The Hasse invariant of the Tate normal form $E_5$ and the class number of $\mathbb{Q}(\sqrt{-5l})$

Patrick Morton

Feb. 8, 2020

Abstract

It is shown that the number of irreducible quartic factors of the form $g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1$ which divide the Hasse invariant of the Tate normal form $E_5$ in characteristic $l$ is a simple linear function of the class number $h(-5l)$ of the field $\mathbb{Q}(\sqrt{-5l})$, when $l \equiv 2, 3$ modulo 5. A similar result holds for irreducible quadratic factors of $g(x)$, when $l \equiv 1, 4$ modulo 5. This implies a formula for the number of linear factors over $\mathbb{F}_p$ of the supersingular polynomial $ss_{5^*}(p)(x)$ corresponding to the Fricke group $\Gamma^*_0(5)$.

1 Introduction

Let $E_5(b)$ be the Tate normal form of an elliptic curve with a point of order 5:

$$E_5 : Y^2 + (1 + b)XY + bY = X^3 + bX^2;$$

and let $H_{5,l}(b)$ denote its Hasse invariant in characteristic $l$, as in [15] and [21]:

$$\hat{H}_{5,l}(b) = (b^4 + 12b^3 + 14b^2 - 12b + 1)^r (b^2 + 1)^s (b^4 + 18b^3 + 74b^2 - 18b + 1)^s 
\times b^{5n_t}(1 - 11b - b^2)^n_t J_t \left( \frac{(b^4 + 12b^3 + 14b^2 - 12b + 1)^3}{b^5(1 - 11b - b^2)} \right).$$

Here, $n_t = [l/12], r = \frac{1}{2}(1 - (-3/l)), s = \frac{1}{2}(1 - (-4/l));$ and $J_t(t)$ is the polynomial

$$J_t(t) \equiv \sum_{k=0}^{n_t} \binom{2n_t + s}{2k + s} \binom{2n_t - 2k}{n_t - k} (-432)^{n_t - k}(t - 1728)^k \pmod{l}. $$
Let $\varepsilon = \frac{-1 + \sqrt{5}}{2}$ and $\bar{\varepsilon} = \frac{-1 - \sqrt{5}}{2}$, and let $h(-5l)$ denote the class number of the quadratic field $K = \mathbb{Q}(\sqrt{-5l})$, where $l > 5$ is a prime number. This paper is devoted to proving the following theorem, which was stated in [21].

**Theorem 1.1.** Let $l > 5$ be a prime.

A) Assume $l \equiv 2, 3 \pmod{5}$. The number of irreducible quartics of the form $g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1$ dividing $\hat{H}_{5,l}(x)$ over $\mathbb{F}_l$ is:

i) $\frac{1}{4} h(-5l)$, if $l \equiv 1 \pmod{4}$;

ii) $\frac{1}{2} h(-5l) - 1$, if $l \equiv 3 \pmod{8}$;

iii) $h(-5l) - 1$, if $l \equiv 7 \pmod{8}$.

B) Furthermore, if $l \equiv 4 \pmod{5}$, the number of irreducible quadratic factors $k(x) = x^2 + rx + s$ dividing $\hat{H}_{5,l}(x)$ over $\mathbb{F}_l$, with $r = \varepsilon^5(s - 1)$ or $r = \bar{\varepsilon}^5(s - 1)$ in $\mathbb{F}_l$ is:

i) $\frac{1}{2} h(-5l)$, if $l \equiv 1 \pmod{4}$;

ii) $h(-5l) - 3$, if $l \equiv 3 \pmod{8}$;

iii) $2h(-5l) - 3$, if $l \equiv 7 \pmod{8}$.

C) If $l \equiv 1 \pmod{5}$, the number of irreducible quadratic factors $k(x) = x^2 + rx + s$ dividing $\hat{H}_{5,l}(x)$ over $\mathbb{F}_l$, with $r = \varepsilon^5(s - 1)$ or $r = \bar{\varepsilon}^5(s - 1)$ in $\mathbb{F}_l$ is:

i) $\frac{1}{2} h(-5l)$, if $l \equiv 1 \pmod{4}$;

ii) $h(-5l) - 1$, if $l \equiv 3 \pmod{8}$;

iii) $2h(-5l) - 1$, if $l \equiv 7 \pmod{8}$.

This theorem is a supplement to [13, Thm. 6.2], which gives the possible degrees of irreducible factors of $\hat{H}_{5,l}(x) \pmod{l}$, depending on the congruence class of $l \pmod{5}$. In Part A, the only possible irreducible factors of $\hat{H}_{5,l}(x)$ are either $x^2 + 1$ or quartic factors $f(x)$ satisfying $x^4f(-1/x) = f(x)$; while in Part B, the possible factors are linear and quadratic; and in Part C, all irreducible factors are quadratic. The class number $h(-5l)$ then shows up in counting the special factors of the form $g(x)$ or $k(x)$ in Theorem 1.1.

In the paper [21] I showed that the number of linear factors of $\hat{H}_{5,l}(x) \pmod{l}$ is a function of the class number $h(-l)$, for $l \equiv 4 \pmod{5}$, and that
the same holds for the number of quadratic factors of the form $x^2 + ax - 1$, when $l \equiv 1 \pmod{5}$. Thus, both class numbers $h(-l)$ and $h(-5l)$ are encoded in the factorization of $\hat{H}_{5,l}(x)$ over $\mathbb{F}_l$, at least when $l \equiv \pm 1 \pmod{5}$. I conjecture that the same is true for the Hasse invariant $\hat{H}_{p,l}(x)$ of the Tate normal form $E_p$ for a point of order $p$, i.e., that its factorization encodes the class numbers $h(-l), h(-pl)$, where $p > 5$ is any prime for which the coefficients of $E_p$ depend on a single parameter.

Theorem 1.1 is an analogue for the Tate normal form $E_5$ of similar results for the Legendre normal form (or equivalently, the Tate normal form $E_4$ for a point of order 4, see [15, p. 255]) and the Deuring normal form. The main theorems of [16] and [17] (and their proofs) show that the counts of certain irreducible quadratic factors of the Hasse invariants of these normal forms are functions of the class numbers $h(-2p), h(-3p)$ of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-5l})$ and $\mathbb{Q}(\sqrt{-20l})$, respectively.

The proof of Theorem 1.1 proceeds along similar lines as the proof of the corresponding result for the Deuring normal form in [17] and [18], and is a combination of theoretical arguments and computational methods. In Section 2 I prove a congruence modulo $l$ for the class equation $K_{5l}(X) = H_{-20l}(X)$ (for $l \equiv 1 \pmod{4}$) or the product of class equations $K_{5l}(X) = H_{-5l}(X)H_{-20l}(X)$ (for $l \equiv 3 \pmod{4}$), using the method of [18]. This requires $l$ to be a prime greater than 379 (or one of a set $S$ of 22 specified primes less than 379; see Corollary 2.2). In Section 3 I show that each factor of the form $g(x)$ or $k(x)$ in Theorem 1.1 corresponds to an elliptic curve $E_5(b)$ for which $\mu = \sqrt{-5l}$ injects into the endomorphism ring $\text{End}(E_5(b))$, where $b$ is a root of $g(x)$ or $k(x)$ over $\mathbb{F}_l$. The proof of this uses the formula in [19] for the nontrivial points of order 5 on $E_5(b)$.

This implies that all factors of $H_{5,l}(x)$ of the form $g(x)$ or $k(x)$ in Theorem 1.1 arise from $j$-invariants which are roots of $K_{5l}(X)$ over $\mathbb{F}_l$. In particular, the factors in Theorem 1.1 divide one of the polynomials

$$F_d(x) = x^{5h(-d)}(1 - 11x - x^2)^{h(-d)}H_{-d}\left(\frac{x^4 + 12x^3 + 14x^2 - 12x + 1}{x^5(1 - 11x - x^2)}\right)$$

over $\mathbb{F}_l$, where $-d = -5l$ or $-d = -20l$ and $h(-d)$ is the class number of the order $\mathcal{O} = \mathcal{R}_{-d}$ of discriminant $-d$ in $K = \mathbb{Q}(\sqrt{-5l})$. This holds because of the formula for $\hat{H}_{5,l}(x)$ given above and the fact that

$$j(b) = j(E_5(b)) = \frac{(b^4 + 12b^3 + 14b^2 - 12b + 1)^3}{b^5(1 - 11b - b^2)}$$
is the $j$-invariant of $E_5(b)$.

In Section 4, I determine computationally how many factors in Theorem 1.1 arise from special factors $H_{-d}(X)$ of $K_{5l}(X)$ in Theorem 2.1, where $d$ equals 20 or is one of the integers in the set 

$$\mathcal{T} = \{4, 11, 16, 19, 24, 36, 51, 64, 84, 91, 96, 99\}.$$ 

For $l > 379$, the class equations corresponding to $d \in \mathcal{T}$ are the factors which occur to the 4-th power in $K_{5l}(X) \mod l$, when their roots are supersingular. I show that each of the factors $H_{-d}$, for $d \in \mathcal{T}$ and $d \neq 4$, yields $\deg(H_{-d}(X))$ factors of the form $g(x)$, or twice that number of factors of the form $k(x)$, dividing $\hat{H}_{5,l}(x)$ over $F_l$, depending on the congruence class of $l$ modulo 5, for $l > 379$ (or $l \in S$).

On the other hand, Theorem 2.1 shows that $K_{5l}(X)$ is also exactly divisible over $F_l$ by a number of factors of the form $(X^2 + a_iX + b_i)^2$. I show in Sections 5 and 6 that each of these factors contributes only one factor of the form $g(x)$, or two factors of the form $k(x)$, to the factorization of $\hat{H}_{5,l}(x)$, depending on the congruence class of $l$ modulo 5. These factors are reductions of irreducible quartic factors of $H_{-5l}(X)$ or $H_{-20l}(X)$ over the $l$-adic field $\mathbb{Q}_l$, because $l = l^2$ in the field $K = \mathbb{Q}(\sqrt{-5l})$, and $l$ splits into primes $p$ of residue class degree $f_p = 2$ in the ring class field $\Omega_f$ of $K$ with conductor $f = 1$ or 2. These factors correspond therefore to unique prime divisors of $l$ in the extension $\Omega_f/K$.

The verification of the facts mentioned in the last paragraph depends on finding an explicit generator for the ray class field $\Sigma_{\wp_5}$ with conductor $\wp_5$ over $K$ (or for $\Sigma_{\wp_5}\Omega_2/K$), where $\wp_5^2 = (5) = 5R_K$ in $K$; and whose minimal polynomial over the decomposition field $L$ of $l$ in the extension $\Omega_f/K$ reduces to a polynomial of the form $g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1$ modulo prime divisors of $l$. Such a generator is provided by a suitable value of the modular function $r(\tau)^5$, where $r(\tau)$ is the Rogers-Ramanujan continued fraction. I show in Section 5, using this generator, that each factor $(X^2 + a_iX + b_i)^2$ of $K_{5l}(X)$ gives rise to at least one factor of $\hat{H}_{5,l}(x)$ of the form $g(x)$, or two factors of the form $k(x)$, over $F_l$. Then in Section 6 I show that no other factors of the appropriate form can occur, using the icosahedral group $G_{60}$ as in [21], together with the fact that an additional factor would yield an additional solution of the equation 

$$\alpha^5 + \beta^5 = \varepsilon^5(1 - \alpha^5\beta^5)$$

over $F_l$, or of the conjugate equation with $\varepsilon$ replaced by $\bar{\varepsilon}$. (See [20], [19].) The proof is completed by the computations in Tables 4-8, which show that
the formulas of Theorem 1.1 also hold for all primes \( l \) for which \( 7 \leq l \leq 379 \).

As was shown in [21, Theorem 7.1], the above theorem, together with the results of [21, Theorems 1.1 and 1.3], implies the following result, which was conjectured by Nakaya [22] (see his conjecture 5 for \( N = 5 \)). This theorem gives a formula for the number of linear factors over \( \mathbb{F}_p \) of the supersingular polynomial \( ss_p(5^*)_p(X) \) corresponding to the Fricke group \( \Gamma_0^*(5) \), introduced by Koike and Sakai [23], [21], [22]. As in [22], \( L(p) \) denotes the number of supersingular \( j \)-invariants of elliptic curves which lie in the prime field \( \mathbb{F}_p \). This number was determined by Deuring [11] and is given by

\[
L(p) = S(\mathbb{F}_p) = \begin{cases} 
\frac{1}{2}h(-p), & \text{if } p \equiv 1 \pmod{4}, \\
2h(-p), & \text{if } p \equiv 3 \pmod{8}, \\
h(-p), & \text{if } p \equiv 7 \pmod{8}; 
\end{cases}
\]

where \( h(-p) \) is the class number of the field \( \mathbb{Q}(\sqrt{-p}) \). (See also [6, p. 97].)

**Theorem 1.2.** If \( p > 5 \), the number of linear factors of the supersingular polynomial \( ss_p(5^*)_p(X) \) corresponding to the Fricke group \( \Gamma_0^*(5) \) over \( \mathbb{F}_p \) is given by the formula

\[
L(5^*)(p) = \frac{1}{2} \left(1 + \left(\frac{-p}{5}\right)\right)L(p)
+ \frac{1}{8} \left\{2 + \left(1 - \left(\frac{-1}{5p}\right)\right) \left(2 + \left(\frac{-2}{5p}\right)\right)\right\} h(-5p)
= \frac{1}{4} \left(1 + \left(\frac{p}{5}\right)\right) h(-p) + \frac{1}{4} h(-5p), \text{ if } p \equiv 1 \pmod{4};
= \left(1 + \left(\frac{p}{5}\right)\right) h(-p) + \frac{1}{2} h(-5p), \text{ if } p \equiv 3 \pmod{8};
= \frac{1}{2} \left(1 + \left(\frac{p}{5}\right)\right) h(-p) + h(-5p), \text{ if } p \equiv 7 \pmod{8}.
\]

This result is analogous to formulas proved by Nakaya [22] for the polynomials \( ss_p(2^*)_p(X) \) and \( ss_p(3^*)_p(X) \).

Nakaya [22] has conjectured [22, Conjectures 1, 6] that the polynomial \( ss_p(5^*)_p(X) \) has degree given by

\[
\deg(ss_p(5^*)_p(X)) = \frac{1}{4} \left(p - \left(\frac{-1}{p}\right)\right) + \frac{1}{2} \left(1 - \left(\frac{-5}{p}\right)\right).
\]
I give a proof of this conjecture in Section 7, using a parametrization discussed in [21, Theorem 6.1]. A similar proof also establishes his conjecture for \( \deg(ss_p^{(7^*)}(X)) \).

Nakaya has also conjectured that \( ss_p^{(5^*)}(X) \) is a product of linear factors (mod \( p \)) if and only if \( p \) is one of the primes in the set \( \{2, 3, 5, 7, 11, 19\} \). Curiously, these are exactly the prime divisors of the order of the Harada-Norton group \( HN \) and of the Janko group \( J_1 \). See [22, Conjecture 2], [8, Ch. 10]. Theorem 1.2 implies that for \( p > 5 \), \( ss_p^{(5^*)}(X) \) is a product of linear factors (mod \( p \)) if and only if

\[
L^{(5^*)}(p) = \frac{1}{4} \left( p - \left( \frac{-1}{p} \right) \right) + \frac{1}{2} \left( 1 - \left( \frac{-5}{p} \right) \right).
\]

Nakaya’s Conjecture 2 (for \( N = 5 \)) can be obtained from this formula using a standard estimate of the class numbers \( h(-p) \) and \( h(-5p) \), along with a straightforward, if tedious, calculation. (See Table 9 in Section 7.) As he has discussed in [22] in connection with a number of examples of the same phenomenon, this is an analogue of Ogg’s observation that the 15 primes for which the supersingular polynomial \( ss_p(X) \) is a product of linear factors over \( \mathbb{F}_p \) coincide with the prime factors of the order of the Monster group. See also [5] and the related papers [3] and [4] of H. Brandt.

2 Factorization of \( K_{5p}(x) \) mod \( p \)

Define \( K_{5p}(X) = H_{-20p}(X) \) if \( p \equiv 1 \) (mod 4) and \( K_{5p}(X) = H_{-5p}(X)H_{-20p}(X) \) if \( p \equiv 3 \) (mod 4). The proof of Theorem 1.1 is based on the following congruence for \( K_{5p}(X) \) modulo \( p \).

**Theorem 2.1.** If \( p > 379 \) is a prime, then we have the factorization

\[
K_{5p}(X) \equiv H_{-20}(X)^{2e_{20}} \prod_{d \in \mathcal{T}} H_{-d}(X)^{4d} \prod_{i} (X^2 + a_i X + b_i)^2 \pmod{p},
\]

where \( H_{-d}(X) \) is the class polynomial for discriminant \(-d\), \( \mathcal{T} \) is the set

\[
\mathcal{T} = \{4, 11, 16, 19, 24, 36, 51, 64, 84, 91, 96, 99\};
\]
\( \epsilon_d \) is defined by

\[
\epsilon_{20} = \frac{1}{4} \left( 1 - \left( \frac{-20}{p} \right) \right) \left( 1 + \left( \frac{5}{p} \right) \right),
\]

\[
\epsilon_d = \frac{1}{2} \left( 1 - \left( \frac{-d}{p} \right) \right), \text{ if } d \in \{4, 11, 16, 19\},
\]

\[
\epsilon_d = \frac{1}{4} \left( 1 - \left( \frac{-d}{p} \right) \right) \left( 1 - \left( \frac{\text{disc}(H_{-d}(X))}{p} \right) \right), \text{ if } d \in \{24, 36, 51, 64, 91, 99\},
\]

\[
\epsilon_{84} = \frac{1}{8} \left( 1 - \left( \frac{-84}{p} \right) \right) \left( 1 - \left( \frac{3}{p} \right) \right) \left( 1 - \left( \frac{7}{p} \right) \right),
\]

\[
\epsilon_{96} = \frac{1}{8} \left( 1 - \left( \frac{-96}{p} \right) \right) \left( 1 - \left( \frac{2}{p} \right) \right) \left( 1 - \left( \frac{3}{p} \right) \right);
\]

and the polynomials \( X^2 + a_iX + b_i \) in the product \( \prod_i \) are certain irreducible factors of the supersingular polynomial \( ss_p(X) \) over \( \mathbb{F}_p \) which are distinct from the factors in the product over \( d \in \pi \).

For the sake of completeness, I note here the discriminants of the quadratic factors \( H_{-d}(X) \), for \( d \in \pi \):

\[
\text{disc}(H_{-24}(X)) = (2^{19})3^613^219^2,
\]

\[
\text{disc}(H_{-36}(X)) = 2^{20}(3^3)7^419^231^2,
\]

\[
\text{disc}(H_{-51}(X)) = 2^{30}3^67^4(17)31^2,
\]

\[
\text{disc}(H_{-64}(X)) = (2^5)3^{14}7^411^419^259^2,
\]

\[
\text{disc}(H_{-91}(X)) = 2^{32}3^312^27^211^4(13)71^2,
\]

\[
\text{disc}(H_{-99}(X)) = 2^{30}(3)7^4(11^3)13^219^479^2.
\]

Factors in parentheses indicate nontrivial contributions to the Legendre symbols in Theorem 2.1. Note that \( d \in \pi \) if and only if \( d \equiv \pm 1 \pmod{5} \) and the prime ideal divisor \( \varphi_5 \) of 5 in \( K = \mathbb{Q}(\sqrt{-d}) \) satisfies \( \varphi_5^2 \sim 1 \) in the ring class group \( \pmod{f} \), where \( -d = d_K f^2 \). See [20], Prop. 3.2.

**Proof of Theorem 2.1.** This is proved by the method of [18] and an extended computer calculation. Here I will just indicate the main features of the proof. Let \( \Phi_5(X,Y) = 0 \) denote the modular curve of level 5. This equation can be computed using the resultant

\[
5^{15}\Phi_5(x, y) = \text{Res}_z((z^2+12z+16)^3+x(z+11), (z^2-228z+496)^3+y(z+11)^5).
\]
We have that
\[
\text{disc}_u(\Phi_5(x, y)) = 5^4 x^4 (x - 1728)^4 \prod_{d \in \mathbb{F}(4)} H_{-d}(x)^2,
\]
\[
\Phi_5(x, x) = -(x^2 - 1264000x - 681472000)(x - 1728)^2(x + 32768)^2
\times (x - 287496)^2(x + 884736)^2
\]
\[
= H_{-20}(x)H_{-4}(x)^2H_{-11}(x)^2H_{-16}(x)^2H_{-19}(x)^2.
\]

Also, let \( Q_5(u, v) \) denote the de-symmetrized form of \( \Phi_5(X, Y) \), so that
\[
Q_5(-x - y, xy) = \Phi_5(x, y).
\]
From [18] (Lemma 2.3) we know that for \( p > 20 \) the irreducible factors of \( K_{5p}(x) \) are the same as the supersingular factors which divide \( \Phi_5(x^p, x) \), and their multiplicities are the same as their multiplicities in \( \Phi_5(x^p, x)^2 \):
\[
K_{5p}(x) = \prod_i q_i(x)^{e_i}, \quad \text{over } q_i(x) | \gcd(ss_p(x), \Phi_5(x^p, x))
\]
and \( q_i(x)^{e_i} | \Phi_5(x^p, x)^2 \). The linear factors can only come from the roots of \( \Phi_5(x, x) \equiv 0 \), i.e. factors of \( H_{-d}(x) \pmod{p} \) for \( d \in \{4, 11, 16, 19, 20\} \), and these factors, for \( d \neq 20 \), are supersingular in characteristic \( p \) if and only if the corresponding \( \epsilon_d = 1 \). For \( d = 20 \), the roots of
\[
H_{-20}(x) = x^2 - 1264000x - 681472000,
\]
which lie in \( \mathbb{Q}(\sqrt{5}) \), are supersingular and contained in \( \mathbb{F}_p \) if and only if \( \epsilon_{20} = 1 \). We must check that the multiplicities of the linear factors are 2, if \( d = 20 \) and 4, if \( d \in \{4, 11, 16, 19\} \).

With \( Q(u, v) = Q_5(u, v) \) let
\[
Q_1 = \frac{\partial Q(u, v)}{\partial u}, \quad Q_2 = \frac{\partial Q(u, v)}{\partial v},
\]
denote the first partials of \( Q \) and \( Q_{ij} \) the second partials. If
\[
F(t) = \Phi_5(t^p, t) = Q(-t^p - t, t^{p+1}),
\]
then in characteristic \( p \),
\[
F'(t) = -Q_1(-t^p - t, t^{p+1}) + t^p Q_2(-t^p - t, t^{p+1}),
\]
\[
F''(t) = Q_{11}(-t^p - t, t^{p+1}) - 2t^p Q_{12}(-t^p - t, t^{p+1}) + t^{2p} Q_{22}(-t^p - t, t^{p+1}).
\]
For the roots $t$ of the linear factors we have
\begin{align*}
F(t) &= Q(-2t, t^2), \quad F'(t) = -Q_1(-2t, t^2) + tQ_2(-2t, t^2), \quad (1) \\
F''(t) &= Q_{11}(-2t, t^2) - 2tQ_{12}(-2t, t^2) + t^2Q_{22}(-2t, t^2). \quad (2)
\end{align*}

The following values can be checked on Maple:

\[
F(1728) = F'(1728) = 0, \quad F''(1728) = 2^{11}3^{24}5^37^811^419^4;
\]
\[
F(-32^3) = F'(-32^3) = 0, \quad F''(-32^3) = -2^{63} \cdot 5 \cdot 7^811^213^417^219^343^2;
\]
\[
F(66^3) = F'(66^3) = 0, \quad F''(66^3) = 2^{21}3^{26} \cdot 5 \cdot 7^811^319^3 \cdot 31 \cdot 43^267^2 \cdot 71 \cdot 79;
\]
\[
F(-96^3) = F'(-96^3) = 0, \quad F''(-96^3) = -2^{63}3^{26} \cdot 5 \cdot 13^419^2 \cdot 31 \cdot 59 \cdot 67^2 \cdot 79.
\]

These values show that the multiplicity of $H_{-d}(x)$ in $\Phi_5(x^p, x)$ over $\mathbb{F}_p$ is 2, for $d \in \{4, 11, 16, 19\}$ and $p > 79$, and therefore the multiplicities of the $q_i(x) = H_{-d}(x)$ in $K_{5p}(x)$ for these $d$ are $\epsilon_i = 4$, when they occur (for $p > 79$). Moreover, the linear factors corresponding to these values of $d$ are distinct (mod $p$), for $p > 67$.

For $d = 20$, we use (1) to evaluate $F(t)$ and its derivative at $t = \alpha = 632000 + 282880\sqrt{5}$, which is a root of $H_{-20}(x)$. We find that $F(\alpha) = 0$, but that $F'(\alpha) = A + B\sqrt{5}$, with

\[
A = -2^{56} \cdot 3 \cdot 5^3 \cdot 7 \cdot 11^7 \cdot 13^5 \cdot 17^3 \cdot 19^4 \cdot 31^3 \cdot 79^2 \cdot 919
\]
\[
B = -2^{54} \cdot 5 \cdot 11^6 \cdot 13^5 \cdot 17^3 \cdot 19^4 \cdot 29 \cdot 31^2 \cdot 79^2 \cdot 467 \cdot 543287,
\]

and

\[
A^2 - 5B^2 = -2^{108} \cdot 5^3 \cdot 11^{12} \cdot 13^{10} \cdot 17^6 \cdot 19^{10} \cdot 31^4 \cdot 59^2 \cdot 71^2 \cdot 79^4.
\]

This calculation shows that the linear factors $(x - \alpha), (x - \alpha')$ of $H_{-20}(x)$ divide $K_{5p}(x)$ to the second power, when they occur and lie in $\mathbb{F}_p[x]$ (for $p > 79$). Factoring $H_{-20}(t)$ for $t = 12^3, -32^3, 66^3, -96^3$ shows that none of the linear factors mentioned above coincides with a factor of $H_{-20}(x)$ (mod $p$), when $p > 79$. This completes the argument for the linear factors of $K_{5p}(x)$.

Next, the class equations $H_{-d}(x)$ are quadratic, for the six values of $d \in \{24, 36, 51, 64, 91, 99\}$. For these polynomials, and for a root $t$ of $H_{-d}(x)$, 1 and $t^p$ are independent over $\mathbb{F}_p$. Letting $t = \alpha_d$ be a root of $H_{-d}(x) = x^2 + ux + v$, for these $d$, we verify that $F(\alpha_d) = Q(u, v) = 0$ and $F'(\alpha_d) =$
\( Q_1(u, v) = Q_2(u, v) = 0 \) in characteristic 0, but that \( F''(\alpha_d) \neq 0 \) in \( F_p \), for \( p > 379 \). To check the latter note that \( F''(t) = D_1(u, v) + \ell^p D_2(u, v) \), where

\[
D_1(u, v) = Q_{11} - vQ_{22}, \quad D_2(u, v) = 2Q_{12} + uQ_{22}.
\]

Recall that

\[
\begin{align*}
H_{-24}(x) &= x^2 - 4834944x + 14670139392, \\
H_{-36}(x) &= x^2 - 153542016x - 1790957481984, \\
H_{-51}(x) &= x^2 + 5541101568x + 6262062317568, \\
H_{-64}(x) &= x^2 - 82226316240x - 7367066619912, \\
H_{-91}(x) &= x^2 + 10359073013760x - 384568902077648, \\
H_{-99}(x) &= x^2 + 37616060956672x - 5617132605381076.
\end{align*}
\]

For \( d = 24 \) we find

\[
\gcd(D_1, D_2) = 2^{36} \cdot 3^{18} \cdot 5 \cdot 13^2 \cdot 19^2 \cdot 37 \cdot 43^2 \cdot 61 \cdot 67 \cdot 109.
\]

For \( d = 36 \) we find

\[
\gcd(D_1, D_2) = 2^{39} \cdot 3^8 \cdot 5 \cdot 7^6 \cdot 19^2 \cdot 43^2 \cdot 67 \cdot 79 \cdot 127 \cdot 139 \cdot 151 \cdot 163.
\]

For \( d = 51 \) we find

\[
\gcd(D_1, D_2) = 2^{46} \cdot 3^{19} \cdot 5 \cdot 7^7 \cdot 17 \cdot 37 \cdot 61 \cdot 79 \cdot 139 \cdot 163 \cdot 211.
\]

For \( d = 64 \) we find

\[
\gcd(D_1, D_2) = 2^{11} \cdot 3^{20} \cdot 5 \cdot 7^6 \cdot 11^3 \cdot 19^2 \cdot 43^2 \cdot 67 \cdot 139 \cdot 163 \cdot 211 \cdot 283 \cdot 307.
\]

For \( d = 91 \) we find

\[
\gcd(D_1, D_2) = 2^{30} \cdot 3^{18} \cdot 5 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 37 \cdot 61 \cdot 67 \cdot 109 \cdot 151 \cdot 163 \cdot 331 \cdot 379.
\]

For \( d = 99 \) we find

\[
\gcd(D_1, D_2) = 2^{46} \cdot 5 \cdot 7^6 \cdot 11 \cdot 13^3 \cdot 19^2 \cdot 29 \cdot 41 \cdot 43^2 \cdot 61 \cdot 109 \cdot 127 \cdot 139 \cdot 211 \cdot 283 \cdot 307.
\]

This shows that the quadratic polynomials \( H_{-d}(x) \) divide \( K_{5p}(x) \) to exactly the fourth power (mod \( p \)), when they occur, for \( p > 379 \). Furthermore, factoring the coefficients of the differences \( H_{-d_1}(x) - H_{-d_2}(x) \) shows that these class polynomials are all distinct (mod \( p \)), when \( p > 307 \).
The only other quadratic factors that can occur in the factorization of \(K_{5p}(x)\) to a power higher than the second are quadratic factors of the quartic polynomials \(H_{-84}(x)\) and \(H_{-96}(x)\), by the formula for the discriminant of \(\Phi_5(x, y)\). (See the argument at the beginning of the proof of [18], Prop. 2.4.)

We start with the polynomial

\[
H_{-84}(x) = x^4 - 3196800946644x^3 - 5663679223085309952x^2 \\
+ 8882124658981008934176x - 513320163210986057826304,
\]

which discriminant is

\[
\text{disc}(H_{-84}(x)) = 2^{116}3^{44}7^{14}13^{12}29^{4}3^{2}5^{5}61^{2}6^{2}7^{3}29^{2}79^{2}.
\]

With some calculation using the above expression, it is straightforward to check that the splitting field of \(H_{-84}(x)\) is \(\mathbb{Q}(\sqrt{3}, \sqrt{7})\). If \(\left(\frac{3}{p}\right) = +1\) and \(\left(\frac{7}{p}\right) = -1\), where \(p > 79\), then \(H_{-84}(x)\) factors into two irreducible quadratics over \(\mathbb{F}_p\). One of these factors is

\[
q_1(x) = x^2 + ux + v = x^2 + (922836934656\sqrt{3} - 1598400473472)x \\
+ 1649310419952599040\sqrt{3} - 285668944809764864,
\]

but

\[
\text{Norm}_\mathbb{Q}(Q(u, v)) = 2^{108}3^{62}7^{12}13^{12}29^{6}43^{2}47^{2}53^{2}61^{2}73^{2}97^{3} \\
\times 157 \cdot 181 \cdot 229 \cdot 241 \cdot 313 \cdot 349 \cdot 397 \cdot 409.
\]

Hence, \(q_1(x)\) and its conjugate \(\tilde{q}_1(x)\) over \(\mathbb{Q}(\sqrt{3})\) do not divide \(\Phi_5(x^p, x)\) (mod \(p\)), for \(p > 409\). Furthermore,

\[
\text{gcd}(N(Q_1), N(Q_2)) = 2^{76}3^{43}7^{8}13^{8}29^{4} \cdot 47 \cdot 53^{2}61^{2} \cdot 73 \cdot 97,
\]

where \(N(a)\) denotes the norm to \(\mathbb{Q}\), so \(q_1(x)\) can occur only to the second power in \(K_{5p}(x)\) and can be absorbed into the final product of the theorem, when it or \(\tilde{q}_1(x)\) occurs, for \(97 < p \leq 409\).

Similarly, if \(\left(\frac{3}{p}\right) = -1\) and \(\left(\frac{7}{p}\right) = +1\), \(H_{-84}(x)\) has the factor

\[
q_2(x) = x^2 + ux + v = x^2 + (604139268096\sqrt{7} - 1598400473472)x \\
- 9357315081633792\sqrt{7} + 24757128541605888.
\]
In this case

\[ \text{Norm}_Q(Q(u,v)) = 2^{108}3^{36}7^{15}13^{12}29^443^247^2 \cdot 53 \cdot 59^261^473^483^2 \]
\[ \times 113 \cdot 131 \cdot 137 \cdot 149 \cdot 197 \cdot 233^2 \cdot 281 \cdot 317 \cdot 389 \cdot 401. \]

Hence, \( q_2(x) \) and \( \tilde{q}_2(x) \) do not divide \( \Phi(x^5, x) \) over \( \mathbb{F}_p \), for \( p > 401 \). In this case,

\[ \gcd(N(Q_1), N(Q_2)) = 2^{76}3^{30}7^{10}13^8 \cdot 47 \cdot 61^273^2 \cdot 83, \]

and so \( q_2(x) \) and \( \tilde{q}_2(x) \) occur only to the second power in \( K_{5p}(x) \), when either occurs, for \( 83 < p \leq 401 \).

On the other hand, if \( \left( \frac{3}{p} \right) = -1 \) and \( \left( \frac{7}{p} \right) = -1 \), \( H_{-84}(x) \) has the factor

\[ q_3(x) = x^2 + ux + v = x^2 + (348799965696\sqrt{21} - 1598400473472)x \]
\[ - 20235870240768\sqrt{21} + 92704725504000, \]

and in this case \( Q(u,v) = Q_1(u,v) = Q_2(u,v) = 0 \) in characteristic 0. Since

\[ \gcd(N(D_1), N(D_2)) = 2^{70}3^{30}5^27^813^629^243^367^2 \]
\[ \times 79 \cdot 127 \cdot 151 \cdot 163 \cdot 211^2 \cdot 331 \cdot 379, \]

it follows that \( q_3(x) \) and its conjugate \( \tilde{q}_3(x) \) divide \( K_{5p}(x) \) over \( \mathbb{F}_p \), with multiplicity 4, exactly when \( \epsilon_{84} = 1 \), for primes \( p > 379 \). Moreover, the largest prime factor of any resultant \( \text{Res}(H_{-84}(x), H_{-d}(x)) \), for the values \( d \in \{ 24, 36, 51, 64, 91, 99 \} \), for which \( H_{-84}(x) \pmod{p} \) is a product of two irreducible quadratics, is 379, so the factors \( q_3 \) and \( \tilde{q}_3 \) are distinct from the quadratic factors found above, for \( p > 379 \). This establishes the contribution of \( H_{-84}(x) \) to the factorization of \( K_{5p}(x) \).

A similar analysis applies to the polynomial

\[ H_{-96}(x) = x^4 - 23340144296736x^3 + 670421055192156288x^2 \]
\[ + 447805364111967209472x - 984163224549635621646336 \]
\[ = (x^2 - 11670072148368x + 10900447400376000)^2 \]
\[ - 2^93^{13}13^217^241^261^2(739x - 690264)^2, \]

whose discriminant is

\[ \text{disc}(H_{-96}(x)) = 2^{56}3^{46}13^{12}17^{12}19^623^237^241^443^261^467^289^2. \]
For \(\left(\frac{2}{p}\right) = +1\) and \(\left(\frac{3}{p}\right) = -1\), the polynomial
\[
x^2 + ux + v = x^2 + (8251987131648\sqrt{2} - 11670072148368)x
\]
\[
+ 12701433452887296\sqrt{2} - 1796253942325764
\]
is a factor of \(H_{-96}(x) \pmod{p}\) and
\[
\text{Norm}_Q(Q(u, v)) = 2^{54}3^{36}13^{12}17^819^423^{10}37^441^243^247^261^667^2
\]
\[
\times 89 \cdot 113 \cdot 137^2139^2257 \cdot 281 \cdot 353 \cdot 401 \cdot 449.
\]
Moreover,
\[
\gcd(N(Q_1), N(Q_2)) = 2^{40}3^{30}13^817^423^537^2 \cdot 47 \cdot 61^4 \cdot 137.
\]
Thus, the above factor only occurs to the second power in \(K_{5p}(x)\), when it or its conjugate occurs, for \(137 < p \leq 449\), so it can be absorbed into the final product in the congruence of the theorem.

For \(\left(\frac{2}{p}\right) = -1\) and \(\left(\frac{3}{p}\right) = +1\), the polynomial
\[
x^2 + ux + v = x^2 + (6737719296672\sqrt{3} - 11670072148368)x
\]
\[
- 197611189074074880\sqrt{3} + 342272619618959808
\]
is a factor of \(H_{-96}(x) \pmod{p}\) and
\[
\text{Norm}_Q(Q(u, v)) = -2^{54}3^{63}13^{12}17^819^423^237^541^643^261^267^289^4
\]
\[
\times 109^3 \cdot 229 \cdot 277^2 \cdot 349 \cdot 373 \cdot 397 \cdot 421.
\]
In this case,
\[
\gcd(N(Q_1), N(Q_2)) = 2^{40}3^{40}13^817^437^241^4 \cdot 71 \cdot 89^2 \cdot 109,
\]
so these factors occur only to the second power in \(K_{5p}(x)\) when they occur, for \(109 < p \leq 421\). Finally, the polynomial
\[
x^2 + ux + v = x^2 - (4764286992816\sqrt{6} + 11670072148368)x
\]
\[
+ 4450089034924416\sqrt{6} + 1090044740037600
\]
is a factor of \(H_{-96}(x)\) when \(\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1\), and \(Q(u, v) = Q_1(u, v) = Q_2(u, v) = 0\), while
\[
\gcd(N(D_1), N(D_2)) = 2^{41}3^{37}5^213^617^219^441^243^361^267^2139^2
\]
\[
\times 163 \cdot 211 \cdot 283 \cdot 307 \cdot 331 \cdot 379.
\]
Thus, the factors of $H_{-96}(x)$ divide $K_{5p}(x)$ to the 4-th power when $\epsilon_{96} = 1$ and $p > 379$. The largest prime dividing a resultant $\text{Res}(H_{-96}(x), H_{-d}(x))$, for $d \in \{24, 36, 51, 64, 84, 91, 99\}$, modulo which $H_{-96}(x)$ factors as a product of two irreducible quadratics, is 379. This completes the discussion of the factors in the first product.

The remaining irreducible quadratic factors $q_i(x) = x^2 + a_i x + b_i$ are exactly the factors of $ss_p(x)$, distinct from the factors of $H_{-d}(x) \ (d \in \mathcal{S})$, for which $Q(a_i, b_i) = Q(a_i, b_i) \equiv 0 \ (\text{mod} \ p)$, by [18], Theorem 3.1, and their multiplicities in $K_{5p}(x)$ are exactly 2. This completes the proof. □

For $p = 379$, the polynomials $H_{-91}(x), H_{-84}(x), H_{-96}(x)$ all have the factor $H_{-91}(x) \equiv x^2 + 114 x + 51$ in common (mod 379), and this factor occurs to the power 6 in the factorization of $K_{5p}(x)$. Thus, the factorization formula in Theorem 2.1 does not hold for $p = 379$ (barely!). By factoring the supersingular polynomial $ss_{379}(x) \ (\text{mod} \ 379)$ and comparing with the factors and multiplicities of $\Phi_5(x^{379}, x) \ (\text{mod} \ 379)$, it can be checked that

$$K_{5.379}(x) = H_{-5.379}(x)H_{-4.5.379}(x) \equiv$$

$$(x + 163)^2 (x + 181)^2 (x + 150)^4 (x + 165)^4 (x + 167)^4$$

$\times (x^2 + 338 x + 303)^4 (x^2 + 359 x + 73)^4 (x^2 + 288 x + 354)^4$

$\times (x^2 + 180 x + 346)^4 (x^2 + 114 x + 51)^6 (x^2 + 47 x + 352)^4 (x^2 + 23 x + 346)^4$

$\times (x^2 + 68 x + 125)^2 (x^2 + 191 x + 240)^2 (x^2 + 320 x + 244)^2 (x^2 + 152 x + 232)^2$

$\times (x^2 + 57 x + 374)^2 \quad \pmod{379}$

This agrees with the fact that $h(-5 \cdot 379) = h(-20 \cdot 379) = 48$. Therefore, the condition $p > 379$ in Theorem 2.1 is sharp.

Moreover, there are 22 primes $p < 379$ which do not occur in any of the factorizations in the proof of Theorem 2.1, and which do not divide the differences $H_{-d_1}(t) - H_{-d_2}(t)$ for $d_1, d_2 \in \{4, 11, 16, 19, 20\}$ or for $d_1, d_2 \in \{24, 36, 51, 64, 91, 99\}$; or the remainders on dividing $H_{-84}(t)$ or $H_{-96}(t)$ by $H_{-d}(t)$, for $d \in \{24, 36, 51, 64, 91, 99\}$; or the resultant $\text{Res}(H_{-84}(t), H_{-96}(t))$, for which $\left(\frac{2}{p}\right) = -1$. These are the primes in the set

$$S = \{101, 103, 107, 167, 173, 179, 191, 193, 199, 223, 227, 239, 251, 263, 269, 271, 293, 311, 337, 347, 359, 367\}.$$

For these primes all the arguments in the proof are valid. This implies the following.
Corollary 2.2. The assertion of Theorem 2.1 also holds for all 22 primes in the set $S$.

Equating degrees in the congruence of Theorem 2.1 yields the following formula. Let

$$a_p = 1 + \frac{1}{2}\left(1 - \left(\frac{-1}{p}\right)\right)\left(2 + \left(\frac{2}{p}\right)\right);$$

so that $a_p = 1, 2, 4$ according as $p \equiv 1 \mod 4$, or $p \equiv 3, 7 \mod 8$.

Theorem 2.3. For primes $p \in S$ and for $p > 379$, the following formula holds:

$$a_p h(-5p) = 4\epsilon_{20} + \sum_{d \in T} 4\epsilon_d \deg(H_{-d}(X)) + 4N_p,$$

where $N_p$ is the number of irreducible quadratic factors $X^2 + a_i X + b_i$ of $J_p(X)$, not dividing any of the factors $H_{-d}(X)^{e_4} \pmod{p}$ in Theorem 2.1, for which $Q_5(a_i, b_i) = 0 \pmod{p}$.

The factors $X^2 + a_i X + b_i$ of $J_p(X)$ in this theorem, whose count is $N_p$, occur to only the first power in $\Phi_5(X^p, X)$ over $\mathbb{F}_p$. See [18, pp. 78, 83, 91, 92]. This yields an easy way of distinguishing them from the other factors of $J_p(X)$ for which $Q_5(a, b) = 0$ in $\mathbb{F}_p$.

3 The endomorphism $\mu = \sqrt{-5l}$

To prepare the next step in the proof, we solve the equation

$$g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1 = 0$$

algebraically, using the cubic resolvent for $g(x - \frac{a}{4})$:

$$y^3 + \left(\frac{3}{4}a^2 - 22a - 4\right)y^2 + \frac{a}{16}(3a - 44)(a^2 - 44a - 16)y + \frac{a^2}{64}(a^2 - 44a - 16)^2$$

$$= (y + \frac{1}{4}(a^2 - 44a - 16))(y^2 + \frac{a^2 - 22a}{2}y + \frac{a^2}{16}(a^2 - 44a - 16)).$$

The roots of this cubic are

$$\Theta_1 = -\frac{1}{4}(a^2 - 44a - 16),$$

$$\Theta_2 = -a\left(\frac{a}{4} - \frac{11 + 5\sqrt{5}}{2}\right) = -a\left(\frac{a}{4} + \epsilon^5\right),$$

$$\Theta_3 = -a\left(\frac{a}{4} - \frac{11 - 5\sqrt{5}}{2}\right) = -a\left(\frac{a}{4} + \epsilon^5\right).$$
Moreover, $\Theta_2\Theta_3 = \frac{a^2}{16}(a^2 - 44a - 16) = -\frac{a^2}{4}\Theta_1$. The roots of $g(x) = 0$ are

$$\rho = \frac{-a}{4} - \frac{1}{2} \varepsilon_1 \sqrt{-\Theta_1} + \frac{1}{2} \varepsilon_2 \sqrt{-\Theta_2} + \frac{1}{2} \varepsilon_3 \sqrt{-\Theta_3},$$

where $\varepsilon_i = \pm 1$ and an odd number of the $\varepsilon_i$ are $+1$.

Let the roots $\rho_i$ be numbered as follows:

$$\rho_1 := \frac{-a}{4} - \frac{1}{2} \sqrt{-\Theta_1} + \frac{1}{2} \sqrt{-\Theta_2} + \frac{1}{2} \sqrt{-\Theta_3},$$
$$\rho_2 := \frac{-a}{4} + \frac{1}{2} \sqrt{-\Theta_1} + \frac{1}{2} \sqrt{-\Theta_2} - \frac{1}{2} \sqrt{-\Theta_3},$$
$$\rho_3 := \frac{-a}{4} - \frac{1}{2} \sqrt{-\Theta_1} - \frac{1}{2} \sqrt{-\Theta_2} - \frac{1}{2} \sqrt{-\Theta_3},$$
$$\rho_4 := \frac{-a}{4} + \frac{1}{2} \sqrt{-\Theta_1} - \frac{1}{2} \sqrt{-\Theta_2} + \frac{1}{2} \sqrt{-\Theta_3}.$$

Straightforward calculation shows that

$$-(\rho_1 + \rho_4) = \varepsilon_5(\rho_1\rho_4 - 1), \quad -(\rho_2 + \rho_3) = \varepsilon_5(\rho_2\rho_3 - 1).$$

It follows that $(x - \rho_1)(x - \rho_4)$ and $(x - \rho_2)(x - \rho_3)$ are polynomials of the form $x^2 + rx + s$, with $r = \varepsilon^5(s - 1)$, as in Theorem 1.1B. Further,

$$-(\rho_1 + \rho_2) = \varepsilon^5(\rho_1\rho_2 - 1), \quad -(\rho_3 + \rho_4) = \varepsilon^5(\rho_3\rho_4 - 1),$$

so that $(x - \rho_1)(x - \rho_2)$ and $(x - \rho_3)(x - \rho_4)$ have the form $x^2 + rx + s$, with $r = \varepsilon^5(s - 1)$.

We also note that $\rho_3 = -1/\rho_1$ and $\rho_4 = -1/\rho_2$. Thus, the factors of the form $k(x)$ in Theorem 1.1B and C come in pairs of factors, whose product has the form $g(x)$. Note also that the roots of $g(x)$ are invariant under $\tau(b) = \frac{b + \varepsilon^5}{\varepsilon^5b + 1}$, since

$$(\varepsilon^5x + 1)^4 g(\tau(x)) = 5^3 \varepsilon^{10} g(x).$$

Also, $-1/\tau(b) = \bar{\tau}(b) = \frac{-b + \varepsilon^5}{\varepsilon^5b + 1}$.

Now assume $b$ is a root of the factor $g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1$ of $\hat{H}_5, l(x) = 0$ over $\mathbb{F}_l$. Then $E_5 = E_5(b)$ is supersingular in characteristic $l$. The calculations of [15] imply that $E_5(b)$ is isogenous to $E_5(\tau(b))$ by an
isogeny $\phi$ of degree 5, for the following reason. By [15, p. 259], there is an isogeny $\psi : E_5 \to E_{5,5}$ defined over $F_l(b)$, where $E_{5,5} = E_{5,5}(b)$ is the curve

$$E_{5,5}(b) : Y^2 + (1 + b)XY + 5bY = X^3 + 7bX^2 + 6(b^3 + b^2 - b)X + b^5 + b^4 - 10b^3 - 29b^2 - b,$$

for which

$$X(\psi(P)) = b^4 + (3b^3 + b^4)x + (3b^2 + b^3)x^2 + (b - b^2 - b^3)x^3 + x^5, \quad x = X(P).$$

Furthermore, $E_{5,5}(b) \cong E_5(\tau(b))$ by an isomorphism $\iota$, since these two curves have the same $j$-invariant, namely

$$j(E_{5,5}(b)) = \frac{(b^4 - 228b^3 + 494b^2 + 228b + 1)^3}{b(1 - 11b - b^2)^5}.$$

The $X$-coordinate of this isomorphism is defined over $F_{l^2}(b)$, since it is given by $\iota(X_1, Y_1) = (X_2, Y_2)$, where

$$\iota(X_1) = X_2 = \lambda^2 X_1 + \lambda^2 \frac{b^2 + 30b + 1}{12} \tau(b)^2 + 6\tau(b) + 1 \frac{12}{12},$$

with $\lambda^2 = \frac{\sqrt{5}\bar{\varepsilon}}{(b - \varepsilon^5)^2}$. Composing the isogeny $\psi$ with this isomorphism $\iota$ gives the isogeny $\phi = \iota \circ \psi$.

**Lemma 3.1.** Let $\phi : E_5(b) \to E_5(\tau(b))$ be the isogeny defined above, and let $\tilde{\phi} : E_5(\tau(b)) \to E_5(b)$ be the corresponding isogeny, gotten by replacing $b$ in the formulas for $\phi$ by $\tau(b)$ (leaving $\sqrt{5}$ fixed). Then $\tilde{\phi} \circ \phi = \alpha \circ [5]$, where $\alpha \in \text{Aut}(E_5(b))$ and [5] is the multiplication-by-5 map on $E_5(b)$. Thus, if $j(E_5(b)) \neq 0, 1728$, $\alpha = \pm 1$ and $\phi = \pm \tilde{\phi}$, where $\phi$ is the dual isogeny of $\tilde{\phi}$.

**Proof.** The following formula from [19] gives the $X$-coordinate on $E_5(b)$ for a point $P$ of order 5, which does not lie in $((0, 0))$:

$$X(P) = \frac{-e^4}{2} \frac{(-2u^2 + (1 + \sqrt{5})u - 3\sqrt{5} - 7)(2u^2 + (2\sqrt{5} + 4)u + 3\sqrt{5} + 7)}{(-2u^2 + (\sqrt{5} + 1)u - 2)(u + 1)^2},$$

where

$$u^5 = \frac{b - \bar{\varepsilon}}{b - \varepsilon^5}.$$
A calculation on Maple shows that

$$X(\psi(P)) = \frac{-5 + \sqrt{5}}{10} (b^2 + \varepsilon^4 b + \varepsilon^2).$$

Then the above formula for \( \iota \) gives \( X_2 = \iota(X(\psi(P))) = 0 \). Hence, the point \( P \) maps to \( \phi(P) = \pm (0,0) \) on \( E_5(\tau(b)) \). Now the kernel of \( \psi \) is the group \( \langle (0,0) \rangle \) on \( E_5(b) \), so \( \ker(\phi) = \langle (0,0) \rangle \), whence it follows that \( \ker(\phi) = \langle (0,0) \rangle \) on \( E_5(\tau(b)) \). But the point \( P \not\in \langle (0,0) \rangle \), so \( (0,0) \) and \( P \) generate \( E_5(b)[5] \).

Since \( \overline{\phi} \circ \phi(P) = \overline{\phi}(\pm (0,0)) = O \) on \( E_5(b) \), we have \( \ker(\phi \circ \phi) = E_5(b)[5] \). Since this is also the kernel of the multiplication-by-5 map on \( E_5(b) \), it follows that \( \overline{\phi} \circ \phi = \alpha \circ [5] \) in \( \text{End}(E_5(b)) \), for some automorphism \( \alpha \) of \( E_5(b) \). Since \( l > 5 \), the only possibility for \( j(E_5) \neq 0, 1728 \) is \( \alpha = \pm [1] \). This proves the lemma. (See [26, pp. 73-74, 103].) \( \square \)

**Remark.** The minimal polynomials of the only values of \( b \), for which \( j(E_5(b)) = 0, 1728 \), divide the respective polynomials

\[
\begin{align*}
c_4(x) &= x^4 + 12x^3 + 14x^2 - 12x + 1, \\
c_6(x) &= -(x^2+1)^2(x^4 + 18x^3 + 74x^2 - 18x + 1).
\end{align*}
\]

The quartic factor of \( c_6(x) \) only has the form of \( g(x) \) in characteristic \( l > 5 \) if \( l = 7 \), and \( c_4(x) \) never has the form of \( g(x) \), for characteristic \( l > 5 \). Note also that the discriminants of these quartic polynomials are only divisible by the primes 2, 3, 5, so neither can be the square of a factor of the form \( k(x) \), for \( p > 5 \).

Suppose that \( l \equiv 1, 4 \mod 5 \) and \( g(x) \) factors into irreducible quadratics over \( \mathbb{F}_l \) of the form given in Theorem 1.1B or C, with \( r = \varepsilon^5(s-1) \). In this case \( \lambda \in \mathbb{F}_2 \), so \( \psi \) is certainly defined over \( \mathbb{F}_l \). An easy calculation shows that \( \tau \) permutes the roots of \( x^2 + r x + s \) and therefore \( \tau(b) = b^l \) over \( \mathbb{F}_l \), since \( \tau(b) \neq b \) are conjugates over \( \mathbb{F}_l \). (The only exception to this is \( k(x) = x^2 + (11 + 5\sqrt{5})x - 1 \), whose roots are the fixed points of \( \tau(x) \). The square \( k(x)^2 \) has the form of the polynomial \( g(x) \) when \( l \equiv \pm 1 \mod 5 \); but \( k(x) \mid x^4 + 22x^3 - 6x^2 - 22x + 1 \), which does not have the form \( g(x) \) when \( l > 5 \).) Then \( \mu = \phi^{-1} \cdot (X,Y) \rightarrow (\phi(X)^l, \phi(Y)^l) \) is an endomorphism of \( E_5(b) \), and if \( P = (x, y) \),

\[
\mu^2(P) = [\phi(\phi(P)^l)]^l = (\pm \overline{\phi} \circ \phi(P))^l,
\]

where \( \overline{\phi} \) is the isogeny from Lemma 3.1, obtained by replacing \( b \) by \( \tau(b)^l = b^l \) in the formulas for \( \phi \) (and leaving \( \sqrt{5} \) fixed). By Lemma 3.1 and the above
remark, \( \tilde{\phi} \circ \phi = \pm [5] \), so that \( \mu^2 = \pm 5l \) in \( \text{End}(E_5(b)) \) (using that \( E_5(b) \) is supersingular; see \([11]\) pp. 86-87). But \( \text{End}(E_5(b)) \) is a definite quaternion algebra, so that \( \mu = \phi' \) satisfies \( \mu^2 = -5l \) and \( \mu = \pm \sqrt{-5l} \). The same conclusion holds if \( r = \tilde{\epsilon}^5(s - 1) \) and \( \bar{\tau}(b) = b' \).

On the other hand, suppose that \( l \equiv 2, 3 \pmod{5} \), and assume \( g(x) \) is an irreducible factor of \( \tilde{H}_{5,l}(X) = 0 \) over \( \mathbb{F}_l \). In this case the isogeny \( \phi \) is defined over \( \mathbb{F}_l(b) = \mathbb{F}_{l^2} \), where \( b \) is a root of \( g(x) = 0 \). The map \( \sigma = \left( b \rightarrow \tau(b) = \frac{b + \sqrt{5}}{\sqrt{5} - b} \right) \) is an automorphism of order \( 4 \) of \( \mathbb{F}_{l^2} \), satisfying \( \sigma^2 = (b \rightarrow -1/b) \). Hence, \( \tau(b) = b' \) or \( \sigma^2(b) = -1/\tau(b) = \bar{\tau}(b) = b' \).

In the first case, the isogeny \( \bar{\phi} : E_5(b) \rightarrow E_5(\bar{\tau}(b)) = E_5(b'^3) \) is obtained by replacing \( \sqrt{5} \) by \(-\sqrt{5} \) in the formulas for \( \phi \). By Lemma 3.1, the isogeny \( \bar{\phi} : E_5(b'^3) \rightarrow E_5(b) \) can be obtained by replacing \( b \) by \( \bar{\tau}(b) \) in the formulas for \( \bar{\phi} \). If the coefficients \( c \) in \( \bar{\phi} \) are replaced by \( c'^3 \), this doesn’t result in \( \tilde{\phi} \), but in an isogeny \( \tilde{\phi} \) taking \( E_5(\bar{\tau}(b)) \) to \( E_5(\bar{\tau}(\tau(b))) \) = \( E_5(-1/b) = E_5(b'^2) \). However, it is still the case that \( \ker(\tilde{\phi}) = \langle (0,0) \rangle \) in \( E_5(\bar{\tau}(b)) \). Hence, if \( \mu = \bar{\phi} \), we have that \( \mu \in \text{End}(E_5(b)) \), and the endomorphism \( \mu^2 \) given by

\[
\mu^2(P) = \left[ \tilde{\phi}(\tilde{\phi}(P)) \right]^l = (\pm \tilde{\phi} \circ \tilde{\phi}(P))^l
\]

still has the kernel \( E_5(b)[5] \). As in the proof of Lemma 3.1, we conclude that \( \mu^2 = -5l \) in \( \text{End}(E_5(b)) \) (in characteristic \( l > 7 \)). A similar argument works if \( \tilde{\tau}(b) = b' \). This proves the following.

**Theorem 3.2.** If \( l > 7 \) is a prime, then for any root \( b \) of an irreducible factor of \( \tilde{H}_{5,l}(x) \) over \( \mathbb{F}_l \) of the form

\[
g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1,
\]

or of the form \( k(x) = x^2 + rx + s \) with \( r = \tilde{\epsilon}^5(s - 1) \) or \( r = \tilde{\epsilon}^5(s - 1) \), there is a multiplier \( \mu \in \text{End}(E_5(b)) \) satisfying \( \mu^2 = -5l \).

Now Deuring’s lifting theorem \([10]\) yields the following theorem.

**Theorem 3.3.** If \( l > 7 \) is a prime, any irreducible factor of \( \tilde{H}_{5,l}(x) \) over \( \mathbb{F}_l \) of the form

\[
g(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1 \text{ or } k(x) = x^2 + rx + s,
\]

with \( r = \tilde{\epsilon}^5(s - 1) \) or \( r = \tilde{\epsilon}^5(s - 1) \), arises by reduction as a factor of

\[
F_d(x) = x^{5h(-d)}(1 - 11x - x^2)^{h(-d)}H_{-d}(j(x)) \text{ modulo } l,
\]

19
with
\[ j(x) = \frac{(x^4 + 12x^3 + 14x^2 - 12x + 1)^3}{x^5(1 - 11x - x^2)}, \]
for one of the discriminants \(-d = -5l\) or \(-d = -20l\).

The factors \(k(x) = x^2 + (11 \pm 5\sqrt{5})x - 1\) mentioned above are also covered by the statements in these two theorems, since
\[
F_{20}(x) = (x^4 + 22x^3 - 6x^2 - 22x + 1)(x^{20} + 50x^{19} + 1150x^{18} + 14550x^{17} + 118525x^{16} + 1746272x^{15} + 34835400x^{14} + 376573200x^{13} + 195087560x^{12} + 4311023700x^{11} + 2400976244x^{10} - 4311023700x^9 + 195087560x^8 - 376573200x^7 + 34835400x^6 - 1746272x^5 + 118525x^4 - 14550x^3 + 1150x^2 - 50x + 1),
\]
when \(\epsilon_{20} = 1\), i.e. when \(p \equiv \pm 1 \pmod{5}\) and \(p \equiv 3 \pmod{4}\).

4 Analyzing the special factors of \(K_{5l}(X)\)

By Theorem 3.3, the \(j\)-invariants corresponding to factors of the form \(g(x)\) or \(k(x)\) of \(\tilde{H}_{5l}(x)\) over \(\mathbb{F}_l\) are reductions of roots of \(K_{5l}(X)\). In this section we will show that each of the factors \(H_{-d}(X)^{4x_d} \ (d \in \mathbb{F})\) in Theorem 2.1 yields \(\deg(H_{-d}(X))\) factors of the form \(g(x)\), when \(l \equiv 2, 3 \pmod{5}\), and \(2\deg(H_{-d}(X))\) factors of the form \(k(x)\) when \(l \equiv 1, 4 \pmod{5}\).

We start with the case \(l \equiv 2, 3 \pmod{5}\). Define
\[
F_d(x) = x^{5h(-d)(1 - 11x - x^2)}H_{-d}(j(x)),
\]
where
\[
j(x) = \frac{(x^4 + 12x^3 + 14x^2 - 12x + 1)^3}{x^5(1 - 11x - x^2)}.
\]
First, \(\epsilon_{20} = 0\) for the prime \(l\), so we can ignore \(F_{20}(x)\) for these primes. For the linear class equations, we have
\[
F_4(x) = (x^2 + 1)^2(x^4 + 18x^3 + 74x^2 - 18x + 1),
F_{11}(x) = (x^4 + 4x^3 + 46x^2 - 4x + 1)
\times (x^8 + 32x^7 + 300x^6 + 32x^5 - 8026x^4 - 32x^3 + 300x^2 - 32x + 1),
F_{16}(x) = (x^4 + 18x^3 + 200x^2 - 18x + 1)
\times (x^8 + 18x^7 - 50x^6 + 18x^5 + 15774x^4 - 18x^3 - 50x^2 - 18x + 1),
F_{19}(x) = (x^4 + 36x^3 + 398x^2 - 36x + 1)(x^8 + 76x^6 - 24474x^4 + 76x^2 + 1).
\]
The factor \((x^2+1)^2\) is a reducible polynomial of the form \(g(x)\), while the last three quartics are irreducible polynomials of the form \(g(x)\) in characteristic zero. These polynomials are denoted by \(Q_d(x)\) in [20 Prop. 4.1], and are irreducible factors of \(F_d(x)\) of degree \(4h(-d)\), for any \(d > 4\) satisfying \(d \equiv \pm 1 \pmod{5}\).

The discriminants of these three quartics are, respectively,

\[
\begin{align*}
\text{disc}(Q_{11}(x)) &= 2^{12}5^311^2, \\
\text{disc}(Q_{16}(x)) &= 2^63^45^311^4, \\
\text{disc}(Q_{19}(x)) &= 2^{12}3^45^219^2.
\end{align*}
\]

If \(\epsilon_d = 1\) for a prime \(l > 19\), then their reductions \((\text{mod } l)\) must divide \(\tilde{H}_{5,l}(x)\). But [15 Thm. 6.2] asserts that \(\tilde{H}_{5,l}(x)\) can only have irreducible factors which are either quartic or \(x^2 + 1\). If one of these factors were reducible \((\text{mod } l)\), then it would have to factor as \((x^2 + 1)^2\) \((\text{mod } l)\), which is impossible for \(l > 19\). Hence, each of these quartics yields an irreducible \(g(x) \pmod{l}\) for any prime \(l\) for which the corresponding \(\epsilon_d = 1\).

On the other hand, the remaining polynomials in the above factorizations are not divisible by polynomials over \(\mathbb{F}_l\) of the form \(g(x)\) for large enough primes, by the following argument. This is obvious for the quartic factor of \(F_4(x)\), when \(l\) does not divide \(11 \cdot 18 + 2 - 74 = 2 \cdot 3^2 \cdot 7\). If

\[
f_{11}(x) = x^8 + 32x^7 + 300x^6 + 32x^5 - 8026x^4 - 32x^3 + 300x^2 - 32x + 1
\]

is divisible \((\text{mod } l)\) by a factor of the form \(g(x) = x^4 + tx^3 + (11t + 2)x^2 - tx + 1\), then since \(x^8f_{11}(-1/x) = f_{11}(x)\) and \(x^4g(-1/x) = g(x)\), we can write

\[
\begin{align*}
f_{11}(x) &= x^4\tilde{f}_{11} \left( x - \frac{1}{x} \right), \\
\tilde{f}_{11}(x) &= x^4 + 32x^3 + 304x^2 + 128x - 7424, \\
g(x) &= x^2\tilde{g} \left( x - \frac{1}{x} \right), \\
\tilde{g}(x) &= x^2 + tx + 11t + 4.
\end{align*}
\]

Then \(g(x) \mid f_{11}(x)\) implies \(\tilde{g}(x) \mid \tilde{f}_{11}(x) \pmod{l}\). On the other hand, the remainder on dividing \(\tilde{f}_{11}(x)\) by \(\tilde{g}(x)\) is

\[
r_{11}(x) = (-t^3 + 54t^2 - 648t)x - 11t^3 + 469t^2 - 3128t - 8624.
\]

If this is 0 \((\text{mod } l)\), then \(l\) must divide the resultant of the coefficients in \(t\), which is

\[
\text{Res}_t(-t^3 + 54t^2 - 648t, -11t^3 + 469t^2 - 3128t - 8624) = -2^{17}7^3 \cdot 11 \cdot 13 \cdot 19 \cdot 43.
\]
It follows that \( f_{11}(x) \) contributes no irreducible factors of the form \( g(x) \) to \( \hat{H}_{5,l}(x) \), for \( l > 43 \). The same argument works for the 8-th degree factors \( f_{16}(x) \) and \( f_{19}(x) \) in the above factorizations, since the corresponding resultants are

\[
\text{Res}_t(-t^3 + 40t^2 - 144t, -11t^3 + 315t^2 + 666t + 15876) = 2^6 \cdot 3^3 \cdot 7^3 \cdot 79 \cdot 19 \cdot 43 \cdot 67;
\]
\[
\text{Res}_t(-t^3 + 22t^2 - 72t, -11t^3 + 117t^2 - 792t - 24624) = 2^5 \cdot 3^9 \cdot 13 \cdot 19 \cdot 67.
\]

This proves that there is one irreducible factor of the form \( \hat{H}_{5,l}(x) \) for each of the factors \( H_{-d}(X)^{4d} \) (when \( \epsilon_d = 1 \)), for \( d = 11, 16, 19 \), and no such factors for \( H_{-d}(X)^{4d} \), for \( l > 67 \). For \( l \equiv 1 \pmod{4} \), this gives one factor \( g(x) \) for each linear factor \( H_{-d}(x) \) dividing \( K_{5l}(x) \); and for \( l \equiv 3 \pmod{4} \), one less than that, since \( H_4(x)^4 \) divides \( K_{5l}(x) \) but does not yield a factor \( g(x) \).

Consider next the quadratic class equations \( H_{-d}(X) \), for \( d \) one of the integers in \( \{24, 36, 51, 64, 91, 99\} \). We see first that

\[
F_{24}(x) = (x^8 - 12x^7 + 16x^6 + 315x^5 + 16878x^4 - 3156x^3 + 16x^2 + 12x + 1) \\
\times (x^{16} + 8x^{15} + 3236x^{14} + 73860x^{13} + 983188x^{12} + 6801300x^{11} \\
+ 18487964x^{10} + 6727524x^9 + 7889398x^8 - 6727524x^7 + 18487964x^6 \\
- 6801300x^5 + 983188x^4 - 73860x^3 + 3236x^2 - 84x + 1) \\
= Q_{24}(x)f_{24}(x),
\]

where \( \epsilon_{24} = 1 \) when \( \left( \frac{-d}{t} \right) = \left( \frac{2}{t} \right) = -1 \), so that \( \left( \frac{-2}{t} \right) = +1 \). Now the 8-th degree factor \( Q_{24}(x) \) is the product of

\[
g_{24}(x) = x^4 + (-6 + 6\sqrt{-3})x^3 + (-64 + 66\sqrt{-3})x^2 + (6 - 6\sqrt{-3})x + 1
\]

and its conjugate over \( \mathbb{Q} \). Since \( \left( \frac{-2}{t} \right) = +1 \), these two factors give two irreducible factors of the form \( g(x) \) mod \( l \), when \( l > 19 \), the largest prime dividing \( \text{disc}(Q_{24}(x)) \). On the other hand, transforming \( f_{24}(x) \) as we did above to yield the 8-th degree polynomial

\[
\tilde{f}_{24}(x) = x^8 + 84x^7 + 3244x^6 + 74448x^5 + 1002624x^4 + 7171776x^3 \\
+ 22449856x^2 + 27501312x + 117842176,
\]

the remainder of \( \tilde{f}_{24}(x) \) on dividing by \( \tilde{g}(x) \) is \( A_{24}(t)x + B_{24}(t) \), with

\[
A_{24}(t) = -t^7 + 150t^6 - 9050t^5 + 280932t^4 - 4646880t^3 + 36376128t^2 \\
- 86966784t;
\]
\[
B_{24}(t) = -11t^7 + 1525t^6 - 83550t^5 + 2295377t^4 - 31830180t^3 + 178683408t^2 \\
- 134106624t + 43877376.
\]
We compute that
\[
\text{Res}_t(A_{24}(t), B_{24}(t)) = -2^{47}3^{23}13^417\cdot 19^523^37\cdot 41\cdot 43^247\cdot 61\cdot 67\cdot 71\cdot 89\cdot 109\cdot 113.
\]
Hence, \( F_{24}(x) \) contributes exactly \( 2 = \deg(H_{-24}(x)) \) irreducible quadratics of the form \( g(x) \), for \( l > 113 \), when \( \epsilon_{24} = 1 \).

The same pattern of argument works for the remaining integers in the set \( \{24, 36, 51, 64, 91, 99\} \). For each such \( d \), \( F_d(x) \) contributes exactly \( 2 = \deg(H_{-d}(x)) \) irreducible quadratics of the form \( g(x) \), for primes \( l \) greater than the largest of the primes dividing the corresponding resultants \( R(d) = \text{Res}(A_d(t), B_d(t)) \), where \( r_d = A_d(t)x + B_d(t) \) is the remainder on dividing the corresponding 8-th degree polynomial \( \tilde{f}_d(x) \) by \( \tilde{g}(x) \). The results are given in Tables 1 and 2. Table 1 contains the quartic polynomials which are factors of each \( Q_d(x) \) and reduce to polynomials of the form \( g(x) \) mod \( l \), and Table 2 lists the factorizations of the resultants \( R(d) \). Table 3 contains the discriminants of the polynomials \( Q_d(x) \).

A similar argument works for \( d = 84 \) and \( d = 96 \). The condition \( \epsilon_{84} = 1 \) implies that
\[
\left( \frac{-84}{l} \right) = \left( \frac{3}{l} \right) = \left( \frac{7}{l} \right) = -1,
\]
hence \( l \equiv 3 \mod 4 \) and
\[
\left( \frac{21}{l} \right) = \left( \frac{-3}{l} \right) = \left( \frac{-7}{l} \right) = +1.
\]
Thus, the polynomial listed in Table 1 for \( d = 84 \) reduces to an irreducible \( g(x) \) (mod \( l \)), and for \( l > 79 \), taking its conjugates (over \( \mathbb{Q} \)) gives four distinct quartic factors of \( \tilde{H}_{5,l}(x) \) of this form. A similar argument applies for \( d = 96 \), since in this case
\[
\left( \frac{-96}{l} \right) = \left( \frac{2}{l} \right) = \left( \frac{3}{l} \right) = -1,
\]
in order for \( \epsilon_{96} = 1 \), which implies once again that \( l \equiv 3 \mod 4 \) and
\[
\left( \frac{6}{l} \right) = \left( \frac{-2}{l} \right) = \left( \frac{-3}{l} \right) = +1.
\]
To complete the argument in these cases, we transform the cofactor \( f_d(x) \) in the factorization \( F_d(x) = Q_d(x)f_d(x) \), obtaining \( \tilde{f}_d(x) \) of degree 16, and divide by \( \tilde{g}(x) \) to obtain the remainder \( r_d = A_d(t)x + B_d(t) \), as before. Then
Table 1: Quartic factors $g_d(x)$ over $\mathbb{F}_l$.

| $d$ | $g_d(x) = x^4 + ax^3 + (11a + 2)x^2 - ax + 1$ |
|-----|------------------------------------------------|
| 11  | $x^4 + 4x^3 + 46x^2 - 4x + 1$                  |
| 16  | $x^4 + 18x^3 + 200x^2 - 18x + 1$               |
| 19  | $x^4 + 36x^3 + 398x^2 - 36x + 1$               |
| 24  | $x^4 - (6 - 6\sqrt{-3})x^3 + (-64 + 66\sqrt{-3})x^2 + (6 - 6\sqrt{-3})x + 1$ |
| 36  | $x^4 + (30 + 22\sqrt{-3})x^3 + (332 + 242\sqrt{-3})x^2 - (30 + 22\sqrt{-3})x + 1$ |
| 51  | $x^4 - (12 - 48\sqrt{-3})x^3 + (-130 + 528\sqrt{-3})x^2 + (12 - 48\sqrt{-3})x + 1$ |
| 64  | $x^4 - (108 - 63\sqrt{-2})x^3 + (-1186 + 693\sqrt{-2})x^2 + (108 - 63\sqrt{-2})x + 1$ |
| 91  | $x^4 - (108 - 144\sqrt{-7})x^3 + (-1186 + 1584\sqrt{-7})x^2 + (108 - 144\sqrt{-7})x + 1$ |
| 99  | $x^4 + (436 + 176\sqrt{-3})x^3 + (4798 + 1936\sqrt{-3})x^2 - (436 + 176\sqrt{-3})x + 1$ |
| 84  | $x^4 - (117 + 57\sqrt{-3} + 27\sqrt{21} + 33\sqrt{-7})x^3 - (1285 + 627\sqrt{-3} + 297\sqrt{21} + 363\sqrt{-7})x^2 + (117 + 57\sqrt{-3} + 27\sqrt{21} + 33\sqrt{-7})x + 1$ |
| 96  | $x^4 + (81 + 159\sqrt{-2} + 129\sqrt{-3} + 33\sqrt{6})x^3 + (893 + 1749\sqrt{-2} + 1419\sqrt{-3} + 363\sqrt{6})x^2 - (81 + 159\sqrt{-2} + 129\sqrt{-3} + 33\sqrt{6})x + 1$ |
Table 2: Prime factorization of $R(d) = \text{Res}(A_d(t), B_d(t))$.

| $d$ | $R(d)$ (Primes with $\epsilon_d = 1$ in bold.) |
|-----|---------------------------------------------|
| 20  | $2^{69}5^{27}11^913^817^419^631^437^3 \cdot 53 \cdot 59 \cdot 71 \cdot 73^2 \cdot 79^2 \cdot 97$ |
| 24  | $-2^{47}3^{23}13^417 \cdot 19^523^337 \cdot 41 \cdot 43^247 \cdot 61 \cdot 67 \cdot 71 \cdot 89 \cdot 109 \cdot 113$ |
| 36  | $2^{52}3^{10}7^{11}16^619^323 \cdot 31 \cdot 43^2 \cdot 67 \cdot 71 \cdot 79 \cdot 83 \cdot 107 \cdot 127 \cdot 139 \cdot 151 \cdot 163 \cdot 167$ |
| 51  | $-2^{75}3^{24}7^{11}17^2 \cdot 31 \cdot 37 \cdot 47^253 \cdot 59 \cdot 61 \cdot 79 \cdot 83 \cdot 139 \cdot 163 \cdot 179 \cdot 211$ |
| 64  | $2^{14}3^{34}7^{12}11^319^5 \cdot 23 \cdot 31^243^2 \cdot 59 \cdot 67 \cdot 79 \cdot 127 \cdot 139 \cdot 151 \cdot 163 \cdot 167 \cdot 211 \cdot 223 \cdot 283 \cdot 307$ |
| 91  | $2^{74}3^{37}7^{13}13^4 \cdot 17 \cdot 37 \cdot 61^2 \cdot 67 \cdot 71 \cdot 103 \cdot 109 \cdot 139 \cdot 151 \cdot 163 \cdot 283 \cdot 331 \cdot 379$ |
| 99  | $2^{75}7^{11}11 \cdot 13^317 \cdot 19^329^341^243^2 \cdot 61 \cdot 79 \cdot 83^2 \cdot 107^2 \cdot 109 \cdot 127 \cdot 139 \cdot 211 \cdot 227 \cdot 283 \cdot 307 \cdot 347$ |
| 84  | $2^{102}3^{87}7^{24}13^{22}29^{10}43^847^553 \cdot 59^61^367^373^279^383^597^3 \cdot 113 \cdot 127 \cdot 131^2 \cdot 137 \cdot 149 \cdot 151 \cdot 157 \cdot 163 \cdot 167^2 \cdot 181 \cdot 197 \cdot 211^2 \cdot 227 \cdot 229 \cdot 233^2 \cdot 241 \cdot 281 \cdot 311 \cdot 313 \cdot 317 \cdot 331 \cdot 349 \cdot 379 \cdot 383 \cdot 389 \cdot 397 \cdot 401 \cdot 409$ |
| 96  | $-2^{104}3^{89}13^{22}17^619^{14}23^{12}37^741^643^847^461^667^71^2 \cdot 89 \cdot 109^311^213^2137^2139^4 \cdot 163 \cdot 167 \cdot 211 \cdot 229 \cdot 239 \cdot 257 \cdot 263^2 \cdot 277^2 \cdot 281 \cdot 283 \cdot 307 \cdot 331 \cdot 349 \cdot 353 \cdot 359 \cdot 373 \cdot 379 \cdot 383 \cdot 397 \cdot 401 \cdot 421 \cdot 431 \cdot 449$ |
Table 3: Discriminant of $Q_d(x)$.

| $d$ | $\text{disc}(Q_d(x))$ | $d$ | $\text{disc}(Q_d(x))$ |
|-----|------------------------|-----|------------------------|
| 11  | $2^{12}5^{3}11^2$      | 19 | $2^{12}3^{4}5^{3}19^2$ |
| 16  | $2^{6}3^{4}5^{3}11^4$  |     |                        |
| 24  | $2^{44}3^{16}5^{18}19^4$ | 64 | $2^{18}3^{24}5^{18}7^{8}11^819^459^4$ |
| 36  | $2^{48}3^{6}5^{18}7^{11}8^{31}4$ | 91 | $2^{64}3^{24}5^{18}7^{4}11^813^{4}71^4$ |
| 51  | $2^{64}3^{16}5^{18}7^{4}31^4$ | 99 | $2^{64}3^{4}5^{18}7^{4}11^{12}19^{8}79^4$ |
| 84  | $2^{192}3^{6}4^{5}8^{4}7^{20}13^{16}29^{8}59^879^4$ | 96 | $2^{96}3^{72}5^{8}4^{13}16^{17}16^{19}8^{4}61^{8}71^8$ |

the resultant $R(d)$ for these two cases is given in Table 2. Moreover, we only need to exclude the primes in bold in Table 2, since the non-bold primes have $\epsilon_d = 0$. Keeping Theorem 2.1 and Corollary 2.2 in mind, this proves the following.

**Proposition 4.1.** When $l \equiv 2, 3 \pmod{5}$ and $l \in S$ or $l > 379$, each of the factors $H_{-d}(X)^{4\epsilon_d}$ of $K_{5l}(X)$ in Theorem 2.1 contributes exactly $\deg(H_{-d}(X))$ irreducible factors of the form $g(x)$ in Theorem 3.3 to the factorization of $\tilde{H}_{5,l}(x) \pmod{l}$, except for the factor $H_{-4}(X)^{4\epsilon_4}$ when $l \equiv 3 \pmod{4}$.

If we prove that each of the remaining factors $(X^2 + a_iX + b_i)^2$ in Theorem 2.1 contributes only one irreducible factor of the form $g(x)$, then this will prove Theorem 1.1A for $l \in S$ or $l > 379$. Namely, the above discussion gives exactly $N = \frac{1}{4}\deg(K_{5l}(X)) = \frac{h(-5l)}{4}$ factors $g(x)$ when $l \equiv 1 \pmod{4}$, and $N - 1 = \frac{1}{4}(h(-5l) + h(-20l) - 4)$ such factors when $l \equiv 3 \pmod{4}$. For the latter primes, $h(-5l) = h(-5l)$ and $h(-20l) = h(-5l)$ or $3h(-5l)$ according as $\left(\frac{-5l}{2}\right) = +1$ or $-1$, which implies the formulas of Theorem 1.1A. This yields all the irreducible factors $g(x)$ of $\tilde{H}_{5,l}(x)$ by Theorem 3.3.

We turn now to the primes $l \equiv 1, 4 \pmod{5}$.

**Proposition 4.2.** If $l \equiv \pm 1 \pmod{5}$ and $l > 79$, then for $d \in \mathcal{V}$, the polynomial $g_d(x)$ in Table 1 is a product of two irreducible polynomials over
\[ F_l \] of the form \( k(x) = x^2 + rx + s \), where \( r = \varepsilon^5(s - 1) \) or \( r = \bar{\varepsilon}^5(s - 1) \).

**Proof.** This follows from the computations at the beginning of Section 3, according to which the roots of \( g_d(x) \) are linear combinations of the square-roots \( \sqrt{-\Theta_i} \), where \( \Theta_2\Theta_3 = -\frac{a^2}{4} \Theta_1 \), and
\[
-\Theta_1 = \frac{1}{4}(a^2 - 44a - 16).
\]

Each of the \( \Theta_i \) lies in \( F_l \), for primes \( l \equiv \pm 1 \pmod{5} \), and none is zero in \( F_l \), since the largest prime factor of any value \( N_Q(a) \) in Table 4 is 19, and the largest prime factor of any value \( N_Q(a^2 - 44a - 16) \) is 79. Moreover, the final column in Table 4 shows that in every case, \( \left( \frac{-\Theta_1}{l} \right) = \left( \frac{-d}{l} \right) = -1 \), so that \( -\Theta_1 \) is always a quadratic nonresidue \( \pmod{l} \). Hence, one of \( -\Theta_2 \) and \( -\Theta_3 \) is a quadratic residue, and one is a quadratic nonresidue. If \( -\Theta_2 \) is a quadratic residue, then
\[
x^2 + rx + s = (x - \rho_1)(x - \rho_2) \quad x^2 + r'x + s' = (x - \rho_3)(x - \rho_4)
\]
are factors of \( g_d(x) \) over \( F_l \) with \( r = \varepsilon^5(s - 1) \) and \( r' = \bar{\varepsilon}^5(s' - 1) \); while if \( -\Theta_3 \) is a quadratic residue, then
\[
x^2 + rx + s = (x - \rho_1)(x - \rho_4) \quad x^2 + r'x + s' = (x - \rho_2)(x - \rho_3)
\]
are factors of \( g_d(x) \) over \( F_l \) with \( r = \varepsilon^5(s - 1) \) and \( r' = \bar{\varepsilon}^5(s' - 1) \). These factors are irreducible over \( F_l \) in every case, since the Pellet-Stickelberger-Voronoi Theorem (see [6, Appendix]) implies that \( g_d(x) \) has an even number of irreducible factors. This is because \( \text{disc}(g_d(x)) = 125a^2(a^2 - 44a - 16)^2 \) is always a square in \( F_l \), and the PSV Theorem says that
\[
\left( \frac{\text{disc}(g_d(x))}{l} \right) = (-1)^{4r},
\]
where \( r \) is the number of irreducible factors \( \pmod{l} \). We know that \( r \geq 2 \). If \( r = 4 \), then all the roots \( \rho_i \in F_l \), implying that all the numbers \( -\Theta_i \) would be squares \( \pmod{l} \), which is not the case. Therefore, \( r = 2 \) and we get two distinct factors of the form \( k(x) = x^2 + rx + s \) satisfying the required conditions, for each factor \( g_d(x) \) in Table 1. This proves the proposition. □

When \( l \equiv 3 \pmod{4} \), the factor \( k(x) = x^2 + 1 \) divides \( F_4(x) \), and is certainly a factor of \( \tilde{H}_{5,l}(x) \). Moreover, in this case \( c_{20} = 1 \), and \( F_{20}(x) \) is divisible by \( Q_{20}(x) = x^4 + 22x^3 - 6x^2 - 22x + 1 = (x^2 + (11 + 5\sqrt{5})x - \ldots
\]

27
Table 4: $-4\Theta_1 = a^2 - 44a - 16$ for $a$ in $g_d(x)$.

| $d$ | $a$ | $a^2 - 44a - 16$ |
|-----|-----|------------------|
| 11  | 4   | $-2^4 \cdot 11$ |
| 16  | 18  | $-2^2 \cdot 11^2$ |
| 19  | 36  | $-2^4 \cdot 19$ |
| 24  | $-6 + 6\sqrt{-3}$ | $2^5 \left(\frac{-3\sqrt{-3}}{2}\right)^2$ |
| 36  | $30 + 22\sqrt{-3}$ | $-2^6 \left(\frac{11-\sqrt{-3}}{2}\right)^2$ |
| 51  | $-12 + 48\sqrt{-3}$ | $2^4(17)(2 - 3\sqrt{-3})^2$ |
| 64  | $-108 + 63\sqrt{-2}$ | $-(90 + 91\sqrt{-2})^2$ |
| 91  | $-108 + 144\sqrt{-7}$ | $2^4(13)(9 - 10\sqrt{-7})^2$ |
| 99  | $436 + 176\sqrt{-3}$ | $-2^4(11)(23 - 18\sqrt{-3})^2$ |
| 84  | $-117 - 57\sqrt{-3} - 27\sqrt{21} - 33\sqrt{-7}$ | $-(-104 + 78\sqrt{-3} - 18\sqrt{21} + 48\sqrt{-7})^2$ |
| 96  | $81 + 159\sqrt{-2} + 129\sqrt{-3} + 33\sqrt{6}$ | $-(-221 + 51\sqrt{-2} + 39\sqrt{-3} - 93\sqrt{6})^2$ |
$1)(x^2 + (11 - 5\sqrt{5})x - 1)$, which is a product of two factors of the form $k(x) = x^2 + rx + s$. Also,

$$\text{disc}(x^2 + (11 + 5\sqrt{5})x - 1) = 250 + 110\sqrt{5} = 2^2(5\sqrt{5})^5.$$ 

Thus, $q(x) = x^2 + (11 + 5\sqrt{5})x - 1$ factors into linear factors (mod $l$) if \( (5+\sqrt{5}/2)^l = +1 \) and is irreducible (mod $l$) otherwise. Now $L_2 = \mathbb{Q}(\sqrt{5+\sqrt{5}}/2)$ is the real subfield of the field $\mathbb{Q}(\zeta_{20})$ (see [21, p. 6]). It corresponds by class field theory to the congruence subgroup $H = \{ \pm 1 \text{ mod } 20 \} \subset (\mathbb{Z}/20\mathbb{Z})^\times$. If $l \equiv 3 \pmod{4}$ and $l \equiv 4 \pmod{5}$, then $l \equiv 19 \pmod{20}$ so the polynomial $Q_{20}(x)$ splits, and $d = 20$ yields no factors of the form $k(x)$. On the other hand, if $l \equiv 3 \pmod{4}$ and $l \equiv 1 \pmod{5}$, then $l \equiv 11 \pmod{20}$, and $l$ has order 2 modulo $H$, implying that $Q_{20}(x)$ is a product of two irreducible polynomials (mod $l$). Thus, $d = 20$ yields two factors of the form $k(x)$, when $l \equiv 1 \pmod{5}$.

Aside from the quadratic factors of $Q_{20}(x)$, the factor $k(x) = x^2 + rx + s$ always occurs with its companion $\bar{k}(x) = \frac{1}{s}x^2k(-1/x) = x^2 - \frac{r}{x} + \frac{1}{s}$, such that $k(x)\bar{k}(x) = g(x)$ is a polynomial of the form $g(x)$. Since the roots of each cofactor $f_d(x)$ are stable under the mapping $x \to -1/x$, the previous calculation shows that none of these cofactors are divisible by a polynomial of the form $k(x)$, for $l \in S$ or $l > 379$. It is only necessary to check that $f_{20}(x)$ is also not divisible by a polynomial of the form $g(x)$ modulo any of these primes, and this follows from the entry $R(20)$ in Table 2.

If we can show that each of the factors $(X^2 + a_iX + b_i)^2$ in Theorem 2.1 yields two factors of the form $k(x)$, then we can complete the proof of Theorems 1.1B and C as follows. For each of the factors $H_{-d}(X)^{\epsilon_d}$ with $d \neq 4$, we have $2\deg(H_{-d}(X))$ factors of the form $k(x)$. By the above comments, this gives a total of

$$\sum_{d \in \mathbb{T}\setminus\{4\}} 2\epsilon_d \deg(H_{-d}(X)) + \sum_{X^2 + a_iX + b_i} 2 + \epsilon_4(1 + 2\delta_{l,1}),$$

factors of the form $k(x)$, where $\delta_{l,1} = 1$ if $l \equiv 1 \pmod{5}$ and is 0 otherwise. But this latter expression equals

$$\frac{1}{2}(\deg(K_{5l}(X)) - 4\epsilon_4 - 4\epsilon_4) + \epsilon_4(1 + 2\delta_{l,1}) = \frac{a_l}{2}h(-5l) - 3\epsilon_4 + 2\epsilon_4\delta_{l,1},$$

29
where the last equality follows from $\epsilon_4 = \epsilon_{20}$. This equals $\frac{q}{\tau^2} h(-5l)$ if $l \equiv 1 \pmod{4}$; $\frac{q}{\tau} h(-5l) - 3$ if $l \equiv 3 \pmod{4}$ and $l \equiv 4 \pmod{5}$; and $\frac{q}{\tau} h(-5l) - 1$ if $l \equiv 3 \pmod{4}$ and $l \equiv 1 \pmod{5}$. This yields the formulas of Theorem 1.1B and C, for $l \in S$ or $l > 379$.

5 Values of $r(\tau)$ over $\mathbb{Q}(\sqrt{-5l})$

In this section we prove that each factor $(X^2 + a_iX + b_i)^2$ in Theorem 2.1 yields at least one factor of the form $g(x)$, or two factors of the form $k(x)$, for the appropriate congruence conditions on $l$. Let $r(\tau)$ denote the Rogers-Ramanujan continued fraction:

\[ r(\tau) = \frac{q^{1/5}}{1 + \frac{q}{1 + \frac{q}{1 + \frac{q^2}{1 + \frac{q^5}{1 + \cdots}}}}} \]

\[ = q^{1/5} \prod_{n \geq 1} (1 - q^n)^{(n/5)}, \quad q = e^{2\pi i \tau}, \quad \tau \in \mathbb{H}. \]

See [1], [2], [13].

Proposition 5.1. (a) If $l \equiv 3 \pmod{4}$ and

\[ \tau_1 = \frac{5 + \sqrt{-5l}}{10}, \]

then $\rho_1 = r(\tau_1)^5$ is a real algebraic number of degree $2h(-5l)$ over $\mathbb{Q}$, contained in the ray class field $\Sigma_{\psi_5}$, where $\psi_5 \cong 5$ in $K = \mathbb{Q}(\sqrt{-5l})$. Moreover, $\Sigma_{\psi_5} = K(\rho_1)$.

(b) Let $f = 1$, if $l \equiv 1 \pmod{4}$; and $f = 2$, if $l \equiv 3 \pmod{4}$. If

\[ \tau_2 = \frac{\sqrt{-5l}}{5}, \]

then $\rho_2 = r(\tau_2)^5$ is a real algebraic number of degree $2h(-20l)$ over $\mathbb{Q}$, contained in the class field $\Sigma_{\psi_5} \Omega_f$. Moreover, $\Sigma_{\psi_5} \Omega_f = K(\rho_2)$.

Proof. (a) We first recall the identity

\[ \frac{1}{r^5(\tau)} - 11 - r^5(\tau) = \left( \frac{\eta(\tau)}{\eta(5\tau)} \right)^6, \]

30
where \( \eta(\tau) \) is the Dedekind \( \eta \)-function. From Schertz \[25\] p. 159, applied to the function \( \left( \frac{\eta(w/5)}{\eta(w)} \right)^6 \gamma_3(w)^2 \), with \( w = 5\tau_1 \), we have that \( \lambda = \left( \frac{\eta(\tau_1)}{\eta(5\tau_1)} \right)^6 \in \Sigma \), the Hilbert class field of \( K \), and
\[
q(r^5(\tau_1), \lambda) = r^{10}(\tau_1) + (11 + \lambda)r^5(\tau_1) - 1 = 0.
\]
The discriminant of the quadratic \( q(x, \lambda) = x^2 + (11 + \lambda)x - 1 \in \Sigma[x] \) is
\[
(11 + \lambda)^2 + 4 = 125 + 22\lambda + \lambda^2 \cong \varphi_5^2 b, \quad (\varphi_5, b) = 1,
\]
using the fact that \( \lambda \cong \varphi_5^2 \) from Deuring’s treatise \[12\] p. 43] and that \( 125 = 5^3 \cong \varphi_5^6 \). Now \( \varphi_5 \) is unramified in \( \Sigma/K \), so is not the square of a divisor in \( \Sigma \). It follows that \( q(x, \lambda) \) is irreducible over \( \Sigma \), so that \( \rho_1 \) generates a quadratic extension of \( \Sigma \). Also,
\[
q_1 = e^{2\pi i \tau_1} = e^{\pi i - \frac{\lambda}{\varphi_5} \tau} = -e^{-\frac{\lambda}{\varphi_5} \tau}
\]
is real, so that \( r(\tau_1)^5 \in \mathbb{R} \).

Now by Thm. 15.16 in \[9\] (a result of Cho \[7\]), the fact that \( r^5(\tau) \) lies in the field \( F_5 \) of modular functions for \( \Gamma(5) \) implies that \( r^5(\tau_1) \in L_{\mathcal{O}_K,5} = \Sigma_5 \), where \( \Sigma_5 \) is the ray class field for the conductor \( 1 = \mathfrak{f} \). On the other hand, \( [\Sigma_5 : \Sigma] = \frac{\varphi_K(5)}{2} = 10 \), and therefore \( \rho_1 \) generates the unique quadratic subfield of \( \Sigma_5/\Sigma \), which is \( \Sigma_{\varphi_5} \). In particular, \( Q(\rho_1) \subseteq \Sigma_{\varphi_5}^+ \), the real subfield of the normal extension \( \Sigma_{\varphi_5}/Q \). Note that \( [\Sigma_{\varphi_5}^+ : Q] = 2h(−5l) \).

Further, the quantity \( j(\tau_1) \) is determined by the identity
\[
j(\tau) = \frac{(r^{20} - 228r^{15} + 494r^{10} + 228r^5 + 1)^3}{r^5(1 - 11r^5 - r^{10})^5}, \quad r = r(\tau).
\]
Hence, \( j(\tau_1) \in Q(r^5(\tau_1)) \), so that \( \rho_1 = r^5(\tau_1) \) has degree \( h(−5l) \) or \( 2h(−5l) \) over \( Q \). Since \( \rho_1 \notin \Sigma^+ = Q(\tau(\tau_1)) \), the latter must hold. Finally, the fact that \( \rho_1 \) is real implies that \( K(\rho_1) = KQ(\rho_1) = K\Sigma_{\varphi_5}^+ = \Sigma_{\varphi_5} \). This completes the proof.

(b) The same arguments work for part (b), if \( \Sigma, \Sigma_5 \) and \( \Sigma_{\varphi_5} \) are replaced everywhere by \( \Omega_2, \Sigma_5\Omega_2 \) and \( \Sigma_{\varphi_5}\Omega_2 \), when \( l \equiv 3 \pmod{4} \). In this case, \( L_{\mathcal{O}_K,5} \) is also to be replaced by \( L_{\mathcal{O}_2,5} \), where \( \mathcal{O}_2 = \mathbb{R}_{−20l} \) is the order of discriminant \( −20l \) in \( K \) and \( h(−20l) \) is its class number. \( \square \)

In the next lemma we use the following notation from \[20\] p. 1184. Let
\[
z(\tau) = r^5(\tau) - r^{-5}(\tau), \quad \tau \in \mathbb{H},
\]

31
so that
\[ z(\tau_k) = -11 - \lambda(\tau_k). \]

From [20, pp. 1180, 1184] we have
\[ j(\tau) = \frac{(z(\tau)^2 + 12z(\tau) + 16)^3}{z(\tau) + 11}. \]

**Lemma 5.2.** For a given ideal \( a = (a, w) \subseteq R_d \) \((d = 5l \text{ or } 20l)\) with ideal basis quotient \( \tau = w/a \), where \((a, f) = 1\) and \(5a \mid N(w)\), there is a unique value of \( z_1 \in \Omega_f \) for which
\[ J(z_1) = \frac{(z_1^2 + 12z_1 + 16)^3}{z_1 + 11} = j(w/a) \]
and \( z_1 + 11 \cong v_5^3 \), and this value is \( z_1 = z(\tau)^{\sigma^{-1}} \), where \( \sigma = \left( \frac{\Omega_f/K}{3K} \right) \).

**Proof.** This is proved as in Lemma 2.2 in [20]. The proof here, in the situation that \( 5 \mid d \), differs only in how the contradiction is obtained. In the proof given in [20], I derived the equations
\[ t^5 + 5t^4 + 15t^3 + 25t^2 + 25t + \frac{125}{z_1 + 11} = 0, \quad t^6 = 5^{3z_2 + 11} \]
assuming that there is some value \( z_2 \in \Omega_f \) different from \( z_1 = z(\tau)^{\sigma^{-1}} \) for which \( J(z_2) = J(z_1) \) and \( z_2 + 11 \cong z_1 + 11 \). In the present situation, \( 5 \cong v_5^2 \) in the field \( K = \mathbb{Q}(\sqrt{-5l}) \), and \( v_5 \) is unramified in the field \( \Omega_f \) (= \( \Sigma \) or \( \Omega_2 \)). The assumptions on \( z_2 \) imply that \( t^6 \cong v_5^6 \), and therefore \( t \cong v_5 \).
Furthermore, if \( p \) is a prime divisor of \( v_5 \) in \( \Omega' = \Omega_f(t) \), then \( p \) divides the algebraic integer \( t \), which implies in turn that
\[ p^5 \mid \theta = t^5 + 5t^4 + 15t^3 + 25t^2 + 25t. \]
But then \( p^5 \mid \frac{125}{z_1 + 11} \cong v_5^2 \), which implies that \( p^2 \mid v_5 \), so that \( v_5 \) is ramified in \( \Omega'/K \). Let \( e \geq 2 \) denote the ramification index of \( p \) over \( v_5 \). Then \( p^e \mid t \).
This contradicts that \( p^{5e} \mid \theta \), while \( p^{3e} \) exactly divides \( \frac{125}{z_1 + 11} = -\theta \). This establishes that no such \( z_2 \), distinct from \( z_1 \), exists. \( \square \)

Note that when \( l \equiv 3 \bmod 4 \) and \( f = 1 \), the quantities \( \frac{-1}{\tau_1} = \frac{-5 + \sqrt{-25l}}{2(5 + l)/4} \) and \( \frac{-1}{5\tau_1} = \frac{-5 + \sqrt{-25l}}{2(5 + 5l)/3} \) are basis quotients for ideals \( a = (\frac{5 + 4}{4}, \frac{-5 + \sqrt{-25l}}{2}) \) with
norm $N(a) = \frac{5+l}{4}$ and $\wp_5 a$ with norm $N(\wp_5 a) = \frac{5^2+5l}{4}$. In this case, we have that

$$\wp_5 a = \left( \frac{5(5+l)}{4}, \frac{-5 + \sqrt{-5l}}{2} \right) = \left( \frac{-5 + \sqrt{-5l}}{2} \right).$$

When $l \equiv 1 \pmod{4}$ or $l \equiv 3 \pmod{4}$ and $f = 2$, $\frac{-1}{\tau_2} = \frac{-\sqrt{-5l}}{l}$ and $\frac{-1}{\sqrt{-5l}} = \frac{-\sqrt{-5l}}{l}$ are basis quotients for the ideals $I = (l, \sqrt{-5l})$ and $\wp_5 I = (5l, \sqrt{-5l}) = (\sqrt{-5l})$, respectively. Let $a$ denote the ideal $I$ in this case, so that $\wp_5 a \sim 1 \pmod{f}$. It is clear that $I \sim \wp_5$ in $K$, so we also have $a \sim I$ when $l \equiv 3 \pmod{4}$ and $f = 1$.

The same arguments as above show that the quantities $r_5(-1/(5\tau_k))$ are quadratic over $\Omega_f$ and lie in $\Sigma_{\wp_5, \Omega_f}$; this also follows from the identity

$$r_5 \left( \frac{-1}{5\tau} \right) = -r_5(\tau) + \varepsilon^5 \varepsilon_{r_5}(\tau) + 1.$$

Since

$$j \left( \frac{-1}{5\tau_k} \right) = j(\wp_5 a) = j(\wp_5)^{\sigma_a^{-1}} = j(\tau_k)^{\sigma_a^{-1}},$$

where $\sigma_a = \left( \frac{\Omega_f/K_a}{a} \right)$, Lemma 5.2 implies that

$$z \left( \frac{-1}{5\tau_k} \right) = z(\tau_k)^{\sigma_a^{-1}},$$

and therefore also

$$\lambda' = \lambda \left( \frac{-1}{5\tau_k} \right) = \lambda(\tau_k)^{\sigma_a^{-1}}.$$

Note that $\lambda' = \lambda \left( \frac{-1}{5\tau_k} \right) = \frac{5^3}{\lambda(\tau_k)}$ by the transformation formula $\eta(-1/\tau) = \sqrt{\tau^2} \eta(\tau)$. Thus, $\lambda'$ and $\lambda$ are conjugate values over $K$ and

$$(x^2 + (11+\lambda)x - 1)(x^2 + (11 + \lambda')x - 1) = (x^2 + (11 + \lambda)x - 1)(x^2 + (11 + \frac{5^3}{\lambda})x - 1) = x^4 + (22 + \lambda + \frac{5^3}{\lambda})x^3 + [11(22 + \lambda + \frac{5^3}{\lambda}) + 2]\lambda^2 x^2 - (22 + \lambda + \frac{5^3}{\lambda})x + 1 = x^4 + j_5^*(\tau_k)x^3 + (11j_5^*(\tau_k) + 2)x^2 - j_5^*(\tau_k)x + 1,$$

33
where the modular function \( j_5^*(\tau) \) is defined by

\[
j_5^*(\tau) = \left( \frac{\eta(\tau)}{\eta(5\tau)} \right)^6 + 22 + 125 \left( \frac{\eta(5\tau)}{\eta(\tau)} \right)^6,
\]
as in [22] (see also [21]). This, together with the proof of Proposition 5.1, implies that

\[
g(x) = x^4 + j_5^*(\tau_k)x^3 + (11j_5^*(\tau_k) + 2)x^2 - j_5^*(\tau_k)x + 1
\]
divides the minimal polynomial of \( r^5(\tau_k) \) over \( K \).

However, \( a \sim \wp_5 \) (mod \( f \)) implies that \( \sigma_a = \sigma_{\wp_5} \) and \( \sigma_a \) has order 2. Then

\[
j_5^*(\tau_k) = 22 + \lambda + \frac{5^3}{\lambda} = -z(\tau_k) - z(\tau_k)^{\sigma_{\wp_5}},
\]
so that \( j_5^*(\tau_k) \in L \), the fixed field of the subgroup \( \langle \sigma_{\wp_5} \rangle \) of \( \text{Gal}(\Omega_f/K) \). Now \( [\Sigma_{\wp_5}\Omega_f : L] = 4 \) implies that \( g(x) \) is the minimal polynomial of \( \rho_k = r^5(\tau_k) \) over \( L \). The fact that the coefficients of \( g(x) \) are linear expressions in \( j_5^*(\tau_k) \) implies that

\[
L = K(j_5^*(\tau_k)) \text{ with } \langle \sigma_{\wp_5} \rangle = \text{Gal}(\Omega_f/L).
\]

It follows from Artin Reciprocity that a prime ideal \( p \) of \( K \) splits in \( L \) if and only if \( p \sim 1 \) or \( \wp_5 \) (mod \( f \)). In particular, \( l \sim \wp_5 \) (mod \( f \)), so that:

\[ I \text{ splits in the field } L. \]

If \( q \) is any prime divisor of \( l \) in \( L \), then \( j_5^*(\tau_k) \) (mod \( q \)) lies in the prime field \( \mathbb{F}_l \), so that the coefficients of \( g(x) \) (mod \( q \)) also lie in \( \mathbb{F}_l \).

If \( l \equiv 2, 3 \) (mod 5), then \( l^2 = (l) \) implies that \( l \) has order 4 in the ray class group \( C_{\wp_5} \) modulo \( \wp_5 \) in \( K \). If \( l \equiv \pm 1 \) (mod 5), then \( l \) has order 2 in \( C_{\wp_5} \). In the first case, a prime divisor \( q \) of \( l \) in \( L \) is inert in \( \Sigma_{\wp_5}\Omega_f \), so that \( g(x) \) is irreducible over the completion \( L_q \), and therefore factors mod \( q \) as a power of an irreducible polynomial over \( R_L/q \cong \mathbb{Z}/l\mathbb{Z} \). In the second case, \( q \) splits into two primes of relative (and absolute) degree 2 in \( \Sigma_{\wp_5}\Omega_f \), so that \( g(x) \) splits into two irreducible quadratics over \( L_q \). (See [14] pp. 288-289, 292.)

Now consider the polynomial \( G(x, j) \) from [21] Section 2.2:

\[
G(x, j) = (x^4 - 228x^3 + 494x^2 + 228x + 1)^3 - jx(1 - 11x - x^2)^5.
\]

Let \( j_1 = j(\tau_k)^{\sigma} \) and \( j_2 = j(\tau_k)^{\sigma_{\wp_5}} \) be two conjugate roots of \( H_{-d}(X) \) (\( d = 5l \) or \( 20l \)) over the field \( L \) (for some \( \sigma \in \text{Gal}(\Sigma_{\wp_5}\Omega_f/K) \)). Then \( \rho_k^\sigma \) has the
minimal polynomial \( q(x, \lambda^\sigma) \) over \( \Omega_f \) from the proof of Proposition 5.1. The identity (5.1) implies that \( \rho_k^\sigma = r^5(\tau_k)^\sigma \) is a root of \( G(x, j_1) = 0 \), so that \( q(x, \lambda^\sigma) | G(x, j_1) \) in \( \Omega_f[x] \). Applying the automorphism \( \sigma_{v_5} \) gives that \( q(x, \lambda^\sigma) | G(x, j_2) \), so that

\[
g(x)^\sigma = q(x, \lambda^\sigma)q(x, \lambda^\sigma) | G(x, j_1)G(x, j_2).
\]

Let \( p \) be a prime divisor of \( l \) in \( \Omega_f \), and \( q \) the prime below \( p \) in \( L \). If \( j_1 \not\equiv j_2 \) (mod \( p \)), and neither \( j_i \) is 0 or 1728 (mod \( p \)), then \( g(x)^\sigma \mod q \in \mathbb{F}_l[x] \) is a quartic dividing \( \tilde{H}_{5,l}(x) \) (mod \( q \)), since \( l \mid -d \) implies that the \( j \)-invariants \( j_i \) reduce to supersingular \( j \)-invariants, which must be roots of \( J_l(t) \) over \( \mathbb{F}_l \). For this we are using \([15, \text{Prop. 5.5}]\), according to which \( \tilde{H}_{5,l}(x) \) can be expressed as a product of factors \( G(x, j) \) over the roots \( j \) of \( J_l(t) \), times certain factors corresponding to \( j = 0 \) and \( j = 1728 \). (See the argument in Section 6 below concerning the polynomials \( G(x, j) \) and \( F(x, j) \).

If \( l \equiv 2, 3 \) (mod 5), then the irreducible factors of \( \tilde{H}_{5,l}(x) \) (mod \( l \)) are either \( x^2 + 1 \) or quartic. Now, \( g(x)^\sigma \in L_q[x] \) is irreducible, and can only have a quadratic factor modulo \( q \) if it is congruent to \((x^2 + 1)^2\). But \( \tilde{H}_{5,l}(x) \) has no repeated factors, so \( g(x)^\sigma \) must remain irreducible modulo \( q \). Hence, \( g(x)^\sigma \equiv x^4 + ax^3 + (11a + 2)x^2 - ax + 1 \) (mod \( q \)) is an irreducible factor of \( \tilde{H}_{5,l}(x) \) over \( \mathbb{F}_l \).

In particular, this holds if \( j_1 \) and \( j_2 \) are two distinct roots mod \( p \) of the factor \( X^2 + a_iX + b_i \) of \( H_{-d}(X) \) in Theorem 2.1. This is because this quadratic is irreducible (mod \( l \)), so it arises by reduction from roots \( j_i \) which are conjugate over \( L \), since \( L \) is the decomposition field of \( l \) in \( \Omega_f/K \) (\( l \) has order 2 in the class group mod \( f \) of \( K \)). It follows that the factor \((X^2 + a_iX + b_i)^2\) contributes at least one irreducible factor of the form \( g(x) \) to \( \tilde{H}_{5,l}(x) \) over \( \mathbb{F}_l \), when \( l \equiv 2, 3 \) (mod 5).

On the other hand, if \( l \equiv \pm 1 \) (mod 5), then the irreducible factors of \( \tilde{H}_{5,l}(x) \) are linear or quadratic. Since \( g(x)^\sigma \mod q \) divides \( \tilde{H}_{5,l}(x) \), then \( g(x)^\sigma \) splits either as a product of two distinct quadratics or four distinct linear polynomials (mod \( q \)), by the proof of Proposition 4.2. However, the latter cannot happen, by Hensel’s Lemma, because \( g(x)^\sigma \) is a product of irreducible quadratics over \( L_q \). Hence, \( g(x)^\sigma \) factors as a product of two irreducible quadratics (mod \( q \)). Now setting \( \lambda_1 = \lambda^\sigma \) and \( a = j_5^2(\tau_k)^\sigma = 22 + \lambda_1 + 5^3 \lambda_1^{-1} \) gives

\[
a^2 - 44a - 16 = \frac{(\lambda_1^2 - 125)^2}{\lambda_1^2}.
\]
It follows that, in the notation of Section 3, $-\Theta_1$ is not a square in $L$, because

$$\left(\lambda_1 - \frac{125}{\lambda_1}\right)^{\sigma_l} = \left(\lambda_1 - \frac{125}{\lambda_1}\right)^{\sigma_1} = -\left(\lambda_1 - \frac{125}{\lambda_1}\right). \quad (5.2)$$

Since $\sigma_l$ is the Frobenius automorphism for $l$ in $\Omega_f^1/K$, this equation implies that the quadratic residue symbol

$$\left(\frac{a^2 - 44a - 16}{q}\right) = -1 \text{ in } L. \quad (5.3)$$

The terms on either side of (5.2) are nonzero (mod $q$), because $a^2 - 44a - 16$ is a factor of the discriminant of $g(x)^9$; and we have shown above that $g(x)^9$ has no multiple factor (mod $q$). Now the proof of Proposition 4.2 shows that $g(x)^9 \equiv k_1(x)k_2(x)$ (mod $q$) factors into two polynomials of the form $k_i(x) = x^2 + r_ix + s_i$, where $r_i, s_i$ satisfy the relation of that proposition.

Hence, when $l \equiv \pm 1$ (mod 5), there are at least two distinct factors of $\hat{H}_{5,l}(x)$ of the form $k(x)$ arising from the factor $(X^2 + a_iX + b_i)^2$ in Theorem 2.1.

6 Completion of the proof

It remains to show that there are no other factors of the form $g(x)$ ($l \equiv 2, 3$ mod 5) or $k(x)$ ($l \equiv 1, 4$ mod 5) arising from a given factor $(X^2 + a_iX + b_i)^2$ of $H_{-d}(X)$ in the product of Theorem 2.1, for $d = 5l$ or $d = 20l$. The same arguments as in [18, Lemma 4.2] show that $H_{-5l}(X)$ and $H_{-20l}(X)$ are both squares (mod $l$), in the case $l \equiv 3$ (mod 4), so that the factor $(X^2 + a_iX + b_i)^2$ only divides one of these class equations (mod $l$). In this part of the proof we use the notation and remarks from [21, Section 2.2]. In particular, we use the linear fractional maps $S(x) = \zeta x, T(x) = \frac{-(1+\sqrt{5})x+2}{2x+1+\sqrt{5}}, U(x) = \frac{1}{x}, A(x) = \zeta^3\frac{(1+\zeta)x+1}{x-1-\zeta^4}$ from that paper ($\zeta$ a primitive 5-th root of unity). These are all elements of the icosahedral group $G_{60}$.

We shall use the fact that a factor of $\hat{H}_{5,l}(x)$ of the form $k(x) = x^2 + rx + s$, satisfying $r = \varepsilon^5(s-1)$, has (nonzero) roots $\alpha^5$ and $\beta^5$ satisfying the equation

$$\alpha^5 + \beta^5 = \varepsilon^5(1 - \alpha^5\beta^5). \quad (6.1)$$

Since there is at least one such factor, we can choose a fixed $\alpha$ satisfying this equation, which is unique up to multiplication by a power of $\zeta$. Since, moreover, $(\alpha, \beta)$ and $(-1/\alpha, -1/\beta)$ are also solutions of this equation, it is
clear that for $M$ in the group $G_{10} = \langle S, U \rangle$, the pairs $(M(\alpha), M(\beta))$ are solutions of (6.1) for which $M(\alpha)^5 = \alpha^5$ or $-1/\alpha^5$, the latter quantity being a root of the companion polynomial

$$\bar{k}(x) = \frac{1}{s}x^2k(-1/x) = x^2 - \frac{r}{s}x + \frac{1}{s}.$$  

Since the roots of $G(x, j) = 0$ have the form $M(\alpha)$, for a single root $\alpha$ and $M \in G_{60}$ (the icosahedral group, see [21]), a second factor of the form $g(x)$ or $k(x)$ (distinct from $\bar{k}(x)$) dividing $G(x, j)$ would yield a solution $(\alpha', \beta')$ of (6.1), where $\alpha' = M_1(\alpha)$ is not in the orbit $G_{10}\alpha$ and $\beta' = M_2(\beta) \notin G_{10}\beta$.

This suffices to prove what we need, since any factor of the form $g(x)$ or $k(x)$ has roots that are invariant under $\tau(x) = \frac{-x}{\varepsilon^5+1}$, and this map takes

$$j(x) = \frac{(x^4 + 12x^3 + 14x^2 - 12x + 1)^3}{x(1 - 11x - x^2)}$$

to

$$j(\tau(x)) = j_5(x) = \frac{(x^4 - 228x^3 + 494x^2 + 228x + 1)^3}{x(1 - 11x - x^2)^5}.$$  

Thus, any factor of the form $g(x)$ or $k(x)$ dividing

$$F(x, j) = (x^4 + 12x^3 + 14x^2 - 12x + 1)^3 - j(x^5(1 - 11x - x^2))$$

over $\mathbb{F}_1$ will also divide $G(x, j)$ (crucially, for the same value of $j$). See [21, Section 2.2].

The relations

$$AU = UTA$$
$$AT = UA$$
$$AT_2 = AUT = TA,$$

along with the fact that the elements $S^iA^j$ are coset representations for the left cosets of $\langle T, U \rangle$ in $G_{60}$, implies that the right cosets of $G_{10}$ in $G_{60}$ are $G_{10}T^iA^j$, for $i = 0, 1$ and $j = 0, 1, 2$. To prove that only one factor of the form $g(x)$, or two factors of the form $k(x)$, correspond to the factor $(X^2 + a_iX + b_i)^2$, we consider the equation

$$M_1(\alpha)^5 + M_2(\beta)^5 = \varepsilon^5(1 - M_1(\alpha)^5M_2(\beta)^5),$$

for pairs of elements of the form $M = T^iA^j$, where $i, j$ are not both 0. We compute the resultants

$$R_{M_1, M_2} = \text{Res}_y(x^5 + y^5 - \varepsilon^5(1 - x^5y^5),$$
$$c_1x + d_1)^5(c_2y + d_2)^5(M_1(x)^5 + M_2(y)^5 - \varepsilon^5(1 - M_1(x)^5M_2(y)^5))).$$
where $M_i(x) = \frac{a_i x + b_i}{c_i x + d_i}$. For example,

$$R_{T,T} = 5^{15}x(x^2 + x - 1)(x^2 + 1)(x^4 - x^3 + x^2 + x + 1)$$
$$\times (x^4 - 2x^3 + 2x + 1)(x^4 + x^3 + 3x^2 - x + 1)$$
$$\times (x^8 + 4x^7 + 10x^6 + 8x^5 + 12x^4 - 8x^3 + 10x^2 - 4x + 1)$$
$$\times (x^8 + 7x^7 + 15x^6 + 15x^5 + 16x^4 - 15x^3 + 15x^2 - 7x + 1)$$
$$\times (x^{16} + 2x^{15} - 4x^{14} - 12x^{13} + 25x^{12} - 18x^{11} + 68x^{10} - 112x^9$$
$$+ 13x^8 + 112x^7 + 68x^6 + 18x^5 + 25x^4 + 12x^3 - 4x^2 - 2x + 1)$$
$$= 5^{15}x(x^2 + x - 1)p_4(x)p_{11}(x)p_{16}(x)p_{19}(x)p_{64}(x)p_{99}(x)p_{84}(x),$$

where $p_d(x)$ is the polynomial defined in [20] (see Tables 1 and 2 in that paper) and $p_4(x) = x^2 + 1$. From [20], $p_d(x)$ divides

$$F_d(x^5) = x^{25h(-d)}(1 - 11x^5 - x^{10})^{h(-d)}H_{-d}(j(x^5)).$$

The factors $x(x^2 + x - 1)$ divide $x(x^{10} + 11x^5 - 1)$ and can be ignored. Thus the solution $(\alpha, \beta)$ arises from one of the factors $H_{-d}(X)^{4\epsilon_d}$, for $d \in \mathfrak{S}$. If $\epsilon_d = 1$, this shows that no solution of (6.1) of the form $(T(\alpha), T(\beta))$ can arise from the same factor $(X^2 + a_1X + b_1)^2$ in Theorem 2.1 that $(\alpha, \beta)$ does, since they correspond to non-conjugate $j$-invariants over $\mathbb{F}_l$. If $d = 84$ and $\epsilon_d = 0$, then factors of $H_{-84}(X) \pmod{l}$ can occur separately in the final product in Theorem 2.1. Considering the case $d = 84$ in the proof of Theorem 2.1 and the computations in Table 2, we must show that these factors, so far as they occur for $l \in \{389, 397, 401, 409\}$, each yield only one factor of the form $g(x)$ (or two of the form $k(x)$). (The prime 383 can be ignored for $d = 84$ in Table 2, since it does not divide a $N(Q(u,v))$ in the proof of Theorem 2.1.) For example, the unique factors of the form $g(x)$ coming from $H_{-84}(X)$ corresponding to these four primes are:

$$g_{389}(x) = (x^2 + 286x + 379)(x^2 + 262x + 350), \ r \equiv 151^5(s - 1) \mod 389;$$
$$g_{397}(x) = x^4 + 253x^3 + 6x^2 + 144x + 1;$$
$$g_{401}(x) = (x^2 + 376x + 362)(x^2 + 205x + 329), \ r \equiv 111^5(s - 1) \mod 401;$$
$$g_{409}(x) = (x^2 + 251x + 304)(x^2 + 240x + 74), \ r \equiv 129^5(s - 1) \mod 409.$$

Each of these polynomials divides the cofactor $f_{84}(x)$ of $Q_{84}(x)$ in $F_{84}(x)$, in the notation of Section 4. In particular, this shows that only one of the quadratic factors of $H_{-84}(X)$ over $\mathbb{F}_l$ can divide $K_{5l}(X)$ for these primes, since we know from Section 5 that each distinct quadratic factor would yield
a different \(g(x)\) or pair of polynomials \(k(x)\) dividing \(\tilde{H}_{5,t}(x)\). (Note: the only primes in the set \(S\) which are listed for \(d = 84\) in Table 2 are 167, 227, 311, and \(H_{-84}(X)\) is a product of linear factors modulo each of them.) This takes care of the pair \((M_1, M_2) = (T, T)\).

For the map \(A(x) = \zeta^{3(\frac{1+\zeta}{2})+1}\), the resultant \(R_{A,A}\) above is a product of polynomials in \(\mathbb{Q}(\zeta)[x]\) whose norm to \(\mathbb{Q}\) is:

\[
N_{\mathbb{Q}}(R_{A,A}) = 5^{60}x^4(x^4 - 3x^3 + 4x^2 - 2x + 1)(x^4 + 2x^3 + 4x^2 + 3x + 1)
\]

\[
\times q_4(x)q_{11}(x)q_{16}(x)q_{19}(x)q_{64}(x)q_{84}(x)q_{99}(x),
\]

where \(Q_d(x^5) = p_d(x)q_d(x)\), as in [20]. The factors \(q_d(x)\) also divide the polynomial \(F_d(x^5) = Q_d(x^5)f_d(x^5)\), so the same arguments apply as above. (The two quartic factors divide \(x^{10} + 11x^5 - 1\) and can be ignored, as above.)

Since \(N_Q(R_{A^2,A^2}) = N_Q(R_{T,A,T}) = N_Q(R_{T,A^2,T,A^2}) = N_Q(R_{A,A})\), we don’t get any new factors from these pairs, either. We still have to check the pairs \((M_1, M_2)\) with \(M_1 \neq M_2\). It suffices to check 10 pairs with \(M_1 \neq M_2\), since \((M_1, M_2)\) and \((M_2, M_1)\) yield the same solutions. We find that the resultants

\[R_{T,A} = R_{T,T} = R_{T,A^2}\]

coincide with \(R_{T,T}\), so these pairs don’t give anything new. Also,

\[R_{T,T,A^2} = 5^{15}e^{25}p_4(x)p_{24}(x)p_{36}(x)p_{51}(x)p_{91}(x)p_{96}(x),\]

\[N_Q(R_{A,T,A^2}) = 5^{60}q_4(x)q_{24}(x)q_{36}(x)q_{51}(x)q_{91}(x)q_{96}(x),\]

so that these two products account for the remaining integers \(d\) in the set \(\mathfrak{T}\). Furthermore, the resultant norms

\[N_Q(R_{A,T,A}) = N_Q(R_{A,A^2}) = N_Q(R_{A^2,T,A})\]

coincide with \(N_Q(R_{A,A})\) above, while the resultant norms

\[N_Q(R_{A^2,T,A^2}) = N_Q(R_{T,A,T,A^2})\]

coincide with \(N_Q(R_{A,T,A^2})\). This accounts for all 10 pairs.

Because the polynomials \(p_{96}(x), q_{96}(x)\) appear as factors of the above resultants, we also need to check that quadratic factors of \(H_{96}(X)\) over \(\mathbb{F}_l\) yield at most one factor of the form \(g(x)\) or two of the form \(k(x)\) for the primes \(l = 383, 397, 401, 421, 431, 449\) in Table 2, since \(\epsilon_{96} = 0\) for these
primes. (The primes 383, 431 can be ignored, because \(H_{-96}(X)\) splits completely for them, as it does for the primes 167, 239, 263, 359. The latter are the primes in \(S\) listed in Table 2 for \(d = 96\).) This is the same calculation that we performed above for \(d = 84\). We find:

\[
g_{397}(x) = x^4 + 30x^3 + 332x^2 + 367x + 1;
g_{401}(x) = (x^2 + 79x + 102)(x^2 + 184x + 287), \quad r \equiv 289^5(s - 1) \text{ mod } 401;\]
\[
g_{421}(x) = (x^2 + 316x + 351)(x^2 + 209x + 6), \quad r \equiv 110^5(s - 1) \text{ mod } 421;\]
\[
g_{449}(x) = (x^2 + 92x + 307)(x^2 + 437x + 332), \quad r \equiv 165^5(s - 1) \text{ mod } 449.
\]

This verifies what we need.

We must also account for possible simultaneous solutions of

\[
\alpha^5 + \beta^5 = \varepsilon^5(1 - \alpha^5\beta^5),
\]
\[
M_1(\alpha)^5 + M_2(\beta)^5 = \varepsilon^5(1 - M_1(\alpha)^5M_2(\beta)^5),
\]

and therefore must also consider the resultants

\[
\bar{R}_{M_1,M_2} = \text{Res}_y(x^5 + y^5 - \varepsilon^5(1 - x^5y^5),
\]
\[
(c_1x + d_1)^5(c_2y + d_2)^5(M_1(x)^5 + M_2(y)^5 - \varepsilon^5(1 - M_1(x)^5M_2(y)^5))).
\]

We check that this yields only the same solutions as before:

\[
\bar{R}_{T,T} = -5^{15}\varepsilon^{25}p_4(x)p_{24}(x)p_{36}(x)p_{51}(x)p_{91}(x)p_{96}(x),
\]
\[
N_{Q}(\bar{R}_{A,A}) = 5^{60}q_4(x)q_{24}(x)q_{36}(x)q_{51}(x)q_{91}(x)q_{96}(x),
\]
\[
N_{Q}(\bar{R}_{T,A,T}A) = N_{Q}(\bar{R}_{A^2,A^2}) = N_{Q}(\bar{R}_{T,A^2,T,A^2})
= N_{Q}(\bar{R}_{A,A});
\]
\[
\bar{R}_{T,A} = \bar{R}_{T,T} = \bar{R}_{T,A}; \quad \bar{R}_{T,T,A^2} = R_{T,T}, \quad \bar{R}_{T,A,T,A^2} = -R_{T,T};
\]
\[
N_{Q}(\bar{R}_{A,T,A}) = N_{Q}(\bar{R}_{A,A}) = N_{Q}(\bar{R}_{A^2,T,A}) = N_{Q}(\bar{R}_{A,A});
\]
\[
N_{Q}(\bar{R}_{A,T,A^2}) = N_{Q}(\bar{R}_{A^2,A}) = N_{Q}(\bar{R}_{T,A,T,A^2}) = N_{Q}(\bar{R}_{A,A}).
\]

When \(l \equiv \pm 1 \pmod{5}\) we would need to do the same calculation for the polynomials \(k(x) = x^2 + rx + s\) with \(r = \varepsilon^5(s - 1)\), and work with the conjugate equation

\[
\alpha^5 + \beta^5 = \varepsilon^5(1 - \alpha^5\beta^5). \tag{6.2}
\]

But these calculations follow from what we have already computed, since we can just apply the automorphism \(\sigma = (\zeta \to \zeta^2)\) to the maps in \(G_{60}\), and this map switches (6.1) and (6.2). This sends the group \(G_{10}\) to itself,
Table 5: Number $N$ of factors $g(x)$ or $k(x)$ modulo $l \equiv 1 \mod 12$.

| $l$ | $N$ | $h(-5l)$ | formula of Thm. 1.1 |
|-----|-----|----------|---------------------|
| 13  | 2   | 8        | 2                   |
| 37  | 4   | 16       | 4                   |
| 61  | 8   | 16       | 8                   |
| 73  | 5   | 20       | 5                   |
| 97  | 5   | 20       | 5                   |
| 109 | 16  | 32       | 16                  |
| 157 | 4   | 16       | 4                   |
| 181 | 12  | 24       | 12                  |
| 229 | 12  | 24       | 12                  |
| 241 | 20  | 40       | 20                  |
| 277 | 12  | 48       | 12                  |
| 313 | 7   | 28       | 7                   |
| 349 | 20  | 40       | 20                  |
| 373 | 12  | 48       | 12                  |

and replaces $T$ by $T^\sigma = T_2 = UT$ and $A$ by $A^\sigma = A^{-1}U = TA^2$. Since $T^\sigma A^\sigma = T_2 A^{-1}U = T_2 A^2 U = T_2 TA^2 = UA^2$, and $T_2 A^j = UTA^j$, we obtain exactly the same polynomials on taking norms as before.

These calculations show that each of the factors $(X^2 + a_iX + b_i)^2$ in Theorem 2.1 contributes exactly one factor of the form $g(x)$ (respectively $k_1(x)k_2(x)$) to the factorization of $\hat{H}_{5,l}(x)$ over $\mathbb{F}_l$, for $l \in S$ or $l > 379$.

This proves Theorem 1.1 for the primes $l \in S \cup \{l : l > 379\}$.

The counts of quartic or quadratic factors for the primes satisfying $7 \leq l \leq 379$ and $l \notin S$ are given in Tables 5-8. The number $N$ of such factors was counted by hand, after computing $\hat{H}_{5,l}(x)$ on Maple. In each case, $N$ agrees with the formula of Theorem 1.1. This shows that Theorem 1.1 holds for all primes $l > 5$.

7 The degree of $ss_p^{(5*)}(X)$

The aim of this section is to prove Nakaya’s conjecture [22, Conjecture 6] for $N = 5$, namely, that

$$
\deg(ss_p^{(5*)}(X)) = \frac{1}{4} \left( p - \left( \frac{-1}{p} \right) \right) + \frac{1}{2} \left( 1 - \left( \frac{-5}{p} \right) \right), \quad p > 5.
$$

41
Table 6: Number $N$ of factors $g(x)$ or $k(x)$ modulo $l \equiv 5 \mod 12$.

| $l$ | $N$ | $h(-5l)$ | formula of Thm. 1.1 |
|-----|-----|----------|---------------------|
| 17  | 1   | 4        | 1                   |
| 29  | 4   | 8        | 4                   |
| 41  | 4   | 8        | 4                   |
| 53  | 2   | 8        | 2                   |
| 89  | 4   | 8        | 4                   |
| 113 | 3   | 12       | 3                   |
| 137 | 3   | 12       | 3                   |
| 149 | 8   | 16       | 8                   |
| 197 | 6   | 24       | 6                   |
| 233 | 5   | 20       | 5                   |
| 257 | 3   | 12       | 3                   |
| 281 | 12  | 24       | 12                  |
| 317 | 6   | 24       | 6                   |
| 353 | 5   | 20       | 5                   |

Table 7: Number $N$ of factors $g(x)$ or $k(x)$ modulo $l \equiv 7 \mod 12$.

| $l$ | $N$ | $h(-5l)$ | $l \mod 8$ | formula of Thm. 1.1 |
|-----|-----|----------|------------|---------------------|
| 7   | 1   | 2        | 7          | 1                   |
| 19  | 5   | 8        | 3          | 5                   |
| 31  | 7   | 4        | 7          | 7                   |
| 43  | 6   | 14       | 3          | 6                   |
| 67  | 8   | 18       | 3          | 8                   |
| 79  | 13  | 8        | 7          | 13                  |
| 127 | 9   | 10       | 7          | 9                   |
| 139 | 21  | 24       | 3          | 21                  |
| 151 | 23  | 12       | 7          | 23                  |
| 163 | 14  | 30       | 3          | 14                  |
| 211 | 35  | 36       | 3          | 35                  |
| 283 | 16  | 34       | 3          | 16                  |
| 307 | 18  | 38       | 3          | 18                  |
| 331 | 43  | 44       | 3          | 43                  |
| 379 | 45  | 48       | 3          | 45                  |
Recall that $s_{sp}(5^*) (X)$ is determined as follows. Define the polynomial $R_5(X,Y)$ by

$$R_5(X,Y) = X^2 - X(Y^5 - 80Y^4 + 1890Y^3 - 12600Y^2 + 7776Y + 3456) + (Y^2 + 216Y + 144)^3.$$ 

Then

$$s_{sp}(5^*) (X) = \prod_{j^*_5} (X - j^*_5) \in \mathbb{F}_p[X],$$

where $j^*_5$ runs over the distinct roots of $R_5(j, j^*_5) \equiv 0$ in $\mathbb{F}_p$ for those values of $j$ which are supersingular in characteristic $p$, i.e., the roots of $s_{sp}(X) = 0$.

We use the parametrization

$$(j, j^*_5) = (X, Y) = \left( -\frac{(z^2 + 12z + 16)^3}{z + 11}, -\frac{z^2 + 4}{z + 11} \right)$$

of $R_5(X,Y) = 0$ given in [21] (see the proof of Theorem 6.1). Note first that

$$\text{disc}_z((z^2 + 12z + 16)^3 + j(z + 11)) = 3125j^4(j - 1728)^2,$$

so that there are exactly 6 values of $z$ for every supersingular value of $j$, except for $j = 0$ and $j = 1728$. For these values

$$j = 0 \quad \text{iff} \quad z^2 + 12z + 16 = 0,$$
$$j = 1728 \quad \text{iff} \quad (z^2 + 4)(z^2 + 18z + 76) = 0;$$

where the two quadratics have discriminants $2^4 \cdot 5$ and $-2^{14} \cdot 3^8 \cdot 5^3$, respectively. Thus exactly 2, respectively 4, values of $z$ correspond to $j = 0$.
and $j = 1728$ in characteristic $p > 5$. Since the number of supersingular $j$-invariants in characteristic $p$ is given by

$$n_p + r_p + s_p = \frac{p - e_p}{12} + \frac{1}{2} \left( 1 - \left( -\frac{3}{p} \right) \right) + \frac{1}{2} \left( 1 - \left( -\frac{1}{p} \right) \right),$$

where $e_p \in \{1, 5, 7, 11\}$ and $p \equiv e_p \pmod{12}$, there are exactly

$$\frac{p - e_p}{2} + \left( 1 - \left( -\frac{3}{p} \right) \right) + 2 \left( 1 - \left( -\frac{1}{p} \right) \right)$$

values of the parameter $z$ altogether. Using that $e_p = 6 - 2 \left( -\frac{3}{p} \right) - 3 \left( -\frac{1}{p} \right)$, we find

$$\frac{1}{2} \left( p - \left( -\frac{1}{p} \right) \right)$$

values of $z$ which correspond to supersingular $j$-invariants in $\mathbb{F}_{p^2}$.

Now note that

$$\text{disc}_z(z^2 + 4 + t(z + 11)) = t^2 - 44t - 16, \quad \text{disc}(t^2 - 44t - 16) = 2^4 \cdot 5^3.$$

It follows that exactly two values of $z$ correspond to a single value of $j_5^*$, except when $t = j_5^*$ is a root of the last quadratic. Since

$$\text{Res}_t(z^2 + 4 + t(z + 11), t^2 - 44t - 16) = (z^2 + 22z - 4)^2,$$

the roots of $z^2 + 22z - 4$ correspond 1–1 to the roots $j_5^*$ of $t^2 - 44t - 16 = 0$. On the other hand, the corresponding values of $j$ are supersingular exactly when they are roots of

$$\text{Res}_z((z^2 + 12z + 16)^3 + j(z + 11), z^2 + 22z - 4) = -5^3(j^2 - 1264000j - 681472000) = -5^3H_{-20}(j).$$

The roots of $H_{-20}(x)$ are supersingular in $\mathbb{F}_{p^2}$ if and only if $\left( -\frac{5}{p} \right) = -1$. Therefore, altogether we have

$$\frac{1}{4} \left( p - \left( -\frac{1}{p} \right) \right)$$

distinct values of $j_5^*$ corresponding to supersingular $j$-invariants, when $\left( -\frac{5}{p} \right) = +1$, and

$$\frac{1}{2} \left( \frac{1}{2} \left( p - \left( -\frac{1}{p} \right) \right) - 2 \right) + 2 = \frac{1}{4} \left( p - \left( -\frac{1}{p} \right) \right) + 1$$

44
Table 9: Degree and number of linear factors of $ss_p^{(5^*)}(X)$.

| $p$ | $\deg(ss_p^{(5^*)}(X))$ | $L^{(5^*)}(p)$ |
|-----|-------------------------|----------------|
| 7   | 2                       | 2              |
| 11  | 4                       | 4              |
| 13  | 4                       | 2              |
| 17  | 5                       | 1              |
| 19  | 6                       | 6              |
| 23  | 6                       | 2              |
| 29  | 7                       | 5              |
| 31  | 9                       | 7              |
| 37  | 10                      | 4              |
| 41  | 10                      | 6              |
| 43  | 11                      | 7              |
| 47  | 12                      | 2              |
| 53  | 14                      | 2              |
| 59  | 16                      | 10             |
| 61  | 15                      | 7              |
| 67  | 17                      | 9              |
| 71  | 19                      | 11             |
| 73  | 19                      | 5              |
| 79  | 21                      | 13             |
| 83  | 21                      | 5              |
| 89  | 22                      | 8              |
| 97  | 25                      | 5              |

distinct values of $j_5^*$ corresponding to supersingular $j$-invariants, when $\left(\frac{-5}{p}\right) = -1$. Hence, the degree of $ss_p^{(5^*)}(X)$ is given by

$$\frac{1}{4} \left(p - \left(\frac{-1}{p}\right)\right) + \frac{1}{2} \left(1 - \left(\frac{-5}{p}\right)\right).$$

This proves Nakaya’s Conjecture 6 for $N = 5$.

The table below gives the degree and number of linear factors of $ss_p^{(5^*)}(X)$, for primes between 7 and 97.
References

[1] George E. Andrews and Bruce C. Berndt, *Ramanujan’s Lost Notebook, Part I*, Springer, 2005.

[2] Bruce C. Berndt, *Number Theory in the Spirit of Ramanujan*, AMS Student Mathematical Library, vol. 34, 2006.

[3] H. Brandt, Idealtheorie in Quaternionenalgebren, Math. Annalen 99 (1928), 1-29.

[4] H. Brandt, Zur Zahlentheorie der quadratischen Formen, Jahresbericht der deutschen Mathematiker Vereinigung 47 (1937), 149-159.

[5] H. Brandt, Zur Zahlentheorie der Quaternionen, Jahresbericht der deutschen Mathematiker Vereinigung 53 (1943), 23-57.

[6] J. Brillhart and P. Morton, Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial, J. Number Theory 106 (2004), 79-111.

[7] B. Cho, Primes of the form $x^2 + ny^2$ with conditions $x \equiv 1 \mod N$ and $y \equiv 0 \mod N$, J. Number Theory 130 (2010), 852-861.

[8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Third edition, Grundlehren der Math. Wissenschaften 290, Springer, 1999.

[9] D. A. Cox, *Primes of the Form $x^2 + ny^2$; Fermat, Class Field Theory, and Complex Multiplication*, 2nd edition, John Wiley & Sons, 2013.

[10] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamb. 14 (1941), 197-272.

[11] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jahresber. Deutsch. Math. Verein. 54 (1944) 2441.

[12] M. Deuring, Die Klassenkörper der komplexen Multiplikation, Enzyklopaedie der math. Wissenschaften I2, 23 (1958), 1-60.
[13] W. Duke, Continued fractions and modular functions, Bull. Amer. Math. Soc. 42, No. 2 (2005), 137-162.

[14] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1963.

[15] P. Morton, Explicit identities for invariants of elliptic curves, J. Number Theory 120 (2006), 234-271.

[16] P. Morton, Legendre polynomials and complex multiplication, I, J. Number Theory 130 (2010), 1718-1731.

[17] P. Morton, The cubic Fermat equation and complex multiplication on the Deuring normal form, Ramanujan J. 25 (2011), 247-275.

[18] P. Morton, Explicit congruences for class equations, Functiones et Approximatio 51 (2014), 77-110.

[19] P. Morton, Product formulas for the 5-division points on the Tate normal form and the Rogers-Ramanujan continued fraction, [arXiv:1612.06268v4], J. of Number Theory 200 (2019), 380-396.

[20] P. Morton, Solutions of diophantine equations as periodic points of \( p \)-adic algebraic functions, II: The Rogers-Ramanujan continued fraction, [arXiv:1806.11079v4], New York J. of Math. 25 (2019), 1178-1213.

[21] P. Morton, On the Hasse invariants of the Tate normal forms \( E_5 \) and \( E_7 \), [arXiv:1906.12206v3], submitted.

[22] T. Nakaya, The number of linear factors of supersingular polynomials and sporadic simple groups, J. of Number Theory 204 (2019), 471-496.

[23] Y. Sakai, The Atkin orthogonal polynomials for the low-level Fricke groups and their application, International J. of Number Theory 7 (2011), 1637-1661.

[24] Y. Sakai, The Atkin orthogonal polynomials for the Fricke groups of levels 5 and 7, International J. of Number Theory 10 (2014), 2243-2255.

[25] R. Schertz, Complex Multiplication, New Mathematical Monographs 15, Cambridge University Press, 2010.
[26] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Springer, 2009.

Dept. of Mathematical Sciences, LD 270
Indiana University - Purdue University at Indianapolis (IUPUI)
Indianapolis, IN 46202
*e-mail: pmorton@iupui.edu*