ON p-ADIC PROPERTIES OF TWISTED TRACES OF SINGULAR MODULI

DANIEL LE, SHELLY MANBER, SHRENIK SHAH

Abstract. We prove that logarithmic derivatives of certain twisted Hilbert class polynomials are holomorphic modular forms modulo p of filtration $p+1$. We derive p-adic information about twisted Hecke traces and Hilbert class polynomials. In this framework we formulate a precise criterion for p-divisibility of class numbers of imaginary quadratic fields in terms of the existence of certain cusp forms modulo p. We explain the existence of infinite classes of congruent twisted Hecke traces with fixed discriminant in terms of the factorization of the associated Hilbert class polynomial modulo p. Finally, we provide a new proof of a theorem of Ogg classifying those p for which all supersingular j-invariants modulo p lie in $\mathbf{F}_p$.

1. Introduction

The class numbers $h(-d)$ for $-d < 0$ are a source of many famously difficult problems. The class number one problem asks for the full list of discriminants $-d < 0$ that satisfy $h(-d) = 1$. This problem was eventually solved by Baker [Bak68], Heegner [Hee52], and Stark [Sta67]. More generally, the question of whether, for fixed $k > 0$, there are finitely many discriminants $-d < 0$ with $h(-d) = k$ was posed by Gauss and later answered in the affirmative.

More recently, there has been a body of work studying the p-divisibility properties of the class numbers $h(-d)$. Since $h(-d) = \#\operatorname{Cl}(\mathbf{Q}(\sqrt{-d}))$ is the order of a group, the question of p-divisibility of $h(-d)$ is equivalent to the existence of elements of order p in the ideal class group $\operatorname{Cl}(\mathbf{Q}(\sqrt{-d}))$. Although Cohen and Lenstra [CL84] predict a precise proportion of class numbers to be p-divisible, the best known lower bound, found by Soundararajan [Sou00], falls far short of guaranteeing a positive proportion. The lower bound of Kohnen and Ono [KO99] on indivisibility of class numbers also falls far short of a positive proportion.

Since the best lower and upper bounds for p-divisibility of class numbers differ so greatly, it seems profitable to obtain a criterion that is *equivalent* to the question of whether $p|h(-d)$ and that translates the question into one which can be answered by applying tools from the well-established theory of modular forms modulo p. Such a connection was critical to Kohnen and Ono's result. To motivate our criterion, we recall an analogous criterion for the divisibility of class numbers of cyclotomic fields.

Kummer was able to prove Fermat's Last Theorem for certain prime exponents called regular primes. A prime p is *regular* if it has the property that p divides the order of the cyclotomic class group $\operatorname{Cl}(\mathbf{Q}(\zeta_p))$, where ζ_p is a p^{th} root of unity. Kummer showed that p is regular exactly when p does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$, where the Bernoulli numbers B_k are defined by the power series expansion $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_k t^k$ [IR90]. While it is known that there are infinitely many irregular primes, the distribution of regular primes is not understood.

There exists a criterion for regularity of primes purely in terms of the existence of certain types of cusp forms in the graded algebra $\widetilde{M}$ of modular forms modulo p. In this paper, we will use $\widetilde{\cdot}$ to indicate that an object is reduced modulo p. We denote the finite dimensional subspace of modular forms modulo p with filtration at most k and grading congruent to k modulo $p-1$ by $\widetilde{M}_k \subseteq \widetilde{M}$. See Section 2.1 for further details.

To connect Bernoulli numbers to modular forms, we recall the definition of the Eisenstein series. Let $\mathfrak{H}$ denote the upper half-plane, and for $k \in 2\mathbf{Z}$, let E_k denote the weight k Eisenstein series,

defined by

$$E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_m(n) = \sum_{d|n} d^m$ and $q = e^{2\pi i \tau}$ for $\tau \in \mathfrak{H}$ throughout the paper. By Kummer's criterion on the numerators of Bernoulli numbers, we find that the normalization of E_k is a cusp form in $\widetilde{M_k}$ for some $k \in \{2, 4, \ldots, p-3\}$ if and only if p is irregular.

While this criterion may appear to be an abstract formulation of regularity with limited utility, Ribet [Rib76] uses this criterion to prove the converse to Herbrand's theorem, obtaining a more precise version of Kummer's condition for regularity by interpreting the congruence in terms of residual Galois representations of eigenforms. Mazur and Wiles [MW84, Wil90] extend Ribet's methods to derive important consequences for Iwasawa theory.

One limitation of this criterion is that it requires checking whether E_k is a cusp form for many values of k in order to determine whether p divides $\#\operatorname{Cl}(\mathbf{Q}(\zeta_p))$. It is also limited to detecting p-torsion in the group $\operatorname{Cl}(\mathbf{Q}(\zeta_p))$, rather than in general cyclotomic class groups.

We find an analogous criterion for studying p-torsion in $\operatorname{Cl}(\mathbf{Q}(\sqrt{-d}))$. Moreover, we bypass both of the above limitations by defining a *single* q-series $\mathscr{F}_d$, independent of p, which plays the role of all the E_k above. Indeed, we have the following theorem.

Theorem 1.1. *Let $-d < -4$ be a fundamental discriminant and $p \geq 5$ a prime such that p does not split in $\mathbf{Q}(\sqrt{-d})$. Then $p|h(-d)$ if and only if there exists a cusp form $f \in M_{p+1}$ such that $f \equiv \mathscr{F}_d \pmod{p}$, where $\mathscr{F}_d$ is defined later.*

Moreover, $\mathscr{F}_d$ has an explicit description in terms of functions that arise naturally from the work of Borcherds and Zagier [Bor95a, Bor95b, Zag02]. Define the Kohnen plus-space of weight $\frac{1}{2}$ to contain weakly holomorphic modular forms with trivial character that have Fourier coefficients supported where the exponents on q are 0 or 1 modulo 4. Borcherds defines a sequence of functions f_d for d congruent to 0 or 3 modulo 4 to be the unique modular forms of the form

$$f_d(\tau) = q^{-d} + \sum_{\substack{D>0 \\ D \equiv 0,1 \pmod{p}}} A(D,d) q^D \tag{1}$$

in the Kohnen-plus space of weight $\frac{1}{2}$. Note that the uniqueness of these forms comes from the structure theory for the Kohnen-plus space [Bor95a]. We take (1) to be our definition of the integers $A(D,d)$. We have that

$$f_0 = \sum_{n \in \mathbf{Z}} q^{n^2} \qquad \text{and} \qquad f_3 = \frac{f_0'(\tau) E_{10}(4\tau)}{4\pi i \Delta(4\tau)} - \frac{f_0(\tau) E_{10}'(4\tau)}{20\pi i \Delta(4\tau)} - \frac{152}{5} f_0, \tag{2}$$

where Δ is the weight 12 cusp form on $\mathrm{SL}_2(\mathbf{Z})$ normalized to have leading coefficient 1. The first few f_d have initial q-coefficients:

$$\begin{aligned}
f_0 &= 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + 2q^{25} + 2q^{36} + 2q^{49} + 2q^{64} + \ldots \\
f_3 &= q^{-3} - 248q + 26752q^4 - 85995q^5 + 1707264q^8 - 4096248q^9 + 44330496q^{12} + \ldots \\
f_4 &= q^{-4} + 492q + 143376q^4 + 565760q^5 + 18473000q^8 + 51180012q^9 + \ldots \\
f_7 &= q^{-7} - 4119q + 8288256q^4 - 52756480q^5 + 5734772736q^8 - 22505066244q^9 + \ldots \\
f_8 &= q^{-8} + 7256q + 26124256q^4 + 190356480q^5 + 29071392966q^8 + 125891591256q^9 + \ldots
\end{aligned}$$

The sequence of f_d's can be obtained recursively via multiplication by $j(4z)$ and diagonalization.

Despite the seemingly chaotic properties of this grid of coefficients, we shall see that the grid contains many remarkable congruences as well as a surprising amount of additional information.

Remark 1. Singular moduli are the values of the j-function at the roots $\alpha_Q \in \mathfrak{H}$ of integral binary quadratic forms Q. These values are algebraic integers, and their minimal polynomials are Hilbert class polynomials. An important paper of Zagier [Zag02] shows that the coefficients $A(n^2D, d)$ encode the twisted Hecke traces of singular moduli. For more information, see Section 2.2.

For $-d < -4$ such that $-d$ is a fundamental discriminant, we define the function

$$\mathscr{F}_d = -\sum_{n=1}^{\infty}\sum_{k|n} A(k^2, d)kq^n. \tag{3}$$

At first glance, there is no information about $h(-d)$ encoded in this function, yet Theorem 1.1 shows that the question of p-divisibility for certain primes $p \geq 5$ is answered by $\mathscr{F}_d$.

Example 1. To illustrate Theorem 1.1, we test the class number $h(-991)$ for divisibility by 17. Since the space of modular forms modulo p of a given weight is a finite dimensional vector space with an explicitly diagonalizable basis, it suffices to check finitely many coefficients of the q-series to determine equality. Using the definition of the functions f_d we compute

$$\begin{aligned}\mathscr{F}_{991} &\equiv 15q + 2q^2 + 2q^4 + 4q^5 + 9q^7 + 11q^8 + 6q^9 + 13q^{10} + 4q^{13} + 8q^{14} + 2q^{16} + \dots \\ &\equiv 15\Delta E_6 \pmod{17}\end{aligned}$$

and thus $\mathscr{F}_{991}$ is a cusp form modulo 17. By Theorem 1.1, we have that $17|h(-991)$.

Borcherds [Bor95a] connects the coefficients $A(D, d)$ to Hilbert class polynomials, which are defined in terms of quadratic forms. We denote by $\mathcal{Q}_d$ the set of (binary integral) quadratic forms $Q(x, y) = aX^2 + bXY + cY^2$ of discriminant $-d$, where $d = b^2 - 4ac$. The group $\Gamma = \mathrm{PSL}_2(\mathbf{Z})$ acts on $\mathcal{Q}_d$ by a change of basis on X, Y by an element of Γ. We associate to each element $[Q]$ of the finite set $\mathcal{Q}_d/\Gamma$ the unique point $\alpha_Q \in \mathfrak{H}$ such that $(\alpha_Q, 1)$ is a root of some form Q in the equivalence class $[Q]$ and α_Q lies in the fundamental domain of Γ.

For $-d < -4$, we define the Hilbert class polynomial of discriminant d by

$$\mathcal{H}_d(j(\tau)) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (j(\tau) - j(\alpha_Q)). \tag{4}$$

We define the twisted Hilbert class polynomial of discriminant $-d < -4$ and twist $D > 0$ by

$$\mathcal{H}_{d,D}(j(\tau)) = \prod_{Q \in \mathcal{Q}_{dD}/\Gamma} (j(\tau) - j(\alpha_Q))^{\chi_{d,D}(Q)}, \tag{5}$$

where $\chi_{d,D}$, the genus character of discriminant d and twist D, is defined by $\chi_{d,D}(Q) = (\frac{D}{\ell}) = (\frac{-d}{\ell})$ for any prime ℓ represented by Q. (The value of $\chi_{d,D}(Q)$ does not depend on the choice of ℓ.) Note that setting $D = 1$ in this definition yields the usual Hilbert class polynomials. For further details on Borcherds-Zagier theory, see Section 2.2.

Remark 2. Zagier [Zag02] shows that $\mathcal{H}_{d,D} \in \mathbf{Q}(\sqrt{D})(j(\tau))$, and that the nontrivial element $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt{D})/\mathbf{Q})$ maps $\mathcal{H}_{d,D}$ to its multiplicative inverse.

Remark 3. The Hilbert class polynomials can also be defined more generally for $-d < 0$. Denote by ω_Q the size of the stabilizer of α_Q in Γ. Then

$$\mathcal{H}_d(j(\tau)) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (j(\tau) - j(\alpha_Q))^{1/\omega_Q}. \tag{6}$$

For $-d < -4$, we always have $\omega_Q = 1$. Since we work here only with $-d < -4$, we simplify the definition of $\mathcal{H}_d$.

We define the Θ operator on a q-series to be $q\frac{d}{dq}$. We then define

$$\mathscr{L}_d(j(\tau)) = \frac{\Theta(\mathcal{H}_d(j(\tau)))}{\mathcal{H}_d(j(\tau))} \quad \text{and} \quad \mathscr{L}_{d,D}(j(\tau)) = \frac{\Theta(\mathcal{H}_{d,D}(j(\tau)))}{\sqrt{D}\mathcal{H}_{d,D}(j(\tau))}. \tag{7}$$

For $D > 1$ the quantity $\frac{\Theta(\mathcal{H}_{d,D}(j(\tau)))}{\mathcal{H}_{d,D}(j(\tau))}$ lies in $\sqrt{D}\mathbf{Z}[[q]]$ by Remark 2. Thus dividing by $\sqrt{D}$ in our definition for $\mathscr{L}_{d,D}$ removes the ambiguity of sign introduced when reducing this expression modulo p.

Let $-d < -4$ and $D > 0$ be a pair of coprime fundamental discriminants. For a prime $p \geq 5$, we say that p is *good* for $-d$ if p does not split in $\mathbf{Q}(\sqrt{-d})$, and *bad* for $-d$ if p does split in $\mathbf{Q}(\sqrt{-d})$. We say that p is *good* for the pair $(-d, D)$ if p does not split in $\mathbf{Q}(-dD)$ and $p \nmid D$, and that p is *bad* for the pair $(-d, D)$ if p splits in $\mathbf{Q}(-dD)$. As another notational remark, in this paper $\mathbf{Z}_{(p)}$ denotes the localization of $\mathbf{Z}$ at (p).

By work of Borcherds [Bor95a], the function $\mathscr{F}_d$ coincides modulo p with the logarithmic derivative $\mathscr{L}_d$ of the Hilbert class polynomial $\mathcal{H}_d$ exactly when $p|h(-d)$. Thus Theorem 1.1 follows immediately from the $D = 1$ case of the following result.

Theorem 1.2. *Let $-d < -4$ and $D > 0$ be coprime fundamental discriminants, and let $p \geq 5$ be a prime good for the pair $(-d, D)$. Then there exists a holomorphic modular form $\mathscr{L}^*_{d,D}$ over $\mathbf{Z}_{(p)}$ of weight $p+1$ such that $\mathscr{L}^*_{d,D} \equiv \mathscr{L}_{d,D} \pmod{p}$. Equivalently, $\widetilde{\mathscr{L}_{d,D}} \in \widetilde{M}_{p+1}$.*

Conversely, if p is bad for the pair $(-d, D)$, then $\widetilde{\mathscr{L}_{d,D}} \in \widetilde{M}_{p+1}$ if and only if $\widetilde{\mathscr{L}_{d,D}} = 0$.

We can reinterpret Theorem 1.2 in terms of the twisted Hecke traces $A(D, d)$.

Corollary 1.3. *The infinite tuple $\mathbf{u}_{d,D} = (A(n^2D, d))_{n \in \mathbf{Z}_{\geq 0}, p \nmid n}$ takes on only finitely many residues modulo p as $-d < -4$ and $D > 0$ range over all pairs of coprime fundamental discriminants such that p is good for $(-d, D)$.*

Let (d, D) and (d', D') be pairs of coprime fundamental discriminants such that $d, d' < -4$ and $D, D' > 0$. If $p \geq 5$ is a prime that is good for the pair $(-d, D)$ and bad for the pair $(-d', D')$, then $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \pmod{p}$ if and only if $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \equiv 0 \pmod{p}$.

Some congruences predicted by Corollary 1.3 are illustrated in Example 4.

Remark 4. Using Serre's theory of divisibility of coefficients of modular forms modulo p [Ser76], we obtain the following p-adic information about the $\mathscr{L}_{d,D}$'s. Let T_n denote the n^{th} Hecke operator, and let p, d, D be as in Theorem 1.2. The three-parameter family of modular forms $\{T_n\mathscr{L}_{d,D}\}_{n,d,D}$ reduce to elements of $\widetilde{M}_{p+1}$ modulo p. For a fixed pair $(-d, D)$ and $\lambda \in \{0, 2\}$, Serre's theorem (see §6 of [Ser76]) shows that $\widetilde{\mathscr{L}_{d,D}}$ is an eigenfunction with eigenvalue λ of a positive proportion of the prime Hecke operators T_ℓ.

The class numbers $h(-dD)$ tend to infinity, so the $\mathcal{H}_{d,D}$ become increasingly complicated. A priori, there is no reason that the $\mathscr{L}_{d,D}$ should be congruent modulo a prime p very often. Yet Theorem 1.2 shows that the reductions of the $\mathscr{L}_{d,D}$ modulo p for infinitely many pairs $(-d, D)$ lie in the same finite dimensional $\mathbf{F}_p$-vector space $\widetilde{M}_{p+1}$, a *finite set*. This observation prompts some natural questions. One question is whether one can determine an *explicit* point in $\widetilde{M}_{p+1}$ that is the reduction modulo p of infinitely many $\mathscr{L}_{d,D}$'s. For certain small primes, Theorem 1.4 achieves this. To state the theorem, we require some notation.

Let $\mathbf{SS} \subseteq \mathbf{F}_{p^2}$ be the set of all j-invariants of supersingular elliptic curves defined over $\mathbf{F}_p$, leaving the dependence on p out of our notation. Let $\mathbf{SS}_1 \subseteq \mathbf{SS}$ be the set of those supersingular j-invariants lying in $\mathbf{F}_p$.

Theorem 1.4. *For*

$$p \in \{5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}, \tag{8}$$

$\mathcal{H}_{d,D} \equiv 1 \pmod{p}$ *and thus* $\mathscr{L}_{d,D} \equiv 0 \pmod{p}$ *for all pairs* $d < -4, D > 0$ *of coprime fundamental discriminants such that* p *is good for the pair* $(-d, D)$ *and inert in* $\mathbf{Q}(\sqrt{D})$*. In addition, we have*

$$\#\mathbf{SS}_1 \leq O(1)p^{\frac{3}{4}} \log p. \tag{9}$$

In particular,

$$\lim_{p\to\infty} \frac{\#\mathbf{SS}_1}{\#\mathbf{SS}} = 0. \tag{10}$$

As a consequence of (9), the list in (8) is a complete list of primes $p \geq 5$ *such that* $\mathbf{SS} = \mathbf{SS}_1$*.*

Ogg [Ogg75] proved that the primes p that appear in (8) are exactly those (other than 2 and 3) such that $\mathbf{SS} = \mathbf{SS}_1$. We provide a new proof of this theorem, following work of Kaneko [Kan89], and provide the concrete bound (9) on the number of supersingular j-invariants that can lie in $\mathbf{F}_p$.

Corollary 1.5. *For* p *in the list (8), if* $d < -4, D > 0$ *are coprime fundamental discriminants such that* p *is good for the pair* $(-d, D)$ *and inert in* $\mathbf{Q}(\sqrt{D})$*, then the infinite tuple* $\mathbf{u}_{d,D}$ *defined in Corollary 1.3 vanishes modulo* p*.*

Remark 5. Corollary 1.5 implies that a positive proportion of twisted Hecke traces are a multiple of

$$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 = 269827498351476065.$$

Example 2. We illustrate Corollary 1.5 by setting $-d = -13$, $D = 19$. The primes $p = 5, 7$, and 11 satisfy the conditions of the corollary for the pair $(-13, 19)$. We check that

$$A(13, 19) = -768928363819511222250 \equiv 0 \pmod{5 \cdot 7 \cdot 11}$$
$$A(2^2 \cdot 13, 19) = 1065892589744245239388924594582357245696000 \equiv 0 \pmod{5 \cdot 7 \cdot 11},$$

as expected.

Remark 6. Ogg's proof depends critically on his ability to characterize those modular curves $X_0(p)$ which are hyperelliptic. To obtain this characterization, Ogg studies the automorphism groups of these modular curves. He uses the Deligne-Rapoport model [DR73] of $X_0(p)$ modulo p and a correspondence between supersingular points and Weierstrass points, which are zeros of the Wronskian of the basis of weight 2 forms on $\Gamma_0(p)$. Our proof completely bypasses this algebraic geometry by studying the space of modular forms modulo p of level 1 and filtration $p + 1$. The connection to Ogg's approach is that the space $S_2(\Gamma_0(p))$ modulo p is S_{p+1} modulo p, in that their elements have identical q-series.

It is also interesting to study the pairs $(-d, D)$ for which $\mathscr{L}_{d,D}$ maps onto a distinguished point of the image. A natural choice to consider is the Eisenstein series E_{p+1}, which is congruent to E_2 modulo p as seen in the Swinnerton-Dyer theory [SD73].

For example, observe that

$$\mathscr{L}_{1447} \equiv -23E_{140} \equiv -h(-1447)E_{140} \pmod{139}.$$

Examining the coefficients of f_{1447}, one also finds that $A(n^2, 1447) \equiv 4 \pmod{139}$ for all n with $139 \nmid n$. This behavior is typical of a general phenomenon illustrated by our characterization in Theorem 1.6 of the conditions under which $\mathscr{L}_d$ is congruent to a multiple of E_{p+1} modulo p.

Notice that in the factorization of $\mathcal{H}_{1447}$ modulo 139, given by

$$\begin{aligned}\mathcal{H}_{1447} \equiv &(x+39)^2(x+74)^2(x+79)(x+95)^2(x+103)^2(x+131)^2 \\ &\cdot(x^2+8x+8)^2(x^2+25x+94)^2(x^2+32x+23)^2 \pmod{139},\end{aligned}$$

every factor except that corresponding to $\rho = 1728 \equiv -79 \pmod{139}$ appears with the same multiplicity. One might be led to guess that the factorization of $\mathcal{H}_d$ modulo p is a multiple of E_{p+1} precisely when each factor modulo p appears with the same multiplicity, with possible exceptions at $\rho = 0$ or $\rho = 1728$.

The precise answer requires some notation. Deligne's factorization of E_{p-1}, discussed in Section 2.1, shows that E_{p-1} vanishes exactly at the set $\mathbf{SS}$. Using this in conjunction with Deuring's theorem on supersingular reductions of elliptic curves with complex multiplication discussed in Section 2.3 we in fact know that $\mathcal{H}_{d,D}$ always factors into a product

$$\widetilde{\mathcal{H}}_{d,D}(X) = \prod_{\rho \in \mathbf{SS}} (X-\rho)^{e_{p,d,D,\rho}} \tag{11}$$

over $\mathbf{F}_{p^2}$ when the pair $(-d, D)$ is good for p. There is an ambiguity of sign of certain exponents $e_{p,d,D,\rho}$ when p splits in $\mathbf{Q}(\sqrt{D})$ corresponding a choice of prime ideal over p. As explained in the proof of Lemma 3.1, our discussion is with respect to a fixed choice of prime $\mathfrak{p}$ over p of $\mathbf{Q}(\sqrt{D})$. When a choice of prime over p is made for two twists, D and D', as in Theorems 1.10 and 1.11, we will explicitly work with a choice of prime $\mathfrak{p}^*$ over p in $\mathbf{Q}(\sqrt{D}, \sqrt{D'})$.

A special consideration arises at j-invariants corresponding to the points i and $e^{\frac{2\pi i}{3}}$, which have nontrivial stabilizers under the action of $\mathrm{PSL}_2(\mathbf{Z})$ on the upper half-plane. The corresponding values of the j-function are 1728 and 0. For supersingular reductions of the corresponding CM elliptic curves, we add a scaling factor ω_ρ defined to be 3 if $\rho = 0$ and 2 if $\rho = 1728$. Otherwise, we set $\omega_\rho = 1$. We then define Exp to be the $\mathbf{F}_p$-vector space consisting of vectors $(\omega_\rho e_\rho)_{\rho \in \mathbf{SS}}$ with $e_\rho \in \mathbf{F}_p$.

We define a vector in Exp to be *flat* if it is of the form $(\ell)_\rho = (\ell, \ldots, \ell)$ for some $\ell \in \mathbf{F}_p$. We define the *vector of exponents* $\mathbf{e}_{d,D}$ of $\mathcal{H}_{d,D}$ to be the vector $(\omega_\rho e_{p,d,D,\rho})_{\rho \in \mathbf{SS}} \pmod{p}$ obtained from $\mathcal{H}_{d,D}$ using (11). (If p splits in $\mathbf{Q}(\sqrt{D})$, this definition is with respect to a fixed choice of prime of $\mathbf{Q}(\sqrt{D})$ over p.) We also set $\mathbf{e}_d = \mathbf{e}_{d,1}$.

In this language, we state a simple criterion for $\mathscr{L}_d$ to be congruent to a multiple of E_{p+1} modulo p. We also mention consequences that follow from the work of Baker [Bak98] discussed in Section 2.4.

Theorem 1.6. *Suppose that $-d < -4$ and $p \geq 5$ is a prime good for $-d$. Then the following are equivalent.*

(i) $\mathscr{L}_d \equiv -h(-d)E_{p+1} \pmod{p}$.
(ii) *The vector of exponents of $\mathcal{H}_d$ is flat.*
(iii) $\mathcal{H}_d \equiv \Delta^{-h(-d)} \widetilde{f}^p \pmod{p}$, *where f is a holomorphic modular form.*
(iv) *For $p \nmid n$, $A(n^2, d) \equiv -24h(-d) \pmod{p}$.*

If $p \nmid h(-d)$ and these equivalent conditions hold then the following are true. Here $\mathscr{L}_d^*$ is the weight $p+1$ lift of $\mathscr{L}_d$ defined in Theorem 1.2.

(1) *For all supersingular elliptic curves E, we have* $\mathscr{L}_d^*(E)^{p-1} \equiv -\left(\frac{-1}{p}\right)\Delta(E)^{\frac{p^2-1}{12}} \pmod{p}$.
(2) *For all supersingular elliptic curves E defined over $\mathbf{F}_p$, we have:*
   (a) *If $|E(\mathbf{F}_{p^2})| = (p+1)^2$, then $\mathscr{L}_d^*(E) \in \mathbf{F}_p^\times$.*
   (b) *If $|E(\mathbf{F}_{p^2})| = (p-1)^2$, then $\mathscr{L}_d^*(E)^2 \in \mathbf{F}_p^\times$, but $\mathscr{L}_d(E) \notin \mathbf{F}_p^\times$.*

Remark 7. The theorem also holds for $\mathscr{L}_{d,D}$ with $D > 1$, but is trivial because in this case, $\mathscr{L}_{d,D}$ is a cusp form. Thus $\mathscr{L}_{d,D}$ can only be congruent to a multiple of E_{p+1} modulo p if $\mathscr{L}_{d,D} \equiv 0 \pmod{p}$, which happens if and only if $e_{d,D} \equiv 0 \pmod{p}$.

We can also obtain a lower bound on the class number for a congruence of the type described by Theorem 1.6 to hold.

Corollary 1.7. *Suppose that $-d < -4$ and $p \geq 5$ is a prime good for $-d$. If $\mathscr{L}_d \equiv kE_{p+1} \pmod{p}$ for $k \in \mathbf{F}_p$, then $h(-d) < \dim(\mathrm{Exp})$.*

Let $\mathcal{P}_d$ denote the $\mathbf{F}_p$-vector space of polynomials of degree $\leq d$ over $\mathbf{F}_p$. There is a notion of an "associated polynomial" for a modular form in $\widetilde{M}_k$ discussed in Section 2.1. This defines a map

$$\widetilde{M}_{p+1} \to \mathcal{P}_{n-1}, \tag{12}$$

where $n = \dim(\widetilde{M}_{p+1})$.

The set **SS** is stable under the Frobenius automorphism σ, as will be shown in Lemma 3.1. By permuting the conjugate elements of the basis of Exp, the Frobenius automorphism extends to a linear involution that we will also denote by σ. We define Exp^* to be the subspace fixed by σ and define $\widetilde{M}^*_{p+1}$ to be the image of Exp^* in $\widetilde{M}_{p+1}$ via the map defined in the proof of Theorem 1.2 (the image is independent of the choice of $\alpha \in \mathbf{F}_p$). We define $\mathrm{Exp}^{*\perp} \subseteq \mathrm{Exp}$ to be the subspace of vectors $\mathbf{v}$ such that $\sigma\mathbf{v} = -\mathbf{v}$ and $\widetilde{M}^{*\perp}_{p+1}$ to be its image in $\widetilde{M}_{p+1}$, also under the map defined in the proof of Theorem 1.2. We obtain a decomposition

$$\mathrm{Exp} = \mathrm{Exp}^* \oplus \mathrm{Exp}^{*\perp}. \tag{13}$$

It is natural to ask whether the map taking the set of twisted Hilbert class polynomials $\mathcal{H}_{d,D}$ such that p is good for $(-d, D)$ to the reduction modulo p of their logarithmic derivatives surjects onto $\widetilde{M}_{p+1}$. This question leads us naturally to consider the images of Exp^* and $\mathrm{Exp}^{*\perp}$ in $\widetilde{M}_{p+1}$, as in the following.

Theorem 1.8. *Fix a prime p. For $\alpha \in \mathbf{F}_p^\times$ and $\beta \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$ such that $\beta^2 \in \mathbf{F}_p$, we obtain associated commutative diagrams of $\mathbf{F}_p$-vector spaces*

$$\begin{array}{ccc} \mathrm{Exp}^* & \xrightarrow{\phi_\alpha} & \mathcal{P}_{n-1} \\ {\scriptstyle\lambda_\alpha}\downarrow\wr & & \downarrow\wr \\ \widetilde{M}^*_{p+1} & \hookrightarrow & \widetilde{M}_{p+1} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathrm{Exp}^{*\perp} & \xrightarrow{\psi_\beta} & \mathcal{P}_{n-1} \\ {\scriptstyle\mu_\beta}\downarrow\wr & & \downarrow\wr \\ \widetilde{M}^{*\perp}_{p+1} & \hookrightarrow & \widetilde{M}_{p+1} \end{array}, \tag{14}$$

with isomorphisms as indicated. These families of diagrams collapse under the projectivization functor $\mathbf{P}(\cdot)$ into two diagrams of projective spaces over $\mathbf{F}_p$ given by

$$\begin{array}{ccc} \mathbf{P}\mathrm{Exp}^* & \xrightarrow{\mathbf{P}\phi} & \mathbf{P}\mathcal{P}_{n-1} \\ {\scriptstyle\mathbf{P}\lambda}\downarrow\wr & & \downarrow\wr \\ \mathbf{P}\widetilde{M}^*_{p+1} & \hookrightarrow & \mathbf{P}\widetilde{M}_{p+1} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbf{P}\mathrm{Exp}^{*\perp} & \xrightarrow{\mathbf{P}\psi} & \mathbf{P}\mathcal{P}_{n-1} \\ {\scriptstyle\mathbf{P}\mu}\downarrow\wr & & \downarrow\wr \\ \mathbf{P}\widetilde{M}^{*\perp}_{p+1} & \hookrightarrow & \mathbf{P}\widetilde{M}_{p+1} \end{array}. \tag{15}$$

Moreover, the images of $\mathbf{P}\lambda$ and $\mathbf{P}\mu$ are disjoint projective linear subspaces. In fact,

$$\widetilde{M}_{p+1} = \widetilde{M}^*_{p+1} \oplus \widetilde{M}^{*\perp}_{p+1}. \tag{16}$$

Remark 8. As a consequence of Theorem 1.8, if p is good for the pairs $(-d, D)$ and $(-d', D')$ and $\left(\frac{D}{p}\right) \neq \left(\frac{D'}{p}\right)$, then $\mathscr{L}_{d,D}$ and $\mathscr{L}_{d',D'}$ are congruent modulo p if and only if they both vanish modulo p. In terms of Hecke traces, $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \pmod{p}$ if and only if $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \equiv 0 \pmod{p}$.

Corollary 1.9. *For primes p outside of the list in (8), the reduction map on the set of all $\mathscr{L}_{d,D}$ such that p is good for the pair $(-d, D)$ does not surject onto $\widetilde{M}_{p+1}$. Moreover,*

$$\lim_{p\to\infty} \frac{\dim \mathrm{Exp}^*}{\dim \mathrm{Exp}} = \frac{1}{2} \qquad \textit{and} \qquad \lim_{p\to\infty} \frac{\dim \mathrm{Exp}^{*\perp}}{\dim \mathrm{Exp}} = \frac{1}{2}. \tag{17}$$

We apply the methods and results of this paper to obtain some consequences for p-adic properties of twisted Hilbert class polynomials. For small class numbers, Theorem 1.2 allows us to determine the residue classes of the twisted Hilbert class polynomials $\mathcal{H}_{d,D}$. We can also use an argument similar to that used in Theorem 1.2 to show that the inverses of certain Hilbert class polynomials are congruent to holomorphic modular forms modulo p.

In order to formalize the notion of congruence between twisted Hilbert class polynomials, we need to define when two Laurent series $f \in \mathbf{Q}(\sqrt{D})((q)), g \in \mathbf{Q}(\sqrt{D'})((q))$ are congruent modulo p. In all cases, we will assume that $D \equiv D' \pmod{p}$.

If p splits in $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{D'})$, we choose prime ideals $\mathfrak{p}, \mathfrak{p}'$ lying over p in $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{D'})$, respectively, such that $\sqrt{D} = \sqrt{D'}$ via the unique isomorphism of the residue fields modulo $\mathfrak{p}$ and $\mathfrak{p}'$. We define $\mathfrak{p}^* \subseteq \mathcal{O}_{\mathbf{Q}(\sqrt{D},\sqrt{D'})}$ over p to be the unique prime lying over the ideals $\mathfrak{p}$ and $\mathfrak{p}'$.

If p is inert in $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt{D'})$, we define $\mathfrak{p}^* \subseteq \mathcal{O}_{\mathbf{Q}(\sqrt{D},\sqrt{D'})}$ to be the prime ideal lying over p such that $\sqrt{D} = \sqrt{D'}$ in the residue field.

We now write $f \equiv g \pmod{\mathfrak{p}^*}$, meaning the comparison is taken over $\mathcal{O}_{\mathbf{Q}(\sqrt{D},\sqrt{D'})}$.

We define the quantity $m_{d,D}$ by

$$m_{d,D} = \max_{\rho \in \mathbf{SS}} \{|\omega_\rho e_{p,d,D,\rho}|\}, \tag{18}$$

and set $m_d = m_{d,1}$. For the purposes of the bound in Theorem 1.10, we also define

$$m^*_{d,D} = \max_{\rho \in \mathbf{SS}} \{|e_{p,d,D,\rho}|\}, \tag{19}$$

and set $m^*_d = m^*_{d,1}$. Note that $m^*_d \le h(-d)$ and $m^*_{d,D} \le \frac{h(-dD)}{2}$ for $D > 1$.

Theorem 1.10. *Let $d, d' < -4$ be fundamental discriminants. Let $p \ge 5$ be a prime good for d and d'. If $\max\{m^*_d, m^*_{d'}\} < p$, then*

$$\mathcal{H}_d \equiv \mathcal{H}_{d'} \pmod{p} \textit{ if and only if } \mathscr{L}_d \equiv \mathscr{L}_{d'} \pmod{p}.$$

Let (d, D) and (d', D') be pairs of coprime fundamental discriminants such that $d, d' < -4$ and $D, D' > 1$. Let $p \ge 5$ be a prime good for the pairs $(-d, D)$ and $(-d', D')$. Moreover, suppose that $D \equiv D' \pmod{p}$. If $m^*_{d,D} + m^*_{d',D'} < p$, then

$$\mathcal{H}_{d,D} \equiv \mathcal{H}_{d',D'} \pmod{\mathfrak{p}^*} \textit{ if and only if } \mathscr{L}_{d,D} \equiv \mathscr{L}_{d',D'} \pmod{\mathfrak{p}^*}.$$

Example 3. It is easy to find examples of d, d', D, D', and p which satisfy the conditions of Theorem 1.10. For example, setting $D = D' = 1$, let $d = 323$, $d' = 723$, and $p = 283$. Note that $m_{-323}, m_{-723} \le h(-323) = h(-723) = 4 < 283$. A calculation shows that $\mathscr{L}_{323} \equiv \mathscr{L}_{723} \pmod{283}$,

which by the corollary implies that

$$\begin{aligned}\mathcal{H}_{323} =& j^4 + 331776588700918528000000j^3 - 4948460732929411210910105600000000j^2 \\ &+ 738045621141021680417888010240000000000000j \\ &- 121974636783103604190112617857024000000000000 \\ \equiv& j^4 + 40j^3 + 36j^2 + 226j + 32 \\ \equiv& j^4 + 485569010710322513612071853606092800 0j^3 \\ &+ 82224507709086980235468281972471455473991680000000j^2 \\ &- 17437817166277457429521660531780027831812096000000000j \\ &+ 43799003445375960815587788104700084092928000000000000000 \\ =& \mathcal{H}_{723} \pmod{283}.\end{aligned}$$

The corollaries to Theorem 1.2 illustrate the many consequences of placing the modular forms $\mathscr{L}_{d,D}$ into a space of small dimension. In this way, we may better understand Hilbert class polynomials by placing them into a finite-dimensional space of modular forms.

Theorem 1.11. *Let (d, D) be a pair of coprime fundamental discriminants, and let $p \geq 5$ be a prime that is good for the pair $(-d, D)$. If p splits in $\mathbf{Q}(\sqrt{D})$, fix a prime ideal $\mathfrak{p}$ lying over $\sqrt{D}$. Otherwise, set $\mathfrak{p} = (p)$. There exists a holomorphic modular form $\mathcal{H}^*_{d,D}$ of weight $m_{d,D}(p-1)$ such that*

$$\mathcal{H}^{-1}_{d,D} \equiv \mathcal{H}^*_{d,D} \pmod{\mathfrak{p}}.$$

Remark 9. In a manner analogous to Remark 4, we obtain congruences by applying the Hecke algebra to the forms obtained from Theorem 1.11. In particular, for p, d, D as in Theorem 1.11, the reductions of the modular forms $\left\{T_n \mathcal{H}^*_{d,D}\right\}_n$ modulo p all lie in the finite dimensional space $M_{m_{d,D}(p-1)}$. For $\lambda \in \{0, 2\}$, $\mathcal{H}^*_{d,D}$ is an eigenfunction with eigenvalue λ of a positive proportion of the prime Hecke operators T_ℓ.

Remark 10. Michel [Mic04] and Elkies, Ono, and Yang [EOY05] prove the following asymptotic for the growth of $m_{d,D}$ for fixed p. Let $\mu_p = \sum_{\rho \in \mathbf{SS}} \frac{1}{\omega_\rho}$. Asymptotically,

$$m_{d,D} = \frac{h(-dD)}{\mu_p} + O_p((dD)^{\frac{1}{2}-\eta})$$

for some constant $\eta > 0$, independent of p and D. The notation O_p means that the implied constant may depend on p.

The paper is organized as follows: In Section 2, we describe the theory of modular forms modulo p in connection with supersingular elliptic curves, as well as the Borcherds-Zagier products for $\mathcal{H}_{d,D}$. In Section 3, we prove Theorems 1.1 and 1.2. We first use Deuring's theory of supersingular reductions of elliptic curves with complex multiplication to identify poles of $\mathscr{L}_d$. We cancel out these poles modulo p using Deligne's theorem on supersingular j-invariants. In Section 4 we provide a new proof of Ogg's theorem using a bound of Kaneko. We prove Theorem 1.6 in Section 5 by showing existence and uniqueness of the solutions to the congruence $\mathscr{L}_d \equiv -h(-d)E_{p+1} \pmod{p}$ via computations in $\widetilde{M}$. In Section 6, we prove the isomorphisms in (14). We prove Theorems 1.10 and 1.11 in Section 7. We provide explicit examples to demonstrate all of the phenomena described in the paper in Section 8.

2. Preliminaries

In Section 2.1 we describe the theory of modular forms modulo a prime p, as well as Deligne's factorization of E_{p-1} modulo p. In Section 2.2, we provide Borcherds' theorem on representing

$\mathcal{H}_{d,D}$ as an infinite product with exponents $A(n^2D, d)$. In Section 2.3 we state Deuring's theorem on supersingular reductions of complex multiplication elliptic curves. We state in Section 2.4 Baker's supersingular congruences for E_{p+1}.

2.1. **Modular Forms modulo p.** Serre and Swinnerton-Dyer [SD73] proposed a theory of modular forms reduced modulo a prime $p \geq 5$. Let M be the graded algebra of modular forms with Fourier expansion in the ring $\mathbf{Z}_{(p)}[[q]]$. Then $M \cong \mathbf{Z}_{(p)}[E_4, E_6]$, where E_4 and E_6 are the Eisenstein series of weight 4 and 6 respectively. We define $\widetilde{M} \subseteq \mathbf{F}_p[[q]]$ to be the image of the map $M \to \mathbf{F}_p[[q]]$ that reduces the coefficients of the modular forms $f \in \mathbf{Z}_{(p)}[[q]]$ modulo p. Swinnerton-Dyer proves the following structure theorem for $\widetilde{M}$.

Theorem 2.1. *Let $p \geq 5$ be prime. Then we have the following.*

1. $E_{p-1} \equiv 1 \pmod{p}$ *and* $E_{p+1} \equiv E_2 \pmod{p}$.
2. $\widetilde{M} \cong \mathbf{F}_p[E_4, E_6]/(E_{p-1} - 1)$.
3. $\widetilde{M}$ *has a natural grading with values in* $\mathbf{Z}/(p-1)\mathbf{Z}$.

While we used $K = \mathbf{Q}$ for simplicity, given any algebraic number field K and prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, we may define modular forms over $(\mathcal{O}_K/\mathfrak{p})[[q]]$ in an identical manner. Replacing $\mathbf{F}_p$ with $\mathcal{O}_K/\mathfrak{p}$, Theorem 2.1 holds.

Swinnerton-Dyer defines the *filtration* $\omega(\widetilde{f})$ of a modular form $\widetilde{f}$ modulo p to be the least weight of a modular form $g \in M$ such that the reduction $\widetilde{g}$ is $\widetilde{f}$. Note that modulo $p-1$, the filtration matches the grading.

The space $\widetilde{M}_{p+1}$ will be of particular interest. We have

$$\dim(M_{p+1}) = \left\lfloor \frac{p+1}{12} \right\rfloor + \epsilon_{p+1}$$

where

$$\epsilon_k = \begin{cases} 0 & \text{if } k \equiv 2 \pmod{12} \\ 1 & \text{otherwise} \end{cases}.$$

We also have that

$$\dim(\widetilde{M}_{p+1}) = \dim(M_{p+1}) = \left\lfloor \frac{p+1}{12} \right\rfloor + \epsilon_{p+1}. \tag{20}$$

We will also be interested in relating the supersingular j-invariants to the space of modular forms modulo p. Any modular form $f(\tau)$ can be written uniquely in the form

$$f(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\epsilon F(f, j(\tau)) \text{ with } m \in \mathbf{Z}_{\geq 0}, \delta \in \{0,1,2\}, \text{ and } \epsilon \in \{0,1\} \tag{21}$$

for some polynomial $F(f, x)$ of degree $\leq m$. Here j is the Klein modular function.

The following result of Deligne [KZ98] precisely determines the zeros of $\widetilde{F}(E_{p-1}, j(\tau))$. As in Section 1, denote by **SS** the set of j-invariants modulo p.

Theorem 2.2. *We have*

$$j(\tau)^\delta (j(\tau) - 1728)^\epsilon \widetilde{F}(E_{p-1}, j(\tau)) = \prod_{\rho \in \mathbf{SS}} (j(\tau) - \rho) \pmod{p}.$$

Note that if $f(\tau) = E_{p-1}$, the corresponding value for m is exactly $\left\lfloor \frac{p-1}{12} \right\rfloor$. Thus we can extend (20) to

$$\dim(\text{Exp}) = \#\mathbf{SS} = \left\lfloor \frac{p+1}{12} \right\rfloor + \epsilon_{p+1} = \dim(\widetilde{M}_{p+1}). \tag{22}$$

2.2. **Borcherds-Zagier Theory.** The work of Borcherds and Zagier [Bor95a, Zag02] connects the coefficients $A(n^2, d)$ defined in the introduction to the Hilbert class polynomial of discriminant d. In this section, $H(-d)$ refers to the Hurwitz-Kronecker class number $\sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{\omega_Q}$. For fundamental discriminants satisfying $-d < -4$, this is equivalent to the usual class number. Borcherds [Bor95a] proved that the Hilbert class polynomials can be written as an infinite product involving the coefficients of the f_d's.

Theorem 2.3. *For any choice of $-d < 0$, the polynomial $\mathcal{H}_d$ defined in (4) can be written as*

$$\mathcal{H}_d(j(\tau)) = q^{-H(-d)} \prod_{n=1}^{\infty} (1-q^n)^{A(n^2,d)}.$$

Theorem 2.3 shows that most of the information about the coefficients of the Hilbert class polynomials are encoded in the coefficients $A(n^2, d)$. Nevertheless, the $A(n^2, d)$ a priori do not give any information about the class number $h(-d)$. Theorem 1.1 reveals that the coefficients $A(n^2, d)$ together with knowledge of the modular forms modulo p with filtration $p + 1$ already determine whether $p|h(-d)$ for suitable primes p.

Zagier [Zag02] generalized Borcherds' product to the twisted setting.

Theorem 2.4. *For any coprime fundamental discriminants $d, D > 0$, the polynomial $\mathcal{H}_{d,D}$ defined in (5) can be written as*

$$\mathcal{H}_{d,D}(j(\tau)) = \prod_{n=1}^{\infty} P_D(q^n)^{A(n^2D,d)},$$

where

$$P_D(t) = \exp\left(-\sqrt{D} \sum_{r=1}^{\infty} \left(\frac{D}{r}\right) \frac{t^r}{r}\right) \in \mathbf{Q}(\sqrt{D})[[t]].$$

Zagier [Zag02] relates the coefficients $A(n^2D, d)$ to twisted Hecke traces of singular moduli. We define a sequence of functions $J_n(\tau)$ by setting $J_n(\tau)$ to be the unique modular function on $\mathrm{SL}_2(\mathbf{Z})$ with q-series

$$J_n(\tau) = q^{-n} + O(q) \tag{23}$$

at the cusp. Then the *twisted Hecke traces* $t_m(d, D)$ for coprime fundamental discriminants $d < 0$, $D > 0$ are defined by

$$t_n(d, D) = \frac{1}{\sqrt{D}} \sum_{Q \in \mathcal{Q}_{dD}/\Gamma} \chi_{d,D}(Q) J_n(\alpha_Q). \tag{24}$$

Zagier proves that

$$t_n(d, D) = \sqrt{D} \sum_{k|n} k \left(\frac{D}{n/k}\right) A(k^2 D, d). \tag{25}$$

As a final remark, the weights ω_Q are nontrivial only when $d = 3$ or 4. For the remainder of the paper, we will consider only $-d < -4$. In this case the Hurwitz-Kronecker class number $H(-d)$ is the usual class number $h(-d)$ and the Hilbert class polynomials are exactly

$$\mathcal{H}_d(j(\tau)) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (j(\tau) - j(\alpha_Q)). \tag{26}$$

2.3. **Deuring's Theorem.** We make use of a theorem of Deuring [Deu41, Lan87] that classifies the supersingular reductions of elliptic curves with complex multiplication.

Theorem 2.5. *Let E be an elliptic curve over a number field K with complex multiplication by the endomorphism ring $\mathcal{O}_{\mathbf{Q}(\sqrt{-d})}$ and let $\mathfrak{P}$ be a prime ideal lying over p. If E has good reduction at $\mathfrak{P}$, then the reduction of E modulo $\mathfrak{P}$ is supersingular if and only if p does not split in $\mathbf{Q}(\sqrt{-d})$.*

We also note that for any rational prime p, any complex multiplication curve over K has a model with good reduction at some prime $\mathfrak{P}$ of K over p.

2.4. **Baker's Theorem.** Fix a prime p. In view of Theorem 1.6, we are interested in the values of E_{p+1} at supersingular elliptic curves in order to provide information about $\mathscr{L}_d$. Baker's theorem [Bak98] provides a restricted set of possible values for E_{p+1}.

Theorem 2.6. *If $p \geq 5$ is prime, then*

$$(E_{p+1})^{p-1} \equiv -\left(\frac{-1}{p}\right) \Delta^{\frac{p^2-1}{12}} \pmod{(p, E_{p-1})}$$

as elements of $\mathbf{Z}_{(p)}[E_4, E_6]$.

Moreover, Baker calculates explicit values of $\Delta^{\frac{p^2-1}{12}}$ at supersingular elliptic curves defined over $\mathbf{F}_{p^2}$.

Theorem 2.7. *If $p \geq 5$ is prime, and if E is a supersingular elliptic curve defined over $\mathbf{F}_{p^2}$, we have*

$$\Delta(E)^{\frac{p^2-1}{12}} \equiv \begin{cases} -\left(\frac{-1}{p}\right) \pmod{(p, E_{p-1})} & \text{if } |E(\mathbf{F}_{p^2})| = (1+p)^2 \\ \left(\frac{-1}{p}\right) \pmod{(p, E_{p-1})} & \text{if } |E(\mathbf{F}_{p^2})| = (1-p)^2 \end{cases}.$$

Combining these two theorems gives us explicit values of $(E_{p+1})^{p-1}$ at supersingular elliptic curves defined over $\mathbf{F}_{p^2}$.

Corollary 2.8. *If $p \geq 5$ is prime, and if E is a supersingular elliptic curve defined over $\mathbf{F}_{p^2}$, we have*

$$E_{p+1}(E)^{p-1} \equiv \begin{cases} 1 \pmod{(p, E_{p-1})} & \text{if } |E(\mathbf{F}_{p^2})| = (1+p)^2 \\ -1 \pmod{(p, E_{p-1})} & \text{if } |E(\mathbf{F}_{p^2})| = (1-p)^2 \end{cases}.$$

3. Proofs of Theorems 1.1 and 1.2

Here we prove Theorem 1.1 and Theorem 1.2 using the theory of modular forms modulo p.

Reduction of Theorem 1.1 to Theorem 1.2. Expressing $\mathscr{L}_d$ using Borcherds' representation of $\mathcal{H}_d$ in Theorem 2.3, we may write $\mathscr{L}_d$ as a q-series

$$\begin{aligned} \mathscr{L}_d &= -h(-d) - \sum_{n=1}^{\infty} \frac{A(n^2, d) n q^n}{1 - q^n} \\ &= -h(-d) - \sum_{n=1}^{\infty} \sum_{k|n} A(k^2, d) k q^n \\ &= -h(-d) + \mathscr{F}_d. \end{aligned}$$

By Theorem 1.2, then there exists a modular form $\mathscr{L}_d^*$ of weight $p+1$ such that $\mathscr{L}_d^* \equiv \mathscr{L}_d \pmod{p}$. If p divides $h(-d)$, then $\mathscr{L}_d^* \equiv \mathscr{L}_d \equiv \mathscr{F}_d \pmod{p}$. Let kp be the leading coefficient of $\mathscr{L}_d^*$. Replacing $\mathscr{L}_d^*$ with $\mathscr{L}_d^* - kpE_{p+1}$ yields a *cusp* form that reduces to $\mathscr{F}_d$ modulo p.

For the converse, suppose that there exists a cusp form $f \in \widetilde{M}_{p+1}$ such that $f \equiv \mathscr{F}_d \pmod p$. Subtracting $h(-d)$ from both sides, we find $f - h(-d) \equiv \mathscr{L}_d \equiv \mathscr{L}_d^* \pmod p$, which yields $h(-d) \equiv f - \mathscr{L}_d^* \pmod p$. The left hand side of this expression, a constant, is a modular form of grading $0 \in \mathbf{Z}/(p-1)\mathbf{Z}$, unless $p|h(-d)$. The right hand side is a modular form of grading $2 \in \mathbf{Z}/(p-1)\mathbf{Z}$. Thus, we must in fact have $p|h(-d)$.

□

Thus to prove Theorem 1.1, it suffices to prove Theorem 1.2. For this we will need the following lemma.

Lemma 3.1. *The Frobenius automorphism σ acts as an involution on the set* **SS** *of supersingular j-invariants modulo p. Moreover, the twisted Hilbert class polynomials have divisors supported on* **SS**.

The subspace $\mathrm{Exp}^* \subseteq \mathrm{Exp}$ *fixed by σ contains all vectors of exponents $\mathbf{e}_{d,D}$ associated to pairs of coprime fundamental discriminants $-d < 0$ and $D > 0$ such that p is good for the pair $(-d, D)$ and p splits in $\mathbf{Q}(\sqrt{D})$.*

The subspace $\mathrm{Exp}^{*\perp} \subseteq \mathrm{Exp}$ *of vectors $\mathbf{v}$ satisfying $\sigma\mathbf{v} = -\mathbf{v}$ contains all vectors of exponents $\mathbf{e}_{d,D}$ associated to pairs of coprime fundamental discriminants $-d < 0$ and $D > 0$ such that p is good for the pair $(-d, D)$ and p is inert in $\mathbf{Q}(\sqrt{D})$.*

Proof. The supersingular j-invariants are the roots of the polynomial $F(E_{p-1}, j(\tau))$ and possibly 0 or 1728. The coefficients of $F(E_{p-1}, j(\tau))$ lie in $\mathbf{Z}_{(p)}$, so the coefficients of $\widetilde{F}(E_{p-1}, j(\tau))$ lie in $\mathbf{F}_p$, and thus the image of a root under the Frobenius automorphism σ is also a root. Since $\mathbf{SS} \subseteq \mathbf{F}_{p^2}$ and 0 and 1728 are self-conjugate, σ preserves the set **SS**. Thus the Frobenius automorphism, which is an involution on $\mathbf{F}_{p^2}$, acts as an involution on **SS**.

For every quadratic form Q of discriminant $-dD$, the endomorphism ring of the elliptic curve $\mathbf{C}/\langle 1, \alpha_Q\rangle$ is $\mathcal{O}_{\mathbf{Q}(\sqrt{-dD})}$. Let $\mathfrak{P}$ be a prime ideal lying over p in the minimal Galois extension $K_{d,D}$ of $\mathbf{Q}$ containing the $j(\alpha_Q)$ for all $Q \in \mathcal{Q}_{dD}$. By Theorem 2.5, the reductions modulo $\mathfrak{P}$ of elliptic curves with j-invariant $j(\alpha_Q)$ are supersingular whenever p is good for the pair $(-d, D)$. Hence when p is good for the pair $(-d, D)$, the reductions of $j(\alpha_Q)$ over $\mathfrak{P}$ are exactly the reductions of supersingular j-invariants over p.

Although the values of the reductions of $j(\alpha_Q)$ modulo $\mathfrak{P}$ are dependent on the choice of $\mathfrak{P}$, we are only concerned with reductions of $\mathcal{H}_{d,D}$ and $\mathscr{L}_{d,D}$. The former has coefficients in $\mathbf{Q}(\sqrt{D})$, so there is ambiguity only over the choice of prime over p if p splits in $\mathbf{Q}(\sqrt{D})$, and none if p is inert. If p is split, our discussion will be with respect to a fixed prime $\mathfrak{p}$ of $\mathbf{Q}(\sqrt{D})$ over p and (although the reduction is unaffected by this choice) a fixed prime $\mathfrak{P}$ of $K_{d,D}$ over $\mathfrak{p}$. If p is inert, we fix any prime $\mathfrak{P}$ of $K_{d,D}$ over p. The latter function $\mathscr{L}_{d,D}$ has a q-series with integer coefficients, so its reduction does not depend on the choice of prime $\mathfrak{P}$ of $K_{d,D}$ over p and lies in $\mathbf{F}_p$ – we will assume a fixed choice of $\mathfrak{P}$ in our discussion. We will hereafter write modulo p where we mean modulo $\mathfrak{P}$ for a prime $\mathfrak{P}$ over p fixed in the manner just described.

When p is good for the pair $(-d, D)$, the numerator and denominator of the rational function

$$\mathcal{H}_{d,D}(j(\tau)) = \prod_{Q \in \mathcal{Q}_{dD}/\Gamma} (j(\tau) - j(\alpha_Q))^{\chi_{d,D}(Q)}$$

factor into linear terms $(x - \rho)$ over $\mathbf{F}_{p^2}$, where $\rho \in \mathbf{SS}$. Thus the vector of exponents of the reduction $\widetilde{\mathcal{H}}_{d,D}$ of $\mathcal{H}_{d,D}$ modulo p corresponds to an element of Exp.

Case 1: The prime p splits in $\mathbf{Q}(\sqrt{D})$. Note that the numerator and denominator of $\widetilde{\mathcal{H}}_{d,D}(j(\tau))$ have coefficients in $\mathbf{F}_p$ by Remark 2 together with the assumption that p splits in $\mathbf{Q}(\sqrt{D})$. Since σ

fixes $\mathbf{F}_p$ and thus $\widetilde{\mathcal{H}}_{d,D}$, conjugate roots or poles have the same multiplicity. Thus $\mathbf{e}_{d,D}$ is invariant under the action of σ on Exp and thus lies in Exp^*.

Case 2: The prime p is inert in $\mathbf{Q}(\sqrt{D})$. Denote by $\widehat{\sigma}$ the nontrivial automorphism in $\mathrm{Gal}(\mathbf{Q}(\sqrt{D})/\mathbf{Q})$. Observe that $\widehat{\sigma}$ acts as the Frobenius automorphism σ in the residue field $\mathbf{F}_{p^2}$ when the Hilbert polynomial is reduced modulo p, since p is inert in $\mathbf{Q}(\sqrt{D})$. By Remark 2, we find that $\mathrm{ord}_\rho \widetilde{\mathcal{H}}_{d,D} = -\mathrm{ord}_{\sigma\rho} \widetilde{\mathcal{H}}_{d,D}$, where $\mathrm{ord}_\rho(\cdot)$ denotes order of vanishing at ρ. By definition of $\mathrm{Exp}^{*\perp}$, this implies that $\mathbf{e}_{d,D} \in \mathrm{Exp}^{*\perp}$.

□

Proof of Theorem 1.2. Theorem 2.4 shows that

$$\mathcal{H}_{d,D}(j(\tau)) = \prod_{n=1}^{\infty} \exp\left(-\sqrt{D}\sum_{r=1}^{\infty}\left(\frac{D}{r}\right)\frac{q^{nr}}{r}\right)^{A(n^2D,d)}.$$

From this and (7) we obtain

$$\mathscr{L}_{d,D} = \sum_{n=1}^{\infty} -A(n^2D,d)\sum_{r=1}^{\infty}\left(\frac{D}{r}\right)nq^{nr} = -\sum_{n=1}^{\infty}\left(\sum_{k|n} A(k^2D,d)\left(\frac{D}{n/k}\right)k\right)q^n. \tag{27}$$

In particular, $\mathscr{L}_{d,D}$ has integer coefficients, and thus has a unique reduction modulo p.

We also have, from (26),

$$\mathscr{L}_{d,D} = \frac{1}{\sqrt{D}}\sum_{Q\in\mathcal{Q}_{dD}/\Gamma}\frac{\chi_{d,D}(Q)\Theta(j(\tau))}{j(\tau)-j(\alpha_Q)}. \tag{28}$$

Since $\mathcal{H}_{d,D}(j(\tau))$ is a modular function, $\mathscr{L}_{d,D}$ is a meromorphic modular form of weight 2. We would like to show that the reduction of $\mathscr{L}_{d,D}$ modulo p is in $\widetilde{M}_{p+1}$. We do so essentially by showing that the denominator of $\mathscr{L}_{d,D}$ modulo p divides E_{p-1}.

As before, we define $\mathbf{SS}_1$ to be the set of supersingular j-invariants lying in $\mathbf{F}_p$. Using Lemma 3.1, we also define $\mathbf{SS}_2$ to contain a single representative for each conjugate pair of supersingular j-invariants lying in $\mathbf{F}_{p^2}$.

Case 1: The prime p splits in $\mathbf{Q}(\sqrt{D})$. Note that we can apply this argument to any element of Exp^*, replacing $\sqrt{D}$ by any element $\alpha \in \mathbf{F}_p^\times$.

By Lemma 3.1, since the divisor of $\mathcal{H}_{d,D}$ is supported on $\mathbf{SS}$ and the multiplicities of conjugate roots are equal, we may write

$$\mathscr{L}_{d,D} \equiv \frac{\Theta(j(\tau))}{\sqrt{D}}\left(\sum_{\rho\in\mathbf{SS}_1}\frac{m_\rho}{j(\tau)-\rho} + \sum_{\rho\in\mathbf{SS}_2}\frac{(2j(\tau)+a_\rho)m_\rho}{j(\tau)^2+a_\rho j(\tau)+b_\rho}\right) \pmod p. \tag{29}$$

where $a_\rho, b_\rho \in \mathbf{F}_p$ are the coefficients of the minimal polynomial of $\rho \in \mathbf{SS}_2$ and m_ρ is the multiplicity of the root ρ in the factorization of $\mathcal{H}_d \pmod p$.

Note that when we compute the reduction of the right hand side of (29) modulo p, we implicitly choose a prime ideal lying over p in $\mathbf{Q}(\sqrt{D})$. By (27), the left hand side of (29) has integer coefficents, so the reduction does not depend on the choice of prime ideal. Thus there is no ambiguity introduced by the presence of a $\sqrt{D}$ in this expression.

We can then combine these terms over a common denominator:

$$\mathscr{L}_{d,D} \equiv \Theta(j(\tau))\frac{\widetilde{P}(j)}{\widetilde{Q}(j)j^a(j-1728)^b} \pmod p$$

where $a, b \in \{0,1\}$, $\widetilde{P}, \widetilde{Q} \in \mathbf{F}_p[j]$, and $\widetilde{Q}$ factors into distinct irreducible factors. Thus, we find that $\mathscr{L}_d$ has at most a simple pole at any supersingular j-invariant.

Case 2: The prime p is inert in $\mathbf{Q}(\sqrt{D})$. Note that we can apply this argument to any element of $\mathrm{Exp}^{*\perp}$, replacing $\sqrt{D}$ by any element $\beta \in \mathbf{F}_{p^2} \setminus \mathbf{F}$ such that $\beta^2 \in \mathbf{F}_p$.

Since $\operatorname{ord}_\rho \mathcal{H}_{d,D} = -\operatorname{ord}_{\sigma\rho} \mathcal{H}_{d,D}$ by Lemma 3.1, we have

$$\mathscr{L}_{d,D} \equiv \Theta(j(\tau)) \sum_{\rho \in \mathbf{SS}_2} \frac{\frac{\rho - \sigma\rho}{\sqrt{D}} m_\rho}{j(\tau)^2 + a_\rho j(\tau) + b_\rho} \pmod{p}. \tag{30}$$

Note that if we write $\rho = a + b\sqrt{D}$ for $a, b \in \mathbf{F}_p$, we see explicitly that $\frac{\rho - \sigma\rho}{\sqrt{D}} = 2b \in \mathbf{F}_p$, so there is no ambiguity of sign in the right hand side.

As in Case 1, we can combine the expression above, which we have observed to have all coefficients in $\mathbf{F}_p$, into an expression

$$\mathscr{L}_{d,D} \equiv \Theta(j(\tau)) \frac{\widetilde{P}(j)}{\widetilde{Q}(j)} \pmod{p}$$

where $\widetilde{P}, \widetilde{Q} \in \mathbf{F}_p[j]$, and $\widetilde{Q}$ factors into distinct irreducible factors. Note that the factors of j and $j - 1728$ do not appear in this case, so we set $a = b = 0$.

Returning to the general case, we next claim that $\deg \widetilde{P} \leq a + b + \deg \widetilde{Q} - 1$. Indeed, in every term of the sum in (29) or (30), the degree of the numerator is less than the degree of the denominator. Thus the same holds over a common denominator.

Factor

$$E_{p-1} = \underbrace{\Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\epsilon}_{R} F(E_{p-1}, j(\tau))$$

using (21), and note that $m = \deg F$. By Theorem 2.2, $\widetilde{Q}(j) | \widetilde{F}(E_{p-1}, j)$.

We may define a polynomial $\widetilde{S} \in \mathbf{F}_p[j]$ by $\widetilde{S}(j) = \frac{\widetilde{F}(E_{p-1}, j)}{\widetilde{Q}(j)}$. Choose arbitrary lifts of $\widetilde{P}$ and $\widetilde{S}$ to polynomials $P, S \in \mathbf{Z}[j]$. We have

$$\mathscr{L}_{d,D} E_{p-1} \equiv \Theta(j(\tau)) \frac{\widetilde{P}(j)}{\widetilde{Q}(j) j^a (j - 1728)^b} R \widetilde{F}(E_{p-1}, j(\tau)) \equiv -\frac{E_4^2 E_6}{\Delta} \frac{\widetilde{P}(j) R \widetilde{S}(j)}{j^a (j - 1728)^b} \pmod{p}.$$

We claim that the function

$$\mathscr{L}^*_{d,D} \triangleq -\frac{E_4^2 E_6 P(j) R S(j)}{\Delta j^a (j - 1728)^b} \equiv \mathscr{L}_{d,D} E_{p-1} \pmod{p} \tag{31}$$

is a holomorphic modular form. (See Example 5 for an explicit example of the construction of $\mathscr{L}^*_d$.)

We begin by observing that the degree of the leading term in q of the power series for $\frac{E_4^2 E_6}{\Delta j^a (j-1728)^b}$, $S(j)$, and R are $-1 + a + b, \deg \widetilde{Q} - m$, and m, respectively, while $\deg P \leq a + b + \deg \widetilde{Q} - 1$. Thus $\mathscr{L}^*_{d,D}$ is holomorphic at infinity.

Recall that $j = \frac{E_4^3}{\Delta}$. If $a = 1$, then $0 \in \mathbf{SS}$, which by Theorem 2.2 implies that $\delta \geq 1$. Thus the factor of E_4^2 together with E_4^δ in R cancel out the pole at $j = 0$. Similarly, if $b = 1$, then $\epsilon \geq 1$. Since $j - 1728 = \frac{E_6^2}{\Delta}$, the factor of E_6^ϵ from R and the factor of E_6 in the numerator cancel out the pole at $j = 1728$.

Thus, $\mathscr{L}^*_{d,D}$ is a holomorphic modular form. Since $E_{p-1} \equiv 1 \pmod{p}$ by Theorem 2.1,

$$\mathscr{L}^*_{d,D} \equiv \mathscr{L}_{d,D} E_{p-1} \equiv \mathscr{L}_{d,D} \pmod{p}$$

so that $\mathscr{L}_{d,D}$ reduces to a modular form modulo p.

Now suppose that p is bad for $(-d, D)$. Then by Theorem 2.5, we may write

$$\mathscr{L}_{d,D} \equiv \frac{\Theta(j(\tau))}{\sqrt{D}} \sum_{\rho \in \overline{\mathbf{F}}_p \setminus \mathbf{SS}} \frac{m_\rho}{j(\tau) - \rho} \pmod{p} \tag{32}$$

in $\Theta(j(\tau))\overline{\mathbf{F}}_p(j)$. By (22) we have $\#\mathbf{SS} = \dim(\widetilde{M}_{p+1})$. Fixing $\gamma \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$ with $\gamma^2 \in \mathbf{F}_p$, the linearly independent rational functions

$$\left\{\frac{\Theta(j(\tau))}{j(\tau)-\rho}\right\}_{\rho \in \mathbf{SS}_1} \bigcup \left\{\frac{\Theta(j(\tau))(2j(\tau)+a_\rho)}{j(\tau)^2 + a_\rho j(\tau) + b_\rho}\right\}_{\rho \in \mathbf{SS}_2} \bigcup \left\{\frac{\Theta(j(\tau))\gamma^{-1}(\rho - \sigma\rho)}{j(\tau)^2 + a_\rho j(\tau) + b_\rho}\right\}_{\rho \in \mathbf{SS}_2} \tag{33}$$

proven above to lie in $\widetilde{M}_{p+1}$ in fact form a basis for $\widetilde{M}_{p+1}$, viewed as a subspace of the $\mathbf{F}_p$-vector space $\Theta(j(\tau))\mathbf{F}_p(j)$. We obtain the basis

$$\left\{\frac{\Theta(j(\tau))}{j(\tau)-\rho}\right\}_{\rho \in \mathbf{SS}}$$

for the $\overline{\mathbf{F}}_p$-vector space $\widetilde{M}_{p+1} \otimes \overline{\mathbf{F}}_p \subseteq \Theta(j(\tau))\overline{\mathbf{F}}_p(j)$. Since the set

$$\left\{\frac{\Theta(j(\tau))}{j(\tau)-\rho}\right\}_{\rho \in \overline{\mathbf{F}}_p} = \left\{\frac{\Theta(j(\tau))}{j(\tau)-\rho}\right\}_{\rho \in \overline{\mathbf{F}}_p \setminus \mathbf{SS}} \bigcup \left\{\frac{\Theta(j(\tau))}{j(\tau)-\rho}\right\}_{\rho \in \mathbf{SS}}$$

is linearly independent in $\Theta(j(\tau))\overline{\mathbf{F}}_p(j(\tau))$, (32) implies that $\mathscr{L}_{d,D}$ cannot be written in the basis for $\widetilde{M}_{p+1}$ unless it vanishes.

□

Proof of Corollary 1.3. By Möbius inversion on (27), given the residue of $\mathscr{L}_{d,D}$ modulo p, we may extract the values $nA(n^2D, d)$ modulo p and thus, for $p \nmid n$, the value of $A(n^2D, d)$.

By Theorem 1.2, there are only finitely many possible residues modulo p for the $\mathscr{L}_{d,D}$. We have just seen that the residue of $\mathbf{u}_{d,D} = (A(n^2D, d))_{n \in \mathbf{Z}_{\geq 0}, p \nmid n}$ modulo p are determined by the residue of $\mathscr{L}_{d,D}$ modulo p, so the $\mathbf{u}_{d,D}$ fall into finitely many residue classes modulo p.

The congruence $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \pmod{p}$ implies the congruence $\mathscr{L}_{d,D} \equiv \mathscr{L}_{d',D'} \pmod{p}$ by (27). If p is good for the pair $(-d, D)$ and bad for the pair $(-d', D')$, Theorem 1.2 implies that $\widetilde{\mathscr{L}_{d,D}} = \widetilde{\mathscr{L}_{d',D'}} = 0$, so $\mathbf{u}_{d,D} \equiv \mathbf{u}_{d',D'} \equiv 0 \pmod{p}$.

□

4. Proof of Theorem 1.4

Suppose that p in the list (8) is good for the pair $(-d, D)$ and inert in $\mathbf{Q}(\sqrt{D})$. For primes in this list, $\mathbf{SS}_2$ is empty. For each $\rho \in \mathbf{SS}_1 = \mathbf{SS}$, Lemma 3.1 implies that

$$\operatorname{ord}_\rho \widetilde{\mathcal{H}}_{d,D}(j) = -\operatorname{ord}_{\sigma\rho} \widetilde{\mathcal{H}}_{d,D}(j) = -\operatorname{ord}_\rho \widetilde{\mathcal{H}}_{d,D}(j).$$

Examining leading coefficients, we have $\mathcal{H}_{d,D}(j) \equiv 1 \pmod{p}$. Thus $\mathscr{L}_{d,D} \equiv 0 \pmod{p}$.

To continue, we require the following bound.

Theorem 4.1 (Kaneko [Kan89])**.** *Every supersingular j-invariant contained in the prime field $\mathbf{F}_p$ is a root of some $\widetilde{\mathcal{H}}_d(X)$ with $d \leq \frac{4}{\sqrt{3}}\sqrt{p}$.*

We also require a classical bound on the class numbers $h(-d)$.

Theorem 4.2 ([Coh93])**.** *For $-d < -4$,*

$$h(-d) < \frac{1}{\pi}\sqrt{d}\log d.$$

The total number of roots of Hilbert class polynomials $\widetilde{\mathcal{H}}_d$ for $d \le \frac{4}{\sqrt{3}}\sqrt{p}$, counted with multiplicity, is

$$\sum_{\substack{d \le \frac{4}{\sqrt{3}}\sqrt{p} \\ d \equiv 0,3 \pmod 4}} h(-d) < \left(\frac{4}{\sqrt{3}}\sqrt{p}\right)\frac{1}{\pi}\sqrt{\frac{4}{\sqrt{3}}\sqrt{p}}\log\left(\frac{4}{\sqrt{3}}\sqrt{p}\right) = O(1)p^{\frac{3}{4}}\log p.$$

By Theorem 4.1, every supersingular j-invariant contained in $\mathbf{F}_p$ must be one of these roots. In particular, $\#\mathbf{SS}_1 \le O(1)p^{\frac{3}{4}}\log p$. It follows from the dimension computation in Section 2.1 that $\lim_{p\to\infty}\frac{\#\mathbf{SS}_1}{\#\mathbf{SS}} = 0$.

With the explicit bound above, we compute that $\#\mathbf{SS}_1 < \#\mathbf{SS}$ for $p \ge 950{,}000$. (Using a better bound on the class number, this can be improved to $p \ge 15{,}000$.) A search for quadratic factors in $\widetilde{\mathcal{H}}_d$ for small d shows that there exists a supersingular j-invariant in $\mathbf{F}_{p^2} \setminus \mathbf{F}_p$ for all primes less than 950,000 except those listed in (8).

Proof of Corollary 1.5. By Theorem 1.4, $\mathscr{L}_{d,D} \equiv 0 \pmod p$ for primes p and pairs $(-d, D)$ meeting the conditions of the corollary. By the same calculation as in the proof of Corollary 1.3, we find that the Hecke traces $A(n^2D, d)$ for $p \nmid n$ vanish modulo p.

□

5. Proof of Theorem 1.6

We may reduce the proof of the theorem to a computation by the following lemma.

Lemma 5.1. *Fix a prime p. For each $\alpha \in \mathbf{F}_p^\times$ or $\beta \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$ such that $\beta^2 \in \mathbf{F}_p$ there exists an injective map*

$$\lambda_\alpha : \mathrm{Exp}^* \to \widetilde{M}_{p+1} \qquad \text{or} \qquad \mu_\beta : \mathrm{Exp}^{*\perp} \to \widetilde{M}_{p+1}.$$

We define the normalized logarithmic derivative maps λ_α and μ_β to send $\{e_\rho\omega_\rho\}_{\rho\in\mathbf{SS}}$ to $\frac{\Theta(f)}{\alpha f}$ and $\frac{\Theta(f)}{\beta f}$, respectively, where

$$f = \prod_{\rho\in\mathbf{SS}}(j-\rho)^{e_\rho}.$$

Proof. The proof of Theorem 1.2 shows that the images of λ_α and μ_β lie in $\widetilde{M}_{p+1}$, so the maps are well-defined.

The logarithmic derivative of a q-series $\widetilde{f}$ coming from an element of Exp^* or $\mathrm{Exp}^{*\perp}$ is 0 modulo p if and only if the coefficients of $\widetilde{f}$ are supported only where the exponents of q are divisible by p. The latter statement is true if and only if $\widetilde{f}$ is a p^{th} power, which is the case exactly when the vector in Exp^* corresponding to $\widetilde{f}$ is 0. Thus the kernels of λ_α and μ_β are trivial and these maps are injective. □

Note that the flat vectors form a one-dimensional subspace of Exp^*. Since Lemma 5.1 shows that the map $\lambda_1 : \mathrm{Exp}^* \to \widetilde{M}_{p+1}$ is injective, to show the equivalence of (i) and (ii) it suffices to show that the image of a particular flat vector is a multiple of E_{p+1}. The factor $-h(-d)$ in the statement of the theorem follows from comparing the constant terms on both sides.

Note that since $p \ge 5$, we must have $p \equiv 1, 5, 7$, or $11 \pmod{12}$. We can write down the flat vectors as the exponent vectors of explicit modular functions $E_{p-1}C_p$, where C_p is defined by

$$C_p = \begin{cases} \Delta^{-\frac{p-1}{12}} & p \equiv 1 \pmod{12} \\ \Delta^{-\frac{p-5}{12}}E_4^{-1}j^{3^{-1}} & p \equiv 5 \pmod{12} \\ \Delta^{-\frac{p-7}{12}}E_6^{-1}(j-1728)^{2^{-1}} & p \equiv 7 \pmod{12} \\ \Delta^{-\frac{p-11}{12}}E_4^{-1}E_6^{-1}j^{3^{-1}}(j-1728)^{2^{-1}} & p \equiv 11 \pmod{12} \end{cases}. \tag{34}$$

Note that in (34), the number n^{-1} indicates a lift to $\mathbf{Z}$ of the inverse of $\widetilde{n} \in \mathbf{F}_p$. The element of Exp associated to C_p is independent of the choice of lift as the exponents e_ρ are only defined modulo p.

Noting that $j = \frac{E_4^3}{\Delta}$ and $j - 1728 = \frac{E_6^2}{\Delta}$, we have

$$C_p = \Delta^{-12^{-1}(p-1)}(\Delta^a E_4^b E_6^c)^p \pmod{p} \tag{35}$$

for some $a, b, c \in \mathbf{Z}$. Since $E_{p-1} \equiv 1 \pmod{p}$ by Theorem 2.1 and the logarithmic derivative vanishes on p^{th} powers, we have

$$\frac{\Theta(E_{p-1}C_p)}{E_{p-1}C_p} \equiv \frac{\Theta(\Delta^{-12^{-1}(p-1)})}{\Delta^{-12^{-1}(p-1)}} \equiv 12^{-1}\frac{\Theta(\Delta)}{\Delta} \pmod{p}.$$

Swinnerton-Dyer [SD73] shows that in $\widetilde{M}$, $\Theta(\Delta) = E_2\Delta$. We then have

$$\frac{\Theta(E_{p-1}C_p)}{E_{p-1}C_p} \equiv 12^{-1}\frac{\Theta(\Delta)}{\Delta} \equiv 12^{-1}E_2 \pmod{p}.$$

To see the equivalence of conditions (i) and (iv), recall that by Theorem 2.1,

$$E_{p+1} \equiv E_2 = 1 - 24\sum_{n\geq 1}\sigma(n)q^n \pmod{p}.$$

Since

$$-h(-d) - \sum_{n=1}^{\infty}\sum_{k|n} A(k^2, d)kq^n = \mathscr{L}_d \equiv -h(-d)E_{p+1} \equiv -h(-d) + h(-d)24\sum_{n\geq 1}\sigma(n)q^n \pmod{p},$$

the Möbius inversion formula implies that

$$A(n^2, d)n \equiv -24h(-d)n \pmod{p}$$

or $A(n^2, d) \equiv -24h(-d) \pmod{p}$ for $p \nmid n$. We may reverse these steps to show that (iv) implies (i).

By taking logarithmic derivatives of $\mathcal{H}_{d,D}$ and $\Delta^{-h(-d)}f^p$ and comparing to (35), we find that (iii) implies (i).

To see that (i) implies (iii), set $g = \mathcal{H}_d\Delta^{h(-d)}$. The modularity of g follows from the modularity of both factors. The holomorphicity of g away from the cusp is clear and since the zero of $\Delta^{h(-d)}$ at the cusp cancels the pole of $\mathcal{H}_d$ at the cusp, g is holomorphic at the cusp as well. Using (35) we derive that

$$\mathcal{H}_d\Delta^{h(-d)} = \mathcal{H}_d C_p^{12h(-d)}(\Delta^a E_4^b E_6^c)^p$$

for some $a, b, c \in \mathbf{Z}$. Note that $\mathcal{H}_d$ and $C_p^{12h(-d)}$ can be written as the product $\prod_{\rho\in\mathbf{SS}}(j-\rho)^{e_\rho}$ modulo p. Assuming (i), the logarithmic derivative of the left side of the equation vanishes modulo p, which means that the logarithmic derivative of $\mathcal{H}_d C_p^{12h(-d)}$ vanishes modulo p. Thus, $p|e_\rho$ for all $\rho \in \mathbf{SS}$. Define $\widetilde{f} = \Delta^a E_4^b E_6^c \prod_{\rho\in\mathbf{SS}}(j-\rho)^{\frac{e_\rho}{p}}$. The modularity and meromorphicity of $\widetilde{f}$ is clear and the holomorphicity of f follows from the fact that $\widetilde{f}^p = \widetilde{g}$. Lifting $\widetilde{f}$ to a modular form f with integer coefficients, we have $\mathcal{H}_d \equiv \Delta^{-h(-d)}f^p \pmod{p}$.

Evaluation of a modular form $g \in \mathbf{Z}_{(p)}[E_4, E_6]$ at a supersingular elliptic curve E modulo p may be computed by evaluating the image of g in $\mathbf{F}_p[E_4, E_6]$ at E using the explicit representations of $E_4(E)$ and $E_6(E)$ in terms of the coefficients of E. Since Theorem 2.1 implies that there is a unique lift of an element of $\widetilde{M}_{p+1}$ to an element of $\mathbf{F}_p[E_4, E_6]$ of weight $p+1$, the congruence of $\mathscr{L}_d^*$ and E_{p+1} as elements of $\widetilde{M}_{p+1}$ implies that $\mathscr{L}_d^*(E) \equiv E_{p+1}(E) \pmod{p}$ for all elliptic curves E.

Thus Theorems 2.7 and 2.6 together with Corollary 2.8 imply consequences (1) and (2).

Proof of Corollary 1.7. Suppose that the vector $\mathbf{e}_d$ in Exp corresponding to $\mathcal{H}_d$ is flat. If $h(-d) < \dim(\mathrm{Exp})$, then $\mathcal{H}_d$ cannot vanish at all $\rho \in \mathbf{SS}$, so one supersingular j-invariant must have exponent 0. Since $\mathbf{e}_d$ is flat, $\mathbf{e}_d = 0$. This implies that $p|h(-d)$. But this cannot happen because $0 < h(-d) < \dim(\mathrm{Exp}) < p$.

□

6. Proof of Theorem 1.8

We need to prove that the diagrams

$$\begin{array}{ccc} \mathrm{Exp}^* & \xhookrightarrow{\phi_\alpha} & \mathcal{P}_{n-1} \\ {\scriptstyle\lambda_\alpha}\downarrow\wr & & \downarrow\wr \\ \widetilde{M}^*_{p+1} & \hookrightarrow & \widetilde{M}_{p+1} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathrm{Exp}^{*\perp} & \xhookrightarrow{\psi_\beta} & \mathcal{P}_{n-1} \\ {\scriptstyle\mu_\beta}\downarrow\wr & & \downarrow\wr \\ \widetilde{M}^{*\perp}_{p+1} & \hookrightarrow & \widetilde{M}_{p+1} \end{array}$$

are commutative and have isomorphisms and injections as indicated. Note that $n = \dim \widetilde{M}_{p+1} = \#\mathbf{SS}$ by (22). By Lemma 5.1, the maps λ_α and μ_β define injections from Exp^* and $\mathrm{Exp}^{*\perp}$ respectively to $\widetilde{M}_{p+1}$. Thus Exp^* is isomorphic via λ_α to $\widetilde{M}^*_{p+1}$, and similarly, $\mathrm{Exp}^{*\perp}$ is isomorphic via μ_β to $\widetilde{M}^{*\perp}_{p+1}$.

We now consider the map $\widetilde{F}(\cdot, j(\tau)) : \widetilde{M}_{p+1} \to \mathcal{P}_{n-1}$, defined by

$$\widetilde{f}(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\epsilon \widetilde{F}(\widetilde{f}, j(\tau))$$

as in Section 2.1. Then $\widetilde{F}(\widetilde{f}, j(\tau))$ has degree $\le m = n-1$ and lies in $\mathcal{P}_{n-1}$. We have $\widetilde{f} = 0$ if and only if $\widetilde{F}(\widetilde{f}, j(\tau)) = 0$. By dimension count, the map $\widetilde{F}(\cdot, j(\tau))$ defines an isomorphism.

The map from $\widetilde{M}^*_{p+1}$ to $\widetilde{M}_{p+1}$ is simply the inclusion map and the maps $\phi_\alpha : \mathrm{Exp}^* \to \mathcal{P}_{n-1}$ and $\psi_\beta : \mathrm{Exp}^{*\perp} \to \mathcal{P}_{n-1}$ are the compositions $\widetilde{F}(\lambda_\alpha(\cdot), j(\tau))$ and $\widetilde{F}(\mu_\beta(\cdot), j(\tau))$. The maps ϕ_α and ψ_β can also be defined in an explicit way in terms of the images of basis elements of Exp^* and $\mathrm{Exp}^{*\perp}$.

Let r be the number of supersingular j-invariants which lie in $\mathbf{F}_p$. Define an ordering $\{\rho_i\}_{i=1}^n$ on $\mathbf{SS}$ such that $\rho_i \in \mathbf{F}_p$ for $i \le r$ and $\rho_i = \sigma\rho_{i+\frac{n-r}{2}}$ for $r < i \le \frac{n+r}{2}$, where σ denotes the Frobenius automorphism on $\mathbf{F}_{p^2}$.

Case 1: Defining ϕ_α. For $1 \le i \le r$, let $\mathbf{f}_i$ be the exponent vector associated to $(j(\tau) - \rho_i)$. For $r < i \le \frac{n+r}{2}$, let $\mathbf{f}_i$ be the exponent vector associated to $(j(\tau) - \rho_i)(j(\tau) - \sigma\rho_i)$. The $\mathbf{f}_i$ constitute a basis of Exp^*. Then

$$\phi_\alpha(\mathbf{f}_i) = \begin{cases} \alpha^{-1} \prod_{\ell \ne i} (j(\tau) - \rho_\ell) & \text{if } 0 \le i \le r \\ \alpha^{-1}(2j(\tau) - \rho_i - \sigma\rho_i) \prod_{\ell \ne i, i+\frac{n-r}{2}} (j(\tau) - \rho_\ell) & \text{if } r < i \le \frac{n+r}{2} \end{cases}. \tag{36}$$

Case 2: Defining ψ_β. For $r < i \le \frac{n+r}{2}$, let $\mathbf{g}_i$ be the exponent vector associated to $(j(\tau) - \rho_i)(j(\tau) - \sigma\rho_i)^{-1}$. The $\mathbf{g}_i$ constitute a basis of $\mathrm{Exp}^{*\perp}$. Then for $r < i \le \frac{n+r}{2}$,

$$\psi_\beta(\mathbf{g}_i) = \beta^{-1}(\rho_i - \sigma\rho_i) \prod_{\ell \ne i, i+\frac{n-r}{2}} (j(\tau) - \rho_\ell). \tag{37}$$

The collapsing of the diagrams in (15) under the projectivization functor $\mathbf{P}(\cdot)$ is immediate from the definitions of the maps λ_α and μ_β.

Since Exp^* and $\mathrm{Exp}^{*\perp}$ have trivial intersection by (13), so do their images $\widetilde{M}^*_{p+1}$ and $\widetilde{M}^{*\perp}_{p+1}$ in $\widetilde{M}_{p+1}$. By (22), together with (13), we have

$$\dim \widetilde{M}^*_{p+1} + \dim \widetilde{M}^{*\perp}_{p+1} = \dim \mathrm{Exp}^* + \dim \mathrm{Exp}^{*\perp} = \dim \mathrm{Exp} = \dim \widetilde{M}_{p+1},$$

yielding (16). It follows that $\mathbf{P}\lambda$ and $\mathbf{P}\mu$ have disjoint images.

Proof of Corollary 1.9. By Theorem 1.4, $\widetilde{M}^*_{p+1}$ and $\widetilde{M}^{*\perp}_{p+1}$ are proper subspaces of $\widetilde{M}_{p+1}$ for p outside of the list in (8). For $(-d, D)$ meeting the conditions of the corollary, $\mathscr{L}_{d,D} \in \widetilde{M}^*_{p+1} \cup \widetilde{M}^{*\perp}_{p+1}$ by Theorem 1.2. Since a vector space cannot be the union of two proper subspaces, the map is not surjective onto $\widetilde{M}_{p+1}$.

By Theorem 1.4,

$$\lim_{p\to\infty} \frac{\dim \mathrm{Exp}^*}{\dim \mathrm{Exp}} = \lim_{p\to\infty} \frac{\#\mathbf{SS}_1 + \frac{1}{2}(\#\mathbf{SS} - \#\mathbf{SS}_1)}{\#\mathbf{SS}} = \frac{1}{2}$$

and

$$\lim_{p\to\infty} \frac{\dim \mathrm{Exp}^{*\perp}}{\dim \mathrm{Exp}} = \lim_{p\to\infty} \frac{\frac{1}{2}(\#\mathbf{SS} - \#\mathbf{SS}_1)}{\#\mathbf{SS}} = \frac{1}{2}.$$

□

7. Proof of Theorems 1.10 and 1.11

Proof of Theorem 1.10. The fact that $\mathscr{L}_{d,D} \equiv \mathscr{L}_{d',D'} \pmod{\mathfrak{p}^*}$ follows easily from $\mathcal{H}_{d,D} \equiv \mathcal{H}_{d',D'} \pmod{\mathfrak{p}^*}$ as one can take the logarithmic derivative formally in the field $\mathbf{F}_{p^2}((q))$ and division by $\sqrt{D}$ and $\sqrt{D'}$ is the same by the remarks preceding Theorem 1.10. In fact, this implication does not require a bound on $m_{d,D}$. The same argument applies to the non-twisted setting.

Now suppose that $\mathscr{L}_{d,D} \equiv \mathscr{L}_{d',D'} \pmod{p}$ and that $m_{d,D} + m_{d',D'} < p$. Then since $\frac{\mathcal{H}_{d,D}}{\mathcal{H}_{d',D'}} \not\equiv 0 \pmod{\mathfrak{p}^*}$, we must have

$$\Theta\left(\frac{\mathcal{H}_{d,D}}{\mathcal{H}_{d',D'}}\right) \equiv 0 \pmod{\mathfrak{p}^*}.$$

This implies that $\frac{\widetilde{\mathcal{H}}_{d,D}}{\widetilde{\mathcal{H}}_{d',D'}}$, regarded as a q-series, has coefficients supported only where the exponents of q are divisible by p. Therefore $\frac{\widetilde{\mathcal{H}}_{d,D}}{\widetilde{\mathcal{H}}_{d',D'}}$ must be a p^{th} power, so the multiplicities of the roots of $\widetilde{\mathcal{H}}_{d,D}$ and $\widetilde{\mathcal{H}}_{d',D'}$ differ by a multiple of p. But since $m_{d,D} + m_{d',D'} < p$, this multiple is 0. Thus $\frac{\widetilde{\mathcal{H}}_{d,D}}{\widetilde{\mathcal{H}}_{d',D'}}$ is a constant modulo $\mathfrak{p}^*$. This constant is 1 since both polynomials have leading coefficient 1.

If $D = D' = 1$, the multiplicities of the roots of $\widetilde{\mathcal{H}}_d$ and $\widetilde{\mathcal{H}}_{d'}$ are both positive. As a consequence, the order of vanishing of $\frac{\widetilde{\mathcal{H}}_d}{\widetilde{\mathcal{H}}_{d'}}$ at any supersingular j-invariant ρ is bounded by $\max\{m_d, m_{d'}\}$. By assumption, $\max\{m_d, m_{d'}\} < p$, so $\frac{\mathcal{H}_d}{\mathcal{H}_{d'}}$ is a constant modulo p. By the same argument as before, this constant must be 1.

□

Proof of Theorem 1.11. In referring to the exponents $e_{p,d,D,\rho}$ from (11), we suppress the p, d, and D from the notation. By (21) we obtain

$$E_{p-1} = \underbrace{\Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\epsilon}_{R} F(E_{p-1}, j(\tau)).$$

By Theorem 2.2, we have

$$\frac{E_{p-1}^{m_{d,D}}}{\mathcal{H}_{d,D}(j)} \equiv j^{-e_0}(j-1728)^{-e_{1728}} R^{m_{d,D}} \prod_{\rho\in\mathbf{SS}} (j-\rho)^{m_{d,D}-e_\rho} \pmod{\mathfrak{p}}.$$

Since $m_{d,D} = \max\{|\omega_\rho e_\rho|\}_{\rho\in\mathbf{SS}}$,

$$\widetilde{P}(j) \triangleq \prod_{\rho\in\mathbf{SS}} (j-\rho)^{m_{d,D}-e_\rho} \in (\mathcal{O}_{\mathbf{Q}(\sqrt{D})}/\mathfrak{p})[j].$$

Let $P(j)$ be a lift of $\widetilde{P}(j)$ to $\mathcal{O}_{\mathbf{Q}(\sqrt{D})}[j]$.

Returning to the general situation, we next claim that

$$\mathcal{H}^*_{d,D} \triangleq j^{-e_0}(j-1728)^{-e_{1728}} R^{m_{d,D}} P(j) \tag{38}$$

is a holomorphic modular form. The order of vanishing at infinity is 0 if $D>1$ and $h(-d)$ if $D=1$, so the modular form is holomorphic at infinity. Thus there can only be poles contributed by the factor $j^{-e_0}(j-1728)^{-e_{1728}}$. We rewrite (38) as

$$\mathcal{H}^*_{d,D} = E_4^{-3e_0} E_6^{-2e_{1728}} \Delta^{e_0+e_{1728}} R^{m_{d,D}} P(j).$$

Note that in the factorization for E_{p-1}, we have $\delta>0$ if $e_0>0$ and $\epsilon>0$ if $e_{1728}>0$. Since $m_{d,D} = \max\{|\omega_\rho e_\rho|\}_{\rho\in\mathbf{SS}} \geq \max\{3e_0, 2e_{1728}\}$, the factors of $E_4^{-3e_0}$ and $E_6^{-2e_{1728}}$ are cancelled out by the powers of E_4 and E_6 in R^{m_d}, so $\mathcal{H}^*_{d,D}$ is holomorphic.

Observe that the weight of $\mathcal{H}^*_{d,D}$ is $m_{d,D}(p-1)$. We have

$$\mathcal{H}^*_{d,D} \equiv \frac{E_{p-1}^{m_{d,D}}}{\mathcal{H}_{d,D}(j)} \equiv \mathcal{H}_{d,D}^{-1} \pmod{\mathfrak{p}}.$$

□

8. Examples

Example 4. We illustrate the phenomenon proved in Corollary 1.3. Consider the following table of values of $A(n^2,d)$ reduced modulo 11. The columns correspond to n and the rows correspond to d.

$A(n^2,d)$	1	2	3	4	5	6	7	8	9	10	11	12	13
47	1	1	1	1	1	1	1	1	1	1	0	1	1
55	7	8	4	7	3	7	6	2	5	3	1	4	9
56	7	8	4	7	3	7	6	2	5	3	0	4	9
59	3	8	10	3	5	3	9	0	4	5	0	10	2

Notice that $A(n^2,55) \equiv A(n^2,56) \pmod{11}$ for all n on the table except $n=11$. Since $\mathscr{L}_{55} \equiv \mathscr{L}_{56}$, it is generally true that $A(n^2,55) \equiv A(n^2,56) \pmod{11}$ when $11 \nmid n$ by the proof of Corollary 1.3. As the corollary shows, the rows d such that 11 is good for d, excluding columns where $11|d$, must be one of a finite set of possible infinite tuples modulo 11, giving infinitely many congruences among the Hecke traces $A(n^2,d)$. The following discriminants have the same Hecke traces when $11 \nmid n$:

$$d = 136, 168, 203, 280, 312, 323, 328, 408, 520, 532, 760, 763, 795, \ldots.$$

Note that $A(n^2,47) \equiv 1 \pmod{11}$ for $11 \nmid n$ is an illustration of Theorem 1.6.

Example 5. In this example we demonstrate the effectiveness of Theorem 1.2, constructing a holomorphic modular form $\mathscr{L}^*_d$ using (31) explicitly.

Let $p=43$. The associated polynomial to E_{42} modulo 43 is

$$\widetilde{F}(E_{42}, j) \equiv j^3 + 21j^2 + 11j + 32 \equiv (j+2)(j^2+19j+16) \pmod{43}.$$

We set $-d=-47$. The Hilbert class polynomial is

$$\begin{aligned}\mathcal{H}_{47} =& j^5 + 2257834125j^4 - 9987963828125j^3 + 5115161850595703125j^2 \\ &- 14982472850828613281250j + 16042929600623870849609375 \\ \equiv& (j+35)(j+2)^2(j^2+19j+16) \pmod{43}.\end{aligned}$$

The first few terms of $\mathscr{L}_{47}$ are

$$\begin{aligned}\mathscr{L}_{47} =& -5 + 2257837845q - 5097838271600148715q^2 + 1151009957268040088231811775 5q^3 \\ & - 25987955089449122838243592107639193835q^4 \\ & + 5867662616353436857508843356715828094247629372 0q^5 + \dots \\ \equiv & 38 + 37q + 40q^2 + 26q^3 + 23q^4 + 14q^5 + \dots \pmod{43}.\end{aligned}$$

In the notation of the proof of Theorem 1.1, since $j + 35 \equiv j - 1728 \pmod{43}$ is a factor, we have $a = 0$, $b = 1$, and $\widetilde{Q}(j) = (j + 2)(j^2 + 19j + 16)$. Then $\widetilde{S}(j) = 1$ since $Q(j)$ includes all factors of $\widetilde{F}(E_{42}, j)$. Let $S(j) = 1$ as well. We compute

$$\frac{1}{j+35} + \frac{2}{j+2} + \frac{2j+19}{j^2+19j+16} = \frac{5j^3+7j^2+23j+31}{(j+35)Q(j)},$$

so $P(j) = 5j^3 + 7j^2 + 23j + 31$. We lastly observe that $R = \Delta^3 E_6$, so that

$$\begin{aligned}\mathscr{L}^*_{47} =& -\frac{E_4^2E_6^2(5j^3+7j^2+23j+31)\Delta^2}{j-1728} \\ =& -5 - 13207q - 15972095q^2 - 11701405891q^3 - 5789768972944q^4 \\ & - 2041825033232734q^5 + \dots \\ \equiv & 38 + 37q + 40q^2 + 26q^3 + 23q^4 + 14q^5 + \dots \\ \equiv & \mathscr{L}_{47} \pmod{43}\end{aligned}$$

as desired.

Example 6. In this example, we illustrate with an explicit computation the consequences of Theorem 1.6.

It can be checked that $\mathcal{H}_{199}$ factors as

$$\mathcal{H}_{199} \equiv (x-8)^3(x^2-6x-6)^3 \pmod{37}$$

and so by Theorem 1.6 we have that $\mathscr{L}_{199} \equiv -h(-199)E_{38}$.

Theorem 1.6 restricts the possible values for $\mathscr{L}_{199}$ at supersingular elliptic curves. For example, consider the elliptic curve E defined over $\mathbf{F}_{37^2} \equiv \mathbf{F}_{37}(\gamma)$ where $\gamma = \sqrt{15}$ by the equation

$$y^2 = 4x^3 - (1 + 10\gamma)x - (16 + 12\gamma).$$

This curve is supersingular as can be seen by expanding $(4x^3 - (1+10\gamma)x - (16+12\gamma))^{18} \pmod{37}$ and checking that the coefficient of x^{36} is 0. We calculate that $|E(\mathbf{F}_{37^2})| = (1 + 37)^2$, so we expect $\mathscr{L}_{199}(E) \in \mathbf{F}_{37}$. Noting that $E_4(E) = 12(1 + 10\gamma)$ and $E_6(E) = -216(16 + 12\gamma)$ and multiplying $\mathscr{L}_{199}$ by E_{p-1} to cancel poles, we confirm that $\mathscr{L}_{199}(E) = 18 \in \mathbf{F}_{37}$.

One can also check that the elliptic curve E' defined over $\mathbf{F}_{37^2}$ by the equation

$$y^2 = 4x^3 - (2 + 20\gamma)x - (1 + 19\gamma)$$

is supersingular. We calculate that $|E'(\mathbf{F}_{37^2})| = (1-37)^2$. Using the fact that $E_4(E') = 12(2+20\gamma)$ and $E_6(E') = -216(16+12\gamma)$, we find that $\mathscr{L}_{199}(E') = -4\gamma \in \mathbf{F}_{37^2} \setminus \mathbf{F}_{37}$, but $\mathscr{L}_{199}(E')^2 = 18 \in \mathbf{F}_{37}$, as expected.

References

[Bak68] Alan Baker, *Linear forms in the logarithms of algebraic numbers. IV*, Mathematika **15** (1968), 204–216.

[Bak98] Andrew J. Baker, *A supersingular congruence for modular forms*, Acta Arith. **86** (1998), no. 1, 91–100.

[Bor95a] R. E. Borcherds, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})$ *and infinite products*, Invent. Math. **120** (1995), no. 1, 161–213.

[Bor95b] ———, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})^+$ *and generalized Kac-Moody algebras*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994) (Basel), Birkhäuser, 1995, pp. 744–752.

[CL84] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[Deu41] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

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

[EOY05] N. Elkies, K. Ono, and T. Yang, *Reduction of CM elliptic curves and modular function congruences*, Int. Math. Res. Not. (2005), no. 44, 2695–2707.

[Hee52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[Kan89] M. Kaneko, *Supersingular j-invariants as singular moduli* $\bmod p$, Osaka J. Math. **26** (1989), no. 4, 849–855.

[KO99] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), no. 2, 387–398.

[KZ98] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126.

[Lan87] S. Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate.

[Mic04] P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*, Ann. of Math. (2) **160** (2004), no. 1, 185–236.

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.

[Ogg75] A. P. Ogg, *Automorphismes de courbes modulaires*, Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7, Secrétariat Mathématique, Paris, 1975, p. 8.

[Rib76] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$, Invent. Math. **34** (1976), no. 3, 151–162.

[SD73] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.

[Ser76] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. (2) **22** (1976), no. 3-4, 227–260.

[Sou00] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.

[Sta67] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1–27.

[Wil90] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540.

[Zag02] D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, pp. 211–244.