New York Journal of Mathematics

New York J. Math. **26** (2020) 526–561.

Eventually stable quadratic polynomials over $\mathbb{Q}$

David DeMark, Wade Hindes, Rafe Jones, Moses Misplon, Michael Stoll and Michael Stoneman

Abstract. We study the number of irreducible factors (over $\mathbb{Q}$) of the nth iterate of a polynomial of the form $f_r(x) = x^2 + r$ for $r \in \mathbb{Q}$. When the number of such factors is bounded independent of n, we call $f_r(x)$ *eventually stable* (over $\mathbb{Q}$). Previous work of Hamblen, Jones, and Madhu [8] shows that f_r is eventually stable unless r has the form $1/c$ for some $c \in \mathbb{Z} \setminus \{0, -1\}$, in which case existing methods break down. We study this family, and prove that several conditions on c of various flavors imply that all iterates of $f_{1/c}$ are irreducible. We give an algorithm that checks the latter property for all c up to a large bound B in time polynomial in $\log B$. We find all c-values for which the third iterate of $f_{1/c}$ has at least four irreducible factors, and all c-values such that $f_{1/c}$ is irreducible but its third iterate has at least three irreducible factors. This last result requires finding all rational points on a genus-2 hyperelliptic curve for which the method of Chabauty and Coleman does not apply; we use the more recent variant known as elliptic Chabauty. Finally, we apply all these results to completely determine the number of irreducible factors of any iterate of $f_{1/c}$, for all c with absolute value at most 10^9.

Contents

1. Introduction 527
2. The case where $f_r(x)$ or $f_r^2(x)$ is reducible 533
3. The proof of cases (1)-(4) of Theorem 1.3 543
4. Proof of cases (5) and (6) of Theorem 1.3 548
5. A fast algorithm and the proof of case (7) of Theorem 1.3 553
6. Applications to the density of primes dividing orbits 558
References 559

Received April 4, 2019.

2010 *Mathematics Subject Classification.* 37P15, 11R09, 37P05, 12E05, 11R32.

Key words and phrases. Iterated polynomials, irreducible polynomials, rational points, hyperelliptic curves, arboreal Galois representation.

ISSN 1076-9803/2020

1. Introduction

Let K be a field with algebraic closure $\overline{K}$, $f \in K[x]$, and $\alpha \in K$. For $n \geq 0$, let $f^n(x)$ be the nth iterate of f (we take $f^0(x) = x$), and $f^{-n}(\alpha)$ the set $\{\beta \in \overline{K} : f^n(\beta) = \alpha\}$. When $f^n(x) - \alpha$ is separable over K for each $n \geq 1$, the set $T_f(\alpha) := \bigsqcup_{n \geq 0} f^{-n}(\alpha)$ acquires the structure of a rooted tree (with root α) if we assign edges according to the action of f.

A large body of recent work has focused on algebraic properties of $T_f(\alpha)$, particularly the natural action of $\mathrm{Gal}\,(\overline{K}/K)$ on $T_f(\alpha)$ by tree automorphisms, which yields a homomorphism $\mathrm{Gal}\,(\overline{K}/K) \to \mathrm{Aut}(T_f(\alpha))$ called the arboreal Galois representation associated to (f, α). A central question is whether the image of this homomorphism must have finite index in $\mathrm{Aut}(T_f(\alpha))$ (see [12] for an overview of work on this and related questions). In the present article, we study factorizations of polynomials of the form $f^n(x) - \alpha$ in the case where $\alpha = 0$.

Definition 1.1. *Let K be a field and $f \in K[x]$, and $\alpha \in K$. We say (f, α) is **eventually stable over** K if there exists a constant $C(f, \alpha)$ such that the number of irreducible factors over K of $f^n(x) - \alpha$ is at most $C(f, \alpha)$ for all $n \geq 1$.*

We say that f is eventually stable over K if $(f, 0)$ is eventually stable.

Apart from its own interest, eventual stability has proven to be a key link in at least two recent proofs of finite-index results for certain arboreal representations [4, 3]. This is perhaps surprising given that eventual stability is, a priori, much weaker than finite index of the arboreal representation – the former only implies that the number of Galois orbits on $f^{-n}(\alpha)$ is bounded as n grows, which is an easy consequence of the latter. There are other applications of eventual stability as well; for instance, if $f \in \mathbb{Q}[x]$ is eventually stable over $\mathbb{Q}$, then a finiteness result holds for S-integer points in the backwards orbit of 0 under f (see [13, Section 3] and [18]).

The paper [13] provides an overview of eventual stability and related ideas. That article defines a notion of eventual stability for rational functions, gives several characterizations of eventual stability, and states some general conjectures on the subject, all of which remain wide open. For example, a special case of [13, Conjecture 1.2] is the following: if $f \in \mathbb{Q}[x]$ is a polynomial of degree $d \geq 2$ such that 0 is not periodic under f (i.e. $f^n(0) \neq 0$ for all $n \geq 1$), then f is eventually stable over $\mathbb{Q}$. Theorems 1.3 and 1.7 of [13] also provide some of the few reasonably general results currently available on eventual stability. The proofs rely on generalizations of the Eisenstein criterion, and crucially assume good reduction of the rational function at the prime in question.

In this article, we address some of the conjectures in [13] in cases where Eisenstein-type methods break down. One of our main results is the following:

Theorem 1.2. *Let $K = \mathbb{Q}$ and $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}\setminus\{0,-1\}$. If $|c| \le 10^9$, then f_r is eventually stable over $\mathbb{Q}$ and $C(f_r, 0) \le 4$. More precisely, Conjecture* 1.7 *below holds for all c with $|c| \le 10^9$.*

The family $x^2 + (1/c)$, $c \in \mathbb{Z} \setminus \{0, -1\}$, is particularly recalcitrant. Eventual stability in this family (with $\alpha = 0$) is conjectured in [13, Conjecture 1.4], and it is the only obstacle to establishing eventual stability (with $\alpha = 0$) in the family $x^2 + r, r \in \mathbb{Q}$. This is because [13, Theorem 1.7] handles the case when there is a prime p with $v_p(r) > 0$. Moreover, [13, Theorem 1.3] uses $p = 2$ to establish eventual stability for $x^2 + 1/c$ when c is odd, but when c is even $x^2 + 1/c$ has bad reduction at $p = 2$, and Eisenstein-type methods break down completely.

We turn to methods inspired by [10], in particular various amplifications of [10, Proposition 4.2] and [11, Theorem 2.2], which state that the irreducibility of iterates can be proven by showing a certain sequence contains no squares. We prove the following theorem, which plays a substantial role in the proof of Theorem 1.2. For the rest of the article, we establish the following conventions:

all irreducibility statements are over $\mathbb{Q}$;

$r = 1/c$, where c is a non-zero integer.

Also, we denote by $\mathbb{Z} \setminus \mathbb{Z}^2$ the set of integers that are not integer squares.

Theorem 1.3. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$. Then $f_r^n(x)$ is irreducible for all $n \ge 1$ if c satisfies one of the following conditions:*

(1) *$-c \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $c < 0$;*
(2) *$-c, c+1 \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $c \equiv -1 \bmod p$ for a prime $p \equiv 3 \bmod 4$;*
(3) *$-c, c+1 \in \mathbb{Z}\setminus\mathbb{Z}^2$ and c satisfies one of the congruences in Proposition* 3.5 *(see Table 1).*
(4) *$-c \in \mathbb{Z} \setminus \mathbb{Z}^2$ and c is odd;*
(5) *$-c \in \mathbb{Z} \setminus \mathbb{Z}^2$, c is not of the form $4m^2(m^2-1), m \in \mathbb{Z}$, and*

$$\frac{\prod\limits_{p:2\nmid v_p(c)} p^{v_p(c)}}{\prod\limits_{p:2\mid v_p(c)} p^{v_p(c)}} > \frac{1.15}{|c|^{1/30}}.$$

This holds whenever c is squarefree.
(6) *$c = k^2$ for some $k \ge 2$ and*

$$\frac{\prod\limits_{p:p\not\equiv 1 \bmod 4} p^{v_p(c)}}{\prod\limits_{p:p\equiv 1 \bmod 4} p^{v_p(c)}} > \frac{1.15}{|c|^{1/30}}.$$

(7) *c is not of the form $4m^2(m^2-1)$ with $m \in \mathbb{Z}$ and $1 \le c \le 10^{1000}$.*

Our next result gives an explicit and relatively small bound for m such that the irreducibility of f^m implies the irreducibility of all f^n (see Corollary 4.6). In the following, $\varepsilon(c)$ is a function bounded above by 4 and decreasing monotonically to 2 as c grows; for a precise definition, see p. 550 in Section 4.

Theorem 1.4. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}$ with $c \geq 4$. If f^m is irreducible for*

$$m = 1 + \Big\lfloor \log_2\Big(1 + \frac{\log 4 + \varepsilon(c)/\sqrt{c}}{\log(1 + 1/\sqrt{c})}\Big)\Big\rfloor,$$

then all f^n are irreducible.

The methods used in the proof of this result can be used to derive a very efficient algorithm that checks the condition in Theorem 1.4 for all c up to a very large bound. This leads to a proof of case (7) of Theorem 1.3, which at the same time verifies Conjecture 1.8 below for all c with $|c| \leq 10^{1000}$. This is explained in Section 5.

We also prove results on unusual factorizations of small iterates in the family $x^2 + 1/c$.

Theorem 1.5. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then*

(a) *We have $k_1 = k_2 = 2$ and $k_3 = 3$ if and only if $c = -16$. In this case $k_n = 3$ for all $n \geq 3$.*
(b) *We have $k_3 \geq 4$ if and only if $c = -(s^2 - 1)^2$ for $s \in \{3, 5, 56\}$. In this case, $k_1 = 2$, $k_2 = 3$, and $k_n = 4$ for all $n \geq 3$.*
(c) *We have $k_1 = 1$ and $k_3 \geq 3$ if and only if $c = 48$. In this case, $k_2 = 2$ and $k_n = 3$ for all $n \geq 3$.*

Observe that part (b) of Theorem 1.5 shows that the bound $C(f_r, 0) \leq 4$ in Theorem 1.2 (and also Conjecture 1.7) cannot be improved. Moreover, a consequence of Conjecture 1.7 is that $C(f_r, 0) = 4$ if and only if $c = -(s^2 - 1)^2$ for $s \in \{3, 5, 56\}$.

To prove Theorem 1.5, we reduce the problem to finding all integer square values of certain polynomials (see Lemma 2.2 in Section 2 for details.) The curve that arises in this way in the proof of part (c) of Theorem 1.5 is of particular interest, as it is a hyperelliptic curve of genus two, whose Jacobian has rank two:

$$y^2 = 8x^6 - 12x^4 - 4x^3 + 4x^2 + 4x + 1. \tag{1}$$

Because the genus and the rank of the Jacobian coincide, we cannot apply the well-known method of Chabauty and Coleman. On the other hand, we are able to use a variant of the standard method, called elliptic Chabauty [5, 7], to prove:

Theorem 1.6. *The only rational points on the curve* (1) *are those with $x \in \{-2, -1, 0, 1\}$.*

The idea is the following:given an elliptic curve E over a number field K and a map $\phi : E \to \mathbb{P}^1$, then one can often compute the set of points in $E(K)$ mapping to $\mathbb{P}^1(\mathbb{Q})$ as long as the rank of $E(K)$ is strictly less than the degree of the extension $K/\mathbb{Q}$.This method is known as elliptic Chabauty. Moreover, in certain situations, one can use a combination of descent techniques and elliptic Chabauty to determine the full set of rational points on a curve C (of higher genus) defined over $\mathbb{Q}$; see, for instance, the proof of Theorem 1.6. Moreover, under suitable conditions, several components of the elliptic Chabauty method are implemented in MAGMA [2], and we make use of these implementations here. Our code verifying the calculations in the proof of Theorem 1.5 can be found within the file called *Elliptic Chabauty* at: `https://sites.google.com/a/alumni.brown.edu/whindes/research`.

The above results furnish evidence for several conjectures. The first is a refinement of Conjecture 1.4 of [13], which states that $x^2 + \frac{1}{c}$ is eventually stable for $c \in \mathbb{Z} \setminus \{0, -1\}$.

Conjecture 1.7. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$. Then f_r is eventually stable and $C(f_r, 0) \leq 4$. More precisely, let k_n denote the number of irreducible factors of $f_r^n(x)$. Then*

1. *If $c = -m^2$ for $m > 0$ with $m + 1 \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $m \neq 4$, then $k_n = 2$ for all $n \geq 1$.*
2. *If $c = -16$, then $k_1 = k_2 = 2$ and $k_n = 3$ for all $n \geq 3$.*
3. *If $c = -(s^2 - 1)^2$ for $s \in \mathbb{Z} \setminus \{3, 5, 56\}$, then $k_1 = 2$ and $k_n = 3$ for all $n \geq 2$.*
4. *If $c = -(s^2 - 1)^2$ for $s \in \{3, 5, 56\}$, then $k_1 = 2$, $k_2 = 3$, and $k_n = 4$ for all $n \geq 3$.*
5. *If $c = 4m^2(m^2 - 1)$ for $m \in \mathbb{Z}$, $m \geq 3$, then $k_1 = 1$ and $k_n = 2$ for all $n \geq 2$.*
6. *If $c = 48$, then $k_1 = 1$, $k_2 = 2$, and $k_n = 3$ for all $n \geq 3$.*
7. *If c is not in any of the above cases, then $k_n = 1$ for all $n \geq 1$.*

We remark that case (7) of Conjecture 1.7 is precisely the case where $f_r^2(x)$ is irreducible (see Proposition 2.1) and thus case (7) asserts that if $f_r^2(x)$ is irreducible, then $f_r^n(x)$ is irreducible for all $n \geq 1$. We state this as its own conjecture:

Conjecture 1.8. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$. If $f_r^2(x)$ is irreducible, then $f_r^n(x)$ is irreducible for all $n \geq 1$.*

As mentioned above, we have verified this conjecture for all c with $|c| \leq 10^{1000}$.

Observe that Conjecture 1.7 gives a uniform bound for k_n, in contrast to Conjecture 1.4 of [13]. It would be of great interest to have a similar uniform bound for $f_r(x)$ as r is allowed to vary over the entire set $\mathbb{Q} \setminus \{0, -1\}$ (as opposed to just the reciprocals of integers, as in Conjecture 1.7). We pose here a much more general question. Given a field K, call $f \in K[x]$

normalized (the terminology *depressed* is also sometimes used, especially for cubics) if $\deg f = d \geq 2$ and $f(x) = a_d x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + a_1 x + a_0$. Note that every $f \in K[x]$ of degree not divisible by the characteristic of K is linearly conjugate over K to a normalized polynomial.

Question 1.9. *Let K be a number field and fix $d \geq 2$. Is there a constant κ depending only on d and $[K : \mathbb{Q}]$ such that, for all normalized $f \in K[x]$ of degree d such that 0 is not periodic under f, and all $n \geq 1$, $f^n(x)$ has at most κ irreducible factors? In the case where $K = \mathbb{Q}$, $d = 2$, and f is taken to be monic, does the same conclusion hold with $\kappa = 4$?*

It is interesting to compare Question 1.9 to [1, Question 19.5], where a similar uniform bound is requested, but under the condition that $f^{-1}(0) \cap \mathbb{P}^1(K) = \emptyset$.

We close this introduction with some further comments on our methods, as well as the statement of one additional result (Theorem 1.12) on the densities of primes dividing orbits of polynomials of the form $x^2 + 1/c$.

A primary tool in our arguments is the following special case of [11, Theorem 2.2]: for $n \geq 2$, f_r^n is irreducible provided that f_r^{n-1} is irreducible and $f_r^n(0)$ is not a square in $\mathbb{Q}$. The proof of this relies heavily on the fact that f_r has degree 2, and is essentially an application of the multiplicativity of the norm map. Using ideas from [11, Theorem 2.3 and discussion preceding], one obtains the useful amplification (proven in Section 3) that for $n \geq 2$, f_r^n is irreducible provided that f_r^{n-1} is irreducible and neither of $(f_r^{n-1}(0) \pm \sqrt{f_r^n(0)})/2$ is a square in $\mathbb{Q}$. When $r = 1/c$, we have

$$f_r(0) = 1/c, \quad f_r^2(0) = (c+1)/c^2, \quad f_r^3(0) = (c^3 + c^2 + 2c + 1)/c^4,$$

and so on. The numerator of $f_r^n(0)$ is obtained by squaring the numerator of $f_r^{n-1}(0)$, and adding $c^{2^{n-1}-1}$. We thus introduce the family of sequences

$$a_1(c) = 1, \qquad a_n(c) = a_{n-1}(c)^2 + c^{2^{n-1}-1} \quad \text{for } n \geq 2. \tag{2}$$

To ease notation, we often suppress the dependence on c, and write a_1, a_2, etc. We can then translate the results of the previous paragraph to:

Lemma 1.10. *Suppose that $c \in \mathbb{Z} \setminus \{0\}$, $r = 1/c$, and f_r^2 is irreducible. Let $a_n = a_n(c)$ be defined as in (2), and set*

$$b_n := \frac{a_{n-1} + \sqrt{a_n}}{2} \in \overline{\mathbb{Q}}. \tag{3}$$

If for every $n \geq 3$, b_n is not a square in $\mathbb{Q}$ (which holds in particular if a_n is not a square in $\mathbb{Q}$), then $f_r^n(x)$ is irreducible for all $n \geq 1$.

We make the following conjecture, which by Lemma 1.10 immediately implies Conjecture 1.8:

Conjecture 1.11. *Let $b_n = b_n(c)$ be defined as in (3). If $c \in \mathbb{Z} \setminus \{0, -1\}$, then b_n is not a square in $\mathbb{Q}$ for all $n \geq 3$.*

Conjecture 1.11 also has strong implications for the density of primes dividing orbits of f_r. We define the orbit of $t \in \mathbb{Q}$ under f_r to be the set $O_{f_r}(t) = \{t, f_r(t), f_r^2(t), \ldots\}$, and we say that a prime p divides $O_{f_r}(t)$ if there is at least one non-zero $y \in O_{f_r}(t)$ with $v_p(y) > 0$. The natural density of a set S of prime numbers is defined to be

$$D(S) = \lim_{B\to\infty} \frac{\#\{p \le B : p \in S\}}{\#\{p \le B\}}.$$

Note that the elements of $O_{f_r}(t)$ also form a nonlinear recurrence sequence, where the relation is given by application of f_r. The problem of finding the density of prime divisors in recurrences has an extensive literature in the case of a linear recurrence; see the discussion and brief literature review in [10, Introduction]. The case of non-linear recurrences is much less-studied, though there are some recent results [8, 10, 17]. The following theorem is an application of [8, Theorem 1.1, part (2)].

Theorem 1.12. *Let $c \in \mathbb{Z}$, let $r = 1/c$, suppose that $-c$ and $c+1$ are non-squares in $\mathbb{Q}$, and assume that Conjecture* 1.11 *holds for c. Then*

$$\text{for any } t \in \mathbb{Q} \text{ we have } D(\{p \text{ prime} : p \text{ divides } O_{f_r}(t)\}) = 0. \tag{4}$$

We remark that in each of the cases of Theorem 1.3, we show that Conjecture 1.11 holds for c. Hence, in cases (2), (3), and (6) of Theorem 1.3 and also in cases (1), (4), and (5), with the additional hypothesis that $c+1$ is not a square in $\mathbb{Q}$, we have that (4) holds. We also note that when the hypotheses of Theorem 1.12 are satisfied, we obtain certain information on the action of $G_{\mathbb{Q}}$ on $T_f(0) = \bigsqcup_{n\ge 0} f^{-n}(0)$; see Section 6.

A complete proof of Conjecture 1.11 appears out of reach at present. One natural approach is to prove the stronger statement that a_n is not a square for each $n \ge 3$, or equivalently that the curve

$$C_n : y^2 = a_n(c) \tag{5}$$

has no integral points with $c \notin \{0, -1\}$ for any $n \ge 3$. It is easy to see that $a_n(c)$ is separable as a polynomial in c (one considers it as a polynomial in $\mathbb{Z}/2\mathbb{Z}[c]$, where it is relatively prime to its derivative), and because the degree of $a_n(c)$ is $2^{n-1}-1$, it follows from standard facts about hyperelliptic curves that the genus of C_n is $2^{n-2}-1$. Siegel's theorem then implies that there are only finitely many c with $a_n(c)$ a square for given $n \ge 3$. However, the size of the genus of C_n prevents us from explicitly excluding the presence of integer points save in the cases of $n = 3$ and $n = 4$ (see Proposition 3.3). One idea that has been used to show families of integer non-linear recurrences contain no squares (see e.g. [19, Corollary 1.3] or [10, Lemma 4.3]) is to show that sufficiently large terms of each sequence are sandwiched between squares: they are generated by adding a small number to a large square. In the case of the family $a_n(c)$, however, the addition of the very large term $c^{2^{n-1}-1}$ to the square a_{n-1}^2 ruins this approach. A similar problem is encountered in a family of important two-variable non-linear recurrence sequences first

considered in [14] (see [14, Theorem 1.8]). The main idea used in [14] to show the recurrence contains no squares is to rule out certain cases via congruence arguments. This is the essence of our method of proof for cases (2) and (3) of Theorem 1.3. Subsequently, Swaminathan [22, Section 4] amplified these congruence arguments and gave new partial results using the idea of sandwiching terms of the sequence between squares. In the end, each of these methods succeeds in giving only partial results, applicable to c-values satisfying certain arithmetic criteria. It would be of great interest to have a proof of Conjecture 1.11 for c-values satisfying some analytic criterion, e.g., for all c sufficiently large. Case (1) of Theorem 1.3 provides one result with this flavor, but at present no other results are known.

Acknowledgements: We thank Jennifer Balakrishnan for conversations related to the proof of Theorem 1.6, and the anonymous referee for many helpful suggestions.

2. The case where $f_r(x)$ or $f_r^2(x)$ is reducible

We begin by studying the factorizations of iterates of $f_r(x)$ when either $f_r(x)$ or $f_r^2(x)$ is reducible. The behavior of higher iterates becomes harder to control because of the presence of multiple irreducible factors of the first two iterates, but we are still able to give some results. At the end of this section we prove Theorem 1.5, which gives a complete characterization of certain subcases.

Proposition 2.1. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$. Then $f_r(x)$ is reducible if and only if $c = -m^2$ for $m \in \mathbb{Z}$. If $f_r(x)$ is irreducible, then $f_r^2(x)$ is reducible if and only if $c = 4m^2(m^2 - 1)$ for $m \in \mathbb{Z}$.*

Proof. The first statement is clear. Assume now that $f_r(x)$ is irreducible over $\mathbb{Q}$. Let α be a root of $f_r^2(x)$, and observe that $f_r(\alpha)$ is a root of $f_r(x)$, and by the irreducibility of $f_r(x)$, we have $[\mathbb{Q}(f_r(\alpha)) : \mathbb{Q}] = 2$. Now $f_r^2(x)$ is irreducible if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, which is equivalent to $[\mathbb{Q}(\alpha) : \mathbb{Q}(f_r(\alpha))] = 2$. But α is a root of $f_r(x) - f_r(\alpha) = x^2 + r - f_r(\alpha)$, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}(f_r(\alpha))] = 2$ is equivalent to $f_r(\alpha) - r$ not being a square in $\mathbb{Q}(f_r(\alpha))$.

Without loss of generality, say $f_r(\alpha) = \sqrt{-r}$. Then $f_r(\alpha) - r$ is a square in $\mathbb{Q}(f_r(\alpha))$ if and only if there are $s_1, s_2 \in \mathbb{Q}$ with

$$-r + \sqrt{-r} = (s_1 + s_2\sqrt{-r})^2 = s_1^2 - rs_2^2 + 2s_1s_2\sqrt{-r}.$$

This holds if and only if $2s_1s_2 = 1$ and $s_1^2 - rs_2^2 = -r$. Substituting $s_2 = 1/(2s_1)$ into the second equation and multiplying through by s_1^2 gives $s_1^4 + rs_1^2 - r/4 = 0$, which by the quadratic formula holds if and only if

$$s_1^2 = \frac{-r \pm \sqrt{r^2 + r}}{2} \tag{6}$$

or equivalently, $2c(-1 \pm \sqrt{1 + c})$ is an integer square (here we have written $1/c$ for r and multiplied both sides of (6) by $4c^2$). If $c < -1$, then $\sqrt{1 + c}$ is

irrational, so we may assume $c > 0$. We may then discard the $-$ part of the $\pm$, since integer squares are positive. Writing $c = k^2 - 1$ for $k > 0$, we then obtain that $2(k^2-1)(-1+k) = 2(k+1)(k-1)^2$ is a square, whence $k+1 = 2m^2$ for some integer m. Thus $c = k^2 - 1 = (2m^2-1)^2 - 1 = 4m^4 - 4m^2$, as desired. □

We now give a lemma, closely related to [10, Proposition 4.2], which we will use often in the sequel.

Lemma 2.2. *Let K be a field of characteristic not equal to 2, let $g \in K[x]$ be monic of degree $d \geq 1$ and irreducible over K, and let $f(x)$ be monic and quadratic with critical point γ. If no element of*

$$\{(-1)^d g(f(\gamma))\} \cup \{g(f^n(\gamma)) : n \geq 2\}$$

is a square in K, then $g(f^n(x))$ is irreducible over K for all $n \geq 1$.

Proof. Let $f(x) = x^2 + bx + c$, so that $\gamma = -b/2$. We proceed by induction on n, with the $n = 0$ case covered by the irreducibility of $g(x)$. Assume then that $g(f^{n-1}(x))$ is irreducible over K for some $n \geq 1$, and let d_1 be the degree of $g(f^{n-1}(x))$. By Capelli's Lemma ([6, Lemma 0.1]), $g(f^n(x))$ is irreducible over K if and only if for any root β of $g(f^{n-1}(x))$, we have $f(x) - \beta$ is irreducible over $K(\beta)$, or equivalently (because K has characteristic different from 2), $\mathrm{Disc}(f(x) - \beta) = b^2 - 4c + 4\beta$ is not a square in $K(\beta)$.

This must hold if $N_{K(\beta)/K}(b^2 - 4c + 4\beta)$ is not a square in K. The Galois conjugates of $b^2 - 4c + 4\beta$ are precisely $b^2 - 4c + 4\alpha$ as α varies over all roots of $g(f^{n-1}(x))$. Thus

$$\begin{aligned} N_{K(\beta)/K}(b^2 - 4c + 4\beta) &= (-4)^{d_1} \prod_{\alpha \text{ root of } g \circ f^{n-1}} \left[\left(-\frac{b^2}{4} + c\right) - \alpha\right] \\ &= (-4)^{d_1} \cdot g(f^{n-1}(-b^2/4 + c)) \\ &= (-4)^{d_1} \cdot g(f^{n-1}(f(\gamma))), \end{aligned}$$

where the second equality holds because $g(f^{n-1}(x))$ is monic. Now d_1 is odd if and only if $n = 1$ and d is odd, which proves the Lemma. □

2.1. The case of f_r reducible. When $c = -m^2$ for some $m \geq 1$, we fix the notation

$$g_1(x) = x - \frac{1}{m} \qquad \text{and} \qquad g_2(x) = x + \frac{1}{m}, \tag{7}$$

so that $f_r(x) = g_1(x)g_2(x)$. We exclude the case $m = 1$ in what follows, as in that case $f_r(x)$ is not eventually stable (see [13, discussion following Corollary 1.5]).

Proposition 2.3. *Let $r = 1/c$ and $c = -m^2$ for $m \geq 2$. Let g_1 and g_2 be as in (7). Then the following hold.*

(1) *We have $g_2(f_r(x))$ irreducible, while $g_1(f_r(x))$ factors if and only if $m + 1$ is a square in $\mathbb{Q}$.*

(2) *If $g_1(f_r(x))$ is irreducible, then $g_1(f_r^n(x))$ is irreducible for all $n \geq 2$.*
(3) *If every term of the sequence $\{g_2(f_r^i(0))\}_{i\geq 2}$ is a non-square in $\mathbb{Q}$, then $g_2(f_r^n(x))$ is irreducible for all $n \geq 2$.*

Proof. The first item follows from observing that $g_1(f_r(x)) = x^2 - \frac{m+1}{m^2}$ and $g_2(f_r(x)) = x^2 + \frac{m-1}{m^2}$. The latter is irreducible because $m \geq 2$ implies $(m-1)/m^2 > 0$. Item (3) is an immediate consequence of item (1) and Lemma 2.2 (with $g = g_2 \circ f_r$ and $f = f_r$). To prove item (2), observe that $g_1(f_r^n(0)) = f_r^n(0) - \frac{1}{m}$. However, one easily checks that $x^2 - \frac{1}{m^2}$ maps the interval $(-1/m, 0)$ into itself, and in particular, $f_r^n(0) < 0$ for all $n \geq 1$. Thus $g_1(f_r^n(0)) < 0$ as well, and hence cannot be a square in $\mathbb{Q}$. Item (2) now follows from Lemma 2.2 with $g = g_1 \circ f_r$ and $f = f_r$. □

Proposition 2.4. *Let $r = 1/c$ and $c = -m^2$ for $m \geq 2$, and let g_1 and g_2 be as in* (7)*. Then $g_2(f_r^2(0))$ is a square in $\mathbb{Q}$ if and only if $m = 4$. Moreover, $g_2(f_r^2(x))$ is reducible if and only if $m = 4$.*

Proof. Observe that

$$g_2(f_r^2(0)) = \frac{m^3 - m^2 + 1}{m^4},$$

and hence $g_2(f_r^2(0))$ is a square in $\mathbb{Q}$ if and only if the elliptic curve $y^2 = x^3 - x^2 + 1$ has an integral point with $x = m$. This is curve 184.a1 in the LMFDB [16], and has only the integral points $(0, \pm 1), (1, \pm 1), (4, \pm 7)$. Because $m \geq 2$, the only m-value for which $g_2(f_r^2(0))$ is a square is $m = 4$. If $m \neq 4$, then [10, Proposition 4.2] (or the proof of Lemma 2.2, with $g = g_2 \circ f_r$ and $f = f_r$) shows that $g_2(f_r^2(x))$ is irreducible. On the other hand, if $m = 4$, then

$$g_2(f_r^2(x)) = (x^2 - x + 7/16)(x^2 + x + 7/16),$$

showing that $g_2(f_r^2(x))$ is reducible. We return to the analysis of the case $m = 4$ in Proposition 2.10. □

We now seek to give congruence conditions on m that ensure the sequence $(g_2(f_r^n(0)))_{n\geq 2}$ contains no squares in $\mathbb{Q}$. Prime factors of the numerators of the terms of this sequence are often related to each other. To formalize this, we require the following definition.

Definition 2.5. *A sequence $(s_n)_{n\geq 1}$ is a rigid divisibility sequence if for all primes p we have the following:*

(1) *if $v_p(s_n) = e > 0$, then $v_p(s_{mn}) = e$ for all $m \geq 1$, and*
(2) *if $v_p(s_n) > 0$ and $v_p(s_j) > 0$, then $v_p(s_{\gcd(n,j)}) > 0$.*

Remark 2.6. If $(s_n)_{n\geq 1}$ is a rigid divisibility sequence and $s_1 = 1$, then from (2) it follows that if $p \mid \gcd(s_n, s_{n-1})$ then $p \mid s_1 = 1$, which is impossible. Hence, $\gcd(s_n, s_{n-1}) = 1$ for all $n \geq 2$. A similar argument shows that for q prime we have $\gcd(s_q, s_i) = 1$ for all $1 \leq i < q$.

Proposition 2.7. *Let $r = 1/c$ and $c = -m^2$ for $m \geq 2$, and let g_2 be as in (7). Then $g_2(f_r^n(x))$ is irreducible for all $n \geq 2$ provided that $m \neq 4$ and at least one of the following holds:*

$m \equiv 3$	(mod 4)	$m \equiv 3$	(mod 5)
$m \equiv 2, 5, 6$	(mod 7)	$m \equiv 4, 6, 7$	(mod 11)
$m \equiv 8, 10$	(mod 13)	$m \equiv 2, 4, 7, 8, 9, 11, 15$	(mod 17)
$m \equiv 3, 5, 11$	(mod 19)	$m \equiv 9, 11, 14, 15, 18, 20, 21, 22$	(mod 23)
$m \equiv 3, 19, 26$	(mod 29)	$m \equiv 2, 12, 30$	(mod 31)
$m \equiv 6, 20$	(mod 37)	$m \equiv 12, 14, 27, 29$	(mod 41)
$m \equiv 15, 21, 30$	(mod 43)	$m \equiv 9, 22, 38, 46$	(mod 47)

If, in addition, $m - 1$ is not a square in $\mathbb{Q}$, then the following congruences also suffice:

$m \equiv 2$	(mod 3)	$m \equiv 5$	(mod 8)
$m \equiv 10$	(mod 11)	$m \equiv 18$	(mod 19)
$m \equiv 2, 13$	(mod 23)	$m \equiv 8, 10, 14$	(mod 29)
$m \equiv 9, 26$	(mod 31)	$m \equiv 13, 31$	(mod 37)
$m \equiv 3, 11, 19, 37, 38$	(mod 41)	$m \equiv 22, 36, 39, 42$	(mod 43)
$m \equiv 3, 10$	(mod 47)		

Proof. By part (3) of Proposition 2.3, it suffices to show that $g_2(f_r^n(0))$ is not a square in $\mathbb{Q}$ for all $n \geq 2$. Note that for each $n \geq 1$, $g_2(f_r^{n-1}(0))$ is a positive rational number with denominator $m^{2^{n-1}}$, and numerator prime to m. We take w_n to be the numerator of $g_2(f_r^{n-1}(0))$. We first observe that the proof of [10, Proposition 5.4] shows that the sequence $(w_n)_{n\geq 1}$ is a rigid divisibility sequence. In particular, if w_2 is not a square in $\mathbb{Q}$, then because $w_2 > 0$ we must have some prime p dividing w_2 to odd multiplicity, and the rigid divisibility condition implies that w_{2j} is not a square for all $j \geq 2$. A similar argument shows that if w_3 is not a square in $\mathbb{Q}$, then neither is w_{3j} for all $j \geq 1$.

By Proposition 2.4 and our assumption that $m \neq 4$, we have that $g_2(f_r^2(0))$ is not a square in $\mathbb{Q}$. It follows that w_{3j} is a non-square for all $j \geq 1$.

Now, for a given modulus k and $m \not\equiv 0 \bmod k$, the sequence $(g_2(f_r^n(0)) \bmod k)_{n\geq 1}$ eventually lands in a repeating cycle, and we search for values of k and congruences classes of m modulo k such that $g_2(f_r^n(0)) \bmod k$ fails to be a square for all $n \geq 2$. Note that this method works even when $g_2(f_r^{3j-1}(0)) \bmod k$ is a square for all $j \geq 1$, since we have shown in the previous paragraph that w_{3j} is a non-square for all $j \geq 1$. A computer search yields the congruences given in the first part of the proposition. If, in addition, $m - 1$ is a non-square in $\mathbb{Q}$, then we have w_{2j} not a square in

$\mathbb{Q}$ for all $j \geq 1$, and the congruences in the second part of the proposition show that $w_{2j+1} = g_2(f_r^{2j}(0)) \bmod k$ is a non-square for all $j \geq 1$. □

Proposition 2.8. *Let $r = 1/c$ and $c = -m^2$ for $m \geq 2$, and let g_2 be as in (7). If $m \equiv -1 \bmod p$ for a prime $p \equiv 7 \bmod 8$, then $g_2(f_r^n(x))$ is irreducible for all $n \geq 2$. The same conclusion holds if $m - 1$ is not a square in $\mathbb{Q}$ and $m \equiv -1 \bmod p$ for a prime $p \equiv 3 \bmod 8$.*

Proof. By part (3) of Proposition 2.3, it suffices to show that $g_2(f_r^n(0))$ is not a square in $\mathbb{Q}$ for all $n \geq 2$. We have $c = -m^2 \equiv -1 \bmod p$, and so $(f_r^n(0) \bmod p)_{n\geq 0}$ is the sequence $0, -1, 0, -1 \ldots$. Thus $(g_2(f_r^n(0)) \bmod p)_{n\geq 0}$ is the sequence $-1, -2, -1, -2, -1, \ldots$. If $p \equiv 7 \bmod 8$, then both -1 and -2 are non-squares modulo p, and the proof is complete. If $p \equiv 3 \bmod 8$, then -1 is a non-square modulo p but -2 is a square, meaning we can only conclude that $g_2(f_r^{2j}(0))$ is a non-square in $\mathbb{Q}$ for $j \geq 1$. However, as in the proof of Proposition 2.7, this implies that b_{2j+1} is a non-square for all $j \geq 1$. If in addition $m - 1$ is not a square, then b_{2j} is not a square for all $j \geq 1$, completing the proof. □

Propositions 2.7 and 2.8 allow us to prove a case of Theorem 1.2. Recall that $g_1(f_r^n(x))g_2(f_r^n(x)) = f_r^{n+1}(x)$.

Corollary 2.9. *Let $r = 1/c$ and $c = -m^2$ for $m \geq 2$, and let g_2 be as in (7). Suppose that $m \neq 4$ and $m^2 \leq 10^9$. Then $g_2(f_r^n(x))$ is irreducible for all $n \geq 1$. If in addition $m+1$ is not a square in $\mathbb{Q}$, then $f_r^n(x)$ is a product of two irreducible factors for all $n \geq 1$.*

Proof. By part (3) of Proposition 2.3, it suffices to show that $g_2(f_r^n(0))$ is not a square in $\mathbb{Q}$ for all $n \geq 2$. Because $m \neq 4$, we may apply both Propositions 2.7 and 2.8. The first group of congruences in Proposition 2.7 applies to all m with $2 \leq m \leq 10^{9/2}$ except for a set of 1326 m-values. After applying the first part of Proposition 2.8, that number decreases to 1021. Of these, 13 have the property that $m - 1$ is a square. We apply the second group of congruences in Proposition 2.7 and the second part of Proposition 2.8 to the remaining 1008 values, and only 196 survive. This leaves 209 values of m that we must handle via other methods.

To do this, we employ a new method to search for primes p such that $g_2(f_r^n(0))$ is a non-square modulo p for all but finitely many n. We search for p such that:

$$\begin{aligned}&\text{the sequence } (g_2(f_r^n(0)) \bmod p)_{n\geq 0} \text{ eventually assumes}\\ &\quad\text{a non-square constant value or eventually cycles between two distinct}\\ &\qquad\qquad\text{values, both of which are non-squares modulo } p. \quad (8)\end{aligned}$$

If we find such a p, it implies that all but finitely many terms of the sequence $(g_2(f_r^n(0)))_{n\geq 2}$ are non-squares in $\mathbb{Q}$. We then reduce modulo other primes to show that the remaining terms are non-squares.

The method proves quite effective. Of the 209 m-values left over from the first paragraph of this proof, all have a prime $p < 500$ that satisfies (8). For each such m and p, we take the finitely many terms of the sequence $(g_2(f_r^n(0)))_{n\geq 2}$ that have still not been proven non-square by (8), and reduce modulo small primes until all have been proven non-square. The m-value producing the largest number of such terms is $m = 4284$, where we must check that each of $g_2(f_r(0)), g_2(f_r^2(0)), \ldots, g_2(f_r^{34}(0))$ is a non-square. In all cases the desired result is achieved by reducing modulo primes less than 100. □

We now consider the case $m = 4$. As shown in Proposition 2.4, it is the only one with $m \geq 2$ for which $g_2(f_r^2(x))$ is reducible; indeed, we have

$$g_2(f_r^2(x)) = (x^2 - x + 7/16)(x^2 + x + 7/16) =: g_{21}(x)g_{22}(x), \tag{9}$$

and we note that both $g_{21}(x)$ and $g_{22}(x)$ are irreducible.

Proposition 2.10. *Let $r = -1/16$ and let g_{21} and g_{22} be as in (9). For all $n \geq 1$, both $g_{21}(f_r^n(x))$ and $g_{22}(f_r^n(x))$ are irreducible for all $n \geq 1$. In particular, $f_r^n(x)$ has precisely three irreducible factors for all $n \geq 3$.*

Proof. Because $m+1$ is not a square, Proposition 2.3 shows that $g_1(f_r^n(x))$ is irreducible for all $n \geq 1$. By Lemma 2.2 and the fact that g_{21} and g_{22} have even degree, it suffices to prove that neither $g_{21}(f_r^n(0))$ nor $g_{22}(f_r^n(0))$ is a square in $\mathbb{Q}$ for all $n \geq 1$. Observe that $f_r^n(0) \equiv 5 \bmod 11$ for $n \geq 3$, and $g_{21}(5) \equiv 6 \bmod 11$. Because 6 is a non-square modulo 11, we must only verify that neither of $g_{21}(f_r(0))$ or $g_{21}(f_r^2(0))$ is a square in $\mathbb{Q}$. The former is $129/256$ and the latter is $(19 \cdot 1723)/2^{16}$, neither of which is a square in $\mathbb{Q}$. For $g_{22}(f_r^n(0))$ we have a simpler argument using $p = 5$: observe that $g_{22}(0) \equiv g_{22}(-1) \equiv 2 \bmod 5$ and $f_r^n(0) \equiv 0$ or $-1 \bmod 5$ for all $n \geq 1$. □

We now consider the case where $m + 1$ is a square. Say $m + 1 = s^2$ with $s \geq 2$, so that $f_r(x) = x^2 - 1/m^2 = x^2 - 1/(s^2 - 1)^2$. We have

$$g_1(f_r(x)) = x^2 - \frac{m+1}{m^2} = \left(x - \frac{s}{s^2-1}\right)\left(x + \frac{s}{s^2-1}\right) =: h_1(x)h_2(x). \tag{10}$$

Now, $h_1(f_r(x)) = x^2 - \frac{s^3-s+1}{(s^2-1)^2}$. Thus, $h_1(f_r(x))$ is irreducible unless s is the x-coordinate of an integral point on the elliptic curve $y^2 = x^3 - x + 1$. This is curve 92.a1 in LMFDB, and has an unusually large number of integral points: $(0, \pm 1), (1, \pm 1), (-1, \pm 1)(3, \pm 5), (5, \pm 11), (56, \pm 419)$. We assume for a moment that $s \notin \{3, 5, 56\}$, so that $h_1(f_r(x))$ is irreducible. Observe that $x^2 - \frac{1}{m^2}$ maps the interval $(-1/m, 0)$ into itself, and in particular, $f_r^n(0) < 0$ for all $n \geq 1$. Thus, $h_1(f_r^n(0)) < 0$ as well, and hence cannot be a square in $\mathbb{Q}$. Then Lemma 2.2 (with $g = h_1 \circ f_r$ and $f = f_r$) proves that $h_1(f_r^n(x))$ is irreducible for all $n \geq 2$. Thus, for $s \notin \{3, 5, 56\}$, we have that $h_1(f_r^n(x))$ is irreducible for all $n \geq 1$. We now present a result that builds on Corollary 2.9.

Corollary 2.11. *Let $r = 1/c$ and $c = -(s^2-1)^2$ for $s \geq 2$, and let g_2 be as in (7) and h_1, h_2 as in (10). Suppose that $(s^2-1)^2 \leq 10^9$. Then for all $n \geq 1$ we have $g_2(f_r^n(x))$ and $h_2(f_r^n(x))$ irreducible. If, in addition, $s \notin \{3, 5, 56\}$ then for all $n \geq 1$ we have $h_1(f_r^n(x))$ irreducible. In particular, if $(s^2-1)^2 \leq 10^9$ and $s \notin \{3, 5, 56\}$, then $f_r^n(x)$ is a product of three irreducible factors for all $n \geq 2$.*

Proof. Observe that $(s^2-1)^2 \leq 10^9$ if and only if $s \leq 177$. We have shown in Corollary 2.9 that $g_2(f_r^n(x))$ is irreducible for all s with $2 \leq s \leq 177$. In the paragraph preceding the present corollary, we showed that $s \notin \{3, 5, 56\}$ implies that $h_1(f_r^n(x))$ is irreducible for all $n \geq 1$. To show that $h_2(f_r^n(x))$ is irreducible for $n \geq 1$, it suffices by Lemma 2.2 to show that $\{-h_2(f_r(0))\} \cup \{h_2(f_r^n(0)) : n \geq 2\}$ contains no squares in $\mathbb{Q}$. Note that $-h_2(f_r(0)) = -\frac{s^3-s-1}{(s^2-1)^2}$, and we have $s^3 - s - 1 > 0$ for $s \geq 2$. Hence, $h_2(f_r(0))$ is not a square in $\mathbb{Q}$. To verify that $h_2(f_r^n(0))$ is a non-square in $\mathbb{Q}$ for all $n \geq 2$, we search for primes p satisfying the condition (8), with h_2 replacing g_2. We find that there exists a prime $p \leq 500$ with the desired property for all s with $2 \leq s \leq 177$ except for $s = 153$. For that s-value, the prime $p = 1051$ suffices.

For each such s and p, we take the finitely many terms of the sequence $(h_2(f_r^n(0)))_{n \geq 2}$ that have still not been proven non-square, and reduce modulo small primes until all have been proven non-square. Unsurprisingly, the s-value producing the largest number of such terms is $s = 153$, where we must check that each of $h_2(f_r(0)), h_2(f_r^2(0)), \ldots, h_2(f_r^{67}(0))$ is a non-square. In all cases the desired result is achieved by reducing modulo primes less than 100. □

Finally, we handle the case of $s \in \{3, 5, 56\}$. These are precisely the s-values for which $s^3 - s + 1$ is a square. In this case, $h_1(f(x))$ is no longer irreducible; indeed, we have

$$h_1(f(x)) = \left(x - \frac{\sqrt{s^3 - s + 1}}{s^2 - 1}\right)\left(x + \frac{\sqrt{s^3 - s + 1}}{s^2 - 1}\right) =: h_{11}(x)h_{12}(x). \tag{11}$$

Proposition 2.12. *Let $r = 1/c$ and $c = -(s^2-1)^2$ for $s \in \{3, 5, 56\}$. Let g_2 be as in (7), h_2 as in (10), and h_{11} and h_{12} as in (11). Then for all $n \geq 1$ we have $g_2(f_r^n(x))$, $h_2(f_r^n(x))$, $h_{11}(f_r^n(x))$, and $h_{12}(f_r^n(x))$ irreducible; in particular, $f_r^n(x)$ is a product of four irreducible factors for all $n \geq 3$.*

Proof. Corollary 2.11 shows that for $s \in \{3, 5, 56\}$, we have $g_2(f_r^n(x))$ and $h_2(f_r^n(x))$ irreducible for all $n \geq 1$. To show that $h_{11}(f_r^n(x))$ and $h_{12}(f_r^n(x))$ are irreducible for $n \geq 1$, it suffices by Lemma 2.2 to show that none of

$$\{-h_{11}(f_r(0))\} \cup \{-h_{12}(f_r(0))\} \cup \{h_{11}(f_r^n(0)) : n \geq 2\} \cup \{h_{12}(f_r^n(0)) : n \geq 2\}$$

is a square in $\mathbb{Q}$. Note that $-h_{11}(f_r(0)) = ((s^2-1)(\sqrt{s^3 - s + 1}) + 1)/(s^2 - 1)^2$. For $s = 3, 5, 56$ respectively, the prime factorization of the numerator

of $-h_{11}(f_r(0))$ is $41, 5 \cdot 53$, $2 \cdot 656783$, none of which is a square. Moreover, $-h_{12}(f_r(0)) < 0$, and hence cannot be a square. Also, one readily sees that $h_{11}(f_r^n(0)) < 0$ for all $n \geq 2$. For $s = 3$, we reduce the sequence $(h_{12}(f_r^n(0))_{n\geq 2}$ modulo 29 and find that it cycles among the four values $17, 15, 26, 21$, none of which is a square modulo 29. For $s = 5$, we reduce modulo 23 and find that the sequence in question cycles between 10 and 11, which are both non-squares modulo 23. For $s = 56$, we reduce modulo 31 and find that the sequence takes only the value 6, i.e. $h_{12}(f_r^n(0)) \equiv 6 \bmod 31$ for all $n \geq 2$. But 6 is non-square modulo 31. □

2.2. The case of f_r irreducible, f_r^2 reducible. Assume now that $c = 4m^2(m^2-1)$ for some $m \geq 2$, in which case we have

$$f_r^2(x) = \left(x^2 - \frac{1}{m}x + \frac{2m^2-1}{4m^2(m^2-1)}\right)\left(x^2 + \frac{1}{m}x + \frac{2m^2-1}{4m^2(m^2-1)}\right). \quad (12)$$

Let $q_1(x) = x^2 - \frac{1}{m}x + \frac{2m^2-1}{4m^2(m^2-1)}$ and $q_2(x) = x^2 + \frac{1}{m}x + \frac{2m^2-1}{4m^2(m^2-1)}$. We note that q_1 and q_2 both have discriminant $-1/(m^2-1)$, and so are irreducible.

Observe that for $m = 2$ we have the factorization

$$q_2(f_r(x)) = (x^2 - (1/2)x + 19/48)(x^2 + (1/2)x + 19/48). \quad (13)$$

However, this is the only m-value for which such a factorization occurs, as the next two results show.

Proposition 2.13. *Let $r = 1/c$ and $c = 4m^2(m^2-1)$ for $m \geq 2$. If $f_3(x)$ has strictly more than two irreducible factors, then either*

$$8m^6-12m^4+4m^3+4m^2-4m+1 \qquad \textit{or} \qquad 8m^6-12m^4-4m^3+4m^2+4m+1$$

is a square in $\mathbb{Q}$.

Proof. Observe that $f_r^3(x)$ has strictly more than two irreducible factors if and only if $q_i(f_r(x))$ is reducible for at least one $i \in \{1, 2\}$. Assume that $q_i(f_r(x))$ is reducible, let α be a root of $q_i(f_r(x))$, and observe that $f_r(\alpha) =: \beta$ is a root of $q_i(x)$. By the irreducibility of $q_i(x)$, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Because $q_i(f_r(x))$ is reducible, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] < 4$, which implies $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 1$, and thus $\alpha \in \mathbb{Q}(\beta)$. But α is a root of $f_r(x) - \beta = x^2 + r - \beta$, and so $\alpha \in \mathbb{Q}(\beta)$ is equivalent to $\beta - r$ being a square in $\mathbb{Q}(\beta)$. Letting β' be the other root of $q_i(x)$, we have

$$\begin{aligned} N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta - r) &= (\beta - r)(\beta' - r) = q_i(r) \\ &= \frac{8m^6 - 12m^4 \mp 4m^3 + 4m^2 \pm 4m + 1}{(4m^4 - 4m^2)^2} \end{aligned}$$

The multiplicativity of the norm map implies that the rightmost expression is a square in $\mathbb{Q}$. □

We now prove Theorem 1.6, which we restate here.

Theorem 2.14. *The only rational points on the curve* $y^2 = 8x^6 - 12x^4 - 4x^3 + 4x^2 + 4x + 1$ *are those with* $x \in \{-2, -1, 0, 1\}$.

Proof. We note first that the map $(x, y) \to (1/x, y/x^3)$ gives a birational transformation from the curve $y^2 = 8x^6 - 12x^4 - 4x^3 + 4x^2 + 4x + 1$ to the curve

$$C : y^2 = F(x) = x^6 + 4x^5 + 4x^4 - 4x^3 - 12x^2 + 8.$$

Therefore, it suffices to find all rational points on C. Next, we see that the polynomial $F(x)$ factors over a small extension of $\mathbb{Q}$. Fix an algebraic number β satisfying $\beta^3 - 8\beta^2 + 20\beta - 8 = 0$, and observe that $F(x)$ factors as

$$\Big(x^2+(-\beta+4)x+1/2(\beta^2-6\beta+8)\Big)\Big(x^4+\beta x^3+1/2(\beta^2-2\beta)x^2-4x-2\beta+4\Big).$$

Let $K = \mathbb{Q}(\beta)$, a number field of class number 1. Therefore, if (x, y) is a rational point on C, then there exist $y_1, y_2, \alpha \in K$ such that

$$\begin{aligned} \alpha y_1^2 &= F_1(x) = x^2 + (-\beta + 4)x + 1/2(\beta^2 - 6\beta + 8) \\ \alpha y_2^2 &= F_2(x) = x^4 + \beta x^3 + 1/2(\beta^2 - 2\beta)x^2 - 4x - 2\beta + 4 \end{aligned} \tag{14}$$

simultaneously; this follows from the fact that $F_1(x)$ and $F_2(x)$ lie in the same square-class in K. Moreover, we may assume that α is in the ring of integers $\mathcal{O}_K$ of K and that the ideal $\alpha\mathcal{O}_K$ is not divisible by the square of an ideal in $\mathcal{O}_K$. On the other hand, since the degrees of F_1 and F_2 are not both odd (see Example 9 and Theorem 11 of [20]), if $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ that divides α and is coprime to 2, then $\mathfrak{p}$ must divide the resultant $R = 36\beta^2 - 240\beta + 400$ of F_1 and F_2. Therefore, we may write

$$\alpha = (-1)^{e_0} \cdot 2^{e_1} \cdot \Big(\frac{\beta^2}{4} - \frac{3\beta}{2} + 2\Big)^{e_2} \cdot \Big(\frac{3\beta^2}{4} - 4\beta + 5\Big)^{e_3} \tag{15}$$

for some $e_i \in \{0, 1\}$ and $0 \le i \le 3$; here we use Sage to factor the fractional ideal generated by R and find generators -1 and $\frac{\beta^2}{4} - \frac{3\beta}{2} + 2$ of the unit group of K. In particular, we have deduced that if $(x, y) \in C(\mathbb{Q})$, then (x, y_2) is a K-point on

$$V_\alpha : \alpha y^2 = F_2(x),$$

for some $y_2 \in K$ and some α in (15). In particular, for such α it must be the case that $V_\alpha(K_v)$ is non-empty for every completion K_v/K. However, we check with MAGMA that only the curves V_α corresponding to $\alpha = 1$ and $\alpha = \frac{\beta^2}{4} - \frac{3\beta}{2} + 2$ have points everywhere locally. On the other hand, $V_\alpha(K)$ is non-empty for both of these choices of α. Therefore, there exist computable elliptic curves E_1 and E_2 (in Weierstrass form) together with birational maps $\phi_1 : E_1 \to V_1$ and $\phi_2 : E_2 \to V_{\frac{\beta^2}{4} - \frac{3\beta}{2} + 2}$ all defined over K. In particular, it suffices to compute the sets

$$S_i = \big\{P \in E_i(K) : x(\phi_i(P)) \in \mathbb{P}^1(\mathbb{Q})\big\}$$

for $i \in \{1,2\}$, to classify the integral points on C. However, $E_1(K)$ and $E_2(K)$ both have rank 2. In particular, $\mathrm{rank}(E_1(K))$ and $\mathrm{rank}(E_2(K))$ are both strictly less than $[K:\mathbb{Q}] = 3$. Therefore, S_1 and S_2 are finite sets, and we may use the elliptic Chabauty method to describe them; see, for instance, [5, §4.2]. Moreover, since both E_1 and E_2 are in Weierstrass form and we succeed in finding explicit generators for their Mordell-Weil groups, we may use an implementation of the elliptic Chabauty method in MAGMA to describe S_1 and S_2; see the file named *Elliptic Chabauty* at the website above for the relevant code. In particular, we deduce that

$$C(\mathbb{Q}) = \{\infty^+, \infty^-, (\pm 1, \pm 1), (-1/2, \pm 19/8)\},$$

from which Theorem 2.14 easily follows. □

Corollary 2.15. *Let $r = 1/c$ and $c = 4m^2(m^2-1)$ for $m \geq 2$. Then $f_r^3(x)$ has more than two irreducible factors if and only if $m = 2$.*

Proof. The sufficiency is clear from (13). To see that $m = 2$ is also necessary, assume that $f_r^3(x)$ has more than two irreducible factors. From Proposition 2.13, we have that m or $-m$ is the x-coordinate of an integral point on the curve $y^2 = 8x^6 - 12x^4 - 4x^3 + 4x^2 + 4x + 1$. It then follows from Theorem 2.14 that $\pm m \in \{-2, -1, 0, 1\}$. Since $m \geq 2$, the only possibility is $m = 2$. □

We have now assembled enough ingredients to prove Theorem 1.5.

Proof of Theorem 1.5. Part (a) is proven in Propositions 2.4 and 2.10. Part (b) follows from Proposition 2.12 and the remarks after (10).

The first assertion of part (c) is proven in Corollary 2.15. To prove the second assertion, let $m = 2$, let q_1 and q_2 be as in (12), and set $v_1(x) = x^2 - (1/2)x + 19/48$ and $v_2(x) = x^2 + (1/2)x + 19/48$, so that $q_2(f_r(x)) = v_1(x)v_2(x)$. We must show that $q_1(f_r^n(x))$ and $v_j(f_r^n(x))$ ($j \in \{1,2\}$) are irreducible for all $n \geq 1$. Because q_1, v_1, and v_2 have even degree, by Lemma 2.2 it suffices to prove $q_1(f_r^n(0))$ and $v_j(f_r^n(0))$ are not squares in $\mathbb{Q}$ for all $n \geq 1$.

We now search for primes p satisfying the condition (8), with q_1 and v_j replacing g_2. We reduce the sequence $q_1(f_r^n(0))$ modulo 239, and find that it only takes the non-square value 13 for $n \geq 7$. For n with $1 \leq n \leq 6$, one verifies directly that $q_1(f_r^n(0))$ is not a square. We reduce the sequence $v_1(f_r^n(0))$ modulo 239, and find that it only takes the non-square value 73 for $n \geq 7$. For n with $1 \leq n \leq 6$, one verifies directly that $v_1(f_r^n(0))$ is not a square. We reduce the sequence $v_2(f_r^n(0))$ modulo 41, and find that it only takes the non-square value 24 for $n \geq 7$. For n with $1 \leq n \leq 6$, one verifies directly that $v_2(f_r^n(0))$ is not a square. □

We close this section with a proof of one case of Theorem 1.2.

Proposition 2.16. *Let $r = 1/c$ and $c = 4m^2(m^2-1)$ for $m \geq 3$, and let q_1 and q_2 be as in (12). Suppose that $4m^2(m^2-1) \leq 10^9$. Then for all $n \geq 1$*

we have $q_1(f_r^n(x))$ and $q_2(f_r^n(x))$ irreducible. Hence, $f_r^n(x)$ is a product of two irreducible factors for all $n \geq 2$.

Proof. Observe that $4m^2(m^2-1) \leq 10^9$ if and only if $m \leq 125$. Because q_1 and q_2 have even degree, by Lemma 2.2 it suffices to prove $q_1(f_r^n(0))$ and $q_2(f_r^n(0))$ are non-squares in $\mathbb{Q}$ for all $n \geq 1$. We search for primes p satisfying the condition (8), with q_1 and q_2 replacing g_2.

For $q_1(f_r^n(0))$, we find that there exists a prime $p \leq 500$ (indeed, $p \leq 337$) with the desired property for all m with $3 \leq m \leq 125$. For $q_2(f_r^n(0))$, we also find that there exists a prime $p \leq 500$ with the desired property for all m with $3 \leq m \leq 125$.

For each such m and p, we take the finitely many terms of the sequence $(q_1(f_r^n(0)))_{n\geq 2}$ (resp. $(q_2(f_r^n(0)))_{n\geq 2}$) that have still not been proven non-square, and reduce modulo small primes until all have been proven non-square. □

3. The proof of cases (1)-(4) of Theorem 1.3

In the last section, we saw the primary importance of whether or not $p(f_r^n(0))$ is a square, for various polynomials $p(x)$. For the remainder of this article, we use similar ideas to study the irreducibility of $f_r(x)$ in the case where $f_r^2(x)$ is irreducible. However, we use a refinement of [10, Proposition 4.2], similar to [11, Theorem 2.3], that is more powerful; see Lemma 1.10 (restated as Lemma 3.2 below).

Recall from the introduction that $r = 1/c$, and that $f_r^n(0)$ is a rational number with denominator $c^{2^{n-1}}$. We define $a_n(c)$ to be the numerator of $f_r^n(0)$. Hence, $a_n(c)$ is described by the recurrence

$$a_1(c) = 1, \qquad a_n(c) = a_{n-1}(c)^2 + c^{2^{n-1}-1} \quad \text{for } n \geq 2. \tag{16}$$

To ease notation, we often suppress the dependence on c, and write a_1, a_2, etc. Recall also that we define

$$b_n := \frac{a_{n-1} + \sqrt{a_n}}{2} \in \overline{\mathbb{Q}}. \tag{17}$$

Proposition 3.1. *If $c < 0$, then a_n is not a square in $\mathbb{Q}$ for all $n \geq 2$.*

Proof. Let $r = 1/c$ and $f_r(x) = x^2 + r$, and consider the image of the interval $I = (-\sqrt{-r}, 0)$ under $f_r : \mathbb{R} \to \mathbb{R}$. We have $f_r(-\sqrt{-r}) = 0$ and $f_r(0) = r \in I$, so as f_r is a continuous function with no critical points in I, it follows that $f_r(I) \subset I$. As $f_r(0) = r \in I$, inductively, $f_r^n(0) \in I$ for all $n \geq 1$. Hence, $0 > f_r^n(0) = a_n/c^{2^n}$, and hence $a_n < 0$ for $n \geq 1$, proving that a_n is not a square in $\mathbb{Q}$. □

We now prove Lemma 1.10, which we restate here.

Lemma 3.2. *Suppose that $c \in \mathbb{Z} \setminus \{0\}$, $r = 1/c$, and f_r^2 is irreducible. Let $a_n = a_n(c)$ and b_n be defined as in* (16) *and* (17)*, respectively. If for every*

$n \geq 3$, b_n is not a square in $\mathbb{Q}$ (which holds in particular if a_n is not a square in $\mathbb{Q}$), then $f_r^n(x)$ is irreducible for all $n \geq 1$.

Proof. This proof is essentially the same as the proof of [11, Theorem 2.3], but for completeness we give the argument here. By hypothesis $f_r^2(x)$ is irreducible; assume inductively that $f_r^n(x)$ is irreducible for some $n \geq 2$. Let α be a root of $f_r^{n+1}(x)$, and observe that $f_r(\alpha) =: \beta$ is a root of $f_r^n(x)$. By our inductive assumption, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2^n$. Now $f_r^{n+1}(x)$ is irreducible if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^{n+1}$, which is equivalent to $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 2$. This holds if and only if $f_r(x) - \beta$ is irreducible over $\mathbb{Q}(\beta)$, i.e. $\beta - r$ is not a square in $\mathbb{Q}(\beta)$. Now factor $f_r^n(x)$ over $K_1 := \mathbb{Q}(\sqrt{-r})$. We have $f_r^n(x) = (f_r^{n-1}(x) - \sqrt{-r})(f_r^{n-1}(x) + \sqrt{-r})$, and because $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2^n$, we must have $[\mathbb{Q}(\beta) : K_1] = 2^{n-1}$, which implies that the minimal polynomial of β over K_1 is one of $f_r^{n-1}(x) \pm \sqrt{-r}$. It follows that $N_{\mathbb{Q}(\beta)/K_1}(\beta - r)$ is the product of $(\beta' - r)$, where β' varies over all roots of $f_r^{n-1}(x) \pm \sqrt{-r}$; this product is just $f_r^{n-1}(r) \pm \sqrt{-r}$ (here we use that $n \geq 2$, so the degree of $f_r^{n-1}(x)$ is even and we may replace the product of $(\beta' - r)$ with the product of $(r - \beta')$). To summarize, we have

$$N_{\mathbb{Q}(\beta)/K_1}(\beta - r) = f_r^{n-1}(r) \pm \sqrt{-r} = f_r^n(0) \pm \sqrt{-r}.$$

Suppose now that $f_r^{n+1}(x)$ is reducible, and hence $\beta - r$ is a square in $\mathbb{Q}(\beta)$. Because the norm map is multiplicative, this implies $N_{\mathbb{Q}(\beta)/K_1}(\beta - r)$ is a square in K_1, i.e. there exist $s_1, s_2 \in \mathbb{Q}$ with $(s_1 + s_2\sqrt{-r})^2 = f_r^n(0) \pm \sqrt{-r}$. Elementary calculations show this last equality implies $s_2 = \frac{1}{2s_1}$ and $s_1^2 - rs_2^2 = f_r^n(0)$, whence

$$s_1^2 = \frac{f_r^n(0) \pm \sqrt{f_r^{n+1}(0)}}{2} = \frac{a_n \pm \sqrt{a_{n+1}}}{2c^{2^{n-1}}}.$$

Now $n \geq 2$, and hence we have that one of $(a_n \pm \sqrt{a_{n+1}})/2$ is a square in $\mathbb{Q}$. If $c < 0$, then this is impossible by Proposition 3.1. Hence, suppose $c > 0$. As $a_{n+1} = a_n^2 + c^{2^n - 1} > a_n^2 > 0$, we have $(a_n - \sqrt{a_{n+1}})/2 < 0$, implying that $(a_n + \sqrt{a_{n+1}})/2$ is a square in $\mathbb{Q}$. But this is contrary to the hypotheses of the lemma, and we thus conclude that $f_r^{n+1}(x)$ is irreducible. □

Proposition 3.3. *Let $c \in \mathbb{Z} \setminus \{0, -1\}$. Then neither a_3 nor a_4 is a square in $\mathbb{Q}$.*

Proof. We have $a_3(c) = c^3 + c^2 + 2c + 1$, and so if $a_3(c) = y_0^2$ for $y_0 \in \mathbb{Q}$, then necessarily $y_0 \in \mathbb{Z}$, and (c, y_0) is an integer point on the elliptic curve $y^2 = x^3 + x^2 + 2x + 1$. This curve has conductor 92, and is curve 92.b2 in the LMFDB [16]. Besides the point at infinity, it has only the rational points $(0, \pm 1)$, but $c = 0$ is excluded by hypothesis.

We now address $a_4(c)$. As in the previous paragraph, if $a_4(c) = y_0^2$ for $y_0 \in \mathbb{Q}$, then (c, y_0) is an integer point on the hyperelliptic curve

$$C : y^2 = x^7 + x^6 + 2x^5 + 5x^4 + 6x^3 + 6x^2 + 4x + 1.$$

One easily checks that $x^7 + x^6 + 2x^5 + 5x^4 + 6x^3 + 6x^2 + 4x + 1$ has no repeated roots, and hence C has genus 3. Denote by J the Jacobian of C. A two-descent using MAGMA [2] shows that $J(\mathbb{Q})$ has rank zero, and hence consists only of torsion. We now use standard reduction techniques to determine all torsion in $J(\mathbb{Q})$ [9, Theorem C.1.4 and Section C.2]. We have a commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{F}_3) & \longrightarrow & J(\mathbb{F}_3) \end{array} \tag{18}$$

where the vertical maps are reduction modulo 3 and the horizontal maps are the Abel-Jacobi maps taking P to the divisor class of $(P - \infty)$. The latter are injective [9, Corollary A.6.3.3]. The discriminant of C is $2^{12} \cdot 23 \cdot 2551$, and it follows that C, and hence J [9, p. 164], has good reduction at all primes $p \notin \{2, 23, 2551\}$. Because $J(\mathbb{Q})$ is torsion, it follows that for any such prime p, the reduction map $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ is injective; see, for instance, the appendix of [15]. Thus, the right vertical map in (18) is injective, and it follows that the left vertical map is injective as well. But one verifies that $\#C(\mathbb{F}_3) = 4$, and hence $C(\mathbb{Q}) = \{\infty, (0, \pm 1), (-1, 0)\}$. Because we have excluded $c = 0, -1$, we arrive at the desired contradiction.

One may attempt the same argument with $a_5(c)$, but a 2-descent on the Jacobian J of the associated genus-7 hyperelliptic curve shows only that the rank of $J(\mathbb{Q})$ is at most 2. □

Proposition 3.4. *The sequence $(a_n)_{n \geq 1}$ is a rigid divisibility sequence. (See Definition 2.5).*

Proof. This is a straightforward application of [8, Lemma 2.5]. □

Proposition 3.5. *Suppose that $c+1$ is not a square in $\mathbb{Z}$. If c satisfies any of the congruences in Table 1, then a_n is not a square in $\mathbb{Q}$ for all $n \geq 2$.*

Proof. By Proposition 3.1, it suffices to consider $c > 0$. Because $a_2 = c + 1 > 0$ is non-square by assumption, there is a prime q with $v_q(c + 1)$ odd. Proposition 3.4 then implies that a_{2m} is non-square for all $m \geq 1$, so we need only check that a_n is non-square for odd $n \geq 2$. To do this, we let $f(x) = x^2 + 1/c$ and we take p to be a fixed prime with $p < 100$ and $p \nmid c$. Let $c_0 \in \{1, \ldots, p-1\}$ satisfy $(1/c) \equiv c_0 \bmod p$ and put $\bar{f} = x^2 + c_0 \in \mathbb{F}_p[x]$. Now $a_n = c^{2^{n-1}} f^n(0)$, and it follows that if $\bar{f}^n(0)$ is not a square in $\mathbb{F}_p$, then a_n is not a square in $\mathbb{Q}$. The sequence $(\bar{f}^n(0) \bmod p)_{n \geq 1}$ eventually lands in a repeating cycle. When this sequence is such that $\bar{f}^{2n+1}(0)$ is a non-square in $\mathbb{F}_p$ for all $n \geq 2$, then a_{2n+1} is a non-square in $\mathbb{Z}$ for all $n \geq 1$ (the $n = 1$ case is by Proposition 3.3). Most of the pairs of p, c listed in Table 1 yield such a result. For instance, when $p = 3$ and $c \equiv 1 \bmod p$, we have $\bar{f}^n(0) = 2$ for all $n \geq 2$. When $p = 5$ and $c \equiv 3 \bmod p$, the sequence $\bar{f}^n(0)$

$c \equiv 1, 2$	(mod 3)
$c \equiv 3$	(mod 4)
$c \equiv 2, 3$	(mod 5)
$c \equiv 1, 2, 5, 6$	(mod 7)
$c \equiv 1$	(mod 8)
$c \equiv 1, 3, 5, 7, 10$	(mod 11)
$c \equiv 3, 4, 5, 6, 8, 11$	(mod 13)
$c \equiv 6, 10, 14, 15$	(mod 17)
$c \equiv 1, 4, 9, 11, 12, 13, 15, 16, 18$	(mod 19)
$c \equiv 6, 10, 12, 18, 20, 22$	(mod 23)
$c \equiv 2, 12, 14, 17, 18, 27$	(mod 29)
$c \equiv 1, 10, 13, 16, 22, 27, 30$	(mod 31)
$c \equiv 6, 18, 23, 31, 32, 35$	(mod 37)
$c \equiv 7, 8, 11, 19, 25, 28, 35, 36$	(mod 41)
$c \equiv 1, 2, 4, 5, 9, 14, 15, 21, 27, 33, 37, 42$	(mod 43)
$c \equiv 6, 7, 9, 10, 24, 25, 28, 33, 46$	(mod 47)
$c \equiv 5, 18, 21, 23, 26, 30, 37, 40, 43, 45, 46, 47$	(mod 53)
$c \equiv 10, 14, 16, 29, 37, 47, 55, 57, 58$	(mod 59)
$c \equiv 2, 3, 11, 13, 15, 27, 30, 32, 34, 40, 45, 50$	(mod 61)
$c \equiv 10, 15, 20, 32, 33, 38, 41, 49, 51, 53, 55, 66$	(mod 67)
$c \equiv 4, 10, 49, 51, 53, 61, 70$	(mod 71)
$c \equiv 1, 3, 35, 43, 44, 50, 51, 71$	(mod 73)
$c \equiv 3, 12, 25, 32, 36, 58, 78$	(mod 79)
$c \equiv 15, 16, 19, 23, 25, 29, 31, 37, 41, 44, 51, 56, 59, 68, 71, 82$	(mod 83)
$c \equiv 13, 25, 49, 63$	(mod 89)
$c \equiv 3, 9, 21, 53, 59, 79, 89$	(mod 97)

TABLE 1. Congruences that ensure a_n is not a square for $n \geq 2$, provided that $c + 1$ is not a square.

is $2, 1, 3, 1, 3, \ldots$, and hence $\bar{f}^{2n+1}(0)$ is a non-square for all $n \geq 1$. The remaining pairs p, c in Table 1 satisfy the condition that both $\bar{f}^{3(n+1)+1}(0)$ and $\bar{f}^{3n+2}(0)$ are non-squares for $n \geq 1$ (the $n+1$ comes from the fact that a_4 is automatically a non-square by Proposition 3.3). Thus, a_{3n+1} and a_{3n+2} are non-squares in $\mathbb{Z}$ for all $n \geq 1$. But by Proposition 3.3 we have that

a_3 is not a square in $\mathbb{Z}$, and it follows from Proposition 3.4 that a_{3n} is a non-square in $\mathbb{Z}$ for all $n \geq 1$. An example is when $p = 7$ and $c \equiv 5 \bmod p$, for which the sequence $\bar{f}^n(0)$ is $3, 5, 0, 3, 5, 0, \ldots$. □

We now prove cases (1)-(4) of Theorem 1.3, which we restate here.

Theorem 3.6. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z} \setminus \{0, -1\}$, and let a_n and b_n be as in (16) and (17). Assume that c satisfies one of the following conditions:*

(1) *$-c \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $c < 0$;*
(2) *$-c, c+1 \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $c \equiv -1 \bmod p$ for a prime $p \equiv 3 \bmod 4$;*
(3) *$-c, c+1 \in \mathbb{Z} \setminus \mathbb{Z}^2$ and c satisfies one of the congruences in Proposition 3.5 (see Table 1);*
(4) *$-c \in \mathbb{Z} \setminus \mathbb{Z}^2$ and c is odd;*

In cases (1)-(3), a_n is not a square in $\mathbb{Q}$ for any $n \geq 2$, while in case (4), b_n is not a square for any $n \geq 2$. In all cases, $f_r^n(x)$ is irreducible for all $n \geq 1$.

Proof. Observe that conditions (1)-(4) each imply that $f_r^2(x)$ is irreducible, by Proposition 2.1 (note that $c = 4m^2(m^2-1)$ implies that $c+1 = (2m-1)^2$, and that this is impossible when c is odd). We now argue that in cases (1)-(3) a_n is not a square in $\mathbb{Q}$ for any $n \geq 2$ and in case (4), b_n is not a square for any $n \geq 2$. In all these cases, Lemma 1.10 proves that $f_r^n(x)$ is irreducible for all $n \geq 1$.

If we are in case (1), then the desired conclusion holds by Proposition 3.1.

Assume we are in case (2). Because we have already established case (1), it suffices to consider $c > 0$. Because $1/c \equiv -1 \bmod p$, we see that modulo p, the orbit of 0 under f_r is $0 \mapsto -1 \mapsto 0 \mapsto \cdots$. Moreover, -1 is not a square modulo p by assumption, and so a_{2n+1} is not a square for all $n \geq 3$. Because $a_2 = c + 1 \geq 2$ is assumed non-square, it must be divisible by some prime to odd multiplicity. From Proposition 3.4, it then follows that a_{2n} is not a square in $\mathbb{Q}$ for all $n \geq 1$.

In case (3) the desired conclusion holds by Proposition 3.5.

In case (4), if a_n is not a square in $\mathbb{Q}$ then b_n cannot be a square in $\mathbb{Q}$, and so we are done. If a_n is square in $\mathbb{Q}$, then from the recursion in (16) and the fact that any integer equals its square modulo 2, we have

$$\sqrt{a_n} \equiv a_n \equiv a_{n-1}^2 + c^{2^{n-1}-1} \equiv a_{n-1}^2 + 1 \equiv a_{n-1} + 1 \pmod 2.$$

Thus, modulo 2, we have $a_{n-1} + \sqrt{a_n} \equiv 2a_{n-1} + 1 \equiv 1$, whence

$$v_2\left(\frac{a_{n-1} + \sqrt{a_n}}{2}\right) = -1,$$

proving that $b_n = \frac{a_{n-1}+\sqrt{a_n}}{2}$ is not a square in $\mathbb{Q}$. □

4. Proof of cases (5) and (6) of Theorem 1.3

In this section we deduce consequences from the assumption that $a_n(c)$ or even $b_n(c)$ is a square. This will lead to a fairly small upper bound on n in terms of c. One application is the proof of cases (5) and (6) of Theorem 1.3. Another is the development of a fast algorithm for checking that all iterates of f are irreducible as soon as f^2 is, for all c up to a very large bound; this is done in the next section.

We denote the set of positive integers by $\mathbb{Z}^+$.

Lemma 4.1. *Let $c \in \mathbb{Z}^+$ and $n \geq 2$ such that $a_n(c)$ is a square. Then we can write $c = uv$ with coprime integers u and v such that*

(1) *if c is odd, then*
$$v^{2^{n-1}-1} - u^{2^{n-1}-1} = 2a_{n-1}(uv);$$
(2) *if c is even, then u is even and*
$$v^{2^{n-1}-1} - \tfrac{1}{4}u^{2^{n-1}-1} = a_{n-1}(uv).$$

If, in addition, $b_n(c) = (a_{n-1}(c) + \sqrt{a_n(c)})/2$ is a square (with the positive square root), then c is even and v is a square (and u and v are positive) or $-u$ is a square (and u and v are negative).

Proof. To simplify notation, we set $N := 2^{n-1} - 1$. By assumption, there is $s \in \mathbb{Z}^+$ such that
$$a_n(c) = c^N + a_{n-1}(c)^2 = s^2$$
and hence
$$c^N = \big(s + a_{n-1}(c)\big)\big(s - a_{n-1}(c)\big).$$
It follows easily by induction that $a_m(c) \equiv 1 \bmod c$ for all $m \geq 1$; in particular, $a_{n-1}(c)$ and s are coprime with c. Since $\gcd(a_{n-1}(c), s)$ divides a power of c, it follows that $a_{n-1}(c)$ and s are also coprime. So we can deduce that
$$\gcd\big(s + a_{n-1}(c), s - a_{n-1}(c)\big) \mid \gcd(2s, 2a_{n-1}(c)) = 2.$$
We set $t_+ := s + a_{n-1}(c)$ and $t_- := s - a_{n-1}(c)$.

(1) If c is odd, then the gcd on the left is odd (since it divides a power of c), so t_+ and t_- are coprime. Then $t_+t_- = c^N$ implies that $c = uv$ with u, v coprime and $t_+ = v^N$, $t_- = u^N$. The claim follows, since $t_+ - t_- = 2a_{n-1}(c)$.
(2) Now assume that c is even. Then $\gcd(s + a_{n-1}(c), s - a_{n-1}(c)) = 2$, since both entries have the same parity and their product is even. We can then write $c = uv$ with coprime u and v and u even such that either $t_+ = 2v^N$ and $t_- = \frac{1}{2}u^N$ or $t_+ = \frac{1}{2}u^N$ and $t_- = 2v^N$. In the first case, the claim again follows from $t_+ - t_- = 2a_{n-1}(c)$. In the second case, we obtain $(-v)^N - \frac{1}{4}(-u)^N = (-t_- + t_+)/2 = a_{n-1}((-u)(-v))$, so we get the claim upon changing the signs of u and v.

For the last claim, observe that

$$0 < \frac{a_{n-1}(c) + \sqrt{a_n(c)}}{2} = \frac{a_{n-1}(c) + s}{2} = \frac{t_+}{2}.$$

If c is odd, then t_+ is odd, and $t_+/2$ cannot be a square. Otherwise, $t_+/2$ is equal to either v^N or $(-u)^N/4$. Since N is odd, the claim follows. □

We set, for $c \geq 4$,

$$F(c) = \frac{1}{2}\Big(1 - \sqrt{1 - \frac{4}{c}}\Big) = \frac{2}{c}\Big(1 + \sqrt{1 - \frac{4}{c}}\Big)^{-1}.$$

From the first expression, it is clear that $F(c)$ decreases monotonically from $1/2$ to 0 as c grows from 4 to infinity. The second expression shows that for large c, $F(c)$ is close to $1/c$.

Lemma 4.2. *Let $c \geq 4$. Then the sequence $(\bar{a}_n(c))_{n\geq 1}$, where*

$$\bar{a}_n(c) = \frac{a_n(c)}{c^{2^{n-1}-1}},$$

satisfies $1 = \bar{a}_1(c) < \bar{a}_2(c) < \dots$ and $\lim_{n\to\infty} \bar{a}_n(c) = cF(c)$.

Proof. We have that $\bar{a}_{n+1}(c) = 1 + \bar{a}_n(c)^2/c$. When $1 \leq x < cF(c)$, then $cF(c) > 1 + x^2/c > x$, so that the sequence is strictly increasing and bounded by $cF(c)$. Since $cF(c)$ is the smallest fixed point ≥ 1 of $x \mapsto 1 + x^2/c$, it must be the limit. □

We make a couple of definitions.

Definition 4.3. *Let $c \geq 2$ be an integer. We set*

$$q(c) = \min\Big\{\frac{v}{u} : u, v \in \mathbb{Z}^+ \text{ coprime with } v > u \text{ and } c = uv\Big\}$$

and

$$\tilde{q}(c) = \min\Big\{\frac{v}{u} : u, v \in \mathbb{Z}^+ \text{ coprime with } v > u,\ c = uv,\ \text{and at least one of } u \text{ and } v \text{ is a square}\Big\}. \quad (19)$$

We note that $\tilde{q}(c) \geq q(c) > 1 + 1/\sqrt{c}$, since $v \geq u + 1$ in the set above, so $q(c) \geq 1 + 1/u$ for the minimizing u, and $u < \sqrt{c}$, since $u^2 < uv = c$.

We write "log" for the natural logarithm.

Definition 4.4. *Let $c \in \mathbb{Z}^+$ and $n \geq 2$. We define $\varepsilon(n, c)$ so that*

$$\log \frac{\sqrt{a_n(c)} + a_{n-1}(c)}{\sqrt{a_n(c)} - a_{n-1}(c)} = \frac{\varepsilon(n, c)}{\sqrt{c}}.$$

It follows from Lemma 4.2 and the properties of $F(c)$ that for fixed $c \geq 4$, $\varepsilon(n, c)$ increases with n with limit

$$\varepsilon(c) := \lim_{n\to\infty} \varepsilon(n, c) = \sqrt{c} \log \frac{1 + \sqrt{F(c)}}{1 - \sqrt{F(c)}}$$

and that $\varepsilon(c)$ decreases monotonically when c increases, with $\lim_{c\to\infty}\varepsilon(c) = 2$. In particular, we have that

$$\varepsilon(n,c) \le \varepsilon(c) \le \varepsilon(4) = 4\log(1+\sqrt{2}) \qquad \text{and} \qquad \frac{\varepsilon(n,c)}{\sqrt{c}} \le 2\log(1+\sqrt{2})\,.$$

Since $(e^x-1)/x$ is monotonically increasing for positive x, this implies that (for $c \ge 4$)

$$\exp\Big(\frac{\varepsilon(n,c)}{\sqrt{c}}\Big) \le 1 + \frac{1+\sqrt{2}}{\log(1+\sqrt{2})}\cdot\frac{\varepsilon(n,c)}{\sqrt{c}} \le 1 + \frac{4(1+\sqrt{2})}{\sqrt{c}}\,. \tag{20}$$

We note that

$$\frac{\varepsilon(c)}{\sqrt{c}\log q(c)} < 3.46 \qquad \text{for } c \ge 4, \tag{21}$$

$$\frac{\varepsilon(c)}{\sqrt{c}\log(1+1/\sqrt{c})} < 2.12 \qquad \text{for } c \ge 100, \tag{22}$$

$$\frac{\varepsilon(c)}{\sqrt{c}\log(1+1/\sqrt{c})} < 2.01 \qquad \text{for } c \ge 10400. \tag{23}$$

(To get (21), we use (22) and the explicit values of $q(c)$ for $c < 100$. The maximum is achieved for $c = 6$.) We will also need the elementary bound

$$\frac{1}{\log(1+1/\sqrt{c})} \le \sqrt{c} + \tfrac{1}{2}\,. \tag{24}$$

We can now deduce an upper bound on n such that $a_n(c)$ can be a square.

Proposition 4.5. *Let $c \ge 4$ be an integer and $n \ge 4$. If c is odd or*

$$n \ge 1 + \log_2\Big(1 + \frac{\varepsilon(n,c)}{\sqrt{c}\log q(c)} + \frac{\log 4}{\log q(c)}\Big),$$

then $a_n(c)$ is not a square. This is the case whenever

$$\sqrt{c} \le \frac{2^{n-1}-1}{\log 4} - 3.$$

If the weaker condition

$$n \ge 1 + \log_2\Big(1 + \frac{\varepsilon(n,c)}{\sqrt{c}\log \tilde{q}(c)} + \frac{\log 4}{\log \tilde{q}(c)}\Big)$$

holds, then $b_n(c)$ is not a square.

Proof. In the following, we write a_m for $a_m(c)$, since c is fixed. We assume that a_n is a square, so by Proposition 3.3 we have $n \ge 5$, and by Lemma 4.1 and its proof we can write $c = uv$ with coprime u, v (and u even when c is even) such that

$$(v^N, u^N) = (\sqrt{a_n} + a_{n-1}, \sqrt{a_n} - a_{n-1}) \qquad \text{if } c \text{ is odd;}$$

$$(v^N, u^N) = \big(\tfrac{1}{2}(\pm\sqrt{a_n} + a_{n-1}), 2(\pm\sqrt{a_n} - a_{n-1})\big) \qquad \text{if } c \text{ is even,}$$

where $N = 2^{n-1} - 1$.

First assume that c is odd. Then $v > u > 0$, and we obtain using (20)

$$\begin{aligned} 1 + \frac{N}{\sqrt{c}} &\leq \Big(1 + \frac{1}{\sqrt{c}}\Big)^N < \Big(\frac{v}{u}\Big)^N = \frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}} \\ &= \exp\Big(\frac{\varepsilon(n,c)}{\sqrt{c}}\Big) \leq 1 + \frac{4(1+\sqrt{2})}{\sqrt{c}}, \end{aligned}$$

which is a contradiction, since $N \geq 15$. So a_n cannot be a square.

Now assume that c is even. If $u, v > 0$ (this corresponds to the positive sign above), then

$$\Big(\frac{v}{u}\Big)^N = \frac{1}{4}\frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}.$$

If $u, v < 0$, then

$$\Big(\frac{u}{v}\Big)^N = 4\frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}.$$

In both cases, we have that $|\log(v/u)| \geq \log q(c)$. This gives

$$N \log q(c) \leq N\Big|\log \frac{v}{u}\Big| \leq \log 4 + \frac{\varepsilon(n,c)}{\sqrt{c}}, \tag{25}$$

which is equivalent to the inequality we wanted to show. If we assume that $b_n(c)$ is a square, then we have in addition that $|u|$ or $|v|$ is a square, hence the bound is valid for $\tilde{q}(c)$ in place of $q(c)$.

The bound on $\sqrt{c}$ follows from the first inequality, together with the estimates $\varepsilon(n,c) \leq \varepsilon(c)$, $q(c) > 1 + 1/\sqrt{c}$, and from (21) and (24). Note that $3.46/(\log 4) + 0.5 < 3$. □

This gives the following.

Corollary 4.6. *Let $c \geq 4$ be an integer and set $f(x) = x^2 + 1/c$.*

(1) *If c is odd, then all f^n are irreducible.*
(2) *If c is even and f^m is irreducible for*

$$m = 1 + \Big\lfloor \log_2\Big(1 + \frac{\log 4 + \varepsilon(c)/\sqrt{c}}{\log(1 + 1/\sqrt{c})}\Big)\Big\rfloor,$$

then all f^n are irreducible.
(3) *If c is even, f^2 is irreducible, and $a_p(c)$ is not a square for all prime numbers p with*

$$5 \leq p \leq 1 + \Big\lfloor \log_2\Big(1 + \frac{\log 4 + \varepsilon(c)/\sqrt{c}}{\log(1 + 1/\sqrt{c})}\Big)\Big\rfloor,$$

then all f^n are irreducible.
(4) *If f^2 is irreducible, $c > 50$, and $\tilde{q}(c) \geq 1.15c^{-1/30}$, then all f^n are irreducible.*

We note that case (1) gives another proof of case (4) of Theorem 1.3 for positive c.

For large c, the bound on n in case (2) of the corollary is close to $1 + \log_2(3 + (\sqrt{c} + \frac{1}{2})\log 4)$.

Proof. We recall that all f^n are irreducible when f^m is irreducible for some m and $a_n(c)$ or $b_n(c)$ is not a square for all $n > m$.

(1) If c is positive and odd, then f is irreducible and f^2 is also irreducible (since c is not of the form $4m^2(m^2-1)$, compare Proposition 2.1). By Proposition 3.3, $a_3(c)$ is never a square when $c > 0$. By Proposition 4.5, $a_n(c)$ is not a square for all $n \geq 4$, so the claim follows.

(2) If c is even and $n > m$, then

$$n \geq 1 + \log_2\Big(1 + \frac{\varepsilon(n,c)}{\sqrt{c}\log q(c)} + \frac{\log 4}{\log q(c)}\Big),$$

since $q(c) > 1 + 1/\sqrt{c}$ and $\varepsilon(n,c) < \varepsilon(c)$. So by Proposition 4.5, $a_n(c)$ is not a square, and the claim again follows.

(3) Let m be as in (2). Then $a_n(c)$ is not a square for $n > m$. For $3 \leq n \leq m$, $a_n(c)$ is not a square by assumption (or by Proposition 3.3 for $n = 3$) if n is prime. Otherwise, n is divisible by 4 or by an odd prime $p \leq m$; then it follows that $a_n(c)$ is not a square either, because $(a_n(c))$ is a rigid divisibility sequence by Proposition 3.4 and neither $a_4(c)$ (by Proposition 3.3 again) nor $a_p(c)$ is a square.

(4) First note that $2^{2/15}\varepsilon(c)^{1/15} < 1.15$ when $c > 50$. The stated inequality then implies that the bound on n in the second statement of Proposition 4.5 is < 5. □

We remark that recent work by one of the authors [21] shows that $a_5(c)$ is never a square when $c \neq 0$, which allow us to replace "5" by "7" in case (3) of the corollary and the condition in case (4) by "$\tilde{q}(c) \geq 1.034c^{-1/126}$".

We can use case (4) of Corollary 4.6 to deduce case (5) of Theorem 1.3; case (6) of this theorem follows by a similar argument.

Proof of cases (5) and (6) of Theorem 1.3. We can assume that $c > 50$ and c is even, since negative c are dealt with by case (1) and odd c are covered by case (4) of the theorem; the few positive even $c \leq 50$ can be checked individually by the methods of this section. Then the assumptions of case (5) imply that f_r^2 is irreducible by Proposition 2.1. Since when c is a square, c cannot be of the form $4m^2(m^2-1)$ either, this is also true in case (6).

We first consider case (5). Assume that $c = uv$ with u and v coprime and (say) $|u|$ a square. Then $|v| \geq \prod_{p:2\nmid v_p(c)} p^{v_p(c)}$ and $|u| \leq \prod_{p:2\mid v_p(c)} p^{v_p(c)}$, so that the inequality in the statement implies that $\tilde{q}(c) > 1.15c^{-1/30}$. The claim follows by invoking case (4) of Corollary 4.6.

We now consider case (6). If the claim is false, then there is $n \geq 5$ such that $a_n(c)$ is a square. By Lemma 4.1 it follows that we can write $c = uv$

with coprime u and v, with u even, such that $v^{2^{n-1}-1} - \frac{1}{4}u^{2^{n-1}-1} = a_{n-1}(c)$. Both u and v are now squares up to sign, so that we have

$$(v^{2^{n-1}-1}, \tfrac{1}{4}u^{2^{n-1}-1}) = \pm(x^2, y^2)$$

with coprime integers x and y, which implies that

$$x^2 - y^2 = \pm a_{n-1}(c). \tag{26}$$

Recall that $a_{n-1}(c) \equiv 1 \bmod c$. Since c is an even square, x is odd, and y is even, we obtain the congruence $1 \equiv \pm 1 \bmod 4$, which shows that we must have the positive sign in (26). Let $p \not\equiv 1 \bmod 4$ be a prime dividing c; since c is a square, $p^2 \mid c$. It follows that $x^2 \equiv y^2 + 1 \bmod p^2$, and since -1 is a non-square mod p^2, $p \mid x$ is impossible, so that we must have $p \mid y$. This in turn implies that $|u| \geq \prod_{p:p\not\equiv 1 \bmod 4} p^{v_p(c)}$ and $|v| \leq \prod_{p:p\equiv 1 \bmod 4} p^{v_p(c)}$. The inequality in the statement then implies that $u/v > 1.15c^{-1/30}$. This contradicts the second inequality in (25), so that we can conclude as in the proof of Proposition 4.5 that $a_n(c)$ cannot be a square, a contradiction. □

5. A fast algorithm and the proof of case (7) of Theorem 1.3

In this section, we always assume that $c \geq 4$ is an even integer. Fix $n \geq 5$ and assume that $a_n = a_n(c)$ is a square. Set $N = 2^{n-1} - 1$. By Lemma 4.1, we can write $c = uv$ with u and v coprime integers and u even such that

$$v^N - \frac{1}{4}u^N = a_{n-1}(c). \tag{27}$$

We now consider equation (27) as a relation between real numbers. First, note that for $c \geq 6$, we have (using Lemma 4.2 for the second inequality)

$$c^{2^{n-2}-1} + c^{2^{n-2}-2} \leq a_{n-1}(c) \leq c^{2^{n-2}} F(c) \leq c^{2^{n-2}-1} + 2c^{2^{n-2}-2},$$

so (27) implies that

$$v^N - \frac{1}{4}u^N = (uv)^M + \lambda(uv)^{M-1}$$

with $1 \leq \lambda \leq 2$, where $M = 2^{n-2} - 1$ (so that $N = 2M + 1$).

We now set $\theta := 2^{1/N}$, $x := \theta^{-1}u$ and $y := \theta v$; this gives

$$y^N - x^N = 2(xy)^M + 2\lambda(xy)^{M-1}.$$

Writing

$$z := \frac{(xy)^M}{x^{2M} + x^{2M-1}y + \ldots + y^{2M}} > 0$$

and recalling that $N = 2M + 1$, this leads to

$$y - x = 2\Big(1 + \frac{\lambda}{xy}\Big)z. \tag{28}$$

We want to estimate z. We expect that z is close to $1/N$, which is the value we obtain when $x = y$. Since $x^{2M-k}y^k + x^k y^{2M-k} \geq 2(xy)^M$, it follows that

$$z \leq \frac{1}{N}.$$

Since $xy = uv = c \geq 6$, we see that $y - x$ has to be small:

$$0 < y - x < \frac{3}{N}. \tag{29}$$

We get a lower bound on z as follows. Write $w_k := x^k + x^{k-1}y + \ldots + y^k$. We consider

$$\begin{aligned}\frac{xy}{(y-x)^2}(1 - Nz) &= \frac{xyw_{2M} - N(xy)^{M+1}}{(y-x)^2 w_{2M}} \\ &= \sum_{j=1}^{M} \frac{(xy)^{M+1-j}(y^j - x^j)^2}{(y-x)^2 w_{2M}} = \sum_{j=0}^{M-1} \frac{(xy)^{M-j} w_j^2}{w_{2M}}. \end{aligned} \tag{30}$$

We note that $(xy)^{M-j}w_j^2$ is given by

$$x^{M+j}y^{M-j} + 2x^{M+j-1}y^{M-j+1} + \ldots + (j+1)x^M y^M + \ldots + x^{M-j}y^{M+j},$$

which is at most $(j+1)w_{2M}$, and this gives that

$$\frac{xy}{(y-x)^2}(1 - Nz) \leq \sum_{j=0}^{M-1}(j+1) = \frac{M(M+1)}{2}.$$

Thus, using (29) for the second inequality,

$$z \geq \frac{1}{N} - \frac{M(M+1)}{2N}\,\frac{(y-x)^2}{xy} \geq \frac{1}{N} - \frac{9M(M+1)}{2N^3}\,\frac{1}{xy}.$$

Using this, $1 \leq \lambda \leq 2$, and $0 < \lambda/(xy) \leq 1/3$ in (28), we obtain

$$\left| y - x - \frac{2}{N} \right| \leq \frac{4}{N}\,\frac{1}{xy}.$$

Going back to our original integral variables u and v, this final bound is equivalent to

$$\left| \theta^2 v - u - \frac{2\theta}{N} \right| \leq \frac{4\theta}{N}\,\frac{1}{uv}. \tag{31}$$

We want to replace $1/(uv)$ on the right by $1/v^2$. The following lemma allows us to do that.

Lemma 5.1. *Let $c \geq 4$ be even. We assume that $a_n(c)$ is a square for some $n \geq 2$ and take u and v as in (27). Then, with $N = 2^{n-1} - 1$ and $\theta = 2^{1/N}$,*

$$(3 - 2\sqrt{2})^{1/N} < \frac{u}{\theta^2 v} < (3 + 2\sqrt{2})^{1/N}$$

and

$$(3 - 2\sqrt{2})^{1/N} < \frac{\theta^2 v}{u} < (3 + 2\sqrt{2})^{1/N}.$$

In particular,

$$\frac{1}{uv} < \frac{(3+2\sqrt{2})^{1/N}}{\theta^2}\,\frac{1}{v^2} \qquad \textit{and} \qquad c > \theta^2(3-2\sqrt{2})^{1/N}v^2.$$

Proof. Note that for $c \geq 4$, we have $a_{n-1}(c) < 2c^{2^{n-2}-1} \leq c^{N/2}$. Using this in (27) and dividing by v^N, this gives

$$\left|1 - \left(\frac{u}{\theta^2 v}\right)^N\right| < 2\sqrt{\left(\frac{u}{\theta^2 v}\right)^N}.$$

Set $\mu := (u/(\theta^2 v))^{N/2} > 0$. Rearranging, we obtain that

$$(\mu-1)^2 < 2 \qquad \text{and} \qquad (\mu+1)^2 > 2,$$

which gives

$$(\sqrt{2}-1)^2 < \mu^2 = \left(\frac{u}{\theta^2 v}\right)^N < (\sqrt{2}+1)^2,$$

from which the bounds in the statement are easily derived. □

Corollary 5.2. *Let $c \geq 6$ be even. We assume that $a_n(c)$ is a square for some $n \geq 2$ and take u and v as in* (27)*. Then, with $N = 2^{n-1}-1$ and $\theta = 2^{1/N}$,*

$$\left|\theta^2 v - u - \frac{2\theta}{N}\right| < \frac{4(3+2\sqrt{2})^{1/N}}{\theta N}\,\frac{1}{v^2}. \tag{32}$$

Proof. This follows immediately from (31) and Lemma 5.1. □

We can use the estimate (32) to compute a large lower bound on v (and therefore on c, by Lemma 5.1), in the following way. We set

$$\delta := \frac{4(3+2\sqrt{2})^{1/N}}{\theta N}.$$

Choose some $\varepsilon > 0$ (roughly of size B^{-2} when B is the desired lower bound for v). Let $\Lambda_\varepsilon \subset \mathbb{R}^2$ be the lattice generated by the vectors (ε, θ^2) and $(0,-1)$. Use lattice basis reduction to find the minimal squared euclidean distance $\sigma(\varepsilon)$ between a lattice point and $(0, 2\theta/N)$. Now, assuming that $(v,u) \in \mathbb{Z}^2$ satisfies $|\theta^2 v - u - 2\theta/N| < \delta/v^2$ (which follows by Corollary 5.2 for suitable (v,u) if $a_n(c)$ is a square), we see that

$$\sigma(\varepsilon) \leq (\varepsilon v)^2 + |\theta^2 v - u - 2\theta/N|^2 < \varepsilon^2 v^2 + \delta^2 v^{-4}.$$

If the polynomial $\varepsilon^2 X^3 - \sigma(\varepsilon)X^2 + \delta^2$ has two positive roots $0 < \xi_- \leq \xi_+$, then it follows that

$$|v| > \sqrt{\xi_+} \qquad \text{or} \qquad |v| < \sqrt{\xi_-}.$$

If we already know (from Proposition 4.5 or a previous application of the method) that $|v|$ must be larger than $\sqrt{\xi_-}$, then we get the new lower bound $|v| > \sqrt{\xi_+}$.

Since the covolume of Λ_ε is ε, we expect that $\sigma(\varepsilon) \approx \varepsilon$. If ε is sufficiently smaller than δ^2, then we get $\sqrt{\xi_-} \approx \sqrt{\delta}/\sqrt[4]{\varepsilon}$ and $\sqrt{\xi_+} \approx 1/\sqrt{\varepsilon}$.

This gives the following algorithm for checking that $a_n(c)$ can never be a square when $4 \le c \le \theta^2(3-2\sqrt{2})^{1/N}B^2$, for a large bound B.

(1) Use Proposition 4.5 and Lemma 5.1 to determine B_0 such that $|v| \ge B_0$ in any solution of $a_n(c) = \square$. For example, we can take

$$B_0 := \left\lceil \frac{(\sqrt{2}-1)^{1/N}}{\theta}\Big(\frac{N}{\log 4} - 3\Big)\right\rceil,$$

where $N = 2^{n-1}-1$ and $\theta = 2^{1/N}$ as usual.

(2) Repeat the following steps until $B_0 > B$.
   (a) Set $\varepsilon := \gamma\delta^2 B_0^{-4}$ with some $\gamma \approx 1$.
   (b) Compute $\sigma(\varepsilon)$ and ξ_-, ξ_+.
   (c) If $\xi_- \ge B_0^2$ (or does not exist), increase γ and go to Step (2a) .
   (d) Set $B_0 := \left\lceil \sqrt{\xi_+} \right\rceil$.

If the algorithm terminates, then this gives a proof that $|v| \ge B$ and therefore (by Lemma 5.1) $c > \theta^2(3-2\sqrt{2})^{1/N}B^2$ in any solution of $a_n(c) = \square$.

Since this uses real numbers, it does not yet give a method that can be implemented on a computer. We need to figure out which precision is necessary. The lattice basis reduction will essentially compute continued fraction approximations to θ^2 with numerators and denominators of size roughly B_0^2. The resulting reduced lattice basis will have lengths of order B_0^{-2}. The vector that is closest to $(0, 2\theta/N)$ will then have coefficients of order B_0^2 in terms of this lattice basis. We need the resulting minimal distance to be computed to an accuracy that is somewhat better than B_0^{-2}. This means that we need more than $6\log_2 B_0$ bits of precision. In practice, we work with an integral lattice obtained by scaling and rounding the basis given above, as follows. We assume that we have computed θ to $> 8\log_2 B_0$ bits of precision. In the following, $\lfloor\alpha\rceil$ denotes any integer a such that $|\alpha - a| \le 1$. We can then make the loop in Step 2 of the algorithm above precise in the following way.

(1) Set $\gamma := \delta^2$.
(2) Let $\Lambda \subset \mathbb{Z}^2$ be the lattice generated by $(\lfloor\gamma B_0^4\rceil, \lfloor\theta^2 B_0^8\rceil)$ and $(0, -B_0^8)$.
(3) Compute the four points of Λ closest to $(0, \lfloor 2\theta B_0^8/N\rceil)$; call (v_j, u_j) (for $j = 1, 2, 3, 4$) their coefficients with respect to the original basis of Λ and set
$(a_j, b_j) := (v_j\lfloor\gamma B_0^4\rceil, v_j\lfloor\theta^2 B_0^8\rceil - u_j B_0^8 - \lfloor 2\theta B_0^8/N\rceil)$.
(4) Set $\sigma := \min\limits_{j=1,2,3,4}\big(\max\{0, |a_j| - |v_j|\}^2 + \max\{0, |b_j| - |v_j| - 1\}^2\big)$.
(5) Set $h(x) = \lfloor\gamma B_0^4\rceil^2 x^6 - \sigma x^4 + \lceil\delta^2 B_0^{16}\rceil \in \mathbb{Z}[x]$.
(6) If $h(B_0) \ge 0$, then set $\gamma := 2\gamma$ and go to Step (2) .
(7) Set $B_0 := \max\{x \in \mathbb{Z}_{>B_0} : h(x) \le 0\} + 1$.

The main point here is that σ/B_0^{16} is a lower bound for $\sigma(\varepsilon)$, where $\varepsilon = \gamma/B_0^4$.

If we denote the successive values taken by B_0 by $B_0, B_1, B_2, \ldots$, then we expect that $B_{k+1} \approx B_k^2/\delta$. So to reach a given bound B, we will have to

make about $\log\log B$ passes through the loop. The computational cost of the last pass dominates all others; it is polynomial in $\log B$.

Example 5.3. We illustrate how the method works in the case $n = 5$. The initial lower bound for $|v|$ is $B_0 = 8$. The lattice Λ has basis $(336, 18401670)$ and $(0, -16777216)$; the target vector is $(0, 2342757)$. We compute $\sigma = 2373638400$ and find that $h(B_0) < 0$. We obtain the new lower bound $B_1 = 145$. In the same way, we find the successive lower bounds

$$\begin{aligned} B_2 &= 56956 \\ B_3 &= 1196488139 \\ B_4 &= 7319637204404186177 \\ B_5 &= 41458361126834155279142315082592517830 \end{aligned}$$

and so on.

This allows us to verify Conjecture 1.8 for all c up to a very large bound X in reasonable time. We just have to run our algorithm for all $n = p \geq 5$ prime and the corresponding bound B for $|v|$, as long as the initial bound B_0 (which grows roughly like 2^p) is less than B. Using a straight-forward implementation in MAGMA [2], it took less than 12 minutes (on the laptop of one of the authors) to prove the following, which by Proposition 2.1 amounts to a proof of case (7) of Theorem 1.3.

Proposition 5.4. *Let $c \in \mathbb{Z}^+$ and set $f(x) = x^2 + 1/c$. If $c \leq 10^{1000}$ and the second iterate f^2 is irreducible, then all iterates of f are irreducible.*

Proof. For $c \in \{1, 2, 3\}$, this can be checked by considering $a_n(c)$ modulo 3, 5, and 11, respectively. So we can assume that $c \geq 4$. By Corollary 4.6, it is enough to show that $a_p(c)$ is not a square for even c as in the statement and primes

$$5 \leq p \leq 1 + \left\lfloor \log_2\left(1 + \frac{\log 4 + \varepsilon(c)/\sqrt{c}}{\log(1 + 1/\sqrt{c})}\right)\right\rfloor \leq 1 + \left\lfloor \log_2\left(3.01 + \frac{\log 4}{\log(1 + 10^{-500})}\right)\right\rfloor,$$

and this last expression is 1662. (For $c \geq 10400$, we use the bound (23). For smaller c, the expression is much smaller than 1662.) This is a finite computation using the algorithm described above. □

We remark that in the course of executing the algorithm, it was never necessary to increase the initial value of γ.

We have now at last assembled all the ingredients required to prove Theorem 1.2.

Proof of Theorem 1.2. Let $f_r(x) = x^2 + r$ with $r = 1/c$, $c \in \mathbb{Z} \setminus \{0, -1\}$ and $|c| \leq 10^9$. If $f_r^2(x)$ is irreducible and c is negative or odd, then the claim follows from parts (1) and (4) of Theorem 1.3 (recall that $f_r(x)$ and so also $f_r^2(x)$ is reducible when $-c$ is a square). If $f_r^2(x)$ is irreducible and c is positive and even, Theorem 1.2 holds by Proposition 5.4.

If $f_r(x)$ or $f_r^2(x)$ is reducible, then the relevant cases of Theorem 1.2 follow from Theorem 1.5, Corollaries 2.9 and 2.11, and Proposition 2.16. □

6. Applications to the density of primes dividing orbits

In this section, we prove Theorem 1.12, which we restate here for the reader's convenience.

Theorem 6.1. *Let $c \in \mathbb{Z}$, let $r = 1/c$, suppose that $-c$ and $c+1$ are non-squares in $\mathbb{Q}$, and assume that Conjecture* 1.11 *holds for c, i.e. that $\frac{a_{n-1}+\sqrt{a_n}}{2}$ is not a square in $\mathbb{Q}$ for all $n \geq 3$. Then for any $t \in \mathbb{Q}$ we have $D(\{p \text{ prime} : p \text{ divides } O_{f_r}(t)\}) = 0$.*

Remark 6.2. Observe that the hypothesis that $\frac{a_{n-1}+\sqrt{a_n}}{2}$ not be a square for $n \geq 2$ is strictly weaker than a_n not being a square for $n \geq 2$; in the latter case the conclusion of Theorem 6.1 follows immediately from part (2) of [8, Theorem 1.1]. To prove Theorem 6.1, we must apply [8, Theorem 1.1] in a non-trivial way.

Remark 6.3. When the hypotheses of Theorem 6.1 are satisfied, we also obtain certain information on the action of $G_{\mathbb{Q}}$ on $T_f(0)$ (see p. 527 for the definition). The index-two subgroup $G_{\mathbb{Q}(\sqrt{-r})}$ acts on both $T_f(\sqrt{-r})$ and $T_f(-\sqrt{r})$. Both of these actions are transitive on each level of the tree, i.e., on $f_r^{-n}(\sqrt{-r})$ (resp. $f_r^{-n}(-\sqrt{-r})$), and the images of the maps $G_{\mathbb{Q}(\sqrt{-r})} \to \mathrm{Sym}(f_r^{-n}(\pm\sqrt{-r})) \cong S_{2^n}$ cannot lie in the alternating subgroup.

Proof. Let $K = \mathbb{Q}(\sqrt{-r})$, so that $f_r = (x+\sqrt{-r})(x-\sqrt{-r})$ over K. Let $g_1 = (x+\sqrt{-r})$ and $g_2 = (x-\sqrt{-r})$. To apply part (2) of [8, Theorem 1.1], we must show that for $i = 1, 2$, $g_i(f_r^{n-1}(0))$ is a non-square in K for all $n \geq 3$, and also that $-g_i(f_r(0))$ is a non-square in K. But $g_i(f_r^{n-1}(0)) = f_r^{n-1}(0) \pm \sqrt{-r}$. As in the final part of the proof of Lemma 3.2, $f_r^{n-1}(0) \pm \sqrt{-r}$ is a square in K if and only if $(f_r^{n-1}(0) \pm \sqrt{f_r^n(0)})/2$ is a square in $\mathbb{Q}$, which in turn is equivalent to $(a_{n-1} + \sqrt{a_n})/2$ being a square in $\mathbb{Q}$. But by assumption $(a_{n-1} + \sqrt{a_n})/2$ is not a square in $\mathbb{Q}$ for any $n \geq 3$. Moreover, $-g_i(f_r(0)) = -r \mp \sqrt{-r}$, which is a square in K if and only if $(-r \pm \sqrt{r^2+r})/2$ is a square in $\mathbb{Q}$. Because $c+1$ is not a square in $\mathbb{Q}$, it follows that r^2+r is not a square in $\mathbb{Q}$ either, proving that $-g_i(f_r(0))$ is not a square in $\mathbb{Q}$.

Therefore we may apply part (2) of [8, Theorem 1.1] twice to show

$$0 = \lim_{B \to \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq B\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) \leq B\}}, \tag{33}$$

where $N(\mathfrak{p})$ is the norm of the ideal $\mathfrak{p}$ and S is the set of primes $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K that divide $g_i(f_r^{n-1}(t))$ for at least one value of $i \in \{1, 2\}$ and at least one $n \geq 2$.

If we exclude the finite set of ramified primes, then the primes $\mathfrak{p}$ in $\mathcal{O}_K$ come in two flavors: those with norm p, where necessarily p splits in $\mathcal{O}_K$; and those with norm p^2, where necessarily p is inert in $\mathcal{O}_K$. Note that

$\#\{n \leq B : n = p^2 \text{ for some prime } p\}$ has asymptotic density zero relative to $\#\{n \leq B : n = p \text{ for some prime } p\}$, and so (33) is equivalent to

$$0 = \lim_{B\to\infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) = p \leq B\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) = p \leq B\}}. \tag{34}$$

Suppose $\mathfrak{p}$ in S, and say $\mathfrak{p} \mid g_i(f_r^{n-1}(t))$ for $n \geq 2$. Then

$$N(\mathfrak{p}) \mid N_{K/\mathbb{Q}}(g_i(f_r^{n-1}(t))) = f_r^n(t),$$

where $N_{K/\mathbb{Q}}$ is the usual field norm. Let $p = \mathbb{Z} \cap \mathcal{O}_K$ be the prime lying below $\mathfrak{p}$. Note that $N(\mathfrak{p}) = p$ if p splits in $\mathcal{O}_K$, i.e. if $-r$ is a quadratic residue modulo p, and $N(\mathfrak{p}) = p^2$ otherwise. But $0 \equiv f_r(f_r^{n-1}(t)) \equiv (f_r^{n-1}(t))^2 + r \bmod p$ and hence $-r$ must be a quadratic residue modulo p. Thus $N(\mathfrak{p}) = p$. It follows that the numerator of (34) is $2\#\{p : p \leq B \text{ and } p \text{ divides } O_f(t)\}$. Clearly the denominator is

$$2\#\{p : p \leq B \text{ and } -r \text{ is a quadratic residue modulo } p\}.$$

But by quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progressions, the latter is asymptotic to $\#\{p : p \leq B\}$. It follows that $D(\{p : p \text{ divides } O_f(t)\}) = 0$, as desired. □

References

[1] Benedetto, Robert; Ingram, Patrick; Jones, Rafe; Manes, Michelle; Silverman, Joseph H.; Tucker, Thomas J. Current trends and open problems in arithmetic dynamics. *Bull. Amer. Math. Soc.*, **56** (2019), no. 4, 611–685. MR4007163, Zbl 07124524, doi: 10.1090/bull/1665. 531

[2] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.*, **24** (1997), no. 3-4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125. 530, 545, 557

[3] Bridy, Andrew; Doyle, John R.; Ghioca, Draghos; Hsia, Liang-Chung; Tucker, Thomas, J. Finite index theorems for iterated Galois groups of unicritical polynomials. arXiv:1810.00990. 527

[4] Bridy, Andrew; Tucker, Thomas J. Finite index theorems for iterated Galois groups of cubic polynomials. *Math. Ann.* **373** (2019), no. 1-2, 37–72. MR3968866, Zbl 07051737, arXiv:1710.02257, doi: 10.1007/s00208-018-1670-3. 527

[5] Bruin, Nils. Chabauty methods using elliptic curves. *J. Reine Angew. Math.* **562** (2003), 27–49. MR2011330, Zbl 1135.11320, doi: 10.1515/crll.2003.076. 529, 542

[6] Fein, Burton; Schacher, Murray. Properties of iterates and composites of polynomials. *J. London Math. Soc.* (2), **54** (1996), no. 3, 489–497. MR1413893, Zbl 0865.12003, doi: 10.1112/jlms/54.3.489. 534

[7] Flynn, E. Victor; Wetherell, Joseph L. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, **100** (1999), no. 4, 519–533. MR1734798, Zbl 1029.11024, doi: 10.1007/s002290050215. 529

[8] Hamblen, Spencer; Jones, Rafe; Madhu, Kalyani. The density of primes in orbits of $z^d + c$. *Int. Math. Res. Not. IMRN* **2015** (2015), no. 7, 1924–1958. MR3335237, Zbl 1395.11128, arXiv:1303.6513, doi: 10.1093/imrn/rnt349. 526, 532, 545, 558

[9] Hindry, Marc; Silverman, Joseph H. Diophantine geometry. Graduate Texts in Mathematics, 201. *Springer-Verlag, New York*, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1 MR1745599, Zbl 0948.11023, doi: 10.1007/978-1-4612-1210-2. 545

[10] Jones, Rafe. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc.* (2) **78** (2008), no. 2, 523–544. MR2439638, Zbl 1193.37144, arXiv:math/0612415, doi: 10.1112/jlms/jdn034. 528, 532, 534, 535, 536, 543

[11] Jones, Rafe. An iterative construction of irreducible polynomials reducible modulo every prime. *J. Algebra*, **369** (2012), 114–128. MR2959789, Zbl 1302.11086, doi: 10.1016/j.jalgebra.2012.05.020. 528, 531, 543, 544

[12] Jones, Rafe. Galois representations from pre-image trees: an arboreal survey. *Actes de la Conférence "Théorie des Nombres et Applications"*, 107–136, Publ. Math. Besançon Algèbre Théorie Nr. (2013), *Presses Univ. Franche-Comté, Besançon.* MR3220023, Zbl 1307.11069, arXiv:1402.6018, 527

[13] Jones, Rafe; Levy, Alon. Eventually stable rational functions. *Int. J. Number Theory*, **13** (2017), no. 9, 2299–2318. MR3704363, Zbl 1391.37072, arXiv:1603.00673, doi: 10.1142/S1793042117501263. 527, 528, 530, 534

[14] Jones, Rafe; Manes, Michelle. Galois theory of quadratic rational functions. *Comment. Math. Helv.*, **89** (2014), no. 1, 173–213. MR3177912, Zbl 1316.11104, arXiv:1101.4339, doi: 10.4171/CMH/316. 533

[15] Katz, Nicholas M. Galois properties of torsion points on abelian varieties. *Invent. Math.*, **62** (1981), no. 3, 481-502. MR0604840, Zbl 0471.14023, doi: 10.1007/BF01394256. 545

[16] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 26 December 2019]. 535, 544

[17] Looper, Nicole. Dynamical Galois groups of trinomials and Odoni's conjecture. *Bull. Lond. Math. Soc.*, **51** (2019), no. 2, 278–292. MR3937588, Zbl 07094881, doi: 10.1112/blms.12227. 532

[18] Sookdeo, Vijay A. Integer points in backward orbits. *J. Number Theory*, **131** (2011), no. 7, 1229–1239. MR2782838, Zbl 1246.37102, arXiv:0808.2679, doi: 10.1016/j.jnt.2011.01.005. 527

[19] Stoll, Michael. Galois groups over $\mathbf{Q}$ of some iterated polynomials. *Arch. Math. (Basel)*, **59** (1992), no. 3, 239–244. MR1174401, Zbl 0758.11045, doi: 10.1007/BF01197321. 532

[20] Stoll, Michael. Rational Points on Curves. *Journal de théorie des nombres de Bordeaux*, **23** (2011), no. 1, 257-277. MR2780629, Zbl 1270.11030, arXiv:1008.1905, doi: 10.5802/jtnb.760. 541

[21] Stoll, Michael. An application of "Selmer group Chabauty" to arithmetic dynamics. arXiv:1912.05893. 552

[22] Swaminathan, Ashvin A. On arboreal Galois representations of rational functions. *J. Algebra*, **448** (2016), 104–126. MR3438308, Zbl 1387.11081, doi: 10.1016/j.jalgebra.2015.09.032. 533

(DeMark) School of Mathematics, University of Minnesota, 206 Church Street SE, Minneapolis, MN 55455, USA
demar180@umn.edu

(Hindes) Department of Mathematics, Texas State University, 601 University Drive, San Marcos, TX 78666, USA
wmh33@txstate.edu

(Jones) Department of Mathematics and Statistics, Carleton College, 1 North College St, Northfield, MN 55057, USA
rfjones@carleton.edu

(Misplon) Department of Mathematics and Statistics, Carleton College, 1 North College St, Northfield, MN 55057, USA
mzrmisplon@gmail.com

(Stoll) Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
Michael.Stoll@uni-bayreuth.de

(Stoneman) Department of Mathematics and Statistics, Carleton College, 1 North College St, Northfield, MN 55057, USA
mstoneman@google.com

This paper is available via http://nyjm.albany.edu/j/2020/26-25.html.