Ogg's theorem via explicit congruences for class equations
by
Patrick Morton

PR # 06-09

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

July 6, 2006
revised
September 10, 2008
Ogg’s theorem via explicit congruences for class equations

Patrick Morton

Dept. of Mathematics,
Indiana University – Purdue University at Indianapolis (IUPUI),
Indianapolis, IN 46202 – 3216, USA
e–mail : pmorton@math.iupui.edu
corresponding address : 1041 W. Auman Dr., Carmel, IN 46032

MSC2000: 11G15, 14H52, 11R11
Abstract

Explicit congruences (mod $p$) are proved for the class equations or the products of class equations corresponding to discriminants $D = -8p, -3p, -12p$ in the theory of complex multiplication, where $p$ is an odd prime. 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 $F_p$. The proof does not make use of any class number estimates. A corollary is that for $p \geq 13$ 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, quadratic field
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

\[
    r = r_p = \frac{1}{2}(1 - (-3/p)), \quad s = s_p = \frac{1}{2}(1 - (-4/p)).
\]

Then the supersingular polynomial is given by

\[
    ss_p(t) = t^r(t - 1728)^s J_p(t), \quad p > 3, \quad (1.1)
\]

with

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

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 \(-12p\). We make use of these congruences in [m3] 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 (Klassenpolynom) \(H_D(t)\) 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], [si2].) Congruences for the class equations $H_{-p}(t)$ and $H_{-4p}(t)$ 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:

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

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

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.

Using some classical results on the transformation polynomial (Invariantengleichung or modular equation) $\Phi_n(x, y)$ [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. $Q_n(-x - y, xy) = Q_n(x, y)$.

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:

$$H_{-8p}(t) \equiv (t-1728)^{2e_1}(t-8000)^{2e_2}(t+3375)^{4e_3}(t^2+191025t-121287375)^{4e_4}$$

$$\times \prod_i(t^2 + a_it + b_i)^2 \pmod{p},$$

where
\[ \epsilon_1 = \frac{1}{2} \left( 1 - \left( \frac{-4}{p} \right) \right), \]
\[ \epsilon_2 = \frac{1}{2} \left( 1 - \left( \frac{-8}{p} \right) \right), \]
\[ \epsilon_3 = \frac{1}{2} \left( 1 - \left( \frac{-17}{p} \right) \right), \]
\[ \epsilon_4 = \frac{1}{4} \left( 1 - \left( \frac{-15}{p} \right) \right) \left( 1 - \left( \frac{5}{p} \right) \right); \]

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

\[-4Q_2(a, b) = (2b+1485a-41097375)^2 + (4a-29025)(a-191025)^2 \equiv 0 \pmod{p}.\]

Since the degree of \( H_{-8p}(t) \) is the class number of the field \( \mathbb{Q}(\sqrt{-2p}) \), equating degrees in the congruence of Theorem 1.1 gives

**Corollary 1.2.** If \( p > 13 \) and \( h(-2p) \) is the class number of the quadratic field \( \mathbb{Q}(\sqrt{-2p}) \), then

\[ h(-2p) = 5 + \left( \frac{-3}{p} \right) - \left( \frac{-4}{p} \right) - \left( \frac{5}{p} \right) - 2 \left( \frac{-7}{p} \right) - \left( \frac{-8}{p} \right) - \left( \frac{-15}{p} \right) + 4\nu_2, \]

where \( \nu_2 \) is the number of irreducible quadratic factors \( t^2 + at + b \) of \( J_p(t) \) over \( \mathbb{F}_p \) for which \( Q_2(a, b) \equiv 0 \pmod{p} \).

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 \( \nu_2 = 2 \) and Corollary 1.2 gives \( h(-2 \cdot 233) = 0 + 4\nu_2 = 8 \).

**Corollary 1.3.** 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
\[
\frac{1}{2}(h(-2p) - 2\epsilon_3 - 4\epsilon_4) = \\
\frac{1}{2} \left( h(-2p) - 2 - \left( \frac{-3}{p} \right) + \left( \frac{5}{p} \right) + \left( \frac{-7}{p} \right) + \left( \frac{-15}{p} \right) \right).
\]

The next congruence involves the class equations for the orders \(O_{-3p}\) and \(O_{-12p}\) in the field \(\mathbb{Q}(\sqrt{-3p})\).

**Theorem 1.4.** 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 \(1 \pmod{4}\). Then we have the congruence

\[
K_{3p}(t) \equiv t^{2\delta_1}(t - 54000)^{2\delta_1}(t - 8000)^{4\delta_2}(t + 32768)^{4\delta_3}
\times H_{-20}(t)^{4\delta_4}H_{-32}(t)^{4\delta_5}H_{-35}(t)^{4\delta_6} \prod_i (t^2 + c_i t + d_i)^2 \pmod{p};
\]

where

\[
\delta_1 = \frac{1}{2}(1 - \left( \frac{-3}{p} \right)), \\
\delta_2 = \frac{1}{2}(1 - \left( \frac{-5}{p} \right)), \\
\delta_3 = \frac{1}{2}(1 - \left( \frac{-7}{p} \right)), \\
\delta_4 = \frac{1}{4}(1 - \left( \frac{-3}{p} \right))(1 - \left( \frac{-5}{p} \right)), \\
\delta_5 = \frac{1}{4}(1 - \left( \frac{-2}{p} \right))(1 - \left( \frac{-5}{p} \right)), \\
\delta_6 = \frac{1}{4}(1 - \left( \frac{-35}{p} \right))(1 - \left( \frac{-5}{p} \right));
\]

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

\[
H_{-20}(t) = t^2 - 1264000 t - 681472000, \\
H_{-32}(t) = t^2 - 522500000 t + 12167000000, \\
H_{-35}(t) = t^2 + 117964800 t - 134217728000;
\]

and the 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

\[
Q_3(c, d) = -2^{45}3^9 c + 2^{30}3^5 5^6 c^2 - 2^{15}3^2 5^3 c^3 + c^4 - 2^{34}5^9 \cdot 23d
\]
\[-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}\equiv 0 \pmod{p}.

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

$$a_{p} = \begin{cases} 4, & \text{if } p \equiv 1 \pmod{8}, \\ 2, & \text{if } p \equiv 5 \pmod{8}, \\ 1, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{1.3}$$

Hence we have

**Corollary 1.5.** If $p > 53$, $h(-3p)$ is the class number of $\mathbb{Q}(\sqrt{-3p})$, and $a_{p}$ is defined in (1.3), then

\[
\begin{align*}
a_{p}h(-3p) &= 9 - 2\left(\frac{-3}{p}\right) + 2\left(\frac{-4}{p}\right) - 2\left(\frac{5}{p}\right) + \left(\frac{-7}{p}\right) - \left(\frac{8}{p}\right) \\
&\quad - 3\left(\frac{-8}{p}\right) - 2\left(\frac{-11}{p}\right) - \left(\frac{-20}{p}\right) - \left(\frac{-35}{p}\right) + 4\nu_{3},
\end{align*}
\]

where $\nu_{3}$ is the number of irreducible quadratic factors $t^{2} + ct + d$ of $J_{p}(t)$ over $\mathbb{F}_{p}$ for which $Q_{3}(c, d) \equiv 0 \pmod{p}$.

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 $4h(-3\cdot 233) = 16 + 4\nu_{3} = 16 + 4\cdot 6 = 40$ and $h(-3\cdot 233) = 10$.

**Corollary 1.6.** 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

$$\frac{1}{2}(a_{p}h(-3p) - 2\delta_{2} - 2\delta_{3} - 4\delta_{4} - 4\delta_{5} - 4\delta_{6}).$$

The factor $H_{-15}(t)$ in Theorem 1.1 and the factors $H_{-20}(t), H_{-32}(t)$ and $H_{-35}(t)$ in Theorem 1.4 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 $\epsilon_4$ and the $\delta_i$. By Deuring’s theory of reduction [d1], the irreducible factors in Theorems 1.1 and 1.4 must be factors of $ss_p(t)$. Thus, we have:

**Theorem 1.7.** The polynomial $J_p(t)$ has irreducible quadratic factors over $F_p$ 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 $F_p$ 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 over $Q$ 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 $Z$ (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 $Z$, 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

$$b_p = 1/2, 2 \text{ or } 1 \text{ according as } p \equiv 1 \text{ (mod 4)}, 3 \text{ (mod 8)} \text{ or } 7 \text{ (mod 8)}.$$ 

Since $ss_p(t)$ has distinct roots over $F_p$, 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
By equating degrees of the linear factors in Theorems 1.1 and 1.4, we have the following necessary conditions for $p$ to be one of Ogg’s primes:

\[ h(-2p) = 4 - (-4/p) - (-8/p) - 2(-7/p), \]
\[ a_p h(-3p) = 6 - 2(-3/p) - 2(-8/p) - 2(-11/p). \] (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 1.8** If $p \geq 13$, 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 1.4 that it is possible to prove separate congruences for $H_{-3p}(t)$ and $H_{-12p}(t) \pmod{p}$, when $p \equiv 1 \pmod{4}$. We can show that

\[
H_{-3p}(t) \equiv (t - 54000)^{2\delta_1} (t - 8000)^{4\delta_2} H_{-20}(t)^{2\delta_4} H_{-32}(t)^{2\delta_5} \prod_i (t^2 - c_i t + d_i)^2, \\
H_{-12p}(t) \equiv t^{2\delta_1} (t + 32768)^{4\delta_1} H_{-20}(t)^{2\delta_4} H_{-32}(t)^{2\delta_5} H_{-35}(t)^{4\delta_6} \prod_i' (t^2 + c_i' t + d_i')^2 \pmod{p},
\]

with the same notation as in Theorem 1.4, where the products $\Pi$ and $\Pi'$ in these congruences have no factors in common. The proof is rather involved, and not directly relevant to the proof of Ogg’s theorem, so we do not include it here.

In the papers [m3] we also show how the explicit congruences in Theorems 1.1 and 1.4 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 the explicit congruences used here.

In an appendix we give an algorithm for computing the transformation polynomial $\Phi_n(x, y)$ 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 transformation polynomial, or *Invariantengleichung* $\Phi_n(x, y)$, 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

$$\Phi_p(t, j) \equiv (t^p - j)(t - j^p) \pmod{p}. \quad (2.1)$$

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

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

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

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

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 \( H_O(x) \) stand for 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] that

\[
\Phi_{dp}(t, t) = H_{-4dp}(t) \cdot \prod_{O} H_O(t)^{r(O, dp)}, \text{ if } dp \equiv 1, 2 \pmod{4},
\]

\[
\Phi_{dp}(t, t) = H_{-dp}(t)H_{-4dp}(t) \cdot \prod_{O} H_O(t)^{r(O, dp)}, \text{ if } dp \equiv 3 \pmod{4}, \quad (2.5)
\]

where

\[
r(O, m) = |\{\alpha \in O : \alpha \text{ is primitive, } N(\alpha) = m\}/O^*|,
\]
and \( r(O, dp) = 0 \) or \( r(O, dp) \geq 2 \) for all the terms occurring in the above products.

In the lemma 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

\[
dp \text{ or } 4dp = x^2 + Dy^2, \quad (x, y) = 1.
\]

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.

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 $tj$ 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:

$$\Phi_2(t,j) = t^3 - t^2 \cdot (j^2 - 1488j + 162000) + t \cdot (1488j^2 + 40773375j + 8748000000) + j^3 - 162000j^2 + 87480000000j - 1574640000000000,$$

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

$$disc_t(\Phi_2(t,j)) = 4(j - 1728) \cdot j^2 \cdot (j + 3375)^2 \cdot (j^2 + 191025j - 121287375)^2.$$  

Also,

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

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

$$disc_t(\Phi_3(t,j)) = -27j^2(j - 1728)^2(j - 8000)^2(j + 32768)^2.$$  

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]:

13
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

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

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 \( p = 3 \), 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

\[
 H_{-8}(j) = j - 8000, H_{-11}(j) = j + 32768.
\] (2.6)

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

\[
 H_{-20}(j) = j^2 - 1264000j - 681472000,
\]

\[
 H_{-32}(j) = j^2 - 52250000j + 12167000000,
\] (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 \((\pmod{73})\). Since 73 = \((1 + 6\sqrt{-2})(1 - 6\sqrt{-2})\) splits into primes which lie in the principal ring class \((\pmod{2})\) in \(\Omega = Q(\sqrt{-2})\), 73 splits completely in the ring class field \((\pmod{2})\) 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 \(Q(\sqrt{5})\). 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].

We now prove a theorem about the multiplicity of factors of \(\Phi_2(t^p, t) \pmod{p}\).

**Proposition 2.4.** If \(p\) is a prime > 3, the multiplicity of an irreducible factor of \(\Phi_2(t^p, t) \pmod{p}\) 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 \(F_p[t, j]\). 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,
\[ F_1(t, j) = 3t^2 - 2t(j^2 - 1488j + 162000) + 1488j^2 + 40783375j + 8748000000, \]

so that

\[ \frac{d}{dt}(F(t, t^p)) = 3t^2 - 2t(t^{2p} - 1488t^p + 162000) + 1488t^{2p} + 40783375t^p + 8748000000, \]

\[ = -2t^{2p+1} + 1488t^{2p} + 2976t^{p+1} + 40783375t^p + 3t^2 - 324000t + 8748000000. \]

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 (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, \((\Phi_2(t, t^p))^n\) is never 0 (mod \(p\)), 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 \(H_{-8p}(t) \pmod{p}\) 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 [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 \(\Phi_2(t^{11}, t) \pmod{11}\), but \(t\) (the other factor of \(ss_{11}(t)\)) does not.

**Corollary 2.6.** For \(p > 3\) the only linear factor of \(\Phi_2(t^p, t) \pmod{p}\) 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 $\Phi_2(t^p, t) \pmod{p}$ are $(t-1728), (t-8000), \text{ and } (t+3375)$. By the computations in the proof of Proposition 2.4, we also have that

$$\frac{d}{dt}(F(t, t^p)) \equiv -2t^3 + 4467t^2 + 40449375t + 8748000000$$
$$\equiv -(t + 3375)(2t^2 - 11217t - 2592000)$$
$$\equiv -(t + 3375)f(t) \pmod{p},$$

for $t$ an element of $F_p$. Hence $(t + 3375)$ is certainly a multiple factor of $\Phi_2(t^p, t) \pmod{p}$. 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 $\Phi_2(t^p, t) \pmod{p}$ 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 $\Phi_3(t^p, t) \pmod{p}$ 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

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

18
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

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

(2.8)

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

$$Q(u, v) = u^4 - 36864000u^3 + 452984832000000u^2 - 18554258718720000000000u$$

$$- 1069960u^2v - 2232uv^2 - 890011238400uv$$

$$- v^2 + 2590058000v^2 - 77175193600000000v$$

$$= u^4 - 2^{15} \cdot 3^2 \cdot 5^3 \cdot u^3 + 2^{30} \cdot 3^3 \cdot 5^6 \cdot u^2 - 2^{45} \cdot 3^3 \cdot 5^9 \cdot u$$

$$- 2^3 \cdot 5 \cdot 23 \cdot 1163 \cdot u^2v - 2^3 \cdot 3^2 \cdot 31 \cdot uv^2 - 2^{15} \cdot 3^3 \cdot 5^3 \cdot 23 \cdot 3499 \cdot uv$$

$$- v^2 + 2^4 \cdot 5^3 \cdot 109^3 \cdot v^2 - 2^{34} \cdot 5^9 \cdot 23 \cdot v.$$

This yields the following partial derivatives:

$$Q_{11}(u, v) = 2^2 \cdot 3 \cdot u^2 - 2^{16} \cdot 3^3 \cdot 5^3 \cdot u + 2^{31} \cdot 3^3 \cdot 5^6 - 2^4 \cdot 5 \cdot 23 \cdot 1163 \cdot v,$$

$$Q_{12}(u, v) = -2^4 \cdot 5 \cdot 23 \cdot 1163 \cdot u - 2^4 \cdot 3^2 \cdot 31 \cdot v - 2^{15} \cdot 3^3 \cdot 5^3 \cdot 23 \cdot 3499,$$

$$Q_{22}(u, v) = -2^4 \cdot 3^2 \cdot 31 \cdot u - 2 \cdot 3 \cdot v + 2^5 \cdot 5^3 \cdot 109^3.$$

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 (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

$$\gcd(D_1, D_2) = 2^{17} \cdot 3 \cdot 5^3 \cdot 13 \cdot 37 \cdot 53, \text{ if } H_{-20}(t) \equiv 0 \pmod{p};$$

$$\gcd(D_1, D_2) = 2^{11} \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 37 \cdot 53, \text{ if } H_{-32}(t) \equiv 0 \pmod{p};$$

19
\[ \gcd(D_1, D_2) = 2^{16} \cdot 3^3 \cdot 7 \cdot 37 \cdot 53, \text{ if } H_{-35}(t) \equiv 0 \pmod{p}. \]

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 \( \Phi_3(t^p, t) \) shows that \( t = 0, 8000, -32768, \) or 54000. We have, using the congruences

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

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

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

while

\[
\begin{align*}
F''(54000) &\equiv -2^{16} \cdot 3^3 \cdot 5^6 \cdot 17 \cdot 23 \cdot 29 \cdot 89 \cdot 1153, \\
F'(54000) &\equiv -2^{19} \cdot 3^3 \cdot 5^9 \cdot 11^2 \cdot 17^2 \cdot 23^2 \cdot 29^2. \tag{2.9}
\end{align*}
\]

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
\[ F'(t) \equiv -Q_1(2t, t^2) + tQ_2(-2t, t^2) \pmod{p}, \]
\[ = -3t^5 + 2^3 \cdot 3^2 \cdot 5 \cdot 31 \cdot t^4 + 2^{12} \cdot 1262587 \cdot t^3 \]
\[ + 2^{15} \cdot 3^3 \cdot 5^4 \cdot 109 \cdot 443 \cdot t^2 - 2^{32} \cdot 5^6 \cdot 7 \cdot 11 \cdot 149 \cdot t + 2^{45} \cdot 3^3 \cdot 5^9 \]
\[ = -(t + 32768)(t - 8000)(3t^3 - 85464t^2 - 2268352000t + 7077888000000). \]

We also have modulo \( p \) that \( F'(0) \equiv 2^{45} \cdot 3^3 \cdot 5^9 \). Equation (2.9) and Proposition 2.7 now imply the assertions of the corollary.

### 3 Explicit congruences for class equations.

The following theorem is preparation for the proof of the explicit congruences in Theorems 1.1 and 1.4. 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

\[ K_{dp}(t) = H_{-4dp}(t) \text{ or } H_{-dp}(t)H_{-4dp}(t) \]

according as \( dp \equiv 1, 2 \) or \( dp \equiv 3 \) (mod 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 \( (t - 1728), (t - 8000), \) and \( (t + 3375) \) are the only possible linear factors of \( H_{-sp}(t) \) over \( \mathbb{F}_p \), and that these factors occur in \( H_{-sp}(t) \) 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 \( H_{-sp}(t) \) (mod \( p \)) to a power higher than 2, because it is the only such quadratic dividing \( \Delta_3(t) \). Its roots are supersingular and quadratic over \( \mathbb{F}_p \) exactly when \( \epsilon_4 = 1 \). Further, it must divide \( H_{-sp}(t) \) when \( \epsilon_4 = 1 \), 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 \( (\Phi_2(t^p, t))^\prime \) 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 \( H_{-sp}(t) \) (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 \( H_{-sp}(t) \) (mod \( p \)) when \( \epsilon_4 = 0 \), or (wlog) when \( (\hat{2}) = +1 \). But in that case \( H_{-15}(t) \) has two linear factors (mod \( p \)), and any contribution to the factorization of \( H_{-sp}(t) \) 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 the integers \( H_{-15}(1728), H_{-15}(8000), H_{-15}(-3375) \).

All other irreducible quadratic factors of \( H_{-sp}(t) \) (mod \( p \)) 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 \( H_{-sp}(t) \), by Lemma 2.3 and the above argument. This completes the proof.
Corollary 1.2 of the Introduction follows immediately from this theorem, since

\[ h(-2p) = \deg H_{-8p}(t) = 2\epsilon_1 + 2\epsilon_2 + 4\epsilon_3 + 8\epsilon_4 + 4(\nu_2 - \epsilon_4). \]

Corollary 1.3 is also immediate, since the count given in this corollary is just the number of distinct roots of \( H_{-8p}(t) \) (mod \( p \)).

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

**Proof of Theorem 1.4.** 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 \( K_{3p}(t) \) (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

\[ H_{-20}(t) = t^2 - 1264000t - 681472000, \]

\[ H_{-32}(t) = t^2 - 5225000t + 12167000000, \]

\[ H_{-35}(t) = t^2 + 117964800t - 134217728000, \]

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

\[ \frac{\partial}{\partial u} Q(u, v) = 2^2 u^3 - 2^{15} \cdot 3^3 \cdot 5^3 u^2 + 2^{31} \cdot 3^3 \cdot 5^6 u - 2^{45} \cdot 3^3 \cdot 5^9 - 2^4 \cdot 5 \cdot 23 \cdot 1163uv \]
\[ -2^3 \cdot 3^2 \cdot 31v^2 - 2^{15} \cdot 3^3 \cdot 5^3 \cdot 23 \cdot 3499v, \]

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

\[ -3v^2 + 2^5 \cdot 5^3 \cdot 109^3 \cdot v - 2^{34} \cdot 5^9 \cdot 23, \]

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 is a double factor of \( \Phi_3(t^p, t) \) whenever it is irreducible (mod \( p \)). By Lemma 2.3 these quadratics divide \( K_{3p}(t) \pmod{p} \) 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 \( \mathbb{Q}(\sqrt{3}) \) 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 \( K_{3p}(t) \pmod{p} \) 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.

Corollary 1.5 of the Introduction is immediate from the congruence in Theorem 1.4, since \( \deg K_{3p}(t) = a_p h(-3p) \), by (1.3) and the well-known relationship between the classnumbers \( h(O_{-3p}) \) and \( h(O_{-12p}) \) in [co, p. 146].

4 A Proof of Ogg’s Theorem.

As noted in the introduction, Theorems 1.1 and 1.4 allow us to give the following proof of Ogg’s Theorem. It is trivial that \( ss_p(x) \) is a linear polynomial for \( p = 2, 3, 5, 7, 13 \), and that \( ss_{11}(x) = x(x - 1728) \) 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 \( ss_p(t) \) splits into linear factors over \( \mathbf{F}_p \). 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
\[ h(-2p) = 2\varepsilon_1 + 2\varepsilon_2 + 4\varepsilon_3 = 4 - \left( -\frac{4}{p} \right) - \left( -\frac{8}{p} \right) - 2\left( -\frac{7}{p} \right), \quad p > 13. \]  \hspace{1cm} (4.1)

Considering the different residue classes of \( p \) (mod 8), we find that
\begin{align*}
    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}.
\end{align*}

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 \( H_{-8p}(t) \) (mod \( p \)), 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 1.4. This gives respectively,
\begin{align*}
    (5/p) &= +1 \text{ or } (-5/p) = +1; \\
    (2/p) &= +1 \text{ or } (-2/p) = +1; \hspace{1cm} (4.2) \\
    (5/p) &= +1 \text{ or } (-35/p) = +1.
\end{align*}

The second of these conditions shows that \( p \) cannot be \( 5 \) (mod 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
\[ a_p h(-3p) = 4\delta_1 + 4\delta_2 + 4\delta_3 = 6 - 2\left( -\frac{3}{p} \right) - 2\left( -\frac{8}{p} \right) - 2\left( -\frac{11}{p} \right), \quad p > 53, \]  \hspace{1cm} (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

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

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:

$$
\begin{align*}
2401 &= 1^2 + 2 \cdot 3 \cdot 20^2, \quad 13^2 + 2 \cdot 31 \cdot 6^2, \quad 15^2 + 2 \cdot 17 \cdot 8^2, \quad 31^2 + 2 \cdot 5 \cdot 12^2, \\
&\text{or } 2401 = 33^2 + 2 \cdot 41 \cdot 4^2, \quad 45^2 + 2 \cdot 47 \cdot 2^2. \quad (4.5)
\end{align*}
$$

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 $\chi_p(q) = (Nq/p)$, 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 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 modulo 131 and \( ss_{167}(x) \) factors into a product of linears times two irreducible quadratics modulo 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

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

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 \( \chi_p(q) = (Nq/p) \) 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

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

27
or $2662 = 35^2 + 3 \cdot 479, \ 29^2 + 3 \cdot 607, \ 1^2 + 3 \cdot 887;$

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

$$g_2(p) = 4 - (-4/p) - (-8/p) - 2(-7/p),$$

$$g_3(p) = 6 - 2(-3/p) - 2(-8/p) - 2(-11/p),$$

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.

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 in (1.3).
This theorem is equivalent to Theorem 1.8 of the Introduction.

Table 1: Comparison of \( h(-2p) \) with \( g_2(p) \) and \( a_p h(-3p) \) 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 Appendix: Computing the Transformation Polynomial \( \Phi_n(t, j) \).

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

$$E_2 : v^2 + d_1uv + d_3v = u^3 + d_2u^2 + d_4u + d_6,$$

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

$$E_1 : Y^2 + aXY + bY = X^3 + bX^2. \quad (A.1)$$

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 $\tau = \tau_{O→-P}$ 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 $A(x), B(x)$. 

30
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

$$\Phi_n(j(E_2), j(E_1)) = 0 \text{ over } k. \quad (A.2)$$

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

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

In other words, the affine curve $\Phi_n(t, j) = 0$ is the projection of the open algebraic set $\subset \mathbb{A}^4$ 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 $\Phi_n(t, j)$ 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
$k[j]$, $j = j(E_1)$. For example, when $n$ is prime, we can express $t^{n+1}$ as a linear combination of $1, t, \ldots, t^n$ 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 $d = [k(a, b) : k(b)] = \deg f_n(a, b)$. 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 $(x, y)^T = (x, y) + (0, 0)$, where

$$x^T = \frac{-y}{x^2}, \quad y^T = \frac{-y}{x^3}.$$

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 \( j(E_2) = \alpha^3(\alpha^3 + 216)/(\alpha^3 - 27)^3 \). 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

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

\[
3^{18} \cdot \{ t^4 + (-j^3 + 2232j^2 - 1069956j + 36864000)t^3 + \\
(2232j^3 + 2587918086j^2 + 890022976000j + 452984832000000)t^2 + \\
(-1069956j^3 + 8900222976000j^2 - 77084596636000000j + 1855425871872000000000)t + \\
j^4 + 36864000j^3 + 452984832000000j^2 + 1855425871872000000000j \}
\]

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

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

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

The quantities $u = x + x^{r^2}$ and $v = y + y^{r^2}$ 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

$$\text{Resultant}_b((1 - 16b + 16b^2)^3 - jb^4(1 - 16b), (1 - 16b + 256b^2)^3 - tb^2(16b - 1)^2)$$

$$= 2^{48} \cdot (t^3 - 162000t^2 + 8748000000t - 157464000000000 + 1488jt^2$$

$$+ 40773375jt + 8748000000j - j^2t^2 + 1488j^2t - 162000j^2 + j^3)^2$$

$$= 2^{48} \cdot \Phi_2(t, j)^2.$$

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 $K_{pd}(t) \pmod{p}$. For the computation of $H_D(t) \pmod{p}$ for a prime $p$ not dividing $D$, see [alv].

**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

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

and

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

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 \( j = t \). In this way one can see that 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

\[
\Phi_5(t, j) \equiv t^6 + (232j^5 + 225j^4 + 16j^3 + 76j^2 + 88j + 41)t^5 \\
+ (225j^5 + 55j^4 + 87j^3 + 28j^2 + 3j + 219)t^4 \\
+ (16j^5 + 87j^4 + 21j^3 + 71j^2 + 19j + 23)t^3 \\
+ (76j^5 + 28j^4 + 71j^3 + 203j^2 + 38j + 169)t^2 \\
+ (88j^5 + 3j^4 + 19j^3 + 38j^2 + 118j + 96)t \\
+ (j^6 + 41j^5 + 219j^4 + 23j^3 + 169j^2 + 96j + 31) \pmod{233}.
\]

Using this expression and the factorization of the polynomial \( s_233(t) = tJ_{233}(t) \) given in the introduction, we find that

\[ \gcd(\Phi_5(t^{233}, t), tJ_{233}(t)) = (t + 148)(t^2 + 64t + 57)(t^2 + 81t + 81) \]

\[ \times (t^2 + 147t + 62)(t^2 + 162t + 216) \pmod{233}. \]

36
Note that the quadratic factors of $\Phi_d(t^p, t)$ over $\mathbb{F}_p$ can be easily determined using the fact that $q(t) = t^2 + at + b$ divides $\Phi_d(t^p, t)$ 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 $h(-5 \cdot 233) = 20$.

### 6 References


[m3] P. Morton, Legendre polynomials and complex multiplication I (submitted) and II (preprint).


