Explicit congruences for class equations

by

Patrick Morton

PR # 11-02

This manuscript and other can be obtained via the
World Wide Web from www.math.iupui.edu

November 10, 2011
Explicit congruences for class equations*†

Patrick Morton

Dept. of Mathematical Sciences,
Indiana University – Purdue University at Indianapolis (IUPUI),
Indianapolis, IN 46202 – 3216, USA
e–mail : pmorton@math.iupui.edu

*Expanded version of a paper previously titled “Ogg’s theorem via explicit congruences for class equations”.
†MSC2000: 11G15, 14H52, 11R11
Abstract

Explicit congruences (mod $p$) are proved for the class equations corresponding to discriminants $D = -8p$, $-3p$, $-12p$ in the theory of complex multiplication, where $p$ is an odd prime. They are explicit in that they can be computed directly from a formula for the supersingular polynomial without first having to know the coefficients of the class equation in characteristic zero. These congruences are used to give a new proof of a theorem of Ogg, which states that there are exactly 15 primes $p$ for which all $j$-invariants of supersingular elliptic curves in characteristic $p$ lie in the prime field $\mathbb{F}_p$. The proof does not make use of any class number estimates. A corollary is that the supersingular polynomial $ss_p(t)$ splits into linear factors (mod $p$) if and only if the same is true of the class equations $H_{-8p}(t), H_{-3p}(t)$ (when $p \equiv 1 \pmod{4}$) and $H_{-12p}(t)$.

Keywords: class equation, supersingular polynomial, modular equation, class number, complex multiplication
1 Introduction.

Let \( ss_p(t) \) denote the supersingular polynomial in characteristic \( p \). This is the monic polynomial over \( \mathbb{F}_p \) whose roots are the distinct \( j \)-invariants of supersingular elliptic curves in characteristic \( p \). See [kaz], [brm], [m2]. The following explicit formulas for \( ss_p(t) \) are taken from [m2].

Let \( p \) be a prime > 3, \( n = (p - e_p)/12 \), with \( p \equiv e_p \pmod{12} \) and \( e_p \in \{1, 5, 7, 11\} \).

Also, define \( r \) and \( s \) by

\[
\begin{align*}
  r &= r_p = \frac{1}{2} \left( 1 - \left( -\frac{3}{p} \right) \right), \\
  s &= s_p = \frac{1}{2} \left( 1 - \left( -\frac{4}{p} \right) \right).
\end{align*}
\]

Then \( ss_p(t) \) is given by

\[
ss_p(t) = t^r(t - 1728)^sJ_p(t), \quad p > 3,
\]

with

\[
J_p(t) \equiv \sum_{k=0}^{n} \binom{2n+s}{2k+s} \binom{2n-2k}{n-k} (-432)^{n-k}(t - 1728)^k \pmod{p}.
\]

Note that \( s = 0 \) or 1 according as \( p \equiv 1 \) or 3 (mod 4). For \( p = 2 \) and 3, we have \( ss_2(t) = t \) and \( ss_3(t) = t \) (see [d1]). The polynomial \( ss_p(t) \) always factors into a product of linear and quadratic factors over \( \mathbb{F}_p \), by the well-known result of Deuring [d1] that the \( j \)-invariant of a supersingular elliptic curve always lies in \( \mathbb{F}_p^2 \). (For a simple proof see [si, p. 138] or [brm, Prop. 1].)

In this paper we shall use this formula for \( ss_p(t) \) to prove several explicit congruences for class equations corresponding to discriminants \(-8p, -3p, \) and \(-12p\). These congruences were used in [m3] and [m4] to study connections between the Legendre polynomials of degree \((p - e)/4 \) or \((p - e)/3 \) and complex multiplication in characteristic \( p \).

Recall that the class equation \( H_D(t) \) of discriminant \( D \) is the monic, irreducible polynomial in \( \mathbb{Z}[t] \) whose roots are the \( j \)-invariants of elliptic curves with complex multiplication by the quadratic order \( O_D \) of discriminant \( D \). (See [co], [d2], [si].) Congruences for the class equations \( H_{-p}(t) \) and \( H_{-4p}(t) \) with \( p \) an odd prime were first proved by Elkies [el]. These congruences were given explicit form in [brm], as follows. If \( p \equiv 3 \pmod{4} \), then from [brm, Prop. 11] we have:

\[
H_{-p}(t) \equiv (t - 1728)\{gcd(J_p(t), (t - 1728)^{(p-1)/2} - 1)\}^2 \pmod{p},
\]
\[ H_{-4p}(t) \equiv (t - 1728)\left\{ \gcd(tJ_p(t), (t - 1728)^{(p-1)/2} + 1) \right\}^2 \pmod{p}; \]

while if \( p \equiv 1 \pmod{4} \), we have

\[ H_{-4p}(t) \equiv \left\{ \gcd(tJ_p(t), (t - 1728)^{(p-1)/2} + 1) \right\}^2 \pmod{p}. \]

In particular, these polynomials always factor into a product of linear factors \((\text{mod } p)\), and every supersingular \( j \)-invariant in \( \mathbb{F}_p \) is a root of \( H_p(t) \) or \( H_{-4p}(t) \). It is clear that the class number \( h(-p) \) of \( \mathbb{Q}(\sqrt{-p}) \) can be determined from these congruences once the linear factors of \( J_p(t) \) \((\text{mod } p)\) are known.

Using some classical results on the modular equation (Invariantengleichung or transformation polynomial) \( \Phi_n(x, y) \) [co, pp. 229-231], [sch] we prove the following two analogous congruences. Recall that \( \Phi_n(x, y) \) is symmetric in \( x \) and \( y \) if \( n > 1 \). We write \( Q_n(u, v) \) for the de-symmetrized form of \( \Phi_n(x, y) \), i.e. \( Q_n(-x-y, xy) = \Phi_n(x, y) \).

The first congruence involves the class equation for the ring of integers \( O_{-8p} \) in the field \( \mathbb{Q}(\sqrt{-2p}) \).

**Theorem 1.1.** For \( p > 13 \), the class equation \( H_{-8p}(t) \) of discriminant \(-8p\) satisfies the congruence:

\[
H_{-8p}(t) \equiv (t - 1728)^{2\epsilon_1} (t - 8000)^{2\epsilon_2} (t + 3375)^{4\epsilon_3} (t^2 + 191025t - 121287375)^{4\epsilon_4} \times \prod_{i} (t^2 + at + b_i)^2 \pmod{p},
\]

where

\[
\begin{align*}
\epsilon_1 & = \frac{1}{2} \left(1 - \left(\frac{-4}{p}\right)\right), \\
\epsilon_2 & = \frac{1}{2} \left(1 - \left(\frac{-8}{p}\right)\right), \\
\epsilon_3 & = \frac{1}{2} \left(1 - \left(\frac{-7}{p}\right)\right), \\
\epsilon_4 & = \frac{1}{4} \left(1 - \left(\frac{-15}{p}\right)\right) \left(1 - \left(\frac{2}{p}\right)\right);
\end{align*}
\]

and the product is over all the irreducible quadratic factors \( t^2 + at + b \) of \( J_p(t) \) distinct from \((t^2 + 191025t - 121287375) = H_{-15}(t) \) which satisfy

\[-4Q_2(a, b) = (2b + 1485a - 41097375)^2 + (4a - 29025)(a - 191025)^2 \equiv 0 \pmod{p}.\]
The next congruence involves the class equations for the orders $O_{-3p}$ and $O_{-12p}$ in the field $\mathbb{Q}(\sqrt{-3p})$.

**Theorem 1.2.** Let $p$ be a prime $> 53$ and set $K_{3p}(t) = H_{-12p}(t)$ or $H_{-3p}(t)H_{-12p}(t)$ according as $p \equiv 3$ or 1 (mod 4). Then we have the congruence

$$K_{3p}(t) \equiv t^{2\delta_1}(t - 54000)^{2\delta_1}(t - 8000)^{4\delta_2}(t + 32768)^{4\delta_3} \times H_{-20}(t)^{4\delta_1}H_{-32}(t)^{4\delta_2}H_{-35}(t)^{4\delta_6} \prod_i(t^2 + c_it + d_i)^2 \pmod{p};$$

where

$$\delta_1 = \frac{1}{2}(1 - \left(\frac{-3}{p}\right)), \quad \delta_2 = \frac{1}{2}(1 - \left(\frac{-8}{p}\right)), \quad \delta_3 = \frac{1}{2}(1 - \left(\frac{-11}{p}\right)), \quad \delta_4 = \frac{1}{4}(1 - \left(\frac{-5}{p}\right))(1 - \left(\frac{5}{p}\right)), \quad \delta_5 = \frac{1}{4}(1 - \left(\frac{-2}{p}\right))(1 - \left(\frac{2}{p}\right)), \quad \delta_6 = \frac{1}{4}(1 - \left(\frac{-35}{p}\right))(1 - \left(\frac{5}{p}\right));$$

where $H_{-20}(t)$, $H_{-32}(t)$ and $H_{-35}(t)$ are the quadratic class equations

$$H_{-20}(t) = t^2 - 1264000t - 681472000, \quad H_{-32}(t) = t^2 - 52250000t + 12167000000, \quad H_{-35}(t) = t^2 + 117964800t - 134217728000,$$

and the product is over all the irreducible quadratic factors $t^2 + c_it + d_i$ of $J_p(t)$ distinct from $H_{-20}(t)$, $H_{-32}(t)$ and $H_{-35}(t)$ which satisfy $Q_3(c, d) \equiv 0$ (mod $p$), with

$$Q_3(c, d) = -2^{45}3^{359}c + 2^{30}3^{356}c^2 - 2^{15}3^{253}c^3 + c^4 - 2^{34}5^9 \cdot 23d$$

$$-2^{15}3^{353} \cdot 23 \cdot 3499cd - 2^3 \cdot 5 \cdot 23 \cdot 1163c^2d + 2^{45}3^{109}d^2 - 2^33^2 \cdot 31cd^2 - d^3.$$

The degree of the polynomial $K_{3p}(t)$ in this theorem is $a_ph(-3p)$, where $h(-3p)$ is the class number of the field $\mathbb{Q}(\sqrt{-3p})$, and $a_p$ is defined as
\[ a_p = \begin{cases} 
4, & \text{if } p \equiv 1 \pmod{8}, \\
2, & \text{if } p \equiv 5 \pmod{8}, \\
1, & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \tag{1.3} \]

The factor \( H_{-15}(t) \) in Theorem 1.1 and the factors \( H_{-20}(t), H_{-32}(t) \) and \( H_{-35}(t) \) in Theorem 1.2 are always irreducible (mod \( p \)) whenever they occur, because their discriminants are non-squares (mod \( p \)), a fact which is incorporated into the definition of \( \epsilon \) and the \( \delta \) (the largest prime dividing their discriminants is \( p = 13 \) for \( d = -15 \) resp. \( p = 29 \) for \( d = -20, -32, -35 \)). By Deuring’s theory of reduction [d1], the irreducible factors in Theorems 1.1 and 1.2 must be factors of \( ss_p(t) \). Thus, we have:

**Theorem 1.3.** The polynomial \( J_p(t) \) has irreducible quadratic factors over \( \mathbb{F}_p \) whenever \( h(2p) > 8 \) or \( a_p h(-3p) > 12 \).

This line of reasoning can be extended to prove the following result of Ogg [o1], without using any class number estimates. (See also [o2].)

**Ogg’s Theorem.** The only primes \( p \) for which the supersingular polynomial \( ss_p(t) \) splits into a product of linear factors over \( \mathbb{F}_p \) are the primes satisfying \( 2 \leq p \leq 31 \) or \( p \in \{41, 47, 59, 71\} \).

We note that this theorem was apparently known to H. Brandt in 1943. He mentions these same 15 primes in [bra3, p. 40] in connection with ideal classes in maximal orders of the quaternion algebra \( D_p \) over \( \mathbb{Q} \) which is only ramified at the infinite prime \( p_\infty \) and a given rational prime \( p \) (whose Grundzahl is therefore \( -p \)). In Brandt’s terminology the above theorem is equivalent to the following statement about quaternary quadratic forms over \( \mathbb{Z} \) (cf. [bra1, pp.8-11], [bra2, p. 154], [bra3, pp. 29, 36-37], [d1, p. 265]):

**The only primes \( p \), for which every positive definite quaternary Stammform \( F \) of discriminant \( p^2 \) represents \( p \) over \( \mathbb{Z} \), are the primes listed in Ogg’s theorem.**

The quaternary quadratic forms which are Stammformen are the norm forms of maximal orders and their ideals in quaternion algebras (see [bra1, p. 11], [bra3, p. 29]). Brandt’s assertion in [bra3] suggests that he had a proof of the italicized assertion, but I have been unable to locate a proof by him in the literature.

The following condition is necessary and sufficient for a prime \( p > 3 \) to be one of the primes listed in Ogg’s theorem. A result of Deuring (see [brm, p.97]) implies that \( ss_p(t) \) has exactly \( b_p h(-p) \) distinct linear factors (mod \( p \)), where
\[ b_p = 1/2, 2 \text{ or } 1 \text{ according as } p \equiv 1 \pmod{4}, 3 \pmod{8} \text{ or } 7 \pmod{8}. \]

Since \( ss_p(t) \) has distinct roots over \( \mathbb{F}_p \), a prime \( p > 3 \) is one of the primes specified by Ogg’s theorem if and only if the degree of \( ss_p(t) \) satisfies

\[
\frac{p - e_p}{12} + r_p + s_p = b_p h(-p). \tag{1.4}
\]

By equating degrees of the linear factors in Theorems 1.1 and 1.2, we have the following necessary conditions for \( p \) to be one of Ogg’s primes:

\[
h(-2p) = 4 - (-4/p) - (-8/p) - 2(-7/p),
\]

\[
a_p h(-3p) = 6 - 2(-3/p) - 2(-8/p) - 2(-11/p). \tag{1.5}
\]

These are very stringent conditions on \( p \). In Section 4, we use the structure of the 2-classgroup in \( \mathbb{Q}(\sqrt{-2p}) \) and \( \mathbb{Q}(\sqrt{-3p}) \) to show that any prime \( p > 53 \) satisfying (1.5) must be one of the primes listed in Ogg’s theorem, i.e. \( p = 59 \) or 71. It turns out that (1.5) is actually necessary and sufficient for (1.4) to hold, when \( p \geq 13 \). This gives the following corollary of our proof. (See Theorem 4.1.)

**Theorem 1.4.** The supersingular polynomial \( ss_p(t) \) is a product of linear polynomials over \( \mathbb{F}_p \) if and only if the polynomials \( H_{-8p}(t), H_{-12p}(t) \) and \( H_{-3p}(t) \) (when \( p \equiv 1 \pmod{4} \)) are products of linear polynomials over \( \mathbb{F}_p \).

We remark in connection with Theorem 1.2 that it is possible to prove separate congruences for \( H_{-3p}(t) \) and \( H_{-12p}(t) \pmod{p} \), when \( p \equiv 1 \pmod{4} \).

**Theorem 1.5.** If \( p > 53 \) is a prime with \( p \equiv 1 \pmod{4} \), then we have the following congruences (mod \( p \)):

\[
H_{-3p}(t) \equiv (t - 54000)^{2\delta_1}(t - 8000)^{4\delta_2}H_{-20}(t)^{2\delta_3}H_{-32}(t)^{2\delta_4}\prod_i(t^2 + c_i t + d_i)^2,
\]

\[
H_{-12p}(t) \equiv t^{2\delta_1}(t + 32768)^{4\delta_3}H_{-20}(t)^{2\delta_4}H_{-32}(t)^{2\delta_5}H_{-35}(t)^{4\delta_6}\prod_j'(t^2 + c_j t + d_j)^2,
\]

with the same notation as in Theorem 1.2, where the products \( \Pi \) and \( \Pi' \) in these congruences have no factors in common.
The proof of the congruences in Theorem 1.5 involves an application of the basic theory of complex multiplication, along with some elementary Galois theory. (See Section 5.) In this proof we also make use of a number of the results of [m4], some of which depend in turn on Sections 2-3 of this paper. As in [m4, p. 274], an important role is played by points on the Fermat curve

\[ \text{Fer}_3 : \quad 27X^3 + 27Y^3 = X^3Y^3 \]

which are defined over certain Hilbert class fields. These points come into play in exhibiting elliptic curves in Deuring normal form with the properties necessary for proving the above congruences.

In the papers [m3] and [m4] we show how the explicit congruences in Theorems 1.1 and 1.2 lead to a connection between the class numbers \( h(-2p) \) and \( h(-3p) \) and the factorization (mod \( p \)) of the Legendre polynomials \( P_{(p-e)/4}(x) \) and \( P_{(p-e)/3}(x) \). This connection was the original motivation for proving these congruences.

In an appendix we give an algorithm for computing the modular equation \( \Phi_n(x, y) \) over an arbitrary field \( k \), which can be used to compute explicit congruences for \( H_{-4dp}(t) \) or \( H_{-dp}(t)H_{-4dp}(t) \) (mod \( p \)), where \( d \) is square-free and relatively prime to \( 2p \). (See Section 2 and the Appendix.)

### 2 Properties of the transformation polynomial.

We begin by proving several important results for the modular equation \( \Phi_n(x, y) \) of order \( n \).

The polynomial \( \Phi_n(x, y) \) is the polynomial whose solutions \( (x, y) \), in characteristic 0 or \( p \) not dividing \( n \), are pairs \((j_0, j_1)\) of \( j \)-invariants satisfying the condition: an elliptic function field \( K_0 \) with \( j \)-invariant \( j_0 \) has an elliptic subfield \( K_1 \) with \( j \)-invariant \( j_1 \) for which \( K_0/K_1 \) is cyclic of degree \( n \). (See [d1], [co], [sch].)

We follow Deuring’s paper [d1] in using the notation \( \Phi_n(x, y) \) also in the case that the characteristic \( p \) does divide \( n \), for the reduction of the characteristic 0 transformation polynomial of order \( n \) modulo \( p \). From [d1, p. 241] we take the well-known formula

\[
\Phi_p(t, j) \equiv (t^p - j)(t - j^p) \pmod{p}.
\] (2.1)
We will also need the fact that if \((m, n) = 1\), then
\[
\Phi_{mn}(t, j) = \prod_{h=1}^{\psi(n)} \Phi_m(t, j_h),
\]  
(2.2)
where the last product is over the \(\psi(n)\) values \(j_h\) for which
\[
\Phi_n(t, j) = \prod_{h=1}^{\psi(n)} (t - j_h).
\]  
(2.3)

We use these facts to prove

**Lemma 2.1.** If \(d > 1\) is a positive integer not divisible by the prime \(p\), then we have
\[
\Phi_{dp}(t, t) \equiv \Phi_d(t^p, t)^2 \pmod{p}.
\]  
(2.4)

**Proof.** From (2.1)-(2.3) we have in characteristic \(p\) that
\[
\Phi_{dp}(t, j) = \prod_{h=1}^{\psi(p)} \Phi_d(t, j_h) = \prod_{h=1}^{p} \Phi_d(t, j_1^h) \cdot \Phi_d(t, j_2^p) = \Phi_d(t^p, j) \Phi_d(t, j^p),
\]
which is a generalization of (2.1). Putting \(j = t\) and using \(\Phi_d(x, y) = \Phi_d(y, x)\) gives (2.4). \(\square\)

We let \(H_D(x)\) or \(H_O(x)\) denote the class equation of the quadratic order \(O = O_D\) whose discriminant is \(D\). In what follows we will be considering the factorization of \(H_{-dp}(x)\) or \(H_{-4dp}(x)\) mod \(p\), where \(p\) is a prime \(> 3\) and \(d = 2\) or \(3\). In the following two lemmas we will take \(d\) to be any positive, square-free integer not divisible by \(p\). We have from [co, p.291] and [d1, p.251] that

\[
\Phi_{dp}(t, t) = \pm H_{-4dp}(t) \cdot \prod_{O} H_O(t)^{r(O, dp)}, \quad \text{if } dp \equiv 1, 2 \pmod{4},
\]
\[
\Phi_{dp}(t, t) = \pm H_{-dp}(t) H_{-4dp}(t) \cdot \prod_{O} H_O(t)^{r(O, dp)}, \quad \text{if } dp \equiv 3 \pmod{4},
\]  
(2.5)
where
\[ r(O, m) = \left| \{ \alpha \in O : \alpha \text{ is primitive, } N(\alpha) = m \} / O^* \right|, \]

and \( r(O, dp) = 0 \) or \( r(O, dp) \geq 2 \) for all the terms occurring in the above products.

We call an irreducible factor of \( \Phi_{dp}(t, t) \pmod{p} \) supersingular if its roots are supersingular \( j \)-invariants in characteristic \( p \).

**Lemma 2.2.** Assume \( d > 1 \) is a square-free, positive integer.

a) If \( p > 4d \), then in (2.5), we have \( \gcd(H_{-dp}(t), H_{O}(t)) = \gcd(H_{-4dp}(t), H_{O}(t)) = 1 \pmod{p} \) for all the orders \( O \) occurring in the product.

b) If \( p > 4d \), all the supersingular factors of \( \Phi_{dp}(t, t) \pmod{p} \) occur as factors of \( H_{-dp}(t) \) or \( H_{-4dp}(t) \pmod{p} \).

**Proof.** Suppose that \( O = O_{-D} \) is an order for which \( r(O, dp) > 1 \) in (2.5). Then
\[ dp \text{ or } 4dp = x^2 + Dy^2, \]
with \( (x, y) = 1 \).

If \( p | D \), then \( p | x \) and we have
\[ d \text{ or } 4d = px_1^2 + \frac{D}{p} y^2. \]

If \( p > 4d \), then \( x_1 \) must be 0, so that \( d = D/p \cdot y^2 \) or \( 4d = D/p \cdot y^2 \). Since \( d \) is square-free, \( y = 1 \) or \( y = 2 \) (in the second case only), so that \( d = D/p \) or \( 4d = D/p \).

Hence, \( D = dp \) or \( D = 4dp \), which is impossible because the orders \( O \) in the product in (2.5) have discriminants different from \(-dp\) or \(-4dp\).

Therefore, \( p \) divides none of the discriminants in the products in (2.5), under the assumption that \( p > 4d \). Hence, \( -D \equiv x^2/y^2 \pmod{p} \), so that the Legendre symbol \((-D/p) = +1\). In this case none of the factors of \( H_{O}(t) = H_{-D}(t) \pmod{p} \) can have supersingular \( j \)-invariants as roots, by Deuring’s theory [d1]. On the other hand, all of the factors of \( H_{-dp}(t) \) and \( H_{-4dp}(t) \pmod{p} \) correspond to supersingular \( j \)-invariants, since \( p \) divides the discriminant. This proves both parts of Lemma 2.2.

\( \square \)

Combining Lemmas 2.1 and 2.2 gives

**Lemma 2.3.** Assume \( d > 1 \) is a square-free, positive integer and \( p > 4d \).

a) The irreducible factors of \( \gcd(ss_p(t), \Phi_d(t^p, t)) \pmod{p} \) are exactly the irreducible factors of \( H_{-4dp}(t) \) or \( H_{-dp}(t)H_{-4dp}(t) \pmod{p} \).
b) The multiplicity of an irreducible factor of $H_{-4dp}(t)$ or $H_{-dp}(t)H_{-4dp}(t)$ (mod $p$) is the same as its multiplicity in $\Phi_d(t^p, t)^2$ (mod $p$).

We note the following expressions for $\Phi_2(t, j)$ and $\Phi_3(t, j)$ in characteristic 0. See [fr, p. 321] [co, p. 234], and the Appendix of this paper, where we give a straightforward algorithm for computing $\Phi_n(t, j)$ for small values of $n$. (See also [d1, p. 247] for the computation of $\Phi_2$, but beware of misprints in the coefficients of $t^j$ and $(t + j)$ in the final answer [d1,(57)]. The powers of 3 in those coefficients should be $3^4$ and $3^7$, respectively.) We have:

$$\Phi_2(t, j) = t^3 - t^2 \cdot (j^2 - 1488j + 162000) + t \cdot (1488j^2 + 40773375j + 8748000000) + j^3 - 162000j^2 + 8748000000j - 157464000000000,$$

$$\Phi_2(t, t) = -(t - 1728)(t - 8000)(t + 3375)^2,$$

$$\Delta_2(j) = \text{disc}_t(\Phi_2(t, j)) = 4(j - 1728)j^2(j + 3375)^2(j^2 + 191025j - 121287375)^2.$$

Also,

$$\Phi_3(t, j) = t \cdot (t + 2^{15} \cdot 3 \cdot 5^3)^3 + j \cdot (j + 2^{15} \cdot 3 \cdot 5^3)^3 - t^3j^3 + 2^3 \cdot 3^2 \cdot 31 \cdot t^2j^2(t + j) - 2^2 \cdot 3^3 \cdot 9907 \cdot tj(t^2 + j^2) + 2 \cdot 3^4 \cdot 13 \cdot 193 \cdot 6367 \cdot t^2j^2 + 2^{16} \cdot 3^5 \cdot 5^3 \cdot 17 \cdot 263 \cdot tj(t + j) - 2^{31} \cdot 5^6 \cdot 22973 \cdot tj,$$

$$\Phi_3(t, t) = -(t - 54000)(t + 32768)^2(t - 8000)^2,$$

$$\Delta_3(j) = \text{disc}_t(\Phi_3(t, j)) = -27j^2(j - 1728)^2(j - 8000)^2(j + 32768)^2,$$

$$(j^2 - 1264000j - 681472000)^2(j^2 - 52250000j + 12167000000)^2.$$

In order to identify the individual factors in these formulae, we make use of a beautiful theorem appearing in Fricke’s *Lehrbuch der Algebra, III* [fr, p. 338]:

**Theorem.** Over the rational field $\mathbb{Q}$, the discriminant $\Delta_0(j)$ of $\Phi_p(t, j)$, for a prime $p$, is divisible by the factors $j = H_{-3}(j)$, $j - 1728 = H_{-4}(j)$, and $H_D(j)$, for every negative integer $D$ satisfying:

$$(i) -4p^2 < D < -4,$$
(ii) $p$ does not divide $D$,
(iii) $4p^2 = a^2 - Db^2$, with integers $a$ and $b \neq 0$ not divisible by $p$,
(iv) $D$ is a quadratic discriminant;
and this exhausts all possible irreducible factors of the discriminant $\Delta_p(j)$.

It follows easily from this theorem, for example, that the irreducible factors of $\Delta_2(j)$ are

$$j, j - 1728, H_{-7}(j) = j + 3375, H_{-15}(j) = j^2 + 191025j - 121287375,$$

since -7 and -15 are the only odd discriminants between -4 and -16 for which the equation in (iii) has a solution, and since $h(-7) = 1$.

For $\Phi_3(t, j)$, there are 5 possible discriminants between -4 and -36 for which condition (iii) holds, namely:

$$D = -8, -11, -20, -32, -35,$$

with corresponding class numbers 1, 1, 2, 2, 2; and 5 irreducible factors of $\Delta_3(j)$ other than $j$ or $j - 1728$. For the formulas

$$H_{-8}(j) = j - 8000, H_{-11}(j) = j + 32768.$$  \hspace{1cm} (2.6)

we refer to [fr, pp. 394, 396] or [co, p. 261]. We also claim that:

$$H_{-20}(j) = j^2 - 1264000j - 681472000,$$
$$H_{-32}(j) = j^2 - 52250000j + 12167000000,$$  \hspace{1cm} (2.7)
$$H_{-35}(j) = j^2 + 117964800j - 134217728000.$$

This can be seen as follows. The second quadratic splits into the product $(j + 52)(j + 63) \pmod{73}$, while the first and third quadratics are irreducible (mod 73). Since 73 = $(1 + 6\sqrt{-2})(1 - 6\sqrt{-2})$ splits into primes which lie in the principal ring class (mod 2) in $\Omega = \mathbb{Q}(\sqrt{-2})$, 73 splits completely in the ring classfield (mod 2) over $\Omega$. This implies that the second quadratic must be $H_{-32}(j)$. The first and third quadratics cannot be distinguished by the splitting of an appropriate prime,
since they both have roots belonging to $\mathbb{Q}(\sqrt{5})$. However, by (2.5), with $d = 1$ and $p = 5$, it is clear that $H_{-20}(t)$ divides $\Phi_5(t, t)$ while $H_{-35}(t)$ does not. Example 3 of the appendix may be used to verify that the first quadratic in (2.7) does indeed divide $\Phi_5(j, j)$ and so is identical with $H_{-20}(j)$. These facts may also be verified by expanding Fricke’s expressions for the roots of $H_{-20}(j)$ on p. 399 and for the roots of $H_{-32}(j)$ on p. 421 of [fr].

We also note that $H_{-12}(j) = j = 54000$ from [fr, p.395] or [co, p.291].

**Proposition 2.4.** If $p$ is a prime $> 3$, the multiplicity of an irreducible factor of $\Phi_2(t^p, t)$ (mod $p$) is at most 3. If $p > 13$, this multiplicity is at most 2.

**Proof.** We set $F(t, j) = \Phi_2(t, j)$, and write $F_i(t, j)$ for the partial derivative of $F(t, j)$ with respect to the $i$-th variable ($t$ or $j$). We consider the discriminant $\Delta_2(j)$ of $F(t, j)$, as above. We know that in characteristic $p$,

$$
\Delta_2(j) = A(t, j)F_1(t, j) + B(t, j)F(t, j),
$$

for some polynomials $A(t, j)$ and $B(t, j)$ in $\mathbb{F}_p[t, j]$. Putting $t^p$ for $j$ gives

$$
\Delta_2(t^p) = A(t, t^p)F_1(t, t^p) + B(t, t^p)F(t, t^p).
$$

Furthermore,

$$
\frac{d}{dt}(F(t, t^p)) = F_1(t, t^p) + p \cdot t^{p-1}F_2(t, t^p) = F_1(t, t^p).
$$

Hence, common factors of $F(t, t^p)$ and its derivative must divide $\Delta_2(t^p)$. Now,

$$
F_1(t, j) = 3t^2 - 2t(j^2 - 1488j + 162000) + 1488j^2 + 40773375j + 8748000000,
$$

so that

$$
\frac{d}{dt}(F(t, t^p)) = 3t^2 - 2t(t^{2p} - 1488t^p + 162000) + 1488t^{2p} + 40773375t^p + 8748000000,
$$

$$
= -2t^{2p+1} + 1488t^{2p} + 2976t^{p+1} + 40773375t^p + 3t^2 - 324000t + 8748000000.
$$

It follows that
\[
\frac{d^2}{dt^2} (F(t, t^p)) = -2t^{2p} + 2976t^p + 6t - 324000,
\]
and \( \frac{d^3}{dt^3} (F(t, t^p)) = 6 \). Therefore, no root of \( F(t, t^p) \) has multiplicity greater than 3.

To prove the second assertion of the lemma, we evaluate \( s(t) = (F(t, t^p))'' \) at the roots of \( \Delta_2(t) \). For the roots 0, 1728, and \(-3375\) we have

\[
s(0) = -2^5 \cdot 3^4 \cdot 5^3, \quad s(1728) = -2^5 \cdot 3^6 \cdot 7^2, \quad s(-3375) = -2^2 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 13.
\]

It remains to evaluate the second derivative \( s(t) \) at the roots of the factor \( H_{-15}(t) = t^2 + 191025t - 121287375 \), which are

\[
t = \frac{-191025 \pm 85995\sqrt{5}}{2} = \alpha_\pm.
\]

If these roots lie in the prime field \( \mathbb{F}_p \), we have

\[
s(\alpha_\pm) = 2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13 \cdot (-71745 \pm 32086\sqrt{5}),
\]

where the norm of the last factor \((-71745 \pm 32086\sqrt{5})\) is \(-5 \cdot 42391\). On the other hand, if the roots \( \alpha_\pm \) are quadratic over the prime field, then we have

\[
s(\alpha_\pm) = 2 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot (-4783 \pm 2139\sqrt{5}),
\]

where the norm of the factor \((-4783 \pm 2139\sqrt{5})\) is \(2^2 \cdot 11^2\). Thus, the only prime for which \( s(\alpha_\pm) \) could possibly be 0 \((\text{mod } p)\), for \( p \geq 17 \), is \( p = 42391 \). Now we note that

\[
H_{-15}(t) \equiv (t + 4410)(t + 17051) \pmod{42391},
\]

but that neither \(-4410\) nor \(-17051\) can be roots of \( F(t, t^p) = \Phi_2(t, t^p) \pmod{42391} \), by the above factorization of \( \Phi_2(t, t) \). Hence, \( (\Phi_2(t, t^p))'' \) is never 0 \((\text{mod } p)\), for a multiple root of \( \Phi_2(t, t^p) = \Phi_2(t^p, t) \). This completes the proof of the proposition. \(\square\)
Corollary 2.5. For a prime \( p > 3 \), the multiplicity of an irreducible factor of \( H_{-8p}(t) \) (mod \( p \)) is even and never greater than 6. If \( p \neq 13 \), this multiplicity is never greater than 4.

**Proof.** Combine Proposition 2.4 with Lemma 2.3 in the case \( d = 2 \). This proves the claim as long as \( p > 13 \). For \( p = 5, 7 \) and 11 the claim follows from

- \( H_{40}(t) \equiv t^2 \) (mod 5);
- \( H_{56}(t) \equiv (t + 1)^4 \) (mod 7);
- \( H_{88}(t) \equiv (t + 10)^2 \) (mod 11).

We also note in the case \( p = 13 \) that

\( H_{104}(t) \equiv (t + 8)^6 \) (mod 13).

(See [fr, pp. 408] for \( H_{40}(t) \).) For \( p = 5, 7, 13 \) these congruences follow from the fact that there is only one supersingular \( j \)-invariant, so \( H_{-8p}(t) \) must be a pure power (mod \( p \)), and the exact power is determined by the class number. For \( p = 11 \) the congruence follows from Lemma 2.3 and the fact that \((t + 10)\) divides \( \Phi_2(t^{11}, t) \) (mod 11), but \( t \) (the other factor of \( ss_{11}(t) \)) does not. \( \Box \)

**Corollary 2.6.** For \( p > 3 \) the only linear factor of \( \Phi_2(t^p, t) \) (mod \( p \)) which is a multiple factor is \( t + 3375 \).

**Proof.** From the formula for \( \Phi_2(t, t) \) we know that the only linear factors of \( \Phi_2(t^p, t) \) (mod \( p \)) are \((t - 1728), (t - 8000)\), and \((t + 3375)\). By the computations in the proof of Proposition 2.4, we have for \( t \in \mathbb{F}_p \) that

\[
\frac{d}{dt}(F(t, t^p)) = -2t^3 + 4467t^2 + 40449375t + 8748000000 \\
= -(t + 3375)(2t^2 - 11217t - 2592000) \\
= -(t + 3375)f(t).
\]

Hence \((t + 3375)\) is certainly a multiple factor of \( \Phi_2(t^p, t) \) (mod \( p \)). On the other hand, \( f(1728) = -2^6 \cdot 3^6 \cdot 7^3 \) and \( f(8000) = 2^6 \cdot 5^3 \cdot 7^3 \cdot 13 \) imply that 1728 and 8000 can be multiple roots of \( \Phi_2(t^p, t) \) (mod \( p \)) only for \( p = 5, 7, 13 \). Since \( 1728 \equiv -3375 \) (mod 7) and \( 8000 \equiv -3375 \) (mod \( 5 \cdot 7 \cdot 13 \)), the assertion of the corollary holds. \( \Box \)

We now prove a similar result for \( \Phi_3(t, j) \):

15
Proposition 2.7. If $p$ is a prime $> 3$, the multiplicity of an irreducible factor of $\Phi_3(t^p, t) \pmod{p}$ is at most 4. If $p > 53$, this multiplicity is at most 2.

Proof. Exactly as in the proof of Proposition 2.4 (but with slightly different notation), multiple factors of $F(t) = \Phi_3(t^p, t) \pmod{p}$ must divide $\Delta_3(t) \pmod{p}$, and can therefore only be one of the linear factors $t, t - 1728$, one of the linear factors in (2.6), or must divide one of the quadratic factors in (2.7).

Since $\Phi_3(x, j)$ is a symmetric polynomial in $x$ and $j$, we may write $\Phi_3(x, j) = Q(u, v)$, where $u = -(x + j)$ and $v = xj$. Write $Q_i(u, v)$ for the partial derivative of $Q$ with respect to the $i$-th variable, $i = 1, 2$, and let $F(t) = \Phi_3(t^p, t) = Q(-t^p - t, t^p+1)$. In characteristic $p$ we have

$$F'(t) = -Q_1(-t^p - t, t^p+1) + t^pQ_2(-t^p - t, t^p+1),$$

and therefore

$$F''(t) = Q_{11}(-t^p - t, t^p+1) - 2t^pQ_{12}(-t^p - t, t^p+1) + t^2pQ_{22}(-t^p - t, t^p+1).$$

If $t$ is a multiple root of $F(t)$ over $\mathbb{F}_p$, then because $t$ is at most quadratic over $\mathbb{F}_p$, we have $t^{2p} = -ut^p - v$, with $u = -t - t^p, v = t^{p+1}$. Hence, the expression for $F''(t)$ becomes

$$F''(t) = Q_{11} - vQ_{22} - t^p(2Q_{12} + uQ_{22}). \quad (2.8)$$

Furthermore, an explicit expression for $Q(u, v)$ is

$$Q(u, v) = u^4 - 36864000u^3 + 4529848320000000u^2 - 185542587187200000000u$$
$$-1069960u^2v - 2232uv^2 - 890112384000uv$$
$$-v^3 + 2590058000v^2 - 7717519360000000v$$
$$= u^4 - 2^{15} \cdot 3^2 \cdot 5^3 \cdot u^3 + 2^{30} \cdot 3^3 \cdot 5^6 \cdot u^2 - 2^{45} \cdot 3^3 \cdot 5^9 \cdot u$$
$$-2^3 \cdot 5 \cdot 23 \cdot 1163 \cdot u^2v - 2^3 \cdot 3^2 \cdot 31 \cdot uv^2 - 2^{15} \cdot 3^3 \cdot 5^3 \cdot 23 \cdot 3499 \cdot uv$$
$$-v^3 + 2^4 \cdot 5^3 \cdot 109^3 \cdot v^2 - 2^{34} \cdot 5^9 \cdot 23 \cdot v.$$ 

This yields the following partial derivatives:

$$Q_{11}(u, v) = 2^2 \cdot 3 \cdot u^2 - 2^{16} \cdot 3^3 \cdot 5^3 \cdot u + 2^{31} \cdot 3^3 \cdot 5^6 - 2^4 \cdot 5 \cdot 23 \cdot 1163 \cdot v,$$
\[ Q_{12}(u, v) = -2^4 \cdot 5 \cdot 23 \cdot 1163 \cdot u - 2^4 \cdot 3^2 \cdot 31 \cdot v - 2^{15} \cdot 3^3 \cdot 5^3 \cdot 23 \cdot 3499, \]
\[ Q_{22}(u, v) = -2^4 \cdot 3^2 \cdot 31 \cdot u - 2 \cdot 3 \cdot v + 2^6 \cdot 5^3 \cdot 109^3. \]

If \( t \) does not lie in \( \mathbb{F}_p \), then 1 and \( t^p \) are independent over \( \mathbb{F}_p \), and (2.8) implies that the combinations

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

must both be zero \((\text{mod } p)\), for \( u = -t^p - t \) and \( v = t^{p+1} \), which are just the coefficients in the quadratic equation satisfied by \( t \) over \( \mathbb{F}_p \). Taking the three possible equations in turn, from (2.7), and computing the gcd of the integers \( D_1 \) and \( D_2 \) in each case, we find

\[ \gcd(D_1, D_2) = 2^{17} \cdot 3 \cdot 5^3 \cdot 13 \cdot 37 \cdot 53, \text{ if } H_{20}(t) \equiv 0 \pmod{p}; \]
\[ \gcd(D_1, D_2) = 2^{11} \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 37 \cdot 53, \text{ if } H_{32}(t) \equiv 0 \pmod{p}; \]
\[ \gcd(D_1, D_2) = 2^{16} \cdot 3 \cdot 5^3 \cdot 7 \cdot 37 \cdot 53, \text{ if } H_{35}(t) \equiv 0 \pmod{p}. \]

Thus \( t \) is never a zero of \( F''(t) \pmod{p} \), when \( p > 53 \), and the multiplicity of such a root of \( \Phi_3(t^p, t) \) is at most 2.

On the other hand, if \( t \) lies in \( \mathbb{F}_p \), then the factorization of \( \Phi_3(t, t) \) shows that \( t = 0, 8000, -32768, \) or 54000. We have, using the congruences

\[ F'(t) \equiv -Q_1(-2t, t^2) + tQ_2(-2t, t^2) \pmod{p}, \]
\[ F''(t) \equiv Q_{11}(-2t, t^2) - 2tQ_{12}(-2t, t^2) + t^2Q_{22}(-2t, t^2) \pmod{p}, \]

the following values of \( F''(t) \pmod{p} \):

\[ F''(0) \equiv 2^{31} \cdot 3^3 \cdot 5^6, \]
\[ F''(8000) \equiv 2^{20} \cdot 3 \cdot 5^6 \cdot 7^4 \cdot 13^2 \cdot 23, \]
\[ F''(-32768) \equiv -2^{32} \cdot 3 \cdot 7^4 \cdot 13^2 \cdot 17 \cdot 29; \]

while

\[ F'(54000) \equiv -2^{19} \cdot 3^3 \cdot 5^9 \cdot 11^2 \cdot 17^2 \cdot 23^2 \cdot 29^2, \quad (2.9) \]
\[ F''(54000) \equiv -2^{16} \cdot 3^3 \cdot 5^6 \cdot 17 \cdot 23 \cdot 29 \cdot 89 \cdot 1153. \]
Hence, $F''(t)$ is never $0 \pmod{p}$ at an $\mathbb{F}_p$-rational double root of $F(t)$, for $p > 29$. Therefore, the multiplicities of all roots of $\Phi_3(t^p, t) \pmod{p}$ are at most 2, for $p > 53$. For primes between 5 and 53, direct calculation shows that the maximum multiplicity of a multiple factor of $\Phi_3(t^p, t) \pmod{p}$ is 4. The polynomial $\Phi_3(t^p, t)$ has an irreducible factor of multiplicity 3 for $p = 17, 23, 29, 37, 53$ and a factor of multiplicity 4 for $p = 5, 7, 13$. □

**Corollary 2.8.** For $p > 53$ the multiplicities of the linear factors $t, t - 54000, t + 32768$ and $t - 8000$ in the factorization of $\Phi_3(t^p, t) \pmod{p}$ are, respectively, 1, 1, 2, and 2.

*Proof.* We have, in the notation of the proof of Proposition 2.7, for $t \in \mathbb{F}_p$, that

$$F'(t) = -Q_1(-2t, t^2) + tQ_2(-2t, t^2)$$

$$= -3t^5 + 2^3 \cdot 3^1 \cdot 5 \cdot 31 \cdot t^4 + 2^{12} \cdot 1262587 \cdot t^3$$

$$+ 2^{15} \cdot 2^3 \cdot 5^1 \cdot 109 \cdot 443 \cdot t^2 - 2^{32} \cdot 5^6 \cdot 7 \cdot 11 \cdot 149 \cdot t + 2^{45} \cdot 3^3 \cdot 5^9$$

$$= -(t + 32768)(t - 8000)(3t^3 - 85464t^2 - 226835200t + 7077888000000).$$

Hence $F'(0) \equiv 2^{45} \cdot 3^3 \cdot 5^9$. Equation (2.9) and Proposition 2.7 now imply the assertions of the corollary. □

### 3  Proofs of Theorems 1.1 and 1.2.

The following theorem is preparation for the proof of the explicit congruences in Theorems 1.1 and 1.2. It allows us to identify which factors of $J_p(t)$ will divide $H_{-4dp}(t)$ or $H_{-dp}(t)H_{-4dp}(t)$ over $\mathbb{F}_p$. For the sake of convenience, let

$$K_{dp}(t) = H_{-4dp}(t) \quad \text{or} \quad H_{-dp}(t)H_{-4dp}(t)$$

according as $dp \equiv 1, 2$ or $dp \equiv 3 \pmod{4}$.

**Theorem 3.1.** Let $d > 1$ be a square-free, positive integer, not divisible by $p$. An irreducible quadratic factor $q(t) = t^2 + at + b$ of $J_p(t)$ over $\mathbb{F}_p$ divides $K_{dp}(t) \pmod{p}$ if and only if $Q_d(a, b) \equiv 0 \pmod{p}$, where $Q_d(u, v)$ is the de-symmetrized form of the transformation polynomial $\Phi_d(x, y)$ defined by $Q_d(-x - y, xy) = \Phi_d(x, y)$.
Proof. By Lemma 2.3 and (1.1), $q(t)$ divides $K_{dp}(t)$ over $\mathbb{F}_p$ if and only if it divides $\gcd(J_p(t), \Phi_d(t^p, t))$; and $q(t)$ divides $\Phi_d(t^p, t)$ if and only if $0 = \Phi_d(j_p, j) = Q_d(-j^p - j, j^{p+1})$, for a root $j$ of $q(t)$. But $-j^p - j = a$ and $j^{p+1} = b$, so this is the case exactly when $Q_d(a, b) = 0$. □

Remark. When $d = 2$ the polynomial $Q_2(u, v)$ is given by

$$4Q_2(u, v) = -(2v + 1485u - 41097375)^2 - (4u - 29025)(u - 191025)^2.$$ 

With this preparation we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. From Lemma 2.3 and the factorization of $\Phi_2(t, t)$ we know that $(t - 1728), (t - 8000), \text{and} (t + 3375)$ are the only possible linear factors of $H_{-8p}(t)$ over $\mathbb{F}_p$, and that these factors occur in $H_{-8p}(t)$ if and only if their roots are supersingular $j$-invariants for the prime $p$. This explains the definitions of the $\epsilon_i, i = 1, 2, 3$, by the discussion preceding Proposition 2.4. Lemma 2.3 shows that the correct exponent of each of these factors is twice the exponent of the same factor in $\Phi_2(t^p, t)$. Proposition 2.4 and Corollary 2.6 show that the exponent for both $(t - 1728)$ and $(t - 8000)$ in $\Phi_2(t^p, t)$ is 1, and for $(t + 3375)$ is 2. This explains the contribution of the linear factors, since their roots (mod $p$) are distinct for $p > 13$.

We turn now to the quadratic factors, beginning with $H_{-15}(t)$. By the initial argument in the proof of Proposition 2.4, $H_{-15}(t)$ is the only irreducible quadratic that can divide $H_{-8p}(t) \pmod{p}$ to a power higher than 2, because it is the only such quadratic dividing $\Delta_2(t)$. Its roots are supersingular and quadratic over $\mathbb{F}_p$ exactly when $\epsilon_1 = 1$. Further, it must divide $H_{-8p}(t)$ when $\epsilon_1 = 1$, because its roots $\alpha_+$ and $\alpha_-$ satisfy $\Phi_2(\alpha_+, \alpha_-) = 0$ in characteristic 0, and therefore in characteristic $p$ for all $p$ (see the expressions for $\alpha_+, \alpha_-$ in the proof of Proposition 2.4). It is straightforward to compute that the derivative $(\Phi_2(t^p, t))'$ is also 0 at $\alpha_+$ and $\alpha_-$, when these roots are quadratic over $\mathbb{F}_p$, using the expression $F_1(t, t^p)$ given in the proof of Proposition 2.4. Hence, $H_{-15}(t)$ must occur to the 4-th power in $H_{-8p}(t) \pmod{p}$ when $\epsilon_1 = 1$, by the result of Proposition 2.4.

It remains to show that $H_{-15}(t)$ makes no contribution to the factorization of $H_{-8p}(t) \pmod{p}$ when $\epsilon_4 = 0$, or (wlog) when $(\frac{2}{p}) = +1$. But in that case $H_{-15}(t)$ has two linear factors (mod $p$), and any contribution to the factorization of $H_{-8p}(t)$ must coincide with one of the factors $(t - 1728), (t - 8000), (t + 3375)$ discussed above. In fact, this happens for $p > 13$ only when $p = 29$, since 29 is the only prime divisor greater than 13 of any of the integers $H_{-15}(1728), H_{-15}(8000), H_{-15}(-3375)$. 

19
All other irreducible quadratic factors of $H_{-8p}(t) \pmod{p}$ are the quadratic factors of $J_p(t)$ (aside from $H_{-15}(t)$) for which $Q_2(a_i, b_i) = 0$ in $\mathbb{F}_p$, by Theorem 3.1. Furthermore, they must occur to exactly the second power in $H_{-8p}(t)$, by Lemma 2.3 and the above argument. This completes the proof. □

**Theorem 3.2.** If $p > 13$ and $h(-2p)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-2p})$, then

$$h(-2p) = 5 + \left(\frac{-3}{p}\right) - \left(\frac{-4}{p}\right) - \left(\frac{5}{p}\right) - 2 \left(\frac{-7}{p}\right) - \left(\frac{-8}{p}\right) - \left(\frac{-15}{p}\right) + 4N_2,$$

where $N_2$ is the number of irreducible quadratic factors $t^2 + at + b$ of $J_p(t)$ over $\mathbb{F}_p$ for which $Q_2(a, b) \equiv 0 \pmod{p}$.

Theorem 3.2 follows immediately from Theorem 1.1 by equating degrees, since

$$h(-2p) = \deg H_{-8p}(t) = 2\epsilon_1 + 2\epsilon_2 + 4\epsilon_3 + 8\epsilon_4 + 4(N_2 - \epsilon_4).$$

As an example, consider the prime $p = 233$, for which we have

$$J_{233}(t) \equiv (t + 46)(t + 50)(t + 56)(t + 148)(t + 222)(t^2 + 25t + 109)(t^2 + 55t + 139) \times (t^2 + 64t + 57)(t^2 + 81t + 81)(t^2 + 147t + 62)(t^2 + 162t + 216) \times (t^2 + 169t + 171) \pmod{233}.$$  

Only the first and third quadratic factors in this factorization satisfy $Q_2(a, b) \equiv 0$, so $N_2 = 2$ and Theorem 3.2 gives $h(-2 \cdot 233) = 0 + 4N_2 = 8$.

**Theorem 3.3.** If $p > 13$, the number of distinct $j$-invariants of supersingular elliptic curves $E$ in characteristic $p$ for which $\sqrt{-2p}$ is an endomorphism of $E$ is

$$\frac{1}{2} (h(-2p) - 2\epsilon_3 - 4\epsilon_4) =$$

$$\frac{1}{2} \left(h(-2p) - 2 - \left(\frac{-3}{p}\right) + \left(\frac{5}{p}\right) + \left(\frac{-7}{p}\right) + \left(\frac{-15}{p}\right)\right).$$

Theorem 3.3 is also immediate, since the count given in this corollary is just the number of distinct roots of $H_{-8p}(t) \pmod{p}$. 

20
We turn now to the analogous theorem for the field \( \mathbb{Q}(\sqrt{-3p}) \).

**Proof of Theorem 1.2.** As in the proof of Theorem 1.1, the linear factors \( H_{-3}(t) = t, H_{-12}(t) = t - 54000, H_{-11}(t) = t + 32768 \) and \( H_{-8}(t) = t - 8000 \) (see (2.6)) certainly divide \( K_{3p}(t) \) when their roots are supersingular in characteristic \( p \), by Lemma 2.3 and the formula

\[
\Phi_3(t, t) = -(t - 54000)(t + 32768)^2(t - 8000)^2.
\]

These are the only possible linear factors of \( K_{3p}(t) \) (mod \( p \)), and they are distinct for \( p > 29 \). Furthermore their multiplicities are, respectively, 2, 2, 4, and 4, when they occur, by Corollary 2.8.

The three quadratic factors

\[
H_{-20}(t) = t^2 - 1264000t - 681472000,
H_{-32}(t) = t^2 - 5225000t + 121670000000,
H_{-35}(t) = t^2 + 117964800t - 134217728000,
\]

are distinct (mod \( p \)) for \( p > 53 \), and all divide \( \Phi_3(t^p, t) \) (mod \( p \)) when they are irreducible over \( \mathbb{F}_p \). This holds because in characteristic 0, the coefficients of each polynomial \( t^2 + ct + d \) satisfy \( Q(c, d) = Q_3(c, d) = 0 \). Furthermore, in the proof of Proposition 2.7 the partial derivatives

\[
\frac{\partial}{\partial u} Q(u, v) = 2^2u^3 - 2^{15}\cdot 3^3\cdot 5^2u^2 + 2^{31}\cdot 3^3\cdot 5^6u - 2^{15}\cdot 3^3\cdot 5^9 - 2^4\cdot 5\cdot 23\cdot 1163uv - 2^3\cdot 3^2\cdot 31v^2 - 2^{15}\cdot 3^3\cdot 5^3\cdot 23\cdot 3499v,
\]

\[
\frac{\partial}{\partial v} Q(u, v) = -2^3\cdot 5\cdot 23\cdot 1163u^2 - 2^4\cdot 3^2\cdot 31uv - 2^{15}\cdot 3^3\cdot 5^3\cdot 23\cdot 3499u - 3v^2 + 2^5\cdot 5^3\cdot 109^3\cdot u - 2^{34}\cdot 5^9\cdot 23,
\]

are employed to give an expression for the derivative

\[
\frac{d}{dt}\Phi_3(t^p, t) \equiv -\frac{\partial}{\partial u} Q(-t^p - t, t^{p+1}) + t^p \frac{\partial}{\partial v} Q(-t^p - t, t^{p+1}) \pmod{p}.
\]

Since \( \frac{\partial}{\partial u} Q(c, d) = \frac{\partial}{\partial v} Q(c, d) = 0 \) in characteristic 0, for each of the three quadratics given above, it follows that each quadratic is a double factor of \( \Phi_3(t^p, t) \) whenever
it is irreducible (mod \( p \)). By Lemma 2.3 these quadratics divide \( K_{3p}(t) \) (mod \( p \)) whenever they are irreducible and supersingular, i.e., when the respective \( \delta_i = 1 \). For the definitions of \( \delta_i \) for \( i = 4, 5, 6 \) note that \( H_D(t) \) has roots in \( \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2}), \) and \( \mathbb{Q}(\sqrt{5}) \) for \( D = -20, -32, -35 \), respectively. Lemma 2.3, Proposition 2.7, and the above argument show that each \( H_D(t) \) has multiplicity 4 when it occurs. Finally, as in the proof of Theorem 1.1, the contributions of \( H_D(t) \) to the factorization of \( K_{3p}(t) \) (mod \( p \)) are accounted for by the linear factors discussed above, when \( H_D(t) \) is reducible (mod \( p \)).

The rest of the argument is now exactly as in the proof of Theorem 1.1. □

**Theorem 3.4.** If \( p > 53 \), \( h(-3p) \) is the class number of \( \mathbb{Q}(\sqrt{-3p}) \), and \( a_p \) is defined in (1.3), then

\[
a_p h(-3p) = 9 - 2 \left( \frac{-3}{p} \right) + 2 \left( \frac{-4}{p} \right) - 2 \left( \frac{5}{p} \right) + \left( \frac{-7}{p} \right) - \left( \frac{8}{p} \right) - 3 \left( \frac{-8}{p} \right) - 2 \left( \frac{-11}{p} \right) - \left( \frac{-20}{p} \right) - \left( \frac{-35}{p} \right) + 4N_3,
\]

where \( N_3 \) is the number of irreducible quadratic factors \( t^2 + ct + d \) of \( J_p(t) \) over \( \mathbb{F}_p \) for which \( Q_3(c, d) \equiv 0 \) (mod \( p \)).

This theorem is immediate from the congruence in Theorem 1.2, since \( \deg K_{3p}(t) = a_p h(-3p) \), by (1.3) and the well-known relationship between the classnumbers \( h(\mathcal{O}_{-3p}) \) and \( h(\mathcal{O}_{-12p}) \) in [co, p. 146].

For example, with \( p = 233 \), all but the third quadratic in the above factorization of \( J_{233}(t) \) satisfy \( Q_3(c, d) \equiv 0 \), so \( 4h(-3 \cdot 233) = 16 + 4N_3 = 16 + 4 \cdot 6 = 40 \) and \( h(-3 \cdot 233) = 10 \).

The analogue of Theorem 3.3 is

**Theorem 3.5.** If \( p > 53 \), the number of distinct \( j \)-invariants of supersingular elliptic curves \( E \) in characteristic \( p \) for which \( \sqrt{-3p} \) lies in \( \text{End}(E) \) is

\[
\frac{1}{2}(a_p h(-3p) - 2\delta_2 - 2\delta_3 - 4\delta_4 - 4\delta_5 - 4\delta_6).
\]
4  A proof of Ogg’s Theorem.

As noted in the introduction, Theorems 1.1 and 1.2 allow us to give the following proof of Ogg’s Theorem. It is trivial that $s_s(p(x))$ is a linear polynomial for $p = 2, 3, 5, 7, 13$, and that $s_{s11}(x) = x(x - 1728)$ is a product of linear factors, by (1.1). We may therefore restrict our attention to primes $p > 13$.

Assume $p > 13$ is a prime for which $s_s(p(t))$ splits into linear factors over $\mathbb{F}_p$. Then no quadratic factors can appear in the factorization of $H_{-sp}(t)$ in Theorem 1.1, and it follows that the degree $h(-2p)$ of $H_{-sp}(t)$ is given by

$$h(-2p) = 2\epsilon_1 + 2\epsilon_2 + 4\epsilon_3 = 4 - \left(\frac{-4}{p}\right) - \left(\frac{-8}{p}\right) - 2 \left(\frac{-7}{p}\right), \quad p > 13. \quad (4.1)$$

Considering the different residue classes of $p \pmod{8}$, we find that

$$h(-2p) = 4, \text{ if } p \equiv 1 \pmod{8};$$
$$h(-2p) = 2 \text{ or } 6, \text{ if } p \equiv 3 \pmod{8};$$
$$h(-2p) = 2 \text{ or } 6, \text{ if } p \equiv 5 \pmod{8};$$
$$h(-2p) = 4 \text{ or } 8, \text{ if } p \equiv 7 \pmod{8}.$$

Whenever $p \equiv 1 \pmod{8}$ or the class number $h(-2p) = 6, 6, 8$ is given by the second possibility in the last three cases listed, we have $(-7/p) = -1$. In any case, the quadratic factor $H_{-15}(t)$ does not appear in the factorization of $H_{-sp}(t) \pmod{p}$, so either $(5/p) = +1$ or $(-15/p) = +1$.

Whenever $p > 53$, we can apply the same reasoning to the quadratic factors $H_{-20}(t), H_{-32}(t), H_{-35}(t)$ in Theorem 1.2. This gives respectively,

$$(5/p) = +1 \text{ or } (-5/p) = +1;$$
$$(2/p) = +1 \text{ or } (-2/p) = +1; \quad (4.2)$$
$$((5/p) = +1 \text{ or } (-35/p) = +1.$$

The second of these conditions shows that $p$ cannot be $5 \pmod{8}$. Thus the third possibility listed above for $h(-2p)$ cannot occur for $p > 53$. Moreover, we have the analogous condition to (4.1), namely
\[ a_p h(-3p) = 4\delta_1 + 4\delta_2 + 4\delta_3 = 6 - 2 \left( -\frac{3}{p} \right) - 2 \left( -\frac{8}{p} \right) - 2 \left( -\frac{11}{p} \right), \quad p > 53, \quad (4.3) \]

where \( a_p \) is defined in (1.3).

**Case 1.** \( p \equiv 1 \pmod{8}, \) \( h(-2p) = 4, \) \( (-7/p) = -1, \) \( p > 13. \)

We have that \( (-2p/7) = +1, \) so the prime 7 splits into two prime ideals in the field \( \mathbb{Q}(\sqrt{-2p}) \). Hence an equation

\[ 7^h = x^2 + 2py^2, \quad (x, y) = 1, \quad y \neq 0, \quad (4.4) \]

holds in \( \mathbb{Z} \), where \( h \) divides 4. It follows that \( 2p < 7^h \). No primes \( p \) greater than 13 satisfy (4.4) with \( h = 1 \) or 2, so we assume \( h = 4 \). Direct calculation shows that the only solutions to (4.4) with \( h = 4 \) are:

\[ 2401 = 1^2 + 2 \cdot 3 \cdot 20^2, \quad 13^2 + 2 \cdot 31 \cdot 6^2, \quad 15^2 + 2 \cdot 17 \cdot 8^2, \quad 31^2 + 2 \cdot 5 \cdot 12^2, \]

or \[ 2401 = 33^2 + 2 \cdot 41 \cdot 4^2, \quad 45^2 + 2 \cdot 47 \cdot 2^2. \quad (4.5) \]

Hence the only primes \( p \) falling into this case are \( p = 17, 41 \), both of which satisfy (4.1).

**Case 2.** \( p \equiv 3 \pmod{4}, \) \( h(-2p) = 6 \) or 8, \( (-7/p) = -1, \) \( p > 13. \)

In this case we have \( (7/p) = +1 \) and so \( (-2p/7) = +1 \). Once again 7 splits into two prime ideals in \( \mathbb{Q}(\sqrt{-2p}) \). Here, \( (7/p) = +1 \) implies that an ideal \( q_7 \) of norm 7 is equivalent to a square in the classgroup, since \( x_p(q) = (Nq/p) \), for ideals \( q \) relatively prime to \( p \), is the unique quadratic character on the classgroup in \( \mathbb{Q}(\sqrt{-2p}) \). (See [h1, p. 516], [h2], [m1].) Hence the ideal \( q_7 \) has order dividing 3 or 4 in the classgroup, and again equation (4.4) must hold. In addition to the solutions in (4.5), where \( h = 4 \), we must also consider the solutions of (4.4) with \( h = 3 \):

\[ 343 = 1^2 + 2 \cdot 19 \cdot 3^2, \quad 3^2 + 2 \cdot 167 \cdot 1^2, \quad 9^2 + 2 \cdot 131 \cdot 1^2, \quad 15^2 + 2 \cdot 59 \cdot 1^2, \quad 17^2 + 2 \cdot 3 \cdot 3^2. \]

From these solutions and from those in (4.5) we find \( p = 19, 31, 47, 59, 131, 167 \). All
of these primes satisfy (4.1) except \( p = 167 \), since \( h(-2 \cdot 167) = 12 \). The prime 131 may also be excluded since it does not satisfy (4.3). (See Table 1 below.) We note that \( ss_{131}(x) \) and \( ss_{167}(x) \) are almost products of linear polynomials since \( ss_{131}(x) \) factors into a product of linears times one irreducible quadratic over \( \mathbb{F}_{131} \) and \( ss_{167}(x) \) factors into a product of linears times two irreducible quadratics over \( \mathbb{F}_{167} \).

Case 3. \( p \equiv 3 \pmod{4} \), \( h(-2p) = 2 \) or 4, \( (-7/p) = +1 \), \( p > 53 \).

If \( (-3/p) = +1 \), then \( (p/3) = +1 = (-2p/3) \), so by the same argument as in Case 1, \( 3^h = x^2 + 2py^2 \) with \( h = 1, 2, \) or 4; but there are no primes > 13 satisfying this condition. Hence we may assume \( (-3/p) = -1 \) and \( (p/3) = -1 \). It follows that \( p \equiv 11 \pmod{12} \). We now focus on primes \( p \) with \( p > 53 \). From (4.3), with \( a_p = 1 \), we conclude that \( h(-3p) = 4, 8 \) or 12. Since the discriminant of \( \mathbb{Q}(\sqrt{-3p}) \) is \( D = -12p \), the rank of the 2-classgroup in \( \mathbb{Q}(\sqrt{-3p}) \) is 2 (see [h2] or [m1]), so the maximum order of an element in the classgroup is 2, 4, or 6.

Now \( (p/7) = +1 \) implies \( (-3p/7) = +1 \) so as above there is an equation

\[
7^h = x^2 + 3py^2, \quad \text{with } (x, y) = 1, \ y \neq 0, \ h \leq 6.
\]

If \( h(-3p) = 4 \) or 8, then we need only consider \( h = 4 \). We have the solutions

\[
2401 = 17^2 + 3 \cdot 11 \cdot 8^2, \quad 22^2 + 3 \cdot 71 \cdot 3^2, \quad 25^2 + 3 \cdot 37 \cdot 4^2, \quad 26^2 + 3 \cdot 23 \cdot 5^2.
\]

Hence \( p = 71 \) is the only prime greater than 53 in this subcase.

On the other hand, if \( h(-3p) = 12 \), (4.3) gives \( (-8/p) = (-11/p) = -1 \). Thus \( (22/p) = +1 \); combining this with \( (-3p/11) = +1 \) and \( (22/3) = +1 \) implies that there is an ideal \( q = p_2p_{11} \) with norm 22 in \( \mathbb{Q}(\sqrt{-3p}) \) which must be a square in the classgroup. This uses the fact that \( \chi_3(q) = (Nq/p) \) and \( \chi_3(q) = (Nq/3) \), for ideals \( q \) relatively prime to \( 3p \), generate the group of quadratic characters for the classgroup associated with this field. Since \( q = p_2p_{11} \) is equivalent to a square and the exponent of the class group is 6, it follows that \( q^3 \) is principal. From \( p_2^2 = (2) \) it follows that \( 2 \cdot 11^3 = 2662 = x^2 + 3py^2 \). The only primitive solutions of this equation with \( p > 53 \) are

\[
2662 = 23^2 + 3 \cdot 79 \cdot 3^2, \quad 47^2 + 3 \cdot 151, \quad 43^2 + 3 \cdot 271, \quad 37^2 + 3 \cdot 431,
\]

or \( 2662 = 35^2 + 3 \cdot 479, \quad 29^2 + 3 \cdot 607, \quad 1^2 + 3 \cdot 887; \)

of which the only solution with \( p \equiv 11 \pmod{12} \) and \( p \) a quadratic residue of 7 is
\( p = 431 \). However, \( h(-2 \cdot 431) = 8 \), so \( p = 431 \) does not satisfy the conditions of Case 3. Hence, \( p = 71 \) is the only prime \( > 53 \) for this case.

To sum up, we see that the only primes left to consider are the primes \( p \leq 53 \) which are 5 (mod 8) or are 3 (mod 4) and quadratic residues (mod 7), i.e., \( p = 23, 29, 37, 43, 53 \). In the adjoining Table 1 we list the values of \( h(-2p) \) and \( a_p h(-3p) \), along with the functions

\[
\begin{align*}
g_2(p) &= 4 - (-4/p) - (-8/p) - 2(-7/p), \\
g_3(p) &= 6 - 2(-3/p) - 2(-8/p) - 2(-11/p),
\end{align*}
\]

which are defined by the right hand sides of (4.1) and (4.3), respectively, for the primes \( 13 \leq p \leq 53 \), \( p = 59, 71, 131, 167 \) and 431. This table shows that the primes 37, 43, and 53 can also be excluded, since (4.1) fails for these primes (43 is also excluded by the first sentence in Case 3). The excluded primes are all shown in boldface. All of the non-excluded primes satisfy the property that \( ss_p(x) \) splits into linear factors (mod \( p \)). This can be checked using the formula (1.1) for \( ss_p(x) \), or using the necessary and sufficient condition (1.4) in the introduction. This completes the proof of Ogg’s Theorem. \( \Box \)

In this analysis we have excluded primes based solely on the conditions (4.1) and (4.3), since (4.3) implies (4.2). Together with the results in Table 1, this implies the following:

**Theorem 4.1** A prime \( p \geq 13 \) satisfies the condition that \( ss_p(x) \) splits into a product of linear factors (mod \( p \)) if and only if it satisfies both of the conditions:

\[
h(-2p) = g_2(p) \quad \text{and} \quad a_p h(-3p) = g_3(p),
\]

where \( g_2(p) \) and \( g_3(p) \) are defined by (4.6) and \( a_p \) is defined by (1.3).

This theorem is equivalent to Theorem 1.4 of the Introduction.

(Note to the editor and printer: Table 1 (next page) goes here.)
Table 1: Comparison of $h(-2p)$ with $g_2(p)$ and $a_ph(-3p)$ with $g_3(p)$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$h(-2p)$</th>
<th>$g_2(p)$</th>
<th>$h(-3p)$</th>
<th>$a_p$</th>
<th>$g_3(p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>23</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>31</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>37</td>
<td>10</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>41</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>43</td>
<td>10</td>
<td>2</td>
<td>12</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>47</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>53</td>
<td>6</td>
<td>2</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>59</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>71</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>131</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>167</td>
<td>12</td>
<td>8</td>
<td>16</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>431</td>
<td>8</td>
<td>4</td>
<td>24</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>
5 The class equations $H_{-3p}(t)$ and $H_{-12p}(t)$.

In this section we shall give a proof of Theorem 1.5. In order to do this we examine each of the explicit factors of $K_{3p}(t) \pmod{p}$ in Theorem 1.2, and determine whether or not that factor – which is itself a class equation – can divide $H_{-3p}(t)$ modulo $p$, when $p \equiv 1 \pmod{4}$. Note that the Gross-Zagier theorem ([gz], [dor]) is not well suited to this situation since it requires the discriminants corresponding to the two class equations being compared to be fundamental discriminants which are relatively prime to each other. Since the discriminants corresponding to five of the seven class equations appearing in the product in Theorem 1.2 are either not fundamental or not relatively prime to $-3p$ resp. $-12p$, this theorem is not applicable to them. Thus, we take an alternate approach. The criterion we use is contained in the following lemma, whose straightforward proof we leave to the reader. (See the arguments in [el] or [brm, Prop. 7].)

**Lemma 5.1.** Let $\mu \in \text{End}(E_\alpha)$ be a multiplier of the curve

$$E_\alpha : \quad Y^2 + \alpha XY + Y = X^3$$

in characteristic $p$, satisfying $\mu^2 = -3p$. Then $\frac{1+\mu}{2} \in \text{End}(E_\alpha)$ if and only if $\mu$ is the identity permutation on the points in $E_\alpha[2]$.

**Lemma 5.2.** If $p \equiv 1 \pmod{4}$, then $H_{-3p}(t)$ is a product of square factors $\pmod{p}$.

**Proof.** This proof is similar to the proof of Prop. 9 and congruence (3.3b) in [brm]. The class number $h = h(-3p)$ is even, and the genus field of $k = \mathbb{Q}(\sqrt{-3p})$ is $\mathbb{Q}(\sqrt{p}, \sqrt{-3})$, so $\mathbb{Q}(\sqrt{p})$ is contained in the real subfield $\Sigma_0$ of the Hilbert class field $\Sigma$ of $k$. The ideal $(p)$ is a square in $\mathbb{Q}(\sqrt{p})$. Moreover the prime ideal $\mathfrak{p}$ over $p$ in $k$ has order 2 in the class group of $k$, and therefore splits into $h/2$ prime ideals of degree 2 in $\Sigma$. Putting these two facts together implies that $p$ splits into the squares of primes of degree 1 or 2 in $\Sigma_0$. Thus, over the $p$-adic field $\mathbb{Q}_p$, the polynomial $H_{-3p}(t)$, either of whose real roots generates the real subfield $\Sigma_0$ over $\mathbb{Q}$, splits into a product of irreducible quadratics or quartics, each belonging to a ramified extension of $\mathbb{Q}_p$ with ramification index $e = 2$. Each of these irreducible factors must reduce to a power of an irreducible factor $\pmod{p}$, by Hensel’s Lemma. Therefore, each of these irreducible factors must be a square $\pmod{p}$. This proves the lemma. \[\square\]

In the situation we are considering, the curve $E_\alpha$ is supersingular in characteristic $p$, because we want its $j$-invariant to be a root of $H_{-3p}(t)$ or $H_{-12p}(t)$ over $\mathbb{F}_p$. We
work on the curve $E_{\alpha}$, which is in Deuring normal form, because a multiplier $\mu$ satisfying $\mu^2 = -3p$ is given explicitly in [m4]. Such a multiplier exists with kernel equal to $\{O, (0, 0), (0, -1)\}$ if and only if $(\alpha, \alpha^p)$ is a point on the curve

$$F_{r_3} : 27X^3 + 27Y^3 = X^3Y^3.$$  

If this is the case, $\mu$ is given by $\mu = \pm \nu \circ \phi$, where $\nu(X, Y) = (X^p, Y^p)$ is the Frobenius map and $\phi = \phi_{\alpha, \beta}$ with $\beta = \alpha^p$ is the isogeny from $E_{\alpha}$ to $E_{\beta}$ given on $X$-coordinates by

$$\phi_{\alpha, \beta}(X) = -\frac{\beta^2}{9\alpha^2} \left(\frac{3X^3 + \alpha^2X^2 + 3\alpha X + 3}{X^2}\right), \quad \beta = \alpha^p. \quad (5.1)$$

Furthermore, by [m4, Thm. 2.3], the parameter $\alpha$ of a supersingular curve $E_{\alpha}$ lies in the finite field $\mathbb{F}_{p^2}$. Hence we may write the $X$-coordinate of the image $\mu(X, Y) = (X^p, Y^p)$ of the point $(X, Y)$ on $E_{\alpha}$ as

$$X^\mu = -\frac{\alpha^2}{9\alpha^2} \left(\frac{3X^3 + \alpha^2X^2 + 3\alpha X + 3}{X^2}\right)^p, \quad \alpha \neq 0. \quad (5.2)$$

If $\alpha = 0$, we have instead that

$$X^\mu = -\frac{1}{3} \left(\frac{X^3 + 1}{X^2}\right)^p, \quad \alpha = 0. \quad (5.3)$$

On the other hand, the points of order 2 on $E_{\alpha}$ are the points $(x, y)$ satisfying the equation

$$\left(y + \frac{\alpha}{2} x + \frac{1}{2}\right)^2 = x^3 + \frac{1}{4}(\alpha x + 1)^2 = 0. \quad (5.4)$$

Replacing $X$ by $x$ and $x^3$ by $-(\alpha x + 1)^2/4$ in the formula (5.2) for $\mu$ gives

$$x^\mu = -\frac{\alpha^2}{36\alpha^2} \left(\frac{(\alpha x + 3)^2 x}{x^2}\right)^p$$

$$= -\frac{\alpha^2}{36\alpha^2} \left(\frac{\alpha x + 3}{x}\right)^{2p}, \quad \alpha \neq 0, \quad (5.5)$$
for solutions $x$ of (5.4). Thus $\mu$ is the identity permutation on the points of $E_0[2]$ if and only if $x^\mu = x$ for all the roots $x$ of (5.4).

**Example.** (The factor $H_{-3}(t) = t$.) The factor $H_{-3}(t) = t$ corresponds to $j = 0$. We consider the curve $E_0 : Y^2 + Y = X^3$ with $\alpha = 0$, and take $p$ to be a prime with $p \equiv 5 \pmod{12}$, in order that $\delta_1 = 1$ in Theorem 1.2. Then the $X$-coordinates of points of order 2 satisfy $x^3 + 1/4 = 0$. Thus we have the three roots

$$x_i = -\frac{\omega^i}{4^{1/3}}, \quad 1 \leq i \leq 3,$$

where $\omega$ is a primitive cube root of unity in $\mathbb{F}_{p^2}$. In this case (5.3) gives that $x_i^\mu = -\frac{1}{4x_i^2}$. Since $4^{1/3} \in \mathbb{F}_p$ but $\omega \notin \mathbb{F}_p$ we have

$$x_i^\mu = -\frac{1}{4} \cdot \frac{\omega^i}{4^{1/3}} = -\frac{\omega^{2i}}{4^{1/3}} = x_{2i}.$$

Thus, $\mu$ does not fix the point $P_1 = (x_1, -1/2)$. By Lemma 5.1, we know that there is no endomorphism of $E_0$ of the form $(1 + \mu)/2$. This assumes that $\ker(\mu) = \{O, (0, 0), (0, -1)\}$.

Now suppose $\mu$ is any endomorphism of $E_0$ satisfying $\mu^2 = -3p$. By arguments of [m4, Section 4], there is an isomorphism of $E_0$ defined over $\mathbb{F}_{p^2}$ taking $E_0$ to a curve $E_{\alpha'}$ with $j(E_{\alpha'}) = 0$, and taking $\mu \to \mu' \in \text{End}(E_{\alpha'})$ such that $\ker(\mu') = \{O', (0, 0), (0, -1)\}$ on $E_{\alpha'}$. Then $\mu'^2 = -3p$ implies that $(\alpha', \alpha'^p)$ is a point on $\text{Fer}_3$. The only possibilities for $\alpha'$ are $\alpha' = 0, 2 \cdot 3^{1/3} \omega^i$, by the fact that

$$j(E_{\alpha'}) = \frac{\alpha'^3(\alpha'^3 - 24)^3}{\alpha'^3 - 27}.$$

If $\alpha' = 2 \cdot 3^{1/3} \omega^i$, it is easy to check that the only $\beta'$s for which $(\alpha', \beta)$ lies on $\text{Fer}_3$ are $\beta = -6\omega^j$, and such a $\beta$ can only equal $\alpha'^p$ if $p = 5$. If we restrict ourselves to primes $p > 5$, then we must have $\alpha' = 0 = \alpha$ and therefore $\mu' = \pm \mu$. It follows that there is no endomorphism $\mu$ of $E_0$ for which $\mu^2 = -3p$ and $(1 + \mu)/2 \in \text{End}(E_0)$.

This proves the following proposition.

**Proposition 5.3.** If $p \equiv 1 \pmod{4}$ and $p > 5$, the factor $H_{-3}(t) = t$ never divides $H_{-3p}(t) \pmod{p}$. Hence we have $t^{2i} | H_{-12p}(t) \pmod{p}$ for all $p > 53$.

This proposition takes care of one of the seven explicit factors of $K_{3p}(t)$ in Theorem 1.2. In the propositions that follow $p$ represents a prime $\equiv 1 \pmod{4}$ with
For the linear factors (Props. 5.4-5.6), the computations in the proofs of Proposition 2.7 (see equation (2.9)) and Theorem 1.2 (Section 3) show that we could improve this to \( p > 29 \).

**Proposition 5.4.** If \( p \equiv 1 \pmod{4} \) and \( p > 53 \), then \( H_{-12}(t)^{241} = (t - 54000)^{241} \) divides \( H_{-3p}(t) \pmod{p} \) and \( (t - 54000) \) does not divide \( H_{-12p}(t) \pmod{p} \).

**Proof.** We only have to show that \( t - 54000 \) divides \( H_{-3p}(t) \pmod{p} \) when \( p \equiv 5 \pmod{12} \). The assertion will then be immediate from Lemma 5.2 and Theorem 1.2.

To show this we take \( \mu = 5 \cdot 4^{1/3} \cdot 2^{1/3} \in \mathbb{F}_p \) so that

\[
j(E_\alpha) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} = 54000.
\]

Note that \((\alpha, \alpha^p) = (\alpha, \alpha)\) is a point on \( \text{Fer}_3 \). The roots \( x_i \) of (5.4) can be determined by noting that

\[
x_i^3 + \frac{\alpha^2}{4}x_i^2 + \frac{\alpha}{2}x_i + \frac{1}{4} = \frac{1}{54} \left( y^3 + \frac{27}{2}y^2 + 27y + \frac{27}{2} \right), \quad (y = \alpha x_i)
\]

\[
= \frac{1}{54} \left( y + \frac{3}{2} \right)(y^2 + 12y + 9).
\]

We find the roots

\[
x_1 = -\frac{1}{4} \cdot 4^{1/3}, \quad x_2 = -\frac{2 + \sqrt{3}}{2} \cdot 4^{1/3}, \quad x_3 = -\frac{2 - \sqrt{3}}{2} \cdot 4^{1/3}.
\]

Using the fact \( \sqrt{3} \notin \mathbb{F}_p \) it is straightforward to verify that \( x_i^\mu = x_i \) for \( i = 1, 2, 3 \), so \( \mu \) fixes all the points of order 2 on \( E_\alpha \). Hence, \( \frac{1 + \sqrt{3}}{2} \) injects into \( \text{End}(E_\alpha) \) under reduction of a suitable elliptic curve with complex multiplication by the order \( O_{-3p} \), and therefore \( j(E_\alpha) = 54000 \) is a root of \( H_{-3p}(t) \pmod{p} \). \( \square \)

The factors \( H_{-8}(t) = t - 8000 \) and \( H_{-11}(t) = t + 32768 \) (see (2.6)) require a little more work, since they occur to the 4th power in the factorization of \( K_{3p}(t) \pmod{p} \) whenever they are present. We first note the following.

In general, if \( \mu \) is an endomorphism in \( E_\alpha \) with \( \mu^2 = -3p \) and \( \text{ker}(\mu) \) is a subgroup of \( E_\alpha[3] \) other than \( \{0, (0, 0), (0, -1)\} \), then there is an isomorphism \( \iota : E_\alpha \to E_{\alpha'} \) defined over \( \mathbb{F}_{p^2} \) for which \( \mu \to \mu' \) with \( \mu'^2 = -3p \) and \( \text{ker}(\mu') = \{0', (0, 0), (0, -1)\} \). Then \( (\alpha', \alpha'^p) \) is a point on \( \text{Fer}_3 \), and \(( x - \alpha'^3)(x - \alpha'^{3p}) = q(x) \) is irreducible.
over \( \mathbb{F}_p \) satisfying \( q(x) = x^2 + Ax + B \) with \( B = -27A \). (This holds whenever \( j = j(E_{\alpha}) \neq 0, 54000 \).) These factors \( q(x) \) have been studied in [m4, Section 5], where they are shown to be in 1-1 correspondence with the quartic factors of \( K_{3p}(t) \) over \( \mathbb{F}_p \) which are powers of irreducibles. In this situation, the endomorphism \( \mu' \) is determined up to sign, by [m4, Prop. 4.1], namely

\[
\mu' = \pm \nu' \circ \phi_{\alpha', \alpha^p},
\]

as in the discussion immediately following equation (5.1) above. Furthermore, \( \mu = \nu^{-1} \circ \mu' \circ \nu \) on \( E_{\alpha} \) is independent of the particular cube root of \( \alpha^3 \) which is chosen, as can be seen from the formula for \( \phi_{\alpha, \alpha^p} \).

Thus, when considering the factors \( H_{-8}(t) = t - 8000 \) and \( H_{-11}(t) = t + 32768 \), whose 4th powers divide \( K_{3p}(t) \) (mod \( p \)), there is only one factor \( q(x) \) of the above form available, for \( p > 53 \). This means that when \( q(\alpha^3) = 0 \) there can only be two independent endomorphisms \( \mu_i \) of \( E_{\alpha} \) satisfying \( \mu_i^2 = -3p \), one of which has \( ker(\mu_1) = \{ O, (0, 0), (0, -1) \} \), the other arising from an isomorphism \( \nu : E_{\alpha} \to E_{\beta} \) in which \( \beta = \alpha^p \).

**Proposition 5.5.** If \( p > 53 \), the factor \( H_{-8}(t)^{4\beta_2} = (t - 8000)^{4\beta_2} \) divides \( H_{-3p}(t) \) (mod \( p \)), so that \( H_{-8}(t) \) does not divide \( H_{-12p}(t) \) (mod \( p \)).

**Proof.** Let \( p \) be a prime \( \equiv 5 \) (mod 8), so that \( (-2/p) = -1 \). We take \( \alpha = -2 + \sqrt{-2} \) and \( \beta = -2 - \sqrt{-2} \) so that \( j(E_{\alpha}) = 8000 \). As noted above, there are two independent endomorphisms \( \mu_i \) in \( \text{End}(E_{\alpha}) \) satisfying \( \mu_i^2 = -3p \). We will show that both of these induce the trivial permutation on the points of order 2. The \( X \)-coordinates of these points satisfy the equation

\[
f_2(x) = x^3 + \frac{\alpha^2}{4} x^2 + \frac{\alpha}{2} x + \frac{1}{4} = (x - x_1)(x - x_2)(x - x_3)
\]

with

\[
x_1 = \frac{1}{2}, \quad x_2 = \frac{(-1 + \sqrt{-1})(1 + \sqrt{2})}{2}, \quad x_3 = \frac{(-1 - \sqrt{-1})(1 - \sqrt{2})}{2}.
\]

Furthermore, \( (\alpha, \beta) = (-2 + \sqrt{-2}, -2 - \sqrt{-2}) \) is a point on \( \text{Fer}_3 \) (even in characteristic 0), so we have the meromorphism \( \mu_1 = \mu \) given by (5.2) or by (5.5) on the roots of \( f_2(x) = 0 \):

\[
x^{\mu_1} = \frac{7 + 4\sqrt{-2}}{324} \left( \frac{\alpha x + 3}{x} \right)^{2p}.
\]
Using that \( \sqrt{-1} \in \mathbb{F}_p \) but \( \sqrt{2}, \sqrt{-2} \notin \mathbb{F}_p \), one computes easily that \( x_i^{\mu_1} = x_i \) for all \( i \).

The second endomorphism \( \mu_2 \) satisfying \( \mu_2^2 = -3p \) in \( \text{End}(E_\alpha) \) is given on \( X \)-coordinates by the formula

\[
X^{\mu_2} = -\frac{1}{3} \left( \frac{X(X^2 + (1 - \sqrt{-2})X - 1 + \sqrt{-2})}{(X - \frac{1 + \sqrt{-2}}{3})^2} \right)^p + \frac{1 + \sqrt{-2}}{3}. \tag{5.6}
\]

This formula can be computed in the following way. We know \( E_\alpha \cong E_\beta \) since \( j(E_\alpha) \in \mathbb{F}_p \). The value

\[
\gamma = \frac{-3\beta}{\alpha(\beta - 3)} = \frac{1 + \sqrt{-2}}{3}
\]

is the \( X \)-coordinate of a point of order 3 on \( E_\alpha \) (see [m4, Thm. 1.3]), and since \( \beta = \alpha^p, \gamma' = \gamma^p \) is the \( X' \)-coordinate of a point of order 3 on \( E_\beta \). By [m4, Prop. 3.10] an isomorphism \( \iota : E_\alpha \to E_\beta \) exists for which \( \iota(X, Y) = (X', Y') \) and

\[
X' = X' = -\frac{\gamma'}{\gamma} X + \gamma' = -\gamma^{p-1} X + \gamma^p = \frac{1 + 2\sqrt{-2}}{3} X + \frac{1 - \sqrt{-2}}{3}, \tag{5.7a}
\]

\[
(X')^{\iota^{-1}} = X = -\frac{1}{\gamma^{p-1}} X' + \gamma = \frac{1 - 2\sqrt{-2}}{3} X' + \frac{1 + \sqrt{-2}}{3}. \tag{5.7b}
\]

(This uses the fact that the linear fractional map \( \sigma_1(z) = 3(z + 6)/(z - 3) \) takes \( \alpha \) to \( \beta \) and vice versa.) The endomorphism \( \mu'_2 = \nu' \circ \phi_{\beta,\alpha} \) on \( E_\beta \) arises by conjugating the coefficients of (5.2) in \( \mathbb{F}_p \):

\[
(X')^{\mu_2} = -\frac{\beta^2}{9\alpha^2} \left( \frac{3X'^3 + \beta^2 X'^2 + 3\beta X' + 3}{X'^2} \right)^p
\]

and satisfies \( \mu_2^2 = -3p \) in \( \text{End}(E_\beta) \). Then \( \mu_2 = \iota \mu_2^{\iota^{-1}} \) (in this order when applied to exponents, i.e. as a meromorphism, but in the reverse order when applied to points) satisfies \( \mu_2^2 = -3p \) in \( \text{End}(E_\alpha) \). The formula (5.6) now follows by using these formulas to compute \( X^{\mu_2} = X^{\mu_2^{\iota^{-1}}} \).
Another straightforward calculation using (5.6) shows that \( \mu_2 \) is the trivial permutation on the roots \( x_i \) of \( f_2(x) = 0 \). Alternatively, since \( \mu_2' \) arises by conjugating the coefficients of the map \( \mu_1 \) in \( \mathbb{F}_{p^2} \) (i.e., raising to \( p \)-th powers), and the points of order 2 on \( E_\beta \) arise in the same way from the points in \( E_\alpha[2] \), it is clear that \( \mu_2' \) induces the trivial automorphism on \( E_\beta[2] \). Then \( \mu_2 \) will also be the trivial permutation on \( E_\alpha[2] \). Note that (5.6) and (5.2) show that \( \ker(\mu_2) \neq \ker(\mu_1) \), so \( \mu_2 \neq \pm \mu_1 \).

It follows that \( (1 + \mu)/2 \in \text{End}(E_\alpha) \) for every endomorphism \( \mu \) for which \( \mu^2 = -3p \). Consequently, there can be no root of \( H_{-12p}(t) \) in characteristic 0 which reduces to \( j \equiv 8000 \) under reduction \( (\text{mod } p) \). If there were, and \( E \) is an elliptic curve with invariant \( j \) and complex multiplication by the order \( O_{12p} \) (i.e., raising to \( p \)-th powers), and the points of order 2 on \( E \) arise in the same way from the points in \( E[2] \), it is clear that \( \mu_2 \) induces the trivial automorphism on \( E[2] \). Then \( \mu_2 \) will also be the trivial permutation on \( E[2] \). Note that (5.6) and (5.2) show that \( \ker(\mu_2) \neq \ker(\mu_1) \), so \( \mu_2 \neq \pm \mu_1 \).

We have the opposite result for the factor \( H_{-11}(t) = t + 32768 \).

**Proposition 5.6.** For \( p > 53 \) we have that \( H_{-11}(t)^{4b_3} = (t + 32768)^{4b_3} \) divides \( H_{-12p}(t) \) \( (\text{mod } p) \), so that \( H_{-3p}(t) \) is not divisible by \( H_{-11}(t) \) \( (\text{mod } p) \).

**Proof.** This follows by a similar argument as in the proof of Proposition 5.5, but with some complications arising from the nature of the solutions of (5.4). We take \( \alpha = -1+\sqrt{-11} \) and \( \beta = -1-\sqrt{-11} \), where \( (\alpha, \beta) \) is a point on \( \text{Fer}_3 \) (in characteristic 0!), and \( j(E_\alpha) = -32768 \). This time we let

\[
f_2(x) = x^3 + \frac{1}{4}(\alpha x + 1)^2 = x^3 - \frac{5 + \sqrt{-11}}{2}x^2 + \frac{-1 + \sqrt{-11}}{2}x + \frac{1}{4}
\]

in characteristic 0, and we set

\[
h(x) = f_2(x)\tilde{f}_2(x) = x^6 - 5x^5 + 8x^4 - \frac{5}{2}x^3 + \frac{7}{4}x^2 - \frac{1}{4}x + \frac{1}{16}.
\]

The polynomials \( h(x) \) is irreducible and normal over \( \mathbb{Q} \) with Galois group \( S_3 \), and since

\[
\text{disc}_x(f_2(x)) = \left(1 - \frac{1}{4}\sqrt{-11}\right)^2,
\]
the splitting field $L$ of $h(x)$ over $\mathbb{Q}$ is a cyclic cubic extension of $k = \mathbb{Q}(\sqrt{-11})$ with Galois group generated by an automorphism $\sigma$, say. Since $L$ arises from $k$ by adjoining the $X$-coordinates of the points of order 2 on $E_\alpha$, a curve with complex multiplication by the ring of integers of $k$, the field $L$ is the ray class field of conductor 2 over $k$. (See [si2, Thm. 5.6, p. 135].) A prime $p$ with $(-11/p) = -1$ splits into 3 primes of degree 2 in $L$, which are cyclically permuted by $\sigma$, because $p$ is inert in $k$ and the ideal $(p)$ lies in the principal ray class (mod 2). For these same primes $E_\alpha$ is supersingular in characteristic $p$.

Now we let $\tau \in Gal(L/\mathbb{Q})$ be complex conjugation and we set $\psi = \tau \circ \phi_{\alpha,\beta}$, which on $X$-coordinates is given by

$$\psi(X) = (\phi_{\alpha,\beta}(X))^\tau = \left(\frac{-\beta^2}{9\alpha^2} \frac{3X^3 + \alpha^2X^2 + 3\alpha X + 3}{X^2}\right)^\tau. \tag{5.8}$$

The map $\psi$ is an endomorphism of $E_\alpha$ in characteristic 0 (but not a morphism!), since $\phi_{\alpha,\beta}$ is an isogeny from $E_\alpha$ to $E_\beta$, and $\tau$ maps $E_\beta$ back to $E_\alpha$ by $(X',Y')^\tau = (X'^\tau,Y'^\tau)$. (See [m4, Prop. 3.5].) It is easy to see that $\psi : E_\alpha[2] \to E_\alpha[2]$ is a permutation, since $ker(\psi) = \{O, (0,0), (0,-1)\}$.

Also, let $\mathfrak{P}$ be a prime divisor of $p$ in $L$ for which the decomposition group of $\mathfrak{P}/p$ is generated by $\tau$, possible because $Gal(L/\mathbb{Q}) \cong S_3$. Let $R_\mathfrak{P}$ denote the ring of $\mathfrak{P}$-adic integers contained in $L$. Since $R_\mathfrak{P}/\mathfrak{P} \cong \mathbb{F}_p^2$, for any $\gamma \in R_\mathfrak{P}$ we can write $\gamma \equiv a + b\sqrt{-11} \pmod{\mathfrak{P}}$ for suitable $a, b \in \mathbb{Z}_p \cap \mathbb{Q}$ (the ring of $p$-adic integers contained in $\mathbb{Q}$) and since $\mathfrak{P}^\tau = \mathfrak{P}$ we have

$$\gamma^\tau \equiv a - b\sqrt{-11} \equiv (a + b\sqrt{-11})^p \equiv \gamma^p \pmod{\mathfrak{P}}.$$

Therefore, it follows that

$$\psi(X) \equiv (\phi_{\alpha,\beta}(X))^p = X^{\mu_1} \pmod{\mathfrak{P}}, \quad X \in R_\mathfrak{P},$$

where $X^{\mu_1}$ is given by (5.2). Now if $x = X(P)$, for $P \in E_\alpha[2]$, is one of the roots of $f_2(x) = 0$, then

$$\psi^2(x) = (\phi_{\alpha,\beta}(\phi_{\alpha,\beta}(x)^\tau))^\tau = (\phi_{\beta,\alpha})(\phi_{\alpha,\beta}(x)^{\tau^2})$$

$$= (\phi_{\beta,\alpha} \circ \phi_{\alpha,\beta})(x) = X(3P) = X(P) = x, \tag{5.9}$$
where we have used the formulas in [m4, Props. 3.5 and 3.6]. This shows that $\psi^2 = 1$ on $E_\alpha[2]$. Therefore, $\psi$ has a fixed point, say $P_1 = (x_1, y_1)$. Then $\psi(x_1) = x_1$ implies that

$$\psi(x_1^\sigma) = \phi_{\alpha, \beta}(x_1^\sigma)^\tau = \phi_{\alpha, \beta}(x_1)^{\tau \sigma} = \psi(x_1)^{\sigma^{-1}} = x_1^{\sigma^{-1}}.$$ 

The roots $x_1, x_2 = x_1^\tau, x_3 = x_1^{\tau^{-1}}$ are distinct (mod $\Psi$), for $p > 3$, so this computation implies that $\mu_1$ is not the identity permutation on the points of order 2 of the reduced curve $\tilde{E}_\alpha = E_\alpha$ (mod $\Psi$).

The same argument as in Proposition 5.5 will prove the assertion, once we apply an appropriate isomorphism $\phi : \tilde{E}_\alpha \to \tilde{E}_\beta$ and demonstrate that the endomorphism $\mu_2 = \iota^{-1} \circ \nu \circ \phi_{\beta, \alpha} \circ \iota$ on $\tilde{E}_\alpha$ has a kernel which is different from $\text{ker}(\mu_1)$. But this follows easily, as in the proof of Proposition 5.5, from the fact that $\sigma_1(z) = 3(z + 6)/(z - 3)$ satisfies $\sigma_1(\alpha) = \beta$ and vice versa, and that $\gamma = (-1 + \sqrt{-11})/6$ is the $X$-coordinate of a point of order 3 on $\tilde{E}_\alpha$. (See [m4, Prop. 3.10].) Then an isomorphism $\iota : \tilde{E}_\alpha \to \tilde{E}_\beta$ exists for which $\iota(X, Y) = (X', Y')$ and

$$X' = X' = -\frac{\gamma'}{\gamma} X + \gamma' = -\gamma^{p-1} X + \gamma^p = \frac{5 - \sqrt{-11}}{6} X + \frac{-1 - \sqrt{-11}}{6},$$

Thus, the kernel of $\mu_2$ contains a point with $X$-coordinate $\gamma \neq 0$, and it follows that $\mu_2 \neq \pm \mu_1$. As in the earlier proof, the endomorphism $\mu'_2 = \nu \circ \phi_{\beta, \alpha}$ has the same behavior on $\tilde{E}_\beta[2]$ that $\mu_1$ has on $\tilde{E}_\alpha[2]$. Hence, $\mu_2$ is not the identity on $\tilde{E}_\alpha[2]$, so that no endomorphism of the form $\lambda(1 + \mu)/2$ with $\mu^2 = -3p$ exists in $\text{End}(\tilde{E}_\alpha)$. This completes the proof.

We turn now to the quadratic factors in Theorem 1.2.

**Proposition 5.7.** The factor $H_{-20}(t)^{2k_1}$ divides both $H_{-3p}(t)$ and $H_{-12p}(t)$ (mod $p$), for $p > 53$.

**Proof.** In this case we take $p$ to be a prime $\equiv 1 \pmod{4}$ with $(5/p) = -1$. We take $\alpha$ and $\beta$ to be

$$\alpha = \frac{-1 + 7\sqrt{-1} + \sqrt{5} + \sqrt{-5}}{2}, \quad \beta = \frac{-1 + 7\sqrt{-1} - \sqrt{5} - \sqrt{-5}}{2}.$$
Note that

\[ j(E_\alpha) = 632000 + 282880\sqrt{5} \]

is a root of \( H_{-20}(t) = t^2 - 1264000t - 681472000 \) and \( 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3 \) in characteristic 0. The \( X \)-coordinates of the points of order 2 on \( E_\alpha \) are the roots of the polynomial

\[ f_2(x, \alpha) = x^3 + \frac{1}{4}(\alpha x + 1)^2 \]

\[ = \left( x - \frac{3\sqrt{-1} - \sqrt{-5}}{4} \right) \left( x^2 + \frac{-6 + \sqrt{-1} - 2\sqrt{5} + \sqrt{-5}}{2} x + \frac{3 + \sqrt{-5}}{4} \right). \]

With \( \mu_1 = \nu \circ \phi_{\alpha, \beta} \) as in (5.2) and \( x_1 = (3\sqrt{-1} - \sqrt{-5})/4 \) we have \( x_1^{\mu_1} = x_1 \), which is obvious anyway because \( \mu_1 \) permutes the roots of \( f_2(x, \alpha) \) and \( x_1 \) is the only root which is rational over \( K = \mathbb{Q}(\sqrt{-1}, \sqrt{5}) \). We take \( x_2 \) to be a root of the quadratic in the above factorization of \( f_2(x, \alpha) \):

\[ x_2 = \frac{6 - \sqrt{-1} + 2\sqrt{5} - \sqrt{-5}}{4} + \frac{1}{2}\sqrt{\Delta}, \]

where

\[ \Delta = \frac{25 - 22\sqrt{-1} + 11\sqrt{5} - 10\sqrt{-5}}{2} = -(2\sqrt{-1} - \sqrt{5}) \left( \frac{1 + \sqrt{5}}{2} \right)^5. \]

Let \( L = \mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{\Delta}) \), and let \( \sigma \) denote complex conjugation and \( \tau \) the automorphism of \( K = \mathbb{Q}(\sqrt{-1}, \sqrt{5}) \) for which \( \tau(\sqrt{5}) = -\sqrt{5} \). Since

\[ \Delta\Delta^\tau = \text{Norm}_{\mathbb{Q}(\sqrt{-1})}(\Delta) = 9, \]

\[ \Delta\Delta^\sigma = \text{Norm}_{\mathbb{Q}(\sqrt{5})}(\Delta) = 9 \left( \frac{1 + \sqrt{5}}{2} \right)^{10}, \]

and

\[ \Delta\Delta^{\sigma\tau} = \text{Norm}_{\mathbb{Q}(\sqrt{-5})}(\Delta) = 1 - 4\sqrt{-5} = (2\sqrt{-1} - \sqrt{5})^2, \]

it is clear that \( L \) is normal over \( \mathbb{Q} \). Further, since \( 1 - 4\sqrt{-5} \) is not a square in \( \mathbb{Q}(\sqrt{-5}) \), it follows that \( \Delta \) is not a square in \( K = \mathbb{Q}(\sqrt{-1}, \sqrt{5}) \). Thus, \( [L : \mathbb{Q}] = 8. \) Setting
\[ \Delta' = \Delta^{\sigma \tau} = \overline{\Delta}, \quad \sqrt{\Delta'} = \frac{2\sqrt{-1} - \sqrt{5}}{\sqrt{\Delta}}, \]

we define the automorphism \( \rho \) on \( L \) by
\[ \rho : \sqrt{\Delta} \to \sqrt{\Delta'} = \frac{2\sqrt{-1} - \sqrt{5}}{\sqrt{\Delta}}, \]
and we extend the automorphisms \( \sigma \) and \( \tau \) to \( L \) by setting
\[ \sigma : \sqrt{\Delta} \to \sqrt{\Delta} = \frac{3\varepsilon^5}{\sqrt{\Delta}}, \quad \varepsilon = \frac{1 + \sqrt{5}}{2}, \]
\[ \tau : \sqrt{\Delta} \to \sqrt{\Delta} = \frac{3}{\sqrt{\Delta}}. \]

Then \( \rho|_K = (\sigma\tau)|_K \), so that \( \rho^2(\sqrt{\Delta}) = -\sqrt{\Delta} \). Hence, \( \rho \) has order 4 and \( L \) is cyclic over \( k_3 = \mathbb{Q}(\sqrt{-5}) \). It is easy to check that \( \sigma^2 = 1 \) and \( \sigma\rho = \rho^{-1}\sigma \), so \( \text{Gal}(L/\mathbb{Q}) \) is the dihedral group \( D_4 \). It is also straightforward to verify that
\[ \tau^2 = 1, \quad \tau\rho = \rho^{-1}\tau, \quad \sigma\tau = \tau\sigma\rho^2. \]

I claim now that \( p \) splits into four primes of degree 2 in \( L/\mathbb{Q} \). This follows from the fact that \( L \) is the 2-ray class field over \( k_3 = \mathbb{Q}(\sqrt{-5}) \), which is the case since the equation for \( E_{\alpha} \) is defined over the Hilbert class field \( K \) of \( k_3 \) and \( E_{\alpha} \) has complex multiplication by the ring of integers of \( k_3 \). The prime ideal \( (p) \) of \( k_3 \) lies in the principal ray class \((\mod 2)\), hence \( p \) splits completely in \( L/k_3 \). (This may also be shown directly. See the proof of Proposition 5.8 below.)

Now \( p \) also splits in \( k_2 = \mathbb{Q}(\sqrt{-1}) \), so \( k_2 \) is contained in the decomposition field of the prime divisors of \( p \) in \( L \). The invariant subgroup of \( k_2 \) in \( \text{Gal}(L/\mathbb{Q}) \) is \( < \rho^2, \tau > \). However, both prime divisors of \( p \) in \( K \) – the fixed field of \( < \rho^2 > \) – have degree 2, so the decomposition group of a prime divisor of \( p \) in \( L \) is either \( < \tau > \) or \( < \rho^2\tau > \). These two subgroups are conjugate in the whole group, so there is a prime divisor \( \mathfrak{p} \) of \( p \) in \( L \) whose decomposition group is generated by \( \tau \). As in the proof of Proposition 5.6 we have that \( X^\tau \equiv X^p \pmod{\mathfrak{p}} \) for \( X \in R_{\mathfrak{p}} \).

We now define \( \psi(X) = (\phi_{\alpha,\beta}(X))^\tau \), as in (5.8). Then a lengthy calculation shows that

38
\[ \psi(x_2) = (\phi_{\alpha, \beta}(x_2))^\tau \]
\[ = \left( \frac{6 - \sqrt{-1} - 2\sqrt{5} + \sqrt{-5}}{4} + \frac{-25 + 22\sqrt{-1} + 11\sqrt{5} - 10\sqrt{-5}}{12} \sqrt{\Delta} \right)^\tau \]
\[ = \frac{6 - \sqrt{-1} + 2\sqrt{5} - \sqrt{-5}}{4} + \frac{-25 + 22\sqrt{-1} - 11\sqrt{5} + 10\sqrt{-5}}{12} \frac{3}{\sqrt{\Delta}} \]
\[ = \frac{6 - \sqrt{-1} + 2\sqrt{5} - \sqrt{-5}}{4} - \frac{\Delta}{2} \frac{1}{\sqrt{\Delta}} \]
\[ = \frac{6 - \sqrt{-1} + 2\sqrt{5} - \sqrt{-5}}{4} - \frac{1}{2} \sqrt{\Delta} = x_3. \]

As in the proof of Proposition 5.6, it follows that \( x_2^{\mu_1} \equiv x_3 \pmod{\mathfrak{P}} \). The discriminant of \( f(x, \alpha) \) is

\[ \text{disc}_x(f(x, \alpha)) = -\frac{35}{16} - \frac{11}{4} \sqrt{-1} - \frac{7}{8} \sqrt{5} - \frac{11}{8} \sqrt{-5}, \]

whose norm to \( \mathbb{Q} \) is \( 3^{12}/2^{16} \), so the \( x_i \) are distinct modulo \( \mathfrak{P} \) for \( p > 3 \). Hence, the endomorphism \( \mu_1 \) is a non-trivial permutation on \( \tilde{E}_\alpha[2] = E_\alpha[2] \pmod{\mathfrak{P}} \). It follows that \( H_{-20}(t)^{2\mu_1} \) divides \( H_{-120}(t) \pmod{p} \).

In this case we know that \( E_\alpha \) and \( E_\beta \) are not isomorphic, because their \( j \)-invariants are conjugate over \( \mathbb{Q} \) but not equal. However, \( E_\alpha \cong E_{\alpha\sigma} \) since \( \sigma \) is complex conjugation and \( j(E_\alpha) \) is real. Thus a second endomorphism \( \mu_2 \) arises from an isomorphism \( \iota : E_\alpha \rightarrow E_{\alpha\sigma} \) by the formula (in characteristic \( p \))

\[ \mu_2 = \iota^{-1} \circ \nu' \circ \phi_{\alpha, \beta \sigma} \circ \iota = \iota^{-1} \circ \mu'_2 \circ \iota, \]

where \( \nu' : \tilde{E}_{\beta \sigma} \rightarrow \tilde{E}_{\alpha \sigma} \) is the Frobenius map. Here we have

\[ \alpha^\sigma = \frac{-1 - 7\sqrt{-1} + \sqrt{5} - \sqrt{-5}}{2}, \quad \beta^\sigma = \frac{-1 - 7\sqrt{-1} - \sqrt{5} + \sqrt{-5}}{2}. \]

Now (once again in characteristic 0) the roots of \( f_2(x, \alpha^\sigma) = 0 \) are \( x_i^\sigma \) (1 \( \leq i \leq 3 \)), which also lie in \( L \) since \( L \) is normal over \( \mathbb{Q} \). Setting
\[
\psi'(X) = (\phi_{\alpha^\sigma, \beta^\sigma}(X))^r
\]
we have
\[
\psi'(x_2^\sigma) = (\phi_{\alpha^\sigma, \beta^\sigma}(x_2^\sigma))^r = (\phi_{\alpha, \beta}(x_2))^{\sigma^r} = (\phi_{\alpha, \beta}(x_2))^{\sigma^r\sigma^2}
\]
\[
= (\phi_{\alpha, \beta}(x_2)^r)^{\sigma^r} = \psi(x_2)^{\sigma^r} = x_3^\sigma = x_2^\sigma,
\]
by the previous calculation, using the fact that \(\rho^2\) is in the center of \(\text{Gal}(L/\mathbb{Q})\). In the same way, \(\psi'\) also fixes \(x_3^\sigma\) and \(x_1^\sigma\). Now the congruence \(\psi'(X) \equiv X^{\mu_2} \pmod{\mathfrak{P}}\) implies that \(\mu'_2\) is the identity permutation on \(\tilde{E}_{\alpha^r}[2]\) (in characteristic \(p\)), so \(\mu_2\) is the identity on \(\tilde{E}_\alpha[2]\). Hence, \(H_{-20}(t)^{2\lambda_1}\) also divides \(H_{-3p}(t) \pmod{p}\). This proves the proposition. \(\square\)

There is a similar result for the factor \(H_{-32}(t)\) in Theorem 1.2.

**Proposition 5.8.** The factor \(H_{-32}(t)^{2\lambda_5}\) divides both \(H_{-3p}(t)\) and \(H_{-12p}(t) \pmod{p}\), for \(p > 53\).

**Proof.** In this case we take \(p\) to be a prime \(\equiv 5 \pmod{8}\) so that \((2/p) = -1\). We take \(\alpha\) and \(\beta\) to be
\[
\alpha = \frac{4 + 2\sqrt{-1} + 5\sqrt{2} + 5\sqrt{-2}}{2}, \quad \beta = \frac{4 + 2\sqrt{-1} - 5\sqrt{2} - 5\sqrt{-2}}{2},
\]
so that
\[
\tilde{j}(\tilde{E}_\alpha) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} = 26125000 + 18473000\sqrt{2}
\]
is a root of \(H_{-32}(t)\). The corresponding polynomial \(f_2(x, \alpha)\) is
\[
f_2(x, \alpha) = x^3 + \frac{1}{4}(\alpha x + 1)^2 = \left(x - \frac{1 - \sqrt{-1} - \sqrt{2} + \sqrt{-2}}{4}\right)
\]
\[
\times \left(x^2 + (1 + 7\sqrt{-1} + \sqrt{2} + 4\sqrt{-2})x + \frac{1 + \sqrt{-1} + \sqrt{2} + \sqrt{-2}}{2}\right),
\]
where the discriminant of the quadratic factor is
\[
4\Delta = 4(-20 + 7\sqrt{-1} - 14\sqrt{2} + 5\sqrt{-2}) = 4(\sqrt{-1} - 2\sqrt{2})(1 + \sqrt{2})^3.
\]
Letting $\sigma$ be complex conjugation on the field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and $\tau$ the automorphism taking $\sqrt{2}$ to $-\sqrt{2}$, we have the norm equations

$$\Delta \Delta^\tau = \text{Norm}_{\mathbb{Q}(\sqrt{-1})}(\Delta) = 9,$$

$$\Delta \Delta^\sigma = \text{Norm}_{\mathbb{Q}(\sqrt{2})}(\Delta) = 9(1 + \sqrt{2})^6,$$

and

$$\Delta \Delta^{\sigma \tau} = \text{Norm}_{\mathbb{Q}(\sqrt{-2})}(\Delta) = 7 - 4\sqrt{-2} = (\sqrt{-1} - 2\sqrt{2})^2.$$

Further, a root $x_2$ of the quadratic factor of $f(x, \alpha)$ is

$$x_2 = -\frac{1 + 7\sqrt{-1} + \sqrt{2} + 4\sqrt{-2}}{2} + \sqrt{\Delta},$$

and $x_2, x_3 \in L = \mathbb{Q}(\sqrt{\Delta})$, where $L$ is normal over $\mathbb{Q}$ with degree 8. As before we define $\rho \in \text{Gal}(L/\mathbb{Q})$ by

$$\rho : \sqrt{\Delta} \rightarrow \sqrt{\Delta}^\rho = \frac{\sqrt{-1} - 2\sqrt{2}}{\sqrt{\Delta}},$$

and we extend the automorphisms $\sigma$ and $\tau$ to $L$ by setting

$$\sigma : \sqrt{\Delta} \rightarrow \sqrt{\Delta} = \frac{3\varepsilon^3}{\sqrt{\Delta}}, \quad \varepsilon = 1 + \sqrt{2},$$

$$\tau : \sqrt{\Delta} \rightarrow \sqrt{\Delta^\tau} = \frac{3}{\sqrt{\Delta}}.$$

These automorphisms satisfy all the same relations as in the proof of Proposition 5.7. Now we compute

$$\psi(x_2) = \phi_{\alpha, \beta}(x_2)^\tau$$

$$= \left(\frac{-1 - 7\sqrt{-1} + \sqrt{2} + 4\sqrt{-2}}{2} + \frac{-20 + 7\sqrt{-1} + 14\sqrt{2} - 5\sqrt{-2}}{3}\sqrt{\Delta}\right)^\tau$$

41
\[
\frac{-1 - 7\sqrt{-1} - \sqrt{2} - 4\sqrt{-2}}{2} + \frac{-20 + 7\sqrt{-1} - 14\sqrt{2} + 5\sqrt{-2}}{3} \frac{3}{\sqrt{\Delta}} = -\frac{1 + 7\sqrt{-1} + \sqrt{2} + 4\sqrt{-2}}{2} + \sqrt{\Delta} = x_2.
\]

Also, setting \(\psi'(X) = (\phi_{\alpha^\sigma, \beta^\sigma}(X))^\tau\), we have

\[
\psi'(x_2^\sigma) = (\phi_{\alpha^\sigma, \beta^\sigma}(x_2)) = (\phi_{\alpha^\sigma, \beta^\sigma}(x_2))^\sigma = (\phi_{\alpha^\sigma, \beta^\sigma}(x_2))^\sigma = \psi(x_2)^{\sigma^2} = x_3^\sigma.
\]

These computations will imply the assertion of the proposition, if we show that there is a prime divisor \( \mathfrak{P} \) of \( p \) in \( L \) with degree 2, whose decomposition group is \( < \tau > \). For this we need only show that \( p \) splits into four primes of degree 2 in \( L \). Note in this case that \( K = \mathbb{Q}(\sqrt{-1}, \sqrt{2}) \) is not the Hilbert class field, but the 2-ray class field over \( k = \mathbb{Q}(\sqrt{-2}) \), so we cannot use \([s, \text{Thm. 5.6, p.135}]\) here. Instead, we must argue directly. Since \( p \) splits into two primes \( p_1 \) and \( p_2 \) of degree 2 in the field \( K \), it will suffice to compute the Legendre symbol

\[
\left( \frac{\Delta}{p_1} \right) = \left( \frac{(-1 - 2\sqrt{2})(1 + \sqrt{2})}{p_1} \right)
\]

\( \equiv (-1 - 2\sqrt{2})^{(p^2 - 1)/2}(1 + \sqrt{2})^{(p^2 - 1)/2} \text{ (mod } p_1). \)

Working with the first factor (mod \( p_1 \)) gives

\[
(-1 - 2\sqrt{2})^{(p^2 - 1)/2} \equiv \left( \frac{(-1 - 2\sqrt{2})^p}{(-1 - 2\sqrt{2})^p} \right)^{(p+1)/2} \equiv \left( \frac{(-1 + 2\sqrt{2})^2}{-9} \right)^{(p+1)/2}
\]

\( \equiv (-1)^{(p+1)/2} \left( \frac{\sqrt{-1} + 2\sqrt{2}}{3} \right)^{p+1} \equiv (-1)^{(p+1)/2}(-1) \equiv 1 \text{ (mod } p_1). \)

In the same way we obtain

\( (1 + \sqrt{2})^{(p^2 - 1)/2} \equiv (-1)^{(p+1)/2}(-1) \equiv 1 \text{ (mod } p_1), \)

42
and therefore \( \left( \frac{\Delta}{\mathfrak{p}_1} \right) = 1 \), as claimed. Conjugating by \( \sigma \) gives \( \left( \frac{\Delta}{\mathfrak{p}_2} \right) = 1 \), and therefore both \( \mathfrak{p}_i \) split into two primes in \( L/K \).

Now the same argument as in Proposition 5.7 shows that there is a prime divisor \( \mathfrak{p} \) of \( p \) in \( L \) whose decomposition group is \( < \tau > \), and this gives the assertion by the same arguments as before. \( \square \)

After the last two propositions, the result of our final proposition is similar to Proposition 5.6.

Proposition 5.9. The factor \( H_{-35}(t)^{4k} \) divides \( H_{-12p}(t) \mod p \), for \( p > 53 \).

Proof. Here \( p \) is a prime \( \equiv 1 \mod 4 \) for which \( (-35/p) = -1 \) and \( (5/p) = -1 \), so that \( (-7/p) = +1 \). We take \( \alpha \) and \( \beta \) to be

\[
\alpha = 3 + \sqrt{-7} + 2\sqrt{5}, \quad \beta = 3 + \sqrt{-7} - 2\sqrt{5}.
\]

Then \( (\alpha, \beta) \) is a point on \( Fer_3 \), as before, and

\[
j(E_\alpha) = -58982400 - 26378240\sqrt{5}
\]

is a root of \( H_{-35}(t) \). The polynomial

\[
f_2(x, \alpha) = x^3 + \frac{1}{4}(\alpha x + 1)^2
\]

has discriminant

\[
D = \frac{117}{16} + 5\sqrt{-7} + \frac{13}{4}\sqrt{5} + \frac{9}{4}\sqrt{-35} = \left( 1 + \frac{\sqrt{5}}{2} \right)^2 \left( \frac{\sqrt{-7} + 2\sqrt{5}}{2} \right)^2.
\]

The norm of \( f_2(x, \alpha) \) to \( \mathbb{Q} \) is the irreducible polynomial

\[
h(x) = x^{12} + 22x^{11} + 199x^{10} - 407x^9 + \frac{1259}{2}x^8 - 295x^7 + \frac{1275}{8}x^6 + \frac{409}{8}x^5
\]

\[
+ \frac{67}{16}x^4 + \frac{37}{16}x^3 + \frac{25}{32}x^2 + \frac{3}{32}x + \frac{1}{256},
\]

whose splitting field is the 2-ray class field \( L \) over \( \mathbb{Q}(\sqrt{-35}) \). We have \( [L : \mathbb{Q}] = 12 \), so that \( h(x) \) is a normal polynomial. Furthermore, \( G = Gal(L/\mathbb{Q}) = D_6 \), the dihedral
group of order 12, by a standard result in the theory of complex multiplication. In particular, \( H = \text{Gal}(L/Q(\sqrt{-35})) \) is cyclic and every element in \( G \) which does not fix \( Q(\sqrt{-35}) \) has order 2.

We take \( \sigma \in G \) to be complex conjugation and \( \tau \) an automorphism which fixes \( \sqrt{-7} \) and changes the sign of \( \sqrt{5} \). Also, let \( \rho \) be a generator of \( H \). Then \( \sigma \tau = \rho^l \), for some \( l \), since \( \sigma \tau \) fixes \( \sqrt{-35} \), and \( \rho^2 \) generates the group of the cyclic extension \( L/K \), where \( K = Q(\sqrt{-7}, \sqrt{5}) \). The automorphism \( \tau \) is defined only up to a factor of \( \rho^{2n} \). Hence we may assume \( l = 0 \) or 1.

As in previous proofs we let \( \psi(X) = (\phi_{\alpha, \beta}(X))^\tau \). The computation analogous to (5.9) shows that \( \psi^2(x) = x \) for the roots of \( f_2(x, \alpha) = 0 \), so \( \psi \) has a fixed point \( x_1 \). If \( x_2 = x_1^{\rho^2} \) and \( x_3 = x_1^{\rho^4} \), then

\[
\psi(x_2) = \psi(x_1^{\rho^2}) = \phi_{\alpha, \beta}(x_1)^{\rho^2 \tau} = \phi_{\alpha, \beta}(x_1)^{\tau \rho^4} = \psi(x_1)^{\rho^4} = x_1^{\rho^4} = x_3.
\]

Hence, \( \psi \) is not the identity on \( E_\alpha[2] \). If \( \psi'(X) = (\phi_{\alpha^\sigma, \beta^\sigma}(X))^\tau \), then

\[
\psi'(x_2) = (\phi_{\alpha^\sigma, \beta^\sigma}(x_2)^\tau) = (\phi_{\alpha, \beta}(x_2))^\sigma \tau = (\phi_{\alpha, \beta}(x_2))^{\rho^l} = (\phi_{\alpha, \beta}(x_2)^\tau)^{\tau \rho^l} = \psi(x_2)^{\tau \rho^l} = x_2^{\rho^2 \tau \rho^l} = (x_2^\sigma)^{\rho^2 \tau \rho^l} = (x_2^\sigma)^{\rho^{2l-2}}.
\]

Similarly, \( \psi'(x_1^\sigma) = (x_1^\sigma)^{\rho^{2l}} \) and \( \psi'(x_3^\sigma) = (x_3^\sigma)^{\rho^{2l+2}} \). If \( l = 0 \), then \( \psi' \) fixes \( x_1^\sigma \) and interchanges \( x_2^\sigma \) and \( x_3^\sigma \); while if \( l = 1 \), \( \psi' \) fixes \( x_2^\sigma \) and interchanges \( x_1^\sigma \) and \( x_3^\sigma \). In either case, \( \psi' \) is not the identity on \( E_{\alpha^\sigma}[2] \).

Since \( L \) is the 2-ray class field of \( k_1 = Q(\sqrt{-35}) \), the prime \( p \) splits into six primes \( \mathfrak{P}_i \) of degree 2 in \( L \). But \( p \) splits in \( k_2 = Q(\sqrt{-7}) \), so \( k_2 \) is contained in the decomposition field of any of the primes \( \mathfrak{P}_i \). The invariant group of \( k_2 \) inside \( \text{Gal}(L/Q) \) is \( < \tau, \rho^2 \rangle \cong S_3 \). The decomposition group of any \( \mathfrak{P}_i \) is generated by an element of order 2, all of which are conjugate inside \( < \tau, \rho^2 \rangle \), so there is a prime divisor \( \mathfrak{P} \) of \( p \) whose decomposition group is generated by \( \tau \).

Thus, all our previous arguments apply, namely \( X^\tau \equiv X^p \pmod{\mathfrak{P}} \), so the endomorphism \( \mu_1 \) is given on \( X \)-coordinates of points in \( E_\alpha = E_\alpha \pmod{\mathfrak{P}} \) by

\[
X^{\mu_1} \equiv \psi(X) \pmod{\mathfrak{P}}, \quad (X, Y) \in E_\alpha,
\]

44
and the endomorphism $\mu'_2$ on points of $\tilde{E}_{\alpha^\sigma}$ by

$$X^{\mu'_2} \equiv \psi'(X) \pmod{\mathfrak{P}} \quad (X, Y) \in E^\sigma.$$ 

Finally, the endomorphism $\mu_2$ on $\tilde{E}_{\alpha}$ is determined by an isomorphism $\iota : \tilde{E}_{\alpha} \to \tilde{E}_{\alpha^\sigma}$ as

$$\mu_2 = \iota^{-1} \circ \mu'_2 \circ \iota.$$ 

As in (5.7), it is easily checked that we may take $\iota$ to be defined on $X$-coordinates by

$$X' = X'' = -\frac{\gamma'}{\gamma} X + \gamma' = -\gamma^{p-1} X + \gamma^p,$$

where

$$\gamma = \frac{5}{12} + \frac{1}{4}\sqrt{7} - \frac{1}{4}\sqrt{5} - \frac{1}{12}\sqrt{-35} = \frac{1}{12}(3 - \sqrt{5})(\sqrt{-7} - \sqrt{5})$$

is the $X$-coordinate of a point of order 3 on $\tilde{E}_{\alpha}$. It follows from this that the points of order 3 given by $(\gamma, \xi)$ are in $\ker(\mu_2)$ and therefore $\ker(\mu_2) \neq \ker(\mu_1)$. Hence, $\mu_1$ and $\mu_2$ are two independent endomorphisms of $\tilde{E}_{\alpha}$ in characteristic $p$ with $\mu_1^2 = -3p$, neither of which is the trivial permutation on $\tilde{E}_{\alpha}[2]$. This proves the proposition. □

Taken together, Lemma 5.2 and Propositions 5.3-5.9 imply Theorem 1.5. As a corollary we have the following analogy to Theorems 3.2 and 3.4.

**Theorem 5.10.** For $p \equiv 1 \pmod{4}$ and $p > 53$ let $n_{3,1}$ denote the number of irreducible quadratic factors $t^2 + at + b$ of $J_p(t)$ distinct from $H_{-20}(t)$, $H_{-32}(t)$, and $H_{-35}(t) \pmod{p}$ which divide $H_{-3p}(t) \pmod{p}$, and $n_{3,2}$ the number of those factors which divide $H_{-12p}(t) \pmod{p}$. Then the class number $h(-3p)$ satisfies the following two equations:

$$h(-3p) = 7 - 4\left(\frac{2}{p}\right) - \left(\frac{3}{p}\right) - 2\left(\frac{5}{p}\right) + 4n_{3,1},$$

$$(a_p - 1)h(-3p) = 9 - 2\left(\frac{2}{p}\right) - \left(\frac{3}{p}\right) - 4\left(\frac{5}{p}\right) + 2\left(\frac{7}{p}\right) - 2\left(\frac{11}{p}\right) - 2\left(\frac{35}{p}\right) + 4n_{3,2},$$

with

$$a_p - 1 = 2 + \left(\frac{2}{p}\right).$$
Thus, we have
\[ n_{3,2} = \left( 2 + \left( \frac{2}{p} \right) \right) n_{3,1} + \eta_p, \]
with
\[ \eta_p = \frac{1}{4} \left( 1 + \left( \frac{2}{p} \right) - \left( \frac{3}{p} \right) - \left( \frac{6}{p} \right) - 2 \left( \frac{7}{p} \right) - 2 \left( \frac{10}{p} \right) + 2 \left( \frac{11}{p} \right) + 2 \left( \frac{35}{p} \right) \right). \]

**Proof.** This follows from equating degrees in the two congruences in Theorem 1.5:

\[ h(-3p) = 2\delta_1 + 4\delta_2 + 4\delta_4 + 4\delta_5 + 4n_{3,1}, \]
\[ (a_p - 1)h(-3p) = 2\delta_1 + 4\delta_3 + 4\delta_4 + 4\delta_5 + 8\delta_6 + 4n_{3,2}, \]
and then subtracting the second equation from \((a_p - 1)\) times the first. \(\Box\)

Adding the two equations in this theorem and comparing with Theorem 3.4 gives the following.

**Corollary.** If \(p > 53\) satisfies \(p \equiv 1 \pmod{4}\), then

\[ n_{3,1} + n_{3,2} = N_3 + \frac{1}{4} \left( -5 + 2 \left( \frac{2}{p} \right) + 3 \left( \frac{5}{p} \right) - \left( \frac{7}{p} \right) + \left( \frac{35}{p} \right) \right), \]

where \(N_3\) is the number of irreducible quadratic factors \(t^2 + ct + d\) of \(J_p(t)\) over \(\mathbb{F}_p\) for which \(Q_3(c, d) \equiv 0 \pmod{p}\). (See Theorems 1.2 and 3.4.) \(\Box\)

Theorem 5.10 and its corollary give the means for determining the numbers of irreducible quadratic factors in the two products in Theorem 1.5. For example, when \(p = 233\), the formulas in Theorem 5.10 give that \(n_{3,1} = 1\) and \(n_{3,2} = 3\), using that \(h(-3 \cdot 233) = 10\) and \(a_{233} = 4\). This agrees with the formula in the corollary since \(N_3 = 6\) (see Section 3). Note that these formulas also make it possible to determine these numbers directly from the factorization of \(J_p(t)\).

Thus we have:

\[ H_{-3,233}(t) \equiv (t - 54000)^2 H_{-20}(t)^2 (t^2 + c_1 t + d_1)^2 \]
\[ \equiv (t + 56)^2 (t^2 + 25t + 109)^2 (t^2 + c_1 t + d_1)^2 \pmod{233}, \]

46
and

\[ H_{-12,233}(t) \equiv t^2(t+32768)^4 H_{-20}(t)^2 H_{-35}(t) \prod_{i=2}^{4} (t^2 + c_it + d_i)^2 \]

\[ \equiv t^2(t + 148)^4(t^2 + 25t + 109)^2(t^2 + 162t + 216)^4 \prod_{i=2}^{4} (t^2 + c_it + d_i)^2 \pmod{233}. \]

To determine exactly which factors \( t^2 + ct + d \) of \( J_p(t) \) with \( Q_3(c, d) \equiv 0 \pmod{p} \) divide \( H_{-3p}(t) \pmod{p} \) one can proceed as in the above proofs. To a root \( j \) of each factor \( t^2 + ct + d \) there are values of \( \alpha \) and \( \beta = \alpha^p \) in \( \mathbb{F}_p^2 \) for which

\[ j = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}, \quad 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3. \]

Then \( t^2 + ct + d \) will divide \( H_{-3p}(t) \) if and only if the endomorphism \( \mu \) given by (5.2) or (5.5) is the trivial permutation on the \( X \)-coordinates of points in \( E_{\alpha}[2] \). By the arguments in [m4, pp. 273-274] there is only one independent endomorphism \( \mu \) in \( \text{End}(E_{\alpha}) \) for which \( \mu^2 = -3p \), so there is no need to construct additional isomorphisms as in the proofs above.

Considering the quadratic factors of \( J_{233}(t) \) given after Theorem 3.2, we check that \( q(t) = (t^2 + c_1t + d_1) = (t^2 + 81t + 81) \) divides \( H_{-3,233}(t) \pmod{233} \). We take

\[ \alpha = 115 + \sqrt{-5}, \quad \beta = 115 - \sqrt{-5} \in \mathbb{F}_{233^2}, \]

so that \( (\alpha, \beta) \) is a point on \( Fer_3 \) over \( \mathbb{F}_{233^2} \), and \( j(E_{\alpha}) = 76 + 155\sqrt{-5} \) is a root of \( q(t) \). Then the roots of \( f_2(x, \alpha) = x^3 + (\alpha x + 1)^2/4 \) are

\[ x_1 = 78 - 34\sqrt{-5}, \quad x_2 = 75 - 109\sqrt{-5}, \quad x_3 = 37 - 31\sqrt{-5} \]

in \( \mathbb{F}_{233^2} \). Using (5.5) one can check easily that \( x_i^\mu = x_i \) for all of these values. Hence \( q(t) \) certainly divides \( H_{-3,233}(t) \pmod{233} \), and we have finally that

\[ H_{-3,233}(t) \equiv (t + 56)^2(t^2 + 25t + 109)^2(t^2 + 81t + 81)^2, \]

\[ H_{-12,233}(t) \equiv t^2(t + 148)^4(t^2 + 25t + 109)^2(t^2 + 162t + 216)^4 \times (t^2 + 55t + 139)^2(t^2 + 147t + 62)^2(t^2 + 169t + 171)^2 \pmod{233}. \]
To conclude, we note the following corollary of Theorems 1.1 and Theorem 1.5.

**Theorem 5.11.** a) If $p > 13$ is a prime with $p \equiv 1 \pmod{8}$ and $(7/p) = +1$, then $H_{-8p}(t)$ has no linear factors over $\mathbb{F}_p$.

b) If $p > 53$ is a prime with $p \equiv 1 \pmod{24}$, then $H_{-3p}(t)$ has no linear factors over $\mathbb{F}_p$.

c) If $p > 53$ is a prime with $p \equiv 1 \pmod{12}$ and $\left(\frac{11}{p}\right) = +1$, then $H_{-12p}(t)$ has no linear factors over $\mathbb{F}_p$.

6 Appendix: Computing the modular equation $\Phi_n(t, j)$.

The algorithm for computing $\Phi_n(t, j)$ which we present here is based on the following proposition. See [m2] for the proof.

**Proposition A.1.** Let $K_1 = k(x, y)$ be an elliptic function field, where $x, y$ satisfy an equation

$$E_1: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

with $a_i \in k$. Let $K_2$ be a subfield of $K_1$ of finite index $m = [K_1 : K_2]$ containing $k$, which is also elliptic, and assume $K_1/K_2$ is separable. Then the elements

$$u = \text{Trace}_{K_1/K_2}(x) \text{ and } v = \text{Trace}_{K_1/K_2}(y)$$

satisfy a Weierstrass equation

$$E_2: v^2 + d_1 uv + d_3 v = u^3 + d_2 u^2 + d_4 u + d_6,$$

and generate $K_2$ over $k$. Furthermore, $d_1 = a_1$ and $d_3 = ma_3$.

The following method for computing $\Phi_n(t, j)$ does not require approximate calculations, and can be used to compute $\Phi_n(t, j)$ over $\mathbb{F}_p$ without first computing it over $\mathbb{Z}$.

If $n \geq 4$ we start with the Tate normal form
\[ E_1 : Y^2 + aXY + bY = X^3 + bX^2. \]  

(A.1)

As is well-known [hus], the point \((X, Y) = (0, 0) = P\) is a point of order \(n\) on \(E_1\) as long as \(a\) and \(b\) satisfy a certain relation \(f_n(a, b) = 0\). The first step is to compute this relation for a given \(n\). Also compute the \(j\)-invariant \(j(E_1)\) in terms of \(a\) and \(b\).

Next, we compute the curve \(E_2\) in the following way. If \(F = k(a, b)\) and \(K_1 = F(x, y)\) is a function field for \(E_1\), where \((X, Y) = (x, y)\) satisfies (A.1), then let \(K_2\) be the fixed field in \(K_1\) of the group generated by the translation \(\tau = \tau_{O \rightarrow P}\) which takes a given point \(Q\) to the point \(Q - P\). This map is given explicitly as \((x^\tau, y^\tau) = (x, y) + (0, 0)\), where the addition is performed on the curve, or

\[ x^\tau = \frac{-by}{x^2}, \quad y^\tau = \frac{b^2(x^2 - y)}{x^3}. \]

By Proposition A.1, \(K_2 = F(u, v)\) where \(u = tr(x)\) and \(v = tr(y)\) are traces from \(K_1\) to \(K_2\). We iterate the map \(\tau\) and form the sums \(u = \sum x^\tau_i\) and \(v = \sum y^\tau_i\), running from \(i = 0\) to \(i = n - 1\) \((\tau^n = 1)\); and we express the results in the form \(A(x) + B(x)y\) with rational functions \(A(x), B(x)\).

Then we use these expressions for \(u\) and \(v\) in terms of \(x\) and \(y\) to compute the relation

\[ v^2 + auv + nbv = u^3 + d_2u^2 + d_4u + d_6, \]

according to the result of Proposition A.1. The curve \(E_2\) is then given by

\[ E_2 : V^2 + aUV + nbV = U^3 + d_2U^2 + d_4U + d_6. \]

The coefficients \(d_i\) will be rational expressions in \(a\) and \(b\). Now compute \(j(E_2)\). Since \(K_1\) is a cyclic extension of \(K_2\) of degree \(n\), we have that

\[ \Phi_n(j(E_2), j(E_1)) = 0 \quad \text{over} \quad k. \]  

(A.2)

This shows that \(\Phi_n(t, j) = 0\) is parametrized by functions on the curve \(f_n(a, b) = 0\). When the Euler function \(\phi(n) > 2\), this parametrization can be simplified, since the curve \(f_n(a, b) = 0\) has a group of \(\phi(n)/2\) automorphisms which fix \(j(E_1)\) and \(j(E_2)\), by the discussion in [m2, section 4]. See Example 3 below.
If \( j(E_1) = A/B \) and \( j(E_2) = C/D \), where \( A, B, C, D \in k[a,b] \), then using the fact that \( E_1 \) is in Tate normal form we can say:

**Proposition A.2** A point \((t, j)\) over the algebraic closure \( \bar{k} \) of \( k \) lies on \( \Phi_n(t, j) = 0 \) if and only if there are \( a, b \in \bar{k} \) for which \( B(a, b)D(a, b) \neq 0 \) (equivalently \( \Delta(E_1)\Delta(E_2) \neq 0 \)) and

\[
A(a, b) - jB(a, b) = C(a, b) - tD(a, b) = f_n(a, b) = 0.
\] (A.3)

In other words, the affine curve \( \Phi_n(t, j) = 0 \) is the projection of the open algebraic set \( \mathcal{V} \) defined by (A.3) and \( B(a, b)D(a, b) \neq 0 \) onto the set of its \((t, j)\) coordinates.

The final step of the algorithm is to compute the polynomial \( n(t, j) \) as the minimal polynomial of \( t = j(E_2) \) over the field \( k(j(E_1)) \subseteq F \), by writing \( t^{deg\Phi_n} = j(E_2)^{deg\Phi_n} \) as a polynomial in lower powers of \( t \) with coefficients in \( k[j] \). For example, when \( n \) is prime, we can express \( t^{n+1} \) as a linear combination of \( 1, t, ..., t^n \) with coefficients in \( k[j] \) of degree at most \( n+1 \) in \( j \). (In fact, all coefficients but the constant term will have degree \( \leq n \) in \( j \), in accordance with the fact that \( \Phi_n(t, j) = \Phi_n(j, t) \).)

Whenever the curve \( f_n(a, b) = 0 \) is rational over \( k \), one can find \( \Phi_n(t, j) \) as follows: let \( F = k(a, b) = k(z) \) and write the two \( j \)-invariants as \( j(E_1) = A/B \) and \( j(E_2) = C/D \), where \( A, B, C, D \in k[z] \) and \( (A(z), B(z)) = (C(z), D(z)) = 1 \). Then let \( j \) and \( t \) be indeterminates and compute the resultant

\[
R = \text{Resultant}_z(A(z) - jB(z), C(z) - tD(z)).
\]

An elementary argument using Proposition A.2 shows that \( R = \text{constant} \cdot \Phi_n(t, j)^m \), for some \( m \).

In the general case, one may first compute the minimal polynomials \( S(j, b) = \text{minpoly}_{k(b)}(j) \) and \( T(t, b) = \text{minpoly}_{k(b)}(t) \) of \( j = j(E_1) \) and \( t = j(E_2) \) over \( k(b) \). These polynomials have degrees which are divisors of the integer \( d = [k(a, b) : k(b)] = \text{deg}_{a} f_n(a, b) \). Then \( R = \text{Resultant}_{b}(S(j, b), T(t, b)) \) will be divisible by \( \Phi_n(t, j) \), and \( \Phi_n(t, j) \) can be determined as the factor for which (A.2) holds identically.

**Example 1.** If \( n = 3 \), we start with the curve
\[ E_1 : Y^2 + \alpha XY + Y = X^3 \]

with \( j(E_1) = \alpha^3(\alpha^3 - 24)^3/(\alpha^3 - 27) \). On this curve we have \((x, y)^\tau = (x, y) + (0, 0)\), where

\[
x^\tau = \frac{-y}{x^2}, \quad y^\tau = \frac{-y}{x^3}.
\]

This leads to the expressions

\[
u = \text{trace}_{K_1/K_2}(x) = \frac{x^3 + \alpha x + 1}{x^2},
\]

\[
v = \text{trace}_{K_1/K_2}(y) = \frac{y(x^3 - 1) - (1 + \alpha x + y)^2}{x^3},
\]

which satisfy the equation of the 3-isogenous curve

\[ E_2 : V^2 + \alpha UV + 3V = U^3 - 6\alpha U - \alpha^3 - 9. \]

This curve has \( j(E_2) = \alpha^3(\alpha^3 + 216)^3/(\alpha^3 - 27)^3 \). To make the computations easier we replace \( \alpha^3 \) by \( z \), so that

\[
j(E_1) = \frac{z(z - 24)^3}{z - 27} = \frac{A(z)}{B(z)}, \quad j(E_2) = \frac{z(z + 216)^3}{(z - 27)^3} = \frac{C(z)}{D(z)}, \quad z = \alpha^3.
\]

Now we use Maple to compute the resultant

\[
\text{Resultant}_z(A(z) - jB(z), C(z) - tD(z)) =
\]

\[
3^{18} \cdot \{t^4 + (-j^3 + 2232j^2 - 1069956j + 36864000)t^3 + (2232j^3 + 2587918086j^2 + 8900222976000j + 452984832000000)t^2 + (-1069956j^3 + 8900222976000j^2 - 770845966336000000j + 1855425871872000000000)j + 18554258718720000000000\}
\]

51
\[ + j^4 + 36864000j^3 + 45298432000000j^2 + 185542587187200000000j \}

\[ = 3^{18} \cdot \Phi_3(t, j). \]

One can check that this equals the expression given for \( \Phi_3(t, j) \) in Section 2.

**Example 2.** \( n = 2 \). We work with the Tate normal form for \( n = 4 \):

\[ E_1 : Y^2 + XY + bY = X^3 + bX^2, \]

for which

\[ j(E_1) = \frac{(1 - 16b + 16b^2)^3}{b^4(1 - 16b)}. \]

In order to compute \( \Phi_2(t, j) \) we find the fixed field \( F(u, v) \) inside \( K = F(x, y) \) of the mapping \( \tau^2 \), which is given by

\[ (x^{\tau^2}, y^{\tau^2}) = \left(-\frac{b(x^2 - y)x}{y^2}, \frac{b(-y^2 + x^3 - xy)x^2}{y^3}\right). \]

The quantities \( u = x + x^{\tau^2} \) and \( v = y + y^{\tau^2} \) satisfy the equation of the curve

\[ E_2 : V^2 + UV + 2bV = U^3 + 4bU^2 - b^2, \]

with \( j \)-invariant

\[ j(E_2) = \frac{(1 - 16b + 256b^2)^3}{b^2(16b - 1)^2}. \]

Now we find

\[
\text{Resultant}_b((1 - 16b + 16b^2)^3 - jb^4(1 - 16b), (1 - 16b + 256b^2)^3 - tb^2(16b - 1)^2) \\
= 2^{48} \cdot (t^3 - 162000t^2 + 8748000000t - 15746400000000 + 1488jt^2 \\
+ 40773375jt + 8748000000j - j^2t^2 + 1488jt^2j - 162000j^2 + j^3)^2 \\
= 2^{48} \cdot \Phi_2(t, j)^2.
\]

It is clear that this method, when computed over \( k = \mathbb{F}_p \) and combined with Lemma 2.3 and (1.1), gives an algorithm for computing \( K_{pd}(t) \) (mod \( p \)). For the computation of \( H_D(t) \) (mod \( p \)) for a prime \( p \) not dividing \( D \), see [alv].

52
Example 3. \( n = 5 \). The Tate normal form for \( n = 5 \) is

\[
E_1 : Y^2 + (1 + b)XY + bY = X^3 + bX^2,
\]

with

\[
j(E_1) = \frac{(1 - 12b + 14b^2 + 12b^3 + b^4)^3}{b^5(1 - 11b - b^2)}.
\]

In this case we have the relation \( f_5(a, b) = a - (1 + b) \). (See [m2] or [hus, p. 94].) By iterating the map \( \tau \) we find that

\[
u = \sum_{i=0}^{4} x^{i+1} = \frac{b^4 + (3b^3 + b^4)x + (3b^2 + b^3)x^2 + (b - b^2 - b^3)x^3 + x^5}{x^2(x + b)^2}
\]

and

\[
v = \sum_{i=0}^{n-1} y^{i+1} = \frac{-1}{x^3(x + b)^3}\left\{(b - b^2)x^6 + (-b^4 - 2b^3 + 6b^2 + b)x^5 + (b^4 + 13b^3 + 5b^2)x^4 + (3b^5 + 14b^4 + 10b^3)x^3 + (b^6 + 8b^5 + 10b^4)x^2 + (2b^6 + 5b^5)x + b^6 + (-x^6 - 3bx^5 + (-b^3 - b^2 + b)x^4 + (b^4 + 3b^3 + 5b^2)x^3 + (3b^4 + 9b^3)x^2 + (b^5 + 7b^4)x + 2b^5)y\right\}.
\]

We compute that \((u, v)\) lies on the curve

\[
E_2 : V^2 + (1 + b)UV + 5bV = U^3 + 7bU^2 + (6b^3 + 6b^2 - 6b)U + b^5 + b^4 - 10b^3 - 29b^2 - b,
\]

the \( j \)-invariant of which is

\[
j(E_2) = \frac{(1 + 228b + 494b^2 - 228b^3 + b^4)^3}{b(1 - 11b - b^2)^5}.
\]

To compute \( \Phi_5(t, j) \) in an efficient manner we note that both \( j(E_1) \) and \( j(E_2) \) are invariant under the mapping \( b \rightarrow -1/b \), and therefore can be expressed as rational functions of \( z = b - 1/b \):

\[
j(E_1) = \frac{-(z^2 + 12z + 16)^3}{z + 11}, \quad j(E_2) = \frac{-(z^2 - 228z + 496)^3}{(z + 11)^5}, \quad z = b - \frac{1}{b}.
\]
These expressions can be used to calculate $\Phi_5(t, j)$ in characteristic 0. A computation on Maple shows that

$$R(t, j) = \text{Resultant}_z((z^2 + 12z + 16)^3 + j(z + 11), (z^2 - 228z + 496)^3 + t(z + 11)^5)$$

$$= 5^{15} \cdot \Phi_5(t, j).$$

One may also calculate the class equations which divide $\Phi_5(t, t)$ directly from the resultant $R(t, t)$ obtained by setting $j = t$. This computation gives that

$$\Phi_5(t, t) = -(t^2 - 1264000t - 681472000)(t - 1728)^2$$

$$\times (t + 32768)^2(t - 287496)^2(t + 884736)^2.$$

Thus, the first quadratic in (2.7) divides $\Phi_5(j, j)$ but the third quadratic in (2.7) does not, showing that the first quadratic is indeed $H_{-20}(j)$.

Here we are content to compute $\Phi_5(t, j)$ over the field $\mathbb{F}_{233}$:

$$\text{Resultant}_z((z^2 + 12z + 16)^3 + j(z + 11), (z^2 - 228z + 496)^3 + t(z + 11)^5)$$

$$\equiv 35 \cdot \Phi_5(t, j) \pmod{233},$$

with

$$\Phi_5(t, j) \equiv t^6 + (232j^5 + 225j^4 + 16j^3 + 76j^2 + 88j + 41)t^5$$

$$+ (225j^5 + 55j^4 + 87j^3 + 28j^2 + 3j + 219)t^4$$

$$+ (16j^5 + 87j^4 + 21j^3 + 71j^2 + 19j + 23)t^3$$

$$+ (76j^5 + 28j^4 + 71j^3 + 203j^2 + 38j + 169)t^2$$

$$+ (88j^5 + 3j^4 + 19j^3 + 38j^2 + 118j + 96)t$$

$$+ (j^6 + 41j^5 + 219j^4 + 23j^3 + 169j^2 + 96j + 31) \pmod{233}.$$
\[ \times(t^2 + 147t + 62)(t^2 + 162t + 216) \pmod{233}. \]

Note that the quadratic factors of \( \Phi_d(p, t) \) over \( \mathbb{F}_p \) can be easily determined using the fact that \( q(t) = t^2 + at + b \) divides \( \Phi_d(p, t) \) if and only if \( q(t) \) divides \( \Phi_d(-a - t, t) \). Lemma 2.3 now implies that the class equation \( H_{-4,5,233}(t) \) is given by

\[
H_{-4,5,233}(t) \equiv (t + 148)^4(t^2 + 64t + 57)^2(t^2 + 81t + 81)^2 \times(t^2 + 147t + 62)^2(t^2 + 162t + 216)^2 \pmod{233},
\]

in agreement with the fact that \( h(-5 \cdot 233) = 20. \)

7 References


[co] David A. Cox, Primes of the Form \( x^2 + ny^2 \); Fermat, Class Field Theory, and Complex Multiplication, John Wiley and Sons, 1989.
