involve
a journal of mathematics

Newly reducible iterates in families of quadratic polynomials

Katharine Chamberlin, Emma Colbert, Sharon Frechette,
Patrick Hefferman, Rafe Jones and Sarah Orchard

msp

2012 vol. 5, no. 4

INVOLVE 5:4 (2012)
dx.doi.org/10.2140/involve.2012.5.481

Newly reducible iterates in families of quadratic polynomials

Katharine Chamberlin, Emma Colbert, Sharon Frechette, Patrick Hefferman, Rafe Jones and Sarah Orchard

(Communicated by Michael Zieve)

We examine the question of when a quadratic polynomial $f(x)$ defined over a number field K can have a newly reducible n-th iterate, that is, $f^n(x)$ irreducible over K but $f^{n+1}(x)$ reducible over K, where f^n denotes the n-th iterate of f. For each choice of critical point γ, we consider the family

$$g_{\gamma,m}(x) = (x-\gamma)^2 + m + \gamma, \quad m \in K.$$

For fixed $n \geq 3$ and nearly all values of γ, we show that there are only finitely many m such that $g_{\gamma,m}$ has a newly reducible n-th iterate. For $n = 2$ we show a similar result for a much more restricted set of γ. These results complement those obtained by Danielson and Fein (*Proc. Amer. Math. Soc.* **130**:6 (2002), 1589–1596) in the higher-degree case. Our method involves translating the problem to one of finding rational points on certain hyperelliptic curves, determining the genus of these curves, and applying Faltings' theorem.

1. Introduction

Let K be a number field and $f(x) \in K[x]$. By the n-th iterate $f^n(x)$ of $f(x)$, we mean the n-fold composition of f with itself. Determining the factorization of $f^n(x)$ into irreducible polynomials has proven to be an important problem. From a dynamical perspective, it is a question about the inverse orbit of zero, namely $O^-(0) := \bigcup_{n\geq 1} f^{-n}(0)$. This set has significance in various ways; for instance, it accumulates at every point of the Julia set of f [Beardon 1991, p. 71]. The field of arithmetic dynamics seeks to understand sets such as $O^-(0)$ from an algebraic perspective, and finding the factorization of $f^n(x)$ fits into this scheme: a nontrivial factorization arises from an "unexpected" algebraic relation among

MSC2010: 11R09, 37P05, 37P15.

Keywords: polynomial iteration, polynomial irreducibility, arithmetic dynamics, rational points on hyperelliptic curves.

This research was partially supported by a supplement to NSF grant DMS-0852826. All the authors are grateful for this support.

elements of $O^-(0)$. In addition, understanding the factorization of $f^n(x)$ has proven to be a key obstacle in determining the Galois groups of $f^n(x)$ (see [Hamblen et al. 2013; Jones 2008] or [Jones and Manes 2011] for the case of some rational functions). These Galois groups provide a sort of dynamical analogue to the well-studied ℓ-adic Galois representations [Boston and Jones 2007].

In general, the factorization of the iterates of f can exhibit a wide variety of behaviors. For instance, in [Fein and Schacher 1996, Lemma 1.1] it is shown that for each $n \geq 1$ and $d \geq 2$, there exists a number field K such that, for some $f(x) \in K[x]$ of degree d, $f^{n+1}(x)$ is *newly reducible*; that is, $f^n(x)$ is irreducible over K but $f^{n+1}(x)$ is reducible over K. More specifically, it follows from [Stoll 1992, p. 243] and [Fein and Schacher 1996, Lemma 1.1] that if $f(x) = x^2 + m$ for $m \in \mathbb{Z}_{>0}$, $m \equiv 1, 2 \bmod 4$, then for any fixed $n \geq 1$ there exists a number field K such that $f^{n+1}(x)$ is newly reducible over K. But what happens when we fix the number field K to start with, and ask about the factorization of $f^n(x)$ as n grows? Many authors have examined this question, in general with the aim of giving criteria that ensure all iterates are irreducible (see, e.g., [Jones 2012; Odoni 1985, Section 4]). Most usefully for our purposes, Danielson and Fein [2002] consider the case when $f(x) = x^d + m$, for $d \geq 2$. They show, for instance, that if $m \in \mathbb{Z}$ and $f(x)$ is irreducible, then all iterates of f are irreducible. In fact they only assume that K is the quotient field of a unique factorization domain R, and in this case they show that certain strong diophantine conditions must be satisfied when $f^n(x)$ is irreducible and $f^{n+1}(x)$ is reducible. In particular, for $K = \mathbb{Q}$, they take $S(d, n)$ to be the set of $m \in \mathbb{Q}$ such that $f^{n+1}(x)$ is newly reducible. Further, let $S(d) = \bigcup_{n \geq 1} S(d, n)$. In [Danielson and Fein 2002, Theorem 7] it is shown that $S(2, 1)$ (and thus $S(2)$) is infinite, $S(3, n)$ is finite for all $n \geq 1$, and $S(d)$ is finite for d odd, $d \geq 5$. Moreover, the abc conjecture implies that $S(d)$ is finite for d even, $d \geq 4$.

One goal of the present paper is to determine whether $S(2, n)$ is finite for $n \geq 2$. Our main result, however, is significantly more general. Consider the family of polynomials

$$g_{\gamma,m}(x) = (x - \gamma)^2 + m + \gamma, \quad \gamma, m \in K, \tag{1-1}$$

where K is a number field. Denote the ring of integers of K by $\mathbb{O}_K$. Our main result is the following:

Theorem 1. *Let K be a number field, $v_{\mathfrak{p}}$ the valuation attached to a prime $\mathfrak{p}$ of $\mathbb{O}_K$, and $g_{\gamma,m}(x)$ as in (1-1). If one of the following holds, then there are only finitely many m such that $g^n_{\gamma,m}(x)$ is irreducible over K and $g^{n+1}_{\gamma,m}(x)$ is reducible over K:*

(1) *$n \geq 3$ and there exists a prime $\mathfrak{p}$ of $\mathbb{O}_K$ with $v_{\mathfrak{p}}(2) = e \geq 1$ and $v_{\mathfrak{p}}(\gamma) = s$ with $s \neq -e2^i$ for all $i \geq 1$;*

(2) *$n = 2$ and $\gamma = r/4$ for for $r \in \mathbb{Z}$ such that $-200 \leq r \leq 200$.*

In particular, when $K = \mathbb{Q}$, part (1) of Theorem 1 holds when $v_2(\gamma)$ is not of the form -2^j for $j \geq 1$. Hence when $\gamma = 0$, we obtain that $S(2, n)$ is finite for $n \geq 2$ (in the notation of [Danielson and Fein 2002]); in other words, for each $n \geq 2$ there are at most finitely many $m \in \mathbb{Q}$ such that $x^2 + m$ has a newly reducible $(n+1)$-st iterate. In Proposition 10, we show further that $S(2, 3)$ is empty. Note also that part (1) of Theorem 1 applies whenever γ belongs to the ring of integers of K, and in particular for $\gamma \in \mathbb{Z}$. In fact, part (1) holds whenever γ is taken so that

$$g^i_{\gamma,m}(\gamma) \in K[m] \text{ does not have repeated roots for any } i \geq 1. \tag{1-2}$$

(See Theorem 6, Proposition 9, and the discussion immediately before Proposition 9.) Condition (1-2) is the same as the condition appearing in [Faber et al. 2009] for the *preimage curve* $Y^{\text{pre}}(i, -\gamma)$, given by the vanishing of the polynomial

$$(g^i_{0,m}(x) + \gamma) \in K[x, m],$$

to be nonsingular for all $i \geq 1$. In Proposition 9, we give a new criterion ensuring that (1-2) holds for given γ, thereby improving [Faber et al. 2009, Proposition 4.8]. The full strength of condition (1-2) is not required to prove part (1) of Theorem 1; see the remark following the proof of Proposition 9.

For given K, denote by $S(2, n, \gamma)$ the set of $m \in K$ such that $g^{n+1}_{\gamma,m}(x)$ is newly reducible. Thus Theorem 1 establishes the finitude of $S(2, n, \gamma)$ for $n \geq 2$ and certain γ. In Theorem 3, we show that for each $\gamma \in K$, the set $S(2, 1, \gamma)$ is infinite, and we explicitly describe its elements. In the case $\gamma = 0$, this result follows from [Danielson and Fein 2002, Proposition 2]. When $n \geq 2$, the sets $S(2, n, \gamma)$ may still be nonempty, even for $K = \mathbb{Q}$. For instance, when $f(x) = x^2 - x - 1$, corresponding to $\gamma = \frac{1}{2}$ and $m = -\frac{7}{4}$, we have that $f(x)$ and $f^2(x)$ are irreducible but

$$f^3(x) = (x^4 - 3x^3 + 4x - 1)(x^4 - x^3 - 3x^2 + x + 1), \tag{1-3}$$

and thus $-\frac{7}{4} \in S\big(2, 2, \frac{1}{2}\big)$. For $K = \mathbb{Q}$, the sets $S(2, n, \gamma)$ are likely to be empty for $n \geq 3$, since as we will see they correspond to rational points on high-genus curves. However, without effective algorithms to find such points, a new approach will be required to precisely determine $S(2, n, \gamma)$.

To prove Theorem 1, we first examine the case where $n \geq 3$ and use the fact that comparing constant terms of a hypothetical nontrivial factorization of $g^{n+1}_{\gamma,m}(x)$ gives rise to K-rational points on a hyperelliptic curve (at least for the γ satisfying part (1) of Theorem 1). This allows us to use Faltings' theorem to conclude that $S(2, n, \gamma)$ is finite for these γ and for $n \geq 3$. We then examine the case $n = 2$ using a system of equations generated from a factorization of the third iterate. After defining certain cases for this system, we use Faltings' theorem on a plane curve arising from the Gröbner basis of the system to show that $S(2, 2, \gamma)$ is finite for certain γ.

2. The case $n = 1$

Before we approach the main theorem, let's examine the case where $n = 1$. It is possible for $g^2_{\gamma,m}(x)$ to be reducible and $g_{\gamma,m}(x)$ irreducible:

Example 2. Let $\gamma = 0$, $m = -\frac{4}{3}$, and $K = \mathbb{Q}$. Then

$$g_{0,-\frac{4}{3}}(x) = x^2 - \tfrac{4}{3}$$

is irreducible over $\mathbb{Q}$ since $\frac{4}{3}$ is not a rational square. However, we have

$$g^2_{0,-\frac{4}{3}}(x) = \left(x^2 - \tfrac{4}{3}\right)^2 - \tfrac{4}{3} = \left(x^2 - 2x + \tfrac{2}{3}\right)\left(x^2 + 2x + \tfrac{2}{3}\right).$$

Because it has degree 4, $g^2_{\gamma,m}(x)$ could a priori have nontrivial factors of degree 1, 2, or 3. We will show in Corollary 5 that if $g_{\gamma,m}(x)$ is irreducible, then the only nontrivial factorization for $g^2_{\gamma,m}(x)$ is $p_1(x)p_2(x)$, with $\deg p_1(x) = \deg p_2(x) = 2$.

Theorem 3. *We have $g_{\gamma,m}(x)$ irreducible and $g^2_{\gamma,m}(x)$ reducible if and only if either*

(1) $\gamma \neq \frac{1}{4}$ *and* $m = (c_1^4 - 4\gamma)/(4 - 4c_1^2)$, *where* $c_1 \in K \setminus \{-1, 1\}$ *and* $(4\gamma - c_1^2)/(1 - c_1^2)$ *is not a square in* K; *or*

(2) $\gamma = \frac{1}{4}$ *and* $-4m - 1$ *is not a square in* K.

In particular, for each $\gamma \in K$, the set $S(2, 1, \gamma)$ is infinite.

Remark. It is interesting to note that when $\gamma = \frac{1}{4}$, we have

$$g^2_{1/4,m}(x) = \left(x^2 - \tfrac{3}{2}x + \left(m + \tfrac{13}{16}\right)\right)\left(x^2 + \tfrac{1}{2}x + \left(m + \tfrac{5}{16}\right)\right), \tag{2-1}$$

and so $g^2_{1/4,m}(x)$ is reducible for all $m \in K$. This phenomenon has already been noticed, albeit in somewhat different language, in [Faber et al. 2009, Remark 2.6 and p. 94].

Proof. Suppose that $g_{\gamma,m}(x)$ is irreducible and $g^2_{\gamma,m}(x)$ is reducible, so that $g^2_{\gamma,m}(x) = p_1(x)p_2(x)$. Write $p_1(x) = (x-\gamma)^2 + b_1(x-\gamma) + b_0$ and $p_2(x) = (x-\gamma)^2 + c_1(x-\gamma) + c_0$, where $b_i, c_i \in K$, and note that

$$g^2_{\gamma,m}(x) = (x-\gamma)^4 + 2m(x-\gamma)^2 + m^2 + m + \gamma. \tag{2-2}$$

Comparing coefficients in the equality $g^2_{\gamma,m}(x) = p_1(x)p_2(x)$ gives the following system of equations:

(a) $c_1 + b_1 = 0$;

(b) $c_0 + b_1c_1 + b_0 = 2m$;

(c) $b_1c_0 + b_0c_1 = 0$;

(d) $b_0c_0 = m^2 + m + \gamma$.

Clearly $b_1 = -c_1$ from (a), and then from (c) we have $c_1(b_0 - c_0) = 0$. If $c_1 = 0$, then from (b) we obtain $c_0 + b_0 = 2m$. Squaring both sides and subtracting four times equation (d), one verifies that $-m-\gamma = \frac{1}{4}(c_0-b_0)^2$. As this is a square, $g_{\gamma,m}(x)$ is reducible (see (1-1) on page 482), and from this contradiction we conclude that $c_1 \neq 0$, and hence $b_0 = c_0$. See (3-1) in the proof of Theorem 6 for a generalization of this statement. From (b) and (d) we now derive the following system of two equations:

(e) $2c_0 - c_1^2 - 2m = 0$;

(f) $c_0^2 - m^2 - m - \gamma = 0$.

Solving (e) for c_0 and substituting the result into (f) gives

$$c_1^4 + 4mc_1^2 - 4m - 4\gamma = 0. \tag{2-3}$$

Note that $c_1 = \pm 1$ if and only if $\gamma = \frac{1}{4}$. Thus in the case where $\gamma \neq \frac{1}{4}$, we may solve (2-3) for m to obtain $m = (c_1^4 - 4\gamma)/(4-4c_1^2)$. Because $g_{\gamma,m}(x)$ is assumed to be irreducible, we have that $-m-\gamma$ is not a square in K, and one computes $-m-\gamma = (c_1^2(4\gamma - c_1^2))/(4(1-c_1^2))$. In the case where $\gamma = \frac{1}{4}$, we may take $c_1 = \pm 1$ and $c_0 = (1+2m)/2$ to get a solution to equations (e) and (f) (this is the same as the factorization in (2-1)). Hence $g^2_{1/4,m}(x)$ is reducible for all $m \in K$. Since $g_{1/4,m}(x)$ is assumed to be irreducible, $-m-\gamma = -m-\frac{1}{4}$ cannot be a square in K, which holds if and only if $-4m-1$ is not a square in K.

Assume now that either of the conditions in the statement of Theorem 3 hold. Then $-m-\gamma$ is not a square in K, so $g_{\gamma,m}(x)$ is irreducible. The other hypotheses ensure that equations (e) and (f) above have solutions in K, and hence $g^2_{\gamma,m}(x)$ is reducible. □

Note that when $\gamma = 0$, taking $c_1 = 2$ in Theorem 3 yields Example 2. We also remark that in the case of $\gamma = 0$, taking $c_1 = 2z$ in Theorem 3 yields Proposition 2 of [Danielson and Fein 2002], at least in the case where K is a number field. (Note that there the polynomial under consideration is $x^2 - m$, and hence the results differ by a minus sign.)

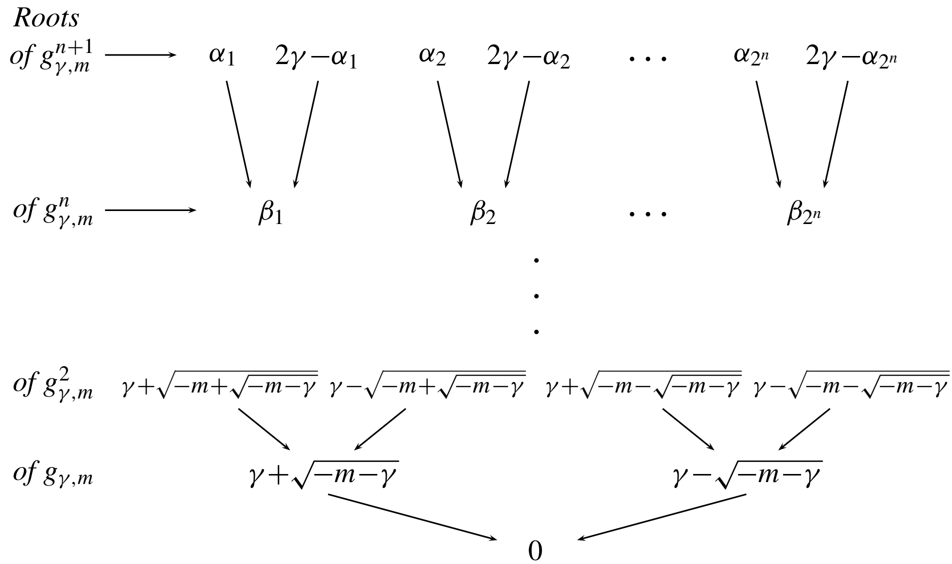
3. The case $n \geq 3$

Having handled the case $n = 1$, we now address the case where $n \geq 3$. We postpone the case $n = 2$ until Section 4 because the curves we must analyze have genus one, while for $n \geq 3$ the curves that arise have genus at least two, allowing us to apply Faltings' theorem.

Understanding the roots of $g^{n+1}_{\gamma,m}(x)$ is central to our analysis. In general, if β_i is a root of $g^n_{\gamma,m}(x)$, then the two roots of $g_{\gamma,m}(x) - \beta_i$ are roots of $g^{n+1}_{\gamma,m}(x)$. Calling them α_i^+ and α_i^-, we have $\alpha_i^+ = \gamma + \sqrt{\beta_i - m - \gamma}$ and $\alpha_i^- = \gamma - \sqrt{\beta_i - m - \gamma}$. Note that

$$2\gamma - \alpha_i^+ = 2\gamma - \left(\gamma + \sqrt{\beta_i - m - \gamma}\right) = \gamma - \sqrt{\beta_i - m - \gamma} = \alpha_i^-.$$

The following picture summarizes the relation of the roots to one another. Note that they are arranged in a tree.



In this section we establish two principal results on the structure of hypothetical factors in the case where $g^{n+1}_{\gamma,m}(x)$ is newly reducible. Our first result is similar to [Jones and Boston 2012, Proposition 2.6].

Theorem 4. *Let $g_{\gamma,m}(x) = (x-\gamma)^2 + m + \gamma$ with $\gamma, m \in K$. Suppose $g^n_{\gamma,m}(x)$ is irreducible, and $g^{n+1}_{\gamma,m}(x) = p_1(x)p_2(x)$ where $p_1(x)$ and $p_2(x)$ are nontrivial factors. If α is a root of $p_1(x)$, then $2\gamma-\alpha$ is a root of $p_2(x)$ but not a root of $p_1(x)$.*

Proof. Let $G_{n+1} = \mathrm{Gal}(E_{n+1}/K)$, where E_{n+1} is the splitting field of $g^{n+1}_{\gamma,m}(x)$ over K. Because $g^n_{\gamma,m}(x)$ is irreducible over K, G_{n+1} acts transitively on the roots of $g^n_{\gamma,m}(x)$. Let α be a root of $p_1(x)$ and α' be a root of $g^{n+1}_{\gamma,m}$ but not a root of p_1. By the transitivity of the action of G_{n+1} on the roots of $g^n_{\gamma,m}$, we may take $\phi \in G_{n+1}$ such that $\phi(g_{\gamma,m}(\alpha)) = g_{\gamma,m}(\alpha')$. Hence

$$\phi((\alpha-\gamma)^2 + \gamma + m) = (\alpha'-\gamma)^2 + \gamma + m,$$

from which we deduce that $\phi(\alpha)-\gamma = \pm(\alpha'-\gamma)$. Indeed, we must have $\phi(\alpha)-\gamma = -(\alpha'-\gamma)$, for otherwise $\phi(\alpha) = \alpha'$, contradicting our assumption that α' is not a root of p_1. We thus obtain $\phi(\alpha) = 2\gamma-\alpha'$. In other words, $2\gamma-\alpha = \phi^{-1}(\alpha')$, and is therefore not a root of p_1. □

Corollary 5. *Let $g_{\gamma,m}(x) = (x-\gamma)^2 + m + \gamma$ with $\gamma, m \in K$. Let $n \in \mathbb{Z}^+$, and assume $g^n_{\gamma,m}(x)$ is irreducible with $g^{n+1}_{\gamma,m}(x) = p_1(x)p_2(x)$, where $p_1(x)$ and $p_2(x)$ are nontrivial factors. Then,* $\deg p_1(x) = \deg p_2(x) = 2^n$, *and $p_1(x)$ and $p_2(x)$ are irreducible.*

Proof. Observe that $\deg g_{\gamma,m}^{n}(x) = 2^n$ and $\deg g_{\gamma,m}^{n+1}(x) = 2^{n+1}$. By Theorem 4, the roots of $p_1(x)$ are in bijection with the roots of $p_2(x)$, whence $\deg p_1(x) = \deg p_2(x) = 2^n$. If $\{\alpha_1, \dots, \alpha_{2^n}\}$ are all the roots of $p_1(x)$, then by Theorem 4, $\{2\gamma - \alpha_1, \dots, 2\gamma - \alpha_{2^n}\}$ are all the roots of $p_2(x)$. Thus the set

$$\{g_{\gamma,m}(\alpha_i) : i = 1, \dots, 2^n\}$$

coincides with the set of all roots of $g_{\gamma,m}^{n}(x)$. Because $g_{\gamma,m}^{n}(x)$ is irreducible, the action of G_{n+1} on $\{g_{\gamma,m}(\alpha_i) : i = 1, \dots, 2^n\}$ consists of a single orbit, and thus the action of G_{n+1} on $\{\alpha_1, \dots, \alpha_{2^n}\}$ must consist of a single orbit. Hence $p_1(x)$ is irreducible. Similar reasoning gives that $p_2(x)$ is irreducible. □

3.1. ***Curves and Faltings' theorem.*** We now use Theorem 4 to show that if $g_{\gamma,m}^{n+1}(x)$ is newly reducible, then there is a K-rational point, depending on m, on a certain curve.

Theorem 6. *If $g_{\gamma,m}^{n}(x)$ is irreducible and $g_{\gamma,m}^{n+1}(x)$ is reducible for some $n \geq 1$, then there exist $x, y \in K$ with $x = m$ such that*

$$y^2 = t_{n+1}(x),$$

where the polynomials $t_i(x)$ are defined by the recurrence relation $t_1(x) = x + \gamma$ and, for $i \geq 2$,

$$t_i(x) = (t_{i-1}(x) - \gamma)^2 + x + \gamma.$$

Remark. Note that $t_i(x) = (g_{\gamma,m}^{i}(\gamma))|_{m=x}$, as will be shown below (or can be easily seen by induction).

Proof. Assume $g_{\gamma,m}^{n}$ is irreducible and $g_{\gamma,m}^{n+1}(x) = p_1(x)p_2(x)$ for some $p_1(x)$, $p_2(x) \in K[x]$ of positive degree. By Theorem 4, if $\{\alpha_1, \dots, \alpha_{2^n}\}$ are all the roots of $p_1(x)$, then $\{2\gamma - \alpha_1, \dots, 2\gamma - \alpha_{2^n}\}$ are all the roots of $p_2(x)$. Then,

$$\begin{aligned} p_1(x) &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2^n}) \quad \text{and} \\ p_2(x) &= (x - (2\gamma - \alpha_1))(x - (2\gamma - \alpha_2)) \cdots (x - (2\gamma - \alpha_{2^n})) \\ &= (x - 2\gamma + \alpha_1)(x - 2\gamma + \alpha_2) \cdots (x - 2\gamma + \alpha_{2^n}). \end{aligned}$$

So we have

$$\begin{aligned} p_1(\gamma) &= (\gamma - \alpha_1)(\gamma - \alpha_2) \cdots (\gamma - \alpha_{2^n}) \quad \text{and} \\ p_2(\gamma) &= (-\gamma + \alpha_1)(-\gamma + \alpha_2) \cdots (-\gamma + \alpha_{2^n}) \\ &= (-1)^{2^n} (\gamma - \alpha_1)(\gamma - \alpha_2) \cdots (\gamma - \alpha_{2^n}), \end{aligned} \tag{3-1}$$

and therefore $p_1(\gamma) = p_2(\gamma)$. Set $y = p_1(\gamma) = p_2(\gamma)$, so $g_{\gamma,m}^{n+1}(\gamma) = y^2$. We have

$$g_{\gamma,m}^{n+1}(\gamma) = g_{\gamma,m}(g_{\gamma,m}^{n}(\gamma)) = (g_{\gamma,m}^{n}(\gamma) - \gamma)^2 + m + \gamma.$$

Moreover, $g_{\gamma,m}(\gamma) = m + \gamma$, and thus $g^i_{\gamma,m}(\gamma)$ satisfies the same recurrence relation as $t_i(x)$, with x replaced by m. □

The polynomials $t_i(x)$ play a critical role in our argument. The first few are

$$t_1(x) = x + \gamma, \quad t_2(x) = x^2 + x + \gamma, \quad t_3(x) = x^4 + 2x^3 + x^2 + x + \gamma,$$
$$t_4(x) = x^8 + 4x^7 + 6x^6 + 6x^5 + 5x^4 + 2x^3 + x^2 + x + \gamma. \tag{3-2}$$

Equations of the form $y^2 = t_i(x)$ may be interpreted geometrically as plane curves. A plane curve defined over a field F is the set of solutions $(x, y) \in F \times F$ of an equation of the form $h(x, y) = 0$, where $h(x, y) \in F[x, y]$. If K is a subfield of F, a K-rational point on the curve is one whose coordinates lie in K. For instance, $(1, -1)$ is a $\mathbb{Q}$-rational point on the curve $y^2 = x^3 + x - 1$, while $(-1, \sqrt{-3})$ is not (though it is K-rational for $K = \mathbb{Q}(\sqrt{-3})$).

The genus of a plane curve is a measure of its geometric complexity, and for curves of the form $y^2 = r(x)$, which is the case of interest to us in light of Theorem 6, there is a convenient way to calculate it — at least, when the roots of $r(x)$ in the algebraic closure of K are distinct.

Theorem 7 [Goldschmidt 2003]. *Consider the curve $C : y^2 = r(x)$. If $r(x)$ is separable and of degree d, then the genus g of C is given by*

$$g = \begin{cases} (d-1)/2 & \text{for } d \text{ odd}, \\ (d-2)/2 & \text{for } d \text{ even}. \end{cases}$$

Assume that $r(x)$ is separable. A curve of the form $y^2 = r(x)$ of genus at least two is called a *hyperelliptic curve*, while when such a curve has genus one it is known as a *elliptic curve*. The reason we care about the genus of a curve is that Faltings' theorem famously connects it to the number of K-rational points on the curve:

Theorem 8 (Faltings; see [Hindry and Silverman 2000, Theorem E.0.1]). *Let K be a number field, and let C be a curve defined over K of genus $g \geq 2$. Then the set of K-rational points on C is finite.*

Suppose for a moment that all of the polynomials $t_i(x)$ in Theorem 6 are separable. Clearly $\deg t_i(x) = 2^{i-1}$. By Theorem 7, the genus g_i of the curve $y^2 = t_i(x)$ then satisfies

$$g_i = \begin{cases} 0 & \text{for } i = 1, \\ 2^{i-2} - 1 & \text{for } i \geq 2. \end{cases} \tag{3-3}$$

Therefore, by Faltings' theorem, the curve $y^2 = t_{n+1}(x)$ has only finitely many K-rational points for $n \geq 3$. In particular, there are only finitely many $x \in K$ such that (x, y) is a K-rational point on $y^2 = t_{n+1}(x)$. Thus, by Theorem 6, when $n \geq 3$ there are only finitely many $m \in K$ with $g^n_{\gamma,m}(x)$ irreducible and $g^{n+1}_{\gamma,m}(x)$ reducible over K.

Hence the lone remaining obstacle to proving part (1) of Theorem 1 is to establish that the $t_i(x)$ in Theorem 6 are separable. Note that this is not true for all $\gamma \in K$. Indeed, if $\gamma = \frac{1}{4}$, then $t_2(x) = \left(x + \frac{1}{2}\right)^2$. The set

$$S := \{\gamma \in \overline{\mathbb{Q}} : t_i(x) \text{ is separable for all } i \geq 1\}$$

is the same as the set of $a \in \overline{\mathbb{Q}}$ such that the preimage curves $Y^{\text{pre}}(N, -a)_{N \geq 1}$ defined in [Faber et al. 2009] are all nonsingular. In general, the set $\overline{\mathbb{Q}} \setminus S$ is poorly understood. One result [Faber et al. 2009, Proposition 4.8] gives a criterion for membership in S. Here we give an improvement on that result.

Proposition 9. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $t_i(x)$ be as in Theorem 6. Suppose there exists a prime $\mathfrak{p}$ of $\mathcal{O}_K$ with $v_{\mathfrak{p}}(2) = e \geq 1$ and $v_{\mathfrak{p}}(\gamma) = s$ with $s \neq -e2^j$ for all $j \geq 1$. Then $t_i(x)$ is separable over K for all $i \geq 1$.*

Remark. When $K = \mathbb{Q}$, Proposition 9 says that if $v_2(\gamma) \neq -2^j$ for all $j \geq 1$, then $t_i(x)$ is separable for all $i \geq 1$.

Proof. It suffices to establish that $t_i(x)$ and $t_i'(x)$ have no common roots in $\overline{K}$, which we do through the use of Newton polygons with respect to the valuation $v_{\mathfrak{p}}$ (we abbreviate these by NP). We assume the reader is familiar with the relationship between slopes of the Newton polygon of a polynomial and the $\mathfrak{p}$-adic valuation of the polynomial's roots (see, e.g., [Silverman 2007, Theorem 5.11]). The proposition is obvious for $i = 1$, so we take $i \geq 2$. We first claim that for each r with $0 \leq r \leq i-2$, $t_i'(x)$ has 2^r roots in $\overline{K}$ with $\mathfrak{p}$-adic valuation $-e/2^r$. The statement is trivial for $i = 2$, so we assume inductively that it holds for given $i \geq 3$, and we consider the NP of $t_i'(x)$ with respect to the $\mathfrak{p}$-adic valuation. By the chain rule,

$$t_{i+1}'(x) = 2(t_i(x) - \gamma)t_i'(x) + 1.$$

Observe that $t_i(x) - \gamma$ is monic, has integer coefficients, and has linear coefficient 1 (and constant term 0). Thus its NP consists of a single horizontal line segment from $(1, 0)$ to $(2^{i-1}, 0)$. From our inductive hypothesis, it follows that the NP of $2(t_i(x) - \gamma)t_i'(x)$ consists of a horizontal line segment from $(1, e)$ to $(2^{i-1}, e)$, followed by a sequence of segments of slope $e/2^{i-2}, e/2^{i-3}, \ldots, e$ and respective lengths $2^{i-2}, 2^{i-3}, \ldots, 1$. Hence the NP of $2(t_i(x)-\gamma)t_i'(x)+1$ consists of a line segment from $(0, 0)$ to $(2^{i-1}, e)$, having slope $e/2^{i-1}$, and otherwise is identical to the NP of $2(t_i(x)-\gamma)t_i'(x)$, since $e/2^{i-1} < e/2^c$ for $0 \leq c \leq i-2$. This proves the claim.

For each $i \geq 1$, $t_i(x)$ is a monic polynomial with degree 2^{i-1} and constant term γ, whose nonconstant coefficients are all integers. If $v_{\mathfrak{p}}(\gamma) \geq 0$, then the NP of $t_i(x)$ consists of nonpositive slopes, and hence all its roots have nonnegative $\mathfrak{p}$-adic valuation, and therefore cannot coincide with roots of $t_i'(x)$ by the above claim. If $v_{\mathfrak{p}}(\gamma) = s < 0$, the NP for $t_i(x)$ consists of a single line segment from $(0, s)$ to $(2^{i-1}, 0)$, with length 2^{i-1} and slope $-s/2^{i-1}$. Hence if $t_i(x)$ and $t_i'(x)$ have a root in common, then by the above claim, $-s/2^{i-1} = e/2^r$ with $0 \le r \le i-2$. But this holds if and only if $s = -e2^{i-1-r}$, and since $i-1-r \ge 1$, the proof is complete. □

Remark. To show that the genus of the curve $y^2 = t_i(x)$ is at least two, we can get by with a much weaker statement than Proposition 9. Indeed, the genus of $y^2 = t_i(x)$ depends on the degree of $t_i(x)/f(x)$, where $f(x)$ is the square polynomial of largest degree dividing $t_i(x)$. It suffices to show that the degree of $t_i(x)/f(x)$ is at least five, for each $i \ge 4$.

4. The case $n = 2$

Consider now the case where $n = 2$. From (3-3), we know that when $t_3(x)$ is separable, $g_3 = 1$, and so $y^2 = t_3(x)$ is an elliptic curve. (When $t_3(x)$ is not separable, $y^2 = t_3(x)$ gives a curve of genus 0.) Thus we cannot directly apply Faltings' theorem, and we must use a different approach to determine the set $S(2, 2, \gamma)$ of $m \in K$ such that $g^2_{\gamma,m}(x)$ is irreducible and $g^3_{\gamma,m}(x)$ is reducible over K.

Now for some number fields K and some $\gamma \in K$, it may still be the case that $y^2 = t_3(x)$ has only finitely many K-rational points, proving the finiteness of $S(2, 2, \gamma)$ over K. This is the case for $\gamma = 0$ and $K = \mathbb{Q}$, as we now show:

Proposition 10. *Let $\gamma = 0$ and C_3 be the curve given by*

$$y^2 = t_3(x) = x^4 - 2x^3 + x^2 - x.$$

The only $\mathbb{Q}$-rational points on C_3 are $(0, 0)$ and the point at infinity. In particular, there are no $m \in \mathbb{Q}$ such that $x^2 + m$ has a newly reducible third iterate.

Proof. Let $y = u/v^2$ and $x = -1/v$ define a birational map ϕ from

$$C'_3 : u^2 = v^3 + v^2 + 2v + 1$$

to C_3. We compute the conductor of the elliptic curve C'_3 to be 92, and locate it as curve 92A1 in [Cremona]. From the same reference, we know that it has rank zero over $\mathbb{Q}$ and torsion subgroup of order 3. Hence the obvious points $(0, \pm 1)$ together with the point at infinity give all $\mathbb{Q}$-rational points on C'_3. If (x, y) is an affine rational point on C_3 with $x \ne 0$, then $\phi^{-1}(x, y)$ is an affine rational point (v, u) on C'_3 with $v \ne 0$. But there are no such points. □

The strategy of Proposition 10, however, won't even work for all number fields K in the case $\gamma = 0$. Indeed, let $K = \mathbb{Q}(i)$ and let ϕ be the same transformation as in Proposition 10. One can check that $(-1, i)$ is a nontorsion point of C'_3 in many ways. One of the more interesting, if not the simplest computationally, is to show that $(-1, i)$ has positive canonical height. Silverman [1990] gives upper and lower bounds for the difference between the canonical height $\hat{h}(P)$ and the Weil height $h(P)$ of a K-rational point P on an elliptic curve, computed in terms of the discriminant and j-invariant of the curve. For C_3', we have $-1.5484 \leq \hat{h}(P) - h(P) \leq 1.4577$. In particular, $\hat{h}(P) \geq h(P) - 1.5484$, so $h(P) > 1.5484$ would imply that P is a nontorsion point. Using MAGMA [Bosma et al. 1997], we find that although $h(P) = 0$ for $P = (-1, i)$ on C_3', we have $h([2]P) = 1.6094$. Thus $\hat{h}(P) = \frac{1}{4}\hat{h}([2]P) > 0$, using algebraic properties of canonical height.

Since $(-1, i)$ is a nontorsion point on C_3', the curve C_3 has infinitely many K-rational points. However, when we check some corresponding x-values on C_3 as our choices for m in $x^2 + m$, we don't find a newly reducible third iterate over $\mathbb{Q}(i)$. Thus we must adopt a different approach to have any hope of proving the case $n = 2$ of Theorem 1, even for $\gamma = 0$.

Let K be a number field and $\gamma \in K$. Suppose that $g^3_{\gamma,m}(x)$ is newly reducible, so that by Corollary 5, $g^3_{\gamma,m}(x) = p_1(x)p_2(x)$ for irreducible polynomials $p_1(x)$, $p_2(x) \in K[x]$ with $\deg p_1(x) = \deg p_2(x) = 4$. Put

$$\begin{aligned} p_1(x) &= (x-\gamma)^4 + a_3(x-\gamma)^3 + a_2(x-\gamma)^2 + a_1(x-\gamma) + a_0, \\ p_2(x) &= (x-\gamma)^4 + b_3(x-\gamma)^3 + b_2(x-\gamma)^2 + b_1(x-\gamma) + b_0 \end{aligned}$$

with $a_i, b_i \in K$. We also have

$$\begin{aligned} g^3_{\gamma,m}(x) = (x-\gamma)^8 + 4m(x-\gamma)^6 + (6m^2+2m)(x-\gamma)^4 \\ + (4m^3+4m^2)(x-\gamma)^2 + m^4 + 2m^3 + m^2 + m + \gamma. \end{aligned}$$

Multiplying $p_1(x)$ and $p_2(x)$ together, setting this product equal to $g^3_{\gamma,m}(x)$ and comparing coefficients, we obtain a system of eight equations. By simplifying this system using Theorem 6, and noting that $a_0 \neq 0$ by the irreducibility of $p_1(x)$, we get two cases:

Case I: $a_1 \neq 0$, which implies $b_1 = -a_1$, $b_2 = a_2$:

(1) $2a_2 - a_3^2 - 4m = 0$;

(2) $2a_0 + a_2^2 - 2a_1a_3 - 6m^2 - 2m = 0$;

(3) $2a_2a_0 - a_1^2 - 4m^3 - 4m^2 = 0$;

(4) $a_0^2 - m^4 - 2m^2 - m^2 - m - \gamma = 0$.

Case II: $a_1 = b_1 = 0$:

(1) $b_2 - a_3^2 + a_2 - 4m = 0$;

(2) $(b_2 - a_2)a_3 = 0$;

(3) $2a_0 + a_2b_2 - 6m^2 - 2m = 0$;

(4) $(a_2 + b_2)a_0 - 4m^3 - 4m^2 = 0$;

(5) $a_0^2 - m^4 - 2m^2 - m^2 - m - \gamma = 0$.

We use Gröbner bases to find the solutions to these systems of nonlinear equations. We dispense with Case II first, noting that it consists of five equations in five variables so we expect it will have only finitely many solutions in $\overline{K}$. We assign an ordering to the variables in which γ is last, and using MAGMA [Bosma et al. 1997] to compute a Gröbner basis for each system, we find that the system in Case II has one K-rational solution for each $m \in K$ with

$$\begin{aligned}0 = m^{14} &+ m^{13}\gamma + \tfrac{13}{3}m^{13} + \tfrac{13}{3}m^{12}\gamma + \tfrac{22}{3}m^{12} + \tfrac{22}{3}m^{11}\gamma + \tfrac{57}{8}m^{11} + \tfrac{33}{4}m^{10}\gamma \\ &+ 5m^{10} + \tfrac{9}{8}m^{9}\gamma^2 + \tfrac{23}{3}m^{9}\gamma + \tfrac{9}{4}m^{9} + \tfrac{8}{3}m^{8}\gamma^2 + \tfrac{25}{6}m^{8}\gamma + \tfrac{7}{12}m^{8} + \tfrac{23}{12}m^{7}\gamma^2 \\ &+ \tfrac{17}{12}m^{7}\gamma - \tfrac{1}{24}m^{7} + \tfrac{13}{12}m^{6}\gamma^2 - \tfrac{1}{12}m^{6}\gamma - \tfrac{1}{12}m^{6} + \tfrac{1}{4}m^{5}\gamma^3 - \tfrac{1}{24}m^{5}\gamma^2 \\ &- \tfrac{1}{4}m^{5}\gamma - \tfrac{1}{24}m^{5} - \tfrac{1}{4}m^{4}\gamma^2 - \tfrac{1}{6}m^{4}\gamma - \tfrac{1}{12}m^{3}\gamma^3 - \tfrac{1}{4}m^{3}\gamma^2 - \tfrac{1}{6}m^{2}\gamma^3 - \tfrac{1}{24}m\gamma^4.\end{aligned}$$

Clearly for any $\gamma \in K$, there are at most 14 such m, and so case II does not affect the finiteness of the number of m for which $g_{\gamma,m}(x)$ has a newly irreducible third iterate.

Case I proves more interesting. We compute that for fixed $\gamma \in K$, Case I has precisely one solution $(a_0, a_1, a_2, a_3, m) \in K^5$ for each K-rational point (a_3, m) on the curve

$$\begin{aligned}C_\gamma : 0 = {} & a_3^{16} + 32a_3^{14}m + 352a_3^{12}m^2 - 32a_3^{12}m + 1792a_3^{10}m^3 - 256a_3^{10}m^2 \\ & + 4352a_3^{8}m^4 - 1536a_3^{8}m^3 - 1792a_3^{8}m^2 - 2176a_3^{8}m - 2176a_3^{8}\gamma \\ & + 4096a_3^{6}m^5 - 8192a_3^{6}m^4 - 12288a_3^{6}m^3 - 10240a_3^{6}m^2 - 10240a_3^{6}m\gamma \\ & - 16384a_3^{4}m^5 - 32768a_3^{4}m^4 - 38912a_3^{4}m^3 - 22528a_3^{4}m^2\gamma - 14336a_3^{4}m^2 \\ & - 14336a_3^{4}m\gamma - 16384a_3^{2}m^4 - 16384a_3^{2}m^3\gamma - 16384a_3^{2}m^3 - 16384a_3^{2}m^2\gamma \\ & + 4096m^2 + 8192m\gamma + 4096\gamma^2.\end{aligned}$$

For instance, when $\gamma = \frac{1}{2}$, one checks that C_γ has the rational point $(1, -\frac{7}{4})$, which corresponds to the newly reducible example given in (1-3). The actual Gröbner basis is far too long to include here; however, we have included the Gröbner basis in the case $\gamma = 1$ in the Appendix to this article. Thus when C_γ has genus at least two, there can be only finitely many K-rational solutions to the system given in Case I, and hence only finitely many $m \in K$ such that $g_{\gamma,m}(x)$ has a newly irreducible third iterate. Part (2) of Theorem 1 is thus proved when the genus C_γ is at least two.

Using MAGMA again, we checked that C_γ has genus 11 for $\gamma = r/4$, $-200 \leq r \leq 200$, except for the cases $g(C_{-2}) = 9$, $g(C_0) = 9$, $g(C_{1/4}) = 7$, $g(C_1) = 10$. Note that we chose γ to have denominator 4 in order to include the case $\gamma = \frac{1}{4}$, where we strongly suspected degeneracies to occur. The map ψ sending C_γ to γ has fibers whose genus appears generally to be 11. Even the degenerate fibers seem to have genus greater than 1, and hence part (2) of Theorem 1 holds even in those cases. Interestingly, if we take a section of ψ by fixing a value of m and letting γ

vary, we appear always to get a curve of genus at most 1. This phenomenon was first noticed by Michael Zieve (personal correspondence). In other words, writing $C_{\gamma,m}$ instead of C_γ, and choosing ψ' to be the map sending $C_{\gamma,m}$ to m, the surface $C_{\gamma,m}$ is (birational to) an elliptic surface. This observation may pave the way for a full understanding of $C_{\gamma,m}$, and hence improvements to part (2) of Theorem 1.

Acknowledgements

The authors are grateful to Michael Zieve for the suggestion of the terminology "newly reducible," and for providing useful comments and computations. The authors also thank the anonymous referee for helpful suggestions.

Appendix

We report the Gröbner basis for Case I from page 491 with $\gamma = 1$ as calculated by MAGMA [Bosma et al. 1997]:

(1) $a_0 - a_1a_3 + \frac{1}{8}a_3^4 - a_3^2q - q^2 + q$

(2) $a_1^2 - a_1a_3^3 + 4a_1a_3q + \frac{1}{8}a_3^6 - \frac{3}{2}a_3^4q + 3a_3^2q^2 + a_3^2q$

(3)
$$\begin{aligned}
&a_1a_3^5 + \tfrac{1920}{571}a_1a_3q^6 - \tfrac{35582}{1713}a_1a_3q^5 + \tfrac{641146}{15417}a_1a_3q^4 - \tfrac{173966}{5139}a_1a_3q^3 \\
&+ \tfrac{254212}{15417}a_1a_3q^2 - \tfrac{4322}{571}a_1a_3q + \tfrac{35}{30834}a_3^{14}q - \tfrac{1}{1152}a_3^14 - \tfrac{4265}{123336}a_3^{12}q^2 \\
&+ \tfrac{200467}{7893504}a_3^{12}q + \tfrac{4199}{2631168}a_3^{12} + \tfrac{1775}{5139}a_3^{10}q^3 - \tfrac{191455}{986688}a_3^{10}q^2 - \tfrac{75881}{986688}a_3^{10}q \\
&- \tfrac{22705}{15417}a_3^8q^4 + \tfrac{516139}{986688}a_3^8q^3 + \tfrac{315853}{493344}a_3^8q^2 + \tfrac{54587}{986688}a_3^8q - \tfrac{7}{48}a_3^8 \\
&+ \tfrac{36880}{15417}a_3^6q^5 + \tfrac{76901}{61668}a_3^6q^4 - \tfrac{148475}{30834}a_3^6q^3 + \tfrac{219505}{61668}a_3^6q^2 - \tfrac{11}{18}a_3^6q \\
&- \tfrac{240}{571}a_3^4q^6 - \tfrac{429961}{61668}a_3^4q^5 + \tfrac{677423}{61668}a_3^4q^4 - \tfrac{402371}{61668}a_3^4q^3 - \tfrac{75667}{123336}a_3^4q^2 \\
&+ \tfrac{131047}{41112}a_3^4q + \tfrac{1920}{571}a_3^2q^7 - \tfrac{35582}{1713}a_3^2q^6 + \tfrac{641146}{15417}a_3^2q^5 - \tfrac{374378}{15417}a_3^2q^4 \\
&+ \tfrac{152233}{15417}a_3^2q^3 - \tfrac{189763}{15417}a_3^2q^2 + \tfrac{960}{571}q^5 - \tfrac{14911}{1713}q^4 + \tfrac{186374}{15417}q^3 - \tfrac{104975}{15417}q^2 + \tfrac{4}{3}q
\end{aligned}$$

(4)
$$\begin{aligned}
&a_1a_3^2q + \tfrac{720}{571}a_1q^6 - \tfrac{17791}{2284}a_1q^5 + \tfrac{320573}{20556}a_1q^4 - \tfrac{86983}{6852}a_1q^3 + \tfrac{53275}{10278}a_1q^2 - \tfrac{4199}{2284}a_1q \\
&- \tfrac{45}{292352}a_3^{15}q^3 + \tfrac{14911}{18710528}a_3^{15}q^2 - \tfrac{93187}{84197376}a_3^{15}q + \tfrac{104975}{168394752}a_3^{15} \\
&+ \tfrac{45}{9136}a_3^{13}q^4 - \tfrac{14911}{584704}a_3^{13}q^3 + \tfrac{93187}{2631168}a_3^{13}q^2 - \tfrac{11415}{584704}a_3^{13}q - \tfrac{1}{3072}a_3^{13} \\
&- \tfrac{495}{9136}a_3^{11}q^5 + \tfrac{161141}{584704}a_3^{11}q^4 - \tfrac{1915915}{5262336}a_3^{11}q^3 + \tfrac{300037}{1754112}a_3^{11}q^2 + \tfrac{206789}{7016448}a_3^{11}q \\
&+ \tfrac{4199}{7016448}a_3^{11} + \tfrac{315}{1142}a_3^9q^6 - \tfrac{101497}{73088}a_3^9q^5 + \tfrac{1170419}{657792}a_3^9q^4 - \tfrac{154417}{219264}a_3^9q^3 \\
&- \tfrac{203785}{877056}a_3^9q^2 - \tfrac{75881}{2631168}a_3^9q - \tfrac{765}{1142}a_3^7q^7 + \tfrac{236207}{73088}a_3^7q^6 - \tfrac{545431}{164448}a_3^7q^5 \\
&- \tfrac{142777}{109632}a_3^7q^4 + \tfrac{4272259}{877056}a_3^7q^3 - \tfrac{4322155}{1315584}a_3^7q^2 + \tfrac{3623737}{2631168}a_3^7q + \tfrac{360}{571}a_3^5q^8 \\
&- \tfrac{9151}{4568}a_3^5q^7 - \tfrac{19973}{5139}a_3^5q^6 + \tfrac{128675}{6852}a_3^5q^5 - \tfrac{4341377}{164448}a_3^5q^4 + \tfrac{1413245}{82224}a_3^5q^3 \\
&- \tfrac{830245}{164448}a_3^5q^2 - \tfrac{41}{48}a_3^5q - \tfrac{1440}{571}a_3^3q^8 + \tfrac{20671}{1142}a_3^3q^7 - \tfrac{258976}{5139}a_3^3q^6 \\
&+ \tfrac{12676049}{164448}a_3^3q^5 - \tfrac{3880925}{54816}a_3^3q^4 + \tfrac{688435}{18272}a_3^3q^3 - \tfrac{881653}{109632}a_3^3q^2 + \tfrac{172159}{109632}a_3^3q \\
&+ \tfrac{2160}{571}a_3q^7 - \tfrac{53373}{2284}a_3q^6 + \tfrac{320573}{6852}a_3q^5 - \tfrac{85543}{2284}a_3q^4 + \tfrac{177007}{13704}a_3q^3 - \tfrac{148651}{41112}a_3q^2
\end{aligned}$$

(5) $a_1q^7 - \frac{68}{9}a_1q^6 + \frac{1606}{81}a_1q^5 - \frac{578}{27}a_1q^4 + \frac{853}{81}a_1q^3 - \frac{50}{9}a_1q^2 + a_1q - \frac{1}{8192}a_3^{15}q^4$
$+ \frac{59}{73728}a_3^{15}q^3 - \frac{1075}{663552}a_3^{15}q^2 + \frac{377}{331776}a_3^{15}q - \frac{25}{73728}a_3^{15} + \frac{1}{256}a_3^{13}q^5$
$- \frac{59}{2304}a_3^{13}q^4 + \frac{1075}{20736}a_3^{13}q^3 - \frac{83}{2304}a_3^{13}q^2 + \frac{35}{3456}a_3^{13}q - \frac{11}{256}a_3^{11}q^6$
$+ \frac{5}{18}a_3^{11}q^5 - \frac{5647}{10368}a_3^{11}q^4 + \frac{9341}{27648}a_3^{11}q^3 - \frac{847}{13824}a_3^{11}q^2 - \frac{275}{27648}a_3^{11}q$
$- \frac{1}{3072}a_3^{11} + \frac{7}{32}a_3^9q^7 - \frac{101}{72}a_3^9q^6 + \frac{3497}{1296}a_3^9q^5 - \frac{5249}{3456}a_3^9q^4 + \frac{203}{1728}a_3^9q^3$
$+ \frac{365}{10368}a_3^9q^2 + \frac{11}{1152}a_3^9q - \frac{17}{32}a_3^7q^8 + \frac{949}{288}a_3^7q^7 - \frac{7261}{1296}a_3^7q^6 + \frac{1103}{3456}a_3^7q^5$
$+ \frac{19607}{3456}a_3^7q^4 - \frac{58525}{10368}a_3^7q^3 + \frac{15673}{5184}a_3^7q^2 - \frac{863}{1152}a_3^7q + \frac{1}{2}a_3^5q^9 - \frac{41}{18}a_3^5q^8$
$- \frac{115}{81}a_3^5q^7 + \frac{4409}{216}a_3^5q^6 - \frac{23737}{648}a_3^5q^5 + \frac{19853}{648}a_3^5q^4 - \frac{2225}{162}a_3^5q^3 + \frac{427}{216}a_3^5q^2$
$- 2a_3^3q^9 + \frac{154}{9}a_3^3q^8 - \frac{37351}{648}a_3^3q^7 + \frac{8318}{81}a_3^3q^6 - \frac{11993}{108}a_3^3q^5 + \frac{3571}{48}a_3^3q^4$
$- \frac{776}{27}a_3^3q^3 + \frac{3539}{432}a_3^3q^2 - \frac{41}{48}a_3^3q + 3a_3q^8 - \frac{68}{3}a_3q^7 + \frac{1606}{27}a_3q^6 - \frac{1147}{18}a_3q^5$
$+ \frac{778}{27}a_3q^4 - \frac{2075}{162}a_3q^3 + \frac{49}{18}a_3q^2$

(6) $a_2 - \frac{1}{2}a_3^2 + 2q$

(7) $a_3^{16} - 32a_3^{14}q + 352a_3^{12}q^2 + 32a_3^{12}q - 1792a_3^{10}q^3 - 256a_3^{10}q^2$
$+ 4352a_3^8q^4 + 1536a_3^8q^3 - 1792a_3^8q^2 + 2176a_3^8q - 4096a_3^6q^5$
$- 8192a_3^6q^4 + 12288a_3^6q^3 - 10240a_3^6q^2 + 16384a_3^4q^5 - 32768a_3^4q^4$
$+ 38912a_3^4q^3 - 14336a_3^4q^2 - 16384a_3^2q^4 + 16384a_3^2q^3 + 4096q^2$

References

[Beardon 1991] A. F. Beardon, *Iteration of rational functions: Complex analytic dynamical systems*, Graduate Texts in Mathematics **132**, Springer, New York, 1991. MR 92j:30026 Zbl 0742.30002

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3–4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Boston and Jones 2007] N. Boston and R. Jones, "Arboreal Galois representations", *Geom. Dedicata* **124** (2007), 27–35. MR 2009e:11103 Zbl 1206.11069

[Cremona] J. E. Cremona, "Elliptic curve data", online tables, University of Warwick, Available at http://homepages.warwick.ac.uk/staff/J.E.Cremona//ftp/data/INDEX.html.

[Danielson and Fein 2002] L. Danielson and B. Fein, "On the irreducibility of the iterates of $x^n - b$", *Proc. Amer. Math. Soc.* **130**:6 (2002), 1589–1596. MR 2002m:12001 Zbl 1007.12001

[Faber et al. 2009] X. Faber, B. Hutz, P. Ingram, R. Jones, M. Manes, T. J. Tucker, and M. E. Zieve, "Uniform bounds on pre-images under quadratic dynamical systems", *Math. Res. Lett.* **16**:1 (2009), 87–101. MR 2009m:11095 Zbl 1222.11086

[Fein and Schacher 1996] B. Fein and M. Schacher, "Properties of iterates and composites of polynomials", *J. London Math. Soc.* (2) **54**:3 (1996), 489–497. MR 97h:12007 Zbl 0865.12003

[Goldschmidt 2003] D. M. Goldschmidt, *Algebraic functions and projective curves*, Graduate Texts in Mathematics **215**, Springer, New York, 2003. MR 2003j:14001 Zbl 1034.14011

[Hamblen et al. 2013] S. Hamblen, R. Jones, and K. Madhu, "The density of primes in orbits of $z^d + c$", preprint, 2013. arXiv 1303.6513

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: An introduction*, Graduate Texts in Mathematics **201**, Springer, New York, 2000. MR 2001e:11058 Zbl 0948.11023

[Jones 2008] R. Jones, "The density of prime divisors in the arithmetic dynamics of quadratic polynomials", *J. Lond. Math. Soc.* (2) **78**:2 (2008), 523–544. MR 2010b:37239 Zbl 1193.37144

[Jones 2012] R. Jones, "An iterative construction of irreducible polynomials reducible modulo every prime", *J. Algebra* **369** (2012), 114–128. MR 2959789

[Jones and Boston 2012] R. Jones and N. Boston, "Settled polynomials over finite fields", *Proc. Amer. Math. Soc.* **140**:6 (2012), 1849–1863. MR 2012m:37142 Zbl 1243.11115

[Jones and Manes 2011] R. Jones and M. Manes, "Galois theory of quadratic rational functions", preprint, 2011. To appear in *Comment. Math. Helv.* arXiv 1101.4339

[Odoni 1985] R. W. K. Odoni, "On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$", *J. London Math. Soc.* (2) **32**:1 (1985), 1–11. MR 87b:11094 Zbl 0574.10020

[Silverman 1990] J. H. Silverman, "The difference between the Weil height and the canonical height on elliptic curves", *Math. Comp.* **55**:192 (1990), 723–743. MR 91d:11063 Zbl 0729.14026

[Silverman 2007] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics **241**, Springer, New York, 2007. MR 2008c:11002 Zbl 1130.37001

[Stoll 1992] M. Stoll, "Galois groups over $\mathbb{Q}$ of some iterated polynomials", *Arch. Math.* (*Basel*) **59**:3 (1992), 239–244. MR 93h:12004 Zbl 0758.11045

Received: 2012-10-15 Revised: 2013-02-19 Accepted: 2013-04-04

kacham12@g.holycross.edu — *Department of Mathematics and Computer Science, College of the Holy Cross, One College Street, Worcester, MA 10610, United States*

ercolb13@g.holycross.edu — *Department of Mathematics and Computer Science, College of the Holy Cross, One College Street, Worcester, MA 01610, United States*

sfrechet@holycross.edu — *Department of Mathematics and Computer Science, College of the Holy Cross, One College Street, Worcester, MA 01610, United States*

peheff13@g.holycross.edu — *Department of Mathematics and Computer Science, College of the Holy Cross, One College Street, Worcester, MA 01610, United States*

rfjones@carleton.edu — *Department of Mathematics, Carleton College, One North College Street, Northfield, MN 55057, United States*

seorch13@g.holycross.edu — *Department of Mathematics and Computer Science, College of the Holy Cross, One College Street, Worcester, MA 01610, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2012 is US $105/year for the electronic version, and $145/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2012 vol. 5 no. 4