# CYCLIC FIBONACCI ALGEBRAS


**D. L. Johnson**

Mathematics Department, University of Nottingham, Nottingham NG7 2RD, U.K.

**A. C. Kim**

Mathemetics Department, Pusan National University, Pusan, Korea



(*Submitted April 1993*)


## 0. INTRODUCTION

A *Fibonacci algebra* is a group equipped with a unary operation $\phi$ satisfying the laws

$$(xy)\phi = x\phi y\phi, \text{ and } xx\phi \ldots x\phi^{m-1} = x\phi^m$$

for a fixed integer $m \geq 2$. If, in addition, the law

$$x\phi^n = x$$

holds for a fixed integer $n \geq 2$, the algebra is called *periodic*. The corresponding variety $\mathfrak{V}(m, n)$ has been studied by several authors (see [4] and the references cited there) and, in particular, it is known that the monogenic free object $A(m, n)$ is just the Fibonacci group

$$F(m, n) = \langle x_1 \ldots x_n | x_i x_{i+1} \ldots x_{i+m-1} = x_{i+m},\ 1 \leq i \leq n, i \bmod n \rangle$$

made abelian.

It is also known [3] that $A(m, n)$ is always a finite group whose order $a_{m,n}$ is the resultant of the polynomials

$$f(x) = x^n - 1,\ \ g(x) = 1 + x + \cdots + x^{m-1} - x^m, \tag{1}$$

namely,

$$a_{m,n} = (m-1)\prod_{k=1}^{n-1} |g(\omega_k)|, \tag{2}$$

where the product is taken over all nontrivial $n^{\text{th}}$ roots of unity, $\omega_k = e^{2\pi k i/n}$, $k = 1, 2, \ldots, n-1$. It follows that, for any prime $p$ dividing $a_{m,n}$, the highest common factor $(f(x), g(x))_p$ over the prime field $GF(p)$ has positive degree. It is shown in [5] that $A(m, n)$ is cyclic if and only if

$$\deg(f(x), g(x))_p = 1 \ \ \forall p | a_{m,n}. \tag{3}$$

We shall apply this criterion to certain (classes of) values of $m$ and $n$ to determine when $A(m, n)$ is cyclic. It follows that, in these cases, the exponent of the free objects in $\mathfrak{V}(m, n)$ is just $a_{m,n}$. This reconfirms some of the results in [2], where a constructive approach is adopted to calculating exponents in $\mathfrak{V}(m, n)$. On the other hand, the case when $A(m, n)$ is noncyclic is also of interest, at least when $m = 2$. For then it follows from results in [1] that $F(2, n)$ maps homomorphically onto the free object of rank two in the variety of groups of exponent $p$ and class *four* for some prime $p$.

In each of the ensuing sections, we consider the $A(m, n)$ with $m, n \geq 2$ and related as in the section heading. We fix the notation in (1) and (2) above along with

$$f_1 := f / (x-1) = 1 + x + \cdots + x^{n-1},$$

and emphasize the fact that, throughout what follows, **we consider only primes $p$ dividing $a_{m,n}$.**

### 1. $m \equiv -1 \pmod n$

Setting $m = qn-1$, we see that $g = (1+x^n = \cdots + x^{(q-1)n})f_1 - 2x^m$, so that $a_{m,n} = (m-1)2^{n-1}$. Also, for $p$ odd, $(g, f_1)_p = (-2x^m, f_1)_p = 1$, so that $(f, g)_p = x-1$ and (3) holds in this case.

When $p = 2$, however, $(g, f_1)_2 = f_1$, whence $(g/(x+1), f_1)_2 = f_1$ or $f_1/(x+1)$, which has degree $\geq 1$ unless $f_1 = x+1$, that is, $n = 2$. In the case $p = n = 2$, $f = 1+x^2$, $g = 1+x+\cdots+x^{2q-1} = (1+x)(1+x^2+\cdots+x^{2q-2})$, and $(f, g)_2 = 1+x$ if and only if $q$ is odd, that is, $m \equiv 1 \pmod 4$.

***Proposition 1:*** When $m \equiv 1 \pmod n$, $A(m, n)$ has order $(m-1)2^{n-1}$ and is cyclic if and only if $n = 2$ and $m \equiv 1 \pmod 4$.

### 2. $m \equiv 0 \pmod n$

Here, the calculation is similar to (but much easier than) the above, and we obtain the following. We leave the proof as an exercise.

***Proposition 2:*** When $m \equiv 0 \pmod n$, $A(m, n)$ has order $(m-1)$ and is cyclic.

### 3. $m \equiv 1 \pmod n$

Setting $m = qn+1$, we see that

$$g = (1+x^n + \cdots + x^{(q-1)n})f_1 + x^{m+1} - x^m,$$

so that $a_{m,n} = (m-1)n$ and we consider primes $p|(m-1)n$. It is clear that, over any field,

$$h_1 := (g, f_1) = (x^{m-1} - x^m, f_1) = (1-x, f_1).$$

Now $f_1(1) = n$, so that for $p \nmid n$, this hcf is 1 and $(f, g)_p = x-1$ satisfies (3).

But if $p|n$, then $h_1 = x-1$ and $(f, g)_p = (x-1)^2$ or $(x-1)$ according as $x-1$ divides

$$g_1 := g/(1-x) = 1+2x+\cdots+(m-1)x^{m-2} + x^{m-1}$$

or not. But

$$g_1(1) = \frac{1}{2}m(m-1)+1 = \frac{1}{2}(qn+1)qn+1,$$

and for $p|n$ this is zero modulo $p$ if and only if

$$p = 2,\ q \text{ is odd, and } n \equiv 2 \pmod 4.$$

***Proposition 3:*** When $m \equiv 1 \pmod n$, $A(m, n)$ has order $(m-1)n$ and is cyclic except when $n \equiv 2 \equiv m-1 \pmod 4$.

### 4. $m \equiv -2 \pmod n$

We let $m = qn-2$ so that

$$g = (1+x^n + \cdots + x^{(q-1)n})f_1 - x^m(2+x),$$

and

$$a_{m,n} = (m-1) \prod_{\omega^n = 1 \neq \omega} |g(\omega)|$$

$$= (m-1) \prod_{\omega^n = 1 \neq \omega} |2+\omega| = (m-1)|f_1(-2)|.$$

Moreover, $(g, f_1) = (2+x, f_1)$, and $(g, f)$ is a divisor of $(x-1)(x+2)$. However, $|f_1(-2)| = (2^n - (-1)^n)/3$, and we distinguish four cases.

(i) $p \nmid (2^n - (-1)^n)/3$, when $(g, f) = x-1$ and (3) holds

(ii) $p \nmid (m-1)$, when $(g, f) = x+2$ and (3) holds.

(iii) $p | (m-1, (2^n - (-1)^n)/3)$ and $p \neq 3$, when $(g, f) = (x-1)(x+2)$ and (3) fails.

(iv) $p = 3 | (m-1, (2^n - (-1)^n)/3)$, when $-2 \equiv 1 \pmod 3$ and

$$(g, f)_3 = (x-1)(1+x+\cdots+x^{n-1}, 1+2x+\cdots+(m-1)x^{m-2}+x^{m-1})_3.$$

But the second term in the hcf, evaluated at $x=1$, is $\frac{1}{2}m(m-1)+1 \equiv 1 \pmod 3$, showing that $(g, f)_3 = x-1$ and (3) holds.

It follows that $A(m, n)$ is cyclic in this case except when case (iii) arises, that is, when there is a prime $p \neq 3$ such that $qn \equiv 3$, $(-2)^n \equiv 1 \pmod p$.

***Proposition 4:*** When $m = -2 \pmod n$, $A(m, n)$ has order $(m-1)(2^n - (-1)^n)/3$ and is cyclic unless there is a prime $p \neq 3$ such that

$$m \equiv 1 \pmod p \quad \text{and} \quad n = ka,$$

where $a$ is the order of $-2 \bmod p$.

Thus, for example, we see that $A(6, 4)$ is noncyclic by taking $p = 5$.

## 5. $n = 2m$

In this case

$$a_{m,n} = (m-1) \prod_{\omega^n = 1 \neq \omega} |(1+\omega+\cdots+\omega^{m-1}) - \omega^m|$$

$$= (m-1) \prod_{\omega^m = -1} \left| 1 + \frac{1-\omega^m}{1-\omega} \right| = (m-1) \prod_{\omega^m = -1} \left| \frac{3-\omega}{1-\omega} \right|$$

$$= (m-1)(1+3^m)/2.$$

As usual, let $p | a_{m,n}$ and assume first that $p$ is odd. Then $f = x^{2m} - 1$ is the product of co-prime polynomials $x^m - 1$ and $x^m + 1$ and we compute $(f, g)_p$ in two stages. Firstly,

$$((x^m - 1)/(x-1), g) = ((x^m - 1)/(x-1), x^m) = 1,$$

so that $((x^m - 1, g)_p = x-1$ or 1 according as $p | (m-1)$ or not. Secondly,

$$(1+x^m, (1-x)g) = (1+x^m, 1-2x^m+x^{m+1}) = (1+x^m, 3-x),$$

which is $x-3$ or 1 according as $p|(1+3^m)$ or not, and since $p$ is odd this is also the hcf of $1+x^m$ and $g$. Thus, for $p$ odd, $(f, g)_p$ is linear unless $p$ divides both $m-1$ and $3^m+1$.

Now let $p=2$ so that $m$ must be odd, $2k+1$ say, and a simple calculation shows that $(f, g)_2 = x+1$ or $x^2+1$ according as $k$ is even or odd.

***Proposition 5:*** When $n=2m$, $A(m,n)$ has the order $(m-1)(1+3^m)/2$ and is cyclic unless either $m \equiv 3 \pmod p$ or there is an odd prime $p$ such that $m \equiv 1 \pmod p$ and $3^m \equiv -1 \pmod p$.

D. A. Burgess has pointed out that these equations certainly have a solution in the case in which $p \equiv 6 \pm 1 \pmod{12}$.

## 6. ACKNOWLEDGMENT

Both authors are grateful to the Royal Society, the Korean Science and Engineering Foundation, and to the British Council, without whose support this collaboration would not have been possible.

## REFERENCES

1. H. Aydin & G. C. Smith. "Finite $p$-Quotients of Some Cyclically-Presented Groups." To appear in *J. London Math. Soc.*
2. M. W. Bunder, D. L. Johnson, & A. C. Kim. "On the Variety of Algebras $V(m,n)$." Preprint.
3. D. L. Johnson. "A Note on the Fibonacci Groups." *Israel J. Math.* **17** (1974):277-82.
4. D. L. Johnson & A. C. Kim. "Periodic Fibonacci Algebras." *Proc. Edinburgh Math. Soc.* **35** (1992):169-72.
5. D. L. Johnson & R. W. K. Odoni. "Some Results on Symmetrically-Presented Groups." To appear in *Proc. Edinburgh Math. Soc.*

AMS Classification Numbers: 20F05, 11T06