Some results on the Flynn–Poonen–Schaefer conjecture

Shalom Eliahou and Youssef Fares

Abstract. For $c \in \mathbb{Q}$, consider the quadratic polynomial map $\varphi_c(z) = z^2 - c$. Flynn, Poonen, and Schaefer conjectured in 1997 that no rational cycle of $\varphi_c$ under iteration has length more than 3. Here, we discuss this conjecture using arithmetic and combinatorial means, leading to three main results. First, we show that if $\varphi_c$ admits a rational cycle of length $n \geq 3$, then the denominator of $c$ must be divisible by 16. We then provide an upper bound on the number of periodic rational points of $\varphi_c$ in terms of the number $s$ of distinct prime factors of the denominator of $c$. Finally, we show that the Flynn–Poonen–Schaefer conjecture holds for $\varphi_c$ if $s \leq 2$, i.e., if the denominator of $c$ has at most two distinct prime factors.

1 Introduction

Let $S$ be a set and $\varphi : S \rightarrow S$ a self map. For $z \in S$, the orbit of $z$ under $\varphi$ is the sequence of iterates

$$O_{\varphi}(z) = (\varphi^k(z))_{k \geq 0},$$

where $\varphi^k$ is the $k$th iterate of $\varphi$ and $\varphi^0 = \text{Id}_S$. We say that $z$ is periodic under $\varphi$ if there is an integer $n \geq 1$ such that $\varphi^n(z) = z$, and then the least such $n$ is the period of $z$. In that case, we identify $O_{\varphi}(z)$ with the finite sequence $\mathcal{C} = (z, \varphi(z), \ldots, \varphi^{n-1}(z))$, and we say that $\mathcal{C}$ is a cycle of length $n$. The element $z$ is said to be preperiodic under $\varphi$ if there is an integer $m \geq 1$ such that $\varphi^m(z)$ is periodic. For every rational fraction in $\mathbb{Q}(X)$ of degree $\geq 2$, its set of preperiodic points is finite, this being a particular case of a well-known theorem of Northcott [10]. However, determining the cardinality of this set is very difficult in general, even for a rational polynomial of degree 2. This paper concerns the following particular case. For any $c \in \mathbb{Q}$, denote

$$\varphi_c : \mathbb{Q} \rightarrow \mathbb{Q}, \quad z \mapsto z^2 - c.$$

In fact, it is essentially the general case in degree 2, because every rational quadratic polynomial is equivalent to $\varphi_c$ for some $c \in \mathbb{Q}$, up to rational linear conjugacy. The following conjecture on $\varphi_c$ is due to Flynn, Poonen, and Schaefer [6].

Conjecture 1.1 Let $c \in \mathbb{Q}$. Then, every periodic point of $\varphi_c$ in $\mathbb{Q}$ has period at most 3.
Some results on the Flynn–Poonen–Schaefer conjecture

599

See also [12] for a refined conjecture on the rational preperiodic points of quadratic maps over $\mathbb{Q}$. In contrast with [12] and other papers, here, we do not count the point at $\infty$ as a preperiodic point.

As the following classical example shows, rational points of period 3 do occur for suitable $c \in \mathbb{Q}$.

**Example 1.2** Let $c = 29/16$. Then, the map $\varphi_c$ admits the cycle $C = (-1/4, -7/4, 5/4)$ of length 3.

Actually, there is a one-parameter family of $c \in \mathbb{Q}$ such that $\varphi_c$ admits a rational cycle of length 3. See [15, Theorem 3, p. 322].

While Conjecture 1.1 has already been explored in several papers, it remains widely open at the time of writing. The main positive results concerning it are that periods 4 and 5 are indeed excluded by Morton [7] and by Flynn, Poonen, and Schaefer [6], respectively.

**Theorem 1.3** (Morton) For every $c \in \mathbb{Q}$, there is no periodic point of $\varphi_c$ in $\mathbb{Q}$ of period 4.

**Theorem 1.4** (Flynn, Poonen, and Schaefer) For every $c \in \mathbb{Q}$, there is no periodic point of $\varphi_c$ in $\mathbb{Q}$ of period 5.

No period higher than 5 has been excluded so far for the rational maps $\varphi_c$. However, Stoll [14] showed that the exclusion of period 6 would follow from the validity of the Birch and Swinnerton-Dyer conjecture.

Conjecture 1.1 is often studied using the height and $p$-adic Julia sets. Here, we mainly use arithmetic and combinatorial means. Among our tools, we shall use the above two results and theorems by Pezda [11] and by Zieve [16] on polynomial iteration over the $p$-adic integers. See also [8, 9] for related methods and results.

Conjecture 1.1 is known to hold for $\varphi_c$ if $c \in \mathbb{Z}$, and more generally if the denominator of $c$ is odd, in which case any rational cycle of $\varphi_c$ is of length at most 2 (see [15]). Here, we focus on the case where the denominator of $c$ is even.

Given $c \in \mathbb{Q} \setminus \mathbb{Z}$, let $s$ denote the number of distinct primes dividing the denominator of $c$, including 2. In [3], Call and Goldstine showed that the number of rational preperiodic points of $\varphi_c$ is bounded above by $2^{s+3}$. Hence, the number of rational periodic points of $\varphi_c$ is bounded above by $2^{s+2}$, because $x \in \mathbb{Q} \setminus \{0\}$ is a preperiodic point of $\varphi_c$ if and only if $-x$ is, whereas at most one of $x$ and $-x$ can be periodic. In [2], the author shows that the number of rational preperiodic points of $\varphi_c$ is bounded above by

$$2s + 3 + \log_2(2s + 3) + \log_2(\log_2(2s + 3) - 1) + 2.$$ (1.1)

Hence, again, the number of rational periodic points is bounded above by one half of (1.1). In this paper, we show that the number of rational periodic points of $\varphi_c$ is bounded above by $2^s + 2$. As pointed out by the referees, this new upper bound is only interesting for $s \leq 5$, as the one given by one half of (1.1) is sharper for $s \geq 6$. We also show that Conjecture 1.1 holds for $\varphi_c$ in case $s \leq 2$. 
For convenience, in order to make this paper as self-contained as possible, we provide short proofs of some already known basic results.

1.1 Notation

Given \( c \in \mathbb{Q} \), we denote by \( \varphi_c : \mathbb{Q} \to \mathbb{Q} \) the quadratic map defined by \( \varphi_c(z) = z^2 - c \) for all \( z \in \mathbb{Q} \). Most papers dealing with Conjecture 1.1 rather consider the map \( z \mapsto z^2 + c \). Our present choice allows statements with positive rather than negative values of \( c \).

For instance, with this choice, we show in [5] that if \( \varphi_c \) admits a cycle of length at least 2, then \( c \geq 1 \).

The sets of rational periodic and preperiodic points of \( \varphi_c \) will be denoted by \( \text{Per}(\varphi_c) \) and \( \text{Preper}(\varphi_c) \), respectively:

\[
\text{Per}(\varphi_c) = \{ x \in \mathbb{Q} \mid \varphi_c^n(x) = x \text{ for some } n \in \mathbb{N} \},
\]

\[
\text{Preper}(\varphi_c) = \{ x \in \mathbb{Q} \mid \varphi_c^m(x) \in \text{Per}(\varphi_c) \text{ for some } m \in \mathbb{N} \}.
\]

For a nonzero integer \( d \), we shall denote by \( \text{supp}(d) \) the set of prime numbers \( p \) dividing \( d \). For instance, \( \text{supp}(45) = \{3, 5\} \). If \( x \in \mathbb{Q} \) and \( p \) is a prime number, the \( p \)-adic valuation \( \nu_p(x) \) of \( x \) is the unique \( r \in \mathbb{Z} \cup \{\infty\} \) such that \( x = p^r x_1/x_2 \) with \( x_1, x_2 \in p \mathbb{Z} \) coprime integers. For \( z \in \mathbb{Q} \), its numerator and denominator will be denoted by \( \text{num}(z) \) and \( \text{den}(z) \), respectively. They are the unique coprime integers such that \( \text{den}(z) \geq 1 \) and \( z = \text{num}(z)/\text{den}(z) \).

As usual, the cardinality of a finite set \( E \) will be denoted by \( |E| \).

2 Basic results over \( \mathbb{Q} \)

2.1 Constraints on denominators

The aim of this section is to show that if \( \varphi_c \) has a periodic point of period at least 3, then \( \text{den}(c) \) is divisible by 16. The result below first appeared in [15].

**Proposition 2.1** Let \( c \in \mathbb{Q} \). If \( \text{Per}(\varphi_c) \neq \emptyset \), then \( \text{den}(c) = d^2 \) for some \( d \in \mathbb{N} \), and \( \text{den}(x) = d \) for all \( x \in \text{Preper}(\varphi_c) \).

Consequently, because we are only interested in rational cycles of \( \varphi_c \), here, we shall only consider those \( c \in \mathbb{Q} \) such that \( \text{den}(c) = d^2 \) for some \( d \in \mathbb{N} \). Moreover, we shall frequently consider the set \( \text{num}(\text{Per}(\varphi_c)) \) of numerators of rational periodic points of \( \varphi_c \). Here is a straightforward consequence, to be tacitly used in the sequel.

**Corollary 2.2** Let \( c \in \mathbb{Q} \). Assume \( \text{Per}(\varphi_c) \neq \emptyset \). Let \( d \in \mathbb{N} \) be such that \( \text{den}(c) = d^2 \). Then, \( \text{num}(\text{Preper}(\varphi_c)) = d \cdot \text{Preper}(\varphi_c) \).

2.2 Basic remarks on periodic points

In this section, we consider periodic points of any map \( f : A \to A \) where \( A \) is a domain.
2.3 Sums of periodic points

**Lemma 2.3** Let A be a commutative unitary ring and \( f: A \to A \) a self map. Let \( z_1 \in A \) be a periodic point of \( f \) of period \( n \), and let \( \{z_1, \ldots, z_n\} \) be the orbit of \( z_1 \). Then,

\[
\prod_{1 \leq i < j \leq n} (f(z_i) - f(z_j)) = (-1)^{n-1} \prod_{1 \leq i < j \leq n} (z_i - z_j).
\]

**Proof.** We have \( f(z_i) = z_{i+1} \) for all \( 1 \leq i < n \) and \( f(z_n) = z_1 \). Hence,

\[
\prod_{1 \leq i < j \leq n} (f(z_i) - f(z_j)) = \prod_{1 \leq i < j \leq n} (z_{i+1} - z_{j+1}) \prod_{1 \leq i < n} (z_{i+1} - z_1)
\]

\[
= (-1)^{n-1} \prod_{1 \leq i < j \leq n} (z_i - z_j).
\]

**Proposition 2.4** Let \( A \) be a domain and \( f: A \to A \) a map of the form \( f(z) = z^2 - c \) for some \( c \in A \). Assume that \( f \) admits a cycle and at least two distinct periodic points in \( A \).

(i) Let \( x, y \in A \) be distinct periodic points of \( f \), of period \( m \) and \( n \), respectively. Let \( r = \text{lcm}(m, n) \). Then, \( \prod_{i=0}^{r-1} (f^i(x) + f^i(y)) = 1 \).

(ii) Assume \( \text{Per}(f) = \{x_1, x_2, \ldots, x_N\} \). Then, \( \prod_{1 \leq i < j \leq N} (x_i + x_j) = \pm 1 \).

**Proof.** First, observe that for all \( u, v \in A \), we have

(2.1) \( f(u) - f(v) = (u - v)(u + v) \).

Because \( f^r(x) = x \) and \( f^r(y) = y \), we have

(2.2) \( \prod_{i=0}^{r-1} (f^{i+1}(x) - f^{i+1}(y)) = \prod_{i=0}^{r-1} (f^i(x) - f^i(y)). \)

Now, it follows from (2.1) that

\( f^{i+1}(x) - f^{i+1}(y) = (f^i(x) - f^i(y))(f^i(x) + f^i(y)). \)

Because the right-hand side of (2.2) is nonzero, the formula in (i) follows.

Moreover, because \( f \) permutes \( \text{Per}(f) \), we have

\[
\prod_{1 \leq i < j \leq n} (f(x_i) - f(x_j)) = \pm \prod_{1 \leq i < j \leq n} (x_i - x_j).
\]

Using (2.1), and because the above terms are nonzero, the formula in (ii) follows. □

2.3 Sums of periodic points

Here are straightforward consequences of Proposition 2.4 for \( \varphi_c \). The result below originally appeared in [4].

**Proposition 2.5** Let \( c \in \mathbb{Q} \). Assume \( \text{Per}(\varphi_c) = \{x_1, x_2, \ldots, x_n\} \) with \( n \geq 1 \). Let \( d = \text{den}(x_1) \) and \( X_i = \text{num}(x_i) \) for all \( 1 \leq i \leq n \). Then,

(2.3)

\[
\prod_{1 \leq i < j \leq n} (X_i + X_j) = \pm d^{n(n-1)/2}.
\]
Proof. By Proposition 2.1, we have \( \text{den}(x_i) = d \) for all \( i \). Now, chase the denominator in the formulas of Proposition 2.4.

These other consequences will play a crucial role in the sequel.

**Corollary 2.6** Let \( c \in \mathbb{Q} \). Let \( x, y \) be two distinct points in \( \text{Per}(\varphi_c) \). Set \( X = \text{num}(x), Y = \text{num}(y), \) and \( d = \text{den}(x) \). Then:

(i) \( \text{supp}(X + Y) \subseteq \text{supp}(d) \). That is, any prime \( p \) dividing \( X + Y \) also divides \( d \).

(ii) \( X \) and \( Y \) are coprime.

(iii) If no odd prime factor of \( d \) divides \( X + Y \), then \( X + Y = \pm 2^t \) for some \( t \in \mathbb{N} \).

Proof. The first point directly follows from equality (2.3). For the second one, if a prime \( p \) divides \( X \) and \( Y \), then it divides \( d \) by the first point, a contradiction because \( X, d \) are coprime. The last point follows from the first one and the hypothesis on the odd factors of \( d \), which together imply \( \text{supp}(X + Y) \subseteq \{2\} \).

**Example 2.7** Consider the case \( c = 29/16 \) of Example 1.2, where \( d = 4 \) and \( \varphi_c \) admits the cycle \( \mathcal{C} = (-1/4, -7/4, 5/4) \). Here, \( \text{num}(\mathcal{C}) = (-1, -7, 5) \), with pairwise sums \(-8, -2, 4\), respectively. This illustrates all three statements of Corollary 2.6. Viewing \( \mathcal{C} \) as a set, we have \( \mathcal{C} \subseteq \text{Per}(\varphi_c) \). We claim \( \mathcal{C} = \text{Per}(\varphi_c) \). For otherwise, let \( x = X/4 \) be yet another periodic point of \( \varphi_c \). Then, \( X - 1, X - 7, X + 5 \) would also be powers of 2 up to sign. The only possibility is \( X = 3 \) as easily seen. But \( 3/4 \) is only a preperiodic point, because under \( \varphi_c \), we have \( 3/4 \mapsto -5/4 \mapsto -1/4 \mapsto -7/4 \mapsto 5/4 \mapsto -1/4 \).

### 2.4 Divisibility properties of \( \text{den}(c) \)

Our bounds on cycle lengths of \( \varphi_c \) involve the denominator of \( c \). The following proposition and corollary already appear in [15].

**Proposition 2.8** Let \( c \in \mathbb{Q} \). If \( \text{den}(c) \) is odd, then \( |\text{Per}(\varphi_c)| \leq 2 \).

Proof. We have \( \text{den}(c) = d^2 \) for some \( d \in \mathbb{N} \), and \( \text{den}(x) = d \) for all \( x \in \text{Preper}(\varphi_c) \). Assume \( \text{Per}(\varphi_c) = \{x_1, \ldots, x_n\} \). Let \( X_i = \text{num}(x_i) \) for all \( i \). Then, by Proposition 2.5, we have

\[
\prod_{1 \leq i < j \leq n} (X_i + X_j) = \pm d^{n(n-1)/2}.
\]

Because \( d \) is odd by assumption, each factor \( X_i + X_j \) is odd as well, whence \( X_i \neq X_j \) \( \text{mod} \ 2 \) for all \( 1 \leq i < j \leq n \). Of course, this is only possible if \( n \leq 2 \).

**Remark 2.9** If \( c \in \mathbb{Z} \), then \( \text{den}(c) = 1 \), and the above result implies that \( \varphi_c \) admits at most two periodic points.

This bound is sharp, as follows from results in [15].
Corollary 2.10 [15] Let $c \in \mathbb{Q}$. If $\varphi_c$ admits a rational cycle of length at least 3, then $\text{den}(c)$ is even.

We shall sharpen below the conclusion of this corollary by showing that $\text{den}(c)$ must in fact be divisible by 16. For that, we shall need Morton’s Theorem 1.3 excluding period 4, as well as a result due to Pezda concerning periodic points of polynomials over the $p$-adic integers.

2.5 Involving $p$-adic numbers

As usual, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will denote the rings of $p$-adic integers and numbers, respectively. A result in [1] contains a generalization of the above proposition. It says that any polynomial $g(x) = x^p + \alpha$ with $\alpha \in \mathbb{Z}_p$ either admits $p$ fixed points in $\mathbb{Q}_p$ or else a cycle of length exactly $p$ in $\mathbb{Q}_p$. For $z \in \mathbb{Q}_p$, we denote by $v_p(z)$ the $p$-adic valuation of $z$.

Here is Pezda’s theorem [11], to be used in our proof of Theorem 2.13 improving Corollary 2.10. For this application, we shall only need its particular case $p = 2$. However, we shall also invoke the case $p = 3$ later on, in Remark 3.16.

Theorem 2.11 [11] Let $p$ be a prime number, and let $g$ be a polynomial in $\mathbb{Z}_p[t]$ of degree at least 2. Let $\alpha \in \mathbb{Z}_p$ be a periodic point of $g$ of period $n$. If $p = 2$, then $n \in \{1, 2, 4\}$. If $p = 3$, then $n \in \{1, 2, 3, 4, 6, 9\}$.

For proving Theorem 3.17 at the end of the paper, we shall further need the following result of Zieve. See also [13, Theorem 2.21, p. 62]. For $p$ prime, we denote by $(\mathbb{Z}/p\mathbb{Z})^*$ the set of invertible elements in $\mathbb{Z}/p\mathbb{Z}$. Moreover, for $g \in \mathbb{Z}_p[t]$ below, the notation $g^m$ means $g$ raised to the power $m$, and $(g^m)'$ is its formal derivative with respect to $t$.

Theorem 2.12 Let $p$ be a prime number, and let $g$ be a polynomial in $\mathbb{Z}_p[t]$ of degree at least 2. Let $\alpha \in \mathbb{Z}_p$ be a periodic point of $g$, and let

\[ n = \text{the exact period of } \alpha \text{ in } \mathbb{Z}_p, \]
\[ m = \text{the exact period of } \alpha \text{ in } \mathbb{Z}/p\mathbb{Z}, \]
\[ r = \begin{cases} 
\text{the multiplicative order of } (g^m)'(\alpha) & \text{if } (g^m)'(\alpha) \in (\mathbb{Z}/p\mathbb{Z})^*, \\
\infty & \text{if not.}
\end{cases} \]

If $r < \infty$, then $n \in \{m, mr, mrp^e\}$ for some integer $e \geq 1$ such that $p^{e-1} \leq 2/(p - 1)$. If $r = \infty$, then $n = m$.

2.6 Sharpening Corollary 2.10

Theorem 2.13 Let $c \in \mathbb{Q}$. If $\varphi_c$ admits a rational cycle of length $n \geq 3$, then $\text{den}(c)$ is divisible by 16.
We are grateful to Prof. W. Narkiewicz who, after reading a preliminary version of this paper, suggested that our original proof of Theorem 2.13 could be simplified by using Pezda's theorem rather than Zieve's theorem in the preceding section.

**Proof.** By Propositions 2.1 and 2.8, we have \( \text{den}(c) = d^2 \) for some even positive integer \( d \). Assume for a contradiction that \( d \) is not divisible by 4. Hence, \( v_2(d) = 1 \) and \( v_2(c) = -2 \). Let \( \mathcal{C} \subseteq \text{Per}(\varphi_c) \) be a rational cycle of \( \varphi_c \) of length \( n \geq 3 \). For all \( z \in \mathcal{C} \), we have \( \text{den}(z) = d \), and hence \( v_2(z) = -1 \) by Proposition 2.1.

Recall that if \( z_1, z_2 \in \mathbb{Q} \) satisfy \( v_2(z) = v_2(z') = r \) for some \( r \in \mathbb{Z} \), then \( v_2(z \pm z') \geq r + 1 \).

In particular, for all \( z \in \mathcal{C} \), we have \( v_2(z - 1/2) \geq 0 \). Therefore, the translate \( \mathcal{C} - 1/2 \) of \( \mathcal{C} \) may be viewed as a subset of the local ring \( \mathbb{Z}_2(2) \subset \mathbb{Q} \), and hence of the ring \( \mathbb{Z}_2 \) of 2-adic integers. That is, we have

\[
\mathcal{C} - 1/2 \subset \mathbb{Z}_2.
\]

**Step 1.** In view of applying Theorem 2.11, we seek a polynomial in \( \mathbb{Z}_2[t] \) admitting \( \mathcal{C} - 1/2 \) as a cycle. The polynomial

\[
f(t) = \varphi_c(t + 1/2) - 1/2 = t^2 + t - (c + 1/4)
\]

will do. Indeed, by construction, we have

\[
f(t - 1/2) = \varphi_c(t) - 1/2.
\]

Because \( \varphi_c(\mathcal{C}) = \mathcal{C} \), it follows that

\[
f(\mathcal{C} - 1/2) = \mathcal{C} - 1/2,
\]

as desired. For the constant coefficient of \( f \), we claim that \( v_2(c + 1/4) \geq 0 \). Indeed, let \( x, y \in \mathcal{C} \) with \( y = \varphi_c(x) \). Thus, \( f(x - 1/2) = y - 1/2 \), i.e.,

\[
(x - 1/2)^2 + (x - 1/2) - (c + 1/4) = y - 1/2.
\]

Because \( v_2(x - 1/2), v_2(y - 1/2) \geq 0 \), it follows that \( v_2(c + 1/4) \geq 0 \), as claimed. Therefore, \( f(t) \in \mathbb{Z}_2[t] \), as desired.

For the next step, we set

\[
\mathcal{C} - 1/2 = (z_1, \ldots, z_n)
\]

with \( f(z_i) = z_{i+1} \) for \( i \leq n - 1 \) and \( f(z_n) = z_1 \).

**Step 2.** By Theorem 2.11, applied to the polynomial \( g = f \) and to its \( n \)-periodic point \( \alpha = z_1 \), we have \( n \in \{1, 2, 4\} \). Because \( n \geq 3 \) by assumption, it follows that \( n = 4 \). But period 4 for \( \varphi_c \) is excluded by Morton’s Theorem 1.3. This contradiction concludes the proof of the theorem.

\[\blacksquare\]

**Remark 2.14** Theorem 2.13 is best possible, as witnessed by Example 1.2 where period 3 occurs for \( \varphi_c \) with \( c = 29/16 \).
3 An upper bound on $|\text{Per}(\varphi_c)|$

Let $c \in \mathbb{Q}$. Throughout this section, we assume $\text{den}(c) = d^2$ with $d \in 4\mathbb{N}$. Recall that this is satisfied whenever $\varphi_c$ admits a rational cycle $C$ of length $n \geq 3$, as shown by Proposition 2.1 and Theorem 2.13.

Let $s = |\text{supp}(d)|$. The following upper bound on $|\text{Preper}(\varphi_c)|$ was shown in [3]:

$$|\text{Preper}(\varphi_c)| \leq 2^{s+3}.$$  

Our aim in this section is to obtain an analogous upper bound on $|\text{Per}(\varphi_c)|$, namely

$$|\text{Per}(\varphi_c)| \leq 2^s + 2,$$

which in fact is valid for any $c \in \mathbb{Q}$, i.e., also when $d$ is odd, by Proposition 2.8. As mentioned in the Introduction, this new upper bound is only better than the one given by (1.1) for $s \leq 5$.

The proof will follow from a string of modular constraints on the numerators of periodic points of $\varphi_c$ developed in this section.

3.1 Constraints on numerators

We start with an easy observation. See also [3, formula (21)].

**Lemma 3.1** Let $c = a/d^2 \in \mathbb{Q}$ with $a, d$ coprime integers. Let $x \in \text{Preper}(\varphi_c)$. Let $X = \text{num}(x)$. Then, $X^2 \equiv a \mod d$.

**Proof.** We have $x = X/d$ by Proposition 2.1. Let $z = \varphi_c(x)$. Then, $z \in \text{Preper}(\varphi_c)$, whence $z = Z/d$ where $Z = \text{num}(z)$. Now, $z = x^2 - c = (X^2 - a)/d^2$, whence

$$Z = (X^2 - a)/d. \quad (3.1)$$

Because $Z$ is an integer, it follows that $X^2 \equiv a \mod d$. \hfill \blacksquare

Here is a straightforward consequence.

**Proposition 3.2** Let $c \in \mathbb{Q}$ be such that $\text{den}(c) = d^2$ with $d \in 4\mathbb{N}$. Let $X, Y \in \text{num(Preper}(\varphi_c))$. Let $p \in \text{supp}(d)$ and $r = v_p(d)$ the $p$-adic valuation of $d$. Then,

$$X \equiv \pm Y \mod p^r.$$  

In particular, $\text{num(Preper}(\varphi_c))$ reduces to at most two opposite classes mod $p^r$.

**Proof.** It follows from Lemma 3.1 that $X^2 \equiv Y^2 \mod d$. Hence,

$$(X + Y)(X - Y) \equiv 0 \mod p^r.$$  

**Case 1.** Assume $p$ is odd. Then, $p$ cannot divide both $X + Y$ and $X - Y$; for otherwise, it would divide $X$ which is impossible, because $X$ is coprime to $d$. Therefore, $p^r$ divides $X + Y$ or $X - Y$, as desired.
Case 2. Assume \( p = 2 \). Then, \( r \geq 2 \) by hypothesis. Let \( x = X/d, y = Y/d \in \text{Preper}(\varphi_c) \).

Let \( x' = \varphi_c(x) = X'/d \) and \( y' = \varphi_c(y) = Y'/d \). Then, \( X', Y' \) are odd because coprime to \( d \). By (3.1), we have \( X' = (X^2 - a)/d \) and \( Y' = (Y^2 - a)/d \). Hence,

\[
X' - Y' = (X^2 - Y^2)/d.
\]

Because \( 2^r \) divides \( d \) and because \( X' - Y' \) is even, it follows that

\[
(X + Y)(X - Y) \equiv 0 \mod 2^{r+1}.
\]

Now, \( 4 \) cannot divide both \( X + Y \) and \( X - Y \) because \( X, Y \) are odd. Therefore, \( X + Y \equiv 0 \mod 2^r \) or \( X - Y \equiv 0 \mod 2^r \), as desired.

Here is a straightforward consequence of Proposition 3.2 and the Chinese Remainder Theorem.

Corollary 3.3 Let \( c \in \mathbb{Q} \) be such that \( \text{den}(c) = d^2 \) with \( d \in 4\mathbb{N} \). Let \( s = |\text{supp}(d)| \). Then, \( \text{num}(\text{Preper}(\varphi_c)) \) reduces to at most \( 2^s \) classes mod \( d \).

We thank one of the referees for pointing out that Corollary 3.3, combined with the result in [3] that the preperiodic points lie in the union of two intervals symmetrical with respect to 0 and each of length at most 2, implies that the number of preperiodic points is less than \( 2^{s+2} \).

The particular case in Proposition 3.2 where \( X, Y \in \text{num}(\text{Per}(\varphi_c)) \) and \( X \equiv Y \mod p' \) for all \( p \in \text{supp}(d) \), i.e., where \( X \equiv Y \mod d \), has a somewhat surprising consequence and will be used more than once in the sequel. It only concerns periodic points, as we need to use Corollary 2.6.

Proposition 3.4 Let \( c \in \mathbb{Q} \) be such that \( \text{den}(c) = d^2 \) with \( d \in 4\mathbb{N} \). Let \( X, Y \in \text{num}(\text{Per}(\varphi_c)) \) be distinct. If \( X \equiv Y \mod d \), then \( X + Y = \pm 2 \).

Proof. As \( X, Y \) are coprime to \( d \), they are odd. We claim that \( \text{supp}(X + Y) = \{2\} \). Indeed, let \( p \) be any prime factor of \( X + Y \). Then, \( p \) divides \( d \) by Corollary 2.6. Hence, \( p \) divides \( X - Y \), because \( d \) divides \( X - Y \) by hypothesis. Therefore, \( p \) divides \( 2X \), whence \( p = 2 \), because \( p \) does not divide \( X \). It follows that \( X + Y = \pm 2^t \) for some integer \( t \geq 1 \). Because \( d \in 4\mathbb{N} \) and \( d \) divides \( X - Y \), it follows that \( 4 \) divides \( X - Y \). Hence, \( 4 \) cannot also divide \( X + Y \), because \( X, Y \) are odd. Therefore, \( t = 1 \), i.e., \( X + Y = \pm 2 \), as desired.

Example 3.5 Consider the case \( c = 29/16 \) of Example 1.2, where \( \varphi_c \) admits the cycle \( \mathcal{C} = (-1/4, -7/4, 5/4) \). In \( \text{num}(\mathcal{C}) = (-1, -7, 5) \), only \(-7 \) and \( 5 \) belong to the same class mod 4, and their sum is \(-2 \) as expected.

### 3.2 From \( \mathbb{Z}/d\mathbb{Z} \) to \( \mathbb{Z} \)

Our objective now is to derive from Proposition 3.2 the upper bound \( |\text{Per}(\varphi_c)| \leq 2^t + 2 \) announced earlier. For that, we shall need the following two auxiliary results.
Lemma 3.6  Let $k \in \mathbb{N}$. Up to order, there are only two ways to express $2^k$ as $2^k = \varepsilon_1 2^{k_1} + \varepsilon_2 2^{k_2}$ with $\varepsilon_1, \varepsilon_2 = \pm 1$ and $k_1, k_2 \in \mathbb{N}$.

Proof.  We may assume $k_1 \leq k_2$. There are two cases.
(1) If $k_1 = k_2$, then $2^{k_1} (\varepsilon_1 + \varepsilon_2) = 2^k$, implying $k_1 = k_2 = k + 1$ and $\varepsilon_1 = \varepsilon_2 = 1$.
(2) If $k_1 < k_2$, then $2^{k_1} (\varepsilon_1 + \varepsilon_2 2^{k_2-k_1}) = 2^k$, implying $k = k_1 = k_2 - 1$, $\varepsilon_1 = -1$, and $\varepsilon_2 = 1$.

Proposition 3.7  Let $\epsilon \in \mathbb{Q}$ be such that $\text{den}(\epsilon) = d^2$ with $d \in 4\mathbb{N}$. If there are four pairwise distinct elements $X_1, Y_1, X_2, Y_2 \in \text{num}(\text{Per}(\phi_{\epsilon}))$ such that $|X_1 + Y_1| = |X_2 + Y_2| = 2^k$ for some $k \in \mathbb{N}$, then

$$X_1 + Y_1 = -(X_2 + Y_2).$$

Proof. Assume for a contradiction that $X_1 + Y_1 = X_2 + Y_2 = \pm 2^k$. Let $p \in \text{supp}(d)$ be odd, if any such factor exists. We claim that $X_1, X_2, Y_1, Y_2$ all belong to the same nonzero class mod $p$. Indeed, we know by Proposition 3.2 that $X_1, X_2, Y_1, Y_2$ belong to at most two opposite classes mod $p$. Because $p$ does not divide $X_i + Y_i$ for $1 \leq i \leq 2$, i.e., $X_i \neq -Y_i$ mod $p$, it follows that $X_i \equiv Y_i$ mod $p$. Because $X_1 \equiv \pm X_2$ mod $p$ and $X_1 + Y_1 = X_2 + Y_2$, it follows that $X_1 \equiv X_2$ mod $p$ and the claim is proved, i.e.,

$$X_1 \equiv X_2 \equiv Y_1 \equiv Y_2 \equiv \text{mod} p.$$

Therefore, no sum of two elements in $\{X_1, Y_1, X_2, Y_2\}$ is divisible by $p$. Hence, by the third point of Corollary 2.6, any sum of two distinct elements in $\{X_1, Y_1, X_2, Y_2\}$ is equal up to sign to a power of 2. Moreover, we have

$$\pm 2^{k+1} = (X_1 + Y_1) + (X_2 + Y_2) = (X_1 + X_2) + (Y_1 + Y_2) = (X_1 + Y_2) + (X_2 + Y_1).$$

It now follows from Lemma 3.6 that at least two of $X_1, Y_1, X_2, Y_2$ are equal, contradicting the hypothesis that they are pairwise distinct. Hence, $X_1 + Y_1 = -(X_2 + Y_2)$, as claimed.

Notation 3.8  For any $h \in \mathbb{Z}$, we shall denote by $\pi_h : \mathbb{Z} \to \mathbb{Z} / h\mathbb{Z}$ the canonical quotient map mod $h$.

Theorem 3.9  Let $\epsilon \in \mathbb{Q}$ be such that $\text{den}(\epsilon) = d^2$ with $d \in 4\mathbb{N}$. Let $m = |\pi_d(\text{num}(\text{Per}(\phi_{\epsilon})))|$. Then,

$$m \leq |\text{Per}(\phi_{\epsilon})| \leq m + 2.$$ 

Proof. The first inequality is obvious. We now show $|\text{Per}(\phi_{\epsilon})| \leq m + 2$.

Claim  Each class mod $d$ contains at most two elements of $\text{num}(\text{Per}(\phi_{\epsilon}))$. 

Assume the contrary. Then, there are three distinct elements $X, Y, Z$ in $\text{num}(\text{Per}(\varphi_c))$ such that $X \equiv Y \equiv Z \mod d$. By Proposition 3.4, all three sums $X + Y$, $X + Z$, and $Y + Z$ belong to $\{\pm 2\}$. Hence, two of them coincide, e.g., $X + Y = X + Z$. Therefore, $Y = Z$, a contradiction. This proves the claim.

Now, assume for a contradiction that $|\text{Per}(\varphi_c)| \geq m + 3$. The claim then implies that there are at least three distinct classes mod $d$ each containing two distinct elements in $\text{num}(\text{Per}(\varphi_c))$. That is, there are six distinct elements $X_1, Y_1, X_2, Y_2$ and $X_3, Y_3$ in $\text{num}(\text{Per}(\varphi_c))$ such that $X_i \equiv Y_i \mod d$ for $1 \leq i \leq 3$. Again, Proposition 3.4 implies $X_i + Y_i = \pm 2$ for $1 \leq i \leq 3$. This situation is excluded by Proposition 3.7, and the proof is complete.

**Remark 3.10**

The above proof shows that if $|\text{Per}(\varphi_c)| = m + 2$, then there are exactly two classes mod $d$ containing more than one element of $\text{num}(\text{Per}(\varphi_c))$, and both classes contain exactly two such elements. Denoting $\{X_1, Y_1\}, \{X_2, Y_2\} \subset \text{num}(\text{Per}(\varphi_c))$ these two special pairs, the proof further shows that $X_1 + Y_1 = \pm 2 = -(X_2 + Y_2)$.

**Corollary 3.11**

Let $c \in \mathbb{Q}$ be such that $\text{den}(c) = d^2$ with $d \in 4\mathbb{N}$. Let $s = |\text{supp}(d)|$. Then,

$$|\text{Per}(\varphi_c)| \leq 2^s + 2.$$

**Proof.** We have $|\text{Per}(\varphi_c)| \leq m + 2$ by the above theorem, and $m \leq 2^s$ by Corollary 3.3.

### 3.3 Numerator dynamics

Let $c = a/d^2 \in \mathbb{Q}$ with $a, d$ coprime integers. Closely related to the map $\varphi_c$ is the map $d^{-1}\varphi_a : \mathbb{Q} \to \mathbb{Q}$. By definition, this map satisfies

$$d^{-1}\varphi_a(x) = (x^2 - a)/d,$$

for all $x \in \mathbb{Q}$. As was already implicit earlier, we now show that cycles of $\varphi_c$ in $\mathbb{Q}$ give rise, by taking numerators, to cycles of $d^{-1}\varphi_a$ in $\mathbb{Z}$.

The proof of the following lemma is left as an easy exercise.

**Lemma 3.12**

Let $c = a/d^2 \in \mathbb{Q}$ with $a, d$ coprime integers. Let $\mathcal{C} \subset \mathbb{Q}$ be a cycle of $\varphi_c$. Then, $\text{num}(\mathcal{C}) \subset \mathbb{Z}$ is a cycle of $d^{-1}\varphi_a$ of length $|\mathcal{C}|$.

### 3.4 The cases $d \not\equiv 0 \mod 3$ or mod $5$

**Lemma 3.13**

Let $c \in \mathbb{Q}$ and $\mathcal{C} \subset \text{Per}(\varphi_c)$ a cycle of positive length $n$.

(i) If $d \not\equiv 0 \mod 3$ and $n \geq 3$, then $\text{num}(\mathcal{C})$ reduces mod 3 to exactly one nonzero element.

(ii) If $d \not\equiv 0 \mod 5$ and $n \geq 4$, then $\text{num}(\mathcal{C})$ reduces mod 5 to exactly one or two nonzero elements mod 5.
Proof. Let us start with some preliminaries. Of course, \( \varphi_c \) induces a cyclic permutation of \( \mathcal{C} \). By Proposition 2.1, we have \( c = a/d^2 \) with \( a, d \) coprime integers. By Lemma 3.12, the rational map \( d^{-1}\varphi_a \) induces a cyclic permutation of \( \text{num}(\mathcal{C}) \), say

\[
d^{-1}\varphi_a \colon \text{num}(\mathcal{C}) \to \text{num}(\mathcal{C}).
\]

Let \( X, Y \in \text{num}(\mathcal{C}) \) be distinct. Then, \( \text{supp}(X + Y) \subseteq \text{supp}(d) \) by Corollary 2.6. In particular, let \( q \) be any prime number such that \( d \not\equiv 0 \mod q \). Then,

\[
X + Y \not\equiv 0 \mod q.
\]

Because \( d \) is invertible mod \( q \), the map \( d^{-1}\varphi_a \) induces a map

\[
f \colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z},
\]

where \( f(x) = d^{-1}(x^2 - a) \) for all \( x \in \mathbb{Z}/q\mathbb{Z} \). Thus, we may view \( \pi_q(\text{num}(\mathcal{C})) \) as a sequence of length \( n \) in \( \mathbb{Z}/q\mathbb{Z} \), where each element is cyclically mapped to the next by \( f \). Note that (3.2) implies that this \( n \)-sequence does not contain opposite elements \( u, -u \) of \( \mathbb{Z}/q\mathbb{Z} \), and in particular contains at most one occurrence of 0.

We are now ready to prove statements (i) and (ii).

(i) Assume \( d \equiv 0 \mod q \) where \( q = 3 \). By the above, the \( n \)-sequence \( \pi_3(\text{num}(\mathcal{C})) \) consists of at most one 0 and all other elements equal to some \( u \in \{ \pm 1 \} \). Because \( n \geq 3 \), this \( n \)-sequence contains two cyclically consecutive occurrences of \( u \). Therefore, \( f(u) = u \). Hence, \( \pi_3(\text{num}(\mathcal{C})) \) contains \( u \) as its unique element repeated \( n \) times.

(ii) Assume \( d \not\equiv 0 \mod q \) where \( q = 5 \). Because \( n \geq 4 \) and the \( n \)-sequence \( \pi_5(\text{num}(\mathcal{C})) \) contains at most one 0, it must contain three cyclically consecutive nonzero elements \( u_1, u_2, u_3 \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\} \). Because that set contains at most two pairwise nonopposite elements, it follows that \( u_i = u_j \) for some \( 1 \leq i < j \leq 3 \). Now, \( u_1 \mapsto u_2 \mapsto u_3 \) by \( f \). Therefore, if either \( u_1 = u_2 \) or \( u_2 = u_3 \), it follows that the whole sequence \( \pi_5(\text{num}(\mathcal{C})) \) consists of the one single element \( u_2 \) repeated \( n \) times. On the other hand, if \( u_1 \neq u_2 \), then \( u_1 = u_3 \). In this case, the \( n \)-sequence \( \pi_5(\text{num}(\mathcal{C})) \) consists of the sequence \( u_1, u_2 \) repeated \( n/2 \) times. This concludes the proof.

Example 3.14 Consider the case \( c = a/d^2 = 29/16 \) of Example 1.2, where \( \varphi_c \) admits the cycle \( \mathcal{C} = (-1/4, -7/4, 5/4) \). Then, \( \text{num}(\mathcal{C}) = (-1, -7, 5) \), a cycle of length 3 of the map \( d^{-1}\varphi_a = 4^{-1}\varphi_{29} \). That cycle reduces mod 3 to \((-1, -1, -1)\), as expected with statement (i) of the lemma. Statement (ii) does not apply because \( n = 3 \), and it would fail anyway because \( \text{num}(\mathcal{C}) \) reduces mod 5 to the sequence \((-1, -2, 0)\).

3.5 Main consequences

Proposition 3.15 Let \( c = a/d^2 \in \mathbb{Q} \) with \( a, d \) coprime integers and with \( d \in 4\mathbb{N} \). Assume \( d \not\equiv 0 \mod 3 \). Let \( s = |\text{supp}(d)| \). For every rational cycle \( \mathcal{C} \) of \( \varphi_c \), we have

\[
|\mathcal{C}| \leq 2^s + 1.
\]

Proof. By Corollary 3.11, we have \( |\mathcal{C}| \leq 2^s + 2 \). If \( |\mathcal{C}| = 2^s + 2 \), then, by Remark 3.10, there exist two pairs \( \{X_1, Y_1\}, \{X_2, Y_2\} \) in \( \text{num}(\mathcal{C}) \) such that \( X_1 + Y_1 = 2 \) and \( X_2 + Y_2 = -2 \). Because \( d \not\equiv 0 \mod 3 \), Lemma 3.13 implies that \( X_1, X_2, Y_1, Y_2 \)
reduce to the same nonzero element $u \mod 3$. This contradicts the equality $X_1 + Y_1 = -(X_2 + Y_2)$.

Again, we are grateful to Prof. W. Narkiewicz for the remark below.

**Remark 3.16** Under the same hypotheses as above, the conclusion $|C| \leq 2^s + 1$ may be improved to $|C| \leq 9$ provided $s \geq 4$. This follows from Pezda’s Theorem 2.11 for $p = 3$. See also [2] for related results.

We may now conclude the paper with one of its main results.

**Theorem 3.17** If $\text{den}(e)$ admits at most two distinct prime factors, then $\varphi_e$ satisfies the Flynn–Poonen–Schaefer conjecture.

**Proof.** Let $C$ be a rational cycle of $\varphi_e$ of length $n \geq 3$. Then, $d$ is even, and hence $s \geq 1$.

- If $s = 1$, then $d$ is a power of 2. By Corollary 3.11 and Proposition 3.15, we have $|\text{Per}(\varphi_e)| \leq 4$ and $|C| \leq 3$. See also [4].
- Assume now $s = 2$. Then, $d = 2^r p^s$ where $p$ is an odd prime and $r_1 \geq 2$. By Theorem 3.9, we have $|C| \leq |\text{Per}(\varphi_e)| \leq 6$. By Theorems 1.3 and 1.4, we have $|C| \neq 4, 5$. It remains to show $|C| \neq 6$. We distinguish two cases. If $p \neq 3$, then $|C| \leq 2^s + 1 = 5$ by Proposition 3.15, and we are done. Assume now $p = 3$, so that $d = 2^s 3^{r_2}$. Let $m$ denote the number of classes of $\text{num}(C) \mod q = 5$. It follows from Lemma 3.13 that $m \leq 2$. Because the order of every element in $(\mathbb{Z}/5\mathbb{Z})^*$ belongs to $\{1, 2, 4\}$, it follows from Zieve’s Theorem 2.12 that $|C|$ is a power of 2. Hence, $|C| \in \{1, 2, 4\}$, and we are done.

**Acknowledgment** The authors are grateful to both anonymous referees for their detailed reading of the original version of this paper and for their highly valuable remarks and suggestions.

**References**

[1] A. Adam and Y. Fares, *On two affine-like dynamical systems in a local field*. J. Number Theory. 132(2012), 2892–2906.

[2] R. Benedetto, *Preperiodic points of polynomials over global fields*. J. Reine Angew. Math. 608(2007), 123–153.

[3] G. Call and S. Goldstine, *Canonical heights on projective space*. J. Number Theory. 63(1997), 211–243.

[4] S. Eliahou and Y. Fares, *Poonen’s conjecture and Ramsey numbers*. Discrete Appl. Math. 209(2016), 102–106.

[5] Y. Fares, *On the iteration over $\mathbb{R}$ of rational quadratic polynomials*. Preprint, 2020. https://hal.archives-ouvertes.fr/hal-02534351/document

[6] E. V. Flynn, B. Poonen, and E. F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*. Duke Math. J. 90(1997), 435–463.

[7] P. Morton, *Arithmetic properties of periodic points of quadratic maps*. Acta Arith. 62(1992), 343–372.

[8] W. Narkiewicz, *Cycle-lengths of a class of monic binomials*. Funct. Approx. Comment. Math. 42(2010), 2, 163–168.

[9] W. Narkiewicz, *On a class of monic binomials*. Proc. Steklov Inst. Math. 280(2013), suppl. 2, S65–S70.
Some results on the Flynn–Poonen–Schaefer conjecture

[10] D. Northcott, Periodic points on an algebraic variety. Ann. of Math. (2). 51(1950), 167–177.
[11] T. Pezda, Polynomial cycles in certain local domains. Acta Arith. 66(1994), 11–22.
[12] B. Poonen, The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture. Math. Z. 228(1998), 11–29.
[13] J. H. Silverman, The arithmetic of dynamical systems, Graduate Texts in Mathematics, 241, Springer, New York, 2007.
[14] M. Stoll, Rational 6-cycles under iteration of quadratic polynomials. LMS J. Comput. Math. 11(2008), 367–380.
[15] R. Walde and P. Russo, Rational periodic points of the quadratic function $Q_c = x^2 + c$. Amer. Math. Monthly. 101(1994), 318–331.
[16] M. Zieve, Cycles of polynomial mappings. Ph.D. thesis, UC Berkeley, 1996.

Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville (LMPA), Université du Littoral Côte d’Opale, UR 2597, F-62100 Calais, France, and CNRS, FR2037, France

e-mail: eliahou@univ-littoral.fr

LAMFA, CNRS-UMR 7352, Université de Picardie, 80039 Amiens, France, and CNRS, FR2037, France

e-mail: youssef.fares@u-picardie.fr