



Some results on the Flynn-Poonen-Schaefer Conjecture

Shalom Eliahou, Youssef Fares

► To cite this version:

Shalom Eliahou, Youssef Fares. Some results on the Flynn-Poonen-Schaefer Conjecture. 2019. hal-02073665

HAL Id: hal-02073665

<https://hal.science/hal-02073665>

Preprint submitted on 20 Mar 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SOME RESULTS ON THE FLYNN-POONEN-SCHAEFER CONJECTURE

SHALOM ELIAHOU AND YOUSSEF FARES

ABSTRACT. For $c \in \mathbb{Q}$, consider the quadratic polynomial map $\varphi_c(x) = x^2 - c$. Flynn, Poonen and Schaefer conjectured in 1997 that no rational cycle of φ_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 φ_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 φ_c in terms of the number of distinct prime factors of the denominator of c . Finally, we show that the Flynn-Poonen-Schaefer conjecture holds for φ_c if that denominator 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 φ is the sequence of iterates

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

where φ^k is the k^{th} iterate of φ and $\varphi^0 = \text{Id}_S$. We say that z is *periodic* under φ 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 $\mathcal{C} = (z, \varphi(z), \dots, \varphi^{n-1}(z))$, and we say that \mathcal{C} is a *cycle* of length n . The element z is said to be *preperiodic* under φ 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 ≥ 2 , its set of preperiodic points is *finite*, this being a particular case of a well known theorem of Northcott [7]. However, determining the cardinality of this set is very difficult in general. The following conjecture due to Flynn, Poonen and Schaefer [5] illustrates the difficulty in understanding, in general, the periodic points of polynomials, even those of degree 2.

Conjecture 1.1. *Let $c \in \mathbb{Q}$. Consider the quadratic map $\varphi_c: \mathbb{Q} \rightarrow \mathbb{Q}$ defined by¹ $\varphi_c(x) = x^2 - c$ for all $x \in \mathbb{Q}$. Then every periodic point of φ_c in \mathbb{Q} has period at most 3.*

See also [8] for a refined conjecture on the rational *preperiodic* points of quadratic maps over \mathbb{Q} . 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 φ_c admits the cycle $\mathcal{C} = (-1/4, -7/4, 5/4)$ of length 3.*

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 period 4 and period 5 are indeed excluded, by Morton [6] and by Flynn, Poonen and Schaefer [5], respectively.

Theorem 1.3 (Morton). *For every $c \in \mathbb{Q}$, there is no periodic point of φ_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 φ_c in \mathbb{Q} of period 5.*

No period higher than 5 has been excluded so far for the rational maps φ_c . However, Stoll showed that the exclusion of period 6 would follow from the validity of the Birch and Swinnerton-Dyer conjecture [10].

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 Theorem 2.11, a particular case of a theorem of Zieve [12] on polynomial iteration over the *p*-adic integers.

Given $0 \neq c \in \mathbb{Q}$, let s denote the number of distinct primes dividing the denominator of c . In [2], Call and Goldstine showed that the number of rational preperiodic points of φ_c does not exceed the upper bound $2^{s+2} + 1$. Among our present results, we show that any rational cycle of φ_c has length at most $2^s + 2$. We also show that the conjecture holds for φ_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 $\varphi_c: \mathbb{Q} \rightarrow \mathbb{Q}$ the quadratic map defined by $\varphi_c(x) = x^2 - c$ for all $x \in \mathbb{Q}$. Most papers dealing with Conjecture 1.1 rather consider the map $x^2 + c$. Our present choice

¹The map $x \mapsto x^2 + c$ is more common in the literature, but we slightly prefer to deal with $x \mapsto x^2 - c$.

allows statements with positive rather than negative values of c . For instance, with this choice, we show in [4] that if φ_c admits a cycle of length at least 2, then $c \geq 1$.

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

$$\begin{aligned}\text{Per}(\varphi_c) &= \{x \in \mathbb{Q} \mid \varphi_c^n(x) = x \text{ for some } n \in \mathbb{N}\}, \\ \text{Preper}(\varphi_c) &= \{x \in \mathbb{Q} \mid \varphi_c^m(x) \in \text{Per}(\varphi_c) \text{ for some } m \in \mathbb{N}\}.\end{aligned}$$

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 $v_p(x)$ of x is the unique $r \in \mathbb{Z} \cup \{\infty\}$ such that $x = p^r x_1/x_2$ with $x_1, x_2 \notin p\mathbb{Z}$ 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 φ_c has a periodic point of period at least 3, then $\text{den}(c)$ is divisible by 16*. The result below first appeared in [11].

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 $x \in \text{Preper}(\varphi_c)$.*

Proof. Let p be a prime dividing $\text{den}(c)$, i.e. such that $v_p(c) < 0$. Let $x \in \mathbb{Q}$.

Claim. *If $v_p(x) \neq v_p(c)/2$, then the orbit of x under φ_c is infinite.*

Indeed, consider the following two cases.

- (1) If $v_p(x) < v_p(c)/2$, then $v_p(\varphi_c(x)) = v_p(x^2 - c) = 2v_p(x)$. Thus $v_p(\varphi_c(x)) < v_p(c) < v_p(c)/2$ since $v_p(c) < 0$. It follows that $v_p(\varphi_c^n(x)) = 2^n v_p(x)$ for all $n \geq 1$.
- (2) If $v_p(x) > v_p(c)/2$, then $v_p(\varphi_c(x)) = v_p(x^2 - c) = v_p(c) < v_p(c)/2$ and we are back in the preceding case. In particular, we have $v_p(\varphi_c^n(x)) = 2^{n-1} v_p(c)$ for all $n \geq 1$.

In both cases, the p -adic valuation of $\varphi_c^n(x)$ tends to $-\infty$ for $n \rightarrow \infty$, whence the claim.

If now $x \in \text{Preper}(\varphi_c)$, then the claim implies $v_p(x) = v_p(c)/2$. Note that such points x exist by hypothesis on φ_c . Hence $v_p(c)$ is even, and since this occurs for all primes p dividing $\text{den}(c)$, it follows that $\text{den}(c) = d^2$ for some $d \in \mathbb{N}$, and that $\text{den}(x) = d$. \square

Consequently, since we are only interested in rational cycles of φ_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 φ_c .

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

$$\text{num}(\text{Per}(\varphi_c)) = d \cdot \text{Per}(\varphi_c), \quad \text{num}(\text{Preper}(\varphi_c)) = d \cdot \text{Preper}(\varphi_c).$$

Proof. Directly follows from the equality $\text{den}(\text{Preper}(\varphi_c)) = \{d\}$ given by Proposition 2.1. \square

2.2. Basic remarks on periodic points. In this section, we consider periodic points of any map $f: A \rightarrow A$ where A is a domain.

Lemma 2.3. *Let A be a commutative unitary ring and $f: A \rightarrow A$ a self map. Let $z_1 \in A$ be a periodic point of f of period n , and let $\{z_1, \dots, z_n\}$ 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

$$\begin{aligned} \prod_{1 \leq i < j \leq n} (f(z_i) - f(z_j)) &= \prod_{1 \leq i < j < n} (z_{i+1} - z_{j+1}) \prod_{1 \leq i < n} (z_{i+1} - z_1) \\ &= (-1)^{n-1} \prod_{1 \leq i < j \leq n} (z_i - z_j). \end{aligned}$$

\square

Proposition 2.4. *Let A be a domain and $f: A \rightarrow A$ a map of the form $f(x) = x^2 - c$ for some $c \in A$. Assume that f admits a cycle in A .*

(i) *Let $x, y \in A$ be two 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 $\text{Per}(f) = \{x_1, x_2, \dots, x_N\}$. 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

$$(1) \quad f(u) - f(v) = (u - v)(u + v).$$

(i) Since $f^r(x) = x$ and $f^r(y) = y$, we have

$$(2) \quad \prod_{i=0}^{r-1} (f^{i+1}(x) - f^{i+1}(y)) = \prod_{i=0}^{r-1} (f^i(x) - f^i(y)).$$

Now, it follows from (1) that

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

Since the right-hand side of (2) is nonzero, the formula in (i) follows.

Moreover, since 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 (1), and since the above terms are nonzero, the formula in (ii) follows. \square

2.3. Sums of periodic points. Here are straightforward consequences of Proposition 2.4 for φ_c . The result below originally appeared in [3].

Proposition 2.5. *Let $c \in \mathbb{Q}$. Assume $\text{Per}(\varphi_c) = \{x_1, x_2, \dots, x_n\}$ 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, for all $1 \leq k \leq n-1$, we have*

$$(3) \quad \prod_{1 \leq i \leq n} (X_i + X_{i+k}) = d^n \text{ (with indices read mod } n),$$

$$(4) \quad \prod_{1 \leq i < j \leq n} (X_i + X_j) = \pm d^{n(n-1)/2}.$$

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. \square

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

Example 2.7. *Consider the case $c = 29/16$ of Example 1.2, where $d = 4$ and φ_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 φ_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, since under φ_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 φ_c involve the denominator of c . The following proposition and corollary already appear in [11].

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 $\text{Per}(\varphi_c) = \{x_1, \dots, x_n\}$. Let $X_i = \text{num}(x_i)$ for all i . Then by equality (4) in Proposition 2.5, we have

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

Since d is odd by assumption, each factor $X_i + X_j$ is odd as well, whence $X_i \not\equiv X_j \pmod{2}$ for all $1 \leq i < j \leq n$. Of course, this is only possible if $n \leq 2$. \square

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

Corollary 2.10 ([11]). *Let $c \in \mathbb{Q}$. If φ_c admits a rational cycle of length at least 3, then $\text{den}(c)$ is even.*

2.5. Involving p -adic numbers. We shall now improve Corollary 2.10 by showing that under the same hypotheses, $\text{den}(c)$ 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 below due to Zieve concerning periodic points of polynomials over the p -adic integers.

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 a particular case of a theorem of Zieve [12] that we shall use to improve Corollary 2.10. See also [9, Theorem 2.21 p. 62].

Theorem 2.11. *Let p be a prime number and let g be a polynomial in $\mathbb{Z}_p[t]$ of degree at least 2. Let α be a periodic point of g in \mathbb{Z}_p and let*

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

Then $n \in \{m, mr, mrp^e\}$ for some integer $e \geq 1$ such that $p^{e-1} \leq 2/(p-1)$.

We may now sharpen Corollary 2.10.

Theorem 2.12. *Let $c \in \mathbb{Q}$. If φ_c admits a rational cycle of length $n \geq 3$, then $\text{den}(c)$ is divisible by 16.*

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 φ_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 $\mathbb{Z}_{(2)} \subset \mathbb{Q}$, 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

$$\begin{aligned} f(t) &= \varphi_c(t + 1/2) - 1/2 \\ &= t^2 + t - (c + 1/4) \end{aligned}$$

will do. Indeed, by construction we have

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

Since $\varphi_c(\mathcal{C}) = \mathcal{C}$, 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.

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

Since $v_2(x - 1/2), v_2(y - 1/2) \geq 0$, 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

$$\mathcal{C} - 1/2 = (z_1, \dots, z_n)$$

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

Step 2. We now apply Theorem 2.11 to the polynomial $g = f$ and to its n -periodic point $\alpha = z_1$. We need to compute the corresponding numbers m and r in that theorem, where m is the period of z_1 in $\mathbb{Z}/2\mathbb{Z}$.

We claim that $m = 1$. By Lemma 2.3, for the cycle (z_1, z_2, \dots, z_n) of f , we have

$$\prod_{1 \leq i < j \leq n}^n \frac{f(z_i) - f(z_j)}{z_i - z_j} = \pm 1.$$

Since $f(x) - f(y) = (x - y)(x + y + 1)$ for all x, y , this yields

$$\prod_{1 \leq i < j \leq n}^n (z_i + z_j + 1) = \pm 1.$$

Therefore $v_2(z_i + z_j + 1) = 0$ for all $1 \leq i < j \leq n$, which in turn implies $v_2(z_i - z_j) \geq 1$ for all $i < j$. Consequently, the cycle (z_1, z_2, \dots, z_n) collapses to the cycle (z_1) of length 1 in $\mathbb{Z}/2\mathbb{Z}$. This settles the claim.

Since $m = 1$, we have $(f^m)'(t) = f'(t) = 2t + 1$ in $\mathbb{Z}_2[t]$, whence $f'(z_1) = 1$ in $\mathbb{Z}/2\mathbb{Z}$. Therefore $r = 1$ by definition.

By Theorem 2.11, it follows that $n \in \{1, 2^e\}$ for some integer $e \geq 1$ such that $2^{e-1} \leq 2/1$. Hence $e \leq 2$ and so $n \in \{1, 2, 4\}$. Since $n \geq 3$ by assumption, it follows that $n = 4$. But period 4 for φ_c is excluded by Morton's Theorem 1.3. This contradiction concludes the proof of the theorem. \square

Remark 2.13. *Theorem 2.12 is best possible, as witnessed by Example 1.2 where period 3 occurs for φ_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 φ_c admits a rational cycle \mathcal{C} of length $n \geq 3$, as shown by Proposition 2.1 and Theorem 2.12.

Let $s = |\text{supp}(d)|$. The following upper bound on $|\text{Preper}(\varphi_c)|$ was shown in [2]:

$$|\text{Preper}(\varphi_c)| \leq 2^{s+2} + 1.$$

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

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

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

3.1. Constraints on numerators. We start with an easy observation.

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 $X^2 \equiv a \pmod{d}$.*

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

$$(5) \quad Z = (X^2 - a)/d.$$

Since Z is an integer, it follows that $X^2 \equiv a \pmod{d}$. \square

Here is a straightforward consequence.

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

$$X \equiv \pm Y \pmod{p^r}.$$

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

Proof. It follows from Lemma 3.1 that $X^2 \equiv Y^2 \pmod{d}$. Hence

$$(X + Y)(X - Y) \equiv 0 \pmod{p^r}.$$

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 since 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 $x' = \varphi_c(x) = X'/d$ and $y' = \varphi_c(y) = Y'/d$. Then X', Y' are odd since coprime to d . By (5), we have $X' = (X^2 - a)/d$ and $Y' = (Y^2 - a)/d$. Hence

$$X' - Y' = (X^2 - Y^2)/d.$$

Since 2^r divides d and since $X' - Y'$ is even, it follows that

$$(X + Y)(X - Y) \equiv 0 \pmod{2^{r+1}}.$$

Now 4 cannot divide both $X + Y$ and $X - Y$ since X, Y are odd. Therefore $X + Y \equiv 0 \pmod{2^r}$ or $X - Y \equiv 0 \pmod{2^r}$, as desired. \square

Corollary 3.3. *Let $c \in \mathbb{Q}$ 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 .*

Proof. Set $\text{supp}(d) = \{p_1, \dots, p_s\}$ and $d = p_1^{r_1} \dots p_s^{r_s}$. By Proposition 3.2, the set $\text{num}(\text{Preper}(\varphi_c))$ covers at most 2 distinct classes mod $p_i^{r_i}$ for all $1 \leq i \leq s$. Therefore, by the Chinese Remainder Theorem, this set covers at most 2^s distinct classes mod d . \square

The particular case in Proposition 3.2 where $X, Y \in \text{num}(\text{Per}(\varphi_c))$ and $X \equiv +Y \pmod{p^r}$ for all $p \in \text{supp}(d)$, i.e. where $X \equiv Y \pmod{d}$, has a somewhat surprising consequence and will be used more than once in the sequel.

Proposition 3.4. *Let $c \in \mathbb{Q}$ 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 $X \equiv Y \pmod{d}$, 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 $X - Y$ since d divides $X - Y$ by hypothesis. Therefore p divides $2X$, whence $p = 2$ since X is odd. It follows that $X + Y = \pm 2^t$ for some integer $t \geq 1$. Since $d \in 4\mathbb{N}$ and d divides $X - Y$, it follows that 4 divides $X - Y$. Hence 4 cannot also divide $X + Y$ since X, Y are odd. Therefore $t = 1$, i.e. $X + Y = \pm 2$ as desired. \square

Example 3.5. *Consider the case $c = 29/16$ of Example 1.2, where φ_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 $|\text{Per}(\varphi_c)| \leq 2^s + 2$ 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 $\varepsilon_2 = 1$. \square

Proposition 3.7. *Let $c \in \mathbb{Q}$ such that $\text{den}(c) = d^2$ with $d \in 4\mathbb{N}$. If there are distinct pairs $\{X_1, Y_1\}, \{X_2, Y_2\} \subseteq \text{num}(\text{Per}(\varphi_c))$ such that $X_1 + Y_1 = \pm(X_2 + Y_2) = \pm 2^k$ 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. 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 . Since p does not divide $X_i + Y_i$ for $1 \leq i \leq 2$, i.e. $X_i \not\equiv -Y_i \pmod{p}$, it follows that $X_i \equiv Y_i \pmod{p}$. Since $X_1 \equiv \pm X_2 \pmod{p}$ and $X_1 + Y_1 = X_2 + Y_2$, it follows that $X_1 \equiv X_2 \pmod{p}$ and the claim is proved. 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

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

It now follows from Lemma 3.6 that at least two of X_1, Y_1, X_2, Y_2 are equal. This contradiction concludes the proof. \square

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

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

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

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

Claim. *Each class mod d contains at most 2 elements of $\text{num}(\text{Per}(\varphi_c))$.*

Assume the contrary. Then there are three distinct elements X, Y, Z in $\text{num}(\text{Per}(\varphi_c))$ such that $X \equiv Y \equiv Z \pmod{d}$. 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 3 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 $X_i \equiv Y_i \pmod{d}$ 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. \square

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 $c \in \mathbb{Q}$ 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. \square

3.3. Numerator dynamics. Let $c = a/d^2 \in \mathbb{Q}$ with a, d coprime integers. Closely related to the map φ_c is the map $d^{-1}\varphi_a: \mathbb{Q} \rightarrow \mathbb{Q}$. 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 φ_c in \mathbb{Q} give rise, by taking numerators, to cycles of $d^{-1}\varphi_a$ in \mathbb{Z} .

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 φ_c . Then $\text{num}(\mathcal{C}) \subset \mathbb{Z}$ is a cycle of $d^{-1}\varphi_a$ of length $|\mathcal{C}|$.*

Proof. Recall that $\text{den}(\mathcal{C}) = \{d\}$ by Proposition 2.1. Let $x \in \mathcal{C}$ and $y = \varphi_c(x)$. Let $X = \text{num}(x), Y = \text{num}(y)$. Then $x = X/d, Y = y/d$. We have $y = x^2 - c = (X^2 - a)/d^2$. Hence $Y = (X^2 - a)/d = d^{-1}\varphi_a(X)$. In particular, we have the formula

$$(6) \quad (d^{-1}\varphi_a)(X) = d\varphi_c(X/d)$$

for all $X \in \text{num}(\mathcal{C})$. \square

3.4. The cases $d \not\equiv 0 \pmod{3}$ or $\pmod{5}$.

Lemma 3.13. *Let $c \in \mathbb{Q}$ and $\mathcal{C} \subseteq \text{Per}(\varphi_c)$ a cycle of positive length n .*

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

(ii) *If $d \not\equiv 0 \pmod{5}$ and $n \geq 4$, then $\text{num}(\mathcal{C})$ reduces mod 5 to exactly one or two nonzero elements mod 5.*

Proof. First some preliminaries. Of course φ_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

$$d^{-1}\varphi_a: \text{num}(\mathcal{C}) \rightarrow \text{num}(\mathcal{C}).$$

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 $d \not\equiv 0 \pmod{q}$. Then

$$(7) \quad X + Y \not\equiv 0 \pmod{q}.$$

Since d is invertible mod q , we may consider the reduced map

$$(8) \quad f = \pi_q \circ (d^{-1}\varphi_a): \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z},$$

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 (7) 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 $d \not\equiv 0 \pmod{q}$ 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 $u \in \{\pm 1\}$. Since $n \geq 3$, 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 $d \not\equiv 0 \pmod{q}$ where $q = 5$. Since $n \geq 4$ and the n -sequence $\pi_5(\text{num}(\mathcal{C}))$ contains at most one 0, it must contain three cyclically consecutive nonzero elements $u_1, u_2, u_3 \in \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$. Since that set contains at most two pairwise non-opposite 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. \square

Example 3.14. Consider the case $c = a/d^2 = 29/16$ of Example 1.2, where φ_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 since $n = 3$, and it would fail anyway since $\text{num}(\mathcal{C})$ 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 $d \not\equiv 0 \pmod{3}$. Let $s = |\text{supp}(d)|$. For every rational cycle \mathcal{C} of φ_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 $X_2 + Y_2 = -2$. Since $d \not\equiv 0 \pmod{3}$, Lemma 3.13 implies that X_1, X_2, Y_1, Y_2 reduce to the same nonzero element $u \pmod{3}$. This contradicts the equality $X_1 + Y_1 = -(X_2 + Y_2)$. \square

Theorem 3.16. *If $\text{den}(c)$ admits at most two distinct prime factors, then φ_c satisfies the Flynn-Poonen-Schaefer conjecture.*

Proof. Let \mathcal{C} be a rational cycle of φ_c 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 3.15, we have $|\text{Per}(\varphi_c)| \leq 2^1 + 1 = 3$ and $|\mathcal{C}| \leq 3$. See also [3].

- Assume now $s = 2$. Then $d = 2^{2r_1}p^{r_2}$ where p is an odd prime. By Theorem 3.9, we have $|\mathcal{C}| \leq |\text{Per}(\varphi_c)| \leq 6$. By Theorems 1.3 and 1.4, we have $|\mathcal{C}| \neq 4, 5$. It remains to show $|\mathcal{C}| \neq 6$. We distinguish two cases. If $p \neq 3$, then $|\mathcal{C}| \leq 2^2 + 1 = 5$ by Corollary 3.15 and we are done. Assume now $p = 3$, so that $d = 2^{2r_1}3^{r_2}$. Let m denote the number of classes of $\text{num}(\mathcal{C}) \pmod{q} = 5$. It follows from Lemma 3.13 that $m \leq 2$. Since the order of every element in $(\mathbb{Z}/5\mathbb{Z})^*$ belongs to $\{1, 2, 4\}$, it follows from Zieve's Theorem 2.11 that $|\mathcal{C}|$ is a power of 2. Hence $|\mathcal{C}| \in \{1, 2, 4\}$ and we are done. \square

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] G. Call and S. Goldstine, Canonical heights on projective space. J. Number Theory **63** (1997) 211–243.
- [3] S. Eliahou and Y. Fares, Poonen's conjecture and Ramsey numbers. Discrete Applied Mathematics **209** (2016) 102–106.
- [4] S. Eliahou and Y. Fares, On the iteration over \mathbb{R} of rational quadratic polynomials. (Preprint)
- [5] 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.
- [6] P. Morton, Arithmetic properties of periodic points of quadratic maps. Acta Arith. **62** (1992) 343–372.
- [7] D. Northcott, Periodic points on an algebraic variety. Annals of Math. **52** (1950) 167–177.
- [8] B. Poonen, The classification of rational preperiodic points of quadratic polynomials over \mathbb{Q} : a refined conjecture. Math. Z. **228** (1998) 11–29.
- [9] J. H. Silverman, The arithmetic of dynamical systems, volume 241 of Graduate texts in mathematics. Springer-Verlag, 2007.
- [10] M. Stoll, Rational 6-cycles under iteration of quadratic polynomials. LMS J. Comput. Math. **11** (2008) 367–380.

- [11] R. Walde and P. Russo, Rational periodic points of the quadratic function $Q_c = x^2 + c$. The Amer. Math. Monthly **101** (1994) 318–331.
- [12] M. Zieve, Cycles of Polynomial Mappings, Ph.D. thesis, UC Berkeley, 1996.

SHALOM ELIAHOU, UNIV. LITTORAL CÔTE D'OPALE, EA 2597 - LMPA -
 LABORATOIRE DE MATHÉMATIQUES PURES ET APPLIQUÉES JOSEPH LIOUVILLE,
 F-62228 CALAIS, FRANCE AND CNRS, FR 2956, FRANCE
E-mail address: eliahou@univ-littoral.fr

YOUSSEF FARES, LAMFA, CNRS-UMR 7352, UNIVERSITÉ DE PICARDIE,
 80039 AMIENS, FRANCE
E-mail address: youssef.fares@u-picardie.fr