Supersingular parameters of the Deuring normal form

by

Patrick Morton

PR # 12-01

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

January 30, 2012

Supersingular parameters of the Deuring normal form *†

Patrick Morton

Abstract

It is proved that the supersingular parameters α of the elliptic curve $E_3(\alpha)$: $Y^2 + \alpha XY + Y = X^3$ in Deuring normal form satisfy $\alpha = 3 + \gamma^3$, where γ lies in the finite field $\mathbb{F}_{p^2}$. This is accomplished by finding explicit generators for the normal closure N of the finite extension $k(\alpha)/k(j(\alpha))$, where α is an indeterminate over $k = \mathbb{F}_{p^2}$ and $j(\alpha)$ is the j-invariant of $E_3(\alpha)$. The function field N is constructed over any field k containing a primitive cube root of unity whose characteristic is different from 2 and 3, and contains the function field of the cubic Fermat curve. This is used to study solutions of the cubic Fermat equation in Hilbert class fields of imaginary quadratic fields in which the prime 3 splits, as well as solutions in modular functions given in terms of the Dedekind η-function.

It has been known since Hasse's 1934 paper [h] that there are only finitely many isomorphism classes of elliptic curves E defined over the algebraic closure of the finite field $\mathbb{F}_p$, for which E has no points of order p. Such a curve is said to be supersingular, and Deuring [d] showed that its j-invariant $j(E)$ lies in $\mathbb{F}_{p^2}$. Supersingular j-invariants are somewhat sparse: in characteristic p there are roughly $(p-1)/12$ of them. They can be characterized as the roots of a certain polynomial (see [d], [brm], [m1]), and it is of interest to find other arithmetic relations that they satisfy. For example, it is proved in [m2] that the j-invariant of any supersingular curve E in characteristic p is a perfect cube in $\mathbb{F}_{p^2}$.

For certain families of elliptic curves, the values of the parameters for which these curves are supersingular also satisfy interesting arithmetic relationships in finite

MSC2010: 14H52, 14H05, 11D41, 11F20

†*Keywords*: Elliptic curves, Deuring normal form, supersingular, algebraic function fields, cubic Fermat curve, modular functions

fields, as has been shown in [m1]. There it is shown that the Tate normal forms $E_4(b)$ and $E_5(b)$, with distinguished points of orders 4 and 5, respectively, have the following property. The values of b in the algebraic closure $\bar{\mathbb{F}}_p$ for which

$$E_4(b) : Y^2 + XY + bY = X^3 + bX^2$$

is supersingular in characteristic p ($\neq 2, 3$) lie in the finite field $\mathbb{F}_{p^2}$ and are fourth powers in that field. A consequence of this is that the supersingular parameters λ of the Legendre normal form

$$E_2(\lambda) : Y^2 = X(X-1)(X-\lambda)$$

are fourth powers in $\mathbb{F}_{p^2}$. (See [m1] and Landweber [lw].) Similarly, the values of b for which

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

is supersingular in characteristic p ($\neq 2, 3$) are fifth powers in $\mathbb{F}_{p^2}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity over $\mathbb{F}_p$.

In the case of $E_2(\lambda)$ there is also a group G_{24} of linear fractional transformations in z, isomorphic to the octahedral group, which maps the set of fourth roots $z = \lambda^{1/4}$ of supersingular parameters into itself. Similar groups exist for each of the normal forms $E_4(b)$ and $E_5(b)$. See [m1] for the precise statements. The existence of these groups shows that the supersingular parameters for these normal forms exhibit deeper structural properties.

The analogue of the Tate normal form for points of order 3 is the Deuring normal form $E_3(\alpha)$ (see below), on which the points $(X, Y) = (0, 0)$ and $(0, -1)$ have order 3. A corresponding arithmetic property for the supersingular parameters of the normal form $E_3(\alpha)$ was stated as a conjecture in [m2]. In this note I shall prove this conjecture:

Theorem 1. Let $p > 3$ be a prime and let α be an element of $\bar{\mathbb{F}}_p$ for which the elliptic curve in Deuring normal form

$$E_3(\alpha) : Y^2 + \alpha XY + Y = X^3$$

is supersingular. Then $\alpha = 3 + \gamma^3$ for some element $\gamma \in \mathbb{F}_{p^2}$. $\square$

The proof of this theorem depends on knowing the precise *algebraic* form of the normal closure N of the finite extension of function fields $k(\alpha)/k(j)$ over the field $k = \mathbb{F}_{p^2}$, where α is an indeterminate and $j = \alpha^3(\alpha^3-24)^3/(\alpha^3-27)$ is the j-invariant of the curve $E_3(\alpha)$. (See Sections 1, 2.) For an arbitrary field k with $char(k) \neq 2, 3$ containing a primitive cube root of unity, the field N is the function field of a covering of the cubic Fermat curve

$$Fer_3 : \ 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3,$$

and the genus of N is 10. The curve Fer_3 plays a key role in the calculation of generators for N, as it does in the arithmetic of the curve $E_3(\alpha)$ (See Section 1 and [m2]).

It is shown in [m2] that the set of supersingular parameters α for $E_3(\alpha)$ is invariant under a group G_{12} of linear fractional transformations in α, which is isomorphic to the tetrahedral group. Here we find evidence of deeper structural properties by showing how the Galois group $Gal(N/k(j))$ acts on the numbers γ in Theorem 1. In Section 4 we prove in a purely algebraic way that if the characteristic of k is not 2 or 3, then $Gal(N/k(j))$ is isomorphic to the modulary group $\bar{\Gamma}(9) = SL_2(\mathbb{Z}/9\mathbb{Z})/\{\pm I\}$. The algebraic form of the automorphisms revealed in this proof implies some interesting new relationships between supersingular parameters of $E_3(\alpha)$ in characteristic p.

In Section 3 we work primarily in characteristic zero, and study solutions (α, β) of Fer_3 which are defined over the Hilbert class field Σ_d of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, with $-d \equiv 1 \pmod 3$. Using the normal closure N we prove that these solutions have the property that

$$\alpha = 3 + \gamma^3, \ \ \beta = 3 + \gamma'^3, \quad \text{for } \gamma, \gamma' \in \Sigma_d.$$

This is really the analogue of Theorem 1 in characteristic zero, because these solutions come from elliptic curves $E_3(\alpha)$ which have complex multiplication by the ring of integers in K, and supersingular curves in characteristic p are known to be reductions of curves with complex multiplication (see [d]). This leads to the existence of points defined over Σ_d on the covering C_{19} of genus 19 of Fer_3, whose equation is

$$C_{19} : \ \ z^3w^3(z^6 + 9z^3 + 27)(w^6 + 9w^3 + 27) = 729,$$

for any positive, square-free integer $d \equiv 2 \pmod 3$. (See Theorem 7.) We include the proof in this paper since it makes use of the same idea used to prove Theorem 1, but this time the base field k is a specific abelian extension of Σ_d.

The isomorphism of $Gal(N/k(j))$ with $\bar{\Gamma}(9)$ also suggests a connection with modular functions. In Section 5 I use the results of Fleckinger [fle, Sections I, II] to show that when $k = \mathbb{C}$ and $j = j(\tau)$ is the modular j-function, N is isomorphic to the field of modular functions $\mathsf{K}_{\Gamma(9)}$ for the principal congruence group $\Gamma(9)$. An identity of Weber [w] is used in Section 5 to give simpler expressions for the functions $l_{(u,v)}(\tau)$ occurring in [fle] in terms of quotients of values of Dedekind's function $\eta(\tau)$. Combining the results of Fleckinger and Weber with the isomorphism $N \cong \mathsf{K}_{\Gamma(9)}$ gives new proofs of several interesting identities for $\eta(\tau)$ (see the corollary to Theorem 11 and Theorem 12), which are equivalent to known identities involving cubic theta functions (see Section 7). In Section 6 we apply these identities to give a simple derivation of a recent identity of Berndt and Hart [bh] involving $\eta(\tau)$.

These identities also lead to a parametrization of the curve C_{19} in terms of modular functions by finding an explicit solution of Fer_3 using modular functions for $\Gamma(9)$, for which the relations $\alpha = 3 + \gamma^3$ and $\beta = 3 + \gamma'^3$ continue to hold. (See Theorem 13.)

Thus, the relation $\alpha = 3+\gamma^3$ will be shown to persist at all three levels: algebraic, arithmetic, and analytic.

1 The normal closure N of $k(\alpha)/k(j)$.

Let α be an indeterminate and set $j = j(\alpha) = \dfrac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}$, the j-invariant of the curve $E_3(\alpha)$. Further, let k be any field whose characteristic is not 2 or 3 and which contains a primitive cube root of unity $\omega = (-1 + \sqrt{-3})/2$. We will prove the above theorem by finding the normal closure N of the algebraic extension $k(\alpha)/k(j)$.

Let β be another indeterminate satisfying the equation

$$Fer_3 : 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3$$

and let $F(x) = x(x - 24)^3 - j(x - 27)$. Then α satisfies the irreducible equation $F(\alpha^3) = 0$ over $k(j)$, and N is the splitting field of the polynomial $F(x^3)$. I will first prove:

Proposition 2. The normal closure of $k(\alpha^3)/k(j)$ is the field $k(\alpha^3, \beta) = k(\beta)$, and

$$Gal(k(\alpha^3, \beta)/k(j)) \cong A_4.$$

Proof. I will use classical formulas to find the roots of the cubic resolvent of $F(x)$. We have

$$F(x) = x^4 - 72x^3 + 1728x^2 - (j + 13824)x + 27j,$$

and

$$F(x + 18) = x^4 - 216x^2 + (1728 - j)x + 9j - 3888 = x^4 + px^2 + qx + r.$$

The cubic resolvent is

$$G(y, j) = y^3 - 2py^2 + (p^2 - 4r)y + q^2 = y^3 + 432y^2 + 36(1728 - j)y + (j - 1728)^2,$$

with discriminant $D = -27j^2(j-1728)^2$. I claim that $G(y, j)$ is irreducible in $k[y, j]$. Note that

$$G(y - 144, j) = y^3 - 36jy + 1728j + j^2 = y^3 + Py + Q, \quad P = -36j, Q = 1728j + j^2.$$

Writing $G(y-144, j)$ as a polynomial in j gives $G(y-144, j) = j^2+(1728-36y)j+y^3$ and the discriminant of this quadratic in j is $\delta = -4(y - 36)(y - 144)^2$. Since the characteristic of k is not 2 or 3, δ is never a square in $k(y)$, and as a polynomial in j, $G(y - 144, j)$ cannot have a root in $k(y)$. This proves the claim.

Since $\sqrt{-3} \in k$, D is a square in k, and since $G(y, j)$ is irreducible over $k(j)$, we know the splitting field of $F(x)$ has Galois group A_4 over $k(j)$. We find the roots of $G(y, j) = 0$ using the Tartaglia-Cardan formulas. If Θ_i are the roots of $G(y, j)$, then one root of $G(y - 144, j)$ is

$$\Theta_1 + 144 = \frac{1}{3}\left(\frac{-27}{2}Q + \frac{3}{2}\sqrt{-3D}\right)^{1/3} + \frac{1}{3}\left(\frac{-27}{2}Q - \frac{3}{2}\sqrt{-3D}\right)^{1/3}. \tag{1}$$

We have

$$\frac{-27}{2}Q + \frac{3}{2}\sqrt{-3D} = \frac{-27}{2}(1728j + j^2) + \frac{3}{2} \cdot 9j(j - 1728) = -2^6 \cdot 3^6 \cdot j,$$

and

$$\frac{-27}{2}Q - \frac{3}{2}\sqrt{-3D} = \frac{-27}{2}(1728j + j^2) - \frac{3}{2} \cdot 9j(j - 1728) = -27j^2,$$

so

$$\Theta_1 + 144 = -12j^{1/3} - j^{2/3}.$$

Note that the product of the cube roots in (1) is $(-36j^{1/3})(-3j^{2/3}) = -3(-36j) = -3P$, as required. Now

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

so that

$$j^{1/3} = \frac{\alpha(\alpha^3-24)}{3\alpha/\beta} = \frac{\beta(\alpha^3-24)}{3} = \frac{\beta(\beta^3+216)}{\beta^3-27},$$

$$j^{2/3} = \frac{\beta^2(\beta^3+216)^2}{(\beta^3-27)^2}.$$

Hence,

$$\Theta_1 = -144 - 12\frac{\beta(\beta^3+216)}{\beta^3-27} - \frac{\beta^2(\beta^3+216)^2}{(\beta^3-27)^2}.$$

and

$$-\Theta_1 = \left(\frac{\beta^4+6\beta^3+54\beta^2-108\beta+324}{\beta^3-27}\right)^2.$$

Thus we take

$$\sqrt{-\Theta_1} = \frac{\beta^4+6\beta^3+54\beta^2-108\beta+324}{\beta^3-27}, \tag{2}$$

an element of the field $k(\beta)$. The other roots of the resolvent cubic are

$$\Theta_2 = -144 - 12\omega\frac{\beta(\beta^3+216)}{\beta^3-27} - \omega^2\frac{\beta^2(\beta^3+216)^2}{(\beta^3-27)^2}$$

and

$$\Theta_3 = -144 - 12\omega^2\frac{\beta(\beta^3+216)}{\beta^3-27} - \omega\frac{\beta^2(\beta^3+216)^2}{(\beta^3-27)^2},$$

which are the images of Θ_1 under the maps $(\beta \to \omega\beta)$ and $(\beta \to \omega^2\beta)$. These maps are automorphisms of the field $k(\beta)/k(j)$, since

$$j = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27} = \frac{\beta^3(\beta^3+216)^3}{(\beta^3-27)^3}. \tag{3}$$

Thus equation (2) implies that

$$\sqrt{-\Theta_2} = \frac{\omega\beta^4 + 6\beta^3 + 54\omega^2\beta^2 - 108\omega\beta + 324}{\beta^3 - 27},$$

and

$$\sqrt{-\Theta_3} = \frac{\omega^2\beta^4 + 6\beta^3 + 54\omega\beta^2 - 108\omega^2\beta + 324}{\beta^3 - 27}.$$

From the formulas in van der Waerden [vdw, pp. 190-192] one root of $F(x) = 0$ is

$$\xi_1 = 18 + \frac{1}{2}(\sqrt{-\Theta_1} + \sqrt{-\Theta_2} + \sqrt{-\Theta_3}) = 18 + \frac{9(\beta^3 + 54)}{\beta^3 - 27} = \frac{27\beta^3}{\beta^3 - 27} = \alpha^3,$$

as we know already. A computation on Maple yields the three additional roots

$$\xi_2 = 18 + \frac{1}{2}(\sqrt{-\Theta_1} - \sqrt{-\Theta_2} - \sqrt{-\Theta_3}) = \frac{(\beta + 6)^3}{\beta^2 + 3\beta + 9} = \frac{(\beta + 6)^3}{(\beta - 3\omega)(\beta - 3\omega^2)},$$

$$\xi_3 = 18 + \frac{1}{2}(-\sqrt{-\Theta_1} + \sqrt{-\Theta_2} - \sqrt{-\Theta_3}) = \frac{\omega(\beta + 6\omega^2)^3}{(\beta - 3)(\beta - 3\omega)},$$

$$\xi_4 = 18 + \frac{1}{2}(-\sqrt{-\Theta_1} - \sqrt{-\Theta_2} + \sqrt{-\Theta_3}) = \frac{\omega^2(\beta + 6\omega)^3}{(\beta - 3)(\beta - 3\omega^2)}.$$

This shows that the roots of the resolvent cubic $G(y, j)$ and the roots of $F(x)$ are contained in the field $k(\beta)$. Since $[k(\beta) : k(j)] = 12$, this proves Proposition 2. $\square$

Now N is the splitting field of the polynomial $F(x^3)$, and is therefore generated by the cube roots of the ξ_i. Since

$$(\beta - 3)(\beta - 3\omega)(\beta - 3\omega^2) = \beta^3 - 27 = \frac{27\beta^3}{\alpha^3},$$

we have

$$\xi_2^{1/3} = \frac{\alpha(\beta + 6)}{3\beta}(\beta - 3)^{1/3}, \quad \xi_3^{1/3} = \frac{\alpha(\beta + 6\omega^2)}{3\beta}(\omega\beta - 3)^{1/3},$$

$$\xi_4^{1/3} = \frac{\alpha(\beta + 6\omega)}{3\beta}(\omega^2\beta - 3)^{1/3}.$$

By Proposition 2, N contains the field $k(\beta)$, so we have

$$N = k(\alpha, \beta, (\beta-3)^{1/3}, (\omega\beta-3)^{1/3}, (\omega^2\beta-3)^{1/3}). \tag{4}$$

Moreover, $\alpha = \dfrac{3\beta}{(\beta^3-27)^{1/3}}$, so it is clear that N is generated by the three cube roots $(\omega^i\beta-3)^{1/3}$.

Before proving Theorem 1 we prove:

Theorem 3. If $char(k) \neq 2, 3$ and $\omega \in k$, then the normal closure N of the extension $k(\alpha)/k(j(\alpha))$ has degree 324 over $k(j)$. N is a Kummer extension of the normal extension $k(\beta)$ of $k(j)$ with

$$Gal(N/k(\beta)) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad Gal(k(\beta)/k(j)) \cong A_4.$$

Proof. It is clear that the cube roots $(\omega^i\beta-3)^{1/3}$ generate independent extensions over $k(\beta)$, since

$$(\beta-3)^{\varepsilon_1}(\omega\beta-3)^{\varepsilon_2}(\omega^2\beta-3)^{\varepsilon_3} = r^3, \quad r \in k(\beta), \quad \varepsilon_i \in \{0,1,2\},$$

implies by unique factorization in $k[\beta]$ that $\varepsilon_i \equiv 0 \pmod 3$, for $1 \leq i \leq 3$. The assertions of the theorem follow from (4) and Kummer theory. $\square$

Remarks. 1. The automorphisms of $G_{12} = Gal(k(\beta)/k(j))$ have been given in [m2], and are generated by the mappings

$$\sigma_1(\beta) = \frac{3(\beta+6)}{\beta-3}, \quad \sigma_2(\beta) = \omega\beta.$$

Furthermore, by Theorem 3.7 of [m2], the subfield $k(\alpha, \beta)$ of N is the field generated by the coordinates of the points of order 3 on the elliptic curve $E_3(\alpha)$.

2. By [od, Lemma 1.1], $Gal(N/k(j))$, as the Galois group of the polynomial $F(x^3)$ over $k(j)$, is isomorphic to a subgroup H of the wreath product $\mathbb{Z}_3$ *wr* A_4. This wreath product has order $3^4 \cdot 12 = 972$, so H has index equal to 3 in $\mathbb{Z}_3$ *wr* A_4.

2 Proof of Theorem 1.

To prove Theorem 1 we use the theory of algebraic function fields in one variable. For this let $k = \mathbb{F}_{p^2}$, where $p > 3$ is prime. We will also need the fact from [m2, Theorem 1.2(a)] that the values of α for which $E_3(\alpha)$ is supersingular lie in the field $\mathbb{F}_{p^2}$. Consider such a value, and call it α_0, to distinguish it from the indeterminate α. Let $j_0 = j(\alpha_0)$ and assume first that $j_0 \neq 0, 1728$. Because the discriminant of $F(x^3)$ is

$$disc(F(x^3)) = -3^{27} j^8 (j - 1728)^6,$$

the prime divisor P_{j_0} of $k(j)$ corresponding to the irreducible polynomial $j - j_0$ is unramified in N. Furthermore, all the roots α_i of $j(\alpha_i) = j_0$ are supersingular parameters for $E_3(\alpha)$, and therefore all lie in the ground field k. Hence, $F(x^3) = 0$ splits completely (mod P_{j_0}), and therefore the prime divisor P_{j_0} splits into 12 prime divisors of degree 1 in the field $k(\alpha)$. It follows that P_{j_0} splits completely in all the conjugate fields of $k(\alpha)$ inside N and thus splits completely in N. Let $\wp$ be the prime divisor of $k(\alpha)$ for which $\alpha \equiv \alpha_0 \pmod{\wp}$, and let $\mathfrak{p}$ be one of the prime divisors of $\wp$ in N. Then $\alpha \equiv \alpha_0$ and $\beta \equiv \beta_0 \pmod{\mathfrak{p}}$, where (α_0, β_0) is a solution of Fer_3 in k. From [m2] we know that β_0, along with α_0, is a root of the polynomial $\hat{H}_p(z)$ (the Hasse invariant) defined by

$$\hat{H}_p(z) = \left(-\frac{z}{3}\right)^{e-1} W_{(p-e)/3}\left(1 - \frac{z^3}{27}\right), \quad p \equiv e \pmod 3,\ e \in \{1, 2\},$$

where

$$W_n(x) = \sum_{r=0}^{n} \binom{n}{r}^2 x^r.$$

See also [brm, Theorem 5]. This is because the curves $E_3(\alpha_0)$ and $E_3(\beta_0)$ are isogenous and therefore both supersingular. Furthermore, as α_0 runs through all the roots of $\hat{H}_p(z)$, then the values of β_0 for which (α_0, β_0) lies on Fer_3 likewise run through all the roots of $\hat{H}_p(z)$, in such a way that

$$\frac{\beta_0^3(\beta_0^3 + 216)^3}{(\beta_0^3 - 27)^3} = j_0 = \frac{\alpha_0^3(\alpha_0^3 - 24)^3}{\alpha_0^3 - 27}. \tag{5}$$

(See equation (3).) Now the element $(\beta - 3)^{1/3}$ is certainly integral for $\mathfrak{p}$, and so $(\beta - 3)^{1/3} \equiv \gamma_0 \pmod{\mathfrak{p}}$ for some element $\gamma_0 \in k$, since $\mathfrak{p}$ has degree 1 over k.

Therefore,

$$\beta \equiv \beta_0 \equiv \gamma_0^3 + 3 \pmod{\mathfrak{p}}.$$

In other words, $\beta_0 = 3 + \gamma_0^3$ for some $\gamma_0 \in k$. In the same way, working with the elements $(\omega^i\beta - 3)^{1/3}$, we obtain $\omega^i\beta_0 = 3 + \gamma_i^3$ for $\gamma_i \in k$. This shows that all the $\beta_0's$ corresponding to $\alpha = \alpha_0$ have the desired property. By the above remarks, if β_0 is any root of $\hat{H}_p(z)$, there is another root α_0 of this polynomial for which (α_0, β_0) lies on Fer_3. Since α_0 was arbitrary (with $j_0 \neq 0, 1728$), this proves the theorem for all the supersingular parameters corresponding to j-invariants other than 0 or 1728.

It remains to prove the theorem if $j_0 = 0$ or 1728. If $j_0 = 0$ we can check directly that the values of $\beta_0 = 0, -6, -6\omega, -6\omega^2$ in (5) are representable as $3 + \gamma^3$ with $\gamma \in k$. In this case the prime $p \equiv 2 \pmod 3$, so for $\beta_0 = 0$, the equation $x^3 + 3 = 0$ has one root in $\mathbb{F}_p$ and therefore two more roots in $\mathbb{F}_{p^2} = k$. The value $\beta_0 = -6 = 3 + \gamma^3$ for three values of $\gamma \in k$ for the same reason. Considering the values $\beta_0 = -6\omega^i$ with $i = 1, 2$ together, note that

$$(x^3 + 3 + 6\omega)(x^3 + 3 + 6\omega^2) = x^6 + 27 = (x^2 + 3)(x^2 + 3x + 3)(x^2 - 3x + 3).$$

This proves the claim for $j_0 = 0$.

Remark 1. Note that the prime divisor P_0 of $k(j)$ corresponding to $j - 0 = j$ ramifies in the field N. This is because the extension

$$k(j^{1/3}) = k\left(\frac{\beta(\beta^3 + 216)}{\beta^3 - 27}\right)$$

is generated by $t = j^{1/3}$ with minimal polynomial $t^3 - j$ over $k(j)$. Since this polynomial is Eisenstein with respect to the prime element j of P_0, P_0 ramifies completely in $k(t)$. It follows that $P_0 = \wp_0^3\wp_1^3\wp_2^3\wp_3^3$ in $k(\beta)$, where $\wp_0$ corresponds to $\beta - 0 = \beta$ and $\wp_i$ corresponds to $\beta + 6\omega^i$, for $1 \leq i \leq 3$. The above argument now shows that each of the prime divisors $\wp_i$ splits completely in N. Thus, P_0 splits into $g = 108$ prime divisors of degree $f = 1$ and ramification index $e = 3$ over P_0.

Now consider $j_0 = 1728$. In this case $p \equiv 3 \pmod 4$ and we have

$$\begin{aligned} x^3(x^3 + 216)^3 - 1728(x^3 - 27)^3 &= (x^2 - 6x - 18)^2(x^4 + 6x^3 + 54x^2 - 108x + 324)^2 \\ &= q_1(x)^2 q_2(x)^2, \end{aligned} \tag{6}$$

where the irreducible quartic $q_2(x) = x^4 + 6x^3 + 54x^2 - 108x + 324$ has Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$ over $\mathbb{Q}$. That the roots β_0 of $q_1(x) = x^2 - 6x - 18$ have the form $3 + \gamma^3$ can be seen by considering the polynomial $q_1(x^3 + 3) = (x^2 - 3)(x^4 + 3x^2 + 9)$. Since $x^4 + 3x^2 + 9$ likewise has Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$ over $\mathbb{Q}$, it splits into a product of linear polynomials or a product of quadratics over $\mathbb{F}_p$, for every prime p. Hence, these values of β_0 have the required form.

We also have $q_2(x^3 + 3) = x^{12} + 18x^9 + 162x^6 + 486x^3 + 729$. The roots of this polynomial are the cube roots of the roots of $q_2(x + 3)$, which over $\mathbb{Q}$ are

$$\eta = \frac{3\sqrt{3}}{2}(1 - \sqrt{3})(1 + i) = \sqrt{3}^3 \frac{(1 - \sqrt{3})(1 + i)}{2} \tag{7}$$

and its conjugates. The root field $L = \mathbb{Q}(\eta^{1/3})$ of the polynomial $q_2(x^3 + 3)$ is a Kummer extension of the abelian extension $K = \mathbb{Q}(\sqrt{3}, i)$. A prime $p \equiv 3 \pmod 4$ is inert in $\mathbb{Q}(i)$ and therefore splits into two primes $\mathfrak{q}_1, \mathfrak{q}_2$ of degree 2 in K. To show that $q_2(x^3 + 3)$ splits modulo p into a product of linear and quadratic polynomials, we must show that the cubic residue symbols

$$\left(\frac{\eta}{\mathfrak{q}_1}\right)_3 = \left(\frac{\eta}{\mathfrak{q}_2}\right)_3 = 1. \tag{8}$$

For this we note $\left(\dfrac{\eta}{\mathfrak{q}_1}\right)_3 \equiv \eta^{(p^2-1)/3} \pmod{\mathfrak{q}_1}$.

If $p \equiv 1 \pmod 3$, then $\left(\dfrac{3}{p}\right) = -\left(\dfrac{p}{3}\right) = -1$, so $\sqrt{3}$ is not rational (mod p), and we have

$$(1 - \sqrt{3})^{(p^2-1)/3} \equiv (-2)^{(p-1)/3} \equiv \left(\frac{2}{p}\right)_3 \pmod{\mathfrak{q}_1}.$$

In this case

$$(1 + i)^{(p^2-1)/3} \equiv 2^{(p-1)/3} \equiv \left(\frac{2}{p}\right)_3 \pmod{\mathfrak{q}_1},$$

and $\left(\dfrac{2}{\mathfrak{q}_1}\right)_3 \equiv \left(\dfrac{4}{p}\right)_3$, which implies by (7) that $\left(\dfrac{\eta}{\mathfrak{q}_1}\right)_3 = 1$.

On the other hand, if $p \equiv 2 \pmod 3$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = +1$, so $\sqrt{3}$ is rational (mod p), and we have

$$(1-\sqrt{3})^{(p^2-1)/3} \equiv \left(\frac{1-\sqrt{3}}{1-\sqrt{3}}\right)^{(p+1)/3} \equiv 1 \pmod{\mathfrak{q}_1}.$$

In this case we have

$$(1+i)^{(p^2-1)/3} \equiv \left(\frac{1-i}{1+i}\right)^{(p+1)/3} \equiv (-i)^{(p+1)/3} \equiv 1 \pmod{\mathfrak{q}_1},$$

since $(p+1)/3$ is divisible by 4. Furthermore, $2^{(p^2-1)/3} \equiv (2^{p-1})^{(p+1)/3} \equiv 1 \pmod p$, so (7) gives also here that $\left(\frac{\eta}{\mathfrak{q}_1}\right)_3 = 1$.

This proves that (8) holds, and therefore that the primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ of K split in L. Hence all the prime divisors of p in the field L have degree 2 over $\mathbb{Q}$, and since $disc(q_2(x^3+3)) = 2^{24}3^{78}$, this implies that $q_2(x^3+3)$ factors modulo p into quadratic factors. Therefore, all the values of β_0 corresponding to $j = 1728$ have the form $3+\gamma^3$ with $\gamma \in \mathbb{F}_{p^2}$. This completes the proof of Theorem 1. $\square$

Remark 2. Let P_∞ be the prime divisor of $k(j)$ given by the degree valuation. It is easy to see that $P_\infty = \wp_{\infty,1}^3\wp_{\infty,2}^3\wp_{\infty,3}^3\wp_{\infty,4}^3$ in $k(\beta)$, where each $\wp_{\infty,i}$ has degree 1 over k. By the Hurwitz genus formula [sti, p. 88], the genus $g' = 0$ of $k(\beta)$ is related to the genus $g = 0$ of $k(j)$ by the formula

$$2g' - 2 = [k(\beta) : k(j)](2g-2) + deg\ \mathsf{Diff}\ k(\beta)/k(j), \tag{9}$$

so the different $\mathsf{Diff}\ k(\beta)/k(j)$ has degree 22 in $k(\beta)$. Because

$$disc(x^3(x^3+216)^3 - j(x^3-27)^3) = -3^{147}j^8(j-1728)^6$$

the only ramified primes in $k(\beta)/k(j)$ are the primes P_0, P_{1728}, P_∞. The primes dividing P_0 and P_∞ contribute 8+8=16 to the different degree, so the primes dividing P_{1728} must contribute 6. On the other hand, P_{1728} splits into at least 6 prime divisors in $k(\beta)$, by (6). Together, these facts imply that P_{1728} splits as a product of

the squares of 6 prime divisors in $k(\beta)$, all having degree 1 over k. By the above computations, and the fact that the roots β_0 of (6) are invariant under $(\beta_0 \to \omega\beta_0)$, these six prime divisors split completely in the field N. Hence, P_{1728} splits in N as the product of the squares of $6 \cdot 27 = 162$ prime divisors of N of degree 1 over k.

The proof of Theorem 1, together with Remarks 1 and 2, shows that the following statement holds.

Theorem 4. If j_0 is the j-invariant of a supersingular elliptic curve in characteristic p, then the numerator divisor P_{j_0} of the linear polynomial $j - j_0$ of the field $\mathbb{F}_{p^2}(j)$ is divisible only by prime divisors of degree 1 in the normal closure N of the field extension $\mathbb{F}_{p^2}(\alpha)/\mathbb{F}_{p^2}(j)$, where α is a root of $F(x^3) = x^3(x^3 - 24)^3 - j(x^3 - 27)$.

Remark 3. Not all j-invariants $j_0 \in \mathbb{F}_{p^2}$ for which the divisor P_{j_0} in Theorem 4 splits completely in N are supersingular. This is shown by the example $p = 31$ and $j_0 = 1$. In this case we have

$$F(x^3) \equiv x^3(x^3 - 24)^3 - 1 \cdot (x^3 - 27) \equiv (x^2 + 16x + 11)(x^2 + 17x + 20)(x^2 + 18x + 27)$$
$$\times(x^2 + 22x + 7)(x^2 + 23x + 4)(x^2 + 28x + 24) \pmod{31, P_1},$$

so that P_1 splits in N/k. As a consequence, the polynomial

$$f(x, j) = x^3(x^3 + 216)^3 - j(x^3 - 27)^3$$

splits completely $(\text{mod } 31, P_1)$, and all the values of β_0 which are roots of $f(x, 1)$ (mod 31) have the form $3 + \gamma^3$ with $\gamma \in \mathbb{F}_{31^2}$. Specifically, we have that

$$f(x^3 + 3, 1) \equiv (x^2 + 5x + 30)(x^2 + 23x + 1)(x^2 + 17x + 3)(x^2 + 22x + 15)(x^2 + 7x + 9)$$
$$\times(x^2 + 4x + 8)(x^2 + 23x + 3)(x^2 + 25x + 6)(x^2 + 28x + 17)(x^2 + 18x + 23)(x^2 + 17x + 15)$$
$$\times(x^2 + 16x + 22)(x^2 + 20x + 14)(x^2 + 22x + 25)(x^2 + 23x + 13)(x^2 + x + 26)(x^2 + 17x + 5)$$
$$\times(x^2 + 22x + 13) \pmod{31}.$$

However, the polynomial $F((x^3+3)^3)$ splits into 6-th degree factors (mod P_1), so that the values of α_0 corresponding to $j_0 = 1$ are not of the form $3+\gamma^3$ with $\gamma \in \mathbb{F}_{31^2}$. Hence, $j_0 = 1$ is not supersingular.

It is clear in this example that the quantity $(\alpha - 3)^{1/3}$ does not lie in N. This is true more generally. See the remark at the end of Section 3 below.

3 Points on a genus 19 curve.

The following theorem is a consequence of Theorem 1.

Theorem 5. Supersingular parameters α_0 of the Deuring normal form $E_3(\alpha)$ in charcteristic $p > 3$ give rise to points on the genus 19 curve

$$C_{19}: \quad z^3w^3(z^6+9z^3+27)(w^6+9w^3+27) = 729 \tag{10}$$

which are defined over $\mathbb{F}_{p^2}$. The number of points on this curve over $\mathbb{F}_{p^2}$ which arise from supersingular parameters is

$$27(p-1) - 9\left(1 - \left(\frac{p}{3}\right)\right).$$

Proof. Let (α_0, β_0) be a point on Fer_3. Then $\alpha_0 = z_0^3 + 3$ and $\beta_0 = w_0^3 + 3$ for $(z_0, w_0) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$, and (z_0, w_0) is a point on the curve

$$27(z^3+3)^3 + 27(w^3+3)^3 = (z^3+3)^3(w^3+3)^3.$$

This equation simplifies to the equation given in the theorem. For every supersingular parameter $\alpha_0 \neq 0$ in $\mathbb{F}_{p^2}$ there are three values of $\beta_0 \neq 0$ for which (α_0, β_0) lies on Fer_3. Since α_0 and β_0 are never equal to 3 (otherwise $E_3(\alpha_0)$ is singular), each of these points gives rise to 9 points (z_0, w_0) on the curve C_{19}. If $p \equiv 1 \pmod 3$ there are $p-1$ parameters α_0, none of which are 0, and therefore $27(p-1)$ corresponding points (z_0, w_0). If $p \equiv 2 \pmod 3$ there are $p-2$ nonzero values of α_0. In this case the supersingular value $\alpha_0 = 0$ corresponds to $\beta_0 = 0$ and there are only 9 points (z_0, w_0) on C_{19} corresponding to $(0,0)$ on Fer_3. This gives the count stated in the theorem. □

Solutions of C_{19} in Hilbert class fields.

Using results of [m2] and [m3] we will now show that there are points on the curve C_{19} defined over the Hilbert class field of any quadratic field $K = \mathbb{Q}(\sqrt{-d})$

whose discriminant satisfies $-d \equiv 1 \pmod 3$. I first summarize the results we need from [m3]. In that paper I have studied the elliptic curves $E_\alpha = E_3(\alpha)$ in Deuring normal form which have complex multiplication by the ring of integers R_K of the field K. The parameter α of such a curve satisfies the equation

$$\alpha^3(\alpha^3 - 24)^3 - j(\alpha^3 - 27) = 0, \tag{11}$$

where $j = j(E_\alpha)$ is a root of the class equation $H_{-d}(x) = 0$. (Note that $\alpha \neq 0$ since $j = 0$ is not a root of $H_{-d}(x) = 0$.) Furthermore, if β is chosen so that (α, β) is a point on Fer_3, then by (3), β is a root of the polynomial

$$G_d(x) = (x^3 - 27)^{3h(-d)} H_{-d}\left(\frac{x^3(x^3 + 216)^3}{(x^3 - 27)^3}\right).$$

By the corollary to [m3, Prop. 3], all the roots of $G_d(x)$ are contained in the field $\Sigma(\omega)$, where Σ is the Hilbert class field of K and ω is a primitive cube root of unity.

Furthermore, for each root j of $H_{-d}(x) = 0$, there is an α satisfying (11), i.e., $j(E_\alpha) = j$, for which $\alpha, \beta \in \Sigma$. In this case $\sigma_1(\beta) = 3(\beta + 6)/(\beta - 3) = \alpha^\tau$ for a certain automorphism τ in $Gal(\Sigma/K)$, and α and β are conjugates over $\mathbb{Q}$. (See Remark 1 following Theorem 3 and [m3, Prop. 4].)

The point (α, β) is related to a *Heegner point* for $X_0(3)$ over K, since there is a cyclic 3-isogeny $\phi_{\alpha,\beta} : E_3(\alpha) \to E_3(\beta)$ and $E_3(\alpha)$ and $E_3(\beta)$ both have complex multiplication by R_K. (See [m2, Prop. 3.5] and [gr].)

We will show that the solution (α, β) of Fer_3 in the Hilbert class field Σ of K has the property that $\alpha = 3 + \gamma_1^3$ and $\beta = 3 + \gamma_0^3$ for certain elements $\gamma_0, \gamma_1 \in \Sigma$. This will yield a point (γ_1, γ_0) on C_{19} which is defined over Σ.

Lemma 6. Let $K = \mathbb{Q}(\sqrt{-d})$, with $-d \equiv 1 \pmod 3$. If $E_\alpha : Y^2 + \alpha XY + Y = X^3$ has complex multiplication by R_K, then the coordinates of the points of finite order on E_α lie in an abelian extension of the Hilbert class field Σ of K. In particular, the parameter α lies in an abelian extension of Σ.

Proof. This follows from [si, Thm. 2.3, p. 108] in the case that $\alpha \in \Sigma$, in which case E_α is defined over the Hilbert class field Σ. (This is an unstated assumption in [si, Thm. 2.3] which is used in Silverman's proof on p. 109.) Suppose now that α is an arbitrary root of (11), for some root j of $H_{-d}(x) = 0$. We choose another root α' of

the same equation which lies in Σ, and for which (α', β') lies on Fer_3. If $\alpha' = \omega^i \alpha$ for some i, then an isomorphism $\iota : E_\alpha \to E_{\alpha'}$ is clearly given by

$$X' = \omega^{2i} X, \quad Y' = Y,$$

and this implies the statement of the lemma for the curve E_α, since ω lies in an abelian extension of Σ.

Otherwise, by the arguments of [m2, pp. 262-263] we may take $\beta' = \sigma_1(\beta) = 3(\beta+6)/(\beta-3)$, by replacing β by $\omega^i \beta$ for some i. Then an isomorphism $\iota : E_\alpha \to E_{\alpha'}$ is given by the equations (3.17) in [m2, Prop. 3.10]:

$$X' = -\frac{\gamma'}{\gamma} X + \gamma', \tag{12a}$$

$$Y' = \frac{\sqrt{-3}(\beta - 3)}{9} \left(Y - \sqrt{-3}\omega^2 \frac{\delta}{\gamma} X - \omega \delta \right), \tag{12b}$$

where

$$\gamma = \frac{-3\beta}{\alpha(\beta - 3)}, \quad \delta = \frac{\beta - 3\omega}{\beta - 3}$$

are the coordinates of a point $(X, Y) = (\gamma, \delta)$ of order 3 on E_α, and

$$\gamma' = -\frac{\beta + 6}{3\alpha'}$$

is the X'-coordinate of a point of order 3 on $E_{\alpha'}$. Now, by the choice of α' and the fact that β is a root of $G_d(x) = 0$, the element γ' lies in $\Sigma(\omega) \subset \Sigma^{ab}$, the maximal abelian extension of Σ inside $\bar{\mathbb{Q}}$. Furthermore, if (X', Y') is a point of finite order on $E_{\alpha'}$, then $X', Y' \in \Sigma^{ab}$ by [si, Thm. 2.3]. It follows from (12a) that $-X/\gamma = \alpha X(\beta - 3)/(3\beta) \in \Sigma^{ab}$ for every point (X, Y) of finite order on E_α, which gives that $\alpha X, Y \in \Sigma^{ab}$, by (12b).

We now use [m2, Prop. 3.6, Remark], according to which the roots x of the cubic equation

$$x^3 - (3 + \alpha)x^2 + \alpha x + 1 = 0$$

are the X-coordinates of points of order 9 on E_α. It follows that

$$x^2(x - 3 - \alpha) = x^3 - (3 + \alpha)x^2 = -\alpha x - 1 \in \Sigma^{ab}. \tag{13}$$

On the other hand, $\alpha^3 = 27\beta^3/(\beta^3 - 27) = r \in \Sigma^{ab}$, so multiplying the inclusion (13) by α^3 gives that $\alpha x - \alpha(3+\alpha) \in \Sigma^{ab}$, whence it follows that $(\alpha^2 + 3\alpha) \in \Sigma^{ab}$. Now form the expression:

$$(\alpha^2 + 3\alpha)^2 - 9(\alpha^2 + 3\alpha) - 6r = \alpha^4 - 27\alpha = (r - 27)\alpha.$$

This gives that $(r - 27)\alpha \in \Sigma^{ab}$. But $r - 27 = \alpha^3 - 27$ is the discriminant of the curve E_α, which is non-zero by (11), so we get that $\alpha \in \Sigma^{ab}$. Hence, $X, Y \in \Sigma^{ab}$ for every point (X, Y) of finite order on E_α, which proves the lemma. $\square$

Now we can prove

Theorem 7. If the discriminant $-d$ of the field $K = \mathbb{Q}(\sqrt{-d})$ satisfies $-d \equiv 1 \pmod 3$, then there is a solution of the equation

$$C_{19}: \quad z^3w^3(z^6 + 9z^3 + 27)(w^6 + 9w^3 + 27) = 729$$

in the Hilbert class field Σ of K.

Proof. We use the same argument (suitably modified) as in the proof of Theorem 1 in Section 2. This time we take the field k to be the splitting field of the polynomial

$$\tilde{H}_d(x) = (x^3 - 27)^{h(-d)} H_{-d}\left(\frac{x^3(x^3 - 24)^3}{x^3 - 27}\right)$$

over $\mathbb{Q}$. Then $\Sigma(\omega) \subset k$ and k/Σ is abelian by Lemma 6. (Note that $\omega \notin \Sigma$ since 3 does not divide $disc(\Sigma/\mathbb{Q})$.) Reverting back to the same notation as in Sections 1 and 2, we take j_0 to be a root of the class equation $H_{-d}(x)$. Then $j_0 \neq 0, 1728$ and all the roots of $j(\alpha_i) = j_0$ lie in the field k. It follows that the prime divisor P_{j_0} of $k(j)$ splits into primes of degree 1 in the field $k(\alpha)$, and therefore splits completely in the normal closure N of $k(\alpha)/k(j)$. Consider a root α_0 of $\tilde{H}_d(x)$ for which $j(\alpha_0) = j_0$ and $\alpha_0, \beta_0 \in \Sigma$, and any prime divisor $\mathfrak{p}$ of N for which

$$\alpha \equiv \alpha_0 \quad \beta \equiv \beta_0 \pmod{\mathfrak{p}},$$

so that $\mathfrak{p}|P_{j_0}$. Since $\mathfrak{p}$ has degree 1 over k, it follows that there is an element $\gamma_0 \in k$ for which

$$(\beta - 3)^{1/3} \equiv \gamma_0 \pmod{\mathfrak{p}},$$

and therefore $\beta_0 \equiv \beta \equiv \gamma_0^3 + 3 \pmod{\mathfrak{p}}$. Hence, $\beta_0 = \gamma_0^3 + 3$ in k. However, γ_0 generates an abelian extension of Σ and $\gamma_0^3 = \beta_0 - 3 \in \Sigma$. This implies that $x^3 - \gamma_0^3$ is reducible over Σ: otherwise, its splitting would have Galois group S_3 over Σ. Therefore, $\beta_0 = 3 + \gamma_0^3$ for some $\gamma_0 \in \Sigma$, and applying the automorphism $\tau^{-1} \in Gal(\Sigma/K)$ to the equation $\sigma_1(\beta_0) = \alpha_0^\tau$ we get that

$$\alpha_0 = \sigma_1(\beta_0^{\tau^{-1}}) = 3 + \frac{27}{\beta_0^{\tau^{-1}} - 3} = 3 + \left(\frac{3}{\gamma_0^{\tau^{-1}}}\right)^3.$$

Therefore, $\alpha_0 = 3 + \gamma_1^3$, with $\gamma_1 = 3/\gamma_0^{\tau^{-1}} \in \Sigma$. Now the equation $27\alpha_0^3 + 27\beta_0^3 = \alpha_0^3\beta_0^3$ implies that $(z, w) = (\gamma_1, \gamma_0)$ is a point on C_{19} defined over Σ, as in the proof of Theorem 5. $\square$

As numerical examples we give the following points (z, w) on C_{19} with coordinates in the Hilbert class field Σ_d of the field $K = \mathbb{Q}(\sqrt{-d})$, for various d with $-d \equiv 1 \pmod 3$ (see [m3]):

$$d = 8: \quad z = 1 + \sqrt{-2}, \quad w = 1 - \sqrt{-2}$$

$$d = 11: \quad z = \frac{1 + \sqrt{-11}}{2}, \quad w = \frac{1 - \sqrt{-11}}{2}$$

$$d = 20: \quad z = (1 + \sqrt{-1})\left(\frac{-1 + \sqrt{-5}}{2}\right), \quad w = (1 + \sqrt{-1})\left(\frac{-1 - \sqrt{-5}}{2}\right)$$

$$d = 35: \quad z = \frac{\sqrt{5} + \sqrt{-7}}{2}, \quad w = \frac{-\sqrt{5} + \sqrt{-7}}{2}$$

$$d = 56: \quad z = \frac{2 - 3\sqrt{2} + \sqrt{-14}}{4} + \frac{1}{2}\sqrt{(1 + \sqrt{2})(\sqrt{2} + \sqrt{-7})},$$

$$w = \frac{2 + 3\sqrt{2} - \sqrt{-14}}{4} + \frac{1}{2}\sqrt{(1 - \sqrt{2})(-\sqrt{2} + \sqrt{-7})}$$

$$d = 68: \quad z = \frac{3 + 2\sqrt{-1} - \sqrt{17}}{4} + \frac{3 + 4\sqrt{-1} + \sqrt{17}}{16}\sqrt{2 + 2\sqrt{17}},$$

$$w = \frac{3 + 2\sqrt{-1} + \sqrt{17}}{4} + \frac{3 + 4\sqrt{-1} - \sqrt{17}}{16}\sqrt{2 - 2\sqrt{17}}$$

Remark. Note that the function field of the curve C_{19} over the field k is the field $L = k(\alpha, \beta, (\alpha - 3)^{1/3}, (\beta - 3)^{1/3})$. Since L has genus 19, it cannot be a subfield of the field N, which has genus 10, as we will see in the next section. This shows that $(\alpha - 3)^{1/3} \notin N$.

4 The genus of N and the modulary group $\bar{\Gamma}_9$.

In this section we return to the situation of Section 1, so that k is any field containing a primitive cube root of unity ω whose characteristic is different from 2 or 3. It is not difficult to compute the genus of the algebraic function field N, using standard arguments. (See [sti].)

For example, from (3) and Remark 2 of Section 2 it is clear that three of the prime divisors $\wp_{\infty,i}$ correspond to the linear factors of $\beta^3 - 27 = (\beta - 3)(\beta - 3\omega)(\beta - 3\omega^2)$, while $\wp_{\infty,4} = \wp_\infty$ is the degree valuation on $k(\beta)$. We relabel the $\wp_{\infty,i}$ for $1 \leq i \leq 3$ as $\wp_{3\omega^i}$, corresponding to $(\beta - 3\omega^i)$. Furthermore, from Remarks 1 and 2 of Section 2, none of the prime divisors of P_0 or P_{1728} is ramified in $N/k(\beta)$. Therefore, the only primes that can ramify in $N/k(\beta)$ are the $\wp_{3\omega^i}$ and $\wp_\infty$. In each of the Kummer extensions $k(t_i)/k(\beta)$ with $t_i = (\omega^i\beta - 3)^{1/3}$ it is clear that $\wp_{3\omega^{2i}}$ is the cube of a prime divisor in $k(t_i)$, as is $\wp_\infty$, while the other $\wp_{3\omega^j}$ are unramified. It follows that $\wp_{3\omega^i}$ is the cube of a product of prime divisors in N having degree 9. On the other hand, Abhyankar's Lemma [sti, p. 125] and the fact that $\wp_\infty$ has ramification index 3 in each of the extensions $k(t_i)/k(\beta)$ imply that $\wp_\infty$ has ramification index 3 in $N/k(\beta)$ also. This can also be seen from the fact that the primes $\wp_\infty$ and $\wp_{3\omega^i}$ are conjugate to each other over $k(j)$, since $k(\beta)$ is normal over $k(j)$. Therefore, the different has degree $deg\ \mathsf{Diff}\ N/k(\beta) = 4 \cdot 9 \cdot 2 = 72$. By the Hurwitz genus formula we have

$$2g(N) - 2 = 27(2g(k(\beta)) - 2) + deg\ \mathsf{Diff}\ N/k(\beta) = -54 + 72 = 18.$$

Hence, the genus of N is $g(N) = 10$.

The data $[N : k(j)] = 324$ and $g(N) = 10$ look suspiciously like the data for the modulary group $\bar{\Gamma}_9$ given in [kf, p. 398]. (See also [sch, p.76].) In fact, we have:

Theorem 8. If $char(k) \neq 2, 3$ and $\omega \in k$, then $Gal(N/k(j)) \cong \bar{\Gamma}_9 = \{(az+b)/(cz+d) : a, b, c, d, \in \mathbb{Z}_9,\ ad - bc \equiv 1 \pmod 9\}$.

I have been assisted in finding this isomorphism by Rodney Lynch (private communication). Following Lynch's calculations, let us define elements of $\bar{\Gamma}_9$ as follows:

$$F(z) = \frac{z}{3z+1}, \quad G(z) = \frac{5z+6}{3z+2}, \quad H(z) = \frac{2z+6}{3z+5},$$

$$A(z) = \frac{-1}{z} = \frac{8}{z}, \quad B(z) = \frac{z+4}{4z+8}, \quad C(z) = \frac{8z+2}{3z+2}.$$

Then F, G, H generate an abelian group A isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, while A, C generate a subgroup S of $\bar{\Gamma}_9$ isomorphic to A_4. Moreover, $CAC^{-1} = B$ and $CBC^{-1} = AB$, where $\{I, A, B, AB\}$ is a Klein 4-group and C has order 3. Further, the group $\mathsf{S} =< A, C >$ acts on $\mathsf{A} =< F, G, H >$ in the following way:

$$CFC^{-1} = H^2, \quad CGC^{-1} = F^2, \quad CHC^{-1} = G, \tag{14}$$

$$AFA^{-1} = F^2GH, \quad AGA^{-1} = H, \quad AHA^{-1} = G. \tag{15}$$

Hence, A is normal in $\bar{\Gamma}_9$, and a lengthy calculation shows that $\bar{\Gamma}_9 = \mathsf{AS}$ is a semi-direct product of A and S.

In accordance with Theorem 3, we now define elements of $Gal(N/k(j))$ as follows: $\phi, \gamma, \eta \in Gal(N/k(\beta))$ are defined by

$$\left((\beta-3)^{1/3}\right)^{\phi} = \omega(\beta-3)^{1/3}, \quad \left((\omega^i\beta-3)^{1/3}\right)^{\phi} = (\omega^i\beta-3)^{1/3}, \quad i = 1, 2; \tag{16$_\phi$}$$

$$\left((\omega\beta-3)^{1/3}\right)^{\gamma} = \omega^2(\omega\beta-3)^{1/3}, \quad \left((\omega^i\beta-3)^{1/3}\right)^{\gamma} = (\omega^i\beta-3)^{1/3}, \quad i = 0, 2; \tag{16$_\gamma$}$$

$$\left((\omega^2\beta-3)^{1/3}\right)^{\eta} = \omega^2(\omega^2\beta-3)^{1/3}, \quad \left((\omega^i\beta-3)^{1/3}\right)^{\eta} = (\omega^i\beta-3)^{1/3}, \quad i = 0, 1. \tag{16$_\eta$}$$

We also define the elements

$$\beta^{\sigma_1} = \frac{3(\beta+6)}{\beta-3}, \quad \beta^{\sigma_2} = \omega\beta$$

generating $G_{12} = Gal\left(k(\beta)/k(j)\right)$, as in the remark following Theorem 3. The automorphism σ_1 has order 2, while σ_2 has order 3, and σ_1 and $\sigma_2\sigma_1\sigma_2^{-1}$ generate a Klein 4-group. We extend the linear fractional maps σ_1 and σ_2 to be automorphisms of $N/k(j)$, as follows. Since

$$\beta^{\sigma_1} = 3 + \frac{27}{\beta-3},$$

we may, on multiplying by a suitable power of ϕ, assume that

$$\left((\beta-3)^{1/3}\right)^{\sigma_1} = \frac{3}{(\beta-3)^{1/3}}. \tag{17$_1$}$$

We also have that

$$(\omega\beta-3)^{\sigma_1} = \omega\frac{3(\beta+6)}{\beta-3} - 3 = \frac{(3\omega-3)\beta+18\omega+9}{\beta-3} = 3(\omega^2-\omega)\frac{\omega^2\beta-3}{\beta-3},$$

so on multiplying by a suitable power of η we may take

$$\left((\omega\beta-3)^{1/3}\right)^{\sigma_1} = (\omega-\omega^2)\frac{(\omega^2\beta-3)^{1/3}}{(\beta-3)^{1/3}}. \tag{17$_2$}$$

Reversing the roles of ω and ω^2 we may also take

$$\left((\omega^2\beta-3)^{1/3}\right)^{\sigma_1} = (\omega^2-\omega)\frac{(\omega\beta-3)^{1/3}}{(\beta-3)^{1/3}}. \tag{17$_3$}$$

Using similar reasoning we may define the action of σ_2 on N by

$$\left((\omega^i\beta-3)^{1/3}\right)^{\sigma_2} = (\omega^{i+1}\beta-3)^{1/3}, \quad i=0,1,2. \tag{18}$$

Using the equations (17) it is easy to see that the automorphism $\sigma_1 \in Gal(N/k(j))$ has order 2, and from (18) it is clear that $\sigma_2 \in Gal(N/k(j))$ has order 3. If we set $\sigma_3 = \sigma_2\sigma_1\sigma_2^{-1}$ and $\sigma_4 = \sigma_2\sigma_3\sigma_2^{-1}$, then

$$\left((\beta-3)^{1/3}\right)^{\sigma_3} = (\omega-\omega^2)\frac{(\omega\beta-3)^{1/3}}{(\omega^2\beta-3)^{1/3}}, \ \left((\omega\beta-3)^{1/3}\right)^{\sigma_3} = (\omega^2-\omega)\frac{(\beta-3)^{1/3}}{(\omega^2\beta-3)^{1/3}},$$

and

$$\left((\omega^2\beta-3)^{1/3}\right)^{\sigma_3} = \frac{3}{(\omega^2\beta-3)^{1/3}};$$

while

$$\left((\beta-3)^{1/3}\right)^{\sigma_4} = (\omega^2-\omega)\frac{(\omega^2\beta-3)^{1/3}}{(\omega\beta-3)^{1/3}}, \ \left((\omega\beta-3)^{1/3}\right)^{\sigma_4} = \frac{3}{(\omega\beta-3)^{1/3}},$$

$$\left((\omega^2\beta-3)^{1/3}\right)^{\sigma_4}=(\omega-\omega^2)\frac{(\beta-3)^{1/3}}{(\omega\beta-3)^{1/3}}.$$

From these equations it is not hard to check that $\sigma_1\sigma_3=\sigma_4=\sigma_3\sigma_1$. Thus $<\sigma_1,\sigma_3,\sigma_4>$ is a Klein 4-group and $\mathsf{S}_1=<\sigma_1,\sigma_2>\cong A_4\cong\mathsf{S}$. It is clear that none of the nontrivial automorphisms in S_1 fixes β since the action of S_1 on $k(\beta)$ coincides with the action of G_{12} on this field. Thus S_1 has only the identity automorphism in common with $\mathsf{A}_1=<\phi,\gamma,\eta>$, which is the invariant group corresponding to $k(\beta)$ inside $Gal(N/k(j))$. Therefore, we know that

$$Gal(N/k(j))=\mathsf{A}_1\mathsf{S}_1. \tag{19}$$

To prove the isomorphism of Theorem 8 it suffices to show that under the isomorphisms taking $\mathsf{A}\to\mathsf{A}_1$ and $\mathsf{S}\to\mathsf{S}_1$ defined by

$$F\to\phi,\quad G\to\gamma,\quad H\to\eta,\quad A\to\sigma_1,\quad C\to\sigma_2$$

the action of S on A coincides with the action of S_1 on A_1. (See [ja, pp. 363-367].) We first check the equations

$$\sigma_2\phi\sigma_2^{-1}=\eta^2,\quad \sigma_2\gamma\sigma_2^{-1}=\phi^2,\quad \sigma_2\eta\sigma_2^{-1}=\gamma \tag{14$'$}$$

corresponding to (14). From (16_ϕ) and (18) we see that

$$\begin{aligned}\left((\omega^2\beta-3)^{1/3}\right)^{\sigma_2\phi\sigma_2^{-1}}&=\left((\beta-3)^{1/3}\right)^{\phi\sigma_2^{-1}}=\left(\omega(\beta-3)^{1/3}\right)^{\sigma_2^{-1}}\\&=\omega(\omega^2\beta-3)^{1/3}=\left((\omega^2\beta-3)^{1/3}\right)^{\eta^2}.\end{aligned}$$

Since ϕ does not move either of the quantities $(\omega^i\beta-3)^{1/3}$ for $i=1,2$, it follows that $\sigma_2\phi\sigma_2^{-1}$ fixes $(\omega^{i-1}\beta-3)^{1/3}$ for $i=1,2$, and so the last calculation implies that $\sigma_2\phi\sigma_2^{-1}=\eta^2$, which is the first identity in (14$'$). The other two identities follow in the same manner.

To finish the proof we check the identities

$$\sigma_1\phi\sigma_1^{-1}=\phi^2\gamma\eta,\quad \sigma_1\gamma\sigma_1^{-1}=\eta,\quad \sigma_1\eta\sigma_1^{-1}=\gamma \tag{15$'$}$$

corresponding to the identities in (15). We have the following calculations, using the fact that $\sigma_1^{-1} = \sigma_1$:

$$\left((\beta-3)^{1/3}\right)^{\sigma_1\phi\sigma_1^{-1}} = \left(\frac{3}{(\beta-3)^{1/3}}\right)^{\phi\sigma_1^{-1}} = \omega^2(\beta-3)^{1/3} = \left((\beta-3)^{1/3}\right)^{\phi^2};$$

$$\left((\omega\beta-3)^{1/3}\right)^{\sigma_1\phi\sigma_1^{-1}} = \left((\omega-\omega^2)\frac{(\omega^2\beta-3)^{1/3}}{(\beta-3)^{1/3}}\right)^{\phi\sigma_1^{-1}} = \left((\omega-\omega^2)\frac{(\omega^2\beta-3)^{1/3}}{\omega(\beta-3)^{1/3}}\right)^{\sigma_1^{-1}}$$

$$= (\omega-\omega^2)(\omega^2-\omega)\frac{(\omega\beta-3)^{1/3}/(\beta-3)^{1/3}}{3\omega/(\beta-3)^{1/3}} = \omega^2(\omega\beta-3)^{1/3} = \left((\omega\beta-3)^{1/3}\right)^{\gamma};$$

and similarly

$$\left((\omega^2\beta-3)^{1/3}\right)^{\sigma_1\phi\sigma_1^{-1}} = \left((\omega^2-\omega)\frac{(\omega\beta-3)^{1/3}}{(\beta-3)^{1/3}}\right)^{\phi\sigma_1^{-1}} = \left((\omega^2-\omega)\frac{(\omega\beta-3)^{1/3}}{\omega(\beta-3)^{1/3}}\right)^{\sigma_1^{-1}}$$

$$= (\omega^2-\omega)(\omega-\omega^2)\frac{(\omega^2\beta-3)^{1/3}/(\beta-3)^{1/3}}{3\omega/(\beta-3)^{1/3}} = \omega^2(\omega^2\beta-3)^{1/3} = \left((\omega^2\beta-3)^{1/3}\right)^{\eta}.$$

These calculations and the definitions in (16) imply that $\sigma_1\phi\sigma_1^{-1} = \phi^2\gamma\eta$, as required. The other two identities in (15′) follow in an entirely analogous manner, and this completes the proof of Theorem 8. □

Action of $Gal(N/k(j))$ on supersingular parameters.

Once again we take $k = \mathbb{F}_{p^2}$. If we let

$$R_p = \{r \in \mathbb{F}_{p^2} : \alpha = r^3 + 3 \text{ is supersingular for } E_3(\alpha)\},$$

then the group $Gal(N/k(j))$ acts on the set R_p in the following sense. Letting $t_i = (\omega^i\beta - 3)^{1/3}$ as before, a prime divisor $\mathfrak{p}$ of N lying over a prime divisor P_{j_0} of $k(j)$ for which j_0 is supersingular determines a triple (r_0, r_1, r_2) of elements in R_p for which

$$t_i = (\omega^i\beta - 3)^{1/3} \equiv r_i \pmod{\mathfrak{p}}, \tag{20}$$

and $r_i^3 + 3 = \omega^i\beta_0$, where $\beta \equiv \beta_0 \pmod{\mathfrak{p}}$. Then for any $\sigma \in Gal(N/k(j))$ we have

$t_i^\sigma \equiv r_i \pmod{\mathfrak{p}^\sigma}$.

By the formulas in (16)-(18) and by (19), for each σ there are constants $c_\sigma^{(i)} \in k$ and a product $p_\sigma^{(i)}(t_0, t_1, t_2)$ of positive or negative powers of the t_i for which

$$t_i^\sigma = c_\sigma^{(i)} p_\sigma^{(i)}(t_0, t_1, t_2), \quad i = 0, 1, 2. \tag{21}$$

Now put $t_i \equiv s_i \pmod{\mathfrak{p}^{\sigma^{-1}}}$ with $s_i \in k$. Allowing σ to act on this congruence gives

$$s_i \equiv t_i^\sigma \equiv c_\sigma^{(i)} p_\sigma^{(i)}(r_0, r_1, r_2) \pmod{\mathfrak{p}}, \quad i = 0, 1, 2,$$

so that

$$s_i = c_\sigma^{(i)} p_\sigma^{(i)}(r_0, r_1, r_2), \quad i = 0, 1, 2.$$

Thus for any $(r_0, r_1, r_2) \in R_p \times R_p \times R_p$ for which $r_i^3 + 3 = \omega^i \beta_0$, for $i = 0, 1, 2$, for some supersingular parameter β_0, we may define

$$\sigma(r_0, r_1, r_2) = (s_0, s_1, s_2).$$

By virtue of the congruence $t_i \equiv s_i \pmod{\mathfrak{p}^{\sigma^{-1}}}$ and $\mathfrak{p}^{\sigma^{-1}} | P_{j_0}$ we know that $s_i^3 + 3 = \omega^i \beta_1$ for some supersingular parameter β_1. Using this definition it is easy to see that

$$\sigma\tau(r_0, r_1, r_2) = \sigma(\tau(r_0, r_1, r_2)),$$

so this is definitely a (left) group action of $Gal(N/k(j))$ on the set

$$S_p = \{(r_0, r_1, r_2) \mid r_i^3 + 3 = \omega^i \beta_0, \beta_0 \in \mathbb{F}_{p^2}, E_3(\beta_0) \text{ supersingular}\}.$$

Since the element j and the prime divisor P_{j_0} are fixed by any element of the group $Gal(N/k(j))$, the value of $j_0 = \dfrac{\beta_0^3(\beta_0^3 + 216)^3}{(\beta_0^3 - 27)^3}$ is invariant under this action (see (3)). On the other hand, the value $j_1 = \dfrac{\beta_0^3(\beta_0^3 - 24)^3}{(\beta_0^3 - 27)}$ will generally change under the action, since $t = \dfrac{\beta^3(\beta^3 - 24)^3}{(\beta^3 - 27)}$ is not an element of $k(j)$. Therefore, triples of supersingular parameters in S_p can be mapped to triples corresponding to different values of $j(E_3(\beta))$. In general, a given value of j_0 will be mapped to four different values j_1 in this manner, since the rational function pair (j, t) parametrizes

the modular curve $\Phi_3(j,t)=0$, which has degree 4 in both j and t. (See [m2, Section 2] and [d, pp. 239-243].)

As examples, note that

$$\sigma_1(r_0,r_1,r_2)=\left(\frac{3}{r_0},(\omega-\omega^2)\frac{r_2}{r_0},(\omega^2-\omega)\frac{r_1}{r_0}\right),$$

$$\sigma_3(r_0,r_1,r_2)=\left((\omega-\omega^2)\frac{r_1}{r_2},(\omega^2-\omega)\frac{r_0}{r_2},\frac{3}{r_2}\right),$$

$$\sigma_4(r_0,r_1,r_2)=\left((\omega^2-\omega)\frac{r_2}{r_1},\frac{3}{r_1},(\omega-\omega^2)\frac{r_0}{r_1}\right).$$

From these formulas we conclude the following.

Theorem 9. If $r_i\in R_p$, for $i=0,1,2$, are such that $r_i^3+3=\omega^i\beta_0$ for a supersingular parameter β_0 for $E_3(\beta)$, then for $i\neq j$ and some sign $\delta_{ij}=\pm1$ depending on i and j,

$$s_{i,j}=\delta_{ij}(\omega-\omega^2)\frac{r_i}{r_j}\in R_p.$$

In other words, $s_{i,j}^3+3$ is also a supersingular parameter for $E_3(\beta)$. $\square$

Also note the following regarding the monomials $p_\sigma^{(i)}(t_0,t_1,t_2)$ in (21). Write

$$p_\sigma^{(i)}(t_0,t_1,t_2)=\prod_j t_j^{\varepsilon_{i,j}},\quad i=0,1,2.$$

In this way, the automorphism σ determines a 3×3 matrix $M_\sigma=(\varepsilon_{i,j})$. If $M_\tau=(\rho_{i,j})$, then

$$t_i^{\sigma\tau}=c_\sigma^{(i)}p_\sigma^{(i)}(t_0,t_1,t_2)^\tau=c_\sigma^{(i)}\prod_j t_j^{\varepsilon_{i,j}\tau}=c_\sigma^{(i)}\prod_j\left(c_\tau^{(j)}\right)^{\varepsilon_{i,j}}\prod_j\left(\prod_k t_k^{\rho_{j,k}}\right)^{\varepsilon_{i,j}},$$

or

$$t_i^{\sigma\tau}=c_{\sigma\tau}^{(i)}\prod_k t_k^{\pi_{i,k}},$$

where

$$\pi_{i,k}=\sum_j\varepsilon_{i,j}\rho_{j,k},\tag{22}$$

and

$$c_{\sigma\tau}^{(i)} = c_{\sigma}^{(i)} \prod_j \left(c_{\tau}^{(j)}\right)^{\varepsilon_{i,j}}. \tag{23}$$

It follows from (22) that $M_{\sigma\tau} = M_\sigma M_\tau$ and $\sigma \to M_\sigma$ is a complex representation of $Gal(N/k(j))$. By the equations in (16), $M_\phi = M_\gamma = M_\eta = I$, so this representation arises from a 3-dimensional representation of the subgroup $\mathsf{S}_1 \cong A_4$.

We have from (17) and (18) that

$$M_{\sigma_1} = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}, \; M_{\sigma_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

The corresponding character $\chi(\sigma) = tr(M_\sigma)$ satisfies $\chi(1) = 3, \chi(\sigma_1) = -1, \chi(\sigma_2) = \chi(\sigma_2^2) = 0$, so this representation corresponds to an irreducible representation of A_4.

5 N as a field of modular functions.

We will now use the results of Fleckinger [fle] to prove the following theorem. This will explain the occurrence of the modulary group in Theorem 8.

Theorem 10. Let $k = \mathbb{C}$ and $j = j(\tau)$ be the modular j-function.

a) The field $k(\beta) = k(\xi_1, \xi_2, \xi_3, \xi_4)$ is isomorphic to the field $\mathsf{K}_{\Gamma(3)}$ of modular functions for the modular group $\Gamma(3)$. Thus, β maps to a *Hauptmodul* for this group.

b) The field $N = k(\alpha, \beta, (\beta-3)^{1/3}, (\omega\beta-3)^{1/3}, (\omega^2\beta-3)^{1/3})$ is isomorphic to the field $\mathsf{K}_{\Gamma(9)}$ of modular functions for the modular group $\Gamma(9)$.

Proof. Following Fleckinger [fle] we set

$$A_{(u,v)}(\tau) = \frac{288\wp^2(u\tau + v; \tau, 1)}{12\wp^2(u\tau + v; \tau, 1) - g_2(\tau, 1)}, \tag{24}$$

where $\wp(z; \tau, 1)$ is the Weierstrass $\wp$-function for the lattice $L_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$; $g_2(\tau, 1)$ is the standard coefficient in the Weierstrass equation for $\wp(z)$ and $\wp'(z)$ [kk, p. 40]; and

$$(u, v) \in \{(0, 1/3), (1/3, 0), (1/3, 1/3), (1/3, -1/3)\}.$$

For the rest of the proof we drop the explicit reference to the lattice in the notation

for $\wp(z)$. Then $(\wp(u\tau+v), \wp'(u\tau+v))$ is a non-trivial 3-division point on the elliptic curve

$$E: \quad Y^2 = 4X^3 - g_2X - g_3.$$

Setting $\lambda = \wp'(u\tau+v)^{-1/3}$, Fleckinger shows that the functions

$$x(z;\tau) = \lambda^2(\wp(z) - \wp(u\tau+v)), \quad x_1(z;\tau) = \lambda^3\wp'(z)$$

satisfy the equation

$$E': \quad x_1^2 = 4x^3 + \alpha^2x^2 + 2\alpha x + 1,$$

where $\alpha = \frac{\lambda^4}{2}(12\wp^2(u\tau+v) - g_2(\tau))$. Therefore, the curve $E_3(\alpha)$, which is isomorphic to E' by the substitution $x_1 = 2y + \alpha x + 1$, is isomorphic to the curve E, and it follows that

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

As a corollary of these calculations [fle, Prop. 1.1], Fleckinger deduces that

$$\alpha^3 = A_{(u,v)}(\tau).$$

Thus, the four functions $A_{(u,v)}(\tau)$ are solutions of the equation $F(x) = 0$ considered in Section 1. Fleckinger proves further that these functions are modular functions for $\Gamma(3)$ and that the function $(A_{(u,v)}(\tau) - 27)^2$ is a quotient of values of the Δ-function [kk, p. 53], [si, pp. 59-62]:

$$(A_{(0,1/3)}(\tau) - 27)^2 = 3^{12}\frac{\Delta(3\tau)}{\Delta(\tau)}, \quad (u,v) = (0,1/3); \tag{25a}$$

$$(A_{(u,v)}(\tau) - 27)^2 = \frac{\Delta(u\tau+v)}{\Delta(\tau)}, \quad (u,v) \neq (0,1/3). \tag{25b}$$

Since the four functions $3^{12}\Delta(3\tau)$, $\Delta(u\tau+v)$ are certainly distinct – they have different q-expansions, for example [kk, p. 82] – it follows that the functions $A_{(u,v)}(\tau)$ are distinct, and therefore represent all the roots of $F(x) = 0$ in the field $\mathsf{K}_{\Gamma(3)}$. Since any two splitting fields of $F(x)$ over $k(j) = k(j(\tau))$ are isomorphic, we have that

$$k(\beta) \cong k\left(A_{(0,1/3)}(\tau), A_{(1/3,0)}(\tau), A_{(1/3,1/3)}(\tau), A_{(1/3,-1/3)}(\tau)\right),$$

and by identifying $k(\beta)$ with its image we may assume that $k(\beta) \subseteq \mathsf{K}_{\Gamma(3)}$. However, by classical results [sch, pp. 76, 129] we have

$$[\mathsf{K}_{\Gamma(3)} : k(j(\tau))] = [\Gamma :< \pm I > \Gamma(3)] = 12.$$

This implies that $k(\beta) = \mathsf{K}_{\Gamma(3)}$ and proves part a).

Fleckinger's results also allow us to prove part b). He defines the following functions in terms of the Dedekind function $\eta(\tau)$:

$$l_{(0,1/3)}(\tau) = \frac{108}{(2\pi i)^4} \frac{g_2(\tau)\eta^4(3\tau)}{\eta^{12}(\tau)(A_{(0,1/3)}(\tau) - 24)},$$

and

$$l_{(u,v)}(\tau) = \frac{12}{(2\pi i)^4} \frac{g_2(\tau)\eta^4(u\tau + v)}{\eta^{12}(\tau)(A_{(u,v)}(\tau) - 24)}, \quad (u,v) \neq (0,1/3).$$

Fleckinger then proves that $l^3_{(u,v)}(\tau) = A_{(u,v)}(\tau)$ and that $l_{(u,v)}(\tau) \in \mathsf{K}_{\Gamma(9)}$. Since the cube roots of the functions $A_{(u,v)}(\tau)$ generate the splitting field of $F(x^3)$ over the field $k(\beta) = \mathsf{K}_{\Gamma(3)}$, we may assume as in the proof of part a) that $N \subseteq \mathsf{K}_{\Gamma(9)}$. However, we also have

$$[\mathsf{K}_{\Gamma(9)} : k(j(\tau))] = [\Gamma :< \pm I > \Gamma(9)] = |\bar{\Gamma}_9| = 324$$

by [sch, p. 76]. Since $[N : k(j(\tau))] = 324$ this shows that $N = \mathsf{K}_{\Gamma(9)}$ and completes the proof. □

We now give simpler expressions for Fleckinger's functions $l_{(u,v)}(\tau)$.

Theorem 11. If $\eta(\tau)$ is Dedekind's η-function, then we have the following formulas:

$$l_{(u,v)}(\tau) = 3 + \left(\frac{\eta(\frac{u\tau+v}{3})}{\eta(\tau)}\right)^3, \quad (u,v) \neq (0,1/3); \tag{26}$$

$$l_{(0,1/3)}(\tau) = 3 + 27\left(\frac{\eta(9\tau)}{\eta(\tau)}\right)^3. \tag{27}$$

Proof. We first prove the formula

$$l_{(1/3,0)}(\tau) = 3 + \left(\frac{\eta(\frac{\tau}{9})}{\eta(\tau)}\right)^3 = f(\tau). \tag{28}$$

Equations (18), (22), and (24) in Weber's treatise [w, pp. 255-256] state in our notation that $t = f^3(\tau)$ satisfies

$$j(\tau)(t-27) = t(t-24)^3,$$

i.e., that $f^3(\tau)$ is a root of $F(x) = 0$. By the results of [s, p.51], $f(\tau)$ is a modular function for the group $\Gamma_0(9)$. Therefore $f(\tau) \in \mathsf{K}_{\Gamma(9)}$. But as one of the four roots of $F(x)$ in the field $\mathsf{K}_{\Gamma(9)}$, the function $f^3(\tau)$ must coincide with one of the functions $A_{(u,v)}(\tau)$. From (24) and the q-expansion of the Weierstrass $\wp$-function [si,p. 50] we have the beginning q-expansions at $\tau = \infty i$, with $q = e^{2\pi i\tau}$:

$$\begin{aligned} A_{(0,1/3)}(\tau) &= 27 + 729q + O(q^2), \\ A_{(1/3,0)}(\tau) &= q^{-1/3} + 15 + 54q^{1/3} + O(q^{2/3}), \\ A_{(1/3,1/3)}(\tau) &= A_{(1/3,0)}(\tau+1) = \omega^2 q^{-1/3} + 15 + O(q^{1/3}), \\ A_{(1/3,-1/3)}(\tau) &= A_{(1/3,0)}(\tau-1) = \omega q^{-1/3} + 15 + O(q^{1/3}). \end{aligned} \tag{29}$$

(The second expansion corrects an error in [fle, p. 27, (2.8)].) On the other hand, from the infinite product expansion

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n),$$

we have that

$$f(\tau)^3 = (q^{-1/9} + 5q^{2/9} - 7q^{5/9} + O(q^{8/9}))^3 = q^{-1/3} + 15 + 54q^{1/3} + O(q^{2/3}).$$

This proves that $f^3(\tau) = A_{(1/3,0)}(\tau) = l^3_{(1/3,0)}(\tau)$. Hence, $f(\tau) = \omega^i l_{(1/3,0)}(\tau)$, and since the leading term of the q-expansion of $l_{(1/3,0)}(\tau)$ is $q^{-1/9}$, it follows that $f(\tau) = l_{(1/3,0)}(\tau)$, as claimed. Now the relations

$$l_{(1/3,1/3)}(\tau) = l_{(1/3,0)}(\tau+1), \quad l_{(1/3,-1/3)}(\tau) = l_{(1/3,0)}(\tau-1)$$

and (28) imply (26). Finally, the identities

$$A_{(0,1/3)}(\tau) = A_{(1/3,0)}(-1/\tau)$$

from [fle, p.25, (2.3)] and

$$\eta\left(\frac{-1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\,\eta(\tau) \tag{30}$$

(see [kk, p. 190]) give that

$$\begin{aligned} A_{(0,1/3)}(\tau) &= \left(3 + \left(\frac{\eta\left(\frac{-1}{9\tau}\right)}{\eta\left(\frac{-1}{\tau}\right)}\right)^3\right)^3 \\ &= \left(3 + \left(\frac{\sqrt{9\tau/i}\,\eta(9\tau)}{\sqrt{\tau/i}\,\eta(\tau)}\right)^3\right)^3 \\ &= \left(3 + 27\left(\frac{\eta(9\tau)}{\eta(\tau)}\right)^3\right)^3. \end{aligned}$$

Since the the q-expansion for $l_{(0,1/3)}(\tau)$ is $3 + O(q)$, equation (27) follows. □

Corollary. We have the equivalent identities

$$\left(\left(\frac{\eta\left(\frac{\tau}{9}\right)}{\eta(\tau)}\right)^9 + 9\left(\frac{\eta\left(\frac{\tau}{9}\right)}{\eta(\tau)}\right)^6 + 27\left(\frac{\eta\left(\frac{\tau}{9}\right)}{\eta(\tau)}\right)^3\right)^2 = \frac{\Delta\left(\frac{\tau}{3}\right)}{\Delta(\tau)},$$

$$\eta^3(\tau)\eta^3\left(\frac{\tau}{9}\right)\left(\eta^6\left(\frac{\tau}{9}\right) + 9\eta^3\left(\frac{\tau}{9}\right)\eta^3(\tau) + 27\eta^6(\tau)\right) = \eta^{12}\left(\frac{\tau}{3}\right).$$

In other words, $\eta^{12}\left(\frac{\tau}{3}\right)$ is equal to the quartic form in X and Y given by

$$Q(X,Y) = XY(X^2 + 9XY + 27Y^2)$$

evaluated at $X = \eta^3\left(\frac{\tau}{9}\right)$ and $Y = \eta^3(\tau)$.

Proof. The first identity is immediate from (28) and (25b) with $(u, v) = (1/3, 0)$. The second follows from the first by taking square roots and comparing leading terms in the q-expansions of both sides, using the fact that $\Delta(\tau) = (2\pi)^{12}\eta^{24}(\tau)$. □

Remark. It can be shown that the second identity in this corollary is equivalent to an identity given by Zagier [z, p.8, Case **B**]. I am grateful to Shaun Cooper (private communication) for making me aware of this fact. See the recent preprint

by Chan and Cooper [cc], Theorem 3.1 and Table 1 (level $\ell = 9$). This identity is also equivalent to an identity involving cubic theta functions. See the discussion of equation (40) in Section 7 below.

We will now use the above insights to investigate a specific isomorphism $N \cong \mathsf{K}_{\Gamma(9)}$ in detail. In particular, we seek to determine the images of α and β under such an isomorphism. We will construct this isomorphism in several stages.

It follows from the fact that $[k(\beta) : k(\alpha^3)] = 3$ that there is an isomorphism $k(\beta) \to \mathsf{K}_{\Gamma(3)}$ taking

$$\xi_1 = \alpha^3 \to A_{(0,1/3)}(\tau), \quad \xi_2 \to A_{(1/3,0)}(\tau).$$

To determine how this isomorphism acts on ξ_3 and ξ_4 we note the following. The equation

$$\xi_2 - 27 = \frac{(\beta+6)^3}{\beta^2+3\beta+9} - 27 = \frac{(\beta-3)^3}{\beta^2+3\beta+9}$$

implies easily that

$$\lambda = (\xi_2 - 27)(\xi_3 - 27)(\xi_4 - 27) = \beta^3 - 27.$$

Since the images of the elements ξ_3 and ξ_4 lie in $\{A_{(1/3,1/3)}(\tau), A_{(1/3,-1/3)}(\tau)\}$, it follows from (25) applied to the last equation that

$$\begin{aligned}\beta^3 - 27 = \frac{27\beta^3}{\alpha^3} &\to \pm\frac{\left(\Delta\left(\frac{\tau}{3}\right)\Delta\left(\frac{\tau+1}{3}\right)\Delta\left(\frac{\tau-1}{3}\right)\right)^{1/2}}{\Delta(\tau)^{3/2}} \\ &= \pm\frac{\eta^{12}\left(\frac{\tau}{3}\right)\eta^{12}\left(\frac{\tau+1}{3}\right)\eta^{12}\left(\frac{\tau-1}{3}\right)}{\eta^{36}(\tau)}. \end{aligned} \tag{31}$$

On the other hand, the infinite product for $\eta(\tau)$ gives that

$$a(\tau) = \frac{\eta^4\left(\frac{\tau}{3}\right)\eta^4\left(\frac{\tau+1}{3}\right)\eta^4\left(\frac{\tau-1}{3}\right)}{\eta^{12}(\tau)} = q^{-1/3}\prod_{n\geq 1, n\not\equiv 0 (mod 3)}(1-q^n)^4 = \frac{\eta^4(\tau)}{\eta^4(3\tau)}. \tag{32}$$

Thus, β maps to a function $b(\tau)$ with leading term $cq^{-1/3}$, where $c^6 = 1$. Now we use the fact that

$$\xi_2 + \omega^2\xi_3 + \omega\xi_4 = \frac{3\beta(\beta^3 - 108)}{\beta^3 - 27},$$

so that

$$\beta = (\xi_2 + \omega^2\xi_3 + \omega\xi_4)\frac{\beta^3 - 27}{3(\beta^3 - 108)}.$$

Consequently, the leading term in the q-expansion of $b(\tau)$ is $1/3$ times the leading coefficient in the expansion of the quantity $\xi_2 + \omega^2\xi_3 + \omega\xi_4$. By (29), we have that

$$A_{(1/3,0)}(\tau) + \omega^2 A_{(1/3,1/3)}(\tau) + \omega A_{(1/3,-1/3)}(\tau) = O(q^{1/3}),$$

while

$$A_{(1/3,0)}(\tau) + \omega A_{(1/3,1/3)}(\tau) + \omega^2 A_{(1/3,-1/3)}(\tau) = 3q^{-1/3} + O(q^{1/3}).$$

Hence, we must have $\xi_3 \to A_{(1/3,-1/3)}(\tau)$ and $\xi_4 \to A_{(1/3,1/3)}(\tau)$, and the leading term of $b(\tau)$ is $q^{-1/3}$.

Now the fact that $[k(\alpha, \beta) : k(\beta)] = 3$ implies that the above isomorphism can be extended to an isomorphism taking $\alpha \to l_{(0,1/3)}(\tau)$. Equations (31) and (32) imply that

$$\frac{3\beta}{\alpha} \to \zeta_6 \frac{\eta^4\left(\frac{\tau}{3}\right)\eta^4\left(\frac{\tau+1}{3}\right)\eta^4\left(\frac{\tau-1}{3}\right)}{\eta^{12}(\tau)} = \zeta_6\, a(\tau),$$

for some 6-th root of unity ζ_6, and then (32) shows that $\zeta_6 = 1$, since the leading term of $l_{(0,1/3)}(\tau)$ is 3. In other words

$$\beta \to b(\tau) = \frac{1}{3}a(\tau)l_{(0,1/3)}(\tau) = \frac{\eta^4(\tau)}{\eta^4(3\tau)}\left(1 + 9\frac{\eta^3(9\tau)}{\eta^3(\tau)}\right).$$

This shows that $b(\tau) \in \mathsf{K}_{\Gamma(3)}$, consequently $a(\tau) \in \mathsf{K}_{\Gamma(9)}$, and

$$b(\tau) = q^{-1/3}(1 + qs(q)), \tag{33}$$

where $s(q)$ is a power series in q with integer coefficients.

I claim now that

$$b(\tau) = 3 + \left(\frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}\right)^3 = 3 + g(\tau)^3. \tag{34}$$

First note that the q-expansion of $3 + g(\tau)^3$ at infinity begins with $q^{-1/3}$:

$$3 + g(\tau)^3 = q^{-1/3}(1 + 5q - 7q^2 + 3q^3 + \cdots). \tag{35}$$

From (31) and (32) we have the identity

$$27 + a(\tau)^3 = b(\tau)^3. \tag{36}$$

On the other hand, putting 3τ for τ in the above corollary gives

$$(3 + g(\tau)^3)^3 - 27 = \left(\frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}\right)^9 + 9\left(\frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}\right)^6 + 27\left(\frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}\right)^3 = \sqrt{\frac{\Delta(\tau)}{\Delta(3\tau)}},$$

where the leading term in the q-expansion of the square-root is q^{-1}. From (32) it is clear that the right-hand side of this equation is just $a(\tau)^3$. Hence, we have

$$b(\tau)^3 = 27 + a(\tau)^3 = (3 + g(\tau)^3)^3,$$

and using (33) and (35) gives $b(\tau) = 3 + g(\tau)^3$, as claimed in (34).

As a corollary of this argument we note the following identity, which follows from equating the two expressions we have derived for the function $b(\tau)$.

Theorem 12. For τ in the upper half-plane $\mathbb{H}$ we have

$$3 + \frac{\eta^3\left(\frac{\tau}{3}\right)}{\eta^3(3\tau)} = \frac{\eta^4(\tau)}{\eta^4(3\tau)}\left(1 + 9\frac{\eta^3(9\tau)}{\eta^3(\tau)}\right),$$

or equivalently,

$$\eta^3\left(\frac{\tau}{3}\right)\eta(3\tau) + 3\eta^4(3\tau) = \eta^4(\tau) + 9\eta^3(9\tau)\eta(\tau).$$

□

So far we have an isomorphism taking

$$\alpha \to l_{(0,1/3)}(\tau) = \frac{3b(\tau)}{a(\tau)}, \quad \beta \to b(\tau) = 3 + g(\tau)^3,$$

$$\xi_2 \to A_{(1/3,0)}(\tau) = l_{(1/3,0)}(\tau)^3, \quad \xi_3 \to A_{(1/3,-1/3)}(\tau) = l_{(1/3,-1/3)}(\tau)^3,$$

$$\xi_4 \to A_{(1/3,1/3)}(\tau) = l_{(1/3,1/3)}(\tau)^3.$$

Since $[N : k(\alpha, \beta)] = 9$ and $\xi_2^{1/3}$ and $\xi_3^{1/3}$ generate independent extensions of $k(\alpha, \beta)$, the isomorphism $N \to \mathsf{K}_{\Gamma(9)}$ may now be chosen so that it extends the above isomorphism and so that

$$\xi_2^{1/3} \to l_{(1/3,0)}(\tau), \quad \xi_3^{1/3} \to l_{(1/3,-1/3)}(\tau).$$

Then $\xi_4^{1/3} \to \omega^r l_{(1/3,1/3)}(\tau)$, for some r. Furthermore, from (33) we have

$$g(\tau+1)^3 = b(\tau+1) - 3 = \omega^2 b(\tau) - 3, \quad g(\tau-1)^3 = \omega b(\tau) - 3. \tag{37}$$

But $(\omega^i \beta - 3)^{1/3} \in N$ maps to a cube root of unity times $(\omega^i b(\tau) - 3)^{1/3} \in \mathsf{K}_{\Gamma(9)}$, hence

$$g(\tau) = \frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}, g(\tau+1), g(\tau-1) \in \mathsf{K}_{\Gamma(9)},$$

and

$$\mathsf{K}_{\Gamma(9)} = k(g(\tau), g(\tau+1), g(\tau-1)).$$

On the other hand, the function $z(\tau) = 3\dfrac{\eta(9\tau)}{\eta(\tau)} = (l_{(0,1/3)}(\tau) - 3)^{1/3}$ lies in $\mathsf{K}_{\Gamma(27)}$, which follows from the general transformation formula for $\eta(\tau)$. (See [ra, p. 163] or [fle, p. 28], but beware of two misprints in the first formula for $\varepsilon(a, b, c, d)$ in [fle].) In particular, (30) easily implies that $z(-1/\tau) = g(\tau/3) = (l_{(1/3,0)}(\tau) - 3)^{1/3}$. Note that $z(\tau)$ does not lie in $\mathsf{K}_{\Gamma(9)}$, since for example,

$$z\left(\frac{\tau}{9\tau+1}\right) = \omega z(\tau).$$

This corresponds to the fact that $(\alpha - 3)^{1/3}$ does not lie in the field N of Section 1.

These observations imply the following theorem.

Theorem 13. The functions

$$\alpha = l_{(0,1/3)}(\tau) = 3 + 27\left(\frac{\eta(9\tau)}{\eta(\tau)}\right)^3, \quad \beta = b(\tau) = 3 + \left(\frac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}\right)^3$$

give a solution (α, β) in $\mathsf{K}_{\Gamma(9)}$ of the Fermat equation

$$Fer_3: \quad 27\alpha^3 + 27\beta^3 = \alpha^3\beta^3.$$

Furthermore, $z = 3\dfrac{\eta(9\tau)}{\eta(\tau)},\ w = \dfrac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}$ is a parametrization of the curve

$$C_{19}: \quad z^3w^3(z^6 + 9z^3 + 27)(w^6 + 9w^3 + 27) = 729$$

in terms of modular functions for $\Gamma(27)$. $\square$

The first assertion follows from the computations of Section 1 and the isomorphism $N \cong \mathsf{K}_{\Gamma(9)}$. The second assertion follows as in the proof of Theorem 5, or can be deduced directly from the Corollary to Theorem 11. The q-expansions at infinity of the modular functions occurring in Theorem 13, as well as those occurring in (36), have rational integral coefficients.

By virtue of (37), the generators $g(\tau), g(\tau+1), g(\tau-1)$ of $\mathsf{K}_{\Gamma(9)}$ satisfy the relationships

$$g(\tau-1)^3 = \omega g(\tau)^3 + 3\omega - 3, \quad g(\tau+1)^3 = \omega^2 g(\tau)^3 + 3\omega^2 - 3.$$

From this and the identity

$$((y+z)^3 - y^3 - z^3)^3 = 27y^3z^3(y+z)^3$$

it follows that the function $X = g(\tau)$ and the primitive element $Y = g(\tau+1)+g(\tau-1)$ for the extension $\mathsf{K}_{\Gamma(9)}/k(g(\tau))$ satisfy

$$\begin{aligned} 0 &= (Y^3 - \omega^2X^3 - 3\omega^2 + 3 - \omega X^3 - 3\omega + 3)^3 - 27(\omega^2X^3 + 3\omega^2 - 3)(\omega X^3 + 3\omega - 3)Y^3 \\ &= (Y^3 + X^3 + 9)^3 - 27(X^6 + 9X^3 + 27)Y^3. \end{aligned}$$

Hence, we have:

Theorem 14. The modular function field $\mathsf{K}_{\Gamma(9)}$ is isomorphic to the function field for the curve

$$f(X,Y) = Y^9 + 3(X^3+9)Y^6 - 3(8X^6 + 63X^3 + 162)Y^3 + (X^3+9)^3 = 0.$$

□

An explicit covering map $(X,Y) \to (\alpha,\beta)$ from $f(X,Y)=0$ to Fer_3 is given by

$$\alpha = \frac{3(3+X^3)(9-2Y^3+X^3)^2}{(Y^6+7X^6-Y^3X^3+45X^3-9Y^3+81)XY^2}, \quad \beta = 3+X^3.$$

Remark. From Theorem 3 and the computation of the genus of N in Section 4 it follows that the curve $f(X,Y)=0$ in Theorem 14 has good reduction at any prime $p \neq 2,3$.

6 Application to an identity of Berndt and Hart.

In this section we consider an application of the formulas of the last section. This concerns the following identity first proved in [bh] by Berndt and Hart (see also the alternate proof in [köh] and a generalization in [cht]):

$$27\eta^3(3w)\eta^3(3z) = \eta^3\left(\tfrac{w}{3}\right)\eta^3\left(\tfrac{z}{3}\right) + i\eta^3\left(\tfrac{w+1}{3}\right)\eta^3\left(\tfrac{z+1}{3}\right) - \eta^3\left(\tfrac{w+2}{3}\right)\eta^3\left(\tfrac{z+2}{3}\right), \qquad (38)$$

for $w,z \in \mathbb{H}$. We will show how this identity follows easily from the identities (34) and (37) for the function $g(\tau) = \dfrac{\eta\left(\frac{\tau}{3}\right)}{\eta(3\tau)}$, where (37) is a consequence of (33). First apply (34) and (37) to the expression

$$\begin{aligned} &g^3(w)g^3(z) + g^3(w+1)g^3(z+1) + g^3(w+2)g^3(z+2) \\ &= (b(w)-3)(b(z)-3) + (\omega^2 b(w)-3)(\omega^2 b(z)-3) + (\omega b(w)-3)(\omega b(z)-3) \\ &= (1+\omega+\omega^2)b(w)b(z) - 3(1+\omega^2+\omega)(b(w)+b(z)) + 27, \end{aligned}$$

so that

$$g^3(w)g^3(z) + g^3(w+1)g^3(z+1) + g^3(w+2)g^3(z+2) = 27. \qquad (39)$$

Now note that

$$g(w+1) = \frac{\eta\left(\frac{w+1}{3}\right)}{\eta(3w+3)} = \frac{\eta\left(\frac{w+1}{3}\right)}{\zeta_8 \eta(3w)},$$

where $\zeta_8 = e^{2\pi i/8}$, so that

$$g^3(w+1)g^3(z+1) = \frac{1}{\zeta_8^6}\frac{\eta^3\left(\frac{w+1}{3}\right)}{\eta^3(3w)}\frac{\eta^3\left(\frac{z+1}{3}\right)}{\eta^3(3z)} = i\frac{\eta^3\left(\frac{w+1}{3}\right)}{\eta^3(3w)}\frac{\eta^3\left(\frac{z+1}{3}\right)}{\eta^3(3z)}$$

and

$$g^3(w+2)g^3(z+2) = \frac{1}{\zeta_8^{12}}\frac{\eta^3\left(\frac{w+2}{3}\right)}{\eta^3(3w)}\frac{\eta^3\left(\frac{z+2}{3}\right)}{\eta^3(3z)} = -\frac{\eta^3\left(\frac{w+2}{3}\right)}{\eta^3(3w)}\frac{\eta^3\left(\frac{z+2}{3}\right)}{\eta^3(3z)}.$$

Plugging these expressions into (39) and clearing denominators yields (38). This proof shows that the Berndt-Hart identity (38) is a direct result of the q-expansion (33) for $b(\tau) = 3 + g(\tau)^3$, which is, in turn, a consequence of the identity in Theorem 12.

7 Connection with cubic theta functions.

The identities in the Corollary to Theorem 11 and in Theorems 12 and 13 are related to the cubic theta functions $a(q), b(q), c(q)$ introduced by the Borweins in [bb, p. 695] and developed further in [bbg]. Also see the paper [cp1] and the references given in [cp2].

Note: In this section we reserve the notation $a(q)$ and $b(q)$ for the functions defined below. They should not be confused with the functions $a(\tau)$ and $b(\tau)$ considered in Sections 5 and 6.

For example, with $q = e^{2\pi i\tau}$, set

$$b(q) = \frac{\eta^3(\tau)}{\eta(3\tau)}, \quad c(q) = 3\frac{\eta(3\tau)^3}{\eta(\tau)},$$

and

$$a(q) = b(q) + 3c(q^3) = \frac{\eta^3(\tau)}{\eta(3\tau)} + 9\frac{\eta(9\tau)^3}{\eta(3\tau)} = \sum_{n,m=-\infty}^{\infty} q^{m^2+mn+n^2}.$$

These relations are from Prop. 2.2 and Lemma 2.1 in [bbg]. With these definitions, it is straightforward to verify that the identity

$$a(q)^3 = b(q)^3 + c(q)^3 \tag{40}$$

discovered by the Borweins is equivalent to the identities in the Corollary to Theorem 11, with τ replaced by 9τ. Furthermore, the solution (α, β) of Fer_3 in Theorem 13 can be expressed in terms of the cubic theta functions as

$$\alpha = 3\frac{a(q)}{b(q)}, \quad \beta = 3\frac{a(q)}{c(q)}.$$

The equation for α follows from the definition of the functions $a(q)$ and $b(q)$, while the equation for β follows from

$$\beta^3 = \frac{27\alpha^3}{\alpha^3 - 27} = \frac{27a(q)^3}{a(q)^3 - b(q)^3} = \frac{27a(q)^3}{c(q)^3}.$$

Alternatively, the relation $\beta = 3a(q)/c(q)$ is equivalent to the identity in Theorem 12. In addition, note that our equation (36) is equivalent to Corollary 2.5 in [bbg].

I am grateful to Shaun Cooper for several enlightening e-mail messages in which he clarified for me the connection between the η-identities of Section 5, Zagier's paper [z], and cubic theta functions, and for bringing the papers [bbg] and [z] to my attention.

References.

[bb] J. M. Borwein and P. B. Borwein, A cubic counterpart of Jacobi's identity and the AGM, Trans. Amer. Math. Soc. 323 (1991), 691-701.

[bbg] J. M. Borwein, P. B. Borwein, and F. G. Garvan, Some cubic modular identities of Ramanujan, Trans. Amer. Math. Soc. 343 (1994), 35-47.

[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.

[bh] B.C. Berndt, W.B. Hart, An identity for the Dedekind eta-function involving two independent complex variables, Bull. London Math. Soc. 39 (2007), 345-347.

[cc] H. H. Chan and S. Cooper, Rational analogues of Ramanujan's series for $1/\pi$, preprint, 2011.

[cht] R. Chapman, W. B. Hart, and P. C. Toh, A new class of theta function identities in two variables, J. of Combinatorics and Number Theory 2 (2012), 201-208.

[cp1] S. Cooper, Cubic theta functions, J. Computational and Applied Math. 160 (2003), 77-94.

[cp2] S. Cooper, A simple proof of an expansion of an eta-quotient as a Lambert series, Bull. Australian Math. Soc. 71 (2005), 353-358.

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

[fle] V. Fleckinger, Monogénéité de l'anneau des entiers de certains corps de classes de rayon, Ann. Inst. Fourier, Grenoble 38, 1 (1988), 17-57.

[gr] B. H. Gross, Heegner points on $X_0(N)$, in: *Modular Forms*, R. A. Rankin, ed., Ellis Horwood Limited, Chichester, 1984, pp. 87-105.

[h] H. Hasse, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrad p über elliptischen Funktionenkörpern der Charakteristik p, J. reine angew. Math. 172 (1934), 77-85, Paper 43 in: Hasse's *Mathematische Abhandlungen*, vol. 2, Walter de Gruyter, Berlin, 1975, pp. 161-169.

[ja] N. Jacobson, *Basic Algebra II*, Dover Publications, Inc., Mineola, New York, 2009.

[kf] F. Klein, R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, 1. Band, reprint of 1890 edition of B. G. Teubner (Leipzig), Cornell University Library, 1992.

[kk] M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, 2. Auflage, Springer Verlag, Berlin, Heidelberg, 2007.

[köh] G. Köhler, Note on an identity presented by B. C. Berndt and W. B. Hart, Bull. London Math. Soc. 40 (2008), 172-173.

[lw] P.S. Landweber, Supersingular curves and congruences for Legendre polynomials, in: P.S. Landweber (ed.), Elliptic Curves and Modular Forms in Topology, in: Lecture Notes in Math., vol. 1326, Springer, Berlin, 1988, 69-93.

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

[m2] P. Morton, The cubic Fermat equation and complex multiplication on the Deuring normal form, The Ramanujan Journal of Math. 25 (2011), 247-275.

[m3] P. Morton, Solutions of the cubic Fermat equation in Hilbert class fields of imaginary quadratic fields, in preparation.

[od] R.W.K. Odoni, Realising wreath products of cyclic groups as Galois groups, Mathematika 35 (1988), 101-113.

[ra] H. Rademacher, *Topics in Analytic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 169, Springer-Verlag, Berlin-Heidelberg, 1973.

[s] R. Schertz, *Complex Multiplication*, New Mathematical Monographs, vol. 15, Cambridge University Press, 2010.

[sch] B. Schoeneberg, *Elliptic Modular Functions*, Grundlehren der mathematischen Wissenschaften vol. 203, Springer, Berlin, 1974.

[si] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Graduate Texts in Math. vol. 151, Springer-Verlag, New York, 1994.

[sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Berlin, 1993.

[vdw] B.L. van der Waerden, *Algebra I*, Frederick Ungar Publishing Co., New York, 1970.

[w] H. Weber, *Lehrbuch der Algebra*, vol. III, Chelsea Publishing Co., New York, reprint of 1908 edition.

[z] D. Zagier, Integral solutions of Apéry-like recurrence equations, in *Groups and Symmetries*, 349-366, CRM Proc. Lecture Notes 47, Amer. Math. Soc., Providence, Rhode Island, 2009.

Department of Mathematical Sciences

Indiana University - Purdue University at Indianapolis (IUPUI)

402 N. Blackford St., LD 270, Indianapolis, Indiana, 46202

e-mail: pmorton@math.iupui.edu