Tr. J. of Mathematics
21 (1997) , 133 – 142.

FIBONACCI SEQUENCES IN FINITE NILPOTENT GROUPS

Ramazan Dikici & Geoff C Smith

Abstract

We have proved that, for the 3-step Fibonacci recurrence and any finite p-group of exponent p and nilpotency class 3, the length of a fundamental period of any loop satisfying the recurrence must divide the period of the ordinary 3-step Fibonacci sequence in the field $GF(p)$.

1. Introduction

We shall be interested in the shortest period of the 3-step Fibonacci sequence the entries of which are taken in any finite p-group of exponent p and nilpotency class 3. This problem has already been the subject of investigation. It seems to have first been addressed by Wall [9] and then Vinson [8] for cyclic groups. This theory has been generalized in [4] to cover the 3-step Fibonacci case. Campbell, Doostie and Robertson [2] have attacked the problem of recurrences in the case of non-abelian finite simple groups.Pinch [6] has studied the relationship between the period of a general linear recurrence modulo a rational prime p and the period modulo a power of that prime. He does this via examining the algebraic number theory of certain finite extensions of the p-adic numbers.

Wall distinguishes the special loop $s = (s_i)$ defined by the recurrence $s_{i+2} = s_i + s_{i+1}$ and the initial data $s_0 = 0$ and $s_1 = 1$ in $\mathbf{Z}/p^n\mathbf{Z}$. Let $k(s, p^n)$ denote the fundamental period of s.

Theorem 1.1: *(D.D. Wall [9]) The number $k(s,p^n)$ divides $k(s,p)p^{n-1}$,and the two quantities are equal provided $k(s,p) \neq k(s,p^2)$.*

Wall goes on to conjecture that for all primes p, we always have $k(s,p) \neq k(s,p^2)$. He announced that he had verified this result for all primes $p < 10^4$. We know by [1] that this is indeed the case for all primes $p < 10^8$. This work has also been a recent one in this area and proves that short loops must be geometric for the 3-step Fibonacci recurrences in H, the additive group of the finite field $GF(p^n)$.

Let $s = (s_i)$ denote the ordinary 3-step Fibonacci sequence in $GF(p)$ defined by the recurrence $s_{i+3} = s_i + s_{i+1} + s_{i+2}$ and the initial data $s_0 = 0, s_1 = 0$ and $s_2 = 1$. This is a bi-infinite periodic sequence or loop indexed by the integers. The shortest period of this sequence is called the fundamental period and it will be denoted by k. We sometimes refer to this quantity as Wall's number [9].

2. The Main Theorem

We consider a 3-step Fibonacci sequence $r = (r_i)$ in a finite p-group G, given some initial data r_0, r_1 and r_2. Such a sequence or loop must be periodic and we denote the shortest period of this sequence sometimes called the fundamental period by $k(r, G)$. From now on k denotes the fundamental period of the standard 3- step Fibonacci sequence $0, 0, 1, 1, 2...$ taken modulo a distinguished prime p.

Theorem 2.1: *Let $p > 3$ be a prime number, then if G is a non-trivial finite p-group of exponent p and nilpotency class 3 then $k(r, G) = k$. Of course if G is the trivial group then $k(r, G) = 1$.*

3. Some Lemmas Concerning 3-Step Fibonacci Sequence

Although the proofs of all the following lemmas are not intricate they are omitted here and can be found in [4]. The notation $\sum_{i<j}$ indicates that we are dealing with a double sum, taken over all i and j subject to the constraint that $0 \le i < j \le k - 1$.

Lemma 3.1: *For all integers α and β we have*

$$\sum_{i<j} s_{j+\alpha} s_{i+\beta} = 0.$$

Lemma 3.2: *For all integers α, β and c we have*

$$\sum_{i<j} s_{j-i+\beta} s_{i+c} s_{i+\beta} = 0.$$

Lemma 3.3: *For all integers α, β and γ we have*

$$\sum_{j=0}^{k-1} s_{j+\alpha} s_{j+\beta} s_{-j+\gamma} s_j = 0.$$

Lemma 3.4: *For all integers $\alpha, \beta, c, d,$ and e we have*

$$\sum_{i<j} s_{-j+\alpha} s_{j+\beta} s_{j-i-d} s_{i+e} s_{i+c} = 0.$$

4. The Proof

We do our preliminary investigations, not with the relatively free group on three generators, but with a carefully selected group H which we now describe. H has two generators x and y. A presentation of H is

$$H =< h_1, h_2, h_3, h_4 : (h_2, h_1) = h_3, (h_3, h_1) = h_4, explaw = p >$$

where pairs of generators with unspecified commutator are implicitly deemed to commute. Thus H is a copy of C_p^3 extended by a cyclic group of order p.

Let G be the 3-generator relatively free exponent p class 3 group on g_1, g_2 and g_3. Thus G has order p^{14} and a power commutator presentation of G is given by

$$\begin{aligned}
(g_2, g_1) &= g_4\\
(g_3, g_1) &= g_5\\
(g_3, g_2) &= g_6\\
(g_4, g_1) &= g_7\\
(g_4, g_2) &= g_8\\
(g_4, g_3) &= g_9\\
(g_5, g_1) &= g_{10}\\
(g_5, g_2) &= g_{11}\\
(g_5, g_3) &= g_{12}\\
(g_6, g_1) &= g_9^{-1} g_{11}\\
(g_6, g_2) &= g_{13}\\
(g_6, g_3) &= g_{14}
\end{aligned}$$

Once again we have the convention that pairs of generators with unspecified commutator are implicitly deemed to commute.

In $GF(p)$-vector notation, we put $g_i = (\delta_{ij}) \in G$, where δ_{ij} in the Krönecker symbol and j ranges from 1 to 14.

The group G is relatively free and so admits an automorphism ϕ, which we call the 3-step *Fibonacci automorphism*, defined by $g_1\phi = g_2, g_2\phi = g_3$ and $g_3\phi = g_1g_2g_3$.

We define two maps $\pi_i : G \longrightarrow H$ via

$$g_1\pi_1 = 1, g_2\pi_1 = h_1 \text{ and } g_3\pi_1 = h_2$$

and

$$g_1\pi_2, = h_1, g_2\pi_2 = h_2 \text{ and } g_3\pi_2 = 1.$$

Let $g_i = (\delta_{ij}) \in G$, where δ_{ij} in the Krönecker symbol and j ranges from 1 to 14.

$$Ker\pi_1 = K_1 = (*, 0, 0, *, *, 0, *, *, *, *, *, *, 0, *);$$

$$Ker\pi_2 = K_2 = (0, 0, *, 0, *, *, 0, *, *, *, *, *, *, *).$$

Let $M = Ker\pi_1 \cap Ker\pi_2$, so that

$$M = (0,0,0,0,*,0,0,*,*,*,*,*,0,*),$$

in the sense that each $*$ can independently be any element of $GF(p)$. Now M is an elementary abelian group of order p^7, and is therefore a $GF(p)$- space of dimension 7. A basis of M is $(g_5, g_8, g_9, g_{10}, g_{11}, g_{12}, g_{14})$.
Computer aided calculations [3] yield that

$$M \cap M\phi = (g_8 g_{11}, g_9, g_{10} g_{11} g_{12}, g_{14}),$$

$$M \cap M\phi \cap M\phi^2 = (g_9 g_{14}^{-2}, g_{10} g_{11}, g12)$$

and

$$M \cap M\phi \cap M\phi^2 \cap M\phi^3 = 1.$$

Thus we have a monomorphism

$$\pi : G \longrightarrow G/K_1 \times G/K_2 \times G/K_1\phi \times G/K_2\phi \times G/K_1\phi^2 \times G/K_2\phi^2 \times G/K_1\phi^3 \times G/K_2\phi^3,$$

where the codomain is isomorphic to $\times_{i=1}^{8} H$. The automorphism ϕ^{-1} and its powers induce isomorphisms $G/K_i\phi^j \longrightarrow G/K_i$ which can be composed co-ordinatewise with π to form a group monomorphism

$$\bar{\pi} : G \longrightarrow x_{j=1}^{4}(G/K_1 \times G/K_2)$$

defined by

$$x \longrightarrow (K_1 x, K_2 x, K_1(x\phi^{-1}), K_2(x\phi^{-1}), K_1(x\phi^{-2}), K_2(x\phi^{-2}) K_1(x\phi^{-3}), K_2(x\phi^{-3})).$$

Now let us examine the image of the loop $, r = (r_i)$ beginning $r_0 = g_1, r_1 = g_2, r_2 = g_3$ under $\bar{\pi}$. We have

$$\bar{\pi} : r_i \longrightarrow (r_i\pi_1, r_i\pi_2, r_{i-1}\pi_1, r_{i-1}\pi_2, r_{i-2}\pi_1, r_{i-2}\pi_2, r_{i-3}\pi_1, r_{i-3}\pi_2).$$

The sequences in the odd positions are just rotations of $(r_i\pi_1)$ and the sequences in the even positions are rotations of $(r_i\pi_2)$. Thus, if we can show that $(r_i\pi_1)$ and $(r_i\pi_2)$ both have Wall Number k, it will follow that r has Wall Number k and will be done.
In H the elements can be regarded as vectors and triple multiplication is determined by the following rules;

$$(a_0, b_0, c_0, d_0).(a_1, b_1, c_1, d_1).(a_2, b_2, c_2, d_2) = (a_3, b_3, c_3, d_3)$$

where

$$a_3 = a_0 + a_1 + a_2,$$
$$b_3 = b_0 + b_1 + b_2,$$
$$c_3 = c_0 + c_1 + c_2 + a_1 b_0 + a_2(b_0 + b_1),$$

and finally

$$d_3 = d_0 + d_1 + d_2 + a_1 c_0 + a_2(c_0 + c_1 + a_1 b_0) + \binom{a_2}{2}(b_0 + b_1) + \binom{a_1}{2} + b_0.$$

We must consider two types of initial data for loops in H. We have a loop v of type I with initial data

$$v_0 = (0, 0, 0, 0)$$
$$v_1 = (1, 0, 0, 0)$$
$$v_2 = (0, 1, 0, 0)$$

and another w of type II with initial data

$$w_0 = (1, 0, 0, 0)$$
$$w_1 = (0, 1, 0, 0)$$
$$w_2 = (0, 0, 0, 0).$$

The analysis of the type II loop is entirely similar to that of type I. Thus the type I loop begins

$$v_0 = (t_0, s_0, 0, 0)$$
$$v_1 = (t_1, s_1, 0, 0)$$
$$v_2 = (t_2, s_2, 0, 0).$$

We focus on the type I loop $(v_i) = (t_i, s_i, c_i, d_i)$, where

$$(s_0, s_1, s_2) = (0, 0, 1)$$

and

$$(t_0, t_1, t_2) = (0, 1, 0).$$

It can be easily seen that the sequence t_i can be written in terms of s_i as $t_i = s_{i+1} - s_i$. Now, it follows from [5] that $c_k = c_{k+1} = c_{k+2} = 0$ which correspondes to prove the similar theorem where the nilpotency class of the group reduces to 2. To conclude, we must demonstrate $d_k = d_{k+1} = d_{k+2} = 0$ and begin with $d_k = 0$.

We shall need a formula for c_α in order to work out the formula for d_α. By induction it is

$$c_\alpha = \sum_{i=0}^{\alpha-1} s_{\alpha-i-1}(s_i t_{i+1} + t_{i+2}(s_i + s_{i+1}))$$

for $\alpha \geq 0$. This enables us, via a similar process, to describe d_α for $\alpha \geq 0$ as

$$d_\alpha = \sum_{i=0}^{\alpha-1} s_{\alpha-i-1} t_{i+1} c_i + \sum_{i=0}^{\alpha-1} s_{\alpha-i-1} \binom{t_{i+1}}{2} s_i + \sum_{i=0}^{\alpha-1} s_{\alpha-i-1} t_{i+2}(c_i + c_{i+1} + t_{i+1} s_i)$$

$$+ \sum_{i=0}^{\alpha-1} s_{\alpha-i-1} \binom{t_{i+1}}{2} (s_i + s_{i+1}).$$

We can break up the expression for d_k as $d_k = \Delta_1 + \Delta_2 + \Delta_3 + \Delta_4$,where

$$\Delta_1 = \sum s_{k-i-1} t_{i+1} c_i,$$

$$\Delta_2 = \sum s_{k-i-1}(2^{t_{i+1}}) s_i,$$

$$\Delta_3 = \sum s_{k-i-1} t_{i+2}(c_i + c_{i+1} + t_{i+1} s_i)$$

and

$$\Delta_4 = \sum s_{k-i-1}(2^{t_{i+1}})(s_i + s_{i+1}),$$

and we shall attempt to show that each of these four expressions Δ_i actually vanishes. To this end, we break these expressions up still further.
Now we have

$$\Delta_1 = \sum s_{k-i-1} t_{i+1} c_i = \sum_{j=0}^{k-1} s_{k-j-1} t_{j+1} c_j$$

$$= \sum_{j=0}^{k-1} s_{k-j-1} t_{j+1} \left(\sum_{i=0}^{j-1} s_{j-i-1} s_i t_{i+1} + \sum_{i=0}^{j-1} s_{j-i-1} t_{i+2}(s_i + s_{i+1})\right),$$

and so $\Delta = \Delta_{11} \ \Delta_{12} \ \Delta_{13}$, where

$$\Delta_{11} = \sum_{j=0}^{k-1} \sum_{i=0}^{j-1} s_{k-j-1} t_{j+1} s_{j-i-1} s_i t_{i+1},$$

$$\Delta_{12} = \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_{k-j-1}t_{j+1}s_{j-i-1}s_{i+1}t_{i+2}$$

and

$$\Delta_{13} = \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_{k-j-1}t_{j+1}s_{j-i-1}s_{i}t_{i+2}.$$

Moving to Δ_2, we find that

$$\Delta_2 = \sum_{j=0}^{k-1} s_{k-j-1}\binom{t_{i+1}}{2}s_j = \frac{1}{2}\sum_{j=0}^{k-1} s_{k-j-1}t_{j+1}(t_{j+1}-1)s_j,$$

so that

$$\Delta_2 = \frac{1}{2}\sum_{j=0}^{k-1} s_{k-j-1}t_{j+1}^2 s_j - \frac{1}{2}\sum_{j=0}^{k-1} s_{k-j-1}t_{j+1}s_j.$$

Next we tackle Δ_3. We have

$$\Delta_3 = \sum_{j=0}^{k-1} s_{k-j-1}t_{j+2}(c_j + c_{j+1} + t_{j+1}s_j),$$

so that

$$\Delta_3 = \sum_{j=0}^{k-1} s_{k-j-1}t_{j+2}\Big(\sum_{i=0}^{j-1} s_{j-i-1}(s_i t_{i+1} + t_{i+2}(s_i + s_{i+1}))\Big)$$

$$+\sum_{j=0}^{k-1} s_{k-j-1}t_{j+2}\Big(\sum_{i=0}^{j-1} s_{j-i}(s_i t_{i+1} + t_{i+2}(s_i + s_{i+1}))\Big)$$

$$+\sum_{j=0}^{k-1} s_{k-j-1}t_{j+2}t_{j+1}s_j.$$

Thus $\Delta_3 = \Delta_{31} + \Delta_{32} + \Delta_{33} + \Delta_{34} + \Delta_{35} + \Delta_{36} + \Delta_{37}$, where

$$\Delta_{31} = \sum_{i<j} s_{k-j-1}t_{j+2}s_{j-i-1}s_i t_{i+1},$$

$$\Delta_{32} = \sum_{i<j} s_{k-j-1} t_{j+2} s_{j-i-1} s_i t_{i+2},$$

$$\Delta_{33} = \sum_{i<j} s_{k-j-1} t_{j+2} s_{j-i-1} s_{i+1} t_{i+2},$$

$$\Delta_{34} = \sum_{i<j} s_{k-j-1} t_{j+2} s_{j-i} s_i t_{i+1},$$

$$\Delta_{35} = \sum_{i<j} s_{k-j-1} t_{j+2} s_{j-i} s_i t_{i+2},$$

$$\Delta_{36} = \sum_{i<j} s_{k-j-1} t_{j+2} s_{j-i} s_{i+1} t_{i+2},$$

and

$$\Delta_{37} = \sum_{j=0}^{k-1} s_{k-j-1} t_{j+2} t_{j+1} s_j.$$

Also we see that

$$\Delta_4 = \sum_{j=0}^{k-1} s_{k-j-1} \binom{t_{i+2}}{2} (s_j + s_{j+1}),$$

so that

$$\Delta_4 = \frac{1}{2} \sum_{j=0}^{k-1} s_{k-j-1} t_{j+2} (t_{j+2} - 1)(s_j + s_{j+1});$$

but $\Delta_4 = \Delta_{41} - \Delta_{42}$, where

$$\Delta_{41} = \frac{1}{2} \sum_{j=0}^{k-1} s_{k-j-1} t_{j+2}^2 (s_j + s_{j+1})$$

and

$$\Delta_{42} = \frac{1}{2} \sum_{j=0}^{k-1} s_{k-j-1} t_{j+2} (s_j + s_{j+1}).$$

We want to show all sums of type Δ actually vanish. In fact, this is simply the upshot of lemmas given in section 2. Thus we have shown $d_k = 0$ for the type I sequence. It is a matter of algebraic manipulation to show that $d_{k+1} = d_{k+2} = 0$. The analysis of the type II sequence is extremely similar to that of the type I sequence.

We acknowledge the computer algebra systems CAYLEY [3] and AXIOM [7], using which many of the results in this area were originally discovered as experimental truths.

References

[1] Aydın, H., Dikici, R.and Smith, G.C.: "Wall and Vinson Revisited", Applications of Fibonacci Numbers, Volume 5. Edited by G.E.Bergum et al. Kluwer Academic Publishers, 61-68(1993).

[2] Campbell, C.M., Doostie, H. and Robertson, E.F.: "Fibonacci Length of Generating Pairs in Groups", Applications of Fibonacci Numbers, Volume 3. Edited by G.E. Bergum et al. Kluwer Academic Publishers, 27-35 (1990).

[3] Cannon, J.J.: "An Introduction to the Group Theory Language Cayley ",Proc. Durham Symposium on Computational Group Theory, Academic Press, London, 145-183 (1984).

[4] Dikici, R.: "Applications of Computer Algebra to the Study of Recurrence in p-Groups", Ph.D.Thesis, University of Bath (1992)

[5] Dikici, R.and Smith, G.C.: "Recurrences in Finite Groups", Tr.J. of Math 19,321-329 (1995).

[6] Pinch, R.G.E.: "Linear Recurrent Sequences Modulo Prime Powers", Proc. 3^{rd} IMA Conference on Coding and Cryptography, Cirencester, England (1991) (*to appear*).

[7] Sutor, R.S.: "AXIOM User Guide", NAG Ltd, (1991).

[8] Vinson, J.: "The Relations of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence", The Fibonacci Quarterly. 1,37-45 (1963).

[9] Wall, D.D.: "Fibonacci Series Modulo m", Amer. Math. Monthly. 67, 525-532 (1960).

Sonlu Nilpotent Gruplarda Fibonacci Dizileri

Özet

Gözönüne alınan 3-basamak Fibonacci dizisi ve nilpotent sınıfı 3, exponenti p olan herhangi bir sonlu p-grup için, bu grubun elemanlarıyla oluşturulan herhangi bir döngünün esas periyodunun uzunluğunun $GF(p)$ cisminde adi 3- basamak Fibonacci dizisinin periyodunu böldüğü ispatlandı.

Ramazan DİKİCİ & Geoff C SMITH
Atatürk Üniversitesi
Kazım Karabekir Eğitim Fakültesi
Matematik Eğitimi Bölümü
25240 Erzurum-TURKEY

Received 18.10.1994