Pure and Applied Mathematics Quarterly
Volume 2, Number 2
(*Special Issue: In honor of
John H. Coates, Part 2 of 2*)
617—636, 2006

The Manin Constant

Amod Agashe, Kenneth Ribet and William A. Stein

Abstract: The Manin constant of an elliptic curve is an invariant that arises in connection with the conjecture of Birch and Swinnerton-Dyer. One conjectures that this constant is 1; it is known to be an integer. After surveying what is known about the Manin constant, we establish a new sufficient condition that ensures that the Manin constant is an *odd* integer. Next, we generalize the notion of the Manin constant to certain abelian variety quotients of the Jacobians of modular curves; these quotients are attached to ideals of Hecke algebras. We also generalize many of the results for elliptic curves to quotients of the new part of $J_0(N)$, and conjecture that the generalized Manin constant is 1 for newform quotients. Finally an appendix by John Cremona discusses computation of the Manin constant for all elliptic curves of conductor up to 130000.

1. Introduction

Let E be an elliptic curve over $\mathbf{Q}$, and and let N be the conductor of E. By [BCDT01], we may view E as a quotient of the modular Jacobian $J_0(N)$. 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 $J_0(N)$.

Let ω be the unique (up to sign) rational 1-form on a minimal Weierstrass model of E over $\mathbf{Z}$ that restricts to a nowhere-vanishing 1-form on the smooth locus. The pullback of ω is a rational multiple of the differential associated to the normalized new cuspidal eigenform $f_E \in S_2(\Gamma_0(N))$ associated to E. The Manin constant c_E of is E is the absolute value of this rational multiple. The Manin constant plays a role in the conjecture of Birch and Swinnerton-Dyer (see, e.g., [GZ86, p. 310]) and in work on modular parametrizations (see [Ste89, SW04, Vat05]). It is known that the Manin constant is an integer; this fact is important to Cremona's computations of elliptic curves (see [Cre97, pg. 45]), and algorithms

Received January 25, 2006.
Stein was supported by the National Science Foundation by Grant No. 0400386.

for computing special values of elliptic curve L-functions. Manin conjectured that $c_E = 1$. In Section 2, we summarize known results about c_E, and give the new result that $2 \nmid c_E$ if 2 is not a congruence prime and $4 \nmid N$.

In Section 3, we generalize the definition of the Manin constant and many of the results mentioned so far to optimal quotients of $J_0(N)$ and $J_1(N)$ of any dimension associated to ideals of the Hecke algebra. The generalized Manin constant comes up naturally in studying the conjecture of Birch and Swinnerton-Dyer for such quotients (see [AS05, §4]), which is our motivation for studying the generalization. We state what we can prove about the generalized Manin constant, and make a conjecture that the constant is also 1 for quotients associated to newforms. The proofs of the theorems stated in Section 3 are in Section 4. Section 5 is an appendix written by J. Cremona about computational verification that the Manin constant is 1 for many elliptic curves.

Acknowledgments. The authors are grateful to A. Abbes, K. Buzzard, R. Coleman, B. Conrad, B. Edixhoven, A. Joyce, L. Merel, and R. Taylor for discussions and advice regarding this paper. The authors wish to thank the referee for helpful comments and suggestions.

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 $n \geq 1$. Suppose f is 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 $a_n(f)$. 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 x to $(\infty) - (x)$ with the quotient map $J_0(N) \to E$, we obtain a surjective morphism of curves $\phi_E : X_0(N) \to E$. The *modular degree* m_E of E is the degree of ϕ_E.

Let $E_{\mathbf{Z}}$ denote the Néron model of E over $\mathbf{Z}$. A general reference for Néron models is [BLR90]; for the special case of elliptic curves, see, e.g., [Sil92, App. C, §15], and [Sil94]. Let ω be a generator for the rank 1 $\mathbf{Z}$-module of invariant differential 1-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 $X_0(N) \to E$, the differential $\phi_E^*\omega$ is a $\mathbf{T}$-eigenvector with the same eigenvalues as $f(z)$, so by [AL70] we have $\phi_E^*\omega = c \cdot 2\pi i f(z)dz$ for some $c \in \mathbf{Q}^*$ (see also

[Man72, §5]). The *Manin constant* c_E of E is the absolute value of the rational number c defined above.

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

Conjecture 2.1 (Manin)**.** *We have* $c_E = 1$.

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

Theorem 2.2 (Edixhoven [Edi91, Prop. 2])**.** *The constant* 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 theorem to quotients of arbitrary dimension in Theorem 3.4.

Theorem 2.3 (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 theorem in Corollary 3.7.

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

Theorem 2.4 (Raynaud [AU96, Prop. 3.1])**.** *If* $4 \mid c_E$, *then* $4 \mid N$.

Theorem 2.5 (Abbes-Ullmo [AU96, Thm. A])**.** *If* $p \mid c_E$, *then* $p \mid N$.

We generalize Theorem 2.4 in Theorem 3.10. However, it is not clear if Theorem 2.5 generalizes to dimension greater than 1. It would be fantastic if the theorem could be generalized. It would imply that the Manin constant is 1 for newform quotients A_f of $J_0(N)$, with N odd and square free, which be useful for computations regarding the conjecture of Birch and Swinnerton-Dyer.

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 the construction of certain stable integral models for $X_0(p^2)$.

See Section 5 for more details about the following computation:

Theorem 2.6 (Cremona)**.** *If E is an optimal elliptic curve over* $\mathbf{Q}$ *with conductor at most* 130000, *then* $c_E = 1$.

To the above list of theorems we add the following:

Theorem 2.7. *If* $p \mid c_E$ *then* $p^2 \mid N$ *or* $p \mid m_E$.

This theorem is a special case of Theorem 3.11 below. In view of Theorem 2.3, 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 optimal elliptic curve quotients of conductor ≤ 120000, only 56 of them satisfy the hypothesis.

3. Quotients of arbitrary dimension

For $N \geq 4$, let Γ a subgroup of $\Gamma_1(N)$ that contains $\Gamma_0(N)$, 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.

For a newform $f = \sum a_n(f)q^n \in S_2(\Gamma)$, consider the ring homomorphism $\mathbf{T} \to \mathbf{Z}[\ldots, a_n(f), \ldots]$ that sends T_n to $a_n(f)$. The kernel $I_f \subset \mathbf{T}$ of this homomorphism is a saturated prime ideal of $\mathbf{T}$. The *newform quotient* A_f associated to f is the quotient J/I_fJ. Shimura introduced A_f in [Shi73] where he proved that A_f is an abelian variety over $\mathbf{Q}$ of dimension equal to the degree of the field $\mathbf{Q}(\ldots, a_n(f), \ldots)$. He also observed that there is a natural map $\mathbf{T} \to \mathrm{End}(A_f)$ with kernel I_f.

For the rest of this section, fix a quotient A associated to a saturated ideal I of $\mathbf{T}$; note that A may or may not be attached to a newform.

3.1. Generalization to quotients of arbitrary dimension.

If R is a subring of $\mathbf{C}$, let $S_2(R) = S_2(\Gamma; R)$ denote the $\mathbf{T}$-submodule of $S_2(\Gamma; \mathbf{C})$ of modular forms whose Fourier expansions have all coefficients in R.

Lemma 3.1. *The Hecke operators leave $S_2(R)$ stable.*

Proof. If $\Gamma = \Gamma_0(N)$, then by the explicit description of the Hecke operators on Fourier expansions (e.g., see [DI95, Prop. 3.4.3]), it is clear that the Hecke operators leave $S_2(R)$ stable. For a general Γ, by [DI95, (12.4.1)], one just has to check in addition that the diamond operators also leave $S_2(R)$ stable, which in turn follows from [DI95, Prop. 12.3.11]. □

Lemma 3.2. *We have $S_2(R) \cong S_2(\mathbf{Z}) \otimes R$.*

Proof. This is [DI95, Thm. 12.3.2] when our spaces $S_2(R)$ and $S_2(\mathbf{Z})$ are replaced by their algebraic analogues (see [DI95, pg. 111]). Our spaces and their algebraic analogues are identified by the natural q-expansion maps according to [DI95, Thm. 12.3.7]. □

If B is an abelian variety over $\mathbf{Q}$ and S is a Dedekind domain with field of fractions $\mathbf{Q}$, then we denote by B_S the Néron model of B over S; also, for ease of notation, we will abbreviate $H^0(B_S, \Omega^1_{B_S/S})$ by $H^0(B_S, \Omega^1_{B/S})$.

The inclusion $X \hookrightarrow J$ that sends the cusp ∞ to 0 induces an isomorphism

$$H^0(X, \Omega^1_{X/\mathbf{Q}}) \cong H^0(J, \Omega^1_{J/\mathbf{Q}}).$$

Let ϕ_2 be the optimal quotient map $J \to A$. Then ϕ_2^* induces an inclusion $\psi : H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}) \hookrightarrow H^0(J, \Omega^1_{J/\mathbf{Q}})[I] \cong S_2(\mathbf{Q})[I]$, and we have the following commutative diagram:

$$\begin{array}{ccccc} H^0(A, \Omega^1_{A/\mathbf{Q}}) & \overset{\cong}{\hookrightarrow} & H^0(J, \Omega^1_{J/\mathbf{Q}})[I] & \overset{\cong}{\longrightarrow} & S_2(\mathbf{Q})[I] \\ \uparrow & & & \overset{\psi}{\nearrow} & \uparrow \\ H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}) & & & & S_2(\mathbf{Z})[I] \end{array}$$

Definition 3.3. The *Manin constant* of A is the (lattice) index

$$c_A = [S_2(\mathbf{Z})[I] : \psi(H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}))].$$

Theorem 3.4 below asserts that $c_A \in \mathbf{Z}$, so we may also consider the Manin module of A, which is the quotient $M = S_2(\mathbf{Z})[I]/\psi(H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}))$, and the Manin ideal of A, which is the annihilator of M in $\mathbf{T}$.

If A is an elliptic curve, then c_A is the usual Manin constant. The constant c as defined above was also considered by Gross [Gro82, 2.5, p.222] and Lang [Lan91, III.5, p.95]. The constant c_A was defined for the winding quotient in [Aga99], where it was called the generalized Manin constant. A Manin constant is defined in the context of $\mathbf{Q}$-curves in [GL01].

3.2. **Motivation: connection with the conjecture of Birch and Swinnerton-Dyer.** On a Néron model, the global differentials are the same as the invariant differentials, so $H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})$ is a free $\mathbf{Z}$-module of rank $d = \dim(A)$. The *real measure* Ω_A of A is the measure of $A(\mathbf{R})$ with respect to the volume given by a generator of $\bigwedge^d H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}) \simeq \mathrm{H}^0(A_{\mathbf{Z}}, \Omega^d_{A_{\mathbf{Z}}/\mathbf{Z}})$. This quantity is of interest because it appears in the conjecture of Birch and Swinnerton-Dyer, which expresses the ratio $L^{(r)}(A,1)/\Omega_A$, in terms of arithmetic invariants of A, where $r = \mathrm{ord}_{s=1} L(A,s)$ (see, e.g., [Lan91, Chap. III, §5] and [AS05, §2.3]).

If we take a $\mathbf{Z}$-basis of $S_2(\mathbf{Z})[I]$ and take the inverse image via the top chain of arrows in the commutative diagram above, we get a $\mathbf{Q}$-basis of $H^0(A, \Omega^1_{A/\mathbf{Q}})$; let Ω'_A denote the volume of $A(\mathbf{R})$ with respect to the wedge product of the elements in the latter basis (this is independent of the choice of the former basis). In doing calculations or proving formulas regarding the ratio in the Birch and Swinnerton-Dyer conjecture mentioned above, it is easier to work with the volume Ω'_A instead of working with Ω_A. 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 conjecture of Birch and Swinnerton-Dyer, since $\Omega_A = c_A \cdot \Omega'_A$. For example, see [AS05, §4.2] when $r = 0$ and [GZ86, p. 310–311] when $r = 1$; in each case, one gets a formula for computing the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group, and the formula contains the Manin constant (see, e.g., [Mc91]).

The method of Section 5 for verifying that $c_A = 1$ for specific elliptic curves is of little use when applied to general abelian varieties, since there is no simple analogue of the minimal Weierstrass model (but see [GL01] for **Q**-curves). This emphasizes the need for general theorems regarding the Manin constant of quotients of dimension bigger than one.

3.3. **Results and a conjecture.** We start by giving several results regarding the Manin constant for quotients of arbitrary dimension. The proofs of most of the theorems are given in Section 4.

Let Γ be a subgroup of $\Gamma_0(N)$ that contains $\Gamma_1(N)$. We have the following generalization of Edixhoven's Theorem 2.2.

Theorem 3.4. *The Manin constant c_A is an integer. (In the notation of Section 3.1 we even have that $\psi(H^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})) \subseteq S_2(\mathbf{Z})[I]$.)*

Proof. Let $J = \mathrm{Jac}(X_\Gamma)$ and $J' = J_1(N)$. Suppose A is an optimal quotient of J. We have natural maps $\mathrm{H}^0(J'_{\mathbf{Z}}, \Omega^1_{J'/\mathbf{Z}}) \hookrightarrow \mathrm{H}^0(J', \Omega^1_{J'/\mathbf{Q}}) \xrightarrow{\cong} S_2(\Gamma_1(N); \mathbf{Q})$; from the proof of Lemma 6.1.6 of [CES03], the image of the composite is contained in $S_2(\Gamma_1(N); \mathbf{Z})$. The maps $J' \to J \to A$ induce a chain of inclusions

$$\mathrm{H}^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}}) \hookrightarrow \mathrm{H}^0(J_{\mathbf{Z}}, \Omega^1_{J/\mathbf{Z}}) \hookrightarrow \mathrm{H}^0(J'_{\mathbf{Z}}, \Omega^1_{J'/\mathbf{Z}}) \hookrightarrow S_2(\Gamma_1(N); \mathbf{Z}) \hookrightarrow \mathbf{Z}[[q]].$$

Combining this chain of inclusions with commutativity of the diagram

$$\begin{array}{ccccc} & & S_2(\Gamma_1(N)) & & \\ & {\scriptstyle f(q)\mapsto f(q)} \nearrow & & \searrow {\scriptstyle F\text{-exp}} & \\ S_2(\Gamma) & & \xrightarrow{\quad F\text{-exp} \quad} & & \mathbf{C}[[q]], \end{array}$$

where F-exp is the Fourier expansion map, we see that the image of $\mathrm{H}^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})$ lies in $S_2(\mathbf{Z})[I]$, as claimed. $\square$

For the rest of the paper, we take $\Gamma = \Gamma_0(N)$. For each prime $\ell \mid N$ with $\mathrm{ord}_\ell(N) = 1$, let W_ℓ be the ℓth Atkin-Lehner operator. Let $J = J_0(N)$ and $A = A_I = J/IJ$ be an optimal quotient of J attached to a saturated ideal I. If ℓ is a prime, then as usual, $\mathbf{Z}_{(\ell)}$ will denote the localization of $\mathbf{Z}$ at ℓ.

Theorem 3.5. *Suppose that ℓ is an odd prime such that $\ell^2 \nmid N$, and that if $\ell \mid N$, then $A^\vee \subset J$ is stable under W_ℓ. Then $\ell \mid c_A$ if and only if $\ell \mid N$ and $S_2(\mathbf{Z}_{(\ell)})[I]$ is not stable under the action of W_ℓ.*

We will prove this theorem in Section 4.2.

Remark 3.6. The condition that $S_2(\mathbf{Z}_{(\ell)})[I]$ is stable under W_ℓ can be verified using standard algorithms. Thus in light of Theorem 3.5, if A is stable under all Atkin-Lehner operators and N is square free, then one can compute the set of odd primes that divide c_A. It would be interesting to refine the arguments of this paper to find an algorithm to compute c_A exactly.

Let J_{old} denote the abelian subvariety of J generated by the images of the degeneracy maps from levels that properly divide N (see, e.g., [Maz78, §2(b)]) and let J^{new} denote the quotient of J by J_{old}. A *new quotient* is a quotient $J \to A$ that factors through the map $J \to J^{\text{new}}$. The following corollary generalizes Mazur's Theorem 2.3:

Corollary 3.7. *If $A = A_f$ is an optimal newform quotient of $J_0(N)$ and $\ell \mid c_A$ is a prime, then $\ell = 2$ or $\ell^2 \mid N$.*

Proof. Since f is a newform, W_ℓ acts as either 1 or -1 on A hence on $S_2(\mathbf{Z}_{(\ell)})[I]$. Thus $S_2(\mathbf{Z}_{(\ell)})[I]$ is W_ℓ-stable. □

Corollary 3.8. *If $A = J_0(N)_{\text{new}}$ is the new subvariety of $J_0(N)$ and $\ell \mid c_A$ is a prime, then $\ell = 2$ or $\ell^2 \mid N$. (In particular, if N is prime then the Manin constant of $J_0(N)$ is a power of 2, since $A = J_0(N)[I]$ for $I = 0$.)*

Proof. We have $W_\ell = -T_\ell$ on A (e.g., see the end of [DI95, §6.3]). Also the new subspace $S_2(\mathbf{Z})_{\text{new}}$ of $S_2(\Gamma_0(N))$ is T_ℓ-stable. □

Remark 3.9. If $A = J_0(33)$, then

$$W_3 = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & -\frac{4}{3} \\ \frac{1}{3} & -\frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

with respect to the basis

$$\begin{aligned} f_1 &= q - q^5 - 2q^6 + 2q^7 + \cdots, \\ f_2 &= q^2 - q^4 - q^5 - q^6 + 2q^7 + \cdots, \\ f_3 &= q^3 - 2q^6 + \cdots \end{aligned}$$

for $S_2(\mathbf{Z})$. Thus W_3 does not preserve $S_2(\mathbf{Z}_{(3)})$. In fact, the Manin constant of $J_0(33)$ is not 1 in this case (see Section 3.4).

The hypothesis of Theorem 3.5 sometimes holds for non-new A. For example, take $J = J_0(33)$ and $\ell = 3$. Then W_3 acts as an endomorphism of J, and a computation shows that the characteristic polynomial of W_3 on $S_2(33)_{\rm new}$ is $x-1$ and on $S_2(33)_{\rm old}$ is $(x-1)(x+1)$, where $S_2(33)_{\rm old}$ is the old subspace of $S_2(33)$. Consider the optimal elliptic curve quotient $A = J/(W_3+1)J$, which is isogenous to $J_0(11)$. Then A is an optimal old quotient of J, and W_3 acts as -1 on A, so W_3 preserves the corresponding spaces of modular forms. Thus Theorem 3.5 implies that $3 \nmid c_A$.

The following theorem generalizes Raynaud's Theorem 2.4 (see also [GL01] for generalizations to $\mathbf{Q}$-curves).

Theorem 3.10. *If $f \in S_2(\Gamma_0(N))$ is a newform and ℓ is a prime such that $\ell^2 \nmid N$, then $\mathrm{ord}_\ell(c_{A_f}) \leq \dim A_f$.*

Note that in light of Theorem 3.5, this theorem gives new information only at $\ell = 2$, when $2 \parallel N$. We prove the theorem in Section 4.4

Let π denote the natural quotient map $J \to A$. When we compose π with its dual $A^\vee \to J^\vee$ (identifying $J^\vee$ with J using the inverse of the principal polarization of J), we get an isogeny $\phi : A^\vee \to A$. The *modular exponent* m_A of A is the exponent of the group $\ker(\phi)$. When A is an elliptic curve, the modular exponent is just the modular degree of A (see, e.g., [AU96, p. 278]).

Theorem 3.11. *If $f \in S_2(\Gamma_0(N))$ is a newform and $\ell \mid c_{A_f}$ is a prime, then $\ell^2 \mid N$ or $\ell \mid m_A$.*

Again, in view of Corollary 3.7, this theorem gives new information only at $\ell = 2$, when $\mathrm{ord}_2(N) \leq 1$. We prove the theorem in Section 4.3.

The theorems above suggest that the Manin constant is 1 for quotients associated to newforms of square-free level. In the case when the level is not square free, computations of [FpS$^+$01] involving Jacobians of genus 2 curves that are quotients of $J_0(N)^{\rm new}$ show that $c_A = 1$ for 28 two-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 suggest the following conjecture, which generalizes Conjecture 2.1:

Conjecture 3.12. *If f is a newform on $\Gamma_0(N)$ then $c_{A_f} = 1$.*

It is plausible that $c_{A_f} = 1$ for any newform on any congruence subgroup between $\Gamma_0(N)$ and $\Gamma_1(N)$. However, we do not have enough data to justify making a conjecture in this context.

3.4. **Examples of nontrivial Manin constants.** We present two sets of examples in which the Manin constant is not 1.

Using results of [Kil02], Adam Joyce [Joy05] proves that there is a new optimal quotient of $J_0(431)$ with Manin constant 2. Joyce's methods also produce examples with Manin constant 2 at levels 503 and 2089. For the convenience of the reader, we breifly discuss his example at level 431. There are exactly two elliptic curves E_1 and E_2 of prime conductor 431, and $E_1 \cap E_2 = 0$ as subvarieties of $J_0(431)$, so $A = E_1 \times E_2$ is an optimal quotient of $J_0(431)$ attached to a saturated ideal I. If f_i is the newform corresponding to E_i, then one finds that $f_1 \equiv f_2 \pmod 2$, and so $g = (f_1 - f_2)/2 \in S_2(\mathbf{Z})[I]$. However g is not in the image of $\mathrm{H}^0(A_{\mathbf{Z}}, \Omega^1_{A/\mathbf{Z}})$. Thus the Manin constant of A is divisible by 2.

As another class of examples, one finds by computation for each prime $\ell \leq 100$ that W_ℓ does not leave $S_2(\Gamma_0(11\ell); \mathbf{Z}_{(\ell)})$ stable. Theorem 3.5 (with $I = 0$) then implies that the Manin constant of $J_0(11\ell)$ is divisible by ℓ for these values of ℓ.

4. Proofs of some of the Theorems

In Sections 4.2, 4.3, and 4.4, we prove Theorems 3.5, 3.11, and 3.10 respectively. In Section 4.1, we state two lemmas that will be used in these proofs. The proofs of the theorems may be read independently of each other, after reading Section 4.1.

4.1. **Two lemmas.** The following lemma is a standard fact; we state it as a lemma merely because it is used several times.

Lemma 4.1. *Suppose $i : A \hookrightarrow B$ is an injective homomorphism of torsion-free abelian groups. If p is a prime, then $B/i(A)$ has no nonzero p-torsion if and only if the induced map $A \otimes \mathbf{F}_p \to B \otimes \mathbf{F}_p$ is injective.*

Proof. Let Q denote the quotient $B/i(A)$. Tensor the exact sequence $0 \to A \to B \to Q \to 0$ with $\mathbf{F}_p$. The associated long exact sequences reveal that $\ker(A \otimes \mathbf{F}_p \to B \otimes \mathbf{F}_p) \cong Q_{\mathrm{tor}}[p]$. □

Suppose ℓ is a prime such that $\ell^2 \nmid N$. In what follows, we will be stating some standard facts taken from [Maz78, §2(e)] (which in turn relies on [DR73]). Let $\mathcal{X}_{\mathbf{Z}_{(\ell)}}$ be the minimal regular resolution of the coarse moduli scheme associated to $\Gamma_0(N)$ (as in [DR73, § VI.6.9]) over $\mathbf{Z}_{(\ell)}$, and let $\Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}}$ denote the relative dualizing sheaf of $\mathcal{X}_{\mathbf{Z}_{(\ell)}}$ over $\mathbf{Z}_{(\ell)}$. The Tate curve over $\mathbf{Z}_{(\ell)}[[q]]$ gives rise to a morphism from Spec $\mathbf{Z}_{(\ell)}[[q]]$ to the smooth locus of $\mathcal{X}_{\mathbf{Z}_{(\ell)}} \to \operatorname{Spec} \mathbf{Z}_{(\ell)}$. Since the module of completed Kahler differentials for $\mathbf{Z}_{(\ell)}[[q]]$ over $\mathbf{Z}_{(\ell)}$ is free of rank 1 on the basis dq, we obtain a map q-exp $: H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}}) \to \mathbf{Z}_{(\ell)}[[q]]$.

The natural morphism $\mathrm{Pic}^0_{\mathcal{X}/\mathbf{Z}_{(\ell)}} \to J_{\mathbf{Z}_{(\ell)}}$ identifies $\mathrm{Pic}^0_{\mathcal{X}/\mathbf{Z}_{(\ell)}}$ with the identity component of $J_{\mathbf{Z}_{(\ell)}}$ (see, e.g., [BLR90, §9.4–9.5]). Passing to tangent spaces along the identity section over $\mathbf{Z}_{(\ell)}$, we obtain an isomorphism $H^1(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \mathcal{O}_{\mathcal{X}_{\mathbf{Z}_{(\ell)}}}) \cong \mathrm{Tan}(J_{\mathbf{Z}_{(\ell)}})$. Using Grothendieck duality, one gets an isomorphism $\mathrm{Cot}(J_{\mathbf{Z}_{(\ell)}}) \xrightarrow{\cong} H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}})$, where $\mathrm{Cot}(J_{\mathbf{Z}_{(\ell)}})$ is the cotangent space at the identity section. On the Néron model $J_{\mathbf{Z}_{(\ell)}}$, the group of global differentials is the same as the group of invariant differentials, which in turn is naturally isomorphic to $\mathrm{Cot}(J_{\mathbf{Z}_{(\ell)}})$. Thus we obtain an isomorphism $H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \cong H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}})$.

Let G be a $\mathbf{T}$-module equipped with an injection $G \hookrightarrow H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}})$ of $\mathbf{T}$-modules such that G is annihilated by I. If $\ell \mid N$, assume moreover that G is a $\mathbf{T}[W_\ell]$-module and that the inclusion in the previous sentence is a homomorphism of $\mathbf{T}[W_\ell]$-modules. As a typical example, $G = H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$, with the injection $\pi^* : H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \hookrightarrow H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}})$. Let Φ be the composition of the inclusions

$$G \hookrightarrow H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \cong H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}}) \xrightarrow{q\text{-exp}} \mathbf{Z}_{(\ell)}[[q]], \tag{1}$$

and let ψ' be the composition of

$$G \hookrightarrow H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}})[I] \hookrightarrow S_2(\mathbf{Z}_{(\ell)})[I],$$

where the last inclusion follows from a "local" version of Theorem 3.4. The maps Φ and ψ' are related by the commutative diagram

$$\begin{array}{ccccc} & & S_2(\mathbf{Z}_{(\ell)})[I] & & \\ & \overset{\psi'}{\nearrow} & & \overset{F\text{-exp}}{\searrow} & \\ G & & \xrightarrow{\quad\Phi\quad} & & \mathbf{Z}_{(\ell)}[[q]], \end{array} \tag{2}$$

where F-exp is the Fourier expansion map (at infinity), as before.

We say that a subgroup B of an abelian group C is *saturated* (in C) if the quotient C/B is torsion free.

Lemma 4.2. *Recall that ℓ is a prime such that $\ell^2 \nmid N$. If ℓ divides N, suppose that $S_2(\mathbf{Z}_{(\ell)})[I]$ is stable under the action of W_ℓ; if $\ell = 2$ assume moreover that W_ℓ acts as a scalar on A. Consider the map*

$$G \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell,$$

which is obtained by tensoring the inclusion $G \hookrightarrow H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}})$ with $\mathbf{F}_\ell$. If this map is injective, then the image of G under the map Φ of (2) is saturated in $\mathbf{Z}_{(\ell)}[[q]]$.

Proof. By Lemma 4.1, it suffices to prove that the map

$$\Phi_\ell : G \otimes \mathbf{F}_\ell \to \mathbf{Z}_{(\ell)}[[q]] \otimes \mathbf{F}_\ell = \mathbf{F}_\ell[[q]]$$

obtained by tensoring (1) with $\mathbf{F}_\ell$ is injective. Let $\mathcal{X}_{\mathbf{F}_\ell}$ denote the special fiber of $\mathcal{X}_{\mathbf{Z}_{(\ell)}}$ and let $\Omega_{\mathcal{X}/\mathbf{F}_\ell}$ denote the relative dualizing sheaf of $\mathcal{X}_{\mathbf{F}_\ell}$ over $\mathbf{F}_\ell$.

First suppose that ℓ does not divide N. Then $\mathcal{X}_{\mathbf{Z}_{(\ell)}}$ is smooth and proper over $\mathbf{Z}_{(\ell)}$. Thus the formation of $\mathrm{H}^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}_{\mathbf{Z}_{(\ell)}}})$ is compatible with any base change on $\mathbf{Z}_{(\ell)}$ (such as reduction modulo ℓ). The injectivity of Φ_ℓ now follows since by hypothesis the induced map $G \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$ is injective, and

$$H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{X}_{\mathbf{F}_\ell}, \Omega_{\mathcal{X}/\mathbf{F}_\ell}) \to \mathbf{F}_\ell[[q]]$$

is injective by the q-expansion principle (which is easy in this setting, since $\mathcal{X}_{\mathbf{F}_\ell}$ is a smooth and geometrically connected curve).

Next suppose that ℓ divides N. First we verify that $\ker(\Phi_\ell)$ is stable under W_ℓ. Suppose $\omega \in \ker(\Phi_\ell)$. Choose $\omega' \in G$ such that the image of ω' in $G \otimes \mathbf{F}_\ell$ is ω, and let $f = \psi'(\omega')$. Because $\Phi_\ell(\omega) = 0$ in $\mathbf{F}_\ell[[q]]$, there exists $h \in \mathbf{Z}_{(\ell)}[[q]]$ such that $\ell h = F\text{-}\exp(f)$. Let $f' = f/\ell \in S_2(\mathbf{Q})$; then f' is actually in $S_2(\mathbf{Z}_{(\ell)})$ (since $F\text{-}\exp(f/\ell) = h \in \mathbf{Z}_{(\ell)}[[q]]$). Now $\ell f' = f$ is annihilated by every element of I, hence so is f'; thus $f' \in S_2(\mathbf{Z}_{(\ell)})[I]$. By hypothesis, $W_\ell(f') \in S_2(\mathbf{Z}_{(\ell)})[I]$. Then

$$\Phi(W_\ell\omega') = F\text{-}\exp(W_\ell f) = \ell \cdot F\text{-}\exp(W_\ell f') \in \ell\mathbf{Z}_{(\ell)}[[q]].$$

Reducing modulo ℓ, we get $\Phi_\ell(W_\ell\omega) = 0$ in $\mathbf{F}_\ell[[q]]$. Thus $W_\ell\omega \in \ker(\Phi_\ell)$, which proves that $\ker(\Phi_\ell)$ is stable under W_ℓ.

Since W_ℓ is an involution, and by hypothesis either ℓ is odd or W_ℓ is a scalar, the space $\ker(\Phi_\ell)$ breaks up into a direct sum of eigenspaces under W_ℓ with eigenvalues ±1. It suffices to show that if $\omega \in \ker(\Phi_\ell)$ is an element of either eigenspace, then $\omega = 0$. For this, we use a standard argument that goes back to Mazur (see, e.g., the proof of Prop. 22 in [MR91]); we give some details to clarify the argument in our situation.

Following the proof of Prop. 3.3 on p. 68 of [Maz77], we have

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

In the following, we shall think of $G \otimes \mathbf{F}_\ell$ as a subgroup of $H^0(\mathcal{X}_{\mathbf{F}_\ell}, \Omega_{\mathcal{X}/\mathbf{F}_\ell})$, which we can do by the hypothesis that the induced map $G \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$ is injective and that

$$H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{X}_{\mathbf{Z}_{(\ell)}}, \Omega_{\mathcal{X}/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{X}_{\mathbf{F}_\ell}, \Omega_{\mathcal{X}/\mathbf{F}_\ell}).$$

Suppose $\omega \in \ker(\Phi_\ell)$ is in the ±1 eigenspace (we will treat the cases of $+1$ and -1 eigenspaces together). We will show that ω is trivial over $\mathcal{X}_{\overline{\mathbf{F}}_\ell}$, the base change of $\mathcal{X}_{\mathbf{F}_\ell}$ to an algebraic closure $\overline{\mathbf{F}}_\ell$, which suffices for our purposes. Since $\ell^2 \nmid N$, we have $\ell \mid\mid N$, and so the special fiber $\mathcal{X}_{\overline{\mathbf{F}}_\ell}$ is as depicted on p. 177 of [Maz77]: it consists of the union of two copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$ identified transversely at the supersingular points, and some copies of $\mathbf{P}^1$, each of which intersects exactly one of the two copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$ and perhaps another $\mathbf{P}^1$, all of them transversally. All the singular points are ordinary double points, and the cusp ∞ lies on one of the two copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$.

In particular, $\mathcal{X}_{\overline{\mathbf{F}}_\ell} \to \operatorname{Spec} \overline{\mathbf{F}}_\ell$ is locally a complete intersection, hence Gorenstein, and so by [DR73, § I.2.2, p. 162], the sheaf $\Omega_{\mathcal{X}/\overline{\mathbf{F}}_\ell} = \Omega_{\mathcal{X}/\mathbf{F}_\ell} \otimes \overline{\mathbf{F}}_\ell$ is invertible. Since $\omega \in \ker(\Phi_\ell)$, the differential ω vanishes on the copy of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$ containing the cusp ∞ by the q-expansion principle (which is easy in this case, since all that is being invoked here is that on an integral curve, the natural map from the group of global sections of an invertible sheaf into the completion of the sheaf's stalk at a point is injective). The two copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$ are swapped under the action of the Atkin-Lehner involution W_ℓ, and thus $W_\ell(\omega)$ vanishes on the other copy that does not contain the cusp ∞. Since $W_\ell(\omega) = \pm\omega$, we see that ω is zero on both copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$. Also, by the description of the relative dualizing sheaf in [DR73, § I.2.3, p. 162], if $\pi : \widetilde{\mathcal{X}}_{\overline{\mathbf{F}}_\ell} \to \mathcal{X}_{\overline{\mathbf{F}}_\ell}$ is a normalization, then ω correponds to a meromorphic differential $\widetilde{\omega}$ on $\widetilde{\mathcal{X}}_{\overline{\mathbf{F}}_\ell}$ which is regular outside the inverse images (under π) of the double points on $\mathcal{X}_{\overline{\mathbf{F}}_\ell}$ and has at worst a simple pole at any point that lies over a double point on $\mathcal{X}_{\overline{\mathbf{F}}_\ell}$. Moreover, on the inverse image of any double point on $\mathcal{X}_{\overline{\mathbf{F}}_\ell}$, the residues of $\widetilde{\omega}$ add to zero. For any of the $\mathbf{P}^1$'s, above a point of intersection of the $\mathbf{P}^1$ with a copy of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$, the residue of $\widetilde{\omega}$ on the inverse image of the copy of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$ is zero (since ω is trivial on both copies of $X_0(N/\ell)_{\overline{\mathbf{F}}_\ell}$), and thus the residue of $\widetilde{\omega}$ on the inverse image of $\mathbf{P}^1$ is zero. Thus $\widetilde{\omega}$ restricted to the inverse image of $\mathbf{P}^1$ is regular away from the inverse image of any point where the $\mathbf{P}^1$ meets another $\mathbf{P}^1$ (recall that there can be at most one such point). Hence the restriction of $\widetilde{\omega}$ to the inverse image of the $\mathbf{P}^1$ is either regular everywhere or is regular away from one point where it has at most a simple pole; in the latter case, the residue is zero by the residue theorem. Thus in either case, $\widetilde{\omega}$ restricted to the inverse image of the $\mathbf{P}^1$ is regular, and therefore is zero. Thus ω is trivial on all the copies of $\mathbf{P}^1$ as well. Hence $\omega = 0$, as was to be shown. □

4.2. **Proof of Theorem 3.5.** We continue to use the notation of Section 4.1.

First suppose that $\ell \mid N$ and $S_2(\mathbf{Z}_{(\ell)})[I]$ is not stable under the action of W_ℓ. Relative differentials and Néron models are functorial, so $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$ is W_ℓ-stable. Thus the map $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \to S_2(\mathbf{Z}_{(\ell)})[I]$ is not surjective. But c_A is the order of the cokernel, so $\ell \mid c_A$.

Next we prove the other implication, namely that if $\ell \mid c_A$, then $\ell \mid N$ and $S_2(\mathbf{Z}_{(\ell)})[I]$ is not stable under W_ℓ. We will prove this by proving the contrapositive, i.e., that if either $\ell \nmid N$ or $S_2(\mathbf{Z}_{(\ell)})[I]$ is stable under W_ℓ, then $\ell \nmid c_A$.

We now follow the discussion preceding Lemma 4.2, taking $G = H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$. To show that $\ell \nmid c_A$, we have to show that c_A is a unit in $\mathbf{Z}_{(\ell)}$. For this, it suffices to check that in diagram (2), the image of $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$ in $\mathbf{Z}_{(\ell)}[[q]]$ under Φ is saturated, since the image of $S_2(\Gamma_0(N); \mathbf{Z}_{(\ell)})[I]$ under F-exp is saturated in $\mathbf{Z}_{(\ell)}[[q]]$. In view of Lemma 4.2, it suffices to show that the map

$$H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$$

is injective.

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

$$0 \to H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \to H^0(B_{\mathbf{Z}_{(\ell)}}, \Omega^1_{B/\mathbf{Z}_{(\ell)}}) \to 0$$

where $B = \ker(J \to A)$. Since $H^0(B_{\mathbf{Z}_{(\ell)}}, \Omega^1_{B/\mathbf{Z}_{(\ell)}})$ is torsion free, by Lemma 4.1 the map $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$ is injective, as was to be shown.

4.3. **Proof of Theorem 3.11.** We continue to use the notation and hypotheses of Section 4.1 (so $\ell^2 \nmid N$) and assume in addition that A is a newform quotient, and that $\ell \nmid m_A$. We have to show that then $\ell \nmid c_A$. Just as in the previous proof, it suffices to check that the image of $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$ in $\mathbf{Z}_{(\ell)}[[q]]$ is saturated. Since A is a newform quotient, if $\ell \mid N$, then W_ℓ acts as a scalar on A and on $S_2(\Gamma_0(N); \mathbf{Z}_{(\ell)})[I]$. So again, using Lemma 4.2, it suffices to show that the map $H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell \to H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$ is injective.

The composition of pullback and pushforward in the following diagram is multiplication by the modular exponent of A:

$$\begin{array}{ccccc} & & H^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) & & \\ & \nearrow^{\pi^*} & & \searrow^{\pi_*} & \\ H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) & & \xrightarrow{\quad m_A \quad} & & H^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \end{array}$$

Since $m_A \in \mathbf{Z}_{(\ell)}{}^\times$, the map π^* is a section to the map π_* up to a unit and hence its reduction modulo ℓ is injective, which is what was left to be shown.

4.4. **Proof of Theorem 3.10.** Theorem 3.10 asserts that if $A = A_f$ is a quotient of $J = J_0(N)$ attached to a newform f, and ℓ is a prime such that $\ell^2 \nmid N$, then $\mathrm{ord}_\ell(c_A) \leq \dim(A)$. Our proof follows [AU96], except at the end we argue using lattice indices 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 $B_{\mathbf{Z}_{(\ell)}} \to J_{\mathbf{Z}_{(\ell)}} \to A_{J_{\mathbf{Z}_{(\ell)}}}$ of Néron models. Because $J_{\mathbf{Z}_{(\ell)}}$ has semiabelian reduction (since $\ell^2 \nmid N$), 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

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

Here Tan is the tangent space at the 0 section; it is a finite free $\mathbf{Z}_{(\ell)}$-module of rank equal to the dimension. In particular, we have $r \leq d = \dim(A)$. Note that Tan is $\mathbf{Z}_{(\ell)}$-dual to the cotangent space, and the cotangent space is isomorphic to the space of global differential 1-forms. The theorem of Raynaud mentioned above is the generalization to $e = \ell - 1$ of [Maz78, Cor. 1.1], which we used above in the proof of Theorem 3.5.

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

$$(3) \qquad \begin{array}{ccccccccc} 0 \to \mathrm{Tan}(B_{\mathbf{Z}_{(\ell)}}) \to & \mathrm{Tan}(J_{\mathbf{Z}_{(\ell)}}) & \longrightarrow & \mathrm{Tan}(A_{\mathbf{Z}_{(\ell)}}) & \to (\mathbf{Z}/\ell\mathbf{Z})^r \to 0. \\ & \searrow\!\!\!\!\searrow & & \nearrow & \\ & & C & & \end{array}$$

Since $C \subset \mathrm{Tan}(A_{\mathbf{Z}_{(\ell)}})$, so C is torsion free, we see that C is a free $\mathbf{Z}_{(\ell)}$-module of rank d. Let $C^* = \mathrm{Hom}_{\mathbf{Z}_{(\ell)}}(C, \mathbf{Z}_{(\ell)})$ be the $\mathbf{Z}_{(\ell)}$-linear dual of C. Applying the $\mathrm{Hom}_{\mathbf{Z}_{(\ell)}}(-, \mathbf{Z}_{(\ell)})$ functor to the two short exact sequences in (3), we obtain exact sequences

$$0 \to C^* \to \mathrm{H}^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \to \mathrm{H}^0(B_{\mathbf{Z}_{(\ell)}}, \Omega^1_{B/\mathbf{Z}_{(\ell)}}) \to 0,$$

and

$$(4) \qquad 0 \to \mathrm{H}^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}}) \to C^* \to (\mathbf{Z}/\ell\mathbf{Z})^r \to 0.$$

The $(\mathbf{Z}/\ell\mathbf{Z})^r$ on the right in (4) occurs as $\mathrm{Ext}^1_{\mathbf{Z}_{(\ell)}}((\mathbf{Z}/\ell\mathbf{Z})^r, \mathbf{Z}_{(\ell)})$.

Since $\mathrm{H}^0(B_{\mathbf{Z}_{(\ell)}}, \Omega^1_{B/\mathbf{Z}_{(\ell)}})$ is torsion free, by Lemma 4.1, the induced map

$$C^* \otimes \mathbf{F}_\ell \to \mathrm{H}^0(J_{\mathbf{Z}_{(\ell)}}, \Omega^1_{J/\mathbf{Z}_{(\ell)}}) \otimes \mathbf{F}_\ell$$

is injective. Since A is a newform quotient, if $\ell \mid N$ then W_ℓ acts as a scalar on C^* and on $S_2(\Gamma_0(N); \mathbf{Z}_{(\ell)})[I]$. Using Lemma 4.2, with $G = C^*$, we see that the image of C^* in $\mathbf{Z}_{(\ell)}[[q]]$ under the composite of the maps in (1) is saturated. The Manin constant for A at ℓ is the index of the image via q-expansion of $\mathrm{H}^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$ in $\mathbf{Z}_{(\ell)}[[q]]$ in its saturation. Since the image of C^* in $\mathbf{Z}_{(\ell)}[[q]]$ is saturated, the image of C^* is the saturation of the image of $\mathrm{H}^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$, so the Manin constant at ℓ is the index of $\mathrm{H}^0(A_{\mathbf{Z}_{(\ell)}}, \Omega^1_{A/\mathbf{Z}_{(\ell)}})$ in C^*, which is ℓ^r by (4), hence is at most ℓ^d.

5. Appendix by J. Cremona: Verifying that $c = 1$

Let f be a normalised rational newform for $\Gamma_0(N)$. Let Λ_f be its period lattice; that is, the lattice of periods of $2\pi i f(z)dz$ over $H_1(X_0(N), \mathbf{Z})$.

We know that $E_f = \mathbf{C}/\Lambda_f$ is an elliptic curve E_f defined over $\mathbf{Q}$ and of conductor N. This is the optimal quotient of $J_0(N)$ associated to f. Our goal is two-fold: to identify E_f (by giving an explicit Weierstrass model for it with integer coeffients); and to show that the associated Manin constant for E_f is 1. In this section we will give an algorithm for this; our algorithm applies equally to optimal quotients of $J_1(N)$.

As input to our algorithm, we have the following data:

(1) a $\mathbf{Z}$-basis for Λ_f, known to a specific precision;
(2) the type of the lattice Λ_f (defined below); and
(3) a complete isogeny class of elliptic curves $\{E_1, \ldots, E_m\}$ of conductor N, given by minimal models, all with $L(E_j, s) = L(f, s)$.

So E_f is isomorphic over $\mathbf{Q}$ to E_{j_0} for a unique $j_0 \in \{1, \ldots, m\}$.

The justification for this uses the full force of the modularity of elliptic curves defined over $\mathbf{Q}$: we have computed a full set of newforms f at level N, and the same number of isogeny classes of elliptic curves, and the theory tells us that there is a bijection between these sets. Checking the first few terms of the L-series (i.e., comparing the Hecke eigenforms of the newforms with the traces of Frobenius for the curves) allows us to pair up each isogeny class with a newform.

We will assume that one of the E_j, which we always label E_1, is such that Λ_f and Λ_1 (the period lattice of E_1) are approximately equal. This is true in practice, because our method of finding the curves in the isogeny class is to compute the coefficients of a curve from numerical approximations to the c_4 and c_6 invariants of $\mathbf{C}/\Lambda_f$; in all cases these are very close to integers which are the invariants of the minimal model of an elliptic curve of conductor N, which we call E_1. The other curves in the isogeny class are then computed from E_1. For the algorithm described here, however, it is irrelevant how the curves E_j were obtained, provided that Λ_1 and Λ_f are close (in a precise sense defined below).

Normalisation of lattices: every lattice Λ in $\mathbf{C}$ which defined over $\mathbf{R}$ has a unique $\mathbf{Z}$-basis ω_1, ω_2 satisfying one of the following:

- **Type 1:** ω_1 and $(2\omega_2 - \omega_1)/i$ are real and positive; or

- **Type 2:** ω_1 and ω_2/i are real and positive.

For Λ_f we know the type from modular symbol calculations, and we know ω_1, ω_2 to a certain precision by numerical integration; modular symbols provide us with cycles $\gamma_1, \gamma_2 \in H_1(X_0(N), \mathbf{Z})$ such that the integral of $2\pi i f(z)dz$ over γ_1, γ_2 give ω_1, ω_2.

For each curve E_j we compute (to a specific precision) a $\mathbf{Z}$-basis for its period lattice Λ_j using the standard AGM method. Here, Λ_j is the lattice of periods of the Néron differential on E_j. The type of Λ_j is determined by the sign of the discriminant of E_j: type 1 for negative discriminant, and type 2 for positive discriminant.

For our algorithm we will need to know that Λ_1 and Λ_f are approximately equal. To be precise, we know that they have the same type, and also we verify, for a specific positive ε, that

$$(*) \qquad \left| \frac{\omega_{1,1}}{\omega_{1,f}} - 1 \right| < \varepsilon \qquad \text{and} \qquad \left| \frac{\mathrm{im}(\omega_{2,1})}{\mathrm{im}(\omega_{2,f})} - 1 \right| < \varepsilon.$$

Here $\omega_{1,j}$, $\omega_{2,j}$ denote the normalised generators of Λ_j, and $\omega_{1,f}$, $\omega_{2,f}$ those of Λ_f.

Pulling back the Néron differential on E_{j_0} to $X_0(N)$ gives $c \cdot 2\pi i f(z)dz$ where $c \in \mathbf{Z}$ is the Manin constant for f. Hence

$$c\Lambda_f = \Lambda_{j_0}.$$

Our task is now to

(1) identify j_0, to find which of the E_j is (isomorphic to) the "optimal" curve E_f; and
(2) determine the value of c.

Our main result is that $j_0 = 1$ and $c = 1$, provided that the precision bound ε in (*) is sufficiently small (in most cases, $\varepsilon < 1$ suffices). In order to state this precisely, we need some further definitions.

A result of Stevens says that in the isogeny class there is a curve, say E_{j_1}, whose period lattice Λ_{j_1} is contained in every Λ_j; this is the unique curve in the class with minimal Faltings height. (It is conjectured that E_{j_1} is the $\Gamma_1(N)$-optimal curve, but we do not need or use this fact. In many cases, the $\Gamma_0(N)$- and $\Gamma_1(N)$-optimal curves are the same, so we expect that $j_0 = j_1$ often; indeed, this holds for the vast majority of cases.)

For each j, we know therefore that $a_j = \omega_{1,j_1}/\omega_{1,j} \in \mathbf{N}$ and also $b_j = \mathrm{im}(\omega_{2,j_1})/\mathrm{im}(\omega_{2,j}) \in \mathbf{N}$. Let B be the maximum of a_1 and b_1.

Proposition 5.1. *Suppose that (*) holds with $\epsilon = B^{-1}$; then $j_0 = 1$ and $c = 1$. That is, the curve E_1 is the optimal quotient and its Manin constant is* 1.

Proof. Let $\varepsilon = B^{-1}$ and $\lambda = \frac{\omega_{1,1}}{\omega_{1,f}}$, so $|\lambda - 1| < \varepsilon$. For some j we have $c\Lambda_f = \Lambda_j$. The idea is that $\mathrm{lcm}(a_1, b_1)\Lambda_1 \subseteq \Lambda_{j_1} \subseteq \Lambda_j = c\Lambda_f$; if $a_1 = b_1 = 1$, then the closeness of Λ_1 and Λ_f forces $c = 1$ and equality throughout. To cover the general case it is simpler to work with the real and imaginary periods separately.

Firstly,

$$\frac{\omega_{1,j}}{\omega_{1,f}} = c \in \mathbf{Z}.$$

Then

$$c = \frac{\omega_{1,1}}{\omega_{1,f}}\frac{\omega_{1,j}}{\omega_{1,1}} = \frac{a_1}{a_j}\lambda.$$

Hence

$$0 \leq |\lambda - 1| = \frac{|a_j c - a_1|}{a_1} < \varepsilon.$$

If $\lambda \neq 1$, then $\varepsilon > |\lambda - 1| \geq a_1^{-1} \geq B^{-1} = \varepsilon$, contradiction. Hence $\lambda = 1$, so $\omega_{1,1} = \omega_{1,f}$. Similarly, we have

$$\frac{\mathrm{im}(\omega_{2,j})}{\mathrm{im}(\omega_{2,f})} = c \in \mathbf{Z}$$

and again we can conclude that $\mathrm{im}(\omega_{2,1}) = \mathrm{im}(\omega_{2,f})$, and hence $\omega_{2,1} = \omega_{2,f}$.

Thus $\Lambda_1 = \Lambda_f$, from which the result follows. □

Theorem 5.2. *For all $N < 60000$, every optimal elliptic quotient of $J_0(N)$ has Manin constant equal to* 1*. Moreover, the optimal curve in each class is the one whose identifying number on the tables* [Cre] *is* 1 *(except for class* 990h *where the optimal curve is* 990h3*).*

Proof. For all $N < 60000$ we used modular symbols to find all newforms f and their period lattices, and also the corresponding isogeny classes of curves. In all cases we verified that (*) held with the appropriate value of ε. (The case of 990h is only exceptional on account of an error in labelling the curves several years ago, and is not significant.) □

Remark 5.3. In the vast majority of cases, the value of B is 1, so the precision needed for the computation of the periods is very low. For $N < 60000$, out of 258502 isogeny classes, only 136 have $B > 1$: we found $a_1 = 2$ in 13 cases, $a_1 = 3$ in 29 cases, and $a_1 = 4$ and $a_1 = 5$ once each (for $N = 15$ and $N = 11$ respectively); $b_1 = 2$ in 93 cases; and no larger values. Class 17a is the only one for which both a_1 and b_1 are greater than 1 (both are 2).

Finally, we give a slightly weaker result for $60000 < N < 130000$; in this range we do not know Λ_f precisely, but only its projection onto the real line. (The reason for this is that we can find the newforms using modular symbols for $H_1^+(X_0(N), \mathbf{Z})$, which has half the dimension of $H_1(X_0(N), \mathbf{Z})$; but to find the exact period lattice requires working in $H_1(X_0(N), \mathbf{Z})$.) The argument is similar to the one given above, using $B = a_1$.

Theorem 5.4. *For all* N *in the range* $60000 < N < 130000$*, every optimal elliptic quotient of* $J_0(N)$ *has Manin constant equal to* 1*.*

Proof. We continue to use the notation above. We do not know the lattice Λ_f but only (to a certain precision) a positive real number $\omega_{1,f}^+$ such that either Λ_f has type 1 and $\omega_{1,f} = 2\omega_{1,f}^+$, or Λ_f has type 2 and $\omega_{1,f} = \omega_{1,f}^+$. Curve E_1 has lattice Λ_1, and the ratio $\lambda = \omega_{1,1}^+/\omega_{1,f}^+$ satisfies $|\lambda - 1| < \varepsilon$. In all cases this holds with $\varepsilon = \frac{1}{3}$, which will suffice.

First assume that $a_1 = 1$.

If the type of Λ_f is the same as that of Λ_1 (for example, this must be the case if all the Λ_j have the same type, which will hold whenever all the isogenies between the E_j have odd degree) then from $c\Lambda_f = \Lambda_j$ we deduce as before that $\lambda = 1$ exactly, and $c = a_1/a_j = 1/a_j$, hence $c = a_j = 1$. So in this case we have that $c = 1$, though there might be some ambiguity in which curve is optimal if $a_j = 1$ for more than one value of j.

Assume next that Λ_1 has type 1 but Λ_f has type 2. Now $\lambda = \omega_{1,1}/2\omega_{1,f}$. The usual argument now gives $ca_j = 2$. Hence either $c = 1$ and $a_j = 2$, or $c = 2$ and $a_j = 1$. To see if the latter case could occur, we look for classes in which $a_1 = 1$ and Λ_1 has type 1, while for some $j > 1$ we also have $a_j = 1$ and Λ_j of type 2. This occurs 28 times for $60000 < N < 130000$, but for 15 of these the level N is odd, so we know that c must be odd. The remaining 13 cases are

$$62516a, 67664a, 71888e, 72916a, 75092a, 85328d, 86452a, 96116a,$$
$$106292b, 111572a, 115664a, 121168e, 125332a;$$

we have been able to eliminate these by carrying out the extra computations necessary as in the proof of Theorem 5.2. We note that in all of these 13 cases, the isogeny class consists of two curves, E_1 of type 1 and E_2 of type 2, with $[\Lambda_1 : \Lambda_2] = 2$, so that E_2 rather than E_1 has minimal Faltings height.

Next suppose that Λ_1 has type 2 but Λ_f has type 1. Now $\lambda = 2\omega_{1,1}/\omega_{1,f}$. The usual argument now gives $2ca_j = 1$, which is impossible; so this case cannot occur.

Finally we consider the cases where $a_1 > 1$. There are only three of these for $60000 < N < 130000$: namely, $91270a$, $117622a$ and $124973b$, where $a_1 = 3$. In each case the Λ_j all have the same type (they are linked via 3-isogenies) and the usual argument shows that $ca_j = 3$. But none of these levels is divisible by 3, so $c = 1$ in each case. □

References

[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.

[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.

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

[ARS] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one* (2005).

[AS05] A. Agashe and W. A. 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, with an appendix by J. Cremona and B. Mazur.

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

[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).

[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/`.

[Cre] J. E. Cremona, *Tables of Elliptic Curves,*
`http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[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/`.

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

[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).

[GL01] Josep González and Joan-C. Lario, $\mathbf{Q}$*-curves and their Manin ideals*, Amer. J. Math. **123** (2001), no. 3, 475–503.

[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.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Joy05] A. Joyce, *The Manin constant of an optimal quotient of* $J_0(431)$, J. Number Theory **110** (2005), no. 2, 325–330.

[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.

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

[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).

[Mc91] W. G. McCallum, *Kolyvagin's work on Shafarevich–Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316.

[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.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[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.

[Ste89] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106.

[Vat05] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316.

Amod Agashe
Department of Mathematics
Florida State University
208 Love Building Tallahassee
FL 32306 U.S.A.
E-mail: agashe@mail.math.fsu.edu

Kenneth A. Ribet
Department of Mathematics, M/C 3840
University of California
Berkeley, CA 94720-3840, USA.
E-mail: ribet@math.berkeley.edu

William A. Stein
Department of Mathematics
Harvard University
Cambridge, MA 02138
E-mail: was@math.harvard.edu