Functiones et Approximatio
51.1 (2014), 77–110
doi: 10.7169/facm/2014.51.1.4

EXPLICIT CONGRUENCES FOR CLASS EQUATIONS

Patrick Morton

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 have previously appeared in print without proof, and have been used to study factorizations of certain Legendre polynomials (mod p).

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

1. Introduction

In this paper we shall prove several explicit congruences modulo p for the class equations corresponding to discriminants $-8p, -3p$, and $-12p$ in the theory of complex multiplication, where p is an odd prime. These congruences were initially presented without proof in [10] and [11] and were used to study connections between the Legendre polynomials of degree $[p/4] = (p-e)/4$ (with $e = 1$ or 3) or $[p/3] = (p-e)/3$ (with $e = 1$ or 2) and complex multiplication in characteristic p.

For example, it is shown in [10] that (for $p > 3$) the number of irreducible binomial quadratic factors of the Legendre polynomial $P_{(p-e)/4}(x)$ over the finite field $\mathbb{F}_p$ is $(h(-2p) - d_p)/4$, where $h(-2p)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-2p})$ and

$$d_p = 2 - \left(\frac{-4}{p}\right) - \left(\frac{-8}{p}\right).$$

These binomial quadratic factors of $P_{(p-e)/4}(x)$ over $\mathbb{F}_p$ reflect the existence of multipliers $\mu \in \mathrm{End}(E)$ of supersingular elliptic curves E for which $\mu^2 = -2p$, and the exact count of these factors depends on Theorem 1.1 below.

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 [2], [4], [14].)

2010 Mathematics Subject Classification: primary: 11G15; secondary: 14H52, 11R11

Congruences for the class equations $H_{-p}(t)$ and $H_{-4p}(t)$ with p an odd prime were first proved by Elkies [6]. These congruences were given explicit form in [1], in terms of the supersingular polynomial $ss_p(t)$, as follows.

The supersingular polynomial $ss_p(t)$ in characteristic p is the monic polynomial over $\mathbb{F}_p$ whose roots are the distinct j-invariants of supersingular elliptic curves in characteristic p. See [8], [1], [9]. It is well-known that

$$ss_p(t) = t^r(t-1728)^s J_p(t), \qquad p > 3, \tag{1.1}$$

where

$$r = r_p = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right), \qquad s = s_p = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right),$$

and where the polynomial $J_p(t) \in \mathbb{F}_p[t]$ has distinct roots (mod p), none of which are 0 or 1728. Furthermore, $J_p(t)$ factors into a product of linear and quadratic factors over $\mathbb{F}_p$, by the well-known result of Deuring [3] that the j-invariant of a supersingular elliptic curve always lies in $\mathbb{F}_{p^2}$. (For a simple proof see [13, p. 145] or [1, Prop. 1].)

The following explicit formula for $J_p(t)$ is proven in [9]. If $n = (p - e_p)/12$, with $p \equiv e_p \pmod{12}$ and $e_p \in \{1, 5, 7, 11\}$, and if the integer $s = 0$ or 1 is defined as above, then

$$J_p(t) \equiv \sum_{k=0}^{n} \binom{2n+s}{2k+s}\binom{2n-2k}{n-k}(-432)^{n-k}(t-1728)^k \pmod{p}. \tag{1.2}$$

Now we can express the congruences of Elkies in the following explicit form: If $p \equiv 3 \pmod 4$, then from [1, Prop. 11] we have:

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

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

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 (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 $J_p(t)$ (mod p) are known.

Here we prove the following two analogous congruences, using some classical results on the modular equation $\Phi_n(x, y)$ [2, pp. 229-231], [12]. 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:*

$$H_{-8p}(t) \equiv (t-1728)^{2\epsilon_1}(t-8000)^{2\epsilon_2}(t+3375)^{4\epsilon_3}(t^2+191025t-121287375)^{4\epsilon_4} \times \prod_{Q_2(a_i,b_i)\equiv 0(p)} (t^2+a_it+b_i)^2 \ (mod\ p);$$

where

$$\epsilon_1 = \frac{1}{2}\left(1-\left(\frac{-4}{p}\right)\right), \qquad \epsilon_2 = \frac{1}{2}\left(1-\left(\frac{-8}{p}\right)\right),$$
$$\epsilon_3 = \frac{1}{2}\left(1-\left(\frac{-7}{p}\right)\right), \qquad \epsilon_4 = \frac{1}{4}\left(1-\left(\frac{-15}{p}\right)\right)\left(1-\left(\frac{5}{p}\right)\right);$$

and the product is over all the irreducible quadratic factors t^2+at+b of $J_p(t)$ distinct from $H_{-15}(t) = t^2+191025t-121287375$ which satisfy $Q_2(a,b) \equiv 0$ (mod p), where

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

An immediate corollary of this theorem is a formula, in terms of the class number $h(-2p)$, for the number of j-invariants of supersingular elliptic curves E in characteristic p which have an endomorphism μ satisfying $\mu^2 = -2p$ (see Theorem 3.3). This is an analogue of Deuring's formula for the number of j-invariants of supersingular curves in characteristic p which have an endomorphism μ satisfying $\mu^2 = -p$. (See [5], [1, p. 97], and [10, Thm. 2.1].) A similar formula is given in Theorem 3.5 for endomorphisms μ satisfying $\mu^2 = -3p$, as a consequence of Theorem 1.2 below. Theorem 1.1 also immediately implies the well-known result that the class number $h(-2p)$ is even, and is divisible by 4 exactly when $p \equiv \pm 1$ (mod 8).

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*

$$K_{3p}(t) \equiv t^{2\delta_1}(t-54000)^{2\delta_1}(t-8000)^{4\delta_2}(t+32768)^{4\delta_3}H_{-20}(t)^{4\delta_4}H_{-32}(t)^{4\delta_5} \times H_{-35}(t)^{4\delta_6} \prod_{Q_3(c_i,d_i)\equiv 0(p)} (t^2+c_it+d_i)^2 \qquad (\text{mod } p);$$

where

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

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

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

and the above product is over all the irreducible quadratic factors t^2+ct+d 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

$$\begin{aligned} Q_3(c,d) = &-2^{45}3^3 5^9 c + 2^{30}3^3 5^6 c^2 - 2^{15}3^2 5^3 c^3 + c^4 - 2^{34}5^9 \cdot 23d \\ &- 2^{15}3^3 5^3 \cdot 23 \cdot 3499cd - 2^3 \cdot 5 \cdot 23 \cdot 1163c^2 d + 2^4 5^3 109^3 d^2 \\ &- 2^3 3^2 \cdot 31cd^2 - d^3. \end{aligned}$$

The degree of the polynomial $K_{3p}(t)$ in this theorem is $a_p h(-3p)$, 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 ϵ_4 and the δ_i (the largest prime dividing their discriminants is $p = 13$ for $d = -15$ resp. $p = 29$ for $d = -20, -32, -35$).

We can extend the result of Theorem 1.2 by proving separate congruences for $H_{-3p}(t)$ and $H_{-12p}(t)$ (mod p), when $p \equiv 1 \pmod 4$.

Theorem 1.3. *If $p > 53$ is a prime with $p \equiv 1$ (mod 4), then we have the following congruences (mod p):*

$$H_{-3p}(t) \equiv (t-54000)^{2\delta_1}(t-8000)^{4\delta_2}H_{-20}(t)^{2\delta_4}H_{-32}(t)^{2\delta_5}\prod_{i\in I}(t^2+c_it+d_i)^2,$$

$$H_{-12p}(t) \equiv t^{2\delta_1}(t+32768)^{4\delta_3}H_{-20}(t)^{2\delta_4}H_{-32}(t)^{2\delta_5}H_{-35}(t)^{4\delta_6}\prod_{j\in J}(t^2+c_jt+d_j)^2,$$

with the same notation as in Theorem 1.2, where the indexing sets I and J in the two products in these congruences are disjoint.

The proof of the congruences in Theorem 1.3 involves an application of the basic theory of complex multiplication, along with some elementary Galois theory. (See Section 4.) In this proof we also make use of a number of the results of [11], some of which depend in turn on Sections 2-3 of this paper. As in [11, p. 274], an important role is played by points on the Fermat curve

$$Fer_3: \quad 27X^3+27Y^3=X^3Y^3$$

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.

To determine exactly *which* factors t^2+ct+d of $J_p(t)$ with $Q_3(c,d) \equiv 0 \pmod p$ divide $H_{-3p}(t) \pmod p$ in Theorem 1.3 one can proceed as follows. To a root $j \in \mathbb{F}_{p^2}$ of each factor t^2+ct+d there correspond values of α and $\beta = \alpha^p$ in $\mathbb{F}_{p^2}$ for which

$$j = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}, \qquad 27\alpha^3+27\beta^3=\alpha^3\beta^3.$$

Now consider the map μ on points of order 2 on the curve

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

which is given on X-coordinates by $\mu : x \to x^\mu$, with

$$x^\mu = -\frac{\alpha^2}{36\alpha^{2p}}\left(\frac{\alpha x+3}{x}\right)^{2p}, \qquad \alpha \neq 0.$$

Then t^2+ct+d will divide $H_{-3p}(t)$ if and only if μ is the trivial permutation on $E_\alpha[2]$. (See Section 4.)

As a further application, it can be shown that the primes $p \geqslant 13$, for which the supersingular polynomial $ss_p(t)$ splits into linear factors over $\mathbb{F}_p$, are the primes for which the class equations $H_{-8p}(x), H_{-12p}(x)$, and $H_{-3p}(x)$ (the last only for $p \equiv 1 \bmod 4$) all split into linear factors mod p (Theorem 3.6). This fact is closely related to Ogg's theorem, that $ss_p(t)$ splits in this way mod p for exactly 15 different primes p. The reader is also referred to Theorem 4.11, which gives three different infinite families of class equations, corresponding to discriminants divisible by p, which have no linear factors at all (mod p). Thus, Theorem 4.11 is a complementary result to Ogg's theorem.

I note finally that it would be possible to prove a result like Theorem 1.2 for the class equations $H_{-dp}(x)$ and $H_{-4dp}(x)$, where d is a fixed, square-free, odd integer (see Lemmas 2.1-2.3 and Theorem 3.1). However, as the reader will notice, the passage from Theorem 1.2 to the explicit and separate congruences in Theorem 1.3 takes up half of the present paper. Thus, establishing explicit congruences for $H_{-dp}(x)$ and $H_{-4dp}(x)$ will most likely require significantly more effort for larger values of d. Even for $d = 7$, for example, it is not clear what curve should play the role that the curve Fer_3 does in establishing Theorem 1.3. For $d = 5$ the analogous curve seems to be the curve $\epsilon^5X^5 + \epsilon^5Y^5 = 1 - X^5Y^5$, with $\epsilon = \frac{1+\sqrt{5}}{2}$. I plan to return to this question in another paper.

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 [3], [2], [12].)

We follow Deuring's paper [3] 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 [3, p. 241] we take the well-known formula

$$\Phi_p(t, j) \equiv (t^p - j)(t - j^p) \qquad (\text{mod } p). \tag{2.1}$$

We will also need the fact that if $(m, n) = 1$, then

$$\Phi_{mn}(t, j) = \prod_{h=1}^{\psi(n)} \Phi_m(t, j_h), \tag{2.2}$$

where the last product is over the $\psi(n)$ values j_h for which

$$\Phi_n(t, j) = \prod_{h=1}^{\psi(n)} (t - j_h). \tag{2.3}$$

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*

$$\Phi_{dp}(t, t) \equiv \Phi_d(t^p, t)^2 \qquad (mod\ p). \tag{2.4}$$

Proof. From (2.1)-(2.3) we have in characteristic p that

$$\Phi_{dp}(t, j) = \prod_{h=1}^{\psi(p)} \Phi_d(t, j_h) = \prod_{h=1}^{p} \Phi_d(t, j^{1/p}) \cdot \Phi_d(t, j^p) = \Phi_d(t^p, j)\Phi_d(t, j^p),$$

which is a generalization of (2.1). Putting $j = t$ and using $\Phi_d(x, y) = \Phi_d(y, x)$ gives (2.4). ∎

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 [2, p.291] and [3, p.251] that

$$\Phi_{dp}(t,t) = \pm H_{-4dp}(t) \cdot \prod_O H_O(t)^{r(O,dp)}, \qquad \text{if } dp \equiv 1, 2 \pmod 4,$$

$$\Phi_{dp}(t,t) = \pm H_{-dp}(t) H_{-4dp}(t) \cdot \prod_O H_O(t)^{r(O,dp)}, \qquad \text{if } dp \equiv 3 \pmod 4, \quad (2.5)$$

where $r(O, m) = |\{\alpha \in O : \alpha \text{ is primitive, } N(\alpha) = m\}/O^*|$, and $r(O, dp) = 0$ or $r(O, dp) \geqslant 2$ 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 charateristic p.

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

a) *If $p > 4d$, then in (2.5), we have $\gcd(H_{-dp}(t), H_O(t)) = \gcd(H_{-4dp}(t), H_O(t)) = 1$ (mod p) for all the orders O occurring in the product.*
b) *If $p > 4d$, all the supersingular factors of $\Phi_{dp}(t, t)$ (mod p) occur as factors of $H_{-dp}(t)$ or $H_{-4dp}(t)$ (mod p).*

Proof. Suppose that $O = O_{-D}$ is an order for which $r(O, dp) > 1$ in (2.5). Then dp or $4dp = x^2 + Dy^2$, with $(x, y) = 1$. If $p|D$, then $p|x$ and we have d 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 [3]. 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. ∎

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 $\gcd(ss_p(t), \Phi_d(t^p, t))$ (mod p) are exactly the irreducible factors of $H_{-4dp}(t)$ or $H_{-dp}(t)H_{-4dp}(t)$ (mod 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 [7, p. 321] or [2, p. 234]. (See also [3, p. 247] for the computation of Φ_2, but beware of misprints in the coefficients of tj and $(t+j)$ in the final answer [3,(57)]. The powers of 3 in those coefficients should be 3^4 and 3^7, respectively.) We have:

$$\begin{aligned}\Phi_2(t,j) &= t^3 - t^2\cdot(j^2-1488j+162000) + t\cdot(1488j^2+40773375j+8748000000)\\ &\quad + j^3 - 162000j^2 + 8748000000j - 157464000000000,\\ \Phi_2(t,t) &= -(t-1728)(t-8000)(t+3375)^2,\\ \Delta_2(j) &= \mathrm{disc}_t(\Phi_2(t,j)) = 4(j-1728)j^2(j+3375)^2(j^2+191025j-121287375)^2.\end{aligned}$$

Also,

$$\begin{aligned}\Phi_3(t,j) &= t\cdot(t+2^{15}\cdot 3\cdot 5^3)^3 + j\cdot(j+2^{15}\cdot 3\cdot 5^3)^3 - t^3j^3\\ &\quad + 2^3\cdot 3^2\cdot 31\cdot t^2j^2(t+j) - 2^2\cdot 3^3\cdot 9907\cdot tj(t^2+j^2)\\ &\quad + 2\cdot 3^4\cdot 13\cdot 193\cdot 6367\cdot t^2j^2 + 2^{16}\cdot 3^5\cdot 5^3\cdot 17\cdot 263\cdot tj(t+j)\\ &\quad - 2^{31}\cdot 5^6\cdot 22973\cdot tj,\\ \Phi_3(t,t) &= -t(t-54000)(t+32768)^2(t-8000)^2,\\ \Delta_3(j) &= \mathrm{disc}_t(\Phi_3(t,j)) = -27j^2(j-1728)^2(j-8000)^2(j+32768)^2\\ &\quad\times(j^2-1264000j-681472000)^2(j^2-52250000j+12167000000)^2\\ &\quad\times(j^2+117964800j-134217728000)^2.\end{aligned}$$

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* [7, p. 338]:

Theorem. *Over the rational field $\mathbb{Q}$, the discriminant $\Delta_p(j)$ 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

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

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

$$H_{-8}(j) = j - 8000, \qquad H_{-11}(j) = j + 32768. \tag{2.6}$$

we refer to [7, pp. 394, 396] or [2, p. 261]. We also claim that:

$$\begin{aligned} H_{-20}(j) &= j^2 - 1264000j - 681472000, \\ H_{-32}(j) &= j^2 - 52250000j + 12167000000, \\ H_{-35}(j) &= j^2 + 117964800j - 134217728000. \end{aligned} \tag{2.7}$$

This can be seen as follows. The second quadratic splits into the product $(j+52)(j+63)$ (mod 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 Ω. 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. The formula

$$\begin{aligned} \Phi_5(t,t) = &-(t^2 - 1264000t - 681472000)(t-1728)^2 \\ &\times (t+32768)^2(t-287496)^2(t+884736)^2 \end{aligned}$$

shows 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 [7].

We also note that $H_{-12}(j) = j - 54000$ from [7, p.395] or [2, 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

$$\begin{aligned}\frac{d}{dt}(F(t,t^p)) &= 3t^2 - 2t(t^{2p} - 1488t^p + 162000) + 1488t^{2p} \\ &\quad + 40773375t^p + 8748000000, \\ &= -2t^{2p+1} + 1488t^{2p} + 2976t^{p+1} + 40773375t^p + 3t^2 \\ &\quad - 324000t + 8748000000.\end{aligned}$$

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

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

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 $0 \pmod p$, for $p \geqslant 17$, is $p = 42391$. Now we note that

$$H_{-15}(t) \equiv (t + 4410)(t + 17051) (\text{mod } 42391),$$

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 $0 \pmod p$, for a multiple root of $\Phi_2(t,t^p) = \Phi_2(t^p,t)$. This completes the proof of the proposition. ∎

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

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

We also note in the case $p = 13$ that

$$H_{-104}(t) \equiv (t+8)^6 \pmod{13}.$$

(See [7, 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. ∎

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

$$\begin{aligned}\frac{d}{dt}(F(t, t^p)) &= -2t^3 + 4467t^2 + 40449375t + 8748000000 \\ &= -(t + 3375)(2t^2 - 11217t - 2592000) \\ &= -(t + 3375)f(t).\end{aligned}$$

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 $1728 \equiv -3375 \pmod 7$ and $8000 \equiv -3375 \pmod{5 \cdot 7 \cdot 13}$, the assertion of the corollary holds. ∎

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

Proposition 2.7. *If p is a prime > 3, the multiplicity of an irreducible factor of $\Phi_3(t^p, t)$ (mod 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 $F(t) = \Phi_3(t^p, t)$ (mod p) must divide $\Delta_3(t)$ (mod 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

$$F'(t) = -Q_1(-t^p - t, t^{p+1}) + t^p Q_2(-t^p - t, t^{p+1}),$$

and therefore

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

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

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

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

$$\begin{aligned} Q(u,v) &= u^4 - 36864000u^3 + 452984832000000u^2 - 1855425871872000000000u \\ &\quad - 1069960u^2v - 2232uv^2 - 8900112384000uv \\ &\quad - v^3 + 2590058000v^2 - 771751936000000000v \\ &= u^4 - 2^{15}\cdot 3^2\cdot 5^3\cdot u^3 + 2^{30}\cdot 3^3\cdot 5^6\cdot u^2 - 2^{45}\cdot 3^3\cdot 5^9\cdot u \\ &\quad - 2^3\cdot 5\cdot 23\cdot 1163\cdot u^2v - 2^3\cdot 3^2\cdot 31\cdot uv^2 - 2^{15}\cdot 3^3\cdot 5^3\cdot 23\cdot 3499\cdot uv \\ &\quad - v^3 + 2^4\cdot 5^3\cdot 109^3\cdot v^2 - 2^{34}\cdot 5^9\cdot 23\cdot v. \end{aligned}$$

This yields the following partial derivatives:

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

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 (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

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

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

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

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

$$F'(54000) \equiv -2^{19} \cdot 3^3 \cdot 5^9 \cdot 11^2 \cdot 17^2 \cdot 23^2 \cdot 29^2, \tag{2.9}$$
$$F''(54000) \equiv -2^{16} \cdot 3^3 \cdot 5^6 \cdot 17 \cdot 23 \cdot 29 \cdot 89 \cdot 1153.$$

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

$$\begin{aligned} F'(t) &= -Q_1(-2t, t^2) + tQ_2(-2t, t^2) \\ &= -3t^5 + 2^3 \cdot 3^2 \cdot 5 \cdot 31 \cdot t^4 + 2^{12} \cdot 1262587 \cdot t^3 \\ &\quad + 2^{15} \cdot 3^3 \cdot 5^4 \cdot 109 \cdot 443 \cdot t^2 - 2^{32} \cdot 5^6 \cdot 7 \cdot 11 \cdot 149 \cdot t + 2^{45} \cdot 3^3 \cdot 5^9 \\ &= -(t + 32768)(t - 8000)(3t^3 - 85464t^2 - 2268352000t + 7077888000000). \end{aligned}$$

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

$$K_{dp}(t) = H_{-4dp}(t) \qquad \textit{or} \qquad H_{-dp}(t)H_{-4dp}(t)$$

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 $K_{dp}(t)$ (mod p) if and only if $Q_d(a, b) \equiv 0$ (mod 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), the given factor $q(t)$ of $J_p(t)$ 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 $(t-1728), (t-8000)$, 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. Since

$$H_{-4}(t) = t - 1728, \qquad H_{-8}(t) = t - 8000, \qquad H_{-7}(t) = t + 3375,$$

by the discussion preceding Proposition 2.4, it is clear that one of these is a linear factor of $ss_p(t)$ if and only if the corresponding discriminant $(-4, -8,$ or $-7)$ is a quadratic non-residue of p. This explains the definitions of the ϵ_i, for $i = 1, 2, 3$. 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 $H_{-8p}(t)$ (mod 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 $\epsilon_4 = 1$. Further, it must divide $H_{-8p}(t)$ when $\epsilon_4 = 1$, because its roots α_+ and α_- satisfy $\Phi_2(\alpha_+, \alpha_-) = 0$ in characteristic 0, and therefore in characteristic p for all p (see the expressions for α_+, α_- in the proof of Proposition 2.4). It is straightforward to compute that the derivative $(\Phi_2(t^p, t))'$ is also 0 at α_+ and α_-, 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 $H_{-8p}(t)$ (mod p) when $\epsilon_4 = 1$, by the result of Proposition 2.4.

It remains to show that $H_{-15}(t)$ makes no contribution to the factorization of $H_{-8p}(t)$ (mod p) when $\epsilon_4 = 0$, or (wlog) when $(\frac{5}{p}) = +1$. 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 $H_{-15}(1728), H_{-15}(8000), H_{-15}(-3375)$.

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

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

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*

$$\begin{aligned} &\frac{1}{2}(h(-2p) - 2\epsilon_3 - 4\epsilon_4) \\ &\qquad = \frac{1}{2}\left(h(-2p) - 2 - \left(\frac{-3}{p}\right) + \left(\frac{5}{p}\right) + \left(\frac{-7}{p}\right) + \left(\frac{-15}{p}\right)\right). \end{aligned}$$

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

We turn now to the analgous 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

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

These are the only possible linear factors of $K_{3p}(t) \pmod p$, 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

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

are distinct (mod p) for $p > 53$, and all divide $\Phi_3(t^p, t) \pmod p$ 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

$$\begin{aligned} \frac{\partial}{\partial u}Q(u,v) &= 2^2u^3 - 2^{15}\cdot 3^3\cdot 5^3u^2 + 2^{31}\cdot 3^3\cdot 5^6u - 2^{45}\cdot 3^3\cdot 5^9 \\ &\quad - 2^4\cdot 5\cdot 23\cdot 1163uv - 2^3\cdot 3^2\cdot 31v^2 - 2^{15}\cdot 3^3\cdot 5^3\cdot 23\cdot 3499v, \\ \frac{\partial}{\partial v}Q(u,v) &= -2^3\cdot 5\cdot 23\cdot 1163u^2 - 2^4\cdot 3^2\cdot 31uv - 2^{15}\cdot 3^3\cdot 5^3\cdot 23\cdot 3499u \\ &\quad - 3v^2 + 2^5\cdot 5^3\cdot 109^3\cdot v - 2^{34}\cdot 5^9\cdot 23, \end{aligned}$$

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 δ_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*

$$\begin{aligned} a_p h(-3p) = 9 &- 2\left(\frac{-3}{p}\right) + 2\left(\frac{-4}{p}\right) - 2\left(\frac{5}{p}\right) + \left(\frac{-7}{p}\right) - \left(\frac{8}{p}\right) \\ &- 3\left(\frac{-8}{p}\right) - 2\left(\frac{-11}{p}\right) - \left(\frac{-20}{p}\right) - \left(\frac{-35}{p}\right) + 4N_3, \end{aligned}$$

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

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 class numbers $h(O_{-3p})$ and $h(O_{-12p})$ in [2, 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 End(E) is*

$$\frac{1}{2}(a_p h(-3p) - 2\delta_2 - 2\delta_3 - 4\delta_4 - 4\delta_5 - 4\delta_6).$$

One more result connects the primes p for which the supersingular polynomial $ss_p(t)$ splits into linear factors (mod p) with the class equations we have been considering.

Theorem 3.6. *If $p \geqslant 13$ is prime, 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 $p \equiv 1$ (mod 4)) are products of linear polynomials over $\mathbb{F}_p$.*

Because of space considerations I omit the proof, which will appear elsewhere.

4. The class equations $H_{-3p}(t)$ and $H_{-12p}(t)$

In this section we shall give a proof of Theorem 1.3. In order to do this we examine each of the explicit factors of $K_{3p}(t)$ (mod 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 $p \equiv 1$ (mod 4). The criterion we use is contained in the following lemma, whose straightforward proof we leave to the reader. (See the arguments in [6] or [1, Prop. 7].)

Lemma 4.1. *Let $\mu \in$ End(E_α) be a multiplier of the curve*

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

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

Lemma 4.2. *If $p \equiv 1$ (mod 4), then $H_{-3p}(t)$ is a product of square factors (mod p).*

Proof. This proof is similar to the proof of Prop. 9 and congruence (3.3b) in [1]. 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 Σ_0 of the Hilbert class field Σ 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 Σ. Putting these two facts together implies that p splits into the squares of primes of degree 1 or 2 in Σ_0. Thus, over the p-adic field $\mathbb{Q}_p$, the polynomial $H_{-3p}(t)$, either of whose real roots generates the real subfield Σ_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 (mod p), by Hensel's Lemma. Therefore, each of these irreducible factors must be a square (mod p). This proves the lemma. ∎

In the situation we are considering, the curve E_α 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_α, which is in Deuring normal form, because a multiplier μ satisfying $\mu^2 = -3p$ is given explicitly in [11]. Such a multiplier exists with kernel equal to $\{O, (0,0), (0,-1)\}$ if and only if (α, α^p) is a point on the curve

$$Fer_3 : \quad 27X^3 + 27Y^3 = X^3Y^3.$$

If this is the case, μ 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_α to E_β given on X-coordinates by

$$\phi_{\alpha,\beta}(X) = -\frac{\beta^2}{9\alpha^2}\frac{3X^3 + \alpha^2X^2 + 3\alpha X + 3}{X^2}, \qquad \beta = \alpha^p. \tag{4.1}$$

Furthermore, by [11, Thm. 2.3], the parameter α of a supersingular curve E_α lies in the finite field $\mathbb{F}_{p^2}$. Hence we may write the X-coordinate of the image $\mu(X,Y) = (X^\mu, Y^\mu)$ of the point (X,Y) on E_α as

$$X^\mu = -\frac{\alpha^2}{9\alpha^{2p}}\left(\frac{3X^3 + \alpha^2X^2 + 3\alpha X + 3}{X^2}\right)^p, \qquad \alpha \neq 0. \tag{4.2}$$

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

$$X^\mu = -\frac{1}{3}\left(\frac{X^3+1}{X^2}\right)^p, \qquad \alpha = 0. \tag{4.3}$$

On the other hand, the points of order 2 on E_α are the points (x,y) satisfying the equation

$$\left(y + \frac{\alpha}{2}x + \frac{1}{2}\right)^2 = x^3 + \frac{1}{4}(\alpha x + 1)^2 = 0. \tag{4.4}$$

Replacing X by x and x^3 by $-(\alpha x+1)^2/4$ in the formula (4.2) for μ gives

$$\begin{aligned} x^\mu &= -\frac{\alpha^2}{36\alpha^{2p}}\left(\frac{\alpha^2x^2 + 6\alpha x + 9}{x^2}\right)^p \\ &= -\frac{\alpha^2}{36\alpha^{2p}}\left(\frac{\alpha x + 3}{x}\right)^{2p}, \qquad \alpha \neq 0, \end{aligned} \tag{4.5}$$

for solutions x of (4.4). Thus μ is the identity permutation on the points of $E_\alpha[2]$ if and only if $x^\mu = x$ for all the roots x of (4.4).

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

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

where ω is a primitive cube root of unity in $\mathbb{F}_{p^2}$. In this case (4.3) gives that $x_i^\mu = -\frac{1}{4x_i^{2p}}$. Since $4^{1/3} \in \mathbb{F}_p$ but $\omega \notin \mathbb{F}_p$ we have

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

Thus, μ does not fix the point $P_1 = (x_1, -1/2)$. By Lemma 4.1, 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 μ is any endomorphism of E_0 satisfying $\mu^2 = -3p$. By arguments of [11, 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 $\mu \to \mu' \in \mathrm{End}(E_{\alpha'})$ such that $\ker(\mu') = \{O', (0,0), (0,-1)\}$ on $E_{\alpha'}$. Then $\mu'^2 = -3p$ implies that (α', α'^p) is a point on Fer_3. The only possibilities for α' 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 (α', β) lies on Fer_3 are $\beta = -6\omega^j$, and such a β can only equal α'^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 μ of E_0 for which $\mu^2 = -3p$ and $(1+\mu)/2 \in \mathrm{End}(E_0)$. This proves the following proposition.

Proposition 4.3. *If $p \equiv 1$ (mod 4) and $p > 5$, the factor $H_{-3}(t) = t$ never divides $H_{-3p}(t)$ (mod p). Hence we have $t^{2\delta_1} \mid H_{-12p}(t)$ (mod 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 $p > 53$. For the linear factors (Props. 4.4-4.6), 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 4.4. *If $p \equiv 1$ (mod 4) and $p > 53$, then $H_{-12}(t)^{2\delta_1} = (t - 54000)^{2\delta_1}$ divides $H_{-3p}(t)$ (mod p) and $(t - 54000)$ does not divide $H_{-12p}(t)$ (mod 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 4.2 and Theorem 1.2. To show this we take $\alpha = 54^{1/3} = 3 \cdot 2^{1/3} \in \mathbb{F}_p$ 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 Fer_3. The roots x_i of (4.4) can be determined by noting that

$$x_i^3 + \frac{\alpha^2}{4}x_i^2 + \frac{\alpha}{2}x_i + \frac{1}{4} = \frac{1}{54}\left(y^3 + \frac{27}{2}y^2 + 27y + \frac{27}{2}\right), \qquad (y = \alpha x_i)$$
$$= \frac{1}{54}\left(y + \frac{3}{2}\right)(y^2 + 12y + 9).$$

We find the roots

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

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 μ fixes all the points of order 2 on E_α. Hence, $\frac{1+\sqrt{-3p}}{2}$ injects into $\mathrm{End}(E_\alpha)$ 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 $H_{-3p}(t) \pmod p$. ∎

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 μ is an endomorphism in E_α with $\mu^2 = -3p$ and $\ker(\mu)$ is a subgroup of $E_\alpha[3]$ other than $\{O, (0,0), (0,-1)\}$, 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 $\ker(\mu') = \{O', (0,0), (0,-1)\}$. Then (α', α'^p) is a point on 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 [11, 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 μ' is determined up to sign, by [11, Prop. 4.1], namely

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

as in the discussion immediately preceding equation (4.1) above. Furthermore, $\mu = \iota^{-1} \circ \mu' \circ \iota$ on E_α is independent of the particular cube root of α'^3 which is chosen, as can be seen from the formula for ϕ_{α, α^p}.

Thus, when considering the factors $H_{-8}(t) = t - 8000$ and $H_{-11}(t) = t + 32768$, whose 4th powers divide $K_{3p}(t) \pmod p$, 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 μ_i of E_α satisfying $\mu_i^2 = -3p$, one of which has $\ker(\mu_1) = \{O, (0,0), (0,-1)\}$, the other arising from an isomorphism $\iota : E_\alpha \to E_\beta$ in which $\beta = \alpha^p$.

Proposition 4.5. *If $p > 53$, the factor $H_{-8}(t)^{4\delta_2} = (t - 8000)^{4\delta_2}$ 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 $\equiv 5 \pmod 8$, 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 endomorpishms μ_i in $\mathrm{End}(E_\alpha)$ 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

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

Furthermore, $(\alpha, \beta) = (-2 + \sqrt{-2}, -2 - \sqrt{-2})$ is a point on Fer_3 (even in characteristic 0), so we have the meromorphism $\mu_1 = \mu$ given by (4.2) or by (4.5) 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 μ_2 satisfying $\mu_2^2 = -3p$ in $\mathrm{End}(E_\alpha)$ is given on X-coordinates by the formula

$$X^{\mu_2} = -\frac{1}{3}\left(\frac{X(X^2 + (1 - \sqrt{-2})X - 1 + \sqrt{-2})}{\left(X - \frac{1+\sqrt{-2}}{3}\right)^2}\right)^p + \frac{1 + \sqrt{-2}}{3}. \tag{4.6}$$

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_α (see [11, Thm. 1.3]), and since $\beta = \alpha^p$, $\gamma' = \gamma^p$ is the X'-coordinate of a point of order 3 on E_β. By [11, Prop. 3.10] an isomorphism $\iota : E_\alpha \to E_\beta$ exists for which $\iota(X, Y) = (X', Y')$ and a

$$X^\iota = X' = -\frac{\gamma'}{\gamma}X + \gamma' = -\gamma^{p-1}X + \gamma^p = \frac{1 + 2\sqrt{-2}}{3}X + \frac{1 - \sqrt{-2}}{3}, \tag{4.7a}$$

$$(X')^{\iota^{-1}} = X = -\frac{1}{\gamma^{p-1}}X' + \gamma = \frac{1 - 2\sqrt{-2}}{3}X' + \frac{1 + \sqrt{-2}}{3}. \tag{4.7b}$$

(This uses the fact that the linear fractional map $\sigma_1(z) = 3(z+6)/(z-3)$ takes α to β and vice versa.) The endomorphism $\mu_2' = \nu' \circ \phi_{\beta,\alpha}$ on E_β arises by conjugating

the coefficients of (4.2) in $\mathbb{F}_{p^2}$:

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

and satisfies $\mu_2'^2 = -3p$ in $\mathrm{End}(E_\beta)$. 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 $\mathrm{End}(E_\alpha)$. The formula (4.6) now follows by using these formulas to compute $X^{\mu_2} = X^{\iota\mu_2'\iota^{-1}}$.

Another straightforward calculation using (4.6) shows that μ_2 is the trivial permutation on the roots x_i of $f_2(x) = 0$. Alternatively, since μ_2' arises by conjugating the coefficients of the map μ_1 in $\mathbb{F}_{p^2}$ (i.e., raising to p-th powers), and the points of order 2 on E_β arise in the same way from the points in $E_\alpha[2]$, it is clear that μ_2' induces the trivial automorphism on $E_\beta[2]$. Then μ_2 will also be the trivial permutation on $E_\alpha[2]$. Note that (4.6) and (4.2) show that $\ker(\mu_2) \neq \ker(\mu_1)$, so $\mu_2 \neq \pm\mu_1$.

It follows that $(1+\mu)/2 \in \mathrm{End}(E_\alpha)$ for every endomorphism μ 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 (mod p). If there were, and E is an elliptic curve with invariant j and complex multiplication by the order $O_{-12p} = \mathbb{Z}[1, \sqrt{-3p}]$, then the reduced curve $\tilde{E}$ would have an endomorphism ring in which O_{-12p} is maximally embedded by $\sqrt{-3p} \to \mu$, by Deuring's result [3, p. 270], since the conductor of O_{-12p} is $f = 2$ and not divisible by p. But this contradicts the fact that we have established above, that $(1+\mu)/2$ is contained in $\mathrm{End}(\tilde{E})$, so that $\mathrm{End}(\tilde{E}) \cap \mathbb{Q}(\mu) = \mathbb{Z}[1, \frac{1+\mu}{2}]$, which is strictly larger than $\mathbb{Z}[1,\mu]$. This proves the proposition. ∎

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

Proposition 4.6. *For $p > 53$ we have that $H_{-11}(t)^{4\delta_3} = (t+32768)^{4\delta_3}$ divides $H_{-12p}(t)$ (mod p), so that $H_{-3p}(t)$ is not divisible by $H_{-11}(t)$ (mod p).*

Proof. This follows by a similar argument as in the proof of Proposition 4.5, but with some complications arising from the nature of the solutions of (4.4). We take $\alpha = -1+\sqrt{-11}$ and $\beta = -1-\sqrt{-11}$, where (α,β) is a point on 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

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

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

$$\mathrm{disc}_x(f_2(x)) = \left(1 - \frac{1}{4}\sqrt{-11}\right)^2,$$

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 σ, say. Since L arises from k by adjoining the X-coordinates of the points of order 2 on E_α, 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 [14, Thm. 4.6, p. 135]). A prime p with $(-11/p) = -1$ splits into 3 primes of degree 2 in L, which are cyclically permuted by σ, because p is inert in k and the ideal (p) lies in the principal ray class (mod 2). For these same primes E_α is supersingular in characteristic p.

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

$$\psi(X) = (\phi_{\alpha,\beta}(X))^\tau = \left(-\frac{\beta^2}{9\alpha^2} \frac{3X^3 + \alpha^2 X^2 + 3\alpha X + 3}{X^2} \right)^\tau. \tag{4.8}$$

The map ψ is an endomorphism of E_α in characteristic 0 (but not a morphism!), since $\phi_{\alpha,\beta}$ is an isogeny from E_α to E_β, and τ maps E_β back to E_α by $(X', Y')^\tau = (X'^\tau, Y'^\tau)$. (See [11, 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 τ, possible because $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. 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

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

where X^{μ_1} is given by (4.2). Now if $x = X(P)$, for $P \in E_\alpha[2]$, is one of the roots of $f_2(x) = 0$, then

$$\begin{aligned} \psi^2(x) &= (\phi_{\alpha,\beta}\,(\phi_{\alpha,\beta}(x)^\tau))^\tau = (\phi_{\beta,\alpha})\left(\phi_{\alpha,\beta}(x)^{\tau^2}\right) \\ &= (\phi_{\beta,\alpha} \circ \phi_{\alpha,\beta})(x) = X(3P) = X(P) = x, \end{aligned} \tag{4.9}$$

where we have used the formulas in [11, Props. 3.5 and 3.6]. This shows that $\psi^2 = 1$ on $E_\alpha[2]$. Therefore, ψ has a fixed point, say $P_1 = (x_1, y_1)$. Then $\psi(x_1) = x_1$ implies that

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

The roots x_1, $x_2 = x_1^\sigma$, $x_3 = x_1^{\sigma^{-1}}$ are distinct (mod $\mathfrak{P}$), for $p > 3$, so this computation implies that μ_1 is not the identity permutation on the points of order 2 of the reduced curve $\tilde{E}_\alpha = E_\alpha \pmod{\mathfrak{P}}$.

The same argument as in Proposition 4.5 will prove the assertion, once we apply an appropriate isomorphism $\iota : \tilde{E}_\alpha \to \tilde{E}_\beta$ 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 $\ker(\mu_1)$. But this follows easily, as in the proof of Proposition 4.5, 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 [11, Prop. 3.10].) Then an isomorphism $\iota : \tilde{E}_\alpha \to \tilde{E}_\beta$ exists for which $\iota(X,Y) = (X',Y')$ and

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

Thus, the kernel of μ_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 μ_1 has on $\tilde{E}_\alpha[2]$. Hence, μ_2 is not the identity on $\tilde{E}_\alpha[2]$, so that no endomorphism of the form $(1+\mu)/2$ with $\mu^2 = -3p$ exists in $\mathrm{End}(\tilde{E}_\alpha)$. This completes the proof. ∎

We turn now to the quadratic factors in Theorem 1.2.

Proposition 4.7. *The factor $H_{-20}(t)^{2\delta_4}$ 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 α and β to be

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

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_α are the roots of the polynomial

$$\begin{aligned} f_2(x,\alpha) &= x^3 + \frac{1}{4}(\alpha x+1)^2 \\ &= \left(x - \frac{3\sqrt{-1}-\sqrt{-5}}{4}\right)\left(x^2 + \frac{-6+\sqrt{-1}-2\sqrt{5}+\sqrt{-5}}{2}x + \frac{3+\sqrt{-5}}{4}\right). \end{aligned}$$

With $\mu_1 = \nu \circ \phi_{\alpha,\beta}$ as in (4.2) and $x_1 = (3\sqrt{-1}-\sqrt{-5})/4$ we have $x_1^{\mu_1} = x_1$, because $\phi_{\alpha,\beta}$ takes roots of $f_2(x,\alpha)$ to roots of $f_2(x,\beta)$ 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 σ denote complex conjugation and τ the automorphism of $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$ over $\mathbb{Q}(\sqrt{-1})$ for which $\tau(\sqrt{5}) = -\sqrt{5}$. Since

$$\Delta\Delta^\tau = \mathsf{Norm}_{\mathbb{Q}(\sqrt{-1})}(\Delta) = 9,$$
$$\Delta\Delta^\sigma = \mathsf{Norm}_{\mathbb{Q}(\sqrt{5})}(\Delta) = 9\left(\frac{1+\sqrt{5}}{2}\right)^{10},$$

and

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

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 Δ is not a square in $K = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$. Thus, $[L : \mathbb{Q}] = 8$. Setting

$$\Delta' = \Delta^{\sigma\tau} = \bar{\Delta}^\tau, \quad \sqrt{\Delta'} = \frac{2\sqrt{-1} - \sqrt{5}}{\sqrt{\Delta}},$$

we define the automorphism ρ on L by

$$\rho : \sqrt{\Delta} \to \sqrt{\Delta'} = \frac{2\sqrt{-1} - \sqrt{5}}{\sqrt{\Delta}},$$

and we extend the automorphisms σ and τ to L by setting

$$\sigma : \sqrt{\Delta} \to \sqrt{\bar{\Delta}} = \frac{3\varepsilon^5}{\sqrt{\Delta}}, \qquad \varepsilon = \frac{1+\sqrt{5}}{2},$$

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

Then $\rho|_K = (\sigma\tau)|_K$, so that $\rho^2(\sqrt{\Delta}) = -\sqrt{\Delta}$. Hence, ρ 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 $\mathrm{Gal}(L/\mathbb{Q})$ is the dihedral group D_4. It is also straightforward to verify that

$$\tau^2 = 1, \qquad \tau\rho = \rho^{-1}\tau, \qquad \sigma\tau = \tau\sigma\rho^2.$$

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_α is defined over the Hilbert class field $K$of k_3 and E_α has complex multiplication by the ring of integers of k_3. The prime ideal (p) lof 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 4.8 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 $\mathrm{Gal}(L/\mathbb{Q})$ is $\langle \rho^2, \tau \rangle$. However, both prime divisors of p in K – the fixed field of $\langle \rho^2 \rangle$ – have degree 2, so the decomposition group of a prime divisor of p in L is either $\langle \tau \rangle$ or $\langle \rho^2 \tau \rangle$. 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 τ. As in the proof of Proposition 4.6 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 (4.8). Then a lengthy calculation shows that

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

As in the proof of Proposition 4.6, it follows that $x_2^{\mu_1} \equiv x_3 \pmod{\mathfrak{P}}$. The discriminant of $f(x, \alpha)$ is

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

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 μ_1 is a non-trivial permutation on $\tilde{E}_\alpha[2] = E_\alpha[2] \pmod{\mathfrak{P}}$. It follows that $H_{-20}(t)^{2\delta_4}$ divides $H_{-12p}(t) \pmod{p}$.

In this case we know that E_α and E_β are not isomorphic, because their j-invariants are conjugate over $\mathbb{Q}$ but not equal. However, $E_\alpha \cong E_{\alpha^\sigma}$ since σ is complex conjugation and $j(E_\alpha)$ is real. Thus a second endomorphism μ_2 arises from an isomorphism $\iota : E_\alpha \to E_{\alpha^\sigma}$ by the formula (in characteristic p)

$$\mu_2 = \iota^{-1} \circ \nu' \circ \phi_{\alpha^\sigma,\beta^\sigma} \circ \iota = \iota^{-1} \circ \mu_2' \circ \iota,$$

where $\nu' : \tilde{E}_{\beta^\sigma} \to \tilde{E}_{\alpha^\sigma}$ is the Frobenius map. Here we have

$$\alpha^\sigma = \frac{-1 - 7\sqrt{-1} + \sqrt{5} - \sqrt{-5}}{2}, \qquad \beta^\sigma = \frac{-1 - 7\sqrt{-1} - \sqrt{5} + \sqrt{-5}}{2}.$$

Now (once again in characteristic 0) the roots of $f_2(x, \alpha^\sigma) = 0$ are x_i^σ $(1 \leqslant i \leqslant 3)$, which also lie in L since L is normal over $\mathbb{Q}$. Setting

$$\psi'(X) = (\phi_{\alpha^\sigma,\beta^\sigma}(X))^\tau$$

we have

$$\psi'(x_2^\sigma) = (\phi_{\alpha^\sigma,\beta^\sigma}(x_2^\sigma))^\tau = (\phi_{\alpha,\beta}(x_2))^{\sigma\tau} = (\phi_{\alpha,\beta}(x_2))^{\tau\sigma\rho^2}$$
$$= (\phi_{\alpha,\beta}(x_2)^\tau)^{\sigma\rho^2} = \psi(x_2)^{\sigma\rho^2} = x_3^{\rho^2\sigma} = x_2^\sigma,$$

by the previous calculation, using the fact that ρ^2 is in the center of $\mathrm{Gal}(L/\mathbb{Q})$. In the same way, ψ' also fixes x_3^σ and x_1^σ. Now the congruence $\psi'(X) \equiv X^{\mu_2'} \pmod{\mathfrak{P}}$ implies that μ_2' is the identity permutation on $\tilde{E}_{\alpha^\sigma}[2]$ (in characteristic p), so μ_2 is the identity on $\tilde{E}_\alpha[2]$. Hence, $H_{-20}(t)^{2\delta_4}$ also divides $H_{-3p}(t) \pmod p$! This proves the proposition. ∎

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

Proposition 4.8. *The factor $H_{-32}(t)^{2\delta_5}$ 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 $\equiv 5 \pmod 8$ so that $(2/p) = -1$. We take α and β to be

$$\alpha = \frac{4 + 2\sqrt{-1} + 5\sqrt{2} + 5\sqrt{-2}}{2}, \qquad \beta = \frac{4 + 2\sqrt{-1} - 5\sqrt{2} - 5\sqrt{-2}}{2},$$

so that

$$j(E_\alpha) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} = 26125000 + 18473000\sqrt{2}$$

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 σ be complex conjugation on the field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and τ the automorphism taking $\sqrt{2}$ to $-\sqrt{2}$, we have the norm equations

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

and

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

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 $\rho \in \mathrm{Gal}(L/\mathbb{Q})$ by

$$\rho : \sqrt{\Delta} \to \sqrt{\Delta'} = \frac{\sqrt{-1}-2\sqrt{2}}{\sqrt{\Delta}},$$

and we extend the automorphisms σ and τ to L by setting

$$\sigma : \sqrt{\Delta} \to \sqrt{\bar{\Delta}} = \frac{3\varepsilon^3}{\sqrt{\Delta}}, \qquad \varepsilon = 1+\sqrt{2},$$

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

These automorphisms satisfy all the same relations as in the proof of Proposition 4.7. Now we compute

$$\begin{aligned}
\psi(x_2) &= \phi_{\alpha,\beta}(x_2)^\tau \\
&= \left(\frac{-1-7\sqrt{-1}+\sqrt{2}+4\sqrt{-2}}{2} + \frac{-20+7\sqrt{-1}+14\sqrt{2}-5\sqrt{-2}}{3}\sqrt{\Delta}\right)^\tau \\
&= \frac{-1-7\sqrt{-1}-\sqrt{2}-4\sqrt{-2}}{2} + \frac{-20+7\sqrt{-1}-14\sqrt{2}+5\sqrt{-2}}{3}\,\frac{3}{\sqrt{\Delta}} \\
&= -\frac{1+7\sqrt{-1}+\sqrt{2}+4\sqrt{-2}}{2} + \sqrt{\Delta} = x_2.
\end{aligned}$$

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

$$\psi'(x_2^\sigma) = (\phi_{\alpha^\sigma,\beta^\sigma}(x_2^\sigma))^\tau = (\phi_{\alpha,\beta}(x_2))^{\sigma\tau} = (\phi_{\alpha,\beta}(x_2)^\tau)^{\sigma\rho^2} = \psi(x_2)^{\rho^2\sigma} = x_3^\sigma.$$

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 $\langle\tau\rangle$. 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 [14, Thm. 4.6, p.135] here. Instead, we must argue directly. Since p splits into two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of degree 2 in the field K, it will suffice to compute the Legendre symbol

$$\begin{aligned}
\left(\frac{\Delta}{\mathfrak{p}_1}\right) &= \left(\frac{(\sqrt{-1}-2\sqrt{2})(1+\sqrt{2})}{\mathfrak{p}_1}\right) \\
&\equiv (\sqrt{-1}-2\sqrt{2})^{(p^2-1)/2}(1+\sqrt{2})^{(p^2-1)/2} \pmod{\mathfrak{p}_1}.
\end{aligned}$$

Working with the first factor (mod $\mathfrak{p}_1$) gives

$$\begin{aligned}(\sqrt{-1}-2\sqrt{2})^{(p^2-1)/2} &\equiv \left(\frac{(\sqrt{-1}-2\sqrt{2})^p}{(\sqrt{-1}-2\sqrt{2})}\right)^{(p+1)/2} \equiv \left(\frac{(\sqrt{-1}+2\sqrt{2})^2}{-9}\right)^{(p+1)/2}\\ &\equiv (-1)^{(p+1)/2}\left(\frac{\sqrt{-1}+2\sqrt{2}}{3}\right)^{p+1}\\ &\equiv (-1)^{(p+1)/2}(-1)\equiv 1 \pmod{\mathfrak{p}_1}.\end{aligned}$$

In the same way we obtain

$$(1+\sqrt{2})^{(p^2-1)/2}\equiv(-1)^{(p+1)/2}(-1)\equiv 1 \text{ (mod } \mathfrak{p}_1),$$

and therefore $\left(\frac{\Delta}{\mathfrak{p}_1}\right)=1$, as claimed. Conjugating by σ 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 4.7 shows that there is a prime divisor $\mathfrak{P}$ of p in L whose decomposition group is $\langle\tau\rangle$, and this gives the assertion by the same arguments as before. ■

After the last two propositions, the result of our final proposition is similar to Proposition 4.6.

Proposition 4.9. *The factor $H_{-35}(t)^{4\delta_6}$ 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 α and β to be

$$\alpha=3+\sqrt{-7}+2\sqrt{5},\qquad \beta=3+\sqrt{-7}-2\sqrt{5}.$$

Then (α,β) 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

$$\begin{aligned}h(x)=x^{12}&+22x^{11}+199x^{10}-407x^9+\frac{1259}{2}x^8-295x^7+\frac{1275}{8}x^6+\frac{409}{8}x^5\\&+\frac{67}{16}x^4+\frac{37}{16}x^3+\frac{25}{32}x^2+\frac{3}{32}x+\frac{1}{256},\end{aligned}$$

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, $G = \mathrm{Gal}(L/\mathbb{Q}) = D_6$, the dihedral group of order 12, by a standard result in the theory of complex multiplication. In particular, $H = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{-35}))$ is cyclic and every element in G which does not fix $\mathbb{Q}(\sqrt{-35})$ has order 2.

We take $\sigma \in G$ to be complex conjugation and τ an automorphism which fixes $\sqrt{-7}$ and changes the sign of $\sqrt{5}$. Also, let ρ be a generator of H. Then $\sigma\tau = \rho^l$, for some l, since $\sigma\tau$ fixes $\sqrt{-35}$, and ρ^2 generates the group of the cyclic extension L/K, where $K = \mathbb{Q}(\sqrt{-7}, \sqrt{5})$. The automorphism τ is defined only up to a factor of ρ^{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 (4.9) shows that $\psi^2(x) = x$ for the roots of $f_2(x,\alpha) = 0$, so ψ has a fixed point x_1. If $x_2 = x_1^{\rho^2}$ and $x_3 = x_1^{\rho^4}$, then

$$\begin{aligned}\psi(x_2) = \psi(x_1^{\rho^2}) &= \phi_{\alpha,\beta}(x_1)^{\rho^2\tau} = \phi_{\alpha,\beta}(x_1)^{\tau\rho^4} \\ &= \psi(x_1)^{\rho^4} = x_1^{\rho^4} = x_3.\end{aligned}$$

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

$$\begin{aligned}\psi'(x_2^\sigma) &= (\phi_{\alpha^\sigma,\beta^\sigma}(x_2^\sigma))^\tau = (\phi_{\alpha,\beta}(x_2))^{\sigma\tau} = (\phi_{\alpha,\beta}(x_2))^{\rho^l} = (\phi_{\alpha,\beta}(x_2)^\tau)^{\tau\rho^l} \\ &= \psi(x_2)^{\tau\rho^l} = x_2^{\rho^2\tau\rho^l} = (x_2^\sigma)^{\sigma\rho^2\tau\rho^l} = (x_2^\sigma)^{\rho^{2l-2}}.\end{aligned}$$

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 ψ' fixes x_1^σ and interchanges x_2^σ and x_3^σ; while if $l = 1$, ψ' fixes x_2^σ and interchanges x_1^σ and x_3^σ. In either case, ψ' is not the identity on $E_{\alpha^\sigma}[2]$.

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

Thus, all our previous arguments apply, namely $X^\tau \equiv X^p \pmod{\mathfrak{P}}$, so the endomorphism μ_1 is given on X-coordinates of points in $\tilde{E}_\alpha = E_\alpha \pmod{\mathfrak{P}}$ by

$$X^{\mu_1} \equiv \psi(X) \pmod{\mathfrak{P}}, \qquad (X,Y) \in E_\alpha,$$

and the endomorphism μ_2' on points of $\tilde{E}_{\alpha^\sigma}$ by

$$X^{\mu_2'} \equiv \psi'(X) \pmod{\mathfrak{P}} \qquad (X,Y) \in E_\alpha^\sigma.$$

Finally, the endomorphism μ_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 (4.7), it is easily checked that we may take ι to be defined on X-coordinates by

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

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 (γ, ξ) are in $\ker(\mu_2)$ and therefore $\ker(\mu_2) \neq \ker(\mu_1)$. Hence, μ_1 and μ_2 are two independent endomorphisms of $\tilde{E}_\alpha$ in characteristic p with $\mu_i^2 = -3p$, neither of which is the trivial permutation on $\tilde{E}_\alpha[2]$. This proves the proposition. ■

Taken together, Lemma 4.2 and Propositions 4.3-4.9 imply Theorem 1.3. As a corollary we have the following analogy to Theorems 3.2 and 3.4.

Theorem 4.10. *For $p \equiv 1$ (mod 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 $H_{-35}(t)$ (mod p) which divide $H_{-3p}(t)$ (mod p), and $n_{3,2}$ the number of those factors which divide $H_{-12p}(t)$ (mod p). Then the class number $h(-3p)$ satisfies the following two equations:*

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

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 1.3:

$$\begin{aligned} h(-3p) &= 2\delta_1 + 4\delta_2 + 4\delta_4 + 4\delta_5 + 4n_{3,1}, \\ (a_p - 1)h(-3p) &= 2\delta_1 + 4\delta_3 + 4\delta_4 + 4\delta_5 + 8\delta_6 + 4n_{3,2}, \end{aligned}$$

and then subtracting the second equation from $(a_p - 1)$ times the first. ■

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 $Q_3(c,d) \equiv 0 \pmod p$.

Theorem 4.10 and its corollary give the means for determining the numbers of irreducible quadratic factors in the two products in Theorem 1.3. For example, when $p = 233$, the formulas in Theorem 4.10 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:

$$\begin{aligned} H_{-3\cdot 233}(t) &\equiv (t - 54000)^2 H_{-20}(t)^2 (t^2 + c_1 t + d_1)^2 \\ &\equiv (t + 56)^2 (t^2 + 25t + 109)^2 (t^2 + c_1 t + d_1)^2 \pmod{233}, \end{aligned}$$

and

$$\begin{aligned} H_{-12\cdot 233}(t) &\equiv t^2 (t + 32768)^4 H_{-20}(t)^2 H_{-35}(t)^4 \prod_{i=2}^{4} (t^2 + c_i t + d_i)^2 \\ &\equiv t^2 (t + 148)^4 (t^2 + 25t + 109)^2 (t^2 + 162t + 216)^4 \\ &\quad \times \prod_{i=2}^{4} (t^2 + c_i t + d_i)^2 \pmod{233}. \end{aligned}$$

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 α and $\beta = \alpha^p$ in $\mathbb{F}_{p^2}$ for which

$$j = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}, \qquad 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3.$$

Then $t^2 + ct + d$ will divide $H_{-3p}(t)$ if and only if the endomorphism μ given by (4.2) or (4.5) is the trivial permutation on the X-coordinates of points in $E_\alpha[2]$. By the arguments in [11, pp. 273-274] there is only one independent endomorphism μ in $\mathrm{End}(E_\alpha)$ 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 $q(t) = (t^2 + c_1 t + d_1) = (t^2 + 81t + 81)$ divides $H_{-3\cdot 233}(t) \pmod{233}$. We take

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

so that (α, β) 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

$$x_1 = 78 - 34\sqrt{-5}, \qquad x_2 = 75 - 109\sqrt{-5}, \qquad x_3 = 37 - 31\sqrt{-5}$$

in $\mathbb{F}_{233^2}$. Using (4.5) one can check easily that $x_i^\mu = x_i$ for all of these values. Hence $q(t)$ certainly divides $H_{-3\cdot 233}(t)$ (mod 233), and we have finally that

$$\begin{aligned} H_{-3\cdot 233}(t) &\equiv (t+56)^2(t^2+25t+109)^2(t^2+81t+81)^2, \\ H_{-12\cdot 233}(t) &\equiv t^2(t+148)^4(t^2+25t+109)^2(t^2+162t+216)^4 \\ &\quad \times (t^2+55t+139)^2(t^2+147t+62)^2(t^2+169t+171)^2 \pmod{233}. \end{aligned}$$

To conclude, we note the following corollary of Theorems 1.1 and Theorem 1.3.

Theorem 4.11.

a) *If $p > 13$ is a prime with $p \equiv 1$ (mod 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 $p \equiv 1$ (mod 24), then $H_{-3p}(t)$ has no linear factors over $\mathbb{F}_p$.*

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

References

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

[2] D.A.Cox, *Primes of the Form $x^2 + ny^2$; Fermat, Class Field Theory, and Complex Multiplication*, John Wiley and Sons, 1989.

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

[4] M. Deuring, *Die Klassenkörper der komplexen Multiplikation, Enzyklopädie der mathematischen Wissenschaften*, Band 12, Heft 10, Teil II, 1958, 1–60.

[5] M. Deuring, *Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl*, Jahresber. Deutsch. Math. Verein. **54** (1944), 24–41.

[6] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Invent. Math. **89** (1987), 561–567.

[7] R. Fricke, *Lehrbuch der Algebra, III: Algebraische Zahlen*, Friedr. Vieweg u. Sohn, Braunschweig, 1928.

[8] M. Kaneko, D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, AMS/IP Studies in Advanced Mathematics, vol. 7, AMS and International Press, Providence, RI, 1998, 97–126.

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

[10] P. Morton, *Legendre polynomials and complex multiplication I*, J. Number Theory **130** (2010), 1718–1731.
[11] P. Morton, *The cubic Fermat equation and complex multiplication on the Deuring normal form*, Ramanujan J. of Math. **25** (2011), 247–275.
[12] B. Schoeneberg, *Elliptic Modular Functions, An Introduction*, in: Die Grundlehren der mathematischen Wissenschaften, Band 203, Springer, Berlin, 1974, 142–146.
[13] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer, Dordrecht, 2009.
[14] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, in: Graduate Texts in Mathematics, vol. 151, Springer, New York, 1994.

Address: Patrick Morton: Dept. of Mathematical Sciences, Indiana University – Purdue University at Indianapolis (IUPUI), Indianapolis, IN 46202-3216, USA.

E-mail: pmorton@math.iupui.edu

Received: 2 February 2013; **revised:** 6 November 2013