ACTA ARITHMETICA
181.1 (2017)

Galois groups of iterates of some unicritical polynomials

by

Michael R. Bush (Lexington, VA), Wade Hindes (New York, NY)
and Nicole R. Looper (Evanston, IL)

1. Introduction. Let K be a number field. For a polynomial $\varphi(x) \in K[x]$ of degree $d \geq 2$, let φ^n denote the nth iterate of φ. Consider the tree associated to the iterated preimages of 0 under φ, given by

$$T_\infty = \bigsqcup_{n \geq 0} \varphi^{-n}(0)$$

where $\varphi^0(0) = \{0\}$. Two vertices $\alpha \in \varphi^{-n}(0)$ and $\beta \in \varphi^{-(n+1)}(0)$ are connected by an edge if and only if $\varphi(\beta) = \alpha$. If we assume that $\varphi^n(x)$ is separable for all $n \geq 1$, then the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on T_∞ by graph automorphisms. When φ is unicritical and K contains a primitive dth root of unity, $\mathrm{Gal}(\overline{K}/K)$ in fact acts by cyclic permutations of the roots of each $\varphi(x) - \alpha$, where α is an element of T_∞. We thus obtain a representation

$$\rho : \mathrm{Gal}(\overline{K}/K) \to [C_d]^\infty$$

where C_d is a cyclic permutation group generated by a d-cycle, and $[C_d]^\infty$ denotes the infinite iterated wreath product of C_d ([11, Lemma 3.3] and [6, Lemma 2.1]). We denote its image by $G_K(\varphi)$.

Much work has been done concerning the structure and size of $G_K(\varphi)$ in the case of quadratic polynomials [7, 9, 22]. For example, if $\varphi(x) \in \mathbb{Z}[x]$ is quadratic and is not post-critically finite, then one expects that $G_{\mathbb{Q}}(\varphi) \leq [C_2]^\infty$ is a finite index subgroup [9, §3]. Moreover, such a statement is known under the *abc*-conjecture and an irreducibility condition [5, Prop. 6.1]. However, unconditional results are scarce [10, 22], and up to this point, there are no examples in degree greater than two. In this article, we generalize a technique of Jones [8, Theorem 1.2] to produce polynomials φ_p of prime degree $p \geq 3$ defined over $\mathbb{Q}(\zeta_p)$ for which $G_{\mathbb{Q}(\zeta_p)}(\varphi_p)$ has finite index in $[C_p]^\infty$.

2010 *Mathematics Subject Classification*: Primary 11R32, 37P15; Secondary 14G05.
Key words and phrases: Galois theory, arithmetic dynamics, rational points on curves.
Received 31 August 2016; revised 6 August 2017.
Published online 13 October 2017.

THEOREM 1.1. *Let p be an odd prime, let ζ_p be a primitive pth root of unity, and let*

$$\varphi_p(x) = (x-1)^p + (2-\zeta_p).$$

Then there exists an explicit constant $C(p)$, depending only on p, such that

$$\big[[C_p]^\infty : G_{\mathbb{Q}(\zeta_p)}(\varphi_p)\big] \le C(p).$$

Moreover, $G_{\mathbb{Q}(\zeta_p)}(\varphi_p) = [C_p]^\infty$ for $p = 3, 5, 7$.

The maps φ_p have several properties that are key to the proof of Theorem 1.1. Each $\varphi_p(x)$ is conjugate to the map $\widetilde{\varphi}_p(x) = x^p + (1-\zeta_p)$, which is studied in [6]. The Galois groups of $\varphi_p^n(x)$ are the same groups one obtains by taking preimages of -1 under $\widetilde{\varphi}_p^n$ instead of preimages of 0. This conjugation has the effect of making the root 0 of T_∞ be strictly preperiodic, a property that we exploit much as in [8]. Moreover, since the principal ideal $(1-\zeta_p)$ is the unique prime ideal of $\mathbb{Z}[\zeta_p]$ lying above the rational prime p (see [14, IV] for details), the polynomial $\varphi_p(x)$ is in fact Eisenstein at $(1-\zeta_p)$. One readily checks that iterates of Eisenstein polynomials are themselves Eisenstein, so $\varphi_p^n(x)$ is Eisenstein at $(1-\zeta_p)$ for all $n \ge 1$.

In addition, we study the family of quadratic polynomials

$$\psi_p(x) = (x-p)^2 + 2p - p^2$$

and prove a theorem concerning the primes p such that the resulting arboreal representation is surjective. We note that it follows from [8, proof of Theorem 1.1] that this family of polynomials induces arboreal representations with finite index in $[C_2]^\infty$; however, this theorem does not yield any bounds on the associated index.

THEOREM 1.2. *Let $p \ge 3$ be a prime and let $\psi_p(x) = (x-p)^2 + 2p - p^2$. Then $G_{\mathbb{Q}}(\psi_p) = [C_2]^\infty$ in any of the following cases:*

(1) $p \equiv 2 \pmod 3$,
(2) $p \equiv 3 \pmod 4$,
(3) $p \equiv 2 \pmod 5$,
(4) $p \equiv 3, 6 \pmod 7$,
(5) $p \equiv 2, 3, 5, 7, 10 \pmod{11}$,
(6) $p \equiv 2, 3, 7, 9, 11 \pmod{13}$.

Moreover, $G_{\mathbb{Q}}(\psi_p) = [C_2]^\infty$ for all primes $p < 5000$.

A crucial step in proving case (6), and a result of independent interest, is the following.

THEOREM 1.3. *For every $p \ge 3$,*

$$\mathrm{Gal}\big(\mathbb{Q}(\psi_p^{-3}(0))/\mathbb{Q}\big) \cong [C_2]^3$$

and ψ_p^n is irreducible over $\mathbb{Q}$ for all $n \ge 1$.

REMARK. Unlike Theorem 1.2, Theorem 1.3 assumes no congruence conditions on the prime. Furthermore, the fact that $\psi_p^n(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$ follows from [8, Proposition 4.6].

The proof of Theorem 1.3 involves a detailed analysis of the rational points on a certain algebraic curve of genus three. We accomplish this by using the method of Chabauty–Coleman and the Mordell–Weil sieve. Taken together, Theorems 1.2 and 1.3 provide evidence for the following conjecture.

CONJECTURE 1.4. *Let $p \geq 3$ be a prime and let $\psi_p(x) = (x-p)^2+2p-p^2$. Then $G_{\mathbb{Q}}(\psi_p) = [C_2]^\infty$.*

In addition to explicit techniques in the theory of rational points on curves, we make use of ideas developed in [6, 8], as well as the computer algebra systems `Magma` [3] and Sage [17].

2. Main arguments. In order to prove Theorem 1.1, we make use of a slight modification of a lemma found in [6]. Let $\sigma \in K[x]$, let $K_n(\sigma)$ be the splitting field of $\sigma^n(x)$ over K, and let $\mathrm{Gal}_K(\sigma^n) = \mathrm{Gal}(K_n(\sigma)/K)$. For $\sigma(x) = (x-\gamma)^d + c \in K[x]$, each $K_n(\sigma)$ is obtained from $K_{n-1}(\sigma)$ by adjoining the dth roots of $\alpha_i - c$ for all roots α_i of $\sigma^{n-1}(x)$. Writing $H_n := \mathrm{Gal}(K_n(\sigma)/K_{n-1}(\sigma))$, we then have an injection

$$H_n \hookrightarrow (\mathbb{Z}/d\mathbb{Z})^m$$

where m is the degree of $\sigma^{n-1}(x)$ and $n \geq 2$. This statement also holds when $n = 1$ provided the base field K contains a dth root of unity, and we will make this assumption from this point on. We say that H_n is *maximal* when the injection is an isomorphism.

LEMMA 2.1. *Let $d \geq 2$ be an integer, and let K be a field of characteristic not dividing d. Let $\sigma(x) = (x-\gamma)^d + c \in K[x]$. Suppose that $n \geq 2$ and $\sigma^{n-1}(x)$ is irreducible. Then H_n is maximal if and only if for all primes $p \mid d$, $\sigma^n(\gamma)$ is not a pth power in $K_{n-1}(\sigma)$.*

REMARK. The proof proceeds exactly as in [6], by noting that adjoining the roots of $(x-\gamma)^d + c - \alpha_i$ for α_i a root of σ^{n-1} yields the same extension of $K(\alpha_i)$ as adjoining the roots of $x^d + c - \alpha_i$.

Let $\mathrm{Orb}_\sigma(P) = \{\sigma^n(P)\}_{n\geq 0}$ denote the forward orbit of a point $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$ under σ. Moreover, for $\alpha \in \mathcal{O}_K$ and $\sigma \in \mathcal{O}_K[x]$, we say a prime divisor $\mathfrak{p}$ of $\sigma^n(\alpha)$ is a *primitive prime divisor* (of $\sigma^n(\alpha)$) if $\mathfrak{p} \nmid \sigma^m(\alpha)$ for all $m < n$.

LEMMA 2.2. *Let $\sigma(x) = (x-\gamma)^d + c \in \mathcal{O}_K[x]$. If $\mathfrak{p}$ is a prime divisor of $\sigma^n(\gamma)$, then $\mathfrak{p}$ is a primitive prime divisor of $\sigma^n(\gamma)$ if $\mathfrak{p}$ does not divide any element of $\mathrm{Orb}_\sigma(0)$.*

Proof. If $\mathfrak{p} \mid \sigma^n(\gamma)$, then for any $1 \le k < n$, we can write $\sigma^n(\gamma) = \sigma^k(\sigma^{n-k}(\gamma)) \equiv 0 \pmod{\mathfrak{p}}$. Therefore, if $\mathfrak{p} \nmid \sigma^k(0)$ for all $k < n$, then $\mathfrak{p}$ is a primitive prime divisor of $\sigma^n(\gamma)$. ∎

Proof of Theorem 1.1. We will need several standard results on the cyclotomic field $\mathbb{Q}(\zeta_p)$, namely that its ring of integers is $\mathbb{Z}[\zeta_p]$, the principal ideal generated by $1-\zeta_p$ is the unique prime ideal lying over p, and the only roots of unity in $\mathbb{Q}(\zeta_p)$ are of the form $\pm\zeta_p^n$. These facts can be found (or follow from stronger results) in [14, IV].

Let $D_p = (-1)^{(p-1)/2}p^{p-2}$ be the discriminant of $K = \mathbb{Q}(\zeta_p)$, let S_∞ be the archimedean places of $\mathbb{Q}(\zeta_p)$ and let

$$S = \{\text{primes } \mathfrak{p} \subseteq \mathbb{Z}[\zeta_p] : \mathrm{N}(\mathfrak{p}) \le (2/\pi)^{p-1}|D_p|^{1/2}\} \cup S_\infty; \tag{1}$$

here $\mathrm{N}(\mathfrak{p}) = \#(\mathbb{Z}[\zeta_p]/\mathfrak{p})$ is the norm of the ideal $\mathfrak{p}$. It follows from [15, Theorem 5.4] that the ring $\mathcal{O}_{K,S}$ of S-integers of K is a principal ideal domain and the free part of the unit group $\mathcal{O}_{K,S}^*$ is generated by elements $u_1, \dots, u_t$ of height at most $(2/\pi)^{2p-2}|D_p|$.

Considering the critical orbit $\mathrm{Orb}_{\varphi_p}(1)$ as a subset of $\mathcal{O}_{K,S}$, we can write

$$\varphi_p^n(1) = d_n y_n^p \quad \text{for some } d_n, y_n \in \mathcal{O}_{K,S} \tag{2}$$

with $0 \le v_\mathfrak{p}(d_n) \le p-1$ for all $\mathfrak{p} \notin S$. We now use Lemma 2.2 and our decomposition in (2) to study primitive prime divisors in $\mathrm{Orb}_{\varphi_p}(1)$. To do this, note that $\varphi_p(0) = 1-\zeta_p$ and $\varphi_p(1-\zeta_p) = 1-\zeta_p$, from which it follows that the ideal $(1-\zeta_p)$ is the only prime dividing the non-trivial elements of the orbit of 0. Moreover, $\varphi_p^n(1) \equiv 1 \mod (1-\zeta_p)$ for all $n \ge 0$, so that Lemma 2.2 implies that the principal ideals generated by $\varphi_p^n(1)$ and $\varphi_p^m(1)$ are coprime for all $n \ne m$.

Now fix some $n \ge 1$ and consider $H_n(\varphi_p) = \mathrm{Gal}(K_n(\varphi_p)/K_{n-1}(\varphi_p))$. Since any prime ramifying in K_{n-1} must divide $\varphi_p^m(1)$ for some $m \le n-1$ by the discriminant formula in [8, Lemma 2.6], we see that Lemma 2.1 implies that H_n is maximal unless $v_\mathfrak{p}(\varphi_p^n(1)) \equiv 0 \pmod{p}$ for all primes $\mathfrak{p}$ of K; here we use the fact that φ_p^m is irreducible over $\mathbb{Q}(\zeta_p)$ for all $m \ge 1$, since φ_p^m is Eisenstein at the prime $(1-\zeta_p)$; see Corollary 3.2 for a more general result. However, $v_\mathfrak{p}(\varphi_p^n(1)) = v_\mathfrak{p}(d_n) + p \cdot v_\mathfrak{p}(y_n)$ for all $\mathfrak{p} \notin S$, so that if H_n is not maximal, then $v_\mathfrak{p}(d_n) = 0$ for all $\mathfrak{p} \notin S$, and so $d_n \in \mathcal{O}_{K,S}^*$. It follows that in this situation, we can rewrite (2) as

$$\varphi_p^n(1) = \zeta_p^{n_0}(u_1^{n_1} \dots u_t^{n_t}) y_n^p \quad \text{for some } n_i \in \mathbb{Z}. \tag{3}$$

We can further assume that $0 \le n_i \le p-1$ for all i by absorbing p-powers into y_n^p; likewise, we can absorb the -1 in a root of unity of the form $-\zeta_p^{n_0}$ into y_n^p.

The index bound in Theorem 1.1 now follows from an effective version of Siegel's integral point theorem applied to the superelliptic curve

$$C_p^{(u)} : uY^p = (X-1)^p + 2 - \zeta_p$$

and the S-integral point $(X,Y) = (\varphi_p^{n-1}(1), y_n)$; here u is one of the finitely many S-units of the form $u = \zeta_p^{n_0}(u_1^{n_1} \dots u_t^{n_t})$ for some $0 \le n_i \le p-1$. To see this, let $s = \#S$ be the number of primes in S, let $Q_S = \prod \mathrm{N}(\mathfrak{p})$ be the product of the norms of the finite primes of S, and let $h : \overline{\mathbb{Q}} \to \mathbb{R}_{\ge 0}$ be the standard logarithmic Weil height function on the algebraic numbers [19, §3.1]. Then the height bound in [2, Theorem 2.1] implies that

$$h(\varphi_p^{n-1}(1)) \le (6ps)^{14p^6 s} |D_p|^{2p^4} Q_S^{3p^4} e^{8p^5(p-1)\bar{h}(p,n)}; \tag{4}$$

here $\bar{h}(p,n)$ is the height of the point $[1, u, a_{p-1}, a_{p-2}, \dots, a_1, 1-\zeta_p]$ in $\mathbb{P}^{p+1}(\overline{\mathbb{Q}})$ and the a_i are the coefficients of φ_p:

$$\varphi_p(x) = x^p + a_{p-1}x^{p-1} + \dots + a_1 x + (1-\zeta_p).$$

However, by construction there are at most $(p-1)(2/\pi)^{p-1}|D_p|^{1/2}$ finite primes in S: each prime $\mathfrak{p} \in S$ lies above a rational prime q of size at most $(2/\pi)^{p-1}|D_p|^{1/2}$ and each rational prime q lies below at most $p-1$ primes of $\mathbb{Q}(\zeta_p)$. Hence, s and the rank of the unit group $\mathcal{O}_{K,S}^*$ are bounded as follows:

$$s \le (p-1) + (p-1)|D_p|^{1/2}, \quad \operatorname{rank}(\mathcal{O}_{K,S}^*) \le \frac{p-1}{2} - 1 + (p-1)|D_p|^{1/2}; \tag{5}$$

here we use $2/\pi < 1$ and $\operatorname{rank}(\mathcal{O}_{K,S}^*) = \operatorname{rank}(\mathcal{O}_K^*) + s - \#S_\infty$; note also that $\operatorname{rank}(\mathcal{O}_K^*) = (p-1)/2 - 1$, since $\mathbb{Q}(\zeta_p)$ is a totally imaginary number field. On the other hand, the height of $[x_0, x_1, \dots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ is bounded above by $\sum h(x_i)$ so that

$$\bar{h}(p,n) \le (p-1)\operatorname{rank}(\mathcal{O}_{K,S}^*)\log(D_p) + (p(p-1)+1)\log(2); \tag{6}$$

here we use the height bound on the generators $u_1, \dots, u_t$ of the free part of $\mathcal{O}_{K,S}^*$ from [15, Theorem 5.4] and the elementary height bounds $h(x_1 + \dots + x_n) \le \sum h(x_i) + \log(n)$ and $h(x_1 \dots x_n) \le \sum h(x_i)$ for all $x_i \in \overline{\mathbb{Q}}$. For these and other useful height estimates, see [2, §3.4]. Moreover, the $\log(2)$ above comes from the bound $\binom{p}{i} \le 2^p$ for all $1 \le i \le p-1$.

Combining the estimates in (4)–(6), we obtain the crude bound

$$h(\varphi_p^{n-1}(1)) \le p^{16p^{p/2+9} + 14p^{p/2+7} + 84p^{p/2+6} + 1.5p^{p/2+5} + 2p^5 - 4p^4}. \tag{7}$$

On the other hand, note that $\varphi_p^{n-1}(1) = \delta_p^{n-1}(0) + 1$ for $\delta_p(x) = x^p + 1 - \zeta_p$. Moreover, $|h(x+1) - h(x)| \le \log(2)$ for all $x \in \overline{\mathbb{Q}}$: for a heavy-handed proof, one can apply the argument in [19, Theorem 3.11] to the morphism $[x,y] \mapsto [x+y, y]$ on $\mathbb{P}^1$. Furthermore, [13, Lemma 5.2] implies that

$$|\hat{h}_{\delta_p}(x) - h(x)| \le h(1-\zeta_p) + \log(2) \le \log(4)$$

for all $x \in \overline{\mathbb{Q}}$, where $\hat{h}_{\delta_p}$ is the canonical height function associated to δ_p; strictly speaking, this result is stated for polynomials $x^d + c$ for $c \in \mathbb{Q}$, although the rationality assumption is not necessary. Finally, by the standard transformation properties of the canonical height, $\hat{h}_{\delta_p}(\delta_p^m(x)) = p^m \hat{h}_{\delta_p}(x)$ for all $m \geq 1$ and $x \in \overline{\mathbb{Q}}$ (see, for instance [19, Theorem 3.20]). The bound in (7) then reduces to

$$p^{n-1} \cdot \hat{h}_{\delta_p}(0) \leq p^{16p^{p/2+9}+14p^{p/2+7}+84p^{p/2+6}+1.5p^{p/2+5}+2p^5-4p^4} + \log(8). \tag{8}$$

Therefore, it suffices to give a lower bound on $\hat{h}_{\delta_p}(0)$ to prove the finite index part of Theorem 1.1. Such a bound is provided by the following general lemma, which is a simple consequence of [19, Exercises 3.3 and 3.17].

LEMMA 2.3. *Let $K/\mathbb{Q}$ be a finite extension, let $\phi(x) \in K(x)$ be a rational map of degree d, and let $P \in \mathbb{P}^1(K)$ be a point with infinite forward orbit under ϕ. Then*

$$\hat{h}_\phi(P) \geq \frac{1}{d^{S_\phi}} \quad \textit{where} \quad S_\phi := 12 \cdot [K : \mathbb{Q}] \cdot 2^{[K:\mathbb{Q}]^2} \cdot (1 + C_\phi)^{[K:\mathbb{Q}]^2 + [K:\mathbb{Q}]};$$

here C_ϕ is the constant bounding the difference $|\hat{h}_\phi(Q) - h(Q)|$ over all points $Q \in \mathbb{P}^1(\overline{\mathbb{Q}})$.

Hence, (8) and Lemma 2.3 (applied to $\phi = \delta_p$) together imply that

$$\begin{aligned} n \leq\ & 16p^{p/2+9} + 14p^{p/2+7} + 84p^{p/2+6} + 1.5p^{p/2+5} \\ & + 2p^5 - 4p^4 + 12(p-1)2^{(p-1)^2}(1 + \log(4))^{p(p-1)} + 2. \end{aligned}$$

In particular, the index of $\mathrm{Gal}_{\mathbb{Q}(\zeta_p)}(\varphi_p^m) \leq [C_p]^m$ is bounded independently of m, as claimed.

Although it is nice to have an explicit upper bound on the iterates n for which the groups H_n are not maximal, these bounds are much too large to be useful in practice. For instance, when $p = 3$, the bound above yields $n < 20031664$. Therefore to prove surjectivity for $p = 3, 5, 7$ we combine the techniques above with local computations. As a sketch, we compute a basis for the group $\mathbb{Z}[\zeta_p]^*/(\mathbb{Z}[\zeta_p]^*)^p$ and rule out the possibility that $\varphi_p^n(1) = u_n \cdot y_n^p$ for all $1 \leq n \leq 4$ by computing the absolute norm of $\varphi_p^n(1)$; here we use the fact that $\mathbb{Q}(\zeta_p)$ has class number one (hence it is not necessary to pass to a ring of S-integers) and that the norm of an algebraic unit is ± 1. In particular, to prove the maximality of $G_{\mathbb{Q},n}(\varphi_p)$ up to the 4th stage, it suffices to show that for all $1 \leq n \leq 4$, $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\varphi_p^n(1))$ is not a pth power in $\mathbb{Z}$. This can be easily verified with `Magma`. To rule out larger $n \geq 5$, we look at the critical orbit $\varphi_p^n(1)$ modulo small primes: e.g. $\mathfrak{q} = (2+\zeta_p)$, $(2-\zeta_p)$, $(3+\zeta_p)$, $(3-\zeta_p)$, $(2-3\zeta_p)$. The key here is that $\varphi_p^n(1) \pmod{\mathfrak{q}}$ is usually constant for all $n \geq 5$, that is, the critical orbit fortuitously enters a fixed point. To make this argument explicit, we proceed in cases:

CASE 1. Let $p = 3$, so that $\mathbb{Q}(\zeta_p)$ is an imaginary quadratic field with class number one and unit rank zero. Note that if $\varphi_3^n(1)$ has a decomposition as in (3), then $\varphi_3^n(1) = \zeta_3^i \cdot y_n^3$ for some $0 \le i \le 2$ and some $y_n \in \mathbb{Z}[\zeta_3]$. On the other hand, if $\varphi_3^n(1)$ takes this form, we may assume that $n \ge 5$, since $\mathrm{N}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\varphi_3^n(1))$ is not a cube in $\mathbb{Z}$ for any $1 \le n \le 4$. However, if $\mathfrak{q} = (2-\zeta_3)$, then $\varphi_3(x) \equiv (x-1)^3 \pmod{\mathfrak{q}}$, and hence $\varphi_3^n(1) \equiv 6 \pmod{\mathfrak{q}}$ for all $n \ge 2$; here we use $\mathbb{Z}[\zeta_3]/\mathfrak{q} = \mathbb{F}_7$. However, the congruence $6 \equiv 2, 4 \cdot y_n^3 \pmod 7$ has no solutions, ruling out the possibility that $i = 1, 2$. On the other hand, if $\mathfrak{q} = (3+\zeta_3)$, then $\varphi_3(x) \equiv (x-1)^3 + 5 \pmod{\mathfrak{q}}$ and $\varphi_3^n(1) \equiv 4 \pmod{\mathfrak{q}}$ for all $n \ge 3$; here again $\mathbb{Z}[\zeta_3]/\mathfrak{q} = \mathbb{F}_7$. However, 4 is not a cube in $\mathbb{F}_7$, and we deduce that i cannot be zero either.

CASE 2. Let $p = 5$, so that $\mathbb{Q}(\zeta_5)$ is a degree 4 extension with class number and unit rank equal to one. Moreover, one computes that $1+\zeta_5$ generates the free part of $\mathbb{Z}[\zeta_5]^*$. Hence, if $\varphi_5^n(1)$ has a decomposition as in (3), then $\varphi_5^n(1) = \zeta_5^i \cdot (1+\zeta_5)^j \cdot y_n^5$ for some $0 \le i, j \le 4$ and some $y_n \in \mathbb{Z}[\zeta_5]$. On the other hand, if $\varphi_5^n(1)$ takes this form, then we may assume that $n \ge 5$, since $\mathrm{N}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(\varphi_5^n(1))$ is not a 5th power in $\mathbb{Z}$ for any $1 \le n \le 4$. However, if $\mathfrak{q} = (2-\zeta_5)$, then $\varphi_5(x) \equiv (x-1)^5 \pmod{\mathfrak{q}}$, and hence $\varphi_5^n(1) \equiv 30 \pmod{\mathfrak{q}}$ for all $n \ge 2$; here we use $\mathbb{Z}[\zeta_5]/\mathfrak{q} = \mathbb{F}_{31}$. However, one checks manually that $(i,j) \in \{(0,0),(1,1),(2,2),(3,3),(4,4)\}$ are the only solutions to $30 \equiv 2^i \cdot 3^j \cdot y_n^5 \pmod{31}$. On the other hand, if $\mathfrak{q} = (2+\zeta_5)$, then $\varphi_5(x) \equiv (x-1)^5 + 4 \pmod{\mathfrak{q}}$ and $\varphi_5^n(1) \equiv 5 \pmod{\mathfrak{q}}$ for all $n \ge 2$; here we use $\mathbb{Z}[\zeta_5]/\mathfrak{q} = \mathbb{F}_{11}$. However, one checks that $(i,j) = (4,4)$ is the only remaining pair that has a solution $5 \equiv (-2)^i \cdot (-1)^j \cdot y_n^5 \pmod{11}$. Finally, if $\mathfrak{q} = (3+\zeta_5)$, then $\varphi_5(x) \equiv (x-1)^5 + 5 \pmod{\mathfrak{q}}$ and $\varphi_5^n(1) \equiv 4 \pmod{\mathfrak{q}}$ for all $n \ge 3$; here we use $\mathbb{Z}[\zeta_5]/\mathfrak{q} = \mathbb{F}_{61}$. Moreover, $4 \equiv (-3)^4 \cdot (-2)^4 \cdot y_n^5 \pmod{61}$ has no solution, and we deduce that $(i,j) = (4,4)$ is also impossible.

CASE 3. Let $p = 7$, so that $\mathbb{Q}(\zeta_7)$ is a degree 6 extension with class number one and unit rank equal to two. Moreover, one computes with `Magma` that $1+\zeta_7$ and $\zeta_7^4+\zeta_7$ generate the free part of $\mathbb{Z}[\zeta_7]^*$. Hence, if $\varphi_7^n(1)$ has a decomposition such as that in (3), then $\varphi_7^n(1) = \zeta_7^i \cdot (1+\zeta_7)^j \cdot (\zeta_7^4+\zeta_7)^k \cdot y_n^7$ for some $0 \le i, j, k \le 6$ and some $y_n \in \mathbb{Z}[\zeta_7]$. On the other hand, if $\varphi_7^n(1)$ takes this form, we may assume that $n \ge 5$, since $\mathrm{N}_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\phi_7^n(1))$ is not a 7th power in $\mathbb{Z}$ for any $1 \le n \le 4$. However, if $\mathfrak{q} = (2-\zeta_7)$, then $\varphi_7(x) \equiv (x-1)^7 \pmod{\mathfrak{q}}$, and hence $\varphi_7^n(1) \equiv -1 \pmod{\mathfrak{q}}$ for all $n \ge 2$; here we use $\mathbb{Z}[\zeta_7]/\mathfrak{q} = \mathbb{F}_{127}$. However, setting $x \equiv i + k \pmod 7$ and $y \equiv j + 2k \pmod 7$, one checks manually that $(x,y) = \{(0,0),(1,5),(2,3),(3,1),(4,6),(5,4),(6,2)\}$ are the only pairs of exponents with solutions $-1 \equiv 2^i \cdot 3^j \cdot 18^k \cdot y_n^7 \pmod{127}$: here 2, 3 and 18 are the images of the unit generators. In particular, there are only 49 possible tuples (i,j,k) that must be ruled out: each choice of

$0 \leq k \leq 6$ and (x, y) in the collection above uniquely determines i and j. We now consider these cases sequentially in terms of k:

If $\boxed{k = 0}$, then $(i, j) = \{(0,0), (1,5), (2,3), (3,1), (4,5), (5,4), (6,2)\}$ follows from the restrictions on (x, y) above. Now let $\mathfrak{q} = (2 + \zeta_7)$ so that $\mathbb{Z}[\zeta_7]/\mathfrak{q} = \mathbb{F}_{43}$ and $\varphi_7(x) \equiv (x-1)^7 + 4 \pmod{\mathfrak{q}}$, and we compute that $\varphi_7^n(1) \equiv 3 \pmod{\mathfrak{q}}$ for all $n \geq 5$. One checks that among these restricted pairs, $(i, j) = (6, 2)$ is the only one having a solution to the congruence $3 \equiv (-2)^i \cdot (-1)^j \cdot y_n^7 \pmod{43}$. Finally, $(i, j) = (6, 2)$ is ruled out modulo $\mathfrak{q} = (3 + \zeta_7)$: in this case $\mathbb{Z}[\zeta_7]/\mathfrak{q} = \mathbb{F}_{547}$ and $\varphi_7(x) \equiv (x-1)^7 + 5 \pmod{\mathfrak{q}}$, and we compute that $\varphi_7^n(1) \equiv 407 \pmod{\mathfrak{q}}$ for all $n \geq 3$. Furthermore, the congruence $407 \equiv (-2)^6 \cdot (-1)^2 \cdot y_n^7 \pmod{547}$ has no solutions.

If $\boxed{k = 1}$, then $(i, j) = \{(6,5), (0,3), (3,4), (5,0), (1,1), (2,6), (4,2)\}$ follows from the restrictions on (x, y) above. Again, let $\mathfrak{q} = (2 + \zeta_7)$ so that $\mathbb{Z}[\zeta_7]/\mathfrak{q} = \mathbb{F}_{43}$ and $\varphi_7(x) \equiv (x-1)^7 + 4 \pmod{\mathfrak{q}}$, and we compute that $\varphi_7^n(1) \equiv 3 \pmod{\mathfrak{q}}$ for all $n \geq 5$. One checks that among these restricted pairs, $(i, j) = (5, 0)$ is the only one having a solution to the congruence $3 \equiv (-2)^i \cdot (-1)^j \cdot y_n^7 \pmod{43}$. Finally, as in the $k = 0$ case, the pair $(i, j) = (5, 0)$ is ruled out modulo $\mathfrak{q} = (3 + \zeta_7)$.

If $\boxed{k = 2, 3, 4, 6}$, then one has seven possible pairs (i, j) coming from the restrictions on (x, y) above. For example, $(i, j) = \{(5,3), (6,1), (0,6), (1,4), (2,2), (3,0), (4,5)\}$ when $k = 2$. As in the previous cases $k = 0$ and $k = 1$, only one pair remains after working modulo $\mathfrak{q} = (2+\zeta_7)$, and this exceptional case is ruled out modulo $\mathfrak{q} = (3 + \zeta_7)$.

If $\boxed{k = 5}$, then $(i, j) = \{(2,4), (3,2), (4,0), (5,5), (6,3), (0,1), (1,6)\}$ follows from the restrictions on (x, y) above. This case is slightly different. As usual, only the pair $(i, j) = (1, 6)$ remains after working modulo $\mathfrak{q} = (2+\zeta_7)$. However, when $\mathfrak{q} = (3+\zeta_7)$, the congruence $\varphi_7^n(1) \equiv \zeta_7^1 \cdot (1+\zeta_7)^6 \cdot (\zeta_7^4+\zeta_7)^5 \cdot y_n^7$ has solutions for all n sufficiently large. Therefore, we need a new prime to finish this case. Let $\mathfrak{q} = (2 + 3\zeta_7)$ so that $\mathbb{Z}[\zeta_7]/\mathfrak{q} = \mathbb{F}_{463}$ and $\varphi_7(x) \equiv (x-1)^7 + 2 - 308 \pmod{\mathfrak{q}}$, and we compute that $\varphi_7^n(1) \equiv 156 \pmod{\mathfrak{q}}$ for all $n \geq 5$. Moreover, the congruence $156 \equiv \zeta^1 \cdot (1 + \zeta_7)^6 \cdot (\zeta_7^4 + \zeta_7)^5 \cdot y_n^7 \equiv -386 \cdot y_n^7 \pmod{463}$ has no solutions.

We have thus shown that the factorization (3) is impossible for all $n \geq 1$ when $p = 3, 5, 7$. It follows that

$$\mathrm{Gal}_{\mathbb{Q}(\zeta_3)}(\varphi_3^n) \cong [C_3]^n, \quad \mathrm{Gal}_{\mathbb{Q}(\zeta_5)}(\varphi_5^n) \cong [C_5]^n \quad \text{and} \quad \mathrm{Gal}_{\mathbb{Q}(\zeta_7)}(\varphi_7^n) \cong [C_7]^n$$

for all $n \geq 1$, as claimed. ∎

The key fact that leads to our finite index result (and surjectivity in certain cases) is that the orbit of 0 under $\varphi_p(x) = (x-1)^p + 2 - \zeta_p$ is strictly preperiodic. With this perspective, we produce a family of quadratic poly-

nomials whose arboreal representations are surjective. In working with this family, we are greatly aided by explicit techniques in the theory of rational points on curves: specifically, we apply the Chabauty–Coleman method and the Mordell–Weil sieve.

Proof of Theorem 1.2. As previously noted, it follows from [8, Proposition 4.6] that $\psi_p^n(x)$ is an irreducible polynomial over $\mathbb{Q}$ for all p and all $n \geq 1$. In fact, Jones shows the stronger statement that for all $n \geq 0$, $\psi_p^n(p)$ is not a square in $\mathbb{Q}$; see [8, Lemma 4.3]. In particular, for each $n \geq 2$ it suffices to produce a prime $q_n \geq 3$ satisfying

$$v_{q_n}(\psi_p^n(p)) \equiv 1 \pmod 2, \qquad v_{q_n}(\psi_p^i(p)) = 0 \quad \text{for all } 1 \leq i \leq n-1 \tag{9}$$

to prove that $\mathrm{Gal}_{\mathbb{Q}}(\psi_p^m) \cong [C_2]^m$ for all m (see [8, Theorem 3.3]). Note that q_n will also depend on p, which we suppress in order to avoid cumbersome notation. To find such a q_n we decompose $\psi_p^n(p)$ into a square part and a square-free part:

$$\psi_p^n(p) = d_n \cdot y_n^2 \quad \text{and} \quad d_n = \prod_i q_i, \tag{10}$$

with the q_i distinct, positive prime numbers; to see that $\psi_p^n(p)$ is positive for all $n \geq 2$, one checks that $\psi_p^2(p) > 2p$ and that $x > 2p$ implies $\psi_p^n(x) \geq 2p$ for all n. Moreover, since $\psi_p^n(p)$ is not a square, d_n must be non-trivial.

Now, if no such prime q_n as in (9) exists, then for all i there exists n_i in the range $1 \leq n_i \leq n-1$ such that $q_i \mid \psi_p^{n_i}(p)$. Hence,

$$0 \equiv \psi_p^n(p) \equiv \psi_p^{n-n_i}(\psi_p^{n_i}(p)) \equiv \psi_p^{n-n_i}(0) \pmod{q_i}. \tag{11}$$

On the other hand $\psi_p(0) = \psi_p^2(0) = 2p$, and it follows from (11) that $2p \equiv 0 \pmod{q_i}$ for all i since $n - n_i \neq 0$. We deduce that $d_n = 2^{\epsilon_1} \cdot p^{\epsilon_2}$ for some $\epsilon_i \in \{0, 1\}$. However,

$$\psi_p(x) \equiv (x-1)^2 + 1 \pmod 2 \quad \text{and} \quad \psi_p^n(p) \equiv 1 \pmod 2$$

for all $n \geq 0$, and hence $\epsilon_1 = 0$. Therefore, (10) reduces to

$$\boxed{\psi_p^n(p) = p \cdot y_n^2 \quad \text{for some } y_n \in \mathbb{Z},\ n \geq 2.} \tag{12}$$

Hence, it suffices to classify the primes p for which (12) is impossible, to prove that the arboreal representations in Theorem 1.2 are surjective. To do this, we first classify the rational points on the curves

$$\mathcal{C}_1 : y^2 = x^3 - 2x^2 + 2 \quad \text{and} \quad \mathcal{C}_2 : y^2 = x^7 - 4x^6 + 4x^5 + 2x^4 - 4x^3 + 2,$$

corresponding to the $\psi_p^2(p) = py^2$ and $\psi_p^3(p) = py^2$ cases, to rule out the possibility that (12) holds for $n = 2, 3$. We later show that for all primes $p < 5000$, (12) cannot hold when $n \geq 4$.

Before continuing the proof of Theorem 1.2, we turn to the proof of Theorem 1.3.

Proof of Theorem 1.3. Note that $\mathcal{C}_1$ is an elliptic curve in Weierstrass form, hence all of the relevant arithmetic functions can be calculated by `Magma`. We compute that $\mathcal{C}_1(\mathbb{Q}) \cong \mathbb{Z}$ with generator $(1,1)$, and that $(1,\pm 1)$ are the only integral points on $\mathcal{C}_1$ (points with integral x-coordinates). Therefore, there are no primes p for which (12) holds when $n = 2$.

On the other hand, since $\mathcal{C}_2$ is a curve of genus 3, the set $\mathcal{C}_2(\mathbb{Q})$ is finite and we prove that

$$\mathcal{C}_2(\mathbb{Q}) = \{(1,\pm 1), \infty\}.$$

To do this, let $\mathcal{J}_2$ be the Jacobian of $\mathcal{C}_2$. We compute with `Magma` that $\#\mathcal{J}_2(\mathbb{F}_3) = 24$ and $\#\mathcal{J}_2(\mathbb{F}_{11}) = 1351$. Moreover, as $\gcd(\#\mathcal{J}_2(\mathbb{F}_3), \#\mathcal{J}_2(\mathbb{F}_{11})) = 1$ and $\mathcal{J}_2$ has good reduction modulo 3 and 11, we deduce that $\mathcal{J}_2(\mathbb{Q})$ has trivial torsion; see [12, Appendix]. As for the free part of the Mordell–Weil group, a descent with `Magma` shows that $\mathcal{J}_2(\mathbb{Q})$ has rank at most 2. Conversely, the divisor class of $Q_0 = [(1,1) - \infty]$ and the point on the Jacobian with Mumford representation $P_0 = [x^2 - x - 1, -x + 1]$ are independent: they generate a non-cyclic subgroup of $\mathcal{J}_2(\mathbb{F}_3) \times \mathcal{J}_2(\mathbb{F}_5)$. Therefore, we have generators of a finite-index subgroup of $\mathcal{J}_2(\mathbb{Q}) \cong \mathbb{Z}^2$, which is sufficient to try explicit forms of the Chabauty–Coleman method [16, 18] in combination with the Mordell–Weil sieve [4] to determine $\mathcal{C}_2(\mathbb{Q})$. The first of these techniques applies since the genus of $\mathcal{C}_2$ is strictly larger than the rank of its Jacobian.

Let G be the subgroup of $\mathcal{J}_2(\mathbb{Q})$ generated by the divisors P_0 and Q_0 above. Since we cannot be sure that we capture the full Mordell–Weil group with G, we first show that the index $[\mathcal{J}_2(\mathbb{Q}) : G]$ is not divisible by the small primes in $S = \{2,3,5,7,11\}$. This is relatively easy: for each $\ell \in S$, we produce an auxiliary set of primes S_ℓ such that the induced map

$$G/\ell G \to \prod_{\ell' \in S_\ell} \mathcal{J}_2(\mathbb{F}_{\ell'})/\ell \mathcal{J}_2(\mathbb{F}_{\ell'})$$

is injective. It is straightforward to verify with `Magma` that the sets $S_2 = \{3,5\}$, $S_3 = \{3,5\}$, $S_5 = \{5,19\}$, $S_7 = \{11,47\}$ and $S_{11} = \{13,37\}$ satisfy this property. In particular, if $\overline{G}_q$ and $\overline{\mathcal{J}_2(\mathbb{Q})}_q$ denote the images of G and $\mathcal{J}_2(\mathbb{Q})$ in $\mathcal{J}_2(\mathbb{F}_q)$ respectively, then it follows from our exclusion of the small indices in S that $\overline{G}_q = \overline{\mathcal{J}_2(\mathbb{Q})}_q$ for all $q \in S' = \{3,5,7,13\}$: the upshot of this step is that it allows us to be sure that any local information gained by reducing $\mathcal{J}_2(\mathbb{Q})$ modulo $q \in S'$ is captured instead by reducing G, which is concrete and explicitly known. We bracket this knowledge for now and proceed with the method of Chabauty and Coleman, which we briefly review; for nice introductions to this technique, see [16, 18].

Let $\iota : \mathcal{C}_2(\mathbb{Q}) \to \mathcal{J}_2(\mathbb{Q})$ be the Abel–Jacobi map given by $P \to [P - \infty]$. This map induces an inclusion of the rational points $\mathcal{C}_2(\mathbb{Q}) \subset \mathcal{J}_2(\mathbb{Q}) \subset$

$\mathcal{J}_2(\mathbb{Q}_q)$ into a q-adic Lie group, and since $\operatorname{rank}(\mathcal{J}_2(\mathbb{Q})) = 2$ is less than $\dim(\mathcal{J}_2(\mathbb{Q}_q)) = 3$, there exists a non-zero regular 1-form ω_q on $\mathcal{J}_2(\mathbb{Q}_q)$ whose integral $P \to \int_0^P \omega_q$ annihilates $\mathcal{J}_2(\mathbb{Q})$; here for simplicity we assume that q is a prime of good reduction of $\mathcal{C}_2$. In particular, this q-adic integral kills the image of $\mathcal{C}_2(\mathbb{Q})$ in $\mathcal{J}_2(\mathbb{Q}_q)$. On the other hand, on fibers of the reduction map $\pi_q : \mathcal{C}_2(\mathbb{Q}_q) \to \mathcal{C}_2(\mathbb{F}_q)$, called *residue classes*, this integral can be computed explicitly in terms of power series. Hence, one can use Newton polygons to bound $\#\mathcal{C}_2(\mathbb{Q})$.

We carry out this procedure for $q = 5$. Since $[\mathcal{J}_2(\mathbb{Q}) : G]$ is coprime to $5 \cdot \#\mathcal{J}_2(\mathbb{F}_5) = 900$, it follows that $P \to \int_0^P \omega_5$ kills $\mathcal{J}_2(\mathbb{Q})$ if and only if it kills G. Hence it suffices to compute ω_5 using G. On the other hand, the embedding $\iota : \mathcal{C}_2 \to \mathcal{J}_2$ induces an isomorphism between the regular 1-forms $\Omega^1_{\mathcal{J}_2}(\mathbb{Q}_5)$ on $\mathcal{J}_2$ and the regular 1-forms $\Omega^1_{\mathcal{C}_2}(\mathbb{Q}_5)$ on $\mathcal{C}_2$. Thus, via this identification, there exist $c_0, c_1, c_2 \in \mathbb{Z}_5$ such that $\omega_5 = ((c_2x^2 + c_1x + c_0)/2y)dx$.

Let $\eta_i = x^i dx/(2y)$ for $0 \le i \le 2$ be the standard basis of $\Omega^1_{\mathcal{C}_2}$. We compute with the Coleman-integral function in Sage [1, 17] that

$$\Big(\int_0^{Q_0} \eta_i\Big)_{0\le i\le 2} = \big(3 + O(5^2),\, 3 + 3\cdot 5 + O(5^2),\, 4 + 2\cdot 5 + O(5^2)\big).$$

On the other hand, the divisor $P_0 + 18Q_0$ is in the kernel of reduction modulo 5, and we compute that $P_0 + 18Q_0 = [U_1 + U_2 + U_3 - 3\infty]$ for some points $U_j \in \mathcal{C}_2(\mathbb{Q}_5)$. Again running the Coleman-integral function in Sage we calculate that

$$\begin{aligned}\Big(\int_0^{P_0+18Q_0} \eta_i\Big)_{0\le i\le 2} &= \Big(\sum_{j=1}^{3} \int_0^{[U_j-\infty]} \eta_i\Big)_{0\le i\le 2}\\ &= \big(2\cdot 5 + O(5^2),\, 5 + O(5^2),\, 3\cdot 5 + O(5^2)\big).\end{aligned}$$

After scaling appropriately and reducing modulo 5, we deduce that $c_0 \equiv 0 \pmod 5$ and that $c_2 \equiv 2c_3 \pmod 5$. Therefore, up to an irrelevant scaling factor, the differential ω_5 that kills $\mathcal{J}_2(\mathbb{Q})$ reduces to

$$\overline{\omega}_5 = \frac{(x^2 + 2x)dx}{2y}, \qquad \overline{\omega}_5 \in \Omega_{\mathcal{C}_2}(\mathbb{F}_5).$$

Note that $\mathcal{C}_2(\mathbb{F}_5) = \{\infty, (1, \pm 1), (3, \pm 2), (4, \pm 2)\}$, so that if $\operatorname{ord}_{\bar{P}}(\overline{\omega}_5) > 0$ for some point $\bar{P} \in \mathcal{C}_2(\mathbb{F}_5)$, then $\bar{P} = (3, \pm 2)$. Therefore, if $\bar{P} \ne (3, \pm 2)$, then the residue class of $\bar{P}$, i.e. the preimage of $\bar{P}$ via the reduction map $\mathcal{C}_2(\mathbb{Q}_5) \to \mathcal{C}_2(\mathbb{F}_5)$, contains at most one rational point (see [21, Proposition 6.3]). In particular, the residue classes of $\bar{P} = \infty$ and $\bar{P} = (1, \pm 1)$ contain exactly one rational point. Hence, it suffices to show that the residue classes of $\bar{P} = (3, \pm 2)$ and $\bar{P} = (4, \pm 2)$ contain no rational points, to prove that $\mathcal{C}_2(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$. To do this, we use the Mordell–Weil sieve [4].

In its simplest form, the Mordell–Weil sieve is a procedure for ruling out rational points in residue classes in the following way: let S' be a set of primes of good reduction and consider the commutative diagram

$$\begin{array}{ccc} \mathcal{C}_2(\mathbb{Q}) & \xrightarrow{\quad\iota\quad} & \mathcal{J}_2(\mathbb{Q}) \\ \downarrow{\scriptstyle \pi_{S'}} & & \downarrow{\scriptstyle \alpha_{S'}} \\ \prod_{q\in S'} \mathcal{C}_2(\mathbb{F}_q) & \xrightarrow{\beta_{S'}} & \prod_{q\in S'} \mathcal{J}_2(\mathbb{F}_q) \end{array}$$

with the horizontal maps given by the basepoint at infinity and the vertical maps induced by reduction. Assuming we have generators of $\mathcal{J}_2(\mathbb{Q})$, we can compute the images of $\alpha_{S'}$ and $\beta_{S'}$ explicitly. Therefore, to rule out the existence of $P \in \mathcal{C}_2(\mathbb{Q})$ such that $\pi_{q_0}(P) = \bar{P}_{q_0}$ for some fixed $q_0 \in S'$, we just need to check that

$$\beta_{S'}\Big(\{\bar{P}_{q_0}\} \times \prod_{q\in S'\setminus\{q_0\}} \mathcal{C}_2(\mathbb{F}_q)\Big) \cap \alpha_{S'}(\mathcal{J}_2(\mathbb{Q})) = \emptyset.$$

On the other hand, for each $q \in S' = \{3, 5, 7, 13\}$, we have seen that any local information obtained from $\mathcal{J}_2(\mathbb{Q})$ can be obtained from G, i.e. that $\alpha_{S'}(G) = \alpha_{S'}(\mathcal{J}_2(\mathbb{Q}))$. Moreover, since G is explicitly known to us, we can verify easily with `Magma` that

$$\beta_{S'}\Big(\{\bar{P}_5\} \times \prod_{q\in S'\setminus\{5\}} \mathcal{C}_2(\mathbb{F}_q)\Big) \cap \alpha_{S'}(G) = \emptyset \quad \text{for all } \bar{P}_5 = (3, \pm 2), (4, \pm 2).$$

In particular, there exist no rational points $P \in \mathcal{C}_2(\mathbb{Q})$ reducing to $(3, \pm 2)$ or $(4, \pm 2)$ mod 5. This completes the proof that $\mathcal{C}_2(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$ and the proof of Theorem 1.3. ∎

To finish the proof of Theorem 1.2, we use the local conditions above (and the fact that the critical orbit tends to end in a fixed point modulo small primes) to prove that (12) is impossible for $n \geq 4$. We do this in cases:

Case 1. If $p \equiv 2 \pmod 3$, then $\psi_p^n(p) \equiv 1 \pmod 3$ for all $n \geq 2$. Therefore, if (12) holds for some $n \geq 4$, then $1 \equiv \psi_p^n(p) \equiv 2 \cdot y_n^2 \equiv 2 \pmod 3$ since 1 is the only square in $\mathbb{F}_3^*$, and we reach a contradiction.

Case 2. Similarly, if $p \equiv 3 \pmod 4$, then $\psi_p^n(p) \equiv 1 \pmod 4$ for all $n \geq 1$. Hence, if (12) holds for some $n \geq 4$, then $1 \equiv \psi_p^n(p) \equiv 3 \cdot y_n^2 \equiv 3 \pmod 4$ since 1 is the only non-zero square modulo 4, and we reach a contradiction.

Case 3. If $p \equiv 2 \pmod 5$, then $\psi_p^n(p) \equiv 4 \pmod 5$ for all $n \geq 2$. Therefore, if (12) holds for some $n \geq 4$, then $4 \equiv \psi_p^n(p) \equiv 2 \cdot y_n^2 \equiv 2, 3 \pmod 5$ since 1 and 4 are the only squares in $\mathbb{F}_5^*$. As in the previous cases, we reach a contradiction.

CASE 4. If $p \equiv 3, 6 \pmod 7$, then $\psi_p^n(p) \equiv 1 \pmod 7$ for all $n \geq 3$. Hence, if (12) holds for some $n \geq 4$, then we see that $1 \equiv \psi_p^n(p) \equiv 3 \cdot y_n^2 \equiv 3, 5, 6 \pmod 7$ since $\{1, 2, 4\} = (\mathbb{F}_7^*)^2$, yielding a contradiction.

CASE 5. If $p \equiv 2 \pmod{11}$, then $\psi_p^n(p) \equiv 4 \pmod{11}$ for all $n \geq 2$ and 2 is not a square in $\mathbb{F}_{11}$. Therefore, for all $n \geq 4$, (12) cannot hold. Likewise, if $p \equiv 3 \pmod{11}$, then $\psi_p^n(p) \equiv 6 \pmod{11}$ for all $n \geq 3$ and 6 is not in the set $3 \cdot (\mathbb{F}_{11}^*)^2$. Hence (12) cannot hold for any $n \geq 4$. Similarly, if $p \equiv 5 \pmod{11}$, then $\psi_p^n(p) \equiv 10 \pmod{11}$ for all $n \geq 3$ and 10 is not in the set $5 \cdot (\mathbb{F}_{11}^*)^2$. We deduce that (12) is impossible for all $n \geq 4$. Finally, if $p \equiv 7, 10 \pmod{11}$, then $\psi_p^n(p) \equiv 1 \pmod{11}$ for all $n \geq 3$ and neither 7 nor 10 is a square modulo 11. Therefore (12) cannot hold for any $n \geq 4$.

CASE 6. If $p \equiv 2 \pmod{13}$, then $\psi_p^n(p) \equiv 4 \pmod{11}$ for all $n \geq 2$ and 2 is not a square modulo 13. Therefore (12) is impossible. Likewise, if $p \equiv 3 \pmod{13}$, then $\psi_p^n(p) \equiv 6 \pmod{11}$ for all $n \geq 4$ and 6 is not in the set $3 \cdot (\mathbb{F}_{13}^*)^2$. Hence (12) cannot hold for any $n \geq 4$. On the other hand, if $p \equiv 9 \pmod{13}$, then the orbit of p enters a 2-cycle: $\psi_p^n(p) \equiv 6, 11 \pmod{13}$ for all $n \geq 3$. However, neither 6 nor 11 is a square modulo 13, and we deduce that (12) is impossible. Finally, if $p \equiv 7, 11 \pmod{13}$, then $\psi_p^n(p) \equiv 1 \pmod{13}$ for all $n \geq 4$, and again (12) cannot hold for any $n \geq 4$.

On the other hand, sieving through the 669 primes $p < 5000$, we see that only

$$p = 229, 1009, 1093, 1321, 1453, 3169, 3229, 3301, 3529, 4153, 4261, 4621, 4789$$

are not captured by any of the congruences above. Nonetheless, we can still show that (12) is impossible for all $n \geq 4$ for these exceptional primes by working locally: for $p = 229, 1093, 1453, 3229, 3301, 4261, 4621, 4789$ work mod 16, for $p = 1009, 3529$ work mod 19, for $p = 1321$ work mod 17, for $p = 3169$ work mod 53, and finally for $p = 4153$ work mod 31. ∎

REMARK. Alternatively, it may be possible to use the explicit theory of heights on hyperelliptic genus 3 Jacobians [20] to prove that $G = \mathcal{J}_2(\mathbb{Q})$; this would shorten the proof of Theorem 1.3.

It is likely that the techniques used to establish Theorem 1.2 can be adapted to other families of unicritical polynomials having zero as a strictly preperiodic point. For instance, we have the following example:

PROPOSITION 2.4. *Let $p \geq 3$ be an odd prime and let*

$$f_p(x) = (x - p)^2 - p^2 - 1.$$

Then $\mathrm{Gal}(\mathbb{Q}(f_p^{-3}(0))/\mathbb{Q}) \cong [C_2]^3$.

Proof. It follows from [8, Proposition 4.7] that f_p^n is irreducible over $\mathbb{Q}$ and that for all n, $f_p^n(p)$ is not a rational square in $\mathbb{Q}$. Moreover, we compute that $\mathrm{Orb}_{f_p}(0) = \{-1, -2p\}$, so that [8, Theorem 3.3] implies that $\mathrm{Gal}_{\mathbb{Q}}(f_p^m) \cong [C_2]^m$ unless there exists $2 \le n \le m$ such that

$$2^{\epsilon_1} \cdot p^{\epsilon_2} \cdot y_n^2 = f_p^n(p); \tag{13}$$

here $\epsilon_i \in \{0, 1\}$ and ϵ_1, ϵ_2 are not both zero. On the other hand, $f_p(x) \equiv (x-1)^2 \pmod 2$. Therefore, when n is even, $f_p^n(p) \equiv f_p^n(1) \equiv 1 \pmod 2$ is odd and $\epsilon_1 = 0$. Similarly, $f_p(x) \equiv x^2 - 1 \pmod p$. Hence, when n is odd, we see that $f_p^n(p) \equiv f_p^n(0) \equiv 1 \pmod p$, and $\epsilon_2 = 0$.

In particular, we must rule out integral points (p, y_n) on the curves

$$X_1 : y^2 = x^3 + 2x^2 + 2x + 2$$

and

$$X_2 : 2y^2 = x^8 + 4x^7 + 8x^6 + 10x^5 + 8x^4 + 4x^3 - 1$$

corresponding to the equations

$$py^2 = f_p^2(p) \quad \text{and} \quad 2y^2 = f_p^3(p)$$

respectively. However, X_1 is an elliptic curve and `Magma` computes that the only integral points on X_1 are $(1, \pm 1)$. Likewise, we compute with `Magma` that the Jacobian $J(X_2)$ of X_2 has rank zero, and that $\#J(X_2)(\mathbb{F}_3) = 25$ and $\#J(X_2)(\mathbb{F}_5) = 66$ are coprime. Hence, $J(X_2)(\mathbb{Q})$ is the trivial group [12, Appendix]. Now let I_1 and I_2 be the two points at infinity of X_2, defined over a quadratic extension. If $P \in X_2(\mathbb{Q})$, then the divisor class $[2P - I_1 - I_2]$ must be zero, since $J(X_2)(\mathbb{Q})$ is the trivial group. However, one checks that the image of the corresponding map $X_2(\mathbb{F}_7) \to J(X_2)(\mathbb{F}_7)$ given by $q \to [2q - I_1 - I_2]$ does not contain zero. Therefore, $X_2(\mathbb{Q})$ must be empty; this last argument, in which we use information modulo a single prime $p = 7$ to rule out the existence of rational points, is a very basic form of the Mordell–Weil sieve. ∎

Remark. It follows from Proposition 2.4 (and the analysis in its proof) that $G_{\mathbb{Q}}(f_p) = [C_2]^\infty$ for all $p \equiv 2 \pmod 5$. To see this, note that $f_p(x) \equiv (x-2)^2 \pmod 5$, and thus $f_p^n(p) \equiv f_p^n(2) \equiv 4 \pmod 5$ for all $n \ge 2$. On the other hand, suppose that (13) holds for some $n \ge 2$. Since $\epsilon_1 = 0$ for n even and $\epsilon_2 = 0$ for n odd, we see that the left hand side of (13) must be 0 or $\pm 2 \pmod 5$; here we use the fact that the only squares in $\mathbb{F}_5$ are $\{0, \pm 1\}$. However, this contradicts the congruence $f_p^n \equiv 4 \pmod 5$ for $n \ge 2$. Therefore, $G_{\mathbb{Q}}(f_p) = [C_2]^\infty$, unless maximality fails for f_p or f_p^2, which is impossible by Proposition 2.4 (stronger statement).

In particular, this example illustrates how one might generalize Theorem 1.2 to the family in Proposition 2.4.

3. Appendix: Stability and conjugation. In this section, we make note of a technique for proving the irreducibility of certain polynomials obtained from Eisenstein polynomials via conjugation.

LEMMA 3.1. *Let $K/\mathbb{Q}$ be finite. Let $p \in \mathbb{Z}$ be an odd prime and $\nu : K \to \mathbb{Z} \cup \{\infty\}$ a normalized exponential valuation above p. Suppose $\nu(p) > 1$ and $f(x) = \sum_{i=0}^{p} c_i x^i \in K[x]$ satisfies the following conditions:*

(i) $\nu(c_p) = 0$,
(ii) $\nu(c_i) > 1$ *for* $1 \le i \le p-1$,
(iii) $\nu(c_0) = 1$.

Then for all $\alpha \in K$ with $\nu(\alpha) \ge 0$, the polynomial $f(x+\alpha) - c_p\alpha^p$ is Eisenstein with respect to ν.

Proof. When $\alpha = 0$, the expression reduces to the polynomial f, which is clearly Eisenstein with respect to ν. In fact, the given conditions on the coefficients are slightly stronger than needed. We now show that the stronger conditions imply the given statement for other choices of $\alpha \in K$ with $\nu(\alpha) \ge 0$.

If we write $f(x+\alpha) = \sum_{j=0}^{p} b_j x^j$ then $b_j = \sum_{i=j}^{p} c_i \binom{i}{j} \alpha^{i-j}$ for $0 \le j \le p$. From this we see that $\nu(b_p) = \nu(c_p) = 0$, and for $0 \le j \le p-1$ we have

$$\nu(b_j) \ge \min_{j \le i \le p} \nu\left(c_i \binom{i}{j}\right).$$

For $1 \le j \le p-1$, we have $\nu(c_p\binom{p}{j}) = \nu(p) > 1$. Combining this with the assumption (ii), we see that $\nu(b_j) > 1$ for $1 \le j \le p-1$. Finally, observe that $b_0 - c_p\alpha^p = c_0 + \sum_{i=1}^{p-1} c_i\alpha^i$. Since $\nu(c_0) = 1$ and $\nu(\sum_{i=1}^{p-1} c_i\alpha^i) > 1$, it follows that $\nu(b_0 - c_p\alpha^p) = 1$.

This shows that the coefficients of $f(x+\alpha) - c_p\alpha^p$ also satisfy the conditions in the statement of the lemma, and hence this polynomial is Eisenstein with respect to ν. ∎

COROLLARY 3.2. *Let p be an odd prime, let ζ_p be a primitive pth root of unity, and let i be an integer in the range $2 \le i \le p$. Then all of the iterates of the polynomial*

$$\varphi_{(p,i)}(x) = (x - \zeta_p^i)^p + 1 + \zeta_p^i - \zeta_p$$

are irreducible over $\mathbb{Q}(\zeta_p)$. Moreover, $\varphi_{(p,i)}(0) = \varphi_{(p,i)}^2(0) = \zeta_p^i - \zeta_p$, so that zero is strictly preperiodic for $\varphi_{(p,i)}$.

Proof. Let ν be the valuation on $\mathbb{Q}(\zeta_p)$ above p such that $\nu(1-\zeta_p) = 1$ and $\nu(p) = p-1 > 1$. Now we apply Lemma 3.1 to $f(x) = x^p + (1-\zeta_p)$ and $\alpha = -\zeta_p^i$, so that the polynomial $g(x) = (x-\zeta_p^i)^p + 2 - \zeta_p$ is Eisenstein at ν. On the other hand, $g(x) - (1-\zeta_p^i) = \varphi_{(p,i)}(x)$; hence, it suffices to show that

$\nu(\varphi_{(p,i)}(0)) = 1$ to deduce that $\varphi_{(p,i)}(x)$ is Eisenstein at ν. To do this, we compute that $\varphi_{(p,i)}(0) = \varphi^2_{(p,i)}(0) = \zeta_p^i - \zeta_p$ and that

$$\zeta_p^{p-i} \cdot \varphi_{(p,i)}(0) = 1 - \zeta_p^{p-i+1}.$$

However, $p - i + 1 \not\equiv 0 \pmod{p}$, by the assumption $2 \le i \le p$. Therefore, $1 - \zeta_p^{p-i+1}$ and $1 - \zeta_p$ generate the same ideal in $\mathbb{Z}[\zeta_p]$, and we deduce that $\nu(\varphi^n_{(p,i)}(0)) = 1$ for all $n \ge 1$. It follows that $\varphi^n_{(p,i)}$ is an Eisenstein polynomial with respect to ν for all $n \ge 1$. ∎

REMARK. For φ_p as in Theorem 1.1, $\varphi_p = \varphi_{(p,p)}$ and $\mathrm{Orb}_{\varphi_{(p,i)}}(\zeta_p^i)$ is finite. Therefore, it is likely that Theorem 1.1 holds if we replace φ_p with $\varphi_{(p,i)}$ for any $2 \le i \le p$.

Acknowledgments. This research began at the May 2016 AIM workshop titled "The Galois theory of orbits in arithmetic dynamics", and we thank AIM and the organizers of this workshop. The second author also thanks Michael Stoll for suggesting the use of the Mordell–Weil sieve to rule out residue classes when determining $\mathcal{C}_2(\mathbb{Q})$. The third author's research is partially supported by an NSF Graduate Research Fellowship. Finally, the authors would like to thank the anonymous referee for very thorough and helpful feedback.

References

[1] J. Balakrishnan, R. Bradshaw and K. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, in: Algorithmic Number Theory, Springer, Berlin, 2010, 16–31.

[2] A. Bérczes, J.-H. Evertse and K. Győry, *Effective results for hyper- and superelliptic equations over number fields*, Publ. Math. Debrecen 82 (2013), 727–756.

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

[4] N. Bruin and M. Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. 13 (2010), 272–306.

[5] C. Gratton, K. Nguyen and T. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics*, Bull. London Math. Soc. 45 (2013), 1194–1208.

[6] S. Hamblen, R. Jones and K. Madhu, *The density of primes in orbits of $z^d + c$*, Int. Math. Res. Notices 2015, no. 7, 1924–1958.

[7] W. Hindes, *Galois uniformity in arithmetic dynamics*, Ph.D. thesis, Brown Univ., Providence, RI, 2015.

[8] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. London Math. Soc. 78 (2008), 523–544.

[9] R. Jones, *Galois representations from pre-image trees: an arboreal survey*, in: Actes de la Conférence "Théorie des Nombres at Applications", Publ. Math. Besançon Algèbre Théorie des Nombres 2013, Press Univ. Franche-Comté, Besançon, 2013, 107–136.

[10] R. Jones and M. Manes, *Galois theory of quadratic rational functions*, Comment. Math. Helv. 89 (2014), 173–213.

[11] J. Juul, P. Kurlberg, K. Madhu and T. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Notices 2016, 3944–3969.
[12] N. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), 481–502.
[13] H. Krieger, *Primitive prime divisors in the critical orbit of* $z^d + c$, Int. Math. Res. Notices 2013, 5498–5525.
[14] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. 110, Springer, New York, 1986.
[15] H. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. 26 (1992), 211–244.
[16] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, http://math.mit.edu/~poonen/papers/chabauty.pdf.
[17] SageMath, the Sage Mathematics Software System (Version 7.2), The Sage Developers, 2016, http://www.sagemath.org; see specifically the implementations for "Hyperelliptic curves over p-adic fields".
[18] S. Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory 7 (2013), 765–793.
[19] J. Silverman, *The Arithmetic of Dynamical Systems*, Grad. Texts in Math. 241, Springer, 2007.
[20] M. Stoll, *An explicit theory of heights for hyperelliptic Jacobians of genus three*, arXiv:1701.00772 (2017).
[21] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. 142 (2006), 1201–1214.
[22] M. Stoll, *Galois groups over* $\mathbb{Q}$ *of some iterated polynomials*, Arch. Math. (Basel) 59 (1992), 239–244.

Michael R. Bush
Department of Mathematics
Washington & Lee University
204 W. Washington Street
Lexington, VA 24450, U.S.A.
E-mail: bushm@wlu.edu

Nicole R. Looper
Department of Mathematics
Northwestern University
2033 Sheridan Road
Evanston, IL 60208, U.S.A.
E-mail: nlooper@math.northwestern.edu

Wade Hindes
Department of Mathematics
The Graduate Center
City University of New York (CUNY)
365 Fifth Avenue
New York, NY 10016, U.S.A.
E-mail: whindes@gc.cuny.edu