

Preperiodic points for quadratic polynomials over quadratic fields

John R. Doyle, Xander Faber and David Krumm

ABSTRACT. To each quadratic number field K and each quadratic polynomial f with K -coefficients, one can associate a finite directed graph $G(f, K)$ whose vertices are the K -rational preperiodic points for f , and whose edges reflect the action of f on these points. This paper has two main goals. (1) For an abstract directed graph G , classify the pairs (K, f) such that the isomorphism class of G is realized by $G(f, K)$. We succeed completely for many graphs G by applying a variety of dynamical and Diophantine techniques. (2) Give a complete description of the set of isomorphism classes of graphs that can be realized by some $G(f, K)$. A conjecture of Morton and Silverman implies that this set is finite. Based on our theoretical considerations and a wealth of empirical evidence derived from an algorithm that is developed in this paper, we speculate on a complete list of isomorphism classes of graphs that arise from quadratic polynomials over quadratic fields.

CONTENTS

1. Introduction	507
2. Quadratic points on algebraic curves	514
3. Classification of preperiodic graph structures	519
4. Computation of preperiodic points	578
5. PCF maps and maps with a unique fixed point	587
Appendix A. Proof of Lemma 3.5	592
Appendix B. Preperiodic graph structures	596
Appendix C. Representative data	599
References	603

1. Introduction

1.1. Background. Let K be a number field and let $f(z) = A(z)/B(z)$ be a rational function defined over K , where $A(z)$ and $B(z)$ are coprime

Received February 7, 2014.

2010 *Mathematics Subject Classification.* 37P35, 14G05.

Key words and phrases. Arithmetic dynamics, quadratic polynomials, preperiodic points, Uniform Boundedness Conjecture, quadratic points.

The second author was partially supported by an NSF postdoctoral research fellowship.

polynomials with coefficients in K . The function $f(z)$ naturally induces a map $f : \mathbb{P}^1(K) \rightarrow \mathbb{P}^1(K)$; a fundamental problem in dynamics is that of describing the behavior of points $P \in \mathbb{P}^1(K)$ under repeated iteration of the map f . Thus, we consider the sequence

$$P, f(P), f(f(P)), f(f(f(P))), \dots$$

For convenience we denote by f^m the m -fold composition of f : f^0 is the identity map, and $f^m = f \circ f^{m-1}$ for all $m \geq 1$. We say that a point $P \in \mathbb{P}^1(K)$ is *preperiodic* for f if the orbit of P under f , i.e., the set

$$\{f^m(P) : m \geq 0\},$$

is finite. Furthermore, we say that P is *periodic* for f if it satisfies the stronger condition that $f^m(P) = P$ for some $m > 0$; in this case, the least positive integer m with this property is called the *period* of P . The set of all points $P \in \mathbb{P}^1(K)$ that are preperiodic for f is denoted by $\text{PrePer}(f, K)$. Finally, the *degree* of $f(z)$ is defined to be the number $d := \max\{\deg A, \deg B\}$.

Using the theory of height functions, Northcott [29] proved that the set $\text{PrePer}(f, K)$ is finite as long as the degree of f is greater than 1. This set can be given the structure of a directed graph by letting the elements $P \in \text{PrePer}(f, K)$ be the vertices of the graph, and drawing directed edges $P \rightarrow f(P)$ for every such point P . Thus, we obtain a finite directed graph representing the K -rational preperiodic points for f . It is then natural to ask how large the set $\text{PrePer}(f, K)$ can be, and what structure the associated graph can have. Drawing an analogy between preperiodic points of maps and torsion points on abelian varieties, Morton and Silverman [27, page 100] proposed the following conjecture regarding the size of the set $\text{PrePer}(f, K)$:

Uniform Boundedness Conjecture (Morton-Silverman). *Fix integers $n \geq 1$ and $d \geq 2$. There exists a constant $M(n, d)$ such that for every number field K of degree n , and every rational function $f(z) \in K(z)$ of degree d ,*

$$\#\text{PrePer}(f, K) \leq M(n, d).$$

Very little is currently known about this conjecture; indeed, it has not been proved that such a constant $M(n, d)$ exists, even in the simplified setting where $K = \mathbb{Q}$ and $f(z) \in K[z]$ is a quadratic polynomial. However, Poonen [31, Cor. 1] proposed an upper bound of 9 in this case, and moreover gave a conjecturally complete list of all possible graph structures arising in this context — see [31, page 17].

Theorem 1.1 (Poonen). *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 with rational coefficients,*

$$\#\text{PrePer}(f, \mathbb{Q}) \leq 9.$$

Moreover, there are exactly 12 graphs that arise from $\text{PrePer}(f, \mathbb{Q})$ as f varies over all quadratic polynomials with rational coefficients.

Regarding the assumption made in Poonen's result, it is known that there is no quadratic polynomial over \mathbb{Q} having a rational periodic point of period $m = 4$ or 5 (see [11, Thm. 1] and [26, Thm. 4]), and assuming standard conjectures on L -series of curves, the same holds for $m = 6$ (see [38, Thm. 7]). In [11] Flynn, Poonen, and Schaefer conjecture that no quadratic polynomial over \mathbb{Q} has a rational point of period greater than 3 , a hypothesis which Hutz and Ingram have verified extensively by explicit computation (see [19, Prop. 1]). However, a proof of this conjecture seems distant at present.

One direction in which to continue the kind of work carried out by Poonen in studying the Uniform Boundedness Conjecture (UBC) is to consider preperiodic points for higher degree polynomials over \mathbb{Q} , such as was done by Benedetto et al. [1] in the case of cubics. In this paper we take a different approach and consider maps defined over number fields of degree $n > 1$. The case of degree $n = 1$ is very special because there is only one number field with this degree; hence, in this case the UBC is a statement only about uniformity as one varies the rational function $f(z)$ with \mathbb{Q} -coefficients. More striking is that the conjecture predicts upper bounds even when all number fields of a fixed degree $n > 1$ are considered. Our goal in this article is to carry out an initial study of preperiodic points for maps defined over quadratic number fields (the case $n = 2$ of the UBC). Having fixed this value of n , we will focus on the simplest family of maps to which the conjecture applies, namely quadratic polynomials. Thus, we wish to address the following questions:

- (1) How large can the set $\text{PrePer}(f, K)$ be as K varies over all quadratic number fields and f varies over all quadratic polynomials with coefficients in K ?
- (2) What are all the possible graph structures corresponding to sets $\text{PrePer}(f, K)$ as K and f vary as above?

1.2. Outline of the paper. Our initial guesses for answers to the above questions were obtained by gathering large amounts of data, and doing this required an algorithm for computing all the preperiodic points of a given quadratic polynomial defined over a given number field. In §4 we develop an algorithm for doing this which relies heavily on a new method, due to the first and third authors [8], for listing elements of bounded height in number fields. Our algorithm for computing preperiodic points can in principle be applied to quadratic polynomials over any number field, but we will focus here on the case of quadratic fields. Using this algorithm we computed the set $\text{PrePer}(f, K)$ for roughly 250,000 pairs (K, f) consisting of a quadratic field K and a quadratic polynomial f with coefficients in K . Our strategy for choosing the fields K and polynomials f is explained in §4.4. The graph structures found by this computation are shown in Appendix B, and for each such graph G we give in Appendix C an example of a pair (K, f) for which the graph associated to $\text{PrePer}(f, K)$ is isomorphic to G .

In order to state the more refined questions addressed in this article and our main results, we introduce some notation. From a dynamical standpoint, quadratic polynomials form a one-parameter family; more precisely, if K is a number field and $f(z) \in K[z]$ is a quadratic polynomial, then $f(z)$ is equivalent, in a dynamical sense, to a unique polynomial of the form $f_c(z) = z^2 + c$. (See the introduction to §3 for more details.) In studying the dynamical properties of quadratic polynomials, we will thus consider only polynomials of the form $f_c(z)$. We denote by $G(f_c, K)$ the directed graph corresponding to the set $\text{PrePer}(f_c, K)$, excluding the point at infinity.

The graphs arising from our computation did not all occur with the same frequency: some of them appeared only a few times, while others were extremely common. For each graph G that was found we may then ask:

- (1) How many pairs (K, c) are there for which the graph $G(f_c, K)$ is isomorphic to G ?
- (2) If there are only finitely many such pairs, can they be completely determined?
- (3) If there are infinitely many such pairs, can they be explicitly described?

Our strategy for addressing these questions is to translate them into Diophantine problems of determining the set of quadratic points on certain algebraic curves over \mathbb{Q} . In essence, the idea is to attach to each graph G an algebraic curve C whose points parameterize instances of the graph G . This philosophy of studying rational preperiodic points via algebraic curves was first taken up by Morton [26], and then pushed much further by Flynn–Poonen–Schaefer [11], Poonen [31], and Stoll [38]. However, the Diophantine questions we need to answer in this article differ from those studied by previous authors, since they were interested primarily in finding \mathbb{Q} -rational points on curves, whereas we need to determine all K -rational points on a given curve C/\mathbb{Q} , where K is allowed to vary over all quadratic number fields. A survey of known theoretical results on this type of question is given in §2, where we also develop our basic computational methods for attacking the problem in practice. In §3 we construct the algebraic curves corresponding to the graphs found by our computation, and the methods of §2 are used to describe or completely determine their sets of quadratic points.

1.3. Main results. In our extensive computation of preperiodic points mentioned above, we obtained a total of 46 nonisomorphic graphs, and the maximum number of preperiodic points for the polynomials considered was 15 (counting the fixed point at infinity). This data may provide the correct answers to questions (1) and (2) posed in §1.1, though it is not our goal here to make this claim and attempt a proof. However, our computations do yield the following result:

Theorem 1.2. *Suppose that there exists a constant N such that*

$$\#\text{PrePer}(f, K) \leq N$$

for every quadratic number field K and quadratic polynomial f with coefficients in K . Then $N \geq 15$. Moreover, there are at least 46 directed graphs that arise from the set $\text{PrePer}(f, K)$ for such a field K and polynomial f .

For each of the 46 graphs that were found we would like to answer questions (1)–(3) stated in §1.2. This can be done easily for 12 of the graphs, namely those that appeared in Poonen’s paper [31] — see §3.1 below. The essential tool for this is Northcott’s theorem on height bounds for the preperiodic points of a given map. For 15 of the 34 remaining graphs we were able to determine all pairs (K, c) giving rise to the given graph. In most cases this was done by finding all quadratic points on the parameterizing curve of the graph, using our results concerning quadratic points on elliptic curves and on curves of genus 2 with Mordell–Weil rank 0. With the notation used in Appendix B, the labels for these graphs are

$$4(1), 5(1,1)\text{b}, 5(2)\text{a}, 5(2)\text{b}, 6(2,1), 7(1,1)\text{a}, 7(1,1)\text{b}, 7(2,1,1)\text{a}, \\ 7(2,1,1)\text{b}, 9(2,1,1), 10(1,1)\text{a}, 12(2,1,1)\text{a}, 14(2,1,1), 14(3,1,1), 14(3,2).$$

With the exception of graph 5(2)a — which occurs for two Galois conjugate pairs, namely $(\mathbb{Q}(i), \pm i)$ — all of these graphs turned out to be unique; i.e., they occur for exactly one pair (K, c) . Moreover, the parameter c in all of these pairs is rational.

Of the remaining 19 graphs, there are 4 for which we were not able to determine all pairs (K, c) giving rise to the graph, but instead proved an upper bound on the number of all such pairs that could possibly exist. This was done by reducing the problem of determining all quadratic points on the parameterizing curve to a problem of finding all *rational* points on certain hyperelliptic curves. Table 1 below summarizes our results for these graphs. The first column gives the label of the graph under consideration, the second column gives the number of known pairs (K, c) corresponding to this graph structure, and the third column gives an upper bound for the number of such pairs.

Graph	Known pairs	Upper bound
12(2)	2	6
12(2,1,1)b	2	6
12(4)	1	6
12(4,2)	1	2

TABLE 1.

In order to complete our analysis of these four graphs we would need to determine all rational points on the hyperelliptic curves defined by the

following equations:

$$\begin{aligned} w^2 &= x^7 + 3x^6 + x^5 - 3x^4 + x^3 + 3x^2 - 3x + 1, \\ s^2 &= -6x^7 - 6x^6 + 34x^5 + 22x^4 - 18x^3 + 38x^2 - 10x + 10, \\ w^2 &= x^{12} + 2x^{11} - 13x^{10} - 26x^9 + 67x^8 + 124x^7 + 26x^6 - 44x^5 \\ &\quad + 179x^4 - 62x^3 - 5x^2 + 6x + 1, \\ w^2 &= (x^2 + 1)(x^2 - 2x - 1)(x^6 - 3x^4 - 16x^3 + 3x^2 - 1). \end{aligned}$$

Of the 15 graphs that remain to be considered, there are 9 for which we showed that the graph occurs infinitely many times over quadratic fields. This is achieved by using results from Diophantine geometry giving asymptotics for counting functions on the set of rational points on a curve.

Theorem 1.3. *For each of the graphs*

$$8(1,1)\text{a}, 8(1,1)\text{b}, 8(2)\text{a}, 8(2)\text{b}, 8(4), 10(2,1,1)\text{a}, 10(2,1,1)\text{b}$$

there exist infinitely many pairs (K, c) consisting of a real (resp. imaginary) quadratic field and an element $c \in K$ for which $G(f_c, K)$ contains a graph of this type. The same holds for the graphs $10(3,1,1)$ and $10(3,2)$, but these occur only over real quadratic fields.

Remark. Showing the existence of infinitely many pairs for which $G(f_c, K)$ not only *contains* a graph of a given type but in fact *is* itself of this type is a more difficult problem. This kind of result was achieved in the article [9] for several of the graphs $G(f_c, \mathbb{Q})$ with $c \in \mathbb{Q}$.

For the six graphs that remain, our methods did not yield a satisfactory upper bound on the number of possible instances — see §1.4 below for more information.

Finally, we point out some results in this article which may be of independent interest. First, our description of quadratic points on elliptic curves in §2.1, though completely elementary, has been useful in practice for quickly generating many quadratic points on a given elliptic curve, as well as for proving several of our results stated above. The formula in §2.2 for the number of “nonobvious” quadratic points on a curve of genus 2 does not seem to be explicitly stated in the literature, nor is its application (in Theorem 2.4) to the study of quadratic points on the modular curves $X_1(N)$ of genus 2. The techniques used here to determine all quadratic points on certain curves also appear to be new. As an example of our methods we mention our study of the graph $12(2,1,1)\text{a}$ in §3.14, which illustrates our approach to finding all quadratic points on a curve C having maps $C \rightarrow E_1$ and $C \rightarrow E_2$, where E_1 and E_2 are elliptic curves of rank 0. A second example is our study of the graph $12(4,2)$ in §3.17, in which we bound the number of quadratic points on a curve C having a map $C \rightarrow X_1$, where X_1 is a curve of genus 2 and Mordell–Weil rank 0, and a map $C \rightarrow X_2$, where X_2 is a curve of genus 3 and Mordell–Weil rank 1.

1.4. Future work. This paper leaves open several questions that we intend to address in subsequent articles. First of all, there are a few graphs in Appendix B for which we are at present not able to carry out a good analysis of the quadratic points on the corresponding curves; precisely, these are the graphs labeled

$$10(1,1)b, 10(2), 10(3)a, 10(3)b, 12(3), \text{ and } 12(6).$$

In most cases the difficulties do not seem insurmountable, but the methods required to study these graphs may be rather different from the ones used in this paper. Second, for some of the graphs analyzed in §3 we have only partially determined the quadratic points on the parameterizing curve, the obstruction being a problem of finding all rational points on certain hyperelliptic curves (listed above). We expect that the method of Chabauty and Coleman can be successfully applied to determine all rational points on these curves, thus completing our study of the corresponding graphs; this analysis will appear in a sequel to the present paper.

The next open question concerns 5-cycles. All evidence currently available suggests that there does not exist a quadratic polynomial f defined over a quadratic field K such that f has a K -rational point of period 5. Such a polynomial did not show up in our computations, nor was it found in a related search carried out by Hutz and Ingram [19]. We therefore set the following goal for future research:

Either find an example of a 5-cycle over a quadratic field, or show that it does not exist.

As a result of their own extensive search for periodic points with large period defined over quadratic fields, Hutz and Ingram [19, Prop. 2] provide evidence supporting the conjecture that 6 is the longest cycle length that can appear in this setting. Moreover, they found exactly one example of a 6-cycle over a quadratic field, which is the same one found during our computations and the same one that had been found earlier by Flynn, Poonen, and Schaefer [11, page 461]; namely the example given in Appendix C under the label 12(6). While the question of proving that 6 is the longest possible cycle length may be too ambitious, we do aim to study the following question:

Determine all instances of a 6-cycle over a quadratic field.

We remark that it follows from known results in Diophantine geometry (see Theorem 2.1 below) applied to the curve parameterizing 6-cycles¹ that there are only finitely many pairs (K, c) , with K quadratic, giving rise to a 6-cycle.

As a final goal, we wish to prove a theorem analogous to Poonen's result (Theorem 1.1), but in the context of quadratic fields. In view of the above discussion, we propose the following:

¹The geometry of this curve, and its set of rational points, were studied by Stoll in [38]. In particular, it is shown that the curve is not hyperelliptic and not bielliptic.

Speculation 1.4. *Assume that there is no quadratic polynomial over a quadratic field having a periodic point of period $n = 5$ or $n > 6$. Then, for every quadratic polynomial f with coefficients in a quadratic field K ,*

$$\# \text{PrePer}(f, K) \leq 15.$$

Moreover, there are exactly 46 graphs that arise from $\text{PrePer}(f, K)$ as f varies over all quadratic polynomials with coefficients in a quadratic field K .

Using techniques similar to those applied in §3, substantial progress towards proving this result — or one very similar to it — has already been made by the first author and will appear in a later paper.

Acknowledgements. Part of the research for this article was undertaken during an NSF-sponsored VIGRE research seminar at the University of Georgia, supervised by the second author and Robert Rumely. The second author was partially supported by an NSF postdoctoral research fellowship. We would like to acknowledge the contributions of the other members of our research group: Adrian Brunyate, Allan Lacy, Alex Rice, Nathan Walters, and Steven Winburn. We are especially grateful to the Brown University Center for Computation and Visualization for providing access to their high performance computing cluster, and to the Institute for Computational and Experimental Research in Mathematics for facilitating this access. Finally, we thank Dino Lorenzini and Robert Rumely for many comments and suggestions; Anna Chorniy for her help in preparing the figures shown in Appendix B; and the anonymous referee for pointing out some gaps in our exposition in §3.

2. Quadratic points on algebraic curves

The material in this section forms the basis for our analysis of preperiodic graph structures in §3. As mentioned in the introduction, questions concerning the sets of preperiodic points for quadratic polynomials over quadratic number fields can be translated into questions about the sets of quadratic points on certain algebraic curves defined over \mathbb{Q} . We will therefore require some basic facts about quadratic points on curves, from a theoretical as well as computational perspective.

Let k be a number field, and fix an algebraic closure \bar{k} of k . Let C be a smooth, projective, geometrically connected curve defined over k . We say that a point $P \in C(\bar{k})$ is *quadratic over k* if $[k(P) : k] = 2$, where $k(P)$ denotes the field of definition of P , i.e., the residue field of C at P . The set of all quadratic points on C will be denoted by $C(k, 2)$. It may well happen that $C(k, 2) = \emptyset$: for instance, it follows from a theorem of Clark [5, Cor. 4] that there are infinitely many curves of genus 1 over k with this property. The set $C(k, 2)$ may also be nonempty and finite; several examples of this will be seen in §3. Finally, the set $C(k, 2)$ may be infinite. Suppose, for

instance, that C is hyperelliptic, so that it admits a morphism $C \rightarrow \mathbb{P}^1$ of degree 2 defined over k . By pulling back k -rational points on \mathbb{P}^1 we obtain — by Hilbert’s irreducibility theorem [13, Chap. 12] — infinitely many quadratic points on C . Similarly, suppose C is bielliptic, so that it admits a morphism of degree 2 to an elliptic curve E/k . If the group $E(k)$ has positive rank, then the same argument as above shows that C has infinitely many quadratic points. Using Faltings’ theorem [10] concerning rational points on subvarieties of abelian varieties (formerly a conjecture of Lang), Harris and Silverman [15, Cor. 3] showed that these are the only two types of curves that can have infinitely many quadratic points.

Theorem 2.1 (Harris–Silverman). *Let k be a number field and let C/k be a curve. If C is neither bielliptic nor hyperelliptic, then the set $C(k, 2)$ is finite.*

Thus, we have simple geometric criteria for deciding whether a given curve C/k has finitely many or infinitely many quadratic points. However, we are not only interested here in abstract finiteness statements, but also in the practical question of explicitly determining all quadratic points on a curve, given a specific model for it. If the given curve has infinitely many quadratic points, then we will require an explicit description of all such points, and if it has only a finite number of quadratic points, then we require that they be determined. For the purposes of this paper we will mostly need to address these questions in the case of elliptic and hyperelliptic curves, or curves with a map of degree 2 to such a curve.

We begin by discussing quadratic points on hyperelliptic curves in general. Suppose that the curve C/k admits a morphism $\varphi : C \rightarrow \mathbb{P}_k^1$ of degree 2. Let σ be the hyperelliptic involution on C , i.e., the unique involution such that $\varphi \circ \sigma = \varphi$. Corresponding to the map φ there is an affine model for C of the form $y^2 = f(x)$, where $f(x) \in k[x]$ has nonzero discriminant. With respect to this equation, σ is given by $(x, y) \mapsto (x, -y)$, and the quotient map $\varphi : C \rightarrow C/\langle \sigma \rangle = \mathbb{P}_k^1$ is given by $(x, y) \mapsto x$. We wish to distinguish between two kinds of quadratic points on C ; first, there is the following obvious way of generating quadratic points: by choosing any element $x_0 \in k$ we obtain a point $(x_0, \sqrt{f(x_0)}) \in C(\bar{k})$ which will often be quadratic as we vary x_0 . Indeed, Hilbert’s irreducibility theorem implies that this will occur for infinitely many $x_0 \in k$. Points of this form will be called *obvious quadratic points* for the given model. Stated differently, these are the quadratic points $P \in C(\bar{k})$ such that $\varphi(P) \in \mathbb{P}^1(k)$, or equivalently $\sigma(P) = \bar{P}$, where \bar{P} is the Galois conjugate of P . Quadratic points that do not arise in this way will be called *nonobvious quadratic points* on C . Though a hyperelliptic curve always has infinitely many obvious quadratic points, this is not the case for nonobvious points; in fact, a theorem of Vojta [39, Cor. 0.3] implies that the set of nonobvious quadratic points on a hyperelliptic curve of genus ≥ 4 is always finite. We focus now on studying the nonobvious quadratic points on elliptic curves and on curves of genus 2.

2.1. Case of elliptic curves. The following result gives an explicit description of all nonobvious quadratic points on an elliptic curve.

Lemma 2.2. *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 that $(x, y) \in E(\bar{k})$ is a quadratic point with $x \notin k$. Then there exist a point $(x_0, y_0) \in E(k)$ and an element $v \in k$ such that $y = y_0 + v(x - x_0)$ and

$$x^2 + \frac{ax_0 - v^2 + b}{a}x + \frac{ax_0^2 + v^2x_0 + bx_0 - 2y_0v + c}{a} = 0.$$

Proof. Since $y \in k(x)$, we can write $y = p(x)$ for some polynomial $p(t) \in k[t]$ of degree at most 1. Note that x is a root of the polynomial

$$F(t) := at^3 + bt^2 + ct + d - p(t)^2,$$

so $F(t)$ must factor as $F(t) = a(t - x_0)m(t)$, where $m(t)$ is the minimal polynomial of x and $x_0 \in k$. Since $F(x_0) = 0$, then $(x_0, p(x_0)) \in E(k)$. Letting $y_0 = p(x_0)$ we can write $p(t) = y_0 + v(t - x_0)$ for some $v \in k$; in particular, $y = p(x) = y_0 + v(x - x_0)$. Carrying out the division

$$F(t)/(a(t - x_0))$$

we obtain

$$m(t) = t^2 + \frac{ax_0 - v^2 + b}{a}t + \frac{ax_0^2 + v^2x_0 + bx_0 - 2y_0v + c}{a}. \quad \square$$

Remark. The description of quadratic points on E given above has the following geometric interpretation: suppose $P = (x, y) \in E(\bar{k})$ is quadratic over k , let $K = k(x, y)$ be the field of definition of P , and let σ be the nontrivial element of $\text{Gal}(K/k)$. We can then consider the point

$$Q = P + P^\sigma \in E(k),$$

where $P^\sigma = (\sigma(x), \sigma(y))$ denotes the Galois conjugate of P . If Q is the point at infinity on E , then the line through P and P^σ is vertical, so that $x = \sigma(x)$ and hence $x \in k$; this gives rise to obvious quadratic points on E . If Q is not the point at infinity, then it is an affine point in $E(k)$, say $Q = (x_0, -y_0)$ for some elements $x_0, y_0 \in k$. The points P, P^σ , and (x_0, y_0) are collinear, and the line containing them has slope in k , say equal to $v \in k$. We then have $y = y_0 + v(x - x_0)$, and this gives rise to the formula in Lemma 2.2.

2.2. Curves of genus 2. Suppose now that C/k is a curve of genus 2. Fix an affine model $y^2 = f(x)$ for C , where $f(x)$ has degree 5 or 6, and let σ be the hyperelliptic involution on C .

Lemma 2.3. *Suppose that C/k has genus 2 and $C(k) \neq \emptyset$. Let J be the Jacobian variety of C .*

- (1) *The set of nonobvious quadratic points for the model $y^2 = f(x)$ is finite if and only if $J(k)$ is finite.*

(2) Suppose that $J(k)$ is finite, and let q denote the number of nonobvious quadratic points for the given model. Then there is a relation

$$q = 2j - 2 + w - c^2,$$

where $j = \#J(k)$, $c = \#C(k)$, and w is the number of points in $C(k)$ that are fixed by σ .

Proof. Fix a point $P_0 \in C(k)$ and let $\iota : C \hookrightarrow J$ be the embedding taking P_0 to 0. Let $\mathcal{S} = \text{Sym}^2(C)$ denote the symmetric square of C . Points in $\mathcal{S}(\bar{k})$ correspond to unordered pairs $\{P, Q\}$, where $P, Q \in C(\bar{k})$. The embedding ι induces a morphism $f : \mathcal{S} \rightarrow J$ taking $\{P, Q\}$ to $\iota(P) + \iota(Q)$. We will need a few facts concerning the fibers of this morphism; see the article of Milne [25] for the necessary background material. There is a copy of \mathbb{P}^1_k inside \mathcal{S} whose points correspond to pairs of the form $\{P, \sigma(P)\}$. The image of \mathbb{P}^1 under f is a single point $* \in J(k)$, and f restricts to an isomorphism $f : U = \mathcal{S} \setminus \mathbb{P}^1 \xrightarrow{\sim} J \setminus \{*\}$. In particular, there is a bijection

$$(2.1) \quad U(k) = \mathcal{S}(k) \setminus \mathbb{P}^1(k) \longleftrightarrow J(k) \setminus \{*\}.$$

Points in $\mathcal{S}(k)$ correspond to pairs of the form $\{P, Q\}$ where either P and Q are both in $C(k)$, or they are quadratic over k and $Q = \bar{P}$; in particular, points in $\mathbb{P}^1(k) \subset \mathcal{S}(k)$ correspond to pairs $\{P, \sigma(P)\}$ where either $P \in C(k)$ or P is an obvious quadratic point. Finally, the points of $U(k)$ are either pairs $\{P, \bar{P}\}$ with P a nonobvious quadratic point, or pairs $\{P, Q\}$ with $P, Q \in C(k)$ but $Q \neq \sigma(P)$.

Hence, there are three essentially distinct ways of producing points in $\mathcal{S}(k)$: first, we can take points P and Q in $C(k)$ and obtain a point

$$\{P, Q\} \in \mathcal{S}(k).$$

Second, we can take an obvious quadratic point P and obtain

$$\{P, \sigma(P)\} \in \mathbb{P}^1(k) \subset \mathcal{S}(k).$$

Finally, we can take a nonobvious quadratic point P and obtain

$$\{P, \bar{P}\} \in U(k) \subset \mathcal{S}(k).$$

Let Q^o and Q^n denote, respectively, the set of obvious and nonobvious quadratic points on C . We then have maps

$$\begin{aligned} \psi^o : Q^o &\rightarrow \mathbb{P}^1(k), \\ \psi^n : Q^n &\rightarrow U(k), \end{aligned}$$

and a map

$$\varphi : C(k) \times C(k) \rightarrow \mathcal{S}(k)$$

defined as above. The proof of the lemma will be a careful analysis of the images of these three maps.

We have $\mathcal{S}(k) = \text{im}(\varphi) \sqcup \text{im}(\psi^o) \sqcup \text{im}(\psi^n)$. Removing the points of $\mathbb{P}^1(k)$ from both sides we obtain

$$(2.2) \quad U(k) = (\text{im}(\varphi) \setminus \mathbb{P}^1(k)) \sqcup \text{im}(\psi^n).$$

To prove part (1), suppose first that Q^n is finite. We know by Faltings' theorem that $C(k)$ is finite, so it follows from (2.2) that $U(k)$ is finite. By (2.1) we conclude that $J(k)$ is finite. Conversely, assume that $J(k)$ is finite. Then $U(k)$ is finite by (2.1), so $\text{im}(\psi^n)$ is finite by (2.2). But ψ^n is 2-to-1 onto its image, so we conclude that Q^n is finite. This completes the proof of part (1).

To prove part (2), suppose that $J(k)$ is finite and let $q = \#Q^n$, so that $\#\text{im}(\psi^n) = q/2$. By (2.1) and (2.2) we have

$$(2.3) \quad q/2 = \#U(k) - \#(\text{im}(\varphi) \setminus \mathbb{P}^1(k)) = j - 1 - \#(\text{im}(\varphi) \setminus \mathbb{P}^1(k)).$$

By simple combinatorial arguments we see that

$$\#\text{im}(\varphi) = c + \frac{c(c-1)}{2} \quad \text{and} \quad \#(\mathbb{P}^1(k) \cap \text{im}(\varphi)) = w + \frac{c-w}{2}.$$

Therefore,

$$\#(\text{im}(\varphi) \setminus \mathbb{P}^1(k)) = c + \frac{c(c-1)}{2} - w - \frac{c-w}{2} = \frac{c^2 - w}{2}.$$

By (2.3) we then have

$$j - 1 = \frac{q}{2} + \frac{c^2 - w}{2},$$

and part (2) follows immediately. \square

2.3. Application to the modular curves $X_1(N)$ of genus 2. For later reference we record here some consequences of Lemma 2.3 in the particular case that $k = \mathbb{Q}$ and C is one of the three modular curves $X_1(N)$ of genus 2. We will fix models for these curves to be used throughout this section. The following equations are given in [31, page 15], [41, page 774], and [32, page 39], respectively:

$$X_1(13) : y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1;$$

$$X_1(16) : y^2 = -x(x^2 + 1)(x^2 - 2x - 1);$$

$$X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Theorem 2.4.

- (1) *Every quadratic point on $X_1(13)$ is obvious.*
- (2) *The only nonobvious quadratic points on $X_1(16)$ are the following four:*

$$(\sqrt{-1}, 0), (-\sqrt{-1}, 0), (1 + \sqrt{2}, 0), (1 - \sqrt{2}, 0).$$

- (3) *The only nonobvious quadratic points on $X_1(18)$ are the following four:*

$$(\omega, \omega - 1), (\omega^2, \omega^2 - 1), (\omega, 1 - \omega), (\omega^2, 1 - \omega^2),$$

where ω is a primitive cube root of unity.

Proof. It is known that the Jacobians $J_1(N)$ for $N \in \{13, 16, 18\}$ have only finitely many rational points (see [24, §4] for the case of $J_1(13)$, [21, Thm. 1] for $J_1(16)$, and [22, Thm. IV.5.7] for $J_1(18)$). Hence, Lemma 2.3 implies that the corresponding curves $X_1(N)$ have only finitely many nonobvious quadratic points. The various quantities appearing in the lemma are either known or can be easily computed. Indeed, Ogg [30, page 226] showed that $\#X_1(N)(\mathbb{Q}) = 6$ for $N \in \{13, 16, 18\}$ and

$$\#J_1(13)(\mathbb{Q}) = 19, \#J_1(16)(\mathbb{Q}) = 20, \#J_1(18)(\mathbb{Q}) = 21.$$

The number w in Lemma 2.3 is determined by the number of rational roots of the polynomial $f(x)$.

Applying Lemma 2.3 to the curve $C = X_1(13)$, we have $j = 19, c = 6, w = 0$, and hence $q = 0$. Therefore, all quadratic points on $X_1(13)$ are obvious.

Similarly, with $C = X_1(16)$ we have $j = 20, c = 6, w = 2$, and hence $q = 4$. We have already listed four nonobvious quadratic points, so these are all.

Finally, with $C = X_1(18)$ we have $j = 21, c = 6, w = 0$, and hence $q = 4$. Therefore, $X_1(18)$ has exactly four nonobvious quadratic points. Since we have already listed four such points, these must be all. \square

3. Classification of preperiodic graph structures

For each graph G appearing in the list of 46 graphs in Appendix B, it is our goal in this section to describe — as explicitly as possible — all the quadratic fields K and quadratic polynomials $f(z) \in K[z]$ such that the graph corresponding to the set $\text{PrePer}(f, K)$ is isomorphic to G . There are several graphs in the list for which this description can be achieved without too much work: see §3.1 below for the case of graphs arising from quadratic polynomials over \mathbb{Q} , and §5 for other graphs with special properties. Together, these two sections will cover all graphs in the appendix up to and including the one labeled 7(2,1,1)b, and also 8(2,1,1), 8(3), and 9(2,1,1); in this section we will focus on studying the remaining graphs. Our general approach is to construct a curve parameterizing occurrences of a given graph, then apply results from §2 to study the quadratic points on this curve, and from there obtain the desired description. As mentioned in §1.4, there are a few graphs for which this approach does not yet yield the type of result we are looking for; hence, we will exclude these graphs from consideration in this section.

For the purpose of studying preperiodic points of quadratic polynomials over a number field K , it suffices to consider only polynomials of the form

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

with $c \in K$. Indeed, for every quadratic polynomial $f(z) \in K[z]$ there is a unique linear polynomial $g(z) \in K[z]$ and a unique $c \in K$ such that

$$g \circ f \circ g^{-1} = f_c.$$

One sees easily that the graph representing the set of preperiodic points is unchanged upon passing from f to $g \circ f \circ g^{-1}$; hence, for our purposes we may restrict attention to the one-parameter family $\{f_c(z) : c \in K\}$. For a quadratic polynomial $f(z)$ with coefficients in K , we denote by $G(f, K)$ the directed graph corresponding to the set of K -rational preperiodic points for f , excluding the fixed point at infinity. If m and n are positive integers, a *point of type m_n* for $f(z)$ is an element $x \in K$ which enters an m -cycle after n iterations of the map f .

3.1. Graphs occurring over \mathbb{Q} . Given a rational number c and a quadratic field K , we may consider the two sets $\text{PrePer}(f_c, K)$ and $\text{PrePer}(f_c, \mathbb{Q})$. For all but finitely many quadratic fields K these sets will be equal, since Northcott's theorem [33, Thm. 3.12] implies that there are only finitely many quadratic elements of $\overline{\mathbb{Q}}$ that are preperiodic for f_c . Therefore, every graph appearing in Poonen's paper [31] — that is, every graph of the form $G(f_c, \mathbb{Q})$ with $c \in \mathbb{Q}$ — will also occur as a graph $G(f_c, K)$ for some quadratic field K (in fact, for all but finitely many such K). These graphs all appear in Appendix B and are labeled

$$0, 2(1), 3(1,1), 3(2), 4(1,1), 4(2), 5(1,1)\text{a}, 6(1,1), 6(2), 6(3), 8(2,1,1), \text{ and } 8(3).$$

For every graph G in the above list, Poonen provided an explicit parameterization of the rational numbers c for which $G(f_c, \mathbb{Q}) \cong G$. This essentially achieves, for each of the graphs above, our stated goal of describing the pairs (K, c) giving rise to a given graph. There still remains the following question, which will not be further discussed here: given $c \in \mathbb{Q}$, how can one determine the quadratic fields K for which $\text{PrePer}(f_c, K) \neq \text{PrePer}(f_c, \mathbb{Q})$ and moreover, what are all the graphs $G(f_c, K)$ that can arise in this way? From the data in Appendix C we see that many of the graphs shown in Appendix B are induced by a rational number c .

3.2. Preliminaries. We collect here a few results that will be used repeatedly throughout this section.

Let X be a smooth, projective, geometrically integral curve defined over \mathbb{Q} ; let g denote the genus of X , and assume that $g \geq 2$. Let r be the rank of the group $\text{Jac}(X)(\mathbb{Q})$, where $\text{Jac}(X)$ denotes the Jacobian variety of X . By Faltings' theorem we know that $X(\mathbb{Q})$ is a finite set; the following three results can be used to obtain explicit upper bounds on the size of this set under the assumption that $r < g$.

Theorem 3.1 (Coleman). *Suppose that $r < g$ and let $p > 2g$ be a prime of good reduction for X . Let \mathcal{X}/\mathbb{Z}_p be a model of X with good reduction. Then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}(\mathbb{F}_p) + 2g - 2.$$

Proof. See the proof of Corollary 4a in [6] and the remark following the corollary. \square

Theorem 3.2 (Lorenzini-Tucker). *Assume that $r < g$. Let p be a prime of good reduction for X , and let \mathcal{X}/\mathbb{Z}_p be a model of X with good reduction. If d is a positive integer such that $p > d$ and $p^d > 2g - 1 + d$, then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}(\mathbb{F}_p) + \left(\frac{p-1}{p-d}\right)(2g-2).$$

Proof. This follows from [23, Thm. 1.1] □

Theorem 3.3 (Stoll). *Suppose that $r < g$ and let $p > 2r + 2$ be a prime of good reduction for X . Let \mathcal{X}/\mathbb{Z}_p be a model of X with good reduction. Then*

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}(\mathbb{F}_p) + 2r.$$

Proof. This is a consequence of [37, Cor. 6.7]. □

The next result is crucial for obtaining equations for the parameterizing curves of the graphs to be considered in this section. Different versions of the various parts of this result have appeared elsewhere (for instance, [31] and [40]), but not exactly in the form we will need. Hence, we include here the precise statements we require for our purposes.

Proposition 3.4. *Let K be a number field and let $f(z) = z^2 + c$ with $c \in K$.*

- (1) *If $f(z)$ has a fixed point $p \in K$, then there is an element $x \in K$ such that*

$$p = x + 1/2, \quad c = 1/4 - x^2.$$

Moreover, the point $p' = 1/2 - x$ is also fixed by $f(z)$.

- (2) *If $f(z)$ has a point $p \in K$ of period 2, then there is a nonzero element $x \in K$ such that*

$$p = x - 1/2, \quad c = -3/4 - x^2.$$

Moreover, the orbit of p under f consists of the points p and

$$f(p) = -x - 1/2.$$

- (3) *If $f(z)$ has a point $p \in K$ of period 3, then there is an element $x \in K$ such that $x(x+1)(x^2+x+1) \neq 0$ and*

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

Moreover, the orbit of p under f consists of the points p and

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

$$f^2(p) = -\frac{x^3 + 2x^2 + 3x + 1}{2x(x+1)}.$$

- (4) If $f(z)$ has a point $p \in K$ of period 4, then there are elements $x, y \in K$ with $y(x^2 - 1) \neq 0$ such that

$$y^2 = F_{16}(x) := -x(x^2 + 1)(x^2 - 2x - 1)$$

and

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

Moreover, the orbit of p under f consists of the points p and

$$f(p) = -\frac{x+1}{2(x-1)} + \frac{y}{2x(x+1)},$$

$$f^2(p) = \frac{x-1}{2(x+1)} - \frac{y}{2x(x-1)},$$

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

Proof. (1) The equation $p^2 + c = p$ can be rewritten as $(p - 1/2)^2 + c - 1/4 = 0$. Letting $x = p - 1/2$ we then have $x^2 + c - 1/4 = 0$, and the result follows.

(2) Since $f^2(p) = p$ and $f(p) \neq p$, then we have the equation

$$p^2 + p + c + 1 = \frac{f^2(p) - p}{f(p) - p} = 0.$$

Letting $x = p + 1/2$, this equation becomes $x^2 + c + 3/4 = 0$, and hence $c = -3/4 - x^2$. Expressing p and c in terms of x we obtain

$$f(p) = p^2 + c = -x - 1/2.$$

We must have $x \neq 0$ since p and $f(p)$ are distinct.

(3) See the proof of [40, Thm. 3].

(4) The existence of x and y and the expressions for p and c in terms of x and y can be obtained from the discussion in [26, page 91–93]; the expressions for the elements of the orbit of p are obtained by a straightforward calculation from the expressions for p and c . Finally, we must have $y \neq 0$ since otherwise p would have period smaller than 4: indeed, note that $p = f^2(p)$ if $y = 0$. \square

Remark. Note that part (2) of Proposition 3.4 implies that $f(z)$ can have at most two points of period 2 in K , so that the graph $G(f, K)$ can have at most one 2-cycle. This fact will be needed in the analysis of some of the graphs below.

The following lemma will allow us to show that certain preperiodic graph structures occur infinitely many times over quadratic fields.

Lemma 3.5. *Let $p(x) \in \mathbb{Q}[x]$ have nonzero discriminant and degree ≥ 3 . For every rational number r , define a field K_r by*

$$K_r := \mathbb{Q}\left(\sqrt{p(r)}\right).$$

Then, for every interval $I \subset \mathbb{R}$ of positive length, the set

$$\Sigma(I, p) = \{K_r : r \in \mathbb{Q} \cap I\}$$

contains infinitely many quadratic fields. In particular, if the polynomial function $p : \mathbb{R} \rightarrow \mathbb{R}$ induced by $p(x)$ takes both positive and negative values, then $\Sigma(I, p)$ contains infinitely many real (resp. imaginary) quadratic fields.

Proof. For the proof of the statement that $\Sigma(I, p)$ contains infinitely many quadratic fields, see Appendix A. The second part follows from this statement by choosing an interval I_1 where $p > 0$ and an interval I_2 where $p < 0$. \square

Use of computational software. In preparing this article we have made extensive use of both the Magma [2] and Sage [34] computer algebra systems. Our data-gathering computations explained in §4.4 were carried out by implementing the algorithms of §4.3 in Sage; these methods rely on the algorithm [8] for listing elements of bounded height in number fields, which is also implemented in Sage. In Magma, we have made use of some rather sophisticated tools; in particular, we apply the `RankBound` function, which implements Stoll’s algorithm [35] of 2-descent for bounding the rank of the group of rational points on the Jacobian of a hyperelliptic curve over \mathbb{Q} . In addition, we frequently use the `CurveQuotient` function relying on Magma’s invariant theory functionality to determine the quotient of a curve by an automorphism. Whenever this function is used in our paper, one can easily check by hand that the output is correct. Finally, for the analysis of the graph 14(3,1,1) in §3.19 we require the `Chabauty` function, which implements a method due to Bruin and Stoll [3, §4.4] combining the method of Chabauty and Coleman with a Mordell–Weil sieve in order to determine the set of rational points on a curve of genus 2 with Jacobian of rank 1.

We can now proceed to the main task of this paper, namely to study the preperiodic graph structures appearing in Appendix B. We will consider the graphs one at a time, following the order in which they are listed in the appendix; however, the graphs discussed in §3.1 and §5 will not be considered henceforth in this section. The format for our discussion of each graph G is roughly the same for all graphs: first, a parameterizing curve C is constructed and an explicit map is given which shows how to use points on C to obtain instances of G . Next, a theorem is proved which describes the set of quadratic points on C ; finally, we use this theorem to deduce information about the instances of G defined over quadratic fields. When there are infinitely many examples of a particular graph occurring over quadratic fields, we will also be interested in deciding whether it occurs over both real and imaginary fields, or only one type of quadratic field.

3.3. Graph 8(1,1)a.

Lemma 3.6. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

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

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$a = -\frac{2x}{x^2 - 1}, \quad b = \frac{y}{x^2 - 1}, \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : (x^4 - 1)(x^2 + 3) \neq 0\}$ to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of type 1_2 for the map f_c satisfying $f_c^2(a) \neq f_c^2(b)$.



FIGURE 1. Graph type 8(1,1)a

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining a, b, c as in the lemma, it is straightforward to verify that a is a point of type 1_2 for the map f_c ; that $f_c^2(b)$ is fixed by f_c ; and that the following relations hold:

$$(3.1) \quad f_c^2(b) - f_c(b) = \frac{2(x^2 + 1)}{x^2 - 1}, \quad f_c^2(b) - f_c^2(a) = \frac{x^2 + 3}{x^2 - 1}.$$

It follows from these relations that if $(x^2 + 1)(x^2 + 3) \neq 0$, then b is of type 1_2 and $f_c^2(a) \neq f_c^2(b)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a and b are points of type 1_2 for the map f_c satisfying $f_c^2(a) \neq f_c^2(b)$. The argument given in [31, page 19] then shows that there exists a point $(x, y) \in C(K)$ with $x^2 \neq 1$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.1) imply that necessarily $(x^2 + 1)(x^2 + 3) \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = \frac{-a}{a^2 + c}, \quad y = \frac{2b}{a^2 + c}. \quad \square$$

Remark. As shown in [31, page 19], the curve C is birational over \mathbb{Q} to the elliptic curve 24a4 in Cremona's tables [7].

Proposition 3.7. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 8(1,1)a.*

Proof. Let $p(x) = -(x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $p(x)$ we obtain infinitely many real (resp. imaginary) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{p(r)})$ with $r \in \mathbb{Q}$. For every such field there is a point $(r, \sqrt{p(r)}) \in C(K_r)$ which necessarily satisfies $(r^4 - 1)(r^2 + 3) \neq 0$; hence, by Lemma 3.6 there is an element $c \in K_r$ such that f_c has points $a, b \in K_r$ of type 1_2 with $f_c^2(a) \neq f_c^2(b)$. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type $8(1,1)a$ we need the additional condition that $ab \neq 0$, so that the points $f_c(a)$ and $f_c(b)$ each have two distinct preimages. We have

$$ab^2 = \frac{2r(r^2 - 3)(r^2 + 1)}{(r^2 - 1)^3},$$

so the condition $ab \neq 0$ will be satisfied as long as $r \neq 0$. □

3.4. Graph $8(1,1)b$.

Lemma 3.8. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

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

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^2 = \text{Spec } \mathbb{Q}[p, c]$ given by

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

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : x^2 \neq 1\}$ to the set of all pairs $(p, c) \in K^2$ such that p is a point of type 1_3 for the map f_c .

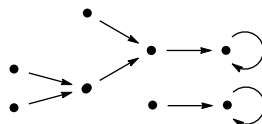


FIGURE 2. Graph type $8(1,1)b$

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining p and c as in the lemma, it is straightforward to verify that p is a point of type 1_3 for the map f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $p, c \in K$ are such that p is a point of type 1_3 for f_c . Then an argument given in [31, page 22] shows that there exists a point $(x, y) \in C(K)$ with $x^2 \neq 1$ such that $\varphi(x, y) = (p, c)$. To see that φ is injective, one can verify that if $\varphi(x, y) = (p, c)$, then

$$x = \frac{f_c(p)}{f_c^2(p)}, \quad y = p(x^2 - 1). \quad \square$$

Remark. As shown in [31, page 23], the curve C is birational over \mathbb{Q} to the elliptic curve 11a3 in Cremona’s tables [7], which is the modular curve $X_1(11)$.

Proposition 3.9. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 8(1,1)b.*

Proof. Let $q(x) = 2(x^3 + x^2 - x + 1) \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $q(x)$ we obtain infinitely many real (resp. imaginary) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{q(r)})$ with $r \in \mathbb{Q}$. For every such field there is a point $(r, \sqrt{q(r)}) \in C(K_r)$ which necessarily satisfies $r^2 \neq 1$; hence, by Lemma 3.8 there is an element $c \in K_r$ such that f_c has a point $p \in K_r$ of type 1₃. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type 8(1,1)b we need the additional condition that $p \cdot f_c(p) \cdot c(4c - 1) \neq 0$. Indeed, the condition $p \cdot f_c(p) \neq 0$ ensures that $f_c(p)$ and $f_c^2(p)$ each have two distinct preimages, while the condition $c(4c - 1) \neq 0$ guarantees that f_c has two distinct fixed points, and each fixed point has a preimage different from itself. Now, one can check that

$$p^2 \cdot f_c(p) \cdot c(4c - 1) = \frac{8r(r^3 + r^2 - r + 1)(r^2 + 1)(r^2 + 3)^2}{(r^2 - 1)^7},$$

so we will have $p \cdot f_c(p) \cdot c(4c - 1) \neq 0$ as long as $r \neq 0$. □

3.5. Graph 8(2)a.

Lemma 3.10. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

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

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

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

For every number field K , the map φ induces a bijection from the set

$$\{(x, y) \in C(K) : x(x^2 - 1)(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of type 2₂ for the map f_c satisfying $f_c^2(a) \neq f_c^2(b)$.

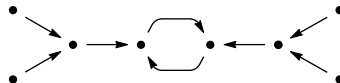


FIGURE 3. Graph type 8(2)a

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining a, b, c as in the lemma, it is a routine calculation to verify that $f_c^2(a) = f_c^4(a)$, $f_c^2(b) = f_c^4(b)$, $f_c^2(b) = f_c^3(a)$, and

$$(3.2) \quad \begin{aligned} f_c^3(a) - f_c^2(a) &= \frac{x^2 + 4x - 1}{x^2 - 1}, \\ f_c^3(a) - f_c(a) &= \frac{4x}{x^2 - 1}, \\ f_c(b) - f_c^3(b) &= \frac{2(x^2 + 2x - 1)}{x^2 - 1}. \end{aligned}$$

From these relations it follows that if $x(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$, then a and b are points of type 2_2 for f_c with $f_c^2(a) \neq f_c^2(b)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a and b are points of type 2_2 for the map f_c satisfying $f_c^2(a) \neq f_c^2(b)$. Since the map f_c can have only one 2-cycle, the points $f_c^2(a)$ and $f_c^2(b)$ must form a 2-cycle. The argument given in [31, page 20] then shows that there is a point $(x, y) \in C(K)$ with $x^2 \neq 1$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.2) imply that $x(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = \frac{a - 1}{a^2 + c}, \quad y = b(x^2 - 1). \quad \square$$

Remark. As shown in [31, page 20], the curve C is birational over \mathbb{Q} to the elliptic curve 40a3 in Cremona's tables [7].

Proposition 3.11. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 8(2)a.*

Proof. Let $p(x) = 2(x^4 + 2x^3 - 2x + 1) \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $p(x)$ we obtain infinitely many quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{p(r)})$ with $r \in \mathbb{Q}^*$. For every such field there is a point $(r, \sqrt{p(r)}) \in C(K_r)$ which necessarily satisfies

$$(r^2 - 1)(r^2 + 4r - 1)(r^2 + 2r - 1) \neq 0;$$

hence, by Lemma 3.10 there is an element $c \in K_r$ such that f_c has points $a, b \in K_r$ of type 2_2 satisfying $f_c^2(a) \neq f_c^2(b)$. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type 8(2)a we need the additional condition $ab \neq 0$ so that $f_c(a)$ and $f_c(b)$ each have two distinct preimages. Now, one can check that

$$(3.3) \quad -ab^2 = \frac{2(r^2 + 1)(r^4 + 2r^3 - 2r + 1)}{(r^2 - 1)^3},$$

so the condition $ab \neq 0$ is automatically satisfied since $r \in \mathbb{Q}$.

Note that the polynomial function $p : \mathbb{R} \rightarrow \mathbb{R}$ induced by $p(x)$ only takes positive values, so that all fields K_r are real quadratic fields. Hence, this argument proves the statement only for real quadratic fields. To prove the statement for imaginary quadratic fields, we first obtain a Weierstrass equation for the elliptic curve birational to C . The following are inverse rational maps between C and the elliptic curve E with equation

$$Y^2 = X^3 - 2X + 1 :$$

$$(x, y) \mapsto \left(\frac{2x^2 + y}{(x-1)^2}, \frac{3x^3 + 3x^2 + 2xy - 3x + 1}{(x-1)^3} \right),$$

$$(X, Y) \mapsto \left(\frac{X^2 + 2Y}{X^2 - 4X + 2}, \frac{2X^4 + 8X^3 + 8X^2Y - 24X^2 - 8XY + 24X - 8}{(X^2 - 4X + 2)^2} \right).$$

Let $q(X) = X^3 - 2X + 1 \in \mathbb{Q}[X]$. Applying Lemma 3.5 to the polynomial $q(X)$ we obtain infinitely many imaginary quadratic fields of the form $K_R = \mathbb{Q}(\sqrt{q(R)})$ with $R \in \mathbb{Q}$. For every such field there is a point $(R, \sqrt{q(R)}) \in E(K_R)$; applying the change of variables above we obtain a point $(r, s) \in C(K_R)$ with

$$(3.4) \quad r = \frac{R^2 + 2\sqrt{q(R)}}{R^2 - 4R + 2}.$$

In particular, r must satisfy $r(r^2 - 1)(r^2 + 4r - 1)(r^2 + 2r - 1) \neq 0$, since otherwise r would be rational or would generate a real quadratic field. We can now apply Lemma 3.10 to see that there is an element $c \in K_R$ such that f_c has points $a, b \in K_R$ of type 2_2 satisfying $f_c^2(a) \neq f_c^2(b)$. From (3.3) and (3.4) it follows that there are only finitely many values of $R \in \mathbb{Q}$ for which we might have $ab = 0$. Hence, for all but finitely many values of R , this construction will yield a graph $G(f_c, K_R)$ containing a subgraph of type 8(2)a. \square

3.6. Graph 8(2)b.

Lemma 3.12. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

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

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^2 = \text{Spec } \mathbb{Q}[p, c]$ given by

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

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : x(x^2 - 1)(x^2 + 4x - 1) \neq 0\}$ to the set of all pairs $(p, c) \in K^2$ such that p is a point of type 2_3 for the map f_c .

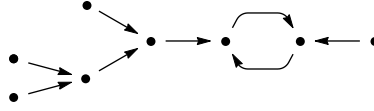


FIGURE 4. Graph type 8(2)b

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining p, c as in the lemma, it is straightforward to verify that $f_c^3(p) = f_c^5(p)$ and

$$(3.5) \quad f_c^4(p) - f_c^2(p) = \frac{4x}{x^2 - 1}, \quad f_c^4(p) - f_c^3(p) = \frac{x^2 + 4x - 1}{x^2 - 1}.$$

From these relations it follows that if $x(x^2 + 4x - 1) \neq 0$, then p is of type 2_3 for f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $p, c \in K$ are such that p is a point of type 2_3 for the map f_c . Then an argument given in [31, page 23] shows that there is a point $(x, y) \in C(K)$ with $x^2 \neq 1$ such that $\varphi(x, y) = (p, c)$. Furthermore, the relations (3.5) imply that we must have $x(x^2 + 4x - 1) \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (p, c)$, then

$$x = \frac{f_c(p) - 1}{f_c^2(p)}, \quad y = p(x^2 - 1). \quad \square$$

Remark. The curve C is the same curve parameterizing the graph 8(1,1)b. As noted earlier, C is birational to the modular curve $X_1(11)$.

Proposition 3.13. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 8(2)b.*

Proof. Let $q(x) = 2(x^3 + x^2 - x + 1) \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $q(x)$ we obtain infinitely many real (resp. imaginary) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{q(r)})$ with $r \in \mathbb{Q}^*$. For every such field there is a point $(r, \sqrt{q(r)}) \in C(K_r)$ which necessarily satisfies $r^2 \neq 1$; hence, by Lemma 3.12 there is an element $c \in K_r$ such that f_c has a point $p \in K_r$ of type 2_3 . In order to conclude that $G(f_c, K_r)$ contains a subgraph of type 8(2)b we need the additional condition $p \cdot f_c(p) \cdot f_c^3(p) \neq 0$ so that $f_c(p), f_c^2(p)$, and $f_c^4(p)$ each have two distinct preimages. One can check that

$$p^2 \cdot f_c(p) \cdot f_c^3(p) = \frac{2(r^3 + r^2 - r + 1)(r^2 + 1)(r^2 + 2r - 1)}{(r^2 - 1)^4},$$

so in fact the condition $p \cdot f_c(p) \cdot f_c^3(p) \neq 0$ is automatically satisfied since $r \in \mathbb{Q}$. □

3.7. Graph 8(4).

Lemma 3.14. *Let C/\mathbb{Q} be the affine curve of genus 2 defined by the equation*

$$y^2 = F_{16}(x) := -x(x^2 + 1)(x^2 - 2x - 1).$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^2 = \text{Spec } \mathbb{Q}[p, c]$ given by

$$(3.6) \quad p = \frac{x-1}{2(x+1)} + \frac{y}{2x(x-1)}, \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x-1)^2(x+1)^2}.$$

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : y(x^2 - 1) \neq 0\}$ to the set of all pairs $(p, c) \in K^2$ such that p is a point of period 4 for the map f_c .

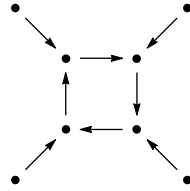


FIGURE 5. Graph type 8(4)

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x(x^2 - 1) \neq 0$. Defining p and c as in the lemma, it is straightforward to verify the relations

$$(3.7) \quad f_c^4(p) = p, \quad p - f_c^2(p) = \frac{y}{x(x-1)}.$$

The condition that $y \neq 0$ thus implies that p has period 4. Hence, φ gives a well-defined map. The fact that φ is surjective follows immediately from Proposition 3.4. To see that φ is injective, one can verify that if $\varphi(x, y) = (p, c)$, then

$$x = \frac{1 + f_c^2(p) + p}{1 - f_c^2(p) - p}, \quad y = \frac{2px(x^2 - 1) - x(x-1)^2}{x+1}. \quad \square$$

Remark. As noted in §2.3, the curve C is birational over \mathbb{Q} to the modular curve $X_1(16)$.

Proposition 3.15. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 8(4).*

Proof. Applying Lemma 3.5 to the polynomial $F_{16}(x)$ we obtain infinitely many real (resp. imaginary) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{F_{16}(r)})$ with $r \in \mathbb{Q}^*$. For every such field there is a point $(r, \sqrt{F_{16}(r)}) \in C(K_r)$ which necessarily satisfies $(r^2 - 1)\sqrt{F_{16}(r)} \neq 0$; hence, by Lemma 3.14 there

is an element $c \in K_r$ such that f_c has a point $p \in K_r$ of period 4. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type 8(4) we need the additional condition that every point in the orbit of p is nonzero, so that each point has two distinct preimages. Using Proposition 3.4(4) we find that if $p \cdot f_c(p) \cdot f_c^2(p) \cdot f_c^3(p) = 0$, then one of the following equations will be satisfied:

$$\begin{aligned} r(r-1)^4 + (r^2+1)(r+1)^2(r^2-2r-1) &= 0, \\ r(r+1)^4 + (r^2+1)(r-1)^2(r^2-2r-1) &= 0. \end{aligned}$$

However, one can verify that neither of these equations has a rational solution; therefore, every point in the orbit of p is necessarily nonzero. \square

Remark. Our search in §4.4 failed to produce an example of a graph of type 8(4) over an imaginary quadratic field, though the previous proposition suggests that there are infinitely many such examples. The reason for this is that, even for rational parameters x of moderate size, the discriminant of the field $K = \mathbb{Q}(\sqrt{F_{16}(x)})$ may be large, and the complexity of the rational function defining c forces the height of c to be large as well, thus placing the pair (K, c) outside of our search range. We obtain an instance of this graph by taking $x = 5$ in (3.6); this leads to the pair $(K, c) = (\mathbb{Q}(\sqrt{-455}), 199/720)$. A computation of preperiodic points using the algorithm developed in §4.3 shows that, indeed, the graph $G(f_c, K)$ for this pair (K, c) is of type 8(4).

We end our discussion of the graph type 8(4) by stating explicitly how to obtain all pairs (K, c) consisting of a quadratic field K and an element $c \in K$ for which $G(f_c, K)$ is of this type.

Theorem 3.16. *Let K be a quadratic field. Suppose that there exists an element $c \in K$ such that $G(f_c, K)$ is of type 8(4). Then there is a rational number $x \notin \{0, \pm 1\}$ such that*

$$(3.8) \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x - 1)^2(x + 1)^2}$$

and $K = \mathbb{Q}(\sqrt{-x(x^2 + 1)(x^2 - 2x - 1)})$.

Proof. By Lemma 3.14 there exists a point $(x, y) \in C(K)$ with $y(x^2 - 1) \neq 0$ such that c is given by (3.8). We claim that (x, y) cannot be a rational point on C . Indeed, C is an affine model of the curve $X_1(16)$, which has exactly six rational points. Therefore, C has five rational points, and it is easy to see that they are $(0, 0)$ and $(\pm 1, \pm 2)$. Thus, if $(x, y) \in C(\mathbb{Q})$, then either $x = 0$ or $x = \pm 1$; however, both possibilities are precluded by the fact that $y(x^2 - 1) \neq 0$. Therefore, (x, y) is a quadratic point on C . Since $y \neq 0$, it follows from Theorem 2.4 that x must be a rational number. In particular, since (x, y) is a quadratic point, then $K = \mathbb{Q}(x, y) = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{-x(x^2 + 1)(x^2 - 2x - 1)})$. \square

3.8. Graph 10(1,1)a. Our search described in §4.4 produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{-7}), \frac{3}{16} \right)$$

for which the graph $G(f_c, K)$ is of type 10(1,1)a. We show here that this is the only such pair (K, c) with K a quadratic number field and $c \in K$.

Lemma 3.17. *Let C/\mathbb{Q} be the affine curve of genus 4 defined by the equations*

$$(3.9) \quad \begin{cases} y^2 = 2(x^3 + x^2 - x + 1) \\ z^2 = -2(x^3 - x^2 - x - 1). \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$a = \frac{y}{x^2 - 1}, \quad b = \frac{z}{x^2 - 1}, \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set $\{(x, y, z) \in C(K) : x(x^2 - 1) \neq 0\}$ to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of type 1_3 for the map f_c satisfying $f_c^2(a) = f_c^2(b)$ and $f_c(a) \neq f_c(b)$.

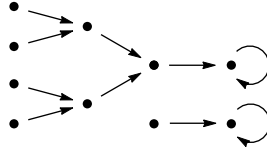


FIGURE 6. Graph type 10(1,1)a

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ satisfies $x^2 \neq 1$. Defining a, b, c as in the lemma, it is a routine calculation to verify that a and b are points of type 1_3 for the map f_c satisfying $f_c^2(a) = f_c^2(b)$; moreover, we have the relation

$$(3.10) \quad f_c(a) - f_c(b) = \frac{4x}{x^2 - 1}.$$

It follows that if $x \neq 0$, then $f_c(a) \neq f_c(b)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a and b are points of type 1_3 for the map f_c satisfying $f_c^2(a) = f_c^2(b)$ and $f_c(a) \neq f_c(b)$. Then an argument given in [31, page 22] shows that there is an element $x \in K \setminus \{\pm 1\}$ such that

$$(3.11) \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}, \quad a^2 = \frac{2(x^3 + x^2 - x + 1)}{(x^2 - 1)^2}.$$

Since $a^2 + c = f_c(a) = -f_c(b) = -b^2 - c$, then using (3.11) we obtain

$$b^2 = \frac{-2(x^3 - x^2 - x - 1)}{(x^2 - 1)^2}.$$

Letting $y = a(x^2 - 1)$ and $z = b(x^2 - 1)$ we then have a point $(x, y, z) \in C(K)$ with $x^2 \neq 1$ such that $\varphi(x, y, z) = (a, b, c)$. Furthermore, the relation (3.10) implies that $x \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y, z) = (a, b, c)$, then

$$x = \frac{f_c(a)}{f_c^2(a)}, \quad y = a(x^2 - 1), \quad z = b(x^2 - 1). \quad \square$$

Theorem 3.18. *With C as in Lemma 3.17 we have the following:*

- (1) $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.
- (2) *If K is a quadratic field different from $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-7})$, then $C(K) = C(\mathbb{Q})$.*
- (3) *For $K = \mathbb{Q}(\sqrt{2})$, $C(K) \setminus C(\mathbb{Q}) = \{(0, \pm\sqrt{2}, \pm\sqrt{2})\}$.*
- (4) *For $K = \mathbb{Q}(\sqrt{-7})$, $C(K) \setminus C(\mathbb{Q})$ consists of the points*
 $(x, \pm(2x - 4), \pm(2x + 4))$ *with* $x^2 + 7 = 0$.

Proof. The equation $y^2 = 2(x^3 + x^2 - x + 1)$ defines the elliptic curve with Cremona label 11a3. This curve has rank 0 and torsion order 5; the affine rational points are $(\pm 1, \pm 2)$. The equation $z^2 = -2(x^3 - x^2 - x - 1)$ defines the same elliptic curve, and the affine rational points are again $(\pm 1, \pm 2)$. Therefore, $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 2$, contradicting the assumption that (x, y, z) is a quadratic point on C ; hence, $x \neq \pm 1$. It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. By the same argument, $z \notin \mathbb{Q}$. Therefore, $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the rational numbers $2(x^3 + x^2 - x + 1)$ and $-2(x^3 - x^2 - x - 1)$ have the same squarefree part, and thus their product is a square. Hence, there is a rational number w such that

$$(3.12) \quad w^2 = -x^6 + 3x^4 + x^2 + 1.$$

Let X be the hyperelliptic curve of genus 2 defined by (3.12). We claim that the following is a complete list of rational points on X :

$$X(\mathbb{Q}) = \{(\pm 1, \pm 2), (0, \pm 1)\}.$$

To see this, note that X has a nontrivial involution given by

$$(x, w) \mapsto (-x, -w).$$

The quotient of X by this involution is the elliptic curve E defined by the equation $v^2 = u^3 + u^2 + 3u - 1$; this is the curve 44a1 in Cremona's tables. The quotient map $X \rightarrow E$ of degree 2 is given by $(x, w) \mapsto (1/x^2, w/x^3)$.

The curve E has exactly 3 rational points, namely the point at infinity and the points $(1, \pm 2)$. It follows that X has at most six rational points, and since we have already listed six points, these must be all.

Returning to (3.12), we have a point $(x, w) \in X(\mathbb{Q})$ with $x \neq \pm 1$, so we conclude that $x = 0$. By (3.9) we then have $y^2 = z^2 = 2$. Thus, we have shown that the only quadratic points on C having a rational x -coordinate are the points $(x, y, z) = (0, \pm\sqrt{2}, \pm\sqrt{2})$.

Case 2. x is quadratic. By Lemma 2.2 applied to the equation

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

there exist a rational number v and a point $(x_0, y_0) \in \{(\pm 1, \pm 2)\}$ such that

$$(3.13) \quad x^2 + \frac{2x_0 - v^2 + 2}{2}x + \frac{2x_0^2 + v^2x_0 + 2x_0 - 2y_0v - 2}{2} = 0.$$

Similarly, applying Lemma 2.2 to the equation $z^2 = -2(x^3 - x^2 - x - 1)$ we see that there exist a rational number w and a point $(x_1, z_1) \in \{(\pm 1, \pm 2)\}$ such that

$$(3.14) \quad x^2 + \frac{2x_1 + w^2 - 2}{2}x + \frac{2x_1^2 - w^2x_1 - 2x_1 + 2z_1w - 2}{2} = 0.$$

Comparing (3.13) and (3.14) we obtain the system

$$\begin{cases} 2x_0 - v^2 + 4 = 2x_1 + w^2 \\ 2x_0^2 + v^2x_0 + 2x_0 - 2y_0v = 2x_1^2 - w^2x_1 - 2x_1 + 2z_1w. \end{cases}$$

For each choice of points $(x_0, y_0), (x_1, z_1)$ the above system defines a zero-dimensional scheme S in the (v, w) plane over \mathbb{Q} , and hence all its rational points may be determined. There are a total of 16 choices of pairs $(x_0, y_0), (x_1, z_1)$, leading to 16 schemes S . Using the Magma function `RationalPoints` we find all the rational points (v, w) on these schemes, and in every case check whether the polynomial (3.13) is irreducible. This occurs for four of these schemes, and for all of these (3.13) becomes $x^2 + 7 = 0$. The equations (3.9) now imply that $y^2 = (2x - 4)^2$ and $z^2 = (2x + 4)^2$. Thus, we have shown that the only quadratic points on C having a quadratic x -coordinate are those of the form $(x, \pm(2x - 4), \pm(2x + 4))$ with $x^2 + 7 = 0$.

In conclusion, the quadratic points on C are the points $(0, \pm\sqrt{2}, \pm\sqrt{2})$ defined over the field $\mathbb{Q}(\sqrt{2})$ and the points $(x, \pm(2x - 4), \pm(2x + 4))$ where $x^2 + 7 = 0$, defined over the field $\mathbb{Q}(\sqrt{-7})$; the theorem now follows immediately. \square

Corollary 3.19. *Let K be a quadratic field and let $c \in K$. Suppose that $G(f_c, K)$ contains a graph of type 10(1,1)a. Then $c = 3/16$ and $K = \mathbb{Q}(\sqrt{-7})$.*

Proof. By Lemma 3.17 there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that

$$(3.15) \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

It follows from Theorem 3.18 that (x, y, z) is a quadratic point on C with $x \neq 0$. Therefore, $K = \mathbb{Q}(\sqrt{-7})$ and $x^2 + 7 = 0$. From (3.15) we then obtain $c = 3/16$. \square

3.9. Graph 10(2,1,1)a.

Lemma 3.20. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

$$y^2 = 5x^4 - 8x^3 + 6x^2 + 8x + 5.$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$a = \frac{3x^2 + 1}{2(x^2 - 1)}, \quad b = \frac{y}{2(x^2 - 1)}, \quad c = -\frac{3x^4 + 10x^2 + 3}{4(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : x(x^2 - 1)(x^2 - 4x - 1) \neq 0\}$ to the set of all triples $(a, b, c) \in K^3$ such that a is a fixed point and b is a point of type 2_2 for the map f_c .

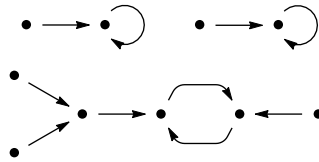


FIGURE 7. Graph type 10(2,1,1)a

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining a, b, c as in the lemma, it is straightforward to verify that a is a fixed point for f_c ; that $f_c^2(b) = f_c^4(b)$, and that the following relations hold:

$$(3.16) \quad f_c^3(b) - f_c^2(b) = \frac{4x}{x^2 - 1}, \quad f_c(b) - f_c^3(b) = \frac{x^2 - 4x - 1}{x^2 - 1}.$$

From these relations it follows that if $x(x^2 - 4x - 1) \neq 0$, then b is of type 2_2 for f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a is a fixed point and b is a point of type 2_2 for the map f_c . Then an argument given in [31, page 21–22] shows that there exists a point $(x, y) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.16)

imply that we must have $x^2 - 4x - 1 \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = \frac{1 + 2f_c^2(b)}{3 - 2a}, \quad y = 2b(x^2 - 1). \quad \square$$

Remark. As shown in [31, page 22], the curve C is birational over \mathbb{Q} to the elliptic curve 17a4 in Cremona's tables [7].

Proposition 3.21. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 10(2,1,1)a.*

Proof. Let $p(x) = 5x^4 - 8x^3 + 6x^2 + 8x + 5 \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $p(x)$ we obtain infinitely many quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{p(r)})$ with $r \in \mathbb{Q}$. For every such field K_r with $r \neq 0$ there is a point $(r, \sqrt{p(r)}) \in C(K_r)$ which necessarily satisfies $r(r^2 - 1)(r^2 - 4r - 1) \neq 0$; hence, by Lemma 3.20 there is an element $c \in K_r$ such that f_c has a fixed point $a \in K_r$ and a point $b \in K_r$ of type 2₂. In order to guarantee that $G(f_c, K_r)$ contains a subgraph of type 10(2,1,1)a we need the additional condition that $b \cdot f_c^2(b) \cdot c(4c - 1) \neq 0$. Indeed, the condition $b \cdot f_c^2(b) \neq 0$ ensures that $f_c(b)$ and $f_c^3(b)$ each have two distinct preimages, and the condition $c(4c - 1) \neq 0$ ensures that f_c has two distinct fixed points, each of which has a preimage different from itself. Now, one can check that

$$(3.17) \quad -b^2 \cdot f_c^2(b) \cdot c(4c - 1) \\ = \frac{(5r^4 - 8r^3 + 6r^2 + 8r + 5)(3r^2 + 1)(r^2 + 4r - 1)(r^2 + 3)(r^2 + 1)^2}{8(r^2 - 1)^7},$$

so the condition $b \cdot f_c^2(b) \cdot c(4c - 1) \neq 0$ is automatically satisfied since $r \in \mathbb{Q}$.

Note that the polynomial function $p : \mathbb{R} \rightarrow \mathbb{R}$ induced by $p(x)$ only takes positive values, so that all fields K_r are real quadratic fields. Hence, this argument proves the statement only for real quadratic fields. To prove the statement for imaginary quadratic fields, we first obtain a Weierstrass equation for the elliptic curve birational to C . We give inverse rational maps between C and the elliptic curve E given by $Y^2 = X^3 - 11X + 6$. The map $C \rightarrow E$ is given by

$$(x, y) \mapsto \left(\frac{2y + x^2 + 2x + 5}{(x - 1)^2}, \frac{2y(x + 3) + 6x^3 - 6x^2 + 18x + 14}{(x - 1)^3} \right).$$

The map back is given by

$$(X, Y) \mapsto \left(\frac{4Y + (X + 1)^2}{X^2 - 2X - 19}, \frac{8Y(X^2 + 10X + 9) + 4(X^4 + 2X^3 + 24X^2 + 46X - 233)}{(X^2 - 2X - 19)^2} \right).$$

Let $q(X) = X^3 - 11X + 6 \in \mathbb{Q}[X]$. Applying Lemma 3.5 to the polynomial $q(X)$ we obtain infinitely many imaginary quadratic fields of the form $K_R = \mathbb{Q}(\sqrt{q(R)})$ with $R \in \mathbb{Q}$. For every such field there is a point $(R, \sqrt{q(R)}) \in E(K_R)$; applying the change of variables above we obtain a point $(r, s) \in C(K_R)$ with

$$(3.18) \quad r = \frac{4\sqrt{q(R)} + (R + 1)^2}{R^2 - 2R - 19}.$$

In particular, r must satisfy $r(r^2 - 1)(r^2 - 4r - 1) \neq 0$, since otherwise r would be rational or would generate a real quadratic field. We can now apply Lemma 3.20 to see that there is an element $c \in K_R$ such that f_c has a fixed point $a \in K_R$ and a point $b \in K_R$ of type 2_2 . Once again, we must check the condition $b \cdot f_c^2(b) \cdot c(4c - 1) \neq 0$. From (3.17) and (3.18) it follows that there are only finitely many values of $R \in \mathbb{Q}$ for which we might have $b \cdot f_c^2(b) \cdot c(4c - 1) = 0$. Hence, for all but finitely many R , the above construction yields a graph $G(f_c, K_R)$ containing a subgraph of type $10(2,1,1)a$. \square

3.10. Graph $10(2,1,1)b$.

Lemma 3.22. *Let C/\mathbb{Q} be the affine curve of genus 1 defined by the equation*

$$y^2 = (5x^2 - 1)(x^2 + 3).$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$a = \frac{y}{2(x^2 - 1)}, \quad b = -\frac{x^2 - 4x - 1}{2(x^2 - 1)}, \quad c = -\frac{3x^4 + 10x^2 + 3}{4(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : x(x^2 - 1)(x^2 + 3) \neq 0\}$ to the set of all triples $(a, b, c) \in K^3$ such that a is a point of type 1_2 and b is a point of period 2 for the map f_c .

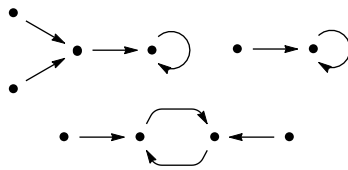


FIGURE 8. Graph type $10(2,1,1)b$

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x^2 \neq 1$. Defining a, b, c as in the lemma, it is straightforward to verify that $f_c^2(a)$ is fixed by f_c ; that $b = f_c^2(b)$; and that

$$(3.19) \quad b - f_c(b) = \frac{4x}{x^2 - 1}, \quad f_c(a) - f_c^2(a) = \frac{x^2 + 3}{x^2 - 1}.$$

From these relations it follows that if $x(x^2 + 3) \neq 0$, then b is a point of period 2 and a is of type 1_2 for f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a is a point of type 1_2 and b is a point of period 2 for the map f_c . Then an argument given in [31, page 21] shows that there exists a point $(x, y) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.19) imply that we must have $x^2 + 3 \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = -\frac{1 + 2f_c^2(b)}{1 + 2f_c^2(a)}, \quad y = 2a(x^2 - 1). \quad \square$$

Remark. As shown in [31, page 21], the curve C is birational over \mathbb{Q} to the elliptic curve 15a8 in Cremona's tables [7].

Proposition 3.23. *There are infinitely many real (resp. imaginary) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type $10(2,1,1)b$.*

Proof. Let $p(x) = (5x^2 - 1)(x^2 + 3) \in \mathbb{Q}[x]$. Applying Lemma 3.5 to the polynomial $p(x)$ we obtain infinitely many real (resp. imaginary) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{p(r)})$ with $r \in \mathbb{Q}$. For every such field K_r with $r \neq 0$ there is a point $(r, \sqrt{p(r)}) \in C(K_r)$ which necessarily satisfies $r(r^2 - 1)(r^2 + 3) \neq 0$; hence, by Lemma 3.22 there is an element $c \in K_r$ such that f_c has a point $a \in K_r$ of type 1_2 and a point $b \in K_r$ of period 2. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type $10(2,1,1)b$ we need the additional condition that $ac(4c - 1)b \cdot f_c(b) \neq 0$. Indeed, the condition $a \neq 0$ ensures that $f_c(a)$ has two distinct preimages, while the condition $c(4c - 1) \neq 0$ guarantees that f_c has two distinct fixed points, each of which has a preimage different from itself; the condition $b \cdot f_c(b) \neq 0$ ensures that b and $f_c(b)$ each have two distinct preimages. Now, one can check that

$$\begin{aligned} & a^2c(4c - 1)b \cdot f_c(b) \\ &= \frac{(5r^2 - 1)(r^2 + 3)^2(3r^2 + 1)(r^2 + 1)^2(r^2 - 4r - 1)(r^2 + 4r - 1)}{16(r^2 - 1)^8}, \end{aligned}$$

so the condition $ac(4c - 1)b \cdot f_c(b) \neq 0$ is automatically satisfied since $r \in \mathbb{Q}$. \square

3.11. Graph $10(3,1,1)$.

Lemma 3.24. *Let C/\mathbb{Q} be the affine curve of genus 2 defined by the equation*

$$y^2 = F_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$\begin{aligned} a &= \frac{x^3 + 2x^2 + x + 1}{2x(x + 1)}, \\ b &= \frac{1}{2} + \frac{y}{2x(x + 1)}, \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set $\{(x, y) \in C(K) : x(x+1)(x^2+x+1) \neq 0\}$ to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of periods 3 and 1, respectively, for the map f_c .

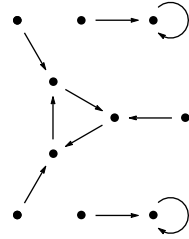


FIGURE 9. Graph type 10(3,1,1)

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x(x + 1) \neq 0$. Defining a, b, c as in the lemma, it is a routine calculation to verify that b is a fixed point for f_c ; that $f_c^3(a) = a$; and that

$$(3.20) \quad a - f_c(a) = \frac{x^2 + x + 1}{x(x + 1)}.$$

It follows from these relations that if $x^2 + x + 1 \neq 0$, then a has period 3 under f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a and b are points of periods 3 and 1, respectively, for the map f_c . Applying Proposition 3.4 we see that there are elements $\rho \in K$ and $x \in K \setminus \{0, -1\}$ such that

$$(3.21) \quad b = 1/2 + \rho, \quad c = 1/4 - \rho^2$$

and

$$(3.22) \quad \begin{aligned} a &= \frac{x^3 + 2x^2 + x + 1}{2x(x + 1)}, \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}. \end{aligned}$$

Equating the two expressions for c given in (3.21) and (3.22) and letting $y = 2x(x+1)\rho$ we obtain

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Thus, we have a point $(x, y) \in C(K)$ with $x(x+1) \neq 0$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.20) imply that $x^2 + x + 1 \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = a^2 + a + c, \quad y = x(x+1)(2b-1). \quad \square$$

Remark. As noted in §2.3, the curve C is birational over \mathbb{Q} to the modular curve $X_1(18)$.

Theorem 3.25. *Let K be a quadratic field. Suppose that there exists an element $c \in K$ such that $G(f_c, K)$ has a subgraph of type $10(3,1,1)$. Then there is a rational number $x \notin \{0, -1\}$ such that*

$$(3.23) \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}$$

and $K = \mathbb{Q}(\sqrt{F_{18}(x)})$. In particular, K is a real quadratic field.

Proof. By Lemma 3.24 there is a point $(x, y) \in C(K)$ with

$$x(x+1)(x^2+x+1) \neq 0$$

such that c is given by (3.23). We claim that (x, y) cannot be a rational point on C . Indeed, C is an affine model of the curve $X_1(18)$, which has exactly six rational points (two of them at infinity). Therefore, C has four rational points, and it is easy to see that they are $(0, \pm 1)$ and $(-1, \pm 1)$. Thus, if $(x, y) \in C(\mathbb{Q})$, then either $x = 0$ or $x = -1$; however, this contradicts the assumption that $x(x+1) \neq 0$. Therefore, (x, y) is a quadratic point on C . Since $x^2 + x + 1 \neq 0$, it follows from Theorem 2.4 that x must be a rational number. In particular, since (x, y) is a quadratic point, then $K = \mathbb{Q}(x, y) = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{F_{18}(x)})$. The fact that K is a real quadratic field now follows from the observation that the polynomial function $F_{18} : \mathbb{R} \rightarrow \mathbb{R}$ induced by $F_{18}(x)$ only takes positive values. \square

Proposition 3.26. *There are infinitely many (real) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type $10(3,1,1)$.*

Proof. Applying Lemma 3.5 to the polynomial $F_{18}(x)$ we obtain infinitely many (real) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{F_{18}(r)})$ with $r \in \mathbb{Q}$. For every such field there is a point $(r, \sqrt{F_{18}(r)}) \in C(K_r)$ which necessarily satisfies $r(r+1)(r^2+r+1) \neq 0$; hence, by Lemma 3.24 there is an element $c \in K_r$ such that f_c has points $a, b \in K_r$ of periods 3 and 1, respectively. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type $10(3,1,1)$ we need the additional condition that $a \cdot f_c(a) \cdot f_c^2(a) \cdot c(4c-1) \neq 0$. Indeed, the condition $c(4c-1) \neq 0$ guarantees that f_c has two distinct fixed points, each of which has a preimage different from itself; and the condition $a \cdot f_c(a) \cdot f_c^2(a) \neq 0$

ensures that every point in the orbit of a has two distinct preimages. The expression for c given in Lemma 3.24 implies that $c < 0$, so in fact the condition $c(4c - 1) \neq 0$ is automatically satisfied. Furthermore, one can verify that

$$-a \cdot f_c(a) \cdot f_c^2(a) = \frac{(r^3 + 2r^2 + r + 1)(r^3 - r - 1)(r^3 + 2r^2 + 3r + 1)}{8r^3(r + 1)^3},$$

so $a \cdot f_c(a) \cdot f_c^2(a) \neq 0$ since $r \in \mathbb{Q}$. □

Remark. Our search in §4.4 failed to produce an example of a graph of type 10(3,1,1), though the previous proposition suggests that there are infinitely many such examples. The reason for this is that, even for rational parameters x of moderate size, the discriminant of the field $K = \mathbb{Q}(\sqrt{F_{18}(x)})$ may be large, and the complexity of the rational function defining c forces the height of c to be large as well, thus placing the pair (K, c) outside of our search range. However, we expected this graph to occur infinitely times over quadratic fields, since Poonen [31, page 15] had showed that the curve parametrizing maps with a fixed point and a point of period 3 is the modular curve $X_1(18)$, which is hyperelliptic and therefore has infinitely many quadratic points. We obtain one instance of the graph by taking $x = 2$ in (3.23); this leads to the pair $(K, c) = (\mathbb{Q}(\sqrt{337}), -301/144)$. A computation of preperiodic points using the algorithm developed in §4.3 shows that, indeed, the graph $G(f_c, K)$ for this pair (K, c) is of type 10(3,1,1).

3.12. Graph 10(3,2).

Lemma 3.27. *Let C/\mathbb{Q} be the affine curve of genus 2 defined by the equation*

$$y^2 = F_{13}(x) := x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1.$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$\begin{aligned} a &= \frac{x^3 + 2x^2 + x + 1}{2x(x + 1)}, \\ b &= -\frac{1}{2} + \frac{y}{2x(x + 1)}, \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y) \in C(K) : xy(x + 1)(x^2 + x + 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of periods 3 and 2, respectively, for the map f_c .

Proof. Fix a number field K and suppose that $(x, y) \in C(K)$ satisfies $x(x + 1) \neq 0$. Defining a, b, c as in the lemma, it is straightforward to verify

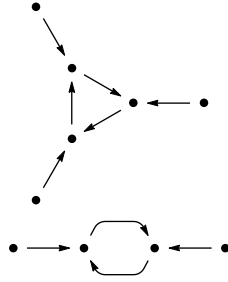


FIGURE 10. Graph type 10(3,2)

that $f_c^3(a) = a$, $f_c^2(b) = b$, and

$$(3.24) \quad a - f_c(a) = \frac{x^2 + x + 1}{x(x + 1)}, \quad b - f_c(b) = \frac{y}{x(x + 1)}.$$

It follows from these relations that if $y(x^2 + x + 1) \neq 0$, then a has period 3 under f_c and b has period 2. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ are such that a and b are points of periods 3 and 2, respectively, for the map f_c . Applying Proposition 3.4 we see that there are elements $\sigma \in K$ and $x \in K \setminus \{0, -1\}$ such that

$$(3.25) \quad c = -3/4 - \sigma^2, \quad b = -1/2 + \sigma$$

and

$$(3.26) \quad a = \frac{x^3 + 2x^2 + x + 1}{2x(x + 1)}, \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}.$$

Equating the two expressions for c given in (3.25) and (3.26) and letting $y = 2x(x + 1)\sigma$ we obtain

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

Thus, we have a point $(x, y) \in C(K)$ with $x(x + 1) \neq 0$ such that $\varphi(x, y) = (a, b, c)$. Furthermore, the relations (3.24) imply that $y(x^2 + x + 1) \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y) = (a, b, c)$, then

$$x = a^2 + a + c, \quad y = x(x + 1)(2b + 1). \quad \square$$

Remark. As noted in §2.3, the curve C is birational over \mathbb{Q} to the modular curve $X_1(13)$.

Theorem 3.28. *Let K be a quadratic field. Suppose that there exists an element $c \in K$ such that $G(f_c, K)$ has a subgraph of type 10(3,2). Then there is a rational number $x \notin \{0, -1\}$ such that*

$$(3.27) \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}$$

and $K = \mathbb{Q}(\sqrt{F_{13}(x)})$. In particular, K is a real quadratic field.

Proof. By Lemma 3.27 there is a point $(x, y) \in C(K)$ with

$$xy(x + 1)(x^2 + x + 1) \neq 0$$

such that c is given by (3.27). We claim that (x, y) cannot be a rational point on C . Indeed, C is an affine model of the curve $X_1(13)$, which has exactly six rational points (two of them at infinity). Therefore, C has four rational points, and it is easy to see that they are $(0, \pm 1)$ and $(-1, \pm 1)$. Thus, if $(x, y) \in C(\mathbb{Q})$, then either $x = 0$ or $x = -1$; however, this contradicts the assumption that $x(x + 1) \neq 0$. Therefore, (x, y) is a quadratic point on C , so it follows from Theorem 2.4 that x must be a rational number. In particular, since (x, y) is a quadratic point, then $K = \mathbb{Q}(x, y) = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{F_{13}(x)})$. The fact that K is a real quadratic field now follows from the observation that the polynomial function $F_{13} : \mathbb{R} \rightarrow \mathbb{R}$ induced by $F_{13}(x)$ only takes positive values. \square

Proposition 3.29. *There are infinitely many (real) quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type 10(3,2).*

Proof. Applying Lemma 3.5 to the polynomial $F_{13}(x)$ we obtain infinitely many (real) quadratic fields of the form $K_r = \mathbb{Q}(\sqrt{F_{13}(r)})$ with $r \in \mathbb{Q}$. For every such field there is a point $(r, \sqrt{F_{13}(r)}) \in C(K_r)$ which necessarily satisfies $r(r + 1)(r^2 + r + 1)F_{13}(r) \neq 0$; hence, by Lemma 3.27 there is an element $c \in K_r$ such that f_c has points $a, b \in K_r$ of periods 3 and 2, respectively. In order to conclude that $G(f_c, K_r)$ contains a subgraph of type 10(3,2) we need the additional condition that all points in the orbits of a and b are nonzero, as this will ensure that every such point has two distinct preimages. One can check that

$$-a \cdot f_c(a) \cdot f_c^2(a) = \frac{(r^3 + 2r^2 + r + 1)(r^3 - r - 1)(r^3 + 2r^2 + 3r + 1)}{8r^3(r + 1)^3},$$

so all points in the orbit of a are nonzero since $r \in \mathbb{Q}$. Now, using Lemma 3.27 we see that if $b \cdot f_c(b) = 0$, then

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

However, one can verify that this equation has no rational solution. Therefore, both points in the orbit of b must be nonzero. \square

3.13. Graph 12(2). Our search described in §4.4 produced the pairs

$$(K, c) = \left(\mathbb{Q}(\sqrt{2}), -\frac{15}{8} \right) \quad \text{and} \quad (K, c) = \left(\mathbb{Q}(\sqrt{57}), -\frac{55}{48} \right)$$

for which the graph $G(f_c, K)$ is of type 12(2). We will show here that, in addition to these known pairs, there are at most four other pairs (K, c) giving rise to this graph structure.

Lemma 3.30. *Let C/\mathbb{Q} be the affine curve of genus 5 defined by the equations*

$$(3.28) \quad \begin{cases} y^2 = 2(x^4 + 2x^3 - 2x + 1) \\ z^2 = 2(x^3 + x^2 - x + 1). \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, s, c]$ given by

$$a = \frac{z}{x^2 - 1}, \quad s = \frac{y}{x^2 - 1}, \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : x(x^2 - 1)(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0\}$$

to the set of all triples $(a, s, c) \in K^3$ such that a is a point of type 2_3 for the map f_c and s is a point of type 2_2 satisfying $f_c^2(s) \neq f_c^3(a)$.

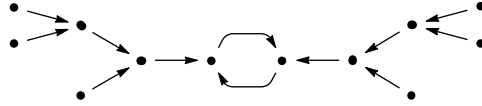


FIGURE 11. Graph type 12(2)

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point with $x^2 \neq 1$. Defining $a, s, c \in K$ as in the lemma, it is a straightforward calculation to verify that $f_c^3(a) = f_c^5(a)$, $f_c^4(a) = f_c^2(s)$, $f_c(s) - f_c^2(s) = 1$, and

$$(3.29) \quad \begin{aligned} f_c^4(a) - f_c^3(a) &= \frac{x^2 + 4x - 1}{x^2 - 1}, \\ f_c^4(a) - f_c^2(a) &= \frac{4x}{x^2 - 1}, \\ f_c(s) - f_c^3(s) &= \frac{2(x^2 + 2x - 1)}{x^2 - 1}. \end{aligned}$$

It follows from these relations that if $x(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$, then a is a point of type 2_3 and s is of type 2_2 for f_c , and moreover that $f_c^2(s) \neq f_c^3(a)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, s, c \in K$ are such that a is a point of type 2_3 for the map f_c and s is a point of type 2_2 satisfying $f_c^2(s) \neq f_c^3(a)$. Let $r = f_c(a)$, so that r is of type 2_2 . Since f_c can have only one 2-cycle, the points $f_c^2(r)$ and $f_c^2(s)$ must form a 2-cycle. Then the argument given in [31, page 20] shows that there is an element $x \in K \setminus \{0, \pm 1\}$ such that

$$(3.30) \quad \begin{aligned} c &= -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}, \\ r &= -\frac{x^2 + 1}{x^2 - 1}, \\ s^2 &= \frac{2(x^4 + 2x^3 - 2x + 1)}{(x^2 - 1)^2}. \end{aligned}$$

Since $a^2 = r - c$, this implies that

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

Letting $y = s(x^2 - 1)$ and $z = a(x^2 - 1)$ we obtain a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ and $\varphi(x, y, z) = (a, s, c)$. Furthermore, the relations (3.29) imply that $(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y, z) = (a, s, c)$, then

$$x = \frac{f_c(a) - 1}{f_c^2(a)}, \quad y = s(x^2 - 1), \quad z = a(x^2 - 1). \quad \square$$

Lemma 3.31. *Let X/\mathbb{Q} be the hyperelliptic curve of genus 3 defined by the equation*

$$w^2 = x^7 + 3x^6 + x^5 - 3x^4 + x^3 + 3x^2 - 3x + 1.$$

Then $X(\mathbb{Q})$ contains the points $\infty, (-1, \pm 2), (0, \pm 1), (1, \pm 2)$ and at most 8 other points.

Proof. Using the Magma function `Points` we search for rational points on X of height at most 10^5 and obtain the points listed above. Using the `RankBounds` function we find that the group $\text{Jac}(X)(\mathbb{Q})$ has rank 2; we may therefore apply the method of Chabauty and Coleman to bound the number of rational points on X . The prime 3 is of good reduction for X , and Magma's `Points` function yields $\#X(\mathbb{F}_3) = 7$. Applying the Lorenzini-Tucker bound (Theorem 3.2) with $p = 3, d = 2$ we obtain $\#X(\mathbb{Q}) \leq 15$. Since we have already listed 7 rational points, we conclude that there are at most 8 additional rational points on X . \square

Theorem 3.32. *With C as in Lemma 3.30 we have the following:*

- (1) $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.
- (2) *If (x, y, z) is a quadratic point on C with $x \in \mathbb{Q}$, then there exists $w \in \mathbb{Q}$ such that $(x, w) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 3.31. Moreover, $x \neq \pm 1$.*
- (3) *The quadratic points (x, y, z) on C with $x \notin \mathbb{Q}$ are the points*

$$(x, \pm(4x + 10), \pm(2x + 4)) \quad \text{with} \quad x^2 - 2x - 7 = 0,$$

which are defined over the field $\mathbb{Q}(\sqrt{2})$, and the points

$$(x, \pm(24x - 10), \pm(6x - 4)) \quad \text{with} \quad x^2 - 16x + 7 = 0,$$

which are defined over the field $\mathbb{Q}(\sqrt{57})$.

Proof. Let C_1 be the hyperelliptic curve of genus 1 defined by equation $y^2 = 2(x^4 + 2x^3 - 2x + 1)$. Since C_1 has a rational point — for instance, the point $(1, 2)$ — it is an elliptic curve; in fact, as mentioned in §3.5, C_1 is the elliptic curve with Cremona label 40a3, which has exactly four rational points. Hence, $\#C_1(\mathbb{Q}) = 4$, and we easily find the four points: $C_1(\mathbb{Q}) = \{(\pm 1, \pm 2)\}$. Similarly, let C_2 be the hyperelliptic curve defined by the equation $z^2 = 2(x^3 + x^2 - x + 1)$. Then C_2 is the elliptic curve 11a3, which has exactly five rational points. Hence, $C_2(\mathbb{Q})$ consists of the point at infinity and four other points, which are easily found to be the points $(\pm 1, \pm 2)$. Knowing $C_1(\mathbb{Q})$ and $C_2(\mathbb{Q})$ we conclude, in particular, that $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ satisfies $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 2$, contradicting the assumption that (x, y, z) is a quadratic point on C . It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. By the same argument, $z \notin \mathbb{Q}$. Since both y and z are quadratic, then $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the numbers $2(x^4 + 2x^3 - 2x + 1)$ and $2(x^3 + x^2 - x + 1)$ must have the same squarefree part; hence their product is a square, so there is a rational number w such that

$$w^2 = x^7 + 3x^6 + x^5 - 3x^4 + x^3 + 3x^2 - 3x + 1.$$

This proves part (2) of the theorem.

Case 2. x is quadratic. By Lemma 2.2 applied to the equation

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

there exist a rational number w and a point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ such that

$$(3.31) \quad x^2 + \frac{2x_0 - w^2 + 2}{2}x + \frac{2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2}{2} = 0.$$

We will now deduce a different expression for the minimal polynomial of x . Making the change of variables

$$(3.32) \quad X = \frac{2x^2 + y}{(x-1)^2}, \quad Y = \frac{3x^3 + 3x^2 + 2xy - 3x + 1}{(x-1)^3}$$

satisfying

$$(3.33) \quad x = \frac{X^2 + 2Y}{X^2 - 4X + 2},$$

the system (3.28) becomes

$$\begin{cases} Y^2 = X^3 - 2X + 1 \\ z^2 = 2(x^3 + x^2 - x + 1). \end{cases}$$

Suppose that $X \in \mathbb{Q}$. Substituting $y = X(x - 1)^2 - 2x^2$, the equation $y^2 - 2(x^4 + 2x^3 - 2x + 1) = 0$ becomes

$$(x - 1)^2 ((X^2 - 4X + 2)x^2 - 2X^2x + X^2 - 2) = 0,$$

so we must have

$$(3.34) \quad x^2 - \frac{2X^2}{X^2 - 4X + 2}x + \frac{X^2 - 2}{X^2 - 4X + 2} = 0.$$

Comparing (3.31) and (3.34) we arrive at the system

$$\begin{cases} (2x_0 - w^2 + 2)(X^2 - 4X + 2) = -4X^2 \\ (2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2)(X^2 - 4X + 2) = 2(X^2 - 2). \end{cases}$$

For every choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$, the above system defines a 0-dimensional scheme in the (X, w) plane over \mathbb{Q} , whose rational points we compute using the Magma function `RationalPoints`. For every solution (X, w) we then check whether the polynomial (3.34) is irreducible. With $(x_0, z_0) = (-1, 2)$ and $(X, w) = (1/2, 2)$ we obtain $x^2 - 2x - 7 = 0$; with $(x_0, z_0) = (1, 2)$ and $(X, w) = (4, 6)$ we obtain $x^2 - 16x + 7 = 0$. All other solutions lead to one of these two equations.

Suppose now that $X \notin \mathbb{Q}$. By Lemma 2.2 applied to the equation $Y^2 = X^3 - 2X + 1$, there exist a rational number v and a point $(X_0, Y_0) \in \{(0, \pm 1), (1, 0)\}$ such that

$$(3.35) \quad X^2 + (X_0 - v^2)X + X_0^2 + v^2X_0 - 2Y_0v - 2 = 0 \quad \text{and} \quad Y = Y_0 + v(X - X_0).$$

The point $(0, -1)$ is excluded in this case because (3.33) would imply that $x = \frac{v}{v-2} \in \mathbb{Q}$. If $(X_0, Y_0) = (0, 1)$, then (3.33) and (3.35) imply that

$$(3.36) \quad x^2 - \frac{4(v+1)}{v^2-2}x - 1 = 0,$$

and if $(X_0, Y_0) = (1, 0)$, then

$$(3.37) \quad x^2 - \frac{4x}{v^2 - 2v - 1} - \frac{v^2 + 2v - 1}{v^2 - 2v - 1} = 0.$$

Suppose that $(X_0, Y_0) = (0, 1)$. Comparing (3.31) and (3.36) we obtain the system

$$\begin{cases} (2x_0 - w^2 + 2)(v^2 - 2) = -8(v + 1) \\ 2x_0^2 + w^2x_0 + 2x_0 - 2z_0w = 0. \end{cases}$$

For each choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ we solve the above system for v and w , and find that $v = -1$. But then (3.36) implies that $x = \pm 1$, which is a contradiction.

Now suppose that $(X_0, Y_0) = (1, 0)$. Comparing (3.31) and (3.37) we obtain the system

$$\begin{cases} (2x_0 - w^2 + 2)(v^2 - 2v - 1) = -8 \\ (2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2)(v^2 - 2v - 1) = -2(v^2 + 2v - 1). \end{cases}$$

For each choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ we consider the above system and find that it has no rational solutions.

The assumption that $X \notin \mathbb{Q}$ has led in every case to a contradiction, so we conclude that X must be rational. Hence, the analysis done earlier shows that either $x^2 - 2x - 7 = 0$ or $x^2 - 16x + 7 = 0$. Assuming $x^2 - 2x - 7 = 0$, the system (3.28) can be solved to obtain $y = \pm(4x + 10)$, $z = \pm(2x + 4)$. Thus, we have found the points $(x, \pm(4x + 10), \pm(2x + 4)) \in C(K)$, where $K = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{2})$. Now assume that $x^2 - 16x + 7 = 0$. Then we solve the system (3.28) and find that $y = \pm(24x - 10)$, $z = \pm(6x - 4)$. Thus, we have found the points $(x, \pm(24x - 10), \pm(6x - 4)) \in C(K)$, where $K = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{57})$. This proves part (3) of the theorem. \square

Corollary 3.33. *In addition to the known pairs*

$$(\mathbb{Q}(\sqrt{2}), -15/8) \quad \text{and} \quad (\mathbb{Q}(\sqrt{57}), -55/48)$$

there are at most four pairs (K, c) , with K a quadratic number field and $c \in K$, for which $G(f_c, K)$ contains a graph of type 12(2). Moreover, for every such pair we must have $c \in \mathbb{Q}$.

Proof. Suppose that (K, c) is such a pair. By Lemma 3.30 there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that

$$(3.38) \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}.$$

We cannot have $(x, y, z) \in C(\mathbb{Q})$ since this would imply, by Theorem 3.32 part (1), that $x \in \{\pm 1\}$. Hence, (x, y, z) is a quadratic point on C . Suppose that x is quadratic. Then Theorem 3.32 implies that either $x^2 - 2x - 7 = 0$ or $x^2 - 16x + 7 = 0$. In the former case we have $K = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{2})$, and (3.38) implies that $c = -15/8$; in the latter case have $K = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{57})$ and (3.38) implies that $c = -55/48$. Thus, we recover the two pairs listed in the corollary. Note also that $c \in \mathbb{Q}$ in this case.

Consider now the case where $x \in \mathbb{Q}$ (and hence $c \in \mathbb{Q}$, by (3.38)). By Theorem 3.32 there is a rational number w such that $(x, w) \in X(\mathbb{Q})$. Since $x \notin \{0, \pm 1\}$, then Lemma 3.31 implies that there are at most four options for x . Each value of x determines the number c by (3.38) and the field K by (3.28). This gives at most four options for the pair (K, c) . \square

3.14. Graph 12(2,1,1)a. Our search described in §4.4 produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{17}), -\frac{13}{16} \right)$$

for which the graph $G(f_c, K)$ is of type 12(2,1,1)a. We will show here that this is the only such pair (K, c) with K a quadratic number field and $c \in K$.

Lemma 3.34. *Let C/\mathbb{Q} be the affine curve of genus 5 defined by the equations*

$$(3.39) \quad \begin{cases} y^2 = 2(x^4 + 2x^3 - 2x + 1) \\ z^2 = 5x^4 + 8x^3 + 6x^2 - 8x + 5. \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^4 = \text{Spec } \mathbb{Q}[r, s, p, c]$ given by

$$\begin{aligned} r &= -\frac{x^2 + 1}{x^2 - 1}, \\ s &= \frac{y}{x^2 - 1}, \\ p &= \frac{1}{2} + \frac{z}{2(x^2 - 1)}, \\ c &= -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : x(x^2 - 1)(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0\}$$

to the set of all tuples $(r, s, p, c) \in K^4$ such that p is a fixed point of the map f_c and r, s are points of type 2_2 for f_c satisfying $f_c^2(r) \neq f_c^2(s)$.

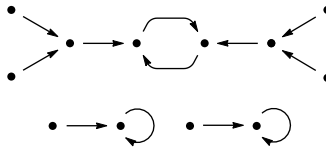


FIGURE 12. Graph type 12(2,1,1)a

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point satisfying $x^2 \neq 1$. Defining $r, s, p, c \in K$ as in the lemma, it is a simple calculation to verify that p is a fixed point of the map f_c ; moreover, Lemma 3.10 implies that if $x(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$, then r and s are points of type 2_2 for f_c with $f_c^2(r) \neq f_c^2(s)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $r, s, p, c \in K$ are such that p is a fixed point of the map f_c and r, s are points of type 2_2 for f_c satisfying $f_c^2(r) \neq f_c^2(s)$. By Lemma 3.10 there are elements $x, y \in K$ satisfying $y^2 = 2(x^4 + 2x^3 - 2x + 1)$ such that $x(x^2 - 1)(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$ and

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

Now, since p is a fixed point for f_c , Proposition 3.4 implies that there is an element $\rho \in K$ such that

$$c = 1/4 - \rho^2 \quad \text{and} \quad p = 1/2 + \rho.$$

Equating the two expressions for c given above and letting $z = 2\rho(x^2 - 1)$, we obtain the relation $z^2 = 5x^4 + 8x^3 + 6x^2 - 8x + 5$. Thus, we have a point $(x, y, z) \in C(K)$ with $x(x^2 - 1)(x^2 + 4x - 1)(x^2 + 2x - 1) \neq 0$ and $\varphi(x, y, z) = (r, s, p, c)$. To see that φ is injective, one can verify that if $\varphi(x, y, z) = (r, s, p, c)$, then

$$x = \frac{r-1}{r^2+c}, \quad y = s(x^2-1), \quad z = (2p-1)(x^2-1). \quad \square$$

Theorem 3.35. *With C as in Lemma 3.34 we have the following:*

- (1) $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 4)\}$.
- (2) *If K is a quadratic field different from $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$, then $C(K) = C(\mathbb{Q})$.*
- (3) *For $K = \mathbb{Q}(\sqrt{5})$,*

$$C(K) \setminus C(\mathbb{Q}) = \{(x, \pm(4x-2), \pm 8x) : x^2 + 4x - 1 = 0\}.$$

- (4) *For $K = \mathbb{Q}(\sqrt{17})$, $C(K) \setminus C(\mathbb{Q})$ consists of the points*

$$(-3, \pm 2\sqrt{17}, \pm 4\sqrt{17}), \quad (1/3, \pm 2\sqrt{17}/9, \pm 4\sqrt{17}/9),$$

and the points $(x, \pm 10x, \pm(16x-4))$ with $x^2 + 8x - 1 = 0$.

Proof. As shown in the proof of Theorem 3.32, the only rational solutions to the equation $y^2 = 2(x^4 + 2x^3 - 2x + 1)$ are $(x, y) = (\pm 1, \pm 2)$. Let C_2 be the hyperelliptic curve of genus 1 defined by the equation

$$z^2 = 5x^4 + 8x^3 + 6x^2 - 8x + 5.$$

Making the change of variables $x \mapsto -x$, it follows from the proof of Proposition 3.21 that C is isomorphic to the elliptic curve 17a4 in Cremona's tables, which has exactly four rational points; hence, C_2 has four rational points, and these are easily found to be $(\pm 1, \pm 4)$. Knowing all rational solutions to each of the defining equations for C , we deduce that $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 4)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ satisfies $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 4$, contradicting the assumption that (x, y, z) is a quadratic point on C . It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. By a similar argument, $z \notin \mathbb{Q}$. Since y and z are both quadratic, we must have $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the numbers $2(x^4 + 2x^3 - 2x + 1)$ and $5x^4 + 8x^3 + 6x^2 - 8x + 5$ must have the same squarefree part, and hence their product is a square; thus, there is a rational number w such that

$$(3.40) \quad w^2 = 10x^8 + 36x^7 + 44x^6 - 12x^5 - 44x^4 + 12x^3 + 44x^2 - 36x + 10.$$

Let X be the hyperelliptic curve of genus 3 defined by (3.40). Searching for rational points on X using Magma's `Points` function we obtain the 8 points $(\pm 1, \pm 8), (-3, \pm 136), (1/3, \pm 136/81)$; we will show that these are all the rational points on X . To see this, note that X has an involution given by $(x, w) \mapsto (-1/x, w/x^4)$. The quotient of X by this involution is the elliptic curve

$$E : v^2 + uv + v = u^3 - u^2 - 6u - 4.$$

The quotient map $X \rightarrow E$ of degree 2 is given by

$$u = \frac{2x^4 + 6x^3 + 4x^2 - 6x - w + 2}{(x^2 - 1)^2},$$

$$v = \frac{-6x^6 - 24x^5 - 22x^4 + 16x^3 + 2x^2w + 22x^2 + 4xw - 24x - 2w + 6}{x^6 - 3x^4 + 3x^2 - 1}.$$

The curve E is the elliptic curve 17a2 in Cremona's tables, and has exactly four rational points. It follows that X can have at most 8 rational points, and since we have already listed 8 points in $X(\mathbb{Q})$, these must be all.

Returning to (3.40), we have a point $(x, w) \in X(\mathbb{Q})$ with $x \neq \pm 1$; we must then have $x = -3$ or $x = 1/3$. Taking $x = -3$ we obtain by (3.39) that $y^2 = 68$ and $z^2 = 272$; if $x = 1/3$, then $y^2 = 68/81$ and $z^2 = 272/81$. Thus, we have shown that the only quadratic points on C having a rational x -coordinate are the points $(-3, \pm 2\sqrt{17}, \pm 4\sqrt{17})$ and $(1/3, \pm 2\sqrt{17}/9, \pm 4\sqrt{17}/9)$.

Case 2. x is quadratic. Starting with the system (3.39), we make the change of variables

$$(3.41) \quad X = \frac{2x^2 + y}{(x - 1)^2}, \quad Y = \frac{3x^3 + 3x^2 + 2xy - 3x + 1}{(x - 1)^3}$$

$$(3.42) \quad S = \frac{5x^2 + 2x + 2z + 1}{(x - 1)^2}, \quad T = \frac{2(7x^3 + 9x^2 + 3xz - 3x + z + 3)}{(x - 1)^3}$$

satisfying

$$(3.43) \quad \frac{X^2 + 2Y}{X^2 - 4X + 2} = x = \frac{S^2 + 2S + 4T + 1}{S^2 - 10S + 5}$$

to obtain the equations

$$\begin{cases} Y^2 = X^3 - 2X + 1 \\ T^2 = S^3 - 11S + 6. \end{cases}$$

The idea of the proof is to use these two equations together with Lemma 2.2 to find the minimal polynomials of X and S , and then using (3.43) to find the minimal polynomial of x . It may occur that X or S are rational rather than quadratic, so we must consider this possibility. If $X \in \mathbb{Q}$, then using the relation $y = X(x - 1)^2 - 2x^2$, the equation

$$y^2 - 2(x^4 + 2x^3 - 2x + 1) = 0$$

becomes

$$(x-1)^2(X^2-4X+2)\left(x^2-\frac{2X^2}{X^2-4X+2}x+\frac{X^2-2}{X^2-4X+2}\right)=0.$$

Since $x \notin \mathbb{Q}$ and the equation $X^2-4X+2=0$ has no rational solution, this implies that

$$(3.44) \quad x^2-\frac{2X^2}{X^2-4X+2}x+\frac{X^2-2}{X^2-4X+2}=0.$$

Similarly, if $S \in \mathbb{Q}$, then using the relation $z = \frac{1}{2}[S(x-1)^2 - 5x^2 - 2x - 1]$, the equation

$$z^2 - (5x^4 + 8x^3 + 6x^2 - 8x + 5) = 0$$

becomes

$$\frac{1}{4}(x-1)^2(S^2-10S+5)\left(x^2-\frac{2S^2+4S+2}{S^2-10S+5}x+\frac{S^2-2S-19}{S^2-10S+5}\right)=0.$$

Since $x \notin \mathbb{Q}$ and the equation $S^2-10S+5=0$ has no rational solution, this implies that

$$(3.45) \quad x^2-\frac{2S^2+4S+2}{S^2-10S+5}x+\frac{S^2-2S-19}{S^2-10S+5}=0.$$

Now, if X is quadratic, then by Lemma 2.2 applied to the equation $Y^2 = X^3 - 2X + 1$, there is a rational number v and a point $(X_0, Y_0) \in \{(0, \pm 1), (1, 0)\}$ such that

$$(3.46) \quad X^2 + (X_0 - v^2)X + X_0^2 + v^2X_0 - 2Y_0v - 2 = 0, \quad Y = Y_0 + v(X - X_0).$$

The point $(0, -1)$ is excluded in this case because (3.43) would imply that $x = \frac{v}{v-2} \in \mathbb{Q}$. If $(X_0, Y_0) = (0, 1)$, then (3.43) and (3.46) imply that

$$(3.47) \quad x^2 - \frac{4(v+1)}{v^2-2}x - 1 = 0.$$

If instead $(X_0, Y_0) = (1, 0)$, then

$$(3.48) \quad x^2 - \frac{4x}{v^2-2v-1} - \frac{v^2+2v-1}{v^2-2v-1} = 0.$$

Similarly, if $S \notin \mathbb{Q}$, then by Lemma 2.2 applied to the equation

$$T^2 = S^3 - 11S + 6,$$

there is a rational number w and a point $(S_0, T_0) \in \{(-1, \pm 4), (3, 0)\}$ such that

$$(3.49) \quad S^2 + (S_0 - w^2)S + S_0^2 + w^2S_0 - 2T_0w - 11 = 0, \quad T = T_0 + w(S - S_0).$$

The point $(-1, -4)$ is excluded because it would lead to $x = \frac{w+1}{w-3} \in \mathbb{Q}$. If $(S_0, T_0) = (3, 0)$, then (3.43) and (3.49) imply that

$$(3.50) \quad x^2 - \frac{8x}{w^2-4w-1} - \frac{w^2+4w-1}{w^2-4w-1} = 0,$$

and if $(S_0, T_0) = (-1, 4)$, then

$$(3.51) \quad x^2 - \frac{8w+8}{w^2-5}x - 1 = 0.$$

We now split the proof into four cases, according to whether X and S are rational or quadratic.

Case 2a. $X, S \in \mathbb{Q}$. We simultaneously have relations (3.44) and (3.45). Comparing these equations we obtain the system

$$\begin{cases} X^2(S^2 - 10S + 5) = (X^2 - 4X + 2)(S^2 + 2S + 1) \\ (X^2 - 2)(S^2 - 10S + 5) = (X^2 - 4X + 2)(S^2 - 2S - 19), \end{cases}$$

whose rational solutions are $(X, S) = (0, -1)$ and $(X, S) = (1, 3)$. However, both solutions lead to $x = \pm 1$ by applying (3.44) and (3.45). We conclude that X and S cannot both be rational.

Case 2b. $X \in \mathbb{Q}, S \notin \mathbb{Q}$. We have (3.44) and (3.49). If $(S_0, T_0) = (3, 0)$, then we compare (3.44) and (3.50) to arrive at the system

$$\begin{cases} X^2(w^2 - 4w - 1) = 4(X^2 - 4X + 2) \\ (X^2 - 2)(w^2 - 4w - 1) = -(X^2 - 4X + 2)(w^2 + 4w - 1), \end{cases}$$

whose only rational solution is $(X, w) = (1, 1)$. However, when $w = 1$, (3.50) becomes $(x + 1)^2 = 0$, a contradiction.

If $(S_0, T_0) = (-1, 4)$, then we compare (3.44) and (3.51) to conclude that $X = 0$ or 2 . Then (3.44) becomes $x^2 - 1 = 0$ (a contradiction) or $x^2 + 4x - 1 = 0$.

Case 2c. $X \notin \mathbb{Q}, S \in \mathbb{Q}$. In this case we have (3.45) and (3.46). If $(X_0, Y_0) = (0, 1)$, then we compare (3.45) and (3.47) to conclude that $S = 7$ and $x^2 + 8x - 1 = 0$.

If $(X_0, Y_0) = (1, 0)$, then we compare (3.45) and (3.48) to arrive at the system

$$\begin{cases} 2(S^2 - 10S + 5) = (v^2 - 2v - 1)(S + 1)^2 \\ -(v^2 + 2v - 1)(S^2 - 10S + 5) = (v^2 - 2v - 1)(S^2 - 2S - 19), \end{cases}$$

whose only rational solution is $(S, v) = (3, 1)$. However, if $v = 1$, then (3.48) becomes $(x + 1)^2 = 0$, a contradiction.

Case 2d. $X, S \notin \mathbb{Q}$. We have (3.46) and (3.49).

- If $(X_0, Y_0) = (1, 0)$ and $(S_0, T_0) = (3, 0)$, then comparing (3.48) and (3.50) we find that $v = w = \pm 1$. But then (3.48) implies that $x = \pm 1$, a contradiction.
- If $(X_0, Y_0) = (1, 0)$ and $(S_0, T_0) = (-1, 4)$, then we compare (3.48) and (3.51) to see that $v = 0$ and $x^2 + 4x - 1 = 0$.
- If $(X_0, Y_0) = (0, 1)$ and $(S_0, T_0) = (3, 0)$, then we compare (3.47) and (3.50) to conclude that $w = 0$, and therefore $x^2 + 8x - 1 = 0$.

- If $(X_0, Y_0) = (0, 1)$ and $(S_0, T_0) = (-1, 4)$, then comparing (3.47) and (3.51) we obtain

$$(v + 1)(w^2 - 5) = 2(w + 1)(v^2 - 2).$$

Let $E \subset \mathbb{P}^2$ be the projective closure of the curve defined by this equation. Then E is a nonsingular plane cubic with at least four rational points, namely the affine point $(-1, -1)$ and three points at infinity. Using Magma we find that E is the elliptic curve with Cremona label 17a4, which has exactly 4 rational points. It follows that $(v, w) = (-1, -1)$ is the only affine point on E . But then (3.47) becomes $x^2 - 1 = 0$, which is a contradiction.

In all cases that have not led to a contradiction we concluded that either $x^2 + 4x - 1 = 0$ or $x^2 + 8x - 1 = 0$. If $x^2 + 4x - 1 = 0$, then (3.39) implies that $y = \pm(4x - 2)$ and $z = \pm 8x$. If $x^2 + 8x - 1 = 0$, then $y = \pm 10x$ and $z = \pm(16x - 4)$. Thus, we have determined all quadratic points on C having a quadratic x -coordinate, and now the theorem follows immediately. \square

Corollary 3.36. *Let K be a quadratic field and let $c \in K$. Suppose that $G(f_c, K)$ contains a graph of type 12(2,1,1)a. Then $c = -13/16$ and $K = \mathbb{Q}(\sqrt{17})$.*

Proof. By Lemma 3.34, there is a point $(x, y, z) \in C(K)$ with

$$(x^2 - 1)(x^2 + 4x - 1) \neq 0$$

such that

$$(3.52) \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}.$$

It follows from Theorem 3.35 that $K = \mathbb{Q}(\sqrt{17})$ and that x is either $-3, 1/3$, or a quadratic number satisfying $x^2 + 8x - 1 = 0$. In all three cases, (3.52) implies that $c = -13/16$. \square

3.15. Graph 12(2,1,1)b. Our search described in §4.4 produced the pairs

$$(K, c) = \left(\mathbb{Q}(\sqrt{-7}), -\frac{5}{16} \right) \quad \text{and} \quad \left(\mathbb{Q}(\sqrt{33}), -\frac{45}{16} \right)$$

for which the graph $G(f_c, K)$ is of type 12(2,1,1)b. We will show here that, in addition to these known pairs, there are at most four other pairs (K, c) giving rise to this graph structure.

Lemma 3.37. *Let C/\mathbb{Q} be the affine curve of genus 5 defined by the equations*

$$(3.53) \quad \begin{cases} y^2 = -3x^4 + 14x^2 + 5, \\ z^2 = 2(x^3 + x^2 - x + 1). \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[p, q, c]$ given by

$$p = \frac{y + 1 - x^2}{2(x^2 - 1)}, \quad q = \frac{z}{x^2 - 1}, \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : y(x^2 - 1) \neq 0\}$$

to the set of all tuples $(p, q, c) \in K^3$ such that p is a point of period 2 and q is a point of type 1_3 for the map f_c .

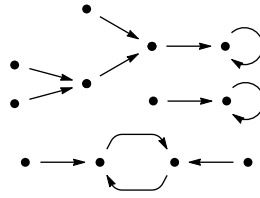


FIGURE 13. Graph type 12(2,1,1)b

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point with $x^2 \neq 1$. Defining $p, q, c \in K$ as in the lemma, it is a simple calculation to verify that q is a point of type 1_3 for f_c and that

$$(3.54) \quad f_c^2(p) = p, \quad p - f_c(p) = \frac{y}{x^2 - 1}.$$

It follows that if $y \neq 0$, then p has period 2 under f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $p, q, c \in K$ are such that p is a point of period 2 and q is a point of type 1_3 for f_c . By Proposition 3.4, there is an element $\sigma \in K$ such that

$$(3.55) \quad p = \sigma - 1/2 \quad \text{and} \quad c = -3/4 - \sigma^2.$$

Since q is of type 1_3 , an argument given in [31, page 22] shows that there is an element $x \in K \setminus \{\pm 1\}$ such that

$$(3.56) \quad q^2 = \frac{2(x^3 + x^2 - x + 1)}{(x^2 - 1)^2} \quad \text{and} \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

Letting $z = q(x^2 - 1)$ we then have $z^2 = 2(x^3 + x^2 - x + 1)$. Equating the expressions for c given in (3.55) and (3.56) we obtain

$$4\sigma^2(x^2 - 1)^2 = -3x^4 + 14x^2 + 5;$$

hence, letting $y = 2\sigma(x^2 - 1)$ we arrive at the equation $y^2 = -3x^4 + 14x^2 + 5$. Thus, we have a point $(x, y, z) \in C(K)$ satisfying $x^2 \neq 1$ and $\varphi(x, y, z) =$

(p, q, c) . Moreover, the relations (3.54) imply that $y \neq 0$. To see that φ is injective, one can verify that if $\varphi(x, y, z) = (p, q, c)$, then

$$x = \frac{f_c(q)}{f_c^2(q)}, \quad y = (2p + 1)(x^2 - 1), \quad z = q(x^2 - 1). \quad \square$$

Lemma 3.38. *Let X/\mathbb{Q} be the hyperelliptic curve of genus 3 defined by the equation*

$$s^2 = -6x^7 - 6x^6 + 34x^5 + 22x^4 - 18x^3 + 38x^2 - 10x + 10.$$

Then $X(\mathbb{Q})$ contains the points $\infty, (\pm 1, \pm 8), (-3, \pm 56), (1/3, \pm 88/27)$ and at most 8 other points.

Proof. Using the Magma function `Points` we search for rational points on X of height at most 10^5 and obtain the points listed above. Using the `RankBounds` function we find that the group $\text{Jac}(X)(\mathbb{Q})$ has rank 1; we may therefore apply the method of Chabauty and Coleman to bound the number of rational points on X . The prime 13 is of good reduction for X , and we compute $\#X(\mathbb{F}_{13}) = 16$. Applying Stoll's bound (Theorem 3.3) we obtain $\#X(\mathbb{Q}) \leq 18$. Since X has no rational point with $s = 0$, the number of rational points must be odd, and therefore $\#X(\mathbb{Q}) \leq 17$. Since we have already listed 9 rational points, we conclude that there are at most 8 additional rational points on X . \square

Theorem 3.39. *With C as in Lemma 3.37 we have the following:*

- (1) $C(\mathbb{Q}) = \{(\pm 1, \pm 4, \pm 2)\}$.
- (2) *If (x, y, z) is a quadratic point on C , then $x \in \mathbb{Q} \setminus \{\pm 1\}$. Moreover, there exists $s \in \mathbb{Q}$ such that $(x, s) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 3.38.*

Proof. Let C_1 be the hyperelliptic curve of genus 1 defined by the equation $y^2 = -3x^4 + 14x^2 + 5$. Making the change of variables $(x, y) \mapsto (1/x, y/x^2)$ we see from [31, page 21] that C_1 is isomorphic to the elliptic curve with Cremona label 15a8, which has exactly four rational points. Therefore, C_1 has four rational points, and these are easily found to be $(\pm 1, \pm 4)$. The curve $z^2 = 2(x^3 + x^2 - x + 1)$ is birational to the elliptic curve 11a3, which is the modular curve $X_1(11)$. This curve has five rational points, the nontrivial ones being $(\pm 1, \pm 2)$. Knowing all rational solutions to both of the equations defining C , we deduce that $C(\mathbb{Q}) = \{(\pm 1, \pm 4, \pm 2)\}$.

To prove part (2) of the theorem, suppose that $(x, y, z) \in C(\overline{\mathbb{Q}})$ satisfies $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 4$ and $z = \pm 2$, contradicting the assumption that (x, y, z) is a quadratic point on C . It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. By a similar argument, $z \notin \mathbb{Q}$. Therefore, $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the numbers $-3x^4 + 14x^2 + 5$ and $2(x^3 + x^2 - x + 1)$ must have the same squarefree part,

and so their product is a square; hence, there is a rational number s such that

$$s^2 = -6x^7 - 6x^6 + 34x^5 + 22x^4 - 18x^3 + 38x^2 - 10x + 10.$$

Thus, we have $(x, s) \in X(\mathbb{Q})$.

Case 2. x is quadratic. By Lemma 2.2 applied to the equation

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

there is a rational number w and a point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ such that

$$(3.57) \quad x^2 + \frac{2x_0 - w^2 + 2}{2}x + \frac{2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2}{2} = 0.$$

With x, y as in (3.53) we make the change of variables

$$(3.58) \quad X = \frac{-x^2 + 4x + y + 1}{2(x-1)^2}, \quad Y = \frac{-3x^3 + 7x^2 + xy + 7x + 3y + 5}{2(x-1)^3}$$

satisfying

$$(3.59) \quad x = \frac{Y + X^2 + 2X}{X^2 + X + 1}$$

to obtain the equations

$$\begin{cases} Y^2 = 4X^3 + 5X^2 + 2X + 1 \\ z^2 = 2(x^3 + x^2 - x + 1). \end{cases}$$

Suppose that $X \in \mathbb{Q}$. Substituting $y = 2X(x-1)^2 + x^2 - 4x - 1$ into the equation $y^2 = -3x^4 + 14x^2 + 5$ we obtain the following expression for the minimal polynomial of x :

$$(3.60) \quad x^2 - \frac{2X^2 + 4X}{X^2 + X + 1}x + \frac{X^2 - X - 1}{X^2 + X + 1} = 0.$$

Comparing (3.57) and (3.60) we arrive at the system

$$\begin{cases} (2x_0 - w^2 + 2)(X^2 + X + 1) = -4X(X + 2) \\ (2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2)(X^2 + X + 1) = 2(X^2 - X - 1). \end{cases}$$

For every choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ the above system defines a 0-dimensional scheme over \mathbb{Q} , whose rational points we compute using the Magma function `RationalPoints`. In every case we find that $X = -1$ or $X = 0$. But then (3.60) implies that $x = \pm 1$, which is a contradiction. Therefore, X cannot be rational, so by Lemma 2.2 applied to the equation $Y^2 = 4X^3 + 5X^2 + 2X + 1$, there is a rational number v and a point $(X_0, Y_0) \in \{(0, \pm 1), (-1, 0)\}$ such that

$$(3.61) \quad X^2 + \frac{4X_0 - v^2 + 5}{4}X + \frac{4X_0^2 + v^2X_0 + 5X_0 - 2Y_0v + 2}{4} = 0, \\ Y = Y_0 + v(X - X_0).$$

The point $(X_0, Y_0) = (0, -1)$ is excluded because (3.59) would imply that $x = \frac{v+3}{v-1} \in \mathbb{Q}$. If $(X_0, Y_0) = (0, 1)$, then (3.59) and (3.61) imply that

$$(3.62) \quad x^2 - \frac{v^2 + 4v - 1}{v^2 - 4v + 7} = 0,$$

and if $(X_0, Y_0) = (-1, 0)$, then

$$(3.63) \quad x^2 - \frac{8v}{v^2 + 3}x - \frac{v^2 - 5}{v^2 + 3} = 0.$$

Suppose that $(X_0, Y_0) = (0, 1)$. Comparing (3.57) and (3.62) we obtain the system

$$\begin{cases} 2x_0 - w^2 + 2 = 0 \\ (2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2)(v^2 - 4v + 7) = -2(v^2 + 4v - 1). \end{cases}$$

For each choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ we solve the above system for v and w , and find that $v = 1$. But then (3.62) implies that $x = \pm 1$, which is a contradiction.

Suppose now that $(X_0, Y_0) = (-1, 0)$. Comparing (3.57) and (3.63) we obtain the system

$$\begin{cases} (2x_0 - w^2 + 2)(v^2 + 3) = -16v \\ (2x_0^2 + w^2x_0 + 2x_0 - 2z_0w - 2)(v^2 + 3) = -2(v^2 - 5). \end{cases}$$

For each choice of point $(x_0, z_0) \in \{(\pm 1, \pm 2)\}$ we solve the above system for v and w , and find that $v = \pm 1$. But then (3.63) implies that $x = \pm 1$, a contradiction.

Since the assumption that $x \notin \mathbb{Q}$ has led in every case to a contradiction, we conclude that x must be rational. The analysis done in Case 1 then proves the theorem. \square

Corollary 3.40. *In addition to the known pairs*

$$(\mathbb{Q}(\sqrt{-7}), -5/16) \quad \text{and} \quad (\mathbb{Q}(\sqrt{33}), -45/16)$$

there are at most four pairs (K, c) , with K a quadratic number field and $c \in K$, for which $G(f_c, K)$ contains a graph of type 12(2,1,1)b. Moreover, for every such pair we must have $c \in \mathbb{Q}$.

Proof. Suppose that (K, c) is such a pair. Since f_c has a point of period 2 and a point of type 1₃ in K , then by Lemma 3.37 there is a point $(x, y, z) \in C(K)$ with $y(x^2 - 1) \neq 0$ such that

$$(3.64) \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

We cannot have $(x, y, z) \in C(\mathbb{Q})$ since this would imply, by Theorem 3.39(1), that $x \in \{\pm 1\}$. Hence, (x, y, z) is a quadratic point on C . By Theorem 3.39(2) we must therefore have $x \in \mathbb{Q}$, and thus $c \in \mathbb{Q}$. Moreover, there is a rational number s such that $(x, s) \in X(\mathbb{Q})$. It follows from Lemma 3.38

that either $x \in \{-3, 1/3\}$ or x belongs to a list of at most 4 other rational numbers. Setting $x = -3$ we obtain by (3.64) and (3.53) that $c = -5/16$ and $y^2 = -112$, so $K = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{-7})$. If $x = 1/3$, then $c = -45/16$ and $y^2 = 176/27$, so $K = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{33})$. Thus, we recover the two pairs (K, c) listed in the statement of the corollary. If $x \notin \{-3, 1/3\}$, then there are at most four options for x ; each value of x determines the number c by (3.64) and the field K by (3.53). This gives at most four options for the pair (K, c) . \square

3.16. Graph 12(4). Our search described in §4.4 produced a unique pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{105}), -95/48 \right)$$

consisting of a quadratic field K and an element $c \in K$ for which the graph $G(f_c, K)$ is of type 12(4). We will show here that, in addition to this known example, there are at most five other such pairs (K, c) .

Lemma 3.41. *Let C/\mathbb{Q} be the affine curve of genus 9 defined by the equations*

$$(3.65) \quad \begin{cases} y^2 = -x(x^2 + 1)(x^2 - 2x - 1) \\ z^2 = x(-x^6 + x^5 + 7x^4 + 10x^3 - 7x^2 + 5x + 1) - 2x(x - 1)(x + 1)^2y. \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^2 = \text{Spec } \mathbb{Q}[p, c]$ given by

$$p = \frac{z}{2x(x^2 - 1)}, \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : y(x^2 - 1)(y(x + 1) + x(x - 1)^2) \neq 0\}$$

to the set of all pairs $(p, c) \in K^2$ such that p is a point of type A_2 for the map f_c .

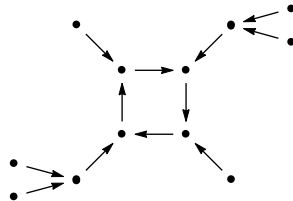


FIGURE 14. Graph type 12(4)

Proof. Fix a number field K , suppose that $(x, y, z) \in C(K)$ is a point satisfying $y(x^2 - 1) \neq 0$, and define $p, c \in K$ as in the lemma. From Lemma 3.14 it follows that the point

$$r := \frac{x-1}{2(x+1)} + \frac{y}{2x(x-1)}$$

has period 4 under f_c . Now, it is a simple calculation to verify that $f_c(p) = -r$; in order to conclude that p is of type 4_2 for f_c it is therefore enough to show that $-r$ is of type 4_1 . Since r has period 4, $-r$ will necessarily be of type 4_1 as long as $r \neq -r$. We have

$$(3.66) \quad r = 0 \iff y(x+1) + x(x-1)^2 = 0,$$

so if we assume that $y(x+1) + x(x-1)^2 \neq 0$, then it follows that p is of type 4_2 for f_c . This proves that φ gives a well-defined map.

To see that φ is surjective, suppose that $p, c \in K$ are such that p is a point of type 4_2 for the map f_c . Then $q := p^2 + c$ is a point of type 4_1 , so $r := -q$ is a point of period 4. By Lemma 3.14 there are elements $x, y \in K$ satisfying $y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$ and $y(x^2 - 1) \neq 0$ such that

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

Clearing denominators in the equation

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

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

$$z^2 = x(-x^6 + x^5 + 7x^4 + 10x^3 - 7x^2 + 5x + 1) - 2x(x-1)(x+1)^2y.$$

Thus, we have a point $(x, y, z) \in C(K)$ with $y(x^2 - 1) \neq 0$ and $\varphi(x, y, z) = (p, c)$. Furthermore, we must have $y(x+1) + x(x-1)^2 \neq 0$ because otherwise (3.66) would imply that $q = r$, and hence that q has period 4, a contradiction.

To see that φ is injective, one can verify that if $\varphi(x, y, z) = (p, c)$, then

$$\begin{aligned} x &= \frac{f_c^4(p) + f_c^2(p) - 1}{f_c^4(p) + f_c^2(p) + 1}, \\ y &= -\frac{2x(x^2 - 1)f_c(p) + x(x-1)^2}{x+1}, \\ z &= 2x(x^2 - 1)p. \end{aligned} \quad \square$$

Lemma 3.42. *Let X/\mathbb{Q} be the hyperelliptic curve of genus 5 defined by the equation*

$$\begin{aligned} w^2 &= x^{12} + 2x^{11} - 13x^{10} - 26x^9 + 67x^8 + 124x^7 + 26x^6 - 44x^5 \\ &\quad + 179x^4 - 62x^3 - 5x^2 + 6x + 1. \end{aligned}$$

Then $X(\mathbb{Q})$ contains the points $\infty^+, \infty^-, (\pm 1, \pm 16), (0, \pm 1), (-3, \pm 368)$ and at most 10 other points.

Proof. Using the Magma function `Points` we search for rational points on X of height at most 10^5 and obtain the points listed above. Using the `RankBound` function we obtain an upper bound of 4 for the rank of $\text{Jac}(X)(\mathbb{Q})$; we are thus in a position to bound the number of rational points on X using the method of Chabauty and Coleman. The prime 7 is of good reduction for X , and Magma’s `Points` function yields $\#X(\mathbb{F}_7) = 12$. Applying the Lorenzini-Tucker bound (Theorem 3.2) with $p = 7$, $d = 2$ we obtain

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_7) + \frac{6}{5}(8) = 12 + \frac{6}{5}(8) < 22,$$

so $\#X(\mathbb{Q}) \leq 21$. However, since X has no rational point with $w = 0$, the number of rational points must be even, and therefore $\#X(\mathbb{Q}) \leq 20$. Since we have already found 10 rational points, we conclude that there are at most 10 additional rational points on X . \square

Theorem 3.43. *With C as in Lemma 3.41 we have the following:*

- (1) $C(\mathbb{Q}) = \{(0, 0, 0), (\pm 1, \pm 2, \pm 4)\}$.
- (2) *If (x, y, z) is a quadratic point on C , then $x \in \mathbb{Q} \setminus \{0, \pm 1\}$. Moreover, there exists $w \in \mathbb{Q}$ such that $(x, w) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 3.42.*

Proof. As noted in §2.3, the curve $y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$ is an affine model for the modular curve $X_1(16)$, which has exactly six rational points:

$$X_1(16)(\mathbb{Q}) = \{\infty, (0, 0), (\pm 1, \pm 2)\}.$$

It follows that if $(x, y, z) \in C(\mathbb{Q})$, then $(x, y) = (0, 0)$ or $(x, y) \in \{(\pm 1, \pm 2)\}$. Setting these values of x, y in the system (3.65) and solving for z we conclude that $C(\mathbb{Q}) = \{(0, 0, 0), (\pm 1, \pm 2, \pm 4)\}$.

Suppose now that $(x, y, z) \in C(\mathbb{Q})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$. We cannot have $x \in \{0, \pm 1\}$ since this would imply that $(x, y, z) \in C(\mathbb{Q})$; it follows that (x, y) cannot be a rational point on $X_1(16)$, and must therefore be quadratic. We claim that x must be rational. Indeed, if $x \notin \mathbb{Q}$, then by Theorem 2.4, either $x^2 = -1$ and $y = 0$, or $x^2 - 2x - 1 = 0$ and $y = 0$. However, in both cases we find that the second equation in (3.65) has no solution in K . Thus, we conclude that x must be a rational number different from $0, \pm 1$. Since $y^2 \in \mathbb{Q}$ and $y \notin \mathbb{Q}$, the Galois conjugate of y is $-y$. Hence, taking norms on both sides of the second equation in (3.65) we obtain

$$\begin{aligned} w^2 = x^{12} + 2x^{11} - 13x^{10} - 26x^9 + 67x^8 + 124x^7 + 26x^6 - 44x^5 \\ + 179x^4 - 62x^3 - 5x^2 + 6x + 1, \end{aligned}$$

where $w = N_{K/\mathbb{Q}}(z)/x$. \square

Corollary 3.44. *In addition to the known pair $(\mathbb{Q}(\sqrt{105}), -95/48)$ there are at most five pairs (K, c) , with K a quadratic number field and $c \in K$,*

for which $G(f_c, K)$ contains a graph of type 12(4). Moreover, for every such pair we must have $c \in \mathbb{Q}$.

Proof. Suppose that (K, c) is such a pair. Since f_c has a point of type 4_2 in K , then Lemma 3.41 implies that there is a point $(x, y, z) \in C(K)$ with $y(x^2 - 1) \neq 0$ such that

$$(3.67) \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x^2 - 1)^2}.$$

We cannot have $(x, y, z) \in C(\mathbb{Q})$ since this would imply that $x \in \{0, \pm 1\}$. Hence, (x, y, z) is a quadratic point on C . By Theorem 3.43, $x \in \mathbb{Q}$ and thus $c \in \mathbb{Q}$. Moreover, there is a rational number w such that $(x, w) \in X(\mathbb{Q})$. It follows from Lemma 3.42 that either $x = -3$ or x belongs to a list of at most 5 other rational numbers. Setting $x = -3$ yields $c = -95/48$, and the system (3.65) becomes

$$\begin{cases} y^2 = 420 \\ z^2 = 2256 - 96y. \end{cases}$$

Hence, $y = \pm 2\sqrt{105}$ and $z = \pm(2y - 24)$. In particular, $K = \mathbb{Q}(\sqrt{105})$, so we have recovered the known pair $(\mathbb{Q}(\sqrt{105}), -95/48)$. If $x \neq -3$, then there are at most five options for x ; each value of x determines the number c by (3.67) and the field K by (3.65). This gives at most five options for the pair (K, c) . \square

3.17. Graph 12(4,2). Our search described in §4.4 produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{-15}), -\frac{31}{48} \right)$$

for which the graph $G(f_c, K)$ is of type 12(4,2). We will show here that in addition to this known example there is at most one other such pair (K, c) consisting of a quadratic number field K and an element $c \in K$.

Lemma 3.45. *Let C/\mathbb{Q} be the affine curve of genus 9 defined by the equations*

$$(3.68) \quad \begin{cases} y^2 = -x(x^2 + 1)(x^2 - 2x - 1) \\ z^2 = -x(x^6 - 3x^4 - 16x^3 + 3x^2 - 1). \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$\begin{aligned} a &= \frac{z - x(x^2 - 1)}{2x(x^2 - 1)}, \\ b &= \frac{x - 1}{2(x + 1)} + \frac{y}{2x(x - 1)}, \\ c &= \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x^2 - 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : yz(x^2 - 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a is a point of period 2 for the map f_c and b is a point of period 4.

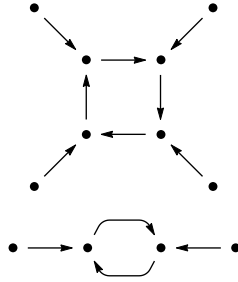


FIGURE 15. Graph type 12(4,2)

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point satisfying $x(x^2 - 1) \neq 0$. Defining $a, b, c \in K$ as in the lemma, it is a straightforward calculation to verify that $f_c^2(a) = a$, $f_c^4(b) = b$, and

$$(3.69) \quad a - f_c(a) = \frac{z}{x(x^2 - 1)}, \quad b - f_c^2(b) = \frac{y}{x(x - 1)}.$$

It follows from these relations that if $yz \neq 0$, then a is a point of period 2 for f_c and b is a point of period 4. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ satisfy the conditions of the lemma. Since a is a point of period 2 for f_c , then by Proposition 3.4 there is an element $\sigma \in K$ such that

$$(3.70) \quad a = \sigma - 1/2, \quad c = -3/4 - \sigma^2.$$

Since b is a point of period 4, then by Proposition 3.4 there are elements $x, y \in K$ with $y(x^2 - 1) \neq 0$ such that $y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$ and

$$(3.71) \quad b = \frac{x - 1}{2(x + 1)} + \frac{y}{2x(x - 1)}, \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x - 1)^2(x + 1)^2}.$$

Equating the two expressions for c given in (3.70) and (3.71), and setting $z = 2x(x - 1)(x + 1)\sigma$, we obtain the relation

$$z^2 = -x(x^6 - 3x^4 - 16x^3 + 3x^2 - 1).$$

Thus, $(x, y, z) \in C(K)$ with $\varphi(x, y, z) = (a, b, c)$ and $y(x^2 - 1) \neq 0$. Furthermore, the relations (3.69) imply that $z \neq 0$. To see that φ is injective, one

can verify that if $\varphi(x, y, z) = (a, b, c)$, then

$$x = \frac{1 + b + f_c^2(b)}{1 - b - f_c^2(b)}, \quad y = \frac{2x(x^2 - 1)b - x(x - 1)^2}{x + 1}, \quad z = x(x^2 - 1)(2a + 1).$$

□

Lemma 3.46. *Let X/\mathbb{Q} be the hyperelliptic curve of genus 4 defined by the equation*

$$w^2 = (x^2 + 1)(x^2 - 2x - 1)(x^6 - 3x^4 - 16x^3 + 3x^2 - 1).$$

Then $X(\mathbb{Q})$ contains the twelve points

$$\infty^+, \infty^-, (\pm 1, \pm 8), (0, \pm 1), (3, \pm 40), (-1/3, \pm 40/243)$$

and at most four other points.

Proof. Using the Magma function `Points` we search for rational points on X of height at most 10^5 and obtain the points listed above. Using the `RankBound` function we find that $\text{Jac}(X)(\mathbb{Q})$ has rank at most 2; thus, we may apply the method of Chabauty and Coleman to bound the number of rational points on X . The prime 11 is of good reduction for X , and we compute $\#X(\mathbb{F}_{11}) = 12$; Stoll's bound (Theorem 3.3) then yields $\#X(\mathbb{Q}) \leq 16$. □

Remark. The curve X from Lemma 3.46 has an automorphism of order 4 given by $(x, w) \mapsto (-1/x, w/x^5)$. Hence, if there is some rational point $(x_0, w_0) \in X(\mathbb{Q})$ missing from the list above, then in fact there are exactly four of them, namely (x_0, w_0) , $(-1/x_0, w_0/x_0^5)$, $(x_0, -w_0)$, and $(-1/x_0, -w_0/x_0^5)$.

Theorem 3.47. *With C as in Lemma 3.45 we have the following:*

- (1) $C(\mathbb{Q}) = \{(0, 0, 0), (\pm 1, \pm 2, \pm 4)\}$.
- (2) *The quadratic points (x, y, z) on C with $x \notin \mathbb{Q}$ are the points*

$$(x, 0, \pm(6x + 2)) \quad \text{with} \quad x^2 - 2x - 1 = 0,$$

which are defined over the field $\mathbb{Q}(\sqrt{2})$.

- (3) *If (x, y, z) is a quadratic point on C with $x \in \mathbb{Q}$, then there exists a rational number w such that $(x, w) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 3.46. Moreover, $x \notin \{0, \pm 1\}$.*

Proof. As noted in §2.3, the curve defined by the equation

$$y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$$

is an affine model for the modular curve $X_1(16)$, which has exactly six rational points:

$$(3.72) \quad X_1(16)(\mathbb{Q}) = \{\infty, (0, 0), (\pm 1, \pm 2)\}.$$

Let C_2 denote the hyperelliptic curve defined by the equation

$$z^2 = -x(x^6 - 3x^4 - 16x^3 + 3x^2 - 1).$$

Note that C_2 has an involution given by $(x, z) \mapsto (-1/x, z/x^4)$. The quotient of C_2 by this involution is the elliptic curve E defined by the Weierstrass equation $s^2 + s = r^3$; the quotient map $C_2 \rightarrow E$ of degree 2 is given by

$$r = \frac{1 - x^2}{4x}, \quad s = \frac{-4x^2 - z}{8x^2}.$$

The elliptic curve E is the curve 27a3 in Cremona’s tables, and has exactly three rational points. It follows that C_2 has at most six rational points, and a search quickly yields six such points:

$$(3.73) \quad C_2(\mathbb{Q}) = \{\infty, (0, 0), (\pm 1, \pm 4)\}.$$

From (3.72) and (3.73) we deduce that $C(\mathbb{Q}) = \{(0, 0, 0), (\pm 1, \pm 2, \pm 4)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. x is quadratic. In the terminology of §2, the point (x, y) is then a nonobvious quadratic point on $X_1(16)$, so Theorem 2.4 implies that either $x^2 + 1 = 0$ or $x^2 - 2x - 1 = 0$. If $x^2 + 1 = 0$, one can check that the equation $z^2 = -x(x^6 - 3x^4 - 16x^3 + 3x^2 - 1)$ has no solution $z \in K$; hence, this cannot occur. Assuming $x^2 - 2x - 1 = 0$, we can solve the system (3.68) to obtain $y = 0, z = \pm(6x + 2)$. Thus, we have shown that the only quadratic points on C having a quadratic x -coordinate are the points $(x, 0, \pm(6x + 2))$ with $x^2 - 2x - 1 = 0$.

Case 2. $x \in \mathbb{Q}$. We cannot have $x \in \{0, \pm 1\}$ since this would imply that $y \in \{0, \pm 2\}$ and $z \in \{0, \pm 4\}$, contradicting the assumption that (x, y, z) is a quadratic point on C ; hence, $x(x^2 - 1) \neq 0$. It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x \in \{0, \pm 1\}$, by (3.72). Similarly, (3.73) implies that $z \notin \mathbb{Q}$. Thus, we have $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the rational numbers $-x(x^2 + 1)(x^2 - 2x - 1)$ and $-x(x^6 - 3x^4 - 16x^3 + 3x^2 - 1)$ must have the same squarefree part; hence, their product is a square, so there is a rational number v such that

$$v^2 = x^2(x^2 + 1)(x^2 - 2x - 1)(x^6 - 3x^4 - 16x^3 + 3x^2 - 1).$$

Letting $w = v/x$ we then have $(x, w) \in X(\mathbb{Q})$. □

Corollary 3.48. *In addition to the known pair $(\mathbb{Q}(\sqrt{-15}), -31/48)$ there is at most one pair (K, c) , with K a quadratic number field and $c \in K$, for which $G(f_c, K)$ contains a graph of type 12(4,2). Moreover, for every such pair we must have $c \in \mathbb{Q}$.*

Proof. Suppose that (K, c) is such a pair. By Lemma 3.45 there is a point $(x, y, z) \in C(K)$ with $y(x^2 - 1) \neq 0$ such that

$$(3.74) \quad c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x - 1)^2(x + 1)^2}.$$

It follows from Theorem 3.47 that there is a rational number w such that $(x, w) \in X(\mathbb{Q})$; in particular, $c \in \mathbb{Q}$. We consider two possibilities: either

$X(\mathbb{Q})$ consists of the 12 points listed in Lemma 3.46, or $\#X(\mathbb{Q}) = 16$ (see the remark following the lemma).

Suppose first that $\#X(\mathbb{Q}) = 12$. Then we must have $x = 3$ or $x = -1/3$, since the values $x = 0, \pm 1$ are not allowed. If $x = 3$, then (3.74) yields $c = -31/48$ and we have $K = \mathbb{Q}(y)$ with $y^2 = -60$, so $K = \mathbb{Q}(\sqrt{-15})$. Thus, we recover the pair (K, c) in the statement of the corollary. With $x = -1/3$ we again obtain $c = -31/48$ and $K = \mathbb{Q}(\sqrt{-15})$.

Suppose now that $\#X(\mathbb{Q}) = 16$. Then there are rational numbers x_0 and w_0 such that $X(\mathbb{Q})$ consists of the twelve points listed in Lemma 3.46 and the four points

$$(x_0, w_0), (-1/x_0, w_0/x_0^5), (x_0, -w_0), (-1/x_0, -w_0/x_0^5).$$

We have already determined what K and c must be if $x \in \{3, -1/3\}$, so it remains only to consider the case where (x, w) is one of the four points listed above. Each one of these points may lead via (3.68) and (3.74) to a new pair (K, c) ; however, we make the following observations: first, the expression for c given in (3.74) is invariant under the change of variables $x \mapsto -1/x$, so that all four points will yield the same value of c . Second, we know that $K = \mathbb{Q}(y)$ and $y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$. One can check that, regardless of whether $x = x_0$ or $x = -1/x_0$, the field K remains the same, since the value of $-x(x^2 + 1)(x^2 - 2x - 1)$ only changes by a factor of x_0^6 when we substitute $x = x_0$ and $x = -1/x_0$. Hence, the case $\#X(\mathbb{Q}) = 16$ will yield at most one other possibility for the pair (K, c) . \square

3.18. Graph 14(2,1,1). Our search described in §4.4 produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{17}), -\frac{21}{16} \right)$$

for which the graph $G(f_c, K)$ is of type 14(2,1,1). We will show here that this is the only such pair (K, c) consisting of a quadratic number field K and an element $c \in K$.

Lemma 3.49. *Let C/\mathbb{Q} be the affine curve of genus 5 defined by the equations*

$$(3.75) \quad \begin{cases} y^2 = 2(x^3 + x^2 - x + 1) \\ z^2 = 2x(x^3 + x^2 + x - 1). \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$a = \frac{y}{x^2 - 1}, \quad b = \frac{z}{x^2 - 1}, \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}.$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : x(x^4 - 1)(x^2 + 4x - 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of type 2₃ for the map f_c satisfying $f_c^2(a) = f_c^2(b)$ and $f_c(a) \neq f_c(b)$.

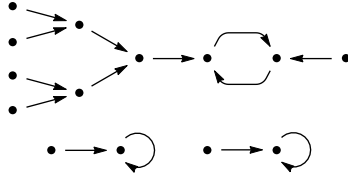


FIGURE 16. Graph type 14(2,1,1)

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point with $x^2 \neq 1$. Defining $a, b, c \in K$ as in the lemma, it is a straightforward calculation to verify $f_c^2(a) = f_c^2(b)$, $f_c^3(a) = f_c^5(a)$ and

$$(3.76) \quad \begin{aligned} f_c(b) - f_c(a) &= \frac{2(x^2 + 1)}{x^2 - 1} \\ f_c^4(a) - f_c^3(a) &= \frac{x^2 + 4x - 1}{x^2 - 1} \\ f_c^4(a) - f_c^2(a) &= \frac{4x}{x^2 - 1}. \end{aligned}$$

It follows from these relations that if $x(x^2 + 1)(x^2 + 4x - 1) \neq 0$, then a and b are points of type 2_3 for f_c such that $f_c^2(a) = f_c^2(b)$ and $f_c(a) \neq f_c(b)$. Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ satisfy the conditions of the lemma. Then an argument given in [31, page 23] shows that there is an element $x \in K \setminus \{-1, 0, 1\}$ such that

$$(3.77) \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2} \quad \text{and} \quad a^2 = \frac{2(x^3 + x^2 - x + 1)}{(x^2 - 1)^2}.$$

Since $f_c(b) = -f_c(a)$, then $b^2 = -a^2 - 2c$, so using (3.77) we obtain

$$(3.78) \quad b^2 = \frac{2x(x^3 + x^2 + x - 1)}{(x^2 - 1)^2}.$$

Letting $y = a(x^2 - 1)$ and $z = b(x^2 - 1)$ we see that $(x, y, z) \in C(K)$ and $\varphi(x, y, z) = (a, b, c)$. Furthermore, the relations (3.76) imply that necessarily $x(x^2 + 1)(x^2 + 4x - 1) \neq 0$.

To see that φ is injective, one can verify that if $\varphi(x, y, z) = (a, b, c)$, then

$$x = \frac{f_c(a) - 1}{f_c^2(a)}, \quad y = a(x^2 - 1), \quad z = b(x^2 - 1). \quad \square$$

Lemma 3.50. *Let X/\mathbb{Q} be the hyperelliptic curve of genus 3 defined by the equation*

$$s^2 = x(x^3 + x^2 + x - 1)(x^3 + x^2 - x + 1).$$

Then $X(\mathbb{Q}) = \{(0, 0), (\pm 1, \pm 2), \infty\}$.

Proof. The curve X has an involution given by $(x, s) \mapsto (-1/x, -s/x^4)$; the quotient of X by this involution is the curve Y of genus 2 defined by the equation

$$r^2 = 2u^5 + 2u^4 + 4u^3 + 3u^2 + 2u + 1,$$

and the quotient map $X \rightarrow Y$ of degree 2 is given by

$$u = \frac{x^2 - 1}{2x}, \quad r = \frac{s(x^2 + 1)}{4x^3}.$$

Using the Magma function `RankBound` we find that $\text{Jac}(Y)(\mathbb{Q})$ has rank 0, so we can easily obtain the rational points on Y (for instance, using the function `Chabauty0`). Carrying out this calculation, we obtain

$$Y(\mathbb{Q}) = \{(0, \pm 1), \infty\}.$$

Since Y has three rational points, then X can have at most six rational points, and we have already listed six points. \square

Theorem 3.51. *With C as in Lemma 3.49 we have the following:*

- (1) $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.
- (2) *If K is a quadratic field different from $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$, then $C(K) = C(\mathbb{Q})$.*
- (3) *For $K = \mathbb{Q}(\sqrt{2})$, $C(K) \setminus C(\mathbb{Q}) = \{(0, \pm\sqrt{2}, 0)\}$.*
- (4) *For $K = \mathbb{Q}(\sqrt{17})$,*

$$C(K) \setminus C(\mathbb{Q}) = \{(x, \pm(4x + 2), \pm(12x + 2)) : x^2 - 8x - 1 = 0\}.$$

Proof. Let C_1 be the elliptic curve defined by the equation

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

As shown in the proof of Theorem 3.32,

$$(3.79) \quad C_1(\mathbb{Q}) = \{\infty, (\pm 1, \pm 2)\},$$

since C_1 is the modular curve $X_1(11)$. Now let C_2 be the hyperelliptic curve of genus 1 defined by the equation $z^2 = 2x(x^3 + x^2 + x - 1)$. Since C_2 has a rational point — for instance, the point $(0, 0)$ — it is an elliptic curve; in fact, C_2 is also the curve $X_1(11)$, as one can check that the map $(x, z) \mapsto (-1/x, z/x^2)$ defines a birational morphism from C_2 to C_1 . We conclude that C_2 has exactly five rational points, and these are easily found:

$$(3.80) \quad C_2(\mathbb{Q}) = \{(0, 0), (\pm 1, \pm 2)\}.$$

From (3.79) and (3.80) we deduce that $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 2$, contradicting the assumption that (x, y, z) is a quadratic point on C . It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$, by (3.79). If $z \in \mathbb{Q}$, then (3.80) implies that $x = z = 0$, and

then $y^2 = 2(x^3 + x^2 - x + 1) = 2$. Thus, we obtain the quadratic points $(0, \pm\sqrt{2}, 0)$.

Suppose now that $z \notin \mathbb{Q}$. Then $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the rational numbers $2(x^3 + x^2 - x + 1)$ and $2x(x^3 + x^2 + x - 1)$ must have the same squarefree part; hence, their product is a square, so there is a rational number s such that

$$s^2 = x(x^3 + x^2 + x - 1)(x^3 + x^2 - x + 1).$$

Since $x \neq \pm 1$, Lemma 3.50 implies that $x = 0$, so $z^2 = 2x(x^3 + x^2 + x - 1) = 0$ and therefore $z = 0 \in \mathbb{Q}$, a contradiction. Hence, the case $z \notin \mathbb{Q}$ cannot occur.

Thus, we have shown that the only quadratic points on C having a rational x -coordinate are the points $(0, \pm\sqrt{2}, 0)$.

Case 2. x is quadratic. Let $t^2 + at + b \in \mathbb{Q}[t]$ be the minimal polynomial of x . By Lemma 2.2 applied to the equation $y^2 = 2(x^3 + x^2 - x + 1)$, there exist a rational number v and a point $(x_0, y_0) \in \{(\pm 1, \pm 2)\}$ such that

$$(3.81) \quad a = \frac{2x_0 - v^2 + 2}{2}, \quad b = \frac{2x_0^2 + v^2x_0 + 2x_0 - 2y_0v - 2}{2}.$$

We now use the relation $z^2 = 2x(x^3 + x^2 + x - 1)$ to obtain a different expression for a and b . Defining $p := -1/x$ and $q := z/x^2$ we have

$$q^2 = 2(p^3 + p^2 - p + 1)$$

with p quadratic, so again by Lemma 2.2, there exist a rational number w and a point $(p_0, q_0) \in \{(\pm 1, \pm 2)\}$ such that the minimal polynomial of p has the form $t^2 + dt + e \in \mathbb{Q}[t]$, where

$$(3.82) \quad d = \frac{2p_0 - w^2 + 2}{2}, \quad e = \frac{2p_0^2 + w^2p_0 + 2p_0 - 2q_0w - 2}{2}.$$

Since x and p are related by $p = -1/x$, it is easy to see that $a = -d/e$ and $b = 1/e$. Hence, we arrive at the system

$$(3.83) \quad \begin{cases} ae + d = 0 \\ be - 1 = 0, \end{cases}$$

where a, b, d, e are given by (3.81) and (3.82). For each choice of the points (x_0, y_0) and (p_0, q_0) , the system (3.83) defines a 0-dimensional scheme S in (v, w) -plane over \mathbb{Q} , so its set of rational points can be determined. There are a total of 16 choices of pairs of points; for each pair we use the Magma function `RationalPoints` to determine all rational points on the corresponding scheme S , and we discard those rational points that lead to a polynomial $t^2 + at + b$ that is reducible. The result of this computation is that in every case when a rational point on one of the 16 schemes S leads to an irreducible polynomial $t^2 + at + b$, this polynomial is $t^2 - 8t - 1$; hence, this must be the minimal polynomial of x . Knowing that $x^2 - 8x - 1 = 0$, the system (3.75) can now be solved to obtain $y = \pm(4x + 2)$ and $z = \pm(12x + 2)$.

We conclude that every quadratic point on C having a quadratic x -coordinate is defined over the field $K = \mathbb{Q}(\sqrt{17})$ and has the form

$$(x, \pm(4x + 2), \pm(12x + 2)) \quad \text{where} \quad x^2 - 8x - 1 = 0.$$

The theorem now follows immediately. \square

Corollary 3.52. *Let $c \in K$ with K a quadratic field. Suppose that $G(f_c, K)$ contains a graph of type $14(2,1,1)$. Then $c = -21/16$ and $K = \mathbb{Q}(\sqrt{17})$.*

Proof. By Lemma 3.49, there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that

$$(3.84) \quad c = -\frac{x^4 + 2x^3 + 2x^2 - 2x + 1}{(x^2 - 1)^2}.$$

It follows from Theorem 3.51 that $K = \mathbb{Q}(\sqrt{17})$ and that $x \in K$ satisfies $x^2 - 8x - 1 = 0$. Using (3.84) we then obtain $c = -21/16$. \square

3.19. Graph 14(3,1,1). Our search described in §4.4 produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{33}), -\frac{29}{16} \right)$$

for which the graph $G(f_c, K)$ is of type $14(3,1,1)$. We will show here that this is the only such pair (K, c) consisting of a quadratic number field K and an element $c \in K$.

Lemma 3.53. *Let C/\mathbb{Q} be the affine curve of genus 9 defined by the equations*

$$(3.85) \quad \begin{cases} y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1 \\ z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1. \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$\begin{aligned} a &= \frac{y + x^2 + x}{2x(x + 1)}, \\ b &= \frac{z}{2x(x + 1)}, \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : x(x + 1)(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a is a fixed point for the map f_c and b is a point of type 3_2 .

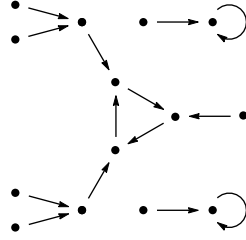


FIGURE 17. Graph type 14(3,1,1)

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point satisfying $x(x + 1) \neq 0$. Defining $a, b, c \in K$ as in the lemma, it is a routine calculation to verify that $f_c(a) = a$, $f_c^5(b) = f_c^2(b)$, and

$$(3.86) \quad f_c^2(b) - f_c^3(b) = \frac{x^2 + x + 1}{x + 1}, \quad f_c^4(b) - f_c(b) = \frac{x^3 + 2x^2 + x + 1}{x^2 + x}.$$

It follows that if $(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0$, then b is a point of type 3_2 for f_c . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ satisfy the conditions of the lemma. Since a is a fixed point for f_c , then by Proposition 3.4 there is an element $\rho \in K$ such that

$$(3.87) \quad a = \rho + 1/2, \quad c = 1/4 - \rho^2.$$

Since b is a point of type 3_2 for f_c , it follows from the discussion in [31, page 23–24] that there is an element $x \in K \setminus \{-1, 0\}$ such that

$$(3.88) \quad b^2 = \frac{x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1}{4x^2(x + 1)^2},$$

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

Letting $z = 2x(x + 1)b$ we then have the relation

$$z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

Equating the two expressions for c given in (3.87) and (3.88), and defining $y = 2x(x + 1)\rho$, we obtain the equation

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Note that

$$a = \frac{1}{2} + \rho = \frac{1}{2} + \frac{y}{2x(x + 1)} = \frac{y + x^2 + x}{2x(x + 1)}.$$

Thus, we have a point $(x, y, z) \in C(K)$ such that $\varphi(x, y, z) = (a, b, c)$ and $x(x + 1) \neq 0$. Furthermore, (3.86) implies that $(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0$.

To see that φ is injective, one can verify that if $\varphi(x, y, z) = (a, b, c)$, then

$$x = f_c^2(b) - f_c(b), \quad y = x(x+1)(2a-1), \quad z = 2x(x+1)b. \quad \square$$

Lemma 3.54. *Let X/\mathbb{Q} be the hyperelliptic curve defined by the equation*

$$33v^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

Then $X(\mathbb{Q}) = \{(-2, \pm 1)\}$.

Proof. Using the Magma functions `RankBounds` and `TorsionSubgroup` we find that $\text{Jac}(X)(\mathbb{Q}) \cong \mathbb{Z}$; thus, we may apply the method of Chabauty and Coleman to bound the number of rational points on X . We will in fact be able to determine all rational points on X by using the method outlined in [3, §4.4], which is available in Magma via the function `Chabauty`. This function will use a Mordell–Weil sieve and Chabauty’s method in order to compute $X(\mathbb{Q})$. The required input is a rational point on X and a generator for $J(\mathbb{Q})$, where $J = \text{Jac}(X)$. For purposes of working with Magma it will be convenient to use a slightly different equation for X , namely

$$y^2 = 33(x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1);$$

we will then show that the only rational points on this curve are the points $P_0 = (-2, 33)$ and $P_1 = (-2, -33)$.

Let $D \in J(\mathbb{Q})$ be the divisor class of $P_1 - P_0$; we claim that D generates $J(\mathbb{Q})$. Assuming this for the moment, we use the `Chabauty` function with input $D \in J(\mathbb{Q})$ and $P_1 \in X(\mathbb{Q})$ to obtain as output the complete list of rational points on X , which consists of the two points we have listed.

In order to show that D generates $J(\mathbb{Q})$ we will use the method proposed by Stoll in [36, §7]. Let h and \hat{h} denote the naive and canonical heights on $J(\mathbb{Q})$, respectively. (See [12, page 335] for the definitions.) Using Magma’s `Height` function we find that $\hat{h}(D) = 4.91745\dots$. In particular, D has infinite order in $J(\mathbb{Q})$. We claim that D is not divisible in $J(\mathbb{Q})$. Suppose that it is, and let $Q \in J(\mathbb{Q})$ be a point such that $[n]Q = D$ for some $n > 1$. Then $n^2\hat{h}(Q) = \hat{h}(D) = 4.91745\dots$, so $\hat{h}(Q) < 4.92/4 = 1.23$. The `HeightConstant` function applied to J yields the number $c = 3.34897\dots$ with the property that $h(P) - \hat{h}(P) \leq c$ for every point $P \in J(\mathbb{Q})$. In particular, we have $h(Q) < 1.23 + c < 4.58$. Using Stoll’s `j-points` program, which is available in Magma via the function `Points`, we compute all points in $J(\mathbb{Q})$ whose naive height does not exceed 4.6. The result is that there is only one such point, namely the trivial point. Thus, we conclude that $Q = 0$, and hence $D = [n]Q = 0$, a contradiction. This shows that D is not divisible in $J(\mathbb{Q})$, and since it has infinite order, it must therefore generate $J(\mathbb{Q})$. This completes the proof. \square

Theorem 3.55. *With C as in Lemma 3.53 we have the following:*

- (1) $C(\mathbb{Q}) = \{(0, \pm 1, \pm 1), (-1, \pm 1, \pm 1)\}$.
- (2) *If K is a quadratic field different from $\mathbb{Q}(\sqrt{33})$, then $C(K) = C(\mathbb{Q})$.*

- (3) For $K = \mathbb{Q}(\sqrt{33})$, we have
 $C(K) \setminus C(\mathbb{Q}) = \{(1, \pm\sqrt{33}, \pm 3), (-2, \pm\sqrt{33}, \pm\sqrt{33})\}.$

Proof. As noted in §2.3, the curve $y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$ is an affine model for the modular curve $X_1(18)$, which has exactly six rational points, namely $\infty^+, \infty^-, (0, \pm 1), (-1, \pm 1)$. The curve

$$z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$$

was studied by Poonen in [31, §4], where it is shown that its only affine rational points are $(-1, \pm 1), (0, \pm 1)$, and $(1, \pm 3)$. Thus, we know all rational solutions to each of the defining equations of C , and we conclude that $C(\mathbb{Q}) = \{(0, \pm 1, \pm 1), (-1, \pm 1, \pm 1)\}.$

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1. x is quadratic. In the terminology of §2, the point (x, y) is then a nonobvious quadratic point on $X_1(18)$, so Theorem 2.4 implies that x is a primitive cube root of unity, and in particular $K = \mathbb{Q}(\sqrt{-3})$. However, in this case one can check that the equation $z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$ has no solution $z \in K$. This is a contradiction, so we conclude that x cannot be quadratic.

Case 2. $x \in \mathbb{Q}$. We cannot have $y \in \mathbb{Q}$, since this would imply that $x \in \{-1, 0\}$, which in turn implies that $z = \pm 1$, contradicting the assumption that (x, y, z) is a quadratic point on C . If $z \in \mathbb{Q}$, then $x \in \{-1, 0, 1\}$; however x cannot equal -1 or 0 , since this would imply that $y = \pm 1 \in \mathbb{Q}$. Therefore, if $z \in \mathbb{Q}$, then $x = 1$. The system (3.85) can then be solved to obtain $y = \pm\sqrt{33}, z = \pm 3$. Thus, we have shown that the only quadratic points on C having $z \in \mathbb{Q}$ are $(1, \pm\sqrt{33}, \pm 3)$.

We assume henceforth that z is quadratic. Define polynomials $f(t), g(t) \in \mathbb{Q}[t]$ by

$$\begin{aligned} f(t) &= t^6 + 2t^5 + 5t^4 + 10t^3 + 10t^2 + 4t + 1, \\ g(t) &= t^6 - 2t^4 + 2t^3 + 5t^2 + 2t + 1. \end{aligned}$$

Since both y and z are quadratic, then $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the rational numbers $f(x)$ and $g(x)$ must have the same squarefree part d ; hence, there are rational numbers u, v such that

$$(3.89) \quad \begin{cases} du^2 = f(x) \\ dv^2 = g(x). \end{cases}$$

Suppose that p is a prime number dividing d . The above equations imply that u, v , and x all lie in the local ring $\mathbb{Z}_{(p)}$, so we may reduce (3.89) modulo p to obtain $f(x) \equiv g(x) \equiv 0 \pmod{p}$. Hence, the polynomials $f(t)$ and $g(t)$ have a common root modulo p , so their resultant, which is $4521 = 3 \cdot 11 \cdot 137$, must be divisible by p . Therefore, d can only be divisible by primes in the set $\{3, 11, 137\}$. Furthermore, the polynomial function $f : \mathbb{R} \rightarrow \mathbb{R}$ induced

by $f(t)$ only takes positive values, so the first equation in (3.89) implies that $d > 0$. Finally, since $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, we cannot have $d = 1$. Therefore, we conclude that

$$d \in \{3, 11, 137, 33, 411, 1507, 4521\}.$$

We proceed now to narrow down the possible values of d . For each number d in the above set, we can check whether the hyperelliptic curves $du^2 = f(x)$ and $dv^2 = g(x)$ have points over all completions of \mathbb{Q} ; the Magma function `HasPointsEverywhereLocally` can be used for this. Carrying out this computation we find that in all cases, except when $d = 33$, at least one of these curves fails to have 2-adic or 3-adic points; in particular, for these values of d the system (3.89) cannot have a rational solution. Therefore, we must have $d = 33$. It follows from (3.89) that $(x, v) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 3.54, so the lemma implies that $x = -2$. The system (3.85) can then be solved to obtain $(x, y, z) = (-2, \pm\sqrt{33}, \pm\sqrt{33})$. Thus, we have shown that the only quadratic points on C are the points $(1, \pm\sqrt{33}, \pm 3)$ and $(-2, \pm\sqrt{33}, \pm\sqrt{33})$. \square

Corollary 3.56. *Let $c \in K$ with K a quadratic field. Suppose that $G(f_c, K)$ contains a graph of type $14(3,1,1)$. Then $c = -29/16$ and $K = \mathbb{Q}(\sqrt{33})$.*

Proof. By Lemma 3.53 there is a point $P = (x, y, z) \in C(K)$ with $x(x+1) \neq 0$ such that

$$(3.90) \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}.$$

Since $x \notin \{0, -1\}$, then P cannot be a rational point on C . It follows from Theorem 3.55 that $K = \mathbb{Q}(\sqrt{33})$ and that $x = 1$ or $x = -2$. Substituting these values of x into (3.90) we obtain $c = -29/16$ in both cases. \square

3.20. Graph $14(3,2)$. Our search described in §4.4 found the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{17}), -29/16\right)$$

for which the graph $G(f_c, K)$ is of type $14(3,2)$. We will show here that this is the only such pair (K, c) consisting of a quadratic number field K and an element $c \in K$.

Lemma 3.57. *Let C/\mathbb{Q} be the affine curve of genus 9 defined by the equations*

$$(3.91) \quad \begin{cases} y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1 \\ z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1. \end{cases}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \text{Spec } \mathbb{Q}[a, b, c]$ given by

$$\begin{aligned} a &= \frac{y - x^2 - x}{2x(x + 1)}, \\ b &= \frac{z}{2x(x + 1)}, \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x + 1)^2}. \end{aligned}$$

For every number field K , the map φ induces a bijection from the set

$$\{(x, y, z) \in C(K) : xy(x + 1)(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a is a point of period 2 and b is a point of type 3_2 for the map f_c .

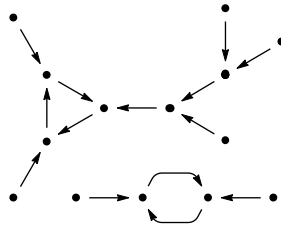


FIGURE 18. Graph type 14(3,2)

Proof. Fix a number field K and suppose that $(x, y, z) \in C(K)$ is a point satisfying $x(x + 1) \neq 0$. Defining $a, b, c \in K$ as in the lemma, it is a straightforward calculation to verify that $f_c^2(a) = a$, $f_c^5(b) = f_c^2(b)$, and

$$\begin{aligned} (3.92) \quad a - f_c(a) &= \frac{y}{x(x + 1)} \\ f_c^2(b) - f_c^3(b) &= \frac{x^2 + x + 1}{x + 1} \\ f_c^4(b) - f_c(b) &= \frac{x^3 + 2x^2 + x + 1}{x^2 + x}. \end{aligned}$$

It follows from these relations that if $y(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0$, then a is a point of period 2 for f_c and b is a point of type 3_2 . Hence, φ gives a well-defined map.

To see that φ is surjective, suppose that $a, b, c \in K$ satisfy the conditions of the lemma. Since a is a point of period 2 for f_c , Proposition 3.4 implies that there is an element $\sigma \in K$ such that

$$(3.93) \quad a = \sigma - 1/2, \quad c = -3/4 - \sigma^2.$$

Since b is a point of type 3_2 for f_c , it follows from the discussion in [31, page 23–24] that there is an element $x \in K \setminus \{-1, 0\}$ such that

$$(3.94) \quad \begin{aligned} b^2 &= \frac{x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1}{4x^2(x+1)^2} \\ c &= -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}. \end{aligned}$$

In particular, letting $z = 2x(x+1)b$ we have the relation

$$z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1.$$

Equating the two expressions for c given in (3.93) and (3.94), and defining $y = 2x(x+1)\sigma$, we obtain the equation $y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$. Note that

$$a = \sigma - \frac{1}{2} = \frac{y}{2x(x+1)} - \frac{1}{2} = \frac{y - x^2 - x}{2x(x+1)}.$$

Thus, we have a point $(x, y, z) \in C(K)$ such that $\varphi(x, y, z) = (a, b, c)$ and $x(x+1) \neq 0$. Finally, the relations (3.92) imply that

$$y(x^2 + x + 1)(x^3 + 2x^2 + x + 1) \neq 0.$$

To see that φ is injective, one can verify that if $\varphi(x, y, z) = (a, b, c)$, then

$$x = f_c^2(b) - f_c(b), \quad y = x(x+1)(2a+1), \quad z = 2x(x+1)b. \quad \square$$

Theorem 3.58. *With C as in Lemma 3.57 we have the following:*

- (1) $C(\mathbb{Q}) = \{(0, \pm 1, \pm 1), (-1, \pm 1, \pm 1)\}$.
- (2) *If K is a quadratic field different from $\mathbb{Q}(\sqrt{17})$, then $C(K) = C(\mathbb{Q})$.*
- (3) *For $K = \mathbb{Q}(\sqrt{17})$, $C(K) \setminus C(\mathbb{Q}) = \{(1, \pm\sqrt{17}, \pm 3)\}$.*

Proof. As noted in the proof of Theorem 3.28, the only rational solutions to the equation $y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$ are $(0, \pm 1)$ and $(-1, \pm 1)$, since the hyperelliptic curve defined by this equation is the modular curve $X_1(13)$. The curve $z^2 = x^6 - 2x^4 + 2x^3 + 5x^2 + 2x + 1$ was studied in [31, §4], where it is shown that its only affine rational points are $(-1, \pm 1)$, $(0, \pm 1)$, and $(1, \pm 3)$. We conclude that $C(\mathbb{Q}) = \{(0, \pm 1, \pm 1), (-1, \pm 1, \pm 1)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$. We claim that x must be rational. Indeed, if x were quadratic, then (x, y) would be a nonobvious quadratic point on $X_1(13)$, and such points do not exist, by Theorem 2.4; hence, $x \in \mathbb{Q}$. We cannot have $y \in \mathbb{Q}$, since this would imply that $x \in \{-1, 0\}$, which in turn implies that $z = \pm 1$, thus contradicting the assumption that (x, y, z) is a quadratic point on C ; hence, $y \notin \mathbb{Q}$.

Case 1. $z \in \mathbb{Q}$. Since $x \in \mathbb{Q}$, then $x \in \{-1, 0, 1\}$. However, x cannot equal -1 or 0 since this would imply that $y = \pm 1 \in \mathbb{Q}$; therefore, $x = 1$. The system (3.91) can then be solved to obtain $y = \pm\sqrt{17}$, $z = \pm 3$. Thus, we obtain the quadratic points $(1, \pm\sqrt{17}, \pm 3)$.

Case 2. z is quadratic. Define polynomials $f(t), g(t) \in \mathbb{Q}[t]$ by

$$\begin{aligned} f(t) &= t^6 + 2t^5 + t^4 + 2t^3 + 6t^2 + 4t + 1, \\ g(t) &= t^6 - 2t^4 + 2t^3 + 5t^2 + 2t + 1. \end{aligned}$$

Since both y and z are quadratic, then $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so the rational numbers $f(x)$ and $g(x)$ must have the same squarefree part d ; hence, there are rational numbers u, v such that

$$(3.95) \quad \begin{cases} du^2 = f(x) \\ dv^2 = g(x). \end{cases}$$

The polynomial function $f : \mathbb{R} \rightarrow \mathbb{R}$ induced by $f(t)$ only takes positive values, so the first equation in (3.95) implies that $d > 0$. Moreover, since $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, we cannot have $d = 1$. Let p be a prime number dividing d . The above equations imply that u, v , and x all lie in the local ring $\mathbb{Z}_{(p)}$, so we may reduce (3.95) modulo p to obtain $f(x) \equiv g(x) \equiv 0 \pmod{p}$. Hence, the polynomials $f(t)$ and $g(t)$ have a common root modulo p , so their resultant, which is $4321 = 29 \cdot 149$, must be divisible by p . Therefore, d can only be divisible by primes in the set $\{29, 149\}$, and so

$$d \in \{29, 149, 4321\}.$$

For the values $d = 29$ and 149 one can check that the hyperelliptic curves $du^2 = f(x)$ and $dv^2 = g(x)$ have no 2-adic point, and hence have no rational point; therefore, d must equal 4321 .

Let X be the hyperelliptic curve defined by the equation $4321u^2 = f(x)$. Using the Magma functions `RankBound` and `TorsionSubgroup` we find that $\text{Jac}(X)(\mathbb{Q})$ is trivial. Since X has no rational Weierstrass point, the number of rational points on X must be even. However, any two points in $X(\mathbb{Q})$ would yield a nontrivial point in $\text{Jac}(X)(\mathbb{Q})$, so we must have $X(\mathbb{Q}) = \emptyset$. This is a contradiction since $(x, u) \in X(\mathbb{Q})$.

Since the assumption that z is quadratic has led to a contradiction, we conclude that this case cannot occur, so the analysis done in the case $z \in \mathbb{Q}$ shows that the only quadratic points on C are $(1, \pm\sqrt{17}, \pm 3)$. \square

Corollary 3.59. *Let K be a quadratic field and let $c \in K$. Suppose that $G(f_c, K)$ contains a graph of type $14(3, 2)$. Then $c = -29/16$ and $K = \mathbb{Q}(\sqrt{17})$.*

Proof. By Lemma 3.57 there is a point $P = (x, y, z) \in C(K)$ with $x(x+1) \neq 0$ such that

$$(3.96) \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}.$$

Since $x \notin \{0, -1\}$, Theorem 3.58 implies that P cannot be a rational point on C and is therefore quadratic. It follows from Theorem 3.58 that $K = \mathbb{Q}(\sqrt{17})$ and $P \in \{(1, \pm\sqrt{17}, \pm 3)\}$. In particular, $x = 1$, so (3.96) yields $c = -29/16$. \square

4. Computation of preperiodic points

We explain in this section the method by which we gathered the data summarized in Appendices B and C. The idea is to systematically choose a collection of number fields of fixed degree, and a list of quadratic polynomials defined over these fields, and then compute the rational preperiodic points for all the chosen polynomials. More precisely, the steps we take for gathering data on preperiodic points over number fields of a fixed degree n are the following:

- (1) Choose a bound D and find all number fields K of degree n whose discriminant satisfies $|\Delta_K| \leq D$.
- (2) Choose a bound B and for each number field K from the previous step, find all elements $c \in K$ such that $H_K(c) \leq B$. Here, H_K denotes the relative height function on K (see §4.2 below).
- (3) For each number field K , and for all $c \in K$ from the previous step, determine the set $\text{PrePer}(f_c, K)$.

The list of fields from step (1) is known to be finite (see [28, §III.2]) and can be obtained for small n and D , for instance, from Jones's online database [20]. For step (2) we use the main algorithm discussed in [8] for listing elements of bounded height in a given number field. The method used to carry out step (3) will be developed in §4.1–§4.3 below. Finally, in §4.4 we describe a specific computation done following the above steps in the case of quadratic fields.

Remark. Hutz [17, 18] has designed a suite of algorithms for studying arithmetic dynamics in Sage, including an alternate approach to computing preperiodic points for morphisms of projective space over \mathbb{Q} .

4.1. Filled Julia sets. In this section we include proofs of the theoretical results upon which the algorithms in §4.3 are based. Let K be a number field and let $c \in K$. The properties of the filled Julia sets of the map f_c at places of K can be used to deduce bounds on the heights of preperiodic points for f_c , as well as to create simple tests for eliminating many points $P \in K$ as possible elements of the set $\text{PrePer}(f_c, K)$. In some cases these tests can even show that f_c has no (finite) K -rational preperiodic point at all — see Lemmas 4.7 and 4.8 in §4.3. Further discussion of filled Julia sets, along with proofs of some closely related results, may be found in [4, §6].

Let M_K denote the set of nontrivial places of K , and let M_K^∞ and M_K^0 denote the sets of archimedean (infinite) places and nonArchimedean (finite) places, respectively. For each $v \in M_K^\infty$ there is an embedding $\sigma_v : K \hookrightarrow \mathbb{C}$ such that $|x|_v = |\sigma_v(x)|_{\mathbb{C}}$, where $|\cdot|_{\mathbb{C}}$ is the usual complex absolute value. For each $v \in M_K^0$ there is a maximal ideal \mathfrak{p} in the ring of integers \mathcal{O}_K such that $|x|_v = (N(\mathfrak{p}))^{-\text{ord}_{\mathfrak{p}}(x)/(e(\mathfrak{p})f(\mathfrak{p}))}$, where $N(\mathfrak{p})$, $e(\mathfrak{p})$, and $f(\mathfrak{p})$ are the norm, ramification index, and residue degree of \mathfrak{p} , respectively. When it is clear from the context which place v is being considered, we write the corresponding absolute value simply as $|\cdot|$.

For a place $v \in M_K$, we denote by K_v the completion of K with respect to v , and we denote by \mathbb{C}_v the completion of an algebraic closure of K_v . For $a \in \mathbb{C}_v$ and $r \in \mathbb{R}_{\geq 0}$, we denote by $D(a, r)$ the closed disk (in \mathbb{C}_v) of radius r centered at a . For all subsequent uses of the notation $D(a, r)$, it will be clear which place v is being considered.

For $c \in K_v$, we define the *filled Julia set* of f_c at v to be the set

$$\mathcal{K}_{v,c} := \{x \in \mathbb{C}_v : \{f_c^n(x)\}_{n \geq 0} \text{ is a bounded set in } \mathbb{C}_v\}.$$

The following properties of $\mathcal{K}_{v,c}$ may be deduced immediately from the definition:

- The filled Julia set $\mathcal{K}_{v,c}$ is totally invariant under f_c ; that is, $f_c^{-1}(\mathcal{K}_{v,c}) = \mathcal{K}_{v,c} = f_c(\mathcal{K}_{v,c})$.
- The set $\mathcal{K}_{v,c}$ is invariant under the map $z \mapsto -z$.
- All of the preperiodic points for f_c — with the exception of the fixed point at ∞ — lie in $\mathcal{K}_{v,c}$.

It is this third property which motivates our consideration of filled Julia sets, as it implies that

$$\text{PrePer}(f_c, K) \subseteq \bigcap_{v \in M_K} (\mathcal{K}_{v,c} \cap K).$$

(Equality actually holds; the reverse containment may be proved using the theory of canonical heights.) In particular, we can in many cases show that, for some $v \in M_K$, the v -adic filled Julia set of f_c has an empty intersection with K , in which case we may conclude that f_c has no K -rational preperiodic point.

We collect now a series of results giving precise bounds on filled Julia sets.

Infinite places. Recall that if v is an infinite place of K , there is a corresponding embedding $\sigma_v : K \hookrightarrow \mathbb{C}$ which extends to an embedding $\sigma_v : K_v \hookrightarrow \mathbb{C}$. The image of K_v is either \mathbb{R} or \mathbb{C} , depending on whether σ_v embeds K into \mathbb{R} . For convenience of notation, throughout this section we will denote by $|\cdot|$ the absolute value corresponding to v , given by $|x| = |\sigma_v(x)|_{\mathbb{C}}$, and we identify K_v with its image under σ_v .

Proposition 4.1. *Let v be an infinite place of the number field K , and let $c \in K_v \subseteq \mathbb{C}$. Then*

$$\mathcal{K}_{v,c} \subseteq D\left(0, \frac{1}{2} + \sqrt{\frac{1}{4} + |c|}\right).$$

Proof. Suppose $|x| > \frac{1}{2} + \sqrt{\frac{1}{4} + |c|}$, and choose $\epsilon > 0$ such that

$$|x| > \frac{1}{2} + \sqrt{\frac{1}{4} + |c|} + \epsilon.$$

Then $|x|^2 - |c| > |x| + \epsilon$, so $|f_c(x)| > |x| + \epsilon$. By induction, we have $|f_c^n(x)| > |x| + n\epsilon$, so $|f_c^n(x)| \rightarrow \infty$. Therefore $x \notin \mathcal{K}_{v,c}$. \square

In the case that $K_v = \mathbb{R}$ it may happen that $\mathcal{K}_{v,c}$ does not intersect K_v . More precisely, we have the following trichotomy:

Proposition 4.2. *Let v be a real place of the number field K , and suppose $c \in K_v = \mathbb{R}$.*

- (1) *If $c > \frac{1}{4}$, then $\mathcal{K}_{v,c} \cap \mathbb{R} = \emptyset$.*
- (2) *If $-2 \leq c \leq \frac{1}{4}$, then $\mathcal{K}_{v,c} \cap \mathbb{R} = [-a, a]$, where $a = \frac{1}{2} + \sqrt{\frac{1}{4} - c}$ is the larger of the two real fixed points of f_c .*
- (3) *If $c < -2$, then $-a - c \geq 0$, and*

$$\mathcal{K}_{v,c} \cap \mathbb{R} \subseteq [-a, -\sqrt{-a-c}] \cup [\sqrt{-a-c}, a].$$

Proof. We start with (1). For any $x \in \mathbb{R}$ we have

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

It follows by induction that $f_c^n(x) \geq x + n(c - \frac{1}{4})$, and since $c > \frac{1}{4}$ this grows without bound as $n \rightarrow \infty$.

Next we prove (2). Suppose $|x| > a$. Choosing $\epsilon > 0$ such that $|x| > \frac{1}{2} + \sqrt{\frac{1}{4} - c} + \epsilon$ we see that

$$\begin{aligned} |x| - \frac{1}{2} > \sqrt{\frac{1}{4} - c} + \epsilon &\implies x^2 - |x| + \frac{1}{4} > \frac{1}{4} - c + \epsilon \\ &\implies f_c(x) = x^2 + c > |x| + \epsilon. \end{aligned}$$

By induction it follows that $f_c^n(x) > |x| + n\epsilon$ for all $n \geq 1$, so $|f_c^n(x)| \rightarrow \infty$. Therefore $\mathcal{K}_{v,c} \subseteq [-a, a]$.

Now suppose that $|x| \leq a$. Then

$$(4.1) \quad 0 \leq x^2 \leq a^2 \implies c \leq x^2 + c \leq a^2 + c \implies c \leq f_c(x) \leq f_c(a) = a.$$

We now claim that $-a \leq c$. Indeed,

$$\begin{aligned} (4.2) \quad -2 \leq c \leq \frac{1}{4} &\implies 0 \leq \frac{1}{4} - c \leq \frac{9}{4} \\ &\implies \sqrt{\frac{1}{4} - c} \leq \frac{3}{2} \\ &\implies -1 \leq \frac{1}{2} - \sqrt{\frac{1}{4} - c} = 1 - a \\ &\implies -a \leq a - a^2 = c. \end{aligned}$$

Combining (4.1) and (4.2) shows that if $|x| \leq a$, then $|f_c(x)| \leq a$, and therefore $|f_c^n(x)| \leq a$ for all $n \geq 1$. It follows that $[-a, a] \subseteq \mathcal{K}_{v,c} \cap \mathbb{R}$, which completes the proof of statement (2).

Finally, we prove (3). If $|x| < \sqrt{-a-c}$, then $x^2 < -a-c$, and hence $f_c(x) < -a$. Therefore $|f_c(x)| > a$, and the argument used to prove statement (2) shows that $|f_c(x)| \rightarrow \infty$. \square

Finite places. As in the case of infinite places, for finite places v of K we can bound the filled Julia set $\mathcal{K}_{v,c}$ and in some cases give obstructions to having K_v -rational points in it.

Proposition 4.3. *Let v be a finite place of the number field K , and let $c \in K_v$.*

- (1) *If $|c| \leq 1$, then $\mathcal{K}_{v,c} = D(0,1)$.*
- (2) *If $|c| > 1$, then $\mathcal{K}_{v,c} \subseteq \{x \in \mathbb{C}_v : |x| = |c|^{1/2}\}$.*

Proof. We begin with the proof of (1). If $|x| \leq 1$, then

$$|f_c(x)| = |x^2 + c| \leq \max\{|x|^2, |c|\} \leq 1.$$

On the other hand, if $|x| > 1$, then $|f_c(x)| = |x|^2 > 1$. By induction we have $|f_c^n(x)| = |x|^{2^n}$, so $|f_c^n(x)| \rightarrow \infty$.

For the proof of (2), if $|x| > |c|^{1/2}$, then $|f_c(x)| = |x|^2 > |c| > |c|^{1/2}$. By induction, $|f_c^n(x)| = |x|^{2^n}$, so $|f_c^n(x)| \rightarrow \infty$. If instead we have $|x| < |c|^{1/2}$, then $|f_c(x)| = |c| > |c|^{1/2}$, and we reduce to the previous case to show that $|f_c^n(x)| \rightarrow \infty$. □

Corollary 4.4. *Let v be a finite place of the number field K . Suppose $c \in K_v$ is such that $|c| > 1$ and $|c| \notin |K_v^\times|^2$. Then $\mathcal{K}_{v,c} \cap K_v = \emptyset$.*

If we assume that v is a finite place that lies above an odd prime in \mathbb{Z} , we can improve the statement of Corollary 4.4 by weakening the hypothesis that $|c| \notin |K_v^\times|^2$.

Proposition 4.5. *Let v be a finite place of the number field K corresponding to a maximal ideal $\mathfrak{p} \subset \mathcal{O}_K$ that lies above an odd rational prime. Suppose $c \in K_v$ is such that $|c| > 1$ and $-c$ is not a square in K_v . Then $\mathcal{K}_{v,c} \cap K_v = \emptyset$.*

Proof. Assume for the sake of a contradiction that there exists some $x \in \mathcal{K}_{v,c} \cap K_v$. The invariance of the filled Julia set implies that $f_c(x) \in \mathcal{K}_{v,c}$ as well, so by Proposition 4.3 we have $|x^2 + c| = |c|^{1/2}$, and therefore

$$(4.3) \quad \left| \frac{x^2}{-c} - 1 \right| = \frac{1}{|c|^{1/2}} < 1.$$

Let π be a uniformizer for the valuation ring $R_v \subset K_v$, and write $-c = \pi^r u$, where $r < 0$ is an integer and $u \in R_v^\times$. Similarly, write $x = \pi^s w$, with $s \in \mathbb{Z}$ and $w \in R_v^\times$. Then (4.3) implies that $\pi^{2s-r} \frac{w^2}{u} \in R_v^\times$, so that $r = 2s$. We can therefore rewrite (4.3) as $|w^2 - u| < 1$. Since \mathfrak{p} lies above an odd prime, it follows by Hensel's Lemma that u must be a square in K_v , so $-c = \pi^{2s} u$ is a square as well. □

Remark. The same statement does not necessarily hold for places v lying above 2. For example, suppose $K = \mathbb{Q}$ and $c = -\frac{3}{4}$. Then $-c$ is not a square in \mathbb{Q}_2 , but the map f_c admits $\pm\frac{1}{2}$ as preperiodic points, and therefore the 2-adic filled Julia set of f_c contains \mathbb{Q}_2 -rational points.

4.2. Height bounds on preperiodic points. Continue with the notation from §4.1. The *relative height* function on K is the map $H_K : K \rightarrow \mathbb{R}_{\geq 1}$ defined by

$$H_K(x) = \prod_{v \in M_K} \max\{|x|_v, 1\}^{n_v},$$

where $n_v = [K_v : \mathbb{Q}_v]$ is the local degree of K at the place v .

It is a well-known fact (see [33, §3.1]) that for any bound B , the set $\{x \in K : H_K(x) \leq B\}$ is finite. Fix an element $c \in K$. The standard way of showing that the set $\text{PrePer}(f_c, K)$ is finite is to prove the existence of a constant $B(K, c)$ such that for all points $P \in \text{PrePer}(f_c, K)$, $H_K(P) \leq B(K, c)$. Since any set of points of bounded height is finite, this observation yields a finite search space for determining all preperiodic points for f_c . The standard technique using canonical heights yields the weak bound $B(K, c) = 2^{[K:\mathbb{Q}]} H_K(c)$. (See, e.g., the proofs of Theorems 3.11 and 3.20 in [33].) Our analysis of filled Julia sets in the previous section allows us to improve this bound significantly, and therefore make the search space substantially smaller when the height of c is large.

Theorem 4.6. *Let K be a number field and let $c \in K$. For all points $P \in \text{PrePer}(f_c, K)$ we have*

$$(4.4) \quad H_K(P) \leq \left(\frac{1 + \sqrt{5}}{2} \right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}.$$

Proof. Let P be a preperiodic point for f_c . Then $P \in \mathcal{K}_{v,c}$ for all places v of K . Applying Proposition 4.1 to the infinite places of K yields

$$(4.5) \quad |P|_v \leq \frac{1}{2} + \sqrt{\frac{1}{4} + |c|_v}$$

for all $v \in M_K^\infty$. Similarly, for finite places v we use Proposition 4.3 to obtain

$$(4.6) \quad |P|_v \leq 1 \text{ if } |c|_v \leq 1 \quad \text{and} \quad |P|_v = |c|_v^{1/2} \text{ if } |c|_v > 1$$

for all $v \in M_K^0$. By combining (4.5) and (4.6), we arrive at the following upper bound for $H_K(P)$:

$$\begin{aligned} H_K(P) &= \prod_{v \in M_K} \max\{|P|_v, 1\}^{n_v} \\ &\leq \prod_{v \in M_K^\infty} \left(\frac{1}{2} + \sqrt{\frac{1}{4} + |c|_v} \right)^{n_v} \cdot \prod_{v \in M_K^0} \max\{|c|_v^{1/2}, 1\}^{n_v} \\ &= H_K(c)^{1/2} \prod_{v \in M_K^\infty} \left(\frac{\frac{1}{2} + \sqrt{\frac{1}{4} + |c|_v}}{\max\{|c|_v^{1/2}, 1\}} \right)^{n_v}. \end{aligned}$$

The maximum value of the function

$$y \mapsto \frac{\frac{1}{2} + \sqrt{\frac{1}{4} + y^2}}{\max\{y, 1\}} \quad , \quad y \in [0, \infty)$$

is $\frac{1+\sqrt{5}}{2}$ (attained at $y = 1$). Therefore,

$$H_K(P) \leq H_K(c)^{1/2} \cdot \prod_{v \in M_K^\infty} \left(\frac{1 + \sqrt{5}}{2} \right)^{n_v} = \left(\frac{1 + \sqrt{5}}{2} \right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}. \quad \square$$

4.3. Algorithm for computing preperiodic points. Using results from the previous sections we discuss here a method for computing the set of K -rational preperiodic points for a collection of maps f_c defined over a number field K . We let \mathcal{O}_K denote the ring of integers in K . For convenience in computations we will work with the valuations $v(\cdot) = \text{ord}_{\mathfrak{p}}(\cdot)$ rather than their corresponding nonarchimedean absolute values $|\cdot|_v$.

We begin by combining the statements of Propositions 4.3 and 4.5 and rephrasing them in terms of these valuations on K , using also the fact that preperiodic points belong to every filled Julia set of f_c .

Lemma 4.7. *Let K be a number field and let $P, c \in K$.*

- (1) *If $\text{ord}_{\mathfrak{p}}(P) < 0 \leq \text{ord}_{\mathfrak{p}}(c)$ for some maximal ideal \mathfrak{p} in \mathcal{O}_K , then P is not preperiodic for f_c .*
- (2) *If $\text{ord}_{\mathfrak{p}}(c) < 0$ and $\text{ord}_{\mathfrak{p}}(P) \neq \frac{1}{2} \text{ord}_{\mathfrak{p}}(c)$ for some maximal ideal \mathfrak{p} in \mathcal{O}_K , then P is not preperiodic for f_c . In particular, if $\text{ord}_{\mathfrak{p}}(c)$ is negative and odd for some maximal ideal \mathfrak{p} , then f_c has no finite K -rational preperiodic point.*
- (3) *If there exists a maximal ideal \mathfrak{p} in \mathcal{O}_K , lying above an odd rational prime, such that $\text{ord}_{\mathfrak{p}}(c) < 0$ and $-c$ is not a square in $K_{\mathfrak{p}}$, then f_c has no finite K -rational preperiodic point.*

We also record the dynamical consequences of Propositions 4.1 and 4.2.

Lemma 4.8. *Let K be a number field and let $P, c \in K$.*

- (1) *If $|\sigma(P)| > \frac{1}{2} + \sqrt{\frac{1}{4} + |\sigma(c)|}$ for some $\sigma : K \hookrightarrow \mathbb{C}$, then P is not preperiodic for f_c .*
- (2) *If $\sigma(c) > \frac{1}{4}$ for some $\sigma : K \hookrightarrow \mathbb{R}$, then f_c has no finite K -rational preperiodic point.*
- (3) *Suppose σ is a real embedding such that $\sigma(c) \leq \frac{1}{4}$, and set $a = \frac{1}{2} + \sqrt{\frac{1}{4} - \sigma(c)}$. If $|\sigma(P)| > a$, then P is not preperiodic for f_c .*
- (4) *Suppose σ is a real embedding such that $\sigma(c) < -2$, and set $a = \frac{1}{2} + \sqrt{\frac{1}{4} - \sigma(c)}$. If*

$$\sigma(P) \notin \left[-a, -\sqrt{-a - \sigma(c)} \right] \cup \left[\sqrt{-a - \sigma(c)}, a \right],$$

then P is not preperiodic for f_c .

Remark. In the case $\sigma(c) < -2$, we still have $\sigma(P) \in [-a, a]$ for all preperiodic points P . However, the set $[-a, -\sqrt{-a - \sigma(c)}] \cup [\sqrt{-a - \sigma(c)}, a]$ has length at most 4, making it much smaller than $[-a, a]$ for large values of $|\sigma(c)|$. Therefore, if $c \in K$ satisfies $\sigma(c) < -2$ for some real embedding $\sigma : K \hookrightarrow \mathbb{R}$, Lemma 4.8(4) provides a considerable reduction in our search space for K -rational preperiodic points for f_c .

We now give the details of a procedure for finding all the preperiodic points for a sample space of quadratic polynomials f_c over an arbitrary number field K . To construct this sample space we fix a positive height bound B and set

$$\mathcal{C} := \{c \in K : H_K(c) \leq B\}.$$

We then take our sample space to be $\{f_c : c \in \mathcal{C}\}$.

By Theorem 4.6, any preperiodic point P for a given map f_c satisfies $H_K(P) \leq \left(\frac{1+\sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}$. Therefore, the set

$$\mathcal{P} := \left\{ P \in K : H_K(P) \leq \left(\frac{1+\sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} B^{1/2} \right\}$$

contains all finite preperiodic points for *all* of the maps in our sample space. The sets \mathcal{C} and \mathcal{P} can be computed using the main algorithm in [8]. However, the output of this algorithm is modified in two ways:

- We delete elements $c \in \mathcal{C}$ for which we can check that f_c has no K -rational preperiodic point, by performing the following steps:
 - (1) For each embedding $\sigma : K \hookrightarrow \mathbb{R}$, determine whether $\sigma(c) > \frac{1}{4}$. If this occurs for some σ , then f_c has no preperiodic point (Lemma 4.8(2)), so we remove c from \mathcal{C} .
 - (2) For each maximal ideal \mathfrak{p} such that $\text{ord}_{\mathfrak{p}}(c) < 0$: if $\text{ord}_{\mathfrak{p}}(c)$ is odd, then f_c has no preperiodic point (Lemma 4.7(2)), and c is removed from \mathcal{C} . If $\text{ord}_{\mathfrak{p}}(c)$ is even and \mathfrak{p} lies over an odd prime, determine whether $-c$ is a square in the completion $K_{\mathfrak{p}}$. If it is not, then f_c has no preperiodic point (Lemma 4.7(3)), so we remove c from \mathcal{C} .

The last test can be done by working in the finite field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, where $R_{\mathfrak{p}}$ is the valuation ring of $K_{\mathfrak{p}}$: assuming that \mathfrak{p} is a prime of \mathcal{O}_K lying over an odd rational prime, and that $\text{ord}_{\mathfrak{p}}(c)$ is negative and even, we let π be a uniformizer in $R_{\mathfrak{p}}$, and write $-c = \pi^{2s}u$ for some integer $s < 0$ and some unit $u \in R_{\mathfrak{p}}^{\times}$. Then $-c$ is a square in $K_{\mathfrak{p}}$ if and only if u is a square in $R_{\mathfrak{p}}$, which happens if and only if u is a square modulo $\mathfrak{p}R_{\mathfrak{p}}$, by Hensel's Lemma.

- We reorder the elements of \mathcal{P} by increasing height. For a given map f_c , every K -rational preperiodic point P of f_c satisfies

$$H_K(P) \leq \left(\frac{1 + \sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}.$$

Rather than searching through *every* element $P \in \mathcal{P}$ to determine whether P is preperiodic for f_c , the ordering by height allows us to search through elements of \mathcal{P} until the height bound

$$\left(\frac{1 + \sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}$$

is exceeded, and then stop.

Having modified the sets \mathcal{C} and \mathcal{P} as explained above, we proceed to determine, for every $c \in \mathcal{C}$, the set of K -rational preperiodic points of the map f_c . First of all, we need not consider all points in \mathcal{P} , but only those meeting the height bound of Theorem 4.6. More importantly, Lemmas 4.7 and 4.8 give us a series of simple tests that can be applied to a point P to conclude that it is not preperiodic. By doing this we quickly eliminate from consideration many elements from the list \mathcal{P} , at which point the naive approach of iterating f_c on each element of \mathcal{P} at most $\#\mathcal{P}$ times becomes reasonable. This is, with small adjustments, the method provided in the algorithms below.

Algorithm 1 (Preperiodicity tests).

Input: A number field K , a number $c \in K$, and a point $P \in K$.

Output: The string “NO” or “MAYBE”, depending on whether P failed one of the tests and is therefore not preperiodic, or P passed all of the tests and is therefore potentially preperiodic.

- (1) For each prime ideal \mathfrak{p} such that $\text{ord}_{\mathfrak{p}}(P) < 0$: if $\text{ord}_{\mathfrak{p}}(c) \geq 0$, return “NO” (Lemma 4.7(1)).
- (2) For each prime ideal \mathfrak{p} such that $\text{ord}_{\mathfrak{p}}(c) < 0$: if $\text{ord}_{\mathfrak{p}}(P) \neq \frac{1}{2} \text{ord}_{\mathfrak{p}}(c)$, return “NO” (Lemma 4.7(2)).
- (3) For each embedding $\sigma : K \hookrightarrow \mathbb{C}$: if $|\sigma(P)| > \frac{1}{2} + \sqrt{\frac{1}{4} + |\sigma(c)|}$, return “NO” (Lemma 4.8(1)).
- (4) For each embedding $\sigma : K \hookrightarrow \mathbb{R}$: set $a = \frac{1}{2} + \sqrt{\frac{1}{4} - \sigma(c)}$.
 - (a) If $|\sigma(P)| > a$, return “NO” (Lemma 4.8(3)).
 - (b) If $\sigma(c) < -2$ and $|\sigma(P)| < \sqrt{-a - \sigma(c)}$, return “NO” (Lemma 4.8(4)).
- (5) If it has not yet been determined whether P is preperiodic for f_c , return “MAYBE”.

The next algorithm goes through the list \mathcal{C} and, for each $c \in \mathcal{C}$, uses Algorithm 1 to find points from the list \mathcal{P} that are definitely not preperiodic for f_c . After this, a relatively small number of points remain whose preperiodicity has not been determined. Each of these is then classified by iterating a number of times which is not greater than the size of the list of undetermined points.

Algorithm 2 (Determining all preperiodic points).

Input: A number field K , and lists \mathcal{C} and \mathcal{P} as described above.

Output: A list whose elements are of the form $\{c, \{P_1, \dots, P_m\}\}$ for all $c \in \mathcal{C}$ such that f_c has a K -rational preperiodic point, and $\{P_1, \dots, P_m\} = \text{PrePer}(f_c, K)$

- (1) Create an empty list \mathcal{L} .
- (2) For each $c \in \mathcal{C}$:
 - (a) Create two empty lists, Y and M .
 - (b) For all $P \in \mathcal{P}$ with $H_K(P) \leq \left(\frac{1+\sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}$: apply Algorithm 1 to P and c . If the output is “MAYBE”, append the point P to the list M .
 - (c) While M is nonempty:
 - (i) Let P be the first element of M .
 - (ii) Construct a list $\mathcal{I} = \{P\}$ to contain iterates of P , and set $Q := f_c(P)$.
 - (iii) While preperiodicity of P has not been determined:
 - (A) if $Q \in Y$, then P is preperiodic; append all elements of \mathcal{I} to the list Y and delete them from M .
 - (B) If $Q \in \mathcal{I}$, then P is preperiodic; append all elements of \mathcal{I} to the list Y and delete them from M .
 - (C) If $Q \notin M$, then P is not preperiodic; delete all elements of \mathcal{I} from M .
 - (D) If no action was taken in steps (A) through (C), append Q to \mathcal{I} , and replace Q with $f_c(Q)$.
 - (d) If Y is nonempty, append $\{c, Y\}$ to the list \mathcal{L} .
 - (3) Return \mathcal{L} .

Remark. The while loop in step 2c (iii) will necessarily terminate in at most $\#M$ steps because, for a given $P \in M$ the first $\#M$ iterates (together with P) determine preperiodicity: if P is preperiodic, then either one of these iterates falls in Y (and then the loop terminates in step A), or they all lie in M ; but then at least two of them must be equal (and the loop terminates in step B). Similarly, if P is not preperiodic, then none of these iterates lies in Y , and since they are all distinct, at least one is not in M (hence the loop will terminate in step C).

4.4. Application to quadratic fields. The algorithms developed in the previous section give us a systematic way of computing preperiodic points

for a sample space of quadratic polynomials defined over a given number field. In this section we apply those algorithms in the context of quadratic fields, following — with minor modifications — the steps outlined at the beginning of §4.

For every quadratic field K with discriminant satisfying $|\Delta_K| \leq 327$ (a total of 200 fields) we computed the set $\text{PrePer}(f_c, K)$ for a collection of elements $c \in K$ chosen as follows: a bound B_K was fixed, and using the main algorithm in [8] we computed all elements $c \in K$ satisfying $H_K(c) \leq B_K$. Rather than choosing the same bound B_K for every field K , we varied B_K between 1,000 and 2,200, increasing together with the discriminant of K in order to keep the quantity of c values considered roughly uniform as K varied. In addition we computed, for each field K , the set $\text{PrePer}(f_c, K)$ for every $c \in \mathbb{Q}$ of *relative height* $\leq B'_K$, where B'_K varied between 300^2 and 600^2 .

In total, the set $\text{PrePer}(f_c, K)$ was computed for 256,588 pairs (K, c) ; this count does not include millions of values of c for which it was determined by local methods that f_c has no K -rational preperiodic point (other than the point at infinity). The resulting 256,588 directed graphs were then classified by isomorphism to arrive at a list of 45 graphs. These graphs — and one additional graph — are displayed in Appendix B, and a representative pair (K, f_c) for each graph is given in Appendix C.

There are three items appearing in the appendices which were not found by the computations described above: the graph 10(3,1,1); an example of the graph 10(2) over a real quadratic field; and an example of the graph 8(4) over an imaginary quadratic field. These examples occur over number fields of large enough discriminant, or for polynomials f_c with the height of c large enough, that they are beyond the search range used for our main computation. For more information we refer the reader to the discussion of these graphs in §3.

5. PCF maps and maps with a unique fixed point

In this section we determine all rational and quadratic algebraic numbers c such that the polynomial f_c has one of two properties: either it is postcritically finite, or it has a unique fixed point. Furthermore, for every such number c we show that all possible graphs $G(f_c, K)$, with K a quadratic field, appear in Appendix B. Recall that a rational function $\varphi \in K(z)$ is called *postcritically finite* (or PCF) if all of its critical points are preperiodic for φ . In particular, a polynomial of the form $f(z) = z^2 + c$ is PCF if and only if 0 is preperiodic for $f(z)$.

We will need two preliminary results concerning heights of algebraic numbers. Recall that the *absolute height* function $H : \overline{\mathbb{Q}} \rightarrow \mathbb{R}_{\geq 1}$ is defined by

$$H(\alpha) = H_K(\alpha)^{1/[K:\mathbb{Q}]},$$

where K is any number field containing α . Here H_K is the relative height function on K defined in §4.2. The following result is an immediate consequence of Theorem 4.6.

Lemma 5.1. *Let K be a quadratic number field and let $c \in K$. If $x \in K$ is preperiodic for the map $f(z) = z^2 + c$, then*

$$H(x) \leq \left(\frac{1 + \sqrt{5}}{2} \right) H(c)^{1/2}.$$

Lemma 5.2. *Let $x \in \overline{\mathbb{Q}}$ be a quadratic algebraic integer such that $H(x) \leq B$. Then x satisfies an equation*

$$x^2 + a_1x + a_0 = 0,$$

where a_0, a_1 are integers with $|a_0| \leq B^2$ and $|a_1| \leq 2B^2$.

Proof. Let $K = \mathbb{Q}(x)$. The minimal polynomial of x has the form

$$m(t) = t^2 + a_1t + a_0$$

for some integers a_0, a_1 . Factor $m(t)$ over K as $m(t) = (t - x)(t - y)$. For every place v of K we have

$$|a_0|_v = |x|_v|y|_v \leq \max(1, |x|_v) \cdot \max(1, |y|_v),$$

so

$$\begin{aligned} |a_0|^2 &= H_K(a_0) = \prod_{v|\infty} \max(1, |a_0|_v^{n_v}) \leq \prod_{v|\infty} \max(1, |x|_v^{n_v}) \cdot \max(1, |y|_v^{n_v}) \\ &= H_K(x)H_K(y) \leq B^4 \end{aligned}$$

and therefore $|a_0| \leq B^2$. Similarly, for every place v we have

$$|a_1|_v \leq |x|_v + |y|_v \leq 2 \cdot \max(|x|_v, |y|_v) \leq 2 \cdot \max(1, |x|_v) \cdot \max(1, |y|_v),$$

so

$$\begin{aligned} |a_1|^2 &= H_K(a_1) = \prod_{v|\infty} \max(1, |a_1|_v^{n_v}) \leq \prod_{v|\infty} 2^{n_v} \cdot \max(1, |x|_v^{n_v}) \cdot \max(1, |y|_v^{n_v}) \\ &= 2^2 H_K(x)H_K(y), \end{aligned}$$

and therefore $|a_1| \leq 2B^2$. □

5.1. PCF maps. Using the above results, we now determine all rational and quadratic numbers c such that the map f_c is PCF. As a result of our analysis, we will be able to list all pairs (K, c) consisting of a quadratic number field K and an element $c \in K$ for which the graph $G(f_c, K)$ has an odd number of vertices.

Proposition 5.3. *Let $c \in \overline{\mathbb{Q}}$ satisfy $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$, and suppose that the map $f(z) = z^2 + c$ is PCF. Then $c \in \{0, -1, -2, \pm i\}$, where i denotes a square root of -1 . Moreover, for every quadratic field K containing c , the graph $G(f, K)$ is isomorphic to one of the graphs listed in Appendix B.*

Proof. Let K be a quadratic number field containing c . Since 0 is preperiodic for f , then also $c = f(0)$ is preperiodic. Hence, c satisfies an equation $f^m(c) = f^n(c)$ for some $m < n$, so c is integral over \mathbb{Z} . In particular, $|c|_v \leq 1$ for every nonArchimedean place v of K . As 0 is preperiodic and therefore in the filled Julia set $\mathcal{K}_{v,c}$ for each Archimedean place v , we find $|c|_v \leq 2$ (Lemma 4.8(2,4)).

Hence, we have

$$(5.1) \quad H(c) = \left(\prod_{v|\infty} \max\{1, |c|_v\}^{n_v} \right)^{1/2} \leq 2.$$

Moreover, since 0 is preperiodic for $f(z)$, then by Lemma 5.1 we have the following for all $n \geq 0$:

$$(5.2) \quad H(f^n(0)) \leq \left(\frac{1 + \sqrt{5}}{2} \right) H(c)^{1/2} < 2.29.$$

If $c \in \mathbb{Q}$, then (5.1) implies $c \in \{0, \pm 1, \pm 2\}$ and (5.2) with $n = 3$ eliminates $c = 1$ and 2, so $c \in \{0, -1, -2\}$. If c is quadratic, we claim that $c = \pm i$. Using Lemma 5.2 we compute the set S of all quadratic algebraic integers of height at most 2. For every element $c \in S$ we then check whether (5.2) is satisfied for $n = 5$ in order to eliminate values of c . After this process, the only possibilities left for c are $\pm i$; this proves the first part of the proposition.

For the second statement, we begin by computing the full list of rational and quadratic preperiodic points for the map $f(z) = z^2 + c$ for each $c \in \{0, -1, -2, \pm i\}$. Note that, since c is an algebraic integer, every preperiodic point for $f(z)$ must also be an algebraic integer.

Consider first the case $c = i$. Since $c \in K$, we must have $K = \mathbb{Q}(i)$. By Lemma 5.1, every element $x \in \text{PrePer}(f, K)$ must satisfy $H(x) < 1.62$. Writing $x = a + bi$ with $a, b \in \mathbb{Z}$, we then have $a^2 + b^2 < 2.63$, so $a, b \in \{0, \pm 1\}$. This shows that $\text{PrePer}(f, K) \subseteq \{0, \pm 1, \pm i, \pm 1 \pm i\}$. The numbers $0, \pm i, \pm(1 - i)$ are easily seen to be preperiodic; the remaining numbers, namely ± 1 and $\pm(1 + i)$, are not preperiodic because their orbits under f are not contained in the set $\{0, \pm 1, \pm i, \pm 1 \pm i\}$. Therefore, we conclude that

$$\text{PrePer}(z^2 + i, \mathbb{Q}(i)) = \{0, \pm i, \pm(1 - i)\}.$$

One can easily check that the corresponding graph $G(f, K)$ appears in the appendix with the label 5(2)a.

We consider now the values $c = 0, -1, -2$. Let $\text{PrePer}_2(f)$ denote the set of all preperiodic points for f in $\overline{\mathbb{Q}}$ of degree at most 2 over \mathbb{Q} . Since c has very small height, we can quickly compute the set $\text{PrePer}_2(f)$ as follows: first, we use Lemma 5.2 to compute the set S of all algebraic integers x satisfying the height bound in Lemma 5.1, so that $\text{PrePer}_2(f) \subseteq S$. We now iterate each element $s \in S$ until a value in its orbit is repeated, in which case s is preperiodic, or its orbit leaves the set S , in which case it is not

preperiodic. This will require at most $1 + \#S$ iterations of s . The results of these calculations are summarized in the table below. Here, ω denotes a primitive cube root of unity.

c	$x \in \overline{\mathbb{Q}}$ is preperiodic for f and $[\mathbb{Q}(x) : \mathbb{Q}] \leq 2$
0	$0, \pm 1, \pm i, \pm \omega, \pm \omega^2$
-1	$0, \pm 1, \pm \sqrt{2}, \pm \frac{1}{2}(1 + \sqrt{5}), \pm \frac{1}{2}(1 - \sqrt{5})$
-2	$0, \pm 1, \pm 2, \pm \sqrt{2}, \pm \sqrt{3}, \pm \frac{1}{2}(1 + \sqrt{5}), \pm \frac{1}{2}(1 - \sqrt{5})$

For each of the above values of c we can now determine the structure of the graphs $G(f, K)$ as K ranges over all quadratic fields. In every case, we find that the graph is one of those listed in the appendix; the corresponding labels are given below.

For $c = 0$ we obtain

$$G(f_c, K) = \begin{cases} 5(1,1)\text{b} & \text{if } K = \mathbb{Q}(i) \\ 7(2,1,1)\text{a} & \text{if } K = \mathbb{Q}(\omega) \\ 3(1,1) & \text{otherwise.} \end{cases}$$

For $c = -1$:

$$G(f_c, K) = \begin{cases} 5(2)\text{b} & \text{if } K = \mathbb{Q}(\sqrt{2}) \\ 7(2,1,1)\text{b} & \text{if } K = \mathbb{Q}(\sqrt{5}) \\ 3(2) & \text{otherwise.} \end{cases}$$

For $c = -2$:

$$G(f_c, K) = \begin{cases} 7(1,1)\text{a} & \text{if } K = \mathbb{Q}(\sqrt{2}) \\ 7(1,1)\text{b} & \text{if } K = \mathbb{Q}(\sqrt{3}) \\ 9(2,1,1) & \text{if } K = \mathbb{Q}(\sqrt{5}) \\ 5(1,1)\text{a} & \text{otherwise.} \end{cases}$$

This completes the proof of the proposition. \square

Corollary 5.4. *Let K be a quadratic field and let $c \in K$. If the graph $G(f_c, K)$ has an odd number of vertices, then it is isomorphic to one of the graphs listed in Appendix B.*

Proof. Note that an element $x \in K$ is preperiodic for f_c if and only if $-x$ is preperiodic. Hence, the preperiodic points for f_c in K can be grouped into pairs $(x, -x)$. If the number of such points is odd, this means that there is some point x such that $x = -x$; in other words, 0 is preperiodic for f_c . By definition, this means that f_c is PCF, and now the conclusion follows from Proposition 5.3. \square

Remark. Proposition 5.3 and its proof achieve, for graphs G with an odd number of vertices, our main classification goal stated in §3; namely, an explicit description of all pairs (K, c) such that $G(f_c, K) \cong G$.

5.2. Maps with a unique fixed point. Having classified the preperiodic graph structures with an odd number of vertices, we consider now the three graphs in our list that have a unique 1-cycle. The following result will give, for each one of these graphs, a complete list of all pairs (K, c) giving rise to the graph.

Proposition 5.5. *Let K be a quadratic field, and suppose that $c \in K$ is such that the map $f(z) = z^2 + c$ has a unique fixed point in K . Then $G(f, K)$ is one of the graphs listed in Appendix B. More precisely, $c = 1/4$ and:*

$$G(f, K) = \begin{cases} 6(2, 1) & \text{if } K = \mathbb{Q}(i) \\ 4(1) & \text{if } K = \mathbb{Q}(\sqrt{-3}) \\ 2(1) & \text{otherwise.} \end{cases}$$

Proof. If $f(z)$ has a unique fixed point, then the equation $z^2 - z + c = 0$ has exactly one solution, so $c = 1/4$. The set $\text{PrePer}(f, \mathbb{Q})$ is easily seen to be equal to $\{\pm \frac{1}{2}\}$: by Lemma 5.1, any rational preperiodic point for f has height at most 3; this gives a short list of possible preperiodic points, and the preperiodicity of each point is decided within a few iterations. The corresponding graph $G(f, \mathbb{Q})$ is the graph 2(1). We will now determine all the quadratic fields K where f might have preperiodic points that are not rational.

Suppose that $x \in \overline{\mathbb{Q}}$ is a quadratic preperiodic point for f , and let $K = \mathbb{Q}(x)$. It follows from Lemma 4.7 that for every nonArchimedean place v of K we have

$$|x|_v \begin{cases} = 2 & \text{if } v|2 \\ \leq 1 & \text{otherwise.} \end{cases}$$

Hence, $2x$ is an algebraic integer. Since x is preperiodic, Lemma 4.8(1) gives

$$|x|_v \leq \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{1}{4}} < 1.21$$

for each $v \mid \infty$. Hence

$$(5.3) \quad \begin{aligned} H(2x) &= \left(\prod_{v|\infty} \max\{1, |2x|_v\}^{n_v} \right)^{1/2} \\ &\leq \left(\prod_{v|\infty} 2^{n_v} \cdot \max\{1, |x|_v\}^{n_v} \right)^{1/2} < 2.42. \end{aligned}$$

Write $m(t) = t^2 + a_1t + a_0$ for the minimal polynomial of $2x$, where $a_0, a_1 \in \mathbb{Z}$. Applying Lemma 5.2 with the bound in (5.3), we find that

$$|a_1| \leq 2(2.42)^2 < 11.7 \quad \text{and} \quad |a_0| \leq (2.42)^2 < 5.9.$$

Since all iterates of x under f are preperiodic, we have $H(f^n(x)) < 3.24$ for all n (Lemma 5.1). Using Sage we consider all quadratic numbers x

satisfying these properties (with $n \leq 3$), and find that the only possibilities have $a_1 = 0, a_0 = 3$ and $a_1 = \pm 2, a_0 = 5$. This leads to the preperiodic points

$$\pm \frac{\sqrt{-3}}{2}, \pm \frac{1}{2} \pm i,$$

and the result now follows easily. \square

Appendix A. Proof of Lemma 3.5

Let $H : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 1}$ be the standard multiplicative height function on \mathbb{Q} given by $H(a/b) = \max\{|a|, |b|\}$ if a and b are coprime integers. Given real numbers $\alpha < \beta$, define a counting function on $\mathbb{R}_{\geq 1}$ by

$$N(T; \alpha, \beta) = \#\{r \in \mathbb{Q}^* : \alpha \leq r \leq \beta \text{ and } H(r) \leq T\}.$$

To prove Lemma 3.5 we will need the following asymptotic estimate for $N(T; \alpha, \beta)$.

Proposition A.1. *There is a constant $c = c(\alpha, \beta)$ such that*

$$N(T; \alpha, \beta) \sim cT^2.$$

Proof. We begin by making a series of reductions. The relation $H(r) = H(-r)$ for $r \in \mathbb{Q}$ implies that

$$N(T; \alpha, \beta) = \begin{cases} N(T; -\beta, -\alpha) & \text{if } \alpha < \beta \leq 0 \\ N(T; 0, -\alpha) + N(T; 0, \beta) & \text{if } \alpha < 0 < \beta. \end{cases}$$

This shows that in order to prove the result it suffices to consider the case $0 \leq \alpha$. Making this assumption, the relation $H(r) = H(1/r)$ for $r \in \mathbb{Q}^*$ implies that

$$N(T; \alpha, \beta) = \begin{cases} N(T; \beta^{-1}, \alpha^{-1}) & \text{if } 1 < \alpha < \beta \\ N(T; \alpha, 1) + N(T; \beta^{-1}, 1) & \text{if } \alpha \leq 1 < \beta. \end{cases}$$

Therefore, it suffices to prove the result when $0 \leq \alpha < \beta \leq 1$. Finally, making this assumption we have $N(T; \alpha, \beta) = N(T; 0, \beta)$ if $\alpha = 0$, and otherwise $N(T; \alpha, \beta) = N(T; 0, \beta) - N(T; 0, \alpha) + \varepsilon$, where $\varepsilon \in \{0, 1\}$; hence, it suffices to prove that for any real number $\eta \in (0, 1]$ there is a constant $c = c(\eta)$ such that $N(T; 0, \eta) \sim cT^2$. The following estimate will be needed to prove this.

Lemma A.2. *Let $\eta \in (0, 1]$ be a real number, and define a function $S : [1, \infty) \rightarrow \mathbb{Z}_{\geq 0}$ by*

$$S(X) = \#\{(x, y) \in \mathbb{Z}^2 : 1 \leq y \leq X \text{ and } 1 \leq x \leq \eta y\}.$$

Then, setting $g(X) = \eta X(X + 1)/2 - S(X)$, we have $0 \leq g(X) < 2X$ for every $X \geq 1$.

Proof. Note that

$$(A.1) \quad S(X) = \sum_{1 \leq y \leq X} \#\{x \in \mathbb{Z} : 1 \leq x \leq \eta y\} = \sum_{1 \leq y \leq X} \lfloor \eta y \rfloor.$$

Applying the trivial bound $\lfloor \eta y \rfloor \leq \eta y$ we obtain $S(X) \leq \eta X(X + 1)/2$, and the inequality $g(X) \geq 0$ follows immediately. To show that $g(X) < 2X$, write $\eta y = \lfloor \eta y \rfloor + \{\eta y\}$ with $0 \leq \{\eta y\} < 1$. Then (A.1) yields

$$\begin{aligned} S(X) &= \sum_{1 \leq y \leq X} \eta y - \sum_{1 \leq y \leq X} \{\eta y\} > \eta \cdot \sum_{1 \leq y \leq X} y - \sum_{1 \leq y \leq X} 1 \\ &= \eta \lfloor X \rfloor (\lfloor X \rfloor + 1)/2 - \lfloor X \rfloor. \end{aligned}$$

Using the inequalities $X - 1 < \lfloor X \rfloor \leq X$ and $\eta \leq 1$ we have

$$\begin{aligned} \eta \lfloor X \rfloor (\lfloor X \rfloor + 1)/2 - \lfloor X \rfloor &> \eta(X - 1)X/2 - X \\ &= \eta X(X + 1)/2 - \eta X - X \\ &\geq \eta X(X + 1)/2 - 2X. \end{aligned}$$

Therefore, $S(X) > \eta X(X + 1)/2 - 2X$, and hence $g(X) < 2X$. □

Fix a real number $\eta \in (0, 1]$. In order to complete the proof of the proposition we need to show that $N(T; 0, \eta) \sim cT^2$ for some constant c depending only on η . For any real number $T \geq 1$ we have

$$\begin{aligned} N(T; 0, \eta) &= \#\{r \in \mathbb{Q} : 0 < r \leq \eta \text{ and } H(r) \leq T\} \\ &= \#\{(x, y) \in \mathbb{N}^2 : \gcd(x, y) = 1, y \leq T, x \leq \eta y\} \\ &= \sum_{1 \leq y \leq T} \#\{x \in \mathbb{N} : \gcd(x, y) = 1, x \leq \eta y\}. \end{aligned}$$

We recall the following facts concerning the Möbius function μ (see [14, Thms. 263, 287]).

$$(A.2) \quad \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases} \quad \text{and} \quad \frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \quad s > 1.$$

Here, ζ denotes the Riemann zeta function. Using the first property of μ we can now write

$$\begin{aligned} N(T; 0, \eta) &= \sum_{y \leq T} \sum_{x \leq \eta y} \sum_{d | \gcd(x, y)} \mu(d) \\ &= \sum_{1 \leq d \leq T} \mu(d) \cdot \#\{(x, y) \in \mathbb{N}^2 : d|x, d|y, y \leq T, x \leq \eta y\} \\ &= \sum_{1 \leq d \leq T} \mu(d) \cdot \#\{(a, b) \in \mathbb{N}^2 : b \leq T/d, a \leq \eta b\} \\ &= \sum_{1 \leq d \leq T} \mu(d) \cdot S(T/d), \end{aligned}$$

where S is the function defined in Lemma A.2. With the notation used in the lemma, we have

$$\begin{aligned} N(T; 0, \eta) &= \sum_{1 \leq d \leq T} \mu(d) \cdot (\eta(T/d)(1 + T/d)/2 - g(T/d)) \\ &= (\eta T^2/2) \cdot \sum_{1 \leq d \leq T} \frac{\mu(d)}{d^2} + (\eta T/2) \cdot \sum_{1 \leq d \leq T} \frac{\mu(d)}{d} \\ &\quad - \sum_{1 \leq d \leq T} \mu(d) \cdot g(T/d). \end{aligned}$$

Let $P(T) = \sum_{1 \leq d \leq T} \mu(d)/d^2$, so that by (A.2), $P(T) \rightarrow 1/\zeta(2)$ as $T \rightarrow \infty$. We have

$$\begin{aligned} \text{(A.3)} \quad & \frac{2 \cdot \zeta(2) \cdot N(T; 0, \eta)}{\eta T^2} \\ &= \zeta(2) \cdot P(T) \cdot \left(1 + \frac{\sum_{1 \leq d \leq T} \frac{\mu(d)}{d}}{T \cdot P(T)} - \frac{2 \cdot \sum_{1 \leq d \leq T} \mu(d)g(T/d)}{\eta T^2 \cdot P(T)} \right). \end{aligned}$$

The bounds $0 \leq g(T/d) < 2T/d$ proved in Lemma A.2 imply that

$$\left| \sum_{1 \leq d \leq T} \mu(d)g(T/d) \right| \leq 2T \cdot \sum_{1 \leq d \leq T} \frac{1}{d} < 2T(\log T + 1).$$

Hence,

$$\lim_{T \rightarrow \infty} \frac{\sum_{1 \leq d \leq T} \mu(d)g(T/d)}{T^2} = 0.$$

Using the fact that $\sum_{d=1}^{\infty} \mu(d)/d = 0$ we see that the right-hand side of (A.3) converges to 1. Therefore,

$$N(T; 0, \eta) \sim \left(\frac{\eta}{2 \cdot \zeta(2)} \right) \cdot T^2,$$

and this completes the proof of the proposition. \square

The final ingredient needed in the proof of Lemma 3.5 is the following special case of [16, Thm. B.6.1].

Theorem A.3. *Let X/\mathbb{Q} be a curve of genus $g > 0$ with $X(\mathbb{Q}) \neq \emptyset$. Let H_X be a multiplicative Weil height on $X(\overline{\mathbb{Q}})$ and define a counting function on $X(\mathbb{Q})$ by*

$$N(X(\mathbb{Q}), T) = \#\{P \in X(\mathbb{Q}) : H_X(P) \leq T\}.$$

Then there are constants a and b such that

$$N(X(\mathbb{Q}), T) \sim \begin{cases} a(\log T)^b & \text{if } g = 1 \text{ (} a > 0, b \geq 0 \text{)} \\ a & \text{if } g \geq 2. \end{cases}$$

Recall the statement of Lemma 3.5: Let $p(x) \in \mathbb{Q}[x]$ have nonzero discriminant and degree ≥ 3 . For every rational number r , define a field K_r by

$$K_r := \mathbb{Q} \left(\sqrt{p(r)} \right).$$

Then, for every interval $I \subset \mathbb{R}$ of positive length, the set

$$\Sigma(I, p) = \{K_r : r \in \mathbb{Q} \cap I\}$$

contains infinitely many quadratic fields.

Proof of Lemma 3.5. Let C be the hyperelliptic curve defined by the equation $y^2 = p(x)$. If d is a squarefree integer, we denote by C_d the quadratic twist of C by d , i.e., the curve defined by $dy^2 = p(x)$. Note that in order to prove the lemma it suffices to consider finite closed intervals I ; hence, we fix an interval $I = [\alpha, \beta]$.

Let d_1, \dots, d_n be squarefree integers, and define $d_0 = 1$. We will show that $\Sigma(I, p)$ must contain a field different from $\mathbb{Q}(\sqrt{d_i})$ for every i , which will prove the lemma. For $T \in \mathbb{R}_{\geq 1}$ define

$$\mathcal{N}(T) = \#\{r \in \mathbb{Q} \cap I : H(r) \leq T \text{ and } K_r = \mathbb{Q}(\sqrt{d_i}) \text{ for some } i\}.$$

For any fixed $d \in \{d_0, \dots, d_n\}$, we define a height function on the curve $X = C_d$ by $H_X(x, y) = H(x)$; this is the naive Weil height on C_d . It follows from Theorem A.3 that (in particular)

$$(A.4) \quad \sum_{d=0}^n N(C_d(\mathbb{Q}), T) \ll T \quad (T \rightarrow \infty).$$

Note that if $r \in \mathbb{Q} \cap I$ is such that the field K_r is equal to $\mathbb{Q}(\sqrt{d})$, then there is a rational number s such that $(r, s) \in C_d(\mathbb{Q})$. Thus, for every real number T ,

$$\#\{r \in \mathbb{Q} \cap I : H(r) \leq T \text{ and } K_r = \mathbb{Q}(\sqrt{d})\} \leq N(C_d(\mathbb{Q}), T).$$

Therefore, by (A.4) we have $\mathcal{N}(T) \ll T$. Now, by Proposition A.1 we know that

$$\#\{r \in \mathbb{Q} \cap I : H(r) \leq T\} \sim cT^2$$

for some constant c depending on α and β . Hence,

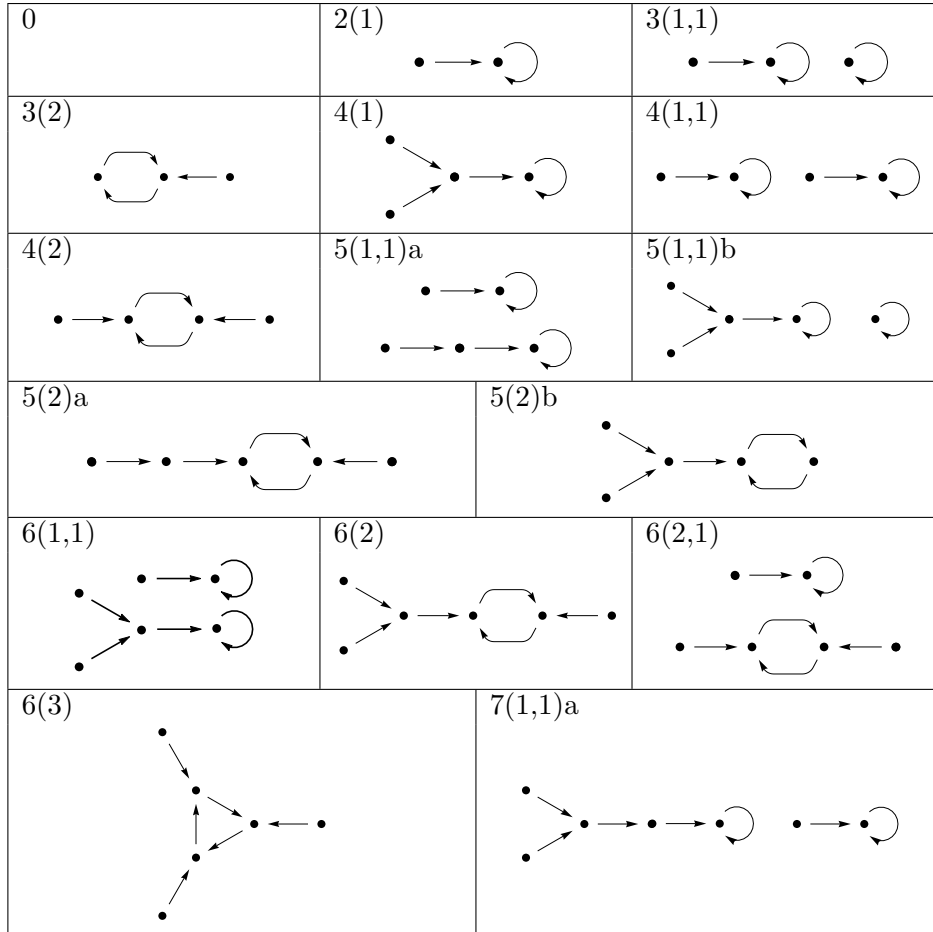
$$\mathcal{N}(T) < \#\{r \in \mathbb{Q} \cap I : H(r) \leq T\} \text{ for } T \gg 0.$$

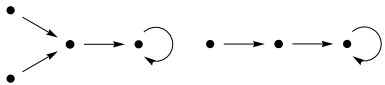
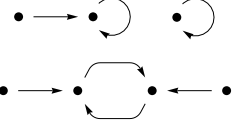
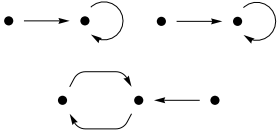
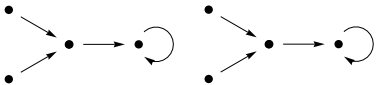
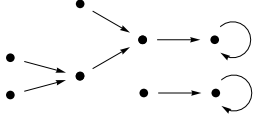
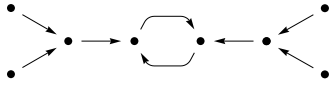
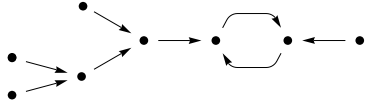
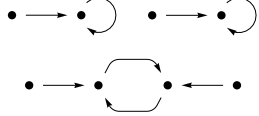
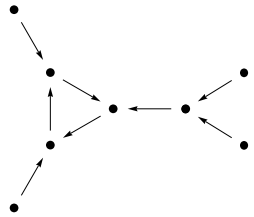
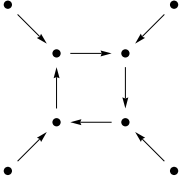
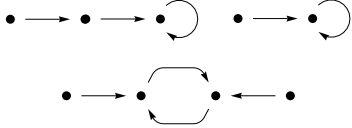
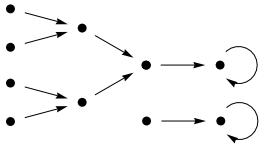
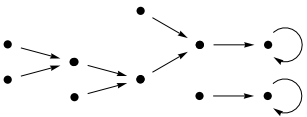
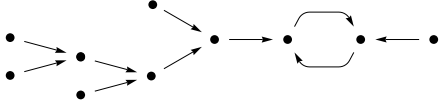
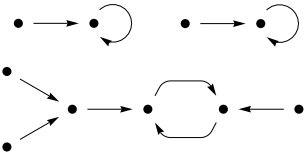
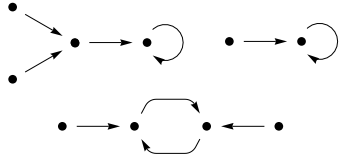
By choosing T large enough, this shows that there is a rational number $r \in I$ for which the field K_r is different from all the fields $\mathbb{Q}(\sqrt{d_i})$. Hence, as claimed, the set $\Sigma(I, p)$ contains a field different from $\mathbb{Q}(\sqrt{d_i})$ for every i . \square

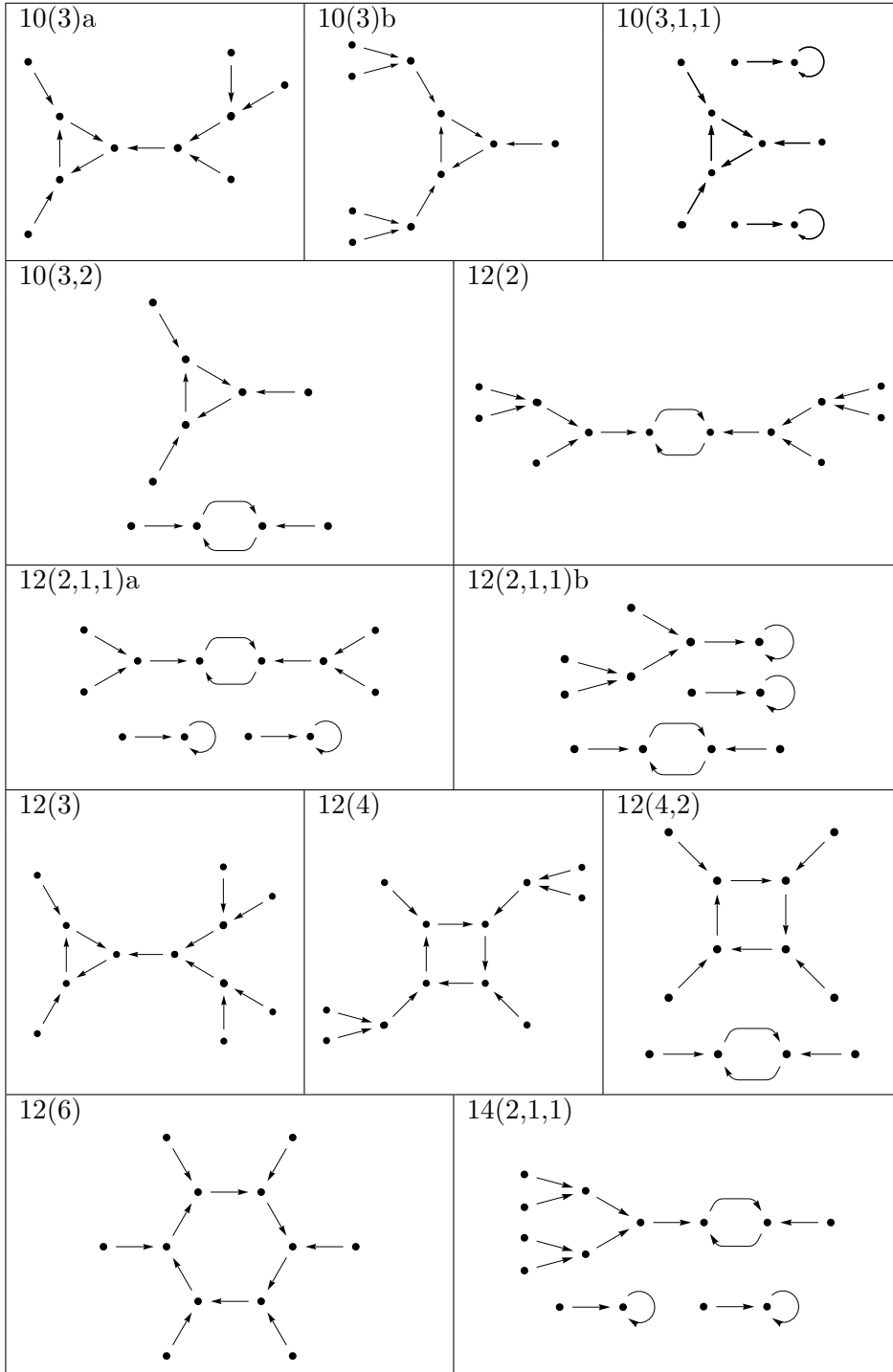
Appendix B. Preperiodic graph structures

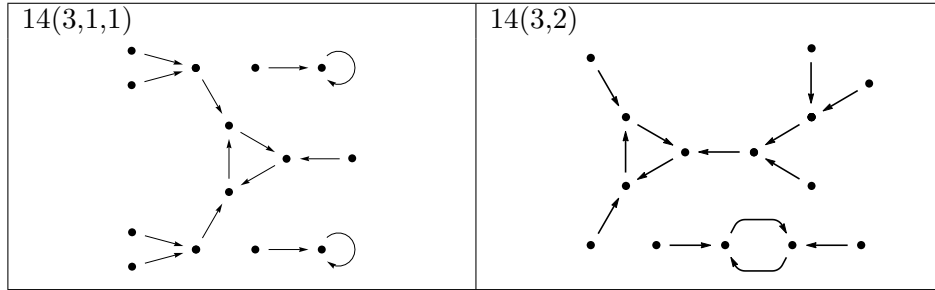
We present 46 graphs representing preperiodic structures discovered via the methods described in §4, applied to the case of quadratic number fields as explained in §4.4. The label of each graph is in the form $N(\ell_1, \ell_2, \dots)$, where N denotes the number of vertices in the graph and ℓ_1, ℓ_2, \dots are the lengths of the directed cycles in the graph in nonincreasing order. If more than one isomorphism class of graphs with this data was observed, we add a lowercase roman letter to distinguish them. For example, the labels $5(1,1)$ and $5(1,1)b$ correspond to the two isomorphism classes of graphs observed that have five vertices and two fixed points. In all figures below we omit the connected component corresponding to the point at infinity.

We remark that all of the graphs from Poonen's paper [31] appear below, with the labels 0 , $2(1)$, $3(1,1)$, $3(2)$, $4(1,1)$, $4(2)$, $5(1,1)a$, $6(1,1)$, $6(2)$, $6(3)$, $8(2,1,1)$, and $8(3)$.



<p>7(1,1)b</p> 	<p>7(2,1,1)a</p> 
<p>7(2,1,1)b</p> 	<p>8(1,1)a</p> 
<p>8(1,1)b</p> 	<p>8(2)a</p> 
<p>8(2)b</p> 	<p>8(2,1,1)</p> 
<p>8(3)</p> 	<p>8(4)</p> 
<p>9(2,1,1)</p> 	<p>10(1,1)a</p> 
<p>10(1,1)b</p> 	<p>10(2)</p> 
<p>10(2,1,1)a</p> 	<p>10(2,1,1)b</p> 





Appendix C. Representative data

We give here a representative set of data for each graph in Appendix B. Each item in the list below includes the following information:

$$K, p(t), c, \text{PrePer}(f_c, K)'$$

Here $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field over which this preperiodic structure was observed; $p(t)$ is a defining polynomial for K with a root $g \in K$; c is an element of K such that the set $\text{PrePer}(f_c, K) \setminus \{\infty\}$, when endowed with the structure of a directed graph, is isomorphic to the given graph; and $\text{PrePer}(f_c, K)'$ is an abbreviated form of the full set of finite K -rational preperiodic points for f_c : since $x \in \text{PrePer}(f_c, K)$ if and only if $-x \in \text{PrePer}(f_c, K)$, we list only one of x and $-x$ in the set $\text{PrePer}(f_c, K)'$. We do not make explicit the correspondence between individual elements of this set and vertices of the graph. If a particular graph was observed over both real and imaginary quadratic fields, we give a representative set of data for each case.

0.

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, 1, \emptyset$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, 2, \emptyset$$

2(1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, \frac{1}{4}, \left\{\frac{1}{2}\right\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, \frac{1}{4}, \left\{\frac{1}{2}\right\}$$

3(1,1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, 0, \{0, 1\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, 0, \{0, 1\}$$

3(2).

$$\mathbb{Q}(\sqrt{3}), t^2 - 3, -1, \{0, 1\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -1, \{0, 1\}$$

4(1).

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, \frac{1}{4}, \left\{ \frac{1}{2}, g - \frac{1}{2} \right\}$$

4(1,1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, \frac{1}{5}, \left\{ \frac{1}{5}g + \frac{2}{5}, \frac{1}{5}g - \frac{3}{5} \right\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, 1, \{g, g - 1\}$$

4(2).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -\frac{4}{5}, \left\{ \frac{1}{5}g + \frac{2}{5}, \frac{1}{5}g - \frac{3}{5} \right\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -\frac{2}{3}, \left\{ \frac{1}{3}g - \frac{2}{3}, \frac{1}{3}g + \frac{1}{3} \right\}$$

5(1,1)a.

$$\mathbb{Q}(\sqrt{13}), t^2 - t - 3, -2, \{0, 2, 1\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -2, \{0, 2, 1\}$$

5(1,1)b.

$$\mathbb{Q}(\sqrt{-1}), t^2 + 1, 0, \{0, 1, g\}$$

5(2)a.

$$\mathbb{Q}(\sqrt{-1}), t^2 + 1, g, \{0, g, g - 1\}$$

5(2)b.

$$\mathbb{Q}(\sqrt{2}), t^2 - 2, -1, \{0, 1, g\}$$

6(1,1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -\frac{3}{4}, \left\{ \frac{1}{2}, g - \frac{1}{2}, \frac{3}{2} \right\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -\frac{3}{4}, \left\{ \frac{1}{2}, \frac{3}{2}, g - \frac{1}{2} \right\}$$

6(2).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -3, \{1, 2, 2g - 1\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -\frac{13}{9}, \left\{ \frac{1}{3}, \frac{4}{3}, \frac{5}{3} \right\}$$

6(2,1).

$$\mathbb{Q}(\sqrt{-1}), t^2 + 1, \frac{1}{4}, \left\{ \frac{1}{2}, g - \frac{1}{2}, g + \frac{1}{2} \right\}$$

6(3).

$$\mathbb{Q}(\sqrt{33}), t^2 - t - 8, -\frac{301}{144}, \left\{ \frac{5}{12}, \frac{19}{12}, \frac{23}{12} \right\}$$

$$\mathbb{Q}(\sqrt{-67}), t^2 - t + 17, -\frac{301}{144}, \left\{ \frac{5}{12}, \frac{19}{12}, \frac{23}{12} \right\}$$

7(1,1)a.

$$\mathbb{Q}(\sqrt{2}), t^2 - 2, -2, \{0, 1, 2, g\}$$

7(1,1)b.

$$\mathbb{Q}(\sqrt{3}), t^2 - 3, -2, \{0, 1, 2, g\}$$

7(2,1,1)a.

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, 0, \{0, 1, g, g - 1\}$$

7(2,1,1)b.

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -1, \{0, 1, g, g - 1\}$$

8(1,1)a.

$$\mathbb{Q}(\sqrt{13}), t^2 - t - 3, -\frac{289}{144}, \left\{\frac{5}{6}g + \frac{1}{12}, \frac{1}{2}g - \frac{13}{12}, \frac{1}{2}g + \frac{7}{12}, \frac{5}{6}g - \frac{11}{12}\right\}$$

$$\mathbb{Q}(\sqrt{-15}), t^2 - t + 4, -\frac{5}{16}, \left\{\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{1}{2}g - \frac{1}{4}\right\}$$

8(1,1)b.

$$\mathbb{Q}(\sqrt{13}), t^2 - t - 3, -\frac{40}{9}, \left\{\frac{4}{3}, \frac{8}{3}, \frac{5}{3}, \frac{4}{3}g - \frac{2}{3}\right\}$$

$$\mathbb{Q}(\sqrt{-2}), t^2 + 2, -\frac{10}{9}, \left\{\frac{2}{3}, \frac{1}{3}g, \frac{4}{3}, \frac{5}{3}\right\}$$

8(2)a.

$$\mathbb{Q}(\sqrt{10}), t^2 - 10, -\frac{13}{9}, \left\{\frac{1}{3}, \frac{1}{3}g, \frac{4}{3}, \frac{5}{3}\right\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -\frac{5}{12}, \left\{\frac{2}{3}g - \frac{5}{6}, \frac{2}{3}g + \frac{1}{6}, \frac{1}{3}g + \frac{5}{6}, \frac{1}{3}g - \frac{7}{6}\right\}$$

8(2)b.

$$\mathbb{Q}(\sqrt{13}), t^2 - t - 3, -\frac{37}{9}, \left\{\frac{4}{3}, \frac{5}{3}, \frac{7}{3}, \frac{4}{3}g - \frac{2}{3}\right\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, -\frac{13}{16}, \left\{\frac{1}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{5}{4}\right\}$$

8(2,1,1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -12, \{3, 3g - 1, 3g - 2, 4\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, \frac{7}{12}, \left\{\frac{2}{3}g + \frac{1}{6}, \frac{2}{3}g - \frac{5}{6}, \frac{4}{3}g - \frac{7}{6}, \frac{4}{3}g - \frac{1}{6}\right\}$$

8(3).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -\frac{29}{16}, \left\{\frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{7}{4}\right\}$$

$$\mathbb{Q}(\sqrt{-3}), t^2 - t + 1, -\frac{29}{16}, \left\{\frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{7}{4}\right\}$$

8(4).

$$\mathbb{Q}(\sqrt{10}), t^2 - 10, -\frac{155}{72}, \left\{\frac{1}{4}g - \frac{1}{6}, \frac{1}{4}g + \frac{1}{6}, \frac{1}{12}g - \frac{3}{2}, \frac{1}{12}g + \frac{3}{2}\right\}$$

$$\mathbb{Q}(\sqrt{-455}), t^2 - t + 114, \frac{199}{720}, \left\{\frac{1}{10}g + \frac{17}{60}, \frac{1}{15}g - \frac{47}{60}, \frac{1}{10}g - \frac{23}{60}, \frac{1}{15}g + \frac{43}{60}\right\}$$

9(2,1,1).

$$\mathbb{Q}(\sqrt{5}), t^2 - t - 1, -2, \{0, 1, 2, g, g - 1\}$$

10(1,1)a.

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, \frac{3}{16}, \left\{ \frac{1}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{3}{4} \right\}$$

10(1,1)b.

$$\mathbb{Q}(\sqrt{17}), t^2 - t - 4, -\frac{1}{2}g - \frac{13}{16}, \left\{ \frac{1}{4}, \frac{1}{2}g + \frac{3}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g + \frac{1}{4} \right\}$$

10(2).

$$\mathbb{Q}(\sqrt{73}), t^2 - t - 18, \frac{1}{9}g - \frac{205}{144}, \left\{ \frac{1}{6}g + \frac{1}{12}, \frac{1}{6}g - \frac{11}{12}, \frac{1}{6}g + \frac{7}{12}, \frac{1}{3}g - \frac{7}{12}, \frac{1}{3}g - \frac{1}{12} \right\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, -\frac{1}{2}g - \frac{5}{16}, \left\{ \frac{1}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{3}{4}, \frac{1}{2}g + \frac{3}{4} \right\}$$

10(2,1,1)a.

$$\mathbb{Q}(\sqrt{17}), t^2 - t - 4, -\frac{273}{64}, \left\{ \frac{11}{8}, \frac{13}{8}, \frac{19}{8}, \frac{5}{4}g - \frac{5}{8}, \frac{21}{8} \right\}$$

$$\mathbb{Q}(\sqrt{-1}), t^2 + 1, \frac{3}{8}g - \frac{1}{4}, \left\{ \frac{3}{4}g + \frac{1}{4}, \frac{3}{4}g - \frac{3}{4}, \frac{1}{4}g - \frac{1}{4}, \frac{1}{4}g + \frac{3}{4}, \frac{1}{4}g - \frac{5}{4} \right\}$$

10(2,1,1)b.

$$\mathbb{Q}(\sqrt{13}), t^2 - t - 3, -\frac{10}{9}, \left\{ \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{1}{3}g - \frac{2}{3}, \frac{1}{3}g + \frac{1}{3} \right\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, -\frac{21}{16}, \left\{ \frac{1}{4}, \frac{7}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{3}{4}, \frac{5}{4} \right\}$$

10(3)a.

$$\mathbb{Q}(\sqrt{41}), t^2 - t - 10, -\frac{29}{16}, \left\{ \frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{7}{4} \right\}$$

10(3)b.

$$\mathbb{Q}(\sqrt{57}), t^2 - t - 14, -\frac{29}{16}, \left\{ \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{2}g - \frac{1}{4} \right\}$$

10(3,1,1)

$$\mathbb{Q}(\sqrt{337}), t^2 - t - 84, -\frac{301}{144}, \left\{ \frac{5}{12}, \frac{19}{12}, \frac{23}{12}, \frac{1}{6}g + \frac{5}{12}, \frac{1}{6}g - \frac{7}{12} \right\}$$

10(3,2).

$$\mathbb{Q}(\sqrt{193}), t^2 - t - 48, -\frac{301}{144}, \left\{ \frac{5}{12}, \frac{19}{12}, \frac{23}{12}, \frac{1}{6}g + \frac{5}{12}, \frac{1}{6}g - \frac{7}{12} \right\}$$

12(2).

$$\mathbb{Q}(\sqrt{2}), t^2 - 2, -\frac{15}{8}, \left\{ \frac{3}{4}g + \frac{1}{2}, \frac{3}{4}g - \frac{1}{2}, \frac{1}{4}g + \frac{1}{2}, \frac{1}{4}g - \frac{3}{2}, \frac{1}{4}g - \frac{1}{2}, \frac{1}{4}g + \frac{3}{2} \right\}$$

12(2,1,1)a.

$$\mathbb{Q}(\sqrt{17}), t^2 - t - 4, -\frac{13}{16}, \left\{ \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g - \frac{1}{4} \right\}$$

12(2,1,1)b.

$$\mathbb{Q}(\sqrt{33}), t^2 - t - 8, -\frac{45}{16}, \left\{ \frac{3}{4}, \frac{9}{4}, \frac{5}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{1}{4} \right\}$$

$$\mathbb{Q}(\sqrt{-7}), t^2 - t + 2, -\frac{5}{16}, \left\{ \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g - \frac{1}{4} \right\}$$

12(3).

$$\mathbb{Q}(\sqrt{73}), t^2 - t - 18, -\frac{301}{144}, \left\{ \frac{1}{6}g - \frac{1}{12}, \frac{5}{12}, \frac{19}{12}, \frac{1}{3}g + \frac{1}{12}, \frac{1}{3}g - \frac{5}{12}, \frac{23}{12} \right\}$$

12(4).

$$\mathbb{Q}(\sqrt{105}), t^2 - t - 26, -\frac{95}{48}, \left\{ \frac{1}{6}g - \frac{13}{12}, \frac{1}{6}g + \frac{11}{12}, \frac{1}{3}g - \frac{5}{12}, \frac{1}{6}g + \frac{5}{12}, \frac{1}{6}g - \frac{7}{12}, \frac{1}{3}g + \frac{1}{12} \right\}$$

12(4,2).

$$\mathbb{Q}(\sqrt{-15}), t^2 - t + 4, -\frac{31}{48}, \left\{ \frac{1}{3}g + \frac{1}{12}, \frac{1}{6}g - \frac{13}{12}, \frac{1}{3}g - \frac{5}{12}, \frac{1}{6}g + \frac{5}{12}, \frac{1}{6}g - \frac{7}{12}, \frac{1}{6}g + \frac{11}{12} \right\}$$

12(6).

$$\mathbb{Q}(\sqrt{33}), t^2 - t - 8, -\frac{71}{48}, \left\{ \frac{1}{6}g - \frac{13}{12}, \frac{1}{6}g - \frac{7}{12}, \frac{1}{3}g - \frac{5}{12}, \frac{1}{6}g + \frac{5}{12}, \frac{1}{3}g + \frac{1}{12}, \frac{1}{6}g + \frac{11}{12} \right\}$$

14(2,1,1).

$$\mathbb{Q}(\sqrt{17}), t^2 - t - 4, -\frac{21}{16}, \left\{ \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g + \frac{1}{4} \right\}$$

14(3,1,1).

$$\mathbb{Q}(\sqrt{33}), t^2 - t - 8, -\frac{29}{16}, \left\{ \frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{7}{4} \right\}$$

14(3,2).

$$\mathbb{Q}(\sqrt{17}), t^2 - t - 4, -\frac{29}{16}, \left\{ \frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{7}{4} \right\}$$

References

- [1] BENEDETTO, ROBERT L.; DICKMAN, BENJAMIN; JOSEPH, SASHA; KRAUSE, BENJAMIN; RUBIN, DANIEL; ZHOU, XINWEN. Computing points of small height for cubic polynomials. *Involve* **2** (2009), no. 1, 37–64. MR2501344 (2010m:11081), Zbl 1194.37187, doi:10.2140/involve.2009.2.37.
- [2] BOSMA, WIEB; CANNON, JOHN; PLAYOUST, CATHERINE. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265. MR1484478, Zbl 0898.68039, doi:10.1006/jsc.1996.0125.
- [3] BRUIN, NILS; STOLL, MICHAEL. The Mordell–Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.* **13** (2010), 272–306. MR2685127 (2011j:11118), Zbl 1278.11069, arXiv:0906.1934, doi:10.1112/S1461157009000187.
- [4] CALL, GREGORY S.; GOLDSTINE, SUSAN W. Canonical heights on projective space. *J. Number Theory* **63** (1997), no. 2, 211–243. MR1443758 (98c:11060), Zbl 0895.14006, doi:10.1006/jnth.1997.2099.
- [5] CLARK, PETE L. There are genus one curves of every index over every number field. *J. Reine Angew. Math.* **594** (2006), 201–206. MR2248157 (2007b:11080), Zbl 1097.14024, arXiv:math/0411413, doi:10.1515/CRELLE.2006.040.
- [6] COLEMAN, ROBERT F. Effective Chabauty. *Duke Math. J.* **52** (1985), no. 3, 765–770. MR0808103 (87f:11043), Zbl 0588.14015, doi:10.1215/S0012-7094-85-05240-8.
- [7] CREMONA, J. E. Algorithms for modular elliptic curves. Second edition. *Cambridge University Press, Cambridge*, 1997. vi+376 pp. ISBN: 0-521-59820-6. MR1628193 (99e:11068), Zbl 0872.14041.
- [8] DOYLE, JOHN R.; KRUMM, DAVID. Computing algebraic numbers of bounded height. To appear in *Math. Comp.*, 2013. arXiv:1111.4963.
- [9] FABER, XANDER. Benedetto’s trick and existence of rational preperiodic structures for quadratic polynomials. To appear in *Proc. Amer. Math. Soc.*, 2013. arXiv:1305.0216.

- [10] FALTINGS, GERD. The general case of S. Lang's conjecture. *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, 175–182, *Perspect. Math.*, 15. Academic Press, San Diego, CA, 1994. MR1307396 (95m:11061), Zbl 0823.14009.
- [11] FLYNN, E. V.; POONEN, BJORN; SCHAEFER, EDWARD F. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.* **90** (1997), no. 3, 435–463. MR1480542 (98j:11048), Zbl 0958.11024, arXiv:math/9508211, doi: 10.1215/S0012-7094-97-09011-6.
- [12] FLYNN, E. V.; SMART, N. P. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.* **79** (1997), no. 4, 333–352. MR1450916 (98f:11066), Zbl 0895.11026.
- [13] FRIED, MICHAEL D.; JARDEN, MOSHE. Field arithmetic. Third edition. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2008. xxiv+792 pp. ISBN: 978-3-540-77269-9. MR2445111 (2009j:12007), Zbl 0625.12001, doi: 10.1007/b138352.
- [14] HARDY, G. H.; WRIGHT, E. M. An introduction to the theory of numbers. Sixth edition. Oxford University Press, Oxford, 2008. xxii+621 pp. ISBN: 978-0-19-921986-5. MR2445243 (2009i:11001), Zbl 1159.11001.
- [15] HARRIS, JOE; SILVERMAN, JOE. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.* **112** (1991), no. 2, 347–356. MR1055774 (91i:11067), Zbl 0727.11023, doi: 10.1090/S0002-9939-1991-1055774-0.
- [16] HINDRY, MARC; SILVERMAN, JOSEPH H. *Diophantine geometry*. An introduction. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1. MR1745599 (2001e:11058), Zbl 0948.11023.
- [17] HUTZ, BENJAMIN. Arithmetic and complex dynamics. <http://wiki.sagemath.org/dynamics/ArithmeticAndComplex>.
- [18] HUTZ, BENJAMIN. Determination of all rational preperiodic points for morphisms of \mathbb{P}^n . To appear in *Math. Comp.*, 2013. arXiv:1210.6246, doi: 10.1090/S0025-5718-2014-02850-0.
- [19] HUTZ, BENJAMIN; INGRAM, PATRICK. On Poonen's conjecture concerning rational preperiodic points of quadratic maps. *Rocky Mountain J. Math.* **43** (2013), no. 1, 193–204. MR3065461, Zbl 06170758, arXiv:0909.5050, doi: 10.1216/RMJ-2013-43-1-193.
- [20] JONES, J. Number fields. <http://hobbes.la.asu.edu/NFDB/>.
- [21] KENKU, M. A. Certain torsion points on elliptic curves defined over quadratic fields. *J. London Math. Soc.* (2) **19** (1979), no. 2, 233–240. MR0533321 (80g:14035), Zbl 0431.14007, doi: 10.1112/jlms/s2-19.2.233.
- [22] KUBERT, DANIEL SION. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc.* (3) **33** (1976), no. 2, 193–237. MR0434947 (55 #7910), Zbl 0331.14010.
- [23] LORENZINI, DINO; TUCKER, THOMAS J. Thue equations and the method of Chabauty–Coleman. *Invent. Math.* **148** (2002), no. 1, 47–77. MR1892843 (2003d:11088), Zbl 1048.11023, arXiv:math/0005186, doi: 10.1007/s002220100186.
- [24] MAZUR, B.; TATE, J. Points of order 13 on elliptic curves. *Invent. Math.* **22** (1973/74), 41–49. MR0347826 (50 #327), Zbl 0268.14009, doi: 10.1007/BF01425572.
- [25] MILNE, J. S. Jacobian varieties. *Arithmetic geometry (Storrs, Conn., 1984)*, 167–212. Springer, New York, 1986. MR0861976, Zbl 0604.14018, doi: 10.1007/978-1-4613-8655-1.7.
- [26] MORTON, PATRICK. Arithmetic properties of periodic points of quadratic maps. II. *Acta Arith.* **87** (1998), no. 2, 89–102. MR1665198 (2000c:11103), Zbl 1029.12002.
- [27] MORTON, PATRICK; SILVERMAN, JOSEPH H. Rational periodic points of rational functions. *Internat. Math. Res. Notices* **1994**, no. 2, 97–110. MR1264933 (95b:11066), Zbl 0819.11045, doi: 10.1155/S1073792894000127.

- [28] NEUKIRCH, JÜRGEN. Algebraic number theory. Grundlehren der Mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999. xviii+571 pp. ISBN: 3-540-65399-6. MR1697859 (2000m:11104), Zbl 0956.11021, doi: 10.1007/978-3-662-03983-0.
- [29] NORTHCOTT, D. G. Periodic points on an algebraic variety. *Ann. of Math.* (2) **51** (1950), 167–177. MR0034607 (11,615c), Zbl 0036.30102.
- [30] OGG, A. P. Rational points on certain elliptic modular curves. *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, 221–231. Amer. Math. Soc., Providence, RI, 1973. MR0337974 (49 #2743), Zbl 0273.14008, doi: 10.1090/pspum/024.
- [31] Poonen, Bjorn. The classification of rational preperiodic points of quadratic polynomials over \mathbb{Q} : a refined conjecture. *Math. Z.* **228** (1998), no. 1, 11–29. MR1617987 (99j:11076), Zbl 0902.11025, arXiv:math/9512217, doi: 10.1007/PL00004405.
- [32] RABARISON, F. PATRICK. Structure de torsion des courbes elliptiques sur les corps quadratiques. *Acta Arith.* **144** (2010), no. 1, 17–52. MR2660554 (2011g:11112), Zbl 1228.11085, doi: 10.4064/aa144-1-3.
- [33] SILVERMAN, JOSEPH H. The arithmetic of dynamical systems. Graduate Texts in Mathematics, 241. Springer, New York, 2007. x+511 pp. ISBN: 978-0-387-69903-5. MR2316407 (2008c:11002), Zbl 1130.37001, doi: 10.1007/978-0-387-69904-2.
- [34] STEIN, WILLIAM ET AL. Sage Mathematics Software (Version 4.8). The Sage Development Team, 2012. <http://www.sagemath.org>.
- [35] STOLL, MICHAEL. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.* **98** (2001), no. 3, 245–277. MR1829626 (2002b:11089), Zbl 0972.11058, doi: 10.4064/aa98-3-4
- [36] STOLL, MICHAEL. On the height constant for curves of genus two. II. *Acta Arith.* **104** (2002), no. 2, 165–182. MR1914251 (2003f:11093), Zbl 1139.11318, doi: 10.4064/aa104-2-6.
- [37] STOLL, MICHAEL. Independence of rational points on twists of a given curve. *Compos. Math.* **142** (2006), no. 5, 1201–1214. MR2264661 (2007m:14025), Zbl 1128.11033, arXiv:math/0603557, doi: 10.1112/S0010437X06002168.
- [38] STOLL, MICHAEL. Rational 6-cycles under iteration of quadratic polynomials. *LMS J. Comput. Math.* **11** (2008), 367–380. MR2465796 (2010b:11067), Zbl 1222.11083, arXiv:0803.2836, doi: 10.1112/S1461157000000644.
- [39] VOJTA, PAUL. A generalization of theorems of Faltings and Thue–Siegel–Roth–Wirsing. *J. Amer. Math. Soc.* **5** (1992), no. 4, 763–804. MR1151542 (94a:11093), Zbl 0778.11037, doi: 10.1090/S0894-0347-1992-1151542-9.
- [40] WALDE, RALPH; RUSSO, PAULA. Rational periodic points of the quadratic function $q_c(x) = x^2 + c$. *Amer. Math. Monthly* **101** (1994), no. 4, 318–331. MR1270956 (95a:11025), Zbl 0804.58036, doi: 10.2307/2975624.
- [41] WASHINGTON, LAWRENCE C. A family of cyclic quartic fields arising from modular curves. *Math. Comp.* **57** (1991), no. 196, 763–775. MR1094964 (92a:11120), Zbl 0743.11058, doi: 10.1090/S0025-5718-1991-1094964-6.

(John R. Doyle) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602
 jdoyle@math.uga.edu

(Xander Faber) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HI 96822
 xander@math.hawaii.edu

(David Krumm) DEPARTMENT OF MATHEMATICS, CLAREMONT MCKENNA COLLEGE, CLAREMONT, CA 91711
 dkrumm@cmc.edu

This paper is available via <http://nyjm.albany.edu/j/2014/20-29.html>.