Solutions of the cubic Fermat equation in ring class fields of imaginary quadratic fields (as periodic points of a 3-adic algebraic function)

Patrick Morton

Abstract

Explicit solutions of the cubic Fermat equation are constructed in ring class fields $\Omega_f$, with conductor $f$ prime to 3, of any imaginary quadratic field $K$ whose discriminant satisfies $d_K \equiv 1 \pmod{3}$, in terms of the Dedekind $\eta$-function. As $K$ and $f$ vary, the set of coordinates of all solutions is shown to be the exact set of periodic points of a single algebraic function and its inverse defined on natural subsets of the maximal unramified, algebraic extension $K_3$ of the 3-adic field $Q_3$. This is used to give a dynamical proof of a class number relation of Deuring. These solutions are also used to give an unconditional proof of one case of Aigner’s conjecture: the cubic Fermat equation has a nontrivial solution in $K = Q(\sqrt{-d})$ if $d_K \equiv 1 \pmod{3}$ and the class number $h(K)$ is not divisible by 3.

1 Introduction.

In the 1950’s Aigner wrote a series of papers [1]-[4] on the cubic Fermat equation in quadratic fields, building on work of Fueter [16]. Most of Aigner’s results had to do with the nonexistence of nontrivial solutions to the cubic Fermat equation in quadratic fields. The character of solutions to this equation in $K = Q(\sqrt{m})$ is the same as in the companion field $K_1 = Q(\sqrt{-3m})$: if there is a nontrivial solution in one field, then the same holds for the companion field. Thus, there are four families of coupled quadratic fields to consider: the fields generated over $Q$ by

$$1 : \sqrt{3n+1} \quad \text{or} \quad \sqrt{-(9n+3)},$$

1
where \( n \geq 0 \). Fueter had proved in 1913 that there is no nontrivial solution of \( x^3 + y^3 = z^3 \) in quadratic fields of the second family, when \( m = -(3n + 1) \) and 3 does not divide the class number \( h(K) \) of the imaginary field \( K = \mathbb{Q}(\sqrt{m}) \) (see [16]). Aigner [1] proved impossibility of solutions for the first family when the class number of the imaginary field is not divisible by 3. Aigner’s further investigations (see [32]) led him to conjecture in [3, p.16] that there always exist nontrivial solutions in the fields of the third and fourth families. The recent paper of Jones and Rouse [21] contains strong evidence for the truth of Aigner’s conjecture. They prove a conditional result, based on the Birch-Swinnerton-Dyer conjecture, for the existence of nontrivial solutions to the cubic Fermat equation in a quadratic field, in terms of the number of solutions of certain ternary quadratic forms; and their result, if shown to be unconditionally true, would imply Aigner’s conjecture.

In this paper I study solutions of the equation

\[
Fer_3 : 27X^3 + 27Y^3 = X^3Y^3
\]

in ring class fields of the imaginary quadratic fields of the fourth family:

\[
K = \mathbb{Q}(\sqrt{-d}), \quad -d \equiv 1 \pmod{3},
\]

and show that they arise as periodic points of a specific (multi-valued) algebraic function \( T(z) \) over \( \mathbb{C} \). Moreover, it turns out that these solutions give all the complex periodic points of \( T(z) \) other than \( z = 3 \), and can be given explicitly in terms of modular functions.

Recall that the ring class field \( \Omega_f \) of an imaginary quadratic field \( K = \mathbb{Q}(\sqrt{-d}) \) is the unique finite algebraic extension of \( K \) whose Galois group \( \text{Gal}(\Omega_f/K) \) is abelian, and which has the property that the prime ideals (relatively prime to \( f \)) of the ring of integers \( R_K \) of \( K \), which split completely into prime ideals of degree 1 in the ring of integers \( R_{\Omega_f} \) of \( \Omega_f \), are exactly the prime ideals \( p \) for which \( p = (\xi) \) is principal in \( R_K \) with \( \xi \equiv r \pmod{f} \) and \( r \in \mathbb{Z} \). It then follows that \( \text{Gal}(\Omega_f/K) \cong A_f/P_f \), where \( A_f \) is the group of fractional ideals of \( K \) which are relatively prime to \( f \) and \( P_f \) is the subgroup of \( A_f \) consisting of principal ideals of the form \( (\xi) \) for numbers \( \xi \equiv r \pmod{f} \) and \( r \in \mathbb{Z} \). The set of all such integers \( \xi \) of \( R_K \) is a ring, which gives rise to
the name ring class field. The properties of these fields are developed in the classical
theory of complex multiplication. (See [8], [13], and the paper of Hasse [17].)

In Sections 2 and 3 I shall exhibit an explicit solution of $Fer_3$ in the ring class
field $\Omega_f$ of $K$ whose conductor $f$ is relatively prime to 3, in terms of the Dedekind
eta function $\eta(z)$, defined as

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^{2n}), \quad q = e^{\pi iz}, \quad z \in \mathbb{H},$$

where $\mathbb{H}$ is the upper half-plane.

**Theorem 1.** If $K = \mathbb{Q}(\sqrt{-d})$, with $-d = -d_1f^2 \equiv 1 \pmod{3}$ and $-d_1 = \text{disc}(K/\mathbb{Q})$, let

$$w = \begin{cases} k + \sqrt{-d}, & \text{if } 2 \mid d, \\ \frac{k+\sqrt{-d}}{2}, & \text{if } (2, d) = 1; \end{cases}$$

where $k^2 \equiv -d/4$ resp. $-d \pmod{9}$ and $k \equiv 1 \pmod{6}$. Then a non-trivial solution $(X, Y) = (\alpha, \beta)$ of $Fer_3$ in the ring class field $\Omega_f$ of $K$ is given by

$$\alpha = 3 + \gamma^3, \quad \beta = \frac{3(\alpha^\tau + 6)}{\alpha^\tau - 3},$$

where $\gamma$ is the unique multiple

$$\gamma = \omega^i \frac{\eta(w/9)}{\eta(w)}, \quad \omega = \frac{-1 + \sqrt{-3}}{2}, \quad i \in \{0, 1, 2\},$$

of $\eta(w/9)/\eta(w)$ which lies in $\Omega_f$, and $\tau = (\Omega_f/K, \wp_3) \in \text{Gal}(\Omega_f/K)$ is the Artin symbol for the prime ideal $\wp_3 = (3, w)$ of $R_K$. The numbers $\alpha$ and $\beta$ are conjugate algebraic integers over $\mathbb{Q}$, and $\Omega_f = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$. In addition, $(\gamma) = \gamma R_{\Omega_f} = \wp_3' R_{\Omega_f}$, where $\wp_3'$ is the conjugate ideal of $\wp_3$ in $R_K$.

The solution $(\alpha, \beta)$ of $Fer_3$ given in Theorem 1 turns out to have some very
pretty properties. If $h(-d) = h(R_{-d}) = [\Omega_f : K]$ denotes the class number of the
order $R_{-d}$ of discriminant $-d$ in $K$, then the minimal polynomial $p_d(x)$ of $\alpha$ over $\mathbb{Q}$
has degree $2h(-d)$ and satisfies the transformation formula

$$(x - 3)^{2h(-d)} p_d \left( \frac{3(x + 6)}{x - 3} \right) = 3^{3h(-d)} p_d(x),$$
while the minimal polynomial $q_d(x)$ of $\gamma$ over $\mathbb{Q}$ satisfies

$$x^{2h(-d)} q_d \left( \frac{3}{x} \right) = 3^{k(-d)} q_d(x).$$

Furthermore, the roots of $p_d(x)$ are periodic points of the dynamical system defined by a single algebraic function and its inverse function in the maximal unramified, algebraic extension $K_3$ of the 3-adic field $\mathbb{Q}_3$.

**Theorem 2.** The roots of the polynomials $p_d(x)$ (as $-d$ varies over quadratic discriminants $\equiv 1 \pmod{3}$) which are prime to the respective ideals $\wp_3 = (3, w)$ in $R_K$ are all the periodic points of the algebraic function

$$T(z) = \frac{z^2}{3}(z^3 - 27)^{1/3} + \frac{z}{3}(z^3 - 27)^{2/3} + \frac{z^3}{3} - 6$$

(1.1)

in its domain $\{z : |z|_3 \geq 1\} \subset K_3$, under the natural embedding $L \to L_p \subset K_3$, where $L = \Omega_f$ and $L_p$ is the completion of $L$ at a prime ideal $p$ for which $p|\wp_3$. The remaining roots of the polynomials $p_d(x)$ (for the same $d$'s) are, together with $z = 3$, all the periodic points of the inverse algebraic function

$$S(z) = \frac{z + 6}{(z^2 + 3z + 9)^{1/3}}$$

in the disk $D_3 = \{z : |z - 3|_3 \leq |3|_3^3\} \subset K_3$.

Viewing $T(z)$ and $S(z)$ as single-valued functions defined on the subsets $|z|_3 \geq 1$ and $D_3$ of the unramified extension $K_3$, respectively, is one way of choosing specific branches of the algebraic functions $T$ and $S$, since the cube roots of unity are not contained in $K_3$; and this is what makes it possible to consider their iterates on these sets. Note also that $T$ and $S$ are conjugate maps on their respective domains (see equation (4.20)).

The analysis of the maps $T(z)$ and $S(z)$ has the following consequence. Let $\mathcal{D}_n$ denote the set of discriminants $-d \equiv 1 \pmod{3}$ of orders in imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ for which the Frobenius automorphism $\tau = (\Omega_f/K, \wp_3)$ in the corresponding ring class field $\Omega_f$ has order $n$. Then

$$\sum_{-d \in \mathcal{D}_n} k(-d) = nN_3(n) = \sum_{k|n} \mu(n/k)3^k, \quad n > 1. \tag{1.2}$$

This equivalent to a class number formula of Deuring [10, p. 269] (corrected in
[11, p. 24]; see Section 4), which he derived as a consequence of his theory of the endomorphism rings of elliptic curves. Here I give an alternative, dynamical interpretation of (1.2) by deriving this formula as a consequence of the arithmetic of the cubic Fermat equation and the dynamical system defined by (1.1) on \( K_3 \). Then the number on either side of (1.2) is the number of periodic points \( \alpha \) of \( T(z) \) of minimal period \( n \), all of which lie in the unit group \( U_3 \) of the ring of 3-adic integers of \( K_3 \).

Thus, the function \( T(z) \) locates the global numbers \( \alpha \) and \( \beta \) which are the roots of \( p_d(x) \) inside of the unramified local 3-adic field \( K_3 \). This is analogous to the way in which we normally envision algebraic numbers over \( \mathbb{Q} \) as elements of the complex field \( \mathbb{C} \). For the infinite set of algebraic numbers defined by the polynomials \( p_d(x) \), the map \( T \) is a common lifting of the Frobenius map to the 3-adic field \( K_3 \), which is generated over \( \mathbb{Q}_3 \) by these numbers. Note the connection to the fact that the unique unramified extension of degree \( n \) over \( \mathbb{Q}_3 \) is generated by primitive roots of unity of order \( 3^n - 1 \), which are periodic points of the map \( F(z) = z^3 \) with minimal period \( n \). Equation (1.2) is an expression of the fact that \( T(z) \) and \( F(z) \) have the same number of periodic points of minimal period \( n \) in the unit group \( U_3 \), for all \( n > 1 \).

The 3-adic proof of Theorem 2 actually yields more, that the only periodic points, suitably defined, of the multi-valued function \( T(z) \) on either the algebraic closure \( \overline{\mathbb{Q}}_3 \) of \( \mathbb{Q}_3 \) or the complex field \( \mathbb{C} \) are \( z = 3 \) and the roots of the polynomials \( p_d(x) \). (See Theorem 4.4.) Thus, the periodic points \( z \neq 3 \) of \( T(z) \) in \( \mathbb{C} \) have number theoretic significance, in that they generate ring class fields, unramified over the prime \( p = 3 \), of the imaginary quadratic fields \( K \) considered in Theorems 1 and 2. It is also possible to show that all pre-periodic points of \( T(z) \) other than \( z = 3 \omega, 3 \omega^2 \) generate ring class fields, ramified over \( p = 3 \), of the same quadratic fields considered above. (See Section 5.)

In another paper [29] I will show that similar considerations apply to the solutions of the quartic Fermat equation which are studied in [24]. Their coordinates also represent periodic points of an algebraic function, which is defined on a subset of the maximal unramified, algebraic extension \( K_2 \) of the 2-adic field \( \mathbb{Q}_2 \), and which yields the analogue of the dynamical relation (1.2) for the prime \( p = 2 \). Based on these examples, and the fact that Deuring’s class number formulas hold for all primes \( p \), it is reasonable to make the following conjecture. (This conjecture is also stated in [29].)

To state the conjecture, define an imaginary quadratic field \( K \) to be \( p \)-admissible,
for a given prime \( p \in \mathbb{Z} \), if \( \left( \frac{d_K}{p} \right) = +1 \), where \( d_K \) is the discriminant of \( K \), so that \( p \) splits into two prime ideals in the ring of integers \( R_K \) of \( K \).

**Conjecture.** Let \( p \) be a fixed prime number. There is an algebraic function \( T_p(z) \), defined on a certain subset of the maximal unramified, algebraic extension \( K_p \) of the \( p \)-adic field \( \mathbb{Q}_p \), with the following properties:

1) All ring class fields of any \( p \)-admissible quadratic field \( K \subset \mathbb{Q}_p \) whose conductors are relatively prime to \( p \) are generated over \( K \) by periodic points of \( T_p(z) \) contained in the unramified extension \( K_p \).

2) All ring class fields of \( K \) whose conductors are divisible by \( p \) are generated over \( K \) by pre-periodic points of \( T_p(z) \) contained in the algebraic closure \( \overline{\mathbb{Q}}_p \).

3) All but finitely many of the periodic and pre-periodic points of \( T_p(z) \) contained in \( \mathbb{Q}_p \) generate ring class fields over \( K \).

The results of this paper show that this conjecture is true for the prime \( p = 3 \), and further papers will show that it is also true for \( p = 2 \) and \( p = 5 \).

I finish this paper by proving Aigner’s conjecture for any imaginary quadratic field \( K = \mathbb{Q}(\sqrt{-d}) \) of the fourth family whose class number \( h(K) \) is not divisible by 3. In particular, Aigner’s conjecture holds unconditionally for a set of quadratic discriminants \( d_K \equiv 1 \pmod{3} \) which has density at least \( 1/2 \) in the set of all such discriminants. As an example, a nontrivial solution of \( Fer_3 \) in \( K = \mathbb{Q}(\sqrt{-17}) \) is computed in Section 7, by finding the trace to \( K \) of the solution given by Theorem 1. Similar arguments (see Theorem 6.4) show that there are infinitely many positive fundamental discriminants \( D \equiv 1 \pmod{12d_1} \) for which the quartic field \( L = \mathbb{Q}(\sqrt{-d}, \sqrt{D}) \) contains a nontrivial solution of \( Fer_3 \), where \( -d \equiv 1 \pmod{3} \) is fixed. If \( d_1 \) is the square-free part of \( d \), this holds for any positive fundamental discriminant \( D \equiv 1 \pmod{12d_1} \) for which \( h(-dD) \not\equiv 0 \pmod{3} \).

I also prove that Aigner’s conjecture is true for \( K \) when \( 3 \mid h(K) \), if the solution \((\alpha, \beta)\) of \( Fer_3 \) constructed in Theorem 1 for the Hilbert class field \( \Sigma = \Omega_1 \) satisfies \( Tr_{\Sigma/K}(1/\alpha) \not\equiv 0 \pmod{\varphi_3} \) in \( K \). Using this criterion, it is verified in Section 6 that Aigner’s conjecture is true for all four fields of the fourth family for which \( h(K) = 3 \). I have also verified in a similar way that Aigner’s conjecture holds for all 39 fields of the fourth family for which the class number satisfies \( h(K) = 3, 6, 9, \) or \( 12 \). Finally, I show in Theorem 6.6 that the rank of the curve \( Fer_3 \) over ring class fields \( \Omega_f \) of imaginary quadratic fields of the fourth family is unbounded. As a corollary of this discussion it follows that the rank of \( Fer_3 \) over \( \Sigma \) is always at least 1 for these fields.
2 Constructing solutions of $Fer_3$ in ring class fields.

The impetus for discovering the solutions in Theorem 1 came from studying a relationship between $Fer_3$ and the elliptic curve

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

in Deuring normal form (with base point $O$). The curve $Fer_3$ parametrizes the 3-isogenies with kernel $T_3 = \{O, (0, 0), (0, -1)\} \subset E_\alpha$ from one elliptic curve in Deuring normal form to another. If $(\alpha, \beta) \in Fer_3(k)$, where the characteristic of $k$ is not 3, then there is an isogeny $\phi_{\alpha,\beta} : E_\alpha \rightarrow E_\beta$ with kernel $T_3$ which is defined over $k(\alpha, \beta, \sqrt{-3})$. Further, let $G_{12}$ be the group of linear fractional mappings in $z$ generated by

$$\sigma_1(z) = \frac{3(z + 6)}{z - 3}, \quad \sigma_2(z) = \omega z, \quad \omega^2 + \omega + 1 = 0.$$ 

If $\phi : E_\alpha \rightarrow E_\beta$ is any isogeny with kernel $T_3$, then for some $\sigma \in G_{12}$, the point $(\sigma(\alpha), \beta)$ lies on $Fer_3$. See [26] for proofs of these facts. In addition, the remaining points of order 3 on $E_\alpha$ can be given in terms of simple rational functions of points $(\alpha, \beta)$ on $Fer_3$: if $\alpha \neq 0$, the points of order 3 on $E_\alpha$ are $(0, 0), (0, -1)$, and the points

$$(x, y) = \left( \frac{-3\beta}{\alpha(\beta - 3)}; \frac{\beta - 3\omega^i}{\beta - 3} \right), \quad i = 1, 2,$$

where $\beta$ runs over the three elements of $\overline{k}$ for which $(\alpha, \beta)$ is a point on $Fer_3$. Exchanging $\alpha$ and $\beta$ in this formula gives the points of order 3 on the isogenous curve $E_\beta$. This representation of the points of order 3 on $E_\alpha$ is key for showing that the numbers $\alpha$ and $\beta$ of Theorem 2 lie in the ring class field $\Omega_f$.

For later use note that the parameter $\alpha$ of the non-singular elliptic curve $E_\alpha$ is never equal to $3\omega^i$ ($0 \leq i \leq 2$), since the $j$-invariant of $E_\alpha$ is

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

and that no solution $(\alpha, \beta)$ of $Fer_3$ can have $\alpha = 3\omega^i$ (since $\text{char}(k) \neq 3$). Thus, any solution $(\alpha, \beta) \neq (0, 0)$ of $Fer_3$ gives a non-trivial solution $(3/\alpha, 3/\beta)$ of the equation $x^3 + y^3 = 1$.

We consider $\alpha$’s for which $E_\alpha$ has complex multiplication by the order $R_{-d}$ of discriminant $-d = -d_1f^2 \equiv 1 \pmod{3}$ in $K$. An algebraic number $\alpha$ will satisfy this
condition if and only if \( j_\alpha \) is a root of the class equation \( H_{-d}(x) \) for the discriminant \(-d\). Hence, these \( \alpha \)'s are the roots of the equation

\[
F_d(x) = (x^3 - 27)^{h(-d)} H_{-d} \left( \frac{x^3(x^3 - 24)^3}{x^3 - 27} \right) = 0. \tag{2.3}
\]

Actually, we will take \( \alpha \) to be a root of the equation

\[
x^3(x^3 - 24)^3 - j(w)(x^3 - 27) = 0, \tag{2.4}
\]
where \( w = 1 + \sqrt{-d}/2 \) if \(-d \equiv 0 \) (mod \(4\)) and \( w = (1 + \sqrt{-d})/2 \) if \(-d \equiv 1 \) (mod \(4\)).

The plan of the proof is to first show that \( \alpha^3 \in \Omega_f \), and then to show \( \beta \in \Omega_f \), for a suitable solution \((\alpha, \beta)\) of \( Fer_3 \). It will then follow that \( \alpha \in \Omega_f \) also.

**Step 1.** We first solve (2.4). Recalling the definition of the Dedekind \( \eta \)-function,

\[
\eta(z) = q^{1/12} \prod_{n=1}^{\infty} (1 - q^{2n}), \quad q = e^{\pi iz},
\]
we have from the discussion in Weber [38, pp. 251-252] that the functions

\[
x_1 = 27 \left( \frac{\eta(3w)}{\eta(w)} \right)^6, \quad x_2 = - \left( \frac{\eta(w/3)}{\eta(w)} \right)^6,
\]

\[
x_3 = - \left( \frac{\eta(4+w/3)}{\eta(w)} \right)^6, \quad x_4 = - \left( \frac{\eta(8+w)}{\eta(3)} \right)^6,
\]
satisfy the quartic equation

\[
x^4 + 18x^2 + \gamma_3(w)x - 27 = 0,
\]
where \( \gamma_3(w) = \sqrt{j(w) - 1728} \). Hence,

\[
j(w) = \gamma_3^2(w) + 1728 = \left( \frac{x^4 + 18x^2 - 27}{x_i} \right)^2 + 1728 = \frac{(x_i^2 + 27)(x_i^2 + 3)^3}{x_i^2}. \tag{2.5}
\]

On the other hand, Weber [38, p. 255] remarks that the function \( x_1 \) transforms into \(-27/x_2 \) under the mapping \( w \to w/3 \), and therefore \( x_2 \) satisfies the equation
\[ 27^3 + 18 \cdot 27x^2 - \gamma_3 \left( \frac{w}{3} \right) x^3 - x^4 = 0, \quad x = x_2. \]  

(2.6)

Hence, we have

\[
j \left( \frac{w}{3} \right) = \gamma_3 \left( \frac{w}{3} \right)^2 + 1728 = \left( \frac{x_2^3 - 18 \cdot 27x_2^2 - 27^3}{x_2^3} \right)^2 + 1728 = \frac{(x_2^2 + 27)(x_2^2 + 243)^3}{x_2^6}. \]

(2.7)

Furthermore, \( x_2(w/3) = y^2/x_2 \), where

\[
y = y(w) = \left( \frac{\eta(w/9)}{\eta(w)} \right)^3, \]

(2.8)

from which Weber obtains the equation

\[ y^8 + 18y^4x_2^2 + \gamma_3 \left( \frac{w}{3} \right) y^2x_2^3 - 27x_2^4 = 0. \]

Eliminating \( \gamma_3(w/3) \) from this equation and (2.6) gives

\[ (y^2 + 27)(x_2^2 - 27y - 9y^2 - y^3)(x_2^2 + 27y - 9y^2 + y^3) = 0. \]

Using the first few terms of the \( q \)-expansion of \( y = q^{-2/9} - 3 + ... \) yields that

\[ 27y + 9y^2 + y^3 = q^{-2/3} - ..., \]

while

\[ -27y + 9y^2 - y^3 = -q^{-2/3} + .... \]

Since \( x_2^2 = q^{-2/3} + ... \) we conclude that \( x_2^2 = 27y + 9y^2 + y^3 = (y + 3)^3 - 27 \). Thus our formulas (2.5) and (2.7) for \( j(w) \) and \( j(w/3) \) yield

\[ j(w) = \frac{(y + 3)^3((y + 3)^3 - 24)^3}{(y + 3)^3 - 27}, \]
\[ j \left( \frac{w}{3} \right) = \frac{(y + 3)^3((y + 3)^3 + 216)^3}{((y + 3)^3 - 27)^3}. \]

The first of these equations implies that
\[ \alpha = y(w) + 3 = \left( \frac{\eta(w/9)}{\eta(w)} \right)^3 + 3 \]
is an identical solution of (2.4), and with \( w = 1 + \sqrt{-d}/2 \) or \( (1 + \sqrt{-d})/2 \) we have
\[
\begin{align*}
j(w) &= \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}, \\
j \left( \frac{w}{3} \right) &= \frac{\alpha^3(\alpha^3 + 216)^3}{(\alpha^3 - 27)^3}, \\
\alpha &= y(w) + 3. \quad (2.9)
\end{align*}
\]

Since \{1, w\} is a basis for \( \mathbb{R}_{-d} \), we know that \( j(w) \) is a root of \( H_{-d}(x) \). Since \(-d \equiv 1 \pmod{3}\), \{3, w\} is a basis for a prime ideal divisor \( \wp_{3,-d} = \wp_3 \cap \mathbb{R}_{-d} \) of 3 in the order \( \mathbb{R}_{-d} \). Hence \( j(w/3) \) is also a root of \( H_{-d}(x) \) and \( j(w) \) and \( j(w/3) \) are conjugate over \( \mathbb{Q} \). By the theory of complex multiplication, both are generators of \( \Omega_f \) over \( K \).

For later use we note that (2.9) also holds when \( w = w_1/w_2 \) and \{\( w_1, w_2 \)\} is a basis for an ideal \( \mathfrak{a} \) in \( \mathbb{R}_{-d} \) such that \{\( w_1, 3w_2 \)\} is a basis for \( \wp_{3,-d}\mathfrak{a} \).

**Step 2.** Next we show that \( \alpha^3 \in \Omega_f \). We choose \( \beta \) so that \( (\alpha, \beta) \) lies on \( \text{Fer}_3 \): then \( \alpha^3 = 27\beta^3/(\beta^3 - 27) \), so that
\[
\begin{align*}
j \left( \frac{w}{3} \right) &= \frac{\alpha^3(\alpha^3 + 216)^3}{(\alpha^3 - 27)^3} = \frac{\beta^3(\beta^3 - 24)^3}{\beta^3 - 27}, \\
j(w) &= \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} = \frac{\beta^3(\beta^3 + 216)^3}{(\beta^3 - 27)^3}. \quad (2.10)
\end{align*}
\]

We conclude from (2.3) and (2.10) that \( \beta \) is also a root of the polynomial \( F_d(x) \).

Now we set \( t = \alpha^3 \), and note that \( t \) satisfies two quartic equations over the ring class field \( \Omega_f \), namely
\[ t(t - 24)^3 - j(w)(t - 27) = 0 \quad \text{and} \quad t(t + 216)^3 - j \left( \frac{w}{3} \right) (t - 27)^3 = 0. \]
We perform the Euclidean algorithm on these two polynomials in $t$. Setting $j = j(w)$ and $k = j(w/3)$ and subtracting the last two equations shows that $t$ is the root of a cubic polynomial over $\Omega_f$:

$$q_1(x) = (k - 720)x^3 - (138240 + 81k)x^2 + (-j + 2187k - 10091520)x + 27j - 19683k.$$ 

Now, $j$ and $k$ satisfy the equation $\Phi_3(j, k) = 0$, where $\Phi_3(x, y)$ is the modular equation for $n = 3$. In fact we have the formula:

$$3^{18}\Phi_3(j, k) = \text{Res}_x(t(t - 24)^3 - j(t - 27), t(t + 216)^3 - k(t - 27)^3).$$

From this it follows that $k \neq 720$, since $j$ and $k$ are conjugates over $\mathbb{Q}$ and $\Phi_3(720, 720) = (2)^{25}(3)^4(5)^4(7)^4(13)^4(23)^2(37) \neq 0$. Taking the remainder of $f(x) = x(x - 24)^3 - j(x - 27)$ with respect to $q_1(x)$ gives

$$(k - 720)^2f(x) - [(k - 720)x + (9k + 190080)]q_1(x) = q_2(x),$$

$${q_2(x) = (270k^2 - 720j + jk + 1990656000 + 25818480k)x^2 + }$$

$$ (-308880j - 319146480k - k^2j - 13824k^2 + 1422jk + 1911029760000)x$$

$$ - 39123jk + 27k^2j + 177147k^2 + 886460j + 3741344640k.$$

Let $a_2(j, k) = 270k^2 - 720j + jk + 1990656000 + 25818480k$ denote the leading coefficient of $q_2(x)$. Then $a_2(j, k)$ is also not zero, since the resultant of $a_2(j, k)$ and $\Phi_3(j, k)$ with respect to the variable $k$ is an irreducible polynomial in $j$ of degree 10 whose roots are not algebraic integers. (We will not make use of this fact, however.) Now we find the remainder of $q_1(x)$ with respect to $q_2(x)$:

$$a_2(j, k)^2q_1(x) - [(k - 720)a_2(j, k)x + (k^3j - 8046k^3 - 1819428480k^2 - 2223k^2j + 1252800j^2k - 7322393260800k - 122860800j - 1375941427200000)]q_2(x)$$

$$ = (k - 720)^2q_3(x) = (k - 720)^2(a_3(j, k)x + b_3(j, k)),$$

with

$$a_3(j, k) = -1512k^3j + j^2k^3 + 374706k^3 - 2232k^2j^2 - 2202104637k^2j$$

$$ + 1252800j^2k - 7322393260800k - 122860800j - 1375941427200000$$

$$ - 39123jk + 27k^2j + 177147k^2 + 886460j + 3741344640k.$$
We claim that $a_3(j, k) \neq 0$ for $d \neq 8, 11, 20, 32, 35$. This is because

\[
Res_k(a_3(j, k), \Phi_3(j, k)) = 354(j - 8000)^2(j + 32768)^2(j^2 - 126400j - 68147200)^2
\times (j^2 - 52250000j + 1216700000000j - 1342177280000)^2
\]

\[= 354H_{-8}(j)^2H_{-11}(j)^2H_{-20}(j)^2H_{-32}(j)^2H_{-35}(j)^2.\]

Leaving aside the $j$’s satisfying the class equations for these discriminants, we see that $t = \alpha^3$ is a root of $q_3(x) = a_3(j, k)x + b_3(j, k) \in \Omega_f[x]$, so that $\alpha^3 = -b_3(j, k)/a_3(j, k) \in \Omega_f$.

\textbf{Step 3.} Now we use a result of [14], according to which the ray class field $\Sigma_3$ of conductor $f = 3$ over $K = \mathbb{Q}(\sqrt{-d})$ satisfies

\[\Sigma_3 \Omega_f = K(j(E_\alpha), h(E_\alpha[3])),\]

(2.12)

where $h(P)$ is a Weber function on points of the curve $E_\alpha$ in (2.0). (See also [36, Thm. 5.6, p. 135] for the case $f = 1$, and Prop. 6.4 in [24].) This theorem is applicable because $E_\alpha$ has complex multiplication by the order $\mathcal{R}_{-d}$, by construction. Using the Weierstrass normal form for $E_\alpha$,

\[Y^2 = 4X^3 - \left(\frac{\alpha^4 - 24\alpha}{12}\right)X + \frac{\alpha^6 - 36\alpha^3 + 216}{216}, \quad \Delta = \alpha^3 - 27,\]

(2.13)

and the fact that $j(E_\alpha) \neq 0, 1728$ (since $-d \neq -4$), we have the following formula for $h(P)$:

\[
h(P) = \frac{g_2g_3}{\Delta} \alpha(P) = \frac{\alpha^4 - 24\alpha \alpha^6 - 36\alpha^3 + 216}{-216} \frac{1}{\alpha^3 - 27} \left(\frac{-3\beta}{\alpha(\beta - 3)} + \frac{\alpha^2}{12}\right)
\]

\[= -\frac{(\alpha^3 - 24)(\alpha^6 - 36\alpha^3 + 216)(\alpha^3 - 36)\beta - 3\alpha^3}{(2^7)(3^5)(\alpha^3 - 27)\beta - 3},\]

(2.14)
where $P$ is the point on (2.13) corresponding to $x = -3\beta/(\alpha(\beta - 3))$ on $E_\alpha$ (see (2.1)). We check that $(\alpha^3 - 24) \neq 0$ since $j_\alpha \neq 0$ and $(\alpha^6 - 36\alpha^3 + 216) \neq 0$ since $j_\alpha \neq 1728$. From the linear fractional form of the right side of (2.1) and the fact that $\alpha^3 \in \Omega_f$ we deduce that $\beta \in \Sigma_3 \Omega_f$ since $h(P) \in \Sigma_3 \Omega_f$. However $\alpha^3 \in \Omega_f$ implies that $\beta^3 = 27\alpha^3/(\alpha^3 - 27)$ also lies in $\Omega_f$. Since $[\Sigma_3 : \Sigma] = 2$ and therefore $[\Sigma_3 \Omega_f : \Omega_f] = 2$ in this case (see [19, p. 72]), $x^3 - \beta^3$ must have a linear factor over $\Omega_f$, so one of the cube roots of $\beta^3$ must lie in $\Omega_f$. By renaming, we may assume that $\beta$ itself lies in $\Omega_f$.

We now know that the isogenous curve $E_\beta$ is defined over the ring class field $\Omega_f$ of $K$ and that it has complex multiplication by $\mathcal{R}_{-d}$ (since $\beta$ is a root of $F_d(x)$). It follows as above that the $X$-coordinate $-3\alpha/(\beta(\alpha - 3))$ of the point obtained by switching the roles of $\alpha$ and $\beta$ in (2.1) lies in $\Sigma_3 \Omega_f$, so $\Omega_f(\alpha)$ is at most quadratic over $\Omega_f$. Changing notation, we assume this root is $\alpha$. In other words, we have $\omega^i\alpha = 3 + y(w)$, where $y(w)$ is given by (2.8), for some $i \in \{0, 1, 2\}$.

We have shown that the point $(\alpha, \beta)$ lies in $\text{Fer}_3(\Omega_f)$, and $\alpha \beta \neq 0$, so the ring class field $\Omega_f$ of $K$ does indeed contain a non-trivial solution of $\text{Fer}_3$.

Finally, in the case of the discriminants $-8, -11, -20, -32, -35$ we have the solutions

\begin{align*}
-d = -8 : & \quad \alpha, \beta = -2 \pm \sqrt{-2}; \\
-d = -11 : & \quad \alpha, \beta = -1 \pm \sqrt{-11}; \\
-d = -20 : & \quad \alpha, \beta = \frac{-1 + 7\sqrt{-1} \pm (\sqrt{5} + \sqrt{-5})}{2}; \\
-d = -32 : & \quad \alpha, \beta = \frac{4 + 2\sqrt{-1} \pm (5\sqrt{2} + 5\sqrt{-2})}{2}; \\
-d = -35 : & \quad \alpha, \beta = 3 + \sqrt{-7} \pm 2\sqrt{5}.
\end{align*}

(2.15)

This completes the proof that solutions of $\text{Fer}_3$ always exist in the ring class field $\Omega_f$, because the class numbers for these discriminants are respectively 1, 1, 2, 2, 2; and in the cases $d = 20$ and $d = 35$ the Hilbert class field is equal to the genus field of $K$. In the remaining case $d = 32$, the 2-ring class field of the field $K = \mathbb{Q}(\sqrt{-2})$ is $\Omega_2 = \mathbb{Q}(\sqrt{2}, \sqrt{-1}) = \mathbb{Q}(\sqrt{2}, \sqrt{-2})$. \[\square\]
Remark. The solutions in (2.15) are the same solutions used in [27] to prove congruences (mod p) for the class equations of discriminants $-3p$ and $-12p$, when $p \equiv 1$ (mod 4).

As a corollary of the above proof we have

**Corollary.** If the discriminant $-d$ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ satisfies $-d \equiv 1$ (mod 3), then the ring class field $\Omega_f$ of conductor $f$ is generated over $K$ by a root $\alpha$ of the equation (2.4), where $w = \sqrt{-d}/2$ if $-d \equiv 0$ (mod 4) and $w = (1 + \sqrt{-d})/2$ if $-d \equiv 1$ (mod 4).

**Proof.** This follows immediately from $\alpha \in \Omega_f$ and $\Omega_f = K(j_\alpha) \subseteq K(\alpha)$. \qed

This corollary is related to Theorem 12.2 of Cox’s book [8, pp. 249-250], a special case of Theorem 5.1 of Schertz’s paper [33, p. 60]. (Also see [34].) This theorem says that the cube root $\gamma_2(w') = (j(w'))^{1/3}$ (defined for general $w'$ in the upper half-plane to be the root which is real on the imaginary axis) generates the same field over $K$ (or $\mathbb{Q}$) that $j(w')$ does, where $w' = \sqrt{-d}/2$ or $(3 + \sqrt{-d})/2$. Since $j(w') = j(w \pm 1) = j(w)$ we have that

$$\gamma_2(w') = \left(\frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}\right)^{1/3} = \frac{\omega^i\beta(\alpha^3 - 24)}{3}, \quad w' = w \pm 1,$$

for some $i$, where $\alpha$ and $\beta$ are in $\Omega_f$. Since $\gamma_2(w') \in \Omega_f$ and $\omega$ is not in $\Omega_f$, this is only possible if $i = 0$. Thus, we have that

$$3\gamma_2(w') = \beta(\alpha^3 - 24), \quad w' = \frac{\sqrt{-d}}{2} \text{ or } \frac{3 + \sqrt{-d}}{2}. \quad (2.16)$$

Reversing the roles of $\alpha$ and $\beta$ gives

$$3\gamma' = \alpha(\beta^3 - 24), \quad \gamma'^3 = j(w/3). \quad (2.17)$$

We also note that $\Sigma_3 \Omega_f = K(j_\alpha, h(E_\alpha[3])) = K(\alpha, \beta, \omega) = \Omega_f(\omega)$ from (2.12) and (2.1).
3 Properties of the solution.

From the argument given in Section 2 we can only conclude that \((\alpha, \beta) \in \text{Fer}_3(\Omega_f)\), where the algebraic number \(\alpha\) satisfies

\[
\omega^{-i}\alpha = 3 + y(w) = 3 + \left(\frac{\eta(w/9)}{\eta(w)}\right)^3, \quad w = \begin{cases} 1 + \frac{\sqrt{-d}}{2}, & \text{if } 2|d, \\ 1 + \frac{\sqrt{-d}}{2}, & \text{otherwise,} \end{cases}
\]

for some \(i\). In this section we will see that \(i = 0\). We begin with the following proposition.

**Proposition 3.1.** a) The algebraic number \(\alpha\) defined by (3.0) has degree \(2h(-d)\) over \(\mathbb{Q}\) and therefore \(\Sigma = \mathbb{Q}(\alpha)\).

b) The minimal polynomial \(p_d(x)\) of \(\alpha\) over \(\mathbb{Q}\) is a normal polynomial.

c) The linear fractional mapping \(\sigma_1(x) = (x+6)/(x-3)\) acts on the roots of \(p_d(x)\).

d) \(\text{Norm}_{\Omega_f/\mathbb{Q}}(\alpha - 3) = 3^{3h(-d)}\).

*Proof.* The degree of \(\alpha\) over \(\mathbb{Q}\) is divisible by \(h = h(-d)\) since it generates \(\Omega_f\) over \(K\). If \(\alpha\) had degree \(h\), then it would follow from \(\mathbb{Q}(j_\alpha) \subseteq \mathbb{Q}(\alpha)\) and the fact that \(j_\alpha\) has degree \(h\) over \(\mathbb{Q}\) that \(\mathbb{Q}(j_\alpha) = \mathbb{Q}(\alpha)\); and since \(j_\alpha = j(w)\) is real, \(\alpha\) would be real. Equation (2.9) would then imply that \(j(w/3)\) is also real. But \(j(w/3)\) is the \(j\)-invariant of the ideal class of a prime divisor \(\varphi_{3,-d}\) of 3 in \(R_{-d}\), and \(\varphi_{3,-d}\) has order \(\leq 2\) in the class group only if \(9 = N(\lambda)\) for some primitive element \(\lambda = (a + b\sqrt{-d})/2\). This can only be the case if \(36 \geq d\), so \(j(w/3)\) is not real for \(d > 36\). The same conclusion follows if \(d = 23\), since in that case \(36 = x^2 + 23y^2\) is not solvable. Thus, \(\alpha\) cannot have degree \(h(-d)\), so it must have degree \(2h(-d)\) since it lies in the field \(\Omega_f\). Otherwise \(d < 36\) and \(d = -8, -11, -20, -32,\) or \(-35\). In the first two cases \(h(-d) = 1\), and \(j = 8000\) and \(-32768\), respectively. Factoring (2.4) in these two cases shows that \(\alpha\) is the root of a quadratic, verifying a). If \(d = -20, -32\) or \(-35\), then \(h(-d) = 2\), and factoring (2.4) for the roots \(j\) of \(H_d(x) = 0\) (see Step 2 in Section 2) shows that \(\alpha\) is the root of a quartic. This proves a) and b).

To prove c), note that \(p_d(x)\) is irreducible over \(\mathbb{Q}(\omega)\) since \(\Omega_f \cap \mathbb{Q}(\omega) = \mathbb{Q}\). From equation (2.10) it is clear that \(p_d(x)\) is a factor of the polynomial

\[
G_d(x) = (x^3 - 27)^{3h(-d)}H_{-d}\left(\frac{x^3(216)^3}{(x^3 - 27)^3}\right).
\]
Since the rational function $r(x) = x^3(x^3 + 216)/(x^3 - 27)^3$ is mapped to itself under any transformation $\sigma = (x \to (ax + b)/(cx + d))$ in the group $G_{12} = Gal(k(x)/k(r(x)))$, where $k = \mathbb{Q}(\omega)$, it follows that

$$p_d^\sigma(x) = (cx + d)^{2h(-d)}p_d(\sigma(x))$$

is an irreducible factor of $G_d(x)$ over $\mathbb{Q}(\omega)$. This is true for any irreducible factor of $G_d(x)$, so $G_{12}$ acts on irreducible factors of $G_d(x)$ over $\mathbb{Q}(\omega)$.

We show that $G_{12}$ is transitive on these factors (up to multiplication by nonzero constants). This follows easily from the Galois theory of the normal extension $k(x)/k(r(x))$, but here is a direct proof. For every root $j$ of $H_{-d}(x)$ there is a root $\xi$ of $p_d(x)$ for which $j = r(\xi)$, because $j(w/3) = r(\alpha)$ by (2.10), and there is an automorphism $\tau$ of $\Omega_f/K$ for which $j = j(w/3)^\tau$. Thus, we can take $\xi = \alpha^\tau$, since the set of roots of $p_d(x)$ is mapped into itself by $Gal(\Omega_f/K)$. If $q(x)$ is any irreducible factor of $G_d(x)$ over $\mathbb{Q}(\omega)$, and $\xi'$ is one of its roots, then $r(\xi') = j = r(\xi)$ is a root of $H_{-d}(x)$, so $\xi'$ and $\xi$ must belong to the same orbit under $G_{12}$ (since the 12-th degree rational function $r(z) - r(w)$ factors into linear factors over $k$, where each factor of the numerator corresponds to an element of $G_{12}$). From this it follows that $q(x) = c \cdot p_d^\sigma(x)$ for some element $\sigma \in G_{12}$ and some nonzero constant $c$.

Now, $deg(G_d(x)) = 12h$ and $deg(p_d(x)) = 2h$, so the stabilizer of $p_d(x)$ has order 2 and there is an involution in $G_{12}$ which fixes $p_d(x)$. There are only three involutions in $G_{12}$, namely

$$\sigma_1(z) = \frac{3(z + 6)}{z - 3}, \quad \sigma_3(z) = \frac{3\omega(z + 6\omega)}{z - 3\omega}, \quad \sigma_4(z) = \frac{3\omega^2(z + 6\omega^2)}{z - 3\omega^2}. \quad (3.2)$$

Suppose, for example, that $\sigma_3(\alpha) = s$ is a root of $p_d(x)$ and therefore lies in $\Omega_f$. Then the cube root of unity $\omega$ satisfies

$$18\omega^2 + (3\alpha + 3s)\omega - s\alpha = 0$$

over $\Omega_f$. But $\omega^2 + \omega + 1 = 0$ implies that $18 = 3(\alpha + s) = -s\alpha$; hence, $\alpha$ is a root of $x^2 - 6x - 18 = 0$ and $\alpha = 3 \pm 3\sqrt{3}$, impossible since $\sqrt{3} \notin \Omega_f$. The same argument shows that $\sigma_4(\alpha)$ cannot lie in $\Omega_f$. Hence, $p_d(x)$ can only be fixed by $\sigma_1(z)$, and this proves c).

It follows from c) that the roots of $p_d(x)$ come in pairs $\xi, \sigma_1(\xi) = 3 + 27/(\xi - 3)$. Therefore $\xi - 3$ and $27/(\xi - 3)$ are conjugates, so the constant term of $p_d(x + 3)$ is $3^{3h(-d)}$, which proves d). □
Corollary. The roots of the polynomial $G_d(x)$ are all contained in the field $\Omega_f(\omega)$.

It follows from part d) of this proposition that the prime divisors of $(\alpha - 3)$ are the same as the prime divisors of the ideal $(3, \alpha)$. We will sharpen this statement below. First we prove the following relationship between $\alpha$ and $\beta$.

Proposition 3.2. If $\tau = (\Omega_f/K, \wp_3)$ is the Artin symbol for the prime ideal $\wp_3 = (3, w)$ in $\Omega_f/K$, then

$$\alpha^\tau = \sigma_1(\beta) = \frac{3(\beta + 6)}{\beta - 3}.$$

Thus, $\beta$ is conjugate to $\alpha$ over $\mathbb{Q}$.

Proof. First note that the automorphism $\tau_1 = (j(w/3) \to j(w))$ is equal to the Artin symbol $\tau = (\Omega_f/K, \wp_3)$. This follows from Hasse’s congruence [13, p. 34], [17, Satz 11]: since $\{w, 1\}$ is a basis for $R_{-d}$, we have

$$j(w/3)^{\tau_1} = j(w) = j(\wp_3^{1/3}w_3) = j(\wp_3, -d)^3 = j(w/3)^3 = j(w/3)^\tau \pmod{\wp_3},$$

which implies that $j(w/3)^{\tau_1} \equiv j(w/3)^\tau \pmod{\wp_3}$ and therefore $\tau_1 = \tau$. This uses the fact that 3 does not divide the discriminant of $H_{-d}(x)$. (See [12].)

Secondly, Deuring’s reduction theory [10] implies that 0 is not a root of $H_{-d}(x) \pmod{3}$. This is because $j = 0$ is supersingular for $p = 3$, but $(-d/3) = +1$, so roots of $H_{-d}(x) \pmod{3}$ are singular but not supersingular. Hence 3 does not divide $H_{-d}(0)$, and the roots $j(w), j(w/3)$ of $H_{-d}(x)$ are relatively prime to 3.

It follows from this that $(\alpha, \beta, 3) = 1$. Suppose some prime divisor $p$ of 3 in $\Omega_f$ did divide $(\alpha, \beta)$. From (2.16) we have $\beta(\alpha^3 - 24) = 3\gamma$, where $\gamma^3 = j(w)$, so that $p^2$ would divide 3, impossible since 3 is not ramified in $\Omega_f/\mathbb{Q}$. On the other hand, every prime divisor of 3 divides $\alpha$ or $\beta$, by the defining equation $27\alpha^3 + 27\beta^3 = \alpha^3\beta^3$.

From equations (2.10) and (2.11) we have that $j(w/3) = r(\alpha)$ and $j(w) = r(\beta)$. Therefore, $j(w) = j(w/3)^\tau = r(\alpha^\tau) = r(\beta)$ implies that $\alpha^\tau = \sigma(\beta)$ for some $\sigma \in G_{12}$. It is easy to check that $\sigma(\beta) \notin \Omega_f$ unless $\sigma = 1$ or $\sigma_1$, because all other elements of $G_{12}$ have coefficients that involve $\omega$. This is obvious for the substitutions

$$x \to \omega x, \quad \frac{3\omega(x + 6)}{x - 3}, \quad \frac{3(x + 6\omega)}{x - 3\omega}$$

and the substitutions obtained from these by replacing $\omega$ by $\omega^2$. For the substitution $(x \to \frac{3\omega(x + 6\omega)}{x - 3\omega})$ it follows by applying the automorphism $(\omega \to \omega^2) \in Gal(\Sigma_3\Omega_f/\Omega_f)$ and subtracting:
\[
\frac{3\omega(x+6\omega)}{x-3\omega} - \frac{3\omega^2(x+6\omega^2)}{x-3\omega^2} = \frac{(3\omega - 3\omega^2)x^2 - 6x - 18}{x^2 + 3x + 9}.
\]

The last expression cannot be zero for \( x \in \Omega_f \) (see the proof of Proposition 3.1), so \( \frac{3\omega(\beta+6\omega)}{\beta-3\omega} \) is not in \( \Omega_f \). A similar argument works for the substitution \( (x \to \frac{3\omega^2(x+6\omega)}{x-3\omega}) \). Thus, \( \alpha^\tau = \sigma(\beta) \) for \( \sigma = 1 \) or \( \sigma_1 \).

From these facts we can rule out the equation \( \alpha^\tau = \beta \). Suppose \( p \) is any prime divisor of \( \wp_3 \) in \( \Omega_f \). Then \( p \) is fixed by the automorphism \( \tau = (\Omega_f/K, \wp_3) \), so that \( \alpha^\tau = \beta \) would imply that \( p \) divides \( \alpha \) and \( \beta \), contradicting \( (\alpha, \beta, 3) = 1 \). This proves that \( \alpha^\tau = \sigma_1(\beta) \). The fact that \( \alpha \) and \( \beta \) are conjugates follows from \( \beta = \sigma_1(\alpha^\tau) \) and Proposition 3.1c). □

**Corollary.** The polynomial \( p_d(x) \) is the only irreducible factor of the polynomial \( G_d(x) \) having roots in \( \Omega_f \).

**Proof.** This follows immediately from Proposition 3.1c) and the statement that \( \sigma(\beta) \notin \Omega_f \) unless \( \sigma = 1 \) or \( \sigma_1 \).

We next prove:

**Lemma 3.3.** The ideal \((\alpha - 3) = a^3\), where \( a = (3, \alpha) \) divides 3.

**Proof.** Using (2.11) we have

\[
\alpha^3(\alpha^3 - 24)^3 = j(w)(\alpha - 3)(\alpha^2 + 3\alpha + 9)
= j(w)(\alpha - 3) \left[ (\alpha - 3)^2 + 9(\alpha - 3) + 27 \right].
\]

(3.3)

Note first that only prime divisors of 3 can divide \( \alpha - 3 \), by Proposition 3.1d). Furthermore, if \( p \) divides 3, then at most the first power of \( p \) divides \( \alpha \), by (2.17). If the prime ideal \( p \) divides \( (\alpha - 3) \) to exactly the first power, then the right side of (3.3) is divisible at most by \( p^3 \), which is impossible since the left side is divisible by \( p^6 \). If \( p^2 \) exactly divides \( (\alpha - 3) \), then at most \( p^5 \) divides the right side of (3.3). Hence, \( p^3 \) must divide \( (\alpha - 3) \). On the other hand, \( p^4 \) cannot divide; otherwise \( p^7 \) divides the right side of (3.3), whereas the left side is divisible exactly by \( p^6 \). □

**Lemma 3.4.** If \( w = k + \sqrt{-d}/2 \) (d even) or \( (k + \sqrt{-d})/2 \) (d odd) is chosen so that

\[ k^2 \equiv -d/4 \text{ or } -d \pmod{9}, \quad k \equiv 1 \pmod{6}, \]

(3.4),
then the 24-th power \( (\eta(w/9)/\eta(w))^{24} \) is a generator of the principal ideal \( \wp_3^{24} \) in the field \( \Omega_f \), where \( (3) = \wp_3 \wp_3' \) in \( K \).

**Proof.** This is classical and well known. We have that
\[
\left( \frac{\eta(w/9)}{\eta(w)} \right)^{24} = \left( \frac{\eta(w/9)}{\eta(w/3)} \right)^{24} \left( \frac{\eta(w/3)}{\eta(w)} \right)^{24} = \left( \frac{\Delta(w,9)}{\Delta(w,3)} \right) \left( \frac{\Delta(w,3)}{\Delta(w,1)} \right)
\]

\[
= \wp_{P_0}(w,3)\wp_{P_0}(w,1),
\]
in Hasse’s notation [17, pp. 10-11], where
\[
\Delta(w_1, w_2) = \left( \frac{2\pi}{w_2} \right)^{12} \eta \left( \frac{w_1}{w_2} \right)^{24},
\]
\[
\wp_M(w_1, w_2) = m^{12} \frac{\Delta(M(w_1, w_2))}{\Delta(w_1, w_2)}, \quad \det(M) = m
\]

\( M \) is a primitive, integral \( 2 \times 2 \) matrix, and \( P_0 \) is the \( 2 \times 2 \) diagonal matrix with diagonal entries 1 and 3. By the choice of \( k \) we know that \( \{w,9\} \) is a basis of the ideal \( \wp_{3, -d}^{2} \). Then \( \{w, 1\} \) is a basis of \( R_{-d} \) and \( \{w, 3\} \) is still a basis of the ideal \( \wp_{3, -d} \), so our previous calculations remain valid. Now Hasse’s Satz 10 in [17] implies that both \( \wp_{P_0}(w, 3) \) and \( \wp_{P_0}(w, 1) \) are generators of the conjugate ideal \( \wp_3^{12} \), and this implies the lemma. (See also [13, p.32] or [23, p. 165].)

**Theorem 3.5.** The ideal \((\alpha - 3) = \wp_3'\) where \( \wp_3' \) is the conjugate ideal of \( \wp_3 \) in \( R_K \), and the element \( \alpha \in \Omega_f \) is given by
\[
\alpha = 3 + y(w) = 3 + \left( \frac{\eta(w/9)}{\eta(w)} \right)^3, \quad w = \begin{cases} k + \frac{\sqrt{d}}{2}, & \text{if } 2|d, \\ k + \frac{\sqrt{d}}{2}, & \text{otherwise}; \end{cases}
\]

where \( k \) satisfies (3.4). For the same value of \( w \) and some \( j \in \{1, 2\} \) we have
\[
\beta = 3\omega^j + \omega^j \left( \frac{3\eta(3w)}{\eta(w/3)} \right)^3.
\]
Proof. We have shown that
\[ \alpha = 3\omega^i + \omega^i \left( \frac{\eta(w/9)}{\eta(w)} \right)^3, \]
for some cube root of unity \( \omega^i \). We wish to show that \( i = 0 \). We have that
\[ \alpha - 3 = 3(\omega^i - 1) + \omega^i \gamma_1^3, \]
where \( \gamma_1 = \eta(w/9)/\eta(w) \). This equation implies that \( \gamma_1^3 \) lies in \( \Sigma_3 \Omega_f = \Omega_f(\omega) \), and Lemma 3.4 implies that \( (\gamma_1^3) = \varphi_3^3 \) in this field. The prime divisors of 3 in \( \Omega_f \) are all ramified in \( \Sigma_3 \Omega_f \), so if \( p \) is a prime divisor of \( (\alpha - 3) \) in \( \Sigma_3 \Omega_f \), then \( p^6 | (\alpha - 3) \) by Lemma 3.3. But then \( p \) divides \( \gamma_1^3 \), which implies that \( p^6 | \gamma_1^3 \). On the other hand, at most \( p^3 \) can divide \( 3(\omega^i - 1) \) unless \( i = 0 \). Equation (3.5) follows, so we have \( (\alpha - 3) = \varphi_3^3 \) because
\[ \beta = \sigma_1(\alpha^i) = 3 + \frac{27}{(\gamma_1^3)^2}. \]
To prove the formula for \( \beta \), note from [28, Theorem 12] (with \( \tau = w/3 \)) that \( (\alpha, \beta') \) is a point on \( Fer_3 \), where
\[ \beta' = 3 + \left( \frac{3\eta(3w)}{\eta(w/3)} \right)^3. \]
Since \( (\alpha, \beta) \) is also a point on \( Fer_3 \) we have \( \beta = \omega^j \beta' \), for some \( j \). But
\[ \left( \frac{3\eta(3w)}{\eta(w/3)} \right)^{24} = \varphi_{P_4}(w, 1) \frac{3^{12}}{\varphi_{P_4}(w, 1)} \cong 1 \cdot \frac{3^{12}}{\varphi_3^{12}} = \varphi_3^{12}, \]
using the same notation as in Lemma 3.4 (see [17, Satz 10] and [13, p. 43]), where \( P_4 \) is the diagonal matrix with entries 3 and 1. Hence, we have that
\[ \left( \frac{3\eta(3w)}{\eta(w/3)} \right)^6 \cong \varphi_3^3 \text{ in } \Omega_f(\omega). \]
This shows that \( j = 0 \) is impossible, since this would imply that \( \left( \frac{3\eta(3w)}{\eta(w/3)} \right)^3 \in \Omega_f \), a domain in which \( \varphi_3^3 \) is not the square of an ideal. \( \square \)

We will now show that the solution \((\alpha, \beta)\) of \( Fer_3 \) in the ring class field \( \Omega_f \) of \( K \) has the property that \( \alpha = 3 + \gamma^3 \) and \( \beta = 3 + \gamma'^3 \) for certain elements \( \gamma, \gamma' \in \Omega_f \).
α' be any algebraic number for which \( E_{\alpha'} \) has complex multiplication by \( R_{-d} \). If \( \beta' \) is chosen so that \((\alpha', \beta') \) is a point on \( Fer_3 \), then \( \beta' \) is a root of the polynomial \( G_d(x) \) in (3.1). By the corollary to Proposition 3.1, all the roots of \( G_d(x) \) are contained in the field \( \Omega_f(\omega) \). Furthermore, for each root \( j \) of \( H_{-d}(x) = 0 \), there is an \( \alpha' \) satisfying (2.11), i.e., \( j(E_{\alpha'}) = j \), for which \( \alpha', \beta' \in \Omega_f \), which we can see by just conjugating the solution of (2.4) that we constructed before by some element of \( Gal(\Omega_f/K) \).

We first prove the following.

**Theorem 3.6.** Let \( K = \mathbb{Q}(\sqrt{-d}) \), with \(-d \equiv 1 \pmod{3} \). If \( \alpha \) is any algebraic number for which \( E_{\alpha} : Y^2 + \alpha XY + Y = X^3 \) has complex multiplication by the order \( R_{-d} \), then \( \alpha \) lies in the class field \( \Sigma_9 \Omega_f \) over \( K \), where \( \Sigma_9 \) is the ray class field of conductor 9 over \( K \). In particular, \( \alpha \) generates an abelian extension of \( K \).

**Proof.** Suppose that \( \alpha \) is an arbitrary root of (2.11), for some root \( j \) of \( H_{-d}(x) = 0 \). We choose another root \( \alpha' \) of the same equation which lies in \( \Omega_f \), and a \( \beta' \in \Omega_f(\omega) \) for which \((\alpha', \beta') \) lies on \( Fer_3 \). If \( \alpha' = \omega^i \alpha \), for some \( i \), then certainly \( \alpha \in \Omega_f(\omega) = \Sigma_3 \Omega_f \subseteq \Sigma_9 \Omega_f \).

Otherwise, we will construct an explicit isomorphism \( E_{\alpha} \cong E_{\alpha'} \). By [26, Thm. 3.3] and the arguments of [26, pp. 262-263] we may take \( \beta' = \sigma_1(\beta) = 3(\beta + 6)/(\beta - 3) \in \Omega_f(\omega) \), by replacing \( \beta \) by \( \omega^i \beta \) for some \( i \). Then an isomorphism \( \iota : E_{\alpha} \rightarrow E_{\alpha'} \) is given by the equations (3.17) in [26, Prop. 3.10]:

\[
X' = -\gamma' X + \gamma,
\]

\[
Y' = \sqrt{-3(\beta - 3)} \frac{9}{9} \left( Y - \sqrt{-3}\omega^2 \delta \gamma X - \omega \delta \right);
\]

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 \( E_{\alpha} \), 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 \( \alpha' \) and the fact that \( \beta \) is a root of \( G_d(x) = 0 \), the element \( \gamma' \) lies in \( \Omega_f(\omega) \subseteq \Sigma_9 \Omega_f \). Furthermore, if \( P' = (X', Y') \) is a point of order 9 on \( E_{\alpha'} \), then \( X' \in \Sigma_9 \Omega_f \) by [14] (see [36, Thm. 5.6]...
for the case \( f = 1 \), since in (2.13), with \( \alpha' \) in place of \( \alpha \), we have that \( g_2, g_3, \Delta \in \Omega_f \).

It follows from (3.6) that \(-X/\gamma = \alpha X(\beta - 3)/(3\beta) \in \Sigma_9 \Omega_f \) for any point \( (X, Y) \) in \( E_{\alpha[9]} \), which gives that \( \alpha X \in \Sigma_9 \Omega_f \).

We now use [26, 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 \( E_{\alpha} \). It follows that

\[
x^2(x - 3 - \alpha) = x^3 - (3 + \alpha)x^2 = -\alpha x - 1 \in \Sigma_9 \Omega_f.
\]

On the other hand, \( \alpha^3 = 27\beta^3/(\beta^3 - 27) = r \in \Sigma_9 \Omega_f \), so multiplying the inclusion (3.7) by \( \alpha^3 \) gives that \( \alpha x - \alpha(3 + \alpha) \in \Sigma_9 \Omega_f \), and therefore \( (\alpha^2 + 3\alpha) \in \Sigma_9 \Omega_f \). 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 \( (r - 27)\alpha \in \Sigma_9 \Omega_f \). But \( r - 27 = \alpha^3 - 27 = \Delta \) is the discriminant of the curve \( E_{\alpha} \), which is non-zero, so we get that \( \alpha \in \Sigma_9 \Omega_f \). □

**Remark.** Calculations on Maple suggest that the following stronger statement holds.

**Conjecture.** Let \( K = \mathbb{Q}(\sqrt{-d}) \), with \( -d = -d_1 f^2 \equiv 1 \pmod{3} \) and \( -d_1 \) a fundamental discriminant. If \( E_{\alpha} : Y^2 + \alpha XY + Y = X^3 \) has complex multiplication by the order \( R_{-d} \) of discriminant \( -d \) in \( K \), then \( \alpha \) lies in the ring class field \( \Omega_9 \Omega_f = \Omega_{9f} \) of conductor \( 9f \) over \( K \).

Now we can prove

**Theorem 3.7.** If \( K = \mathbb{Q}(\sqrt{-d}) \) with \( -d = -d_1 f^2 \equiv 1 \pmod{3} \) and \( -d_1 \) a fundamental discriminant, then

a) \( \alpha = 3 + \gamma^3 \), where \( \gamma \in \Omega_f \) and \( \langle \gamma \rangle = \varphi_3' \).

b) For some \( i \), \( \gamma = \omega i \frac{\eta(w/9)}{\eta(w)} \), where \( w \) is defined by (3.5) and (3.4).

c) There is an integral solution \( (z, w) \) of the equation

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

in the ring class field \( \Omega_f \) of \( K \).
Proof. We use the same argument (suitably modified) as in the proof of [28, Theorem 1]. (Also see [24, Prop. 8.9].) For $k$ we take the field $k = \Sigma_d \Omega_f$, which by Theorem 3.6 contains the splitting field of the polynomial

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

over $\mathbb{Q}$ (see (2.3)). Then $\Omega_f(\omega) \subset k$ and $k/\Omega_f$ is abelian.

Now we let $j = j(\alpha) = \frac{\alpha^3 (\alpha^3 - 24)^3}{\alpha^3 - 27}$, where $\alpha$ is an indeterminate over $k$. We define $\beta$ by the condition $(\alpha, \beta) \in Fer_3$, as before. We will use the fact from [28] that the normal closure of the algebraic extension $k(\alpha)/k(j)$ is the function field $N$ given by

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

Consider a root $j_0$ of the class equation $H_{-d}(x)$. Then $j_0 \neq 0, 1728$ and all the roots of $j(\alpha) = j_0$ lie in the field $k$, by Theorem 3.6. If $P_{j_0}$ is the prime divisor of the rational function field $k(j)$ corresponding to the polynomial $j - j_0$, this implies that $P_{j_0}$ 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 $\alpha_0$ of $F_d(x)$ for which $j(\alpha_0) = j_0$ and $\alpha_0, \beta_0 \in \Omega_f$, and any prime divisor $\mathfrak{P}$ of $N$ for which

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

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, $\gamma_0$ generates an abelian extension of $\Omega_f$ and $\gamma_0^3 = \beta_0 - 3 \in \Omega_f$. This implies that $x^3 - \gamma_0^3$ is reducible over $\Omega_f$: otherwise, its splitting field would have Galois group $S_3$ over $\Omega_f$, since $\omega \notin \Omega_f$. Therefore, $\beta_0 = 3 + \gamma_0^3$ for some $\gamma_0 \in \Omega_f$, and applying the automorphism $\tau^{-1} \in Gal(\Omega_f/K)$ to the equation $\sigma_1(\beta_0) = \alpha^\tau_0$ 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, $\alpha_0 = 3 + \gamma^3$, with $\gamma = 3/\gamma_0^{\tau_1} \in \Omega_f$. The remainder of part a) and part b) is immediate from this and Theorem 3.5. Finally, the curve $C_{19}$ arises from setting
\( \alpha = 3 + z^3, \beta = 3 + w^3 \) in \( \text{Fer}_3 \) and simplifying. Thus, \((z, w) = (\gamma, \gamma_0)\) is a point on \( C_{19} \) defined over \( \Omega_f \). (See [28, Thm. 5].) \( \square \)

This theorem verifies several assertions made in [28, p. 341]. In particular, part a) is an analogue of [28, Thm. 1] in characteristic 0.

**Remark.** Part b) of this theorem is related to a theorem of Fricke-Hasse-Deuring (see [15, III, p. 362], [18], or [13, p. 41]), which says that with \( \gamma_1 = \eta(w/9)/\eta(w) \), the number \( \gamma_1^{24} = 3^{24}\Delta(w, 9)/\Delta(w, 1) \) is the 24-th power of an element of \( \Omega_f \). With \( \gamma \in \Omega_f \) as in Theorem 3.7a) we have \( \gamma^3 = \gamma_1^3 \) and therefore \( \gamma_1^{24} = \gamma^{24} \), so their theorem for our situation is a consequence of Theorem 3.7. But note that to handle the present case, in which \( w/9 \) is the ideal basis quotient for the ideal \( \wp_2^3 \), which is not relatively prime to 6 (see [13, p. 41]), one has to use the extension of this theorem due to Kubert and Lang [22, p. 296], and this extension only applies in the case \( \Omega_1 = \Sigma \).

Propositions 3.1 and 3.2 and Theorem 3.7 are summarized in Theorem 1 of the introduction, which is now completely proved.

**Proposition 3.8.** Let \( p_d(x) \) be the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \), and \( q_d(x) \) the minimal polynomial of the element \( \gamma \) of \( \Omega_f \) for which \( \alpha = 3 + \gamma^3 \). Then we have the identities

\[
(x - 3)^{2h(-d)}p_d \left( \frac{3(x + 6)}{x - 3} \right) = 3^{3h(-d)}p_d(x),
\]

\[
x^{2h(-d)}q_d \left( \frac{3}{x} \right) = 3^{h(-d)}q_d(x).
\]

(3.8)

**Proof.** We know the mapping \( x \to \sigma_1(x) = \frac{3(x + 6)}{x - 3} = 3 + \frac{27}{x - 3} \) permutes the roots of \( p_d(x) \), so

\[
(x - 3)^{2h(-d)}p_d \left( \frac{3(x + 6)}{x - 3} \right) = c \cdot p_d(x),
\]

for some constant \( c \). Now put \( x = 3 + 3\sqrt{3} \), a fixed point of the linear fractional map \( \sigma_1(x) \). This gives

\[
(3\sqrt{3})^{2h(-d)}p_d(3 + 3\sqrt{3}) = c \cdot p_d(3 + 3\sqrt{3}).
\]

The quantity \( p_d(3 + 3\sqrt{3}) \) cannot be 0, since 3 does not ramify in \( \Omega_f \). Hence, \( c = 3^{3h(-d)} \). We also know that

\[
p_d(3 + x^3) = q_d(x)q_d(\omega x)q_d(\omega^2 x).
\]
Now note that
\[ \sigma_1(3 + x^3) = 3 + \frac{27}{x^3}. \]
This gives that
\[ x^{6h(-d)p_d} \left( 3 + \frac{27}{x^3} \right) = 3^{3h(-d)p_d}(3 + x^3), \]
hence that
\[ x^{6h(-d)q_d} \left( \frac{3}{x} \right) q_d \left( \frac{3\omega}{x} \right) q_d \left( \frac{3\omega^2}{x} \right) = 3^{3h(-d)p_d}(x)q_d(\omega x)q_d(\omega^2 x). \]
Since the roots of \( x^{2h(-d)q_d}(3/x) \) lie in \( \Omega_f \), we must have
\[ x^{2h(-d)q_d} \left( \frac{3}{x} \right) = c_1 q_d(x), \]
with some constant \( c_1 \), and putting \( x = \sqrt[3]{3} \) shows immediately that \( c_1 = 3^{h(-d)}. \)

4 Solutions of \( \text{Fer}_3 \) as periodic points.

The substitution
\[ x = \frac{9\beta}{\alpha(\beta - 3)}, \quad y = \frac{9\beta}{\beta - 3} \quad (4.0) \]
converts the solution \((\alpha, \beta)\) of \( \text{Fer}_3 \) into a point \((x, y)\) on the elliptic curve
\[ E : \ Y^2 - 9Y = X^3 - 27. \quad (4.1) \]
(Putting \(-Y + 4\) for \(Y\) in (4.1) shows this is the curve (27B) in [9].) Proposition 3.2 shows that the coordinates of the point \((x, y)\) on the new curve are
\[ x = \frac{\alpha^\tau + 6}{\alpha}, \quad y = \alpha^\tau + 6 = \alpha x. \quad (4.2) \]
In particular, the point \((x, y)\) has integral coordinates.

We write the equation expressing the fact that the point \( P_d = (\frac{\alpha^\tau + 6}{\alpha}, \alpha^\tau + 6) \) lies on \( E \) in the following form:
\[
(a^\tau + 6)^2 - 9(a^\tau + 6) - \left( \frac{(a^\tau + 6)^3}{\alpha^3} \right) + 27 = \frac{((a^\tau)^2 + 3a^\tau + 9)a^3 - (a^\tau + 6)^3}{a^3} = \frac{g(\alpha, a^\tau)}{a^3},
\]
where
\[ g(x, y) = (y^2 + 3y + 9)x^3 - (y + 6)^3. \] (4.3)

Now define the following functions:
\[ T(z) = \frac{z^2}{3}(z^3 - 27)^{1/3} + \frac{z}{3}(z^3 - 27)^{2/3} + \frac{z^3}{3} - 6, \] (4.4)
\[ S(z) = \frac{z + 6}{(z^2 + 3z + 9)^{1/3}}. \] (4.5)

These functions satisfy the equations
\[ g(x, T(x)) = 0, \quad g(S(y), y) = 0 \]
so they are solutions of the implicit relation \( g(x, y) = 0 \) and inverse functions of each other. Note that the formula for \( T(z) \) can be obtained by using the Ferrarro-Tartaglia-Cardan formulas to solve \( g(z, y) = 0 \) as a cubic in \( y \).

We will take \( T(z) \) and \( S(z) \) to be defined on certain subsets of the maximal unramified extension \( K_3 \) of \( \mathbb{Q}_3 \) inside its algebraic closure \( \overline{\mathbb{Q}}_3 \). This is permissible because the cube root \((z^3 - 27)^{1/3}\) can be defined as the convergent 3-adic series
\[
(z^3 - 27)^{1/3} = z \sum_{k=0}^{\infty} \left( \frac{1}{3} \right) \left( \frac{-3}{z} \right)^{3k}, \quad w_3(z) \leq 0,
\]
for \( z \)'s satisfying \( 3w_3(-3/z) > 3/2 \), i.e. whenever \( |z|_3 \geq 1 \) in \( K_3 \). (See [31, p. 34].) Thus we have
\[
T(z) = -6 + z^3 + \frac{z^3}{3} \sum_{k=1}^{\infty} \left( \left( \frac{1}{3} \right)_k + \left( \frac{2}{3} \right)_k \right) \left( \frac{-3}{z} \right)^{3k}
= z^3 - 15 - z^3 \sum_{k=2}^{\infty} \frac{3^{2k-1}b_k}{k!} \frac{1}{z^{3k}}, \quad |z|_3 \geq 1, \] (4.6)
where \( b_k \) are the rational integers defined by \( b_1 = 3 \) and
\[
b_k = (3k - 4)(3k - 7) \cdots 5 \cdot 2 + 2 \cdot (3k - 5)(3k - 8) \cdots 4 \cdot 1, \quad k \geq 2.
\]
We note that $3^{k-1}b_k/k! \in \mathbb{Z}$ for $k \geq 1$ since $(1/3)$ and $(2/3)$ are $p$-adic integers for any prime $p \neq 3$ and since $w_3(3^k/k!) > w_3(3) = 1$ implies that $w_3(3^{k-1}/k!) > 0$. (See [20, pp. 264-265].) Note that the field $K_3$ is not complete with respect to its valuation, but every finite subextension is complete, so the series for $T(z)$ converges to an element of the field $\mathbb{Q}_3(z)$.

It is clear from (4.6) that $T(z)$ is a 3-adic unit whenever $z$ is, and that

$$T(z) \equiv -6 + z^3 \pmod{9}, \quad w_3(z) = 0. \quad (4.7)$$

More generally, (4.6) implies that

$$|T(z) - z^3|_3 < 1, \text{ for } |z|_3 \geq 1,$$

and therefore

$$|T(z)|_3 = |z|_3^3, \text{ for } |z|_3 > 1. \quad (4.8)$$

Hence, we may iterate the function $T(z)$ on the set $\{ z : |z|_3 \geq 1 \} \subset K_3$. In particular, (4.8) shows that $T(z)$ has no periodic points in the region $|z|_3 > 1$, so all of its periodic points must lie in the unit group $U_3$ of $K_3$.

On the other hand, the function $S(z)$ is convergent in a disc about $z = 3$, since

$$S(3 + 27z) = \frac{3(1 + 3z)}{(1 + 9z + 27z^2)^{1/3}} = 3(1 + 3z) \sum_{k=0}^{\infty} \left( \frac{-3}{3} \right)^k 3^{2k}z^k(1 + 3z)^k$$

$$= 3 + 27z^3 - 243z^4 + 1458z^5 - 6804z^6 + \cdots \equiv 3 \pmod{27}, \quad w_3(z) \geq 0.$$

This shows that we may iterate $S(z)$ on the disc $D_3 = \{ z : |z - 3|_3 \leq |3|_3^3 \}$.

**Lemma 4.1.** If $z \in K_3$ satisfies $|z|_3 \geq 1$ and $g(z, w) = 0$ for some $w \in K_3$, then $w = T(z)$. Similarly, $z \in D_3$ and $g(w, z) = 0$ for $w \in K_3$ implies that $w = S(z)$.

**Proof.** Let $t = T(z)$. Then $g(z, t) = g(z, w) = 0$ implies that

$$0 = \frac{(w + 6)^3g(z, t) - (t + 6)^3g(z, w)}{z^3} = (t^2 + 3t + 9)(w + 6)^3 - (w^2 + 3w + 9)(t + 6)^3$$

$$= (w - t) \left( (t^2 + 3t + 9)w^2 + (3t^2 - 45t - 54)w + 9t^2 - 54t + 324 \right).$$

If $w \neq t$, then $w$ would be a root of the quadratic in the last equation, which has discriminant $\delta = -27(t + 6)^2(t - 3)^2$. This would imply that $\mathbb{Q}_3(w, t) = \mathbb{Q}_3(\sqrt{-3}, t)$
is contained in $K_3$, which is impossible. The second assertion follows in the same way. □

The functions $T(z)$ and $S(z)$ allow us to express the relation $g(\alpha, \alpha^\tau) = 0$ as $g(\alpha, T(\alpha)) = 0$ or $g(\alpha^{\tau-1}, \alpha) = g(S(\alpha), \alpha) = 0$ depending on which embedding of $\Omega_f$ we are considering:

\begin{align*}
g(\alpha, \alpha^\tau) = 0 & \text{ and } \alpha \in U_3 \Rightarrow \alpha^\tau = T(\alpha), \quad (4.9) \\
g(\alpha, \alpha^\tau) = 0 & \text{ and } \alpha \in D_3 \Rightarrow \alpha^{\tau-1} = S(\alpha). \quad (4.10)
\end{align*}

Recall that if $p$ is a prime divisor of $\wp_3$ or $\wp'_3$ in $\Omega_f$, $L$ is the decomposition field of $p$, and $p_L$ is the prime divisor of $L$ which $p$ divides, then $Gal(\Omega_f/L) \cong Gal((\Omega_f)_p/L_{p_L}) = Gal((\Omega_f)_p/\mathbb{Q}_3)$ is generated by $\tau$. Thus we may apply $\tau$ to elements of $(\Omega_f)_p = \mathbb{Q}_3(\alpha) \subset K_3$, and we have

$$T(z)^\tau = T(z^\tau), \text{ for } z \in \mathbb{Q}_3(\alpha), \ |z|_3 \geq 1,$$

$$S(z)^{\tau^{-1}} = S(z^{\tau^{-1}}), \text{ for } z \in \mathbb{Q}_3(\alpha) \cap D_3.$$

Then $\tau^n = 1$ implies that

$$\alpha = \alpha^{\tau^n} = T^n(\alpha), \quad (\alpha, p) = 1,$$

$$\alpha = \alpha^{\tau^{-n}} = S^n(\alpha), \quad p|\alpha.$$

Hence, the solutions of $Fer_3$ we have constructed in ring class fields over $K$ (with conductors prime to 3) are periodic points of the algebraic functions $S$ and $T$!

We may find the minimal polynomials $p_d(x)$ of the periodic points of $S$ and $T$ using iterated resultants. To find the points of period $n$, we look for the integers $d \equiv 2 \pmod{3}$ for which the Frobenius automorphism $\tau = (\Omega_f/K, \wp_3)$ has order $n$. Then the point $(\alpha, \alpha^\tau)$ is a point on the curve $g(x, y) = 0$. Applying $\tau$ repeatedly to this point gives the equations

$$g(\alpha, \alpha^\tau) = g(\alpha^{\tau}, \alpha^{\tau^2}) = \cdots = g(\alpha^{\tau^{n-1}}, \alpha) = 0, \quad \tau^n = 1. \quad (4.11)$$

Then we know that $\alpha$ will be the root of a series of nested resultants.

As an example, we find the periodic points of period 3. The condition $\tau^3 = 1$ implies the equations

$$g(\alpha, \alpha^\tau) = g(\alpha^{\tau}, \alpha^{\tau^2}) = g(\alpha^{\tau^2}, \alpha) = 0.$$
Now compute the double resultant

\[ R_3(x) = \text{Res}_{x_2}(\text{Res}_{x_1}(g(x, x_1), g(x_1, x_2)), g(x_2, x)) = (x-3)(x^2+4x+6)(x^2+2x+12) \]
\[ \times(x^6 + 11x^5 + 65x^4 + 191x^3 + 441x^2 + 405x + 675) \]
\[ \times(x^6 + 20x^5 + 126x^4 + 172x^3 + 180x^2 - 1188x + 1188) \]
\[ \times(x^6 + 22x^5 + 208x^4 - 40x^3 + 144x^2 - 3456x + 6912) \]
\[ \times(x^6 + 6x^5 + 560x^4 - 1384x^3 + 576x^2 - 12960x + 43200) \]
\[ \times(x^6 - 74x^5 + 1680x^4 - 6184x^3 + 2736x^2 - 43200x + 172800) \]
\[ \times(x^6 - 13x^5 + 841x^4 - 2567x^3 + 1071x^2 - 20493x + 75141) \]
\[ \times(x^{12} - 44x^{11} + 724x^{10} + 11008x^9 + 30440x^8 - 125456x^7 - 806960x^6 - 1971936x^5 \]
\[ + 4056480x^4 + 17611776x^3 + 46267200x^2 + 10730880x + 24681024). \]

By our theory, every ring class field \( \Omega_f \) for which \(-d \equiv 1 \pmod{3} \) and \( \tau^3 = 1 \) must show up as the splitting field of one of the factors of this double resultant. Note that the factors \( x^2 + 4x + 6 \) and \( x^2 + 2x + 12 \) have the respective discriminants \(-d = -8\) and \(-2^2d = -44\) and the corresponding fields \( K \) have class number 1, i.e. \( \tau = 1 \). Further, \( z = 3 \) is a fixed point of the mapping \( S(z) \).

The sextic factors of \( R_3(x) \) are the minimal polynomials \( p_d(x) \) of \( \alpha \) corresponding to the values of \( d = 23, 44, 59, 83, 107, 92 \), respectively, and the 12th degree polynomial is the minimal polynomial of \( \alpha \) for \( d = 104 \). The second sextic is the polynomial \( p_{44}(x) \), whose splitting field is the ring class field with conductor 2 over \( \mathbb{Q}(\sqrt{-11}) \). The sixth polynomial \( p_{92}(x) \) corresponds to the ring class field with conductor 2 over \( K = \mathbb{Q}(\sqrt{-23}) \), which in this case coincides with the Hilbert class field of \( K \). (This gives a second set of integral solutions of \( \text{Fer}_3 \) in this field.) Thus there are exactly 4 quadratic fields \( K \) with \(-d \equiv 1 \pmod{3}\) and \( h(K) = 3 \), namely:

\[
 h(K) = 3 \ \text{and} \ \text{ord}(\tau) = 3 \ \text{iff} \ d = 23, 59, 83, 107. \quad (4.12)
\]

Taking \( n = 1 \), note that

\[
 R_1(x) = g(x, x) = (x - 3)(x^2 + 4x + 6)(x^2 + 2x + 12), \quad (4.13)
\]

so no fields with \( h(K) > 1 \) have \( \tau = 1 \). We also note that the above computation implies that there is only one field \( K = \mathbb{Q}(\sqrt{-d}) \) of the required form, namely
\(d = 104\), for which \(h(K) = 6\) and the Frobenius automorphism \(\tau = (\Sigma/K, \wp)\) has order 3.

Similarly, the resultant
\[
R_2(x) = \text{Res}_{x_1}(g(x, x_1), g(x_1, x)) = -(x - 3)(x^2 + 4x + 6)(x^2 + 2x + 12)
\]
\[
\times (x^4 - 12x^3 + 28x^2 + 48x + 576)(x^4 - 8x^3 + 26x^2 + 60x + 450)
\]
\[
\times (x^4 + 2x^3 + 26x^2 + 60x + 180)
\]
shows there are no fields \(K\) with \(h(K) = 6\) for which \(\tau\) has order 2. So in all cases where \(h(K) = 6\) except the case \(d = 104\), the automorphism \(\tau\) has order 6.

(The values of \(d\) corresponding to the the three quartics in this factorization are, respectively, \(d = 35\), \(d = 32\), and \(d = 20\).)

In the case of \(n = 3\), one could, of course, determine the values of \(d\) in (4.12) by solving the equations \(4^r \cdot 3^3 = x^2 + dy^2\) for \(r = 0, 1\), but computing the double resultant \(R_3(x)\) immediately gives minimal polynomials for the generators of the corresponding class fields!

We apply these insights to generalize the factorizations of \(R_n(x)\) for \(n = 1, 2, 3\). We define \(R_n(x)\) as follows. First define \(R^{(1)}(x, x_1) = g(x, x_1)\) and
\[
R^{(2)}(x, x_2) = \text{Res}_{x_1}(g(x, x_1), g(x_1, x_2)),
\]
and then recursively define
\[
R^{(k)}(x, x_k) = \text{Res}_{x_{k-1}}(R^{(k-1)}(x, x_{k-1}), g(x_{k-1}, x_k)), \quad k \geq 3.
\]
Then we set \(x_n = x\) in \(R^{(n)}(x, x_n)\) to obtain \(R_n(x)\):
\[
R_n(x) = R^{(n)}(x, x), \quad n \geq 1.
\]
From this definition it is easy to see that the roots of \(R_n(x)\) are exactly the \(a\)’s for which there exist common solutions of the equations
\[
g(a, a_1) = 0, \quad g(a_1, a_2) = 0, \quad \cdots \quad g(a_{n-1}, a) = 0.
\]
If \(a \in \mathbb{U}_3\) or \(D_3\), then
\[
a = T(a_{n-1}) = T^2(a_{n-2}) = \cdots = T^{n-1}(a_1) = T^n(a)
\]
or
\[ a = S(a_1) = S^2(a_2) = \cdots = S^{n-1}(a_{n-1}) = S^n(a), \]
respectively. The roots of \( R_n(x) \) in \( U_3 \cup D_3 \) are therefore points in \( K_3 \) whose periods with respect to \( S \) or \( T \) divide \( n \). We will now show that all the roots of \( R_n(x) \) are in \( U_3 \cup D_3 \).

We first compute the total number of roots of \( R_n(x) \) (with multiplicities) by considering the polynomial
\[ g(x, x_1) \equiv x_1^2 x^3 - x_1^3 \equiv x_1^2 (x^3 - x) \pmod{3}. \]

The definition of the resultant gives that
\[ R^{(2)}(x_1, x_2) = \text{Res}_{x_1}(x_1^2 (x^3 - x), x_2^2 (x_1^3 - x_2)) = -x_2^8 (x^9 - x_2), \]
\[ R^{(3)}(x_1, x_3) = \text{Res}_{x_2}(-x_2^8 (x^9 - x_2), x_3^2 (x_2^3 - x_3)) = x_3^{26} (x^{27} - x_3), \]
and recursively
\[ R^{(i+1)}(x_i, x_{i+1}) = \text{Res}_{x_i} \left( (-1)^{i-1} x_{i+1}^{3^{i-1}} (x^3 - x_i), x_{i+1}^2 (x_i^3 - x_{i+1}) \right) \]
\[ = (-1)^i x_{i+1}^{3^{i+1}-1} (x^{3i+1} - x_{i+1}) \pmod{3}. \]

Hence, taking \( i = n - 1 \) and \( x_n = x \) we have
\[ R_n(x) \equiv (-1)^{n-1} x_n^{3^n - 1} (x_3^n - x_n) \equiv (-1)^{n-1} x^{3^n-1} (x^{3^n} - x) \pmod{3}. \quad (4.18) \]

We deduce easily from (4.15) and the fact that the highest degree terms in \( g(x, y) \) in \( x \) and \( y \) do not vanish \( \pmod{3} \) that
\[ \text{deg}(R_n(x)) = 2 \cdot 3^n - 1, \quad n \geq 1. \]

It is clear from (4.17) that the roots of \( R_k(x) \) are all roots of \( R_n(x) \) whenever \( k|n \). I will show that \( R_n(x) \) has distinct roots for all \( n \geq 1 \). It will follow that the points of primitive period \( n \) are the roots of a polynomial \( P_n(x) \), for which
\[ R_n(x) = \pm \prod_{k|n} P_k(x), \quad (4.19a) \]
and therefore
\[ P_n(x) = \pm \prod_{k|n} R_k(x)^{(n/k)}. \quad (4.19b) \]
From (4.18) and Hensel’s Lemma it is clear that for each irreducible factor $\bar{f}_i(x)$ of degree $n$ of $R_n(x)$ (mod 3) (for $n \geq 2$) there exists a monic irreducible polynomial $f_i(x)$ of degree $n$ in $\mathbb{Z}_3[x]$, dividing $R_n(x)$, for which $f_i(x) \equiv \bar{f}_i(x) \pmod{3}$. Moreover, if $\zeta$ is a root of $f_i(x)$ in $\mathbb{Q}_3$, then $\mathbb{Q}_3(\zeta)$ is an unramified extension of $\mathbb{Q}_3$ of degree $n$, and therefore $\zeta \in K_3$. By (4.18), $\zeta$ is not a root of $R_k(x)$ with $k < n$, so the fact that $\zeta \in U_3$ (for $n > 1$) implies that $\zeta$ is a periodic point of $T$ with primitive period $n$. It follows that $T(\zeta)$ is also a periodic point of primitive period $n$, and from (4.7) we know that

$$T(\zeta) \equiv \zeta^3 \pmod{3}.$$ 

It follows from this congruence that $T(\zeta)$ and $\zeta$ are roots of the same $\bar{f}_i(x)$ (mod 3), and therefore they must be roots of the same factor $f_i(x)$, since (4.18) shows that the roots of $\bar{f}_i(x)$ are simple roots of $R_n(x)$ (mod 3). Hence, the map

$$\zeta \rightarrow T(\zeta), \quad f_i(\zeta) = 0$$

represents an automorphism of the field $\mathbb{Q}_3(\zeta)/\mathbb{Q}_3$. The function $T(z)$ is therefore a lift of the Frobenius automorphism to $\mathbb{Q}_3(\zeta)$ (when applied to the roots of $f_i(x)$). This argument shows that $R_n(x)$ has the $N_3(n)$ simple factors $f_i(x)$ of degree $n$ whose roots are units in $K_3$, where $N_3(n)$ is the number of monic irreducible polynomials of degree $n$ in $\mathbb{F}_3[x]$.

Now we consider the numbers $\sigma_1(\zeta) = \frac{3(\zeta + 6)}{\zeta - 3} = 3 + \frac{27}{\zeta - 3}$, for a root $\zeta$ of any of the polynomials $f_i(x)$. Since $\zeta \in U_3$, it is clear that $\sigma_1(\zeta) \in D_3 - \{3\}$. I claim that $\sigma_1(\zeta)$ is a periodic point of $S(z)$ with primitive period $n$, and therefore also a root of $R_n(x)$. To show this I will use the identity

$$S(\sigma_1(\zeta)) = \sigma_1(T(\zeta)).$$

To prove this, let $z = \zeta$ and $t = T(\zeta)$ in the identity

$$(\sigma_1(z) + 6)^3(t - 3)^3 - 27(t + 6)^3(\sigma_1(z)^2 + 3\sigma_1(z) + 9)
= \frac{-3^9}{(z - 3)^3} \left((t^2 + 3t + 9)\zeta^3 - (t + 6)^3\right) = \frac{-3^9}{(z - 3)^3} g(z, t).$$

This gives

$$S(\sigma_1(\zeta))^3 = \sigma_1(T(\zeta))^3.$$ 

The cube roots of unity do not lie in $K_3$, so we may take cube roots in the last
equation, yielding (4.20). This identity implies that the maps $S$ and $T$ are conjugate maps on their respective domains.

Now (4.20) gives that
\[ S^n(\sigma_1(\zeta)) = S^{n-1}(\sigma_1(T(\zeta))) = S^{n-2}(\sigma_1(T^2(\zeta))) = \cdots = \sigma_1(T^n(\zeta)) = \sigma_1(\zeta). \]

Hence $\sigma_1(\zeta)$ is a periodic point of $S$ with primitive period dividing $n$. A similar argument shows that if $\sigma_1(\zeta)$ had period less than $n$, then the period of $\zeta$ with respect to $T$ would also be less than $n$. Hence, $\sigma_1(\zeta)$ is a root of $R_n(x)$ but not a root of $R_k(x)$ for any proper divisor $k$ of $n$. Since $\sigma_1(z)$ is a linear fractional map it is clear that $\sigma_1 : U_3 \to D_3$ is 1-1. Furthermore, the sets $U_3$ and $D_3$ are disjoint. This yields an additional $nN_3(n)$ distinct primitive roots of $R_n(x)$, and therefore a total of $2nN_3(n)$ primitive roots. Since roots of $R_k(x)$ are also roots of $R_n(x)$ for $k|n$, and $x - 3$ is the only factor of $R_1(x)$ in (4.13) to which the above analysis does not apply, it follows that the number of distinct roots of $R_n(x)$ is at least
\[ \sum_{k|n} 2kN_3(k) - 1 = 2 \cdot 3^n - 1 = \deg(R_n(x)). \]

Hence, all the roots of $R_n(x)$ are simple. This allows us to define the polynomial $P_n(x)$ by (4.19), and the degree of $P_n(x)$ is given by
\[ \deg(P_n(x)) = \sum_{k|n} \mu(n/k) \deg(R_k(x)) = 2nN_3(n), \quad n > 1. \quad (4.21) \]

By the above arguments we also know that $P_n(x)$ factors over $\mathbb{Q}_3$ as
\[ P_n(x) = \prod_i f_i(x) \tilde{f}_i(x), \quad (4.22) \]
where the roots of $\tilde{f}_i(x)$ are the images of the roots of $f_i(x)$ under $\sigma_1$. Therefore, all irreducible factors of $P_n(x)$ over $\mathbb{Q}_3$ have degree $n$. (By (4.13) this is even true for $P_1(x) = R_1(x)$.) Moreover, we may write the polynomial $f_i(x)$ in the form
\[ f_i(x) = \prod_{k=0}^{n-1} (x - T^k(\zeta_i)), \]
where $\zeta_i$ is a representative of the orbit under $T$ whose elements are the roots of $f_i(x)$.
Now it is obvious from the definition (4.19b) of the polynomial $P_n(x)$ that it has coefficients in $\mathbb{Q}$. Furthermore, we also know from (4.9) that if $(\alpha, \beta)$ is the solution of $F_{er_3}$ we constructed in the ring class field of $K$ corresponding to the discriminant $-d$ and $p_d(x)$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$, then

$$\text{ord}(\tau) = n \Rightarrow p_d(x) | P_n(x).$$

Conversely, every root $\zeta$ of $P_n(x) = 0$ is of course algebraic over $\mathbb{Q}$, and by (4.2) and (4.10) either $\left(\frac{T(\zeta)}{\zeta}+6, T(\zeta) + 6\right)$ or $\left(\frac{\zeta^6}{S(\zeta)}, \zeta + 6\right)$ is a point on the elliptic curve $E$, because $g(\zeta, T(\zeta)) = 0$ or $g(S(\zeta), \zeta) = 0$. Replacing $\zeta$ in the second of these points by $\sigma_1(\zeta)$ for a 3-adic unit $\zeta$, these points convert via the inverse of (4.0) to the points $(\alpha, \beta) = (\zeta, \sigma_1(T(\zeta)))$ and $(S(\sigma_1(\zeta)), \zeta) = (\beta, \alpha)$ on $F_{er_3}$ in an extension $L = \mathbb{Q}(\alpha, \beta) \subset K_3$ which is unramified over the prime 3.

The factorization of the resultants $R_n$ for $1 \leq n \leq 5$ suggests the following theorem.

**Theorem 4.2.** For $n > 1$, the polynomial $P_n(x)$ is the product of the polynomials $p_d(x)$ over all discriminants $-d \equiv 1 \pmod{3}$ for which the Frobenius automorphism $\tau = (\Omega_f/K, \wp_3)$ has order $n$. This fact is equivalent to the formula

$$\sum_{-d \equiv 1(3), \text{ord}(\tau) = n} h(-d) = n N_3(n) = \sum_{k|n} \mu(n/k) 3^k, \quad n > 1. \quad (4.23)$$

**Proof.** Let $\zeta \in U_3$ be a root of $P_n(x)$ in $K_3$. As stated above, the point $(\alpha, \beta) = (\zeta, \sigma_1(T(\zeta)))$ lies on $F_{er_3}$. This implies that there is an isogeny $\phi : E_\alpha \to E_\beta$ of degree 3, where $E_\alpha$ is the curve (2.0) in Deuring normal form. (See [28, Prop. 3.5].) Let $\tau$ denote the automorphism $\tau : \zeta \to T(\zeta)$ on $\mathbb{Q}_3(\zeta)$. By (2.2) and the fact that $(\alpha, \beta)$ lies on $F_{er_3}$ we have

$$j(E_\beta) = \frac{\beta^3(\beta^3 - 24)^3}{\beta^3 - 27} = \frac{\alpha^3(\alpha^3 + 216)^3}{(\alpha^3 - 27)^3}. \quad (4.24)$$

Since the last rational function in this equation is invariant under the substitution $\alpha \to \sigma_1(\alpha) = \sigma_1(\zeta) = \beta^{r^{-1}}$, we have

$$j(E_\beta) = \frac{(\beta^{r^{-1}})^3((\beta^{r^{-1}})^3 + 216)^3}{((\beta^{r^{-1}})^3 - 27)^3} = \frac{(\alpha^{r^{-1}})^3((\alpha^{r^{-1}})^3 - 24)^3}{(\alpha^{r^{-1}})^3 - 27} = j(E_{\alpha^{r^{-1}}}).$$
Therefore $E_\beta \cong E_{\alpha^r-1}$ and there is an isogeny $\phi_1 : E_\alpha \to E_{\alpha^r-1}$. Applying the isomorphism $\tau^{-1+1}$ to the coefficients gives an isogeny $\phi_i : E_{\alpha^r-(i-1)} \to E_{\alpha^r-i}$, and therefore an isogeny

$$\iota = \phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_1 : E_\alpha \to E_\alpha.$$ 

This isogeny has degree $\deg(\iota) = 3^n$, and we claim that $\Phi_{3^n}(j(E_\alpha), j(E_\alpha)) = 0$, where $\Phi_m(X, Y) = 0$ is the modular equation. We use several facts from [26]. From [26, Prop. 3.5] the $X'$-coordinate of $\phi(X, Y)$ on the curve $E_\beta$ is given by

$$X' = \frac{-\beta^2 3X^3 + \alpha^2 X^2 + 3\alpha X + 3}{9\alpha^2},$$

and so the 3-torsion points $P = \left( \frac{-3\beta}{\alpha(\beta - 3)}, \frac{\beta - 3\omega}{\beta - 3} \right)$ on $E_\alpha$ map to $(0, 0), (0, -1)$ on $E_\beta$. Further, using [26, Prop. 3.10] the isomorphism between $E_\beta$ and $E_{\alpha^r-1}$ may be chosen so that the $X_1$-coordinate on $E_{\alpha^r-1}$ is given in terms of $X'$ on $E_\beta$ by

$$X_1 = -\frac{\gamma_1}{\gamma_0} X' + \gamma_1, \quad \gamma_0 = -\frac{3\alpha}{\beta(\alpha - 3)}, \quad \gamma_1 = \left( \frac{-3\beta}{\alpha(\beta - 3)} \right)^{\tau^{-1}}.$$ 

Consequently we have $\phi_1(P) = \pm P^{\tau^{-1}}$, assuming that $\tau$ is defined so that it fixes $\omega$. Now, successive isogenies $\phi_i$ are defined by conjugating the coefficients in $\phi_1$ by powers of $\tau^{-1}$, so plugging in conjugate points gives

$$\phi_i(P^{\tau^{-(i-1)}}) = \pm P^{\tau^{-i}}, \quad 1 \leq i \leq n, \quad \implies \phi_n(P^{\tau^{-(n-1)}}) = \pm P^{\tau^{-n}} = \pm P.$$ 

Hence, we have $\iota(P) = \pm P$, which implies that $P$ does not lie in the kernel of $\iota$. From this and the fact that $P \in E_\alpha[3]$ we conclude that $\ker(\iota)$ is cyclic, and therefore $\Phi_{3^n}(j(E_\alpha), j(E_\alpha)) = 0$, as claimed. Now by a classical result [8, p.287] we have the factorization

$$\Phi_{3^n}(x, x) = c_n \prod_{-d} H_{-d}(x)^{r(d, 3^n)},$$

where the product is over discriminants of orders $R_{-d}$ of imaginary quadratic fields and

$$r(d, m) = |\{ \xi \in R_{-d} : \xi \text{ primitive}, \ N(\xi) = m \}|/R_{-d}^\times.$$ 

The exponent $r(d, 3^n)$ can only be nonzero when $4^k \cdot 3^n = x^2 + dy^2$ has a primitive
solution. The fact that $P_\alpha(x)$ splits in $K_3$ implies that all the conjugate fields of $Q(\alpha) = Q(\zeta) \subset Q_3(\zeta)$ over $Q$ are unramified at $p = 3$. This implies that $j(E_\alpha)$ is a root of $H_{-d}(x)$ for some $d$ which is not divisible by 3; hence, $(3, xyd) = 1$ and $-d \equiv 1 \pmod{3}$.

Since $j(E_\beta) = j(E_\alpha)^{\tau-1}$ by the first part of the proof, we know that $j(E_\beta)$ is also a root of $H_{-d}(x)$ and by (4.24), the minimal polynomial $p(x)$ of $\alpha$ over $Q$ is a factor of the polynomial $G_d(x)$ in (3.1). By the arguments in the proof of Proposition 3.1, $G_d(x)$ factors over $K_1 = Q(\omega)$ as a product of 6 factors, one of which is $p_d(x)$, whose stabilizer in the group $G_{12}$ is generated by the involution $\sigma_1(x) = \frac{3(x+6)}{x-3}$. Furthermore, we have that

$$(x - 3)^{2h(-d)}p_d(\sigma_1(x)) = 3^{3h(-d)}p_d(x), \quad (4.25)$$

by Proposition 3.8. Two factors of $G_d(x)$ are the monic factors $\omega^{h(-d)}p_d(\omega x)$ and $\omega^{2h(-d)}p_d(\omega^2 x)$, which lie in $K_1[x]$ but not in $Q[x]$. (In case $3|h(-d)$, $p_d(x)$ is not a polynomial in $x^3$ because the cube of a root of $p_d(x)$ generates the corresponding ring class field $\Omega_f$ over $Q$ and therefore cannot lie in a proper subfield of $\Omega_f$.) It follows that the roots of these two polynomials generate extensions which are ramified at the prime 3.

Next, the factor $\tilde{p}(x) = p_d(3\omega)^{-1}p_d^{\sigma_3}(x)$ with $\sigma_3(x) = \frac{3\omega^2(x+6\omega)}{x-3\omega}$ lies in $Q[x]$ (see (3.2)). This is because the mapping $\sigma_4(x) = \frac{3\omega^2(x+6\omega)}{x-3\omega} = \sigma_1(\sigma_3(x))$, so that (4.25) implies:

$$p_d(3\omega^2)^{-1}p_d^{\sigma_4}(x) = p_d(3\omega^2)^{-1}(x - 3\omega^2)^{2h(-d)}p_d(\sigma_1 \circ \sigma_3(x)) = p_d(3\omega^2)^{-1}(x - 3\omega^2)^{2h(-d)}(\sigma_3(x) - 3)^{-2h(-d)}3^{3h(-d)}p_d(\sigma_3(x)) = p_d(3\omega^2)^{-1}(-\omega)^{-h(-d)}(x - 3\omega)^{2h(-d)}p_d(\sigma_3(x)).$$

Putting $x = 3\omega$ in (4.25) and noting $\sigma_1(3\omega) = 3\omega^2$ gives $(-\omega)^{h(-d)}p_d(3\omega^2) = p_d(3\omega)$, yielding

$$p_d(3\omega^2)^{-1}p_d^{\sigma_4}(x) = p_d(3\omega)^{-1}p_d^{\sigma_3}(x),$$

as claimed. Now, because $\sigma_3$ has order 2, the roots of $\tilde{p}(x)$ are the numbers $\sigma_3(\xi) = \frac{3\omega(\xi+6\omega)}{\xi-3\omega}$, where $\xi = 3 + \pi^3$ runs through the roots of $p_d(x)$ and $\pi$ is a generator in $\Omega_f$. 

36
of the ideal \( \wp_3 \) or its conjugate \( \wp'_3 \). Let \( p \) be a prime divisor of 3 in the field \( \Omega_f(\omega) \). If \( p \parallel \pi \), then certainly \( p \) does not divide the numerator or denominator of
\[
\frac{\pi^3 + 3(1 + 2\omega)}{\pi^3 + 3(1 - \omega)} = \frac{\sigma_3(\xi)}{3\omega}.
\]
On the other hand, if \( p \nmid \pi \), then certainly \( p \) does not divide the numerator or denominator of
\[
\pi^3 + 3(1 + 2\omega) = \sigma_3(\xi) + 3(1 - \omega).
\]
Hence, \( w_p(\pi^3 + 3(1 + 2\omega)) = 0 \) in any case, and consequently \( \sigma_3(\xi) \equiv 0 \pmod{3} \). This implies that
\[
\tilde{p}(x) \equiv x^{2h(-d)} \pmod{3}
\]
and proves that \( \alpha \) cannot be a root of \( \tilde{p}(x) \). The same argument obviously applies to the factors \( \tilde{p}(\omega x) \) and \( \tilde{p}(\omega^2 x) \), which are the last two irreducible factors of \( G_d(x) \). This proves that \( \alpha \) can only be a root of the factor \( p_d(x) \). Then \( \beta = \sigma_1(\alpha^\tau) = \sigma_1(T(\xi)) \) is a root of the same factor. This shows that every root of \( P_n(x) \) is a root of some \( p_d(x) \).

To complete the proof, we must show that the Frobenius automorphism \( \tau_d = (\Omega_f/Q(\sqrt{-d}), \wp_3) \) has order \( n \). Since \( p_d(x) \) divides \( P_n(x) \), \( \alpha \) is a periodic point of the map \( T \) of exact period \( n \). The assertion is now clear from (4.9).

Finally, since \( P_n(x) \) has no multiple roots, and \( p_d(x) \) has degree \( 2h(-d) \), the formula (4.23) is a consequence of what we have proved, Proposition 3.1a), and the fact that
\[
\sum_{-d \equiv 1(3), \ ord(\tau) = n} 2h(-d) = deg(P_n(x)) = 2 \sum_{k|n} \mu(n/k) 3^k, \quad n > 1.
\]
Conversely, (4.23) implies that every root of \( P_n(x) \) is a root of some \( p_d(x) \) for which \( \tau_d \) has order \( n \). □

This theorem has several interesting consequences.

**Corollary 1.** Every periodic point of the maps \( T \) or \( S \) in the respective sets \( \{ z : |z|_3 \geq 1 \} \) or \( \mathbb{D}_3 - \{3\} \) is a root of \( p_d(x) \) for some integer \( d \equiv 2 \pmod{3} \), and generates a ring class field over the imaginary quadratic field \( K = Q(\sqrt{-d}) \).

To derive the second consequence, we note the following. From (2.2) we have
\[
j_\alpha = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27} \equiv \alpha^9 \pmod{\wp_3},
\]
if \( (\alpha, \beta) \) is the solution of \( Fer_3 \) that we constructed in Section 2. It follows that \( j_\alpha \) is
conjugate to $\alpha \pmod{p}$ for every prime divisor $p$ of $\varphi_3$ in $\Omega_f$. Since 3 does not divide the discriminant of the class equation $H_{-d}(x)$ and $\Omega_f = K(j_\alpha)$, $H_{-d}(x)$ factors (mod $\varphi_3$) into a product of $r = r(d) = h(-d)/n$ distinct polynomials $g_i(x)$ of degree $n$, where $n = \text{ord}(\tau)$ is the degree of the prime divisors $p_i = (3,g_i(j_\alpha))$ over $\varphi_3$ (also the order of $\varphi_3$ in the ring class group (mod $f$) of $K$). Since $\alpha$ is conjugate to $j_\alpha$ (mod $p_i$) for each $p_i$, its minimal polynomial $m_d(x)$ over $K$ factors exactly the same way, and hence

$$m_d(x) \equiv \prod_{i=1}^{r} g_i(x) \equiv H_{-d}(x) \pmod{\varphi_3}. \tag{4.26}$$

Furthermore, $\beta^\sigma \equiv 0 \pmod{\varphi_3}$, for all $\sigma \in \text{Gal}(\Omega_f/K)$, which implies the congruence

$$p_d(x) \equiv x^{h(-d)}H_{-d}(x) \pmod{3}. \tag{4.27}$$

Now let $\mathcal{D}_n$ denote the set of discriminants $-d \equiv 1 \pmod{3}$ of orders in imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ for which the Frobenius automorphism $\tau$ in the corresponding ring class field $\Omega_f$ has order $n$. Then (4.26) yields a map from the set $\mathcal{D}_n$ to the power set of the set of all monic irreducible polynomials ($\not\equiv x$) of degree $n$ in $\mathbb{F}_3[x]$: $-d \in \mathcal{D}_n \rightarrow S_d = \{\text{irred. } g_i(x) \in \mathbb{F}_3[x] : g_i(x) \mid H_{-d}(x) \pmod{3}, \deg(g_i(x)) = n\}$. Different integers $-d \in \mathcal{D}_n$ yield disjoint sets $S_d$, for the following reason. If some polynomial $g(x) \in \mathbb{F}_3[x]$ different from $x$ divides both $H_{-d_1}(x)$ and $H_{-d_2}(x) \pmod{3}$, then $g(x)$ would divide both $p_{d_1}(x)$ and $p_{d_2}(x) \pmod{3}$, by (4.27). But then $g(x)^2$ divides $R_n(x) \pmod{3}$ by Theorem 4.2 and (4.19a), which contradicts (4.18). It follows that

$$\sum_{-d \in \mathcal{D}_n} r(d) \leq N_3(n) = \frac{1}{n} \sum_{k \mid n} \mu(n/k)3^k$$

and the above theorem implies that this inequality is actually an equality. This gives the following corollary.

**Corollary 2.** Every monic irreducible polynomial $f(x) \not\equiv x$ of degree $n \geq 1$ in $\mathbb{F}_3[x]$ divides a unique class equation $H_{-d}(x) \pmod{3}$ with $-d \in \mathcal{D}_n$.

For example, when $n = 3$, each of the eight irreducible cubics over $\mathbb{F}_3$ corresponds to a unique discriminant $-d \in \mathcal{D}_3$, as follows:

$$S_{23} = \{x^3 + 2x^2 + 2x + 2\}, \quad S_{59} = \{x^3 + x^2 + x + 2\}, \quad S_{83} = \{x^3 + 2x + 2\},$$

38
\[ S_{107} = \{ x^3 + x^2 + 2 \}, \quad S_{44} = \{ x^3 + 2x^2 + 1 \}, \quad S_{92} = \{ x^3 + 2x^2 + x + 1 \}, \quad S_{104} = \{ x^3 + 2x + 1, x^3 + x^2 + 2x + 1 \}. \]

This leads to the following question. The polynomials \( g_i(x) \in \mathbb{F}_3[x] \) which divide a given polynomial \( p_d(x) \) (mod 3) in (4.26) appear to satisfy \( g_i(x) \equiv g_j(x) \) (mod \( x^2 \)) in \( \mathbb{F}_3[x] \); i.e., the \( g_i(x) \) all have the same linear and constant terms \( ax + b \). If this does hold for the irreducible factors \( g_i(x) \not\equiv x \) of \( p_d(x) \) (mod 3), then there can be no more than \( 3^{n-2} \) such factors, from which it would follow that \( h(-d) \leq n \cdot 3^{n-2} \). If \( g(x) \) is a given irreducible of degree \( n \) in \( \mathbb{F}_3[x] \), is it possible to determine its companions \( g_i(x) \) in (4.26) directly from \( g(x) \) itself, and thereby determine the class number \( h(-d) \) corresponding to the unique polynomial \( p_d(x) \) which it divides (mod 3)?

**Remark.** The relation (4.23) is equivalent to a class number relation discovered by Deuring [10], [11], which for the prime \( p = 3 \) can be stated as follows:

\[
\sum_{-d_{3^n}} h(-d_{3^n}) = 3^n - 1,
\]

the sum being taken over all discriminants \( -d_{3^n} \) of binary quadratic forms for which the principal form of discriminant \( -d_{3^n} \) properly represents \( 3^n \). This formula follows by summing (4.23) over the divisors \( d \neq 1 \) of \( n \), and noting from (4.13) that \( h(-8) + h(-11) = 3 - 1 \), which gives the formula corresponding to (4.23) for \( n = 1 \). The proof given above shows how this formula follows from the theory of the 3-adic periodic points of the functions \( T(z) \) and \( S(z) \), which is closely related to the cubic Fermat equation. Note also that Corollary 2 follows from Deuring’s lifting theorem [10].

The above analysis also implies the following theorem.

**Theorem 4.3.** The unique unramified extension of \( \mathbb{Q}_3 \) of degree \( n \geq 1 \) is the splitting field of any polynomial \( p_d(x) \) over \( \mathbb{Q}_3 \) for which \( -d \in \mathbb{D}_n \). In particular, the maximal unramified extension \( K_3 \) of \( \mathbb{Q}_3 \) inside its algebraic closure is the field generated over \( \mathbb{Q}_3 \) by the roots of all of the polynomials \( p_d(x) \), as \( -d \) ranges over discriminants \( \equiv 1 \) (mod 3) of orders in imaginary quadratic fields. In other words, \( K_3 \) is generated over \( \mathbb{Q}_3 \) by solutions of the cubic Fermat equation \( Fer_3 \).

One only has to note that by Corollary 2, there is, for every \( n \geq 1 \), a corresponding polynomial \( p_d(x) \). Thus there exists at least one discriminant \( -d \in \mathbb{D}_n \).

Finally, note that Theorem 4.2, together with (4.19a), actually shows that the only numbers \( a \) in either of the fields \( \mathbb{Q}_3 \) or \( \mathbb{C} \) which satisfy (4.17) are \( a = 3 \) and the
roots of the polynomials $p_d(x)$. Thus if we define a periodic point of $T(z)$ in $\mathbb{Q}_3$ or $\mathbb{C}$ to be any number $a$ for which there exist numbers $a_1, a_2, \cdots, a_{n-1}$ in $\mathbb{Q}_3$ resp. $\mathbb{C}$ satisfying (4.17), then we have shown the following.

**Theorem 4.4.** The set of periodic points (as defined above) of the multi-valued function $T(z)$ on either of the fields $\mathcal{K} = \mathbb{Q}_3$ or $\mathcal{K} = \mathbb{C}$ coincides with the set

$$S(\mathcal{K}) = \{3\} \cup \{\alpha \in \mathcal{K} : (\exists n \geq 1)(\exists -d \in D_n) \text{ s.t. } p_d(\alpha) = 0\}.$$ 

The same result holds for the algebraic closure $\mathcal{K} = \overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

5 **Pre-periodic points of $T(z)$.**

As above, we consider the algebraic function

$$T(z) = \frac{z^2}{3}(z^3 - 27)^{1/3} + \frac{z}{3}(z^3 - 27)^{2/3} + \frac{z^3}{3} - 6,$$

initially defined on the subset $\{z : |z|_3 \geq 1\} \subset \mathbb{K}_3$, where $\mathbb{K}_3$ is the maximal unramified, algebraic extension of the 3-adic field $\mathbb{Q}_3$. In this section, we consider this function on either the algebraic closure $\overline{\mathbb{Q}}_3$ of the rational field $\mathbb{Q}$ or on the algebraic closure $\overline{\mathbb{Q}}_3$ of $\mathbb{Q}_3$. Denote either of these fields by $\mathcal{K}$.

We consider $T(z)$ to be a multi-valued function, and define a pre-periodic point $\xi \in \mathcal{K}$ to be a number for which

$$T^k(\xi) = \alpha, \quad k \geq 1, \quad k \text{ minimal},$$

where $\alpha$ is a periodic point of $T(z)$, i.e., either 3 or a root of one of the polynomials $p_d(x)$. The only pre-periodic points for which $T^k(\xi) = 3$ are $\xi = 3\omega, 3\omega^2$, and then $k = 1$. We shall leave these points out of consideration for the rest of our discussion.

Using the same definition that was given in Section 4 above, and setting

$$g(x, y) = (y^2 + 3y + 9)x^3 - (y + 6)^3,$$

there is a sequence $\xi = \xi_k, \xi_{k-1}, \cdots, \xi_1$ of elements of $\mathcal{K}$ for which

$$g(\xi, \xi_k) = g(\xi_{k-1}, \xi_{k-2}) = \cdots = g(\xi_2, \xi_1) = g(\xi_1, \alpha) = 0.$$
This holds because any branch of the function $T(z)$ satisfies $g(z, T(z)) = 0$. We say $\xi_j$ is a pre-periodic point of level $j$.

Since $\alpha$ is a periodic point with some minimal period $n$, then $\alpha_1 = T^{n-1}(\alpha)$ satisfies $T(\alpha_1) = \alpha$. Thus $g(\alpha_1, \alpha) = 0$. However, the form of $g(x, y)$ shows that $g(\omega \alpha_1, \alpha) = 0$, $g(\omega^2 \alpha_1, \alpha) = 0$, and $g(\omega \beta, \alpha) = 0$, $g(\omega^2 \beta, \alpha) = 0$, so that $\xi = \omega \alpha_1, \omega^2 \alpha_1$ are pre-preperiodic with pre-period $k = 1$. It follows, since $\alpha_1$ is also a root of the polynomial $p_d(x)$, that there are at least $4h(-d)$ pre-periodic points having $k = 1$ and $p_d(T(\xi)) = 0$. On the other hand, the points $\xi$ for which $k = 1$ and $T(\xi)$ is a root of $p_d(x)$ are all roots of the resultant

$$R_1(x) = \text{Res}_y(p_d(y), g(x, y)) = \prod_{p_d(\alpha) = 0} g(x, \alpha).$$

This polynomial has degree $6h(-d)$ in $x$, since none of the roots of $p_d(y)$ are roots of $y^2 + 3y + 9 = 0$. However, $p_d(x)|R_1(x)$, so there are at most $6h(-d) - 2h(-d) = 4h(-d)$ pre-periodic points at level $k = 1$. It follows that there are exactly $4h(-d)$ pre-periodic points at level $k = 1$ corresponding to roots of $p_d(x)$, and these are just the roots of the irreducible polynomial (over $\mathbb{Q}$):

$$r_d(x) = p_d(\omega x)p_d(\omega^2 x).$$

Now consider points $\xi$ for which $T^2(\xi) = \alpha$ is a root of $p_d(x)$. Then $T(\xi) = \xi_1$, where $\xi_1 = \omega \beta$ or $\omega^2 \beta$ for some root $\beta$ of $p_d(x)$, and $\xi$ is a root of the polynomial

$$R_2(x) = \text{Res}_y(r_d(y), g(x, y)) = \prod_{p_d(\alpha) = 0} g(x, \omega \alpha)g(x, \omega^2 \alpha). \quad (5.1)$$

Setting

$$\sigma_1(z) = \frac{3(z + 6)}{z - 3},$$

we have the following lemma, which is easily verified.

**Lemma 5.1.** If $\omega = \frac{-1 + \sqrt{-3}}{2}$, then the identity holds:

$$81\sqrt{-3}g(x, \omega^2 y) = (y - 3)^3 g(x, \omega \sigma_1(y)).$$
From Proposition 3.1 we know that $\sigma_1(z)$ is an involution on the roots of $p_d(x)$. It follows from (5.1) and this lemma that $R_2(x)$ has at most $6h(-d)$ roots, i.e. $R_2(x) = c s_d(x)^2$ for some constant $c \in \mathbb{Z}$. We will see that $s_d(x)$ is an irreducible polynomial over $\mathbb{Q}$.

Let $w = \frac{(k + \sqrt{-d})}{2}$ or $k + \sqrt{-d}$ with $k^2 \equiv d \pmod{9}$ and $k \equiv 1 \pmod{6}$, as in Theorem 2. By replacing $k$ by $k + 18$ we may assume that $9 | N(w)$, where $N(w)$ is the norm of $w$ to $\mathbb{Q}$. Then $\{w, 9\}$ is a basis for the ideal $\wp_2 \cap \mathbb{R}_{-d}$ and $j(w/9)$ is a root of the class equation $H_{-d}(x)$ for the discriminant $-d$. It follows from the discussion in Section 2 that there is a root $\alpha$ of $p_d(x)$ for which

$$j\left(\frac{w}{9}\right) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}. \quad (5.2)$$

**Lemma 5.2.** If $T(\xi) = \xi'$, then

$$j(w') = \frac{\xi'^3(\xi'^3 - 24)^3}{\xi'^3 - 27} \implies j\left(\frac{w'}{3}\right) = \frac{\xi'^3(\xi'^3 - 24)^3}{\xi'^3 - 27}.$$

**Proof.** Let $\eta'$ satisfy the equation

$$27\xi'^3 + 27\eta'^3 = \xi'^3 \eta'^3.$$

We have that $g(\xi, \xi') = 0$, and so $\xi'^3 = \frac{(\xi'+6)^3}{\xi'^3 + 3\xi'^3 + 1}$ implies that

$$\frac{\xi'^3(\xi'^3 - 24)^3}{\xi'^3 - 27} = \frac{\xi'^3(\xi'^3 + 216)^3}{(\xi'^3 - 27)^3}.$$

Using the relation between $\xi'$ and $\eta'$ gives that

$$\frac{\xi'^3(\xi'^3 + 216)^3}{(\xi'^3 - 7)^3} = \frac{\eta'^3(\eta'^3 - 24)^3}{\eta'^3 - 27} = j\left(\frac{w'}{3}\right),$$

by the computations in §2. Putting these facts together proves the lemma. □

**Remark.**

1. See [7] for more examples of the relationship given in Lemma 5.2.

2. If $\eta$ is chosen so that $27\xi^3 + 27\eta^3 = \xi^3 \eta^3$, then

$$\frac{\xi^3(\xi^3 - 24)^3}{\xi^3 - 27} = \frac{\eta^3(\eta^3 + 216)^3}{(\eta^3 - 27)^3}.$$
implies that $\xi' = T(\xi) = \sigma(\eta)$ for some substitution $\sigma$ in the tetrahedral group $G_{12}$.

**Lemma 5.3.** If $r \geq 1$, then with the quantity $w$ defined above, $j\left(\frac{w}{3^{r+2}}\right)$ generates the ring class field $\Omega_{3^r f}$ of conductor $3^r f$ over $K = \mathbb{Q}(\sqrt{-d})$.

*Proof.* This follows from the fact that $9 | | N(w)$, so the minimal polynomial of $w/3^{r+2}$ is $f_k(x) = 3^{2r+2}x^2 - 3^r k x + N(w)/9$ ($d$ odd) or $f_k(x) = 3^{2r+2}x^2 - 2 \cdot 3^r k x + N(w)/9$ ($d$ even). Then the discriminant of $f_k(x)$ is $-3^{2r}d = -3^{2r} f^2 d_1$, where $-d_1$ is the discriminant of the field $K = \mathbb{Q}(\sqrt{-d})$. This implies the assertion. \(\square\)

**Theorem 5.4.** If $\xi$ satisfies $T^r(\xi) = \alpha$, where $\alpha$ satisfies (8.2) and $r \geq 1$ is minimal, then $K(\xi) = \Omega_{3^r f}$ and

$$\frac{\xi^3(\xi^3 - 24)^3}{\xi^3 - 27} = j\left(\frac{w}{3^{r+2}}\right). \quad (5.3)$$

*Proof.* We prove this by induction on $r$. For $r = 1$ we have $\xi = \omega \beta$ or $\omega^2 \beta$, for some root of $p_d(x)$. By Proposition 3.1, $\mathbb{Q}(\beta) = \mathbb{Q}(\beta^3) = \Omega_f$, so $\mathbb{Q}(\omega \beta) = \mathbb{Q}(\omega) = \Omega_{3f}$. Equation (5.3) holds for $r = 1$ by (5.2) and Lemma 5.2. Assume now that $T^{r-1}(\xi') = \alpha$, with $K(\xi') = \Omega_{3^{r-1} f} = K(j(w/3^{r-1+1}))$, for some $r \geq 2$, that (5.3) holds for $r - 1$ in place of $r$, and that $T(\xi) = \xi'$. Then $g(\xi, \xi') = 0$ implies that $[K(\xi, \xi') : K(\xi')] \leq 3$. On the other hand, putting $w' = w/3^{r+1}$, we have from Lemmas 5.2 and 5.3 that

$$K(\xi') = K(j(w')) \subset K(j(w'/3)) \subset K(\xi).$$

Since $[\Omega_{3^r f} : \Omega_{3^{r-1} f}] = 3$ for $r \geq 2$, this inclusion shows that $[K(\xi) : K(\xi')] = 3$ and $K(\xi) = \Omega_{3^r f}$, as desired. \(\square\)

It follows from this theorem that there are at least $[\Omega_{3^r f} : K] = 2 \cdot 3^{r-1} h(-d)$ conjugates of $\xi$ over $K$ and therefore at least this many pre-periodic points at level $r \geq 1$. Combining this with what we found for level $r = 2$, we see that there are exactly $6h(-d)$ pre-periodic points at level $r = 2$ attached to roots of $p_d(x)$, and they are all conjugates of $\xi = \xi_2$ over the quadratic field $K$. Thus the polynomial $s_d(x) \in \mathbb{Q}[x]$ has degree $6h(-d)$ and is therefore irreducible over $\mathbb{Q}$. Note that the $j$-invariants in Theorem 5.4 are algebraic integers, so by (5.3), the numbers $\xi$ are also always algebraic integers. Hence we can assume $s_d(x) \in \mathbb{Z}[x]$.

Now let $s_d^{(r)}(x)$ be the minimal polynomial of a pre-periodic point $\xi$ of level $r$ attached to the root $\alpha$ of $p_d(x)$, as before, with $s_d^{(2)}(x) = s_d(x)$. Then $s_d^{(r+1)}(x)$ is a
factor of the resultant $\text{Res}_y(s_d^{(r)}(y), g(x, y))$. On the other hand, the degree of this resultant is $3 \cdot \deg(s_d^{(r)}(x))$, so we see inductively that

$$\text{Res}_y(s_d^{(r)}(y), g(x, y)) = cr_{r+1}s_d^{(r+1)}(x), \quad r \geq 2.$$ 

Hence, all pre-periodic points of a given level $r \geq 1$ are conjugate over $\mathbb{Q}$, and this gives:

**Theorem 5.5.** All pre-periodic points $\xi \neq 3\omega, 3\omega^2$ of $T(z)$, such that $T^r(\xi)$ is a root of $p_d(x)$, $r \geq 1$, generate ring class fields over $K = \mathbb{Q}(\sqrt{-d})$ with conductors divisible by 3. Every ring class field over $K$ is generated by a periodic point or pre-periodic point of the function $T(z)$.

This theorem verifies the conjecture put forth in the introduction for the prime $p = 3$.

Remarkably, the polynomial $s_d(x)$ has real roots, even though all the roots of $p_d(x)$ are complex! Why is this true? The reason is that for some root $\alpha$ of $p_d(x)$, the quantity $\sigma_1(\alpha)$ is the complex conjugate $\bar{\alpha}$ of $\alpha$, and for this $\alpha$ the following relation holds:

$$\frac{(\omega \alpha + 6)^3}{\omega^2 \alpha^2 + 3\omega \alpha + 9} = \frac{(\omega^2 \bar{\alpha} + 6)^3}{\omega \bar{\alpha}^2 + 3\omega^2 \bar{\alpha} + 9}.$$ 

Therefore, at least one of the cube roots $\xi$ of this real quantity is real, as well, and this cube root satisfies the equation $g(\xi, \omega \alpha) = 0$, so that $T(\xi) = \omega \alpha$.

## 6 Aigner’s Conjecture and the rank of $E(\Sigma)$.

In this section I shall give two applications of the results obtained in sections 3 and 4. We first restrict our attention to the case when $f = 1$, so that $-d = d_K = \text{disc}(K/\mathbb{Q})$, and $\Omega_f = \Sigma$ is the Hilbert class field of $K$.

**Lemma 6.1.** Assume that $(\alpha, \beta)$ is a point on $Fer_3$ with $\alpha, \beta \neq 0, 3, \infty$ and $\alpha \neq \beta$. Let

$$P = (x, y) = \left( \frac{9\beta}{\alpha(\beta - 3)}, \frac{9\beta}{\beta - 3} \right)$$

and

$$Q = (x_1, y_1) = \left( \frac{9\alpha}{\beta(\alpha - 3)}, \frac{9\alpha}{\alpha - 3} \right)$$
be the points on $E$ corresponding to $(\alpha, \beta)$ and $(\beta, \alpha)$ on $Fer_3$. Then $P + Q = (3, 9)$.

**Proof.** We have the rational identity

$$-3 - x - x_1 + \left(\frac{y - y_1}{x - x_1}\right)^2 = \frac{3(2\alpha\beta - 3\alpha - 3\beta)(\alpha^3\beta^3 - 27\alpha^3 - 27\beta^3)}{(\alpha\beta - 3\alpha - 3\beta)^2\alpha\beta(\alpha - 3)(\beta - 3)}.$$

Since the resultant of $\alpha\beta - 3\alpha - 3\beta$ and $\alpha^3\beta^3 - 27\alpha^3 - 27\beta^3$ is $-243\alpha^4(\alpha - 3) \neq 0$, the denominator in the last expression is not zero, so the right hand side is zero. Hence, the $X$-coordinate of the sum $P + Q$ on $E$ is 3. The fact that the $Y$-coordinate of $P + Q$ is $Y = 9$ follows from the equation

$$9 - Y = \left(\frac{y - y_1}{x - x_1}\right)(3 - x) + y = \frac{-3\alpha\beta}{\alpha\beta - 3\alpha - 3\beta}\left(\frac{3(\alpha\beta - 3\alpha - 3\beta)}{\alpha(\beta - 3)}\right) + \frac{9\beta}{\beta - 3} = 0.$$

This proves the lemma. □

We apply Lemma 6.1 to the point

$$P_d = \left(\frac{9\beta}{\alpha(\beta - 3)}, \frac{9\beta}{\beta - 3}\right) = \left(\frac{\alpha^\tau + 6}{\alpha}, \frac{\alpha^\tau + 6}{\beta} \right)$$

in $E(\Sigma)$ whose coordinates are given in (4.2). By Proposition 3.2, the map $\phi$ defined by $\alpha^\phi = \sigma_1(\alpha^\tau) = \beta$ is an automorphism of $\Sigma$ of order 2 and therefore switches $\alpha$ and $\beta$. Lemma 6.1 implies that $P_d + P_\phi^d = (3, 9)$ and therefore

$$P_\phi^d = (3, 9) - P_d.$$

Letting $G = \text{Gal}(\Sigma/K)$, we have therefore that

$$P_d^{\sigma\phi} = P_d^{\phi\sigma^{-1}} = (3, 9) - P_d^{\sigma^{-1}}, \quad \sigma \in G,$$

and hence

$$\left(\sum_{\sigma \in G} P_d^{\sigma}\right)^{\phi} = \sum_{\sigma \in G} P_d^{\sigma\phi} = \sum_{\sigma \in G} (3, 9) - \sum_{\sigma \in G} P_d^{\sigma^{-1}} = [h(K)](3, 9) - \sum_{\sigma \in G} P_d^{\sigma},$$

where $h(K)$ is the class number of $K$. Hence, $Q_K = \sum_{\sigma \in G} P_d^{\sigma}$ satisfies
\[ Q^\phi_K = [h(K)](3, 9) - Q_K. \] (6.2)

(Cf. [5, eq. (8)].) Now if \( Q_K \) lies in \( E(\mathbb{Q}) \), then \( Q^\phi_K = Q_K \), and the last equation gives

\[ [2]Q_K = [2] \sum_{\sigma \in G} P^\sigma_d = [h(K)](3, 9). \]

By the doubling formula on the curve \( E \), if \( Q_K \neq O \) and \( x = x(Q_K) \), then either \( 4x^3 - 27 = 0 \) or

\[
\frac{x^4 + 54x}{4x^3 - 27} = 3 \Rightarrow (x - 3)(x^3 - 9x^2 - 27x - 27) = 0.
\]

Since both cubics \( 4x^3 - 27 \) and \( x^3 - 9x^2 - 27x - 27 \) are irreducible over \( \mathbb{Q} \) (both have roots which generate ramified extensions over \( p = 3 \)), it follows that

\[ Q_K \in E(\mathbb{Q}) \Rightarrow Q_K = [2h(K)](3, 9) = [h(K)](3, 0). \] (6.3)

In other words, \( Q_K \) is determined by the residue class of \( h(K) \) (mod 3).

Now let \( p \) be a prime divisor in \( \Sigma \) of \( \varphi_3 \), and consider the reduction of \( E \) mod \( p = \bar{E} \) taking \( P \) to \( P \) (mod \( p \)) = \( \bar{P} \). We have that

\[ \bar{E} : y^2 = x^3, \]

with singular point \( S = (0, 0) \) mod \( p \). The set \( \bar{E}_{ns} \) of non-singular points on \( \bar{E} \) forms a group isomorphic to \( k_p^+ = (R_{\Sigma}/p)^+ \), which is a vector space of dimension \( f(p/\varphi_3) \) over \( \mathbb{F}_3 \). Since the point \( S \) is a cusp and the tangent line to \( \bar{E} \) at \( S \) is the line \( y = 0 \), an isomorphism between \( \bar{E}_{ns} \) and \( k_p^+ \) is given by the map

\[ (x, y) \in \bar{E}_{ns} \rightarrow \frac{x}{\alpha} = \frac{1}{\alpha} \in k_p^+. \] (6.4)

(See [37, p. 56].) Furthermore, the set

\[ E_p(\Sigma) = \{ P \in E(\Sigma) : \bar{P} \in \bar{E}_{ns} \} \]

is a subgroup of \( E(\Sigma) \). Now the point \( P_d = (\frac{\alpha^2 + 6}{\alpha}, \alpha^2 + 6) \) has nonzero coordinates (mod \( p \)), since \( \alpha \) and therefore \( \alpha^2 \) have no prime divisors in common with \( \varphi_3 \), by
Theorem 3.7a) and the fact that $\tau = (\Sigma/K, \varphi_3)$ fixes $p$. Therefore, $\tilde{P}_d \neq S$ and hence $P_d \in E_p(\Sigma)$. Since the automorphisms $\sigma \in G$ permute the prime divisors of $\varphi_3$ among themselves, we also have $P_d^\sigma \in E_p(\Sigma)$, for $\sigma \in G$. Since $E_p(\Sigma)$ is a subgroup, the sum
\[ Q_K = \sum_{\sigma \in G} P_d^\sigma \in E_p(\Sigma). \quad (6.5) \]
But the reductions of the points $(3, 0)$ and $(3, 9)$ are $S$, so that $(3, 0), (3, 9) \notin E_p(\Sigma)$. Therefore $Q_K \neq (3, 0)$ or $(3, 9)$. Now (6.3) shows that $[3]Q_K \neq (0, 0)$ if the class number of $K$ is prime to 3.

**Theorem 6.2.** Aigner’s conjecture is true for the imaginary quadratic field $K$ if $\text{disc}(K/\mathbb{Q}) = -d \equiv 1 \pmod{3}$ and 3 does not divide the class number $h(K)$. In this case there is always a nontrivial solution to the cubic Fermat equation in $K$.

It is known that the relative density of quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ with $-d \equiv 1 \pmod{3}$ and $h(-d) \neq 0 \pmod{3}$ is at least $1/2$. (See [30, Thm. 1] and [6, Lemma 2.2].) In fact, there are 229 square-free integers $d_0 \equiv 2 \pmod{3}$ less than 1000, and if the discriminant of $\mathbb{Q}(\sqrt{-d_0})$ is $-d$, the class number $h(-d)$ is not divisible by 3 for 165 of these $d_0$. Thus, 3 divides $h(-d)$ for only $64/229 \approx 0.279$ of these discriminants. Theorem 6.2 shows that Aigner’s conjecture is true for infinitely many quadratic fields.

This result is a counterpart to the results of Fueter and Aigner for the first and second families of quadratic fields mentioned in the Introduction, since those results also require the class number of the imaginary quadratic field in question to be relatively prime to 3. Equation (6.3) shows furthermore that when $h(K) \equiv 0 \pmod{3}$, the point $Q_K \in E(K)$ can only be trivial if $Q_K = O$.

We can also apply the above argument to intermediate fields between $K$ and $\Sigma$. If $L$ is any intermediate field between $K$ and $\Sigma$ and $H$ is the corresponding subgroup of $G$ in the Galois correspondence, then the point
\[ Q_L = \sum_{\sigma \in H} P_d^\sigma \]
satisfies the identity
\[ Q_L^\phi = |H|(3, 9) - Q_L. \quad (6.6) \]

The same arguments used to prove Theorem 6.2 give the following result.
**Theorem 6.3.** Let $H$ be a subgroup of $G = \text{Gal}(\Sigma/K)$ whose order is not divisible by 3, and let $L$ be the subfield of $\Sigma$ corresponding to $H$ in the sense of Galois theory. Then the cubic Fermat equation has a nontrivial solution in the field $L$. Such a solution corresponds to the point $Q_L$ in $E(L)$ defined by $Q_L = \sum_{\sigma \in H} P_{d}^{\sigma}$.

This theorem allows us to prove the following result.

**Theorem 6.4.** Let $K = \mathbb{Q}(\sqrt{-d})$ with $-d \equiv 1 \pmod{3}$ and $3 \mid h(K)$, and let $d_1$ be the square-free part of $d$. Then there are infinitely many positive fundamental discriminants $D \equiv 1 \pmod{12d_1}$ for which the cubic Fermat equation has a nontrivial solution in the quartic field $L = \mathbb{Q}(\sqrt{-d}, \sqrt{D})$.

For the proof we require a lemma from Byeon’s paper [6].

**Lemma.** ([6, Prop. 3.1] ) Let $d_1$ be the square-free part of $d$. For any square-free integer $t$ there are infinitely many positive fundamental discriminants $D \equiv 1 \pmod{12d_1}$ with positive density for which the class numbers of the fields $K_1 = \mathbb{Q}(\sqrt{tD})$ and $K_2 = \mathbb{Q}(\sqrt{D})$ are not divisible by 3.

**Proof of Theorem 6.4.** Take $t$ in the lemma to be the square-free part of $d_K = -d$. Then for infinitely many fundamental discriminants $D \equiv 1 \pmod{12d_1}$ we have $h(-dD) \not\equiv 0 \pmod{3}$. Hence, Theorem 6.3 applies to the field $L = \mathbb{Q}(\sqrt{-d}, \sqrt{D})$, which is an intermediate field between $K_1 = \mathbb{Q}(\sqrt{-dD})$ and its genus field and is therefore contained in the Hilbert class field of $K_1$. We conclude that the point $Q_L$ is a nontrivial point in $E(L)$. □

Note that under the isomorphism between $\tilde{E}_{ns}$ and $k_p^+$ (for $p|\wp_3$) the point $\tilde{Q}_L = \sum_{\sigma \in H} \tilde{P}_{d}^{\sigma}$ maps to the residue class in $k_p^+$ of the element

$$\sum_{\sigma \in H} \frac{1}{\alpha^\sigma} = \text{Tr}_{\Sigma/L} \left( \frac{1}{\alpha} \right) \pmod{p}. \quad (6.7)$$

Thus $\tilde{Q}_L = \tilde{O}$ if and only if $p \mid \text{Tr}_{\Sigma/L}(1/\alpha)$. This gives the following criterion in the case that $h(K)$ is divisible by 3.

**Theorem 6.5.** If $3 \mid h(K)$ and the solution $(\alpha, \beta)$ of $Fer_3$ in the Hilbert class field $\Sigma$ of $K$ satisfies the condition

$$\text{Tr}_{\Sigma/K} \left( \frac{1}{\alpha} \right) \not\equiv 0 \pmod{\wp_3} \text{ in } K,$$
then \( Q_{K} \) is a nontrivial point in \( \text{Fer}_{3}(K) \).

From (4.26) the minimal polynomial \( m_{d}(x) \) of \( \alpha \) over \( K \) satisfies the congruence

\[
m_{d}(x) \equiv H_{-d}(x) \pmod{\wp_{3}}.
\]

Now if \( m_{d}(x) = x^{h} + \cdots + c_{1}x + c_{0} \), we have that \( Tr_{\Sigma/K}(1/\alpha) = -c_{1}/c_{0} \). Since 3 does not divide \( H_{-d}(0) \) (see the proof of Proposition 3.2), the above congruence gives

\[
Tr_{\Sigma/K}(1/\alpha) = -\frac{c_{1}}{c_{0}} \equiv -\frac{H_{-d}'(0)}{H_{-d}(0)} \pmod{\wp_{3}}.
\]

Using (4.27), this yields the following restatement of Theorem 6.5.

**Corollary of Theorem 6.5.** If 3 divides \( h(-d) \) but does not divide \( H_{-d}'(0) \), the cubic Fermat equation has a nontrivial solution in \( K = \mathbb{Q}(\sqrt{-d}) \). The condition \( H_{-d}'(0) \not\equiv 0 \pmod{3} \) is equivalent to the coefficient of \( x^{h(-d)+1} \) in \( p_{d}(x) \) not being divisible by 3.

For example, the discriminants \(-23, -59, -83\) satisfy the hypothesis of the corollary because \( h(-d) = 3 \) for each of these discriminants and

\[
\begin{align*}
p_{23}(x) & = x^{6} + 11x^{5} + 65x^{4} + 191x^{3} + 441x^{2} + 405x + 675, \\
p_{59}(x) & = x^{6} + 22x^{5} + 208x^{4} - 40x^{3} + 144x^{2} - 3456x + 6912, \\
p_{83}(x) & = x^{6} + 6x^{5} + 560x^{4} - 1384x^{3} + 576x^{2} - 12960x + 43200.
\end{align*}
\]

Thus, there is a nontrivial solution of \( \text{Fer}_{3} \) in each of the fields \( \mathbb{Q}(\sqrt{-23}), \mathbb{Q}(\sqrt{-59}), \) and \( \mathbb{Q}(\sqrt{-83}) \). The discriminant \(-d = -107\) does not satisfy this condition, since

\[
p_{107}(x) = x^{6} - 74x^{5} + 1680x^{4} - 6184x^{3} + 2736x^{2} - 43200x + 172800;
\]

nonetheless, there is still a nontrivial solution of \( \text{Fer}_{3} \) in \( K = \mathbb{Q}(\sqrt{-107}) \). There are several ways of verifying this, but here is one way. Since \( 29 = (9 + 107)/4 \), the prime \( p = 29 \) splits completely in the Hilbert class field \( \Sigma \) of \( K \), and for the prime ideal divisor \( \wp_{29} = \left(29, \frac{-3 + \sqrt{-107}}{2}\right) \) of 29 in \( R_{K} \) we have

\[
m_{107}(x) = x^{3} - (37 - \sqrt{-107})x^{2} + (102 + 6\sqrt{-107})x + 40 - 40\sqrt{-107} \\
\equiv (x + 2)(x + 7)(x + 15) \pmod{\wp_{29}}.
\]
Hence, converting the points $(-2, -13), (-7, 15), (-15, 9)$ on $\text{Fer}_3(\mathbb{F}_{29})$ to points on $E(\mathbb{F}_{29})$ (using (4.0)) gives that

$$Q_K \equiv (19, 20) + (16, 4) + (2, 28) \equiv (10, 19) \pmod{\wp_{29}}.$$ 

Since $(10, 19)$ is not the base point on $E(\mathbb{F}_{29})$, this shows that $Q_K \neq O$ on $E(K)$. Therefore, $Q_K \in E(K)$ is nontrivial.

These computations and the factorization of the iterated resultant $R_3(x)$ in Section 4 show that $\text{Fer}_3$ has a nontrivial solution in all of the fields $K = \mathbb{Q}(\sqrt{-d})$ for which $-d \equiv 1 \pmod{3}$ and $h(K) = 3$. Using the formal group of the elliptic curve $E$ in (4.1) it can be shown in a similar way that Aigner’s conjecture is true for all 39 of the fields $K$ of this type for which $h(K) = 3, 6, 9$ or 12. For the sake of brevity the details will not be given here. Based on these results I put forward the following conjecture.

**Conjecture.** If $Q_K$ is the point in (6.5), then for any quadratic field $K = \mathbb{Q}(\sqrt{-d})$ of the fourth family, $Q_K$ is a point of infinite order on the elliptic curve $E$ in (4.1), defined over $K$.

We finish this section by proving the following theorem. Here we consider the solutions $(\alpha, \beta)$ in ring class fields $\Omega_f$ with $(f, 3) = 1$.

**Theorem 6.6.** Let $p$ be a prime divisor of $\wp_3$ in the ring class field $\Omega_f$ of $K$ (with $(f, 3) = 1$) and let

$$\ell = \dim_{\mathbb{F}_3}\left\langle \frac{1}{\alpha^\sigma} \pmod{p} \right\rangle, \quad \sigma \in G, \quad G = \text{Gal}(\Omega_f/K),$$

be the dimension of the vector space generated by the residue classes of the numbers $1/\alpha^\sigma$ in $R_{\Omega_f}/p = \mathbb{F}_{3^\ell}$, where $\alpha$ is the number defined in Theorem 1. Then the rank of $\text{Fer}_3$ over the ring class field $\Omega_f$ is at least $\ell$. In particular, the rank of $\text{Fer}_3$ over the Hilbert class field $\Sigma$ is always at least 1.

**Proof.** Let $\{1/\alpha^\sigma | \sigma \in S \subseteq G\}$ be a maximal set of linearly independent conjugates of $1/\alpha$ over $\mathbb{F}_3$. I claim that the corresponding set $\{P_d^\sigma | \sigma \in S\}$ is a set of independent points in $E(\Omega_f)$. Suppose that $\sum_{\sigma \in S} c_\sigma P_d^\sigma = O$, for some integers $c_\sigma$. We then have

$$\sum_{\sigma \in S} c_\sigma P_d^\sigma = \hat{O} \in R_{\Omega_f}/p.$$ 

By the isomorphism (6.4), this implies that

$$\sum_{\sigma \in S} c_\sigma \frac{1}{\alpha^\sigma} \equiv 0 \pmod{p} \quad \text{in} \quad R_{\Omega_f}/p.$$ 

50
It follows that $3|c_σ$ for all $σ \in S$. Hence, the sum
\[ \sum_{σ \in S} \left( \frac{c_σ}{3} \right) P_σ^ε \]
is a point of order 1 or 3 in $E(Ω_f)$. But the only points of order 3 in $E(Ω_f)$ are $(3,0)$ and $(3,9)$, since $E[3]$ is elementary abelian of order 9 and contains the points $(3ω,0),(3ω,9)$. Since the sum in (6.8) lies in $E_p(Ω_f)$, with the same notation as above, it follows that
\[ \sum_{σ \in S} \left( \frac{c_σ}{3} \right) P_σ^ε = O. \]

This argument can be repeated indefinitely if some $c_σ \neq 0$, giving a contradiction. Hence the points $P_σ^ε$, $σ \in S$, are independent and they generate a subgroup of $E(Ω_f)$ of rank $ℓ$. □

**Corollary.** If $D_n$ is defined as in Section 4, then for at least one discriminant $−d = d_Kf^2 ∈ D_n$, the rank of $Fer_3(Ω_f)$ is at least $n$. Thus, the rank of $Fer_3(Ω_f)$ is unbounded over ring class fields $Ω_f$ of imaginary quadratic fields $K$ of the fourth family.

*Proof.* By Corollary 2 of Theorem 4.2, there is at least one value of $−d ∈ D_n$ and an irreducible $f(x) ∈ \mathbb{F}_3[x]$ of degree $n$ dividing $H_{−d}(x)$ (mod 3) for which the reciprocal $1/α$ of a root of $f(x)$ generates a normal basis of $\mathbb{F}_3^n$ over $\mathbb{F}_3$. For this $d$, $ℓ = n$ in Theorem 6.5. This proves the corollary. □

An easy computation shows that the only cubics in $\mathbb{F}_3[x]$ for which $1/α$ does not generate a normal basis over $\mathbb{F}_3$ are $f(x) = x^3+x^2+2, x^3+2x^2+1$. Hence, the rank of $Fer_3(Σ)$ is at least 3 for each of the discriminants in the set $\{-23, -59, -83, -104\}$.

### 7 The example $d = 4 \cdot 17$.

For $K = \mathbb{Q}(\sqrt{−17})$, with $−d = −68$, $α$ and $β$ are roots of
\[ p_{68}(x) = x^8 − 30x^7 + 390x^6 − 908x^5 + 1640x^4 − 24360x^3 + 43416x^2 + 36720x + 550800. \]

This polynomial divides the iterated resultant $R_4(x)$ in (4.16). We work with the factor $q_{68}(x)$ of $p_{68}(3 + x^3)$ given by
\[ q_{68}(x) = x^8 − 6x^7 + 9x^6 + 16x^5 − 64x^4 + 48x^3 + 81x^2 − 162x + 81, \]

51
whose discriminant is \( \text{disc}(q_{68}(x)) = 2^{12}3^{12}5^417^4 \). Transforming by the map \( z = x + \frac{3}{x} \) gives the polynomial

\[
r_{68}(z) = z^4 - 6z^3 - 3z^2 + 70z - 100, \quad \text{disc}(r_{68}(z)) = -2^45^217^2.
\]

This polynomial has the dihedral group \( D_4 \) as its Galois group, so \( q_{68}(x) \) is indeed a normal polynomial. Factoring \( q_{68}(x) \) modulo 3 and 5 shows that neither of these primes is ramified in the splitting field \( \Sigma = \Omega_1 \). The mod 3 factorization shows that \( p_3 = (3, \gamma^4 + \gamma + 2) \) is a prime divisor of 3 with degree 4 over \( \mathbb{Q} \), where \( \gamma \) is a root of \( q_{68}(x) = 0 \). Factoring mod 2 shows that the prime divisors of 2 in \( \Sigma \) have inertial degree \( \geq 2 \) over \( \mathbb{Q} \).

Over \( K = \mathbb{Q}(\sqrt{-17}) \) the polynomial \( q_{68}(x) \) factors as

\[
f_1f_2 = (x^4 - 3x^3 + (8 - \sqrt{-17})x - 8 + \sqrt{-17}) \times (x^4 - 3x^3 + (8 + \sqrt{-17})x - 8 - \sqrt{-17}).
\]

Further, \( f_2 \) factors over \( \Omega = \mathbb{Q}(\sqrt{-17}, \sqrt{-1}) \) as \( f_2 = f_3f_4 \), where

\[
f_3 = x^2 + \left(\frac{-3 - 2\sqrt{-1} + \sqrt{17}}{2}\right)x + \frac{(1 - \sqrt{-1})(1 - \sqrt{-17})}{2},
\]

and

\[
D = \text{disc}(f_3) = \frac{7 + 10\sqrt{-1} + \sqrt{17} + 2\sqrt{-17}}{2}.
\]

Thus, \( \Omega \subset \Sigma \) and since \( \Omega/K \) is unramified, the relative degrees of the prime divisors of 2 in the extension \( \Sigma/\Omega \) must be 2 (note that 2 splits in \( \mathbb{Q}(\sqrt{17}) \); so if \( (2) = \wp_2^2 \) in \( K \), then \( \wp_2 \) splits in \( \Omega \)). This shows that the prime divisors of 2 are unramified in \( \Sigma/K \), and it follows from \( h(K) = 4 \) that \( \Sigma \) is indeed the Hilbert class field of \( K \). We take \( \gamma \) to be a root of \( f_3 \), so that

\[
\gamma = \frac{1}{4}(3 + 2\sqrt{-1} - \sqrt{17}) + \frac{1}{2}\sqrt{D} = \frac{1}{4}(3 + 2\sqrt{-1} - \sqrt{17}) + \frac{1}{4}\sqrt{14 + 20\sqrt{-1} + 2\sqrt{17} + 4\sqrt{-17}} = \frac{1}{4}(3 + 2\sqrt{-1} - \sqrt{17}) + \frac{1}{16}(3 + 4\sqrt{-1} + \sqrt{17})\Theta,
\]

52
where $\Theta = \sqrt{2 + 2\sqrt{17}}$. We have $N_{\Sigma/\Omega}(\gamma) = \frac{(1 - \sqrt{-1})(1 - \sqrt{-17})}{2}$ and $N_{\Sigma/K}(\gamma) = -8 - \sqrt{-17} \cong (\varphi_3)^4$, with $\varphi_3 = (3, -8 + \sqrt{-17}) = (3, 1 + \sqrt{-17})$ in $K$ and $p_3 = R_{\Sigma} \varphi_3$. (Also note that as a complex number $|\gamma| = \sqrt{3}$.)

Now we take $\alpha = 3 + \gamma^3$, so that

$$\alpha = \frac{15 + 13\sqrt{-1} - 5\sqrt{17} - 3\sqrt{-17}}{4} - \frac{8 - 11\sqrt{-1} - 2\sqrt{17} + \sqrt{-17}}{8} \Theta.$$ 

A root $\beta$ of $\beta^3 = 27\alpha^3/(\alpha^3 - 27)$ is given by

$$\beta = \frac{1}{4}(15 + 13\sqrt{-1} + 5\sqrt{17} + 3\sqrt{-17}) - \frac{1}{16}(3 + 13\sqrt{-1} + 5\sqrt{17} + 3\sqrt{-17})\Theta = \frac{1}{4}(15 + 13\sqrt{-1} + 5\sqrt{17} + 3\sqrt{-17}) - \frac{1}{8}(8 - 11\sqrt{-1} + 2\sqrt{17} - \sqrt{-17})\Theta',$$

where $\Theta' = \sqrt{2 - 2\sqrt{17}} = \frac{8\sqrt{-1}}{6}$ (with positive imaginary part). The expressions for $\alpha$ and $\beta$ make it clear that $\alpha$ and $\beta$ are indeed algebraic conjugates over $\mathbb{Q}$ (but not complex conjugates of each other).

Using Proposition 3.2, $\alpha^\tau$ is given by

$$\alpha^\tau = \frac{15 - 13\sqrt{-1} + 5\sqrt{17} - 3\sqrt{-17}}{4} - \frac{3 - 13\sqrt{-1} + 5\sqrt{17} - 3\sqrt{-17}}{16} \Theta = \frac{15 - 13\sqrt{-1} + 5\sqrt{17} - 3\sqrt{-17}}{4} - \frac{8 + 11\sqrt{-1} + 2\sqrt{17} + \sqrt{-17}}{8} \Theta',$$

Thus, $\tau$ is the automorphism $\tau = (\sqrt{-1} \rightarrow -\sqrt{-1}, \sqrt{17} \rightarrow -\sqrt{17}, \Theta \rightarrow \Theta')$, a generating automorphism of $\Sigma/K$, in agreement with the fact that the ideal $p_3$ has degree 4 over $K$.

With this information we compute an explicit solution to the cubic Fermat equation in $K = \mathbb{Q}(\sqrt{-17})$. Using $P_{68} = ((\alpha^\tau + 6)/\alpha, \alpha^\tau + 6)$ from (4.2), we compute

$$P_{68} = \left(\frac{-3 - \sqrt{-1} - \sqrt{17} + 11 + 6\sqrt{-1} + 3\sqrt{17} + 2\sqrt{-17}}{2}\Theta, \frac{39 - 13\sqrt{-1} + 5\sqrt{17} - 3\sqrt{-17} + 3 - 13\sqrt{-1} + 5\sqrt{17} - 3\sqrt{-17}}{4}\Theta\right).$$
Acting on $P_{68}$ with $\tau^2 = (\Theta \rightarrow -\Theta)$, the non-trivial automorphism of $\Sigma/K(\sqrt{-1})$, we find that
$$Q_\Omega = P_{68} + P_{68}^{\tau^2} = (9 - 10\sqrt{-1} - \sqrt{17} + 3\sqrt{-17}, -1 + 62\sqrt{-1} - \sqrt{17} - 17\sqrt{-17}).$$

Letting $\sigma = \tau|_{K(\sqrt{-1})}$ be the nontrivial automorphism of $K(\sqrt{-1})/K$, we find further that
$$Q_K = Q_\Omega + Q_\Omega^\sigma = \left(\frac{359 + 58\sqrt{-17}}{169}, \frac{5180 - 2030\sqrt{-17}}{2197}\right) \quad (7.1)$$
is a nontrivial solution of (4.1) in $K$. This also shows that the elliptic curve $E$ in (4.1) has at least $14 = 8 + 2 + 4$ integral points in $\Sigma$, since $Q_\Omega$ and its conjugates have integral coordinates.

The solution of $Fer_3$ corresponding to (7.1) is the solution
$$(X, Y) = \left(\frac{-280 - 2030\sqrt{-17}}{4771}, \frac{-280 + 2030\sqrt{-17}}{4771}\right).$$

This gives the integral solution
$$(-4 + 29\sqrt{-17})^3 + (-4 - 29\sqrt{-17})^3 = 70^3$$
of $F : x^3 + y^3 = z^3$.

Exactly the same process can be applied to find a nontrivial point on $E$ with coordinates in the real quadratic field $\tilde{K} = \mathbb{Q}(\sqrt{17})$. This time we take $\psi$ to be complex conjugation and we compute
$$Q_{\tilde{K}} = Q_\Omega + Q_\Omega^\psi = \left(\frac{14799 - 2286\sqrt{17}}{2809}, \frac{-1242540 + 445770\sqrt{17}}{148877}\right).$$

This leads to the solution
$$(\alpha, \beta) = \left(\frac{-42120 + 148590\sqrt{17}}{272897}, \frac{-42120 - 148590\sqrt{17}}{272897}\right)$$
on $Fer_3$, and to the solution
$$(36 + 127\sqrt{17})^3 + (36 - 127\sqrt{17})^3 = 390^3$$
on $F$. This is one of the solutions listed by Aigner in [aig1, p.251].

54
8 References

[1] A. Aigner, Weitere Ergebnisse über $x^3 + y^3 = z^3$ in quadratischen Körpern, Monatshefte für Mathematik 56 (1952), 240-252.

[2] A. Aigner, Ein zweiter Fall der Unmöglichkeit von $x^3 + y^3 = z^3$ in quadratischen Körpern mit durch 3 teilbarer Klassenzahl, Monatshefte für Mathematik 56 (1952), 335-338.

[3] A. Aigner, Die kubische Fermatgleichung in quadratischen Körpern, J. reine angew. Math. 195 (1955), 3-17.

[4] A. Aigner, Unmöglichkeitskernzahlen der kubischen Fermatgleichung mit Primfaktoren der Art $3n + 1$, J. reine angew. Math. 195 (1955), 175-179.

[5] B. J. Birch and N. M. Stephens, Computation of Heegner points, ch. 1 of Modular Forms, R. A. Rankin, ed., Ellis Horwood Limited, Chichester, England, 1984, pp. 13-41.

[6] D. Byeon, Class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-D})$, Proc. Amer. Math. Soc. 132 (2004), 3137-3140.

[7] H. Cohn, Iterated Ring Class Fields and the Icosahedron, Mathematische Annalen 255 (1981), 107-122.

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

[9] J.E. Cremona, Algorithms for Elliptic Modular Curves, Cambridge University Press, 1992.

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

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

[12] M. Deuring, Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung, Commentarii math. Helvetici 19 (1946), 74-82.

[13] M. Deuring, Die Klassenkörper der komplexen Multiplikation, Enzyklopädie der math. Wissenschaften I2, 23 (1958), 1-60.

[14] W. Franz, Die Teilwerte der Weberschen Tau-Funktion, J. reine angew. Math. 173 (1935), 60-64.
[15] R. Fricke, *Lehrbuch der Algebra*, II, III, Vieweg, Braunschweig, 1928.

[16] R. Fueter, Über kubische diophantische Gleichungen, Commentarii Math. Helvetici 2(1930), 69-89.

[17] H. Hasse, Neue Begründung der komplexen Multiplikation. I. Einordnung in die allgemeine Klassenkörpertheorie, J. reine angew. Math. 157 (1927), 115-139; paper 33 in *Mathematische Abhandlungen*, Bd. 2, Walter de Gruyter, Berlin, 1975, pp. 3-27.

[18] H. Hasse, Zum Hauptidealsatz der komplexen Multiplikation, Monatshefte für Math. u. Physik 38 (1931), 315-322; paper 35 in *Mathematische Abhandlungen*, Bd. 2, Walter de Gruyter, Berlin, 1975, pp. 53-60.

[19] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg, 1933.

[20] H. Hasse, *Number Theory*, Springer, Berlin, 2002.

[21] M. Jones and J. Rouse, Solutions of the cubic Fermat equation in quadratic fields, Intl. J. Number Theory 9 (2013), 1579-1591.

[22] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer, New York, 1981.

[23] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, Mass., 1973.

[24] R. Lynch and P. Morton, The quartic Fermat equation in Hilbert class fields of imaginary quadratic fields, http://arxiv.org/abs/1410.3008, to appear in Intl. J. Number Theory.

[25] D. Mirimanoff, Racines cubiques de nombres entiers et multiplication complexe dans les fonctions elliptiques, Mathematische Annalen 56 (1903), 115-128.

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

[27] P. Morton, Explicit congruences for class equations, Functiones et Approximatio Commentarii Mathematici 51 (2014), 77-110.

[28] P. Morton, Supersingular parameters of the Deuring normal form, Ramanujan Journal of Math 33 (2014), 339-366.

[29] P. Morton, Solutions of diophantine equations as periodic points of $p$-adic algebraic functions I, http://arxiv.org/abs/1410.4618, submitted.

[30] J. Nakagawa and K. Horie, Elliptic curves with no rational points, Proc. Amer. Math. Soc. 104 (1988), 20-24.
[31] M. Ram Murty, *Introduction to $p$-adic Analytic Number Theory*, AMS/IP Studies in Advanced Mathematics, vol. 27, American Math. Soc. and International Press, Providence, 2002.

[32] P. Ribenboim, *13 Lectures on Fermat’s Last Theorem*, Springer, New York, 1979.

[33] R. Schertz, Die singulären Werte der Weberschen Funktionen $f$, $f_1$, $f_2$, $\gamma_2$, $\gamma_3$, J. reine angew. Math. 286/287 (1976), 46-74.

[34] R. Schertz, Weber’s class invariants revisited, J. de Théorie de Nombres de Bordeaux 14 (2002), 325-343.

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

[36] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, in: Graduate Texts in Mathematics, vol. 151, Springer, New York, 1994.

[37] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, in: Graduate Texts in Mathematics, vol. 106, Springer, New York, 2009.

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

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