Journal of Number Theory 130 (2010) 1718–1731

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Legendre polynomials and complex multiplication, I

Patrick Morton[*]

Dept. of Mathematics, Indiana University - Purdue University at Indianapolis (IUPUI), Indianapolis, IN 46202-3216, USA

ARTICLE INFO

Article history:
Received 24 August 2007
Revised 5 March 2010
Available online 13 May 2010
Communicated by David Goss

MSC:
11C08
11G07
14K22

Keywords:
Legendre polynomial
Class number
Elliptic curve
Multiplier
Finite field
Factorization

ABSTRACT

The factorization of the Legendre polynomial of degree $(p-e)/4$, where p is an odd prime, is studied over the finite field $\mathbf{F}_p$. It is shown that this factorization encodes information about the supersingular elliptic curves in Legendre normal form which admit the endomorphism $\sqrt{-2p}$, by proving an analogue of Deuring's theorem on supersingular curves with multiplier $\sqrt{-p}$. This is used to count the number of irreducible binomial quadratic factors of $P_{(p-e)/4}(x)$ over $\mathbf{F}_p$ in terms of the class number $h(-2p)$.

1. Introduction

In this paper I continue the investigation begun in [brm] on the relationship between the factorization of certain Legendre polynomials $P_n(x)$ (mod p), multipliers (or endomorphisms) on elliptic curves, and class numbers of special quadratic fields. It turns out that the existence of special multipliers on supersingular elliptic curves is reflected by relationships involving class numbers in modular factorizations of $P_n(x)$.

The investigation of this paper was motivated by the empirical discovery of the following fact. It concerns the number of binomial quadratic factors (*bqf*'s), or irreducible factors of the form x^2+a, of the Legendre polynomial $P_{(p-e)/4}(x)$ over the finite field of p elements, where p is an odd prime with $p \equiv e$ (mod 4) and $e = 1$ or 3.

[*] Address for correspondence: 1041 W. Auman Dr., Carmel, IN 46032, United States.
E-mail address: pmorton@math.iupui.edu.

0022-314X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2010.03.009

Theorem 1.1. *If p is an odd prime, then the number of distinct, irreducible, binomial quadratic factors of $P_{(p-e)/4}(x) \pmod p$, is $(h(-2p) - d_p)/4$, where $h(-2p)$ is the class number of the field $\mathbf{Q}(\sqrt{-2p}\,)$ and*

$$d_p = 2 - \left(\frac{-4}{p}\right) - \left(\frac{-8}{p}\right) = 0, 2, 2, 4$$

according as $p \equiv 1, 3, 5, 7 \pmod 8$.

In [brm] the number of binomial quadratic factors of the Legendre polynomial $P_{(p-1)/2}(x) \pmod p$ was calculated to be

$$N_2\big(p, (p-1)/2\big) = \begin{cases} h(-p)/2, & \text{if } p \equiv 1 \pmod 4, \\ (mh(-p) - 1)/2, & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

where $m = 3$ or 1 according as p is 3 or 7 (mod 8). The occurrence of the class number $h(-p)$ in this formula was seen to be a consequence of the fact that $P_{(p-1)/2}(x)$ is related to the Hasse invariant of the elliptic curve

$$E_\lambda\colon\ Y^2 = X(X-1)(X-\lambda). \tag{1.1}$$

The expression for $N_2(p, (p-1)/2)$ reflects two aspects of the arithmetic on this curve, when E_λ is supersingular: 1) a criterion in terms of λ for the existence of a multiplier μ in $\mathrm{End}(E_\lambda)$ for which $\mu^2 = -p$; and 2) a complete factorization of the class equations $H_{-p}(t)$ and $H_{-4p}(t)$ modulo p.

As in [brm], the proof of Theorem 1.1 relies on a criterion, expressed in terms of λ, for the curve E_λ to have a special multiplier; and a factorization of the class equation $H_{-8p}(t) \pmod p$.

I use the term *multiplier* for what Hasse [h1] and Deuring [d] call a normalized meromorphism, which is any isomorphism $\mu : z \to z^\mu$ of the function field $K = \bar{\mathbf{F}}_p(x, y)$ of the curve (1.1) into itself which leaves all constants fixed and for which the prime divisor $\mathbf{o}$ at infinity on (1.1) is a pole divisor of x^μ and y^μ. Such a meromorphism determines an endomorphism on the curve, and every endomorphism of E_λ gives rise to a meromorphism of K, so that the meromorphism ring of K and the endomorphism ring of E_λ can be naturally identified (see [d] and [brm, Section 2]).

The multiplier criterion which is needed for the proof of Theorem 1.1 will be proved in the following form. For its statement recall the definition of the polynomial

$$W_n(t) = (1-t)^n P_n\left(\frac{1+t}{1-t}\right) = \sum_{k=0}^{n} \binom{n}{k}^2 t^k.$$

As is well known, the roots of $W_{(p-1)/2}(t)$ over $\mathbf{F}_p$ are the λ's for which the curve E_λ is supersingular. We know from [brm, Proposition 1] that these values of λ all lie in $\mathbf{F}_{p^2}$, so that irreducible factors of $W_{(p-1)/2}(t)$ over $\mathbf{F}_p$ are exclusively linear or quadratic.

Theorem 1.2. *Let the elliptic curve E_λ be supersingular, where λ is a root of the polynomial $t^2 + ut + v$ over $\mathbf{F}_p$, which is either an irreducible factor of $W_{(p-1)/2}(t) \pmod p$ or $(t-\lambda)^2$, when λ is in $\mathbf{F}_p$. Then there exists a multiplier μ in $\mathrm{End}(E_\lambda)$ satisfying $\mu^2 = -2p$ if and only if one of the following three congruences holds*:

$$(u + v + 1)^2 \equiv 16v \pmod p,$$

$$v^2 \equiv 16(u + v + 1) \pmod p,$$

$$16(u + v + 1)v \equiv 1 \pmod p.$$

When it exists, this multiplier μ is always defined over the field $\mathbf{F}_{p^2}$.

This theorem is a natural analogue of Deuring's theorem that $\sqrt{-p}$ is a multiplier for the curve if and only if its j-invariant lies in $\mathbf{F}_p$. To see this, we use the fact, proved in [brm, Proposition 6], that j lies in $\mathbf{F}_p$ if and only if the corresponding values of λ, which can be computed from the formula

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{(\lambda^2 - \lambda)^2}, \tag{1.2}$$

either lie in $\mathbf{F}_p$ themselves, or satisfy irreducible quadratics over $\mathbf{F}_p$ of one of the forms $t^2 - t + v$, $t^2 + ut + 1$, $t^2 + ut - u$. If we consider a λ in $\mathbf{F}_p$ to satisfy the polynomial $(t - \lambda)^2$, we obtain the following restatement of Deuring's result:

> $\sqrt{-p}$ is a multiplier on the supersingular curve E_λ if and only if λ satisfies $t^2 + ut + v = 0$ over $\mathbf{F}_p$, where $(u+1)(v-1)(u+v)(u^2 - 4v) \equiv 0 \pmod{p}$.

In Section 2 I give a simple proof of Deuring's criterion from the formulas for the multiplier $\sqrt{-p}$ developed in [brm, Section 3], without using Deuring's theory [d]. In Section 3, the analogous idea is used to prove Theorem 1.2 for the multiplier $\sqrt{-2p}$ in place of $\sqrt{-p}$.

In Section 4 the proof of Theorem 1.1 is completed by showing that (for $p > 13$) the binomial quadratic factors of $P_{(p-e)/4}(x) \pmod{p}$ are in 1–1 correspondence with the pairs of irreducible quadratic factors $\pmod{p}$ of $W_{(p-1)/2}(t)$ of the form $t^2 + ut + v$, $t^2 + (u/v)t + 1/v$ with $v \not\equiv 1 \pmod{p}$, which satisfy the first condition in Theorem 1.2. In other words, the binomial quadratic factors of $P_{(p-e)/4}(x)$ correspond 1–1 to pairs of reciprocal quadratic factors of $W_{(p-1)/2}(t) \pmod{p}$ whose corresponding curves E_λ admit the multiplier $\sqrt{-2p}$. Then we show that these pairs of reciprocal factors of $W_{(p-1)/2}(t)$ are in 1–1 correspondence with the quartic factors of the class equation $H_{-8p}(t) \pmod{p}$ which are powers of irreducibles. This fact yields the count of *bqf*'s given in Theorem 1.1.

In [m3] a similar formula is proved for the number of *bqf*'s in the factorization of $P_{(p-e)/3}(x) \pmod{p}$ which involves the class number $h(-3p)$ and an interesting connection to the elliptic curve $Y^2 + \alpha XY + Y = X^3$.

2. Another proof of Deuring's theorem

We begin by giving a proof of Deuring's theorem that will generalize to other situations. In our proof we use several facts from [brm]: 1) that the values of λ for which the curve E: $Y^2 = X(X-1)(X-\lambda)$ is supersingular lie in the field $\mathbf{F}_{p^2}$; and 2) that the multiplier $(x, y)^\mu = (x^{p^2}, y^{p^2})$ is equal to ± 1 times the multiplier p in $\mathrm{End}(E)$. (See [brm, pp. 87–88]; beware the misprint in the last line of Proposition 2.)

Theorem 2.1. *(See Deuring [d].) For $p > 3$, the j-invariant of the supersingular curve E_λ: $Y^2 = X(X-1)(X-\lambda)$ lies in $\mathbf{F}_p$ if and only if* End(E_λ) *contains a multiplier μ for which $\mu^2 = -p$.*

We have given a proof of this theorem in Proposition 5 of [brm] which uses facts from the theory of ideals in the quaternion algebra D_p, where

$$D_p = \{a + bi + cj + dk;\ i^2 = -r,\ j^2 = -p,\ ij = -ji = k;\ a, b, c, d \in \mathbf{Q}\},$$

and r is either 1, if $p \equiv 3 \pmod{4}$; or r is a prime quadratic non-residue of p of the form $r = 4k + 3$, when $p \equiv 1 \pmod{4}$. (In [h2] and [brm] r is erroneously taken to be the smallest quadratic non-residue of $p \equiv 1 \pmod{4}$; see [ro, p. 144]. This does not affect the validity of the proof in [brm].) The endomorphism rings of supersingular elliptic curves in characteristic p are always maximal orders in D_p. The following proof does not use the ideal theory of D_p.

We draw on the computations of [brm, pp. 92–93]. As in [brm], we let (x, y) be indeterminates which satisfy the equation for $E = E_\lambda$ and $K = \bar{\mathbf{F}}_p(x, y)$ the function field for E. We assume μ is an element of $\mathrm{End}(E)$ for which $\mu^2 = -p$. Since p is odd, $\mu^2 = -p$ is the identity map on the subgroup $E[2]$ of points of order 2 on E. We denote these points by

$$\mathbf{q}_0 = (0, 0), \qquad \mathbf{q}_1 = (1, 0), \qquad \mathbf{q}_\lambda = (\lambda, 0),$$

where points on E are identified with the corresponding prime divisors of K. It follows that μ is an automorphism on $E[2]$, and therefore permutes the three points of order 2.

Case 1. μ interchanges $\mathbf{q}_1$ and $\mathbf{q}_\lambda$. Comparing zero divisors, it is easy to see that $x^\mu = ax^p$, $(x-1)^\mu = b(x-\lambda)^p$, and $(x-\lambda)^\mu = c(x-1)^p$. Putting these equations together, using the fact that μ fixes constants, we see that $a = b = c = \lambda$ and $\lambda^p = 1/\lambda$, so the norm of λ to $\mathbf{F}_p$ is 1 when λ does not lie in $\mathbf{F}_p$. If λ does lie in $\mathbf{F}_p$, then $\lambda = -1$. In either case, $x^\mu = \lambda x^p$, which gives that

$$\left(y^\mu\right)^2 = \lambda x^p\left(\lambda x^p - 1\right)\left(\lambda x^p - \lambda\right) = \lambda^3 x^p\left(x^p - \lambda^p\right)\left(x^p - 1\right) = \lambda^3 y^{2p}.$$

Hence, $y^\mu = \pm\lambda\sqrt{\lambda}y^p$ so we have

$$(x, y)^\mu = \left(\lambda x^p, \pm\lambda\sqrt{\lambda}y^p\right). \tag{2.1}$$

Case 2. μ interchanges $\mathbf{q}_0$ and $\mathbf{q}_1$. In this case we have $x^\mu = a(x-1)^p$, $(x-1)^\mu = bx^p$, and $(x-\lambda)^\mu = c(x-\lambda)^p$. Putting these equations together gives $a = b = c = -1$ and $\lambda^p = 1 - \lambda$, so that the trace of λ to $\mathbf{F}_p$ is 1 when λ does not lie in $\mathbf{F}_p$. (If $\lambda \in \mathbf{F}_p$, then $\lambda = 1/2$.) Hence $x^\mu = -x^p + 1$. This implies that

$$\left(y^\mu\right)^2 = \left(-x^p + 1\right)\left(-x^p\right)\left(-x^p + 1 - \lambda\right) = -x^p\left(x^p - 1\right)\left(x^p - \lambda^p\right) = -y^{2p},$$

so that $y^\mu = \pm\sqrt{-1}y^p$, and

$$(x, y)^\mu = \left(-x^p + 1, \pm\sqrt{-1}y^p\right). \tag{2.2}$$

Case 3. μ interchanges $\mathbf{q}_0$ and $\mathbf{q}_\lambda$. Here we have $x^\mu = a(x-\lambda)^p$, $(x-1)^\mu = b(x-1)^p$, and $(x-\lambda)^\mu = cx^p$. These equations imply easily that $a = b = c = 1 - \lambda$ and $\lambda^p = \lambda/(\lambda - 1)$, so that the norm and trace of λ to $\mathbf{F}_p$ are equal when λ does not lie in $\mathbf{F}_p$, i.e., $\mathrm{Norm}(1-\lambda) = 1$. (If $\lambda \in \mathbf{F}_p$, then $\lambda = 2$.) Hence $x^\mu = (1-\lambda)x^p + \lambda$, which implies

$$\begin{aligned}\left(y^\mu\right)^2 &= \left((1-\lambda)x^p + \lambda\right)\left((1-\lambda)x^p + \lambda - 1\right)(1-\lambda)x^p\\ &= (1-\lambda)^3\left(x^p - \lambda^p\right)\left(x^p - 1\right)x^p = (1-\lambda)^3 y^{2p}.\end{aligned}$$

Thus we have $y^\mu = \pm(1-\lambda)\sqrt{1-\lambda}y^p$, and therefore

$$(x, y)^\mu = \left((1-\lambda)x^p + \lambda, \pm(1-\lambda)\sqrt{1-\lambda}y^p\right). \tag{2.3}$$

Case 4. In the last case the multiplier μ is the identity on $E[2]$. Then we have $x^\mu = ax^p$, $(x-1)^\mu = b(x-1)^p$, and $(x-\lambda)^\mu = c(x-\lambda)^p$. We conclude in this case that $a = b = c = 1$ and $\lambda^p = \lambda$, so that $\lambda \in \mathbf{F}_p$ and $x^\mu = x^p$. This implies that

$$(x, y)^\mu = \left(x^p, \pm y^p\right). \tag{2.4}$$

Note that in Cases 1–3, $\lambda \in \mathbf{F}_p$ implies $j = 1728$.

These calculations show: if there is an element $\mu \in \mathrm{End}(E)$ for which $\mu^2 = -p$, then either $\lambda \in \mathbf{F}_p$ or $\lambda \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $\mathrm{Norm}(\lambda) = 1$, $\mathrm{Trace}(\lambda) = 1$, or $\mathrm{Trace}(\lambda) = \mathrm{Norm}(\lambda)$, the last condition being equivalent to $\mathrm{Norm}(1-\lambda) = 1$.

Conversely, if one of these conditions holds for λ, then using the corresponding equation (2.1)–(2.4), it is easy to check directly that $(x, y) \to (x, y)^\mu$ is an element of $\mathrm{End}(E)$, meaning simply that μ maps the point (x, y) to a point on E; and that $x^{\mu^2} = x^{p^2}$ and therefore $y^{\mu^2} = \pm y^{p^2}$. (One needs also to check that the pole divisor of x divides the pole divisors of x^μ and y^μ, so that the meromorphism μ is normalized, but this verification is trivial here.) By the second fact mentioned above, this implies that $\mu^2 = \pm p$ in $\mathrm{End}(E)$. But $\mathrm{End}(E)$ is a definite quaternion algebra, so only $\mu^2 = -p$ is possible. Therefore, the above conditions on λ are equivalent to the existence of a multiplier μ for which $\mu^2 = -p$.

Now if λ satisfies one of the above conditions, respectively

$$\lambda^p = 1/\lambda,\ 1-\lambda,\ \lambda/(\lambda-1),\ \text{or}\ \lambda \tag{2.5}$$

in the above 4 cases, then the mapping $\lambda \to \lambda^p$ fixes the j-invariant of the curve E, since

$$\begin{aligned} 2^{-7}j - 3 &= 2\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2} - 3 \\ &= \lambda^2 + \frac{1}{\lambda^2} + (1-\lambda)^2 + \frac{1}{(1-\lambda)^2} + \left(1-\frac{1}{\lambda}\right)^2 + \left(\frac{\lambda}{\lambda-1}\right)^2, \end{aligned}$$

so that $j^p = j$ and $j = j(E) \in \mathbf{F}_p$.

Conversely, if $j^p = j$, then the set $S = \{\lambda, 1-\lambda, 1/\lambda, 1/(1-\lambda), \lambda/(\lambda-1), 1-1/\lambda\}$ is invariant under the Frobenius mapping $a \to a^p$. Hence λ^p is an element of S. Either $\lambda^p = 1/(1-\lambda)$ or $\lambda^p = 1-1/\lambda$, in which case λ satisfies $\lambda^{p^3} = \lambda$; or λ^p is equal to one of the expressions in (2.5). In the former case, λ is quadratic over $\mathbf{F}_p$, so $\lambda^{p^3} = \lambda^p$ gives $\lambda^p = \lambda$. Thus, condition (2.5) is still satisfied.

Hence, condition (2.5) is equivalent to $j \in \mathbf{F}_p$, on the one hand, and to the existence of an injection of $\sqrt{-p}$ into $\mathrm{End}(E)$, on the other. This proves Deuring's theorem.

3. Curves with $\sqrt{-2p}$ as multiplier

In this section we derive conditions on the coefficients of an irreducible quadratic factor t^2+ut+v of $W_{(p-1)/2}(t)$ mod p so that $\sqrt{-2p}$ injects into the endomorphism ring $\mathrm{End}(E)$ of the supersingular elliptic curve $E = E_\lambda$ and λ is a root of t^2+ut+v over $\mathbf{F}_p$.

With the same notation as in Section 2, we assume that μ is an element of $\mathrm{End}(E_\lambda)$ for which $\mu^2 = -2p$. Since $\mathrm{Norm}(\mu) = 2p$ in $\mathrm{End}(E_\lambda)$, it follows that the kernel of μ is $\{\mathbf{o}, \mathbf{p}\}$, where $\mathbf{p}$ has order 2. Furthermore, $[K : K^\mu] = \mathrm{Norm}(\mu) = 2p$ (see [h1]), so the degree of inseparability of K/K^μ is p.

Now μ is an endomorphism on the subgroup of points of order 2, so μ maps the points of order 2 different from $\mathbf{p}$ to $\mathbf{p}$ itself. Thus, if

$$(x) = \mathbf{q}_0^2/\mathbf{o}^2, \qquad (x-1) = \mathbf{q}_1^2/\mathbf{o}^2, \qquad (x-\lambda) = \mathbf{q}_\lambda^2/\mathbf{o}^2,$$

there are three cases.

Case 1. $\mathbf{p} = \mathbf{q}_0$. The formula $(\mu\mathbf{p})^\mu = N_\mu(\mathbf{p})$, where N_μ is the norm function from K to K^μ (see [d, p. 205]), shows that $\mathbf{q}_0^\mu = N_\mu(\mathbf{q}_1) = N_\mu(\mathbf{q}_\lambda)$. The prime divisor $\mathbf{q}_0^\mu$ of K^μ is divisible by at most two distinct prime divisors of K, so we must have $\mathbf{q}_0^\mu = \mathbf{q}_1^p\mathbf{q}_\lambda^p$ as divisors in K. Similarly, $\mathbf{o}^\mu = \mathbf{o}^p\mathbf{q}_0^p$. Therefore,

$$(x^\mu) = \frac{(\mathbf{q}_0^\mu)^2}{(\mathbf{o}^\mu)^2} = \frac{(\mathbf{q}_1\mathbf{q}_\lambda)^{2p}}{(\mathbf{o}\mathbf{q}_0)^{2p}}.$$

It follows that

$$x^{\mu} = a\frac{(x-1)^p(x-\lambda)^p}{x^p} = a\left(\frac{x^2-(1+\lambda)x+\lambda}{x}\right)^p, \tag{3.1}$$

for some nonzero constant a in $\bar{\mathbf{F}}_p$. On the other hand, $\mu^2 = -2p$ and Proposition 2 of [brm] imply that x^{μ^2} is the x-coordinate of the point $2(x^{p^2}, \pm y^{p^2})$ on the curve E_λ/K. Hence,

$$x^{\mu^2} = \frac{(x^{2p^2}-\lambda)^2}{4x^{p^2}(x^{p^2}-1)(x^{p^2}-\lambda)}. \tag{3.2}$$

Iterating the formula in (3.1) gives

$$x^{\mu^2} = a\left(\frac{b^2(x+\lambda/x-\lambda-1)^2 - b(1+\lambda^p)(x+\lambda/x-\lambda-1)+\lambda^p}{b(x+\lambda/x-\lambda-1)}\right)^{p^2},$$

with $a = b^p$, where we have used the fact that λ is an element of $\mathbf{F}_{p^2}$. Simplifying and factoring the resulting numerator gives

$$x^{\mu^2} = a\left(\frac{(b\lambda-(1+b+b\lambda)x+bx^2)(b\lambda-(b+b\lambda+\lambda^p)x+bx^2)}{bx(x-1)(x-\lambda)}\right)^{p^2}. \tag{3.3}$$

Comparing leading coefficients with (3.2) shows that $ab^{p^2} = 1/4$, or $a^{p+1} = 1/4$. Hence $a^{p^2-1} = 1$, so that a lies in $\mathbf{F}_{p^2}$. Setting the right-hand sides of (3.2) and (3.3) equal, taking p^2-th roots on both sides, and using $a^{p^2} = a$ gives the necessary equation

$$4a\big(b\lambda-(1+b+b\lambda)x+bx^2\big)\big(b\lambda-\big(b+b\lambda+\lambda^p\big)x+bx^2\big) = b\big(x^2-\lambda\big)^2. \tag{3.4}$$

The coefficient of x on the left side of this equation is $-4ab\lambda(2b+1+2b\lambda+\lambda^p) = 0$, so that $b = -(\lambda^p+1)/(2\lambda+2)$, if $\lambda \neq -1$. Hence,

$$a = b^p = -\frac{\lambda+1}{2(\lambda^p+1)}, \quad \lambda \neq -1. \tag{3.5}$$

If $\lambda = -1$, then (3.4) and $4ab = 1$ easily give that $a = -b$, whence $a^2 = -1/4$.

We now equate coefficients of x^2 on both sides of (3.4):

$$4a\big(2b^2\lambda + (b\lambda+b+1)\big(b\lambda+b+\lambda^p\big)\big) = -2b\lambda.$$

Multiplying out and using $4ab = 1$ gives

$$b\big(\lambda^2+6\lambda+1\big) + 4a\lambda^p + \big(\lambda^p+1\big)(\lambda+1) = 0.$$

Substituting for a and b using (3.5) gives

$$-\big(\lambda^p+1\big)^2\big(\lambda^2+6\lambda+1\big) + 2\big(\lambda^p+1\big)^2(\lambda+1)^2 - 4(\lambda+1)^2\lambda^p = 0, \tag{3.6}$$

which holds whether or not $\lambda = -1$. Writing (3.6) in the form

$$\big(\lambda^p+1\big)^2(\lambda+1)^2 - 4\lambda\big(\lambda^p+1\big)^2 - 4\lambda^p(\lambda+1)^2 = 0,$$

we see that the left-hand side is a symmetric polynomial in λ and λ^p, and so may be written as a polynomial in the elementary symmetric functions $u = -\lambda - \lambda^p$ and $v = \lambda^{p+1}$. This gives the condition

$$u^2 + 2uv + v^2 + 2u - 14v + 1 = (u + v + 1)^2 - 16v \equiv 0 \pmod{p}. \tag{3.7}$$

Conclusion. If $\mu \in \mathrm{End}(E_\lambda)$ satisfies $\mu^2 = -2p$ and $\mu\mathbf{q}_0 = \mathbf{o}$ in the group E_λ, then λ is a root of $t^2 + ut + v$ over $\mathbf{F}_p$, where u and v satisfy (3.7). In that case the mapping μ satisfies (3.1), where a is given by (3.5) when $\lambda \neq -1$, and $a^2 = -1/4$ otherwise.

Case 2. $\mathbf{p} = \mathbf{q}_1$. We reduce this case to Case 1 by setting $\lambda' = 1 - \lambda$ and $x' = 1 - x$. Then x', y satisfy the equation

$$-y^2 = x'\bigl(x' - 1\bigr)\bigl(x' - \lambda'\bigr).$$

Since $(x') = \mathbf{q}_1^2/\mathbf{o}^2$ in $K = \bar{\mathbf{F}}_p(x, y) = \bar{\mathbf{F}}_p(x', y)$, this curve satisfies the conditions of Case 1. If λ satisfies the equation $t^2 + ut + v = 0$, then $\lambda' = 1 - \lambda$ satisfies the equation $t^2 - (u + 2)t + u + v + 1 = 0$. From Case 1 we get that $v^2 \equiv 16(u + v + 1) \pmod{p}$.

Case 3. $\mathbf{p} = \mathbf{q}_\lambda$. We reduce this case to Case 1 by setting $\lambda'' = 1 - 1/\lambda$ and $x'' = 1 - x/\lambda$. Then x'', y satisfy the equation

$$y^2 = (-\lambda)^3 x''\bigl(x'' - 1\bigr)\bigl(x'' - \lambda''\bigr).$$

Since $(x'') = \mathbf{q}_\lambda^2/\mathbf{o}^2$ in $K = \bar{\mathbf{F}}_p(x, y) = \bar{\mathbf{F}}_p(x'', y)$, this curve also satisfies the conditions of Case 1. If λ satisfies the equation $t^2 + ut + v = 0$, then $\lambda'' = 1 - 1/\lambda$ satisfies the equation $t^2 - (u + 2v)t/v + (u + v + 1)/v = 0$. From Case 1 we get that $1/v^2 \equiv 16(u + v + 1)/v \pmod{p}$, or $1 \equiv 16(u + v + 1)v \pmod{p}$.

We note that the above argument only uses the fact that λ is a root of the "characteristic" polynomial $t^2 + ut + v = (t - \lambda)(t - \lambda^p)$ over $\mathbf{F}_p$, not that this polynomial is irreducible over $\mathbf{F}_p$. Thus we have proved the following proposition.

Proposition 3.1. *Assume that μ satisfies $\mu^2 = -2p$ in the endomorphism ring* $\mathrm{End}(E_\lambda)$ *of the supersingular elliptic curve E_λ: $Y^2 = X(X - 1)(X - \lambda)$, where λ is a root of $t^2 + ut + v$ over $\mathbf{F}_p$, the latter polynomial being irreducible or a perfect square* (*with $v \neq 0$*)*. Then the kernel of μ in E_λ is $\{\mathbf{p}, \mathbf{o}\}$, where $\mathbf{p} = \mathbf{q}_0, \mathbf{q}_1$, or $\mathbf{q}_\lambda$, and we have*

$$\begin{aligned} (u + v + 1)^2 &\equiv 16v \pmod{p}, && \text{if } \mu\mathbf{q}_0 = \mathbf{o} \text{ in } E_\lambda; \\ v^2 &\equiv 16(u + v + 1) \pmod{p}, && \text{if } \mu\mathbf{q}_1 = \mathbf{o} \text{ in } E_\lambda; \\ 16(u + v + 1)v &\equiv 1 \pmod{p}, && \text{if } \mu\mathbf{q}_\lambda = \mathbf{o} \text{ in } E_\lambda. \end{aligned}$$

Notice that the only values of λ in the prime field $\mathbf{F}_p$ for which $(t - \lambda)^2$ satisfies one of the three conditions of this proposition are those which are roots over $\mathbf{F}_p$ of the respective polynomials

$$\bigl(\lambda^2 - 6\lambda + 1\bigr)(\lambda + 1)^2, \qquad \bigl(\lambda^2 + 4\lambda - 4\bigr)(\lambda - 2)^2, \qquad \bigl(4\lambda^2 - 4\lambda - 1\bigr)(2\lambda - 1)^2. \tag{3.8}$$

In that case either $\lambda = -1, 2$, or $1/2$, and the corresponding j-invariant is $j = 1728$; or one of the three quadratics in (3.8) is reducible (mod p), so that the Legendre symbol $(2/p) = +1$, and $j = 8000$. These j-invariants are easily verified by factoring the polynomial $2^8(\lambda^2 - \lambda + 1)^3 - j(\lambda^2 - \lambda)^2$, for $j = 1728$ and $j = 8000$.

We shall now prove the converse of Proposition 3.1, which says that any one of these quadratic conditions on the coefficients of the polynomial $t^2 + ut + v$ satisfied by λ implies the existence of a multiplier μ in $\mathrm{End}(E_\lambda)$ with $\mu^2 = -2p$.

By transforming the equation for E_λ as in Cases 2 and 3 above, it is enough to consider the first condition in Proposition 3.1: $(u+v+1)^2 \equiv 16v \pmod{p}$. Assuming this congruence holds, we must show that there is a multiplier μ of K for which $\mu^2 = -2p$. Assume first that $\lambda \neq -1$. As our candidate we take the map $\mu : (x, y) \to (x^\mu, y^\mu)$ defined on x by

$$x^\mu = -\frac{\lambda+1}{2(\lambda^p+1)}\left(\frac{x^2-(\lambda+1)x+\lambda}{x}\right)^p = -\frac{\lambda+1}{2(\lambda^p+1)}\frac{y^{2p}}{x^{2p}}.$$

The argument in Case 1 may be reversed, with a given by (3.5), to show that Eq. (3.4) holds, since the coefficient of x^3 on the left side of (3.4) is $1/\lambda$ times the coefficient of x, and is therefore zero. It follows from (3.2) and (3.3) that x^{μ^2} is the x-coordinate of $2(x^{p^2}, \pm y^{p^2}) = \pm 2p(x, y)$ on the curve E_λ/K. We must compute y^μ and show that in fact $(x, y)^{\mu^2} = -2p(x, y)$.

By definition of μ, y^μ must satisfy the equation $(y^\mu)^2 = x^\mu(x^\mu - 1)(x^\mu - \lambda)$, so after some simplification we have

$$(y^\mu)^2 = -\frac{\lambda+1}{8(\lambda^p+1)^3}\frac{y^{2p}}{x^{6p}} \cdot \left(\left[(\lambda^p+1)y^2 + 2(\lambda+1)x^2\right]\left[(\lambda^p+1)y^2 + 2\lambda^p(\lambda+1)x^2\right]\right)^p. \quad (3.9)$$

Calling the term inside the large parentheses in the last equation A, we have

$$\begin{aligned} A &= x^2\left((\lambda^p+1)(x-1)(x-\lambda) + 2(\lambda+1)x\right)\left((\lambda^p+1)(x-1)(x-\lambda) + 2\lambda^p(\lambda+1)x\right) \\ &= x^2\left((\lambda^p+1)x^2 + (1-\lambda^p)(1+\lambda)x + \lambda(\lambda^p+1)\right)\left((\lambda^p+1)x^2 + (\lambda^p-1)(1+\lambda)x + \lambda(\lambda^p+1)\right). \end{aligned}$$

The two quadratics in the last equation have the same discriminant, namely

$$(1-\lambda^p)^2(1+\lambda)^2 - 4\lambda(\lambda^p+1)^2 = (1+\lambda^p)^2(1+\lambda)^2 - 4\lambda^p(1+\lambda)^2 - 4\lambda(\lambda^p+1)^2. \quad (3.10)$$

But this is the symmetric expression in λ and λ^p that we discovered in Case 1 to be equal to the left-hand side of (3.7), which is zero by assumption. Hence A is a perfect square in K:

$$\begin{aligned} A/x^2 &= \left[(\lambda^p+1)x^2 + \lambda(\lambda^p+1)\right]^2 - (\lambda^p-1)^2(\lambda+1)^2x^2 \\ &= (\lambda^p+1)^2x^4 + \left[2\lambda(\lambda^p+1)^2 - (\lambda^p-1)^2(\lambda+1)^2\right]x^2 + \lambda^2(\lambda^p+1)^2 \\ &= \left[(\lambda^p+1)x^2 - \lambda(\lambda^p+1)\right]^2 = (\lambda^p+1)^2(x^2-\lambda)^2, \end{aligned}$$

where the penultimate equality follows from the fact that the left side of (3.10) is zero. Thus we take

$$y^\mu = \pm\sqrt{\frac{-(\lambda+1)}{2(\lambda^p+1)}}\frac{(\lambda+1)}{2(\lambda^p+1)}\frac{y^p}{x^{2p}}(x^2-\lambda)^p, \quad \lambda \neq -1.$$

Setting γ equal to the square-root in this expression, we have

$$\gamma^2 = -\frac{(\lambda+1)}{2(\lambda^p+1)} = -\frac{1}{2}\frac{(\lambda+1)^2}{v-u+1},$$

assuming $\lambda \neq -1$, so that γ lies in $\mathbf{F}_{p^2}$. In case $\lambda = -1$, we easily compute in the same way that

$$x^\mu = \frac{1}{2\sqrt{-1}}\frac{x^{2p}-1}{x^p}, \qquad y^\mu = \frac{\pm 1}{2(-1+\sqrt{-1})}\frac{y^p}{x^{2p}}(x^2+1)^p, \quad \lambda = -1.$$

This shows that the mapping $\mu : K \to K$ is an isomorphism which is defined over $\mathbf{F}_{p^2}$. In order to know that μ corresponds to an endomorphism of E_λ, or in other words, that μ is a normalized meromorphism, we must check that the prime divisor $\mathbf{o}$ at infinity divides the denominators of x^μ and y^μ. But this is easily done. Hence, μ is a multiplier of the elliptic function field K.

Now we know already that $x^{\mu^2} = x^{(-2p)}$, where $(-2p)$ denotes the meromorphism $-2p$ and not an ordinary exponent. Since (x^{μ^2}, y^{μ^2}) and $(x^{(-2p)}, y^{(-2p)})$ both satisfy the equation for E_λ, it follows that $y^{\mu^2} = \pm y^{(-2p)}$, and therefore $\mu^2 = \pm 2p$. But, $\mu^2 = +2p$ is impossible, since the quaternion algebra $\mathrm{End}(E_\lambda)$ is definite, so we must have $\mu^2 = -2p$. This completes the proof of Theorem 1.2.

The result of Theorem 1.2 at the λ-level corresponds to the following criterion at the j-level: $\sqrt{-2p}$ injects into $\mathrm{End}(E_\lambda)$ if and only if $\Phi_2(j, j^p) \equiv 0 \pmod p$, where $\Phi_2(x, y)$ is the transformation polynomial or modular equation [co, p. 229]. This can be proved using Deuring's theory as in [m2, Theorem 3.1] or can be deduced directly by a somewhat elaborate calculation from Theorem 1.2 and the formula (1.2) for j in terms of λ. It is interesting that the extremely simple criterion in Theorem 1.2 translates to the much more complex criterion (in terms of the size of the coefficients) involving $\Phi_2(x, y)$. The fact that $\Phi_2(x, y)$ is symmetric in x and y leads to the equivalent criterion (4.2) in Theorem 4.1 below.

This criterion for $\sqrt{-2p}$ at the j-level can easily be generalized, using Deuring's theory [d]: if d is positive, square-free, and relatively prime to p, then $\sqrt{-dp}$ injects into $\mathrm{End}(E_\lambda)$ if and only if $\Phi_d(j, j^p) \equiv 0 \pmod p$. See [m2, Theorem 3.1]. When $d = 1$ this is just Deuring's theorem, since $\Phi_1(x, y) = x - y$. See [m3] for the case $d = 3$, where the Legendre normal form is replaced by the Deuring normal form (or Hessian) $Y^2 + \alpha XY + Y = X^3$.

4. Binomial quadratic factors of $P_{(p-e)/4}(x)$

The second ingredient in the proof of Theorem 1.1 is the following factorization. To state this theorem let $ss_p(t)$ denote the supersingular polynomial in characteristic p. This is the monic polynomial in t over $\mathbf{F}_p$ whose roots are the distinct j-invariants of supersingular elliptic curves in characteristic p. (See [m1,kaz,brm].) Recall also that the class equation $H_D(t)$ of discriminant D is the monic, irreducible polynomial in $\mathbf{Z}[t]$ whose roots are the j-invariants of elliptic curves with complex multiplication by the quadratic order of discriminant D.

Theorem 4.1. *(See [m2].) For $p > 13$, the class equation $H_{-8p}(t)$ of discriminant $-8p$ satisfies the congruence*:

$$\begin{aligned} H_{-8p}(t) \equiv {} & (t-1728)^{2\epsilon_1}(t-8000)^{2\epsilon_2}(t+3375)^{4\epsilon_3} \\ & \times \left(t^2 + 191025t - 121287375\right)^{4\epsilon_4} \prod_i \left(t^2 + a_i t + b_i\right)^2 \pmod p, \end{aligned} \tag{4.1}$$

where

$$\epsilon_1 = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right),$$

$$\epsilon_2 = \frac{1}{2}\left(1 - \left(\frac{-8}{p}\right)\right),$$

$$\epsilon_3 = \frac{1}{2}\left(1 - \left(\frac{-7}{p}\right)\right),$$

$$\epsilon_4 = \frac{1}{4}\left(1 - \left(\frac{-15}{p}\right)\right)\left(1 - \left(\frac{5}{p}\right)\right);$$

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

$$(2b + 1485a - 41097375)^2 \equiv -(4a - 29025)(a - 191025)^2 \pmod{p}. \tag{4.2}$$

Explicit formulas for $ss_p(t)$ are given in [brm,m1,kaz,bgns], so that Theorem 4.1 gives a completely explicit factorization of $H_{-8p}(t) \pmod{p}$. The proof of Theorem 4.1 can be found in [m2].

In order to count binomial quadratic factors of $P_{(p-e)/4}(t)$, we have to relate these factors first of all to factors of $W_{(p-1)/2}(t)$, and then we must relate the latter factors to the class number $h(-2p)$, using the factorization in Theorem 4.1.

We shall show that for $p > 13$ the binomial quadratic factors of $P_{(p-e)/4}(x) \pmod{p}$ are in 1–1 correspondence with the *quartic* factors in $H_{-8p}(t)$ which are powers of irreducibles $(\text{mod } p)$. In other words, each factor $(t + 3375)^4$, $(t^2 + a_i t + b_i)^2$ in Theorem 4.1 contributes 1 binomial quadratic to the count in Theorem 1.1, while $(t^2 + 191025t - 121287375)^4$ contributes 2 to that count. This yields $(h(-2p) - d_p)/4$ binomial quadratics in all, where $d_p = 2\epsilon_1 + 2\epsilon_2 = 0, 2, 2, 4$ according as $p \equiv 1, 3, 5, 7 \pmod{8}$.

To do this, we use the following identity (4.3) (see [psz, VI, Problem 85]) and congruence (4.4) (see [brm, p. 85]):

$$W_n(x) = (1 - x)^n P_n\left(\frac{1 + x}{1 - x}\right), \tag{4.3}$$

$$z^{(e-1)/2} W_{(p-e)/4}\bigl(1 - z^2\bigr) \equiv P_{(p-1)/2}(z) \pmod{p}. \tag{4.4}$$

Let $x^2 + a$ be an irreducible, binomial quadratic factor of $P_{(p-e)/4}(x) \pmod{p}$. Then $W_{(p-e)/4}(x)$ has $(1 + x)^2 + a(1 - x)^2$ as an irreducible factor $(\text{mod } p)$, which is a constant multiple of the factor

$$x^2 + 2\frac{1 - a}{1 + a}x + 1.$$

Thus, *bqf*'s of $P_{(p-e)/4}(x)$ correspond to irreducible palindromic factors of $W_{(p-e)/4}(x) \pmod{p}$, i.e., those with constant term 1. By (4.4) these palindromic factors correspond to certain quartic factors of $P_{(p-1)/2}(z)$ which must factor as a product of quadratics $(\text{mod } p)$:

$$z^4 - \frac{4}{1 + a}z^2 + \frac{4}{1 + a} = \bigl(z^2 + rz + s\bigr)\bigl(z^2 - rz + s\bigr). \tag{4.5}$$

These quadratics are 1) irreducible and 2) distinct, because: 1) by (4.4) roots of the irreducible palindromic factors we're considering are expressible as $1 - z^2$ for roots of $z^2 \pm rz + s \equiv 0 \pmod{p}$; and 2) $P_{(p-1)/2}(z)$ has distinct roots $(\text{mod } p)$. Thus $r \not\equiv 0 \pmod{p}$. Furthermore, the product $(z^2 + rz + s)(z^2 - rz + s)$ has the form (4.5) if and only if $s^2 + 2s \equiv r^2 \pmod{p}$.

This shows that *bqf*'s of $P_{(p-e)/4}(x)$ are in 1–1 correspondence with pairs $(z^2 + rz + s)(z^2 - rz + s)$ of irreducible quadratic factors of $P_{(p-1)/2}(z)$ for which $r \not\equiv 0$ and $s^2 + 2s \equiv r^2 \pmod{p}$.

Now we use (4.3) again to translate this condition in terms of irreducible factors of $W_{(p-1)/2}(t)$. The transformation $t \to z = (1 + t)/(1 - t)$ associates the factor $z^2 + rz + s$ of $P_{(p-1)/2}(z)$ with the factor

$$t^2 + ut + v = t^2 + \frac{2(1 - s)}{1 - r + s}t + \frac{1 + r + s}{1 - r + s}$$

of $W_{(p-1)/2}(t)$; and the factor $t^2 + ut + v$ of $W_{(p-1)/2}(t)$ with the factor

$$z^2 + rz + s = z^2 + \frac{2(v - 1)}{1 + u + v}z + \frac{1 - u + v}{1 + u + v}$$

of $P_{(p-1)/2}(z)$. Thus, the above conditions for r and s translate to the conditions:

$$v \neq 1; \qquad (2v-2)^2 = (1-u+v)^2 + 2(1-u+v)(1+u+v) \pmod{p}.$$

Simplifying the last condition gives $(u+v+1)^2 \equiv 16v \pmod{p}$, the first of the three conditions in Theorem 1.2! Furthermore, replacing r by $-r$ in the above formulas for u and v takes the pair (u,v) to $(u/v, 1/v)$. Thus we have the following

Proposition 4.2. *The irreducible, binomial quadratic factors of $P_{(p-e)/4}(x) \pmod{p}$ are in 1–1 correspondence with the pairs of irreducible quadratic factors of $W_{(p-1)/2}(t)$ of the form t^2+ut+v, $t^2+ut/v+1/v$, where $v \neq 1$ and $(u+v+1)^2 \equiv 16v \pmod{p}$.*

Thus, binomial quadratic factors of $P_{(p-e)/4}(x)$ over $\mathbf{F}_p$ correspond 1–1 to certain pairs of reciprocal quadratic factors of $W_{(p-1)/2}(t)$.

In order to prove Theorem 1.1, we must see how these factors are related to the quartics occurring in the factorization of $H_{-8p}(t) \pmod{p}$, as described above. We know that the curves E_λ, for λ a root of one of the polynomials t^2+ut+v in Proposition 4.2, all have multipliers μ with $\mu^2=-2p$, by Theorem 1.2. Hence their j-invariants are roots of $H_{-8p}(t) \pmod{p}$. We must show that one pair of quadratics t^2+ut+v, $t^2+ut/v+1/v$ from Proposition 4.2 corresponds to each of the terms $(t+3375)^4$ and $(t^2+a_it+b_i)^2$, while two pairs correspond to the factor $H_{-15}(t)^4 = (t^2+191025t-121287375)^4$; and that this exhausts all pairs of irreducible factors in Proposition 4.2.

The parameter λ and the j-invariant j of E_λ are related by the equation $f(\lambda, j)=0$ in $\mathbf{F}_p$, where

$$f(t,j) = \left(t^2-t+1\right)^3 - \frac{j}{2^8}\left(t^2-t\right)^2.$$

It is easy to see that $j=1728$ and $j=8000$ contribute no pairs of reciprocal factors in Proposition 4.2, since

$$f(t,1728) = (t-2)^2(t+1)^2(t-1/2)^2,$$

and

$$f(t,8000) = \left(t^2-6t+1\right)\left(t^2+4t-4\right)\left(t^2-t-1/4\right).$$

For $j=8000$ note that the middle quadratic satisfies the congruence of Proposition 4.2 only when $p=5$ or 13. Furthermore, $j=-3375$ accounts for exactly one pair of reciprocal quadratics satisfying $(u+v+1)^2 \equiv 16v$, since

$$f(t,-3375) = \left(t^2-31t/16+1\right)\left(t^2-t+16\right)\left(t^2-t/16+1/16\right),$$

and t^2-t+16 is irreducible $\pmod{p}$ exactly when $(\frac{-3^2\cdot 7}{p})=-1$, i.e., exactly when $\epsilon_3=1$ in (4.1).

Next, consider the factor $H_{-15}(t) = t^2+191025t-121287375 = (t-\alpha_+)(t-\alpha_-)$, when $(\frac{-15}{p}) = (\frac{5}{p}) = -1$. We form the polynomial

$$\begin{aligned} 2^{16} f(t,\alpha_+) f(t,\alpha_-) &= \left(256t^4-272t^3+33t^2-272t+256\right) \\ &\quad \times \left(t^4-2t^3+753t^2-752t+256\right)\left(256t^4-752t^3+753t^2-2t+1\right) \\ &= g_1(t)g_2(t)g_3(t), \end{aligned} \tag{4.6}$$

in which the 3 quartics on the right are irreducible over **Q**. The values of λ corresponding to the roots of $H_{-15}(t)$ are the roots of the polynomials $g_i(t)$, where $g_2(t)$ and $g_3(t)$ are reciprocal polynomials. The roots of $g_2(t)$ are easily computed to be

$$\lambda = \frac{1 \pm 16\sqrt{-3} \pm 7\sqrt{-15}}{2},$$

and $disc(g_2(t)) = 2^{16} \cdot 3^6 \cdot 5^2 \cdot 7^4 \cdot 11^2$. Using the fact that $(\frac{-3}{p}) = +1$, we consider the factor

$$t^2 + ut + v = (t - \lambda_1)(t - \lambda_2), \quad \text{where } \lambda_1, \lambda_2 = \frac{1 + 16\sqrt{-3} \pm 7\sqrt{-15}}{2}.$$

This factor is irreducible over $\mathbf{F}_p$ and its coefficients $u = -1 - 16\sqrt{-3}$, $v = -8 + 8\sqrt{-3}$ satisfy $(u + v + 1)^2 - 16v = 0$ for all p. Furthermore, its constant term v is congruent to 1 (mod p) at most when $p = 3, 7, 13$. Thus, this factor and its reciprocal, which is a factor of $g_3(t)$, are a reciprocal pair in Proposition 4.2. Another reciprocal pair of factors is obtained by replacing $\sqrt{-3}$ by $-\sqrt{-3}$. This gives at least two reciprocal pairs corresponding to the factor $H_{-15}(t)$, and the product of these 4 polynomials is a constant times $g_2(t)g_3(t)$.

To see that the remaining factor $g_1(t)$ contributes no reciprocal pairs, all we have to do is apply the inverse map of $z = (1 + t)/(1 - t)$ to this factor and compare its form to (4.5). This gives

$$(z + 1)^4 g_1\left(\frac{z - 1}{z + 1}\right) = z^4 + 3006z^2 + 1089;$$

but the sum of the last two coefficients $3006 + 1089 = 3^2 \cdot 5 \cdot 7 \cdot 13$ is never zero (mod p) when $p > 13$. Hence, the factors of $g_1(t)$ never yield a reciprocal pair for $p > 13$. Therefore, the factor $H_{-15}(t)^4$ does in fact contribute two pairs of reciprocal factors in Proposition 4.2, for all primes $p > 13$ for which $\epsilon_4 = 1$.

To complete the proof of Theorem 1.1, we must show that any irreducible factor $h(t) = t^2 + a_i t + b_i$ of $H_{-8p}(t)$ distinct from $H_{-15}(t)$ (mod p) contributes just one pair of reciprocal factors in Proposition 4.2. Let j be a root in $\mathbf{F}_{p^2}$ of $h(t) = 0$. Then $f(t, j)f(t, j^p)$ factors as a product of 6 quadratics over $\mathbf{F}_p$, similar to the factorization in (4.6):

$$f(t, j)f\big(t, j^p\big) = q_1(t)\tilde{q}_1(t) \cdot q_2(t)\tilde{q}_2(t) \cdot q_3(t)\tilde{q}_3(t), \tag{4.7}$$

where $\tilde{q}(t)$ denotes the reciprocal polynomial of $q(t)$. This follows from the arguments of Section 2, according to which λ and $1/\lambda$ are conjugate over $\mathbf{F}_p$ only if $j \in \mathbf{F}_p$. By the arguments in Cases 2 and 3 of Section 3, mappings of λ by the anharmonic group permute the three congruences in Proposition 3.1. By those arguments, there is always at least one factor in (4.7), say $q_1(t)$, which satisfies the first congruence in Proposition 3.1. Then its reciprocal $\tilde{q}_1(t)$ satisfies the same congruence, while $q_2(t)$ and $q_3(t)$, say, will satisfy the second and third congruences, respectively. The nature of these congruences implies that $\tilde{q}_2(t)$ then satisfies the third congruence, while $\tilde{q}_3(t)$ satisfies the second.

Now $q_1(t)$, $\tilde{q}_1(t)$ are a reciprocal pair for Proposition 4.2. Suppose that one of the other pairs $q_i(t)$, $\tilde{q}_i(t)$ is a second reciprocal pair in Proposition 4.2. Then, wlog, the factor $q_i(t) = t^2 + ut + v$ satisfies the first and second congruences of Proposition 3.1, while $\tilde{q}_i(t) = t^2 + ut/v + 1/v$ satisfies the first and third. To find all such factors, compute the resultants

$$Resultant_u\big((u + v + 1)^2 - 16v, v^2 - 16(u + v + 1)\big) = v(v - 16)\big(v^2 + 16v + 256\big),$$
$$Resultant_v\big((u + v + 1)^2 - 16v, v^2 - 16(u + v + 1)\big) = (u + 1)^2\big(u^2 + 2u + 769\big).$$

If $v = 0$, then $u = -1$, giving a reducible $q_i(t)$; while if $v = 16$, then $u = -1$ and $q_i(t) = t^2 - t + 16$, which, by the above computations, corresponds to $j = -3375$. On the other hand, if

$v^2+16v+256=0$, then $v=-8\pm 8\sqrt{-3}$ yields $u=-1\mp 16\sqrt{-3}$, giving as j-invariants the roots of $H_{-15}(t)$ (mod p). This proves that $h(t)=t^2+a_it+b_i$ contributes only one pair of reciprocal polynomials satisfying Proposition 4.2.

Finally, every pair of reciprocal factors of $W_{(p-1)/2}(t)$ in Proposition 4.2 yields a j which is a root of $H_{-8p}(t)$ (mod p), by Theorem 1.2 and Deuring's theory [d], and so comes from one of the factors we have already considered. This completes the proof of Theorem 1.1 for primes $p>13$. For $p\leqslant 13$ it can be checked directly.

The above argument also makes it clear that (for $p>13$) the number of pairs of reciprocal quadratic factors of $W_{(p-1)/2}(t)$, one of which satisfies the second congruence, while the other satisfies the third congruence, in Theorem 1.2, is twice the number given in Theorem 1.1, as long as: the factor $t^2-31t/16+1$ is counted as one pair whenever it occurs (since it is palindromic and satisfies both congruences); and the factors of $g_1(t)$ in (4.6) are counted as two pairs when they occur. The factors of $g_1(t)$ always satisfy the second *and* third congruences in Theorem 1.2, whenever $(-15/p)=(5/p)=-1$, because these factors will be reductions (mod p) of the two quadratics

$$x^2-17(1\pm\sqrt{-3})/32\cdot x+(-1\pm\sqrt{-3})/2.$$

Concluding Remarks. It follows from results of [brm] that $P_{(p-e)/4}(x)$ always factors into linear and quadratic polynomials (mod p). For example, taking $p=97$ and $e=1$, we have

$$\begin{aligned}P_{24}(x)\equiv{}&79(x+39)(x+58)\big(x^2+5\big)\big(x^2+23\big)\big(x^2+46\big)\big(x^2+80\big)\big(x^2+90\big)\\&\cdot\big(x^2+19x+29\big)\big(x^2+78x+29\big)\big(x^2+46x+54\big)\big(x^2+51x+54\big)\\&\cdot\big(x^2+3x+96\big)\big(x^2+94x+96\big)\ (\mathrm{mod}\ 97).\end{aligned}$$

In this case, $P_{24}(x)$ has $5=(h(-2\cdot 97)-0)/4=20/4$ binomial quadratic factors (mod 97), in agreement with Theorem 1.1.

The linear factors of $P_{(p-e)/4}(x)$ (mod p) were counted in [brm], in terms of the class number $h(-p)$ of the quadratic field $\mathbf{Q}(\sqrt{-p})$. (See [brm, Theorem 1(c)].) The number of linear factors turns out to be

$$\begin{gathered}h(-p)/2,\quad \text{if } p\equiv 1\ (\mathrm{mod}\ 4);\\ 3h(-p)-1,\quad \text{if } p\equiv 3\ (\mathrm{mod}\ 8);\\ 2h(-p)-1,\quad \text{if } p\equiv 7\ (\mathrm{mod}\ 8).\end{gathered}$$

This result, together with Theorem 1.1, shows that both class numbers $h(-p)$ and $h(-2p)$ are encoded in the factorization of the polynomial $P_{(p-e)/4}(x)$ (mod p).

References

[bgns] S. Basha, J. Getz, H. Nover, E. Smith, Systems of orthogonal polynomials arising from the modular j-function, J. Math. Anal. Appl. 289 (2004) 336–354.

[brm] 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.

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

[d] Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg 14 (1941) 197–272.

[h1] Helmut Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper, I, II, III, J. Reine Angew. Math. 175 (1936) 55–62, 69–88, 193–208, Papers 47–49 in: Hasse's *Mathematische Abhandlungen*, vol. 2, Walter de Gruyter, Berlin, 1975, pp. 223–266.

[h2] Helmut Hasse, Punti razionali sopra curve algebriche a congruenze, Reale Academia d'Italia, Fondazione Alessandro Volta, Atti Convegni 9 (1943) 85–140, Paper 52 in: Hasse's *Mathematische Abhandlungen*, vol. 2, Walter de Gruyter, Berlin, 1975, pp. 295–350.

[kaz] M. Kaneko, D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, in: AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc. and International Press, Providence, RI, 1998, pp. 97–126.

[m1] P. Morton, Explicit identities for invariants of elliptic curves, J. Number Theory 120 (2006) 234–271.

[m2] P. Morton, Ogg's theorem via explicit congruences for class equations, preprint, available as pr06-09 in the IUPUI Math. Dept. Preprint Series, at www.math.iupui.edu/research/preprint/2006/pr06-09.pdf.

[m3] P. Morton, The cubic Fermat equation and complex multiplication on the Deuring normal form, submitted for publication.

[psz] G. Polya, G. Szegő, Aufgaben und Lehrsätze aus der Analysis I, II, Grundlehren Math. Wiss., vol. 20, Springer-Verlag, Berlin, 1964.

[ro] P. Roquette, The Riemann hypothesis in characteristic p, its origin and development, Part 3: The elliptic case, Mitt. Math. Ges. Hamburg 25 (2006) 103–176.