The Manin Constant, Congruence Primes, and the Modular Degree

Amod Agashe Kenneth Ribet William A. Stein

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 equal; they are not, but we prove a theorem relating them and make a conjecture. We also prove results and make conjectures about Manin constants of quotients of $J_1(N)$ of arbitrary dimension. For optimal elliptic curves E, we give a new condition under which the Manin constant of E is odd.

1 Introduction

Let E be an elliptic curve over $\mathbf{Q}$. By [BCDT01], we may view E as a quotient of the modular Jacobian $J_0(N)$, where N is the conductor of E. After possibly replacing E by an isogenous curve, we may assume that the kernel of the map $J_0(N) \to E$ is connected, i.e., that E is an *optimal* quotient of $J_0(N)$.

The pullback of a minimal differential on E is a multiple c of some normalized new cuspidal eigenform $f_E \in S_2(\Gamma_0(N))$. The absolute value of c is the Manin constant c_E of E. Manin conjectured that $c_E = 1$. In Section 2.1, we summarize results about c_E, then extend techniques of Abbes and Ullmo [AU96] to show that $2 \nmid c_E$ under certain hypothesis.

The congruence number $r_{\scriptscriptstyle E}$ of E is the largest integer such that there is a nonzero element of $S_2(\Gamma_0(N))$ that is orthogonal to f_E and congruent to f_E modulo $r_{\scriptscriptstyle E}$. The modular degree $m_{\scriptscriptstyle E}$ is the degree of the composite map $X_0(N) \to J_0(N) \to E$. Section 2.2 is about relations between $r_{\scriptscriptstyle E}$ and $m_{\scriptscriptstyle E}$. For example, $m_{\scriptscriptstyle E} \mid r_{\scriptscriptstyle E}$. In [FM99, Q. 4.4], Frey and Müller asked whether $r_{\scriptscriptstyle E} = m_{\scriptscriptstyle E}$. We give examples in which $r_{\scriptscriptstyle E} \neq m_{\scriptscriptstyle E}$, then conjecture that for any prime p, $\mathrm{ord}_p(r_{\scriptscriptstyle E}/m_{\scriptscriptstyle E}) \leq \frac{1}{2}\,\mathrm{ord}_p(N)$. We prove this conjecture when $\mathrm{ord}_p(N) \leq 1$.

We generalize the Manin constant, congruence primes, and modular degree to optimal quotients of $J_0(N)$ and $J_1(N)$ of any dimension associated to ideals of the Hecke algebra. Section 3 is concerned with the congruence number and the modular degree and Section 4 with the Manin constant. We also conjecture that the Manin constant is 1 for newform quotients of $J_0(N)$ and $J_1(N)$.

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 kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots]$ 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 $2\pi i f(z)dz = f(q)dq/q$ on $X_0(N)$. Because the action of Hecke operators is compatible with the map $X_0(N) \to E$, [AL70] implies 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.

The Manin constant plays a role in the Birch and Swinnerton-Dyer conjecture (see Section 4.1), and its integrality is important to Cremona's computations of elliptic curves (see [Cre97, pg. 45]).

The following conjecture is implicit in [Man72, §5].

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

Significant progress has been made towards this conjecture. In the following list of theorems, 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 using an integral q-expansion map, whose existence and properties follow from results in [KM85]. We generalize his argument to quotients of arbitrary dimension in Section 4.1.

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

Mazur proved this by applying theorems of Raynaud about exactness of sequences of differentials, then using the "q-expansion principle" in characteristic p and a property of the Atkin-Lehner involution. We generalize Mazur's argument in Section 4.1.

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 4.1. However, it is not clear if one can generalize Theorem 2.7 to dimension greater than 1 (see Remark 4.16). It would be fantastic if the theorem could be generalized, since it would imply that for newform 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 10000. 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 $g \in S_2(\Gamma_0(N))$ 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 $p \mid m_E$.*

This theorem is a special case of Theorem 4.13 below, which we prove in Section 4.4. In fact, Theorem 4.13 asserts that if $p \mid c_E$ then $p^2 \mid N$ or $p \mid r_E$. However, Theorem 2.10 implies that when $\mathrm{ord}_p(N) = 1$ then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$. In view of Theorem 2.5, our new contribution is that if m_E is odd and $\mathrm{ord}_2(N) = 1$, then c_E is odd. This hypothesis is *very stringent*—of the 125357 optimal elliptic curve quotients of conductor ≤ 30000, only 31 of them satisfy the hypothesis. In the notation of [Cre97], they are

14A, 46A, 142C, 206A, 302B, 398A, 974C, 1006B, 1454A, 1646A, 1934A, 2606A, 2638B, 3118B, 3214B, 3758D, 4078A, 7054A, 7246C, 11182B, 12398B, 12686C, 13646B, 13934B, 14702C, 16334B, 18254A, 21134A, 21326A, 22318A, 26126A.

It is unknown if there are infinitely many elliptic curves that satisfy our hypothesis. The third author conjectured in [SW04, Conj. 4.2] that there are infinitely many elliptic curves (of prime conductor) with odd modular degree.

2.2 Congruence Primes and the Modular Degree

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. 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]). Thus results that relate congruence primes and the modular degree are of great interest.

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 in [Zag85] the divisibility was mistakenly written in the opposite direction. For some other expositions of the proof, see [AU96, Lem 3.2] and [CK04]. We generalize this divisibility in Proposition 3.11. The second part of Theorem 2.10, i.e., that if $\mathrm{ord}_p(N) = 1$ then $\mathrm{ord}_p(r_E) = \mathrm{ord}_p(m_E)$, follows from the more general Theorem 3.5 below. Note that [AU96, Prop. 3.3–3.4] 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 16 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. For example, for the curve 242B of conductor $N = 2 \cdot 11^2$ we have

$$m_E = 2^4 \neq r_E = 2^4 \cdot 11.$$

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 $N \leq 539$.

3 Quotients of arbitrary dimension: generalization of the congruence number and the modular degree

Let Γ be either $\Gamma_0(N)$ or $\Gamma_1(N)$, for $N \geq 4$, let X be the modular curve over $\mathbf{Q}$ associated to Γ, and let J be the Jacobian of X. Let I be a *saturated* ideal of the corresponding Hecke algebra $\mathbf{T}$, so $\mathbf{T}/I$ is torsion free. Then $A = A_I = J/IJ$ is an optimal quotient of J since IJ is an abelian subvariety.

Definition 3.1 (Newform quotient). If $f \in S_2(\Gamma)$ and $I_f = \ker(\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots])$, then $A = A_f = J/I_fJ$ is the *newform quotient* associated to f. It is an abelian variety over $\mathbf{Q}$ of dimension to the degree of the field $\mathbf{Q}(\ldots, a_n(f), \ldots)$.

In Section 3.1, we generalize the notions of the congruence number and the modular degree to quotients $A = A_I$, and state a theorem relating the two, which we prove in Sections 3.2–3.3.

3.1 The congruence number and the modular degree

If C is an abelian variety, let $C^\vee$ denote the dual of C. 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 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 obtain 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, $\ker(\phi_2^\vee)$ is trivial, so $\phi_2^\vee$ and ϕ_1 are injections. Let ϕ be the composition

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

PROPOSITION 3.2. *The map ϕ is a polarization.*

Proof. Let i be the injection $\phi_2^\vee : A^\vee \to J^\vee$, and let Θ denote the theta divisor. From 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]). □

The *exponent* of a finite group G is the smallest positive integer n such that every element of G has order dividing n.

DEFINITION 3.3. 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. When A is an elliptic curve, the modular exponent is equal to the modular degree of A, and the modular number is the square of the modular degree (see, e.g., [AU96, p. 278]).

If R is a subring of $\mathbf{C}$, let $S_2(\Gamma; R)$ denote the subgroup of $S_2(\Gamma)$ consisting of cups forms whose Fourier expansions at the cusp ∞ have coefficients in R. Let $W(I) = S_2(\Gamma;\mathbf{Z})[I]^\perp$ denote the orthogonal complement of $S_2(\Gamma;\mathbf{Z})[I]$ in $S_2(\Gamma;\mathbf{Z})$ with respect to the Petersson inner product.

DEFINITION 3.4. The exponent of the quotient group

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

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

Our definition of r_A generalizes the definition in Section 2.2 when A is an elliptic curve (see [AU96, p. 276]), and the following generalizes Theorem 2.10:

THEOREM 3.5. *If $f \in S_2(\mathbf{C})$ is a newform, then*

(a) We have $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$, and

(b) If $p^2 \nmid N$, then $\mathrm{ord}_p(\tilde{r}_{A_f}) = \mathrm{ord}_p(\tilde{n}_{A_f})$.

REMARK 3.6. When A_f is an elliptic curve, Theorem 3.5 implies that the modular degree divides the congruence number, i.e., $\sqrt{n_{A_f}} \mid r_{A_f}$. In general, the divisibility $n_{A_f} \mid r_{A_f}^2$ need not hold. For example, there is a newform of degree 24 in $S_2(\Gamma_0(431))$ such that

$$n_{A_f} = (2^{11} \cdot 6947)^2 \nmid r_{A_f} = (2^{10} \cdot 6947)^2.$$

Note that 431 is prime and 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 V2.11 or greater.

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

3.2 Proof of Theorem 3.5 (a)

The polarization of J induced by the theta divisor need not be Hecke equivariant, because 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 (see e.g., [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 $\mathbf{T}$.

Recall that f is a newform, $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$, $J = J_0(N)$, Let $B = I_f J$, so that $A^\vee + B = J$, and $J/B \cong A$. The following lemma is well known, but we prove it here for the convenience of the reader.

Lemma 3.7. $\mathrm{Hom}(A^\vee, B) = 0$.

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 $\mathbf{T}$ in $\mathrm{End}(A^\vee)$, and 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 3.7 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 3.11 below.

The *denominator* of any $\varphi \in \mathrm{End}(J) \otimes \mathbf{Q}$ is the smallest positive integer n such that $n\varphi \in \mathrm{End}(J)$.

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 3.8. *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 3.9. *The group $(\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ is isomorphic to the quotient (1) in Definition 3.4, 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

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

of $\mathbf{T}$ modules. Here we use that $\mathrm{Hom}(\mathbf{T}_2, \mathbf{Z})$ is the unique saturated Hecke-stable complement of $S_2(\mathbf{Z})[I_f]$ in $S_2(\mathbf{Z})$, hence must equal $S_2(\mathbf{Z})[I_f]^{\perp} = W(I_f)$. 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 3.10. *The element $e_1 \in (\mathbf{T}_1 \oplus \mathbf{T}_2)/\mathbf{T}$ has order $\tilde{r}_A$.*

Proof. By Lemma 3.9, 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 3.11. *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 that of e_1. Now apply Lemmas 3.8 and 3.10. □

This finishes the proof of the first statement in Theorem 3.5.

3.3 PROOF OF THE THEOREM 3.5 (B)

Write $N = pM$ with p prime and $p \nmid M$. (Note: The argument below also works if $p = 1$, which addresses the case when no prime exactly divides N.) Let $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots]$ be the subring of $\mathrm{End}(J_0(N))$ generated by the Hecke operators T_n for all $n \geq 1$. Let $\mathbf{T}'$ be the saturation of $\mathbf{T}$ in $\mathrm{End}(J_0(N))$, so

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

where the intersection is taken inside $\mathrm{End}(J_0(N)) \otimes \mathbf{Q}$. The quotient $\mathbf{T}'/\mathbf{T}$ is a finitely generated abelian group because both $\mathbf{T}$ and $\mathrm{End}(J_0(N))$ are finitely generated over $\mathbf{Z}$.

Suppose for the moment that $N = 1$, so $p = pM$. 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 $\mathbf{T} = \mathrm{End}(J_0(p))$.

3.3.1 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 M 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 $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ has dimension ≤ 1. (Here ℓ is the residue characteristic of $\mathfrak{m}$.) In other words, multiplicity one for $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ implies that $\mathbf{T}$ and $\mathbf{T}'$ agree at $\mathfrak{m}$. We record this fact as a lemma.

Lemma 3.12. *Suppose $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ of residue characteristic ℓ and that*

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

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 $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$. The easiest case is that ℓ is prime to the level pM.

Lemma 3.13. *If $\ell \nmid pM$, then $\ell \nmid \#(\mathbf{T}/\mathbf{T}')$.*

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

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

for all $\mathfrak{m} \mid \ell$. Now apply Lemma 3.12 □

In the context of Mazur's paper, where $p = pM$, we see from Lemma 3.13 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 $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_\ell}, \Omega)[\mathfrak{m}]$ 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 from $S_2(\Gamma_0(M))$.)

Lemma 3.14 (Wiles). *If $\mathfrak{m}$ is an ordinary prime of $\mathbf{T}$ of characteristic ℓ and $\mathrm{ord}_\ell(pM) = 1$, 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 $\mathrm{H}^0(X_0(pM)_{\mathbf{F}_p}, \Omega)[\mathfrak{m}]$ 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 $T_p \notin \mathfrak{m}$. (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 exactly divides the level (which is pM here). We make a few further comments about the proof of this lemma.

1. Wiles considers $X_1(M, p)$ instead of $X_0(pM)$, which means that he is using $\Gamma_1(M)$-structure instead of $\Gamma_0(M)$-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 is not relevant to our question.

3. The condition that $\mathfrak{m}$ is ordinary does not appear explicitly in the statement of the lemma; instead it is 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 3.13 and Lemma 3.14) imply that $\mathbf{T}$ and $\mathbf{T}'$ agree locally at each rational prime that is prime to the level pM, 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 some level $N \geq 1$. Then $\mathbf{T} = \mathbf{T}'$ locally at each maximal ideal $\mathfrak{m}$ that is either prime to N or that satisfies the following supplemental hypothesis: the residue characteristic of $\mathfrak{m}$ divides N only to the first power and $\mathfrak{m}$ is ordinary. In Mazur's original context, the level N is prime. Moreover, we have $T_N^2 = 1$ because there are no forms of level 1. Accordingly, each $\mathfrak{m}$ dividing N is ordinary, and we recover Mazur's equality $\mathbf{T} = \mathbf{T}'$ in this special case.

3.3.2 Degrees and Congruences

Let $e \in \mathbf{T} \otimes \mathbf{Q}$ be as in Section 3.2. Let $A \subset J_0(pM)$ be the image of e (note that we denoted this image by $A^\vee$ in Section 3.2). 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 of $\mathrm{End}(A)$ consisting of the various t_A, and define $\mathbf{T}_B$ similarly. As before, 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 3.15 (Congruence Ideal). The *congruence ideal* associated with the projector e is $I = \pi_A(\ker(\pi_B)) \subset \mathbf{T}_A$.

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 $\mathbf{T}_A \times \mathbf{T}_B$, via the map j.

LEMMA 3.16. *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 3.17. *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 3.18. *We have $J = \mathbf{T}_A \cap \mathrm{End}(J_0(pM)) = \mathbf{T}_A \cap \mathbf{T}'$.*

Proof. This is elementary; it is an analogue of Lemma 3.16. □

PROPOSITION 3.19. *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

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

By Lemma 3.16 and Lemma 3.18, 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 3.20. *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 $J_0(pM)$, 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 3.14 and Proposition 3.19 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 3.14. By Lemma 3.13, we have $\mathbf{T} = \mathbf{T}'$ locally at primes away from the level pM. Thus we conclude that $I = J$ locally at all primes $\ell \nmid pM$ and also at p, a prime that divides the level pM exactly once.

Suppose, finally, that A is the abelian variety associated to a newform f of level pM. The ideal $I \subset \mathbf{T}_A$ measures congruences between f and the space of forms in $S_2(\Gamma_0(pM))$ 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 $\tilde{n}_{A_f} \mid \tilde{r}_{A_f}$, and we have equality at primes at which $I = J$ locally. We conclude that the congruence exponent and the modular exponent agree both at p and at primes not dividing pM, which completes our proof of Theorem 3.5.

Remark 3.21. The ring

$$R = \mathrm{End}(J_0(pM)) \cap (\mathbf{T}_A \times \mathbf{T}_B)$$

is often of interest, where the intersection is taken in $\mathrm{End}(J_0(pM)) \otimes \mathbf{Q}$. We proved above that there is a natural inclusion $J/I \hookrightarrow \mathbf{T}'/\mathbf{T}$. This inclusion yields an isomorphism $J/I \xrightarrow{\sim} R/\mathbf{T}$. Indeed, if (t_A, u_B) is an endomorphism of $J_0(pM)$, 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 R coincide. Even when $\mathbf{T}'$ is bigger than $\mathbf{T}$, its subring R may be not far from $\mathbf{T}$.

4 Quotients of arbitrary dimension: generalization of the Manin Constant

Let the notation be as in the beginning of Section 3. Let J_{old} denote the abelian subvariety of J generated by the images of the degeneracy maps from levels that properly divide N (e.g., see [Maz78, §2(b)]) and let J^{new} denote the quotient of J by J_{old}.

In Section 4.1, we generalize the notion of the Manin constant to quotients A as above, and conjecture that this constant is 1 for newform quotients of $J_0(N)$ and $J_1(N)$. In Section 4.2, we show that the (generalized) Manin constant is an integer. In the next two sections, we give generalizations of some of the results from Section 2 to quotients A that factor through $J_0(N)^{\mathrm{new}}$. In Section 4.3, we show that if the level N is squarefree and A is a factor of $J_0(N)^{\mathrm{new}}$, then the Manin constant is a power of 2, whose exponent is bounded above by the dimension of A if A is a newform quotient. In Section 4.4, we prove that if A is a newform quotient of $J_0(N)$ and the level is squarefree, then the Manin constant is coprime to the congruence number.

4.1 The definition of the generalized Manin constant and a conjecture

As in Section 3.1, if R is a subring of $\mathbf{C}$, let $S_2(R) = S_2(\Gamma; R)$ denote the $\mathbf{T}$-submodule of $S_2(\Gamma; \mathbf{C})$ consisting of modular cuspforms whose Fourier expansions at ∞ have coefficients in R. Note that $S_2(R) \cong S_2(\mathbf{Z}) \otimes R$.

If A is an abelian variety over $\mathbf{Q}$ and n is a positive integer, let $A_{\mathbf{Z}[1/n]}$ denote the Néron model of A over $\mathbf{Z}[1/n]$. On a Néron model, the global differentials are the same as the group of invariant differentials, so 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 [AS05]). Let $g_1, \dots, g_d$ be a $\mathbf{Z}$-basis of $S_2(\mathbf{Z})[I]$, and for $j = 1, \dots, d$, 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 $j = 1, \dots, d$, let $\omega_j = (\phi_2^*)^{-1}\omega'_j$.

In calculations (see [AS05]), 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 4.1. 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 as in Definition 2.2. The constant c as defined above was considered 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, since $\Omega_A = c_A \cdot \Omega_{A'}$. This is our 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 general A.

Note that the Manin constants c_A might not equal 1, especially if A is not a quotient of J^{new} (see Remark 4.10). At the same time, if A is a newform quotient and the level N is squarefree, then Theorems 4.11, 4.12, and 4.13 suggest that the Manin constant is 1 for such quotients.

In the case when the level is not square free, computations of [FpS$^+$01] involving Jacobians of genus 2 curves that are quotients of $J_0(N)^{\mathrm{new}}$ show that

$c_A = 1$ in 28 case of 2-dimensional newform 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 4.2. *If f is a newform on $\Gamma_0(N)$ or $\Gamma_1(N)$, then $c_{A_f} = 1$.*

Remark 4.3. The above conjecture does not hold if all we know is that $J_0(N) \to A$ factors through $J_0(N)^{\text{new}}$. Adam Joyce [Joy03] found an optimal quotient of $J_0(431)^{\text{new}}$ whose Manin constant is 2 (this example is motivated by [Kil02]); note that this optimal quotient is not attached to a single newform.

4.2 Integrality of the Manin constant

We continue to use the notation introduced so far in Section 4. In this section we prove Theorem 4.7, which asserts that the (generalized) Manin constant is an integer, which generalizes Thm. 2.4 of Edixhoven (see also [CES03, §6.1.2] for a similar argument). The proof is itself a generalization of that of [Edi91, Prop. 2]. The main idea 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 assume that $N > 4$, which is harmless, since $J_1(N)$ has dimension 0 for $N \leq 10$.

Using the standard immersion $X \hookrightarrow J$ sending ∞ to 0, we have maps

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

If $X = X_1(N)$, then we obtain 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 $X_1(N)$ whose affine points parametrize isomorphism classes of pairs (E, i), where E is an elliptic curve and $i : \mu_N \hookrightarrow E^{\text{reg}}$ is an immersion, 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]), the Néron mapping property implies that 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, gives 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 relate q-exp to the usual Fourier-expansion over $\mathbf{C}$. Since $\mathcal{X}_\mu(N)\otimes\mathbf{C} \cong X_1(N)_{\mathbf{C}}$, 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, gives 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.

We obtain a commutative diagram

$$\begin{tikzcd}
H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}}) \arrow[r, "\phi_A^*"] \arrow[d] & H^0(\mathcal{X}_\mu(N), \Omega^1_{\mathcal{X}_\mu(N)/\mathbf{Z}}) \arrow[r, "q\text{-exp}"] \arrow[d] & \mathbf{Z}[[q]] \arrow[d] \\
H^0(A_{\mathbf{C}}, \Omega^1_{A_{\mathbf{C}}/\mathbf{C}}) \arrow[r, "\phi_A^*\otimes\mathbf{C}"] & H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}}) \arrow[r, "F\text{-exp}"] & \mathbf{C}[[q]]
\end{tikzcd} \tag{6}$$

in which the first and last vertical maps are injections.

The relation of F-exp to the Fourier expansion of cusp forms is given by the following lemma. Let ψ be the isomorphism

$$\psi : S_2(\Gamma_1(N), \mathbf{C}) \overset{\cong}{\to} H^0(X_1(N)_{\mathbf{C}}, \Omega^1_{X_1(N)/\mathbf{C}})$$

given by $f(z) \mapsto 2\pi i f(z) dz$.

LEMMA 4.4. *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 4.5. *The group* $q\text{-exp}\left(\phi_A^*\left(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})\right)\right)$ *is a subgroup of* $F\text{-exp}(\psi(S_2(\Gamma_1(N), \mathbf{Z})[I]))$.

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 4.4, the Fourier expansion of $\psi^{-1}(y) \in S_2(\Gamma_1(N), \mathbf{C})$ is the same as $q\text{-exp}(x)$, 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 4.6. *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

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

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 4.5 and diagram (6), we have $\phi(H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}/\mathbf{Z}})) \subseteq \phi(\oplus_j \mathbf{Z}\omega_j)$. As ϕ is injective, $H^0(A_{\mathbf{Z}}, \Omega^1_{A_{\mathbf{Z}}}) \subseteq \bigoplus_j \mathbf{Z}\omega_j$. □

We obtain the following theorem as a corollary of Proposition 4.6:

Theorem 4.7. *The Manin constant* c_A *is an integer.*

We finish this section with a few remarks.

Remark 4.8. 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.

Remark 4.9. The reason we used the model $\mathcal{X}_\mu(N)$ was that we needed a smooth model over $\mathbf{Z}$ so that we can use the Néron mapping property to 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 use a model for $X_0(N)$ 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 $\tau : \operatorname{Spec}\mathbf{Z}[[q]] \to M_0(N)$ and composing with the map $\operatorname{Spec}\mathbf{Z} \to \operatorname{Spec}\mathbf{Z}[[q]]$ (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 $\mathbf{C}$.

Remark 4.10. The Manin constants c_A might not equal 1. For example, let $\Gamma = \Gamma_0(N)$, and suppose $A = J_0(N)$ is the quotient by the trivial ideal. Let us work in the setting of Remark 4.9, 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 4.6 we see that c_A is the order of the cokernel of the map

$$H^0(M_0(N)^0, \Omega^1_{M_0(N)^0/\mathbf{Z}}) \xrightarrow{q\text{-exp}} S_2(\mathbf{Z}), \tag{7}$$

where q-exp is the q-expansion map discussed in Remark 4.9. The map (7) 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 observed 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 (7) is surjective if and only if there are no old spaces in $S_2(\Gamma_0(N), \mathbf{C})$ (cf. [Edi03]). See also Remark 4.3 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 1 when there are old forms involved (see [Aga00, §4.2.1] for details).

4.3 Generalizations of theorems of Mazur and Raynaud

In this section, we prove the following two theorems:

Theorem 4.11. *Let A be a quotient of $J = J_0(N)$ by an ideal of the Hecke algebra such that the quotient map factors through $J_0(N)^{\mathrm{new}}$. If p is a prime such that $p \mid c_A$, then $p^2 \mid 4N$.*

Theorem 4.12. *Let f be a newform on $\Gamma_0(N)$, and let A_f be the associated newform quotient. If $4 \nmid N$, then $\mathrm{ord}_2(c_{A_f}) \leq \dim A_f$.*

Theorem 4.11 generalizes Mazur's Theorem 2.5, while Theorem 4.12 generalizes Raynaud's Theorem 2.6.

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 4.11, 4.12, and 4.13.

Proof of Theorem 4.11. 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 the proof of [Maz78, Prop. 3.1].

Let $R = \mathbf{Z}[\frac{1}{2m}]$, and let J_R denote 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

$$H^0(A_R, \Omega_{A_R}) \xrightarrow{\pi^*} H^0(J_R, \Omega_{J_R}) \cong H^0(\mathcal{X}, \Omega_{\mathcal{X}}) \xrightarrow{q\text{-exp}} R[[q]], \qquad (8)$$

where the map q-exp is as in [Maz78, §2(e)]. (Note that we defined a different q-expansion map in Section 4.2.)

The composite of the maps in (8) must be an inclusion because $H^0(A_R, \Omega_{A_R})$ 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 $H^0(A_R, \Omega_{A_R})$ 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 $S_2(\Gamma_0(N); R)[I] \otimes \mathbf{Q} = H^0(A_R, \Omega_{A_R}) \otimes \mathbf{Q}$.

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

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

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

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

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 $D[\ell] = 0$, it suffices to prove injectivity of

$$\Phi : H^0(A_R, \Omega_{A_R}) \otimes \mathbf{F}_\ell \longrightarrow \mathbf{F}_\ell[[q]].$$

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

$$0 \to H^0(A_{\mathbf{Z}_\ell}, \Omega_{A_{\mathbf{Z}_\ell}}) \to H^0(J_{\mathbf{Z}_\ell}, \Omega_{J_{\mathbf{Z}_\ell}}) \to H^0(B_{\mathbf{Z}_\ell}, \Omega_{B_{\mathbf{Z}_\ell}}) \to 0$$

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

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

is injective. We also remark that

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

because $\mathbf{Z}_\ell$ is torsion free, hence flat over R. This proves injectivity of

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

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. If $\omega \in \ker(\Phi)$, then the q-expansion principle implies that ω vanishes on the irreducible component containing the cusp ∞. The action of W_ℓ on $H^0(A_R, \Omega_{A_R}) \otimes \mathbf{F}_\ell$ is diagonalizable since its minimal polynomial divides $X^2 - 1$, and $X^2 - 1$ 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. □

Proof of Theorem 4.12. 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. 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 4.11.

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

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Tan}(B_{\mathbf{Z}_2}) \arrow[r] & \mathrm{Tan}(J_{\mathbf{Z}_2}) \arrow[rr] \arrow[dr, two heads] & & \mathrm{Tan}(A_{\mathbf{Z}_2}) \arrow[r] & (\mathbf{Z}/2\mathbf{Z})^r \arrow[r] & 0. \qquad (9) \\
& & & C \arrow[ur, hook] & & &
\end{tikzcd}$$

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 (9), 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

$$0 \to \mathrm{H}^0(A_{\mathbf{Z}_2}, \Omega_{A/\mathbf{Z}_2}) \to C^* \to (\mathbf{Z}/2\mathbf{Z})^r \to 0. \qquad (10)$$

Note that the $(\mathbf{Z}/2\mathbf{Z})^r$ on the right in (10) is really $\mathrm{Ext}^1_{\mathbf{Z}_2}((\mathbf{Z}/2\mathbf{Z})^r, \mathbf{Z}_2)$, which is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^r$. Also, (10) implies that $r \leq d = \dim(A)$.

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

Arguing as in the last two paragraphs of the proof of Theorem 4.11 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 4.11, 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 (9), hence is at most 2^d. □

4.4 The Manin constant and congruence primes

In this section, we prove the following theorem, whose proof builds on techniques of [AU96]:

Theorem 4.13. *Let $A = A_f$ be a quotient of $J = J_0(N)$ attached to a newform f. If $p \mid c_{A_f}$ is a prime, then $p^2 \mid N$ or $p \mid \tilde{r}_{A_f}$.*

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 the proof of Theorem 4.11. 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 4.17). However, this does not add anything new, in light of Theorem 4.11.

We will use notation consistent with [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 $J^\vee \cong J$. By Proposition 3.2, the composite

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

is an isogeny. As in Definition 3.3, we denote the exponent of the kernel of this isogeny by $\tilde{n}_A$. There is an isogeny $\phi' : A \to A^\vee$ such that the composite

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

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

$$A \xrightarrow{\phi'} A^\vee \xrightarrow{\phi_1} J \xrightarrow{\phi_2} A \tag{13}$$

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

Pulling back differentials along ϕ_2 then ϕ_1 in (11), we obtain maps:

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

Let m denote the largest square that divides the level N and let $S = \operatorname{Spec} \mathbf{Z}[1/m]$. Let $M_0(N)$ be as in Remark 4.9. 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 4.9). Note that we are abusing notation slightly since we had defined a different q-expansion map in Section 4.2.

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

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

(this really follows from the discussion in Section 4.2). This map is not an isomorphism in general, but it induces an isomorphism

$$q\text{-exp} : H^0(M_0(N)_{\mathbf{F}_p}, \Omega) \xrightarrow{\cong} S_2(\mathbf{F}_p) \tag{14}$$

for each prime p that does not divide N (see [AU96, §2.1], and the arguments in the proof of Theorem 4.11).

We have

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

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

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

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 (14), 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

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

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

$$0 \to \frac{H^0(A^\vee_S, \Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to \frac{\phi_1^*(S_2(\mathbf{Z}[1/m]))}{\phi_1^*\phi_2^* H^0(A_S, \Omega^1_{A/S})} \to C \to 0. \tag{15}$$

Now ϕ_1^* is injective when restricted to $\phi_2^* H^0(A_{\mathbf{C}}, \Omega^1_{A/\mathbf{C}})$, because the pullback of the composite of the maps in (13) is injective, since it is 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

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

If n and m are positive integers, let n_m denote the largest divisor of n that is coprime to m.

By the discussion in Section 4.2,

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

So

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

Hence

$$\#\left(\frac{\phi_1^*(S_2(\mathbf{Z}[1/m]))}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right) = (c_A)_m\cdot\ \#\left(\frac{\phi_1^*(S_2(\mathbf{Z}[1/m]))}{\phi_1^*(S_2(\mathbf{Z})[I]\otimes\mathbf{Z}[1/m])}\right). \tag{16}$$

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

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

Thus

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

Putting this in (16) and then using (15), we get

$$(c_A)_m\cdot(r_A)_m = \#\left(\frac{H^0(A_S^\vee,\Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)\cdot\#C. \tag{17}$$

Since the composite of the maps in (12) 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 obtain the following lemma:

Lemma 4.14. *If* $p\ \Big|\ \#\left(\frac{H^0(A_S^\vee,\Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)$ *is a prime, 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, which further controls the primes that can divide $\#C$:

Proposition 4.15. *If* $A=A_f$ *is a newform quotient of* $J_0(N)$ *and* $p\mid\#C$ *is a prime, then* $p^2\mid N$ *or* $p\mid\tilde{r}_A$.

Before proving Proposition 4.15 we use it to prove Theorem 4.13.

Proof of Theorem 4.13. Suppose $p^2\nmid N$ and $p\mid c_A$. Then $p\mid(c_A)_m$, and so by equation (17), $p\mid\#\left(\frac{H^0(A_S^\vee,\Omega^1_{A^\vee/S})}{\phi_1^*\phi_2^*H^0(A_S,\Omega^1_{A/S})}\right)$ or $p\mid\#C$. In the former case, by Lemma 4.14, $p\mid\tilde{n}_A$, and hence by Proposition 3.11, $p\mid\tilde{r}_A$ and in the latter case, by Proposition 4.15, $p\mid\tilde{r}_A$. □

Remark 4.16. The obstruction to proving a generalization of Theorem 2.7 to dimension greater than 1 lies in equation (17). When A is an elliptic curve, Abbes-Ullmo [AU96] prove that the quotient of differentials on the right hand side of (17) 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 3.6 suggests that divisibility might sometimes fail when multiplicity one fails.

Proof of Proposition 4.15. We have the exact sequence

$$0 \to \phi_1^*(H^0(M_0(N)_S, \Omega)) \to \phi_1^*(S_2(\mathbf{Z}[1/m])) \to C \to 0. \tag{18}$$

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 (18) and using the snake lemma, we get:

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

(note the similarity to the situation in the proof of Theorem 4.11). Then to show that $p \nmid \#C$, i.e., that $C[p]$ is trivial, all we have to show is that the map

$$\phi_1^*(H^0(M_0(N)_S, \Omega)) \otimes \mathbf{F}_p \xrightarrow{q\text{-exp}} \phi_1^*\left(S_2\left(\mathbf{Z}[1/m]\right)\right) \otimes \mathbf{F}_p \tag{19}$$

is injective.

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

$$A^\vee \overset{\phi_1}{\to} J \overset{\phi_2}{\to} A \overset{\phi'}{\to} A^\vee \tag{20}$$

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

$$H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}}) \xrightarrow{\phi''^*} H^0(J_{\mathbf{C}}, \Omega^1_{J/\mathbf{C}}) \xrightarrow{\phi_1^*} H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}}), \tag{21}$$

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

By the Néron mapping property, the maps (20) 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

$$S_2(\mathbf{Z}[1/m]) \otimes \mathbf{F}_p = S_2(\mathbf{Z}[1/m])[I] \otimes \mathbf{F}_p \oplus (W(I) \cap S_2(\mathbf{Z}[1/m])[I]) \otimes \mathbf{F}_p.$$

Thus if $f \in S_2(\mathbf{Z}[1/m]) \otimes \mathbf{F}_p$, then there exist unique $f_1 \in S_2(\mathbf{Z}[1/m])[I] \otimes \mathbf{F}_p$ and $f_2 \in (W(I) \cup S_2(\mathbf{Z}[1/m])[I]) \otimes \mathbf{F}_p$ such that $f = f_1 + f_2$. It then follows that $\phi_1^* f = \phi_1^* f_1$, and so $\phi''^*(\phi_1^* f) = \tilde{n}_{A} f_1 \in S_2(\mathbf{Z}[1/m]) \otimes \mathbf{F}_p$. Thus the image of $\phi_1^*(S_2(\mathbf{Z}[1/m])) \otimes \mathbf{F}_p$ under ϕ''^* lands in $S_2(\mathbf{Z}[1/m]) \otimes \mathbf{F}_p$.

Hence, applying the maps in (21) to the groups in (19), which are subgroups of $H^0(A^\vee_{\mathbf{C}}, \Omega^1_{A^\vee/\mathbf{C}})$, we get the following commutative diagram:

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

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 (19), 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 $S_2(\mathbf{Z}[1/m]) \otimes \mathbf{F}_p$ 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 the proof of Theorem 4.11.

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 3.11 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 (19), then $x = 0$. This shows that the map (19) is injective, which is what was left to prove. □

Remark 4.17. 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 the proof of Theorem 4.11; the paragraph at the beginning of Section 3.2 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 $J_0(N)^{\text{new}}$, 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.missouri.edu/ agashe/math.html`.

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

[AS05] A. Agashe and W. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. 74 (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur.

[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.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939 (electronic).

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

[CK04] Alina Carmen Cojocaru and Ernst Kani, *The modular degree and the congruence number of a weight 2 cusp form*, Acta Arith. 114 (2004), no. 2, 159–167.

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

[CES03] B. Conrad, S. Edixhoven, and W. A. Stein, $J_1(p)$ *Has Connected Fibers*, Documenta Mathematica 8 (2003), 331–408.

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.maths.nott.ac.uk/personal/jec/book/`.

[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$^+$01] 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*, Math. Comp. 70 (2001), no. 236, 1675–1697 (electronic).

[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.

[SW04] W. Stein and M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. (2004), no. 27, 1395–1405.

[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.