Math. Res. Lett. **16** (2009), *no.* 1, 87–101

UNIFORM BOUNDS ON PRE-IMAGES UNDER QUADRATIC DYNAMICAL SYSTEMS

Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve

Abstract. For any elements a, c of a number field K, let $\Gamma(a, c)$ denote the backwards orbit of a under the map $f_c : \mathbb{C} \to \mathbb{C}$ given by $f_c(x) = x^2 + c$. We prove an upper bound on the number of elements of $\Gamma(a, c)$ whose degree over K is at most some constant B. This bound depends only on a, $[K : \mathbb{Q}]$, and B, and is valid for all a outside an explicit finite set. We also show that, for any fixed $N \geq 4$ and any $a \in K$ outside a finite set, there are only finitely many pairs $(y_0, c) \in \mathbb{C}^2$ for which $[K(y_0, c) : K] < 2^{N-3}$ and the value of the N^{th} iterate of $f_c(x)$ at $x = y_0$ is a. Moreover, the bound 2^{N-3} in this result is optimal.

1. Introduction

1.1. Bounding the Number of Pre-Images. For an elliptic curve E over a number field K, the Mordell–Weil theorem implies finiteness of the group $E_{\text{tors}}(K)$ of K-rational torsion points on E. Merel [8], building on work of Mazur, Kamienny, and others, proved that $\#E_{\text{tors}}(K)$ is bounded by a function of $[K : \mathbb{Q}]$ (uniformly over all K and E). This implies the following uniform bound on torsion points over extensions of K of bounded degree (see [10, Cor. 6.64]):

Theorem 1.1. *Fix positive integers B and D. There is an integer $\lambda(B, D)$ such that for any number field K with $[K : \mathbb{Q}] \leq D$, and for any elliptic curve E/K, we have*

$$\#\{P \in E(\overline{K}) : [K(P) : K] \leq B \text{ and } [N]P = \mathcal{O} \text{ for some } N \geq 1\} \leq \lambda(B, D).$$

From a dynamical perspective, Theorem 1.1 controls the number of bounded-degree pre-images of the point $\mathcal{O}$ under the various maps $[N] : E \to E$. In this paper we prove an analogue of this result for maps $\mathbb{A}^1 \to \mathbb{A}^1$ defined by the iterates of a degree-2 polynomial $f \in \overline{\mathbb{Q}}[x]$. Write f^N for the N^{th} iterate of the polynomial f. A height argument similar to the one used by Mordell and Weil shows that, for any number field K, any quadratic $f \in K[x]$, and any $a \in K$ and $B > 0$, the set

$$\{x_0 \in \overline{K} : [K(x_0) : K] \leq B \text{ and } f^N(x_0) = a \text{ for some } N \geq 1\}$$

is finite. The sizes of these sets cannot be bounded in terms of K, a, and B: for any $N \geq 1$, put $f(x) := (x - b)^2 + b$ where $b := a - 2^{2^N}$, and note that $f^N(b + 2) = a$. However, we will prove such a bound on these sets in case f varies over the family of polynomials

$$f_c(x) := x^2 + c.$$

Received by the editors May 6, 2008.
2000 *Mathematics Subject Classification.* 14G05, 11G18 (primary); 37F10 (secondary).

Theorem 1.2. *Fix positive integers B and D. For all but finitely many values $a \in \overline{\mathbb{Q}}$, there is an integer $\kappa(B, D, a)$ with the following property: for any number field K such that $[K : \mathbb{Q}] \le D$ and $a \in K$, and for any $c \in K$, we have*

$$\#\left\{x_0 \in \overline{\mathbb{Q}} : [K(x_0) : K] \le B \text{ and } f_c^N(x_0) = a \text{ for some } N \ge 1\right\} \le \kappa(B, D, a).$$

Further, we give an explicit description of the excluded values a: they are the critical values of the polynomials $f_c^j(0) \in \mathbb{Z}[c]$, for $2 \le j \le 4 + \log_2(BD)$. It follows that the number of such values is less than $16BD$, and we will show that these values do not have the form α/m with α an algebraic integer and m an odd integer. We do not know whether the result would remain true if we did not exclude these finitely many values a. We prove that this is the case if $B = D = 1$ (see Theorem 4.1).

We do not assert any uniformity in a in Theorem 1.2, and in fact such uniformity cannot hold (since a can be chosen as $f_c^N(x_0)$ for fixed c, N, x_0). Also, our proof gives no explicit bound on the constant $\kappa(B, D, a)$, since we use a noneffective result due to Vojta (which generalizes the Mordell conjecture). Our proof of Theorem 1.2 carries over immediately to the family of polynomials $g_c(x) := x^k + c$ for any fixed $k \ge 2$; it would be interesting to analyze other families of polynomials.

In a different direction, if we fix N and vary c, the choices of B and D become crucial:

Theorem 1.3. *Let K be a number field and fix $a \in K$ and $N \ge 4$. There is a finite extension L of K for which infinitely many pairs $(y_0, c) \in \overline{K} \times \overline{K}$ satisfy $f_c^N(y_0) = a$ and $[L(y_0, c) : L] \le 2^{N-3}$. Conversely, if a is not a critical value of $f_c^j(0)$ for any $2 \le j \le N$, then only finitely many pairs $(y_0, c) \in \overline{K} \times \overline{K}$ satisfy $f_c^N(y_0) = a$ and $[K(y_0, c) : K] < 2^{N-3}$.*

In this result, some values a must be excluded: for $a = -1/4$, we will show that infinitely many pairs $(y_0, c) \in \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$ satisfy $f_c^N(y_0) = a$ and $[\mathbb{Q}(y_0, c) : \mathbb{Q}] \le 2^{N-4}$. Note that $a = -1/4$ is the unique critical value of $f_c^2(0) = c^2 + c = (c + 1/2)^2 - 1/4$. If we fix c (and N and a), then only finitely many $y_0 \in \overline{\mathbb{Q}}$ satisfy $f_c^N(y_0) = a$; thus the first part of Theorem 1.3 would remain true if we required the occurring values of c to be distinct. We will discuss Theorem 1.3 further in the next subsection after defining the analogues of modular curves for this problem.

A different dynamical analogue of Merel's result has been conjectured by Morton and Silverman [9]. For a field K and a non-constant endomorphism ϕ of a variety V over K, define the set of preperiodic points for ϕ to be

$$\mathrm{PrePer}(\phi) = \{P \in V(\overline{K}) : \phi^N(P) = \phi^M(P) \text{ for some } N > M \ge 0\}.$$

In case V is an elliptic curve and $\phi = [R]$ for some $R > 1$, the set $\mathrm{PrePer}(\phi)$ coincides with $V_{\mathrm{tors}}(\overline{K})$. This motivates the following special case of the Morton–Silverman conjecture:

Conjecture. *For any positive integer D, there is an integer $\mu(D)$ such that, for all number fields K of degree at most D and all $c \in K$, we have*

$$\#(\mathrm{PrePer}(f_c) \cap \mathbb{A}^1(K)) \le \mu(D).$$

See [10, §3.3] for a discussion of this conjecture.

1.2. Notation, Pre-Image Curves, and the Proof Strategy. Let K be a field whose characteristic is not 2. For $c \in K$, view $f_c(x) := x^2 + c$ as a mapping $\mathbb{A}^1_K \to \mathbb{A}^1_K$. We will study the dynamics of this mapping, by which we mean the behavior of points under repeated application of this map.

In order to prove results valid for all $c \in K$, it is convenient to first treat c as an indeterminate. This will be our convention unless otherwise specified.

Definition 1.4. Fix an element $a \in K$ and a positive integer N. We write $Y^{\text{pre}}(N, a)$ for the algebraic set in $\mathbb{A}^2$ defined by $f_c^N(x) - a$. If $Y^{\text{pre}}(N, a)$ is geometrically irreducible (that is, irreducible over $\overline{K}$), we define the N^{th} **pre-image curve** $X^{\text{pre}}(N, a)$ to be the completion of the normalization of $Y^{\text{pre}}(N, a)$.

Note that a point $(x_0, c_0) \in \mathbb{A}^2(\overline{K})$ lies on $Y^{\text{pre}}(N, a)$ if and only if x_0 is a pre-image of a under the N^{th} iterate of the map $x \mapsto f_{c_0}(x)$. For example, since the map $x \mapsto f_{a-a^2}(x)$ fixes $x = a$, the point $(a, a - a^2)$ lies on $Y^{\text{pre}}(N, a)$ for every $N \geq 1$. Likewise, since f_{-a^2-a-1} maps

$$a \longmapsto -a - 1 \longmapsto a,$$

for every $N \geq 1$ the points $(a, -a^2 - a - 1)$ and $(-a - 1, -a^2 - a - 1)$ lie on $Y^{\text{pre}}(2N, a)$ and $Y^{\text{pre}}(2N - 1, a)$, respectively.

The following result gives a sufficient condition for irreducibility of $Y^{\text{pre}}(N, a)$.

Theorem 1.5. *Suppose N is a positive integer and $a \in K$ is not a critical value of $f_c^j(0)$ for any $2 \leq j \leq N$. Then $Y^{\text{pre}}(N, a)$ is geometrically irreducible, and the genus of $X^{\text{pre}}(N, a)$ is $(N - 3)2^{N-2} + 1$.*

We now restate the main part of Theorem 1.3:

Corollary 1.6. *Let K be a number field and fix $N \geq 4$ and $a \in K$ that is not a critical value of $f_c^j(0)$ for any $2 \leq j \leq N$. Then only finitely many $P \in X^{\text{pre}}(N, a)(\overline{K})$ satisfy $[K(P) : K] < 2^{N-3}$, but there is a finite extension L of K for which infinitely many $P \in X^{\text{pre}}(N, a)(\overline{K})$ satisfy $[L(P) : L] = 2^{N-3}$.*

This result should be compared with a conjecture of Abramovich and Harris [1, p. 229], which says that a curve C over a number field K admits a rational map of degree at most d to a curve of genus 0 or 1 if and only if there is a finite extension L of K for which infinitely many $P \in C(\overline{\mathbb{Q}})$ satisfy $[L(P) : L] \leq d$. In light of the above result, this conjecture says that 2^{N-3} should be the minimal degree of any rational map from $X^{\text{pre}}(N, a)$ to a curve of genus 0 or 1. We will prove that this is in fact the case (one minimal degree map is the composition $\delta_4 \circ \delta_5 \circ \cdots \circ \delta_N$, whose image is the genus 1 curve $X^{\text{pre}}(3, a)$, where the maps δ_M are defined below). It should be noted, however, that Debarre and Fahlaoui have produced counterexamples to the Abramovich–Harris conjecture [3, 5.17]. Still, the conjecture is known to be true when d is small (due to Abramovich, Harris, Hindry, Silverman, and Vojta), and it is important to understand when it holds.

Define a degree-2 morphism $\delta \colon \mathbb{A}^2 \to \mathbb{A}^2$ by $\delta(x, c) = (x^2 + c, c)$. For $N > 1$, let δ_N be the restriction of δ to $Y^{\text{pre}}(N, a)$, so the image of δ_N is $Y^{\text{pre}}(N - 1, a)$. For any fixed $a \in K$, this gives a tower of algebraic sets and maps

$$\cdots \xrightarrow{\delta_{N+1}} Y^{\text{pre}}(N, a) \xrightarrow{\delta_N} Y^{\text{pre}}(N - 1, a) \xrightarrow{\delta_{N-1}} \cdots \xrightarrow{\delta_2} Y^{\text{pre}}(1, a)\,.$$

When $Y^{\mathrm{pre}}(N,a)$ and $Y^{\mathrm{pre}}(N-1,a)$ are geometrically irreducible, δ_N induces a degree-2 morphism $\delta_N\colon X^{\mathrm{pre}}(N,a) \to X^{\mathrm{pre}}(N-1,a)$.

Our strategy for proving Theorem 1.2 in case $B = D = 1$ is as follows: if $a \in \mathbb{Q}$ is not a critical value of $f_c^j(0)$ for any $j \in \{2,3,4\}$, then Theorem 1.5 implies that $X^{\mathrm{pre}}(4,a)$ is a geometrically irreducible curve of genus 5. By the Mordell conjecture (Faltings' theorem [4]), $X^{\mathrm{pre}}(4,a)(\mathbb{Q})$ is finite. An argument involving heights shows that any point in $\mathbb{A}^2(\mathbb{Q})$ has a total of finitely many pre-images in $\mathbb{A}^2(\mathbb{Q})$ under the various iterates of δ. Thus the union of all $Y^{\mathrm{pre}}(N,a)(\mathbb{Q})$ with $N \geq 4$ is finite. To deduce Theorem 1.2 in case $B = D = 1$, note that for each $N < 4$ the number of points in $Y^{\mathrm{pre}}(N,a)(\overline{\mathbb{Q}})$ having fixed values of a and c is at most 2^N, and in particular is bounded independently of c. The proof of Theorem 1.2 for other values of B and D follows the same strategy, but instead of Faltings' theorem we use a consequence of Vojta's inequality on arithmetic discriminants [14]; this requires some additional arguments adapting Vojta's result to our situation.

We remark that the algebraic sets $Y^{\mathrm{pre}}(N,0)$ have arisen previously in the context of the p-adic Mandelbrot set [6]. Also the sets $Y^{\mathrm{pre}}(2,a)$ occur implicitly in the study of uniform lower bounds on canonical heights of morphisms [5]; we will discuss the connection between such bounds and our results in Remark 4.9.

The remainder of the paper is organized as follows. In §2 we give a criterion for nonsingularity of $Y^{\mathrm{pre}}(N,a)$ and prove that nonsingularity implies irreducibility. In §3, in case $Y^{\mathrm{pre}}(N,a)$ is nonsingular, we compute the genus of $X^{\mathrm{pre}}(N,a)$, as well as the minimal degree of any rational map from $X^{\mathrm{pre}}(N,a)$ to a curve of genus 0 or 1. We then prove our arithmetic results in §4.

2. Smoothness and Irreducibility

In this section we determine when $Y^{\mathrm{pre}}(N,a)$ is nonsingular, and we show that $Y^{\mathrm{pre}}(N,a)$ is irreducible whenever it is nonsingular. Throughout this section, K is an algebraically closed field whose characteristic is not 2.

Proposition 2.1. *Fix a positive integer N. For $a \in K$, the following assertions are equivalent:*

(a) *$Y^{\mathrm{pre}}(N,a)$ is nonsingular.*
(b) *$Y^{\mathrm{pre}}(M,a)$ is nonsingular for $1 \leq M \leq N$.*
(c) *There do not exist an integer j with $2 \leq j \leq N$ and an element $c_0 \in K$ such that*

$$f_{c_0}^j(0) = a \quad \textit{and} \quad \frac{\partial f_c^j(0)}{\partial c}\Big|_{c=c_0} = 0.$$

Remark 2.2. Condition (c) says that a is not a critical value of $f_c^j(0)$ for any $2 \leq j \leq N$.

Proof. It suffices to show that (a) and (c) are equivalent, since if (c) holds for some N then it automatically holds for every smaller N. In order to prove equivalence of (a) and (c), we must describe the singular points on $Y^{\mathrm{pre}}(N,a)$. A point $(x_0,c_0) \in \mathbb{A}^2(K)$ is a singular point on $Y^{\mathrm{pre}}(N,a)$ if and only if the following three equations are satisfied:

$$f_{c_0}^N(x_0) = a \tag{1}$$

$$\frac{\partial f_{c_0}^N(x)}{\partial x}\Big|_{x=x_0} = 0 \tag{2}$$

$$\frac{\partial f_c^N(x_0)}{\partial c}\Big|_{c=c_0} = 0. \tag{3}$$

By repeatedly applying the chain rule (and using that $f'_{c_0}(x) = 2x$), we find

$$\begin{aligned}\frac{\partial f_{c_0}^N(x)}{\partial x}\Big|_{x=x_0} &= f'_{c_0}\left(f_{c_0}^{N-1}(x_0)\right)\cdot f'_{c_0}\left(f_{c_0}^{N-2}(x_0)\right)\cdot\dots\cdot f'_{c_0}\left(f_{c_0}(x_0)\right)\cdot f'_{c_0}\left(x_0\right)\\ &= 2^N\prod_{i=0}^{N-1} f_{c_0}^i(x_0).\end{aligned}$$

Thus, equation (2) is equivalent to the existence of an integer i with $0 \le i \le N-1$ such that $f_{c_0}^i(x_0) = 0$. For any such i, we have

$$\begin{aligned}\frac{\partial f_c^N(x_0)}{\partial c}\Big|_{c=c_0} &= \frac{\partial\left(f_c^{N-i}\left(f_c^i(x_0)\right)\right)}{\partial c}\Big|_{c=c_0}\\ &= \frac{\partial f_{c_0}^{N-i}(y)}{\partial y}\Big|_{y=0}\cdot\frac{\partial f_c^i(x_0)}{\partial c}\Big|_{c=c_0} + \frac{\partial f_c^{N-i}(0)}{\partial c}\Big|_{c=c_0}.\end{aligned}$$

Since $f_{c_0}^{N-i}(y) = f_{c_0}^{N-i-1}(y^2+c_0)$ is a polynomial in $K[y^2]$, its partial derivative with respect to y has zero constant term, so

$$\frac{\partial f_c^N(x_0)}{\partial c}\Big|_{c=c_0} = \frac{\partial f_c^{N-i}(0)}{\partial c}\Big|_{c=c_0}.$$

If $i = N-1$ then this common value is $\frac{\partial f_c(0)}{\partial c} = 1$, which in particular is nonzero. Thus, a point $(x_0, c_0) \in \mathbb{A}^2(K)$ is a singular point of $Y^{\mathrm{pre}}(N,a)$ if and only if all three of the following are satisfied:

$$f_{c_0}^N(x_0) = a \tag{4}$$

$$f_{c_0}^i(x_0) = 0 \text{ for some } i \text{ satisfying } 0 \le i \le N-2 \tag{5}$$

$$\frac{\partial f_c^{N-i}(0)}{\partial c}\Big|_{c=c_0} = 0. \tag{6}$$

When (5) holds, equation (4) is equivalent to

$$f_{c_0}^{N-i}(0) = a. \tag{7}$$

Conversely, if c_0 and i satisfy (6) and (7), then there exists $x_0 \in K$ satisfying (5). This implies the equivalence of (a) and (c) (with $j = N-i$). □

Remark 2.3. Assertion (c) of Proposition 2.1 gives a criterion for checking whether $Y^{\mathrm{pre}}(N,a)$ is smooth. In fact, it allows us to bound the number of values $a \in K$ for which smoothness fails. Namely, (c) associates to any such value $a \in K$ a pair (j, c_0), where $2 \le j \le N$ and c_0 is a root of $\frac{\partial f_c^j(0)}{\partial c}$. Since this last polynomial has degree $2^{j-1}-1$, there are at most that many possibilities for c_0 corresponding to a specified value j. Summing over $2 \le j \le N$, we find that $Y^{\mathrm{pre}}(N,a)$ is smooth for all but at most $2^N - N - 1$ values $a \in K$. We checked that equality holds if K has characteristic zero and $N \leq 6$, and we suspect equality holds in most situations. For $2 \leq N \leq 6$, there are precisely $2^{N-1} - 1$ values $a \in \overline{\mathbb{Q}}$ for which $Y^{\mathrm{pre}}(N, a)$ is singular but $Y^{\mathrm{pre}}(N-1, a)$ is nonsingular, and in each case these values a are conjugate over $\mathbb{Q}$.

Corollary 2.4. *The algebraic set $Y^{\mathrm{pre}}(1, a)$ is nonsingular for any $a \in K$. The algebraic set $Y^{\mathrm{pre}}(2, a)$ is nonsingular for any $a \in K \smallsetminus \{-1/4\}$.*

Proposition 2.5. *For $a \in K$ and $N \geq 1$, if $Y^{\mathrm{pre}}(N, a)$ is nonsingular then it is irreducible.*

Proof. First note that $Y^{\mathrm{pre}}(1, a)$ is irreducible for any $a \in K$, since the defining polynomial $x^2 + c - a \in K[x, c]$ is linear in c. Henceforth we assume $N > 1$. If $Y^{\mathrm{pre}}(N, a)$ is nonsingular, then Proposition 2.1 implies $Y^{\mathrm{pre}}(M, a)$ is also nonsingular for all $M < N$. We will show that, for $M - 1 < N$, if $Y^{\mathrm{pre}}(M-1, a)$ is irreducible, then $Y^{\mathrm{pre}}(M, a)$ is irreducible as well. By induction, this implies $Y^{\mathrm{pre}}(N, a)$ is irreducible.

Write the function field of $Y^{\mathrm{pre}}(M-1, a)$ as $K(y, c)$, where $f_c^{M-1}(y) = a$. The function fields of the components of $Y^{\mathrm{pre}}(M, a)$ are the extensions of $K(y, c)$ defined by the factors of $x^2 + c - y$ in $K(y, c)[x]$. Since each such factor is monic in x, and has coefficients in $K[y, c]$, the corresponding component contains a point (x_0, c_0) lying over any prescribed point (y_0, c_0) of $Y^{\mathrm{pre}}(M-1, a)$. Choose $c_0 \in K$ satisfying $f_{c_0}^{M-1}(c_0) = a$, so (c_0, c_0) is a point of $Y^{\mathrm{pre}}(M-1, a)$. Then $(0, c_0)$ is the unique point $P \in Y^{\mathrm{pre}}(M, a)$ for which $\delta_M(P) = (c_0, c_0)$. Thus $(0, c_0)$ is contained in each component of $Y^{\mathrm{pre}}(M, a)$, so since $Y^{\mathrm{pre}}(M, a)$ is nonsingular it must be irreducible. □

One can also prove this result geometrically: for the key step, note that δ_M is a finite morphism, so if $Y^{\mathrm{pre}}(M-1, a)$ is irreducible then δ_M maps each component of $Y^{\mathrm{pre}}(M, a)$ surjectively onto $Y^{\mathrm{pre}}(M-1, a)$.

Remark 2.6. In fact, $Y^{\mathrm{pre}}(N, a)$ is typically irreducible even when it is singular. For each $N \geq 1$, the previous two results imply irreducibility of $Y^{\mathrm{pre}}(N, a)$ for all values $a \in K$ not on a short list of potential exceptions. For $N \leq 4$, we checked the values a on these lists, and found that $Y^{\mathrm{pre}}(N, a)$ is irreducible for all $a \in K$ except $a = -1/4$. On the other hand, $Y^{\mathrm{pre}}(N, -1/4)$ has two components for each N with $2 \leq N \leq 6$. We suspect that larger values of N behave the same way.

3. Genus and gonality

In this section, for all values of N and a for which $Y^{\mathrm{pre}}(N, a)$ is nonsingular, we compute the genus and gonality of $X^{\mathrm{pre}}(N, a)$. Recall that the **gonality** is the minimum degree of a non-constant morphism $X^{\mathrm{pre}}(N, a) \to \mathbb{P}^1$. We also compute the minimum degree of a non-constant morphism from $X^{\mathrm{pre}}(N, a)$ to a curve of genus one.

Throughout this section, K is an algebraically closed field whose characteristic is not 2.

For a fixed value $a \in K$, we will compute the genus of $X^{\mathrm{pre}}(N, a)$ inductively, by applying the Riemann-Hurwitz formula to the map $\delta_N : X^{\mathrm{pre}}(N, a) \to X^{\mathrm{pre}}(N-1, a)$ defined in Section 1. We begin by computing the ramification of this map.

Lemma 3.1. *Pick $a \in K$ and $N \geq 2$ for which $Y^{\mathrm{pre}}(N,a)$ is nonsingular. Then $f_c^N(0) = a$ for precisely 2^{N-1} values $c \in K$, and the corresponding points $(0,c) \in Y^{\mathrm{pre}}(N,a)(K)$ comprise all points of $X^{\mathrm{pre}}(N,a)(K)$ at which $\delta_N\colon X^{\mathrm{pre}}(N,a) \to X^{\mathrm{pre}}(N-1,a)$ ramifies.*

Proof. Since $Y^{\mathrm{pre}}(N,a)$ is nonsingular, for each $1 \leq M \leq N$ it follows that $Y^{\mathrm{pre}}(M,a)$ is nonsingular (by Proposition 2.1) and hence irreducible (by Proposition 2.5).

First consider δ_N on $Y^{\mathrm{pre}}(N,a)$, which is defined by $\delta_N(x,c) = (x^2+c,c)$. The points with fewer than two pre-images are the images of points with $x = 0$, so δ_N ramifies at precisely the points $(0,c)$ on $Y^{\mathrm{pre}}(N,a)$. For $c \in K$, the point $(0,c) \in \mathbb{A}^2(K)$ lies on $Y^{\mathrm{pre}}(N,a)$ if and only if $f_c^N(0) = a$. Note that $f_c^N(0) - a$ is a polynomial in $K[c]$ of degree 2^{N-1}. If $c_0 \in K$ is a repeated root of $f_c^N(0) - a$, then

$$f_{c_0}^N(0) = a \quad \text{and} \quad \frac{\partial f_c^N(0)}{\partial c}\Big|_{c=c_0} = 0,$$

contradicting our nonsingularity hypothesis (by Proposition 2.1). Thus $f_c^N(0) = a$ for precisely 2^{N-1} values $a \in K$, and the corresponding points $(0,c) \in Y^{\mathrm{pre}}(N,a)(K)$ comprise all points of $Y^{\mathrm{pre}}(N,a)(K)$ at which δ_N ramifies.

It remains to show that δ_N is unramified at the 'cusps' $X^{\mathrm{pre}}(N,a) \setminus Y^{\mathrm{pre}}(N,a)$. Write the function field of $X^{\mathrm{pre}}(M,a)$ as $K(x_M,c)$ where $x_M^2 + c = x_{M-1}$ for $M > 1$ and $x_1^2 + c = a$. At the infinite place P_1 of $K(x_1,c)$, the functions x_1 and c have poles of orders 1 and 2. Inductively, assume x_M and c have poles of orders 1 and 2 at a place P of $K(x_M,c)$ which lies over P_1. Then $y := x_{M+1}/x_M$ satisfies $y^2 = (x_M - c)/x_M^2$, and since the right side has a nonzero finite value at P, there are two possibilities for the value of y at P. Thus, Kummer's theorem [12, Thm. III.3.7] implies that P lies under two places of $K(x_{M+1},c)$, neither of which is ramified. □

Theorem 3.2 (Genus Formula)**.** *Let $a \in K$, and let $N \geq 1$ be an integer for which $Y^{\mathrm{pre}}(N,a)$ is nonsingular. Then $X^{\mathrm{pre}}(N,a)$ is irreducible and has genus $(N-3)2^{N-2}+1$.*

Proof. For each $M \leq N$, the algebraic set $Y^{\mathrm{pre}}(M,a)$ is nonsingular (by Proposition 2.1) and hence irreducible (by Proposition 2.5), so also $X^{\mathrm{pre}}(M,a)$ is irreducible. All that remains is to calculate its genus.

We proceed by induction on N. Let $g(N)$ denote the genus of $X^{\mathrm{pre}}(N,a)$. Since $Y^{\mathrm{pre}}(1,a)$ is defined by $x^2 + c = a$, it is isomorphic to the x-line, so $g(1) = 0$ as desired. Inductively, suppose $g(N-1) = (N-4)2^{N-3} + 1$ for some $N \geq 2$. We compute $g(N)$ by applying the Riemann-Hurwitz formula to the degree-2 morphism $\delta_N\colon X^{\mathrm{pre}}(N,a) \to X^{\mathrm{pre}}(N-1,a)$. Lemma 3.1 shows that δ_N ramifies at precisely 2^{N-1} points, so

$$\begin{aligned} 2g(N) - 2 &= 2\left[2g(N-1) - 2\right] + \sum_{\substack{\text{ramified points} \\ \text{of } X^{\mathrm{pre}}(N,a)}} 1 \\ &= 2\left[2g(N-1) - 2\right] + 2^{N-1}, \end{aligned}$$

whence

$$\begin{aligned} g(N) &= 2g(N-1) - 1 + 2^{N-2} \\ &= (N-4)2^{N-2} + 2 - 1 + 2^{N-2} \\ &= (N-3)2^{N-2} + 1. \end{aligned}$$

□

Example 3.3. For a general choice of $a \in K$, we saw above that $Y^{\mathrm{pre}}(N, a)$ is irreducible and nonsingular. Passing to the completed curves, the generic picture looks like

$$\begin{array}{ccccccccc} \cdots \xrightarrow{2-1} & X^{\mathrm{pre}}(4,a) & \xrightarrow{2-1} & X^{\mathrm{pre}}(3,a) & \xrightarrow{2-1} & X^{\mathrm{pre}}(2,a) & \xrightarrow{2-1} & X^{\mathrm{pre}}(1,a) \\ & g(4)=5 & & g(3)=1 & & g(2)=0 & & g(1)=0 \end{array}$$

The fact that $X^{\mathrm{pre}}(4, a)$ has genus larger than 1 will be of arithmetic value to us in the next section.

For later use, we also summarize the relevant behavior for small values of N and those values of a for which $Y^{\mathrm{pre}}(N, a)$ is singular. We used Magma [2] to compute the data in the following table.

$a \in \overline{\mathbb{Q}}$	Algebraic Set	Irreducible Components	Genus
$a \in A_2$	$Y^{\mathrm{pre}}(2, -1/4)$	2	$0, 0$
	$Y^{\mathrm{pre}}(3, -1/4)$	2	$0, 0$
	$Y^{\mathrm{pre}}(4, -1/4)$	2	$1, 1$
	$Y^{\mathrm{pre}}(5, -1/4)$	2	$5, 5$
$a \in A_3$	$Y^{\mathrm{pre}}(3, a)$	1	0
	$Y^{\mathrm{pre}}(4, a)$	1	3
$a \in A_4$	$Y^{\mathrm{pre}}(4, a)$	1	4

TABLE 3.4. We denote by A_N the set of values $a \in \overline{\mathbb{Q}}$ for which $Y^{\mathrm{pre}}(N, a)$ is singular but $Y^{\mathrm{pre}}(N-1, a)$ is nonsingular. These sets may be computed using the criterion in Proposition 2.1. For example, $A_2 = \{-1/4\}$. Also $\#A_3 = 3$ and $\#A_4 = 7$. The last column gives the genera of the irreducible components of the given algebraic set.

Remark 3.5. The case $a = -1/4$ is of special interest for various reasons. Here we note that $Y^{\mathrm{pre}}(4, -1/4)$ has infinitely many rational points (since each of its components is the affine part of a rank-one elliptic curve over $\mathbb{Q}$). By contrast, for any other value $a \in \mathbb{Q}$, the above results imply that $Y^{\mathrm{pre}}(4, a)$ is an irreducible curve of genus greater than one, and thus has only finitely many rational points by the Mordell conjecture (Faltings' theorem [4]).

We now compute the gonality of $X^{\mathrm{pre}}(N, a)$:

Theorem 3.6. *Let $a \in K$, and let $N \geq 2$ be an integer for which $Y^{\mathrm{pre}}(N, a)$ is nonsingular. Then the gonality of $X^{\mathrm{pre}}(N, a)$ is 2^{N-2}.*

Our proof uses Castelnuovo's bound on the genus of a curve on a split surface (see [7, 2.16] or [12, Thm. III.10.3]):

Theorem 3.7. *Let C_1, C_2, and C be smooth, projective, geometrically integral curves over K, and supose there is a generically injective map $\psi\colon C \to C_1 \times_K C_2$. Let g_i be the genus of C_i, let π_i denote projection from $C_1 \times_K C_2$ onto its i^{th} factor, and let n_i be the degree of the map $\pi_i \circ \psi\colon C \to C_i$. Then the genus g of C satisfies*

$$g \leq n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1).$$

Proof of Theorem 3.6. By Theorem 3.2, the curve $X^{\text{pre}}(2,a)$ has genus zero, so it is isomorphic to $\mathbb{P}^1$. The composition

$$\delta_N \circ \cdots \circ \delta_3 \colon X^{\text{pre}}(N,a) \to X^{\text{pre}}(2,a) \cong \mathbb{P}^1$$

has degree 2^{N-2}, so the gonality of $X^{\text{pre}}(N,a)$ is at most 2^{N-2}. We prove equality by induction on N. Since this is clear for $N = 2$, we may assume that $X^{\text{pre}}(N-1,a)$ has gonality 2^{N-3}. Let $\phi\colon X^{\text{pre}}(N,a) \to \mathbb{P}^1$ be a non-constant morphism of minimal degree. If ϕ factors through the map δ_N, then $\deg \phi$ is twice the gonality of $X^{\text{pre}}(N-1,a)$, as desired. So assume ϕ does not factor through δ_N. Since δ_N has degree 2, it follows that the map

$$(\delta_N, \phi)\colon X^{\text{pre}}(N,a) \to X^{\text{pre}}(N-1,a) \times \mathbb{P}^1$$

is generically injective, and now Castelnuovo's inequality implies that

$$\begin{aligned} g(N) &\leq 2g(N-1) + (2-1)(\deg \phi - 1) \\ (N-3)2^{N-2} + 1 &\leq 2\left((N-4)2^{N-3} + 1\right) + \deg \phi - 1 \\ 2^{N-2} &\leq \deg \phi. \end{aligned}$$

Thus the gonality of $X^{\text{pre}}(N,a)$ is $\deg \phi = 2^{N-2}$. □

Corollary 3.8. *Let $a \in K$, and let $N \geq 3$ be an integer for which $Y^{\text{pre}}(N,a)$ is nonsingular. Then 2^{N-3} is the minimal degree of any nonconstant morphism from $X^{\text{pre}}(N,a)$ to a genus one curve.*

Proof. Since the gonality of $X^{\text{pre}}(N,a)$ is 2^{N-2}, and any genus one curve admits a degree-2 map to $\mathbb{P}^1$, any nonconstant morphism from $X^{\text{pre}}(N,a)$ to a genus-1 curve has degree at least 2^{N-3}. Conversely, this degree occurs for the map

$$\delta_N \circ \cdots \circ \delta_4 \colon X^{\text{pre}}(N,a) \to X^{\text{pre}}(3,a)\,.$$ □

4. Arithmetic of pre-images

Let K be a number field. For $a, c \in K$, we are interested in the size of

$$\{x_0 \in K : f_c^N(x_0) = a \text{ for some } N \geq 1\},$$

the set of pre-images of a under iterates of f_c. These sets can be arbitrarily large if we allow a to vary (even if c is fixed). Indeed, if we choose $b \in K$ to be a non-preperiodic point for f_c, and put $a = f_c^N(b)$, then the above set contains (at least) the N elements $b, f_c(b), \ldots, f_c^{N-1}(b)$. In this section we show that the situation is different if we fix a and allow c to vary.

In particular, we prove Theorem 1.2. To illustrate the method, we begin by proving the following special case (in which no values a need to be excluded):

Theorem 4.1. *Let K be a number field and pick $a \in K$. There is an integer $\nu(K,a)$ such that any $c \in K$ satisfies*

$$\#\left\{x_0 \in K : f_c^N(x_0) = a \text{ for some } N \geq 1\right\} \leq \nu(K,a).$$

Proof. Suppose $M > 0$ is chosen so that $Y^{\text{pre}}(M,a)(K)$ is finite. For each $c \in K$, we must bound the union of the following two sets:

$$U_c := \{x_0 \in K : f_c^N(x_0) = a \text{ for some } N < M\}$$
$$V_c := \{x_0 \in K : f_c^N(x_0) = a \text{ for some } N \geq M\}.$$

For fixed c and N, the polynomial $f_c^N(z)$ has degree 2^N, so $\#U_c \leq \sum_{N=1}^{M-1} 2^N = 2^M - 2$. If V_c is nonempty, so $f_c^N(x_0) = a$ for some $N \geq M$ and $x_0 \in K$, then $(f_c^{N-M}(x_0), c) \in Y^{\text{pre}}(M,a)(K)$. Hence there are only finitely many $c \in K$ for which $\#V_c > 0$, and for each such c the following lemma shows that V_c is finite. Letting S be the maximum value of $\#V_c$, it follows that $\#(U_c \cup V_c) \leq 2^M - 2 + S$.

It remains to prove that $Y^{\text{pre}}(M,a)(K)$ is finite for some M. If $Y^{\text{pre}}(4,a)$ is nonsingular, then $X^{\text{pre}}(4,a)$ has genus 5 by Theorem 3.2. We apply the Mordell conjecture (Faltings' theorem) to conclude that $X^{\text{pre}}(4,a)(K)$ is finite. This implies that $Y^{\text{pre}}(4,a)(K)$ is finite, so we may take $M = 4$. If $Y^{\text{pre}}(4,a)$ is singular and $a \neq -1/4$, then (as noted in Table 3.4) $Y^{\text{pre}}(4,a)$ is geometrically irreducible of genus more than 1, so again Faltings' theorem implies $Y^{\text{pre}}(4,a)(K)$ is finite. Finally, if $a = -1/4$ then (again from Table 3.4) the set $Y^{\text{pre}}(5,a)$ has two geometrically irreducible components, both of genus 5, so again Faltings' theorem implies $Y^{\text{pre}}(5,a)(K)$ is finite. Thus, for each $a \in K$, we have exhibited an integer M for which $Y^{\text{pre}}(M,a)(K)$ is finite, and the proof is complete. □

Lemma 4.2. *Let a, c be elements of a number field K. For any integer B, the set*

$$\left\{x_0 \in \overline{\mathbb{Q}} : [K(x_0) : K] \leq B \text{ and } f_c^N(x_0) = a \text{ for some } N \geq 1\right\}$$

is finite.

Proof. We use standard properties of canonical heights of morphisms, which can be found for instance in [10, §3.4]. The canonical height function $\hat{h}$ associated to f_c satisfies the properties

$$\hat{h}(z) \geq 0$$
$$\hat{h}(f_c(z)) = 2\hat{h}(z)$$
$$\hat{h}(z) = h(z) + O(1)$$

for all $z \in \overline{\mathbb{Q}}$, where h is the absolute logarithmic Weil height and the implied constant depends only on c.

If $f_c^N(x_0) = a$ for some $N \geq 1$, then

$$h(x_0) = \hat{h}(x_0) + O(1) = 2^{-N}\hat{h}(a) + O(1) \leq \hat{h}(a) + O(1) = h(a) + O(1).$$

In particular, the set described in the lemma is a collection of algebraic numbers of bounded height and degree, and so is finite (for instance by [10, Thm. 3.7]). □

The proof of Theorem 1.2 follows the same strategy as that of Theorem 4.1, but instead of Faltings' theorem we use a consequence of a more powerful theorem due to Vojta. We need some notation to state this consequence.

If $\phi\colon C \to C'$ is a non-constant morphism of smooth projective curves with ramification divisor R_ϕ, define

$$\rho(\phi) = \frac{\deg R_\phi}{2 \deg \phi}.$$

Theorem 4.3 (Song–Tucker–Vojta). *If $\phi\colon C \to C'$ is a non-constant morphism of smooth projective curves defined over a number field K, then the set*

$$\Gamma(C, \phi) = \big\{ P \in C(\overline{\mathbb{Q}}) : [K(P) : K] < \rho(\phi) \text{ and } K(\phi(P)) = K(P) \big\}$$

is finite.

Vojta proved this result in case $C' = \mathbb{P}^1$ (see [14, Cor. 0.3] and [13, Thm. A]), as a consequence of a deep inequality on arithmetic discriminants. Song and Tucker [11, Prop. 2.3] generalized Vojta's proof to deduce Theorem 4.3 for arbitrary C'. Note that Theorem 4.3 implies the Mordell conjecture: if C has genus at least 2, then any non-constant morphism $\phi\colon C \to \mathbb{P}^1$ satisfies $\rho(\phi) > 1$, so the finite set $\Gamma(C, \phi)$ includes $C(K)$.

Remark 4.4. We advise the reader of some typographical errors in [11]. Specifically, the inequality $\geq$ in [11, Cor. 2.1] should be a strict inequality $>$, the displayed equality in [11, Rem. 2.4] should say $\deg R_f = (2g - 2) - (2g' - 2) \deg f$, and the inequality $>$ in the next line should be $<$.

We will apply Theorem 4.3 to composite maps of the form $\delta_M \circ \delta_{M+1} \circ \cdots \circ \delta_{M+J}$. First we give a consequence of Theorem 4.3 for arbitrary composite maps.

Lemma 4.5. *Let*

$$X_N \xrightarrow{\phi_N} X_{N-1} \xrightarrow{\phi_{N-1}} \cdots \xrightarrow{\phi_3} X_2 \xrightarrow{\phi_2} X_1 \xrightarrow{\phi_1} X_0$$

be a sequence of smooth projective curves defined over a number field K, equipped with non-constant K-morphisms $\phi_M\colon X_M \to X_{M-1}$ for each $1 \leq M \leq N$, and put

$$B_N := \min_{1 \leq M \leq N} 2^{N-M} \rho(\phi_M)$$
$$b_N := \min_{1 \leq M \leq N} \rho(\phi_M).$$

Then the set

$$\big\{ P \in X_N(\overline{\mathbb{Q}}) : [K(P) : K] < B_N \text{ and } [K(\phi_1 \circ \cdots \circ \phi_N(P)) : K] \geq b_N \big\} \tag{8}$$

is finite.

Proof. By Theorem 4.3, for each M with $1 \leq M \leq N$ the set

$$\Gamma(M) := \big\{ P \in X_M(\overline{\mathbb{Q}}) : [K(P) : K] < \rho(\phi_M) \text{ and } K(P) = K(\phi_M(P)) \big\}$$

is finite. For $1 \leq M \leq N$, define $\psi_M\colon X_N \to X_{N-M}$ by

$$\psi_M := \phi_{N-M+1} \circ \phi_{N-M+2} \circ \cdots \circ \phi_N,$$

and let ψ_0 be the identity on X_N. Since ψ_M is a finite morphism,

$$\Gamma := \bigcup_{M=0}^{N} \left\{P \in X_N(\overline{\mathbb{Q}}) : \psi_M(P) \in \Gamma(N-M)\right\}$$

is a finite union of finite sets, and so is finite. We will show that if $P \in X_N(\overline{\mathbb{Q}}) \smallsetminus \Gamma$ satisfies $[K(\psi_N(P)) : K] \geq b_N$ then $[K(P) : K] \geq B_N$, which proves that the set defined in (8) is contained in the finite set Γ.

Suppose $P \in X_N(\overline{\mathbb{Q}}) \smallsetminus \Gamma$ satisfies $[K(\psi_N(P)) : K] \geq b_N$. Then

$$K(\psi_N(P)) \subset K(\psi_{N-1}(P)) \subset \cdots \subset K(\psi_0(P)) = K(P).$$

If we choose j with $0 \leq j \leq N-1$ and $\rho(\phi_{N-j}) = b_N$, then

$$[K(\psi_j(P)) : K] \geq [K(\psi_N(P)) : K] \geq b_N = \rho(\phi_{N-j}).$$

Let $0 \leq J \leq N-1$ be the least integer such that

$$[K(\psi_J(P)) : K] \geq \rho(\phi_{N-J}).$$

We may assume $J \geq 1$, since otherwise we obtain the desired conclusion

$$[K(P) : K] = [K(\psi_0(P)) : K] \geq \rho(\phi_N) \geq B_N.$$

By minimality, for $0 \leq j < J$ we have

$$[K(\psi_j(P)) : K] < \rho(\phi_{N-j});$$

but $P \notin \Gamma$ implies $\psi_j(P) \notin \Gamma(N-j)$, so

$$K(\psi_j(P)) \neq K(\psi_{j+1}(P)),$$

and thus $[K(\psi_j(P)) : K(\psi_{j+1}(P))] \geq 2$. It follows that

$$\begin{aligned}[K(P) : K] &= \Big(\prod_{j=0}^{J-1} [K(\psi_j(P)) : K(\psi_{j+1}(P))]\Big)[K(\psi_J(P)) : K] \\ &\geq 2^J \rho(\phi_{N-J}) \geq B_N.\end{aligned}$$

This completes the proof that the finite set Γ contains the set defined in (8). □

We now prove Theorem 1.3.

Proof of Theorem 1.3. Since the algebraic set $Y^{\mathrm{pre}}(3,a)$ has a geometrically irreducible component of genus 0 or 1, there is a finite extension L of K for which $Y^{\mathrm{pre}}(3,a)(L)$ is infinite. Since the composite map $\psi := \delta_4 \circ \delta_5 \circ \cdots \circ \delta_N$ defines an endomorphism of $\mathbb{A}^2$ of degree 2^{N-3}, if $\psi(P) \in Y^{\mathrm{pre}}(3,a)(L)$ then $[L(P) : L] \leq 2^{N-3}$. But $\psi(P) \in Y^{\mathrm{pre}}(3,a)(\overline{\mathbb{Q}})$ if and only if $P \in Y^{\mathrm{pre}}(N,a)(\overline{\mathbb{Q}})$. This proves the first part of Theorem 1.3.

Now suppose a is not a critical value of $f_c^j(0)$ for any $2 \leq j \leq N$, so $Y^{\mathrm{pre}}(M,a)$ is nonsingular for $M \leq N$, whence $X^{\mathrm{pre}}(M,a)$ is defined. Consider the tower of smooth projective curves

$$X^{\mathrm{pre}}(N,a) \xrightarrow{\delta_N} X^{\mathrm{pre}}(N-1,a) \xrightarrow{\delta_{N-1}} \cdots \xrightarrow{\delta_2} X^{\mathrm{pre}}(1,a),$$

where $\delta_M : X^{\mathrm{pre}}(M,a) \to X^{\mathrm{pre}}(M-1,a)$ is the usual map. By Lemma 3.1, the degree of the ramification divisor of δ_M is 2^{M-1}, so $\rho(\delta_M) = 2^{M-3}$. If we apply

Lemma 4.5 to this tower of curves, we have (in the notation of that lemma) $B_N = 2^{N-3}$ and $b_N = 1/2$. Theorem 1.3 follows. □

Remark 4.6. By Remark 3.5, the set $Y^{\text{pre}}(4, -1/4)(\mathbb{Q})$ is infinite, so the above proof implies that $Y^{\text{pre}}(N, -1/4)(\overline{\mathbb{Q}})$ contains infinitely many points of degree at most 2^{N-4}. Thus, the critical value hypothesis in Theorem 1.3 cannot be removed.

The following refinement of Theorem 1.2 is our main result:

Theorem 4.7 (Uniform Boundedness for Pre-Images)**.** *Fix a positive integer B, and put $N = \lfloor 4 + \log_2(B) \rfloor$. For any $a \in \overline{\mathbb{Q}}$ such that $Y^{\text{pre}}(N, a)$ is nonsingular, there is an integer $\kappa(B, a)$ with the following property: for any $c \in \overline{\mathbb{Q}}$, we have*

$$\#\left\{x_0 \in \overline{\mathbb{Q}} : [\mathbb{Q}(a, c, x_0) : \mathbb{Q}(a)] \le B \text{ and } f_c^M(x_0) = a \text{ for some } M \ge 1\right\} \le \kappa(B, a).$$

Moreover, $Y^{\text{pre}}(N, a)$ is singular for fewer than $16B$ values $a \in \overline{\mathbb{Q}}$.

Proof. By Remark 2.3, there are at most $2^N - N - 1$ values $a \in \overline{\mathbb{Q}}$ for which $Y^{\text{pre}}(N, a)$ is singular, which implies the final statement.

Choose $a \in \overline{\mathbb{Q}}$ such that $Y^{\text{pre}}(N, a)$ is nonsingular. For any $c \in \overline{\mathbb{Q}}$, the set described in the theorem is contained in $U_c \cup V_c$, where

$$U_c := \{x_0 \in \overline{\mathbb{Q}} : f_c^M(x_0) = a \text{ for some } M < N\},$$

$$V_c := \{x_0 \in \overline{\mathbb{Q}} : [\mathbb{Q}(a, c, x_0) : \mathbb{Q}(a)] < 2^{N-3} \text{ and } f_c^M(x_0) = a \text{ for some } M \ge N\}.$$

By Theorem 1.3, there are only finitely many points $(y_0, c_0) \in Y^{\text{pre}}(N, a)(\overline{\mathbb{Q}})$ for which $[\mathbb{Q}(a, y_0, c_0) : \mathbb{Q}(a)] < 2^{N-3}$. For each such c_0, Lemma 4.2 implies V_{c_0} is finite; for any other c we have $\#V_c = 0$. Letting S be the maximum of $\#V_c$ over all $c \in \overline{\mathbb{Q}}$, it follows that S is an integer depending only on N and a. Since $f_c^M(z)$ has degree 2^M, we have $\#U_c < 2^N$, so $\#(U_c \cup V_c) < S + 2^N$. □

Theorem 4.7, as well as several other results in this paper, applies to values a for which a particular $Y^{\text{pre}}(N, a)$ is nonsingular. We now describe a large class of such values a.

Proposition 4.8. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let $a \in K$. Suppose a is integral with respect to some prime ideal of $\mathcal{O}_K$ lying over 2; in other words, $a = a_1/a_2$ with $a_1, a_2 \in \mathcal{O}_K$ and $a_2 \notin \mathfrak{p}$ for some $\mathfrak{p} \mid 2$. Then $Y^{\text{pre}}(N, a)$ is nonsingular for every $N \ge 1$.*

Proof. By Proposition 2.1, it suffices to show there do not exist an integer $2 \le j \le N$ and an element $c_0 \in \overline{\mathbb{Q}}$ for which

$$f_{c_0}^j(0) = a \quad \text{and} \quad \left.\frac{\partial f_c^j(0)}{\partial c}\right|_{c=c_0} = 0.$$

Suppose j and c_0 satisfy these conditions, and write $P(c) = f_c^j(0) - a \in K[c]$. Letting R be the localization of $\mathcal{O}_K$ at the prime ideal $\mathfrak{p}$, our hypothesis on a shows that P is a monic polynomial over R. Since $P(c_0) = 0$, the ring $R[c_0]$ is integral over R, and so contains a prime ideal $\mathfrak{q}$ lying above $\mathfrak{p}$.

Writing $P(c) = Q(c)^2 + c - a$ with $Q = f_c^{j-1}(0) \in \mathbb{Z}[c]$, we have $P'(c) = 2Q(c)Q'(c) + 1$. By assumption, c_0 is a double root of $P(c)$, and so

$$0 = P'(c_0) = 2Q(c_0)Q'(c_0) + 1.$$

Since $Q(c_0)Q'(c_0) \in R[c_0]$, we may reduce this equation modulo $\mathfrak{q}$ to obtain the contradiction

$$0 \equiv 1 \pmod{\mathfrak{q}}.$$

Thus $Y^{\text{pre}}(N, a)$ is nonsingular. □

In particular, this result applies to any algebraic integer a, or more generally to any ratio $a = \alpha/m$ with α an algebraic integer and m an odd integer. For such values a, we know the genus and gonality of $X^{\text{pre}}(N, a)$, and moreover we have uniform bounds on the pre-images of a under the various maps f_c.

Remark 4.9. Our results are related to the study of uniform lower bounds on the canonical height $\hat{h}$ associated to f_c, as c varies. A special case of a conjecture of Silverman [10, Conj. 4.98] asserts that, for every number field K, there exists a constant $\epsilon = \epsilon(K) > 0$ such that either $\hat{h}(\alpha) = 0$ or $\hat{h}(\alpha) \geq \epsilon \max(1, h(c))$ for each $\alpha, c \in K$. (This is a dynamical analogue of a conjecture of Lang's on heights of non-torsion rational points on elliptic curves.) If this conjecture were true, we could prove Theorem 4.1 without using Faltings' theorem, so long as we assume that a is not preperiodic for f_c. For such a and c, if $f_c^N(x_0) = a$ then x_0 is not preperiodic for f_c, so $\hat{h}(x_0) \neq 0$ and thus

$$2^N \epsilon \max(1, h(c)) \leq 2^N \hat{h}(x_0) = \hat{h}(a) \leq h(a) + h(c) + \log 2,$$

where the last inequality follows from decomposing the heights into sums of local heights. This bounds N in terms of K, $h(a)$, and ϵ; the rest of the proof is as before. Partial results in the direction of Silverman's conjecture (see [5]) imply an effective version of Theorem 1.2 if the bound κ is allowed to depend on the number of primes of K at which c is not integral (in addition to BD and a). Of course, this is much weaker than Theorem 1.2, in which κ does not depend on c.

In the other direction, since $X^{\text{pre}}(3, 0)$ is a rank-one elliptic curve over $\mathbb{Q}$, with unbounded real locus, there are infinitely many $(x_0, c) \in Y^{\text{pre}}(3, 0)(\mathbb{Q})$ with $|c| > 4$. For such (x_0, c) we have $f_c^4(x_0) = f_c(0) = c$, so [5, Lemmas 3 and 6] imply

$$\hat{h}(x_0) = 2^{-4}\hat{h}(c) \leq \frac{1}{16}h(c) + \frac{\log(5) - 2\log(2)}{16}.$$

Thus, if $\epsilon(\mathbb{Q})$ exists then it is at most $1/16$. A similar construction was given in [5, §5], using the points $(k, -k^2 - k + 1)$ on $Y^{\text{pre}}(2, -3k + 2)$ to deduce an upper bound of $1/8$; note that that construction exhibits an infinite family of integral points, whereas each curve $X^{\text{pre}}(2, a)$ has only finitely many such points (since it is a genus zero curve with two rational points at infinity).

Acknowledgements

This project began at the American Institute of Mathematics, during the workshop on "The Uniform Boundedness Conjecture in Arithmetic Dynamics". We thank AIM for the opportunity to enjoy its productive atmosphere. We also thank the workshop organizers and participants for contributing to this stimulating week. We especially thank the participants with whom we discussed this work: Jordan Ellenberg, Susan Goldstine, Bjorn Poonen, Joseph Silverman, Vijay Sookdeo, Michael Stoll, and Justin Sukiennek. The research of the third author was partially supported by a PDF grant from NSERC of Canada.

References

[1] D. Abramovich and J. Harris, *Abelian varieties and curves in* $W_d(C)$, Compositio Math. **78** (1991), no. 2, 227–238.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24(3-4)** (1997) 235–265.

[3] O. Debarre and R. Fahlaoui, *Abelian varieties in* $W_d^r(C)$ *and points of bounded degree on algebraic curves*, Compositio Math. **88** (1993), no. 3, 235–249.

[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[5] P. Ingram, *Lower bounds on the canonical height associated to the morphism* $\phi(z) = z^d + c$, Monatsh. Math. **to appear** ArXiv:0709.4154v3.

[6] R. Jones, *Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set*, Compos. Math. **143** (2007), no. 5, 1108–1126.

[7] E. Kani, *On Castelnuovo's equivalence defect*, J. Reine Angew. Math. **352** (1984) 24–70.

[8] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.

[9] P. Morton and J. H. Silverman, *Rational periodic points of rational functions*, Internat. Math. Res. Notices (1994), no. 2, 97–110.

[10] J. H. Silverman, The Arithmetic of Dynamical Systems, Vol. 241 of *Graduate Texts in Mathematics*, Springer-Verlag (2007).

[11] X. Song and T. J. Tucker, *Arithmetic discriminants and morphisms of curves*, Trans. Amer. Math. Soc. **353** (2001), no. 5, 1921–1936.

[12] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin (1993), ISBN 3-540-56489-6.

[13] P. Vojta, *Arithmetic discriminants and quadratic points on curves*, in Arithmetic algebraic geometry (Texel, 1989), Vol. 89 of *Progr. Math.*, 359–376, Birkhäuser Boston, Boston, MA (1991).

[14] ———, *A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing*, J. Amer. Math. Soc. **5** (1992), no. 4, 763–804.

Department of Mathematics and Statistics, McGill University, Montréal, QC H3A 2K6, CANADA
E-mail address: xander@math.mcgill.ca
URL: http://www.math.mcgill.ca/xander/

Department of Mathematics and Computer Science, Amherst College, Amherst, MA 01002, USA
E-mail address: bhutz@amherst.edu

Department of Pure Mathematics, University of Waterloo, Waterloo, ON N2L 3G1, CANADA
E-mail address: pingram@math.uwaterloo.ca

Department of Mathematics, College of the Holy Cross, Worcester, MA 01610, USA
E-mail address: rjones@holycross.edu
URL: http://math.holycross.edu/ rjones

Department of Mathematics, University of Hawaii, Honolulu, HI 96822, USA
E-mail address: mmanes@math.hawaii.edu

Department of Mathematics, University of Rochester, Rochester, NY 14627, USA
E-mail address: ttucker@math.rochester.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA
E-mail address: zieve@math.rutgers.edu
URL: http://www.math.rutgers.edu/∼zieve/