([\Gamma_0(N)])$ is normal (by [KM85, 8.1.2]). So one can use [KM85, §8.6] to compactify it; call the resulting compactification $M_0(N)$. Let $M_0(N)^0$ be the open part of $M_0(N)$ where the projection to $\operatorname{Spec} \mathbf{Z}$ is smooth. For the case where $J = J_0(N)$, we could have used $M_0(N)^0$ instead of $\mathcal{X}_\mu(N)$ for proving integrality of the Manin constant. This is what was done in the proof of Prop. 2 in [Edi91], but some of the details were skipped, which we mention two paragraphs below.

Note that q-expansion maps over $\mathbf{Z}$ or $\mathbf{Z}[1/m]$ (where m is the largest square that divides N) on differentials on certain models of $X_0(N)$ have been constructed in several places in the literature (e.g., [Maz78, p.141], [AU96, p.271]), and the usual reference given is [DR73]. However, this seems inadequate, since in [DR73], one has to invert N to get a moduli-theoretic interpretation at the cusps. And in [KM85], while the models are over $\mathbf{Z}$, they do not give a moduli interpretation at the cusps. We now indicate how the construction of a q-expansion map over $\mathbf{Z}$ for differentials on $M_0(N)^0$ can be justified (this is probably well-known to experts).

One method, communicated to us by B. Edixhoven, is as follows: Consider the Tate curve $\mathrm{Tate}(q)$ over $\mathbf{Z}((q))$ as in [KM85, p.258] along with its canonical subgroup μ_N. This gives us an element of $M_0(N)(\mathbf{Z}((q)))$ as in [KM85, §8.11]. One then verifies that this element extends uniquely to an element of $M_0(N)(\mathbf{Z}[[q]])$. Thus we get a map $\tau : \operatorname{Spec} \mathbf{Z}[[q]] \rightarrow M_0(N)$ and composing with the map $\operatorname{Spec} \mathbf{Z} \rightarrow \operatorname{Spec} \mathbf{Z}[[q]]$ (given by $q \mapsto 0$)), we get a point in $M_0(N)(\mathbf{Z})$, called the cusp ∞. The structure along ∞ of $M_0(N)$ is described in [Edi90, §1.2]; in particular, the completion along ∞ is given by $\mathbf{Z}[[q]]$, and so ∞ is a smooth point. Thus the map τ factors through $M_0(N)^0$, and so we can define a q-expansion map on $H^0(M_0(N)^0, \Omega_{M_0(N)^0/\mathbf{Z}})$ as we did (for $\mathcal{X}_\mu(N)$) above. The usual q-expansion map over $\mathbf{C}$ is just given by extending scalars from $\mathbf{Z}$ to $\mathbf{C}$ in the description just above, and hence our q-expansion map is compatible with the usual one over $\mathbf{C}$.

Another method, which is more moduli-theoretic, was communicated to us by B. Conrad, and is as follows: it is shown in [Con03] that one can merge the "affine" moduli-theoretic $\mathbf{Z}$-theory in [KM85] with the "proper" moduli-theoretic $\mathbf{Z}[1/N]$-theory in [DR73]. Using this, one can show that the proper schemes over $\mathbf{Z}$ in [KM85] are in fact moduli schemes for generalized elliptic curves with "Drinfeld structure". Then, by the moduli interpretation, the Tate curve with its canonical subgroup gives a map τ and the cusp ∞ as in the previous paragraph. Next, one can use a deformation theoretic argument to show that the cusp ∞ is a smooth point, i.e., that τ factors through $M_0(N)^0$. As in the previous paragraph, one can now pullback via τ to get the q-expansion map over $\mathbf{Z}$, which by the moduli interpretation agrees with the usual q-expansions over $\mathbf{C}$.

3.2.3 Results and a Conjecture

For the rest of this paper, we restrict to the case of quotients of $J_0(N)$ (i.e., $\Gamma = \Gamma_0(N)$ henceforth). Note that the Manin constants c_A might not equal 1! For example, suppose $A = J_0(N)$ is the quotient by the trivial ideal. Let us work in the setting of Remark 3.16, using the model $M_0(N)^0$

over $\mathbf{Z}$ of $X_0(N)$. Then, since $A = J_0(N)$, the map ϕ_A^* is just

$$H^0(J_0(N)_{\mathbf{Z}}, \Omega^1_{J_0(N)/\mathbf{Z}}) \to H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}),$$

which is an isomorphism. Let us identify $S_2(\mathbf{Z})$ with its image in $\mathbf{Z}[[q]]$. Then using the argument in the proof of Proposition 3.14 we see that c_A is the order of the cokernel of the map

$$H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}) \xrightarrow{q\text{-exp}} S_2(\mathbf{Z}), \tag{6}$$

where q-exp is the q-expansion map discussed in Remark 3.16. The map (6) need not be surjective, and the order of its cokernel can be calculated by using methods in [DR73, VII.3.17] (see [Edi03]). For example, B. Edixhoven communicated to us that for $N = 33$ the cokernel has order 3, so $c_{J_0(33)} = 3$. B. Edixhoven also informed us that if N is square free, then the map (6) is surjective if and only if there are no old spaces in $S_2(\Gamma_0(N), \mathbf{C})$ (cf. [Edi03]). See also Remark 3.21 below for an example of a quotient of $J_0(N)$, with N prime, and with Manin constant 2.

Note that $H^0(M_0(N)^0_{\mathbf{Z}}, \Omega^1_{M_0(N)^0/\mathbf{Z}})$ is precisely the subgroup of $S_2(\mathbf{Q}) = H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Q}})$ of elements that have integral Fourier expansion at all the cusps (this follows from the interpretation in [Edi03] of the integrality condition in terms of a differential having no pole along along any irreducible component of $M_0(N)^0$). Whereas $S_2(\mathbf{Z})$ consists of differentials that are required only to have integral Fourier expansion at the cusp ∞.

If one assumes the BSD conjecture, then a comparison of formulas for the ratio $L(J_e, 1)/\Omega_{J_e}$, where J_e is the winding quotient of prime level, and the corresponding formulas for winding quotients of level a product of two distinct primes (see [Aga00, Thm. 3.2.2 and Thm. 4.2.1]) suggests that the Manin constant of such winding quotients is not one when there are old forms involved (see [Aga00, §4.2.1] for details).

At the same time, we were able to prove the following results for quotients of the new part of $J_0(N)$. We postpone the proofs until Sections 4 and 5. In the following, p always denotes a prime, A is an optimal quotient of $J_0(N)$ attached to a saturated ideal $I \subset \mathbf{T}$, and if we write $A = A_f$, then we mean that I is the annihilator of a newform of level N.

The following theorem generalizes Theorem 2.5 of Mazur:

Theorem 3.17. *Suppose the quotient map $J_0(N) \to A$ factors through $J_0(N)^{\mathrm{new}}$. If $p \mid c_A$, then $p^2 \mid N$ or $p = 2$.*

The following theorem generalizes Theorem 2.6 of Raynaud:

Theorem 3.18. *If* $4 \nmid N$*, then* $\mathrm{ord}_2(c_{A_f}) \leq \dim A_f$*.*

We also have the following theorem (which is a generalization of Theorem 2.9 whose proof builds on techniques of [AU96]):

Theorem 3.19. *If* $p \mid c_{A_f}$*, then* $p^2 \mid N$ *or* $p \mid \tilde{r}_{A_f}$*.*

Note that the techniques of the proof of this theorem can be used to prove that if the quotient map $J_0(N) \to A$ factors through $J_0(N)^{\mathrm{new}}$, and if $p \mid c_A$, then $p^2 \mid N$ or $p = 2$ or $p \mid \tilde{r}_A$ (see Remark 5.4). However, this does not add anything new, in light of Theorem 3.17.

In the case when the level is not square free, computations of [FpS$^+$99] involving Jacobians of genus 2 curves that are quotients of $J_0(N)^{\mathrm{new}}$ show that $c_A = 1$ in 28 case of two-dimensional quotients. These include quotients having the following non-square-free levels:

$$3^2 \cdot 7, \quad 3^2 \cdot 13, \quad 5^3, \quad 3^3 \cdot 5, \quad 3 \cdot 7^2, \quad 5^2 \cdot 7, \quad 2^2 \cdot 47, \quad 3^3 \cdot 7.$$

The above observations are evidence for the following conjecture, which generalizes Conjecture 2.3 of Manin:

Conjecture 3.20. *If* f *is a newform, then* $c_{A_f} = 1$*.*

Remark 3.21. One may wonder if the conjecture above might hold when the quotient map $J_0(N) \to A$ factors through $J_0(N)^{\mathrm{new}}$. However, Adam Joyce [Joy03] found an optimal quotient of $J_0(431)^{\mathrm{new}}$ whose Manin constant is 2 (this example is motivated by [Kil02]); note that this optimal quotient is not attached to a single newform.

4 Proofs of Theorem 3.17 and Theorem 3.18

The proofs of the theorems are similar. Suppose $p \mid\mid N$. The reduction $X_0(N)_{\mathbf{F}_p}$ is a union of two copies of $X_0(N/p)_{\mathbf{F}_p}$, identified at the supersingular points. A differential on $X_0(N)_{\mathbf{F}_p}$ has q-expansion 0 if and only if it vanishes on the component X of $X_0(N)_{\mathbf{F}_p}$ that contains ∞. Since there can be differentials that vanish on X, but not on the other component, the q-expansion map on differentials on $X_0(N)_{\mathbf{F}_p}$ need not be injective. However, as Mazur observed in [Maz78], if a differential is an eigenvector for the Atkin-Lehner involution W_p, then it is 0 on one component if and only if it is 0 on both components, since W_p swaps the two components. That the q-expansion map *is* injective on each eigenspace for W_p is one of the key ideas behind the proofs of Theorems 3.17, 3.18, and 3.19.

4.1 Proof of Theorem 3.17

Let A be a quotient of $J = J_0(N)$ by an ideal of the Hecke algebra such that the quotient map factors through $J_0(N)^{\mathrm{new}}$. Recall that we want to prove that that c_A is a unit in $\mathbf{Z}[\frac{1}{2m}]$, where m is the largest square dividing N. We do this by generalizing techniques of Mazur (the proof of [Maz78, Prop. 3.1]).

Let $R := \mathbf{Z}[\frac{1}{2m}]$, and let $\mathcal{A}$ denote the Néron model of A over R, and $\mathcal{J}$ the Néron model of $J_0(N)$ over R. Let $\mathcal{X}$ be the smooth locus of a minimal proper regular model for $X_0(N)$ over R, and let $\Omega_{\mathcal{X}}$ denote the sheaf of "regular differentials", denoted Ω in [Maz78, §2(e)].

Let π denote the map $J_0(N) \to A$. Consider the diagram

$$H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \xrightarrow{\pi^*} H^0(\mathcal{J}, \Omega_{\mathcal{J}}) \cong H^0(\mathcal{X}, \Omega_{\mathcal{X}}) \xrightarrow{q\text{-exp}} R[[q]], \tag{7}$$

where the map q-exp is as in [Maz78, §2(e)]. We are slightly abusing notation here, since we had defined a different q-expansion map in Section 3.2.2.

The composite of the maps in (7) must be an inclusion because $H^0(\mathcal{A}, \Omega_{\mathcal{A}})$ is torsion free and the composite is an inclusion after tensoring with $\mathbf{C}$. To show that the generalized Manin constant is a unit in R, it suffices to check that the image of $H^0(\mathcal{A}, \Omega_{\mathcal{A}})$ in $R[[q]]$ is *saturated*, in the sense that the cokernel is torsion free. This is because the image of $S_2(\Gamma_0(N); R)[I]$ is saturated in $R[[q]]$ and $S_2(\Gamma_0(N); R)[I] \otimes \mathbf{Q} = H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \otimes \mathbf{Q}$.

For the image of $H^0(\mathcal{A}, \Omega_{\mathcal{A}})$ in $R[[q]]$ to be saturated means that the quotient D is torsion free. Let ℓ be a prime not dividing $2m$. Tensoring the sequence

$$0 \to H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \xrightarrow{q\text{-exp}} R[[q]] \to D \to 0$$

with $\mathbf{F}_\ell$, we obtain

$$0 \to D[\ell] \to H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \to \mathbf{F}_\ell[[q]] \to D \otimes \mathbf{F}_\ell \to 0.$$

Here we have used either the snake lemma applied to multiplication-by-ℓ or that $\mathrm{Tor}^1(D, \mathbf{F}_\ell)$ is the ℓ-torsion in D, and that $\mathrm{Tor}^1(-, \mathbf{F}_\ell)$ vanishes on the torsion-free group $R[[q]]$. To show that $D[\ell] = 0$, it suffices to prove that the map $\Phi : H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \to \mathbf{F}_\ell[[q]]$ is injective.

Since A is optimal, J has good or semistable reduction at ℓ, and $\ell \neq 2$, [Maz78, Cor 1.1] gives an exact sequence

$$0 \to H^0(\mathcal{A}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{A}_{\mathbf{Z}_\ell}}) \to H^0(\mathcal{J}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{J}_{\mathbf{Z}_\ell}}) \to H^0(\mathcal{B}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{B}_{\mathbf{Z}_\ell}}) \to 0$$

where $\mathcal{B} = \ker(\mathcal{J} \to \mathcal{A})$. Since $H^0(\mathcal{B}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{B}_{\mathbf{Z}_\ell}})$ is torsion free, the map

$$H^0(\mathcal{A}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{A}_{\mathbf{Z}_\ell}}) \otimes \mathbf{F}_\ell \to H^0(\mathcal{J}_{\mathbf{Z}_\ell}, \Omega_{\mathcal{J}_{\mathbf{Z}_\ell}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{X}_{\mathbf{F}_\ell}, \Omega_{\mathcal{X}_{\mathbf{F}_\ell}})$$

is injective. We also remark that

$$H^0(\mathcal{A},\Omega_{\mathcal{A}})\otimes \mathbf{F}_\ell \cong H^0(\mathcal{A}_{\mathbf{Z}_\ell},\Omega_{\mathcal{A}_{\mathbf{Z}_\ell}})\otimes \mathbf{F}_\ell,$$

because $\mathbf{Z}_\ell$ is torsion free, hence flat over R. Thus the map

$$H^0(\mathcal{A},\Omega_{\mathcal{A}})\otimes \mathbf{F}_\ell \to H^0(\mathcal{X}_{\mathbf{F}_\ell},\Omega_{\mathcal{X}_{\mathbf{F}_\ell}})$$

is injective.

If $\ell\nmid N$, then injectivity of Φ now follows from the q-expansion principle, which asserts that the q-expansion map $H^0(\mathcal{X}_{\mathbf{F}_\ell},\Omega_{\mathcal{X}_{\mathbf{F}_\ell}})\to \mathbf{F}_\ell[[q]]$ is injective. (This part of the argument does not assume that A is new.)

Next suppose that $\ell\mid N$; note that $\ell \mid\mid N$ because $\ell\nmid m$. As mentioned above, the reduction $\mathcal{X}_{\mathbf{F}_\ell}$ is a union of two copies of $X_0(N/\ell)_{\mathbf{F}_\ell}$ identified transversely at the supersingular points, and these two copies are swapped under the action of the Atkin-Lehner involution W_ℓ. The q-expansion principle implies that ω vanishes on the irreducible component containing the cusp ∞. Now the action of W_ℓ on $H^0(\mathcal{A},\Omega_{\mathcal{A}})\otimes\mathbf{F}_\ell$ is diagonalizable since its minimal polynomial divides X^2-1, the polynomial X^2-1 has distinct roots since $\ell\neq 2$, and the eigenvalues $\pm$ 1 are in $\mathbf{F}_\ell$. Let $\omega\in\ker(\Phi)$ be in the $+1$ eigenspace for the action of W_ℓ. If ω is also nonzero on the component that does not contain ∞, then $\omega = W_\ell(\omega)$ is nonzero when restricted to the component that contains ∞, which is a contradiction. Therefore $\omega=0$. A similar argument shows that if $\omega\in\ker(\Phi)$ is in the -1 eigenspace for the action of W_ℓ, then $\omega=0$. Hence Φ is injective, as required.

4.2 Proof of Theorem 3.18

Recall that we want to prove that if $A=A_f$ is a quotient of $J=J_0(N)$ attached to a newform f, and $4\nmid N$, then $\mathrm{ord}_2(c_A\leq \dim(A)$. The proof closely follows the one in [AU96], except at the end we argue using indexes instead of multiples.

Let B denote the kernel of the quotient map $J\to A$. Consider the exact sequence $0\to B\to J\to A\to 0$, and the corresponding complex $B_{\mathbf{Z}_2}\to J_{\mathbf{Z}_2}\to A_{J_{\mathbf{Z}_2}}$ of Néron models. Because $J_{\mathbf{Z}_2}$ has semiabelian reduction (since $4\nmid N$), Theorem A.1 of the appendix of [AU96, pg. 279–280], due to Raynaud, implies that there is an integer r and an exact sequence

$$0\to \mathrm{Tan}(B_{\mathbf{Z}_2})\to\mathrm{Tan}(J_{\mathbf{Z}_2})\to\mathrm{Tan}(A_{\mathbf{Z}_2})\to(\mathbf{Z}/2\mathbf{Z})^r\to 0.$$

Here Tan is the tangent space at the 0 section; it is a free abelian group of rank equal to the dimension (it gives an integral structure on the usual tangent space, just as differentials on the Néron model give an integral structure on the differentials on the abelian variety). Note that Tan is $\mathbf{Z}_2$-dual to the cotangent space, and the cotangent space is isomorphic to the global differential 1-forms. The theorem of Raynaud mentioned above is the generalization to $e = p-1$ of [Maz78, Cor. 1.1], which we used above in the proof of Theorem 3.17.

Let C be the cokernel of $\mathrm{Tan}(B_{\mathbf{Z}_2}) \to \mathrm{Tan}(J_{\mathbf{Z}_2})$. We have a diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Tan}(B_{\mathbf{Z}_2}) \arrow[r] & \mathrm{Tan}(J_{\mathbf{Z}_2}) \arrow[rr] \arrow[dr, two heads] & & \mathrm{Tan}(A_{\mathbf{Z}_2}) \arrow[r] & (\mathbf{Z}/2\mathbf{Z})^r \arrow[r] & 0. \\
& & & C \arrow[ur, hook] & & &
\end{tikzcd} \qquad (8)$$

Note that $C \subset \mathrm{Tan}(A_{\mathbf{Z}_2})$, so C is torsion free, hence C is a free $\mathbf{Z}_2$-module of rank $d = \dim(A)$. Let $C^* = \mathrm{Hom}_{\mathbf{Z}_2}(C, \mathbf{Z}_2)$ be the $\mathbf{Z}_2$-linear dual of C. Applying the $\mathrm{Hom}_{\mathbf{Z}_2}(-, \mathbf{Z}_2)$ functor to the two short exact sequences in (8), we obtain exact sequences

$$0 \to C^* \to \mathrm{H}^0(J_{\mathbf{Z}_2}, \Omega_{J/\mathbf{Z}_2}) \to \mathrm{H}^0(B_{\mathbf{Z}_2}, \Omega_{B/\mathbf{Z}_2}) \to 0,$$

and

$$0 \to \mathrm{H}^0(A_{\mathbf{Z}_2}, \Omega_{A/\mathbf{Z}_2}) \to C^* \to (\mathbf{Z}/2\mathbf{Z})^r \to 0. \tag{9}$$

Note that the $(\mathbf{Z}/2\mathbf{Z})^r$ on the right in (9) is really $\mathrm{Ext}^1_{\mathbf{Z}_2}((\mathbf{Z}/2\mathbf{Z})^r, \mathbf{Z}_2)$, which is canonically isomorphic to $(\mathbf{Z}/2\mathbf{Z})^r$. Also, (9) implies that $r \leq d = \dim(A)$.

Let $\mathcal{X}'$ be the smooth locus a minimal proper regular model for $X_0(N)$ over $\mathbf{Z}[1/m]$ (recall that m is the largest square dividing N), and let $\Omega_{\mathcal{X}'}$ denote the sheaf of "regular differentials" (denoted Ω in [Maz78, §2(e)]).

Arguing as in the last two paragraphs of the proof of Theorem 3.17 above (note that since A is attached to a single newform, the Atkin-Lehner involution W_2 acts either as $+1$ or as -1), we see that the composition

$$C^* \otimes \mathbf{F}_2 \to \mathrm{H}^0(J_{\mathbf{Z}_2}, \Omega_{J/\mathbf{Z}_2}) \otimes \mathbf{F}_2 \cong \mathrm{H}^0(\mathcal{X}'_{\mathbf{F}_2}, \Omega_{\mathcal{X}'_{\mathbf{F}_2}}) \xrightarrow{q\text{-exp}} \mathbf{F}_2[[q]]$$

is injective. Thus, just as in the proof of Theorem 3.17, we see that the image of C^* in $\mathbf{Z}_2[[q]]$ is saturated. The Manin constant for A at 2 is the index of the image via q-expansion of $\mathrm{H}^0(A_{\mathbf{Z}_2}, \Omega)$ in $\mathbf{Z}_2[[q]]$ in its saturation. Since the image of C^* in $\mathbf{Z}_2[[q]]$ is saturated, the image of C^* is the saturation of the image of $\mathrm{H}^0(A_{\mathbf{Z}_2}, \Omega)$, so the Manin index at 2 is the index of $\mathrm{H}^0(A_{\mathbf{Z}_2}, \Omega)$ in C^*, which is 2^r by (8), hence is at most 2^d.

5 Proof of Theorem 3.19

Let $A = A_f$ be a quotient of $J = J_0(N)$ attached to a newform f. Recall that we want to prove that if $p \mid c_A$, then $p^2 \mid N$ or $p \mid \tilde{r}_A$. The key idea is to project the "Manin index" to the differentials on the dual of A and to use a "conjugate isogeny" to bring it back to differentials on a model of $X_0(N)$, and then use an argument similar to the one in the last two paragraphs of Section 4.1.

We will try to use notation consistent with the one in [AU96] since we will follow their techniques closely. If G is a finite group, we denote its order by $\# G$.

Suppose A_1 and A_2 are abelian varieties such that there is an isogeny $f : A_1 \to A_2$. If n is a positive integer which annihilates $\ker f$, then the multiplication by n map on A_1 factors through $A_1/\ker f \cong A_2$, thus giving an isogeny $f' : A_2 \to A_1$ such that $f' \circ f$ is the multiplication by n map on A_1. Also one sees that $f \circ f'$ is the multiplication by n map on A_2.

We apply this to our situation as follows. Recall that ϕ_2 denotes the quotient map $J \to A$, and ϕ_1 denotes the composition of the dual map $A^\vee \to J^\vee$ with the canonical polarization $J^\vee \cong J$.

The composite

$$A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A \tag{10}$$

is an isogeny (by Proposition 3.1), and as in Definition 3.2, we denote the exponent of the kernel of this isogeny by $\tilde{n}_A$. Applying the argument in the previous paragraph to the composite map in (10), we see that there is an isogeny $\phi' : A \to A^\vee$ such that the composite

$$A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A \xrightarrow{\phi'} A^\vee \tag{11}$$

is the multiplication by $\tilde{n}_A$ map on $A^\vee$, and the composite

$$A \xrightarrow{\phi'} A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A \tag{12}$$

is the multiplication by $\tilde{n}_A$ map on A.

Pulling back differentials along ϕ_2 and ϕ_1 in (10), we obtain maps:

$$H^0(A_{\mathbf{C}}, \Omega^1_{A/\mathbf{C}}) \xrightarrow{\phi_2^*} H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}) \xrightarrow{\phi_1^*} H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}}).$$

As before, let m denote the largest square that divides the level N and let $S = \operatorname{Spec} \mathbf{Z}[\frac{1}{m}]$. Let $M_0(N)$ be as in Remark 3.16. Then $M_0(N)_S$ is semistable over S. Let Ω be the relative dualizing sheaf of $M_0(N)_S$ over S. Consider the map

$$q\text{-exp} : H^0(M_0(N)_S, \Omega) \hookrightarrow \mathbf{Z}[1/m][[q]]$$

in [AU96, §2.1] (cf. Remark 3.16). Note that we are abusing notation slightly since we had defined a different q-expansion map in Section 3.2.2.

As mentioned in [AU96, §2.1] we have an inclusion

$$q\text{-exp} : H^0(M_0(N)_S, \Omega) \hookrightarrow S_2(\mathbf{Z}[\tfrac{1}{m}])$$

(this really follows from the discussion in Section 3.2.2). This map is not an isomorphism in general, but it induces an isomorphism

$$q\text{-exp} : H^0(M_0(N)_{\mathbf{F}_p}, \Omega) \xrightarrow{\cong} S_2(\mathbf{F}_p) \qquad (13)$$

for each prime p that does not divide N (this is stated in [AU96, §2.1] and follows, for example, using the arguments in Section 4.1).

We have

$$H^0(M_0(N)_S, \Omega) \hookrightarrow S_2(\mathbf{Z}[\tfrac{1}{m}]) \hookrightarrow S_2(\mathbf{C}) \cong H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}).$$

Applying ϕ_1^* to the first two groups, we get an injection

$$\phi_1^*(H^0(M_0(N)_S, \Omega)) \hookrightarrow \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])),$$

where the source and target are viewed as sitting in $H^0(A^\vee_{\mathbf{C}}, \Omega_{A^\vee/\mathbf{C}})$. Denote the cokernel of the above map by C. It is a finite group and, by (13), the only primes that can divide its order are the primes that divide N. An easy generalization of [AU96, Prop. 3.2] gives

$$\phi_1^*(H^0(M_0(N)_S, \Omega)) = H^0(A^\vee_S, \Omega^1_{A^\vee/S}),$$

so we have an exact sequence

$$0 \to H^0(A^\vee_S, \Omega^1_{A^\vee/S}) \to \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \to C \to 0.$$

On considering the quotient of the middle group above by the pullback of $H^0(A_S, \Omega^1_{A/S})$ under $\phi_2 \circ \phi_1$, we obtain

$$0 \to \frac{H^0(A^\vee_S, \Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to \frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to C \to 0. \qquad (14)$$

Now ϕ_1^* is injective when restricted to $\phi_2^* H^0(A_{\mathbf{C}}, \Omega^1_{A/\mathbf{C}})$ (this follows because the pullback of the composite of the maps in (12) is injective, being multiplication by $\tilde{n}_A$ on a vector space over $\mathbf{C}$). So, since

$$S_2(\mathbf{Z})[I] \subseteq \phi_2^* H^0(A_{\mathbf{C}}, \Omega^1_{A/\mathbf{C}}),$$

we have a natural isomorphism

$$\frac{S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}]}{\phi_2^* H^0(A_S, \Omega^1_{A/S})} \xrightarrow{\cong} \frac{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])}{\phi_1^*(\phi_2^* H^0(A_S, \Omega^1_{A/S}))}.$$

If i is a positive integer, then let i_m denote the largest divisor of i that is prime to m. By the discussion in Section 3.2.2,

$$(c_A)_m = \# \left(\frac{S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}]}{\phi_2^* H^0(A_S, \Omega^1_{A/S})} \right).$$

So

$$(c_A)_m = \# \left(\frac{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])}{\phi_1^*(\phi_2^* H^0(A_S, \Omega^1_{A/S}))} \right).$$

Hence

$$\# \left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \right) = (c_A)_m \cdot \# \left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))}{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])} \right). \qquad (15)$$

As in the proof of [AU96, Prop. 3.3], we have the isomorphisms

$$\begin{aligned} \left(\frac{S_2(\mathbf{Z})}{S_2(\mathbf{Z})[I] \oplus W(I} \right) \otimes \mathbf{Z}[\tfrac{1}{m}] \quad & \xrightarrow{\cong} \quad \frac{S_2(\mathbf{Z}[\frac{1}{m}])}{(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}]) \oplus (W(I) \otimes \mathbf{Z}[\frac{1}{m}])} \\ & \xrightarrow{\cong} \quad \frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}])))}{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])}. \end{aligned}$$

Thus

$$\# \left(\frac{\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}])))}{\phi_1^*(S_2(\mathbf{Z})[I] \otimes \mathbf{Z}[\frac{1}{m}])} \right) = (r_A)_m.$$

Putting this in (15) and then using (14), we get

$$(c_A)_m \cdot (r_A)_m = \# \left(\frac{H^0(A_S^\vee, \Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \right) \cdot \# C. \qquad (16)$$

Since the composite of the maps in (11) is multiplication by $\tilde{n}_A$, we see that multiplication by some power of $\tilde{n}_A$ kills $\left(\frac{H^0(A_S^\vee, \Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \right)$. Thus we have the following lemma:

Lemma 5.1. *If p is a prime such that p divides $\#\left(\frac{H^0(A_S^\vee,\Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S,\Omega^1_{A/S})}\right)$, then $p \mid \tilde{n}_A$.*

We already remarked that a prime can divide $\#C$ only if it divides N. The main addition to the techniques of [AU96] is the following result that further controls the primes that can divide $\#C$:

Proposition 5.2. *If A is a quotient of $J_0(N)$ attached to a newform and p is a prime such that $p \mid \#C$, then $p^2 \mid N$ or $p \mid \tilde{r}_A$.*

We will prove Proposition 5.2 shortly, but note that now Theorem 3.19 follows easily. Indeed, suppose $p^2 \nmid N$ and $p \mid c_A$. Then $p \mid (c_A)_m$, and so by equation (16), $p \mid \#\left(\frac{H^0(A_S^\vee,\Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S,\Omega^1_{A/S})}\right)$ or $p \mid \#C$. In the former case, by Lemma 5.1, $p \mid \tilde{n}_A$, and hence by Proposition 3.9, $p \mid \tilde{r}_A$ and in the latter case, by Proposition 5.2, $p \mid \tilde{r}_A$.

Remark 5.3. The obstruction to proving a generalization of Theorem 2.7 to dimension greater than one lies in equation (16). When A is an elliptic curve, Abbes-Ullmo [AU96] prove that the quotient of differentials on the right hand side of (16) divides $(r_A)_m$. Thus $(c_A)_m \mid \#C$, which proves Theorem 2.7, since the prime divisors of $\#C$ divide N. When A has dimension bigger than 1, the relationship between the quotient of differentials and $(r_A)_m$ is unclear. For example, Remark 3.10 suggests that divisibility might sometimes fail when multiplicity one fails.

We now prove the proposition.

Proof of Proposition 5.2. We have the exact sequence

$$0 \to \phi_1^*(H^0(M_0(N)_S,\Omega)) \to \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}])) \to C \to 0. \qquad (17)$$

Suppose p is a prime such that $p^2 \nmid N$ and $p \nmid \tilde{r}_A$. We want to show that $p \nmid \#C$. We already know that the only primes that can divide $\#C$ are those that divide N; so we may assume that p exactly divides N. Then considering the multiplication by p map applied to each term of the sequence of maps (17) and using the snake lemma, we get:

$$0 \to C[p] \to \phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p \xrightarrow{q\text{-exp}} \phi_1^*(S_2(\mathbf{Z}[\tfrac{1}{m}]))\otimes\mathbf{F}_p \to C\otimes\mathbf{F}_p \to 0$$

(note the similarity to the situation in Section 4.1). Then to show that $p \nmid \#C$, i.e., that $C[p]$ is trivial, all we have to show is that the map

$$\begin{tikzcd}
\phi_1^*(H^0(M_0(N)_S,\Omega)) \otimes \mathbf{F}_p \arrow[d, "q\text{-exp}"] \\
\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}])) \otimes \mathbf{F}_p
\end{tikzcd} \tag{18}$$

is injective.

The key idea is to use the isogeny ϕ' defined at the beginning of this section. Then we have maps

$$A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A \xrightarrow{\phi'} A^\vee \tag{19}$$

such that the composite is multiplication by $\tilde{n}_A$. Let $\phi'' = \phi' \circ \phi_2$. Pulling back differentials, we get the maps

$$H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}}) \xrightarrow{\phi''^*} H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}) \xrightarrow{\phi_1^*} H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}}), \tag{20}$$

where the composite is again multiplication by $\tilde{n}_A$.

By the Néron mapping property, the maps (19) extend to the corresponding Néron models, and we see that $\phi''^*(\phi_1^*(H^0(J_S,\Omega_{J/S}))) \subseteq H^0(J_S,\Omega_{J/S})$. By [AU96, p.271], the canonical morphism $X_0(N) \to J_0(N)$ induces a canonical isomorphism $H^0(J_S,\Omega_{J/S}) \overset{\cong}{\to} H^0(M_0(N)^0_S,\Omega) = H^0(M_0(N)_S,\Omega)$. Thus we see that the image of $\phi_1^*(H^0(M_0(N)_S,\Omega)) = \phi_1^*(H^0(J_S,\Omega_{J/S}))$ under ϕ''^* lands in $H^0(M_0(N)_S,\Omega) = H^0(J_S,\Omega_{J/S})$. Also, since $p \nmid \tilde{r}_A$, we have $S_2(\mathbf{Z}[\frac{1}{m}]) \otimes \mathbf{F}_p = S_2(\mathbf{Z}[\frac{1}{m}])[I] \otimes \mathbf{F}_p \oplus (W(I) \cap S_2(\mathbf{Z}[\frac{1}{m}])[I]) \otimes \mathbf{F}_p$. Thus if $f \in S_2(\mathbf{Z}[\frac{1}{m}]) \otimes \mathbf{F}_p$, then there exist unique $f_1 \in S_2(\mathbf{Z}[\frac{1}{m}])[I] \otimes \mathbf{F}_p$ and $f_2 \in (W(I) \cup S_2(\mathbf{Z}[\frac{1}{m}])[I]) \otimes \mathbf{F}_p$ such that $f = f_1 + f_2$. It then follows that $\phi_1^* f = \phi_1^* f_1$, and so $\phi''^*(\phi_1^* f) = \tilde{n}_A f_1 \in S_2(\mathbf{Z}[\frac{1}{m}]) \otimes \mathbf{F}_p$. Thus the image of $\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}])) \otimes \mathbf{F}_p$ under ϕ''^* lands in $S_2(\mathbf{Z}[\frac{1}{m}]) \otimes \mathbf{F}_p$.

Hence, applying the maps in (20) to the groups in (18) (which are subgroups of $H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}})$), we get the following commutative diagram:

$$\begin{tikzcd}
\phi_1^*(H^0(M_0(N)_S,\Omega))_{\mathbf{F}_p} \arrow[r, "\phi''^*"] \arrow[d, "q\text{-exp}"] & H^0(M_0(N)_S,\Omega)_{\mathbf{F}_p} \arrow[r, "\phi_1^*"] \arrow[d, "q\text{-exp}"] & \phi_1^*(H^0(M_0(N)_S,\Omega))_{\mathbf{F}_p} \arrow[d, "q\text{-exp}"] \\
\phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))_{\mathbf{F}_p} \arrow[r, "\phi''^*"] & S_2(\mathbf{Z}[\frac{1}{m}])_{\mathbf{F}_p} \arrow[r, "\phi_1^*"] & \phi_1^*(S_2(\mathbf{Z}[\frac{1}{m}]))_{\mathbf{F}_p}.
\end{tikzcd}$$

The Atkin-Lehner involution W_p acts on $\phi_1^*(H^0(M_0(N)_S,\Omega)) \otimes \mathbf{F}_p$ and since A is attached to a newform, W_p acts as either $+1$ or -1. Suppose x is an element of $\phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p$ that is in the $+1$ eigenspace for the action of W_p and in the kernel of the map in (18), i.e., the left-most q-exp map above. Then its image $y=(\phi''^*)(x)$ in $H^0(M_0(N)_S,\Omega)\otimes\mathbf{F}_p$ above maps to zero in $S_2(\mathbf{Z}[\frac{1}{m}])\otimes\mathbf{F}_p$ under the middle q-exp map (by commutativity of the first square). But we have $H^0(M_0(N)_S,\Omega)\otimes\mathbf{F}_p\cong H^0(M_0(N)_{\mathbf{F}_p},\Omega)$. Since $p^2\nmid N$, $M_0(N)_{\mathbf{F}_p}$ is a union of two irreducible components. Now q-exp$(y)=0$ means that $y\in H^0(M_0(N)_{\mathbf{F}_p},\Omega)$ is zero on the component that contains the cusp ∞. But x is an eigenvector for W_p, and hence so is y. But W_p is an involution that swaps the two components of $M_0(N)_{\mathbf{F}_p}$. Hence y is zero on all of $M_0(N)_{\mathbf{F}_p}$; i.e., $y=0$. Note that this part of the argument is very similar to the one towards the end of Section 4.1.

Looking at the top line in the diagram above, we find that x maps to zero under the composite. But its image under this composite is $\tilde{n}_A x$, and so $\tilde{n}_A x=0$. Since $p\nmid\tilde{r}_A$, Proposition 3.9 shows that $p\nmid\tilde{n}_A$, and so $x=0$. A similar argument shows that if x is an element of $\phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p$ in the -1 eigenspace for the action of W_p and in the kernel of the map in (18), then $x=0$. This shows that the map (18) is injective, which is what was left to prove. □

Remark 5.4. Note that the fact that A is associated to a single newform was used only in the last two paragraphs of the proof above. We could have used the fact that the action of W_p on $\phi_1^*(H^0(M_0(N)_S,\Omega))\otimes\mathbf{F}_p$ is diagonalizable if $p\neq 2$ (e.g., see the last paragraph of Section 4.1; Remark 3.4 is also relevant here), to prove that if A is a quotient of $J_0(N)$ by an ideal of the Hecke algebra such that the quotient map factors through $J_0(N)^{\mathrm{new}}$, and if $p\mid\#C$, then $p^2\mid N$ or $p=2$ or $p\mid\tilde{r}_A$. Then one would have the statement that for such a quotient, if $p\mid c_A$, then $p^2\mid N$ or $p=2$ or $p\mid\tilde{r}_A$.

References

[Aga99] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374.

[Aga00] A. Agashe, *The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero*, Ph.D. thesis, University of California, Berkeley (2000), `http://www.math.utexas.edu/~amod/math.html`.

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[AS03] A. Agashe and W. A. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture*, to appear in Math. Comp. (2003).

[AU96] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[CK03] J. Cojocaru and E. Kani, *The modular degree and the congruence number of a weight 2 cusp form*, preprint (2003).

[Con03] B. Conrad, *Modular curves, descent theory, and rigid analytic spaces*, in preparation (2003).

[CES03] B. Conrad, B. Edixhoven, and W. A. Stein, $J_1(p)$ *Has Connected Fibers*, to appear in Documenta Math. (2003).

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[DI95] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Edi89] B. Edixhoven, *Stable models of modular curves and applications*, Thèse de doctorat à l'université d'Utrecht (1989), `http://www.maths.univ-rennes1.fr/~edix/publications/prschr.html`.

[Edi90] B. Edixhoven, *Minimal resolution and stable reduction of* $X_0(N)$, Ann. Inst. Fourier (Grenoble) **40** (1990), no. 1, 31–67.

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[Edi03] B. Edixhoven, *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one*, preprint (2003).

[FM99] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[FpS$^+$99] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, submitted (1999).

[Fre97] G. Frey, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 527–548.

[Gro82] B. H. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), Birkhäuser Boston, Mass., 1982, pp. 219–236.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Joy03] A. Joyce, *The manin constant of an optimal quotient of* $j_0(431)$, preprint (2003).

[Kat76] N. M. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571.

[Kil02] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, J. Number Theory **97** (2002), no. 1, 157–164.

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.

[Lan83] S. Lang, *Abelian varieties*, Springer-Verlag, New York, 1983, Reprint of the 1959 original.

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry.

[Li75] W-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

[Man72] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[MR91] B. Mazur and K. A. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque (1991), no. 196-197, 6, 215–255 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mur99] M. R. Murty, *Bounds for congruence primes*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999, pp. 177–192.

[Rib75] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562.

[Rib81] K. A. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight* 2, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser Boston, Mass., 1981, pp. 263–276.

[Rib83] K. A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205.

[Shi73] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[Stu87] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Zag85] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384.