ACTA ARITHMETICA
LXXXVII.2 (1998)

Arithmetic properties of periodic points of quadratic maps, II

by

Patrick Morton (Wellesley, Mass.)

1. Introduction. In this paper we prove that the quadratic map $x \to f(x) = x^2 + c$, for c in $\mathbb{Q}$ and x in the complex field $\mathbb{C}$, has no rational 4-cycles. The periodic points of f of minimal period 4 are roots of the 12th degree polynomial,

$$\Phi_4(x,c) = \frac{f^4(x) - x}{f^2(x) - x}$$

(see [bo], [mp], [vh1]), where f^n denotes the nth iterate of f. We show that the curve $\Phi_4(x,c) = 0$ has no rational points by proving it is *modular*, being a model for $X_1(16)$, the compactification of the upper half-plane modulo the action of $\Gamma_1(16) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0, a \equiv d \equiv 1 \pmod{16} \right\}$, and then using results of Washington [w1] on the rational points of $X_1(16)$.

There are no finite rational points on $\Phi_4(x,c) = 0$ even though the curve $\Phi_4(x,c) = 0$ has infinitely many points defined over each p-adic completion $\mathbb{Q}_p$ and over $\mathbb{R}$. The latter property is shared by all the curves $\Phi_n(x,c) = 0$, $n \geq 1$, where $\Phi_n(x,c)$ is the polynomial whose roots are the periodic points of f of minimal period n:

$$\Phi_n(x,c) = \prod_{d|n} (f^d(x) - x)^{\mu(n/d)}.$$

Thus the 12th degree curve $\Phi_4(x,c) = 0$ provides an affine counterexample to the Hasse principle, and may be the first in an infinite family of such examples. The results of [fps] show that f has no rational 5-cycles either, so that the 30th degree curve $\Phi_5(x,c) = 0$ provides another such counterexample.

In a previous version of this paper I asked if the curves $\Phi_n(x,c) = 0$

1991 *Mathematics Subject Classification*: 11D41, 11F03.

The work for this paper was partially supported by a Brachman–Hoffman fellowship from Wellesley College and by NSF Grant DMS-9200575.

with $n \geq 5$ might also be modular, but in [fps] it is shown that $\Phi_5(x,c) = 0$ is definitely not modular, and from the arguments of that paper it seems unlikely that $\Phi_n(x,c) = 0$ would be modular for $n > 5$.

This parametrization of the curve $\Phi_4(x,c) = 0$ by modular functions leads to the simple substitution $c = -1/(4q^2) - 3/4$, which we consider in Section 4. We show in Proposition 5 that all the periodic points of $f_q(x) = x^2 - 1/(4q^2) - 3/4$ in the algebraic closure of the Laurent series field $\mathbb{Q}((q))$ have q-expansions of the form

$$\frac{\pm 1}{2q} \pm \frac{1}{2} + \sum_{k=1}^{\infty} a_k q^k,$$

where the coefficients a_k are rational integers. In particular, when q is a p-adic integer divisible by p, these expansions give convergent p-adic expressions for the roots of the polynomial $\Phi_n(x, -1/(4q^2) - 3/4)$ in $\mathbb{Q}_p$. Formal Laurent series expansions of the periodic points of a quadratic map seem to have been first considered by Bach [ba]. (Cf. also [tvw], [m3, Lemma 1].)

Furthermore, if $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$ is an n-cycle of the map f_q in $\mathbb{Q}((q))$, then

$$\xi_i = \frac{\varepsilon_i}{2q} + \sum_{k=0}^{\infty} a_k^{(i)} q^k,$$

where $\varepsilon_i = \pm 1$, the sequence $\{\varepsilon_k\}_{k \geq 0}$ has minimal period n, and the coefficients $a_k^{(i)}$ satisfy the following system of recurrences:

$$\varepsilon_i a_{k+1}^{(i)} = a_k^{(i+1)} - \sum_{j=0}^{k} a_j^{(i)} a_{k-j}^{(i)} \quad \text{for } k \geq 1 \text{ and } i = 0, \ldots, n-1,$$

with initial conditions $a_0^{(i)} = \varepsilon_i \varepsilon_{i+1}/2$, $a_1^{(i)} = \varepsilon_i (a_0^{(i+1)} + 1/2)$. The sequence $\{a_k^{(0)}\}$ we get in this manner for $n = 1$ is essentially the sequence of Catalan numbers, and for $n = 3$ and 4 the sum of the sequences $\{a_k^{(i)}\}$ in a given orbit appears to be an analogue of the Catalan numbers. It would be interesting to know if, like the Catalan numbers, these sequences have other combinatorial interpretations.

In Section 4, I give an application of the above q-expansions to computing various polynomials related to the dynamical system $x \to x^2 + c$, including the polynomials whose roots are the multipliers (or traces) of the orbits of a given period n.

I am grateful to Joe Silverman for making me aware of the article [w1]. I also thank Franco Vivaldi for his remarks concerning the series expansions in Section 4 and Andrew Bremner for his help in the computations of Section 2.

2. Rational points on $\Phi_4(x,c)=0$. If we let $f(x)=x^2+c$, as above, the polynomial $\Phi_4(x,c)$ is given explicitly by

$$\begin{aligned}\Phi_4(x,c) = {} & x^{12}+6cx^{10}+x^9+(3c+15c^2)x^8+4cx^7+(1+12c^2+20c^3)x^6\\ & +(2c+6c^2)x^5+(4c+3c^2+18c^3+15c^4)x^4+(1+4c^2+4c^3)x^3\\ & +(c+5c^2+6c^3+12c^4+6c^5)x^2+(2c+c^2+2c^3+c^4)x\\ & +1+2c^2+3c^3+3c^4+3c^5+c^6,\end{aligned}$$

and from [mv] the discriminant of $\Phi_4(x,c)$ is

$$\begin{aligned}(1)\qquad \operatorname{disc}_x \Phi_4(x,c) &= (5+4c)^2(5-8c+16c^2)^3(135+108c+144c^2+64c^3)^4\\ &= \Delta_{4,2}^2\Delta_{4,1}^3\Delta_{4,4}^4,\end{aligned}$$

where

$$\Delta_{4,1}(c)=5-8c+16c^2,\qquad \Delta_{4,2}(c)=-(5+4c),$$
$$\Delta_{4,4}(c)=135+108c+144c^2+64c^3.$$

By results of [mv], the roots of $\Delta_{4,d}=0$ for $d=1$ or 2 are the values of c for which one of the 4-cycles collapses to a d-cycle, and the roots of $\Delta_{4,4}=0$ are the values of c for which two 4-cycles coincide.

LEMMA 1. *If p is an odd prime, then $\Phi_4(x,c)$ is irreducible over $\overline{\mathbb{F}}_p$.*

P r o o f. Let $\tau_4(z)$ be the polynomial whose roots are the traces of roots of $\Phi_4(x,c)$ in an orbit, i.e., the numbers $t=\alpha+f(\alpha)+f^2(\alpha)+f^3(\alpha), \Phi_4(\alpha,c)=0$. A computation on Mathematica shows that $\tau_4(z)=z^3+(4c+3)z+4$. This polynomial is irreducible over $\overline{\mathbb{F}}_p$. For if $\tau_4(z)$ were reducible, it could only have a factor of the form $z-a$, where a is constant, and then $z-a$ would have to divide $4z$ and z^3+3z+4, which is impossible if p is odd. We may therefore apply Proposition 18 of [m3], which states that $\Phi_4(x,c)$ is irreducible over $\overline{\mathbb{F}}_p$ for any odd prime p for which $\tau_4(z)$ is irreducible and for which two conditions hold:

(i) p does not divide disc $\Delta_{4,1}(c)=-256$;

(ii) some irreducible factor of $\Delta_{4,1}(c) \pmod p$ does not divide $\Delta_{4,2}(c)$.

Since $\operatorname{Res}(\Delta_{4,1}(c),\Delta_{4,2}(c))=2^7\cdot 5$, it suffices to check condition (ii) for the prime 5: $\Delta_{4,1}(c)=c(c+2)$, $\Delta_{4,2}(c)=c \pmod 5$. This proves the lemma.

Lemma 1 implies that the equation $\Phi_4(x,c)=0$ defines a function field $K=\mathbb{Q}(x,c)$ of degree 12 over $\mathbb{Q}(c)$. Since the map $\sigma:(x,c)\to(f(x),c)$ is an automorphism of $K/\mathbb{Q}(c)$ it follows that the fixed field K_σ of this automorphism has degree 3 over $\mathbb{Q}(c)$. As in Lemma 1, we let z be the trace of x to the field K_σ:

$$\begin{aligned}(2)\qquad z &= \operatorname{tr}_{K_\sigma/\mathbb{Q}(c)}(x)=(1+\sigma+\sigma^2+\sigma^3)(x)\\ &= (1+\sigma)(1+\sigma^2)(x)=(1+\sigma)w,\end{aligned}$$

where

$$w = (1+\sigma^2)(x) = x + f^2(x) = x^4 + 2cx^2 + x + c + c^2. \tag{3}$$

A straightforward computation shows that

$$z = x^8+4cx^6+(1+2c+6c^2)x^4+(1+2c+4c^2+4c^3)x^2+x+3c+2c^2+2c^3+c^4.$$

The quantity x has degree 12 over $\mathbb{Q}(c)$, so this computation shows that $z \notin \mathbb{Q}(c)$ and z generates K_σ over $\mathbb{Q}(c)$. As was already pointed out in the proof of Lemma 1, the minimal polynomial of z is $h(Z) = Z^3+(4c+3)Z+4$, which implies that $c = (-z^3-3z-4)/(4z)$. Hence $K_\sigma = \mathbb{Q}(z)$ is rational. Furthermore, the minimal polynomial of w over $K_\sigma = \mathbb{Q}(z)$ is $k(W) = W^2 - zW - 1$, so that $z = (w^2-1)/w$ and the intermediate field $\mathbb{Q}(w)$ between K_σ and K is also rational.

By factoring $\Phi_4(x,c) = \Phi_4(x,(-z^3-3z-4)/(4z))$ over K_σ we find that x is a root of the quartic polynomial

$$p(X,z) = X^4 - zX^3 - \frac{z^2+3z+4}{2z}X^2 + \frac{z^3+2z^2+5z+8}{4}X - \frac{z^6+2z^5+4z^4+6z^3-5z^2-8z-16}{16z^2}. \tag{4}$$

This gives a generic factorization which is similar to the factorization of $\Phi_3(x,-(s^2+7)/4)$ in [m1, Lemma 4]. Similarly, after replacing z by $(w^2-1)/w$ and factoring over $\mathbb{Q}(w)$ we find that x is a root of the quadratic polynomial

$$q(x,w) = x^2 - wx + \frac{w^6-2w^4-2w^3-2w+1}{4w^2(w^2-1)}.$$

We have

$$\operatorname{disc}_x q(x,w) = \frac{(w^2+1)(w^2+2w-1)}{w^2(w^2-1)},$$

and so $\mathbb{Q}(x,c)$ is generated over $\mathbb{Q}(w)$ by the square root of this discriminant. In particular, the genus of $\mathbb{Q}(x,c)$ is 2 (cf. [bo] or [m3, Theorem C]). Summarizing, we have

PROPOSITION 2. *The curve defined by $\Phi_4(x,c) = 0$ has genus 2. Its function field is generated by w and Δ, where $\Delta^2 = (w^4-1)(w^2+2w-1)$ and x is determined by*

$$x = \frac{w}{2} \pm \frac{\Delta}{2(w^3-w)}. \tag{5}$$

Moreover, w is given in terms of x and c by equation (3).

Because the discriminant of $(w^4-1)(w^2+2w-1)$ is -2^{21}, the above calculations are also valid in characteristic p, where p is odd, and 2 is the only prime of bad reduction for the curve $\Phi_4(x,c) = 0$.

In order to show that the curve $\Phi_4(x,c) = 0$ is modular, we put $u = -(w+1)/(w-1)$. Then

$$w = \frac{u-1}{u+1}, \qquad \Delta^2 = (w^4-1)(w^2+2w-1) = \frac{-16u(u^2+1)(u^2-2u-1)}{(u+1)^6}.$$

Setting $v = (u+1)^3\Delta/4$ gives the birationally equivalent curve

$$v^2 = u(u^2+1)(1+2u-u^2). \tag{6}$$

This is the equation given by Washington [w1, p. 774] for the modular curve $X_1(16)$. The above discussion proves

PROPOSITION 3. *The curve $\Phi_4(x,c) = 0$ is birationally equivalent to the modular curve $X_1(16)$.*

THEOREM 4. *There are no finite rational solutions (x,c) of the equation $\Phi_4(x,c) = 0$. In other words, there are no rational values of c for which the quadratic map $f(x) = x^2 + c$ has a rational 4-cycle.*

P r o o f. From (5) we have

$$x = \frac{u-1}{2(u+1)} \pm \frac{v}{2u(u-1)}.$$

Washington [w1] shows that the only rational points on the curve (6) are the six points $(0,0)$, $(\pm1, \pm2)$ and the point at infinity (see [w1]). Hence the only prime divisors of the function field of (6) having degree 1 over $\mathbb{Q}$ are the six prime divisors $p_\infty, p, q_1, q_2, r_1, r_2$ for which, in multiplicative notation,

$$(u) = \frac{p^2}{p_\infty^2}, \qquad (v) = \frac{pa}{p_\infty^5},$$
$$(u-1) = \frac{q_1q_2}{p_\infty^2}, \qquad (u+1) = \frac{r_1r_2}{p_\infty^2},$$
$$(v-2) = \frac{q_1r_1b_1}{p_\infty^5}, \qquad (v+2) = \frac{q_2r_2b_2}{p_\infty^5}.$$

Here a, b_1 and b_2 are divisors which do not involve any of the six primes listed above. To prove the theorem, it suffices to show that each of these six prime divisors is a pole divisor of x. From the above equations it is clear that the pole divisor of $v/(u(u-1))$ is $pp_\infty q_1q_2$, and the pole divisor of $(u-1)/(u+1)$ is r_1r_2. Hence the pole divisor of x is exactly the product of these six primes (agreeing with the fact that $[K : \mathbb{Q}(x)] = 6$). This proves the theorem.

3. Four-cycles of quadratic maps and modular functions. We pursue the connection between our curve and $X_1(16)$ more fully by using

$\Phi_1(x) = f(x) - x = x^2 - x + c$ to define the expression

$$\begin{aligned}\eta &= \frac{\Phi_1(f^2(x))}{\Phi_1(x)} \\ &= x^6 + x^5 + (3c+1)x^4 + (2c+1)x^3 \\ &\quad + (3c^2+3c)x^2 + (c^2+2c)x + c^3 + 2c^2 \\ &= (x^2+x+c)(x^4 + (2c+1)x^2 + c^2 + 2c).\end{aligned}$$

By results of [ms] this expression is a unit in the ring $\mathbb{Q}[x,c]$. (In [ms] it is called a dynamical unit since it is defined in terms of the dynamics of the map $x \to f(x)$.) This is convenient since η is conjugate to its reciprocal:

$$\sigma^2(\eta) = \frac{\Phi_1(x)}{\Phi_1(f^2(x))} = \frac{1}{\eta}.$$

It follows that η is quartic over $K_\sigma = \mathbb{Q}(z)$, and is expressed in terms of x and z by

$$\begin{aligned}(7)\qquad \eta &= \frac{-12 - 7z + 6z^2 + 2z^3 + 2z^4 + z^5}{8} - \frac{4 + 9z + 7z^2 + 3z^3 + z^4}{4}x \\ &\quad + \frac{3z - z^3}{2}x^2 + (z + z^2)x^3.\end{aligned}$$

With this expression the minimal polynomial of η over K_σ is easily seen to be

$$h_\eta(Y) = Y^4 - z^2Y^3 - (z^3 + 2z^2 + 4z + 2)Y^2 - z^2Y + 1.$$

But this is the same polynomial that Washington gives as $f_H(X)$ in [w1]:

$$f_H(X) = X^4 - H^2X^3 - (H^3 + 2H^2 + 4H + 2)X^2 - H^2X + 1.$$

The function H is a modular function on $\Gamma_0(16)$, the "Hauptmodul", which generates the function field for the curve $X_0(16)$:

$$\begin{aligned}(8)\qquad H(\tau) &= \frac{2\sum_{n\in\mathbb{Z}} q^{(2n)^2}}{\sum_{n\in\mathbb{Z}} q^{(2n+1)^2}} \\ &= \frac{1}{q} + 2q^3 - q^7 + \ldots = \frac{\prod_{n=0}^{\infty}(1+q^{8n+4})^2}{q\prod_{n=1}^{\infty}(1+q^{8n})^2}, \qquad q = e^{2\pi i\tau}.\end{aligned}$$

The polynomial $f_H(X)$ is the minimal polynomial over $\mathbb{C}(H)$ of the function

$$(9)\qquad \beta_1(\tau) = q^{-2} \prod_{\substack{n\equiv\pm5,\pm7 \pmod{16}\\ n>0}} (1-q^n) \prod_{\substack{n\equiv\pm1,\pm3 \pmod{16}\\ n>0}} (1-q^n)^{-1},$$

and of its "conjugate" function

$$(10)\qquad \beta_2(\tau) = -q^{-1} \prod_{\substack{n\equiv\pm3,\pm7 \pmod{16}\\ n>0}} (1-q^n) \prod_{\substack{n\equiv\pm1,\pm5 \pmod{16}\\ n>0}} (1-q^n)^{-1},$$

both of which are modular functions for $\Gamma_1(16)$. (See [w1]. I use β_i in place of Washington's notation α_i^*. There is a misprint in the definition of the function α_2 in [w1]: the Klein forms $k(0,1/16)$ and $k(0,3/16)$ should be interchanged in the formula for α_2 on p. 772. This gives the above product expansion (10) of $\beta_2 = \alpha_2^*$, in which the positions of the terms with $n \equiv \pm 1$ and $n \equiv \pm 3 \pmod{16}$ are reversed from what they are in [w1]. This misprint does not affect any of Washington's arguments.)

Thus we can give an explicit parametrization of the curve $\Phi_4(x,c) = 0$ by setting $z = H(\tau)$, $\eta = \beta_1(\tau)$. From our calculations above we have immediately

$$c = c(\tau) = -\frac{H^3 + 3H + 4}{4H}. \tag{11}$$

Using (7) and (4) we also find that

$$\begin{aligned} z(z+2)x = {} & \tfrac{1}{2}(z+1)(z^2 - 2z - 2) + z(z+1)(z^2 + z + 2)\eta \\ & + (z+1)(z^2 - z + 1)\eta^2 - z\eta^3. \end{aligned} \tag{12}$$

Hence the curve $\Phi_4(x,c) = 0$ can be parametrized in terms of H and β_1 by (11) and

$$\begin{aligned} x = x(\tau) = {} & \frac{\tfrac{1}{2}(H+1)(H^2 - 2H - 2) + H(H+1)(H^2 + H + 2)\beta_1}{H(H+2)} \\ & + \frac{(H+1)(H^2 - H + 1)\beta_1^2 - H\beta_1^3}{H(H+2)}. \end{aligned} \tag{13}$$

From (8) and (9), (11) and (12) we find the q-expansions

$$\begin{aligned} c(\tau) = {} & \frac{-1}{4q^2} - \frac{3}{4} - q - q^2 + 2q^5 - \frac{1}{2}q^6 - 5q^9 + 2q^{10} + 10q^{13} \\ & + \frac{1}{4}q^{14} - 18q^{17} - 5q^{18} + 32q^{21} + \frac{1}{2}q^{22} + \dots, \end{aligned} \tag{14}$$

$$\begin{aligned} x(\tau) = {} & \frac{1}{2q} + \frac{1}{2} + q + q^3 - q^4 - q^5 + q^6 - \frac{1}{2}q^7 + q^8 + q^9 \\ & - q^{10} - q^{12} - 2q^{13} - \frac{1}{2}q^{15} + 3q^{16} + 4q^{17} - q^{18} \\ & + 2q^{19} - 5q^{20} - 4q^{21} + 3q^{22} + \dots \end{aligned} \tag{15}$$

It is clear from (8), (9), (11) and (13) that $c(\tau)$ has coefficients in $(1/4)\mathbb{Z}$ and $x(\tau)$ has coefficients in $(1/2)\mathbb{Z}$. By (2), the Hauptmodul H can be recovered as the trace of the function $x(\tau)$:

$$H(\tau) = x + f(x) + f^2(x) + f^3(x), \qquad x = x(\tau).$$

This parametrization raises the question: how does the automorphism $\sigma : x \to f(x) = x^2 + c$ sit inside the automorphisms of $\mathbb{C}(H, \beta_1)/\mathbb{C}(H)$? Using

the above results and [w1, p. 772] it is not hard to check that σ coincides with the action of the linear fractional transformation $\tau \to (11\tau-2)/(-16\tau+3)$: if $q = e^{2\pi i\tau}$ and $A = \left(\begin{smallmatrix} 11 & -2 \\ -16 & 3 \end{smallmatrix}\right)$, then $x(\tau)|A = x^2(\tau) + c(\tau)$.

The above parametrization yields q-expansions for one 4-cycle of the map f. The following proposition shows that there are q-expansions for *all* of the n-periodic points of $f(x) = x^2 + c$, for $c = -(H^3 + 3H + 4)/(4H)$, for *any* $n \geq 1$ (cf. [m3, Lemma 1], [ba] and [tvw]).

PROPOSITION 5. *Let c be the formal power series*

$$c = -\frac{1}{4q^2} - \frac{3}{4} + \sum_{k=1}^{\infty} c_k q^k,$$

where the c_k are rational numbers. If $n \geq 1$, then all the n-periodic points of $f(x) = x^2 + c$ in the algebraic closure of $\mathbb{Q}((q))$ lie in $\mathbb{Q}((q))$ and have the form

$$\xi_n = \pm\frac{1}{2q} \pm \frac{1}{2} + \sum_{k=1}^{\infty} a_k q^k, \tag{16}$$

where the coefficients a_k (for $k \geq 1$) lie in $\mathbb{Z}[c_1, c_2, \ldots]$. In the case where c is given by (11)*, the a_k lie in $(1/2)\mathbb{Z}$.*

Proof. We let $\{\varepsilon_0, \varepsilon_1, \ldots\}$ be an infinite sequence of ± 1's. We will first show that there is a unique series ξ_n of the form (16) for which

$$f^j(\xi_n) = \varepsilon_j \frac{1}{2q} + O(1) \quad \text{for } j \geq 0, \tag{17}$$

where $O(1)$ represents a power series in $\mathbb{Q}[[q]]$. If $\xi_n = \varepsilon_0/(2q) + \ldots$ is a series of the form (16), then

$$\begin{aligned} f(\xi_n) &= \left(\varepsilon_0 \frac{1}{2}\frac{1}{q} + a_0 + \sum_{k=1}^{\infty} a_k q^k\right)^2 - \frac{1}{4q^2} - \frac{3}{4} + \sum_{k=1}^{\infty} c_k q^k \\ &= \frac{\varepsilon_0 a_0}{q} + \varepsilon_0 a_1 + a_0^2 - \frac{3}{4} + \sum_{k=1}^{\infty} \Big(\varepsilon_0 a_{k+1} + c_k + \sum_{i+j=k} a_i a_j\Big) q^k. \end{aligned} \tag{18}$$

For condition (17) to hold with $i = 1$ we must have $a_0 = \varepsilon_0\varepsilon_1/2$. Then for $f^2(\xi_n)$ to be $\varepsilon_2/(2q) + O(1)$ it is necessary that $\varepsilon_0 a_1 - 1/2 = \pm 1/2 = \varepsilon_1\varepsilon_2/2$, i.e., a_1 is determined by ε_2 and equals $-1, 0$ or 1. If the coefficients a_k have been determined for $k \leq i-1$ so that (17) holds for $j \leq i$, then

$$f^i(\xi_n) = \frac{\varepsilon_i}{2q} + b_0 + \sum_{k=1}^{\infty} b_k q^k,$$

where

$$b_k = \varepsilon_0\varepsilon_1 \ldots \varepsilon_{i-1} a_{k+i} + p_k(c_1, \ldots, c_{k+i-1}, a_1, \ldots, a_{k+i-1}), \quad k \geq 0,$$

and the polynomial p_k has integer coefficients for $k \geq 1$. (Note that the terms involving a_0 in $\sum_{i+j=k} a_i a_j$ combine to give $2a_0 a_k = \pm a_k$.) Hence condition (17) with $j = i+1$, and equation (18) with ε_i for ε_0, b_0 for a_0 and b_1 for a_1, determine $b_0 = \pm 1/2$ and a_i uniquely. This proves existence and uniqueness of the series ξ_n.

Now consider a periodic sequence $\{\varepsilon_0, \varepsilon_1, \ldots\}$ with period n. The unique series ξ_n satisfying (17) must be an n-periodic point of f by virtue of the equations

$$f^i(f^n(\xi_n)) = \varepsilon_{i+n}/(2q) + O(1) = \varepsilon_i/(2q) + O(1) = f^i(\xi_n) \quad \text{for } i \geq 0.$$

Since there are 2^n distinct periodic sequences $\{\varepsilon_0, \varepsilon_1, \ldots\}$ having period n, and distinct sequences correspond to different periodic points, all of the 2^n n-periodic points of f are accounted for by this method and lie in $\mathbb{Q}((q))$.

We can also show that the coefficients a_k, for $k \geq 1$, of any n-periodic point ξ_n lie in the ring $\mathbb{Z}[c_1, c_2, \ldots]$. This is clear for $k = 1$ since $a_1 = 0$ or ± 1 from above. Suppose this is true of the coefficients a_i for $i \leq k$, for any n-periodic point ξ_n. If a_k and a'_k are the coefficients of ξ_n and $f(\xi_n)$, respectively, then from (18) we have $\varepsilon_0 a_{k+1} + c_k + \sum_{i+j=k} a_i a_j = a'_k$, whence the claim follows for a_{k+1}.

If the c_k all lie in $\mathbb{Z}$, for $k \geq 1$, then the same is true of the a_k, by this argument. It remains to prove the claim that $a_k \in (1/2)\mathbb{Z}$ if the series c is defined by (11). The series ξ_n and c satisfy the relation $\Phi_n(\xi_n, c) = 0$, where

$$\Phi_n(x, c) = \prod_{d|n} (f^d(x) - x)^{\mu(n/d)} = \prod_i (x \pm 1/(2q) + a_0^{(i)} + \ldots),$$

and the second product is over the $d_n = \deg_x \Phi_n(x, c)$ primitive n-periodic points of $f(x)$. I claim that $(2q)^{d_n} \Phi_n(x, c) = A_n(2qx, 4q^2 c)$, where $A_n(u, v)$ is a polynomial with coefficients in $\mathbb{Z}[q]$ and is monic in u. To see this, it suffices to show that any term $c^k x^l$ in Φ_n satisfies $2k + l \leq d_n$. From the above product for $\Phi_n(x, c)$ it is clear that the leading term of the coefficient of x^l has degree $\geq -(d_n - l)$ in q. Since $\deg_q c = -2$, it follows that $-2k \geq -(d_n - l)$, or that $2k + l \leq d_n$ holds, as claimed.

Because the series $4q^2 c$ lies in $\mathbb{Z}[[q]]$ it follows that $2q\xi_n$ is integral over $\mathbb{Z}[[q]]$. But the ring $\mathbb{Z}[[q]]$ is integrally closed in its quotient field $\mathbb{Q}((q))$. (This follows from the fact that $\mathbb{Z}_p[[q]]$, as a unique factorization domain, is integrally closed in $\mathbb{Q}_p((q))$, for all primes p; cf. [w2, p. 115 and p. 268].) Hence $2q\xi_n$ lies in $\mathbb{Z}[[q]]$, i.e., the coefficients of ξ_n lie in $(1/2)\mathbb{Z}$, as claimed.

A similar proposition can be proved for maps of the form $f(x) = x^2 + qx$.

4. The substitution $c = -1/(4q^2) - 3/4$ and remarks on computation. Proposition 5 suggests using the simpler substitution $c = -1/(4q^2) - 3/4$ in place of the substitution $c = -(H^2 + 3H + 4)/(4H)$. In this case the

coefficients a_k ($k \geq 1$) of all the periodic points of $f(x) = x^2+c$ lie in $\mathbb{Z}$. With a slight variation from the notation in Section 3 we let $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$ be an n-cycle of the map $f_q(x) = x^2 - 1/(4q^2) - 3/4$ in the field $\mathbb{Q}((q))$, for $n \geq 1$, and we set

$$\xi_i = \frac{\varepsilon_i}{2q} + \sum_{k=0}^{\infty} a_k^{(i)} q^k,$$

where $\varepsilon_i = \pm 1$ and the sequence $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$ has minimal period n. Note that the orbit $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$ is completely determined by the sequence $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$, by Proposition 5. Equation (18) and the equation $f(\xi_i) = \xi_{i+1}$ imply the following system of recurrences for the coefficients of the ξ_i:

$$\varepsilon_i a_{k+1}^{(i)} = a_k^{(i+1)} - \sum_{j=0}^{k} a_j^{(i)} a_{k-j}^{(i)} \quad \text{for } k \geq 1 \text{ and } i = 0, \ldots, n-1, \tag{19}$$

with the initial conditions

$$a_0^{(i)} = \varepsilon_i \varepsilon_{i+1}/2, \quad a_1^{(i)} = \varepsilon_i (a_0^{(i+1)} + 1/2). \tag{20}$$

Proposition 6. *The curve $\Phi_n(x, c) = 0$ has infinitely many points defined over the p-adic field $\mathbb{Q}_p$, for any prime p.*

Proof. Set $c = -1/(4q^2) - 3/4$, where q is any p-adic integer divisible by p. Then the series given above for ξ_i is clearly convergent in $\mathbb{Q}_p$, and the computations of Proposition 5 show that this series represents a root of $\Phi_n(x, c)$ in $\mathbb{Q}_p$.

It can also be shown that the series ξ_i is convergent for complex q satisfying $|q|^{-1} > M$ for large enough M, so that $\Phi_n(x, c) = 0$ also has infinitely many points defined over $\mathbb{R}$. Alternatively, by [m1, Thm. 4] or [rw], the rational curve $\Phi_3(x, c) = 0$ has infinitely many real points (x, c), and for any such c, $f(x) = x^2 + c$ has real periodic points of all periods, by Sharkovskiĭ's theorem [de, p. 60]. This implies that $\Phi_n(x, c) = 0$ violates the Hasse principle whenever $\Phi_n(x, c) = 0$ has no finite rational points. By Theorem 4 and the results of [fps], this is the case for $n = 4$ and 5.

The q-series we get with $c = -1/(4q^2) - 3/4$ are particularly useful for computing various polynomials related to the dynamical system $x \to x^2 + c$, including the multiplier polynomial $\delta_n(x, c)$, whose roots are the multipliers of the different orbits of a given period n (see [vh1], [vh2], [mv]), and the trace polynomial $\tau_n(x, c)$, whose roots are the traces of the different orbits. We now indicate how the polynomial $\tau_n(x, c)$ may be computed.

Using the map $f_q(x) = x^2 - 1/(4q^2) - 3/4$, find the q-expansion of the trace $z_i(q)$ of the ith orbit of period n, where $1 \leq i \leq r$ and r is the total number of orbits of period n. This is very easy to do using the above

recurrences (19)–(20). Then form the polynomial

$$\tau(x,q)=\prod_{i=1}^{r}(x-z_i(q)).$$

Since this polynomial, when expressed in terms of x and c, lies in $\mathbb{Z}[x,c]$, no positive powers of q will occur in the coefficients. Therefore it is only necessary to compute to the term q^{r-1} in $z_i(q)$ in order to get an accurate result; if the $z_i(q)$ are known to the q^{r-1} term, then the product of d of these series will be correct to the q^{r-d} term. Once the product $\tau(x,q)$ has been computed, drop all positive powers of q, and then substitute $q^2=-1/(4c+3)$ in the coefficients of $\tau(x,q)$ to get $\tau_n(x,c)$.

For example, with $n=5$, we compute

$$z_1(q)=\frac{3}{2q}+\frac{1}{2}+q-2q^2-3q^3+4q^4-4q^5+O(q^6)\quad\text{for orbit }(++++-),$$
$$z_2(q)=\frac{1}{2q}+\frac{1}{2}+q+2q^2+5q^3-2q^4-8q^5+O(q^6)\quad\text{for orbit }(+++--),$$
$$z_3(q)=\frac{1}{2q}-\frac{3}{2}-q+q^3-2q^4+2q^5+O(q^6)\quad\text{for orbit }(++-+-).$$

Then

$$\begin{aligned}\tau(x,q)&=\prod_{i=1}^{3}(x-z_i(q))(x-z_i(-q))\\&=x^6+x^5-\left(\frac{21}{4}+\frac{11}{4q^2}\right)x^4\\&\quad-\left(\frac{5}{2}+\frac{9}{2q^2}\right)x^3+\left(\frac{647}{16}+\frac{19}{8q^2}+\frac{19}{16q^4}\right)x^2\\&\quad+\left(\frac{1017}{16}+\frac{99}{8q^2}+\frac{17}{16q^4}\right)x+\frac{1901}{64}+\frac{269}{64q^2}+\frac{79}{64q^4}-\frac{9}{64q^6}.\end{aligned}$$

Putting $-(4c+3)$ for $1/q^2$ yields the polynomial

$$\begin{aligned}\tau_5(x,c)&=x^6+x^5+(3+11c)x^4+(11+18c)x^3+(44+19c+19c^2)x^2\\&\quad+(36-24c+17c^2)x+32+28c+40c^2+9c^3.\end{aligned}$$

A similar computation shows that

$$\begin{aligned}\tau_6(x,c)&=x^9-x^8+(2+24c)x^7+(14+8c)x^6+(49+16c+144c^2)x^5\\&\quad+(175+16c+112c^2)x^4+(140-136c+160c^2+256c^3)x^3\\&\quad+(196+552c+480c^2+256c^3)x^2\\&\quad+(448+416c-304c^2-256c^3)x-384c-592c^2-256c^3.\end{aligned}$$

The fact that $\operatorname{disc}_x \tau_n(x,c)$ is equal to a square times the polynomial $\Delta_{n,n}(c)$ (by [m3, Corollary 3 to Theorem B, and Proposition 9d]), whose roots are the complex values of c for which two n-cycles collide, allows an efficient means of computing the latter polynomial (see [mv]).

Exactly the same process works for the multiplier polynomial $\delta_n(x,c)$, except that here the individual periodic points need to be computed to the term q^{nr-1} in order that the multiplier, which is a product of n series in an orbit, may be correct up to the term $q^{n(r-1)}$ (the leading term of the q-series for a multiplier is $\pm 1/q^n$; cf. [vh2]).

The q-series can also be used to establish irreducibility in individual cases. For example, we may use the above series $z_i(q)$ to show that $\tau_5(x,c)$ is irreducible over any field F of odd characteristic. Since $c = -1/(4q^2) - 3/4$ is invariant under $q \to -q$, the same must be true of any irreducible factor of $\tau_5(x, -1/(4q^2) - 3/4)$. If the latter is reducible, then it must have an irreducible factor of the form $(x - z_i(q))(x - z_i(-q))$. But it is easy to see that positive powers of q will occur in each of the sums $z_i(q) + z_i(-q)$:

$$\begin{aligned} z_1(q) + z_1(-q) &= 1 - 4q^2 + 8q^4 + \dots, \\ z_2(q) + z_2(-q) &= 1 + 4q^2 - 4q^4 + \dots, \\ z_3(q) + z_3(-q) &= -3 - 4q^4 + \dots \end{aligned}$$

Hence no combination $(x - z_i(q))(x - z_i(-q))$ lies in $F[x,c]$, which proves the claim that $\tau_5(x,c)$ is irreducible over F.

As in Section 2 the irreducibility of $\tau_5(x,c)$ and Proposition 18 of [m3] may be used to show that $\Phi_5(x,c)$ is irreducible over any field of odd characteristic (see [mv] for the computation of the polynomials $\Delta_{5,1}(c)$ and $\Delta_{5,5}(c)$). A somewhat more elaborate calculation shows the same for $\tau_6(x,c)$ and $\Phi_6(x,c)$ (see [m3]). I conjecture that this is true of the polynomials $\tau_n(x,c)$ and $\Phi_n(x,c)$, for any n.

5. Cyclic quartic extensions with quadratic automorphisms. In this section we use the arithmetic of the function field K developed in Sections 2 and 3 to characterize the quartic fields considered in [w1] by means of their automorphism polynomials. At the same time this gives a characterization of the cyclic quartic extensions of $\mathbb{Q}$ which have $\theta \to \theta^2 + a$ as an automorphism. The fields that Washington considers are defined using the polynomial

$$f_h(x) = x^4 - h^2x^3 - (h^3 + 2h^2 + 4h + 2)x^2 - h^2x + 1.$$

Whenever $f_h(x)$ is irreducible over F, its roots generate a cyclic quartic extension of F.

THEOREM 7. *Let F be a field whose characteristic is different from* 2, *and let N be a cyclic quartic extension of F. The following are equivalent*:

(a) *There is an h in F so that $f_h(x)$ is irreducible over F and N is generated by a root of $f_h(x)$.*

(b) *There are a in F and θ in N so that $N = F(\theta)$ and* $\mathrm{Gal}(N/F)$ *is generated by the map $\theta \to \theta^2 + a$.*

In other words, a field N is one of Washington's cyclic quartic fields if and only if there is a generator of $\mathrm{Gal}(N/F)$ *whose automorphism polynomial* (*in terms of an appropriate generator*) *is quadratic.*

REMARK. 1) If an automorphism of $\mathrm{Gal}(N/F)$ is expressible as a quadratic polynomial in some generator of N, then by completing the square it is easy to see that this polynomial may be taken to have the form $x^2 + a$.

2) The proof will show that the quantities a and h are related by $a = -(h^3 + 3h + 4)/(4h)$.

3) See [m2, Theorem 2] for an analogous result concerning cyclic cubic extensions.

P r o o f (of Theorem 7). First assume that $N = F(\theta)$ is a cyclic quartic extension of F and that $\theta \to \theta^2 + a$ is a generating automorphism for N/F. Then (θ, a) is a point on the curve $\Phi_4(x, c) = 0$; hence, there is a prime divisor P of the function field $K = F(x, c)$ for which $x \equiv \theta$ and $c \equiv a \pmod P$. Further, if $t = \mathrm{trace}_F\, \theta$, then $z \equiv t \pmod P$, so that (t, a) satisfies the equation $t^3 + (4a + 3)t + 4 = 0$. It follows that $t \neq 0$ by assumption on the characteristic of F. Thus $a = -(t^3 + 3t + 4)/(4t)$, and looking at $p(x, z) = 0$ (see (4)) modulo P gives that $p(\theta, t) = 0$. Since $[N : F] = 4$, the quartic polynomial $p(X, t)$ is irreducible over F. Defining the constant ξ to be $\eta \pmod P$, we find that $f_t(\xi) = 0$, and from (7) it is clear that $\xi \in N$. We need to show that $f_t(X)$ is irreducible over F also. If it is not irreducible, then ξ has degree 1 or 2 over F. This is impossible if $t \neq -2$, by (12) (θ would also have degree 1 or 2 over F). Moreover, t cannot be -2, since $p(x, -2) = (x^2 + x - 1/4)^2$ is reducible. Hence $N = F(\xi)$, showing that (b) implies (a).

To prove (a) implies (b), assume that $N = F(\xi)$, where $f_h(\xi) = 0$ and $f_h(X)$ is irreducible over F. Then h cannot be a zero of the discriminant $h^2(h^2 + 4)^3(h + 2)^6$ of $f_h(X)$, since otherwise $f_h(X)$ would be reducible. Hence the solution $(\eta, z) = (\xi, h)$ on $f_z(\eta) = 0$ defines a prime divisor P of $K = F(z, \eta) = F(x, c)$. Thus we can define θ by $x \equiv \theta \pmod P$, or

$$h(h + 2)\theta = \tfrac{1}{2}(h + 1)(h^2 - 2h - 2) + h(h + 1)(h^2 + h + 2)\xi + (h + 1)(h^2 - h + 1)\xi^2 - h\xi^3,$$

and we have $p(\theta, h) = 0$. Considering (7) mod P shows that θ generates

N over F, so that $p(X,h)$ is irreducible over F. Finally, $p(X,z)$ divides $p(X^2+c,z) = p(X^2-(z^3+3z+4)/(4z),z)$ identically in X and z, so that the roots of $p(X,h)$ are just the elements of the orbit of θ under $f(x)=x^2+a$, where $a=-(h^3+3h+4)/(4h)$. Hence $\theta \to \theta^2+a$ generates $\mathrm{Gal}(N/F)$, and this completes the proof of the theorem.

References

[ba] E. Bach, *Toward a theory of Pollard's rho method*, Inform. and Comput. 90 (1991), 139–155.

[bo] T. Bousch, *Sur quelques problèmes de dynamique holomorphe*, thèse, Université de Paris-Sud, Centre d'Orsay, 1992.

[de] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, Addison-Wesley, 1987.

[fps] V. Flynn, B. Poonen and E. Schaefer, *Cycles of quadratic polynomials and rational points on a genus 2 curve*, Duke Math. J. 90 (1997), 435–463.

[m1] P. Morton, *Arithmetic properties of periodic points of quadratic maps*, Acta Arith. 62 (1992), 343–372.

[m2] —, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory 49 (1994), 183–208.

[m3] —, *On certain algebraic curves related to polynomial maps*, Compositio Math. 103 (1996), 319–350.

[mp] P. Morton and P. Patel, *The Galois theory of periodic points of polynomial maps*, Proc. London Math. Soc. 68 (1994), 225–263.

[ms] P. Morton and J. Silverman, *Periodic points, multiplicities and dynamical units*, J. Reine Angew. Math. 461 (1995), 81–122.

[mv] P. Morton and F. Vivaldi, *Bifurcations and discriminants for polynomial maps*, Nonlinearity 8 (1995), 571–584.

[rw] P. Russo and R. Walde, *Rational periodic points of the quadratic function* $Q_c(x) = x^2+c$, Amer. Math. Monthly 101 (1994), 318–331.

[tvw] E. Thiran, D. Verstegen and J. Weyers, *p-adic dynamics*, J. Statist. Phys. 54 (1989), 893–913.

[vh1] F. Vivaldi and S. Hatjispyros, *Galois theory of periodic orbits of rational maps*, Nonlinearity 5 (1992), 961–978.

[vh2] —, —, *A family of rational zeta functions for the quadratic map*, ibid. 8 (1995), 321–332.

[w1] L. Washington, *A family of cyclic quartic fields arising from modular curves*, Math. Comp. 57 (1991), 763–775.

[w2] —, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

Department of Mathematics
Wellesley College
Wellesley, Massachusetts 02481-8203
U.S.A.
E-mail: pmorton@wellesley.edu

Received on 23.4.1997
and in revised form on 18.2.1998 (3171)