Research in Number Theory

RESEARCH

Quadratic points on dynamical modular curves

John R. Doyle[1*] and David Krumm[2]

*Correspondence:
john.r.doyle@okstate.edu
[1] Department of Mathematics,
Oklahoma State University,
Stillwater, OK 74078, USA
[2] San José, Costa Rica
Full list of author information is
available at the end of the article

Abstract

Among all the dynamical modular curves associated to quadratic polynomial maps, we determine which curves have infinitely many quadratic points. This yields a classification statement on preperiodic points for quadratic polynomials over quadratic fields, extending previous work of Poonen, Faber, and the authors.

Keywords: Arithmetic dynamics, Dynatomic curve, Preperiodic portrait, Uniform boundedness conjecture

Mathematics Subject Classification: Primary 37P05, 37P35, Secondary 37P15, 11G30, 14G05

1 Introduction

Let K be a field with algebraic closure $\overline{K}$, and let f be a rational function in one variable over K. Corresponding to f there are a morphism of algebraic varieties $\mathbb{P}^1_K \to \mathbb{P}^1_K$ and a map on point sets $\mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$, both of which we also denote by f. A point $P \in \mathbb{P}^1(\overline{K})$ is called **periodic** for f if there exists a positive integer n such that $f^n(P) = P$, where f^n denotes the n-fold composition of f with itself; in that case, the smallest such n is called the (**exact**) **period** of P. More generally, the point P is **preperiodic** for f if there exists $m \geq 0$ such that $f^m(P)$ is periodic; the smallest such m is then called the **preperiod** of P, and we call the period of $f^m(P)$ the **eventual period** of P. Here, f^0 is interpreted as the identity map, so that periodic points are considered preperiodic.

For any intermediate field $K \subseteq L \subseteq \overline{K}$ we define a directed graph $G(f, L)$, called the **preperiodic portrait** of f over L, whose vertices are the points $P \in \mathbb{P}^1(L)$ that are preperiodic for f, and whose directed edges are the ordered pairs $(P, f(P))$ for all vertices P. In the terminology of graph theory, $G(f, L)$ is a *functional graph*, i.e., a directed graph in which every vertex has out-degree 1. Throughout this paper we will use the term **portrait** instead of functional graph in order to emphasize our dynamical perspective.

1.1 Portraits for quadratic maps

Assume henceforth that K is a number field. We will primarily, though not exclusively, be interested in the case where K is a quadratic extension of $\mathbb{Q}$; we refer to such fields simply as *quadratic fields*. A type of problem that has received much attention in the field

of arithmetic dynamics is that of classifying the portraits $G(f, K)$ up to graph isomorphism as f is allowed to vary in an infinite family of rational functions. An early example of this classification problem is Poonen's study [44] of the portraits $G(f, \mathbb{Q})$ as f varies over the family of all quadratic polynomials with rational coefficients.

Theorem 1.1 (Poonen [44]) *Assume that there is no quadratic polynomial over $\mathbb{Q}$ having a rational periodic point of period greater than* 3. *Then, for every quadratic polynomial $f \in \mathbb{Q}[z]$, the portrait $G(f, \mathbb{Q})$ is isomorphic to one of the following twelve graphs (using the labels from Appendix B):*

$$\emptyset, \ 2(1), \ 3(1, 1), \ 3(2), \ 4(1, 1), \ 4(2), \ 5(1, 1)a, \ 6(1, 1), \ 6(2), \ 6(3), \ 8(2, 1, 1), \ 8(3).$$

Regarding the assumption in Theorem 1.1, it is known that a quadratic polynomial over $\mathbb{Q}$ cannot have rational periodic points of period 4 (Morton [39]), period 5 (Flynn–Poonen–Schaefer [19]), or, assuming that the conclusions of the Birch and Swinnerton-Dyer conjecture hold for a certain Jacobian variety, period 6 (Stoll [48]). In addition, a substantial amount of empirical evidence supporting the assumption in Poonen's theorem has been provided by Hutz and Ingram [24] and Benedetto et al. [1]. However, it remains an open problem to prove that this assumption is valid. Portraits for other families of quadratic maps over $\mathbb{Q}$ are studied in the articles [3,7,33,34]. The present paper concerns the preperiodic portraits of quadratic polynomials defined over quadratic fields, a topic previously explored in [11,13,14].

1.2 Analogy with torsion points

A guiding principle that has proved fruitful in arithmetic dynamics is to regard the set of preperiodic points of a map as being analogous to the set of torsion points on an abelian variety. In fact, this is more than just an analogy: The torsion points on an abelian variety A are precisely the points which are preperiodic under the multiplication-by-2 map. It is well known that for an abelian variety A defined over a number field K, the set of K-rational torsion points on A is finite. The dynamical analogue is a theorem of Northcott [42], a special case of which says that for every rational function f of degree at least 2 defined over K, the set of K-rational preperiodic points of f is finite.

Motivated by this analogy, Morton and Silverman formulated the following dynamical analogue of a standard uniform boundedness conjecture for abelian varieties. We state the dynamical conjecture only in the case of endomorphisms of the projective line, although a similar statement applies to arbitrary projective spaces.[1]

Conjecture 1.2 (Morton–Silverman [40]) *For a number field K and morphism $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ of degree greater than* 1, *the number of K-rational preperiodic points of f is bounded above by a constant depending only on the degree of f and the absolute degree of K.*

In both contexts—torsion points on abelian varieties and preperiodic points for rational functions—the set of K-rational points of interest has additional structure: The torsion points form a finite abelian group, and the preperiodic points form a portrait. Thus, even stronger than a *bound* on the number of such K-rational points would be a *classification*

---

[1]Interestingly, work of Fakhruddin [18] shows that the more general Morton–Silverman conjecture in fact implies its analogue for abelian varieties. See also [46, §3.3], where Merel's theorem for elliptic curves is shown to follow from Conjecture 1.2.

of the structures that can be realized by the set of such K-rational points. For example, Mazur's celebrated torsion theorem [35] says not only that an elliptic curve $E/\mathbb{Q}$ has at most 16 rational torsion points, but also that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ must be isomorphic to one of 15 specific abelian groups.

On the dynamical side, Conjecture 1.2 would imply, for example, that there are only finitely many isomorphism classes of portraits $G(f, \mathbb{Q})$ as f ranges over all quadratic polynomials with rational coefficients. Theorem 1.1 can thus be seen as a refinement of the conjecture in this case, as it provides a (conditionally) complete list of all possible portraits for the family of quadratic polynomial maps, analogous to Mazur's torsion theorem.

Similarly, the Morton–Silverman conjecture would imply that the portraits $G(f, K)$, where K is a quadratic field and f is a quadratic polynomial over K, fall into finitely many isomorphism classes. A conjecturally complete list of classes was first proposed in [14] and is included here in Appendix B. The list is comprised of 46 portraits, and can be viewed as analogous to the list of 26 abelian groups, known by work of Kamienny [26] and Kenku–Momose [27], that can arise as torsion subgroups of elliptic curves over quadratic fields.

1.3 Infinitely occurring portraits

Our primary objective in this paper is to determine, under a suitable notion of equivalence of maps, which of the 46 graphs in [14] arise as the preperiodic portrait of infinitely many inequivalent quadratic polynomials over quadratic fields. In the context of elliptic curves, both over $\mathbb{Q}$ and over quadratic fields, the corresponding question is well understood: *every* abelian group that arises as the torsion subgroup of an elliptic curve can be realized as such by infinitely many non-isomorphic curves (see [25]).

In order to state our questions more precisely, we begin by defining the appropriate equivalence relation on maps. Two morphisms $f, h : \mathbb{P}^1_K \to \mathbb{P}^1_K$ are called **linearly conjugate** over K if there exists an automorphism $\sigma \in \mathrm{PGL}_2(K)$ such that

$$h = \sigma^{-1} \circ f \circ \sigma.$$

(Similarly, one can define linear conjugacy over any extension of K.) In that case, a simple argument shows that the portraits $G(f, K)$ and $G(h, K)$ are isomorphic as directed graphs; hence, the isomorphism class of $G(f, K)$ is determined by the linear conjugacy class of f.

In the case of quadratic polynomials, it is well known (see, for example, [46, p. 156]) that every such map $f \in K[z]$ is linearly conjugate to a unique map of the form

$$f_c(z) := z^2 + c,$$

where $c \in K$. Thus, in studying the portraits of quadratic polynomials we may restrict attention to the one-parameter family of maps f_c.

Returning to the question of portraits arising infinitely often, the case of quadratic polynomials over $\mathbb{Q}$ was answered by Faber, who showed in addition that Poonen's list in [44] does not omit any such portrait.

Theorem 1.3 (Faber [17]) *For a portrait $\mathcal{P}$, the following are equivalent:*

(i) *There exist infinitely many $c \in \mathbb{Q}$ such that $G(f_c, \mathbb{Q}) \cong \mathcal{P}$.*

(ii) *$\mathcal{P}$ is isomorphic to one of the following graphs (using the labels from Appendix B):*

$$\emptyset, \ 4(1, 1), \ 4(2), \ 6(1, 1), \ 6(2), \ 6(3), \ 8(2, 1, 1).$$

Motivated by Faber's theorem, we now state the main questions to be addressed here.

Question 1.4 Among the 46 known isomorphism classes of portraits arising as $G(f_c, K)$, with K a quadratic field and $c \in K$, which ones can be realized as such by infinitely many algebraic numbers c? In addition, must every infinitely occurring portrait belong to one of the 46 known isomorphism classes?

1.4 Main results

We define the following sets of portraits using labels as in Appendix B:

$$\Gamma_0 := \{\emptyset,\ 4(1, 1),\ 4(2),\ 6(1, 1),\ 6(2),\ 6(3),\ 8(2, 1, 1)\};$$

$$\Gamma_{\text{rat}} := \{8(1, 1)\text{a},\ 8(2)\text{a},\ 8(4),\ 10(3, 1, 1),\ 10(3, 2)\};$$

$$\Gamma_{\text{quad}} := \{8(1, 1)\text{b},\ 8(2)\text{b},\ 8(3),\ 10(2, 1, 1)\text{a/b}\};$$

$$\Gamma := \Gamma_0 \cup \Gamma_{\text{rat}} \cup \Gamma_{\text{quad}}.$$

We provide two answers to Question 1.4 which differ in their level of specificity. The simplest is Theorem 1.5, with Theorems 1.6 and 1.7 providing additional information in terms of the above subsets of Γ. For an integer $n \geq 1$, we define

$$\mathbb{Q}^{(n)} := \{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n\}.$$

Theorem 1.5 *For a portrait $\mathcal{P}$, the following are equivalent:*

(i) *There exist infinitely many $c \in \mathbb{Q}^{(2)}$ such that $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K containing c.*

(ii) *$\mathcal{P} \in \Gamma$.*

Theorem 1.5 can be refined in order to take into account certain subtleties illustrated by the following example: We see from Theorem 1.3 that the portrait $\mathcal{P} = 4(2)$ is realized as $G(f_c, \mathbb{Q})$ for infinitely many $c \in \mathbb{Q}$. For each such c, the set of preperiodic points for f_c is a set of bounded height, and therefore f_c has only finitely many preperiodic points of algebraic degree 2 over $\mathbb{Q}$. Hence, for each of the infinitely many $c \in \mathbb{Q}$ with $G(f_c, \mathbb{Q}) \cong \mathcal{P}$, we must also have $G(f_c, K) \cong \mathcal{P}$ for all but finitely many quadratic fields K.

We therefore show that each of the portraits $\mathcal{P} \in \Gamma$ is realized infinitely often—even if one excludes the infinitely many "trivial" realizations in the sense of the previous paragraph. This is done in the next two theorems, which are stated separately in order to distinguish between polynomials with rational coefficients and those with quadratic algebraic coefficients.

Theorem 1.6 *For a portrait $\mathcal{P}$, the following are equivalent:*

(i) *There exist infinitely many $c \in \mathbb{Q}$ such that $G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \mathcal{P}$ for some quadratic field K.*

(ii) *$\mathcal{P} \in \Gamma \smallsetminus \{\emptyset, 6(3)\}$.*

Theorem 1.7 *For a portrait $\mathcal{P}$, the following are equivalent:*

(i) *There exist infinitely many $c \in \mathbb{Q}^{(2)} \smallsetminus \mathbb{Q}$ such that $G(f_c, \mathbb{Q}(c)) \cong \mathcal{P}$.*

(ii) *$\mathcal{P} \in \Gamma_0 \cup \Gamma_{\text{quad}}$.*

Note that every portrait in Γ is covered by at least one of Theorems 1.6 and 1.7, since $\emptyset$ and 6(3) are elements of Γ_0. In particular, these two theorems together imply Theorem 1.5.

1.5 Quadratic points on dynamical modular curves

The proofs of our main results rely heavily on the concept of a *dynamical modular curve*. To each of the 46 portraits from [14], and more generally to any portrait that could potentially be realized as the preperiodic portrait of a quadratic polynomial over a number field, we associate an algebraic curve parametrizing instances of the portrait as a preperiodic portrait $G(f_c, K)$. The curve corresponding to a portrait $\mathcal{P}$ will be denoted $X_1(\mathcal{P})$ by analogy with the classical modular curves $X_1(N)$ parametrizing elliptic curves with a torsion point of order N. To avoid confusion, the latter curve will henceforth be denoted $X_1^{\mathrm{ell}}(N)$. The details of the construction as well as basic properties of dynamical modular curves are discussed in [12]. A more general construction of dynamical moduli spaces appears in [16].

The core of our analysis in this paper is a study of basic geometric invariants, such as genus and gonality, of the curves $X_1(\mathcal{P})$. We then turn this geometric data into arithmetic data using Faltings' theorem on rational points on subvarieties of abelian varieties, via the following result of Harris and Silverman:

Theorem 1.8 [Harris–Silverman [22, Cor. 3]] *Let X be a smooth, irreducible, projective curve of genus $g \geq 2$ defined over a number field K. If X is neither hyperelliptic nor bielliptic then X has only finitely many points that are quadratic over K.*

In addition, we consider arithmetic questions regarding the fields of definition of quadratic points on $X_1(\mathcal{P})$. In particular, if $X_1(\mathcal{P})$ has a point defined over a quadratic number field K, what can be said about basic arithmetic invariants of K, such as discriminant and class number? For the curves $X_1^{\mathrm{ell}}(N)$, arithmetic questions of this kind have been discussed by several authors: Momose [36] shows that if K is the field of definition of a quadratic point on $X_1^{\mathrm{ell}}(13)$, then the prime 2 splits in K, and 3 is unramified in K; Bosman et al. [5] show that K must be a real quadratic field, an observation also made in [14]. In the case of the modular curves $X_0^{\mathrm{ell}}(N)$, Najman and Trbović [41] prove arithmetic results of this type for several values of N.

For the dynamical modular curves $X_1(\mathcal{P})$ we prove the following two theorems. Though our methods can be applied to several portraits in the set Γ (namely, those for which the corresponding modular curve is hyperelliptic), the portraits 8(4) and 10(3,1,1) are highlighted here due to their significance in the context of elliptic curves, explained below.

By a **quadratic point** on an algebraic curve over a field k, we mean a point whose field of definition is a quadratic extension of k.

Theorem 1.9 *Let $\mathcal{P}$ denote the portrait* 8(4).

(a) *For every prime p and every residue class $\mathfrak{c} \in \mathbb{Z}/p\mathbb{Z}$, there exist infinitely many squarefree integers $d \in \mathfrak{c}$ such that $X_1(\mathcal{P})$ has a quadratic point defined over $\mathbb{Q}(\sqrt{d})$.*

(b) *There exist infinitely many imaginary quadratic fields K with class number divisible by 10 such that $X_1(\mathcal{P})$ has a quadratic point defined over K.*

As noted in [14], the above curve $X_1(\mathcal{P})$ is isomorphic to $X_1^{\text{ell}}(16)$. Thus, Theorem 1.9 provides new information about the collection of quadratic fields K such that there exists an elliptic curve E/K with a K-rational torsion point of order 16.

Similarly, taking $\mathcal{P} = 10(3, 1, 1)$, the curve $X_1(\mathcal{P})$ is known to be isomorphic to $X_1^{\text{ell}}(18)$; see [44, p. 15]. The next theorem strengthens earlier results by Kenku–Momose [27] regarding the splitting of rational primes in the fields of definition of quadratic points on this curve.

Theorem 1.10 *Let $\mathcal{P}$ denote the portrait* 10(3, 1, 1) *and let K be the field of definition of a quadratic point on $X_1(\mathcal{P})$.*

   (a) *The prime* 2 *splits in K, and* 3 *is not inert in K.*
   (b) *There exists an infinite and computable set of primes, denoted π, that is independent of K, and such that every prime in π is unramified in K.*

1.6 Points of higher degree

Though our primary focus here is on quadratic fields, we make one observation concerning arbitrary number fields. The next result is a straightforward consequence of a theorem of Frey [20] together with the main theorem of [15].

Theorem 1.11 *Fix a positive integer n. For any portrait $\mathcal{P}$, let $\gamma(\mathcal{P})$ denote the set of algebraic numbers $c \in \mathbb{Q}^{(n)}$ such that $\mathcal{P} \cong G(f_c, K)$ for some number field K satisfying $c \in K \subset \mathbb{Q}^{(n)}$. There are only finitely many portraits $\mathcal{P}$ such that $\gamma(\mathcal{P})$ is infinite.*

Note that Theorem 1.5 is a more refined version of Theorem 1.11 in the case $n = 2$.

1.7 Outline of the paper

In Section 2 we define the notion of a *generic quadratic portrait* and discuss basic facts concerning dynamical modular curves associated to such portraits, followed by general properties of algebraic curves in Section 3.

In Section 4, we apply geometric arguments to determine all generic quadratic portraits $\mathcal{P}$ for which the curve $X_1(\mathcal{P})$ has infinitely many quadratic points. This proves, in particular, the implication (i) $\Rightarrow$ (ii) in Theorem 1.5; see Theorem 4.1 and the immediately preceding discussion.

Section 5 addresses the issue that K-rational points on $X_1(\mathcal{P})$ correspond to instances where $G(f_c, K)$ simply *contains* the portrait $\mathcal{P}$; that is, we need not have an isomorphism $G(f_c, K) \cong \mathcal{P}$, and in fact, in many cases we do not. The section culminates with the proofs of Theorems 1.6 and 1.7 in Sect. 5.3.

Finally, Section 6 is devoted to arithmetic questions concerning the fields of definition of quadratic points on the curves $X_1(\mathcal{P})$, and in particular to proving Theorems 1.9 and 1.10.

2 Dynamical modular curves
2.1 Dynatomic polynomials

If f is a polynomial with coefficients in a field K and $\alpha \in \overline{K}$ is a point of exact period n for f, then α is a root of the polynomial $f^n(z) - z$. However, the roots of $f^n(z) - z$ may have

period strictly dividing n, and indeed there is a factorization

$$f^n(z) - z = \prod_{d|n} \Phi_{d,f}(z),$$

where (generically) the roots of $\Phi_{d,f}$ have exact period d for f. Möbius inversion yields

$$\Phi_{n,f}(z) = \prod_{d|n}(f^d(z) - z)^{\mu(n/d)},$$

where μ denotes the Möbius function. We call $\Phi_{n,f}$ the nth **dynatomic polynomial** of f.

More generally, for $m, n \geq 1$ we define

$$\Phi_{m,n,f}(z) := \frac{\Phi_{n,f}(f^m(z))}{\Phi_{n,f}(f^{m-1}(z))}.$$

Then $\Phi_{m,n,f}$ is a polynomial whose roots are (again, generically) points of preperiod m and eventual period n for f. (That $\Phi_{n,f}$ and $\Phi_{m,n,f}$ are indeed polynomials is proven in [23,46].)

Since we are specifically interested in the family $f_c(z) = z^2 + c$, we write

$$\Phi_n(c, z) := \Phi_{n,f_c}(z) \quad \text{and} \quad \Phi_{m,n}(c, z) := \Phi_{m,n,f_c}(z).$$

Then Φ_n (resp., $\Phi_{m,n}$) is a polynomial in $\mathbb{Z}[c, z]$, and the vanishing locus defines an affine curve $Y_1(n)$ (resp., $Y_1(m, n)$), which we refer to as a **dynatomic curve**. Thus, for example, if α has period n for f_c, then (c, α) is a point on the dynatomic curve $Y_1(n)$. We denote by $X_1(\cdot)$ the normalization of the projective closure of the affine curve $Y_1(\cdot)$, and we also refer to $X_1(\cdot)$ as a dynatomic curve.

2.2 Dynamical modular curves associated to portraits

The dynamical properties of quadratic polynomial maps impose certain restrictions on those portraits that may be realized as $G(f, K)$ for some number field K and a quadratic polynomial $f \in K[z]$. First, no point may have more than two preimages under f. Also, for each positive $n \in \mathbb{Z}$, the nth dynatomic polynomial for a quadratic polynomial f has degree

$$D(n) := \deg \Phi_{n,f}(z) = \sum_{d|n} \mu(n/d)2^d. \tag{2.1}$$

Thus, a quadratic polynomial has at most $D(n)$ points of period n, partitioned into at most $R(n) := D(n)/n$ cycles of length n. With these restrictions in mind, we make the following definition:

Definition 2.1 A **quadratic portrait** is a portrait $\mathcal{P}$ satisfying the following properties:

(a) Every vertex of $\mathcal{P}$ has in-degree at most 2.
(b) For each $n \geq 1$, the number of n-cycles in $\mathcal{P}$ is at most

$$R(n) := \frac{1}{n} \sum_{d|n} \mu(n/d)2^d.$$

For any number field K and quadratic polynomial $f \in K[z]$, the portrait $G(f, K)$ is quadratic. However, for *most* quadratic polynomials (in the sense that there are only finitely many exceptions over any given number field), we can say more about the structure of the set of K-rational preperiodic points. For the model $f_c(z) = z^2 + c$, if α is a preperiodic point for f_c, then $-\alpha$ is also preperiodic, since both are preimages of $f(\alpha)$.

Fig. 1 A generic quadratic portrait
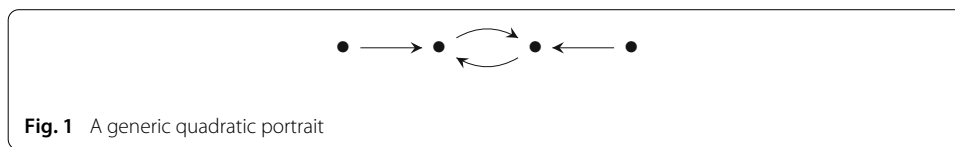
Thus, a preperiodic point typically has either no K-rational preimages or exactly two K-rational preimages. The exception to this rule occurs when $\alpha = 0$ is a preperiodic point, in which case exactly one preperiodic point (namely, $c = f_c(0)$) has a single K-rational preimage.

Along the same lines, if a polynomial f_c has a K-rational fixed point β, then β is a root of the quadratic polynomial $f_c(z) - z = z^2 - z + c$; thus, unless we have $\mathrm{disc}(f_c(z) - z) = 1 - 4c = 0$ (i.e., $c = 1/4$), there is a second fixed point β', necessarily defined over K.

With these observations in mind, we make the following definition.

Definition 2.2 A **generic quadratic portrait** is a quadratic portrait $\mathcal{P}$ with the following additional properties:

(a) The in-degree of any vertex of $\mathcal{P}$ is equal to 0 or 2.
(b) If $\mathcal{P}$ has a fixed point, then $\mathcal{P}$ has exactly two fixed points.

Remark 2.3 We will sometimes refer to the results of [12], in which the term "strongly admissible" is used instead of "generic quadratic."

Given a quadratic portrait $\mathcal{P}$, there is a **dynamical modular curve** $Y_1(\mathcal{P})$, defined over $\mathbb{Q}$, whose K-points—for any extension $K/\mathbb{Q}$—correspond to tuples $(c, z_1, \ldots, z_n)$ such that $z_1, \ldots, z_n$ are preperiodic points forming a subportrait of $G(f_c, K)$ isomorphic to $\mathcal{P}$. In other words, $Y_1(\mathcal{P})$ is a (coarse) moduli space for the problem of classifying quadratic polynomials with marked preperiodic points. If Q is the point on $Y_1(\mathcal{P})$ corresponding to such a tuple, then the field of definition of Q is $\mathbb{Q}(c, z_1, \ldots, z_n)$. We denote by $X_1(\mathcal{P})$ the smooth projective curve birational to $Y_1(\mathcal{P})$.

A few specific dynamical modular curves $Y_1(\mathcal{P})$ were used to prove the classification results in [11,13,14,44], while dynamical modular curves are treated more generally in [12]. In the latter article, the curves $Y_1(\mathcal{P})$ are defined only in the case that $\mathcal{P}$ is a generic quadratic portrait. We lose no generality in making such a restriction: Given *any* quadratic portrait $\mathcal{P}$, there is a unique portrait $\mathcal{P}'$ that is minimal among generic quadratic portraits containing $\mathcal{P}$ as a subportrait. In the language of [12], $\mathcal{P}'$ is the generic quadratic portrait *generated by* the vertices of $\mathcal{P}$. It follows from the results of [12, §2] that $X_1(\mathcal{P}) \cong X_1(\mathcal{P}')$, so we may as well assume that $\mathcal{P}$ is generic quadratic.

Rather than formally defining $X_1(\mathcal{P})$ (we refer the interested reader to [12] or, for a different approach in a more general setting, [16]), we give an example.

Example 2.4 Consider the generic quadratic portrait $\mathcal{P}$ appearing in Fig. 1. One could construct a curve birational to $X_1(\mathcal{P})$ simply by giving one equation for each relation coming from an edge in $\mathcal{P}$: if we label the vertices 1, 2, 3, 4 from left to right, we have

$$z_1^2 + c = z_2, \qquad z_2^2 + c = z_3,$$
$$z_3^2 + c = z_2, \qquad z_4^2 + c = z_3. \tag{2.2}$$

Note that we must also impose certain Zariski open conditions of the form $z_i \neq z_j$ to remove extraneous components; for example, there is a full component of the curve defined by (2.2) on which $z_1, z_2, z_3,$ and z_4 are all equal. It is this approach that is taken in [16].

An alternative approach, which is particular to quadratic polynomials, is to note that any generic quadratic portrait containing a point of period 2 must necessarily contain $\mathcal{P}$. Thus, another (affine) model for $X_1(\mathcal{P})$ is the plane curve defined by the vanishing of the dynatomic polynomial

$$\Phi_2(c,z) = \frac{(z^2+c)^2 + c - z}{z^2 + c - z} = z^2 + z + c + 1.$$

In other words, $X_1(\mathcal{P})$ is isomorphic to the dynatomic curve $X_1(2)$. This second model has the advantage of being defined in a lower-dimensional affine space ($\mathbb{A}^2$, rather than $\mathbb{A}^5$), and it is this second approach which is described in detail in [12].

We conclude this example by pointing out that $X_1(\mathcal{P}) \cong X_1(2)$ also has "degenerate" points where two or more of the vertices of the portrait $\mathcal{P}$ collapse. For example, the equation $\Phi_2(c,z) = 0$ has the solution $(c,z) = \left(-\frac{3}{4}, -\frac{1}{2}\right)$ despite the fact that $-\frac{1}{2}$ is a fixed point for $f_{-3/4}$. However, for a given portrait $\mathcal{P}$, there are only finitely many such degenerate points on $X_1(\mathcal{P})$.

Before summarizing the required properties of dynamical modular curves, we recall the following terminology:

Definition 2.5 Let X be a smooth, irreducible projective curve defined over a field k. The **k-gonality** of X, denoted $\text{gon}_k(X)$, is the minimal degree of a nonconstant morphism $X \to \mathbb{P}^1$ defined over k.

Proposition 2.6 *Let $\mathcal{P}$ be a generic quadratic portrait, and let k be any field of characteristic* 0.

(a) *The curve $X_1(\mathcal{P})$ is irreducible over k.*
(b) *If $\mathcal{P}'$ is a generic quadratic portrait properly contained in $\mathcal{P}$, then there is a finite morphism $\pi_{\mathcal{P},\mathcal{P}'} : X_1(\mathcal{P}) \to X_1(\mathcal{P}')$ of degree at least 2 defined over k.*
(c) *Given any ordering $\mathcal{P}_1, \mathcal{P}_2, \ldots$ of all generic quadratic portraits, the k-gonalities of the curves $X_1(\mathcal{P}_i)$ tend to ∞.*

Proof Parts (a) and (b) are proven in [12, Thm. 1.7] and [12, Prop. 3.3], respectively. Note that the morphism $\pi_{\mathcal{P},\mathcal{P}'}$ is obtained simply by forgetting the preperiodic points corresponding to vertices of $\mathcal{P} \smallsetminus \mathcal{P}'$, hence is defined over the base field k.

Statement (c) is a slight generalization of, but follows directly from, [15, Thm. 1.1(b)], which says that as $m + n \to \infty$, the gonalities of the curves $X_1(m,n)$ tend to ∞. Given a bound B, there are only finitely many quadratic portraits $\mathcal{P}$ such that *every* vertex v of $\mathcal{P}$ has preperiod m and eventual period n satisfying $m + n \leq B$. In other words, if for every generic quadratic portrait $\mathcal{P}$ we choose a vertex $v_{\mathcal{P}}$ with preperiod $m_{\mathcal{P}}$ and eventual period $n_{\mathcal{P}}$ maximizing the sum $m_{\mathcal{P}} + n_{\mathcal{P}}$, we must have $m_{\mathcal{P}} + n_{\mathcal{P}} \to \infty$ as $\mathcal{P}$ ranges over all generic quadratic portraits in any order. Since there is a nonconstant morphism from $X_1(\mathcal{P})$ to $X_1(m_{\mathcal{P}}, n_{\mathcal{P}})$ (e.g., by part (b)), we have $\text{gon}_k(X_1(\mathcal{P})) \geq \text{gon}_k(X_1(m_{\mathcal{P}}, n_{\mathcal{P}}))$, and the latter expression tends to ∞. □

Proof of Theorem 1.11 Fix $n \geq 1$ and a portrait $\mathcal{P}$, and suppose there are infinitely many $c \in \mathbb{Q}^{(n)}$ such that $G(f_c, K) \cong \mathcal{P}$ for some degree-n number field K containing c. Then the dynamical modular curve $X_1(\mathcal{P})$ has infinitely many points of degree at most n. It follows from [20, Prop. 2] (cf. [9, Thm. 5]) that $X_1(\mathcal{P})$ must have gonality at most $2n$, hence there are only finitely many such portraits $\mathcal{P}$ by part (c) of Proposition 2.6. □

3 Some useful properties of algebraic curves

In this section, we collect a few facts about algebraic curves that will be used throughout the rest of the paper.

First, we provide a statement that follows from Hilbert's irreducibility theorem; see [45, §3.4] and [32, §9.2] for details.

Proposition 3.1 *Let K be a number field, let X be a curve defined over K, and let $\varphi : X \to \mathbb{P}^1$ be a dominant morphism of degree $d \geq 2$ defined over K. Then the set*

$$\mathcal{T} := \left\{ P \in \mathbb{P}^1(K) : [K(Q) : K] < d \text{ for some } Q \in \varphi^{-1}(P) \right\}$$

is a thin subset of $\mathbb{P}^1(K)$.

Remark 3.2 Thin subsets $\mathcal{T} \subset \mathbb{P}^1(K)$ have density 0, in the sense that

$$\lim_{N \to \infty} \frac{\left| \{ P \in \mathcal{T} : h(P) \leq N \} \right|}{\left| \{ P \in \mathbb{P}^1(K) : h(P) \leq N \} \right|} = 0,$$

where h is the naïve Weil height on $\mathbb{P}^1(\overline{\mathbb{Q}})$. In particular, for any maximal ideal $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ and any mod-$\mathfrak{p}$ residue class $\mathfrak{c}$ in $\mathbb{P}^1(K)$, the set $\mathfrak{c} \setminus \mathcal{T}$ is infinite.

Given an elliptic curve E with Weierstrass equation $y^2 = f(x)$, where $f \in K[x]$ is squarefree of degree 3, it is easy to construct infinitely many quadratic points on E: For "most" $x \in K$, the point $(x, y) = (x, \sqrt{f(x)})$ is quadratic over K. More precisely, since f is not a square in $K[x]$, it follows from Hilbert irreducibility that $f(x_0)$ is a nonsquare in K for all x_0 outside a thin subset of K. The following result, proven in [14, Lem. 2.2], gives a useful characterization of quadratic points (x, y) with $x \notin \mathbb{Q}$:

Lemma 3.3 *Let K be a number field, and let E/K be an elliptic curve defined by an equation of the form*

$$y^2 = ax^3 + bx^2 + cx + d,$$

where $a, b, c, d \in K$ and $a \neq 0$. Suppose $(x, y) \in E(\overline{K})$ is a quadratic point with $x \notin K$. Then there exist $(x_0, y_0) \in E(K)$ and $t \in k$ such that $y = y_0 + t(x - x_0)$ and

$$x^2 + \frac{ax_0 - t^2 + b}{a} x + \frac{ax_0^2 + t^2 x_0 + bx_0 - 2y_0 t + c}{a} = 0.$$

By Theorem 1.8, a curve with infinitely many quadratic points must admit a degree-2 morphism to either $\mathbb{P}^1$ or an elliptic curve, hence must have gonality at most 4. Thus, to prove that a curve has finitely many quadratic points, it suffices to show that the gonality of the curve is greater than 4. The following inequality is a standard tool for finding lower bounds for gonalities.

Proposition 3.4 [Castelnuovo–Severi inequality [47, Thm. 3.11.3]] *Let Y, Y_1, and Y_2 be curves of genera g_Y, g_1, and g_2, respectively. Suppose we have maps $\varphi_1 : Y \to Y_1$ and $\varphi_2 : Y \to Y_2$ of degrees d_1 and d_2, and suppose further that there is not an intermediate curve Z and a map $\psi : Y \to Z$ of degree at least 2 such that both φ_1 and φ_2 factor through ψ. Then*

$$g_Y \le d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1). \tag{3.1}$$

4 Dynamical modular curves with infinitely many quadratic points

The purpose of this section is to prove one direction of Theorem 1.5, namely that if there are infinitely many $c \in \mathbb{Q}^{(2)}$ such that $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K containing c, then $\mathcal{P} \in \Gamma$. Since any such realization of $\mathcal{P}$ as $G(f_c, K)$ yields a quadratic point on the dynamical modular curve $Y_1(\mathcal{P})$, it suffices to prove the following:

Theorem 4.1 *Let $\mathcal{P}$ be a generic quadratic portrait. Then $X_1(\mathcal{P})$ has infinitely many quadratic points if and only if $\mathcal{P} \in \Gamma$.*

Remark 4.2 If we just assume that $\mathcal{P}$ is a quadratic portrait (i.e., not necessarily generic), then $X_1(\mathcal{P})$ has infinitely many quadratic points if and only if $\mathcal{P}$ is a subportrait of some portrait in Γ. This follows from Theorem 4.1 as well as the fact that for any quadratic portrait $\mathcal{P}$, if we let $\mathcal{P}'$ be the minimal generic quadratic portrait containing $\mathcal{P}$, then $X_1(\mathcal{P})$ and $X_1(\mathcal{P}')$ are isomorphic over $\mathbb{Q}$. (See the discussion preceding Example 2.4.)

One direction of Theorem 4.1 is straightforward: For every portrait $\mathcal{P} \in \Gamma$, the curve $X_1(\mathcal{P})$ is described in at least one of the articles [39,44,50]. All the curves in those articles have genus at most 2 and at least one rational point, hence have infinitely many quadratic points. Thus, we must show that if $\mathcal{P}$ is generic quadratic but not in Γ, then $X_1(\mathcal{P})$ has only finitely many quadratic points.

To help organize the arguments in the rest of this section, we introduce some terminology:

Definition 4.3 The **cycle structure** of a portrait $\mathcal{P}$ is the nonincreasing sequence of cycle lengths appearing in $\mathcal{P}$. Note that the empty portrait has cycle structure ( ).

If K is a quadratic field and $c \in K$, then the cycle structure of $G(f_c, K)$ may contain the integer 1 at most twice and each of the integers 2, 3, and 4 at most once; for periods 1 and 2 this follows from the fact that a quadratic polynomial can have at most two fixed points and at most one 2-cycle, and for periods 3 and 4 this comes from [11, Cor. 4.16]. More precisely, the results of [11] imply that the "period at most 4" portion of the cycle structure of $G(f_c, K)$ must be (4,1,1), (4,2), or one of the following:

$$( ), \ (1, 1), \ (2), \ (3), \ (4), \ (2, 1, 1), \ (3, 1, 1), \ (3, 2). \tag{4.1}$$

Moreover, it follows from [14, Cor. 3.48] (resp., [11, Thm. 4.21]) that no portrait with both a 4-cycle and a 1-cycle (resp., 4-cycle and a 2-cycle) may be realized infinitely often as $G(f_c, K)$ for K a quadratic field and $c \in K$. For our purposes, therefore, we may exclude the cycle structures (4,1,1) and (4,2) from consideration.

By enumerating generic quadratic portraits with few vertices, one can verify that if $\mathcal{P}$ is a generic quadratic portrait which is not in Γ, then $\mathcal{P}$ has a cycle of length $n \ge 5$ or $\mathcal{P}$ properly contains a portrait in Γ_{rat} or Γ_{quad}. We handle these two possibilities separately,

showing in each case that the dynamical modular curve $X_1(\mathcal{P})$ has only finitely many quadratic points.

4.1 Points of period $n \geq 5$

If $\mathcal{P}$ is a generic portrait with a cycle of length n, then there is a dominant morphism $X_1(\mathcal{P}) \to X_1(n)$ defined over $\mathbb{Q}$. In particular, every quadratic point on $X_1(\mathcal{P})$ maps to a rational or quadratic point on $X_1(n)$, so we need only to show that if $n \geq 5$, then $X_1(n)$ has only finitely many points defined over quadratic fields; we prove this in Proposition 4.5.

For $n \geq 1$, the cyclic group C_n acts on $X_1(n)$ as follows: Given a point $(c, z) \in X_1(n)$, we also have $\sigma_n(c, z) := (c, f_c(z)) \in X_1(n)$, so σ_n defines an order-n automorphism of $X_1(n)$. We denote by $X_0(n)$ the quotient of $X_1(n)$ by this cyclic group action, which parametrizes maps f_c together with a marked *cycle* of length n. Note that $c : X_1(n) \to \mathbb{P}^1$ factors through the quotient map $X_1(n) \to X_0(n)$; to avoid confusion, we denote by c_0 the corresponding map $X_0(n) \to \mathbb{P}^1$.

For a curve X, we will denote by g_X its genus; for simplicity, for each $n \geq 1$ we will write $g_{0,n}$ for the genus of $X_0(n)$. Finally, recall that $D(n)$ denotes the degree (in z) of the polynomial $\Phi_n(c, z)$; equivalently, $D(n)$ is the degree of the morphism $c : X_1(n) \to \mathbb{P}^1$. As in Definition 2.1, we let $R(n) := D(n)/n$. Note that $R(n)$ is the degree of $c_0 : X_0(n) \to \mathbb{P}^1$ and, since $D(n) \leq 2^n$ for all $n \geq 1$, we have $R(n) \leq 2^n/n$.

Lemma 4.4 *For all $n \geq 8$, we have $g_{0,n} > R(n) + 1$.*

Proof In [38, Thm. 13], Morton gives an explicit formula for $g_{0,n}$, and with this formula one can check that the conclusion holds whenever $8 \leq n \leq 16$. Thus, we assume $n \geq 17$.

In the proof of [38, Thm. 13], Morton also provides the lower bound

$$g_{0,n} \geq \frac{3}{2} + \left(\frac{1}{4} - \frac{1}{n}\right) 2^n - (n+1)2^{n/2-1}.$$

This implies that

$$g_{0,n} - 1 > \frac{2^n}{n} \cdot \left(\frac{n}{4} - 1 - n(n+1)2^{1-n/2}\right).$$

Thus, since $R(n) = D(n)/n \leq 2^n/n$, it suffices to show that $\frac{n}{4} - 1 - n(n+1)2^{1-n/2} \geq 1$ for all $n \geq 17$. The desired inequality is equivalent to

$$(n+1)2^{3-n/2} \leq 1 - \frac{8}{n},$$

and it is a calculus exercise to show that, for all $n \geq 17$,

$$(n+1)2^{3-n/2} < \frac{1}{2} < 1 - \frac{8}{n}.$$

$\square$

Proposition 4.5 *Let $n \geq 1$.*

(a) *$X_0(n)$ has infinitely many quadratic points if and only if $n \leq 5$.*
(b) *$X_1(n)$ has infinitely many quadratic points if and only if $n \leq 4$.*

Remark 4.6 The fact that $X_0(n)$ (hence also $X_1(n)$) has only finitely many quadratic points for sufficiently large n follows from Theorem 1.8, together with [15, Thm. 1.1], which states that the gonality of $X_0(n)$ tends to infinity with n. For our purposes, however, we need the more precise statement of Proposition 4.5.

Proof of Proposition 4.5 We first prove (a). For $n \leq 4$, the curve $X_0(n)$ is isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$, hence has infinitely many quadratic points—as does the curve $X_0(5)$, which has genus 2. We now show that if $n \geq 6$, then $X_0(n)$ has finitely many quadratic points.

By Theorem 1.8, it suffices to show that for each $n \geq 6$, $X_0(n)$ does not admit a degree-2 morphism to a curve of genus at most 1. This statement was proven by Stoll [48] for $n = 6$, so we suppose that $n \geq 7$, and we let φ be a degree-d morphism to a curve C of genus $g_C \leq 1$. We claim that $d > 2$.

For $n = 7$, one can find a model for $X_0(7)$ using the same approach as Stoll for $X_0(6)$; doing so, we find a model of the form $F(c, t) = 0$ for a polynomial $F \in \mathbb{Q}[c, t]$ of degree 18 in t and degree 9 in c. In particular, the morphism $t : X_0(7) \to \mathbb{P}^1$ has degree 9.

If there does not exist an intermediate curve Z and a morphism $\psi : X_0(7) \to Z$ of degree at least 2 such that both φ and t factor through ψ, then, since $X_0(7)$ has genus 16, the Castelnuovo–Severi inequality tells us that $16 \leq dg_C + 8(d-1)$, hence $d \geq \frac{24}{g_C+8} > 2$. On the other hand, if there is such a morphism $\psi : X_0(7) \to Z$, then $\deg \psi$ must be divisible by 3, hence $d = \deg \varphi$ must be as well.

Now let $n \geq 8$. It follows from [6, §3, Thm. 3] that the Galois group of (the Galois closure of) the cover c_0 is the full symmetric group $S_{R(n)}$; in particular, c_0 does not admit a proper subcover $X_0(n) \to Z \to \mathbb{P}^1$, so we may apply the Castelnuovo–Severi inequality to c_0 and φ to get

$$g_{0,n} \leq dg_C + (R(n) - 1)(d - 1) \leq d + (R(n) - 1)(d - 1).$$

Since $R(n) - 1 < g_{0,n} - 2$ by Lemma 4.4, we have

$$g_{0,n} < d + (g_{0,n} - 2)(d - 1) = d(g_{0,n} - 1) - g_{0,n} + 2,$$

hence $d > 2$.

We now turn to part (b). For $n \leq 4$, the curve $X_1(n)$ has genus at most 2, hence has infinitely many quadratic points. It remains to show that if $n \geq 5$, then $X_1(n)$ has finitely many quadratic points. Note that this follows from (a) for all $n \geq 6$, so we need only to show that $X_1(5)$ has finitely many quadratic points. As in part (a), it suffices to show that $X_1(5)$ is not a double cover of a curve of genus at most 1. Thus, we let $\varphi : X_1(5) \to \mathbb{P}^1$ be a degree-d morphism to a curve of genus $g_C \leq 1$, and we show that $d > 2$.

A calculation in Magma [4] shows that the morphism $X_1(5) \to \mathbb{P}^1$ given by the dynatomic polynomial $\Phi_2(c, z) = z^2 + z + c + 1$ has degree 7. If φ factors through Φ_2, then $d \geq 7$. If not, then the Castelnuovo–Severi inequality applies to the morphisms φ and Φ_2, hence

$$g_{1,5} \leq dg_C + 6(d - 1).$$

The curve $X_1(5)$ has genus $g_{1,5} = 14$, and we assumed $g_C \leq 1$, so it follows that $d > 2$. □

Remark 4.7 The fact that Φ_2 has low degree on $X_1(5)$ seems related to the fact that, as polynomials in $\overline{\mathbb{Q}}[c, z]$, the dynatomic polynomials Φ_2 and Φ_5 have no common zeros (c, z). In particular, all zeros and poles of Φ_2 on $X_1(5)$ lie above ∞, which restricts the possible number of such points.

4.2 Generic quadratic portraits properly containing the portraits in Γ_{rat} and Γ_{quad}

By enumerating portraits with few vertices, one finds that any generic quadratic portrait $\mathcal{P}$ that has its cycle structure listed in (4.1), but which is not contained in Γ, must properly

Fig. 2 The portrait 10(4)
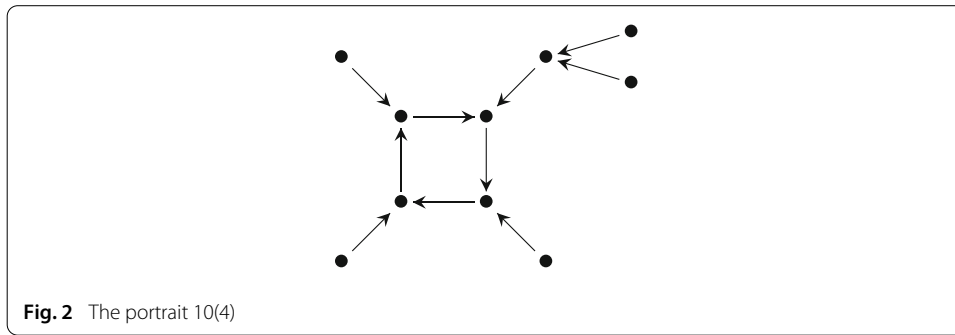
contain a portrait from Γ_{rat} or Γ_{quad}, and moreover, $\mathcal{P}$ must have a subportrait isomorphic to one of the following portraits:

$$10(1, 1)\text{a/b}, \ 10(2), \ 10(3)\text{a/b}, \ 10(4), \ 12(2, 1, 1)\text{a/b}, \ \text{or } G_n \text{ for some } 1 \le n \le 10. \qquad (4.2)$$

All portraits listed above appear in Appendix B except 10(4), which is the label we give to the subportrait of 12(4) shown in Fig. 2.

Proposition 4.8 *For each of the portraits $\mathcal{P}$ appearing in* (4.2)*, the curve $X_1(\mathcal{P})$ has only finitely many quadratic points.*

The cases $\mathcal{P} = 10(1, 1)\text{b}$ and $\mathcal{P} = 10(2)$ form the majority of the proof of Proposition 4.8. We include only the proof for 10(1, 1)b, as the argument for 10(2) is very similar.

Lemma 4.9 *Let $C \subset \text{Spec } \mathbb{Q}[x, z]$ be the curve of genus 5 defined by the equation*

$$\left(z^2 - 2(x^2 + 1)\right)^2 = 2(x^2 - 1)^2(x^3 + x^2 - x + 1).$$

Let $(c, p) \in \mathbb{A}^2(K)$ be such that p has preperiod 4 and eventual period 1 for f_c. Then there exists a point $(x, z) \in C(K)$ such that $c = -2(x^2 + 1)/(x^2 - 1)^2$.

Proof Let $q = f_c(p) = p^2 + c$, so that q has preperiod 3 (and still eventual period 1). A calculation in [44, p. 22] shows that there is an element $x \in K \smallsetminus \{\pm 1\}$ such that

$$c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2} \ \text{ and } \ q^2 = \frac{2(x^3 + x^2 - x + 1)}{(x^2 - 1)^2}.$$

Hence we have

$$2(x^3 + x^2 - x + 1) = q^2(x^2 - 1)^2 = (p^2 + c)^2(x^2 - 1)^2 = \left(\frac{p^2(x^2 - 1)^2 - 2(x^2 + 1)}{x^2 - 1}\right)^2.$$

Letting $z = p(x^2 - 1)$ we obtain

$$\left(z^2 - 2(x^2 + 1)\right)^2 = (x^2 - 1)^2 \cdot 2(x^3 + x^2 - x + 1)$$

with $x, z \in K$. Thus $(x, z) \in C(K)$.   □

Proposition 4.10 *For the portraits $\mathcal{P} = 10(1, 1)\text{b}$ and $\mathcal{P} = 10(2)$, the set of quadratic points on $X_1(\mathcal{P})$ is finite.*

Proof As mentioned above, we only give a proof for $\mathcal{P} = 10(1, 1)\text{b}$. By Lemma 4.9, it suffices to show that the curve C has only finitely many quadratic points. The latter curve admits a dominant map to the elliptic curve with Weierstrass equation

$w^2 = 2(x^3 + x^2 - x + 1)$, which is the modular curve $X_1^{\text{ell}}(11)$. Explicitly, a natural map $\varphi : C \to X_1^{\text{ell}}(11)$ is given by

$$\varphi(x, z) = \left(x, \frac{z^2 - 2(x^2 + 1)}{x^2 - 1} \right).$$

The curve $X_1^{\text{ell}}(11)$ has exactly four affine rational points, namely, $(\pm 1, \pm 2)$. Suppose that (x, z) is a quadratic point on C with field of definition K. Then $x \notin \{\pm 1\}$, so the point $\varphi(x, z)$ cannot be a rational point on $X_1(11)$. Thus $\varphi(x, z)$ is a quadratic point, and $K = \mathbb{Q}(\varphi(x, z))$. Letting

$$w = \frac{z^2 - 2(x^2 + 1)}{x^2 - 1}, \tag{4.3}$$

we therefore have $w^2 = 2(x^3 + x^2 - x + 1)$ and $K = \mathbb{Q}(x, w)$. We now consider two cases.

Suppose first that $x \in \mathbb{Q}$. Then $K = \mathbb{Q}(w)$, and by (4.3) we have $z^2 = 2(x^2+1)+(x^2-1)w$. Applying the norm map $N_{K/\mathbb{Q}}$ to this equation we obtain

$$y^2 = 4(x^2 + 1)^2 - 2(x^2 - 1)^2(x^3 + x^2 - x + 1),$$

where $y = N_{K/\mathbb{Q}}(z)$. The above equation defines a hyperelliptic curve of genus 3, and therefore has only finitely many rational solutions. We conclude that C has only finitely many quadratic points with rational x-coordinate.

Now suppose that $x \notin \mathbb{Q}$, so that $K = \mathbb{Q}(x)$. By Lemma 3.3 applied to the equation $w^2 = 2(x^3 + x^2 - x + 1)$, there is a rational number t and a point $(x_0, w_0) \in \{(\pm 1, \pm 2)\}$ such that $w = w_0 + t(x - x_0)$ and

$$x^2 + \frac{2x_0 - t^2 + 2}{2}x + \frac{2x_0^2 + t^2x_0 + 2x_0 - 2w_0t - 2}{2} = 0. \tag{4.4}$$

For each point $(x_0, w_0) \in \{(\pm 1, \pm 2)\}$ we consider the relation

$$z^2 = 2(x^2 + 1) + (x^2 - 1)(w_0 + t(x - x_0)). \tag{4.5}$$

Using (4.4) we express the right-hand side of (4.5) as a linear combination of 1 and x. Applying the norm map $N_{K/\mathbb{Q}}$ and letting $u = 2 \cdot N_{K/\mathbb{Q}}(z)$, we obtain a relation of the form $u^2 = g(t)$, where g is a polynomial of degree 7 with integral coefficients and nonzero discriminant. Each of the resulting four equations $u^2 = g(t)$ defines a hyperelliptic curve of genus 3, and therefore has only finitely many rational solutions. Since t has only finitely many possible values, (4.4) implies the same for x. Therefore C has finitely many quadratic points with quadratic x-coordinate. $\square$

Proof of Proposition 4.8 The proposition has already been proven in [14] and [11] for all of the portraits except 10(1, 1)b, 10(2), and 10(3)a/b. Moreover, Proposition 4.10 shows that the statement is true for the portraits 10(1,1)b and 10(2), so all that remains is to show that $X_1(\mathcal{P})$ has only finitely many quadratic points when $\mathcal{P} = 10(3)\text{a}$ or $\mathcal{P} = 10(3)\text{b}$.

Each of the curves $X_1(\mathcal{P})$ with $\mathcal{P} = 10(3)\text{a/b}$ has genus 9, and each admits a degree-2 map φ to the genus-2 curve $X_1(\mathcal{P}')$, where $\mathcal{P}' = 8(3)$. Now suppose we have a degree-d map $\psi : X_1(\mathcal{P}) \to C$, where C is a curve of genus $g_C \leq 1$. Then, by Proposition 3.4, either ψ factors through φ, in which case $\deg \psi > \deg \varphi = 2$, or the Castelnuovo–Severi inequality (3.1) applies to φ and ψ, in which case we have

$$4 + dg_C + (d - 1) \geq 9, \quad \text{hence } d \geq \frac{6}{g_C + 1} \geq 3.$$

It follows that $X_1(\mathcal{P})$ is not hyperelliptic or bielliptic, hence $X_1(\mathcal{P})$ has only finitely many quadratic points by Theorem 1.8. $\square$

4.3 Proof of Theorem 4.1

We now combine Propositions 4.5 and 4.8 to complete the proof of Theorem 4.1, which in turn proves one direction of Theorem 1.5.

Proof of Theorem 4.1 As mentioned previously, the fact that $X_1(\mathcal{P})$ has infinitely many quadratic points for each $\mathcal{P} \in \Gamma$ follows from the work of Walde–Russo [50], Morton [39], and Poonen [44]. Now suppose $\mathcal{P}$ is a generic quadratic portrait such that $X_1(\mathcal{P})$ has infinitely many quadratic points. Proposition 4.5 asserts that $\mathcal{P}$ cannot have a cycle of length $n \geq 5$; combining this with the paragraph following Definition 4.3, the cycle structure of $\mathcal{P}$ must be one of those appearing in (4.1). By simply enumerating all small generic quadratic portraits with the allowable cycle structures, one finds that if $\mathcal{P}$ is not contained in Γ, then $\mathcal{P}$ has a subportrait isomorphic to one of the portraits listed in (4.2), hence there is a dominant morphism $X_1(\mathcal{P}) \to X_1(\mathcal{P}')$ for some $\mathcal{P}'$ in that list. Proposition 4.8 shows that each such $X_1(\mathcal{P}')$ has only finitely many quadratic points, hence $X_1(\mathcal{P})$ does as well. □

5 Preperiodic portraits realized infinitely often over quadratic fields

In this section, we show that if $\mathcal{P} \in \Gamma$, then there are infinitely many $c \in \mathbb{Q}$ such that $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K. We also determine for which portraits $\mathcal{P}$ the same is true for infinitely many $c \in \mathbb{Q}^{(2)} \smallsetminus \mathbb{Q}$.

It follows from Theorem 4.1 that Γ is precisely the set of generic quadratic portraits that can be realized infinitely often as a *subportrait* of $G(f_c, K)$; the difficulty is in proving that we infinitely often have equality. This step requires two main tools: The first is Hilbert irreducibility, and the second is the following dynamical result giving an upper bound for the lengths of periodic cycles of maps over number fields that depends only on the primes of bad reduction of those maps; for a proof, see, for example, [43,46,51].

Proposition 5.1 *Let K be a number field, and let $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ be a prime ideal of norm q. There exists a bound $B := B(q)$ such that if $c \in K$ and $v_{\mathfrak{p}}(c) \geq 0$, then f_c has no K-rational points of period larger than B.*

We will also repeatedly use the observation that given any portrait $\mathcal{P}$ and any bound C, there are only finitely many generic portraits $\mathcal{P}'$ that are minimal (relative to inclusion) among those generic portraits containing $\mathcal{P}$ *and* having no cycles of length larger than C. This is due to the fact that there are only finitely many generic quadratic portraits with a given number of vertices.

5.1 Rational *c*-values

For any $c \in \mathbb{Q}$, there are infinitely many quadratic fields K for which $G(f_c, K) \cong G(f_c, \mathbb{Q})$. This is a consequence of Northcott's theorem: The set of preperiodic points for f_c has bounded height, hence there are only finitely many preperiodic points which are quadratic over $\mathbb{Q}$, and therefore only finitely many quadratic fields over which f_c gains *new* preperiodic points.

In particular, if a portrait $\mathcal{P}$ is realized as $G(f_c, \mathbb{Q})$ for infinitely many $c \in \mathbb{Q}$, then $\mathcal{P}$ must also be realized as $G(f_c, K)$ for infinitely many $c \in \mathbb{Q}$ and, for each such c, infinitely many quadratic fields K. The portraits realized infinitely often over $\mathbb{Q}$ are precisely the portraits in Γ_0; this is the main result of [17].

Table 1 For each pair $(\mathcal{P}, \mathcal{P}')$, there is a degree-2 morphism $X_1(\mathcal{P}) \to X_1(\mathcal{P}')$ defined over $\mathbb{Q}$

$\mathcal{P}$	4(1,1)	4(2)	6(1,1)	6(2)	8(2,1,1)
$\mathcal{P}'$	$\emptyset$	$\emptyset$	4(1,1)	4(2)	4(1,1) **or** 4(2)

A more interesting problem, then, is to determine the set of portraits $\mathcal{P}$ for which there are infinitely many $c \in \mathbb{Q}$ with $G(f_c, \mathbb{Q}) \subsetneq \mathcal{P}$ but $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K.

Proposition 5.2 *Let $\mathcal{P} \in \Gamma$. Then there exist infinitely many $c \in \mathbb{Q}$ such that $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K. Moreover, if $\mathcal{P} \in \Gamma \smallsetminus \{\emptyset, 6(3)\}$, the infinitely many $c \in \mathbb{Q}$ may be chosen so that*

$$G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \mathcal{P}.$$

Remark 5.3 The portraits $\emptyset$ and $6(3)$ are genuine exceptions to the second statement, as asserted in Theorem 1.6 and proven in Sect. 5.3. The empty portrait must be excluded simply because it has no proper subportraits. For the portrait $6(3)$ this is more subtle: Morton proved in [37, Thm. 3] that if $c_0 \in \mathbb{Q}$, then the third dynatomic polynomial $\Phi_3(c_0, z) \in \mathbb{Q}[z]$ cannot have irreducible quadratic factors over $\mathbb{Q}$. In other words, if a quadratic polynomial with rational coefficients has points of period 3 defined over a quadratic extension, then those points must be rational.

Proof of Proposition 5.2 It follows from the discussion preceding the statement of Proposition 5.2 that for both $\mathcal{P} = \emptyset$ and $\mathcal{P} = 6(3)$, which are elements of Γ_0, there are infinitely many $c \in \mathbb{Q}$ such that $G(f_c, K) \cong \mathcal{P}$ for some quadratic field K. We henceforth assume $\mathcal{P} \in \Gamma \smallsetminus \{\emptyset, 6(3)\}$ and prove the stronger statement that there are infinitely many $c \in \mathbb{Q}$ such that $G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \mathcal{P}$ for some quadratic field K.

For all $\mathcal{P} \in \Gamma \smallsetminus \{\emptyset, 6(3)\}$, there is a model for $X_1(\mathcal{P})$ of the form $y^2 = F(x)$, with $F(x) \in \mathbb{Q}[x]$ nonconstant and squarefree, such that the morphism $c : X_1(\mathcal{P}) \to \mathbb{P}^1$ factors through $x : X_1(\mathcal{P}) \to \mathbb{P}^1$. In the case that $X_1(\mathcal{P})$ has genus 0, this is because there is a proper (generic quadratic) subportrait $\mathcal{P}' \subsetneq \mathcal{P}$ for which the natural morphism

$$\pi_{\mathcal{P},\mathcal{P}'} : X_1(\mathcal{P}) \longrightarrow X_1(\mathcal{P}')$$

described in Proposition 2.6(b) has degree exactly 2; see Table 1 for the list of such pairs $(\mathcal{P}, \mathcal{P}')$. For the curves of genus 1 or 2, explicit models from [44] are provided in Appendix A. $\qquad\square$

Now fix a portrait $\mathcal{P} \in \Gamma \smallsetminus \{\emptyset, 6(3)\}$, and let $y^2 = F(x)$ be the model for $X_1(\mathcal{P})$ described in the previous paragraph. Choose any value of $x_0 \in \mathbb{Q}$, and choose a prime $p \in \operatorname{Spec} \mathbb{Z}$ of good reduction for $c : X_1(\mathcal{P}) \to \mathbb{P}^1$ such that $v_p(c(x_0)) \geq 0$. Let $B = B(p^2)$ be the bound from Proposition 5.1, let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be the generic quadratic portraits that properly contain $\mathcal{P}$ and that have no cycles of length larger than B, and for each $i = 1, \ldots, n$ let $\pi_i := \pi_{\mathcal{P}_i, \mathcal{P}} : X_1(\mathcal{P}_i) \to X_1(\mathcal{P})$ be the natural projection morphism from Proposition 2.6(b).

By Hilbert's Irreducibility Theorem, the sets

$$\{x \in \mathbb{Q} : \sqrt{F(x)} \in \mathbb{Q}\}$$

and, for each $i = 1, \ldots, n$,

$$\left\{ x \in \mathbb{Q} : \left[\mathbb{Q}\left(\pi_i^{-1}\left(x, \sqrt{F(x)} \right) \right) : \mathbb{Q} \right] \leq 2 \right\},$$

are thin subsets of $\mathbb{P}^1(\mathbb{Q})$. Since the residue class

$$[x_0]_p := \{x \in \mathbb{P}^1(\mathbb{Q}) : x \equiv x_0 \pmod{p}\}$$

is not thin, there are infinitely many $x \in [x_0]_p$ such that $K := \mathbb{Q}\left(\sqrt{F(x)}\right)$ is a quadratic field and $\left(x, \sqrt{F(x)}\right) \in X_1(\mathcal{P})(K)$ does not lift to a K-rational point on $X_1(\mathcal{P}_i)$ for any $i = 1, \ldots, n$.

Now let $c = c(x)$ for any of the infinitely many x from the previous paragraph. Excluding at most finitely many $x \in [x_0]_p$, we may assume that $G(f_c, K)$ is a generic quadratic portrait. Since c lifts to a quadratic point Q on $X_1(\mathcal{P})$, we have

$$G(f_c, \mathbb{Q}) \subsetneq \mathcal{P} \subseteq G(f_c, K).$$

On the other hand, since c does *not* lift to a quadratic point on $X_1(\mathcal{P}_i)$ for any $i = 1, \ldots, n$, the portrait $G(f_c, K)$ is either isomorphic to $\mathcal{P}$ or contains a cycle of length greater than B. Finally, since $v_p(c) \geq 0$, the portrait $G(f_c, K)$ has no cycles of length greater than B, and thus we have

$$G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \mathcal{P}.$$

5.2 Quadratic *c*-values

The purpose of this section is to determine which portraits $\mathcal{P}$ may be realized infinitely often as $G(f_c, \mathbb{Q}(c))$ for some quadratic algebraic number c. We begin with the simplest case, namely, where $X_1(\mathcal{P})$ has genus 0.

Proposition 5.4 *Suppose $\mathcal{P} \in \Gamma_0$, and let $K/\mathbb{Q}$ be a quadratic field. Then there are infinitely many $c \in K \smallsetminus \mathbb{Q}$ such that $G(f_c, K) \cong \mathcal{P}$.*

Proof Let $X := X_1(\mathcal{P}) \cong_{\mathbb{Q}} \mathbb{P}^1$. Choose an *inert* prime $p \in \operatorname{Spec}\mathbb{Z}$ such that $c : X \to \mathbb{P}^1$ has good reduction at p and such that $p > D := \deg(c : X \to \mathbb{P}^1)$. Let $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ be the unique prime lying above p. The good reduction condition implies that the mod-$\mathfrak{p}$ reduction $\tilde{c}$ of the map $c : X \to \mathbb{P}^1$ has degree D, and the condition that $D < p$ implies that $\tilde{c}$ cannot map all of $\mathbb{P}^1(\mathbb{F}_{p^2})$ to $\mathbb{P}^1(\mathbb{F}_p)$. In other words, we may choose a point $P_0 \in X(K)$ such that $c(\widetilde{P_0}) = \tilde{c}(\widetilde{P_0}) \in \mathbb{P}^1(\mathbb{F}_{p^2}) \smallsetminus \mathbb{P}^1(\mathbb{F}_p)$. Note that since $\infty \in \mathbb{P}^1(\mathbb{F}_p)$ and $c(\widetilde{P_0}) \notin \mathbb{P}^1(\mathbb{F}_p)$, we must have $v_{\mathfrak{p}}(c(P_0)) \geq 0$. Then, for any P in the residue class $[P_0]_{\mathfrak{p}}$, the image $c(P)$ must be in $K \smallsetminus \mathbb{Q}$, and $v_p(c(P)) \geq 0$. In particular, for all $P \in [P_0]_{\mathfrak{p}}, f_{c(P)}$ has no K-rational points of period greater than $B = B(p^2)$, the bound from Proposition 5.1.

Let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be the complete list of generic quadratic portraits that minimally contain $\mathcal{P}$ and which have no cycles of length larger than B, and for each $i = 1, \ldots, n$ let

$$\pi_i := \pi_{\mathcal{P}_i, \mathcal{P}} : X_1(\mathcal{P}_i) \longrightarrow \mathbb{P}^1$$

be the morphism from Proposition 2.6(b). If $P \in [P_0]_{\mathcal{P}}$ and $G(f_{c(P)}, K)$ properly contains $\mathcal{P}$, then $G(f_{c(P)}, K)$ must contain one of the portraits $\mathcal{P}_i$. By Hilbert irreducibility, the set

$$[P_0]_{\mathfrak{p}} \smallsetminus \bigcup_{i=1}^n \pi_i\big(X_1(\mathcal{P}_i)(K)\big)$$

is infinite. Thus, there are infinitely many $c \in K \smallsetminus \mathbb{Q}$ such that $G(f_c, K) \cong \mathcal{P}$. □

We now consider the portraits $\mathcal{P} \in \Gamma \smallsetminus \Gamma_0$; that is, the portraits for which $X_1(\mathcal{P})$ has genus 1 or 2. We begin with a useful consequence of Theorem 4.1.

Corollary 5.5 *Let $\mathcal{P}$ be a generic quadratic portrait such that $X_1(\mathcal{P})$ has positive genus. If $\mathcal{P}'$ is any generic quadratic portrait properly containing $\mathcal{P}$, then $X_1(\mathcal{P}')$ has finitely many quadratic points.*

Proof If $X_1(\mathcal{P}')$ has infinitely many quadratic points, then so does $X_1(\mathcal{P})$, and therefore both $\mathcal{P}$ and $\mathcal{P}'$ are elements of Γ. By simply inspecting the portraits in Γ, the only way we can have $\mathcal{P}, \mathcal{P}' \in \Gamma$ and $\mathcal{P} \subsetneq \mathcal{P}'$ is if $\mathcal{P} \in \Gamma_0$; that is, if $X_1(\mathcal{P})$ has genus 0.   □

Combining Corollary 5.5 and Proposition 5.1 gives us the following sufficient condition for $\mathcal{P}$ to be realized infinitely often as $G(f_c, K)$ over quadratic fields K. For an algebraic curve X defined over a field k, we denote by $X(k, 2)$ the set of all points on X of degree at most 2 over k. For a prime $p \in \operatorname{Spec} \mathbb{Z}$ and an element $\alpha \in \overline{\mathbb{Q}}$, the phrase "$v_p(\alpha) \geq 0$" should be read to mean "there exists some extension $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_{\mathbb{Q}(\alpha)}$ of p such that $v_{\mathfrak{p}}(\alpha) \geq 0$."

Lemma 5.6 *Let $\mathcal{P}$ be a generic quadratic portrait such that $X_1(\mathcal{P})$ has genus 1 or 2. Fix a prime $p \in \operatorname{Spec} \mathbb{Z}$, and consider the set*

$$\mathcal{S}_{p,\mathcal{P}} := \{\beta \in X_1(\mathcal{P})(\mathbb{Q}, 2) : v_p(c(\beta)) \geq 0\}.$$

For all but finitely many $\beta \in \mathcal{S}_{p,\mathcal{P}}$, we have $G(f_{c(\beta)}, \mathbb{Q}(\beta)) \cong \mathcal{P}$.

Proof Suppose $\beta \in \mathcal{S}_{p,\mathcal{P}}$, set $c := c(\beta)$, and let $K := \mathbb{Q}(\beta)$. Removing at most finitely many points $\beta \in \mathcal{S}_{p,\mathcal{P}}$, we may assume that $G(f_c, K)$ is generic quadratic. It follows that $G(f_c, K)$ has a subportrait isomorphic to $\mathcal{P}$, since $\beta \in X_1(\mathcal{P})(K)$.

Let $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ be a prime lying above p. Since $\mathfrak{p}$ has norm at most p^2, the map f_c has no K-rational points of period larger than $B := B(p^2)$. Thus, as explained following Proposition 5.1, if $G(f_c, K) \not\cong \mathcal{P}$, then $G(f_c, K)$ must contain one of the finitely many portraits $\mathcal{P}_1, \ldots, \mathcal{P}_n$ properly containing $\mathcal{P}$. But each of the curves $X_1(\mathcal{P}_i)$ has only finitely many quadratic points by Corollary 5.5; this completes the proof.   □

Proposition 5.7 *Let $\mathcal{P} \in \Gamma_{\mathrm{rat}}$. If K is a quadratic field and $c \in K$ satisfies $G(f_c, K) \cong \mathcal{P}$, then $c \in \mathbb{Q}$.*

Proof For $\mathcal{P} \in \{8(4), 10(3, 1, 1), 10(3, 2)\}$, this follows immediately from Theorems 3.16, 3.25, and 3.28 of [14]. For the remaining portraits $\mathcal{P}$—namely, 8(1,1)a and 8(2)a—the proofs are similar, so we only provide the details for 8(1,1)a.

Let $\mathcal{P} = 8(1, 1)$a. As shown in Appendix A, the curve $X_1(\mathcal{P})$ is isomorphic to the elliptic curve E with affine model $y^2 = x^3 - x^2 + x$, which is the curve labeled 24A4 in [10] and 24.a5 in [49]. We claim that if $P = (x, y)$ is a quadratic point on E, then $c(P) = -\frac{(x^2+1)^2}{4x(x-1)^2} \in \mathbb{Q}$. This is certainly the case if $x \in \mathbb{Q}$, so assume that x is quadratic.

By Lemma 3.3, there exist $P_0 = (x_0, y_0) \in E(\mathbb{Q}) \smallsetminus \infty$ and $t \in \mathbb{Q}$ such that

$$x^2 + (x_0 - t^2 - 1)x + (x_0^2 + t^2 x_0 - x_0 - 2y_0 t + 1) = 0. \tag{5.1}$$

The only affine rational points (x_0, y_0) on E are $(0, 0)$ and $(1, \pm 1)$, and for each of these points we can use (5.1) to rewrite $c(P)$ as a function of t and x which has degree at most 1 in x. For the points $(0, 0)$, $(1, 1)$, and $(1, -1)$, respectively, we get

$$c = -\frac{(t^2 + 1)^2}{4(t - 1)(t + 1)},$$

$$c = -\frac{t^2\left(t^2 - 2t + 2\right)}{4(t-1)^2}, \text{ and}$$

$$c = -\frac{t^2\left(t^2 + 2t + 2\right)}{4(t+1)^2}.$$

In any case, since $t \in \mathbb{Q}$, we must also have $c \in \mathbb{Q}$. $\qquad\square$

Proposition 5.8 *For all* $\mathcal{P} \in \Gamma_0 \cup \Gamma_{\text{quad}}$ *there exist infinitely many* $c \in \mathbb{Q}^{(2)}$ *such that*

$$G(f_c, \mathbb{Q}(c)) \cong \mathcal{P}.$$

Proof For the portraits in Γ_0, this follows from Proposition 5.4. The proofs for 8(1,1)b and 8(2)b (resp., 10(2,1,1)a and 10(2,1,1)b) are very similar, so we only provide the details for

8(1,1)b, 10(2,1,1)a, and 8(3).

First, let $\mathcal{P}$ be the portrait 8(1,1)b. Appendix A shows that $X_1(\mathcal{P})$ is isomorphic to the curve X with affine model $y^2 = 2(x^3 + x^2 - x + 1)$, with $c : X \to \mathbb{P}^1$ given by

$$c = -\frac{2(x^2 + 1)}{(x+1)^2(x-1)^2}.$$

Set $P_0 = (x_0, y_0) := (1, 2) \in X(\mathbb{Q})$. For $t \in \mathbb{Q}$, the line $y - 2 = t(x - 1)$ intersects the curve X at P_0 and two additional points P_t and $\overline{P}_t$. Since t and P_0 are rational, either P_t and $\overline{P}_t$ are rational as well, or P_t and $\overline{P}_t$ are quadratic conjugates. Since $X(\mathbb{Q})$ is finite, we may, at the expense of excluding finitely many t, assume that P_t and $\overline{P}_t$ are quadratic Galois conjugates. Let $K := \mathbb{Q}(P_t)$, and let τ be the nontrivial element of $\text{Gal}(K/\mathbb{Q})$. With this setup, we have $P_t + \overline{P}_t = -P_0 \neq \mathcal{O}$, so $y(P_t) \neq -y(\overline{P}_t) = -y(P_t)^\tau$, and therefore $x(P_t) \notin \mathbb{Q}$. By calculating the intersection of $y - 2 = t(x - 1)$ with the affine curve X, we find that the minimal polynomial of $x(P_t)$ must be

$$x^2 - \frac{t^2 - 4}{2}x + \frac{t^2 - 4t + 2}{2}.$$

Thus, we may rewrite $c(P_t)$ as

$$c(P_t) = \frac{t+2}{8(t-2)}x(P_t) - \frac{t^5 - 10t^3 + 8t^2 + 8t + 32}{16(t-2)^2 t}.$$

Finally, for any $t \in \mathbb{Q}$ with $t \equiv 1 \pmod 3$, we see that $x(P_t)$ and $c(P_t)$ are integral at $p = 3$, so $P_t \in S_{3,\mathcal{P}}$. By Lemma 5.6, we conclude that there are infinitely many quadratic c with $G(f_c, \mathbb{Q}(c)) \cong \mathcal{P}$.

Next, we let $\mathcal{P}$ be the portrait 10(2,1,1)a, and we take X to be the curve defined by $y^2 + xy + y = x^3 - x^2 - x$ with map $c : X \to \mathbb{P}^1$ given by

$$c = \frac{x-2}{4x(x-1)}y - \frac{x^4 - x^3 + 3x - 1}{4x^2(x-1)}.$$

By Hilbert irreducibility, there are infinitely many points on X with $x \in \mathbb{Q}, x \equiv 2 \pmod 3$, and $y \notin \mathbb{Q}$. For all such points $P = (x, y)$, $c(P)$ must be quadratic, and we have $P \in \mathcal{S}_{3,\mathcal{P}}$. The desired conclusion again follows from Lemma 5.6.

Finally, we let $\mathcal{P}$ be the portrait 8(3). Let X be the curve $y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$ with $c : X \to \mathbb{P}^1$ given by

$$c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}.$$

The curve X has two rational points at infinity; we denote these by ∞^+ and ∞^-. These two points are transposed by the hyperelliptic involution $\iota : X \to X$ given by $\iota(x, y) = (x, -y)$.

Let J be the Jacobian of the genus-2 curve X. For a thorough treatment of the arithmetic of genus-2 curves, we recommend [8]; here, we just summarize the necessary properties. Points on J correspond to degree-0 divisor classes on X. Moreover, by the Riemann–Roch theorem, every nontrivial divisor class can be written *uniquely* as

$$\{P, Q\} := [P + Q - \infty^+ - \infty^-]$$

with $P, Q \in X$ and $Q \neq \iota(P)$, up to swapping P and Q. (The trivial class $\mathcal{O}$ is equal to $\{P, \iota(P)\}$ for all $P \in X$.) A point $\{P, Q\} \neq \mathcal{O}$ is rational if and only if either P and Q are both rational themselves, or P and Q are Galois-conjugate quadratic points.

Fix the point

$$P_0 := \left(-\frac{1}{4}\left(1 + \sqrt{-15}\right), -\frac{1}{16}\left(17 + 9\sqrt{-15}\right) \right) \in X(\mathbb{Q}, 2),$$

for which we have $c(P_0) = \frac{1}{48}\left(7 + 8\sqrt{-15}\right) \notin \mathbb{Q}$. If we let

$$\overline{P}_0 := \left(-\frac{1}{4}\left(1 - \sqrt{-15}\right), -\frac{1}{16}\left(17 - 9\sqrt{-15}\right) \right)$$

be the Galois conjugate of P_0, then $\mathcal{D}_0 := \{P_0, \overline{P}_0\} \in J(\mathbb{Q})$. Note that $\overline{P}_0 \neq \iota(P_0)$, so $\mathcal{D}_0 \neq \mathcal{O}$. Poonen showed in [44, Prop. 1] that $J(\mathbb{Q}) \cong \mathbb{Z}$, so $\mathcal{D}_0$ has infinite order.

The curve X (hence also its Jacobian J) has good reduction at the prime $p = 7$. A straightforward computation (e.g., in Magma) shows that the reduction $\widetilde{\mathcal{D}}_0 \in J(\mathbb{F}_7)$ has order 21, so $\mathcal{D}_n := (1 + 21n)\mathcal{D}_0 \equiv \mathcal{D}_0 \pmod{7}$ for all $n \in \mathbb{Z}$. For each n we write $\mathcal{D}_n = \{P_n, \overline{P}_n\}$ with $P_n \equiv P_0 \pmod{7}$ and $\overline{P}_n \equiv \overline{P}_0 \pmod{7}$. We claim that $P_n \in \mathcal{S}_{7,\mathcal{P}}$ for all $n \in \mathbb{Z}$, from which the result follows by Lemma 5.6.

Since $-15 \equiv -1 \pmod{7}$ is not a square in $\mathbb{F}_7$, the reduction $\widetilde{P}_0$ is quadratic over $\mathbb{F}_7$, thus the same is true for $\widetilde{P}_n$ for all $n \in \mathbb{Z}$. This implies that P_n is quadratic over $\mathbb{Q}$ for all n.

The map $c : X \to \mathbb{P}^1$ has good reduction at $p = 7$, so $P_n \equiv P_0 \pmod{7}$ implies that $c(P_n) \equiv c(P_0) \pmod{7}$. Arguing as in the previous paragraph, we conclude that $c(P_n)$ is quadratic over $\mathbb{Q}$. Finally, we note that since $c(P_n) \equiv c(P_0) \not\equiv \infty \pmod{7}$, we have $v_7(c(P_n)) \geq 0$, so $P_n \in \mathcal{S}_{7,\mathcal{P}}$. □

5.3 Proofs of Theorems 1.6 and 1.7

Proof of Theorem 1.6 That (ii) implies (i) is precisely the second statement in Proposition 5.2, so it remains only to show that (i) implies (ii).

Assume there are infinitely many $c \in \mathbb{Q}$ such that $G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \mathcal{P}$ for some quadratic field K. Every such occurrence of $\mathcal{P}$ as $G(f_c, K)$ yields a quadratic point on $Y_1(\mathcal{P})$, so there are infinitely many quadratic points on $X_1(\mathcal{P})$. Thus $\mathcal{P} \in \Gamma$ by Theorem 4.1.

All that remains for us to show is that $\mathcal{P}$ cannot be isomorphic to $\emptyset$ or 6(3). Certainly one cannot have $G(f_c, \mathbb{Q}) \subsetneq G(f_c, K) \cong \emptyset$, so we need only show that if $c \in \mathbb{Q}$ and K is a quadratic field with $G(f_c, K) \cong 6(3)$, then in fact $G(f_c, \mathbb{Q}) \cong 6(3)$.

Supposing that $G(f_c, K) \cong 6(3)$, the map f_c then has a period-3 point $\alpha \in K$, and the six K-rational preperiodic points prescribed by the portrait 6(3) are $\pm\alpha$, $\pm f_c(\alpha)$, and $\pm f_c^2(\alpha)$. It therefore suffices to show that $\alpha \in \mathbb{Q}$.

Let τ be the nontrivial element of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Since f_c is defined over $\mathbb{Q}$, α^τ is also a K-rational point of period 3, hence lies in the cycle $\{\alpha, f_c(\alpha), f_c^2(\alpha)\}$ (because

the portrait 6(3) has only one 3-cycle[2]). Write $\alpha^\tau = f_c^k(\alpha)$ for some $k \in \{0, 1, 2\}$. Then

$$\alpha = (\alpha^\tau)^\tau = f_c^k(\alpha^\tau) = f_c^{2k}(\alpha).$$

Since α has exact period 3, this implies that $k = 0$; that is, $\alpha^\tau = \alpha$. Thus $\alpha \in \mathbb{Q}$, and therefore $G(f_c, \mathbb{Q}) \cong 6(3)$.   □

Proof of Theorem 1.7 First suppose that (i) holds; i.e., there are infinitely many $c \in \mathbb{Q}^{(2)} \smallsetminus \mathbb{Q}$ such that $G(f_c, \mathbb{Q}(c)) \cong \mathcal{P}$. The curve $X_1(\mathcal{P})$ then has infinitely many quadratic points, and therefore $\mathcal{P} \in \Gamma$ by Theorem 4.1. By Proposition 5.7, we must have

$$\mathcal{P} \in \Gamma \smallsetminus \Gamma_{\text{rat}} = \Gamma_0 \cup \Gamma_{\text{quad}}.$$

Thus, (i) implies (ii). The converse is precisely Proposition 5.8.   □

6 Fields of definition of quadratic points

In this section we address the question of whether the existence of a given preperiodic portrait over a given quadratic field has implications regarding standard arithmetic invariants of that field. In particular, we focus on the portraits that occur infinitely often over quadratic fields, namely those in the set Γ.

To be precise, we are interested in arithmetic invariants of the fields of definition of quadratic points on dynamical modular curves $X_1(\mathcal{P})$. To partially justify the transition from *realizations of portraits* to simply *points on dynamical modular curves*, we begin by proving the following result:

Proposition 6.1 *For a number field K and a generic quadratic portrait $\mathcal{P}$, the following are equivalent:*

  (i)   *There exist infinitely many $c \in K$ such that $G(f_c, K) \cong \mathcal{P}$.*
  (ii) *The curve $X_1(\mathcal{P})$ has infinitely many K-rational points.*

Proof That (i) implies (ii) is immediate from the definition of $X_1(\mathcal{P})$, so suppose that $X_1(\mathcal{P})(K)$ is infinite. Since $X_1(\mathcal{P})$ is irreducible (see Proposition 2.6(a)), this implies that $X_1(\mathcal{P})$ is isomorphic over K either to $\mathbb{P}^1$ or to an elliptic curve.

In the former case, the result follows from essentially the same proof as for Proposition 5.4. In fact, the appropriate modification of that proof shows that there are infinitely many $c \in K$ such that $\mathbb{Q}(c) = K$ and such that $G(f_c, K) \cong \mathcal{P}$.

In the latter case, choose a non-torsion point $Q_0 \in X_1(\mathcal{P})(K)$, and choose a prime $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ of good reduction for the morphism $c : X_1(\mathcal{P}) \to \mathbb{P}^1$ such that $\nu_{\mathfrak{p}}(Q_0) \geq 0$. Since Q_0 is non-torsion, there are infinitely many points $Q \in X_1(\mathcal{P})(K)$ such that $Q \equiv Q_0 \pmod{\mathfrak{p}}$, and since the morphism c has good reduction at $\mathfrak{p}$, we have $c(Q) \equiv c(Q_0) \pmod{\mathfrak{p}}$ for every such Q. In particular, we have infinitely many $Q \in X_1(\mathcal{P})(K)$ such that $\nu_{\mathfrak{p}}(c(Q)) \geq 0$, so the desired result follows from Lemma 5.6.   □

We now move on to a result concerning the splitting of rational primes in the quadratic fields over which the portrait 10(3, 1, 1) is realized as a preperiodic portrait. This example is included in order to illustrate our methods, but similar reasoning can be applied to any portrait in Γ for which the corresponding modular curve is hyperelliptic.

---

[2]In fact, if K is any quadratic field and $c \in K$, then f_c has at most one 3-cycle defined pointwise over K. This follows from [37, Thm. 3] when $c \in \mathbb{Q}$ and [11, Thm. 4.5] in general.

As noted in [44], the dynamical modular curve corresponding to the portrait 10(3, 1, 1) is isomorphic to $X_1^{\mathrm{ell}}(18)$. If K is the field of definition of a quadratic point on this curve, Kenku and Momose [27, Prop. 2.4] show that

- either 2 splits or 3 does not split in K;
- 3 is not inert in K; and
- 5 and 7 are unramified in K.

In what follows, for every polynomial $f \in \mathbb{Z}[x]$, we denote by π_f the set of all integer primes p such that f does not have a root modulo p. Extending the results of Kenku and Momose, we prove the following. (Note that this proves Theorem 1.10.)

Theorem 6.2 *Let K be a quadratic field such that $G(f_c, K) \cong 10(3, 1, 1)$ for some $c \in K$. Then the prime 2 splits in K, 3 is not inert in K, and letting*

$$f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1,$$

every prime in the set π_f (which includes 5 and 7) is unramified in K. Moreover, π_f has Dirichlet density $13/18$.

For every nonzero rational number r, we let $\mathrm{sqf}(r)$ denote the squarefree part of r, i.e., the unique squarefree integer d such that r/d is the square of a rational number.

Lemma 6.3 *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of even degree, and let p be an odd prime. If $p \in \pi_f$, then p is unramified in every quadratic field of the form $\mathbb{Q}(\sqrt{f(r)})$ with $r \in \mathbb{Q}$.*

Proof Given a quadratic field $K = \mathbb{Q}(\sqrt{f(r)})$, we must show that p does not divide the discriminant of K. Let $D = \mathrm{sqf}(f(r))$, so that $K = \mathbb{Q}(\sqrt{D})$. Since p is odd, it suffices to show that p does not divide D. Set $g(x, y) = y^{2k} f(x/y) \in \mathbb{Z}[x, y]$, where $\deg(f) = 2k$, and write $r = n/d$ with $\gcd(n, d) = 1$. Then $D = \mathrm{sqf}(g(n, d))$, so that

$$g(n, d) = Ds^2, \quad s \in \mathbb{Z}.$$

We now consider two cases. If $d \equiv 0 \pmod{p}$, then the above equation can be reduced modulo p to obtain $n^{2k} \equiv Ds^2 \pmod{p}$. Since p cannot divide n (given that n and d are coprime), we conclude that p does not divide D, as required.

Suppose now that $d \not\equiv 0 \pmod{p}$. We can then consider the equation $d^{2k} f(n/d) = Ds^2$ as taking place in the ring $\mathbb{Z}_p$. If $p \mid D$, then reducing modulo p we obtain $f(n/d) \equiv 0 \pmod{p}$, contradicting the hypothesis that f has no root modulo p. Therefore p cannot divide D.   □

Proof of Theorem 6.2 By [14, Thm. 3.25], we have $K = \mathbb{Q}(\sqrt{f(r)})$ for some $r \in \mathbb{Q} \smallsetminus \{0, -1\}$. Writing $r = n/d$ in lowest terms, it follows that $K = \mathbb{Q}(\sqrt{g(n, d)})$, where

$$g(n, d) := d^6 f(n/d) = n^6 + 2n^5 d + 5n^4 d^2 + 10n^3 d^3 + 10n^2 d^4 + 4nd^5 + d^6.$$

We claim that $g(n, d) \equiv 1 \pmod{8}$. If n, d are both odd, then

$$g(n, d) \equiv 1 + 2nd + 5 + 10nd + 10 + 4nd + 1 = 17 + 16nd \equiv 1 \pmod{8}.$$

If n is even and d is odd, then $g(n, d) \equiv d^6 \equiv 1 \pmod{8}$. If n is odd and d is even, then $g(n, d) \equiv 1 + 2nd + 5d^2 \pmod{8}$. Writing $n = 2k + 1$ for some integer k we see that

$$g(n, d) \equiv 5d^2 + 2d + 1 \equiv (d + 1)^2 \equiv 1 \pmod{8},$$

which proves the claim. Letting $D = \text{sqf}(g(n, d))$, the fact that $g(n, d) \equiv 1 \pmod 8$ implies that $D \equiv 1 \pmod 8$ and therefore 2 splits in $\mathbb{Q}(\sqrt{D}) = K$.

Similar reasoning shows that $g(n, d)$ is congruent to either 0 or 1 modulo 3. Considering all possible values of n and d modulo 9, we find that if $g(n, d)$ is divisible by 9, then n and d are both divisible by 3, which is a contradiction; hence $9 \nmid g(n, d)$. Writing $g(n, d) = Ds^2$ for some integer s, this implies that s is not divisible by 3, and therefore $g(n, d) \equiv D \pmod 3$. Hence, D is congruent to 0 or 1 modulo 3, and therefore 3 is not inert in K.

A computation in Magma based on [29, Thm. 2.1] shows that π_f has Dirichlet density 13/18. Finally, Lemma 6.3 implies that every odd prime in π_f is unramified in K, and we have already shown that 2 is unramified in K.   □

An argument very similar to the proof of Theorem 6.2 yields the following result, in which the relevant dynamical modular curve is known to be isomorphic to $X_1^{\text{ell}}(13)$.

Theorem 6.4 *Let K be a quadratic field such that $G(f_c, K) \cong 10(3, 2)$ for some $c \in K$. Then the prime 2 splits in K, and every prime in π_f is unramified in K, where*

$$f(x) = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1.$$

Moreover, the set π_f has Dirichlet density 13/18.

The results stated in Theorem 6.2, Lemma 6.3, and Theorem 6.4 initially appeared in the second author's thesis [28], where the curves are considered as classical modular curves rather than dynamical modular curves.

Our next result concerns the curve $X_1^{\text{ell}}(16)$, which is isomorphic to the modular curve for the portrait 8(4); see Section 3.7 of [14]. In contrast to Theorems 6.2 and 6.4, we show that the discriminants of quadratic fields defined by points on $X_1^{\text{ell}}(16)$ are not restricted to any residue class. (Note that this proves Theorem 1.9(a).)

Theorem 6.5 *Let $\mathcal{P}$ denote the portrait 8(4). For every prime integer p and every residue class $\mathfrak{c} \in \mathbb{Z}/p\mathbb{Z}$, there exist infinitely many squarefree integers $d \in \mathfrak{c}$ such that the curve $X_1(\mathcal{P})$ has a quadratic point defined over the field $\mathbb{Q}(\sqrt{d})$.*

For the proof of the theorem we use the methods of [30] and [31]; the following lemma, which follows from Proposition 14 in [31], collects the main tools to be used.

Lemma 6.6 *Let $f \in \mathbb{Z}[x]$ be a squarefree polynomial of degree at least 3, and such that every irreducible factor of f has degree at most 6. Let*

$$\mathcal{S}(f) = \{\text{sqf}(f(x)) : x \in \mathbb{Q} \text{ and } f(x) \neq 0\}.$$

Let D be the largest integer dividing all integer values of f. Fix a prime p such that f has an irreducible factor whose discriminant is not divisible by p, and let $\varepsilon = \varepsilon_p \in \{0, 1\}$ be the parity of $\text{ord}_p(D)$. Finally, for $\mathfrak{c} \in \mathbb{Z}/p\mathbb{Z}$ and $v \in \mathbb{Z}$, define a statement $\sigma(p, \mathfrak{c}, v)$ by

$$\sigma(p, \mathfrak{c}, v) : \begin{cases} \text{There exist } h \in \mathfrak{c} \text{ and } x_0, y_0 \in \mathbb{Z} \text{ satisfying} \\ \bullet \ \ hy_0^2 \equiv f(x_0) \pmod{p^{2(v+\varepsilon)+1}} \text{ and} \\ \bullet \ \ \text{ord}_p(y_0) = v + \varepsilon. \end{cases} \tag{6.1}$$

Suppose $\mathfrak{c}$ is nonzero and $\sigma(p, \mathfrak{c}, v)$ holds for some $v \geq 0$. Then the set $\mathcal{S}(f) \cap \mathfrak{c}$ is infinite.

Proof of Theorem 6.5 By [39, p. 93], the curve $X_1(\mathcal{P})$ is hyperelliptic and has an affine model given by $y^2 = f(x)$, where $f(x) = -x(x^2 + 1)(x^2 - 2x - 1)$.

In order to prove the theorem it suffices to show that, for every prime p and residue class $\mathfrak{c} \in \mathbb{Z}/p\mathbb{Z}$, the set $\mathcal{S}(f) \cap \mathfrak{c}$ is infinite. Indeed, if d belongs to this set, we may write $dy_0^2 = f(x_0)$ for some rational numbers x_0, y_0 with $y_0 \neq 0$. The pair $(x_0, y_0\sqrt{d})$ then represents a quadratic point on $X_1(\mathcal{P})$ whose field of definition is $\mathbb{Q}(\sqrt{d})$. Hence, the theorem follows.

In the notation of Lemma 6.6, for the above polynomial $f(x)$ we have $D = 2$; moreover, the irreducible factor x of $f(x)$ has discriminant 1, which is coprime to every prime p. It follows in particular that

$$
\varepsilon_p = \begin{cases} 0 & \text{if } p \text{ is odd,} \\ 1 & \text{if } p = 2. \end{cases}
$$

Fix a prime p. For the class $\mathfrak{c} = 0 \in \mathbb{Z}/p\mathbb{Z}$, Theorem 2.1 in [30] implies that the set $\mathcal{S}(f) \cap \mathfrak{c}$ is infinite, as desired. (When $p = 2$, the hypotheses of the cited theorem are not all satisfied, but the proof still applies.) Next, we claim that

for every nonzero $\mathfrak{c} \in \mathbb{Z}/p\mathbb{Z}$, either $\sigma(p, \mathfrak{c}, 0)$ or $\sigma(p, \mathfrak{c}, 1)$ must hold.

Assuming this claim for the moment, Lemma 6.6 implies that the set $\mathcal{S}(f) \cap \mathfrak{c}$ is infinite, completing the proof of the theorem.

To prove the claim we consider first the case $p = 2$: taking $\mathfrak{c} = 1$, the statement $\sigma(p, \mathfrak{c}, 1)$ can be shown to hold by setting $(h, x_0, y_0) = (1, 16, 4)$ in (6.1). The remainder of the proof is divided into three cases.

Case $p \le 5$: Taking $p = 3$, we check that $\sigma(p, \mathfrak{c}, 1)$ holds for $\mathfrak{c} = 1, 2$ by using the tuples

$$(h, x_0, y_0) = (1, 9, 3) \quad \text{and} \quad (h, x_0, y_0) = (2, 18, 3).$$

Similarly, taking $p = 5$, we check that $\sigma(p, \mathfrak{c}, 1)$ holds for $\mathfrak{c} = 1, 2, 3, 4$, respectively, by using the following tuples (h, x_0, y_0):

$$(1, 25, 5), \ (2, 18, 5), \ (3, 75, 5), \ (4, 7, 5).$$

In the remaining two cases we show that $\sigma(p, \mathfrak{c}, 0)$ holds. For $r \in \mathfrak{c}$, let X_r be the hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $ry^2 = f(x)$. Since $\varepsilon_p = 0$, the statement $\sigma(p, \mathfrak{c}, 0)$ is equivalent to the requirement that X_r have an affine point $(x_0, y_0) \in X_r(\mathbb{F}_p)$ with $y_0 \neq 0$; we refer to such points as *nontrivial* points on X_r. Thus, it remains to show that X_r has at least one nontrivial point.

Case $7 \le p \le 23$: A straightforward search for points verifies that $\#X_r(\mathbb{F}_p) \ge 7$ for every nonzero $r \in \mathbb{F}_p$. (Note that it suffices to check this for just two values of r, one in each square class modulo p.) The number of affine points $(x_0, y_0) \in X_r(\mathbb{F}_p)$ having $y_0 = 0$ is at most 5, so there must exist at least one nontrivial point in $X_r(\mathbb{F}_p)$, as required.

Case $p \geq 29$: For $r \in \mathbb{F}_p \smallsetminus 0$, the curve X_r has genus 2, so the Hasse–Weil bound yields

$$\#X_r(\mathbb{F}_p) \geq \lfloor p + 1 - 4\sqrt{p} \rfloor \geq 7.$$

The same reasoning as in the previous case implies that X_r has a nontrivial $\mathbb{F}_p$-point.   □

We end the paper by proving Theorem 1.9(b).

Proposition 6.7 *Let* $\mathcal{P} = 8(4)$. *There exist infinitely many imaginary quadratic fields* K *with class number divisible by* 10*, such that* $X_1(\mathcal{P})$ *has a quadratic point defined over* K.

Proof As noted earlier, the curve $X_1(\mathcal{P})$ is isomorphic to $X_1^{\mathrm{ell}}(16)$. The result follows from [21, Cor. 3.2], since the Jacobian $J_1(16)$ has a rational torsion point of order 10.   □

Remark 6.8 Experimental evidence supports a statement stronger than Proposition 6.7: for *every* imaginary quadratic field $K \neq \mathbb{Q}(\sqrt{-15})$ that is the field of definition of a point on $X_1(\mathcal{P})$, the class number of K is divisible by 10. One approach to proving this is suggested by the methods of [2,21]; however, the required computational tools (in particular, for computing quotients of abelian varieties) do not seem to be presently available.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Author details
[1] Department of Mathematics, Oklahoma State University, Stillwater, OK 74078, USA,
[2] San José, Costa Rica.

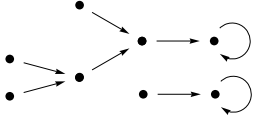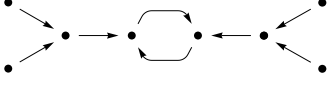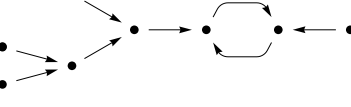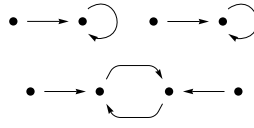## Appendix A: Dynamical modular curves of genera 1 and 2
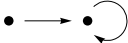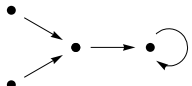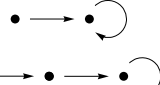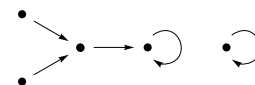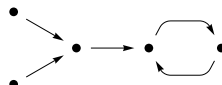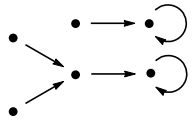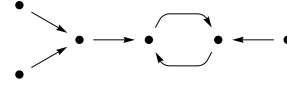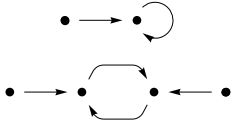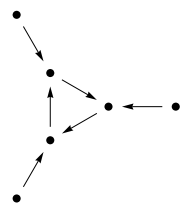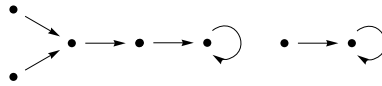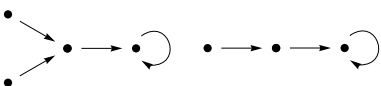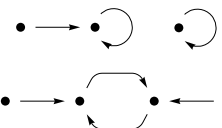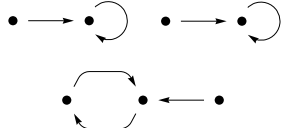
We provide here models for all dynamical modular curves $X_1(\mathcal{P})$ of genus 1 or 2, together with an explicit description of the morphism $c : X_1(\mathcal{P}) \to \mathbb{P}^1$. Each of these models appears in [44]. Note that in some cases we provide two models—one of the form $y^2 = F(x)$, and another that turns out to be more useful for certain aspects of our proofs.
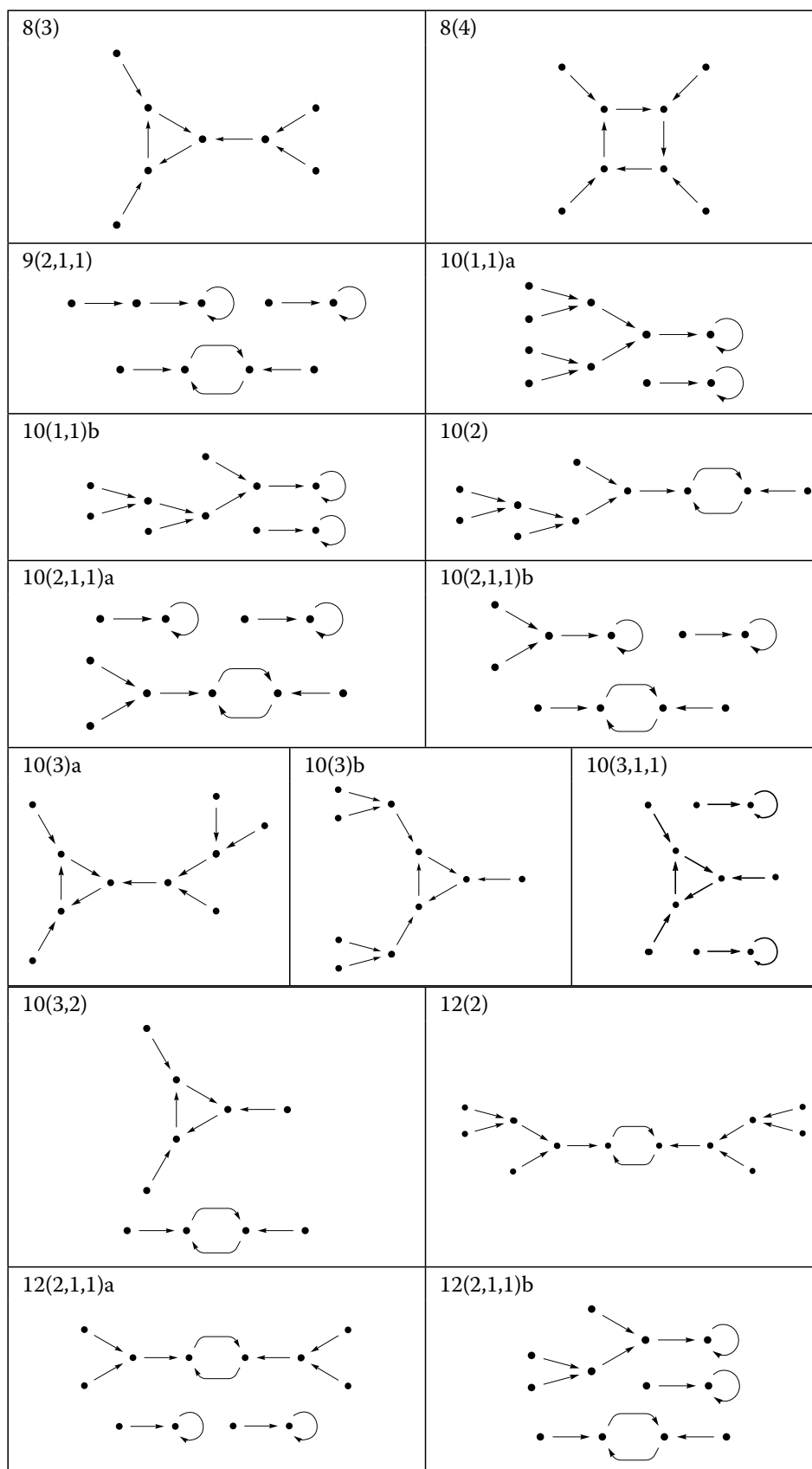
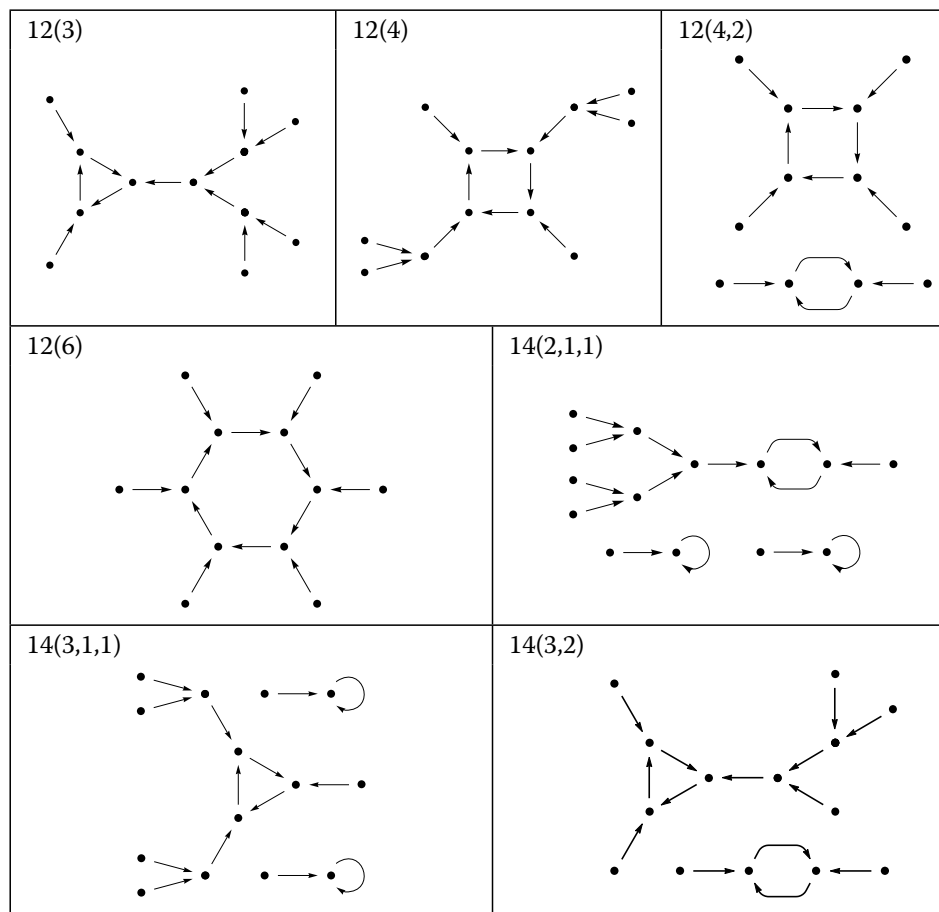| Portrait $\mathcal{P}$	Model(s) for $X_1(\mathcal{P})$	Morphism $c : X_1(\mathcal{P}) \to \mathbb{P}^1$
8(1,1)a	$y^2 = x^3 - x^2 + x$	$-\dfrac{(x^2+1)^2}{4x(x-1)^2}$
8(1,1)b	$y^2 = 2(x^3 + x^2 - x + 1)$	$-\dfrac{2(x^2+1)}{(x+1)^2(x-1)^2}$
8(2)a	$y^2 = x^3 - 2x + 1$	$-\dfrac{(x^2-2x+2)(x^2+2x-2)}{4x^2(x-1)}$
8(2)b	$y^2 = 2(x^3 + x^2 - x + 1)$	$-\dfrac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x+1)^2(x-1)^2}$
10(2,1,1)a	$y^2 = 5x^4 - 8x^3 + 6x^2 + 8x + 5$	$-\dfrac{(3x^2+1)(x^2+3)}{4(x+1)^2(x-1)^2}$
	$y^2 + xy + y = x^3 - x^2 - x$	$\dfrac{x-2}{4x(x-1)}y - \dfrac{x^4 - x^3 + 3x - 1}{4x^2(x-1)}$
10(2,1,1)b	$y^2 = (5x^2 - 1)(x^2 + 3)$	$-\dfrac{(3x^2+1)(x^2+3)}{4(x+1)^2(x-1)^2}$
	$y^2 + xy + y = x^3 + x^2$	$-\dfrac{x+2}{4x(x+1)}y - \dfrac{x^4 + 4x^3 + 6x^2 + 3x + 1}{4x^2(x+1)}$
8(3)	$y^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$	$-\dfrac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}$
8(4)	$y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$	$\dfrac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x+1)^2(x-1)^2}$
10(3,1,1)	$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$	$-\dfrac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}$
10(3,2)	$y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$	$-\dfrac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}$

Appendix B: Tables of preperiodic portraits

B.1 Preperiodic portraits realized over quadratic fields

We list here the 46 portraits known to be realized as $G(f_c, K)$ for some quadratic field K and $c \in K$. These were found in the search described in [14]. The label of each portrait is in the form $N(\ell_1, \ell_2, \ldots)$, where N is the number of vertices in the portrait and $\ell_1, \ell_2, \ldots$ are the lengths of the directed cycles in the portrait in nonincreasing order. If more than one isomorphism class with this data was observed, we add a lowercase Roman letter to distinguish them. For example, the labels 5(1,1)a and 5(1,1)b correspond to the two isomorphism classes of portraits observed that have five vertices and two fixed points. In all figures, we omit the vertex corresponding to the fixed point at infinity.
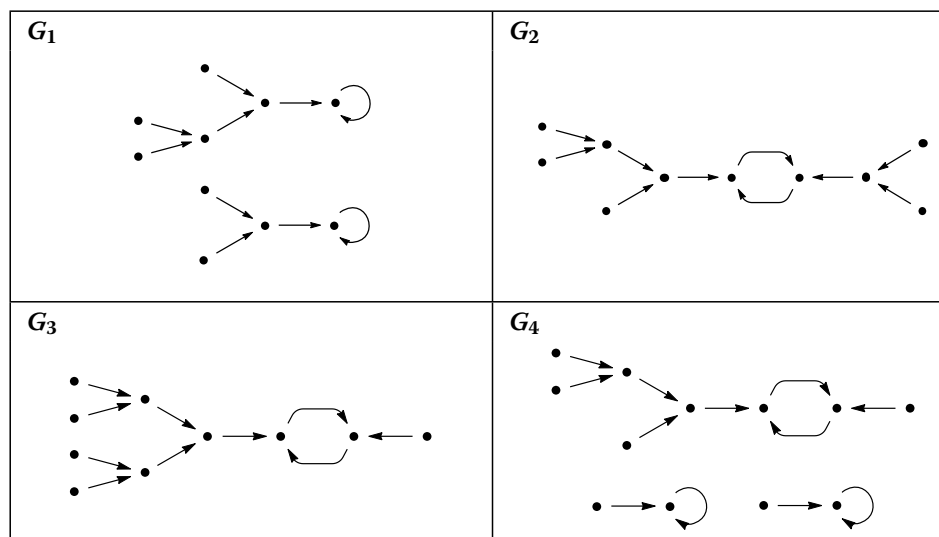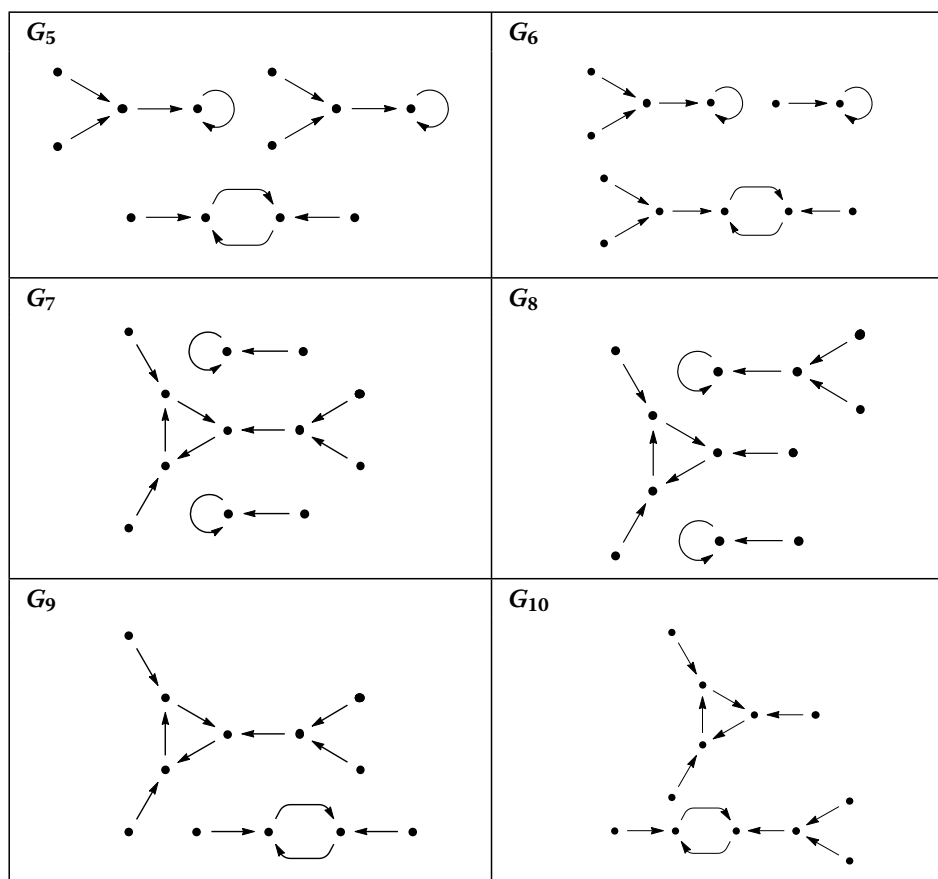
B.2 Additional portraits

The following portraits are not known to be realized over quadratic fields (and, in some cases, have been shown not to be); however, they make an appearance in the discussion in Section 4.2, so we include them here. The labels $G_1, \ldots, G_{10}$ are taken from [11].

References

1. Benedetto, R.L., Chen, R., Hyde, T., Kovacheva, Y., White, C.: Small dynamical heights for quadratic polynomials and rational functions. Exp. Math. **23**(4), 433–447 (2014)
2. Bilu, Y., Gillibert, J.: Chevalley–Weil theorem and subgroups of class groups. Isr. J. Math. **226**(2), 927–956 (2018)
3. Blanc, J., Canci, J.K., Elkies, N.D.: Moduli spaces of quadratic rational maps with a marked periodic point of small order. Int. Math. Res. Not. IMRN **23**, 12459–12489 (2015)
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997). Computational algebra and number theory (London, 1993)
5. Bosman, J., Bruin, P., Dujella, A., Najman, F.: Ranks of elliptic curves with prescribed torsion over number fields. Int. Math. Res. Not. IMRN **11**, 2885–2923 (2014)
6. Bousch, T.: Sur quelques problèmes de dynamique holomorphe. PhD thesis, Université de Paris-Sud, Centre d'Orsay (1992)
7. Canci, J.K., Vishkautsan, S.: Quadratic maps with a periodic critical point of period 2. Int. J. Number Theory **13**(6), 1393–1417 (2017)
8. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2. London Mathematical Society Lecture Note Series, vol. 230. Cambridge University Press, Cambridge (1996)
9. Clark, P.L.: On the Hasse principle for Shimura curves. Isr. J. Math. **171**, 349–365 (2009)
10. Cremona, J.E.: Algorithms for Modular Elliptic Curves, 2nd edn. Cambridge University Press, Cambridge (1997)
11. Doyle, J.R.: Preperiodic points for quadratic polynomials with small cycles over quadratic fields. Math. Z. **289**(1–2), 729–786 (2018)
12. Doyle, J.R.: Dynamical modular curves for quadratic polynomial maps. Trans. Am. Math. Soc. **371**(8), 5655–5685 (2019)
13. Doyle, J.R.: Preperiodic points for quadratic polynomials over cyclotomic quadratic fields. Acta Arith. **196**(3), 219–268 (2020)
14. Doyle, J.R., Faber, X., Krumm, D.: Preperiodic points for quadratic polynomials over quadratic fields. N. Y. J. Math. **20**, 507–605 (2014)
15. Doyle, J.R., Poonen, B.: Gonality of dynatomic curves and strong uniform boundedness of preperiodic points. Compos. Math. **156**(4), 733–743 (2020)
16. Doyle, J.R., Silverman, J.H.: Moduli spaces for dynamical systems with portraits. Illinois J. Math. **64**(3), 375–465 (2020)
17. Faber, X.: Benedetto's trick and existence of rational preperiodic structures for quadratic polynomials. Proc. Am. Math. Soc. **143**(2), 685–694 (2015)

18. Fakhruddin, N.: Questions on self maps of algebraic varieties. J. Ramanujan Math. Soc. **18**(2), 109–122 (2003)
19. Flynn, E.V., Poonen, B., Schaefer, E.F.: Cycles of quadratic polynomials and rational points on a genus-2 curve. Duke Math. J. **90**(3), 435–463 (1997)
20. Frey, G.: Curves with infinitely many points of fixed degree. Isr. J. Math. **85**(1–3), 79–83 (1994)
21. Gillibert, J., Levin, A.: Pulling back torsion line bundles to ideal classes. Math. Res. Lett. **19**(6), 1171–1184 (2012)
22. Harris, J., Silverman, J.: Bielliptic curves and symmetric products. Proc. Am. Math. Soc. **112**(2), 347–356 (1991)
23. Hutz, B.: Determination of all rational preperiodic points for morphisms of PN. Math. Comput. **84**(291), 289–308 (2015)
24. Hutz, B., Ingram, P.: On Poonen's conjecture concerning rational preperiodic points of quadratic maps. Rocky Mountain J. Math. **43**(1), 193–204 (2013)
25. Jeon, D., Kim, C.H., Schweizer, A.: On the torsion of elliptic curves over cubic number fields. Acta Arith. **113**(3), 291–301 (2004)
26. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**(2), 221–229 (1992)
27. Kenku, M.A., Momose, F.: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **109**, 125–149 (1988)
28. Krumm, D.: Quadratic Points on Modular Curves. Ph.D. Thesis, University of Georgia. ProQuest LLC, Ann Arbor, MI, p. 161 (2013). https://www.proquest.com/docview/2189108231
29. Krumm, D.: A local-global principle in the dynamics of quadratic polynomials. Int. J. Number Theory **12**(8), 2265–2297 (2016)
30. Krumm, D.: Squarefree parts of polynomial values. J. Théor. Nombres Bordeaux **28**(3), 699–724 (2016)
31. Krumm, D., Pollack, P.: Twists of hyperelliptic curves by integers in progressions modulo p. Acta Arith. **192**(1), 63–71 (2020)
32. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
33. Lukas, D., Manes, M., Yap, D.: A census of quadratic post-critically finite rational functions defined over $\mathbb{Q}$. LMS J. Comput. Math. **17**(Suppl. A), 314–329 (2014)
34. Manes, M.: $\mathbb{Q}$-rational cycles for degree-2 rational maps having an automorphism. Proc. Lond. Math. Soc. (3) **96**(3), 669–696 (2008)
35. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. (1977), **47**, 33–186 (1978)
36. Momose, F.: p-torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **96**, 139–165 (1984)
37. Morton, P.: Arithmetic properties of periodic points of quadratic maps. Acta Arith. **62**(4), 343–372 (1992)
38. Morton, P.: On certain algebraic curves related to polynomial maps. Compos. Math. **103**(3), 319–350 (1996)
39. Morton, P.: Arithmetic properties of periodic points of quadratic maps. II. Acta Arith. **87**(2), 89–102 (1998)
40. Morton, P., Silverman, J.H.: Rational periodic points of rational functions. Int. Math. Res. Not. **2**, 97–110 (1994)
41. F. Najman and A. Trbović, Splitting of primes in number fields generated by points on some modular curves. Res. Number Theory **8**(2), Paper No. 28 (2022)
42. Northcott, D.G.: Periodic points on an algebraic variety. Ann. Math. (2) **51**, 167–177 (1950)
43. Pezda, T.: Polynomial cycles in certain local domains. Acta Arith. **66**(1), 11–22 (1994)
44. Poonen, B.: The classification of rational preperiodic points of quadratic polynomials over Q: a refined conjecture. Math. Z. **228**(1), 11–29 (1998)
45. Serre, J.-P.: Topics in Galois Theory, 2nd edn. Research Notes in Mathematics, vol. 1. A K Peters, Ltd., Wellesley (2008). With notes by Darmon, H
46. Silverman, J.H.: The Arithmetic of Dynamical Systems. Graduate Texts in Mathematics, vol. 241. Springer, New York (2007)
47. Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd edn. Graduate Texts in Mathematics, vol. 254, Springer, Berlin (2009)
48. Stoll, M.: Rational 6-cycles under iteration of quadratic polynomials. LMS J. Comput. Math. **11**, 367–380 (2008)
49. The LMFDB Collaboration: The L-functions and modular forms database (2022). http://www.lmfdb.org. Accessed 12 Dec 2022
50. Walde, R., Russo, P.: Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$. Am. Math. Mon. **101**(4), 318–331 (1994)
51. Zieve, M.: Cycles of polynomial mapping. Ph.D. thesis, University of California, Berkeley (1996)

Publisher's Note