ON THE ITERATIONS OF CERTAIN MAPS \( x \mapsto k \cdot (x + x^{-1}) \)
OVER FINITE FIELDS OF ODD CHARACTERISTIC

S. UGOLINI

Abstract. In this paper we describe the dynamics of certain rational maps of the form \( k \cdot (x + x^{-1}) \) over finite fields of odd characteristic.

1. Introduction

The dynamics of rational maps over finite fields has drawn the attention of some investigators over the last years. Our first work in this area was [6], where we studied the iterations of the map \( \vartheta(x) = x + x^{-1} \) over finite fields of characteristic two relying upon the relation between \( \vartheta \) with an endomorphism over Koblitz curves.

After this first work we attempted at a possible description of the dynamics of \( \vartheta \) over finite fields of odd characteristic. In general it seems that the behaviour of the map \( \vartheta \) over finite fields of odd characteristic is chaotic. Notwithstanding, there are two remarkable exceptions. In [7] we gave a complete description of the dynamics of \( \vartheta \) over finite fields of characteristic three and five, being in characteristic three the map \( \vartheta \) conjugated with the square map and in characteristic five related to an endomorphism of the elliptic curve with equation \( y^2 = x^3 + x \).

In this paper we address the problem of studying the iterations of certain rational maps which are obtained by a slight modification of the map \( \vartheta \), namely maps of the form \( k \cdot (x + x^{-1}) \), where \( k \) is a non-zero element of a prime field.

If \( p \) is an odd prime and \( q \) is a \( p \)-power, then, for any \( k \in F_p^* \), we can define a map \( \vartheta_k \) over the projective line \( \mathbb{P}^1(F_q) = F_q \cup \{\infty\} \) as follows:

\[
\vartheta_k : x \mapsto \begin{cases} 
\infty & \text{if } x \in \{0, \infty\}, \\
 k \cdot (x + x^{-1}) & \text{otherwise.}
\end{cases}
\]

As in [6] and [7] it is possible to associate a directed graph \( G_{\vartheta_k}^q \) with the map \( \vartheta_k \) over the finite field \( F_q \). More precisely, we can label each node of \( G_{\vartheta_k}^q \) by an element of \( \mathbb{P}^1(F_q) \) and connect with an arrow the nodes \( \alpha \) and \( \beta \) if \( \beta = \vartheta_k(\alpha) \). We say that an element \( \gamma \) of \( G_{\vartheta_k}^q \) is \( \vartheta_k \)-periodic if \( \vartheta_k^l(\gamma) = \gamma \) for some positive integer \( l \). Moreover, we notice that an element \( \gamma \) which is not \( \vartheta_k \)-periodic is pre-periodic, since \( \vartheta_k^l(\gamma) \) is periodic for some positive integer \( s \).

We can notice some properties of the digraph \( G_{\vartheta_k}^q \):

- the indegree of a node \( \beta \) of any \( G_{\vartheta_k}^q \) can be 0, 1 or 2. In fact, if \( \beta \in F_q \), then there exists \( \alpha \in F_q \) such that \( \vartheta_k(\alpha) = \beta \) if and only if there exists a root \( \alpha \) in \( F_q \) of the quadratic polynomial \( p_k(x) = kx^2 - \beta x + k \). In particular, we notice that the indegree of \( \beta \) is 1 exactly for \( \beta = \pm 2k \), since the discriminant of \( p_k \) is \( \beta^2 - 4k^2 \);
- any connected component of \( G_{\vartheta_k}^q \) is formed by a cycle, whose elements can be viewed as roots of reverse binary trees.

Key words and phrases. Dynamical systems, finite fields, arithmetic dynamics, elliptic curves.
Constructing some digraphs $G_\theta^q$, one can notice that their structure is not particularly symmetric. Nonetheless, they present remarkable symmetries when $k$ falls into one of the following three cases.

1. Case 1: $k \equiv \pm \frac{1}{2}$ (mod $p$).
2. Case 2: $k$ is a root of the polynomial $x^2 + \frac{1}{2} \in \mathbb{F}_p[x]$, being $p \equiv 1 \pmod{4}$;
3. Case 3: $k$ is a root of the polynomial $x^2 + \frac{1}{2}x + \frac{1}{2} \in \mathbb{F}_p[x]$, being $p \equiv 1, 2,$
or $4 \pmod{7}$.

The just mentioned maps generalize, for different reasons, our previous works [6] and [7]. More precisely, the map $\vartheta$ belongs to the family of maps dealt with in case 1. As regards the map $\vartheta$ defined on $\mathbb{P}^1(\mathbb{F}_q)$, the iterations of this latter map can be studied considering that $\vartheta$ is conjugated to the square map. Indeed,

\[
\vartheta_1 = \psi \circ s_2 \circ \psi,
\]

where $s_2$ and $\psi$ are maps defined on $\mathbb{P}^1(\mathbb{F}_q)$ as follows:

\[
s_2(x) = \begin{cases} x^2 & \text{if } x \in \mathbb{F}_q, \\ \infty & \text{if } x = \infty, \end{cases} \quad \psi(x) = \begin{cases} \frac{x + 1}{x - 1} & \text{if } x \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{1, \infty\}, \\ 1 & \text{if } x = \infty, \\ \infty & \text{if } x = 1. \end{cases}
\]

As regards the map $\vartheta_{-\frac{1}{2}}$, the iterations of this latter map can be studied considering that

\[
\vartheta_{-\frac{1}{2}} = \psi \circ s_{-2} \circ \psi,
\]

where $s_{-2}$ is the map defined on $\mathbb{P}^1(\mathbb{F}_q)$ as follows:

\[
s_{-2}(x) = \begin{cases} x^{-2} & \text{if } x \in \mathbb{F}_q^*, \\ 0 & \text{if } x = \infty, \\ \infty & \text{if } x = 0. \end{cases}
\]

We state now a result about $\vartheta_{\frac{1}{2}}$-periodic and $\vartheta_{-\frac{1}{2}}$-periodic elements.

**Lemma 2.1.** The following hold.

- The elements 1 and $-1$ are $\vartheta_{\frac{1}{2}}$-periodic and form two cycles of length 1 each.
- The elements 1 and $-1$ are $\vartheta_{-\frac{1}{2}}$-periodic and form a cycle of length 2.
- The element $\infty$ is $\vartheta_{\frac{1}{2}}$-periodic and $\vartheta_{-\frac{1}{2}}$-periodic of period 1.
- An element $\alpha \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{-1, 1, \infty\}$ is $\vartheta_{\frac{1}{2}}$-periodic (resp. $\vartheta_{-\frac{1}{2}}$-periodic) of period $l$ if and only if $\psi(\alpha)$ is $s_2$-periodic (resp. $s_{-2}$-periodic) of period $l$. Moreover, the integer $l$ is equal to the multiplicative order $\text{ord}_d(2)$ of 2.
(resp. \( \text{ord}_d(-2) \) of \(-2\)) in \((\mathbb{Z}/d\mathbb{Z})^*\), where \(d\) is the odd multiplicative order of \(\psi(\alpha)\) in \(\mathbb{F}_q^*\).

**Proof.** The proof is the same as the proof of Lemma 2.1 in [7] once one replaces all occurrences of \(3^n, k, \vartheta\) with \(p^n, l\) and \(\vartheta_{\frac{1}{2}}\) (resp. \(\vartheta_{-\frac{1}{2}}\)). \(\square\)

The forthcoming theorems furnish a description of the number and the length of the cycles of the graphs \(G_{\vartheta_{\frac{1}{2}}}^q\) and \(G_{\vartheta_{-\frac{1}{2}}}^q\) respectively.

**Theorem 2.2.** Let \(D = \{d_1, \ldots, d_m\}\) be the set of the distinct odd integers greater than 1 which divide \(q - 1\). Denote by \(\text{ord}_d(2)\) the multiplicative order of 2 in \((\mathbb{Z}/d\mathbb{Z})^*\). Consider the set
\[
L = \{\text{ord}_d(2) : 1 \leq i \leq m\} = \{l_1, \ldots, l_r\}
\]
of cardinality \(r\), where \(r \leq m\), and the map
\[
l : D \rightarrow L, \quad d_i \mapsto \text{ord}_d(2).
\]
Then:
- \(L \cap \{1\} = \emptyset\);
- the length of a cycle in \(G_{\vartheta_{\frac{1}{2}}}^q\) is a positive integer belonging to \(L \cup \{1\}\);
- in \(G_{\vartheta_{-\frac{1}{2}}}^q\) there are exactly three cycles of length 1 formed respectively by 1, \(-1\) and \(\infty\);
- for any \(k\) such that \(1 \leq k \leq r\) there are
\[
c_k = \frac{1}{l_k} \sum_{d_i \in \mathcal{L}_{l_k}} \varphi(d_i)
\]
cycles of length \(l_k\) in \(G_{\vartheta_{\frac{1}{2}}}^q\), being \(\varphi\) the Euler’s totient function;
- the number of connected components of \(G_{\vartheta_{\frac{1}{2}}}^q\) is
\[
3 + \sum_{k=1}^r c_k.
\]
**Proof.** We notice that \(L \cap \{1\} = \emptyset\), since \(\text{ord}_d(2) \geq 2\), being \(d_i \geq 3\) for any \(i\). According to Lemma 2.1 the elements 1, \(-1\) and \(\infty\) are \(\vartheta_{\frac{1}{2}}\)-periodic of period 1. The proof of the remaining statements follows the same lines as the proof of Theorem 2.2 in [7], just replacing all occurrences of \(3^n, \vartheta\) by \(p^n, 2\) and \(\vartheta_{\frac{1}{2}}\) respectively. As regards the number of connected components of \(G_{\vartheta_{\frac{1}{2}}}^q\), we notice that there are \(\sum_{k=1}^r c_k\) connected components due to the cycles formed by the periodic elements of \(\mathbb{P}^1(\mathbb{F}_q) \setminus \{-1, 1, \infty\}\) and 3 more connected components due to the three cycles formed by 1, \(-1\) and \(\infty\). \(\square\)

**Theorem 2.3.** Let \(D = \{d_1, \ldots, d_m\}\) be the set of the distinct odd integers greater than 1 which divide \(q - 1\). Denote by \(\text{ord}_d(-2)\) the multiplicative order of \(-2\) in \((\mathbb{Z}/d\mathbb{Z})^*\). Consider the set
\[
L = \{\text{ord}_d(-2) : 1 \leq i \leq m\} = \{l_1, \ldots, l_r\}
\]
of cardinality \(r\), where \(r \leq m\), and the map
\[
l : D \rightarrow L, \quad d_i \mapsto \text{ord}_d(-2).
\]
Then:
• $L \cap \{2\} = \emptyset$;
• the length of a cycle in $G_q^\vartheta - \frac{1}{2}$ is a positive integer belonging to $L \cup \{1, 2\}$;
• the number of cycles of length 1 in $G_q^\vartheta - \frac{1}{2}$ is
  \[
  \begin{cases} 
  3, & \text{if } p \equiv 1 \pmod{3} \text{ or } 2 \mid n \text{ and } p \neq 3; \\
  1, & \text{otherwise}; 
  \end{cases}
  \]
• in $G_q^\vartheta - \frac{1}{2}$ there is exactly 1 cycle of length 2 formed by 1 and $-1$;
• for any integer $k$ such that $1 \leq k \leq r$ there are
cycles of length $l_k$ in $G_q^\vartheta - \frac{1}{2}$ formed by elements of $\mathbf{P}^1(F_q)\setminus\{-1, 1, \infty\}$, being $\varphi$ the Euler's totient function;
• the number of connected components of $G_q^\vartheta - \frac{1}{2}$ is
  \[
  2 + \sum_{k=1}^r c_k.
  \]

Proof. At first we notice that $2 \not\in L$. In fact, if $\text{ord}_q(-2) = 2$ for some odd integer $d > 1$, then $(-2)^2 \equiv 1 \pmod{d}$, which is possible only if $d = 3$. Since $\text{ord}_q(-2) = 1$, we conclude that $2 \not\in L$.

As regards the $\vartheta - \frac{1}{2}$-periodic elements of period 1, we notice that $\infty$ is $\vartheta - \frac{1}{2}$-periodic of period 1 by definition. Moreover, an element $x \in F_q^*$ is $\vartheta - \frac{1}{2}$-periodic of period 1 if and only if $-\frac{1}{2}(x + x^{-1}) = x$, namely if and only if $x^{-1}(3x^2 + 1) = 0$. Therefore, $x \in F_q^*$ is $\vartheta - \frac{1}{2}$-periodic of period 1 if and only if $p \neq 3$ and $x$ is a square root of $-\frac{1}{2}$. Since $-\frac{1}{2}$ is a square in $F_q^*$ if and only if $p \equiv 1 \pmod{3}$ or $n$ is even and $p \neq 3$, the thesis follows. Moreover, being $2 \not\in L$, in $G_q^\vartheta - \frac{1}{2}$ there is exactly one cycle of length 2 formed by 1 and $-1$.

All the other assertions regarding the elements of $\mathbf{P}^1(F_q)\setminus\{-1, 1, \infty\}$ can be proved as in [7, Theorem 2.2], just replacing all occurrences of $3^n$ and $\vartheta$ by $p^n$ and $\vartheta - \frac{1}{2}$ respectively. The number of connected components of $G_q^\vartheta - \frac{1}{2}$ is equal to the sum of the number of cycles formed by the periodic elements of $\mathbf{P}^1(F_q)\setminus\{-1, 1, \infty\}$, the cycle formed by 1 and $-1$ and the cycle formed by $\infty$. $\square$

The following lemma generalizes Lemma 2.3 of [7] and its proof is the same, after the replacement of any occurrence of $3^n$, $s$ and $\vartheta$ by $p^n$, $s - 2$ and $\vartheta - \frac{1}{2}$ respectively.

Lemma 2.4. Let $2^e$, for some positive integer $e$, be the greatest power of 2 dividing $q - 1$. Let $\gamma \in F_q$ be a non-$\vartheta - \frac{1}{2}$-periodic element (in particular $\gamma \not\in \{1, -1\}$). Then, $\vartheta - \frac{1}{2}(x) = \gamma$ for exactly two distinct elements $x \in F_q$, provided that $\text{ord}(\psi(\gamma)) \not\equiv 0 \pmod{2^e}$, where $\text{ord}(\psi(\gamma))$ is the multiplicative order of $\psi(\gamma)$ in $F_q^*$. If, on the contrary, $\text{ord}(\psi(\gamma)) \equiv 0 \pmod{2^e}$, then there is no $x \in F_q$ such that $\vartheta - \frac{1}{2}(x) = \gamma$.

The adapted version of Lemma 2.4 reads as follows.

Lemma 2.5. Let $2^e$, for some positive integer $e$, be the greatest power of 2 dividing $q - 1$. Let $\gamma \in F_q$ be a non-$\vartheta - \frac{1}{2}$-periodic element (in particular $\gamma \not\in \{1, -1\}$). Then, $\vartheta - \frac{1}{2}(x) = \gamma$ for exactly two distinct elements $x \in F_q$, provided that $\text{ord}(\psi(\gamma)) \not\equiv 0 \pmod{2^e}$, where $\text{ord}(\psi(\gamma))$ is the multiplicative order of $\psi(\gamma)$ in $F_q^*$. If, on the contrary, $\text{ord}(\psi(\gamma)) \equiv 0 \pmod{2^e}$, then there is no $x \in F_q$ such that $\vartheta - \frac{1}{2}(x) = \gamma$. 

Proof. We observe that \( \vartheta_{-\frac{1}{2}}(-1) = -1 \), \( \vartheta_{\frac{1}{2}}(1) = 1 \) and \( \vartheta_{\frac{1}{2}}(0) = \infty \). Therefore, if \( \vartheta_{\pm\frac{1}{2}}(x) = \gamma \) as in the hypotheses, then \( x \not\in \{-1,0,1\} \). The remaining assertions can be proved as in the proof of Lemma 2.3 of \cite{7}, replacing any occurrence of \( 3^n \), \( s \), \( -2 \) and \( \vartheta \) by \( p^n \), \( s_2 \), \( 2 \) and \( \vartheta_{\pm\frac{1}{2}} \) respectively. \( \square \)

The following theorem is a generalization of Theorem 2.4 of \cite{7}.

**Theorem 2.6.** Let \( \alpha \in \mathbb{P}_1(F_q) \) be a \( \vartheta_{\pm\frac{1}{2}} \)-periodic (resp. \( \vartheta_{-\frac{1}{2}} \)-periodic) element. If \( \alpha \in \{-1,1\} \), then \( \alpha \) is not root of any tree in \( G^q_{\vartheta_{\pm\frac{1}{2}}} \) (resp. \( G^q_{\vartheta_{-\frac{1}{2}}} \)). If \( \alpha \not\in \{1,-1\} \), then \( \alpha \) is the root of a reversed binary tree of depth \( e \) in \( G^q_{\vartheta_{\pm\frac{1}{2}}} \) (resp. \( G^q_{\vartheta_{-\frac{1}{2}}} \)), where \( 2^e \) is the greatest power of \( 2 \) which divides \( q - 1 \). In particular:

- there are \( 2^{k-1} \) vertices at any level \( 1 \leq k \leq e \) of the tree;
- the root has one child and all the other vertices at any level \( 0 < k < e \) have two children;
- if \( \beta \in F_q \) belongs to the level \( k > 0 \) of the tree rooted at \( \alpha \), then \( 2^k \) is the greatest power of \( 2 \) dividing \( \text{ord}(\psi(\beta)) \).

**Proof.** Firstly we notice that no tree grows on \( 1 \) and \( -1 \), since

\[
\begin{align*}
\vartheta_{\pm\frac{1}{2}}(x) = 1 & \iff x^2 \mp 2x + 1 = 0 \iff (x \mp 1)^2 = 0; \\
\vartheta_{\pm\frac{1}{2}}(x) = -1 & \iff x^2 \pm 2x + 1 = 0 \iff (x \pm 1)^2 = 0.
\end{align*}
\]

All other assertions can be proved as in the proof of Theorem 2.4 of \cite{7} replacing all occurrences of \( 3^n \), \( \vartheta \) and \( s \) by \( p^n \), \( \vartheta_{\pm\frac{1}{2}} \) (resp. \( \vartheta_{-\frac{1}{2}} \)) and \( s_2 \) (resp. \( s_{-2} \)) respectively. \( \square \)

**Example 2.7.** Hereafter the graph \( G^{29}_{\vartheta_{-\frac{1}{2}}} \) is represented. The vertex numbering refers to the exponents \( k \) of the powers \( \alpha^k \), where \( \alpha \) is the root of the Conway polynomial \( x - 2 \in F_{29}[x] \).

We notice that \( q = 29 \) and \( q - 1 = 2^2 \cdot 7 \). According to the notation of Theorem 2.2, \( D = \{7\} \) and \( \text{ord}_2(-2) = 6 \). This implies that there exists \( \frac{1}{6} \cdot \varphi(7) = 1 \) cycle of length 6. According to the same theorem the elements 1 and \( -1 \) (which here are denoted by 0 and 14) form a cycle of length 2, while \( \infty \) forms a cycle of length 1. Moreover, being \( e = 2 \) according to the notation of Theorem 2.3 any cyclic element different from 1 and \( -1 \) is root of a binary tree of depth 2.
Example 2.8. In this example the graph of $G^{7^2}_{-1/2}$ is represented. The vertex numbering refers to the exponents $k$ of the powers $\alpha^k$, where $\alpha$ is a root of the Conway polynomial $x^2 - 2x + 3 \in \mathbb{F}_7[x]$.

We note that $q = 7^2$ and $q - 1 = 2^4 \cdot 3$. According to the notation of Theorem 2.2, $D = \{3\}$ and $\text{ord}_3(-2) = 1$. This implies that there exist $\frac{1}{1} \cdot \varphi(3) = 2$ cycles of length $1$ due to the elements of order $3$ in $\mathbb{F}_{49}^*$. According to the same theorem, the elements $1$ and $-1$ (which here are denoted by $0$ and $24$) form a cycle of length $2$, while $\infty$ forms a cycle of length $1$. Moreover, being $e = 4$ according to the notation of Theorem 2.6, any cyclic element different from $1$ and $-1$ is root of a binary tree of depth $4$.

3. Case 2: $k^2 \equiv -\frac{1}{4} \pmod{p}$ with $p \equiv 1 \pmod{4}$

The starting point for this and the following section is [5], Proposition 2.3.1. From (i) of the proposition one can deduce that the endomorphism ring of the elliptic curve $y^2 = x^3 + x$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}[i]$. In particular, the curve possesses an endomorphism $[\alpha]$ of degree $2$, which takes a point $(x, y)$ of the curve to

$$[\alpha](x, y) = \left(\alpha^{-2} \left(x + \frac{1}{x}\right), \alpha^{-3} y \left(1 - \frac{1}{x^2}\right)\right),$$

where $\alpha = 1 + \sqrt{-1}$

Let $p$ be an odd prime such that $p \equiv 1 \pmod{4}$. The elliptic curve with equation $y^2 = x^3 + x$ over $\mathbb{Q}$ has good reduction modulo $p$ (see [4], Chapter V, Proposition 5.1 or [3], page 59) and from now on we will denote by $E$ its reduction modulo $p$.

The quadratic equation

$$x^2 - 2x + 2 = 0$$

(3.1)
admits two distinct roots in \( F_p \), since its discriminant is equal to \(-4\), which is a quadratic residue in \( F_p \). Denote by \( \alpha_{\omega} \) and \( \alpha_{\overline{\omega}} \) the roots of \( \Delta \) in \( F_p \), set \( k_{\omega} = \alpha_{\omega}^{-2} \) and \( k_{\overline{\omega}} = \alpha_{\overline{\omega}}^{-2} \). We notice in passing that \( k_{\omega}^2 \equiv k_{\overline{\omega}}^2 \equiv -\frac{1}{4} \pmod{p} \) and \( k_{\omega} \equiv -k_{\overline{\omega}} \pmod{p} \).

Fixed a positive integer \( n \) we want to study the iterations over \( P^1(F_{p^n}) \) of the maps \( \vartheta_{k_{\omega}} \), for \( \sigma \in \{\omega, \overline{\omega}\} \).

The two maps

\[
e_{k_{\omega}}(x, y) = \left( k_{\omega} \cdot \left( \frac{x^2 + 1}{x}, \frac{k_{\omega}}{\alpha_{\omega}} \cdot y \cdot \frac{x^2 - 1}{x^2} \right) \right),
\]

\[
e_{k_{\overline{\omega}}}(x, y) = \left( k_{\overline{\omega}} \cdot \left( \frac{x^2 + 1}{x}, \frac{k_{\overline{\omega}}}{\alpha_{\overline{\omega}}} \cdot y \cdot \frac{x^2 - 1}{x^2} \right) \right)
\]

are endomorphisms of the elliptic curve

\[E : y^2 = x^3 + x\]

over \( F_p \). Hence, we can study the iterations of the maps \( \vartheta_{k_{\omega}} \) and \( \vartheta_{k_{\overline{\omega}}} \) taking into account the fact that

\[
e_{k_{\omega}}(x, y) = \left( \vartheta_{k_{\omega}}(x), \frac{k_{\omega}}{\alpha_{\omega}} \cdot y \cdot \frac{x^2 - 1}{x^2} \right),
\]

\[
e_{k_{\overline{\omega}}}(x, y) = \left( \vartheta_{k_{\overline{\omega}}}(x), \frac{k_{\overline{\omega}}}{\alpha_{\overline{\omega}}} \cdot y \cdot \frac{x^2 - 1}{x^2} \right).
\]

Since the endomorphism ring of the elliptic curve defined by \( y^2 = x^3 + x \) over \( Q \) is isomorphic to \( Z[i] \), according to \( [2] \), Chapter 13, Theorem 12 the endomorphism ring \( \text{End}(E) \) of \( E \) over \( F_p \) is also isomorphic to \( R = Z[i] \), which is an Euclidean ring with euclidean function

\[N(a + bi) = a^2 + b^2,\]

for any arbitrary choice of \( a, b \) in \( Z \).

By \( [8] \), Theorem 2.3(a), there exists an isomorphism

\[\psi_n : E(F_{p^n}) \rightarrow R/(\pi_p^n - 1)R,\]

where \( \pi_p \) is the Frobenius endomorphism. Theorem 2.4 of \( [8] \) furnishes a representation of \( \pi_p \) as an element of \( R \), namely

\[\pi_p = \frac{p + 1 - m + \sqrt{d}}{2},\]

where

\[m = |E(F_p)|,\]

\[d = (p + 1 - m)^2 - 4p.\]

Moreover, \( 2 = e_{k_{\omega}} \circ e_{k_{\overline{\omega}}} \), being 2 the duplication map over the curve \( E \). Since in \( R \) we have that \( 2 = \alpha \cdot \overline{\alpha} \), the endomorphisms \( e_{k_{\omega}} \) and \( e_{k_{\overline{\omega}}} \) are represented in \( R \) by \( \alpha \) and \( \overline{\alpha} \).

Fix once for the remaining part of the current section \( \sigma = \omega \) or \( \sigma = \overline{\omega} \). Before studying the structure of the graph \( G_{n}^{\sigma} \) we partition \( P^1(F_{p^n}) \) as follows.

1. If \( n \) is odd and \( p \equiv \pm 3 \pmod{8} \), then we define

\[A_n = \{ x \in F_{p^n} : (x, y) \in E(F_{p^n}) \text{ for some } y \in F_{p^n} \} \cup \{\infty\};\]

\[B_n = \{ x \in F_{p^n} : (x, y) \in E(F_{p^n}) \text{ for some } y \in F_{p^n} \setminus F_{p^n} \} \setminus \{1, -1\};\]

\[C_n = \{1, -1\}.\]
(2) If \( n \) is even or \( n \) is odd and \( p \equiv \pm 1 \pmod{8} \), then we define
\[
A_n = \{ x \in \mathbb{F}_p^n : (x, y) \in E(\mathbb{F}_p^n) \text{ for some } y \in \mathbb{F}_p^n \} \cup \{ \infty \};
\]
\[
B_n = \{ x \in \mathbb{F}_p^n : (x, y) \in E(\mathbb{F}_p^n) \text{ for some } y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p^n \}.
\]

We notice that in both cases \( A_n \cap B_n = \emptyset \). Moreover, the sets \( A_n \) and \( C_n \) satisfy the following properties.

**Lemma 3.1.** The following hold.

- If \( n \) is odd and \( p \equiv \pm 3 \pmod{8} \), then \( A_n \cap C_n = \emptyset \).
- If \( n \) is even or \( n \) is odd and \( p \equiv \pm 1 \pmod{8} \), then \( \{1, -1\} \subseteq A_n \).

**Proof.** From the equation \( y^2 = x^3 + x \) we get that
\[
1 \in A_n \iff 2 \text{ is a square in } \mathbb{F}_p^n;
\]
\[
-1 \in A_n \iff -2 \text{ is a square in } \mathbb{F}_p^n.
\]

We note that 2 is a square in \( \mathbb{F}_p \) if and only if \( \left( \frac{2}{p} \right) = 1 \), while -2 is a square in \( \mathbb{F}_p \) if and only if \( \left( \frac{-2}{p} \right) = 1 \). Since \( p \equiv 1 \pmod{4} \), we get that
\[
\left( \frac{2}{p} \right) = \left( \frac{-2}{p} \right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}
\]

Therefore, 2 and -2 are squares in \( \mathbb{F}_p \) if and only if \( p \equiv \pm 1 \pmod{8} \). In the other cases, the equations \( y^2 = \pm 2 \) have solutions in \( \mathbb{F}_{p^2} \). Since \( \mathbb{F}_{p^2} \subseteq \mathbb{F}_p^n \) if and only if \( 2 \mid n \), the thesis follows. \( \square \)

The following lemmas hold.

**Lemma 3.2.** Let \( \tilde{x} \in \mathbb{F}_{p^n} \). Then, in \( E(\mathbb{F}_{p^n}) \) there are exactly two rational points, \((\tilde{x}, \tilde{y})\) and \((\tilde{x}, -\tilde{y})\), with such an \( x \)-coordinate except for
\[
\tilde{x} \in \{0, i_p, -i_p\},
\]
where \( i_p \) and \( -i_p \) are the two square roots of -1 in \( \mathbb{F}_p \), in which case \( \tilde{y} = 0 \) and \( \tilde{x} \) is not \( \vartheta_{k_a} \)-periodic.

**Proof.** The thesis is immediate if we notice that the equation \( y^2 = \tilde{x}^3 + \tilde{x} \) has exactly two distinct roots \( y_1 \) and \( y_2 \) in \( \mathbb{F}_{p^2} \) unless \( \tilde{x}^3 + \tilde{x} = 0 \). As regards the last statement, we notice that \( \vartheta_{k_a} (\pm i_p) = 0 \) and \( \vartheta_{k_a} (0) = \infty \). Hence, none of the three points having \( y \)-coordinate equal to 0 is \( \vartheta_{k_a} \)-periodic. \( \square \)

**Lemma 3.3.** The map \( \vartheta_{k_a} \) takes the elements of \( A_n \) to \( A_n \), the elements of \( B_n \) to \( B_n \) and the elements of \( C_n \) to \( A_n \).

**Proof.** If \( \tilde{x} = \infty \), then \( \vartheta_{k_a}(\tilde{x}) = \infty \). If \( \tilde{x} \in A_n \setminus \{\infty\} \), then there exists \( \tilde{y} \in \mathbb{F}_{p^n} \) such that \((\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \). Therefore, \( \vartheta_{k_a}(\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \) and \( \vartheta_{k_a}(\tilde{x}) \in A_n \).

If \( \tilde{x} \in B_n \), then there exists \( \tilde{y} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_{p^n} \) such that \((\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^2}) \). We notice that \( \vartheta_{k_a}(\tilde{x}, y_j) \) and \( \vartheta_{k_a}(\tilde{x}, y_2) \), with
\[
y_j = \left( -1 \right)^j \frac{k_a}{\alpha_o} \cdot \tilde{y} \cdot \frac{\tilde{x}^2 - 1}{\tilde{x}^2}, \quad \text{for } j \in \{1, 2\},
\]
are the only rational points in \( E(\mathbb{F}_{p^2}) \) having \( \vartheta_{k_a}(\tilde{x}) \) as \( x \)-coordinate. Since \( y_j \in \mathbb{F}_{p^n} \) if and only if \( \tilde{x}^2 = 1 \), because \( \tilde{y} \notin \mathbb{F}_{p^n} \), and \( \{1, -1\} \notin B_n \), we conclude that \( \vartheta_{k_a}(\tilde{x}) \in B_n \).

As regards the elements of \( C_n \) we notice that
\[
\vartheta_{k_a}(\pm 1) = \pm 2k_a \in \{ \pm i_p \} \subseteq A_n.
\]
\( \square \)
According to Lemma 3.3, we can study the iterations of \( \vartheta_{k_n} \) on \( \mathbf{P}^1(\mathbf{F}_{p^n}) \) separately on the elements of \( A_n \) and \( B_n \). Let us firstly define

\[
\rho_n = \begin{cases} 
\alpha, & \text{if } \alpha^{-2} \equiv k_\sigma \pmod{\pi_p}; \\
\overline{\alpha}, & \text{if } \overline{\alpha}^{-2} \equiv k_\sigma \pmod{\pi_p}.
\end{cases}
\]

Since \( E(\mathbf{F}_{p^n}) \) is isomorphic to \( R/(\pi_p^n - 1)R \) via the isomorphism given by \( \psi_n \), the iterations of \( \vartheta_{k_n} \) on \( A_n \) can be studied relying upon the iterations of \( [\rho_0] \) in \( R/(\pi_p^n - 1)R \).

Now we define

\[
E(\mathbf{F}_{p^n})_{B_n} = \{(x, y) \in E(\mathbf{F}_{p^n}) : x \in B_n\}
\]

and denote by \( \lambda, \tau \) two elements of \( \mathbf{F}_{p^n} \) such that

\[
(\pm \lambda)^2 = 2; \\
(\pm \tau)^2 = -2.
\]

If \( n \) is odd and \( p \equiv \pm 3 \pmod{8} \), then we define

\[
E(\mathbf{F}_{p^n})_{B_n} = \{O, (0, 0), (\pm i, 0), (1, \pm \lambda), (-1, \pm \tau)\}.
\]

In all other cases we define

\[
E(\mathbf{F}_{p^n})_{B_n} = \{O, (0, 0), (\pm i, 0)\}.
\]

In both cases \( O \) denotes the point at infinity.

The following holds.

**Lemma 3.4.** Let \( \tilde{x} \in \mathbf{F}_{p^n} \) and \( P = (\tilde{x}, \tilde{y}) \in E(\mathbf{F}_{p^n}) \). We have that \( (\pi_p^n + 1)P = O \) if and only if \( P \in E(\mathbf{F}_{p^n})_{B_n} \cup E(\mathbf{F}_{p^n})^*_{B_n} \).

**Proof.** Suppose that \( (\pi_p^n + 1)P = O \). If \( \tilde{y} = 0 \), then \( P \in E(\mathbf{F}_{p^n})_{B_n} \). Suppose on the contrary that \( \tilde{y} \neq 0 \). Since \( \tilde{y} \in \mathbf{F}_{p^n} \) only if \( \tilde{y}^n = \tilde{y} \) and by hypothesis \( \tilde{y}^n = -\tilde{y} \), it follows that \( \tilde{y} \in \mathbf{F}_{p^n} \) only if \( \tilde{y} = -\tilde{y} \), namely only if \( 2\tilde{y} = 0 \). Since \( \tilde{y} \neq 0 \), we conclude that \( \tilde{y} \in \mathbf{F}_{p^n} \setminus \mathbf{F}_{p^n} \). In this latter case \( P \in E(\mathbf{F}_{p^n})_{B_n} \), unless \( n \) is odd, \( p \equiv \pm 3 \pmod{8} \) and \( \tilde{x} \in \{1, -1\} \), in which case \( P \in E(\mathbf{F}_{p^n})_{B_n} \).

Vice versa, suppose that \( P \in E(\mathbf{F}_{p^n})_{B_n} \). Then, \( \pi_p^n(P) = (x, y^n) \) and \( y^n \neq y \), since \( y \in \mathbf{F}_{p^n} \setminus \mathbf{F}_{p^n} \). Therefore, \( \pi_p^n(P) = -P \). Finally, if \( P \in E(\mathbf{F}_{p^n})^*_{B_n} \), then we can check by direct computation that \( (\pi_p^n + 1)P = O \). \( \square \)

With the notation till now introduced and in virtue of Lemma 3.4, we can say that there exists an isomorphism

\[
\tilde{\psi}_n : E(\mathbf{F}_{p^n})_{B_n} \cup E(\mathbf{F}_{p^n})^*_{B_n} \rightarrow R/(\pi_p^n + 1)R.
\]

Hence, the iterations of \( \vartheta_{k_n} \) on \( B_n \) can be studied by means of the iterations of \( [\rho_0] \) on \( R/(\pi_p^n + 1)R \).

Suppose that \( \pi_p - 1 \) (resp. \( \pi_p + 1 \)) factors in \( R \), up to units, as

\[
(3.2) \quad \rho_0^c \cdot \left( \prod_{i=1}^v p_i^{e_i} \right) \cdot \left( \prod_{i=v+1}^w r_i^{e_i} \right),
\]

where

1. any \( e_i \) is a non-negative integer, for \( 0 \leq i \leq w \);
2. \( N(\rho_0^c) = 2^c \);
3. for \( 1 \leq i \leq v \) the elements \( p_i \in \mathbf{Z} \) are distinct primes of \( R \) and \( N(p_i^{e_i}) = p_i^{2e_i} \);
4. for \( v + 1 \leq i \leq w \) the elements \( r_i \in R \setminus \mathbf{Z} \) are distinct primes of \( R \), different from \( \rho_0 \) and \( \overline{\rho}_0 \), and \( N(r_i^{e_i}) = p_i^{2e_i} \), for some rational integer \( p_i \) such that \( r_i r_i = p_i \).
For the sake of clarity we define, for $1 \leq i \leq w$,
\[
\rho_i = \begin{cases} p_i, & \text{if } 1 \leq i \leq v; \\ r_i, & \text{if } v + 1 \leq i \leq w. 
\end{cases}
\]
As a consequence of the factorization (3.2) the ring $R/(\pi_0^n - 1)R$ (resp. $R/(\pi_0^n + 1)R$) is isomorphic to
\[
(3.3) \quad S = \prod_{i=0}^{w} R/\rho_i^n R.
\]
As regards the additive structure of the quotient rings involved in (3.3), we notice the following.

- The additive group of $R/\rho_0^n R$ is cyclic of orders $2^{n_0}$. Hence, there are $\varphi(2^{n_0})$ elements in $R/\rho_0^n R$ of order $2^{n_0}$, for each integer $0 \leq h_0 \leq e_0$.

- For any $i \in \{1, \ldots, v\}$ the additive group of $R/\rho_i^n R$ is isomorphic to the direct sum of two cyclic groups of order $p_i^{e_i}$. This implies that, for each integer $0 \leq h_i \leq e_i$, there are $N_{h_i}$ elements in $R/\rho_i^n R$ of order $p_1^{h_i}$, where
\[
N_{h_i} = \begin{cases} 1, & \text{if } h_i = 0, \\ p_i^{2h_i} - p_i^{2(h_i-1)}, & \text{otherwise}. 
\end{cases}
\]

- For any $i \in \{v+1, \ldots, w\}$ the additive group of $R/\rho_i^n R$ is cyclic of order $p_i^{e_i}$. Hence, there are $\varphi(p_i^{h_i})$ elements in $R/\rho_i^n R$ of order $p_i^{h_i}$, for each integer $0 \leq h_i \leq e_i$.

If $(x, y)$ is a rational point of $E(F_{p^n})$ (resp. $E(F_{p^{2n}})_{B_n}$), then we write $P(x, y)$ for the image of $(x, y)$ in $S$.

Now we define the sets
\[
Z_i = \{0, 1, \ldots, e_i\}, \quad \text{for any } 0 \leq i \leq w
\]
and
\[
H = \prod_{i=0}^{w} Z_i.
\]
If $P = (P_0, P_1, \ldots, P_w) \in S$, then we define $h_i = (h_0^P, h_1^P, \ldots, h_w^P)$ in $H$ if

- $P_0$ has additive order $2^{n_0}$ in $R/\rho_0^n R$;

- each $P_i$, for $1 \leq i \leq w$, has additive order $p_i^{h_i}$ in $R/\rho_i^n R$.

Moreover, we define $o(P) = (o(P_0), o(P_1), \ldots, o(P_w))$, where $o(P_i)$ denotes, for any $0 \leq i \leq w$, the additive order of $P_i$ in $R/\rho_i^n R$.

The following two lemmas furnish a characterization of $\vartheta_{h_0}$-periodic elements.

**Lemma 3.5.** Let $\tilde{x} \in A_n$ (resp. $B_n$) be $\vartheta_{h_0}$-periodic. Then, one of the following holds:

- $\tilde{x} = \infty$;

- $\tilde{x}$ is the $x$-coordinate of a rational point $(\tilde{x}, \tilde{y}) \in E(F_{p^n})$ (resp. $E(F_{p^{2n}})_{B_n}$) such that $P(\tilde{x}, \tilde{y}) = (P_0, P_1, \ldots, P_w)$, where $P_0 = 0$.

**Proof.** If $\tilde{x} \in A_n \setminus \{\infty\}$ (resp. $B_n$), then $(\tilde{x}, \tilde{y}) \in E(F_{p^n})$ (resp. $E(F_{p^{2n}})_{B_n}$) for some $\tilde{y}$ in $F_{p^n}$ (resp. $F_{p^{2n}}$). Moreover, $[p_0]^l P(\tilde{x}, \tilde{y}) = \pm P(\tilde{x}, \tilde{y})$ for some positive integer $l$, namely $[p_0 + 1]P_0 = 0$. Since $p_0$ does not divide $p_0 + 1$ in $R$, we have that $P_0 = 0$. \qed

**Lemma 3.6.** Let $P = (P_0, P_1, \ldots, P_w)$ be a point in $S$ such that $P_0 = 0$ and denote by $l_i$, for any $0 \leq i \leq w$, the smallest among the positive integers $s$ such that either $[p_0]^s \cdot P_i = P_i$ or $[p_0]^s \cdot P_i = -P_i$. 

Let \( l' = \text{lcm}(l_0, l_1, \ldots, l_w) \) and denote by \( l \) the smallest among the positive integers \( s \) such that \([\rho_0]_s^P = P \) or \([\rho_0]_s^P = -P \).

Then, any \( l_i \) is the smallest among the positive integers \( s \) such that \( \rho_i^{l_i} \) divides either \( \rho_0^s + 1 \) or \( \rho_0^s - 1 \) in \( R \). Moreover, \( l \) is determined as follows:

\[
 l = \begin{cases} 
 l' & \text{if either } \rho_i^{l_i} \mid (\rho_0^s + 1) \text{ for all } i \text{ or } \rho_i^{l_i} \mid (\rho_0^s - 1) \text{ for all } i, \\
 2l' & \text{otherwise}.
\end{cases}
\]

**Proof.** Fix \( i \) such that \( 0 \leq i \leq w \). If \( P_i = 0 \), then \( h_i^{l_i} = 0 \), \( l_i = 1 \) and \( \rho_0^s = 1 \) divides both \( \rho_0^s + 1 \) and \( \rho_0^s - 1 \). Suppose now that \( P_i \neq 0 \). We notice that \( o(P_i) \cdot P_i = 0 \) and that, whichever \( i \) is, \( \gcd(\rho_i^{l_i}, o(P_i)) = \rho_i^{l_i} \). Therefore,

\[
\frac{\rho_i^{l_i}}{\gcd(\rho_i^{l_i}, o(P_i))} = \rho_i^{l_i - h_i^{l_i}} \mid P_i.
\]

Hence, if \( s \) is a positive integer such that \( \rho_i^{l_i} \) divides either \( \rho_0^s + 1 \) or \( \rho_0^s - 1 \), then \( \rho_i^{l_i} = h_i^{l_i} \cdot \rho_i^{l_i - h_i^{l_i}} \) divides either \( (\rho_0^s + 1)P_i \) or \( (\rho_0^s - 1)P_i \), namely

\[
[\rho_0]^s \cdot P_i = P_i \quad \text{or} \quad [\rho_0]^s \cdot P_i = -P_i.
\]

We can therefore conclude that \( l_i \) is also the smallest among the positive integers \( s \) such that \( \rho_i^{l_i} \) divides either \( \rho_0^s + 1 \) or \( \rho_0^s - 1 \) in \( R \).

Since \( [\rho_0]^s P = P \) or \( [\rho_0]^s P = -P \), we have that either \([\rho_0]^s P_i = P_i \) for all \( i \) or \([\rho_0]^s P_i = -P_i \) for all \( i \). Then, \( l \) must be a common multiple of all \( l_i \). In fact, suppose that for a chosen integer \( i \) such that \( 0 \leq i \leq w \)

\[
\begin{align*}
 l = l_i \cdot q_i + t_i \\
 0 \leq t_i < l_i
\end{align*}
\]

for integers \( q_i, t_i \). Then,

\[
[\rho_0]^s P_i = [\rho_0]^s q_i + t_i = [\rho_0]^{l_i} (\pm P_i) = \pm P_i.
\]

By definition of \( l_i \), we conclude that \( t_i = 0 \). Hence, \( l_i \mid l \) and \( l' \mid l \). Since \([\sigma]^l P_i = \pm P_i \) for any \( i \), we get the thesis. \( \square \)

The following holds.

**Lemma 3.7.** Let \( x_0 \in \mathbb{F}_{p^n}^* \) be \( \vartheta_{k_x} \)-periodic, \( s \) a positive integer and \( x_s = \vartheta_{k_x}^s (x_0) \). Let \((x_0, y_0) \in E(\mathbb{F}_{p^n}) \) (resp. \( E(\mathbb{F}_{p^{2n}})_{B_n} \)) for some \( y_0 \in \mathbb{F}_{p^n} \) (resp. \( \mathbb{F}_{p^{2n}} \)) and \((x_s, y_s) \in E(\mathbb{F}_{p^n}) \) (resp. \( E(\mathbb{F}_{p^{2n}})_{B_n} \)) for some \( y_s \in \mathbb{F}_{p^n} \) (resp. \( \mathbb{F}_{p^{2n}} \)). If \( Q^{(0)} = P(x_0, y_0) \) and \( Q^{(s)} = P(x_s, y_s) \), then \( h^{Q^{(0)}} = h^{Q^{(s)}} \).

**Proof.** Since \( x_s = \vartheta_{k_x}^s (x_0) \), we deduce that \( Q^{(s)} = \pm [\rho_0]^s Q^{(0)} \). Therefore, if \( Q^{(0)} = (Q_0^{(0)}, Q_1^{(0)}, \ldots, Q_w^{(0)}) \), then \( Q^{(s)} = \pm ([\rho_0]^s Q_0^{(0)}, \ldots, [\rho_0]^s Q_w^{(0)}) \). For any \( i \neq 0 \) we have that \( \rho_0 \) and \( \rho_i \) are coprime. Therefore, \( h_i^{Q^{(0)}} = h_i^{Q^{(s)}} \) for any \( i \neq 0 \). Finally, \( Q_0^{(0)} = 0 \), implying that \( h_0^{Q^{(0)}} = h_0^{Q^{(s)}} = 0 \). Therefore we can conclude that \( h^{Q^{(0)}} = h^{Q^{(s)}} \). \( \square \)

We introduce the following notation.

**Definition 3.8.** If \( x \in \mathbb{P}^1(\mathbb{F}_{p^n}) \) is \( \vartheta_{k_x} \)-periodic, then we denote by

\[
(x)_{\vartheta_{k_x}} = \{ \vartheta_{k_x}^r (x) : r \in \mathbb{N} \}
\]

the elements of the cycle of \( x \) with respect to the map \( \vartheta_{k_x} \).

In virtue of Lemmas 3.6 and 3.7 we can give the following definition.
Definition 3.9. If \( h = (h_0, h_1, \ldots, h_w) \in H \), then \( C_h \) denotes the set of all cycles \( (x)_{h_{x'}} \) of \( G^\infty_{h_{x''}} \) where \( x \in A_n \) (resp. \( B_n \)) and exactly one of the following conditions holds:

- \( x = \infty \) (and \( h = (0, 0, \ldots, 0) \));
- \((x, y) \in E(F_{p^n}) \) (resp. \( E(F_{p^n})_{B_n} \)) for some \( y \in F_{p^n} \) (resp. \( F_{p^n} \)) and \( h_{(x, y)} = h \).

Moreover, we introduce the following notations:

- \( l_h \) is the length of the cycles in \( C_h \);
- \( C_{A_n} = \{ (x)_{h_{x'}} \in G^\infty_{h_{x''}} : x \in A_n \} \);
- \( C_{B_n} = \{ (x)_{h_{x'}} \in G^\infty_{h_{x''}} : x \in B_n \} \);
- \( N_h = \frac{1}{2l_h} \cdot \phi(2^{h_0}) \cdot \left( \prod_{i=1}^w N_{h_i} \right) \cdot \left( \prod_{i=v+1}^w \phi(p^{h_i}) \right) \).

Now we state two theorems, concerning respectively the cycles of \( C_{A_n} \) and \( C_{B_n} \).

Theorem 3.10. Let \( S \cong R/(\pi^n_2 - 1)R \) and let \( H_A \subseteq H \) be the set formed by all \( h \in H \) such that \( h_0 = 0 \). Then,

\[ C_{A_n} = \bigsqcup_{h \in H_A} C_h. \]

Moreover, \( |C_h| = 1 \) if \( h_i = 0 \) for all \( 0 \leq i \leq w \), while \( |C_h| = N_h \).

Proof. Since \( C_h \subseteq C_{A_n} \) for any \( h \in H_A \), we have that \( \bigsqcup_{h \in H_A} C_h \subseteq C_{A_n} \). Vice versa, if \( (\bar{x})_{h_{x'}} \in C_{A_n} \), then either \( \bar{x} = \infty \), or \((\bar{x}, \bar{y}) \in E(F_{p^n}) \) for some \( \bar{y} \in F_{p^n} \) and \( P = P(\bar{x}, \bar{y}) = (0, P_1, \ldots, P_w) \) by Lemma 3.3. Hence, \( h_0^P = 0 \) and \( h^P \in H_A \). Therefore, \( C_{A_n} \subseteq \bigsqcup_{h \in H_A} C_h \).

If \( (\bar{x})_{h_{x'}} \in C_h \), where \( h \in H_A \) with all \( h_i = 0 \), then \( h = h^P \), where all \( P_i = 0 \).

Now consider \( (\bar{x})_{h_{x'}} \in C_h \) for some \( h \in H_A \}\{\{(0, \ldots, 0)\} \}. Then, \((\bar{x}, \bar{y}) \in E(F_{p^n}) \) for some \( \bar{y} \in F_{p^n} \) and the additive order of \( P(\bar{x}, \bar{y}) \) is not 2. Hence, there are two distinct rational points in \( E(F_{p^n}) \) with such a \( x \)-coordinate. Since the length of the cycle \((\bar{x})_{h_{x'}} \) is \( l_h \) and the number of points \( Q \) in \( S \) such that \( h^Q = h \) is

\[ \phi(2^{h_0}) \cdot \left( \prod_{i=1}^w N_{h_i} \right) \cdot \left( \prod_{i=v+1}^w \phi(p^{h_i}) \right), \]

the thesis follows.

\(\square\)

Theorem 3.11. Let \( S \cong R/(\pi^n_2 + 1)R \) and let \( H_B \subseteq H \) be the set formed by all \( h \in H \) such that \( h_0 = 0 \) and \( h_i \neq 0 \) for some \( 1 \leq i \leq w \). Then,

\[ C_{B_n} = \bigsqcup_{h \in H_B} C_h \]

and \( |C_h| = N_h \) for any \( h \in H_B \).

Proof. Since \( C_h \subseteq C_{B_n} \) for any \( h \in H_B \), we have that \( \bigsqcup_{h \in H_B} C_h \subseteq C_{B_n} \). Vice versa, if \( (\bar{x})_{h_{x'}} \in C_{B_n} \), then \( \bar{x} \in F_{p^n} \) and \((\bar{x}, \bar{y}) \in E(F_{p^n})_{B_n} \) for some \( \bar{y} \in F_{p^n} \) \( \setminus \) \( F_{p^n} \). In particular, \( P = P(\bar{x}, \bar{y}) \) is not the point at infinity and \( h^P \neq (0, 0, \ldots, 0) \). At the
same time $h_0^P = 0$ by Lemma 3.5 and consequently $h_i^P \neq 0$ for some $1 \leq i \leq w$. Therefore, $C_{B_n} \subseteq \bigcup_{h \in H_B} C_h$.

Consider now $\langle \tilde{x}, q \rangle \in C_h$ for some $h \in H_B$. Then, $\langle \tilde{x}, y \rangle \in E(F_{p^{2n}})$ for some $y \in F_{p^{2n}}$. Moreover, by definition of $H_B$, the additive order of $P(\tilde{x}, y)$ is not $2$. Hence, there are two distinct rational points in $E(F_{p^{2n}})_{B_n}$ having $\tilde{x}$ as $x$-coordinate. Since the length of the cycle $\langle \tilde{x}, q \rangle$ is $l_h$ and the number of points $Q$ in $S$ such that $hQ = h$ is

$$\varphi(2^{h_0}) \cdot \left( \prod_{i=1}^v N_{h_i} \right) \cdot \left( \prod_{i=v+1}^w \varphi(p_i^{h_i}) \right),$$

the thesis follows. $\square$

In the following we will denote by $V_{A_n}$ (resp. $V_{B_n}$) the set of the $\varphi_{k_n}$-periodic elements of $A_n$ (resp. $B_n$). Before proceeding with the description of the trees rooted in vertices of $V_{A_n}$ and $V_{B_n}$ we notice that, according to [3],

$$R/p_0^\infty R = \left\{ \sum_{i=0}^{e_0-1} \delta_i \cdot [p_0]^i : \delta_i = 0 \text{ or } 1 \right\}.$$

The following theorem characterizes the reversed trees having root in $V_{A_n}$ (resp. $V_{B_n}$).

**Theorem 3.12.** Any element $x_0 \in V_{A_n}$ (resp. $V_{B_n}$) is the root of a reversed binary tree having the following properties.

- If $x_0 \neq \infty$, then the depth of the tree is $e_0$, the root has exactly one child, while all other vertices have two distinct children.
- If $x_0 = \infty$, $n$ is odd and $p \equiv \pm 3 \pmod{8}$, then the tree has depth $3$, the root and the two vertices at the level 2 have exactly one child each, while the vertex at the level 1 has two distinct children.
- If $x_0 = \infty$, $n$ is odd and $p \equiv \pm 1 \pmod{8}$ or $n$ is even, then the tree has depth $e_0$, the root and the two vertices at the level 2 have exactly one child each, while all other vertices have two distinct children.

**Proof.** At first we notice that any vertex of the tree rooted in $x_0$ has at most two children. In fact, consider a vertex $x_r$ at the level $r \geq 0$ of such a tree. If $x_r = \infty$, then $\varphi_{k_n}(x) = x$, if and only if $x \in \{0, \infty\}$. Since $\infty$ is $\varphi_{k_n}$-periodic, it follows that $\infty$ has exactly one child. If $x_r \neq \infty$, then $\varphi_{k_n}(x) = x_r$ if and only if $x^2 - 2k_n x + 1 = 0$.

This quadratic equation has exactly one root if its discriminant $x^2 - 2k_n x + 1 = 0$ is zero. This happens if and only if $x_r = \pm 2k_n$. Since $(\pm 2k_n)^2 = -1$, we deduce that the discriminant is zero if and only if $x_r \in \{i_p, -i_p\}$. We notice in passing that $i_p$ and $-i_p$ have one child each, namely $1$ and $-1$. Moreover, $\varphi_{k_n}(\pm i_p) = 0$ and $\varphi_{k_n}(0) = \infty$. Therefore we can conclude that, provided that $x_0 \neq \infty$, the root $x_0$ has exactly one child, while all other vertices have zero or two distinct children. If $x_0 = \infty$, then $x_0$ has exactly one child, any other vertex $x_r$ of the tree has zero or two distinct children, unless $x_r$ is one of the two vertices at the level 2 of the tree having exactly one child each.

According to Lemma 3.5 the map $\varphi_{k_n}$ takes the elements of $A_n$ to $A_n$, the elements of $B_n$ to $B_n$ and the elements of $C_n$ to $A_n$. The elements of $C_n$, namely $1$ and $-1$, are the only two vertices belonging to the level 3 of the tree rooted in $x_0 = \infty$ in the case that $n$ is odd and $p \equiv \pm 3 \pmod{8}$. Under such hypotheses $1$ and $-1$ are also the leaves of the tree rooted in $\infty$. In all other circumstances, if $x_0 \in V_{A_n}$ (resp. $V_{B_n}$), then $x_0$ is root of a tree whose vertices belong to $A_n$ (resp. $B_n$) and whose depth is $e_0$. In fact, $x_0 = \infty$ or is the $x$-coordinate of a point
\((x_0, y_0) \in E(F_{p^n})\) (resp. \(E(F_{p^{2n}})_{B_n}\)). Let \(P = (0, P_1, \ldots, P_w)\) be the image of the point at infinity or \((x_0, y_0)\) in \(S = \prod_{i=0}^{w-1} R/\rho_i \cdot R\). If \(Q = (Q_0, Q_1, \ldots, Q_w)\) is any point of \(S\), then \([\rho_0]^{\alpha} Q_0 = 0\) in \(R/\rho_0 \cdot R\). Therefore, \([\rho_0]^{\alpha} Q\) is the image in \(S\) of a rational point of \(E(F_{p^n})\) (resp. \(E(F_{p^{2n}})_{B_n}\)) whose \(x\)-coordinate is \(\vartheta_{k_n}\)-periodic. This fact implies that \(x_0\) cannot be the root of a tree of depth greater than \(e_0\).

Suppose now that
\[
Q_0 = [1];
\]
\[
Q_i = [\rho_0]^{-\alpha} P_i, \text{ for any } 1 \leq i \leq w.
\]
Then, \([\rho_0]^{\alpha} Q_0 \neq 0\) in \(R/\rho_0 \cdot R\) for any \(0 \leq r < e_0\). Nonetheless, \([\rho_0]^{\alpha} Q_0 = 0\) in \(R/\rho_0 \cdot R\) and \([\rho_0]^{\alpha} Q_i = P_i\) for any \(1 \leq i \leq w\). Therefore, \([\rho_0]^{\alpha} Q = P\). If \(Q\) is the image in \(S\) of a rational point \((\hat{x}, \hat{y}) \in E(F_{p^n})\) (resp. \(E(F_{p^{2n}})_{B_n}\)), then \(\vartheta_{k_n}^{\alpha}(\hat{x}) = x_0\) and \(\vartheta_{k_n}^{\alpha}(\hat{y})\) is not \(\vartheta_{k_n}\)-periodic for any \(0 \leq r < e_0\), namely \(\hat{x}\) belongs to the level \(e_0\) of the tree rooted in \(x_0\).

Consider now a vertex \(x_r \neq \infty\) at the level \(r < e_0\) of the tree rooted in \(x_0\). Then, \((x_r, y_r) \in E(F_{p^n})\) (resp. \(E(F_{p^{2n}})_{B_n}\)) for some \(y_r \in F_{p^n}\) (resp. \(F_{p^{2n}}\)).

If \(Q = Q(x_r, y_r) = (Q_0, Q_1, \ldots, Q_w) \in S\), then
\[
Q_0 = [\rho_0]^{\alpha} - r + \sum_{i=0}^{e_0-1} \delta_i \cdot [\rho_0]^i
\]
for some choice of the coefficients \(\delta_i \in \{0, 1\}\). Now we prove that there exists at least a rational point \((x_{r+1}, y_{r+1}) \in E(F_{p^n})\) (resp. \(E(F_{p^{2n}})_{B_n}\)) such that \(\vartheta_{k_n}(x_{r+1}) = x_r\). Consider in fact the point \(\tilde{Q} = \tilde{Q}(x_{r+1}, y_{r+1}) = (\tilde{Q}_0, \tilde{Q}_1, \ldots, \tilde{Q}_w) \in S\), where
\[
\tilde{Q}_0 = [\rho_0]^{\alpha} - r - 1 + \sum_{i=0}^{e_0-2} \delta_{i+1} \cdot [\rho_0]^i;
\]
\[
\tilde{Q}_i = [\rho_0]^{-r} Q_i, \text{ for } 1 \leq i \leq w.
\]
Since \([\rho_0] \tilde{Q} = Q\) we are done. Finally, \(\infty\) has exactly one child.

All considered, we have proved that any vertex \(x_r\) at the level \(r < e_0\) of the tree rooted in a vertex \(x_0\) of \(V_{A_n}\) (resp. \(V_{B_n}\)) has exactly two children, unless \(x_r \in \{x_0, i_p, -i_p\}\), in which case \(x_r\) has exactly one child.

We conclude this section with one example.

**Example 3.13.** Let \(p = 53\). Then, the two roots in \(F_p\) of the equation
\[
x^2 - 2x + 2 = 0
\]
are
\[
\alpha_\omega = 24 \text{ and } \alpha_{\omega} = 31.
\]
Consequently,
\[
k_\omega = 15 \text{ and } k_{\omega} = 38.
\]

In the following we will describe thoroughly the structure of the graphs \(G^{53}_{\omega_{15}}\) and \(G^{53}_{\omega_{38}}\). At first we notice that \(|E(F_{53})| = 68\) and that the representation of the Frobenius endomorphism \(\pi_{53}\) as an element of \(R\) is
\[
\pi_{53} = -7 + 2i.
\]

We deal firstly with the graph \(G^{53}_{\omega_{15}}\). Since \(\pi^{-2} \equiv 15 \pmod{53}\), we define \(\rho_0 = \pi\) and study the iterations of the map \(\vartheta_{15}\) on \(A_1\) by means of the iterations of \([\rho_0]\) on \(S \cong R/(\pi_{53} - 1)R\). We have that
\[
S = R/\rho_0^2 R \times R/\rho_1 R,
\]
where $\rho_1 = -1 - 4i$. Since $e_0 = 2$, the depth of the trees rooted in elements of $A_1 \setminus \{\infty\}$ is 2, while the depth of the tree rooted in $\infty$ is 3, because $p \equiv -3 \pmod{8}$ and $n = 1$. The $\vartheta_{15}$-periodic elements in $A_1$ are $x$-coordinates of the points $P = (0, P_1) \in S$. In $R/\rho_1 R$ there are 16 points of additive order 17 and 1 point of additive order 1, namely $P_1 = 0$. In this latter case $P = (0, 0)$, namely $P$ is the point at infinity, which gives rise to one cycle of length 1. In the former case the 16 points give rise to a cycle of length 8, since 8 is the smallest among the positive integers $s$ such that $\rho_1$ divides either $\rho_s^5 + 1$ or $\rho_s^5 - 1$.

The iterations of $\vartheta_{15}$ on $B_1$ can be studied by means of the iterations of $[\rho_0]$ on $S \cong R/(\pi_{53} + 1) R$. We have that

$$S = R/\rho_0^5 R \times R/\rho_1 R,$$

where $\rho_1 = 1 - 2i$. Since $e_0 = 3$, the depth of the trees rooted in elements of $B_1$ is 3. The $\vartheta_{15}$-periodic elements in $B_1$ are $x$-coordinates of the points $P = (0, P_1) \in S$, where $P_1 \neq 0$. The 4 points $P_1 \neq 0$ in $R/\rho_1 R$ have additive order 5. They give rise to one cycle of length 2, since 2 is the smallest among the positive integers $s$ such that $\rho_1$ divides either $\rho_s^5 + 1$ or $\rho_s^5 - 1$.

The graph $G^5_{\vartheta_{15}}$ is represented below. We notice that the vertex labels, different from $\infty$ and '0' (the zero in $F_{53}$), refer to the exponents of the powers $\gamma^i$ for $0 \leq i \leq 51$, being $\gamma$ the root of the Conway polynomial $x - 2 \in F_{53}[x]$.

The following 2 connected components are due to the elements of $A_1$. The following connected component is due to the elements of $B_1$. 
We deal now with the graph $G_{\vartheta_{38}}^{53}$. Since $\alpha^{-2} \equiv 38 \pmod{\pi_{53}}$, we define $\rho_0 = \alpha$ and study the iterations of the map $\vartheta_{38}$ on $A_1$ by means of the iterations of $[\rho_0]$ on $S \cong R/(\pi_{53} - 1)R$. We have that

$$S = R/\rho_0^2R \times R/\rho_1R,$$

where $\rho_1 = 1 + 4i$. The length of the cycles due to the elements of $A_1$ and the depth of the trees attached to $\vartheta_{38}$-periodic elements can be found as explained in the case of the map $\vartheta_{15}$.

The iterations of $\vartheta_{38}$ on $B_1$ can be studied by means of the iterations of $[\rho_0]$ on $S \cong R/(\pi_{53} + 1)R$. We have that

$$S = R/\rho_0^3R \times R/\rho_1R,$$

where $\rho_1 = 2 + i$. Since $e_0 = 3$, the depth of the trees rooted in elements of $B_1$ is 3. The $\vartheta_{38}$-periodic elements in $B_1$ are $x$-coordinates of the points $P = (0, P_1) \in S$, where $P_1 \neq 0$. The 4 points $P_1 \neq 0$ in $R/\rho_1R$ have additive order 5. They give rise to 2 cycles of length 1, since 1 is the smallest among the positive integers $s$ such that $\rho_1$ divides either $\rho_0^s + 1$ or $\rho_0^s - 1$.

The graph $G_{\vartheta_{38}}^{53}$ is here represented. The following 2 connected components are due to the elements of $A_1$.

The following 2 connected components are due to the elements of $B_1$. 
4. Case 3: $k$ is a root of $x^2 + \frac{1}{2}x + \frac{1}{2} \in \mathbb{F}_p[x]$ with $p \equiv 1, 2, 4 \pmod{7}$

The endomorphism ring of the elliptic curve with equation $y^2 = x^3 - 35x + 98$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}[\alpha]$, where $\alpha = \frac{1 + \sqrt{-7}}{2}$, as one can deduce from [5], Proposition 2.3.1 (iii). In particular, the curve possesses an endomorphism of degree 2, namely the map $[\alpha]$, which takes a point $(x, y)$ of the curve to

$$[\alpha](x, y) = \left(\alpha^{-2} \left(x - \frac{7(1 - \alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3}y \left(1 + \frac{7(1 - \alpha)^4}{(x + \alpha^2 - 2)^2}\right)\right).$$

If $p$ is an odd prime such that

$$p \equiv 1, 2 \text{ or } 4 \pmod{7},$$

then the elliptic curve with equation $y^2 = x^3 - 35x + 98$ has good reduction modulo $p$ (see [4], Chapter V, Proposition 5.1 or [3], page 59). Hence, from now on we suppose that $p$ is a fixed prime number as in (4.1) and we denote by $E$ the elliptic curve with equation

$$y^2 = x^3 - 35x + 98$$

over $\mathbb{F}_p$. Being $-7$ a quadratic residue in $\mathbb{F}_p$ we also get that

$$x^2 - x + 2 = 0$$

has two solutions $\omega, \overline{\omega}$ in $\mathbb{F}_p$.

Fixed a positive integer $n$ we want to study the iterations over $\mathbb{P}^1(\mathbb{F}_{p^n})$ of the maps $\vartheta_{k_{\omega}}$, for $\sigma \in \{\omega, \overline{\omega}\}$, where

$$k_{\omega} \equiv \omega - \frac{1}{2} \pmod{p}, \quad k_{\overline{\omega}} \equiv \overline{\omega} - \frac{1}{2} \pmod{p}.$$

Firstly we notice that $k_{\omega}$ and $k_{\overline{\omega}}$ are the two roots in $\mathbb{F}_p$ of the quadratic equation

$$x^2 + \frac{1}{2}x + \frac{1}{2} = 0.$$

Now we show that, for $\sigma \in \{\omega, \overline{\omega}\}$, the map $\vartheta_{k_{\sigma}}$ is conjugated to the map $\eta_{k_{\sigma}}$, defined over $\mathbb{P}^1(\mathbb{F}_{p^n})$ as follows:

$$\eta_{k_{\sigma}}(x) = \begin{cases} \infty & \text{if } x = -\sigma^2 + 2 \text{ or } \infty, \\ \frac{1}{\sigma} \cdot \left(\frac{x - \frac{7(1 - \sigma)^4}{x + \sigma^2 - 2}}{2}\right) & \text{otherwise}. \end{cases}$$

Before proving this fact, we notice that the two maps $\eta_{k_{\sigma}}$, for $\sigma \in \{\omega, \overline{\omega}\}$, are involved in the definition of two endomorphisms of the curve $E$, namely the maps
\( e_{k_\sigma} \) which take a rational point \((x, y)\) in \( E(\mathbb{F}_p) \) to
\[\begin{align*}
e_{k_\sigma}(x, y) &= \left( \eta_{k_\sigma}(x), \frac{1}{\sigma^3} \cdot y \cdot \left( 1 + \frac{7 \cdot (1 - \sigma)^4}{(x + \sigma^2 - 2)^2} \right) \right).
\end{align*}\]
The fact that any map \( \vartheta_{k_\sigma} \) is conjugated to the respective map \( \eta_{k_\sigma} \) enables us to study the iterations of the former maps relying upon the action of the endomorphisms \( e_{k_\sigma} \) on the rational points of the curve \( E \).

With the aim to prove the conjugation between the maps \( \vartheta_{k_\sigma} \) and \( \eta_{k_\sigma} \), for \( \sigma \) equal to \( \omega \) or \( \overline{\omega} \) respectively, we set
\[\begin{align*}
b_\sigma &\equiv k_\sigma + \frac{5}{2} \pmod{p}, \\
e_\sigma &\equiv -\frac{1}{4k_\sigma + 1} \pmod{p}, \\
d_\sigma &\equiv \frac{1}{4} + k_\sigma \pmod{p}
\end{align*}\]
and define two bijective maps \( \chi_{k_\sigma} \) on \( \mathbb{P}^1(\mathbb{F}_p) \) in such a way:
\[\chi_{k_\sigma} : x \mapsto \begin{cases}
\frac{x}{e_\sigma} & \text{if } x = \infty, \\
\infty & \text{if } x = -\frac{d_\sigma}{e_\sigma}, \\
x + b_\sigma & \text{in all other cases},
\end{cases}\]
The inverses of the maps \( \chi_{k_\sigma} \) are
\[\chi_{k_\sigma}^{-1} : x \mapsto \begin{cases}
\frac{1}{x} & \text{if } x = \frac{1}{e_\sigma}, \\
\frac{d_\sigma}{e_\sigma} & \text{if } x = \infty, \\
{x + b_\sigma - d_\sigma} & \text{in all other cases}.
\end{cases}\]

With the notation just introduced we can prove the following technical result.

**Lemma 4.1.** For any \( x \in \mathbb{P}^1(\mathbb{F}_p) \),
\[
(4.5) \quad \chi_{k_\sigma}^{-1} \circ \eta_{k_\sigma} \circ \chi_{k_\sigma}(x) = \vartheta_{k_\sigma}(x).
\]

**Proof.** As a first step we notice that \( \sigma^2 \equiv 2k_\sigma - 1 \pmod{p} \). Therefore,
\[
\eta_{k_\sigma}(x) = \frac{1}{2k_\sigma - 1} \cdot \left( x - \frac{14 \cdot (3k_\sigma + 1)}{x + 2k_\sigma - 3} \right).
\]
Taking into account the fact that \( k_\sigma^2 \equiv -\frac{1}{2}k_\sigma - \frac{1}{2} \pmod{p} \), we have that in \( \mathbb{F}_p(x) \)
\[
\eta_{k_\sigma} \circ \chi_{k_\sigma}(x) = \frac{56k_\sigma + 28}{(8k_\sigma - 12)} \cdot x^2 + \frac{(-84k_\sigma + 98) \cdot x + (56k_\sigma + 28)}{(8k_\sigma - 12)}.
\]
Since in \( \mathbb{F}_p(x) \)
\[
\chi_{k_\sigma}^{-1} \circ \eta_{k_\sigma}(x) = \frac{(42k_\sigma + 7) \cdot x^2 + (42k_\sigma + 7) + 1}{(-14k_\sigma + 35)x} \equiv k_\sigma \cdot \frac{x^2 + 1}{x}.
\]
we get the thesis. \(\square\)

According to Lemma 4.1, any of the two maps \( \vartheta_{k_\sigma} \) is conjugated to the respective map \( \eta_{k_\sigma} \). Therefore, since the graphs \( G_{\psi_{\eta_{k_\sigma}}}^p \) are isomorphic to the graphs \( G_{\vartheta_{k_\sigma}}^p \), we will concentrate on the study of these latter graphs.

### 4.1. Structure of the graphs \( G_{\eta_{k_\sigma}}^p \)

We remind that the endomorphism ring of the curve \( y^2 = x^3 - 35x + 98 \) over \( \mathbb{Q} \) is isomorphic to \( \mathbb{Z}[\alpha] \). Therefore, according to [2], Chapter 13, Theorem 12, the endomorphism ring \( \text{End}(E) \) of \( E \) over \( \mathbb{F}_p \) is isomorphic to \( R = \mathbb{Z}[\alpha] \) too. We notice that \( R \) is an Euclidean ring with Euclidean function
\[
N(a + ba) = (a + ba) \cdot (a + \overline{ba}),
\]
for any arbitrary choice of \( a, b \) in \( \mathbb{Z} \) (here \( \overline{()} \) denotes the complex conjugation).

By [8], Theorem 2.3(a), there exists an isomorphism
\[
\psi_n : E(\mathbb{F}_p) \to R/(\pi_n^p - 1)R,
\]
Lemma 4.2. Let \( \tilde{x} \in \mathbb{F}_{p^n} \). Then, in \( E(\mathbb{F}_{p^n}) \) there are two distinct rational points, \( (\tilde{x}, \tilde{y}) \) and \( (\tilde{x}, -\tilde{y}) \), with such an \( x \)-coordinate except for
\[
\tilde{x} \in \{-7, \sigma + 3, \overline{\sigma} + 3\},
\]
in which case \( \tilde{y} = 0 \).

Proof. The equation \( y^2 = \tilde{x}^3 - 35\tilde{x} + 98 \) has exactly two distinct roots \( y_1 \) and \( y_2 \) in \( \mathbb{F}_{p^{2n}} \) except in the case that \( \tilde{x} \) makes vanish the polynomial \( x^3 - 35x + 98 \), whose set of roots is \( \{-7, \sigma + 3, \overline{\sigma} + 3\} \). \( \square \)

Lemma 4.3. The following hold.

- \(-\sigma^2 + 2 = \overline{\sigma} + 3 \) in \( \mathbb{F}_p \);
- \( \eta_{\sigma}(-7) = \sigma + 3 \);
- \( \eta_{\sigma}(\overline{\sigma} + 3) = \infty \);
- \( \eta_{\sigma}(x) = x \) if and only if \( x \in \{\sigma + 3, -2\sigma + 1, \infty\} \).

Proof. All assertions can be checked by direct computation reminding that
\[
\sigma^2 - \sigma + 2 = 0 \quad \text{and} \quad \sigma + \overline{\sigma} = 1.
\]

Let us begin with the first assertion:
\[
-\sigma^2 + 2 = -\sigma + 4 = \overline{\sigma} + 3.
\]

The second assertion can be proved as follows:
\[
\eta_{\sigma}(-7) = \frac{1}{\sigma^2} \cdot \left( -7 - \frac{7 \cdot (1 - \sigma)^4}{7 + \sigma^2 - 2} \right) = \left( \frac{1}{4} \sigma - \frac{1}{4} \right) \cdot \left( -7 - \frac{21\sigma - 7}{\sigma - 11} \right) = \sigma + 3.
\]

The third assertion follows from the first one and from the definition of \( \eta_{\sigma} \). Finally, \( \eta_{\sigma}(x) = x \) if and only if \( x = \infty \) or
\[
\sigma^2 \cdot (x + \sigma^2 - 2) \cdot \eta_{\sigma}(x) = \sigma^2 \cdot (x + \sigma^2 - 2) \cdot x.
\]
After some algebraic manipulations we get that this latter is equivalent to the quadratic equation

\[ (-\sigma + 3) \cdot x^2 + (6\sigma - 10) \cdot x - (21\sigma - 7) = 0, \]

whose roots are \( \sigma + 3 \) and \( -2\sigma + 1 \).

**Lemma 4.4.** The map \( \eta_{k_n} \) takes the elements of \( A_n \) to \( A_n \) and the elements of \( B_n \) to \( B_n \).

**Proof.** By definition \( \eta_{k_n}(\infty) = \infty \in A_n \) and, by Lemma 4.3 we have that \( -\sigma^2 + 2 = \overline{\sigma} + 3 \in A_n \), since \( (\overline{\sigma} + 3, 0) \in E(\mathbb{F}_{p^n}) \) according to Lemma 4.2.

If \( \tilde{x} \in A_n \setminus \{-\sigma^2 + 2, \infty\} \), then there exists \( \tilde{y} \in \mathbb{F}_{p^n} \) such that \( (\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \). Therefore, \( e_{k_n}(\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \) and \( \eta_{k_n}(\tilde{x}) \in A_n \).

Consider finally an element \( \tilde{x} \in B_n \). In this case \( (\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \) for some \( \tilde{y} \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^n} \). Moreover, \( (\eta_{k_n}(\tilde{x}), \tilde{y}_1) \) and \( (\eta_{k_n}(\tilde{x}), \tilde{y}_2) \), with

\[ \tilde{y}_j = (-1)^j \cdot \frac{1}{\sigma^3} \cdot \tilde{y} \cdot \left( 1 + \frac{7 \cdot (1 - \sigma^4)}{(x + \sigma^2 - 2)^2} \right), \quad \text{for } j \in \{1, 2\}, \]

are the only rational points in \( E(\mathbb{F}_{p^n}) \) having \( \tilde{x} \) as \( x \)-coordinate. In addition, \( \tilde{y} \not\in \mathbb{F}_{p^n} \), unless \( \tilde{y} = 0 \). Nevertheless, this happens if and only if \( \tilde{x} \in \{-7, \sigma + 3, \overline{\sigma} + 3\} \subseteq A_n \). Since \( \tilde{x} \not\in A_n \), we get the thesis. \( \square \)

Before dealing with the iterations of \( \eta_{k_n} \) on \( B_n \), we introduce the set

\[ E(\mathbb{F}_{p^n})_{B_n} = \{(x, y) \in E(\mathbb{F}_{p^n}) : x \in B_n \}. \]

Moreover we define the set

\[ E(\mathbb{F}_{p^n})_{B_n}^* = \{(\alpha, (\sigma, 0), (\overline{\sigma} + 3, 0))\}, \]

where \( O \) denotes the point at infinity of \( E \).

The following holds.

**Lemma 4.5.** Let \( \tilde{x} \in \mathbb{F}_{p^n} \) and \( P = (\tilde{x}, \tilde{y}) \in E(\mathbb{F}_{p^n}) \). We have that \( (\pi_p^n + 1)P = O \) if and only if \( P \in E(\mathbb{F}_{p^n})_{B_n} \cup E(\mathbb{F}_{p^n})_{B_n}^* \).

**Proof.** The proof is verbatim the same as in Lemma 4.4 just considering the new definition of the set \( E(\mathbb{F}_{p^n})_{B_n}^* \).

With the notation till now introduced and in virtue of Lemma 4.5 we can say that there exists an isomorphism

\[ \psi_n : E(\mathbb{F}_{p^n})_{B_n} \cup E(\mathbb{F}_{p^n})_{B_n}^* \rightarrow R/(\pi_p^n + 1)R. \]

All considered we can study the graph \( G_{\eta_{k_n}} \) separately on the elements of \( A_n \) and \( B_n \). To do that we will rely upon the action of \([\rho_0]\) on the elements of \( R/(\pi_p^n - 1)R \) (resp. \( R/(\pi_p^n + 1)R \)), where

\[ \rho_0 = \begin{cases} \alpha, & \text{if } \alpha \equiv \sigma \pmod{\pi_p}; \\ \overline{\sigma}, & \text{if } \overline{\sigma} \equiv \sigma \pmod{\pi_p}. \end{cases} \]

Suppose that \( \pi_p^n - 1 \) (resp. \( \pi_p^n + 1 \)) factors in \( R \) up to units, as

\[ \rho_0^\omega = \left( \prod_{i=1}^w \pi_{e_i}^{v_i} \right) \cdot \left( \prod_{i=v+1}^w r_i^{e_i} \right) \cdot (\sqrt{-\pi_p})^y, \quad (4.6) \]

where

(1) all \( e_i \), for \( 0 \leq i \leq w \), and \( e_f \) are non-negative integers;
(2) \( N(p_{e_i}^{v_i}) = 2^w \);
(3) for \( 1 \leq i \leq v \) the elements \( p_i \in \mathbb{Z} \) are distinct primes of \( R \) and \( N(p_i^{e_i}) = p_i^{2e_i} \);
If, on the contrary, $e_f$ is odd, then we define $\rho_j$ for $j \in \{1, \ldots, v\}$ as

$$\rho_j = \begin{cases} p_j & \text{if } j \in \{1, \ldots, e\}, \\ r_j & \text{if } j \in \{v+1, \ldots, w\}, \\ \sqrt{-7} & \text{if } j = f. \end{cases}$$

As a consequence of the factorization, the ring $R/(\pi_p^n - 1)R$ (resp. $R/(\pi_p^n + 1)R$) is isomorphic to

$$S = \prod_{j \in J} R/\rho_j^{e_j} R.$$  \hspace{1cm} (4.7)

The additive structure of the quotient rings involved in (4.7) has been discussed in Section 3. Herein we just notice that the additive group of $R/(\sqrt{-7})^{e_f} R$ is isomorphic to the direct sum of two cyclic groups of order $7^{e_f/2}$, if $e_f$ is even, or to the direct sum of two cyclic groups of order respectively $7^{(e_f - 1)/2}$ and $7^{(e_f + 1)/2}$, if $e_f$ is odd. In the case that $e_f$ is even, for each integer $0 \leq h_f \leq e_f/2$ there are $N_{h_f}$ elements in $R/(\sqrt{-7})^{e_f} R$ of order $7^{h_f}$, where

$$N_{h_f} = \begin{cases} 1 & \text{if } h_f = 0, \\ 7^{2h_f} - 7^{2(h_f - 1)} & \text{if } h_f = 1, \\ 7^{e_f} - 7^{e_f - 1} & \text{otherwise.} \end{cases}$$

If, on the contrary, $e_f$ is odd, then

$$N_{h_f} = \begin{cases} 1 & \text{if } h_f = 0, \\ 7^{2h_f} - 7^{2(h_f - 1)} & \text{if } 1 \leq h_f \leq (e_f - 1)/2, \\ 7^{e_f} - 7^{e_f - 1} & \text{if } h_f = (e_f + 1)/2. \end{cases}$$

If $(x, y)$ is a rational point of $E(F_{p^n})$ (resp. $E(F_{p^{2n}})B_n$), then we write $P_{(x,y)}$ for the image of $(x, y)$ in $S$.

Now we define the sets

$$Z_j = \{0, 1, \ldots, e_j\}, \text{ for any } j \in J \setminus \{f\},$$

$$Z_f = \{0, 1, \ldots, \lceil e_f/2 \rceil\}$$

and

$$H = \prod_{j \in J} Z_j.$$  

If $P = (P_0, P_1, \ldots, P_f) \in S$, then we define $h_P = (h_0^P, h_1^P, \ldots, h_f^P)$ in $H$ if

- $P_0$ has additive order $2^{h_0^P}$ in $R/\rho_0^{e_0} R$;
- each $P_i$, for $1 \leq i \leq w$, has additive order $p_i^{h_i^P}$ in $R/\rho_i^{e_i} R$;
- $P_f$ has additive order $7^{h_f^P}$ in $R/\rho_f^{e_f} R$.

Moreover, we define $o(P) = (o(P_0), o(P_1), \ldots, o(P_f))$, where $o(P_j)$ denotes, for any $j \in J$, the additive order of $P_j$ in $R/\rho_j^{e_j} R$.

The following two lemmas furnish a characterization of $\eta_{h_x}$-periodic elements.

Lemma 4.6. Let $\tilde{x} \in A_n$ (resp. $B_n$) be $\eta_{h_x}$-periodic. Then, one of the following holds:

- $\tilde{x} = \infty$;
- $\tilde{x}$ is the $x$-coordinate of a rational point $(\tilde{x}, \tilde{y}) \in E(F_{p^n})$ (resp. $E(F_{p^{2n}})B_n$) such that $P_{(\tilde{x}, \tilde{y})} = (P_0, P_1, \ldots, P_f)$, where $P_0 = 0$. 

Moreover, we introduce the following notations:

Definition 4.9. If \( x \in \mathbf{P}^1(\mathbf{F}_p^n) \) is \( \eta_{ks} \)-periodic, then we denote by

\[ \langle x \rangle_{\eta_{ks}} = \{ \eta_{ks}(x) : r \in \mathbb{N} \} \]

the elements of the cycle of \( x \) with respect to the map \( \eta_{ks} \).

In virtue of Lemmas 4.17 and 4.8 we can give the following definition.

Definition 4.10. If \( h = (h_0, h_1, \ldots, h_f) \in H \), then \( C_h \) denotes the set of all cycles \( \langle x \rangle_{\eta_{ks}} \) of \( G_{\eta_{ks}}^{p^n} \), where \( x \in A_n \) (resp. \( B_n \)) and exactly one of the following conditions holds:

- \( x = \infty \) (and \( h = (0, 0, \ldots, 0) \));
- \( (x, y) \in E(\mathbf{F}_p^n) \) (resp. \( E(\mathbf{F}_p^{2n})_{B_n} \)) for some \( y \in \mathbf{F}_p^n \) (resp. \( \mathbf{F}_p^{2n} \)) and \( h^{\varphi(2h_0)} = h \).

Moreover we introduce the following notations:

- \( l_h \) is the length of the cycles in \( C_h \);
- \( C_{A_n} = \{ \langle x \rangle_{\eta_{ks}} \in G_{\eta_{ks}}^{p^n} : x \in A_n \} \);
- \( C_{B_n} = \{ \langle x \rangle_{\eta_{ks}} \in G_{\eta_{ks}}^{p^n} : x \in B_n \} \);
- \( N_h = \frac{1}{2l_h} \cdot \varphi(2h_0) \cdot \left( \prod_{i=1}^w N_{h_i} \right) \cdot \left( \prod_{i=w+1}^w \varphi(p_i^{h_i}) \right) \cdot N_{h_f} \).

Now we state two theorems, concerning respectively the cycles of \( C_{A_n} \) and \( C_{B_n} \).

Theorem 4.11. Let \( S \cong R/(\pi_p^n - 1)R \) and let \( H_A \subseteq H \) be the set formed by all \( h \in H \) such that \( h_0 = 0 \). Then,

\[ C_{A_n} = \bigsqcup_{h \in H_A} C_h. \]

Moreover, \( |C_h| = 1 \) in the following cases:
In all other cases \(|C_h| = N_h\).

Proof. Since \(C_h \subseteq C_{A_n}\) for any \(h \in H_A\), we have that \(\bigcup_{h \in H_A} C_h \subseteq C_{A_n}\). Vice versa, if \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_{A_n}\), then either \(\tilde{x} = \infty\), or \(\langle \tilde{x}, \tilde{y} \rangle \in E(F_{p^n})\) for some \(\tilde{y} \in F_{p^n}\) and \(P = P_{\langle \tilde{x}, \tilde{y} \rangle} = (0, P_1, \ldots, P_j)\) by Lemma 4.6. Hence, \(h_0^P = 0\) and \(h^P \in H_A\). Therefore, \(C_{A_n} \subseteq \bigcup_{h \in H_A} C_h\), analysing separately the different cases.

- Let \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_h\), where \(h \in H_A\) and \(h_j = 0\) for all \(j \in J\). Then \(h = h^P\), where \(P_j = 0\) for all \(j \in J\). Therefore, \(\tilde{x} = \infty\) and \(|C_h| = 1\).

- Let \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_h\), where \(h \in H_A\), \(h_j = 1\) for some \(1 \leq j \leq w\) and \(h_j = 0\) for \(j \neq \tilde{j}\). Then \(h = h^P\), where \(P_j = 0\) for \(j \neq \tilde{j}\). Moreover, \(P_j\) has additive order 2. Hence, also \(P\) has additive order 2 and \(P = P_{\langle \tilde{x}, \tilde{y} \rangle}\). Therefore, \(\tilde{x} \in \{-7, \sigma + 3, \tilde{\sigma} + 3\}\). Since \(-7\) and \(\tilde{\sigma} + 3\) are not \(n_{\sigma}\)-periodic, we conclude that \(\tilde{x} = \sigma + 3\) and \(|C_h| = 1\).

- Let \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_h\), for some \(h \in H_A\) such that none of the previous conditions occurs. Then, \(\langle \tilde{x}, \tilde{y} \rangle \in E(F_{p^n})\) for some \(\tilde{y} \in F_{p^n}\) and the additive order of \(P_{\langle \tilde{x}, \tilde{y} \rangle}\) is not 2. Hence, there are exactly two distinct rational points in \(E(F_{p^n})\) having such a \(x\)-coordinate. Since the length of the cycle \(\langle \tilde{x} \rangle_{n_{\sigma}}\) is \(l_h\) and the number of points \(Q\) in \(S\) such that \(h^Q = h\) is

\[
\varphi(2^{h_0}) \cdot \left(\prod_{i=1}^{w} N_{h_i}\right) \cdot \left(\prod_{i=w+1}^{\infty} \varphi(p_i^{h_i})\right) \cdot N_{h_f},
\]

the thesis follows.

\(\square\)

**Theorem 4.12.** Let \(S \cong R/(\pi_p^2 + 1)R\) and let \(H_B \subseteq H\) be the set formed by all \(h \in H\) such that

- \(h_0 = 0;\)
- \(h \neq (0, 0, \ldots, 0);\)
- if \(\rho_j = \tilde{\pi}_0\) for some \(1 \leq \tilde{j} \leq w\) and \(h_j = 1\), then \(h_j \neq 0\) for some \(j \neq \tilde{j}\).

Then,

\[
C_{B_n} = \bigcup_{h \in H_B} C_h
\]

and \(|C_h| = N_h\) for any \(h \in H_B\).

Proof. Since \(C_h \subseteq C_{B_n}\) for any \(h \in H_B\), we have that \(\bigcup_{h \in H_B} C_h \subseteq C_{B_n}\). Vice versa, if \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_{B_n}\), then \(\tilde{x} \in F_{p^n}\) and \(\langle \tilde{x}, \tilde{y} \rangle \in E(F_{p^{2n}})_{B_n}\) for some \(\tilde{y} \in F_{p^{2n}}\setminus F_{p^n}\). In particular, \(P = P_{\langle \tilde{x}, \tilde{y} \rangle}\) is not the point at infinity and \(h^P \neq (0, 0, \ldots, 0)\). At the same time \(h_0^P = 0\) by Lemma 4.6. Moreover, if \(\rho_j = \tilde{\pi}_0\) for some \(1 \leq \tilde{j} \leq w\) and \(h_j = 1\), then \(h_j \neq 0\) for some \(j \neq \tilde{j}\). On the contrary, \(P\) would have additive order 2, namely \(\tilde{y} = 0\). Hence, \(C_{B_n} \subseteq \bigcup_{h \in H_B} C_h\).

Let \(\langle \tilde{x} \rangle_{n_{\sigma}} \in C_h\) for some \(h \in H_B\). Then, \(\langle \tilde{x}, \tilde{y} \rangle \in E(F_{p^{2n}})_{B_n}\) for some \(\tilde{y} \in F_{p^{2n}}\). Moreover, by definition of \(H_B\), the additive order of \(P_{\langle \tilde{x}, \tilde{y} \rangle}\) is not 2. This latter fact implies that there are exactly two distinct points in \(E(F_{p^{2n}})_{B_n}\) having \(\tilde{x}\) as
x-coordinate. Since the length of the cycle $⟨\tilde{x}⟩_{η_{kσ}}$ is $l_h$ and the number of points $Q$ in $S$ such that $h^Q = h$ is

$$\varphi(2^{h_0}) \cdot \left( \prod_{i=1}^w N_{h_i} \right) \cdot \left( \prod_{i=w+1}^w \varphi(p_{h_i}^2) \right) \cdot N_{h_1},$$

the thesis follows.

In the following we will denote by $V_{A_n}$ (resp. $V_{B_n}$) the set of the $η_{kσ}$-periodic elements of $A_n$ (resp. $B_n$). Before proceeding with the description of the trees rooted in vertices of $V_{A_n}$ and $V_{B_n}$ we notice that, according to [3],

$$R/R_0 ∩ R = \left\{ \sum_{i=0}^{σ-1} \delta_i \cdot [p_0]^i : \delta_i = 0 \text{ or } 1 \right\}.$$

The following theorem characterizes the reversed trees having root in $V_{A_n}$ (resp. $V_{B_n}$).

**Theorem 4.13.** Any element $x_0 \in V_{A_n}$ (resp. $V_{B_n}$) is the root of a reversed binary tree of depth $e_0$ with the following properties.

- If $x_0 \notin \{σ+3, ∞\}$, then $x_0$ has exactly one child, while all other vertices have two distinct children.
- If $x_0 \in \{σ+3, ∞\}$, then $x_0$ and the vertex at the level 1 of the tree have exactly one child each, while all other vertices have two distinct children.

**Proof.** The proof that the depth of the tree is $e_0$ and that any vertex at the level $r < e_0$ of the tree has at least one child follows the same lines as the proof of Theorem 4.12. More precisely, we have to replace the map $δ_{kσ}$ with the map $η_{kσ}$, the index set $\{0, 1, \ldots, w\}$ with the current index set $J$ and modify consequently the points $F, Q$ and $\hat{Q}$ considering the new index set.

As regards the number of children of any vertex $x_r \neq ∞$ at a certain level $r < e_0$ of the tree rooted in $x_0$, we now prove that $x_r$ has exactly two distinct children, unless $x_r \in \{-7, τ+3\}$. To do that we momentarily consider the isomorphic graph $G_{δ_{kσ}}$, and the vertex $γ_r = \chi_{kσ}^{-1}(x_r)$ belonging to the level $r$ of the tree rooted in $\chi_{kσ}(x_0)$. The vertex $γ_r$ has exactly two distinct children, unless the discriminant of the quadratic equation $x^2 - \frac{2}{k_σ}x + 1 = 0$ is zero, namely $γ_r^2 - 4k_σ^2 = 0$. This latter happens if and only if $γ_r = ±2k_σ$. We prove now that

$$\chi_{kσ}(2k_σ) = -7;$$
$$\chi_{kσ}(-2k_σ) = τ + 3.$$

Actually, both the assertions can be proved by explicit computation. Let us consider the first assertion.

$$\chi_{kσ}(2k_σ) = \frac{3k_σ + \frac{5}{2}}{\frac{k_σ + \frac{5}{2}}{3k_σ + 1}} = \frac{7k_σ - \frac{7}{2}}{\frac{k_σ + \frac{7}{2}}{3k_σ + 1}} = -7.$$

Finally consider the second assertion. We have that

$$\chi_{kσ}(-2k_σ) = \frac{-k_σ + \frac{5}{2}}{\frac{k_σ + \frac{5}{2}}{3k_σ + 1}} = \frac{11k_σ + \frac{9}{2}}{\frac{k_σ + \frac{9}{2}}{3k_σ + 1}} = -σ + 4 = -σ^2 + 2 = τ + 3$$

by Lemma 4.13. By the same lemma,

$$η_{kσ}(-7) = σ + 3 \quad \text{and} \quad η_{kσ}(σ + 3) = σ + 3,$$

while

$$η_{kσ}(τ + 3) = ∞ \quad \text{and} \quad η_{kσ}(∞) = ∞.$$

Hence, the thesis follows. □
4.2. Structure of the graphs $G^{p^n}_{0,\omega}$. As stated in the first part of the current section, the graphs $G^{p^n}_{0,\omega}$ are isomorphic to the graphs $G^{p^n}_{0,\eta}$. Hence we can study the former relying upon the structure of the latter ones.

**Example 4.14.** Let $p = 53$. Then, the two roots in $F_p$ of the equation

$$x^2 + \frac{1}{2}x + \frac{1}{2} = 0$$

are

$$k_\omega = 7 \quad \text{and} \quad k_\varpi = 19,$$

being

$$\omega = 15 \quad \text{and} \quad \varpi = 39.$$

In this example we aim at describing thoroughly the structure of the graphs $G_{53}^7$ and $G_{53}^3$. At first we notice that $|E(F_{53})| = 64$ and that the representation of the Frobenius endomorphism $\pi_{53}$ as an element of $R$ is

$$\pi_{53} = -7 + 4\alpha,$$

being $\alpha = \frac{1+\sqrt{-7}}{2}$.

We focus now on the graph $G_{53}^7 \simeq G_{53}^3$. We notice that $\alpha \equiv 15 \pmod{\pi_{53}}$. Therefore we define $\rho_0 = \alpha$ and study the iterations of the map $\eta_7$ on $A_1$ by means of the iterations of $[\rho_0]$ on $S \cong R/(\pi_{53} - 1)R$. We have that

$$S = R/\rho_0^4R \times R/\rho_0^2R,$$

where $\rho_1 = \bar{\eta}_0$. Since $e_0 = 4$, the depth of the trees rooted in elements of $A_1$ is 4. The $\eta_7$-periodic elements in $A_1$ are $x$-coordinates of the points $P = (0, P_1)$ in $S$. In $R/\rho_0^2R$ there are 2 points of additive order 4, which give rise to a cycle of length 1, there is 1 point of additive order 2, which gives rise to a cycle of length 1, and one more point of order 1, which gives rise to one more cycle of length 1.

We concentrate now on the iterations of $\eta_7$ on $B_1$. To do that we consider the iterations of $[\rho_0]$ on $S \cong R/(\pi_{53} + 1)R$. We have that

$$S = \prod_{i=0}^2 R/\rho_iR,$$

where

- $\rho_1 = \bar{\eta}_0$;
- $\rho_2 = -3 + 2\alpha$ (and $N(\rho_2) = 11$).

Since $e_0 = 1$, the depth of the trees rooted in the elements of $B_1$ is 1. The $\eta_7$-periodic elements in $B_1$ are $x$-coordinates of the points $P = (0, P_1, P_2)$ in $S$ such that, if $P_1$ has additive order 2 in $R/\rho_1R$ (namely $P_1 \neq 0$), then $P_2 \neq 0$ by Theorem 4.12

In $S$ there are exactly 10 points $P$ where $P_1 \neq 0$ and $P_2 \neq 0$. The smallest among the positive integers $s$ such that $\rho_1$ divides either $\rho_0^s + 1$ or $\rho_0^s - 1$ is 1. Moreover, the smallest among the positive integers $s$ such that $\rho_2$ divides either $\rho_0^s + 1$ or $\rho_0^s - 1$ is 5. We can conclude that the 10 points we are considering give rise to 1 cycle of length 5. The remaining $\eta_7$-periodic elements are $x$-coordinates of the 10 points $P = (0, 0, P_2) \in S$, where $P_2 \neq 0$. Such points give rise to another cycle of length 5.

The graph $G_{53}^3$, isomorphic to $G_{53}^7$, is below represented. We notice that the vertex labels, different from $\infty$ and ‘0’ (the zero in $F_{53}$), refer to the exponents of the powers $\gamma^i$ for $0 \leq i \leq 51$, being $\gamma$ a root of the Conway polynomial $x-2 \in F_{53}[x]$.

The following 3 connected components are due to the elements of $A_1$. 


The following 2 connected components are due to the elements of \( B_1 \).

\[
\begin{array}{c}
\includegraphics[width=\textwidth]{diagram.png}
\end{array}
\]

We focus now on the graph \( G_{G_{\eta_{19}}}^{53} \cong G_{\bar{\eta}_{19}}^{53} \). Since \( \bar{\pi} \equiv 39 \pmod{\pi_{53}} \), we define \( \rho_0 = \overline{\alpha} \) and study the iterations of the map \( \eta_{19} \) on \( A_1 \) by means of the iterations of \( [\rho_0] \) on \( S \cong R/(\pi_{53} - 1)R \). We have that

\[
S = R/\rho_0^2R \times R/\rho_1^4R,
\]

where \( \rho_1 = \overline{\alpha} \). Since \( \epsilon_1 = 2 \), the depth of the trees rooted in the elements of \( A_1 \) is 2. The \( \eta_{19} \)-periodic elements in \( A_1 \) are \( x \)-coordinates of the points \( P = (0, P_1) \) in \( S \). The additive order of \( P_1 \) (and \( P \)) in \( R/\rho_1^4R \) (in \( S \)) can be 16, 8, 4, 2, or 1. The 8 points \( P \) of additive order 16 give rise to 1 cycle of length 4, since 4 is the smallest among the positive integers \( s \) such that \( \rho_1 \) divides either \( \rho_0^s + 1 \) or \( \rho_0^s - 1 \). In a similar way we get that in \( G_{g_{\eta_{19}}}^{53} \) there is 1 cycle of length 2 due to the 4 points of additive order 8 and 3 cycles of length 1 each due respectively to the 2 points of additive order 4, to the only point of order 2 and to the only point of order 1 (namely the point \( (0, 0) \)).

We concentrate now on the iterations of \( \eta_{19} \) on \( B_1 \). To do that we consider the iterations of \( [\rho_0] \) on \( S \cong R/(\pi_{53} + 1)R \). In this case we have that

\[
S = \prod_{i=0}^{2} R/\rho_i R,
\]

where

\[
\begin{align*}
\rho_1 & = \overline{\alpha}; \\
\rho_2 & = -3 + 2\alpha \quad \text{and} \quad N(\rho_2) = 11.
\end{align*}
\]

The dynamics of \( [\rho_0] \) on \( B_1 \) can be described employing the same arguments used for the description of the dynamics of \( [\rho_0] \) over \( B_1 \) in the graph \( G_{G_{\eta_{19}}}^{53} \) (actually, the connected components formed by the elements of the current set \( B_1 \) are isomorphic to the connected components corresponding to the former set \( B_1 \)).

The graph \( G_{G_{\eta_{19}}}^{53} \), isomorphic to \( G_{\bar{\eta}_{19}}^{53} \), is represented below. Firstly we represent the 5 connected components due to the elements of \( A_1 \).
Now we represent the 2 connected components due to the elements of $B_1$.

References

1. W. J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl. 83 (1981), no. 1, 264–274.
2. S. Lang, *Elliptic functions*, Springer-Verlag, New York, 1987.
3. J. S. Milne, *Elliptic curves*, BookSurge Publishers, Charleston, 2006.
4. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
5. S. Ugolini, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.
6. S. Ugolini, *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two*, Theory and Applications of Finite Fields, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI, 2012.
7. S. Ugolini, *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three and five*, Journal of Number Theory 133 (2013), 1207–1228.
8. C. Wittmann, *Group structure of elliptic curves over finite fields*, Journal of Number Theory 88 (2001), 335–344.

E-mail address: sugolini@gmail.com