hexagon:2611.00991v1

THE RATIONAL TORSION OF $J_1(p)$ IS GENERATED BY DIFFERENCES OF RATIONAL CUSPS

FILIP NAJMAN

ABSTRACT. Let $p \geq 5$ be a prime. Conrad, Edixhoven and Stein conjectured that the rational torsion subgroup of the Jacobian $J_1(p)$ of the modular curve $X_1(p)$ is generated by the differences of the rational cusps of $X_1(p)$. Ohta proved the conjecture up to 2-primary torsion, and it has been verified computationally for all $p \leq 157$. We prove the conjecture for all primes p. The main new ingredient is the injectivity of the reduction map $J_1(N)(\mathbb{Q})_{\mathrm{tors}} \to J_1(N)(\mathbb{F}_2)$, which we prove for every odd integer $N \geq 5$ using the unbounded denominators theorem of Calegari, Dimitrov and Tang. For $N = p$ this allows us to extend Ohta's method to the prime 2.

1. Introduction

Let p be a prime and let $J_0(p)$ and $J_1(p)$ be the Jacobians of the modular curves $X_0(p)$ and $X_1(p)$. By the Manin-Drinfeld theorem [13, 17], the classes of divisors of degree 0 supported on the cusps of a modular curve are torsion points of its Jacobian. Ogg [20] showed that the class of $(0)-(\infty)$ generates a subgroup of $J_0(p)(\mathbb{Q})$ of order n, the numerator of $(p-1)/12$, and conjectured [21] that this subgroup is all of $J_0(p)(\mathbb{Q})_{\mathrm{tors}}$. Mazur [18] proved Ogg's conjecture, as a part of his study of the Eisenstein ideal.

For $J_1(p)$ the corresponding statement was conjectured by Conrad, Edixhoven and Stein. We use the model of $X_1(p)$ over $\mathbb{Q}$ whose non-cuspidal points parametrize pairs (E, P) consisting of an elliptic curve E and a point $P \in E$ of order p (see Section 2). Exactly $(p-1)/2$ of the $p-1$ cusps of $X_1(p)$ are defined over $\mathbb{Q}$. We denote by $C_1(p)$ the subgroup of $J_1(p)(\mathbb{Q})$ generated by the classes of the differences of these cusps, and call it the *rational cuspidal subgroup*.

Conjecture 1.1 ([6, Conjecture 6.2.2])**.** *Let $p \geq 5$ be a prime. Then $J_1(p)(\mathbb{Q})_{\mathrm{tors}} = C_1(p)$.*

The order of $C_1(p)$ was computed by Kubert and Lang [16, Chapter 6, Theorem 3.4], following Klimek:

$$|C_1(p)| = |c(p)|, \qquad \text{where} \qquad c(p) := p \prod_{\chi} \frac{B_{2,\chi}}{4}, \tag{1.1}$$

2020 *Mathematics Subject Classification.* 11G18, 14G35, 11F11, 14G05.

Key words and phrases. modular Jacobians, rational torsion, cuspidal subgroup, Eisenstein ideal, unbounded denominators.

The author was supported by the Croatian Science Foundation under the project no. IP-2022-10-5008, by the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, via an institutional grant of the University of Zagreb Faculty of Science, IK IA 1.1.3, Impact4Math.

χ runs through the nontrivial even Dirichlet characters modulo p, and $B_{2,\chi}$ is the second generalized Bernoulli number of χ (see also [6, Section 6.2.3] and [22, (3.2.3)]). Hence Conjecture 1.1 is equivalent to the equality $|J_1(p)(\mathbb{Q})_{\mathrm{tors}}| = |c(p)|$.

Ogg [20] showed that $J_1(13)(\mathbb{Q}) \simeq \mathbb{Z}/19\mathbb{Z}$. Conrad, Edixhoven and Stein computed an upper bound for $|J_1(p)(\mathbb{Q})_{\mathrm{tors}}|$ for all primes $p \leq 157$ and found that it is equal to $|c(p)|$ for all of them except $p \in \{29, 97, 101, 109, 113\}$ [6, Section 6.2.3 and Table 1], proving Conjecture 1.1 for the other primes $p \leq 157$. Derickx, Kamienny, Stein and Stoll proved the conjecture for $p = 29$ [10, Theorem 3.2], and De Leo and Stoll for $p \in \{97, 101, 109, 113\}$ [8, Theorem 1.3], so the conjecture is known for all $p \leq 157$. De Leo and Stoll also determined the structure of $J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ for all $p \leq 113$ [8, Table 4.5].

Kamienny [14] showed that if a prime $\ell \geq 5$ divides the order of the rational torsion subgroup of the quotient of $J_1(p)$ by the image of $J_0(p)$, then ℓ divides $c(p)$. Ohta [22, Theorem I] proved Conjecture 1.1 up to 2-primary torsion: for every odd prime ℓ (including $\ell = p$) he showed that

$$J_1(p)(\mathbb{Q})[\ell^\infty] = C_1(p)[\ell^\infty].$$

His proof follows Mazur's approach through the Eisenstein ideal: he shows that a certain Eisenstein ideal of the ℓ-adic Hecke algebra annihilates $J_1(p)(\mathbb{Q})[\ell^\infty]$ and that its index is the ℓ-part of $c(p)$. The 2-primary part remained open. Ohta remarks that his proof that the Eisenstein ideal annihilates $J_1(p)(\mathbb{Q})[\ell^\infty]$ also works for $\ell = 2$, except for the element $T_2 - 1 - 2\langle 2\rangle$, and that this is "the only (but serious) obstacle" to the annihilation at 2 [22, Remark 3.1.4].

In this paper we prove Conjecture 1.1.

Theorem 1.2. *Let $p \geq 5$ be a prime. Then $J_1(p)(\mathbb{Q})_{\mathrm{tors}} = C_1(p)$. In particular $|J_1(p)(\mathbb{Q})_{\mathrm{tors}}| = |c(p)|$.*

By Ohta's theorem, Theorem 1.2 is equivalent to the equality

$$J_1(p)(\mathbb{Q})[2^\infty] = C_1(p)[2^\infty],$$

which we prove in Section 5. We also show that $J_1(p)(\mathbb{Q})[2^\infty]$ is isomorphic, as a module over the 2-adic Hecke algebra, to the quotient of this algebra by the Eisenstein ideal (Corollary 5.3), which is the analogue at 2 of [22, Proposition 3.2.7].

The main new ingredient is the following theorem, which we prove in Section 3. Unlike Theorem 1.2, it holds at every odd level.

Theorem 1.3. *Let $N \geq 5$ be an odd integer. Then the reduction map $J_1(N)(\mathbb{Q})_{\mathrm{tors}} \to J_1(N)(\mathbb{F}_2)$ is injective.*

Here $J_1(N)$ is the Jacobian of the modular curve $X_1(N)$ (see Section 2). As N is odd, $J_1(N)$ has good reduction at 2, so the reduction map is defined. For every odd prime $\ell \nmid N$ the reduction map $J_1(N)(\mathbb{Q})_{\mathrm{tors}} \to J_1(N)(\mathbb{F}_\ell)$ is injective (see [6, Section 6.1.1]), so Theorem 1.3 shows that $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ injects into $J_1(N)(\mathbb{F}_\ell)$ for every prime $\ell \nmid N$. In the proof of Theorem 1.2 we only use the case $N = p$. For the primes p for which $J_1(p)(\mathbb{Q})$ is finite, this case was proved by Derickx, Kamienny, Stein and Stoll [10, Proposition 3.4], by an explicit computation for $p \in \{17, 29, 31, 41\}$. For an odd prime $\ell \neq p$, the statement that $J_1(p)(\mathbb{Q})[\ell^\infty]$ injects into $J_1(p)(\mathbb{F}_\ell)$ also follows from a theorem of Raynaud [23, Théorème 3.3.3], and this is what Ohta uses at ℓ (see [22, proof of Lemma 3.1.3 and Section 3.2]). Raynaud's theorem does not apply when $\ell = 2$, and the analogue of Theorem 1.3 for $J_0(N)$ is false. For example, $J_0(17)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, and the reduction modulo 2 of a generator has

order 2 [10, Remark after Proposition 3.4]. Similarly, $J_0(15)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has order 8, while $\#J_0(15)(\mathbb{F}_2) = 4$. In contrast, $X_1(15)$ is the elliptic curve with Cremona label 15a8, and the reduction map $J_1(15)(\mathbb{Q}) \to J_1(15)(\mathbb{F}_2)$ is an isomorphism of groups of order 4 (see Section 6).

The proof of Theorem 1.3 goes as follows. Suppose that $P \in J_1(N)(\mathbb{Q})$ is a point of order 2 that reduces to 0 modulo 2. Then the schematic closure of $\{0, P\}$ in the Néron model of $J_1(N)$ over $\mathbb{Z}_2$ is isomorphic to μ_2, and from this we obtain an isogeny $\varphi\colon A \to J_1(N)$ of degree 2 that extends to an étale morphism of Néron models over $\mathbb{Z}_\ell$ for every prime ℓ, including $\ell = 2$ (Lemma 3.3). Pulling φ back along an Abel-Jacobi map based at a rational cusp gives a geometrically connected finite étale double cover W of the modular curve, with a rational point w above that cusp. Using a smooth model of the modular curve over $\mathbb{Z}$ near the cusp and the Néron mapping property, we show that every function on W that is integral over $\mathbb{Z}[j]$ has a q-expansion at w with coefficients in $\mathbb{Z}$ (Lemma 3.5). The theorem of Calegari, Dimitrov and Tang [4, Theorem 1.0.1] then shows that the subgroup of index 2 of $\Gamma_1(N)$ (up to ± 1) that corresponds to W is a congruence subgroup. As W is unramified over the modular curve, this subgroup has the same cusp widths as $\Gamma_1(N)$, so by Wohlfahrt's theorem [27, Theorem 2] it contains $\Gamma(N)$. This is impossible, as $\Gamma(N)$ has odd index N in $\Gamma_1(N)$. For $J_0(N)$ the argument breaks down exactly at this last step (see Remark 3.8).

Our argument is an adaptation of the argument of Chi, Liu and Nie in their recent work on the Manin constant [5, Section 4]. They use [4, Theorem 1.0.1] and Wohlfahrt's theorem to show that the lift of a modular parametrization of an elliptic curve through an isogeny is modular, provided that its q-expansion has bounded denominators, and they indicate how to extend their method to abelian varieties [5, Remark 4.8]. In our setting the integrality of q-expansions comes from the fact that φ extends to an étale morphism over every $\mathbb{Z}_\ell$. This is the only place where we use that P reduces to 0 modulo 2.

With Theorem 1.3 at hand, Ohta's proof for odd primes [22, Sections 2, 3.1 and 3.2] can be carried out at the prime 2. Theorem 1.3 and the Eichler-Shimura relation show that $T_2 - 1 - 2\langle 2\rangle$ annihilates $J_1(p)(\mathbb{Q})[2^\infty]$ (Lemma 5.1), and Theorem 1.3 also replaces Raynaud's theorem in the counting argument of [22, Section 3.2]. Ohta's computation of the index of the Eisenstein ideal [22, Theorem 2.4.2] uses that the residue characteristic is odd only to see that the constant terms $-B_{2,\chi}/4$ of certain Eisenstein series are integral (in two places). We remove this restriction by writing $B_{2,\chi}/4$ as a linear combination of the values of χ with 2-integral coefficients (Lemma 4.1). Finally, Ohta's multiplicity one result [22, Lemma 3.2.6] is stated for odd residue characteristic. We prove it in characteristic 2 along the same lines (Lemma 5.2), using Cartier duality instead of the isomorphism of Cartier and Serre, so that the compatibility with the Hecke operator T_2 is clear.

The proofs in this paper do not use computer calculations. In Section 6 we describe some computations, for $p \leq 139$ and for $N = 15$, that are consistent with Theorem 1.3 and Theorem 1.2. As Conjecture 1.1 was already known for $p \leq 157$, they only test the intermediate statements and our conventions. The code for these computations, together with the logs of our runs, can be found at

`https://github.com/F-Najman/J1_p_tors`

In the digital form of this article, the words reporting a computation, such as "we compute", are hyperlinks to the script that carries it out, at the revision

`0b1ad1c7fc5536eca2f899cf0603d285028cab95`

of the repository. Each claim of Section 6 is labelled in the code by a comment such as `// Claim 1`, is checked there by an `assert` statement, and is confirmed in the log by the line `Claim 1 successfully verified`. The file `README.md` lists, for each claim, the script and the log.

We fix our conventions in Section 2. We prove Theorem 1.3 in Section 3, compute the index of the Eisenstein ideal at 2 in Section 4, and prove Theorem 1.2 in Section 5.

AI disclosure and comments. AI models were extensively used in the work leading to this paper. OpenAI's GPT-6.2 Astra produced the first version of the proof. Anthropic's Claude Opus 5.5 and Fable 5.2 reviewed that version, ran the computations of Section 6, and wrote the draft of the present manuscript, which differs from the first version mainly in the proof of Theorem 1.3 and in the details given in Sections 4 and 5.

2. Conventions and notation

For an abelian group M and an integer n, we denote by $M[n]$ the kernel of multiplication by n and by $M[2^\infty]$ the 2-primary part of M. For an abelian variety A over $\mathbb{Q}$ and a prime ℓ, we denote by $\mathcal{A}_\ell$ the Néron model of $A_{\mathbb{Q}_\ell}$ over $\mathbb{Z}_\ell$. By the Néron mapping property, every morphism from a smooth $\mathbb{Z}_\ell$-scheme $\mathcal{U}$ to $\mathcal{A}_\ell$ is determined by its generic fibre, and every morphism $\mathcal{U}_{\mathbb{Q}_\ell} \to A_{\mathbb{Q}_\ell}$ extends to a morphism $\mathcal{U} \to \mathcal{A}_\ell$ [2, Section 1.2]. In particular, homomorphisms of abelian varieties extend to homomorphisms of their Néron models. If A has good reduction at ℓ, then $\mathcal{A}_\ell$ is an abelian scheme [2, Section 1.2], and we denote by $A(\mathbb{F}_\ell)$ the group of $\mathbb{F}_\ell$-points of its special fibre and by $A(\mathbb{Q}) \to A(\mathbb{F}_\ell)$ the reduction map.

Let $N \geq 5$ be an integer. We use the models of modular curves over $\mathbb{Q}$ of [6] and [22]. The curve $X_1(N)$ is the smooth projective curve over $\mathbb{Q}$ that contains, as a dense open subscheme, the coarse moduli scheme of pairs (E, P) of an elliptic curve E and a point $P \in E$ of order N, and $J_1(N)$ is its Jacobian. By Igusa's theorem [12, Theorem 8.6.1], the curve $X_1(N)$ has good reduction at every prime $\ell \nmid N$, and hence so does $J_1(N)$.

We also use the curve $X_\mu(N)$, which is defined in the same way using pairs (E, α) of an elliptic curve E and a closed immersion $\alpha\colon \mu_N \hookrightarrow E$ of group schemes [5, Definition 1.3]. The curves $X_1(N)$ and $X_\mu(N)$ are isomorphic over $\mathbb{Z}[1/N]$, via $(E, P) \mapsto (E/\langle P\rangle, E[N]/\langle P\rangle)$, where $E[N]/\langle P\rangle$ is identified with μ_N by the Weil pairing [6, proof of Lemma 6.1.6]. Hence the Jacobian $J_\mu(N)$ of $X_\mu(N)$ is isomorphic to $J_1(N)$ over $\mathbb{Q}$. Let $\infty \in X_\mu(N)(\mathbb{Q})$ be the cusp given by the standard 1-gon together with the embedding of μ_N into its smooth locus $\mathbb{G}_m$.

Let $\mathcal{X}_\mu(N)$ be the coarse moduli scheme over $\mathbb{Z}$ of pairs (E, α), where E is a generalized elliptic curve with irreducible geometric fibres and $\alpha\colon \mu_N \hookrightarrow E^{\mathrm{sm}}$ is a closed immersion of group schemes. We will use the following facts, which are stated in [6, proof of Lemma 6.1.6] (where they are deduced from [15] and [9], see [11, Sections 9.3 and 12.3]).

a) The scheme $\mathcal{X}_\mu(N)$ is smooth over $\mathbb{Z}$, and its generic fibre is an open subscheme of $X_\mu(N)$ containing ∞.
b) The cusp ∞ extends to a point $\infty \in \mathcal{X}_\mu(N)(\mathbb{Z})$, and the Tate curve gives an isomorphism between $\operatorname{Spf}\mathbb{Z}[[q]]$ and the formal completion of $\mathcal{X}_\mu(N)$ along ∞. In particular, the expansion of the j-invariant in q is the j-invariant of the Tate curve, $j = q^{-1} + 744 + 196884q + \cdots \in q^{-1}\mathbb{Z}[[q]]$.
c) The choice $\zeta_N = e^{2\pi i/N}$ identifies $X_\mu(N)(\mathbb{C})$ with $\Gamma_1(N)\backslash\mathcal{H}^*$, where $\mathcal{H}^*$ is the union of the upper half plane $\mathcal{H}$ and $\mathbb{P}^1(\mathbb{Q})$. Under this identification the point ∞ is the cusp ∞ and the parameter q of b) is $e^{2\pi i\tau}$.

We write $\mathbb{Z}((q)) = \mathbb{Z}[[q]][q^{-1}]$, and similarly for other rings of coefficients. By b), the formal completion of $X_\mu(N)$ at ∞ is $\operatorname{Spf}\mathbb{Q}[[q]]$, and we call the induced embedding $\mathbb{Q}(X_\mu(N)) \hookrightarrow \mathbb{Q}((q))$ the *q-expansion* at ∞.

Now let $p \geq 5$ be a prime. Then $X_1(p)$ is the compactified moduli space of pairs (E, β), where E is a generalized elliptic curve and $\beta\colon \mathbb{Z}/p\mathbb{Z} \hookrightarrow E^{\mathrm{sm}}$ is an embedding into its smooth locus [22, Section 3.1], and $X_\mu(p)$ is the curve of [22, Section 1.1]. Exactly $(p-1)/2$ cusps of $X_1(p)$ are defined over $\mathbb{Q}$ (they are called 0-cusps in [22]), and the other $(p-1)/2$ are defined over $\mathbb{Q}(\zeta_p)^+$, the maximal real subfield of $\mathbb{Q}(\zeta_p)$. We denote by $C_1(p)$ the subgroup of $J_1(p)(\mathbb{Q})$ generated by the classes of divisors of degree 0 supported on the rational cusps (this is the group C_0 of [22]).

Let $G = (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. For $a \in G$ we denote by $\langle a\rangle$ the diamond operator, and for an integer $n \geq 1$ by T_n the Hecke operator ($T(n)$ in the notation of [22]). For a ring R, let $h_2(\Gamma_1(p); R)$ be the Hecke algebra of [22, Definition 1.2.5], i.e. the R-algebra of endomorphisms of $S_2(\Gamma_1(p); R)$ generated by all T_n and $\langle a\rangle$. By [22, Remark 1.3.8(1)], $h_2(\Gamma_1(p); R) = h_2(\Gamma_1(p); \mathbb{Z}) \otimes_{\mathbb{Z}} R$. We put

$$\mathbb{T} := h_2(\Gamma_1(p); \mathbb{Z}_2) = h_2(\Gamma_1(p); \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_2.$$

As in [22, (3.1.1)], we let $h_2(\Gamma_1(p); \mathbb{Z})$ act on $J_1(p)$ through Albanese (covariant) functoriality. These endomorphisms extend to the Néron models of $J_1(p)$, so they commute with the reduction maps. With this convention, for every prime $\ell \neq p$ the Eichler-Shimura relation reads

$$T_\ell = \mathrm{Frob}_\ell + \langle \ell\rangle \,\mathrm{Ver}_\ell \tag{2.1}$$

on the special fibre of the Néron model of $J_1(p)$ over $\mathbb{Z}_\ell$, where Frob_ℓ and Ver_ℓ are the Frobenius and the Verschiebung [22, proof of Lemma 3.1.3].

The *Eisenstein ideal* I of $\mathbb{T}$ is the ideal generated by

$$\eta_\ell := T_\ell - 1 - \ell\langle \ell\rangle \quad (\ell \neq p \text{ prime}), \qquad T_p - 1 \qquad \text{and} \qquad \tau := \sum_{a \in G} \langle a\rangle.$$

This is the ideal $I_{\infty,\mathbb{Z}_2}$ of [22, Definition 2.1.12], and by [22, Corollary 2.1.14] it is generated by τ and the elements η_ℓ. For a ring R we denote by $I_{\infty,R}$ the ideal of $h_2(\Gamma_1(p); R)$ generated by the same elements.

For a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of finite index containing $-I$ and a cusp $\kappa = \sigma\infty$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, the *width* of κ for Γ is the smallest integer $m \geq 1$ such that $\sigma U^m \sigma^{-1} \in \Gamma$, where $U = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. It is the ramification index at κ of the map $\Gamma\backslash\mathcal{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$. The (Wohlfahrt) *level* $L(\Gamma)$ is the least common multiple of the cusp widths of Γ [4, Section 4.1]. The group Γ is a *congruence subgroup* if it contains $\Gamma(M)$ for some $M \geq 1$. For a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ we denote by $\pm\Gamma$ the subgroup generated by Γ and $-I$. Finally, $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} \in q\mathbb{Z}[[q]]$ is the discriminant modular form, of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$, which has no zeros on $\mathcal{H}$.

3. Reduction modulo 2 is injective

We first prove some lemmas about abelian varieties with a point of order 2 in the kernel of reduction modulo 2.

Lemma 3.1. *Let A be an abelian variety over $\mathbb{Q}$ with good reduction at 2. If the kernel of the reduction map $A(\mathbb{Q})_{\mathrm{tors}} \to A(\mathbb{F}_2)$ is nontrivial, then it contains a point of order 2.*

Proof. Let m be an odd integer. The group scheme $\mathcal{A}_2[m]$ is finite and étale over $\mathbb{Z}_2$, so by Hensel's lemma the reduction map $\mathcal{A}_2[m](\mathbb{Z}_2) \to \mathcal{A}_2[m](\mathbb{F}_2)$ is injective. Hence the kernel of reduction contains no nonzero points of odd order. Let Q be a nonzero point in the kernel, and write its order as $2^a m$ with m odd. Then $2^a Q$ lies in the kernel and has order m, so $m = 1$, and $a \geq 1$ as $Q \neq 0$. The point $2^{a-1}Q$ has order 2 and lies in the kernel. □

Lemma 3.2. *Let $\mathcal{A}$ be an abelian scheme over $\mathbb{Z}_2$, and let $P \in \mathcal{A}(\mathbb{Z}_2)$ be a point whose generic fibre has order 2 and whose reduction is $0 \in \mathcal{A}(\mathbb{F}_2)$. Then the schematic closure H of $\{0, P_{\mathbb{Q}_2}\}$ in $\mathcal{A}$ is a finite flat subgroup scheme of $\mathcal{A}$ isomorphic to μ_2.*

Proof. The group scheme $\mathcal{A}[2] = \operatorname{Spec} B$ is finite and flat over $\mathbb{Z}_2$, and its generic fibre contains $\{0, P_{\mathbb{Q}_2}\}$. Hence H is a closed subscheme of $\mathcal{A}[2]$, flat over $\mathbb{Z}_2$, and $H = \operatorname{Spec} R$, where R is the image of B in the ring of functions on $\{0, P_{\mathbb{Q}_2}\}$, which we identify with $\mathbb{Q}_2 \times \mathbb{Q}_2$ by evaluation at 0 and at P. Note that H is a subgroup scheme, as the multiplication of $\mathcal{A}[2]$ maps $H \times H$, which is flat over $\mathbb{Z}_2$ and hence the closure of its generic fibre, into H.

Since 0 and P are $\mathbb{Z}_2$-points of $\mathcal{A}[2]$, we have $R \subseteq \mathbb{Z}_2 \times \mathbb{Z}_2$, and $(1,1) \in R$. If $(x,y) \in R$, then $(0, y-x) = (x,y) - x(1,1) \in R$. Hence $R = \mathbb{Z}_2(1,1) \oplus \mathbb{Z}_2 t$, where $t = (0, 2^h)$ and $2^h\mathbb{Z}_2$ is the ideal of second coordinates of the elements of R with first coordinate 0. Since 0 and P have the same reduction, $x \equiv y \pmod 2$ for every $(x,y) \in R$, so $h \geq 1$.

The comultiplication $\Delta\colon R \to R \otimes_{\mathbb{Z}_2} R$ is given by $\Delta(f)(x,y) = f(x+y)$ for $x, y \in \{0, P\}$. The function t takes the value 0 at 0 and 2^h at P, so $\Delta(t)$ takes the values $0, 2^h, 2^h, 0$ at $(0,0), (0,P), (P,0), (P,P)$. The function $t \otimes 1 + 1 \otimes t$ takes the values $0, 2^h, 2^h, 2^{h+1}$, and $t \otimes t$ takes the value 2^{2h} at (P,P) and 0 at the other three points. It follows that

$$\Delta(t) = t \otimes 1 + 1 \otimes t - 2^{1-h}\, t \otimes t.$$

As $R \otimes_{\mathbb{Z}_2} R$ is a free $\mathbb{Z}_2$-module with basis $1 \otimes 1$, $t \otimes 1$, $1 \otimes t$, $t \otimes t$, we obtain $2^{1-h} \in \mathbb{Z}_2$, so $h = 1$. Then $x := 1 - t = (1, -1)$ generates R as a $\mathbb{Z}_2$-algebra and satisfies $x^2 = 1$ and $\Delta(x) = x \otimes x$. Hence $H \simeq \operatorname{Spec} \mathbb{Z}_2[x]/(x^2 - 1) = \mu_2$ as group schemes. □

Lemma 3.3. *Let J be a principally polarized abelian variety over $\mathbb{Q}$ with good reduction at 2, and let $P \in J(\mathbb{Q})$ be a point of order 2 whose reduction in $J(\mathbb{F}_2)$ is 0. Then there exist an abelian variety A over $\mathbb{Q}$ and isogenies $\varphi\colon A \to J$ and $\psi\colon J \to A$ over $\mathbb{Q}$ such that $\deg \varphi = 2$ and $\psi \circ \varphi = [2]$, and such that for every prime ℓ the extension $\varphi_\ell\colon \mathcal{A}_\ell \to \mathcal{J}_\ell$ of φ to the Néron models over $\mathbb{Z}_\ell$ is étale.*

Proof. Let $\lambda\colon J \to J^\vee$ be the principal polarization and put $P' = \lambda(P)$. Let $c\colon J^\vee \to A' := J^\vee/\langle P' \rangle$ be the quotient isogeny, let $A = (A')^\vee$, and let $\varphi\colon A \to J$ be the dual isogeny $c^\vee$, composed with the canonical isomorphism $(J^\vee)^\vee \simeq J$. Then $\deg \varphi = \deg c = 2$, so $\ker \varphi \subseteq A[2]$, and hence there is an isogeny $\psi\colon J \to A$ with $\psi \circ \varphi = [2]$.

Suppose first that $\ell = 2$. The varieties J, $J^\vee$, A and A' are isogenous, so they all have good reduction at 2 and their Néron models over $\mathbb{Z}_2$ are abelian schemes. The polarization λ extends to an isomorphism $\mathcal{J}_2 \to \mathcal{J}_2^\vee$, so P' has order 2 and reduction 0. By Lemma 3.2, the schematic closure H of $\{0, P'\}$ in $\mathcal{J}_2^\vee$ is isomorphic to μ_2. The isogeny c extends to an isogeny $c_2\colon \mathcal{J}_2^\vee \to \mathcal{A}_2'$ of abelian schemes, whose kernel is finite and flat over $\mathbb{Z}_2$ with generic fibre $\{0, P'\}$. As a finite flat scheme over $\mathbb{Z}_2$ is the schematic closure of its generic fibre, $\ker c_2 = H$. The dual abelian scheme of $\mathcal{A}_2'$ is an abelian scheme with generic fibre A, hence equal to $\mathcal{A}_2$, and the dual isogeny $c_2^\vee$ is the extension φ_2 of φ. Its special fibre is the dual of the special fibre of c_2, whose kernel is $H_{\mathbb{F}_2} \simeq \mu_{2,\mathbb{F}_2}$. By [19, Section 15, Theorem 1], the kernel of the special fibre of φ_2 is the Cartier dual of $\mu_{2,\mathbb{F}_2}$, which is the constant group

scheme $\mathbb{Z}/2\mathbb{Z}$ and is étale. The generic fibre of $\ker\varphi_2$ is also étale, so the finite flat group scheme $\ker\varphi_2$ is étale over $\mathbb{Z}_2$ [25, Tag 02GU], and hence the isogeny φ_2 of abelian schemes is étale.

Suppose now that ℓ is odd. By the Néron mapping property, φ and ψ extend to homomorphisms φ_ℓ and ψ_ℓ of Néron models with $\psi_\ell \circ \varphi_\ell = [2]$. Since 2 is invertible in $\mathbb{Z}_\ell$, multiplication by 2 is étale on $\mathcal{A}_\ell$ [2, Section 7.3]. As $\psi_\ell \circ \varphi_\ell$ is étale, φ_ℓ is unramified [25, Tag 02GG]. On each fibre over $\mathbb{Z}_\ell$, φ_ℓ is an unramified morphism between smooth varieties of the same dimension, hence flat [25, Tag 00R4]. Since $\mathcal{A}_\ell$ and $\mathcal{J}_\ell$ are flat over $\mathbb{Z}_\ell$, it follows from the fibrewise criterion of flatness [25, Tag 039B] that φ_ℓ is flat, and hence étale. □

Lemma 3.4. *Let X be a smooth projective geometrically connected curve over $\mathbb{Q}$, let $x_0 \in X(\mathbb{Q})$, let J be the Jacobian of X and $\iota\colon X \to J$, $x \mapsto [x - x_0]$ the Abel-Jacobi map, and let $\varphi\colon A \to J$ be an isogeny of degree 2 of abelian varieties over $\mathbb{Q}$. Then*

$$W := X \times_{\iota,J,\varphi} A$$

is a geometrically connected finite étale cover of X of degree 2, and $w := (x_0, 0) \in W(\mathbb{Q})$.

Proof. As an isogeny in characteristic 0, φ is finite and étale of degree 2, and hence so is its base change $W \to X$. Since $\iota(x_0) = 0 = \varphi(0)$, we have $w \in W(\mathbb{Q})$. Suppose that W is not geometrically connected, so that $W_{\mathbb{C}}$ is not connected. Then $W_{\mathbb{C}}$ is the disjoint union of two copies of $X_{\mathbb{C}}$, so $W_{\mathbb{C}} \to X_{\mathbb{C}}$ has a section. Composing a section with the projection $W \to A$ gives a morphism $g\colon X_{\mathbb{C}} \to A_{\mathbb{C}}$ such that $\varphi \circ g = \iota$. Let $g' = g - g(x_0)$. Then $g'(x_0) = 0$ and $\varphi \circ g' = \iota - \varphi(g(x_0)) = \iota - \iota(x_0) = \iota$. By the universal property of the Jacobian [1, 11.4.1], there is a homomorphism $h\colon J_{\mathbb{C}} \to A_{\mathbb{C}}$ such that $g' = h \circ \iota$. Then $(\varphi \circ h) \circ \iota = \iota$, and by the uniqueness part of the same universal property, $\varphi \circ h$ is the identity of $J_{\mathbb{C}}$. As $\dim A = \dim J$, the homomorphism h is an isogeny, and $1 = \deg(\varphi \circ h) = 2 \deg h$, which is a contradiction. □

Let $N \geq 5$ be an integer, let W be a smooth geometrically connected curve over $\mathbb{Q}$ with a finite étale morphism $W \to X_\mu(N)$, and let $w \in W(\mathbb{Q})$ be a point above ∞. As $W \to X_\mu(N)$ is étale at w and both w and ∞ are rational points, it induces an isomorphism of the completed local rings at ∞ and at w [25, Tags 039H and 039M]. The completed local ring at ∞ is $\mathbb{Q}[[q]]$, so we obtain an embedding

$$\epsilon_w\colon \mathbb{Q}(W) \hookrightarrow \mathbb{Q}((q))$$

extending the q-expansion at ∞, which we call the *q-expansion at w*.

Lemma 3.5. *Let $N \geq 5$ be an integer, let $\iota\colon X_\mu(N) \to J_\mu(N)$ be the Abel-Jacobi map based at ∞, and let $\varphi\colon A \to J_\mu(N)$ be an isogeny of degree 2 over $\mathbb{Q}$ such that for every prime ℓ the extension $\varphi_\ell\colon \mathcal{A}_\ell \to \mathcal{J}_\ell$ of φ to the Néron models over $\mathbb{Z}_\ell$ is étale. Let $W = X_\mu(N) \times_{\iota,J_\mu(N),\varphi} A$ and $w = (\infty, 0) \in W(\mathbb{Q})$. If $z \in \mathbb{Q}(W)$ is integral over $\mathbb{Z}[j]$, then $\epsilon_w(z) \in \mathbb{Z}((q))$.*

Proof. Fix a prime ℓ and let $\mathcal{U} = \mathcal{X}_\mu(N) \otimes \mathbb{Z}_\ell$. By Section 2 a), $\mathcal{U}$ is smooth over $\mathbb{Z}_\ell$ and its generic fibre is an open subscheme of $X_\mu(N)_{\mathbb{Q}_\ell}$ containing ∞. By the Néron mapping property, the restriction of ι to $\mathcal{U}_{\mathbb{Q}_\ell}$ extends to a morphism $\iota_\ell\colon \mathcal{U} \to \mathcal{J}_\ell$. As $\iota(\infty) = 0$, the composition of ι_ℓ with the section $\infty \in \mathcal{U}(\mathbb{Z}_\ell)$ is the zero section. Let

$$\mathcal{V} = \mathcal{U} \times_{\iota_\ell,\mathcal{J}_\ell,\varphi_\ell} \mathcal{A}_\ell.$$

Then $\mathcal{V} \to \mathcal{U}$ is étale, as a base change of φ_ℓ, and $(\infty, 0)$ is a section of $\mathcal{V}$ over $\mathbb{Z}_\ell$ whose generic fibre is w. The generic fibre $\mathcal{V}_{\mathbb{Q}_\ell} = \mathcal{U}_{\mathbb{Q}_\ell} \times_{J_\mu(N)} A$ is an open subscheme of $W_{\mathbb{Q}_\ell}$, which is irreducible by Lemma 3.4.

Let $u \in \mathcal{U}$ and $v \in \mathcal{V}$ be the closed points of the sections ∞ and $(\infty, 0)$, and let $\mathcal{O} = \mathcal{O}_{\mathcal{U},u}$ and $R = \mathcal{O}_{\mathcal{V},v}$. The homomorphism $\mathcal{O} \to R$ is étale and both residue fields are $\mathbb{F}_\ell$, so it induces an isomorphism $\widehat{\mathcal{O}} \to \widehat{R}$ of completions [25, Tags 039H and 039M]. By Section 2 b), $\widehat{\mathcal{O}} = \mathbb{Z}_\ell[[q]]$, and the section ∞ corresponds to the ideal (q). The ring R is a regular local ring, flat over $\mathbb{Z}_\ell$, so it is a domain whose generic point lies in $\mathcal{V}_{\mathbb{Q}_\ell}$, and its field of fractions is the function field $\mathbb{Q}_\ell(W)$ of $W_{\mathbb{Q}_\ell}$. We obtain field embeddings

$$\mathbb{Q}(W) \subseteq \mathbb{Q}_\ell(W) = \mathrm{Frac}(R) \hookrightarrow \mathrm{Frac}(\widehat{R}) = \mathrm{Frac}(\mathbb{Z}_\ell[[q]]) \subseteq \mathbb{Q}_\ell((q)),$$

and we denote their composition by ϵ_ℓ.

We claim that $\epsilon_\ell(f) = \epsilon_w(f)$ for all $f \in \mathbb{Q}(W)$. Let $\mathfrak{p} \subset R$ be the prime ideal of the section $(\infty, 0)$. Then $\mathfrak{p}\widehat{R} = q\mathbb{Z}_\ell[[q]]$, so ϵ_ℓ maps the local ring $\mathcal{O}_{W,w} \subseteq R_\mathfrak{p}$ into the completion $\mathbb{Q}_\ell[[q]]$ of $\mathbb{Z}_\ell[[q]]_{(q)}$, by a local homomorphism. By Section 2 b), the restriction of ϵ_ℓ to $\mathcal{O}_{X_\mu(N),\infty}$ is the q-expansion. The same holds for ϵ_w. Since $\mathcal{O}_{X_\mu(N),\infty} \to \mathcal{O}_{W,w}$ induces an isomorphism of completions, there is at most one local homomorphism $\mathcal{O}_{W,w} \to \mathbb{Q}_\ell[[q]]$ extending the q-expansion on $\mathcal{O}_{X_\mu(N),\infty}$. Hence ϵ_ℓ and ϵ_w agree on $\mathcal{O}_{W,w}$, and so on its field of fractions $\mathbb{Q}(W)$, proving the claim.

Now let $z \in \mathbb{Q}(W)$ be integral over $\mathbb{Z}[j]$. By Section 2 b), $\epsilon_\ell(j) \in q^{-1}\mathbb{Z}[[q]]$, so $\epsilon_\ell(z) \in \mathrm{Frac}(\mathbb{Z}_\ell[[q]])$ is integral over $\mathbb{Z}_\ell((q)) = \mathbb{Z}_\ell[[q]][q^{-1}]$. The ring $\mathbb{Z}_\ell[[q]]$ is regular, hence normal, and so is its localization $\mathbb{Z}_\ell((q))$, whose field of fractions is $\mathrm{Frac}(\mathbb{Z}_\ell[[q]])$. It follows that $\epsilon_\ell(z) \in \mathbb{Z}_\ell((q))$, and by the claim, the coefficients of $\epsilon_w(z) \in \mathbb{Q}((q))$ lie in $\mathbb{Z}_\ell$. As this holds for every prime ℓ, we conclude that $\epsilon_w(z) \in \mathbb{Z}((q))$. □

Lemma 3.6. *Let $N \geq 3$ be an odd integer and let L be a subgroup of index 2 of $\pm\Gamma_1(N)$ containing $-I$ such that every cusp has the same width for L as for $\pm\Gamma_1(N)$. Then L is not a congruence subgroup.*

Proof. The group $\Gamma(N) \subseteq \pm\Gamma_1(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, so $\sigma U^N \sigma^{-1} \in \pm\Gamma_1(N)$ for every $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, and hence every cusp width of $\pm\Gamma_1(N)$ divides N. By assumption the same holds for L, so $L(L)$ divides N. Suppose that L is a congruence subgroup. By Wohlfahrt's theorem [27, Theorem 2], in the form given at the end of the proof of [4, Lemma 4.4.1], every congruence subgroup Γ containing $-I$ contains $\pm\Gamma(L(\Gamma))$. Hence $\pm\Gamma(N) \subseteq \pm\Gamma(L(L)) \subseteq L$. As $N \geq 3$, no element of $-\Gamma(N)$ lies in $\Gamma_1(N)$, so the group $\pm\Gamma_1(N)/\pm\Gamma(N)$ is isomorphic to $\Gamma_1(N)/\Gamma(N)$, which is cyclic of order N (generated by the image of U). Hence $2 = [\pm\Gamma_1(N) : L]$ divides $[\pm\Gamma_1(N) : \pm\Gamma(N)] = N$, which is a contradiction, as N is odd. □

Lemma 3.7. *Let $N \geq 5$ be an odd integer, let $W \to X_\mu(N)$ be a geometrically connected finite étale cover of degree 2, and let $w \in W(\mathbb{Q})$ be a point above ∞. Then there is no $z \in \mathbb{Q}(W) \setminus \mathbb{Q}(X_\mu(N))$ that is integral over $\mathbb{Z}[j]$ and satisfies $\epsilon_w(z) \in \mathbb{Z}((q))$.*

Proof. Suppose the opposite, and let z be such a function. Write $X = X_\mu(N)$ and identify $X(\mathbb{C})$ with $\Gamma_1(N)\backslash\mathcal{H}^*$ as in Section 2 c). Since $N \geq 5$, the group $\pm\Gamma_1(N)/\{\pm I\} \simeq \Gamma_1(N)$ acts freely on $\mathcal{H}$. The cover $W(\mathbb{C}) \to X(\mathbb{C})$ is a connected unramified cover of degree 2, so its restriction to $\Gamma_1(N)\backslash\mathcal{H}$ corresponds to a subgroup L of index 2 of $\pm\Gamma_1(N)$ containing $-I$, and $W(\mathbb{C}) = L\backslash\mathcal{H}^*$. The two points of $W(\mathbb{C})$ above ∞ are interchanged by the nontrivial automorphism of W over X, so we may choose this identification such that w is the cusp ∞ of $L\backslash\mathcal{H}^*$. As $W \to X$ is unramified, the ramification index of $W(\mathbb{C}) \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$ at

every cusp is equal to that of $X(\mathbb{C}) \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$ at its image. Hence every cusp has the same width for L as for $\pm\Gamma_1(N)$. In particular, the cusp ∞ has width 1 for L, so $q = e^{2\pi i\tau}$ is a local parameter at ∞ on $L\backslash\mathcal{H}^*$, and it is the pullback of the parameter q at $\infty \in X(\mathbb{C})$. It follows that the Fourier expansion at ∞ of z, viewed as an L-invariant meromorphic function on $\mathcal{H}$, is $\epsilon_w(z) \in \mathbb{Z}((q))$.

Since z satisfies a monic equation whose coefficients are polynomials in j, and j is holomorphic on $\mathcal{H}$, the function z is holomorphic on $\mathcal{H}$. Choose $m \geq 0$ such that $q^m\epsilon_w(z) \in \mathbb{Z}[[q]]$, and let $F = z\Delta^m$. Then F is holomorphic on $\mathcal{H}$, satisfies $F(\gamma\tau) = (c\tau + d)^{12m}F(\tau)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in L$, is meromorphic at the cusps, and its Fourier expansion at ∞ lies in $\mathbb{Z}[[q]]$, as $\Delta \in q\mathbb{Z}[[q]]$. Note that $\mathbb{Z}[[q]] \subseteq \mathbb{Z}[[e^{\pi i\tau}]]$, which is the normalization used in [4]. By [4, Theorem 1.0.1], F is a modular form for some congruence subgroup Γ'. As Δ^m is a modular form of weight $12m$ for $\mathrm{SL}_2(\mathbb{Z})$ without zeros on $\mathcal{H}$, the function $z = F/\Delta^m$ is invariant under Γ'.

On the other hand, let σ be the nontrivial automorphism of W over X, which is defined over $\mathbb{Q}$ as $W \to X$ is finite étale of degree 2. As $z \notin \mathbb{Q}(X) = \mathbb{Q}(W)^\sigma$, we have $\sigma(z) \neq z$ in $\mathbb{Q}(W) \subseteq \mathbb{C}(W)$. As W is geometrically connected, $W_\mathbb{C} \to X_\mathbb{C}$ is a Galois cover whose Galois group is generated by σ, so $\mathbb{C}(X) = \mathbb{C}(W)^\sigma$, and hence $z \notin \mathbb{C}(X)$. Thus z is not invariant under $\pm\Gamma_1(N)$, and its stabilizer in $\pm\Gamma_1(N)$ is L. It follows that $\Gamma' \cap \pm\Gamma_1(N) \subseteq L$, so L is a congruence subgroup, which contradicts Lemma 3.6. □

Proof of Theorem 1.3. Suppose the opposite. The isomorphism $J_1(N) \simeq J_\mu(N)$ over $\mathbb{Q}$ extends to an isomorphism of Néron models over $\mathbb{Z}_2$, so the kernel of the reduction map $J_\mu(N)(\mathbb{Q})_{\mathrm{tors}} \to J_\mu(N)(\mathbb{F}_2)$ is nontrivial. By Lemma 3.1, it contains a point P of order 2. The Jacobian $J_\mu(N)$ is principally polarized and has good reduction at 2, as N is odd, so by Lemma 3.3 there is an isogeny $\varphi\colon A \to J_\mu(N)$ of degree 2 over $\mathbb{Q}$ such that φ_ℓ is étale for every prime ℓ. Let $\iota\colon X_\mu(N) \to J_\mu(N)$ be the Abel-Jacobi map based at ∞. By Lemma 3.4, $W = X_\mu(N) \times_{\iota, J_\mu(N), \varphi} A$ is a geometrically connected finite étale cover of $X_\mu(N)$ of degree 2, and $w = (\infty, 0) \in W(\mathbb{Q})$.

Let $y \in \mathbb{Q}(W) \setminus \mathbb{Q}(X_\mu(N))$. As $\mathbb{Q}(X_\mu(N))$ is a finite extension of $\mathbb{Q}(j)$, the function y is algebraic over $\mathbb{Q}(j)$. Let $y^n + a_1y^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathbb{Q}(j)$, and let $d \in \mathbb{Z}[j]$ be nonzero with $da_i \in \mathbb{Z}[j]$ for all i. Then $z = dy$ satisfies $z^n + da_1z^{n-1} + \cdots + d^na_n = 0$, so it is integral over $\mathbb{Z}[j]$, and $z \notin \mathbb{Q}(X_\mu(N))$. By Lemma 3.5, $\epsilon_w(z) \in \mathbb{Z}((q))$, which contradicts Lemma 3.7. □

Remark 3.8. The analogue of Theorem 1.3 for $J_0(N)$ is false. For example, $J_0(17)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and the reduction modulo 2 of a generator has order 2 [10, Remark after Proposition 3.4], and $J_0(15)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has order 8, while $\#J_0(15)(\mathbb{F}_2) = 4$ (see Section 6). The step of the proof above that has no analogue for $X_0(N)$ is Lemma 3.6, where we use that $[\pm\Gamma_1(N) : \pm\Gamma(N)] = N$ is odd. The index $[\pm\Gamma_0(15) : \pm\Gamma(15)] = 60$ is even, and so is $[\pm\Gamma_0(p) : \pm\Gamma(p)] = p(p-1)/2$ for a prime $p \equiv 1 \pmod 4$, and $\pm\Gamma_0(17)$ does have a congruence subgroup of index 2 with the same cusp widths, namely the group of matrices in $\pm\Gamma_0(17)$ whose lower right entry is a square modulo 17.

Remark 3.9. One could also try to conclude the proof of Theorem 1.3 using [4, Theorem 7.4.10], which says that the connected component containing the cusp ∞ of the smooth locus of the minimal regular model of the modular curve $X(N)$ over the ring of integers $\mathcal{O}_K$ of a finite extension K of $\mathbb{Q}(\zeta_N)$ has the same algebraic fundamental group as $\operatorname{Spec}\mathcal{O}_K$. The pullback of W to $X(N)$ is geometrically connected, as $[\pm\Gamma_1(N) : \pm\Gamma(N)] = N$ is odd, and one would show, using the Néron mapping property and purity of the branch locus,

that it extends to a finite étale cover of this model, which is impossible. The proof of [4, Theorem 7.4.10] is only sketched in [4], so we have used [4, Theorem 1.0.1] instead.

4. The index of the Eisenstein ideal at 2

In this section we extend Ohta's computation of the index of the Eisenstein ideal [22, Theorem 2.4.2] to the prime 2. We use the notation of [22, Sections 1 and 2], with $N = p$. The proof of [22, Theorem 2.4.2] uses that the residue characteristic is odd only to show that the constant terms $-B_{2,\chi}/4$ of the Eisenstein series $E_{2,\chi}$ of [22, (2.1.3)] are integral, at the beginning of the proof and at the end of the proof of [22, Lemma 2.4.6]. The following lemma takes care of both places.

Lemma 4.1. *Let $p \geq 5$ be a prime and let χ be a nontrivial even Dirichlet character modulo p. Then*

$$\frac{B_{2,\chi}}{4} = \sum_{a=1}^{(p-1)/2} \beta(a)\chi(a), \qquad \text{where} \qquad \beta(a) = \frac{a(a-p)}{2p} \in \frac{1}{p}\mathbb{Z}.$$

Proof. By [22, (2.1.5)] (see also [26, Exercise 4.2]), $B_{2,\chi} = \frac{1}{p}\sum_{a=1}^{p} \chi(a)a^2$. As $\chi(p) = 0$ and $\chi(p-a) = \chi(a)$, grouping the terms for a and $p-a$ gives

$$B_{2,\chi} = \frac{1}{p}\sum_{a=1}^{(p-1)/2} \chi(a)\left(a^2 + (p-a)^2\right) = \frac{1}{p}\sum_{a=1}^{(p-1)/2} \chi(a)\left(2a(a-p) + p^2\right).$$

Since χ is even and nontrivial, $\sum_{a=1}^{(p-1)/2} \chi(a) = \frac{1}{2}\sum_{a=1}^{p-1} \chi(a) = 0$, so

$$B_{2,\chi} = \frac{2}{p}\sum_{a=1}^{(p-1)/2} \chi(a)a(a-p),$$

which is the claimed formula. Since p is odd, exactly one of a and $a-p$ is even, so $\beta(a) \in \frac{1}{p}\mathbb{Z}$. □

Proposition 4.2. *Let $p \geq 5$ be a prime and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_2$. Then*

$$|h_2(\Gamma_1(p); \mathcal{O}) : I_{\infty,\mathcal{O}}| = |\mathcal{O} : c(p)\mathcal{O}|.$$

In particular, $|\mathbb{T}/I| = 2^{v_2(c(p))} = |C_1(p)[2^\infty]|$.

Proof. Ohta proves the first statement for the ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_\ell$, where $\ell \neq 2, p$ [22, Theorem 2.4.2]. We go through his proof for $\ell = 2$. Note that $c(p) \neq 0$ by (1.1). The results of [22, Sections 1 and 2.1–2.3] that the proof uses, namely [22, Corollary 1.3.6, Remark 1.3.8, Proposition 2.1.13, Corollary 2.1.14, Corollary 2.2.7, Proposition 2.2.8, Proposition 2.3.4 and Proposition 2.3.6], are stated and proved for all $\mathbb{Z}[1/p]$-algebras, all integral domains of characteristic 0, all principal ideal domains, or all rings of integers of finite extensions of $\mathbb{Q}_\ell$ with $\ell \neq p$, so they hold for $\ell = 2$. In particular, by [22, Proposition 2.3.6], the group $h_2(\Gamma_1(p); \mathcal{O})/I_{\infty,\mathcal{O}}$ is isomorphic to the congruence module attached to the exact sequence

$$0 \to S_2(\Gamma_1(p); \mathcal{O}) \to M_2^\infty(\Gamma_1(p); \mathcal{O}) \xrightarrow{\text{Res}} \mathcal{O}[C_\infty]^0 \to 0$$

of [22, (2.3.5)] and its splitting over the field of fractions of $\mathcal{O}$. As in [22, Section 2.4], since the formation of congruence modules commutes with flat extensions, we may assume that $\mathcal{O}$ contains the values of all characters of G.

As explained above, Ohta's computation of the order of this congruence module in [22, Section 2.4] uses that ℓ is odd at two places, and we now show that both remain valid for $\ell = 2$. First, [22, Lemma 2.4.6] and the definition of the lattice L_2 before it require that the Eisenstein series $E_{2,\chi}$ lie in $M_2^\infty(\Gamma_1(p);\mathcal{O})$. By [22, (2.1.3)] the q-expansion of $E_{2,\chi}$ is

$$-\frac{B_{2,\chi}}{4} + \sum_{n\geq 1}\Big(\sum_{0<t|n}\chi(t)t\Big)q^n,$$

which lies in $\mathcal{O}[[q]]$ by Lemma 4.1, as $\beta(a) \in \frac{1}{p}\mathbb{Z} \subseteq \mathcal{O}$. Hence $E_{2,\chi} \in M_2^\infty(\Gamma_1(p);\mathcal{O})$ by the q-expansion principle [22, Proposition 1.1.10]. Second, at the end of the proof of [22, Lemma 2.4.6] it is shown that condition (iii) there implies condition (i). Let χ_0 be a generator of the character group of G, let $r = (p-3)/2$, and suppose that $x_1, \dots, x_r$ satisfy condition (iii), i.e. that

$$v(a) := \sum_{i=1}^{r} x_i \chi_0^i(a) \in \mathcal{O} \qquad \text{for all } a \in G.$$

Then by Lemma 4.1,

$$\sum_{i=1}^{r} x_i \frac{B_{2,\chi_0^i}}{4} = \sum_{i=1}^{r} x_i \sum_{a=1}^{(p-1)/2} \beta(a)\chi_0^i(a) = \sum_{a=1}^{(p-1)/2} \beta(a)v(a) \in \mathcal{O},$$

which is condition (i). The other parts of the proof of [22, Lemma 2.4.6] use an auxiliary prime different from p and from the residue characteristic, which exists for $\ell = 2$ as well, and [22, Lemmas 2.4.8 and 2.4.9] only use that p is invertible in $\mathcal{O}$. The conclusion $|h_2(\Gamma_1(p);\mathcal{O}) : I_{\infty,\mathcal{O}}| = |\mathcal{O} : c(p)\mathcal{O}|$ now follows as in [22, proof of Theorem 2.4.2].

For the last statement, take $\mathcal{O} = \mathbb{Z}_2$. Then $h_2(\Gamma_1(p);\mathbb{Z}_2) = \mathbb{T}$ and $I_{\infty,\mathbb{Z}_2} = I$, so $|\mathbb{T}/I| = |\mathbb{Z}_2 : c(p)\mathbb{Z}_2| = 2^{v_2(c(p))}$, which is equal to $|C_1(p)[2^\infty]|$ by (1.1). □

5. Proof of Theorem 1.2

Lemma 5.1. *Let $p \geq 5$ be a prime. Then the Eisenstein ideal I annihilates $J_1(p)(\mathbb{Q})[2^\infty]$.*

Proof. By [22, Corollary 2.1.14], I is generated by τ and the elements η_ℓ, for primes $\ell \neq p$. The element τ annihilates $J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ by [22, Lemmas 3.1.5 and 3.1.6], and for every odd prime $\ell \neq p$, the element η_ℓ annihilates $J_1(p)(\mathbb{Q})[2^\infty]$ by [22, Remark 3.1.4]. It remains to show that η_2 annihilates $J_1(p)(\mathbb{Q})[2^\infty]$.

By (2.1), $T_2 = \mathrm{Frob}_2 + \langle 2\rangle \mathrm{Ver}_2$ on the special fibre of the Néron model of $J_1(p)$ over $\mathbb{Z}_2$. The Frobenius Frob_2 acts trivially on $J_1(p)(\mathbb{F}_2)$, and since $\mathrm{Ver}_2 \circ \mathrm{Frob}_2 = [2]$, the Verschiebung Ver_2 acts on $J_1(p)(\mathbb{F}_2)$ as multiplication by 2. Hence $\eta_2 = T_2 - 1 - 2\langle 2\rangle$ annihilates $J_1(p)(\mathbb{F}_2)$. Let $P \in J_1(p)(\mathbb{Q})[2^\infty]$. As η_2 commutes with the reduction map, $\eta_2(P) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ reduces to 0 in $J_1(p)(\mathbb{F}_2)$, and so $\eta_2(P) = 0$ by Theorem 1.3. □

The following lemma is the analogue at 2 of [22, Lemma 3.2.6], and its proof follows Ohta's. Instead of the isomorphism of Cartier and Serre we use Cartier duality, which makes the compatibility with all the Hecke operators, including T_2, transparent.

Lemma 5.2. *Let $p \geq 5$ be a prime, let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ and $\kappa = \mathbb{T}/\mathfrak{m}$, and let B be the special fibre of the Néron model of $J_1(p)$ over $\mathbb{Z}_2$. Then* $\dim_\kappa B(\overline{\mathbb{F}}_2)[\mathfrak{m}] \leq 1$.

Proof. Let $k = \overline{\mathbb{F}}_2$, and denote the base change of B to k also by B. As $\mathbb{T}$ is finite over $\mathbb{Z}_2$, we have $2 \in \mathfrak{m}$, so $B(k)[\mathfrak{m}] \subseteq B(k)[2]$. For a commutative group scheme D over k we denote by ω_D its cotangent space at the origin.

Let $B^\vee$ be the dual abelian variety of B. Applying [19, Section 15, Theorem 1] to multiplication by 2, whose dual is multiplication by 2 on $B^\vee$, we see that $B^\vee[2]$ is canonically the Cartier dual of $B[2]$. Let $e_2\colon B[2] \times B^\vee[2] \to \mu_2$ be the corresponding pairing. It follows from the construction of this duality that $e_2(uP, Q) = e_2(P, u^\vee Q)$ for every endomorphism u of B. For $P \in B[2](k)$ let $\chi_P = e_2(P, \cdot)\colon B^\vee[2] \to \mu_2$. Let s be the coordinate on $\mu_2 = \operatorname{Spec} k[s]/(s^2 - 1)$, and define

$$\iota\colon B[2](k) \otimes_{\mathbb{F}_2} k \to \omega_{B^\vee[2]}, \qquad P \otimes c \mapsto c\, \chi_P^*(ds/s).$$

This is well defined, as $\chi_{P+Q} = \chi_P \chi_Q$ and the pullback of the invariant differential ds/s by a product of two homomorphisms to μ_2 is the sum of the two pullbacks. We claim that ι is injective. As k is perfect, the reduced subgroup scheme of $B[2]$ is a direct factor of $B[2]$, and it is the constant group scheme $(\mathbb{Z}/2\mathbb{Z})^r$, where $r = \dim_{\mathbb{F}_2} B[2](k)$. Dually, μ_2^r is a direct factor of $B^\vee[2]$, and if $P_1, \dots, P_r$ is a basis of $B[2](k)$, then $\chi_{P_1}, \dots, \chi_{P_r}$ are the compositions of the projection $B^\vee[2] \to \mu_2^r$ with the r coordinate projections. The differentials ds_i/s_i form a basis of $\omega_{\mu_2^r}$, and pullback by a projection onto a direct factor is injective on cotangent spaces, so ι is injective. Note also that the tangent space of $B^\vee[2]$ is the kernel of the differential of $[2]$ on the tangent space of $B^\vee$, and this differential is 0, so restriction gives an isomorphism $\omega_{B^\vee} \simeq \omega_{B^\vee[2]}$.

Let $\lambda\colon B \to B^\vee$ be the principal polarization, i.e. the reduction of the canonical polarization of $J_1(p)$, and for an endomorphism u of B let $u^\dagger = \lambda^{-1} u^\vee \lambda$ be its Rosati transpose. Composing ι with the isomorphism $\omega_{B^\vee[2]} \simeq \omega_{B^\vee}$ and with $\lambda^*\colon \omega_{B^\vee} \to \omega_B$, we obtain an injection $\iota_B\colon B[2](k) \otimes_{\mathbb{F}_2} k \hookrightarrow \omega_B$. Since $\chi_{uP} = \chi_P \circ u^\vee$ and $u^\vee \lambda = \lambda u^\dagger$, it satisfies

$$\iota_B(uP) = (u^\dagger)^* \iota_B(P) \qquad \text{for every endomorphism } u \text{ of } B. \tag{5.1}$$

We now identify ω_B with a space of cusp forms. Fix a primitive p-th root of unity ζ in k, and the corresponding isomorphism $\mathbb{Z}/p\mathbb{Z} \simeq \mu_p$ over k. It identifies $X_1(p)_k$ with $X_\mu(p)_k$, compatibly with the diamond and Hecke operators [22, Section 3.1]. Hence $\omega_B = H^0(X_\mu(p)_k, \Omega^1) = S_2(\Gamma_1(p); k)$ [22, Definition 1.1.7 and Proposition 1.1.8], and $t \in \mathbb{T}$ acts on $S_2(\Gamma_1(p); k)$ as the pullback t^* by the corresponding endomorphism of B. This holds over $\mathbb{Q}$ by [22, Section 1.2], the space $S_2(\Gamma_1(p); \mathbb{Z}_2) = H^0(X_\mu(p)_{\mathbb{Z}_2}, \Omega^1)$ is the cotangent space at the origin of the Néron model of $J_\mu(p)$ over $\mathbb{Z}_2$, to which these endomorphisms extend, and the statement over k follows by base change. Note that this description of the action of T_2 on $S_2(\Gamma_1(p); k)$ does not use the Hecke correspondence in characteristic 2.

Finally, we compare $t^\dagger$ with t. Let $w = w_\zeta$ be the involution of [22, (1.2.6)], which is defined over $\mathbb{Q}(\zeta_p)^+$, and denote by the same symbol the automorphisms it induces on $J_\mu(p)$ and on B. The Rosati involution of the canonical polarization of a Jacobian maps the endomorphism induced by a correspondence to the endomorphism induced by the transposed correspondence [1, Proposition 11.5.3]. The transpose of $\langle a \rangle$ is $\langle a \rangle^{-1}$. For a prime $\ell \neq p$, the transpose of T_ℓ is $\langle \ell \rangle^{-1} T_\ell$, since for an isogeny $\phi\colon E \to E/C$ of degree ℓ and $\alpha\colon \mu_p \hookrightarrow E$ we have $\widehat{\phi} \circ \phi \circ \alpha = \ell\alpha$. Comparing with [22, (1.2.7)], we get $t^\dagger = w^{-1} t w$ for $t = \langle a \rangle$ and for $t = T_\ell$ with $\ell \neq p$, as endomorphisms of $J_\mu(p)$ over $\mathbb{Q}(\zeta_p)$. As $h_2(\Gamma_1(p); \mathbb{Z})$ is commutative, both $t \mapsto t^\dagger$ and $t \mapsto w^{-1} t w$ are ring homomorphisms from $h_2(\Gamma_1(p); \mathbb{Z}[1/p])$ to $\operatorname{End}(J_\mu(p)_{\mathbb{Q}(\zeta_p)}) \otimes \mathbb{Z}[1/p]$, and $h_2(\Gamma_1(p); \mathbb{Z}[1/p])$ is generated over $\mathbb{Z}[1/p]$ by the $\langle a \rangle$ and the T_ℓ with $\ell \neq p$ [22, Remark 1.3.8(3)]. Hence $t^\dagger = w^{-1} t w$ for all $t \in h_2(\Gamma_1(p); \mathbb{Z})$, in

particular for T_2 and T_p, and these identities between endomorphisms of $J_\mu(p)$ also hold for their reductions on B. By (5.1), $\iota_B(tP) = (w^{-1}tw)^*\iota_B(P) = w^*t^*(w^{-1})^*\iota_B(P)$, so $\iota' := (w^{-1})^* \circ \iota_B$ satisfies $\iota'(tP) = t^*\iota'(P)$ for all $t \in \mathbb{T}$. Restricting ι' to the $\mathfrak{m}$-torsion, we obtain an injective homomorphism of $\mathbb{T}$-modules

$$B(k)[\mathfrak{m}] \otimes_{\mathbb{F}_2} k \hookrightarrow S_2(\Gamma_1(p); k)[\mathfrak{m}] = S_2(\Gamma_1(p); \mathbb{F}_2)[\mathfrak{m}] \otimes_{\mathbb{F}_2} k.$$

Here $\mathbb{T}$ acts on $S_2(\Gamma_1(p); \mathbb{F}_2)$ through $\mathbb{T}/2\mathbb{T} = h_2(\Gamma_1(p); \mathbb{F}_2)$ [22, Remark 1.3.8(1)]. By the perfect pairing

$$S_2(\Gamma_1(p); \mathbb{F}_2) \times h_2(\Gamma_1(p); \mathbb{F}_2) \to \mathbb{F}_2, \qquad (f, t) \mapsto a(1; f|t)$$

of [22, Remark 1.3.8(2)], the space $S_2(\Gamma_1(p); \mathbb{F}_2)[\mathfrak{m}]$ is isomorphic to $\mathrm{Hom}_{\mathbb{F}_2}(\kappa, \mathbb{F}_2)$, which has dimension $[\kappa : \mathbb{F}_2]$ over $\mathbb{F}_2$. It follows that $\dim_{\mathbb{F}_2} B(k)[\mathfrak{m}] \leq [\kappa : \mathbb{F}_2]$, i.e. $\dim_\kappa B(k)[\mathfrak{m}] \leq 1$. □

Proof of Theorem 1.2. By [22, Theorem I], $J_1(p)(\mathbb{Q})[\ell^\infty] = C_1(p)[\ell^\infty]$ for every odd prime ℓ, so it suffices to show that $M := J_1(p)(\mathbb{Q})[2^\infty]$ is equal to $C_1(p)[2^\infty]$. As $C_1(p)[2^\infty] \subseteq M$, it suffices to show that $|M| \leq |C_1(p)[2^\infty]|$.

The group M is a finite $\mathbb{T}$-module, and it is annihilated by I by Lemma 5.1. As $\mathbb{T}$ is finite over $\mathbb{Z}_2$, we have $\mathbb{T} = \prod_{\mathfrak{m}} \mathbb{T}_{\mathfrak{m}}$ and $M = \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$, where $\mathfrak{m}$ runs through the maximal ideals of $\mathbb{T}$. Fix $\mathfrak{m}$, let $\kappa = \mathbb{T}/\mathfrak{m}$, and let $D = \mathrm{Hom}(M_{\mathfrak{m}}, \mathbb{Q}_2/\mathbb{Z}_2)$ be the Pontryagin dual of $M_{\mathfrak{m}}$, which is a $\mathbb{T}_{\mathfrak{m}}$-module annihilated by $I\mathbb{T}_{\mathfrak{m}}$, with $|D| = |M_{\mathfrak{m}}|$. The reduction map is injective by Theorem 1.3 and commutes with the action of $\mathbb{T}$, so it embeds $M_{\mathfrak{m}}[\mathfrak{m}]$ into $B(\overline{\mathbb{F}}_2)[\mathfrak{m}]$, where B is as in Lemma 5.2. By Lemma 5.2, $\dim_\kappa M_{\mathfrak{m}}[\mathfrak{m}] \leq 1$. The κ-vector space $D/\mathfrak{m}D$ is dual to $M_{\mathfrak{m}}[\mathfrak{m}]$, so it has dimension at most 1, and by Nakayama's lemma D is a cyclic $\mathbb{T}_{\mathfrak{m}}$-module. As D is annihilated by $I\mathbb{T}_{\mathfrak{m}}$, it is a quotient of $\mathbb{T}_{\mathfrak{m}}/I\mathbb{T}_{\mathfrak{m}}$, so $|M_{\mathfrak{m}}| = |D| \leq |\mathbb{T}_{\mathfrak{m}}/I\mathbb{T}_{\mathfrak{m}}|$. Taking the product over all $\mathfrak{m}$ and using Proposition 4.2, we obtain

$$|M| \leq |\mathbb{T}/I| = |C_1(p)[2^\infty]|,$$

completing the proof. □

Corollary 5.3. *Let $p \geq 5$ be a prime. Then $J_1(p)(\mathbb{Q})[2^\infty] \simeq \mathbb{T}/I$ as $\mathbb{T}$-modules. In particular, I is the annihilator of $J_1(p)(\mathbb{Q})[2^\infty]$ in $\mathbb{T}$.*

Proof. The group G acts simply transitively on the rational cusps of $X_1(p)$ through the diamond operators (see [22, (1.2.9)]). Let c be a rational cusp and g a generator of G. Then the group of divisors of degree 0 supported on the rational cusps is isomorphic, as a $\mathbb{Z}[G]$-module, to the augmentation ideal of $\mathbb{Z}[G]$, so it is generated as a $\mathbb{Z}[G]$-module by $\langle g\rangle c - c$, as G is cyclic (see also [22, proof of Proposition 3.2.7]). The map from divisors to $J_1(p)$ commutes with the diamond operators, so $C_1(p)$ is generated as a $\mathbb{Z}[G]$-module by the class of $\langle g\rangle c - c$, where G acts on $J_1(p)$ through the diamond operators. As the diamond operators lie in $h_2(\Gamma_1(p); \mathbb{Z})$, it follows that $C_1(p)[2^\infty]$ is a cyclic $\mathbb{T}$-module, and as it is annihilated by I (Lemma 5.1), it is a quotient of $\mathbb{T}/I$. These two groups have the same order by Proposition 4.2, so $C_1(p)[2^\infty] \simeq \mathbb{T}/I$, and $C_1(p)[2^\infty] = J_1(p)(\mathbb{Q})[2^\infty]$ by Theorem 1.2. □

6. Numerical checks

The proofs above do not use computer calculations. In this section we describe the computations we did to test Theorem 1.3, Proposition 4.2 and our conventions in small cases. As Conjecture 1.1 was already known for $p \leq 157$, these computations do not prove

anything new. We used Magma [3]. For integers $a_1, \dots, a_k$ we write $(a_1, \dots, a_k)$ for the group $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}$, and an exponent denotes repetition, so that $(2^3) = (2, 2, 2)$.

By Theorem 1.3 and Theorem 1.2, the reduction map embeds $C_1(p)$ into $J_1(p)(\mathbb{F}_2)$, so $c(p)$ divides $\#J_1(p)(\mathbb{F}_2)$ and

$$\dim_{\mathbb{F}_2} C_1(p)[2] \leq \dim_{\mathbb{F}_2} J_1(p)(\mathbb{F}_2)[2].$$

To compute $c(p)$ we use Lemma 4.1. Let $n = (p-1)/2$, let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, and extend β to G by $\beta(\pm a) = \beta(a)$ for $1 \leq a \leq n$. Then $|c(p)| = p \,|\, \mathrm{Res}(\Phi, F)|$, where $\Phi = (x^n - 1)/(x - 1)$ and $F = \sum_{i=0}^{n-1} \beta(g^i)x^i$. We compute $\#J_1(p)(\mathbb{F}_2)$ using the Eichler-Shimura relation, as the product, over the Galois orbits of even Dirichlet characters ε modulo p, of the norms of $\det(1 + 2\varepsilon(2) - T_2)$ on $S_2(\Gamma_0(p), \varepsilon)$. We compute T_2 on the cuspidal subspace of the sign $+1$ quotient of the space of modular symbols of weight 2 and character ε, which is isomorphic to $S_2(\Gamma_0(p), \varepsilon)$ as a Hecke module (the full space of cuspidal modular symbols has twice the dimension, and would give the square of $\#J_1(p)(\mathbb{F}_2)$). For all primes $11 \leq p \leq 139$ we compute that $c(p)$ divides $\#J_1(p)(\mathbb{F}_2)$ [`orders.m`, Claim 1]. The primes p in this range for which $c(p)$ is even are listed in Table 1, where $N_2 := \#J_1(p)(\mathbb{F}_2)$ and $d_2 := \dim_{\mathbb{F}_2} J_1(p)(\mathbb{F}_2)[2]$ [`orders.m`, Claim 2].

We also compute d_2 for the primes in Table 1 [`two_rank.m`, Claim 3]. The isomorphism of Cartier and Serre [24, Proposition 10], which sends the class of a divisor D with $2D = \mathrm{div}(f)$ to df/f, identifies $J_1(p)(\mathbb{F}_2)[2]$ with the space of regular differentials on $X_\mu(p)_{\mathbb{F}_2}$ that are defined over $\mathbb{F}_2$ and fixed by the Cartier operator. On q-expansions at ∞, the Cartier operator on $S_2(\Gamma_1(p); \mathbb{F}_2)$ is $U_2 \colon \sum a_k q^k \mapsto \sum a_{2k} q^k$, so $J_1(p)(\mathbb{F}_2)[2]$ is isomorphic to the kernel of $U_2 - 1$ on $S_2(\Gamma_1(p); \mathbb{F}_2)$. We compute $S_2(\Gamma_1(p); \mathbb{Z})$ as the lattice of cusp forms with integral q-expansions, reduce it modulo 2, and compute the matrix of U_2 from the q-expansions up to twice the Sturm bound.

Finally, we compute the congruence module of Proposition 4.2 directly. For $f = \sum_\chi x_\chi E_{2,\chi}$, where χ runs through the nontrivial characters of G, put $v(d) = \sum_\chi x_\chi \chi(d)$ for $d \in G$, so that $\sum_{d \in G} v(d) = 0$. By [22, Proposition 2.2.8] and Lemma 4.1, the residue of f is

$$\begin{aligned} \mathrm{Res}(f) &= -\sum_{a \in G} \Big(\sum_{c \in G} \beta(c) v(ac) \Big) [a^{-1}]_\infty \\ &= \sum_{i=1}^{n-1} \Big(\sum_{j=1}^{n-1} H_{ij} v(g^j) \Big) \big([g^{-i}]_\infty - [1]_\infty \big), \end{aligned}$$

where $H_{ij} = \beta(g^{-i}) - \beta(g^{j-i})$, and by [22, Lemma 2.4.6] (see the proof of Proposition 4.2) f lies in the lattice L_1 of [22, (2.4.3)] if and only if all $v(d)$ are integral. It follows that the congruence module of Proposition 4.2 is isomorphic to the cokernel of H over $\mathcal{O}$ (first for $\mathcal{O}$ containing the values of the characters of G, and then, by flat base change, for $\mathcal{O} = \mathbb{Z}_2$). For $\mathcal{O} = \mathbb{Z}_2$ this cokernel is isomorphic to $\mathbb{T}/I$ by [22, Proposition 2.3.6], and hence to $J_1(p)(\mathbb{Q})[2^\infty]$ by Corollary 5.3. We compute the 2-primary part of the cokernel of pH for the primes in Table 1 [`congruence_module.m`, Claim 4]. For $p \leq 113$ it agrees with the group $J_1(p)(\mathbb{Q})[2^\infty]$ determined by De Leo and Stoll [8, Table 4.5] [`congruence_module.m`, Claim 5].

In all cases in Table 1, the 2-rank of $\mathrm{coker}(H) \otimes \mathbb{Z}_2$ is at most $\dim_{\mathbb{F}_2} J_1(p)(\mathbb{F}_2)[2]$, as it must be by Theorem 1.3 and Corollary 5.3. For $p \in \{17, 31, 43, 73, 97, 127\}$ we have $v_2(c(p)) = v_2(\#J_1(p)(\mathbb{F}_2))$, so Theorem 1.3 and Theorem 1.2 imply that the reduction map induces an

TABLE 1. The primes $11 \leq p \leq 139$ for which $c(p)$ is even.

p	$v_2(c(p))$	$v_2(N_2)$	d_2	$\operatorname{coker}(H) \otimes \mathbb{Z}_2$	$J_1(p)(\mathbb{Q})[2^\infty]$ [8]
17	3	3	1	(8)	(8)
29	6	8	5	(4^3)	(4^3)
31	2	2	2	(2^2)	(2^2)
41	4	8	2	(16)	(16)
43	2	2	2	(2^2)	(2^2)
73	3	3	3	(2^3)	(2^3)
89	3	11	5	(2^3)	(2^3)
97	4	4	1	(16)	(16)
109	4	10	6	(4^2)	(4^2)
113	20	32	9	$(4^2, 16^4)$	$(4^2, 16^4)$
127	8	8	8	(2^8)	
137	5	10	2	(32)	

isomorphism $C_1(p)[2^\infty] \simeq J_1(p)(\mathbb{F}_2)[2^\infty]$. In these cases the 2-rank of $J_1(p)(\mathbb{F}_2)$ is equal to the 2-rank of $\operatorname{coker}(H) \otimes \mathbb{Z}_2$. For example, for $p = 73$ the group $J_1(73)(\mathbb{F}_2)[2^\infty]$ has order 8 and 2-rank 3, which is the smallest 2-rank allowed by Theorem 1.3, as $J_1(73)(\mathbb{Q})[2^\infty] \simeq (2^3)$. For $p = 127$, which is outside the range of [8, Table 4.5], the group $J_1(127)(\mathbb{F}_2)[2^\infty]$ has order 2^8 and 2-rank 8, so it is isomorphic to (2^8), in agreement with $\operatorname{coker}(H) \otimes \mathbb{Z}_2$.

We also test Theorem 1.3 at the composite level $N = 15$. The curve $X_1(15)$ has genus 1 and rational points (its rational cusps), so $J_1(15)$ is isomorphic to $X_1(15)$. Using the Tate normal form $y^2 + (1-c)xy - by = x^3 - bx^2$ of an elliptic curve with the point $(0, 0)$ of order 15, we compute that $X_1(15)$ is isomorphic to the elliptic curve with Cremona label 15a8 [7], that $J_1(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and $J_1(15)(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$, and that the reduction map $J_1(15)(\mathbb{Q}) \to J_1(15)(\mathbb{F}_2)$ is injective, and hence an isomorphism [`level15.m`, Claim 6]. For each of the other seven elliptic curves E in the isogeny class of 15a8, the reduction map $E(\mathbb{Q})_{\mathrm{tors}} \to E(\mathbb{F}_2)$ is not injective. One of them is $J_0(15)$, which is 15a1, and $J_0(15)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has order 8, while $\#J_0(15)(\mathbb{F}_2) = 4$ [`level15.m`, Claim 7]. Thus $J_1(15)$ is the only elliptic curve in its isogeny class whose rational torsion injects into its group of $\mathbb{F}_2$-points.

All computations were done with Magma V2.30-1 on the *Mordell* server at the Department of Mathematics, University of Zagreb (AMD EPYC 9175F, 384 GB of RAM). The computations of d_2 for the primes in Table 1 took about 13 minutes of CPU time, about 6 minutes of which for $p = 137$, and the other computations a few seconds.

REFERENCES

[1] C. BIRKENHAKE AND H. LANGE, *Complex abelian varieties*, vol. 302 of Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin, second ed., 2004. 3, 5

[2] S. BOSCH, W. LÜTKEBOHMERT, AND M. RAYNAUD, *Néron models*, vol. 21 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Springer-Verlag, Berlin, 1990. 2, 3

[3] W. BOSMA, J. CANNON, AND C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. 6

[4] F. CALEGARI, V. DIMITROV, AND Y. TANG, *The unbounded denominators conjecture*, J. Amer. Math. Soc., 38 (2025), pp. 627–702. 1, 2, 3, 3, 3.9

[5] Z. Chi, S. Liu, and P. Nie, *On the Manin constant*. preprint, https://arxiv.org/abs/2610.25672v2, 2026. 1, 2
[6] B. Conrad, B. Edixhoven, and W. Stein, $J_1(p)$ *has connected fibers*, Doc. Math., 8 (2003), pp. 331–408. 1.1, 1, 1, 2
[7] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, second ed., 1997. 6
[8] D. De Leo and M. Stoll, *On some open cases of a conjecture of Conrad, Edixhoven and Stein*, Int. J. Number Theory, (2026). https://doi.org/10.1142/S1793042126501447, https://arxiv.org/abs/2505.10777. 1, 6, 1, 6
[9] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), vol. 349 of Lecture Notes in Math., Springer, Berlin, 1973, pp. 143–316. 2
[10] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, Algebra Number Theory, 17 (2023), pp. 267–308. 1, 1, 3.8
[11] F. Diamond and J. Im, *Modular forms and modular curves*, in Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), vol. 17 of CMS Conf. Proc., Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. 2
[12] F. Diamond and J. Shurman, *A first course in modular forms*, vol. 228 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2005. 2
[13] V. G. Drinfel'd, *Two theorems on modular curves*, Funkcional. Anal. i Priložen., 7 (1973), pp. 83–84. 1
[14] S. Kamienny, *On torsion in* $J_1(N)$, Acta Arith., 120 (2005), pp. 185–190. 1
[15] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, vol. 108 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1985. 2
[16] D. S. Kubert and S. Lang, *Modular units*, vol. 244 of Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin-New York, 1981. 1
[17] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat., 36 (1972), pp. 19–66. 1
[18] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., (1977), pp. 33–186. 1
[19] D. Mumford, *Abelian varieties*, vol. 5 of Tata Institute of Fundamental Research Studies in Mathematics, Oxford University Press, London, 1970. 3, 5
[20] A. P. Ogg, *Rational points on certain elliptic modular curves*, in Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, RI, 1973, pp. 221–231. 1, 1
[21] ———, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc., 81 (1975), pp. 14–27. 1
[22] M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties*, J. Math. Soc. Japan, 65 (2013), pp. 733–772. 1, 1, 1, 2, 2, 4, 4, 4, 5, 5, 5, 6
[23] M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France, 102 (1974), pp. 241–280. 1
[24] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, in Symposium internacional de topología algebraica, Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958, pp. 24–53. 6
[25] The Stacks project authors, *The Stacks project*. https://stacks.math.columbia.edu, 2026. 3, 3, 3
[26] L. C. Washington, *Introduction to cyclotomic fields*, vol. 83 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1997. 4
[27] K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math., 8 (1964), pp. 529–535. 1, 3

University of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr