MODULARITY OF A CERTAIN CALABI-YAU THREEFOLD

Scott Ahlgren and Ken Ono

Abstract. The Langlands program predicts that certain Calabi-Yau threefolds are modular in the sense that their L-series correspond to the Mellin transforms of weight 4 newforms. Here we prove that the L-function of the threefold given by $\sum_{i=1}^{4}(x_i + x_i^{-1}) = 0$ is $\eta^4(2z)\eta^4(4z)$, the unique normalized eigenform in $S_4(\Gamma_0(8))$.

1. Introduction and Statement of Results

In a recent paper [vG-N], van Geemen and Nygaard study the arithmetic of certain threefolds. Among other results, they prove that if the threefold X is the resolution of

$$x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1} + x_4 + x_4^{-1} = 0,$$

then the L-function of the 2-adic Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(H^3(X(\overline{\mathbb{Q}}), \mathbb{Z}_2))$$

is the Hecke L-function associated to the weight 4 newform $\eta^4(2z)\eta^4(4z) \in S_4(\Gamma_0(8))$. Here $\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is the usual Dedekind eta-function and $q := e^{2\pi i z}$. This threefold has also been studied by Verrill (see [V, V2]).

To prove that X is modular, van Geemen and Nygaard employ the Serre-Faltings criterion for determining when two Galois representations are isomorphic. The modularity then follows from checking that enough terms of the two L-series agree. The goal in this paper is to give a direct proof that this threefold is indeed modular. In view of the resolution of singularities (see [vG-N, V, V2]), it suffices to prove:

Theorem 1. *If p is prime, then define $N(p)$ by*

$$N(p) := \#\left\{(x_1, x_2, x_3, x_4) \in (\mathbb{F}_p^{\times})^4 \ : \ x_1 + x_1^{-1} + x_2 + x_2^{-1} + x_3 + x_3^{-1} + x_4 + x_4^{-1} = 0\right\}.$$

If the integers $a(n)$ are defined by

$$\eta^4(2z)\eta^4(4z) = q - 4q^3 - 2q^5 + 24q^7 - 11q^9 - \cdots = \sum_{n=1}^{\infty} a(n)q^n,$$

then for every odd prime p we have

$$a(p) = p^3 - 2p^2 - 7 - N(p).$$

The second author is supported by grants from the NSF and NSA, and he is also supported by an Alfred P. Sloan Foundation Research Fellowship.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

To prove this result we decompose the reduced threefold over each finite field $\mathbb{F}_p$ as a product of elliptic curves in Legendre normal form. After an analysis of the 2-power torsion structure of these curves we use work of Deuring and Schoof to obtain a closed formula for $p^3 - 2p^2 - 7 - N(p)$ in terms of certain orders in imaginary quadratic fields. Via case-by case analysis, we then show that this formula agrees with the value of the trace of the Hecke operator $T(p)$ acting on the space $S_4(\Gamma_0(8))$ which is given by the Eichler-Selberg trace formula. Since this space is one-dimensional, the trace of $T(p)$ is in fact equal to $a(p)$, and our theorem follows.

Remark. In [A-O], the authors show that Theorem 1 leads to a proof of one of Beukers' "Super Congruence" conjectures for Apéry numbers.

2. A formula for $N(p)$ in terms of elliptic curves

If p is an odd prime, then we shall denote by $\mathbb{F}_p$ the finite field with p elements. Let ϕ_p be the quadratic character of $\mathbb{F}_p$ (i.e. the Legendre symbol). To ease notation we will write ϕ for ϕ_p since the prime p will be clear from context. Unless noted otherwise, our sums run over all elements of $\mathbb{F}_p$. We begin with the following fact, whose proof is routine.

Lemma 2.1. *Let p be an odd prime, and suppose that $a \in \mathbb{F}_p$. Then*

$$\sum_x \phi(x^2 + ax) = \sum_x \phi(x^2 + a) = \begin{cases} p - 1 & \text{if } a = 0, \\ -1 & \text{if } a \neq 0. \end{cases}$$

Our goal for the remainder of the section is to obtain a simple formula (Theorem 2 below) for the quantity $p^3 - 2p^2 - 7 - N(p)$. We shall accomplish this goal via a series of lemmas.

Lemma 2.2. *Let $N(p)$ be defined as in Theorem 1. If p is an odd prime, then $N(p) = F(p) + p^3 - 4p^2 + 6p - 4$, where*

$$F(p) := \sum_i \left(\sum_x \phi(x^2 - 1)\phi((x + i)^2 - 1) \right)^2 .$$

Proof. We have

$$N(p) = \sum_a \sum_b \sum_c \#\{x + \tfrac{1}{x} = a\}\#\{y + \tfrac{1}{y} = b\}\#\{z + \tfrac{1}{z} = c\}\#\{w + \tfrac{1}{w} = -a - b - c\}.$$

Notice that $x + 1/x = a$ precisely when $(x - a/2)^2 = a^2/4 - 1$. Therefore

$$\#\{x + \tfrac{1}{x} = a\} = \phi(a^2/4 - 1) + 1 = \phi(a^2 - 4) + 1.$$

Therefore (after replacing a, b, c with $2a$, $2b$, $2c$), we have

$$N(p) = \sum_a \sum_b \sum_c \{\phi(a^2 - 1) + 1\}\{\phi(b^2 - 1) + 1\}\{\phi(c^2 - 1) + 1\}\{\phi((a + b + c)^2 - 1) + 1\}.$$

Replacing c with $c - b$, and subsequently replacing b with $-b$, we find that

$$N(p) = \sum_c \left(\sum_a \{\phi(a^2 - 1) + 1\}\{\phi((a + c)^2 - 1) + 1\} \right)^2 .$$

Expanding and using Lemma 2.1 yields

$$N(p) = \sum_c \left(\sum_a \phi(a^2-1)\phi((a+c)^2-1) + p - 2 \right)^2 .$$

Expanding again and using Lemma 2.1 gives

$$N(p) = F(p) + 2(p-2) + p(p-2)^2 = F(p) + p^3 - 4p^2 + 6p - 4,$$

and Lemma 2.2 is proved. □

Lemma 2.3. *If p is an odd prime, then*

$$p^3 - 2p^2 - 7 - N(p) = p^2 - 3p - 3 - \sum_{i \neq 0,-1} h(i)^2,$$

where

$$h(i) := \sum_x \phi(x)\phi(x-4i-4)\phi(x+i^2). \tag{2.1}$$

Proof of Lemma 2.3. We may write $F(p) = \sum_i f(i)^2$, where

$$f(i) := \sum_x \phi(x^2-1)\phi((x+i)^2-1).$$

Factoring and rearranging, we find that

$$\begin{aligned} f(i) &= \sum_x \phi(x^2+ix-1-i)\phi(x^2+ix-1+i) \\ &= \sum_x \phi((x+\tfrac{i}{2})^2 - (\tfrac{i}{2}+1)^2)\phi((x+\tfrac{i}{2})^2 - (\tfrac{i}{2}-1)^2) \\ &= \sum_x \phi(x^2 - (\tfrac{i}{2}+1)^2)\phi(x^2 - (\tfrac{i}{2}-1)^2). \end{aligned}$$

Replacing i with $2(i+1)$, we obtain $F(p) = \sum_i g(i)^2$, where

$$g(i) := \sum_x \phi(x^2-i^2)\phi(x^2-(i+2)^2).$$

Making the change of variables $y = x^2 - i^2$ gives

$$g(i) = \sum_y \phi(y)\phi(y-4i-4)\{\phi(y+i^2)+1\}.$$

Using Lemma 2.1, we find that

$$g(i) = \begin{cases} h(i) + p - 1 & \text{if } i = -1 \\ h(i) - 1 & \text{if } i \neq -1. \end{cases}$$

Therefore

$$F(p) = \sum_i g(i)^2 = \sum_i \{h(i)-1\}^2 - \{h(-1)-1\}^2 + \{h(-1)+p-1\}^2.$$

It is easy to find that $h(-1) = -1$; from this we obtain

$$F(p) = (p-2)^2 - 4 + \sum_i \{h(i)-1\}^2 = p^2 - 3p + \sum_i h(i)^2 - 2\sum_i h(i). \tag{2.2}$$

Note that $h(0)^2 = h(-1)^2 = 1$. Therefore, in view of the last equation and Lemma 2.2, the proof of Lemma 2.3 will be complete after we prove

Lemma 2.4. *Let $h(i)$ be defined as in* (2.1)*. Then $\sum_i h(i) = 1$.*

Proof of Lemma 2.4. Recall that $h(-1) = -1$. If $i \neq -1$, then we may replace x by $(4i+4)x$ in the definition of $h(i)$ to obtain

$$h(i) = \sum_x \phi(x)\phi(x-1)\phi((4i+4)x + i^2) \quad \text{if} \quad i \neq -1. \tag{2.3}$$

Therefore,

$$\sum_{i\neq -1} h(i) = \sum_{x\neq 0,1} \phi(x^2 - x) \sum_{i\neq -1} \phi(i^2 + (4i+4)x).$$

Since $x \neq 0, 1$, Lemma 2.1 gives

$$\begin{aligned}\sum_{i\neq -1} \phi(i^2 + (4i+4)x) &= \sum_{i\neq -1} \phi((i+2x)^2 - 4x^2 + 4x)\\ &= -1 - \phi((2x-1)^2 - 4x^2 + 4x) = -1 - \phi(1) = -2.\end{aligned}$$

Therefore, using Lemma 2.1, we have

$$\sum_{i\neq -1} h(i) = -2\sum_x \phi(x^2 - x) = 2.$$

Lemma 2.4 (and therefore Lemma 2.3) follows. □

If $\lambda \neq 0$ or 1, then let $E(\lambda)$ denote the Legendre normal form elliptic curve

$$E(\lambda): \quad y^2 = x(x-1)(x-\lambda). \tag{2.4}$$

Moreover, if p is prime and $\lambda \not\equiv 0 \pmod{p}$, then define $N(p,\lambda)$ and $a(p,\lambda)$ by

$$N(p,\lambda) := 1 + \#\{(x,y) \pmod{p} \ : \ y^2 \equiv x(x-1)(x-\lambda) \pmod{p}\}, \tag{2.5}$$

$$a(p,\lambda) := p + 1 - N(p,\lambda) = -\sum_x \phi(x(x-1)(x-\lambda)). \tag{2.6}$$

If $\lambda \not\equiv 0 \pmod{p}$, then it is well known (see [Ch. V, S], [Ch. 13, H]) that there is an algebraic integer $\pi(p,\lambda)$ which lies in an imaginary quadratic field and such that

$$\pi(p,\lambda) + \overline{\pi(p,\lambda)} = a(p,\lambda), \tag{2.7}$$

$$\pi(p,\lambda)\overline{\pi(p,\lambda)} = p. \tag{2.8}$$

Formula (2.7) is the well known expression for the "trace of Frobenius". For the remainder, let $F(x,y)$ denote the polynomial

$$F(x,y) := x^2 + xy + y^2. \tag{2.9}$$

We can now state the main result in this section.

Theorem 2. *If p is an odd prime, then*

$$p^3 - 2p^2 - 7 - N(p) = -4 - \sum_{y=2}^{p-2} F(\pi(p,y^2), \overline{\pi(p,y^2)}).$$

Proof. After Lemma 2.3, we need only to show that

$$\sum_{i \neq 0,-1} h(i)^2 = p^2 - 3p + 1 + \sum_{y=2}^{p-2} F(\pi(p,y^2), \overline{\pi(p,y^2)}). \tag{2.10}$$

It follows immediately from (2.7), (2.8), and (2.9) that

$$a(p,\lambda)^2 = F(\pi(p,\lambda), \overline{\pi(p,\lambda)}) + p, \quad \lambda \in \mathbb{F}_p \setminus \{0,1\}. \tag{2.11}$$

Now, using (2.3), we have

$$\sum_{i \neq 0,-1} h(i)^2 = \sum_{i \neq 0,-1} \left(\sum_{x \neq 0} \phi(x)\phi(x-1)\phi(\tfrac{4i+4}{i^2}x + 1) \right)^2 .$$

Replacing x by $1/x$ and setting $i = 2/(y-1)$ yields

$$\sum_{i \neq 0,-1} h(i)^2 = \sum_{y \neq \pm 1} \left(\sum_{x} \phi(x)\phi(1-x)\phi(x + y^2 - 1) \right)^2 .$$

Then replacing x by $-x+1$ and using (2.6) and (2.11) gives

$$\begin{aligned} \sum_{i \neq 0,-1} h(i)^2 &= \sum_{y \neq \pm 1} \left(\sum_{x} \phi(x)\phi(x-1)\phi(x - y^2) \right)^2 \\ &= 1 + \sum_{y=2}^{p-2} a(p,y^2)^2 = 1 + p(p-3) + \sum_{y=2}^{p-2} F(\pi(p,y^2), \overline{\pi(p,y^2)}). \end{aligned}$$

This establishes (2.10) and therefore proves Theorem 2. □

3. 2-power torsion and a closed formula for $N(p)$

We begin by recalling some basic facts regarding elliptic curves (see [Prop. III.1.7, S], [4 §1, H]).

Proposition 3.1. *Let K be a field with* $\mathrm{char}(K) \neq 2$.

(1) *Every elliptic curve E/K is isomorphic over $\overline{K}$ to an elliptic curve $E(\lambda)$.*

(2) *If $\lambda \neq 0, 1$, then the j-invariant of $E(\lambda)$ is*

$$j(E(\lambda)) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

(3) *The only λ for which $j(E(\lambda)) = 1728$ are $\lambda = 2, -1,$ and $\frac{1}{2}$.*

(4) *The only λ for which $j(E(\lambda)) = 0$ are $\lambda = \dfrac{1 \pm \sqrt{-3}}{2}$.*

(5) *For every $j \neq 0$ or 1728, the map $K/\{0,1\} \to j(E(\lambda))$ is six to one. In particular, we have*

$$S(\lambda) := \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\} \longrightarrow j(E(\lambda)).$$

If $D \in \mathbb{F}_p \setminus \{0\}$, then define $E_D(\lambda)$, the D-quadratic twist of $E(\lambda)$, by

$$E_D(\lambda): \quad y^2 = x(x-D)(x-D\lambda). \tag{3.1}$$

If D is a square in $\mathbb{F}_p$, then $E_D(\lambda)$ is isomorphic to $E(\lambda)$ over $\mathbb{F}_p$. It is easy to check the following proposition.

Proposition 3.2. *Suppose that $p \geq 5$ is prime and that $\lambda \in \mathbb{F}_p \setminus \{0,1\}$.*

(1) *$E(\lambda)$ is the λ quadratic twist of $E(1/\lambda)$.*

(2) *$E(\lambda)$ is the -1 quadratic twist of $E(1-\lambda)$.*

(3) *$E(\lambda)$ is the $-(\lambda-1)$ quadratic twist of $E\left(\frac{\lambda}{\lambda-1}\right)$.*

We shall rely heavily on the following important proposition which characterizes those elliptic curves E over $\mathbb{F}_p$ whose group of $\mathbb{F}_p$-rational points contains $\mathbb{Z}2 \times \mathbb{Z}4$ or $\mathbb{Z}4 \times \mathbb{Z}4$.

Proposition 3.3. *Let $p \geq 5$ be prime.*

(1) *Let $E/\mathbb{F}_p$ be an elliptic curve whose group of $\mathbb{F}_p$-rational points contains $\mathbb{Z}2 \times \mathbb{Z}4$. Then there is a $\lambda \in \mathbb{F}_p \setminus \{0, \pm 1\}$ for which $E(\lambda^2)$ is isomorphic over $\mathbb{F}_p$ to E. Moreover, if $\lambda \in \mathbb{F}_p \setminus \{0, \pm 1\}$, then the group of $\mathbb{F}_p$-rational points of $E(\lambda^2)$ contains $\mathbb{Z}2 \times \mathbb{Z}4$.*

(2) *Suppose that $\lambda \in \mathbb{F}_p \setminus \{0, \pm 1\}$. Then the group of $\mathbb{F}_p$-rational points of $E(\lambda^2)$ contains $\mathbb{Z}4 \times \mathbb{Z}4$ if and only if $p \equiv 1 \pmod 4$ and $\lambda^2 - 1$ is a square in $\mathbb{F}_p$.*

Proof. Let $E/\mathbb{F}_p$ be an elliptic curve given by

$$E: \quad y^2 = (x-\alpha)(x-\beta)(x-\gamma) \tag{3.2}$$

where $\alpha, \beta, \gamma \in \mathbb{F}_p$. A complete 2-descent on the curve (see [Prop. X.1.4, S], [Th. 4.1, H]), shows that an $\mathbb{F}_p$-rational $P = (x', y')$ on E is of the form $2Q = P$ for some $\mathbb{F}_p$-rational point Q if and only if

$$x' - \alpha, \ x' - \beta, \ x' - \gamma$$

are all squares in $\mathbb{F}_p$.

First we prove (1). Without loss of generality we may assume that E is of the form (3.2) where $\alpha = 0$ (i.e. $(0,0)$ is a point of order 2). We may also assume that some order four $\mathbb{F}_p$ rational point Q has the property that $2Q = (0,0)$. By 2-descents, this implies that E is of the form

$$E: \quad y^2 = x(x+m^2)(x+n^2). \tag{3.3}$$

If $p \equiv 1 \pmod 4$, then we may choose $\tilde{m}, \tilde{n} \in \mathbb{F}_p$ such that $\tilde{m}^2 = -m^2$ and $\tilde{n}^2 = -n^2$. If $p \equiv 3 \pmod 4$, then either $m^2 - n^2$ or $n^2 - m^2$ is a square in $\mathbb{F}_p$; for the sake of concreteness, suppose that there exists $\tilde{n} \in \mathbb{F}_p$ such that $\tilde{n}^2 = m^2 - n^2$. Replacing x by $x - m^2$ in (3.3) gives

$$E: \quad y^2 = x(x - m^2)(x - (m^2 - n^2)) = x(x - \tilde{m}^2)(x - \tilde{n}^2),$$

where $\tilde{m} = m$. In either case, therefore, we conclude that E is of the form

$$E: \quad y^2 = x(x - \tilde{m}^2)(x - \tilde{n}^2).$$

From this we see that E is isomorphic over $\mathbb{F}_p$ to $E\left(\tilde{n}^2/\tilde{m}^2\right)$.

To see that each $E(\lambda^2)$ with $\lambda \in \mathbb{F}_p \setminus \{0, 1\}$ contains $\mathbb{Z}2 \times \mathbb{Z}4$, note that if $p \equiv 1 \pmod 4$, then $(0, 0)$ is twice an $\mathbb{F}_p$ point, and if $p \equiv 3 \pmod 4$, then either $(1, 0)$ or $(\lambda^2, 0)$ is twice an $\mathbb{F}_p$-point.

We turn to the proof of (2). The group of $\mathbb{F}_p$-points of $E(\lambda^2)$ contains $\mathbb{Z}4 \times \mathbb{Z}4$ if and only if the order two points $(0, 0), (1, 0)$, and $(\lambda^2, 0)$ are all doubles of other $\mathbb{F}_p$-points. This happens if and only if all of $0, -1, -\lambda^2, 1, 1 - \lambda^2, \lambda^2, \lambda^2 - 1$ are squares. This is impossible if $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then this occurs if and only if $\lambda^2 - 1$ is a square. □

Since the Eichler-Selberg trace formula for the Hecke operators is expressed in terms of orders of imaginary quadratic fields, it is important to our purpose to obtain a formula for $N(p)$ in terms of such orders (after Deuring [D], we know that these orders correspond to the endomorphism rings of elliptic curves over $\mathbb{F}_p$).

We fix some notation. If $\Delta < 0$, $\Delta \equiv 0, 1 \pmod 4$, then denote by $\mathcal{O}(\Delta)$ the unique imaginary quadratic order with discriminant Δ. Let $h(\Delta) = h(\mathcal{O}(\Delta))$ denote the order of the class group of $\mathcal{O}(\Delta)$ and let $\omega(\Delta) = \omega(\mathcal{O}(\Delta))$ denote half the number of roots of unity in $\mathcal{O}(\Delta)$. Further, define

$$H(\Delta) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\max}} h(\mathcal{O}'), \quad H^*(\Delta) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\max}} \frac{h(\mathcal{O}')}{\omega(\mathcal{O}')}, \tag{3.4}$$

where the sum is over all orders $\mathcal{O}'$ between $\mathcal{O}$ and the maximal order $\mathcal{O}_{\max}$. Notice that $H^*(\Delta) = H(\Delta)$ unless $\mathcal{O}_{\max} = \mathbb{Z}[i]$ or $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, and that in the latter cases only the term corresponding to $\mathcal{O}_{\max}$ differs.

With this notation, Schoof proves the following

Theorem 3. [(4.8), (4.9), Sc] *Let p be an odd prime.*

1. *Suppose that n and s are integers such that $s^2 \leq 4p$, $p \nmid s$, $n^2 \mid p+1-s$, and $n \mid p-1$. Then the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ whose group of $\mathbb{F}_p$-rational points has order $p + 1 - s$ and contains $\mathbb{Z}n \times \mathbb{Z}n$ is $H\left(\frac{s^2-4p}{n^2}\right)$.*
2. *If $p \equiv 7 \pmod 8$, then the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ which are supersingular at p and whose $\mathbb{F}_p$-rational points contain $\mathbb{Z}2 \times \mathbb{Z}4$ is $h(-p)$.*

By using Theorems 2 and 3 we can obtain the desired formula for $N(p)$. We first require some notation. If p is an odd prime and s is an integer such that $|s| \leq 2\sqrt{p}$, then let $x_p(s)$ and $y_p(s)$ denote the roots of the polynomial

$$x^2 - sx + p = 0. \tag{3.5}$$

By (2.6), (2.7), (2.8), and (3.5), it is clear that if $\lambda \in \mathbb{F}_p \setminus \{0, 1\}$ has the property that the group of $\mathbb{F}_p$-rational points of $E(\lambda)$ has $p + 1 - s$ points, then $\{\pi(p, \lambda), \overline{\pi(p, \lambda)}\} = \{x_p(s), y_p(s)\}$. Using this notation, we obtain the following theorem.

Theorem 4. *If p is prime, then define $A(p)$ by*

$$A(p) := p^3 - 2p^2 - 7 - N(p).$$

(1) *If $p \equiv 1 \pmod 4$ is prime, then*

$$A(p) = -4 - 4 \sum_{\substack{|s| \leq 2\sqrt{p} \\ s \equiv p+1 \pmod 8}} F(x_p(s), y_p(s)) H^*\left(\tfrac{s^2-4p}{4}\right) - 8 \sum_{\substack{|s| \leq 2\sqrt{p} \\ s \equiv p+1 \pmod{16}}} F(x_p(s), y_p(s)) H^*\left(\tfrac{s^2-4p}{16}\right).$$

(2) *If $3 < p \equiv 3 \pmod 8$ is prime, then*

$$A(p) = -4 - 4 \sum_{\substack{|s| \leq 2\sqrt{p} \\ s \equiv 4 \pmod 8}} F(x_p(s), y_p(s)) H^*\left(\tfrac{s^2-4p}{4}\right).$$

(3) *If $p \equiv 7 \pmod 8$ is prime, then*

$$A(p) = -4 + 4ph(-p) - 4 \sum_{\substack{0 < |s| \leq 2\sqrt{p} \\ s \equiv 0 \pmod 8}} F(x_p(s), y_p(s)) H^*\left(\tfrac{s^2-4p}{4}\right).$$

During the proof, we shall require the following fact (see [Sc], for example). Let s and n be as in part (1) of Theorem 3. If E is a non-supersingular curve over $\mathbb{F}_p$ with $p+1-s$ points, and E has $j = 1728$ (resp. $j = 0$), then E contains $\mathbb{Z}n \times \mathbb{Z}n$ if and only if $\mathcal{O}(\frac{s^2-4p}{n^2}) \subseteq \mathbb{Z}[i]$ (resp. $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$).

Proof of Theorem 4. In view of Proposition 3.3 and (2.6), the only $s = \pi(p, y^2) + \overline{\pi(p, y^2)}$ which occur in Theorem 2 are those for which $s^2 \leq 4p$ and $s \equiv p+1 \pmod 8$. Since $p > 3$, these curves are supersingular only if $s = 0$, which implies that $p \equiv 7 \pmod 8$.

First we prove assertion (1). Choose s with $s^2 \leq 4p$ and $s \equiv p+1 \pmod 8$. There are three cases to consider; first we suppose that $s \not\equiv p+1 \mod 16$. Proposition 3.3 shows that the isomorphism classes containing those curves $E(y^2)$ with $p+1-s$ points are precisely the classes comprised of curves with $p+1-s$ points and the subgroup $\mathbb{Z}2 \times \mathbb{Z}2$. By Propositions 3.1, 3.2, and 3.3, we see that if such a class $\mathcal{C}$ has $j \neq 0, 1728$, then $\mathcal{C}$ contains $E(y^2)$ for exactly 4 values of y. We see (by Lemma 4.2 below) that $\mathcal{C}$ cannot have $j = 0$. If $j = 1728$, then $\mathcal{O}(\frac{s^2-4p}{4}) \subseteq \mathbb{Z}[i]$, and Lemma 4.2 shows that $p \equiv 5 \pmod 8$. In this case Proposition 3.1 shows that $\mathcal{C}$ contains $E(y^2)$ for exactly 2 values of y. We conclude in any event that the number of y such that $E(y^2)$ falls in this first case is always $4H^*(\frac{s^2-4p}{4})$.

We next suppose that $s \equiv p+1 \pmod{16}$. The isomorphism classes containing those curves $E(y^2)$ with $p+1-s$ points and the subgroup $\mathbb{Z}4 \times \mathbb{Z}4$ comprise all classes with $p+1-s$ points and $\mathbb{Z}4 \times \mathbb{Z}4$. If $\mathcal{C}$ is such a class and $j \neq 0, 1728$, then Propositions 3.1, 3.2 and 3.3 show that $\mathcal{C}$ contains $E(y^2)$ for exactly 12 values of y. If $\mathcal{C}$ has $j = 1728$ then $\mathcal{O}(\frac{s^2-4p}{4}) \subseteq \mathbb{Z}[i]$ and (by Lemma 4.2 below), we must have $p \equiv 1 \pmod 8$. Proposition 3.1 then shows that

$\mathcal{C}$ contains $E(y^2)$ for 6 values of y. If $\mathcal{C}$ has $j = 0$ then $\mathcal{O}(\frac{s^2-4p}{4}) \subseteq \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ and (since some curve $E(\lambda^2) \in \mathcal{C}$), we see by Proposition 3.1 that both of $\frac{1\pm\sqrt{-3}}{2}$ are squares. In this case $\mathcal{C}$ contains $E(y^2)$ for 4 values of y. We conclude that the number of y such that $E(y^2)$ has $p+1-s$ points and $\mathbb{Z}4 \times \mathbb{Z}4$ is $12H^*(\frac{s^2-4p}{16})$.

Only the curves $E(y^2)$ with $s \equiv p+1 \pmod{16}$ and which do not contain $\mathbb{Z}4 \times \mathbb{Z}4$ remain. The classes containing such $E(y^2)$ are precisely those which contain $\mathbb{Z}2 \times \mathbb{Z}2$ but not $\mathbb{Z}4 \times \mathbb{Z}4$. By the fact above, such curves cannot have $j = 0, 1728$. Therefore each class of such curves contains $E(y^2)$ for 4 values of y. By Theorem 3, there are $H(\frac{s^2-4p}{4}) - H(\frac{s^2-4p}{16}) = H^*(\frac{s^2-4p}{4}) - H^*(\frac{s^2-4p}{16})$ such classes. So the number of y such that $E(y^2)$ falls in this third case is $4H^*(\frac{s^2-4p}{4}) - 4H^*(\frac{s^2-4p}{16})$. Assertion (1) now follows from Theorem 2 after adding the contribution from each of the three cases.

Assertions (2) and (3) are proved with similar arguments. If $p \equiv 3 \pmod 4$ and $s \equiv p+1 \pmod 8$ then congruence considerations show that $\mathcal{C}$ cannot have $j = 0, 1728$. As above, the isomorphism classes containing those curves $E(y^2)$ with $p+1-s$ points are precisely the classes comprised of curves with $p+1-s$ points and the subgroup $\mathbb{Z}2 \times \mathbb{Z}2$. If $\mathcal{C}$ is such a class, and $E(y^2) \in \mathcal{C}$, then $S(y^2)$ contains exactly 4 squares. Proposition 3.2 shows that only two of the four corresponding curves lie in $\mathcal{C}$; therefore $\mathcal{C}$ contains $E(y^2)$ for four values of y. If $s \neq 0$, then by Theorem 3, the number of classes is $H(\frac{s^2-4p}{4}) = H^*(\frac{s^2-4p}{4})$.

It remains only to consider the supersingular case $s = 0$ (this can occur only when $p \equiv 7 \pmod 8$). Here Theorem 3 shows that the number of classes is $h(-p)$. Theorem 4 follows since $F(x_p(0), y_p(0)) = -p$. $\square$

4. The Eichler-Selberg Trace formula and $N(p)$

Since it is easy to verify Theorem 1 for $p = 3$, to prove Theorem 1 it suffices to prove for every prime $p \geq 5$ that $a(p) = A(p)$, where $a(p)$ and $A(p)$ are defined in Theorems 1 and 4, respectively. Let $T(p)$ denote the usual Hecke operator acting on $S_4(\Gamma_0(8))$. Since this space is one-dimensional (see [C-O]), we in fact need only to show that $\operatorname{Tr} T(p) = A(p)$ for all $p \geq 5$.

We shall fix some notation to be used for the duration. If p is an odd prime and s an integer such that $s^2 - 4p < 0$, then we may write

$$s^2 - 4p = t^2 D,$$

where t is a positive integer and D is a fundamental discriminant of an imaginary quadratic field. We shall always use the symbol f to denote a positive divisor of t. The following theorem results from a simplification of the trace formula in our special case. We use a version of the trace formula due to Hijikata [Hi] which is recorded as Theorem 2.2 of [H-P-S]. We omit the details in this simplification.

Theorem 5 (The Trace Formula). *Let p be an odd prime, and let $T(p)$ denote the p-th Hecke operator on $S_4(\Gamma_0(8))$. Then*

$$\operatorname{Tr} T(p) = -4 + \delta(p) - \sum_{\substack{0<|s|\leq 2\sqrt{p} \\ s\equiv p+1 \pmod 8}} F(x_p(s), y_p(s)) \cdot \sum_{f|t} \frac{h\left(\frac{s^2-4p}{f^2}\right)}{\omega\left(\frac{s^2-4p}{f^2}\right)} \cdot c(s, f).$$

Here

$$\delta(p) := \begin{cases} 0 \ \text{ if } \ p \not\equiv 7 \pmod 8, \\ 4 \cdot ph(-p) \ \text{ if } \ p \equiv 7 \pmod 8, \end{cases}$$

and, if $s^2 - 4p = t^2 D$ *as above, and* $f \mid t$*, then the integer* $c(s, f)$ *is defined as follows:*

(1) *Suppose that* $p \equiv 1 \pmod 4$*.*

(i) If D *is even, then*

$$c(s, f) := \begin{cases} 0 & \text{if} \quad \operatorname{ord}_2 t = \operatorname{ord}_2 f, \\ 2 & \text{if} \quad \operatorname{ord}_2 t = \operatorname{ord}_2 f + 1, \\ 4 & \text{if} \quad \operatorname{ord}_2 t \geq \operatorname{ord}_2 f + 2. \end{cases}$$

(ii) If $D \equiv 5 \pmod 8$*, then*

$$c(s, f) := \begin{cases} 0 & \text{if} \quad \operatorname{ord}_2 t \leq \operatorname{ord}_2 f + 1, \\ 4 & \text{if} \quad \operatorname{ord}_2 t \geq \operatorname{ord}_2 f + 2. \end{cases}$$

(iii) If $D \equiv 1 \pmod 8$*, then*

$$c(s, f) := \begin{cases} 2 & \text{if} \quad \operatorname{ord}_2 t = \operatorname{ord}_2 f, \\ 6 & \text{if} \quad \operatorname{ord}_2 t = \operatorname{ord}_2 f + 1, \\ 4 & \text{if} \quad \operatorname{ord}_2 t \geq \operatorname{ord}_2 f + 2. \end{cases}$$

(2) *Suppose that* $p \equiv 3 \pmod 4$*. Then we have* $\operatorname{ord}_2 t = 1$*, and*

$$c(s, f) := \begin{cases} 3 & \text{if} \quad \operatorname{ord}_2 f = 0, \\ 1 & \text{if} \quad \operatorname{ord}_2 f = 1. \end{cases}$$

To finish the proof, we show that $\operatorname{Tr} T(p) = A(p)$ for all p via case-by-case analysis. We shall require the following lemma repeatedly (see [Co, Corollary 7.28]).

Lemma 4.1. *Let* $\mathcal{O}$ *be an order of discriminant* Δ *in an imaginary quadratic field, and let* $\mathcal{O}'$ *be a suborder of index* N*. Then*

$$\frac{h(\mathcal{O}')}{\omega(\mathcal{O}')} = \frac{h(\mathcal{O})}{\omega(\mathcal{O})} \cdot N \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \left(1 - \left(\frac{\Delta}{\ell}\right) \frac{1}{\ell}\right).$$

We recall that if Δ is the discriminant of an order, then the Kronecker symbol $\left(\frac{\Delta}{2}\right)$ is defined by

$$\left(\frac{\Delta}{2}\right) := \begin{cases} 0 \ \text{ if } \ 2 \mid \Delta \\ 1 \ \text{ if } \ \Delta \equiv 1 \pmod 8 \\ -1 \ \text{ if } \ \Delta \equiv 5 \pmod 8. \end{cases}$$

We turn to the proof of Theorem 1. The case when $p \equiv 3 \pmod 4$ is simplest. For every s such that $0 < |s| \leq 2\sqrt{p}$ and such that $s \equiv p + 1 \pmod 8$ we must show that the coefficients on $F(x_p(s), y_p(s))$ in Theorems 4 and 5 are equal. In order to simplify notation, we shall adopt the following convention: given integers t and f with $f \mid t$, define

$$a := \operatorname{ord}_2 t \quad \text{and} \quad \rho := \operatorname{ord}_2 f.$$

Unless specified otherwise, our sums will run over all positive divisors f of t. Finally, we define the function h^* by

$$h^*(d) := \frac{h(d)}{\omega(d)}.$$

Congruence considerations show that in this case we have $D \equiv 1 \pmod 8$ and $a = \operatorname{ord}_2 t = 1$. By (3.4) we have

$$H^*\left(\tfrac{s^2-4p}{4}\right) = \sum_{\rho=0} h^*\left(\tfrac{s^2-4p}{4f^2}\right). \tag{4.1}$$

It is clear that

$$\sum_{\rho=0} h^*\left(\tfrac{s^2-4p}{4f^2}\right) = \sum_{\rho=1} h^*\left(\tfrac{s^2-4p}{f^2}\right). \tag{4.2}$$

Further, by Lemma 4.1, we see that if $\rho = 0$ we have

$$h^*\left(\tfrac{s^2-4p}{f^2}\right) = h^*\left(\tfrac{s^2-4p}{4f^2}\right) \cdot 2 \cdot \left(1 - \left(\tfrac{(t/2f)^2 D}{2}\right) \cdot \tfrac{1}{2}\right) = h^*\left(\tfrac{s^2-4p}{4f^2}\right). \tag{4.3}$$

Here we have used the fact that $\left(\frac{(t/2f)^2 D}{2}\right) = 1$ since $t/2f$ is odd and $D \equiv 1 \pmod 8$. Combining (4.1), (4.2), and (4.3) gives

$$-4H^*\left(\tfrac{s^2-4p}{4}\right) = -3\sum_{\rho=0} h^*\left(\tfrac{s^2-4p}{f^2}\right) - \sum_{\rho=1} h^*\left(\tfrac{s^2-4p}{f^2}\right),$$

which shows that the formulae in Theorems 4 and 5 do indeed agree in this case.

In the case when $p \equiv 1 \pmod 4$ the computations are not as straightforward. In particular, given $s \equiv p+1 \pmod 8$, we must determine under which conditions we have $s \equiv p+1 \pmod{16}$. The following lemma answers this question.

Lemma 4.2. *Suppose that $p \equiv 1 \pmod 4$ is prime and that $s^2 - 4p = t^2 D$, where D is a fundamental discriminant of an imaginary quadratic field. Suppose further that $s \equiv p+1 \pmod 8$. Under these assumptions,*

(1) *We have $s \equiv p+1 \pmod{16}$ if*
  - *(a) $p \equiv 1 \pmod 8$ and $D \equiv 1, 4, 5 \pmod 8$, or*
  - *(b) $p \equiv 1 \pmod 8$, $D \equiv 0 \pmod 8$, and $\operatorname{ord}_2 t \geq 2$, or*
  - *(c) $p \equiv 5 \pmod 8$ and $D \equiv 1, 5 \pmod 8$.*

(2) *We have $s \not\equiv p+1 \pmod{16}$ if*
  - *(d) $p \equiv 1 \pmod 8$, $D \equiv 0 \pmod 8$, and $\operatorname{ord}_2 t \leq 1$, or*
  - *(e) $p \equiv 5 \pmod 8$ and $D \equiv 4 \pmod 8$.*

The case $p \equiv 5 \pmod 8$, $D \equiv 0 \pmod 8$ *does not occur.*

We omit the proof of this lemma, since it follows solely from congruence considerations.

We now give an example of the sort of analysis which is required to complete the proof by considering in detail the case when $s^2 - 4p = t^2 D$ with $D \equiv 1 \pmod 8$. In this case (using Lemma 4.2), the coefficient on $F(x_p(s), y_p(s))$ in Theorem 4 is given by

$$-4H^*\left(\tfrac{s^2-4p}{4}\right) - 8H^*\left(\tfrac{s^2-4p}{16}\right).$$

By the definition of H^*, we see that

$$H^*\left(\tfrac{s^2-4p}{4}\right) = \sum_{a \geq \rho+1} h^*\left(\tfrac{s^2-4p}{4f^2}\right). \tag{4.4}$$

Using Lemma 4.1, we see that if $a \geq \rho + 1$, then

$$h^*\left(\tfrac{s^2-4p}{f^2}\right) = h^*\left(\tfrac{s^2-4p}{4f^2}\right) \cdot 2 \cdot \left(1 - \left(\tfrac{(t/2f)^2 D}{2}\right) \cdot \tfrac{1}{2}\right) = h^*\left(\tfrac{s^2-4p}{4f^2}\right) \cdot \begin{cases} 1 & \text{if } \ a = \rho+1, \\ 2 & \text{if } \ a \geq \rho+2. \end{cases}$$

This together with (4.4) shows that

$$-4H^*\left(\tfrac{s^2-4p}{4}\right) = -4 \sum_{a=\rho+1} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 2 \sum_{a \geq \rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right). \tag{4.5}$$

Similar analysis shows that

$$-8H^*\left(\tfrac{s^2-4p}{16}\right) = -4 \sum_{a=\rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 2 \sum_{a \geq \rho+3} h^*\left(\tfrac{s^2-4p}{f^2}\right). \tag{4.6}$$

By (4.5) and (4.6) we obtain

$$-4H^*\left(\tfrac{s^2-4p}{4}\right) - 8H^*\left(\tfrac{s^2-4p}{16}\right) = -4 \sum_{a=\rho+1} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 4 \sum_{a \geq \rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 2 \sum_{a=\rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right).$$

Finally, using Lemma 4.1, we find that

$$\sum_{a=\rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right) = 2 \sum_{a=\rho+1} h^*\left(\tfrac{s^2-4p}{f^2}\right) = 2 \sum_{a=\rho} h^*\left(\tfrac{s^2-4p}{f^2}\right).$$

Therefore,

$$-4H^*\left(\tfrac{s^2-4p}{4}\right) - 8H^*\left(\tfrac{s^2-4p}{16}\right) = -2 \sum_{a=\rho} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 6 \sum_{a=\rho+1} h^*\left(\tfrac{s^2-4p}{f^2}\right) - 4 \sum_{a \geq \rho+2} h^*\left(\tfrac{s^2-4p}{f^2}\right),$$

in agreement with the trace formula.

The other cases proceed along similar lines, and we omit the details. One must notice that in cases (d) and (e) of Lemma 4.2, we necessarily have $\operatorname{ord}_2 t = 1$. In every case we conclude that $\operatorname{Tr} T(p) = A(p)$, from which we obtain Theorem 1. □

Acknowledgements

We thank the referee for informing us of the paper by van Geemen and Nygaard, and we thank H. Verrill for her preprints.

References

[A-O] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, to appear, J. reine ange. Math..

[Co] D. Cox, *Primes of the form $x^2 + ny^2$*, Wiley and Sons, 1989.

[C-O] H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, Modular functions of one variable, VI. Springer Lect. Notes **627** (1977), 69-78.

[D] M. Deuring, *Die typen der multiplikatorenringe elliptscher funktionenkörper*, Math. Zeit. **47** (1941), 47-56.

[vG-N] B. van Geemen and N. Nygaard, *On the geometry and arithmetic of some Siegel modular threefolds*, J. Number Theory **53** (1995), 45-87.

[H] D. Husemoller, *Elliptic curves*, Springer Verlag, New York, 1987.

[Hi] H. Hijikata, *Explicit formula of the traces of the Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), 56-82.

[H-P-S] H. Hijikata, A. Pizer, and T. Shemanske, *The basis problem for modular forms on* $\Gamma_0(N)$, Memoirs Amer. Math. Soc. **82** (1989).

[Sc] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Comb. Th., Ser. A **46** (1987), 183-211.

[S] J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.

[V] H. Verrill, *Arithmetic of a certain Calabi-Yau threefold*, preprint.

[V2] H. Verrill, *The L-series of certain rigid Calabi-Yau threefolds*, preprint.

Department of Mathematics, Colgate University, Hamilton, NY 13346
E-mail address: ahlgren@math.colgate.edu

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: ono@math.wisc.edu