Mathematica Balkanica

Mathematical Society of South-Eastern Europe
A quarterly published by
the Bulgarian Academy of Sciences – National Committee for Mathematics

---

Mathematica
Balkanica

New Series Vol. 17, 2003, Fasc. 3-4

On Fibonacci Sequences in Nilpotent Groups

Erdal Karaduman, Huseyin Aydin

Presented by Bl. Sendov

In this paper, we will constitute 2-step Fibonacci sequences by the two generating elements of a group of exponent p(p is prime) and nilpotency class n.

Key Words: Fibonacci sequences, nilpotent group, nilpotency class

1. Introduction

The study of Fibonacci sequences in groups began with the earlier work of Wall [15], where the ordinary Fibonacci sequences in cyclic groups were investigated. In the mid eighties Wilcox extended the problem to abelian groups [16]. Prolific co-operation of Campell, Doostie and Robertson expanded the theory to some finite simple groups [6]. Aydin and Smith proved in [4] that the lengths of ordinary 2-step Fibonacci sequences are equal to the lengths of ordinary 2-step Fibonacci recurrences in finite nilpotent groups of nilpotency class 4 and a prime exponent. The theory has been generalized in [7] to the ordinary 3-step Fibonacci sequences in finite nilpotent groups of nilpotency class 2 and exponent p. Then it is shown in [2] that the period of 2-step general Fibonacci sequence is equal to the length of fundamental period of the 2-step general recurrence constructed by two generating elements of the group of exponent p and nilpotency class n.

Let (s_i) denote the ordinary Fibonacci sequence in $GF(p)$ defined by the recurrence $s_{i+2} = s_i + s_{i+1}$ with initial data $s_0 = 1$, $s_1 = 1$. This sequence or loop must be periodic. One can define sequences by a linear recurrence in any group. Let G be a finite group. We define a family of recurrences, parameterized by some integer n, via equations

$$(R_n) \qquad x_i = x_{i-1}x_{i-2}\ldots x_{i-n}.$$

We fix $n > 1$. We may start the recurrence with any initial data $g_0, g_1, \ldots, g_{n-1}$ and then the recurrence will define a periodic bi-infinite sequence indexed by the integers. The term loop is used to describe a bi-infinite sequence satisfying the recurrence. Notice that if $I \in Z$, then putting $h_i = g_{i+1}$ for $0 \leq i < n$ we obtain another set of initial data. The recurrence (R_n) then gives us another loop (h_i) of G. Notice that (h_i) is just (g_i) shifted through I steps. We say that (h_i) is a rotation of (g_i).

The fundamental period of a loop is clearly a significant number, and sometimes is called the Wall's number. Following Wall [15] the letter k is used (suitably adorned) to describe this period.

Wall investigated the recurrence R_2 in finite cyclic groups. This subject immediately reduces to the study of cyclic groups of prime power order. This paradigm is exploited elsewhere [1,5,4] to study recurrences in finite nilpotent groups, since they are the cartesian product of their Sylow -subgroups. Another early contributor to this field was Vinson [14], who was particularly interested in ranks of apparition, mistranslated from the French. More interest has come in the form of [6,9,12,13] and [16].

Wall distinguishes the special loop $s = (s_i)$ with initial data $s_0 = 0$, $s_1 = 1$ in $Z/p^n Z$. Let $k(s, p^n)$ denote the fundamental period of s.

Let us consider the more general recurrences written multiplicatively as

$$x_1 = x_{i-1}^{a_1} x_{i-2}^{a_2} \ldots x_n^{a_n},$$

or additively as

$$(A_n) \qquad x_i = \sum_{r=1}^{n} a_i x_{i-r}.$$

The exponents (coefficients) are deemed to be integers. Such a recurrence may not be so well behaved as R_n, for it may be singular in particular group. This means that initial data may not define a unique bi-infinite periodic sequence; the problem arises when attempting to extend the sequence through negative integer subscripts.

2. Two step recurrences

The theory of general two-step recurrences is very well understood. See [11], and Chapter 2 of [3]. The following result of this section is well-known [5,15].

Theorem 2.1. *Let H be the additive group of a finite field $k = GF(p')$. Consider the standard sequence $s = (s_i)$ for the recurrence A_2. Let $k(s)$ denote* *the Wall number of s. Suppose $b = (b_i)$ is any loop satisfying A_2 in H, then $k(b)$ divides $k(s)$. If $k(b) < k(s)$, then b must either be the trivial loop (all entries 0) or must be a geometric sequence [3].*

A result of this theorem is that any short loop must be trivial, or contain no entry which is zero. Suppose that b is of the latter form. Choose $i \in Z$ and let b^{+i} be the rotation of b through i steps, so $b_0^{+i} = b_i$ and $b_i^{+i} = b_{i+1}$. Put $c = b_0 b_i^{-1} b$. Thus $k(c) = k(b)$. Now $k(c - b)$ must divide $k(b)$ and so $d = c - b$ is a short loop. However, $d_0 = 0$ so d is a trivial loop. Thus $b_1 = b_0 b_i^{-1} b_{i+1}$. We conclude that $\mu = b_i^{-1} b_{i+1}$ is independent of i so b is a geometric progression with common ratio μ. The ratio μ must be a root of $x^2 + a_1 x + a^2$.

Definition 2.2. A group G is torsion-free if every nonidentity element of G has infinite order.

Definition 2.3. Let $H \triangleleft G$, $K \triangleleft G$ and $K \leq H$. If H/K is contained in the center of G/K, then H/K is called a central factor of G. A group G is called nilpotent if it has finite series of normal subgroups

$$G = G_0 \geq G_1 \geq \ldots G_r = 1$$

such that G_{i-1}/G_i is a central factor of G for each $i = 1, 2, \ldots, r$. The smallest possible r is called the nilpotency class of G.

Consider a group $H = H^Z$ with the following presentation:

$$H^Z = \langle x, y, z, t, u : [y, x] = z, [z, x] = t, [t, x] = u \rangle$$

where those pairs of generators with unspecified commutators are implicitly deemed to commute. This is a torsion-free nilpotent group of nilpotency class 4. In fact, the group is generated by x and y. Each element of the group will have a unique representation as $x^a y^b z^c t^d u^e$ where $a, b, c, d, e \in Z$. In fact, we may as well think of this group as being a rather strange group structure on Z^5. The group multiplication law will be given by rational polynomials in 10 variables, and inversion by rational polynomials in 5 variables. These polynomials must, of course, have the property that, regarded as maps, they assume integral values when supplied with integral arguments.

Let p be a prime, and work in $(Z/pZ)^5$ instead. There are no difficulties associated with this reduction modulo p, because the polynomials involved don't have primes other than 2 or 3 involved in denominators of co-efficients. We regard the variables $a, b, c, d, e \in Z$ as being in Z/pZ and obtain a group structure on $(Z/pZ)^5$. We call this group $H^{Z/pZ}$ and for $p > 3$ this will be a group of exponent p. We shall demonstrate this shortly. The natural ring epimorphism $Z \to Z/pZ$ induces a natural epimorphism of groups $\psi : H^Z \to H^{Z/pZ}$. We abuse the letters x, y, z, t, u to denote the images of the corresponding elements of H^Z under ψ.

The relatively free two generator nilpotent groups of class 4 with exponent laws 2 and 3 are,respectively, C_2XC_2 and the (class 2) extra-special group of order 27. These are, in a sense, degenerate, since for all other primes p, the relatively free two generator exponent p class 4 groups are all of genuine class 4, and have order p^8. It is on these primes which we shall focus.

We examine the details of the multiplication law of the groups $H^{Z/pZ}$. The element u is central, and the group $V = \langle y, z, t, u\rangle$ is abelian. A concrete representation of this group is to think of V as a four dimensional $GF(p)$-vector space. This space admits an automorphism β (really x) given by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The group $H^{Z/pZ}$ is then realized as the semi-direct product of V with $\langle\beta\rangle$.

Notice that the matrix of β^n is

$$\begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} \\ 0 & 1 & \binom{n}{1} & \binom{n}{2} \\ 0 & 1 & 1 & \binom{n}{1} \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

so for primes p other than and we have $\beta^p = 1$. We wish to show that for primes $p > 3$, the group $H^{Z/pZ}$ has exponent p.

Suppose $v \in V$ and that $n \in N$, then

$$(\beta^n.\nu)^p = \beta^{np}.\nu(1 + \beta^n + \cdots \beta^{n(p-1)}$$

by the definition of semi-direct products. Assuming that p is a prime other than 2 or 3, we have that $\beta^p = 1$, so $\beta^{np} = 1$. It remains to show that

$$\eta = 1 + \beta^n + \cdots + \beta^{n(p-1)} = 0.$$

Let $m_n \in GF(p)[X]$ denote the minimum polynomial of β^n, so m_n is irreducible and divides

$$1 - X^p = (1 - X)(1 + X + X^2 + \ldots + X^{p-1}).$$

The ring $GF(p)[X]$ is a unique factorization domain. If m_n divides $(1-X)$ then $\beta^n = 1$ so $\eta = 0$. Conversely, if m_n fails to divide $(1 - X)$ then it must divide

$1 + X + X^2 + \ldots + X^{p-1}$ so $\eta = 0$. Thus for primes p greater than 3 the group $H^{Z/pZ}$ has exponent p.

We now investigate the group law of $H^{Z/pZ}$ in some detail, reverting to the description of $H^{Z/pZ}$ as being $(Z/pZ)^S$ with a particular group law. In the obvious notation

$$(a, b, c, d, e)(a', b', c', d', e') = (a'', b'', c'', d'', e'')$$

represents the group law. Up to knowledge in above we can give the following lemma.

Lemma 2.4. *If G is the group of exponent p, nilpotency class 4 and with the presentation*

$$G = \langle x, y, z, t, u : [y, x] = z, [z, x] = t, [t, x] = u \rangle,$$

then according to the group law $(a, b, c, d, e)(a', b', c', d', e') = (a'', b'', c'', d'', e'')$, the entries of the 2-step Fibonacci sequence constructed by two elements of G has the following form [4]:

$$\begin{aligned} a'' &= a + a' \\ b'' &= b + b' \\ c'' &= c + c' + a'b \\ d'' &= d + d' + a'c + \tbinom{a'}{2}b \\ e'' &= e + e' + a'd + \tbinom{a'}{2}c + \tbinom{a'}{3}b. \end{aligned}$$

3. Main Result

Now we want to generalize the formulas in the above lemma for a group of exponent p and nilpotency class n.

Theorem 3.1. *If G is a group of exponent p, nilpotency class n and with the presentation*

$$G = \langle x_1, x_2, \ldots, x_n, x_{n+1} : [x_2, x_1] = x_3, [x_3, x_1] = x_4, \ldots, [x_n, x_1] = x_{n+1} \rangle,$$

then entries of the two-step Fibonacci sequences formed by two elements of G

have the following form:

$$
\begin{aligned}
c_1 &= a_1 + b_1 \\
c_2 &= a_2 + b_2 \\
c_3 &= a_3 + b_3 + b_1 a_2 \\
c_4 &= a_4 + b_4 + b_1 a_3 + \tbinom{b_1}{2} a_2 \\
c_5 &= a_5 + b_5 + b_1 a_4 + \tbinom{b_1}{2} a_3 + \tbinom{b_1}{3} a_2 \\
c_6 &= a_6 + b_6 + b_1 a_5 + \tbinom{b_1}{2} a_4 + \tbinom{b_1}{3} a_3 + \tbinom{b_1}{4} a_2 \\
&\vdots \\
c_{n+1} &= a_{n+1} + b_{n+1} + b_1 a_n + \tbinom{b_1}{2} a_{n-1} + \tbinom{b_1}{3} a_{n-2} + \cdots + \tbinom{b_1}{n-1} a_2 \,.
\end{aligned}
$$

Proof. Let G be the group which has the following presentation

$$G = \langle x_1, x_2, \ldots, x_n, x_{n+1} : [x_2, x_1] = x_3, [x_3, x_1] = x_4, \ldots, [x_n, x_1] = x_{n+1} \rangle,$$

where those pairs of generators with unspecified commutators are implicitly deemed to commute. This is a group of nilpotecy class n and exponent p . In fact this group is generated by $x = x_1$ and $y = x_2$. Each element of the group will have a unique representation as $x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n+1}^{a_{n+1}}$ where $a_1, a_2, a_3, \cdots, a_{n+1} \in Z/pZ$. The element $x_{n+1}^{a_{n+1}}$ is central and the group $H = \langle x_2, x_3, \cdots, x_n, x_{n+1} \rangle$ is Abelian. Let $x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n+1}^{a_{n+1}}$, $x_1^{b_1} x_2^{b_2} x_3^{b_3} \cdots x_{n+1}^{b_{n+1}}$ be elements of G. Then, suppose that

$$(x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n+1}^{a_{n+1}})(x_1^{b_1} x_2^{b_2} x_3^{b_3} \cdots x_{n+1}^{bn+1}) = (x_1^{c_1} x_2^{c_2} x_3^{c_3} \cdots x_{n+1}^{cn+1}) \,.$$

Under the group law, we can calculate the entries of two-step Fibonacci sequences as follows:

$$
\begin{aligned}
&(x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n+1}^{a_{n+1}})(x_1^{b_1} x_2^{b_2} x_3^{b_3} \cdots x_{n+1}^{b_{n+1}}) = (x_1^{c_1} x_2^{c_2} x_3^{c_3} \cdots x_n^{c_{n+1}}) \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_n^{a_n} x_1^{b_1} x_2^{b_2} x_3^{b_3} \cdots x_{n+1}^{a_{n+1}+b_{n+1}} \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n-1}^{a_{n-1}} x_1^{b_1} x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n+a_n} x_{n+1}^{a_{n+1}+b_{n+1}+a_n b_1} \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n-1}^{a_{n-1}-1} x_{n-1} x_1 x_1^{b_1-1} x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n+a_n} x_{n+1}^{a_{n+1}+b_{n+1}+a_n b_1} \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n-1}^{a_{n-1}-1} x_1 x_{n-1} x_1^{b_1-1} x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n+a_n} x_{n+1}^{a_{n+1}+b_{n+1}+a_n b_1} \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n-1}^{a_{n-1}-1} x_1 x_{n-1} x_1^{b_1-1} x_n x_{n+1}^{b_1-1} x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n+a_n} x_{n+1}^{a_{n+1}+b_{n+1}+a_n b_1} \\
&= x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_{n-1}^{a_{n-1}-1} x_1 x_{n-1} x_1 x_1^{b_1-2} x_n x_{n+1}^{b_1-1} x_2^{b_2} x_3^{b_3} \cdots x_n^{b_n+a_n} x_{n+1}^{a_{n+1}+b_{n+1}+a_n b_1}
\end{aligned}
$$

$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-1}^{a_{n-1}-1}x_1^2x_{n-1}x_nx_1^{b_1-2}x_nx_{n+1}^{b_1-1}$$
$$\times\, x_2^{b_2}x_3^{b_3}\cdots x_n^{b_n+a_n}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1}$$
$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-1}^{a_{n-1}-1}x_1^2x_{n-1}x_n^2x_1^{b_1-2}x_n^2x_{n+1}^{b_1-1+b_1-2}$$
$$\times\, x_2^{b_2}x_3^{b_3}\cdots x_n^{b_n+a_n}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1}$$
$$\vdots$$
$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-1}^{a_{n-1}-1}x_1^{b_1}x_{n-1}x_{n+1}^{b_1-1+\cdots+1}x_2^{b_2}x_3^{b_3}\cdots x_n^{b_n+a_n}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1}$$
$$\vdots$$
$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-2}^{a_{n-2}}x_1^{b_1}x_{n-1}^{a_{n-1}}x_n^{b_1a_{n-1}}x_{n+1}^{\binom{b_1}{2}a_{n-1})}$$
$$\times\, x_2^{b_2}x_3^{b_3}\cdots x_n^{b_n+a_n}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1}$$
$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-2}^{a_{n-2}}x_1^{b_1}x_2^{b_2}x_3^{b_3}\cdots x_{n-1}^{a_{n-1}+b_{n-1}}$$
$$\times\, x_n^{b_n+a_n+b_1a_{n-1}}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1+\binom{b_1}{2}a_{n-1}}.$$

We can do the same operations between $x_{n-2}^{a_{n-2}}$ and $x_1^{b_1}$. Then the last equation is

$$= x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_{n-3}^{a_{n-3}}x_1^{b_1}x_2^{b_2}x_3^{b_3}\cdots x_{n-2}^{a_{n-2}+b_{n-2}}x_{n-1}^{b_{n-1}+a_{n-1}+b_1a_{n-2}}$$
$$\times\, x_n^{a_n+b_n+a_{n-1}b_1+\binom{b_1}{2}a_{n-1}}x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1+\binom{b_1}{2}a_{n-1}+\binom{b_1}{3}a_{n-2}}.$$

So, we can do the same operations between $x_{n-3}^{a_{n-3}}, x_{n-4}^{a_{n-4}}\cdots x_2^{a_2}$ and $x_1^{b_1}$. Then the last equation is

$$= x_1^{a_1+b_1}x_2^{a_2+b_2}x_3^{a_3+b_3+b_1a_2}\cdots x_n^{a_n+b_n+a_{n-1}b_1+\binom{b_1}{2}a_{n-1}+\cdots+\binom{b_1}{n-2}a_2}$$
$$\times\, x_{n+1}^{a_{n+1}+b_{n+1}+a_nb_1+\binom{b_1}{2}a_{n-1}+\binom{b_1}{3}a_{n-2}+\ldots+\binom{b_1}{n-1}a_2}.$$

We are done. ■

Now we use these formulas to calculate the Fibonacci loop $l(x, y, \ldots)$. For example let $n = 5$. The first few terms are as follows (reduce modulo p of your choice):

$$(1,0,0,0,0,0)\qquad (0,1,0,0,0,0)\qquad (1,1,0,0,0,0)$$
$$(1,2,1,0,0,0)\qquad (2,3,2,0,0,0)\qquad (3,5,7,4,1,0)$$
$$(5,8,18,18,10,2).$$

References

[1] H. Aydin. *Recurrence Relations in Finite Nilpotent Groups*, Ph.D. Thesis, Univerty of Bath (1991).

[2] H. Aydin and R. Dikici. General Fibonacci sequences in finite groups. *The Fibonacci Quarterly* **36**, No 3, June-July (1998), 216–221.

[3] H. Aydin, R. Dikici & G. C. Smith. Wall and Vinson revisited. *Applications of Fibonacci Numbers* **5** (1993), 61-68.

[4] H. Aydin and G. C. Smith. Finite -quotients of some cyclicaly presented groups. *J. London Math. Soc.* **49**, No 2 (1994), 83–92.

[5] H. Aydin and G.C. Smith. *Remarks on Fibonacci Sequences in Groups*, Bath Mathematics and Computer Science Technical Report 91-50, University of Bath (1991).

[6] C. M. Campbell, H. Doostie and E. F. Robertson. *Fibonacci length of generating pairs in groups.* Applications of Fibonacci Numbers (Ed. G. E. Bergum et al.) Kluwer Academic Publishers **3** (1990), 27-35.

[7] R. Dikici and G.C. Smith. Recurrences in finite groups. *Turkish J. Math.* **19** (1995), 321–329.

[8] R. Dikici and G. C. Smith. Fibonacci sequances in finite nilpotent groups. *Turkish J. Math.* **21** (1997), 133–142.

[9] H. Doostie. *Fibonacci-type Sequences and Classes of Groups*, Ph.D. Thesis, University of St. Andrews (1988).

[10] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.* **1** (1878), 184–240 and 289–321.

[11] P. Ribenboim. *The Little Book of Big Primes*, Springer-Verlag (1991).

[12] L. Somer. The divisibility properties of primary Lucas recurrences with respect to primes. *The Fibonacci Quarterly* **18**, No 4 (1980), 316–334.

[13] R. M. Thomas. The Fibonacci groups revisited. *Proceedings of Groups St. Andrews 1989*, Volume 2 LMS Lecture Note Series 160, CUP. (Edited by C.M. Campbell and E.F. Robertson) (1991), 445–454.

[14] J. Vinson. The relations of the period modulo m to the rank of apparition of m in the fibonacci sequence. *The Fibonacci Quarterly* **1**, No 1 (1963), 37–45.

[15] D. D. Wall. Fibonacci series module m. *Amer. Math. Monthly* **67** (1969), 525–532.

[16] H. J. Wilcox. Fibonacci sequences of period in groups. *The Fibonacci Quarterly* **24** (1986), 356–361.

Atatürk Üniversitesi
Fen Edebiyat Fakültesi, Matematik Bölömü
25240-Erzurum, TURKEY

Received: 02.10.2001