FIBONACCI SEQUENCES OF QUATERNIONS

MARCO ABRATE

ABSTRACT. In this paper Fibonacci sequences of quaternions are introduced, generalizing Fibonacci sequences over commutative rings, and properties of such sequences are investigated. In particular we are concerned with two kinds of Fibonacci sequences of generalized quaternions over finite fields $\mathbb{F}_p$, with p an odd prime, and their periods.

1. INTRODUCTION

Let u, v be invertible elements of an arbitrary field $\mathbb{F}$ with characteristic not 2 and let $\left(\frac{u,v}{\mathbb{F}}\right)$ be a generalized quaternion algebra over $\mathbb{F}$. $\left(\frac{u,v}{\mathbb{F}}\right)$ is a four-dimensional vector space over $\mathbb{F}$ with the four basis elements $1, i_1, i_2, i_3$ satisfying the following multiplication laws:

$$i_1^2 = u, \quad i_2^2 = v, \quad i_3 = i_1 i_2 = -i_2 i_1,$$

and 1 acting as the unit element. Since the ring homomorphism

$$\begin{aligned} \mathbb{F} &\longrightarrow \left(\frac{u,v}{\mathbb{F}}\right) \\ c &\longmapsto c1 \end{aligned}$$

injects $\mathbb{F}$ into $\left(\frac{u,v}{\mathbb{F}}\right)$ we consider $\mathbb{F} \subset \left(\frac{u,v}{\mathbb{F}}\right)$.

For $q = (q_0, q_1, q_2, q_3)$ in $\left(\frac{u,v}{\mathbb{F}}\right)$, where $q_0, q_1, q_2, q_3 \in \mathbb{F}$ are the components of q with respect to $1, i_1, i_2, i_3$, let $\overline{q} = (q_0, -q_1, -q_2, -q_3)$ be the conjugate of q; define as usual *trace* and *norm* of a quaternion by

$$Tr(q) = q + \overline{q} \quad \text{and} \quad N(q) = q\overline{q}.$$

Furthermore, we introduce the function δ by setting

$$\delta(q) = q_0^2 - N(q). \tag{1.1}$$

Denote by $\left(\frac{u,v}{\mathbb{F}}\right)^*$ the group of all invertible elements of $\left(\frac{u,v}{\mathbb{F}}\right)$. It is well-known that $\left(\frac{u,v}{\mathbb{F}}\right)^*$ coincides with the set of quaternions q such that $N(q) \neq 0$ and $q^{-1} = N(q)^{-1}\overline{q}$.

In [4] Fibonacci quaternions were introduced as the elements of the algebra of real quaternions whose components are Fibonacci numbers, and in [5] quaternions whose components are generalized Fibonacci numbers or products of generalized Fibonacci numbers were considered. Our approach is different, as our purpose is to examine recurring sequences in any quaternion algebra defined by a linear equation, extending the definition of Fibonacci sequence in commutative rings.

Let $\left(\frac{u,v}{\mathbb{F}}\right)[x]$ be the polynomial ring over $\left(\frac{u,v}{\mathbb{F}}\right)$, and let $P(x)$ be a monic second degree left polynomial in $\left(\frac{u,v}{\mathbb{F}}\right)[x]$:

$$P(x) = x^2 - ax + b. \tag{1.2}$$

Definition 1.1. *If $P(x)$ is a polynomial as in Equation (1.2), the (left) Fibonacci sequence of quaternions $U = U(a,b)$ with characteristic polynomial $P(x)$ is the recurring sequence of the second order with initial values 1 and a defined by the following relations:*

$$\begin{cases} U_1 = 1, \\ U_2 = a, \\ U_n = aU_{n-1} - bU_{n-2}, \text{ for all } n > 2. \end{cases}$$

If $N(b) \neq 0$ we can define the terms U_n of the sequence U for negative values of n:

$$U_{n-2} = b^{-1}(aU_{n-1} - U_n) \quad \text{for all } n \leq 2. \tag{1.3}$$

An important relation between the roots of the characteristic polynomial $P(x)$ and the terms of the Fibonacci sequence with parameters a and b is stated in the next theorem.

Theorem 1.2. *Let α, β be distinct roots of $P(x)$. If $\alpha - \beta$ is invertible and n is a positive integer*

$$U_n = (\alpha^n - \beta^n)(\alpha - \beta)^{-1}. \tag{1.4}$$

Furthermore, if $N(b) \neq 0$ equation (1.4) holds true for every $n \in \mathbb{Z}$.

Proof. Let us suppose that α, β are roots of $P(x)$ and that $\alpha - \beta$ is invertible. For $n = 1$

$$(\alpha - \beta)(\alpha - \beta)^{-1} = 1 = U_1,$$

and for $n = 2$

$$(\alpha^2 - \beta^2)(\alpha - \beta)^{-1} = (a\alpha - b - a\beta + b)(\alpha - \beta)^{-1} = a = U_2.$$

Now let $n > 2$ and suppose that (1.4) is true for $n-1$ and $n-2$. Then

$$\begin{aligned} (\alpha^n - \beta^n)(\alpha - \beta)^{-1} &= (\alpha^2\alpha^{n-2} - \beta^2\beta^{n-2})(\alpha - \beta)^{-1} \\ &= (a\alpha^{n-1} - b\alpha^{n-2} - a\beta^{n-1} + b\beta^{n-2})(\alpha - \beta)^{-1} \\ &= (a(\alpha^{n-1} - \beta^{n-1}) - b(\alpha^{n-2} - \beta^{n-2}))(\alpha - \beta)^{-1} \\ &= aU_{n-1} - bU_{n-2} = U_n. \end{aligned}$$

If $N(b) \neq 0$, since $b = ax - x^2 = (a - x)x$, it follows that

$$N(b) = N(a - x)N(x) \neq 0,$$

that is every root of $P(x)$ is invertible. Hence the same argument as above can be applied to Equation (1.3) to prove the theorem when for $n \leq 0$. □

Equation (1.4) is analogous to the Binet formula for the terms of the Fibonacci sequences in the commutative case. It will be very useful in the following to deduce properties on the terms of the Fibonacci sequences of quaternions when the powers of the roots of the characteristic polynomial P are known. Recall that the positive powers of q can be determined by equation

$$q^n = F_n q - N(q)F_{n-1}, \tag{1.5}$$

where F_k are the kth terms of the generalized Fibonacci sequence with parameters $Tr(q)$ and $N(q)$ [2].

In particular, if $\mathbb{F}$ is a finite field with m elements we have the following lemma.

Lemma 1.3. *Let* $\left(\frac{u,v}{\mathbb{F}}\right)$ *be a generalized quaternion algebra over a finite field with characteristic not* 2 *and* $|\mathbb{F}| = m$ *and let* $q \in \left(\frac{u,v}{\mathbb{F}}\right)$. *If* $\delta(q) \neq 0$ *then* $q^m = q$ *or* $q^m = \overline{q}$ *according as* $\delta(q)$ *is a square in* $\mathbb{F}$ *or not.*

Proof. Suppose $q \in \left(\frac{u,v}{\mathbb{F}}\right)$ and $\delta(q) \neq 0$. Let $F = F(Tr(q), N(q))$ be the generalized Fibonacci sequence with parameters $Tr(q)$ and $N(q)$ in $\mathbb{F}$. The discriminant of F is

$$Tr(q)^2 - 4N(q) = 4\delta(q) \neq 0.$$

If $\delta(q)$ is a square in $\mathbb{F}$ then the period of F in $\mathbb{F}$ divides m, that is $F_{m-1} = 0$, $F_m = 1$ and, by Equation (1.5),

$$q^m = F_m q - N(q)F_{m-1} = q.$$

If $\delta(q)$ is not a square in $\mathbb{F}$ the period of F in $\mathbb{F}$ divides m^2: we have $F_{m+1} = 0$, $F_m = -1$ and $N(q)F_{m-1} = -Tr(q)$. Then by Equation (1.5)

$$q^m = F_m q - N(q)F_{m-1} = -q + Tr(q) = \overline{q}.$$

□

2. Fibonacci sequences over finite fields

In this section we deal with the Fibonacci sequences in quaternion algebras over finite fields. It is known [3, Theorems 9.7 and 9.8] that if u, v are invertible in the field $\mathbb{F}_p$ with p elements and p is an odd prime, the structure of the quaternion algebra $\left(\frac{u,v}{\mathbb{F}_p}\right)$ over $\mathbb{F}_p$ does not depend on u and v. Throughout we denote by $\mathbf{H}_p$ the quaternion algebra over $\mathbb{F}_p$ and, if $r \in \mathbb{F}_p$, $\left(\frac{r}{p}\right)$ denote the Legendre symbol, that is

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } r \text{ is a quadratic residue mod } p \\ 0 & \text{if } p|r \\ -1 & \text{if } r \text{ is a quadratic nonresidue mod } p. \end{cases}$$

We begin a study of any Fibonacci sequence of quaternions $U = U(a, b)$ starting from properties of the roots of its characteristic polynomial $P(x) = x^2 - ax + b \in \mathbf{H}_p[x]$. In order to do this it is convenient to introduce the following auxiliary parameters:

$$\begin{aligned} \hat{a} &= 4^{-1}Tr(a), \\ \tau &= Tr(ab) - 2\hat{a}(\delta(a) + Tr(b)), \\ \lambda &= Tr(b) - 2\hat{a}^2 - \delta(a), \\ \nu &= N(b) + \hat{a}^2(\hat{a}^2 - \delta(a) + Tr(b)) - \hat{a}(Tr(a)Tr(b) - Tr(ab)), \\ \mu &= \delta(a)^2 - 4\delta(b) + Tr(a)\left(\tau + \hat{a}\delta(a)\right), \end{aligned}$$

and the auxiliary polynomials in $\mathbb{F}_p[x]$:

$$\begin{aligned} c_{a,b}(x) &= x^6 + 2\lambda x^4 + (\lambda^2 - 4\nu)x^2 - \tau^2, \\ d_{a,b}(x) &= x^6 + 4\lambda x^4 + 4\lambda^2 x^2 - 4\tau^2, \\ e_{a,b}(x) &= x^8 - 2\delta(a)x^6 + \mu x^4 + 2\tau^2 x^2 - \delta(a)\tau^2. \end{aligned}$$

We can identify different kinds of sequences depending on the relations between a, b and p. In the following, two kinds of Fibonacci sequences are considered, namely *Fibonacci sequences of the first* and *of the second kind*.

3. Fibonacci Sequences of the First Kind

Definition 3.1. *Let p be an odd prime. A* sequence of the first kind with respect to p *is a Fibonacci sequence of quaternions with parameters a and b such that*

$$\tau\delta(a)\left(4\delta(a)(b_0^2 - \nu) - \tau^2\right) \not\equiv 0 \pmod{p}. \tag{3.1}$$

If a and b are such to satisfy Equation (3.1), the roots of the characteristic polynomial of U are given by Theorem 2.5 of [1] and are at most six in $\mathbb{K} \otimes \mathbf{H}_p$, where $\mathbb{K}$ is an algebraic closure of $\mathbb{F}$. Moreover we know that their traces are solutions of equation $c_{a,b}(x + 2\hat{a}) \equiv 0 \pmod{p}$, where

$$c_{a,b}(x) = x^6 + 2\lambda x^4 + (\lambda^2 - 4\nu)x^2 - \tau^2$$

is a polynomial in $\mathbb{F}_p[x]$. If $t \in \mathbb{K}$ is a root of $c_{a,b}(x)$ there exists a pair of roots α, β of the characteristic polynomial $P(x)$ of U such that $Tr(\alpha) + 2\hat{a} = -(Tr(\beta) + 2\hat{a}) = t$:

$$\begin{aligned} \alpha &= \frac{(t + a - (\delta(a)t)^{-1}\tau a')}{2} + \frac{(t + a')\left(b - \overline{b} - (2\hat{a} + \delta(a)^{-1}\tau)a'\right)}{2(\delta(a) - t^2)}, \\ \beta &= \frac{(-t + a + (\delta(a)t)^{-1}\tau a')}{2} + \frac{(-t + a')\left(b - \overline{b} - (2\hat{a} + \delta(a)^{-1}\tau)a'\right)}{2(\delta(a) - t^2)}, \end{aligned} \tag{3.2}$$

where $a' = a - 2\hat{a}$.

The next theorem gives a sufficient condition for applying Theorem 1.2 to evaluate the terms of U.

Theorem 3.2. *Let*

$$e_{a,b}(x) = x^8 - 2\delta(a)x^6 + \mu x^4 + 2\tau^2 x^2 - \delta(a)\tau^2.$$

If $c_{a,b}(x)$ does not divide $e_{a,b}(x)$ then there are two distinct roots α, β of $P(x)$ such that

$$Tr(\alpha) + Tr(\beta) + Tr(a) = 0 \quad \text{and} \quad \alpha - \beta \in (\mathbb{K} \otimes \mathbf{H}_p)^*.$$

Proof. Let us consider two distinct roots α, β of $P(x)$ such that

$$Tr(\alpha) + 2\hat{a} = -(Tr(\beta) + 2\hat{a}) = t.$$

By the equations in (3.2) it follows that

$$\alpha - \beta = t - (\delta(a)t)^{-1}\tau(a - 2\hat{a}) + t(\delta(a) - t^2)^{-1}\left(b - \overline{b} - \delta(a)^{-1}(2\hat{a}\delta(a) + \tau)(a - 2\hat{a})\right)$$

and, by direct calculation,

$$N(\alpha - \beta) = (t^2(t^2 - \delta(a))^2)^{-1}\left(t^8 - 2\delta(a)t^6 + \mu t^4 + 2\tau^2 t^2 - \tau^2\delta(a)\right).$$

So $\alpha - \beta$ is invertible if and only if t is not among the roots of the polynomial

$$e_{a,b}(x) = x^8 - 2\delta(a)x^6 + \mu x^4 + 2\tau^2 x^2 - \delta(a)\tau^2.$$

Hence, if $c_{a,b}(x) \nmid e_{a,b}(x)$ there is a pair α, β of roots of $P(x)$ such that $Tr(\alpha) + Tr(\beta) = -Tr(a)$ and $N(\alpha - \beta) \neq 0$. □

Theorem 3.3. *Let U be the Fibonacci sequence of quaternions of the first kind with respect to p and with characteristic polynomial $P(x) = x^2 - ax + b$. If $c_{a,b}(x) \nmid e_{a,b}(x)$ then there are two distinct roots α, β of $P(x)$ such that $Tr(\alpha) + Tr(\beta) + Tr(a) = 0$ and*

$$U_n = (\alpha^n - \beta^n)(\alpha - \beta)^{-1}.$$

Proof. This theorem immediately follows by Theorem 1.2 and Theorem 3.2. □

Let us introduce the following polynomial in $\mathbb{F}_p[x]$:

$$\tilde{c}_{a,b}(x) = x^3 + 2\lambda x^2 + \left(\lambda^2 - 4\nu\right) x - \tau^2. \tag{3.3}$$

Since $c_{a,b}(x) = \tilde{c}_{a,b}(x^2)$, we can use $\tilde{c}_{a,b}(x)$ to determine the splitting field of $c_{a,b}(x)$, and then the quaternion algebra containing all the roots of $P(x)$.

From now on $N_p(\tilde{c}_{a,b}(x))$ will denote the number of roots of $\tilde{c}_{a,b}(x)$ in $\mathbb{F}_p$. (See [6] for a full discussion on the number of roots of third degree polynomials over finite fields).

Theorem 3.4. *Let $c_{a,b}(x)$ and $\tilde{c}_{a,b}(x)$ be as above. If $N_p(\tilde{c}_{a,b}(x)) = 0$ then $c_{a,b}(x)$ is completely reducible in $\mathbb{F}_{p^3}$.*

Proof. Denote by $\gamma_1, \gamma_2, \gamma_3$ the roots of $\tilde{c}_{a,b}(x)$. Since $N_p(\tilde{c}_{a,b}(x)) = 0$ we have $\gamma_i \in \mathbb{F}_{p^3}$, and $\gamma_i^{p^3-1} = 1$. But

$$\gamma_i^{\frac{p^3-1}{2}} = \left(\gamma_i^{p^2+p+1}\right)^{\frac{p-1}{2}} = \left(\gamma_1\gamma_2\gamma_3\right)^{\frac{p-1}{2}} = \left(\tau^2\right)^{\frac{p-1}{2}} = 1,$$

thus, every root of $\tilde{c}_{a,b}(x)$ is a square in $\mathbb{F}_{p^3}$, and every root of $c_{a,b}(x)$ is in $\mathbb{F}_{p^3}$. □

Theorem 3.5. *Let $P(x) = x^2 - ax + b \in \mathbf{H}_p[x]$, the characteristic polynomial of a Fibonacci sequence of the first kind with respect to p, and let $\tilde{c}_{a,b}(x) \in \mathbb{F}_p[x]$ as in Equation* (3.3)*. The polynomial $P(x)$ has six roots in $\mathbb{F}_{p^3} \otimes \mathbf{H}_p$ if $N_p(\tilde{c}_{a,b}(x)) = 0$, has six roots in $\mathbb{F}_{p^4} \otimes \mathbf{H}_p$ if $N_p(\tilde{c}_{a,b}(x)) = 1$ and has six roots in $\mathbb{F}_{p^2} \otimes \mathbf{H}_p$ if $N_p(\tilde{c}_{a,b}(x)) = 3$.*

Proof. By [6] and Theorem 3.4 the roots of $c_{a,b}(x)$ are in $\mathbb{F}_{p^3}, \mathbb{F}_{p^4}$ or $\mathbb{F}_{p^2}$ according as $N_p(\tilde{c}_{a,b}(x))$ is $0, 1$ or 3. Since the roots of $P(x)$ are determined by the roots of $c_{a,b}(x)$ as shown in [2] the assertion follows. □

To complete the study of the properties of the roots α and β of $P(x)$ as a characteristic polynomial of a Fibonacci sequence of the first kind we present the following theorems about $\delta(\alpha) \bmod p$ and $\delta(\beta) \bmod p$.

Theorem 3.6. *Let $a, b \in \mathbf{H}_p$ be parameters of a Fibonacci sequence U of the first kind with respect to p and let $P(x)$ be the characteristic polynomial of U. Let $d_{a,b}(x) \in \mathbb{F}_p[x]$ be the polynomial*

$$d_{a,b}(x) = x^6 + 4\lambda x^4 + 4\lambda^2 x^2 - 4\tau^2.$$

If $\gcd(c_{a,b}(x), d_{a,b}(x)) = 1$ and if α is a root of $P(x)$ then

$$\delta(\alpha) \not\equiv 0 \pmod{p}.$$

Proof. Let α be a root of $P(x)$. We know that there exists a root $\beta \neq \alpha$ of $P(x)$ such that $Tr(\alpha) + Tr(\beta) + Tr(a) = 0$. We can assume, without any loss of generality, that such roots are given by the equations in (3.2). Setting $t = Tr(\alpha) + 2\hat{a}$ one has

$$4\delta(\alpha) = t^2 - 2t^2 - 2(Tr(b) - 2\hat{a}^2) + 2\delta(a) - t^{-1}\tau = -t^{-1}\left(t^3 + 2\lambda t + \tau\right),$$

and

$$4\delta(\beta) = t^2 - 2t^2 - 2(Tr(b) - 2\hat{a}^2) + 2\delta(a) + t^{-1}\tau = -t^{-1}\left(t^3 + 2\lambda t - \tau\right),$$

thus, $\delta(\alpha)\delta(\beta) \equiv 0 \pmod{p}$ if and only if

$$\left(t^3 + 2\lambda t + \tau\right)\left(t^3 + 2\lambda t - \tau\right) \equiv 0 \pmod{p},$$

if and only if t is a root of $d_{a,b}(x)$ and $c_{a,b}(x)$.

It follows that if $\gcd(c_{a,b}(x), d_{a,b}(x)) = 1$

$$\delta(\alpha) \not\equiv 0 \pmod{p}.$$

□

Let us denote by $W(p)$ the period of the Fibonacci sequence $U = U(a, b)$ modulo p.

Theorem 3.7. *Let $a, b \in \mathbf{H}_p$ be parameters of a Fibonacci sequence U of the first kind with respect to p and let $P(x) = x^2 - ax + b$ be the characteristic polynomial of U. If $c_{a,b}(x) \nmid e_{a,b}(x)$ and $\gcd(c_{a,b}(x), d_{a,b}(x)) = 1$ then*

$$\begin{aligned} W(p) | p^6 - 1 \quad &\text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 0, \\ W(p) | p^8 - 1 \quad &\text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 1, \\ W(p) | p^4 - 1 \quad &\text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 3. \end{aligned}$$

Proof. Since $c_{a,b}(x)$ does not divide $e_{a,b}(x)$, by Theorem 3.2 there are two roots α, β of $P(x)$ such that $Tr(\alpha) + Tr(\beta) + Tr(a) = 0$ and $N(\alpha - \beta) \not\equiv 0 \pmod{p}$, and those roots can be used to obtain the nth term of the sequence U by (1.4). Furthermore, by Theorem 3.6 $\delta(\alpha)\delta(\beta) \not\equiv 0 \pmod{p}$.

If $N_p(\tilde{c}_{a,b}(x)) = 0$, by Theorem 3.5 $\alpha, \beta \in \mathbb{F}_{p^3} \otimes \mathbf{H}_p$. Thus, setting $n = kp^6 + m$, by Lemma 1.3 we have

$$\begin{aligned} U_{p^6k+m} &= (\alpha^{p^6k+m} - \beta^{p^6k+m})(\alpha - \beta)^{-1} \\ &= (\alpha^{p^6k}\alpha^m - \beta^{p^6k}\beta^m)(\alpha - \beta)^{-1} \\ &\equiv (\alpha^{k+m} - \beta^{k+m})(\alpha - \beta)^{-1} \equiv U_{k+m} \pmod{p}. \end{aligned}$$

If $N_p(\tilde{c}_{a,b}(x)) = 1$ then $c_{a,b}(x)$ has all the roots in $\mathbb{F}_{p^4}$ and $\alpha, \beta \in \mathbb{F}_{p^4} \otimes \mathbf{H}_p$. Thus for $n \in \mathbb{N}$, $n = kp^8 + m$

$$\begin{aligned} U_{kp^8+m} &= (\alpha^{p^8k+m} - \beta^{p^8k+m})(\alpha - \beta)^{-1} \\ &= (\alpha^{p^8k}\alpha^m - \beta^{p^8k}\beta^m)(\alpha - \beta)^{-1} \\ &\equiv \alpha^{k+m} - \beta^{k+m})(\alpha - \beta)^{-1} \equiv U_{k+m} \pmod{p}. \end{aligned}$$

Finally, if $N_p(\tilde{c}_{a,b}(x)) = 3$ all the roots of $c_{a,b}(x)$ are in $\mathbb{F}_{p^2}$, and $\alpha, \beta \in \mathbb{F}_{p^2} \otimes \mathbf{H}_p$. Hence, for $n \in \mathbb{N}$, setting $n = kp^4 + m$ we have

$$\begin{aligned} U_{kp^4+m} &= (\alpha^{p^4k+m} - \beta^{p^4k+m})(\alpha - \beta)^{-1} \\ &= (\alpha^{p^4k}\alpha^m - \beta^{p^4k}\beta^m)(\alpha - \beta)^{-1} \\ &\equiv (\alpha^{k+m} - \beta^{k+m})(\alpha - \beta)^{-1} \equiv U_{k+m} \pmod{p}. \end{aligned}$$

□

Theorem 3.8. *Let $P(x) = x^2 - ax + b$ be the recurring polynomial of the Fibonacci sequence of quaternions U of the first kind, and $N(b) \neq 0$.*

If $c_{a,b}(x) \nmid e_{a,b}(x)$ and $\gcd(c_{a,b}(x), d_{a,b}(x)) = 1$ then for every $k \in \mathbb{Z}$

$$\begin{aligned} U_{k(p^6-1)} &\equiv 0 \pmod{p} \quad \text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 0, \\ U_{k(p^8-1)} &\equiv 0 \pmod{p} \quad \text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 1, \\ U_{k(p^4-1)} &\equiv 0 \pmod{p} \quad \text{if} \quad N_p(\tilde{c}_{a,b}(x)) = 3. \end{aligned}$$

Proof. If $N(b) \neq 0$, we have $U_0 = b^{-1}(a - a) = 0$. Since the order of U divides $p^6 - 1, p^8 - 1$ or $p^4 - 1$ according as $N_p(\tilde{c}_{a,b}(x)) = 0, 1$ or 3, applying Theorem 3.7 the assertion follows. □

4. Fibonacci Sequences of the Second Kind

Definition 4.1. *Let p be an odd prime. The Fibonacci sequence of quaternions $U = U(a, b)$ with parameters a and b is said to be of the second kind with respect to p if*

$$\delta(a)\nu(\lambda^2 - 4\nu) \not\equiv 0 \pmod{p} \quad \text{and} \quad \tau \equiv 0 \pmod{p}.$$

Since a and b are such that $\tau \equiv 0 \pmod{p}$ it follows that $c_{a,b}$ has 0 as a double root and by [1] (Theorem 2.5) there are two roots of $P(x)$, namely α and β, such that $Tr(\alpha) = Tr(\beta) = 2\hat{a}$:

$$\begin{aligned} \alpha &= \frac{-2\hat{a}(\lambda^2 - 4\nu)^{\frac{1}{2}} + \left(\delta(a) - (\lambda^2 - 4\nu)^{\frac{1}{2}}\right) a + 2(a - 2\hat{a})(b - \bar{b})}{2\delta(a)}, \\ \beta &= \frac{2\hat{a}(\lambda^2 - 4\nu)^{\frac{1}{2}} + \left(\delta(a) + (\lambda^2 - 4\nu)^{\frac{1}{2}}\right) a + 2(a - 2\hat{a})(b - \bar{b})}{2\delta(a)}. \end{aligned} \tag{4.1}$$

It is easy to check that

$$\begin{aligned} \delta(\alpha) &= -2^{-1}\lambda + 2^{-1}(\lambda^2 - 4\nu)^{\frac{1}{2}}, \\ \delta(\beta) &= -2^{-1}\lambda - 2^{-1}(\lambda^2 - 4\nu)^{\frac{1}{2}}. \end{aligned} \tag{4.2}$$

Moreover $\alpha - \beta = (a - 2\hat{a})\delta(a)^{-1}(\lambda^2 - 4\nu)^{\frac{1}{2}}$ and

$$N(\alpha - \beta) = -\delta(a)^{-1}(\lambda^2 - 4\nu). \tag{4.3}$$

Since $\lambda^2 - 4\nu \not\equiv 0 \pmod{p}$ the terms of U are given by formula (1.4) using α and β as in Equations (4.1).

By [1] we know that if $\left(\dfrac{\lambda^2 - 4\nu}{p}\right) = 1$ then $\alpha, \beta \in \mathbf{H}_p$, while if $\left(\dfrac{\lambda^2 - 4\nu}{p}\right) = -1$ then $\alpha, \beta \in \mathbb{F}_{p^2} \otimes \mathbf{H}_p$.

We can prove the following theorems about the order $W(p)$ of the sequence of the second kind U.

Theorem 4.2. *Let $P(x) = x^2 - ax + b \in \mathbf{H}_p[x]$ be the characteristic polynomial of U such that*

$$\delta(a)\nu(\lambda^2 - 4\nu) \not\equiv 0 \pmod{p} \quad \text{and} \quad \tau \equiv 0 \pmod{p},$$

and let α *be a root of* $P(x)$ *as in Equation* (4.1). *If* $\left(\frac{\lambda^2-4\nu}{p}\right)=1$ *and* $\left(\frac{\nu}{p}\right)=1$ *then*

$$U_p \equiv \left(\frac{\delta(\alpha)}{p}\right) \pmod{p}$$
$$U_{p+1} \equiv \left(\frac{\delta(\alpha)}{p}\right)(a-\hat{a})+\hat{a} \pmod{p}.$$

Furthermore, if $\left(\frac{\delta(\alpha)}{p}\right)=1$ *then* $W(p)|p-1$, $W(p)|p^2-1$, *otherwise.*

Proof. By the equations in (4.2) we have

$$\delta(\alpha)\delta(\beta)=4^{-1}\left(\lambda^2-\lambda^2+4\nu\right)=\nu. \tag{4.4}$$

Hence,

$$\left(\frac{\delta(\alpha)\delta(\beta)}{p}\right)=\left(\frac{\nu}{p}\right)$$

and

$$\left(\frac{\delta(\alpha)}{p}\right)=\left(\frac{\delta(\beta)}{p}\right). \tag{4.5}$$

Evaluating the pth term of the Fibonacci sequence, bearing in mind that $Tr(\alpha-\beta)\equiv 0 \pmod{p}$, we get

$$\begin{aligned} U_p &= (\alpha^p-\beta^p)(\alpha-\beta)^{-1} \\ &\equiv 2^{-1}\left(\left(\frac{\delta(\alpha)}{p}\right)(\alpha-\overline{\alpha})-\left(\frac{\delta(\beta)}{p}\right)(\beta-\overline{\beta})\right)(\alpha-\beta)^{-1} \\ &\equiv 2^{-1}\left(\frac{\delta(\alpha)}{p}\right)(\alpha-\beta-\overline{(\alpha-\beta)})(\alpha-\beta)^{-1} \\ &\equiv \left(\frac{\delta(\alpha)}{p}\right)(\alpha-\beta)(\alpha-\beta)^{-1}\equiv\left(\frac{\delta(\alpha)}{p}\right) \pmod{p}. \end{aligned}$$

Suppose $\left(\frac{\delta(\alpha)}{p}\right)=1$. By Equation (4.5), $\left(\frac{\delta(\beta)}{p}\right)=1$ and by Lemma 1.3 $\alpha^p\equiv\alpha \pmod{p}$, $\beta^p\equiv\beta \pmod{p}$, so that

$$U_{p+1}=(\alpha^{p+1}-\beta^{p+1})(\alpha-\beta)^{-1}\equiv(\alpha^2-\beta^2)(\alpha-\beta)^{-1}\equiv a \pmod{p}, \tag{4.6}$$

and the period of U divides $p-1$.

Otherwise, if $\delta(\alpha)$ is a quadratic nonresidue mod p by Lemma 1.3, $\alpha^p=\overline{\alpha}$ and $\beta^p=\overline{\beta}$, and

$$\begin{aligned} U_{p+1} &= (\alpha^{p+1}-\beta^{p+1})(\alpha-\beta)^{-1}\equiv(N(\alpha)-N(\beta))(\alpha-\beta)^{-1} \\ &\equiv -(\delta(\alpha)-\delta(\beta))(\alpha-\beta)^{-1}. \end{aligned}$$

Furthermore by Equation (4.3), we have

$$(\alpha-\beta)^{-1}\equiv(\lambda^2-4\nu)^{-1/2}(a-2\hat{a}) \pmod{p}.$$

On the other hand by the equations in (4.2) it follows $\delta(\alpha)-\delta(\beta)\equiv(\lambda^2-4\nu)^{1/2} \pmod{p}$, thus

$$U_{p+1}\equiv -(a-2\hat{a}). \tag{4.7}$$

Equations (4.6) and (4.7) can be briefly written as

$$U_{p+1} \equiv \left(\frac{\delta(\alpha)}{p}\right)(a - \hat{a}) + \hat{a} \pmod{p}.$$

Evaluating the p^2th term and the (p^2+1)th term of the sequence U we obtain

$$U_{p^2} = (\alpha^{p^2} - \beta^{p^2})(\alpha - \beta)^{-1} \equiv (\alpha - \beta)(\alpha - \beta)^{-1} \equiv 1 \pmod{p}$$

and

$$U_{p^2+1} = (\alpha^{p^2+1} - \beta^{p^2+1})(\alpha - \beta)^{-1} \equiv (\alpha^2 - \beta^2)(\alpha - \beta)^{-1} \equiv a \pmod{p},$$

that is $W(p)|p^2 - 1$. □

Theorem 4.3. *Let U be the Fibonacci sequence in $\mathbf{H}_p$ with parameters a and b, and suppose U is of the second kind with respect to p and let α be a root of $P(x)$ as in the first equation of (4.1). If*

$$\left(\frac{\lambda^2 - 4\nu}{p}\right) = \left(\frac{\nu}{p}\right) = 1$$

then if k is a positive integer

$$U_{k(p-1)} \equiv 0 \pmod{p} \quad \text{if} \quad \left(\frac{\delta(\alpha)}{p}\right) = 1,$$

$$U_{k(p^2-1)} \equiv 0 \pmod{p} \quad \text{if} \quad \left(\frac{\delta(\alpha)}{p}\right) = -1.$$

Proof. Suppose $\left(\frac{\delta(\alpha)}{p}\right) = 1$, and let $\{F_n\}$ the Fibonacci sequence with parameters $Tr(\alpha)$ and $N(\alpha)$. By Equation (1.5) we know that $\alpha^{p-1} = F_{p-1}\alpha - N(\alpha)F_{p-2}$ that is, since $\delta(\alpha)$ is a quadratic residue mod p,

$$\alpha^{p-1} = -N(\alpha)F_{p-2}.$$

Furthermore, $N(\alpha)F_{p-2} = Tr(\alpha)F_{p-1} - F_p = -1$, i.e.

$$\alpha^{p-1} = 1.$$

The same argument proves that $\beta^{p-1} = 1$, so that for every integer k we have $\alpha^{k(p-1)} = \beta^{k(p-1)} = 1$, and

$$U_{k(p-1)} = \left(\alpha^{k(p-1)} - \beta^{k(p-1)}\right)(\alpha - \beta)^{-1} \equiv 0 \pmod{p}.$$

Analogously, if $\left(\frac{\delta(\alpha)}{p}\right) = -1$ we have $\alpha^{p^2-1} = \beta^{p^2-1} = 1$ and

$$U_{k(p^2-1)} = \left(\alpha^{k(p^2-1)} - \beta^{k(p^2-1)}\right)(\alpha - \beta)^{-1} \equiv 0 \pmod{p}.$$

□

Theorem 4.4. *Let $P(x) = x^2 - ax + b \in \mathbf{H}_p[x]$ be the recurring polynomial of the Fibonacci sequence U of the second kind with respect to p with parameters a and b. If*

$$\left(\frac{\lambda^2 - 4\nu}{p}\right) = -1$$

then $W(p)|p^4 - 1$.

Proof. Our assumption on $\lambda^2 - 4\nu$ implies $\alpha, \beta \in \mathbb{F}_{p^2} \otimes \mathbf{H}_p$, where α and β are given by the equations in (4.1). Hence, by Lemma 1.3 $\alpha^{p^4} \equiv \alpha$ and $\beta^{p^4} \equiv \beta$. Thus,

$$U_{p^4} = (\alpha^{p^4} - \beta^{p^4})(\alpha - \beta)^{-1} \equiv (\alpha - \beta)(\alpha - \beta)^{-1} \equiv 1 \pmod{p}$$

and

$$U_{p^4+1} = (\alpha^{p^4+1} - \beta^{p^4+1})(\alpha - \beta)^{-1} \equiv (\alpha^2 - \beta^2)(\alpha - \beta)^{-1} \equiv a \pmod{p},$$

and it follows $W(p)|p^4 - 1$. □

Theorem 4.5. *Let $P(x) = x^2 - ax + b \in \mathbf{H}_p[x]$ be the characteristic polynomial of the Fibonacci sequence U of the second kind with respect to p with parameters a and b. If*

$$\left(\frac{\lambda^2 - 4\nu}{p}\right) = -1$$

then for every $k \in \mathbb{N}$

$$U_{k(p^4-1)} \equiv 0 \pmod{p}.$$

Proof. Since $\left(\frac{\lambda^2 - 4\nu}{p}\right) = -1$ the roots of the characteristic polynomial of the sequence U described by the equations in (4.1) are in the algebra $\mathbb{F}_{p^2} \otimes \mathbf{H}_p$. By Equation (4.4) it follows that $\delta(\alpha)$ and $\delta(\beta)$ are both invertible and by Lemma 1.3 $\alpha^{p^4-1} = \beta^{p^4-1} = 1$. This implies

$$U_{k(p^4-1)} = \left(\alpha^{k(p^4-1)} - \beta^{k(p^4-1)}\right)(\alpha - \beta)^{-1} \equiv 0 \pmod{p}.$$

□

References

[1] M. Abrate, *Quadratic Formulas for Generalized Quaternions*, Journal of Algebra and its Applications, to appear.

[2] M. Abrate, *The Root of a Generalized Quaternion*, Proceedings of the 13th International Conference on Fibonacci Numbers and Their Applications, to appear.

[3] A. J. Hahn, *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*, Springer, New York, (2002).

[4] A. F. Horadam, *Complex Fibonacci Numbers and Fibonacci Quaternions*, The American Mathematical Monthly, **70.3** (1963), 289–291.

[5] A. F. Horadam, *Quaternion Recurrence Relations*, Ulam Quarterly, **2.2** (1993), 22–33.

[6] Z.-H. Sun, *Cubic and Quartic Congruences Modulo a Prime*, Journal of Number Theory, **102.1** (2003), 41–89.

MSC2000: 11B39, 15A66

Dipartimento di Matematica, Università di Torino, Via C. Alberto 10, 10123 Torino, Italy
E-mail address: marco.abrate@unito.it