Solutions of diophantine equations as periodic points of p-adic algebraic functions, I

Patrick Morton

Abstract

Solutions of the quartic Fermat equation in ring class fields of odd conductor over quadratic fields $K = \mathbb{Q}(\sqrt{-d})$ with $-d \equiv 1 \pmod 8$ are shown to be periodic points of a fixed algebraic function $T(z)$ defined on the punctured disk $0 < |z|_2 \le \frac{1}{2}$ of the maximal unramified, algebraic extension K_2 of the 2-adic field $\mathbb{Q}_2$. All ring class fields of odd conductor over imaginary quadratic fields in which the prime $p = 2$ splits are shown to be generated by complex periodic points of the algebraic function T, and conversely, all but two of the periodic points of T generate ring class fields over suitable imaginary quadratic fields. This gives a dynamical proof of a class number relation originally proved by Deuring. It is conjectured that a similar situation holds for an arbitrary prime p in place of $p = 2$, where the case $p = 3$ has been previously proved by the author, and the case $p = 5$ will be handled in Part II.

1 Introduction.

In this paper and its sequel it will be shown that the periodic points of an algebraic function, suitably defined, have, in several particularly interesting cases, number theoretic significance. I shall primarily consider algebraic functions defined on subsets of $\mathfrak{p}$-adic fields.

An important problem in algebraic number theory is to classify the finite extensions L of an algebraic number field K for which $\mathrm{Gal}(L/K)$ is abelian. These are the *abelian extensions* of K, and for certain fields K we have a good understanding of how to find explicit generators for these extensions. For example, a famous theorem known as the Kronecker-Weber Theorem says that all abelian extensions of the rational field $K = \mathbb{Q}$ are subfields of cyclotomic fields $\mathbb{Q}(\zeta_f)$, where ζ_f is a primitive

f-th root of unity with $f \geq 3$. In the case that $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic extension of $\mathbb{Q}$, the abelian extensions of K are known to be subfields of *ray class fields*, where the latter fields are generated over K by the coordinates of torsion points on elliptic curves E whose endomorphism rings are isomorphic to certain subrings (orders) of K (see [h1] and [si]). Such a curve is said to have complex multiplication by the subring $\mathsf{R} \subset R_K$, where R_K is the ring of algebraic integers contained in K, if $\text{End}_{\overline{\mathbb{Q}}}(E) \cong \mathsf{R}$ and $\mathbb{Z} \subsetneq \mathsf{R}$. There is an important subclass of these abelian extensions known as *ring class fields*, which are generated over K by the j-invariants $j(E)$ of elliptic curves E with complex multiplication by orders contained in K. The properties of ring class fields are developed in the classical theory of complex multiplication, which is the main focus of the book by Cox [co1].

In class field theory (see [ch], [d3], or [h1]), the ring class fields over K are characterized as follows. If f is a positive integer, the ring class field (mod f) of $K = \mathbb{Q}(\sqrt{-d})$, denoted by Ω_f, is the unique abelian extension of K having the property that the prime ideals $\mathfrak{p}$ (not dividing 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_{Ω_f} of Ω_f, are exactly those $\mathfrak{p}$ for which $\mathfrak{p} = (\xi)$ is principal in R_K with $\xi \equiv r$ (mod f) and $r \in \mathbb{Z}$. It follows from class field theory 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 (ξ) for numbers $\xi \equiv r$ (mod f) and $r \in \mathbb{Z}$. The set of all such integers ξ of R_K is a ring R_{-d}, which gives rise to the name *ring class field*. If d_K is the discriminant of K, the integer $-d = d_K f^2$ is called the discriminant of the ring (order) R_{-d}. In [co1, pp. 190-192] it is shown that the subfields of the fields Ω_f are exactly the abelian extensions L of K for which $\text{Gal}(L/\mathbb{Q})$ is a generalized dihedral group.

Let K_p be the maximal unramified, algebraic extension of the p-adic field $\mathbb{Q}_p$. Call an imaginary quadratic field K 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. If K is p-admissible, then its discriminant is a square in $\mathbb{Q}_p$, and K can therefore be embedded in $\mathbb{Q}_p$. Moreover, if $p \nmid f$, then Ω_f/K is unramified at p and can also be embedded in K_p. My goal in this paper is to prove a special case of the following conjecture, which was stated in [m3].

Conjecture 1. *Let p be a fixed prime number. There is an algebraic function $T_p(z)$, defined on a certain subset $\mathsf{D}_p \subseteq \mathsf{K}_p$ of the maximal unramified, algebraic extension of $\mathbb{Q}_p$, such that $T_p(\mathsf{D}_p) \subseteq \mathsf{D}_p$, with the following properties:*

(a) *Any ring class field $\Omega_f \subset \mathsf{K}_p$ of a p-admissible field $K \subset \mathbb{Q}_p$, whose conductor f*

is relatively prime to p, is generated over K by a periodic point ξ of $T_p(z)$ contained in D_p;
(b) *All but finitely many periodic points ξ of $T_p(z)$ contained in $\overline{\mathbb{Q}}_p$ generate ring class fields $\Omega_f = K(\xi)$ over some p-admissible quadratic field K.*

The situation referred to in this conjecture is analogous to the fact that the fields $\mathbb{Q}(\zeta_f)$, where ζ_f is a primitive f-th root of unity and $(f,p) = 1$, are generated over $\mathbb{Q}$ by periodic points of the map $F(z) = z^p$. In fact, ζ_f is a periodic point of $F(z)$ with period n, where n is the order of the prime p modulo f. Furthermore, the fields $\mathbb{Q}(\zeta_{p^k f})$ are generated over $\mathbb{Q}$ by *pre-periodic* points of $F(z)$, since $\zeta_{p^k f}$ is a root of $F^{k+n}(z) - F^k(z) = 0$, for the same value of n.

An algebraic function $T_3(z)$ satisfying Conjecture 1 for the prime $p = 3$ was given in [m3], namely

$$T_3(z) = \frac{z^2}{3}(z^3-27)^{1/3} + \frac{z}{3}(z^3-27)^{2/3} + \frac{z^3}{3} - 6, \quad \text{for } z \in \mathsf{K}_3, \ |z|_3 \ge 1,$$

where $T_3(z)$ is defined using the binomial series. The periodic points of the function $T_3(z)$ in its 3-adic domain were shown to be solutions of the cubic Fermat equation in ring class fields Ω_f over 3-admissible quadratic fields $K = \mathbb{Q}(\sqrt{-d})$, whose conductors f are prime to 3. Furthermore, every such Ω_f is generated over $\mathbb{Q}$ by one of these periodic points.

In this paper I will show that a certain 2-adic branch of the function

$$T(z) = \frac{\sqrt[4]{1-z^4}+1}{\sqrt[4]{1-z^4}-1} = 1 - \frac{2}{z^4}\left(1 + (1-z^4)^{1/4} + (1-z^4)^{1/2} + (1-z^4)^{3/4}\right)$$

satisfies the statement of the above conjecture for the prime $p = 2$. I will show that all of the periodic points of $T(z)$ in its 2-adic domain $\mathsf{D}_2 = \{z : 0 < |z|_2 \le \frac{1}{2}\} \subset \mathsf{K}_2$ are solutions of the quartic Fermat equation in ring class fields of 2-admissible quadratic fields. These solutions have been given in [lm] as follows. Though the precise formulas are not necessary for the proofs in this paper, it is worth noting that these solutions can be represented in terms of modular functions.

Let $\eta(\tau)$ be the Dedekind η-function [co1, p. 256]. The Schläfli functions $\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau)$ (see [sch, p. 148] or [co1, p. 256]) are defined to be:

$$\mathfrak{f}(\tau) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}, \quad \mathfrak{f}_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}, \quad \mathfrak{f}_2(\tau) = \sqrt{2}\, \frac{\eta(2\tau)}{\eta(\tau)}.$$

These functions have the infinite product representations

$$\mathfrak{f}(\tau) = q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1 + q^{n-\frac{1}{2}}), \quad \mathfrak{f}_1(\tau) = q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1 - q^{n-\frac{1}{2}}),$$

$$\mathfrak{f}_2(\tau) = \sqrt{2}\, q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 + q^n), \quad q = e^{2\pi i \tau},$$

convergent on the upper half-plane $\mathbb{H}$. Let $K = \mathbb{Q}(\sqrt{-d})$ be a 2-admissible quadratic field, where $-d \equiv 1 \pmod 8$ is the discriminant of the order R_{-d} in K, with conductor f, satisfying $-d = d_K f^2$. Further, let $w \in K$ be defined by

$$w = \frac{v + \sqrt{-d}}{2}, \quad v^2 \equiv -d \pmod{16}, \quad v = 1 \text{ or } 3,$$

and set

$$a \equiv \begin{cases} \frac{-3d+5}{16} \pmod 4, & \text{if } v = 3 \text{ and } d \equiv 7 \pmod{16}, \\ \frac{-d+31}{16} \pmod 4, & \text{if } v = 1 \text{ and } d \equiv 15 \pmod{16}. \end{cases}$$

Then the numbers

$$\pi_d = i^a \frac{\mathfrak{f}_2(w/2)^2}{\mathfrak{f}(w/2)^2}, \quad \xi_d = \frac{\beta}{2} = i^{-v} \frac{\mathfrak{f}_1(w/2)^2}{\mathfrak{f}(w/2)^2} \tag{1}$$

lie in the ring class field Ω_f of conductor f over K, and satisfy

$$\pi_d^4 + \xi_d^4 = 1.$$

(See [lm, Sec. 10].) The numbers π_d and ξ_d are conjugate algebraic integers over $\mathbb{Q}$ and Ω_f is generated over $\mathbb{Q}$ by either of them. Furthermore, if $\wp_2 = (2, w)$ is one of the prime ideal divisors of 2 in K, then with $(2) = 2R_K = \wp_2 \wp_2'$, we have

$$(\pi_d) = \pi_d R_{\Omega_f} = \wp_2 R_{\Omega_f}, \quad (\xi_d) = \xi_d R_{\Omega_f} = \wp_2' R_{\Omega_f}, \text{ in } \Omega_f,$$

where R_L denotes the ring of algebraic integers in the field L. In other words, π_d and ξ_d are principal ideal generators in R_{Ω_f} of the prime ideal divisors of 2 in R_K, when those ideals are extended to the larger ring R_{Ω_f}.

Denote by $b_d(x)$ the minimal polynomial over $\mathbb{Q}$ of the numbers π_d and ξ_d. Then $b_d(x)$ is a normal polynomial over $\mathbb{Q}$ (meaning that one of its roots generates a normal extension of $\mathbb{Q}$) and

$$\deg(b_d(x)) = 2h(-d),$$

where $h(-d) = |A_f/P_f|$ is the class number of the order R_{-d}, i.e. the number of elements of the ideal class group of R_{-d}. See [co1, pp. 132-148]; and see Section 6 for some examples of these polynomials.

To explicitly define the branch of $T(z)$ that we will be considering, let

$$T_1(z) = \frac{2z^4 - 4 - 4\sqrt{1-z^4}}{z^4}, \quad T_2(z) = \frac{z}{2} - \frac{z}{2}\sqrt{1 - \frac{4}{z^2}},$$

where the square-roots are defined 2-adically by the binomial series. We have:

Theorem 1. *a) The function $T(z) = T_2 \circ T_1(z)$ maps the set*

$$\mathsf{D}_2 = \{z : 0 < |z|_2 \le \frac{1}{2}\} \subset \mathsf{K}_2$$

to itself.

b) The periodic points of $T(z)$ in D_2 are the roots ξ_d of the polynomials $b_d(x)$, as $-d$ varies over quadratic discriminants $\equiv 1$ (mod 8), along with the conjugates of ξ_d over $K = \mathbb{Q}(\sqrt{-d})$, under the natural embedding of Ω_f in its completion $(\Omega_f)_{\mathfrak{p}} \subset \mathsf{K}_2$, for a prime ideal $\mathfrak{p}$ of R_{Ω_f} which divides $\wp_2'$.

c) The number of periodic points of $T(z)$ in the domain D_2 with minimal period n is given by

$$\sum_{-d \in \mathfrak{D}_n} h(-d) = nN_4(n) = \sum_{k|n} \mu(n/k) 2^{2k}, \quad n > 1.$$

Here $\mathfrak{D}_n$ is the set of discriminants $-d \equiv 1$ (mod 8) for which the square of the corresponding Frobenius auotmorphism $\tau = \left(\frac{\Omega_f/K}{\wp_2}\right)$ has order n in $Gal(\Omega_f/K)$, and μ is the Möbius μ-function. For $n = 1$, the number of fixed points of $T(z)$ in D_2 is

$$\sum_{-d \in \mathfrak{D}_1} h(-d) = h(-7) + h(-15) = 4 - 1.$$

Thus, our analysis gives a dynamical interpretation of the class number formula occurring in part c), which is equivalent to a special case of a class number formula of Deuring [d1], [d2, Eq. (1)]. As in [m3], the proof implies a similar statement about the periodic points of the multi-valued function $T(z)$ on either of the fields $\overline{\mathbb{Q}}_2$ or $\mathbb{C}$. For this it is necessary to define what we mean by a periodic point of a multi-valued algebraic function.

Let $f(z)$ be any algebraic function defined over a given field F, so that $f(z)$ lies in the algebraic closure $\overline{F(z)}$ of $F(z)$, and let $g(z, w) \in F[z, w]$ be the minimal polynomial of $w = f(z)$ over $F(z)$. Define a periodic point a over F of the algebraic function $f(z)$ to be any number $a \in F$ for which there exist $a_1, a_2, \cdots, a_{n-1} \in F$ for which

$$g(a, a_1) = g(a_1, a_2) = \cdots = g(a_{n-2}, a_{n-1}) = g(a_{n-1}, a) = 0.$$

By cyclically permuting the equations in the definition it is clear that all the numbers a_i are also periodic points of $f(z)$ of period n. Thus, when writing $f(a_{i-1}) = a_i$, each individual element $a_i = f_i(a_{i-1})$ will be defined using one particular branch $f_i(z)$ of $f(z)$, for $1 \le i \le n$ (taking $a_0 = a_n = a$), and different branches f_i, f_j may or may not coincide. With this definition we have the following.

Theorem 2. *The set of periodic points of the multi-valued function $T(z)$ on any of the fields $\mathcal{K} = \mathsf{K}_2$, $\overline{\mathbb{Q}}_2$ or $\mathbb{C}$ coincides with the set*

$$\mathcal{S}(\mathcal{K}) = \{0, -1\} \cup \{\xi \in \mathcal{K} : (\exists n \ge 1)(\exists\ (-d) \in \mathfrak{D}_n) \text{ s.t. } b_d(\xi) = 0\}.$$

Thus, all the periodic points of $T(z)$ distinct from 0 and -1 in any of these fields generate ring class fields over 2-admissible quadratic extensions of $\mathbb{Q}$, and give solutions of the quartic Fermat equation.

In part II of this paper, I shall verify the above conjecture for the prime $p = 5$, by considering solutions of the diophantine equation

$$\varepsilon^5 X^5 + \varepsilon^5 Y^5 = 1 - X^5 Y^5, \quad \varepsilon = \frac{1 + \sqrt{5}}{2},$$

in certain class fields of 5-admissible quadratic fields.

The following conjecture is also stated in [m3].

Conjecture 2. *Any ring class field of a p-admissible quadratic field $K = \mathbb{Q}(\sqrt{-d}) \subset \overline{\mathbb{Q}}_p$, whose conductor is divisible by p, is generated over K by some pre-periodic point of the multi-valued function $T_p(z)$ contained in the algebraic closure $\overline{\mathbb{Q}}_p$.*

This statement was proved for $p = 3$ and the above function $T_3(z)$ in [m3] and will be proved for $p = 2$ and the 2-adic function $T(z)$ elsewhere. (See [cn].)

2 The quartic Fermat equation.

The numbers π_d and ξ_d defined in (1) were shown in [lm] to be algebraic conjugates of each other over $\mathbb{Q}$. This fact was deduced from the relationship

$$\pi_d^{\tau^2} = \frac{\xi_d + 1}{\xi_d - 1},$$

where τ is a certain automorphism in the Galois group of Ω_f/K, uniquely defined by the condition that

$$\alpha^\tau \equiv \alpha^2 \pmod{\wp_2},$$

for all elements α of the ring of integers Ω_f, R_{Ω_f}. Actually, this congruence holds for all $\alpha \in \Omega_f$ whose denominators are relatively prime to $\wp_2$ – these are the elements of Ω_f which are integral for $\wp_2$. This automorphism is denoted by

$$\tau = \left(\frac{\Omega_f/K}{\wp_2}\right),$$

and is called the Frobenius automorphism for the prime ideal $\wp_2$ of R_K. An automorphism of $\mathrm{Gal}(\Omega_f/K)$ can be assigned to any prime ideal $\mathfrak{p}$ in R_K which is relatively prime to f (and therefore unramified in Ω_f), satisfying

$$\alpha^\sigma \equiv \alpha^{\mathrm{Norm}(\mathfrak{p})} \pmod{\mathfrak{p}}, \quad \alpha \in R_{\Omega_f}, \quad \sigma = \left(\frac{\Omega_f/K}{\mathfrak{p}}\right),$$

where $\mathrm{Norm}(\mathfrak{p}) = |R_K/\mathfrak{p}|$ is the absolute norm of $\mathfrak{p}$. (See [ch], [co1], or [h2].) Recall that f is the positive integer for which $K = \mathbb{Q}(\sqrt{-d})$ and $-d = d_K f^2$, where d_K is the discriminant of $K/\mathbb{Q}$. Although the square-roots of the numbers $-d_K f^2$ all generate the same quadratic field K, the degrees of the numbers π_d and ξ_d and the field they generate over $\mathbb{Q}$ depend strongly on the parameter f. We always assume $-d \equiv 1 \pmod 8$, so that d_K and f are odd integers.

Replacing x by $(x+1)/(x-1)$ in the Fermat equation $x^4 + y^4 = 1$ leads to the curve $f(x, y) = 0$ defined by the equation

$$f(x, y) = y^4(x-1)^4 + 8x(x^2+1). \tag{2}$$

Writing $\pi = \pi_d, \xi = \xi_d$, the relation $(\pi^{\tau^2})^4 + (\xi^{\tau^2})^4 = 1$ yields

$$f(\xi, \xi^{\tau^2}) = 0, \quad \xi = \frac{\beta}{2}. \tag{3}$$

It follows that ξ^{τ^2} can be considered as one of the values of the algebraic function

$$y = S(x) = \sqrt[4]{\frac{-8x(x^2+1)}{(x-1)^4}} = \sqrt[4]{1 - \left(\frac{x+1}{x-1}\right)^4}$$

at $x = \xi$. It is natural to try to expand $S(x)$ as follows:

$$S(x) = 1 + \sum_{k=1}^{\infty} (-1)^k \binom{\frac{1}{4}}{k} \left(\frac{1+x}{1-x} \right)^{4k}.$$

Unfortunately, this cannot be expressed as a convergent 2-adic series in powers of x, since

$$S(0) = 1 + \sum_{k=1}^{\infty} (-1)^k \binom{\frac{1}{4}}{k}$$

does not even converge (2-adically). Instead, we apply τ^{-2} to $f(\xi, \xi^{\tau^2}) = 0$, obtaining $f(\xi^{\tau^{-2}}, \xi) = 0$, and we consider $\xi^{\tau^{-2}}$ as one of the values of the inverse algebraic function

$$x = T(y) = \frac{\sqrt[4]{1-y^4}+1}{\sqrt[4]{1-y^4}-1}, \quad f(x,y) = 0, \tag{4}$$

evaluated at $y = \xi$.

We first find an expression for a particular 2-adic branch of the function $T(y)$. Expanding and dividing $f(x,y)$ by y^4 gives

$$\begin{aligned} \frac{f(x,y)}{y^4} &= x^4 + \frac{8-4y^4}{y^4}x^3 + 6x^2 + \frac{8-4y^4}{y^4}x + 1 \\ &= x^4 + tx^3 + 6x^2 + tx + 1, \quad t = \frac{8-4y^4}{y^4}. \end{aligned}$$

Hence,

$$\begin{aligned} \frac{f(x,y)}{x^2y^4} &= \left(x^2 + \frac{1}{x^2} \right) + t \left(x + \frac{1}{x} \right) + 6 \\ &= z^2 + tz + 4, \quad z = x + \frac{1}{x}. \end{aligned}$$

Thus we have

$$z = \frac{-t \pm \sqrt{t^2-16}}{2} = \frac{2y^4 - 4 \pm 4\sqrt{1-y^4}}{y^4}.$$

We define

$$T_1(y) = \frac{2y^4 - 4 - 4\sqrt{1-y^4}}{y^4}. \tag{5}$$

This function can be expanded into a 2-adic Laurent series in y, as follows.

$$\begin{aligned} T_1(y) &= 2 - \frac{4}{y^4} - \frac{4}{y^4}\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-1)^n y^{4n} \\ &= 2 - \frac{4}{y^4} - \frac{4}{y^4}(1 - \frac{1}{2}y^4 - \frac{1}{8}y^8 - \cdots) \\ &= \frac{-8}{y^4} + 4 + 4\sum_{n=2}^{\infty}\binom{\frac{1}{2}}{n}(-1)^{n+1}y^{4n-4}. \end{aligned}$$

It is not hard to verify that the series for $T_1(y)$ converges 2-adically for $0 < |y|_2 \leq \frac{1}{2}$. To see this, set $y = 2y_1$. With this substitution, the series becomes

$$T_1(2y_1) + \frac{1}{2y_1^4} - 4 = \sum_{n=2}^{\infty} 2^{4n-2}\binom{\frac{1}{2}}{n}(-1)^{n+1}y_1^{4n-4} = \sum_{n=2}^{\infty} 2^{2n-1}C_{n-1}y_1^{4n-4}, \tag{6}$$

where $C_{n-1} = (-1)^{n+1}2^{2n-1}\binom{\frac{1}{2}}{n} \in \mathbb{Z}$ is the Catalan number. Hence, the coefficient of y_1 in the series (6) is divisible by 2^{2n-1}, and the series is therefore convergent for $|y_1| \leq 1$. This proves the above claim. Moreover, the infinite series in (6) represents a 2-adic integer for $|y|_2 \leq \frac{1}{2}$, so it is clear that

$$|T_1(y)|_2 \geq 2, \quad \text{if } 0 < |y|_2 \leq \frac{1}{2}, \tag{7}$$

because of the leading term $\frac{-8}{y^4}$. The second solution of $z^2 + tz + 4 = 0$ is then

$$-t - T_1(y) = -4\sum_{n=2}^{\infty}\binom{\frac{1}{2}}{n}(-1)^{n+1}y^{4n-4} = \frac{4}{T_1(y)},$$

which is a 2-adic integer.

Solving the equation $x^2 - zx + 1 = 0$ for x gives

$$x = \frac{z \pm \sqrt{z^2-4}}{2}.$$

Now we set

$$\begin{aligned} T_2(z) &= \frac{z}{2} - \frac{z}{2}\sqrt{1 - \frac{4}{z^2}} = \frac{z}{2} - \frac{z}{2}\sum_{n=0}^{\infty}(-1)^n\binom{\frac{1}{2}}{n}\frac{2^{2n}}{z^{2n}} \\ &= \sum_{n=1}^{\infty}(-1)^{n+1}\binom{\frac{1}{2}}{n}\frac{2^{2n-1}}{z^{2n-1}} = \sum_{n=1}^{\infty}\frac{C_{n-1}}{z^{2n-1}} \\ &= \frac{1}{z} + \frac{1}{z^3} + \frac{2}{z^5} + \frac{5}{z^7} + \frac{14}{z^9} + \frac{42}{z^{11}} + \cdots, \end{aligned}$$

which is convergent for $|z|_2 \geq 2$, as above. It is clear from this series expansion that

$$0 < |T_2(z)|_2 \leq \frac{1}{2} \ \text{ for } |z|_2 \geq 2, \tag{8}$$

since $\frac{4}{z^2} \neq 0$. The second solution of $x^2 - zx + 1 = 0$ is then $z - T_2(z) = \frac{1}{T_2(z)}$, which is *not* a 2-adic integer.

By the above arguments, setting $z = T_1(y)$ gives the solution

$$x = T_2(z) = T_2(T_1(y)), \ \text{ for } 0 < |y|_2 \leq \frac{1}{2}, \tag{9}$$

of $f(x, y) = 0$. By (7) and (8), the function

$$T = T_2 \circ T_1$$

maps the region $0 < |y|_2 \leq \frac{1}{2}$ of K_2 into itself. It is clear that this is also true of the region $|y|_2 = \frac{1}{2}$. This is the branch of T which we will use throughout our discussion. To summarize, we have:

Proposition 3. *The algebraic function* $T(y) = T_2(T_1(y))$, *where*

$$T_1(y) = \frac{-8}{y^4} + 4 + 4\sum_{n=2}^{\infty} \binom{\frac{1}{2}}{n} (-1)^{n+1} y^{4n-4},$$
$$T_2(z) = \sum_{n=1}^{\infty} (-1)^{n+1} \binom{\frac{1}{2}}{n} \frac{2^{2n-1}}{z^{2n-1}},$$

is defined on the punctured disk

$$\mathsf{D}_2 = \{y \in \mathsf{K}_2 : \ 0 < |y|_2 \leq \frac{1}{2}\}$$

in the field K_2, *and maps* D_2 *to itself. For any* $y \in \mathsf{D}_2$, *we have* $f(T(y), y) = 0$.

We now prove the following theorem.

Theorem 4. *Let* (π, ξ) *be any solution of* $X^4 + Y^4 = 1$ *in the ring class field* Ω_f *of odd conductor* f *over* $K = \mathbb{Q}(\sqrt{-d})$ *which is conjugate over* K *to the solution (1). Then under the embedding of* Ω_f *in the maximal unramified extension* K_2 *of the 2-adic field* $\mathbb{Q}_2$ *given by* $\Omega_f \to (\Omega_f)_{\mathfrak{p}}$, *where* $\mathfrak{p}$ *is a prime divisor of* $\wp_2'$ *in* R_{Ω_f}, *we have*

$$\xi^{\tau^{-2}} = T(\xi), \ \text{with } \tau^{-1} = \left(\frac{\Omega_f/K}{\wp_2'}\right),$$

where $T(y)$ is the 2-adic algebraic function from Proposition 3. Thus, $\xi \rightarrow T(\xi)$ is a lift of the square of the Frobenius automorphism corresponding to $\wp_2'$ on Ω_f/K.

Proof. The Galois group $\mathrm{Gal}(\Omega_f/K)$ is a generalized dihedral group (see [co1, pp. 190-191]), so the automorphism $\tau = \left(\frac{\Omega_f/K}{\wp_2}\right)$ (applied exponentially) satisfies

$$\tau^{-1} = \phi^{-1}\tau\phi = \left(\frac{\Omega_f/K}{\wp_2'}\right),$$

(see [co1, p. 107]) where ϕ is an automorphism of Ω_f which restricts to the nontrivial automorphism of K, sending $\wp_2$ to its conjugate ideal $\wp_2'$. Hence, we know that

$$\left(\frac{\xi}{2}\right)^{\tau^{-2}} \equiv \left(\frac{\xi}{2}\right)^4 \ (\mathrm{mod}\ \wp_2') \ \text{ in } \Omega_f.$$

Embedding Ω_f into K_2 by completing at a prime $\mathfrak{p}$ of Ω_f lying over $\wp_2'$, we obtain that the images of $\xi, \xi^{\tau^{-2}}$, which we denote by the same symbols, satisfy

$$\left(\frac{\xi}{2}\right)^{\tau^{-2}} \equiv \left(\frac{\xi}{2}\right)^4 \ (\mathrm{mod}\ 2) \ \text{ in } \ (\Omega_f)_{\mathfrak{p}} \subset \mathsf{K}_2,$$

and, since both sides of this congruence are units for $\wp_2'$, that

$$\frac{2^3\xi^{\tau^{-2}}}{\xi^4} \equiv 1 \ (\mathrm{mod}\ 2) \ \text{ in } \ (\Omega_f)_{\mathfrak{p}} \subset \mathsf{K}_2.$$

Now we have from (7) and the series for $T_2(z)$ that $T_2(T_1(y)) \equiv \frac{1}{T_1(y)}$ (mod 2^3), so

$$\frac{2^3T(\xi)}{\xi^4} = \frac{2^3T_2(T_1(\xi))}{\xi^4} \equiv \frac{2^3}{\xi^4T_1(\xi)} \equiv -1 \equiv 1 \ (\mathrm{mod}\ 2), \ \text{ for } 0 < |\xi|_2 \leq \frac{1}{2}. \tag{10}$$

It follows that

$$\frac{\xi^{\tau^{-2}}}{T(\xi)} = \eta^{-1} \equiv 1 \ (\mathrm{mod}\ 2),$$

and therefore $T(\xi) = \eta\xi^{\tau^{-2}}$, where η is a 2-adic unit. But $T(\xi)$ and $\xi^{\tau^{-2}}$ are both roots of $f(x,\xi) = 0$ in K_2. From the above argument we know there is a second root of $f(x,\xi) = 0$ in K_2 given by $T_1(\xi) - T_2(T_1(\xi)) = T_1(\xi) - T(\xi)$, which is not a 2-adic integer, by (7), since $T(\xi) \in \mathsf{D}_2$ by Proposition 3. (Recall that $(\xi) = \wp_2'$ in R_{Ω_f}, so that $|\xi|_2 = \frac{1}{2}$ in K_2.) Thus, $T(\xi)$ is distinct from this root.

Now I claim that the polynomial

$$g(x) = \frac{f(x,\xi)}{\xi^4} = x^4 + tx^3 + 6x^2 + tx + 1, \quad t = \frac{8 - 4\xi^4}{\xi^4},$$

has at most two roots in K_2. To see this, note that the Ferrari cubic resolvent of $g(x)$ [co2, pp. 358-359], whose roots are rational expressions over $\mathbb{Q}_2(\xi)$ in the roots of $g(x)$, is

$$r(y) = y^3 - 6y^2 + (t^2 - 4)y - 2t^2 + 24 = (y - 2)(y^2 - 4y + t^2 - 12),$$

where the discriminant of the quadratic factor is given by

$$\delta = -4(t^2 - 16) = \frac{256(\xi^4 - 1)}{\xi^8}.$$

We have $1 - \xi^4 \equiv 1 \pmod{16}$ since $|\xi|_2 = \frac{1}{2}$, so Hensel's Lemma implies that $\delta = -\mu^2$ for some $\mu \in \mathsf{K}_2$. Therefore, $\sqrt{\delta} \notin \mathsf{K}_2$, since $\mathbb{Q}_2(\sqrt{-1})$ is a ramified extension, and the resolvent $r(y)$ has exactly one root in K_2. This shows that the polynomial $g(x)$ has exactly two roots in K_2 and that $T(\xi) = \xi^{\tau^{-2}}$.

It is clear that the above discussion also holds for any conjugate of $\xi = \xi_d$ over $K = \mathbb{Q}(\sqrt{-d})$, since the ideal $\wp_2'$ is fixed by the elements of $\mathrm{Gal}(\Omega_f/K)$, and since this Galois group is abelian. $\square$

We use Theorem 4 to prove

Theorem 5. *With notation as in Theorem 4, ξ is a periodic point of the algebraic function $T(y)$ on the domain $\mathsf{D}_2 := \{y : |y|_2 \le \frac{1}{2}\} \subset \mathsf{K}_2$, whose period n is equal to the order of the automorphism τ^{-2} in $Gal(\Omega_f/K)$.*

Proof. This follows from the fact that τ^{-2}, as an automorphism on the completion $(\Omega_f)_{\mathfrak{p}}$ fixing the prime ideal $\wp_2'\mathbb{Z}_2 = 2\mathbb{Z}_2$ of $(R_K)_{\wp_2'} = \mathbb{Z}_2$, satisfies

$$T(z)^{\tau^{-2}} = T(z^{\tau^{-2}}), \quad \text{for } z \in (\Omega_f)_{\mathfrak{p}} \cap \mathsf{D}_2,$$

since the coefficients of $T_1(2y_1) - \frac{1}{2y_1^4}$ (see (6)) and $T_2(z)$ lie in $\mathbb{Z}$. Therefore,

$$T^2(\xi) = T(T(\xi)) = T(\xi^{\tau^{-2}}) = T(\xi)^{\tau^{-2}} = \xi^{\tau^{-4}},$$

and more generally, $T^k(\xi) = \xi^{\tau^{-2k}}$, $k \ge 1$. Since ξ generates Ω_f over K, we have $\xi^{\tau^{-2k}} \ne \xi$ for $k < n$. Hence, $T^n(\xi) = \xi^{\tau^{-2n}} = \xi$, which shows that ξ is a periodic point of T with minimal period n. $\square$

This proves part (a) of Conjecture 1 of the Introduction, since every ring class field Ω_f of odd conductor over the 2-admissible field K is generated by the coordinates of a solution of the quartic Fermat equation.

We would now like to prove the converse; namely, that any periodic point of T on the domain D_2 comes from one of the solutions (π, ξ) in some ring class field Ω_f over $K = \mathbb{Q}(\sqrt{-d})$, with $-d \equiv 1 \pmod 8$.

3 Iterated resultants.

Define the following iterated resultants, as in [m3]. Set $R^{(1)}(x, x_1) = f(x, x_1)$,

$$R^{(2)}(x, x_2) = Res_{x_1}(f(x, x_1), f(x_1, x_2)),$$

and recursively define

$$R^{(k)}(x, x_k) = Res_{x_{k-1}}(R^{(k-1)}(x, x_{k-1}), f(x_{k-1}, x_k)), \quad k \geq 3. \tag{11}$$

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

$$f(a, a_1) = 0, \quad f(a_1, a_2) = 0, \quad \cdots \quad f(a_{n-1}, a) = 0. \tag{12}$$

In particular, (12) holds for

$$a = \xi = T^n(\xi),\ a_{n-1} = T(\xi),\ a_{n-2} = T(a_{n-1}) = T^2(\xi), \cdots, a_1 = T(a_2) = T^{n-1}(\xi),$$

by Proposition 3 and Theorem 5, so that $T^k(\xi)$ is a root of $R_n(x)$ for any k with $0 \leq k \leq n$. It is straightforward to show by induction that

$$R^{(n)}(x, x_n) \equiv x_n^{4^n}(x+1)^{4^n} \pmod 2,$$

and therefore

$$R_n(x) \equiv x^{4^n}(x+1)^{4^n} \pmod 2.$$

In the following lemma, we show that $R_n(x)$ is monic and has degree $2 \cdot 4^n$.

Lemma. a) *For $n \geq 2$, $R^{(n)}(x, x_n) = A_n(x)x_n^{4^n} + S_n(x, x_n)$, where $A_n(x) \in \mathbb{Z}[x]$ is a monic polynomial satisfying deg$(A_n(x)) = 4^n$, and*

$$\deg_{x_n}(S_n(x, x_n)) \leq 4^n - 4, \quad \deg_x(S_n(x, x_n)) \leq 4^n - 1.$$

b) *deg$(R_n(x)) = 2 \cdot 4^n$, and the leading coefficient of $R_n(x)$ is* 1.

Proof. a) The assertion is obvious for $n = 1$ by (2). Assume it holds for $n-1$, where $n \geq 2$. Then x_n^4 is the leading coefficient of x_{n-1} in $f(x_{n-1}, x_n)$, so by (11) and the definition of the resultant, we have that

$$R^{(n)}(x, x_n) = x_n^{4^n} \prod_{i=1}^{4} R^{(n-1)}(x, \beta_i) = \prod_{i=1}^{4} x_n^{4^{n-1}} R^{(n-1)}(x, \beta_i),$$

where $x_{n-1} = \beta_i, 1 \leq i \leq 4$, are the roots of the equation $f(x_{n-1}, x_n) = 0$. Dividing this equation by x_n^4 and expanding with $x_{n-1} = \beta_i$ shows that

$$\beta_i^4 - \left(4 - \frac{8}{x_n^4}\right)\beta_i^3 + 6\beta_i^2 - \left(4 - \frac{8}{x_n^4}\right)\beta_i + 1 = 0.$$

It follows that the elementary symmetric functions in the β_i have degree 0 in x_n, and in the product

$$R^{(n)}(x, x_n) = \prod_{i=1}^{4}(x_n^{4^{n-1}} A_{n-1}(x)\beta_i^{4^{n-1}} + x_n^{4^{n-1}} S_{n-1}(x, \beta_i)),$$

the leading term is $x_n^{4^n} A_{n-1}(x)^4(\beta_1\beta_2\beta_3\beta_4)^{4^{n-1}} = x_n^{4^n} A_{n-1}(x)^4$, since the product of the β_i is 1. By the inductive hypothesis, the degree in x of $S_{n-1}(x, x_{n-1})$ is at most $4^{n-1} - 1$, so in multiplying out the remaining terms have degree at most $3 \cdot 4^{n-1} + 4^{n-1} - 1 = 4^n - 1$ in x. In collecting the remaining terms that involve $x_n^{4^n}$, and adding them to $A_{n-1}(x)^4$, the highest degree term in x occurs only in the leading term and $A_n(x)$ is therefore monic of degree 4^n. It is also clear that in the product, the degrees of the terms involving x_n will all be multiples of 4. This proves part a) of the lemma. Part b) follows immediately from a) on setting $x_n = x$. □

We will now show that the polynomials $R_n(x)$ have distinct roots.

We define similar quantities for the curve

$$f_1(x, y) = \frac{f(2x, 2y)}{16} = (16x^4 - 32x^3 + 24x^2 - 8x + 1)y^4 + 4x^3 + x.$$

We have

$$f_1(x,y) \equiv y^4 + x \pmod{2}.$$

Define the iterated resultants for $f_1(x,y)$ by $\tilde{R}^{(1)}(x,x_1) = f_1(x,x_1)$,

$$\begin{aligned} \tilde{R}^{(2)}(x,x_2) &= Res_{x_1}(f_1(x,x_1), f_1(x_1,x_2)),\\ \tilde{R}^{(k)}(x,x_k) &= Res_{x_{k-1}}(\tilde{R}^{(k-1)}(x,x_{k-1}), f_1(x_{k-1},x_k)), \quad k \geq 3. \end{aligned}$$

It follows easily by induction that

$$\tilde{R}^{(n)}(x,x_n) \equiv x_n^{4^n} + x \pmod{2}, \quad n \geq 1,$$

and therefore

$$\tilde{R}_n(x) = \tilde{R}^{(n)}(x,x) \equiv x^{4^n} + x \pmod{2}, \quad n \geq 1. \tag{13}$$

This congruence and Hensel's Lemma [h, p. 169] imply that $\tilde{R}_n(x)$ has at least 4^n distinct roots in K_2, of which $4^n - 1$ are units, corresponding to the $4^n - 1$ nonzero roots of the congruence (13). Furthermore, the relation

$$R_n(2x) = 2^{4^n}\tilde{R}_n(x) \tag{14}$$

implies that $R_n(x)$ also has at least 4^n distinct roots, as well, and $N_2(k)$ monic irreducible factors of degree k in $\mathbb{Z}_2[x]$, for each divisor k of $2n$, where $N_2(k)$ is the number of monic irreducible polynomials of degree k in $\mathbb{F}_2[x]$. The roots a of these irreducible factors (except for $a = 0$, note $f(0,0) = 0$) are prime elements in the ring of integers R_2 of K_2, i.e. $a \cong 2$ ($\cong$ is Hasse's notation [h3], denoting equality up to a unit factor).

Now we make use of the identity

$$(x-1)^4(y-1)^4 f\left(\frac{x+1}{x-1}, \frac{y+1}{y-1}\right) = 16f(y,x). \tag{15}$$

Putting

$$b = \frac{a+1}{a-1}, \quad b_k = \frac{a_k+1}{a_k-1}, \quad 1 \leq k \leq n-1,$$

where a and the a_k satisfy (12), the identity (15) gives that

$$f(b, b_{n-1}) = 0, \quad f(b_{n-1}, b_{n-2}) = 0, \quad \cdots \quad f(b_1, b) = 0.$$

It follows that $b = \frac{a+1}{a-1}$ is a root of $R_n(x) = 0$ whenever a is. If a is a prime element, then b is clearly a unit in R_2. This proves that $R_n(x)$ has $2 \cdot 4^n$ distinct roots in K_2, for any $n \geq 1$ (including the roots $x = 0, -1$), exactly half of which are units.

It follows as in [m3] that there are polynomials $\mathsf{P}_n(x)$ and $\widetilde{\mathsf{P}}_n(x)$ in $\mathbb{Z}[x]$ for which

$$R_n(x) = \prod_{k|n} \mathsf{P}_k(x), \quad \mathsf{P}_n(x) = \prod_{k|n} R_k(x)^{\mu(n/k)}, \tag{16}$$

$$\tilde{R}_n(x) = \prod_{k|n} \widetilde{\mathsf{P}}_k(x), \quad \widetilde{\mathsf{P}}_n(x) = \prod_{k|n} \tilde{R}_k(x)^{\mu(n/k)}, \tag{17}$$

and

$$\text{deg } \mathsf{P}_n(x) = \text{deg } \widetilde{\mathsf{P}}_n(x) = 2\sum_{k|n} \mu(n/k)4^k. \tag{18}$$

We note also that

$$R_1(x) = \mathsf{P}_1(x) = x(x+1)(x^2-x+2)(x^4-4x^3+5x^2-2x+4) \tag{19}$$

$$\tilde{R}_1(x) = \widetilde{\mathsf{P}}_1(x) = x(2x+1)(2x^2-x+1)(4x^4-8x^3+5x^2-x+1).$$

Setting

$$\tilde{T}(z) = \frac{1}{2}T(2z), \quad |z|_2 \leq 1,$$

we see from (10) that

$$\tilde{T}(x) \equiv x^4 \text{ (mod 2)}, \quad |x|_2 = 1. \tag{20}$$

From (13) and (17) and the above arguments it is clear that all the irreducible factors of $\widetilde{\mathsf{P}}_n(x)$ (i.e., its reduction modulo 2) over $\mathbb{F}_4$ have degree n. It is clear that $\tilde{T}(a)$ is a root of $\widetilde{\mathsf{P}}_n(x)$ whenever the unit a is, since a and therefore $\tilde{T}(a)$ are both periodic points of $\tilde{T}$ with minimal period n. This is because $\tilde{T}^k(a) = a$ for $k < n$ would imply that $a^{4^k} \equiv a$ (mod 2), and a would therefore be a root of a polynomial of degree less than n over $\mathbb{F}_4$.

For such a unit a, $\tilde{T}(a)$ reduces (mod 2) to a root of the right side of (13). Since (13) does not have multiple roots, and by (14), half of the roots of $\widetilde{\mathsf{P}}_n(x)$ are non-units, (20) shows that a and $\tilde{T}(a)$ are roots of the same irreducible factor over $\mathbb{F}_4$, and therefore they must be roots of the same irreducible factor over $\mathbb{Q}_2$. It follows that

$$\mathsf{P}_n(x) = \prod_i g_i(x)\tilde{g}_i(x),$$

where the irreducible factor $g_i(x) \in \mathbb{Z}_2[x]$ has degree n or $2n$;

$$\tilde{g}_i(x) = (x-1)^{\deg(g_i)} g_i\left(\frac{x+1}{x-1}\right);$$

and T maps the set of roots of $g_i(x)$ into itself, for each i. Since $\mathsf{P}_n(x) \in \mathbb{Z}[x]$, Theorem 5 implies that the minimal polynomial $b_d(x)$ of ξ_d over $\mathbb{Q}$ divides $\mathsf{P}_n(x)$, for any d for which the automorphism $\tau_d^{-2} = \tau^{-2}$ has order n in $\mathrm{Gal}(\Omega_f/K)$. In Section 5 we will prove that these are the only irreducible factors of $\mathsf{P}_n(x)$, for $n > 1$.

4 A cyclic isogeny of degree 4.

We will now use several results from [m1, pp. 253-254] and [lm]. First, the quantity

$$j_1(\alpha) = \frac{(\alpha^8 - 16\alpha^4 + 16)^3}{\alpha^8 - 16\alpha^4},$$

is the j-invariant of the elliptic curve

$$E_1(\alpha): \quad Y^2 + XY + \frac{1}{\alpha^4}Y = X^3 + \frac{1}{\alpha^4}X^2, \tag{21}$$

which is the Tate normal form for a curve with a point of order $n = 4$; meaning that the point $(0, 0)$ has order 4 on this curve. Further,

$$j_2(\alpha) = \frac{(\alpha^8 - 16\alpha^4 + 256)^3}{\alpha^8(\alpha^4 - 16)^2} \tag{22}$$

is the j-invariant of the elliptic curve

$$E_2(\alpha): \quad Y^2 + XY + \frac{2}{\alpha^4}Y = X^3 + \frac{4}{\alpha^4}X^2 - \frac{1}{\alpha^8},$$

and $E_1(\alpha)$ is 2-isogenous to $E_2(\alpha)$ by the map $\psi_\alpha = (\psi_{\alpha,1}, \psi_{\alpha,2}) : E_1(\alpha) \rightarrow E_2(\alpha)$ with

$$\psi_{\alpha,1}(X) = \frac{X^2}{X+b}, \quad \psi_{\alpha,2}(X, Y) = \frac{-b^2}{X+b} + \frac{X(X+2b)Y}{(X+b)^2}, \quad b = \frac{1}{\alpha^4}.$$

From [lm, Eq. (4.8)] we know that $E_1(\alpha)[2]$ – the group of 2-torsion points on $E_1(\alpha)$ – consists of the base point O, together with the points

$$\left(\frac{-1}{\alpha^4}, 0\right), \ \left(-\frac{\beta^2 - 4}{8\beta^2}, \frac{(\beta^2 - 4)^2}{32\beta^4}\right), \ \left(-\frac{\beta^2 + 4}{8\beta^2}, \frac{(\beta^2 + 4)^2}{32\beta^4}\right), \tag{23}$$

where $16\alpha^4 + 16\beta^4 = \alpha^4\beta^4$. Reversing the roles of α and β in (23) gives the points of order 2 on the curve $E_1(\beta)$.

Furthermore, still with $b = 1/\alpha^4$, the isogeny $\rho_\alpha = (\rho_{\alpha,1}(X), \rho_{\alpha,2}(X,Y))$, with

$$\rho_{\alpha,1}(X) = \frac{X^2 - b}{X + 4b}, \tag{24}$$

$$\rho_{\alpha,2}(X,Y) = \frac{bX^2 + (b - 8b^2)X + 3b^2 - 32b^3}{(X+4b)^2} + \frac{X^2 + 8bX + b}{(X+4b)^2}Y, \tag{25}$$

maps $E_2(\alpha)$ to the curve

$$E_3(\alpha): \quad Y^2 + XY + \frac{4}{\alpha^4}Y = X^3 + \frac{16}{\alpha^4}X^2 + \frac{6}{\alpha^4}X + \frac{\alpha^4 - 4}{\alpha^8}, \tag{26}$$

and the j-invariant of this curve is

$$j_3(\alpha) = \frac{(\alpha^8 - 256\alpha^4 + 4096)^3}{\alpha^{16}(16 - \alpha^4)}. \tag{27}$$

We first use these facts to prove the following result. Although we do not make explicit use of this result, we will use several of the facts mentioned in the proof in Section 5. Moreover, the result itself is of independent interest, since it gives an interesting application for solutions of the Fermat quartic, and corresponds to the analogous result for the Fermat cubic given in [m2, Prop. 3.5].

Theorem 6. *If (α, β) is a point on the curve*

$$Fer_4: \ 16X^4 + 16Y^4 = X^4Y^4,$$

then there is a cyclic isogeny $\phi_{\alpha,\beta} : E_1(\alpha) \to E_1(\beta)$ of degree 4, whose kernel is $ker(\phi_{\alpha,\beta}) = \langle (0,0) \rangle$.

Proof. The relation

$$\alpha^4 = \frac{16\beta^4}{\beta^4 - 16}$$

implies easily using (22) that $j_2(\alpha) = j_2(\beta)$ and therefore $E_2(\alpha) \cong E_2(\beta)$. On the other hand, there is the dual isogeny $\hat{\psi}_\beta : E_2(\beta) \to E_1(\beta)$. Therefore, if $\iota : E_2(\alpha) \to E_2(\beta)$ is an isomorphism, the map

$$\phi = \hat{\psi}_\beta \circ \iota \circ \psi_\alpha : E_1(\alpha) \to E_1(\beta)$$

is an isogeny of degree 4. To determine $\ker(\phi)$, we find an explicit isomorphism ι. Note that with $Y_1 = Y + \frac{X}{2} + \frac{1}{\alpha^4}$ the equation for $E_2(\alpha)$ becomes

$$Y_1^2 = X\left(X + \frac{1}{4}\right)\left(X + \frac{4}{\alpha^4}\right).$$

Using the relation

$$\frac{4}{\alpha^4} = \frac{1}{4} - \frac{4}{\beta^4}$$

and putting $X = -X_2 - \frac{1}{4}, Y_1 = -\sqrt{-1}Y_2$ gives the curve

$$Y_2^2 = X_2\left(X_2 + \frac{1}{4}\right)\left(X_2 + \frac{4}{\beta^4}\right). \tag{28}$$

Therefore, the map $\iota(X,Y) = (\iota_1(X), \iota_2(X,Y))$ can be taken to be the map

$$(\iota_1(X), \iota_2(X,Y)) = \left(-X - \frac{1}{4}, \sqrt{-1}Y + \frac{1+\sqrt{-1}}{2}X + \frac{1+\sqrt{-1}}{\alpha^4} + \frac{1}{16}\right). \tag{29}$$

On the other hand, the X-coordinate of the dual isogeny $\hat{\psi}_\beta : E_2(\beta) \to E_1(\beta)$ is given by

$$\hat{\psi}_{\beta,1}(X) = \frac{X^2 - \frac{1}{\beta^4}}{4X+1}.$$

Thus, we have

$$\phi((0,0)) = \hat{\psi}_\beta \circ \iota((0, -\frac{1}{\alpha^4})) = \hat{\psi}_\beta((-\frac{1}{4}, \frac{1}{\alpha^4} + \frac{1}{16})) = O_1,$$

where O_1 is the base point on $E_1(\beta)$. Since ϕ has degree 4 and the point $(0,0)$ has order 4, this shows that $\ker(\phi) = \langle(0,0)\rangle$ is cyclic. $\square$

We note that the X-coordinate of the map $\phi = \phi_{\alpha,\beta}$ is given by the rational function

$$\phi_1(X) = \hat{\psi}_{\beta,1} \circ \iota_1 \circ \psi_{\alpha,1}(X) = \hat{\psi}_{\beta,1}\left(-\frac{X^2}{X + \frac{1}{\alpha^4}} - \frac{1}{4}\right)$$

$$= -\frac{(4\alpha^4\beta^2X^2 + \alpha^4(\beta^2-4)X + \beta^2 - 4)(4\alpha^4\beta^2X^2 + \alpha^4(\beta^2+4)X + \beta^2 + 4)}{64\alpha^4\beta^4X^2(\alpha^4X+1)}.$$

5 Periodic points of $T(z)$.

In this section we will prove the following theorem.

Theorem 7. *For $n > 1$, the polynomial $\mathsf{P}_n(x)$ is the product of the polynomials $b_d(x)$, where $-d$ runs through all quadratic discriminants $-d \equiv 1$ (mod 8) for which τ^2 has order n in the Galois group of the corresponding ring class field Ω_f. Here $\tau = \left(\frac{\Omega_f/K}{\wp_2}\right)$ is the Artin symbol (Frobenius automorphism) for the prime divisor $\wp_2$ of 2 in $K = \mathbb{Q}(\sqrt{-d})$.*

Let ξ be an arbitrary periodic point of $T(z)$ of minimal period $n \geq 1$ in the domain $\mathsf{D}_2 = \{z : 0 < |z|_2 \leq \frac{1}{2}\} \subset \mathsf{K}_2$, and set

$$\beta = 2\xi, \quad \alpha^4 = \frac{16\beta^4}{\beta^4 - 16} = 16\frac{\xi^4}{\xi^4 - 1}, \quad \beta \in \mathsf{K}_2, \ \alpha \in \mathsf{K}_2(\zeta_8), \tag{30}$$

where $\zeta_8 = \sqrt[4]{-1}$ is an eighth root of unity. Then (α, β) is a point on Fer_4 (see Theorem 6) defined over $\mathsf{K}_2(\zeta_8)$. Since $\mathbb{Q}_2(\xi)$ is an unramified extension of $\mathbb{Q}_2$, and $\mathbb{Q}_2(\zeta_8)$ is totally ramified over $\mathbb{Q}_2$, there is an automorphism

$$\bar{\tau} \in \mathrm{Gal}(\mathbb{Q}_2(\xi, \zeta_8)/\mathbb{Q}_2), \text{ with } \bar{\tau} := (\xi \to T(\xi), \ \zeta_8 \to \zeta_8). \tag{31}$$

(Recall that ξ and $T(\xi)$ are roots of the same irreducible polynomial over $\mathbb{Q}_2$, by the last assertion of Section 3.)

I claim now that $E_3(\beta) \cong E_1(\alpha^{\bar{\tau}})$, where E_3 and E_1 are the curves defined in (26) and (21). To prove this, let $\sigma(z)$ be the linear fractional map

$$\sigma(z) = \frac{2(z+2)}{z-2}.$$

From the fact that $f(T(\xi), \xi) = 0$ we have that

$$\xi^4 = 1 - \left(\frac{T(\xi)+1}{T(\xi)-1}\right)^4$$

and therefore

$$\left(\frac{T(\xi)+1}{T(\xi)-1}\right)^4 = 1 - \xi^4.$$

Since $\beta^{\bar{\tau}} = 2\xi^{\bar{\tau}} = 2T(\xi)$, this gives

$$\left(\frac{\beta^{\bar{\tau}}+2}{\beta^{\bar{\tau}}-2}\right)^4 = 1 - \frac{\beta^4}{16},$$

and hence

$$\sigma(\beta^{\bar{\tau}})^4 = 16 - \beta^4. \tag{32}$$

Therefore, as in the proof of [lm, Prop. 8.5], and using the relation between α and β, we have

$$\begin{aligned} j(E_1(\alpha^{\bar{\tau}})) &= \left(\frac{(\alpha^8 - 16\alpha^4 + 16)^3}{\alpha^4(\alpha^4 - 16)}\right)^{\bar{\tau}} \\ &= \left(\frac{(\beta^8 + 224\beta^4 + 256)^3}{\beta^4(\beta^4 - 16)^4}\right)^{\bar{\tau}} \\ &= \left(\frac{(\sigma(\beta)^8 + 224\sigma(\beta)^4 + 256)^3}{\sigma(\beta)^4(\sigma(\beta)^4 - 16)^4}\right)^{\bar{\tau}}, \end{aligned}$$

since $r(z) = \frac{(z^8+224z^4+256)^3}{z^4(z^4-16)^4}$ is invariant under the substitution $(z \rightarrow \sigma(z))$. (See [m1, Thm. 5.2] or [lm, Section 8].) Thus, (32) gives that

$$\begin{aligned} j(E_1(\alpha^{\bar{\tau}})) &= \frac{((16-\beta^4)^2 + 224(16-\beta^4) + 256)^3}{(16-\beta^4)\beta^{16}} \\ &= \frac{(\beta^8 - 256\beta^4 + 4096)^3}{\beta^{16}(16-\beta^4)} \\ &= j(E_3(\beta)). \end{aligned}$$

From the isomorphism just established and the beginning remarks in Section 4, we have an isogeny

$$\varphi_1 = \bar{\iota} \circ \psi_{\alpha^{\bar{\tau}}} \circ \iota_3 \circ \rho_\beta \tag{33}$$

of degree 4 from $E_2(\beta)$ to $E_2(\beta^{\bar{\tau}})$, where $\bar{\iota}$ and ι_3 are isomorphisms

$$\bar{\iota} : E_2(\alpha^{\bar{\tau}}) \rightarrow E_2(\beta^{\bar{\tau}}), \quad \iota_3 : E_3(\beta) \rightarrow E_1(\alpha^{\bar{\tau}}).$$

(Note that $E_2(\alpha^{\bar{\tau}}) \cong E_2(\beta^{\bar{\tau}})$ by the beginning of the proof of Theorem 6.) Applying the isomorphism $\bar{\tau}^{i-1}$ to the coefficients gives an isogeny $\varphi_i : E_2(\beta^{\bar{\tau}^{(i-1)}}) \rightarrow E_2(\beta^{\bar{\tau}^i})$, and therefore an isogeny

$$\varsigma = \varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_1 : E_2(\beta) \rightarrow E_2(\beta), \tag{34}$$

since $\bar{\tau}^n = 1$. This isogeny has degree $\deg(\varsigma) = 4^n$, and I claim that

$$\Phi_{4^n}(j_2(\beta), j_2(\beta)) = 0, \tag{35}$$

where $\Phi_m(X,Y)=0$ is the modular equation. (See [co1] and [d1].) It is well-known that (35) is equivalent to the assertion that $\ker(\varsigma) \subset E_2(\beta)$ is cyclic.

From (28), the points of order 2 on $E_2(\beta)$ are

$$\left(0, -\frac{1}{\beta^4}\right), \quad \left(-\frac{1}{4}, \frac{1}{8}-\frac{1}{\beta^4}\right), \quad \left(-\frac{4}{\beta^4}, \frac{1}{\beta^4}\right). \tag{36}$$

The last of these points is in $\ker(\rho_\beta)$, and ρ_β maps the first two points to the point $P_1 = \left(-\frac{1}{4}, \frac{2}{\alpha^4}\right)$ on $E_3(\beta)$. The other two points of order 2 on $E_3(\beta)$ are the points

$$P_2, P_3 = \left(-8\frac{\alpha^2 \pm \sqrt{-1}\beta^2}{\alpha^2\beta^4}, 2\frac{\alpha^2 \pm 2\sqrt{-1}\beta^2}{\alpha^2\beta^4}\right).$$

From (23), with α replaced by $\alpha^{\bar\tau}$, the points of order 2 on $E_1(\alpha^{\bar\tau})$ are

$$Q_1 = \left(\frac{-1}{(\alpha^{\bar\tau})^4}, 0\right), \; Q_2 = \left(-\frac{(\beta^{\bar\tau})^2-4}{8(\beta^{\bar\tau})^2}, \frac{((\beta^{\bar\tau})^2-4)^2}{32(\beta^{\bar\tau})^4}\right), Q_3 = \left(-\frac{(\beta^{\bar\tau})^2+4}{8(\beta^{\bar\tau})^2}, \frac{((\beta^{\bar\tau})^2+4)^2}{32(\beta^{\bar\tau})^4}\right).$$

Now from (32) we have that

$$\sigma(\beta^{\bar\tau})^4 = -\frac{16\beta^4}{\alpha^4},$$

which implies that

$$\sigma(\beta^{\bar\tau}) = \frac{2\beta}{\zeta_8\alpha},$$

for some primitive eighth root of unity ζ_8. Therefore, since σ is an involution,

$$\beta^{\bar\tau} = \sigma\left(\frac{2\beta}{\zeta_8\alpha}\right) = 2\frac{\beta+\zeta_8\alpha}{\beta-\zeta_8\alpha}. \tag{37}$$

With (37), the points of order 2 on $E_1(\alpha^{\bar\tau})$ can be expressed in terms of α and β:

$$Q_1 = \left(-\frac{\zeta_8\alpha\beta(\beta^2+\zeta_8^2\alpha^2)}{2(\beta+\zeta_8\alpha)^4}, 0\right), \quad Q_2 = \left(-\frac{\zeta_8\alpha\beta}{2(\beta+\zeta_8\alpha)^2}, \frac{\zeta_8^2\alpha^2\beta^2}{2(\beta+\zeta_8\alpha)^4}\right),$$

$$Q_3 = \left(-\frac{\beta^2+\zeta_8^2\alpha^2}{4(\beta+\zeta_8\alpha)^2}, \frac{(\beta^2+\zeta_8^2\alpha^2)^2}{8(\beta+\zeta_8\alpha)^4}\right).$$

Converting the curves $E_3(\beta)$ and $E_1(\alpha^{\bar{\tau}})$ to Weierstrass normal form and using standard arguments, it can be shown that the X-coordinate of an isomorphism $\iota_3 : E_3(\beta) \to E_1(\alpha^{\bar{\tau}})$ is given by

$$\iota_{3,1}(X) = \frac{\beta^4 + \alpha^4}{(\beta + \zeta_8\alpha)^4} X - \frac{\zeta_8\alpha(\beta^2 + \zeta_8^2\alpha^2)}{2(\beta + \zeta_8\alpha)^3}.$$

Hence, we have that

$$\iota_{3,1}\left(-\frac{1}{4}\right) = -\frac{\beta^2 + \zeta_8^2\alpha^2}{4(\beta + \zeta_8\alpha)^2}.$$

Using (24), and comparing X-coordinates of the different representations of the points of order 2 on $E_1(\alpha^{\bar{\tau}})$, we have

$$\iota_3 \circ \rho_\beta \left(0, -\frac{1}{\beta^4}\right) = Q_3 = \left(-\frac{(\beta^{\bar{\tau}})^2 + 4}{8(\beta^{\bar{\tau}})^2}, \frac{((\beta^{\bar{\tau}})^2 + 4)^2}{32(\beta^{\bar{\tau}})^4}\right). \qquad (38)$$

Now a straightforward calculation shows that

$$\bar{\iota}_1 \circ \psi_{\alpha^{\bar{\tau}},1}\left(-\frac{(\beta^{\bar{\tau}})^2 + 4}{8(\beta^{\bar{\tau}})^2}\right) = \bar{\iota}_1\left(-\frac{1}{4}\right) = 0, \qquad (39)$$

by (29), with α replaced by $\alpha^{\bar{\tau}}$. It follows from (33), (38), (39), and (36), that

$$P = \left(0, -\frac{1}{\beta^4}\right) \implies \varphi_1(P) = \left(0, -\frac{1}{(\beta^{\bar{\tau}})^4}\right) = P^{\bar{\tau}}.$$

Applying $\bar{\tau}^{i-1}$ gives that $\varphi_i(P^{\bar{\tau}^{i-1}}) = P^{\bar{\tau}^i}$, and therefore (34) gives that

$$\varsigma(P) = P^{\bar{\tau}^n} = P.$$

Since P has order 2 on $E_2(\beta)$, this shows that $P \notin \ker(\varsigma)$. It follows that $\ker(\varsigma)$ is a cyclic group, and this implies (35).

Now by a classical result [co1, p.287] we have the factorization

$$\Phi_{4^n}(x, x) = c_n \prod_{-d} H_{-d}(x)^{r(d,4^n)},$$

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

$$r(d, m) = |\{\lambda \in \mathsf{R}_{-d} : \lambda \text{ primitive}, \ N(\lambda) = m\}/\mathsf{R}_{-d}^\times|.$$

The exponent $r(d, 4^n)$ can only be nonzero when $4^k \cdot 4^n = x^2 + dy^2$ has a primitive solution ($k = 0$ or 1). Since $\mathbb{Q}_2(\beta) = \mathbb{Q}_2(\xi)$ is unramified and normal over $\mathbb{Q}_2$, equation (35) implies $j_2(\beta) = j(E_2(\beta))$ is a root of $H_{-d}(x)$ for some odd integer d; hence, $(2, xyd) = 1$ and for $n > 1$ we have $-d \equiv 1 \pmod 8$.

Consequently, equation (22) shows that $\xi^4 = \beta^4/16$ is a root of the polynomial

$$L_d(x) = (x^2 - x)^{2h(-d)} H_{-d}\left(\frac{2^8(x^2 - x + 1)^3}{x^2(x-1)^2}\right).$$

By the proof of [lm, Prop. 8.4], this polynomial factors into a product of three irreducible polynomials of degree $2h(-d)$, exactly one of which has roots which are integral for the prime 2. If this factor is $g(x)$, then from [lm, Eq. (8.4)] and $\deg(g(x)) = 2h(-d)$ it follows that

$$g(x^4) = b_d(x) b_d(-x) h(x), \tag{40}$$

where the irreducible polynomial $h(x) = b_d(ix)b_d(-ix)$ belongs to an extension of $\mathbb{Q}$ which is ramified over $p = 2$. Thus, ξ is a root of one of the first two factors in (40). Now the set of roots of $b_d(x)$ is stabilized by the map $\left(x \rightarrow \frac{x+1}{x-1}\right)$, and that of $b_d(-x)$ is stabilized by $\left(x \rightarrow \frac{1-x}{1+x}\right)$ (see [lm, Prop. 8.2]). But by the factorization of $\mathsf{P}_n(x)$ in Section 3, the roots of $\mathsf{P}_n(x)$ are stabilized by $\left(x \rightarrow \frac{x+1}{x-1}\right)$. If $\frac{1-\xi}{1+\xi}$ were a root of $\mathsf{P}_n(x)$, then

$$\frac{\frac{1-\xi}{1+\xi} + 1}{\frac{1-\xi}{1+\xi} - 1} = \frac{-1}{\xi}$$

would also be a root of $\mathsf{P}_n(x)$. But $\xi \in \mathsf{D}_2$, so $-1/\xi$ is not an algebraic integer, and therefore cannot be a root of $\mathsf{P}_n(x)$. This proves that ξ is a root of the polynomial $b_d(x)$ and hence that $b_d(x)$ divides $\mathsf{P}_n(x)$. From Theorem 4 and (31) we have finally that $\bar{\tau} = \tau^{-2}$, and since ξ generates the ring class field Ω_f over $\mathbb{Q}$ and $\tau^{-2n}(\xi) = T^n(\xi) = \xi$, the automorphism τ^{-2} has order n in $\mathrm{Gal}(\Omega_f/K)$, where $K = \mathbb{Q}(\sqrt{-d})$. Recalling the final remark of Section 3, this completes the proof of Theorem 7. $\square$

For $n = 1$, we have the factorization $\mathsf{P}_1(x) = x(x+1)b_7(x)b_{15}(x)$, by (19). Hence, Theorem 7 and the formulas in (16) imply part (b) of Conjecture 1: all but two of the periodic points of T in $\overline{\mathbb{Q}}_p$ generate ring class fields over $\mathbb{Q}$. In addition, this proves Theorem 2 of the introduction, since the formulas in (16) hold over $\mathbb{Q}$, and therefore also over $\mathbb{C}$.

Denote the set of discrimimants $-d$ referred in Theorem 7 by $\mathfrak{D}_n$. Using (18) and the fact that $\deg(b_d(x)) = 2h(-d)$, Theorem 7 implies the following class number relation.

Theorem 8. *If $h(-d)$ is the class number of the order R_{-d} of discriminant $-d \equiv 1$ (mod 8) in $K = \mathbb{Q}(\sqrt{-d})$, then*

$$\sum_{-d \in \mathfrak{D}_n} h(-d) = nN_4(n) = \sum_{k|n} \mu(n/k) 2^{2k}, \quad n > 1,$$

where $\mathfrak{D}_n$ is the set of discriminants $-d \equiv 1$ (mod 8) for which $\tau^2 = \left(\frac{\Omega_f/K}{\wp_2}\right)^2$ has order n in the Galois group of the corresponding ring class field Ω_f. This equation gives the total number of periodic points of $T(z)$ having minimal period n in the domain $\mathsf{D}_2 := \{y : 0 < |y|_2 \le \frac{1}{2}\} \subset \mathsf{K}_2$. All of these periodic points (for $n > 1$) are prime elements in the local field K_2.

Finally, Theorem 1 summarizes the results in Proposition 3 and Theorems 4, 5, 7, and 8.

6 Examples.

The iterated resultants considered in Section 3 are useful in computing the polynomials $b_d(x)$ which are the minimal polynomials of the periodic points of $T(z)$. For example, factoring $R_2(x)$ on Maple yields the polynomial $\mathsf{P}_1(x)$ in (19) times

$$\begin{aligned}\mathsf{P}_2(x) &= (x^8 + 20x^7 + 110x^6 - 100x^5 + 49x^4 - 80x^3 - 40x^2 + 40x + 16)\\ &\times (x^8 + 6x^7 + 78x^6 - 84x^5 + 53x^4 - 66x^3 - 12x^2 + 24x + 16)\\ &\times (x^8 - 6x^7 + 42x^6 - 60x^5 + 53x^4 - 54x^3 + 24x^2 + 16)\\ &= b_{63}(x) b_{55}(x) b_{39}(x).\end{aligned}$$

(See [lm, Section 12, Table 3].) In addition, factoring $R_3(x)$ on Maple gives $\mathsf{P}_1(x)$ times the polynomial

$$\mathsf{P}_3(x) = A_6(x) A_{12}(x) A_{24}(x),$$

where

$$\begin{aligned}A_6(x) &= (x^6 + x^5 + 9x^4 - 13x^3 + 18x^2 - 16x + 8)\\ &\times (x^6 + 7x^5 + 11x^4 - 15x^3 + 16x^2 - 20x + 8)\\ &= b_{23}(x) b_{31}(x);\end{aligned}$$

$$
\begin{aligned}
A_{12}(x) = (&x^{12} - 262x^{11} + 20035x^{10} + 13096x^9 - 13397x^8 - 15878x^7 - 24435x^6 \\
& - 14516x^5 + 14372x^4 + 15128x^3 + 5440x^2 + 416x + 64) \\
& \times (x^{12} - 36x^{11} + 2271x^{10} + 1586x^9 - 1689x^8 - 1800x^7 - 2527x^6 \\
& - 2310x^5 + 2664x^4 + 832x^3 + 1296x^2 - 288x + 64) \\
& \times (x^{12} - 166x^{11} + 8027x^{10} + 5200x^9 - 5565x^8 - 6446x^7 - 9659x^6 \\
& - 6172x^5 + 6540x^4 + 5600x^3 + 2672x^2 - 32x + 64) \\
& \times (x^{12} + 16x^{11} + 395x^{10} + 398x^9 - 357x^8 - 316x^7 - 155x^6 \\
& - 1058x^5 + 1332x^4 - 704x^3 + 800x^2 - 352x + 64) \\
& \times (x^{12} + 184x^{11} + 57491x^{10} + 39206x^9 - 36669x^8 - 44260x^7 - 70067x^6 \\
& - 41690x^5 + 37644x^4 + 43072x^3 + 13616x^2 + 1472x + 64) \\
& = b_{207}(x)b_{135}(x)b_{175}(x)b_{87}(x)b_{247}(x);
\end{aligned}
$$

and

$$
\begin{aligned}
A_{24}(x) = (&x^{24} - 160x^{23} + 39806x^{22} - 404188x^{21} + 1735295x^{20} - 4082916x^{19} \\
& + 6591016x^{18} - 7995792x^{17} + 7025423x^{16} - 3646952x^{15} - 2986282x^{14} \\
& + 8218276x^{13} - 7410127x^{12} + 8124428x^{11} - 590812x^{10} - 4737592x^9 \\
& + 2208800x^8 - 5462688x^7 + 644992x^6 + 672768x^5 + 631808x^4 + 875008x^3 \\
& + 496640x^2 + 53248x + 4096) \\
& \times (x^{24} + 484x^{23} + 67682x^{22} - 315500x^{21} + 1778351x^{20} - 3320880x^{19} \\
& + 7580476x^{18} - 12603888x^{17} + 15479855x^{16} - 14728444x^{15} + 4226978x^{14} \\
& + 12258548x^{13} - 20944063x^{12} + 22569256x^{11} - 11161888x^{10} - 5859992x^9 \\
& + 9241280x^8 - 9494496x^7 + 2773504x^6 + 2227200x^5 - 1364224x^4 + 780800x^3 \\
& + 708608x^2 + 100352x + 4096) \\
& = b_{231}(x)b_{255}(x).
\end{aligned}
$$

That each of the above polynomials is given by the corresponding $b_d(x)$ can be verified by factoring the polynomial modulo primes of the form $q = x^2 + dy^2$, checking that it splits completely into linear factors (mod q). Thus, we have the factorization

$$\mathsf{P}_3(x) = b_{23}(x)b_{31}(x)b_{207}(x)b_{135}(x)b_{175}(x)b_{87}(x)b_{247}(x)b_{231}(x)b_{255}(x)$$

for the periodic points of minimal period 3.

7 References.

[ch] N. Childress, *Class Field Theory*, Springer, 2009.

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

[co1] David A.Cox, *Primes of the Form $x^2 + ny^2$; Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, 1989.

[co2] David A. Cox, *Galois Theory*, John Wiley & Sons, 2004.

[d1] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamb. 14 (1941), 197-272.

[d2] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jahresber. Deutsch. Math. Verein. 54 (1944), 24-41.

[d3] M. Deuring, Die Klassenkörper der komplexen Multiplikation, Enzyklopädie der math. Wissenschaften I2, 23 (1958), 1-60.

[h1] 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.

[h2] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica Verlag, Würzburg, 1967.

[h3] H. Hasse, *Number Theory*, Springer Verlag, 2002.

[lm] R. Lynch and P. Morton, The quartic Fermat equation in Hilbert class fields of imaginary quadratic fields, http://arxiv.org/abs/1410.3008, Intl. J. of Number Theory 11 (2015), 1961-2017.

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

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

[m3] P. Morton, Solutions of the cubic Fermat equation in ring class fields of imaginary quadratic fields (as periodic points of a 3-adic algebraic function), http://arxiv.org /abs/1410.6798, to appear in Intl. J. Number Theory.

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

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

Department of Mathematical Sciences
Indiana University - Purdue University at Indianapolis
402 N. Blackford St., LD 270
Indianapolis, Indiana, 46202
e-mail: pmorton@math.iupui.edu