PHD

Recurrence relations in finite nilpotent groups

Aydin, Hueseyin

Award date:
1991

Awarding institution:
University of Bath

RECURRENCE RELATIONS IN FINITE NILPOTENT GROUPS

Submitted by Hüseyin AYDIN

for the degree of PhD
of the University of Bath
1991

Summary

The contents of this thesis can be viewed in two equivalent two ways. The straightforward view is that the bulk of the material concerns linear recurrences (usually the *Fibonacci* recurrence) in finite p-groups. The other perspective is to build the recurrence into the presentation of a group, and then examine which finite p-groups can occur as quotients of this group. Though this thesis is principally concerned with the *Fibonacci* recurrence, it has recently become clear that, contrary to our initial expectations, some of the results generalize to (almost) arbitrary linear recurrences.

The method of working has been to discover experimental "truths" via computational experiment, usually using the system CAYLEY, and then to set about providing formal mathematical proofs to confirm that the apparent truths are actually theorems. The mathematical technique we have developed to accomplish this task has been a calculus of Fourier Sums, where a periodic function, sometimes of considerable complexity, is summed over a fundamental period.

The thesis ends with some material concerning the search for natural algebraic invariants to discriminate between isoclinic finite p-groups. This work is not directly related to the rest of the thesis.

Acknowledgements

Firstly, I would like to thank my supervisor Dr. G.C. Smith for his patience and encouragement. I am also grateful to many group theorists for a lot of valuable discussions during conferences and workshops, particularly Dr. D. Johnson, Dr. R. Thomas, Prof M. Newman and Dr. E.A. O'Brien.

Secondly, many thanks go to School of Mathematical Science particularly Prof J. Davenport and Mrs. J. Parker for facilitating my work.

Thirdly, I am grateful to Atatürk University and the Goverment of Turkey for funding my programme in the U.K.

Finally, I thank my family and friends back in Turkey for their moral support and enduring love.

CONTENTS

CHAPTER 0

Introduction

Firstly, we define the *Fibonacci* groups. These are groups parameterized by natural numbers r and n and described by the following presentations

$$F(r,n) =< x_1, x_2, x_3, \cdots, x_n : x_1x_2x_3\cdots x_r = x_{r+1}, x_2x_3x_4\cdots x_{r+1} = x_{r+2},$$

$$\cdots, x_{n-1}x_nx_1\cdots x_{r-2} = x_{r-1}, x_nx_1x_2\cdots x_{r-1} = x_r > .$$

Thomas gave a table describing our knowledge of the structure of Fibonacci groups with small parameters in his survey of Fibonacci groups. This survey appears as a Technical Report [Th89b]. We will now briefly describe the history of Fibonacci Groups.

Study of these groups began with a question of Conway [Co]. His question was to determine whether or not $F(2,5)$ is cyclic of order 11. The question was quickly answered (in the affirmative) independently by large number of mathematicians.

The groups $F(2,1)$ and $F(2,2)$ are trivial. The group $F(2,3)$ is the quaternion group of order 8. The group $F(2,4)$ is cyclic of order 5. The group $F(2,5)$ is cyclic of order 11 and $F(2,6)$ is infinite. $F(2,7)$ was shown to be cyclic of order 29 using a computer by Brunner [Br] and Chalk and Johnson [CJ]. An algebraic proof was given by Havas [Ha]. Brunner showed that the groups $F(2,8)$ and $F(2,10)$ are infinite [Br]. The group $F(2,9)$ is infinite, a fact that was demonstrated by Newman [Ne]. Now, $F(2,n)$ is infinite, where $n \geq 11$. This was shown by Lyndon. We have summarized the existing knowledge of $F(2,n)$. Now, we will enumerate some of the known properties of Fibonacci groups.

1. Johnson showed that the derived quotient $F(r,n)/F'(r,n)$ is always finite and the order of $F(r,n)/F'(r,n)$ is equal to $\mid \prod_{i=1}^{r}(\xi_i^n - 1) \mid$, where $f(x) = 1 + x + x^2 + \cdots + x^{r-1} - x^r$ and the ξ_i are the roots of this polynomial [Jo].

2. Johnson, Wamsley and Wright proved that if n divides r, then $F(r, n)$ is cyclic of order $r - 1$ [JWW].

3. Campbell and Robertson proved that if $r \equiv 1 \pmod{n}$, then $F(r, n)$ is metacyclic of order $r^n - 1$ [CR74a], [CR74b].

4. It was shown by Campbell and Thomas [CT], [Th83] that $F(r, n)$ is infinite if $(r+1, n) > 3$ or if $(r+1, n) = 3$ with n even or $r > 2$, where $(r+1, n)$ denotes greatest common divisor of $r + 1$ and n.

5. If r is even, then $F(r, 2)$ is cyclic of order $r - 1$. If r is odd the $F(r, 2)$ is metacyclic of order $r^2 - 1$. It was shown by Johnson, Wamsley and Wright [JWW].

6. The group $F(r, 3)$ is cyclic of order $r - 1$ if $r \equiv 0 \pmod{3}$, metacyclic of order $r^3 - 1$ if $r \equiv 1 \pmod{3}$, and infinite if $r \equiv 2 \pmod{3}$ with $r > 2$. This result appears in [JWW].

7. The group $F(r, 4)$ is cyclic of order $r - 1$ if $r \equiv 0 \pmod{4}$, metacyclic of order $r^4 - 1$ if $r \equiv 1 \pmod{4}$, metacyclic of order $(4k+1)[2^{4k+1} + (-1)^k 2^{2k+1} + 1]$ if $r \equiv 2 \pmod{4}$ where $r = 4k + 2$ and $F(r, 4)$ is infinite if $r \equiv 3 \pmod{4}$. These results were due to Thomas [Th89a] and Seal [Se]. There appear to be no known results of similar type for the group $F(r, 5)$. It is not known, for example, whether or not $F(7, 5)$ is finite.

8. Chalk and Johnson showed that if n does not divide any of $r \pm 1$, $r \pm 2$, $2r \pm 1$, $3r$, $4r$ or $5r$, then $F(r, n)$ is infinite [CJ].

9. If r is odd and if n does not divide any of $r \pm 1$, $r + 2$, $2r$, $2r + 1$ or $3r$ then $F(r, n)$ is infinite. This result is a generalization of the previous remark, and was proved by Seal [Se].

10. If $s \geq 0$ such that 2^s divides (r, n), 2^{s+1} does not divide r, and n does not divide any of $r \pm 1$, $r + 2$, $2r$, $2r + 1$ or $3r$, then $F(r, n)$ is infinite [Se].

11. If n does not divide any of $r \pm 2$, $r \pm 3$,2r, $2r \pm 1$, $2r \pm 2$, or $3r \pm 1$, then $F(r, n)$ is infinite [Se].

12. As a result, if $n > 2r + 1$, then $F(r, n)$ is infinite unless $r = 2$, $n = 7$ or (perhaps) $r = 3$, $n = 9$.

Next we will give the definition and some properties of finite p-groups.

Definition: Let G be a finite group. If every element of G has order a power of p, then G is called p-group, where p is a prime number.

1. Every non-trivial finite p-group has a central subgroup of order p.

2. If order of the p-group G is p^n, then every maximal subgroup of G has order p^{n-1}.

3. A finite p-group is nilpotent.

4. A p-group G of order p^n can have nilpotency class at most $n - 1$, since either p-group is cyclic or p^2 divides the index of the Frattini subgroup of G. This result was due to Burnside. See, for example, [Har].

Now we will give some information about commutators, commutator groups, nilpotent groups and the notion of nilpotency class.

Definition: Let G be a group. If x and y elements of G then $(x, y) = x^{-1}y^{-1}xy$ is called the commutator of x and y. If A and B are subgroups of G, then (A, B) is the subgroup generated by all the commutators (x, y) with $x \in A$, $y \in B$. $G' = (G, G)$ is called the derived group of G.

Definition: Let $H \lhd G$, $K \lhd G$, $K \leq H$. If H/K is contained in the centre 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

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_r = 1 \tag{1}$$

such that G_{i-1}/G_i is a central factor of G for each i=1, 2, 3, $\cdots$, r. The smallest possible r is called the nilpotency class of G.

If the nilpotency class of G is 1, then the group is Abelian. If the nilpotency class of G is 2, then the group is metabelian. Now, we will define the upper central series and the lower central series.

Definition: Let G be a group.

$$1 = \delta_0(G) \leq \delta_1(G) \leq \cdots$$

is called the upper central series of G if $\delta_{i+1}(G)/\delta_i(G)$ is the centre of $G/\delta_i(G)$.

Definition: Let G be a group.

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$$

is called the lower central series if $\gamma_{i+1}(G) = (\gamma_i(G), G)$.

If (1) is any central series of G then for all integers i, j we have

$$\delta_i(G) \geq G_{r-i}, \ \gamma_{j+1}(G) \leq G_j.$$

We will use these properties and following properties in Chapter 4.

In any group G we have the following commutator formulas, mostly due to Philip Hall [Ha79].

1. $(y,x) = (x,y)^{-1}$, $x^y = x(x,y)$, $x^{yz} = x(x,z)(x,y)^z = x(x,yz)$, $(xy)^z = xy(xy,z)$, $x^z y^z = x(x,z)y(y,z) = xy(x,z)^y(y,z)$,

2. $(x,yz) = (x,z)(x,y)^z$, $(xy,z) = (x,z)^y(y,z)$,

3. $(x,y^{-1},z)^y(y,z^{-1},x)^z(z,x^{-1},y)^x = 1$ due to Witt ,

4. $(x,y,z^x)(z,x,y^z)(y,z,x^y) = 1$,

5.

$$(\gamma_i(G), \gamma_j(G)) \leq \gamma_{i+j}(G)$$

and

6. if $i \geq j$,

$$(\delta_i(G), \gamma_j(G)) \leq \delta_{i-j}(G)$$

and in particular $(\delta_i(G), \gamma_i(G)) = 1$.

Originality of Material in this Thesis.

In this section, we describe, for the sake of the examiners, exactly which parts of the thesis are the original work of the author. More than half of this thesis has appeared as a Bath Technical Report [AS], but for the purposes of this explanation, we shall not deem that to be a publication. As well as the following summary, we have indicated in the body of the thesis when results are not original.

In chapter 1, we list the main theorems and announcements. In chapter 2, proof techniques are joint work between the author and his supervisor. Some of results belong to Wall[Wa] and Vinson[Vi]. We reproved their results using new techniques. In chapter 3, lemma 3.12 and 3.13 are due to Smith (this work being unpublished and original). Ninety percent of the rest of the work in that chapter was the work of the author of this thesis. In this chapter, most of the results are unpublished and original, save that some of the early formulas are well known. The rest of the results are due to the author under the guidance of Smith. Chapter 4 is joint work with Smith. In chapter 5, theorems 5.1 and 5.2 were proved by Wall[Wa]. The algorithm and program were conceived and written by Smith (unpublished). In chapter 6, lemma 6.3 is due to Johnson (personal communication), and lemma 6.4 was the upshot of discussions between the author, Johnson and Smith. The rest of the results are due to the author. None of the work in this chapter is published. In chapter 7 the work is due to the author. The final chapter was the first successful research work accomplished by the author, and was done at the suggestion of Eamonn O'Brien of A.N.U. Canberra. It appears in another Bath Technical Report [Ay].

CHAPTER 1

Preliminaries

We shall prove two major theorems in the course of this document. They are as follows.

Theorem A.

If G is a p-group for some prime p, and that G has exponent p central length n, then if any two elements of G are used to initiate a Fibonacci sequence in G, then that sequence must have minimum period dividing kp^{n-1} where k is the minimum period of the ordinary Fibonacci sequence modulo p.

Recall the definition of a Fibonacci group; The Fibonacci Group $F(r,n)$ is the group with the following presentation:

$$< \; x_1, \ldots, x_n \mid x_1 x_2 \ldots x_r = x_{r+1}, \; x_2 x_3 \ldots x_{r+1} = x_{r+2}, \ldots, \; x_n x_1 \ldots x_{r-1} = x_r \; >$$

where all subscripts are taken modulo n.

Theorem B.

If the Fibonacci Group $F(2,n)$ has the two generator relatively free group in the variety of exponent p groups of class 1 as a homomorphic image, then $F(2,n)$ has the two generator relatively free group G in the variety of exponent p groups of class 4 as a homomorphic image.

Put less cleanly but perhaps more clearly, Theorem B says that if $C_p \times C_p$ is a quotient of $F(2,n)$, then a larger quotient can be described (unless the prime p is even). Johnson and Odoni have characterized the circumstances under which $F(2,n)$ made Abelian is cyclic [JO], in turn, they have therefore characterized the circumstances under which the Abelian quotient is non-cyclic, and so Theorem B applies. Computer experiments indicate that Theorem B is best possible, in the sense that it cannot be extended to class 5.

We also announce two computer results – using the system CAYLEY.

Announcement C.

Any Fibonacci sequence constructed by starting off with two elements from the restricted Burnside group $R(2,5)$ must have minimum period dividing 20. This is the least number with this property. Indeed, the number 20 is also the minimum period of a Fibonacci sequence in $C_5 \times C_5$.

Announcement D.

Wall's conjecture that for each prime p, the minimum period of the ordinary Fibonacci sequence modulo p^2 is greater than the minimum period of the Fibonacci sequence modulo p has been verified to hold for all primes less than 10^8 by computer search.

Theorem A is proved in Chapter 2, and Theorem B is proved in Chapter 4, using results on Fourier sums established in the lengthy and technical Chapter 3. The results of Chapter 3 may be of some interest in their own right. Announcement C is a calculation which may be performed quite easily via CAYLEY, in particular using the nilpotent quotient algorithm. The background to Announcement D is explained in Chapter 5.

CHAPTER 2

D.D. Wall Revisited, and a Proof of Theorem A

The notion of a Fibonacci Group $F(r,n)$ followed on the heels of Conway's Advanced Problem 5327 in the American Mathematical Monthly [Co]. Since then considerable effort has been expended in attempting to understand Fibonacci groups (the reader not familiar with this notation should see Chapter 1). This enterprise has met with considerable success. For example we now know exactly when $F(2,n)$ is finite. Roger Lyndon's [Ly] application of small cancellation theory almost finished the problem, though some corrections (or perhaps amplifications) to the arguments were needed, and were, according to a personal communication from D. L. Johnson, supplied in Chalk's thesis [Ch]. The author of this document has not yet had the opportunity to read Chalk's thesis, and relies on the evidence of D.L. Johnson for the accuracy of this information. The 'hard' cases not covered by Lyndon's work were $F(2,8)$ and $F(2,10)$ – these were covered by Brunner [Br], and $F(2,9)$ by Newman [Ne].

In general, we know quite a lot about Abelianized Fibonacci Groups, thanks to the work of Johnson and others in a sequence of papers in the mid-seventies, for example in [CJ], [Jo] and [JWW]. Recent developments include work on structure of Abelianized Fibonacci groups (and more generally cyclically presented groups). Papers are in preparation in this area, see (when they exist) [BJK] and [JO]. This is a most felicitous and timely development since [JO] will, among other things, describe exactly when $F(2,n)$ can be the subject of Theorem B of this document.

The co-operation between Thomas, Robertson and Campbell has proved very fruitful, and has given us some insight into groups which have presentations closely related to those of Fibonacci Groups. Thomas has an excellent survey article in the form of a technical report [Th89b] which appears more widely in abbreviated form in [Th91]. This article is also a good source of references. One possibility for future work by the author of this document will be generalization of the results contained here to Fibonacci-like groups and, if possible, cyclically presented groups in general. The methods in the sequel do not admit of ready generalization, but Dikici and Smith are in the process of developing alternative methods to cover more general cases.

What we will do in this work is to investigate which groups $F(2,n)$ have a given finite quotient G of a particular form. This problem has already been the subject of investigation. It seems to have first been addressed by Wall [Wa] and then Vinson [Vi] for cyclic groups. This case amounts to the study of the instance where the image group is cyclic of prime-power order – thanks to the Chinese remainder theorem. We are able to generalize the Wall-Vinson theory to address the case where the image group is an arbitrary finite $p-$group. This is the content of Theorem A. We shall reprove some of the early results for two reasons. Firstly we wish to make this work self-contained, but secondly we have a slightly different perspective from these earlier workers -- and we contend that our viewpoint is more illuminating.

Campbell, Robertson and Doostie have, in an excellent preprint [CDR], addressed the similar questions where the image group is simple. This work overlaps in some degree with Doostie's thesis [Do].

We must gratefully acknowledge the use of the Computer Algebra system CAYLEY [Ca82], which enabled us to guess some truths via computational experiments, and to effect calculations with specific groups where appropriate.

In *Remarks on Fibonacci Loops 2* (to appear) the author and his supervisor will summarize computational results on various relatively free nilpotent finite $p-$groups. Work is also in progress (Dikici and Smith) concerning similar questions about $F(r,n)$ where $r \geq 3$. We expect this to appear in *Remarks on Fibonacci loops 3* . Dikici and Smith claim to be able to generalize both Theorem A and Theorem B of this document.

Let G be a finite group. We define a Fibonacci loop or *loop* g of G as follows. Suppose $g_0, g_1 \in G$, then for $i \geq 2$ define $g_i = g_{i-2}g_{i-1}$ recursively. For $i \leq 0$ define $g_i = g_{i+2}g_{i+1}^{-1}$ also recursively. We obtain a *loop*, a "bi-infinite sequence" $\mathrm{g} = (g_i)_{i \in \mathbf{Z}}$, for which both recurrence equations hold for every integer i.

Such a loop must be periodic, since G is finite. We will use the term *length* to describe the minimum period of a loop $\mathbf{f}$, and write it as $l(\mathbf{f})$. Thus if a loop $\mathbf{f}$ is known to be periodic with period t, then we may deduce that $l(\mathbf{f})$ divides t. There will be exactly $|G|^2$ distinct loops, since that is the number of distinct ordered pairs of group elements. The rôle of the indexing is not particularly significant, and we can eliminate it easily. We define an equivalence relation $\sim$ on loops by writing $(g_i) \sim (h_i)$ if and only if there exists an integer s such that $g_{i+s} = h_i$ for each integer i. We introduce the term *eloop* for the equivalence classes of loops. The period of a loop is constant on equivalence classes, so the notion of the length of an eloop makes sense. We deliberately blur the distinction between $\mathbf{f}$ and the eloop containing $\mathbf{f}$ in order to avoid notational explosion. If $\mathbf{f}$ is a loop or an eloop, we write $l(\mathbf{f})$ for its length.

Notice that $Aut(G)$ acts naturally on both the loops and the eloops; moreover, group homomorphisms send loops to loops and eloops to eloops, though length may drop.

The set of loops of G will be denoted $L(G)$. The set of all periodic bi-infinite sequences of elements of G form a group under componentwise composition, and if G is Abelian then $L(G)$ is a finite subgroup isomorphic to the Cartesian square of G.

Notation:

If $\mathbf{f}$ is a loop of length l then we may elect to write it as

$$\mathbf{f} = (f_0, f_1, \dots f_{l-1})$$

and we may, by abuse, refer to the associated eloop in the same way. This gives us a unique representation for loops, but, in general, non-unique representations for eloops. We refer to the process of selecting a loop in the same eloop class as $\mathbf{f} \in L(G)$ as *rotating* $\mathbf{f}$.

The case when G is cyclic of prime order has been studied by Wall [Wa] , Vinson [Vi] and Wilcox [Wi]. We reprove some of their results from our perspective, and throw a little light on some of their results.

We may assume that G is the additive group of a field $GF(p)$ with p elements. The automorphism group of G will then be handily realized as multiplication by units.

Having chosen this particular representation of G, there is an obvious distinguished loop $\mathbf{s}$ with $s_0 = 0$ and $s_1 = 1$. We call this the *standard* loop, and refer to its associated eloop as the standard eloop. The appellation *trivial* would seem appropriate for the loop $\mathbf{0} = (0, 0, \ldots)$ and its associated eloop.

Following Wall [Wa] we let $k(p^n)$ denote the length of the standard eloop of the cyclic group of order p^n, thought of as the additive group of $\mathbf{Z}/p^n\mathbf{Z}$.

Lemma 2.1.

(i) Let H be the additive group of the finite field $GF(p^t)$. If $\mathbf{f} \in L(H)$ then $l(\mathbf{f})$ divides $k(p)$. A non-trivial short loop $\mathbf{h}$ ($l(\mathbf{h}) < k(p)$) must have all its entries non-zero and be a geometric sequence (i.e. $h_i^{-1}h_{i+1}$ must be independent of i).

(ii) For non-trivial loops $\mathbf{f}$ in C_p we have $l(\mathbf{f}) = k(p)$ unless $p \equiv 0, 1$ or $4 \bmod 5$.

Proof.

(i) Let $\mathbf{s} = (0, 1, 1, \ldots)$ be the standard loop of length $k(p)$, so $\mathbf{s}$ is a loop in $GF(p)$, a subfield of $GF(p^t)$. We can rotate this loop to obtain other loops of length $k(p)$ in the same equivalence class. We can also multiply each element of the loop by an element of $GF(p^t)$ to obtain another loop. Suppose $\mathbf{f} \in L(H)$ is an arbitrary loop. In the obvious notation,

$$\mathbf{f} = (f_0, f_1, \ldots) = f_0 \cdot (1, 0, \ldots) + f_1 \cdot (0, 1, \ldots).$$

Notice that $(1, 0, \ldots)$ is a rotation of the standard loop so the loop $\mathbf{f}$ has period $k(p)$ and $l(\mathbf{f})$ must divide $k(p)$.

Suppose $\mathbf{f}$ has 0 as an entry, but is not the trivial loop. By rotation we may assume that $\mathbf{f} = (0, x, \ldots)$ where $x \neq 0$. Now $\mathbf{f} = x \cdot \mathbf{s}$ (and $\mathbf{s} = x^{-1} \cdot \mathbf{f}$) so $l(\mathbf{f}) = k(p)$.

We may now assume that $\mathbf{f}$ has only no zero entries, and we shall suppose that $l(\mathbf{f}) < k(p)$. Suppose $\mathbf{f} = (w, wx, \ldots)$ and that $\mathbf{g}$ is any rotation of $\mathbf{f}$. Thus $\mathbf{g} = (y, yz, \ldots)$ and then $\mathbf{f} - wy^{-1} \cdot \mathbf{g} = (0, w(x-z), \ldots)$ is a loop of length less than $k(p)$ containing an entry which is 0. It must be the trivial loop and so $x = z$. Thus there exists at most one $\beta \in GF(p^t)$ which can occur as a ratio of consecutive elements in any given short loop. Thus a non-trivial short loop must have no zero entries. This completes the proof of part (i).

(ii) The recurrence equation forces such a β to satisfy $\beta^2 = \beta + 1$. If $t = 1$ such a β will exist in $GF(p)$ exactly when 5 is a square in $GF(p)$. The condition for this special case is that either $p = 5$ or, by quadratic reciprocity, $p \equiv 1$ or 4 mod 5.

□

Thus non-trivial short loops of C_p can only exist when a *golden ratio* occurs in $GF(p)$. The polynomial $X^2 - X - 1$ has coincident roots in $GF(5)$, and otherwise it has distinct roots. Thus for $p \equiv 1$ or 4 mod 5 there are two rival golden ratios in play, either of which might be the common ratio of a non-trivial short loop. The length of a loop with common ratio β, a golden ratio, is simply the multiplicative order of β. In fact at most one of the golden ratios can cause a loop to be short.

Lemma 2.2. Let H be the additive group of a finite field $GF(p^t)$ where $p \neq 5$. Suppose $\mathbf{f} \in L(H)$ is a non-trivial short loop with common ratio β_1. Let β_2 ($\neq \beta_1$) be the other root of $X^2 - X - 1$ in $GF(p^t)$. There are no short loops, which are non-trivial, in $L(H)$ with common ratio β_2.

Proof.

We may multiply $\mathbf{f}$ by f_0^{-1} to obtain a loop $\mathbf{a} = (1, \beta_1, \ldots)$ of the same length as $\mathbf{f}$. Let $\mathbf{b} = (1, \beta_2, \ldots)$. Put $n = l(\mathbf{a}) = o(\beta_1)$ and observe that $\beta_1\beta_2 = -1$. Thus $\beta_2^{2n} = (-1)^{2n} = 1$. We can exchange the rôles of β_2 and β_1 to obtain that the multiplicative orders of β_1 and β_2 either coincide or differ by a factor of 2.

Thus $l(\mathbf{a} - \mathbf{b})$ divides $m = max\{o(\beta_1),\ o(\beta_2)\}$. Now $\mathbf{a} - \mathbf{b}$ commences with 0 and so must either be $\mathbf{0}$ or of length $k(p)$. It cannot be $\mathbf{0}$ else $\beta_1 = \beta_2$ and then $p = 5$.

It follows that $k(p)$ divides m.

On the other hand, m is the length of a loop of H and so, by Lemma 2.1, we know that m divides $k(p)$. Thus $m = k(p)$ as required.

$\square$

In the case $p = 5$ the polynomial $X^2 - X - 1$ has the double root 3. This gives rise to short loops of length 4 of the form $(a, 3a, 4a, 2a)$ where $a \neq 0$. In fact $k(5) = 20$ by direct calculation:

$$\mathbf{s} = (0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1).$$

Lemma 2.3. (Wall) Suppose p is an odd prime.

(i) If $p \equiv 1$ or 4 mod 5 then $k(p)$ divides $p - 1$.

(ii) If $p \equiv 2$ or 3 mod 5 then $k(p)$ divides $2p + 2$.

Proof.

Choose $\beta \in GF(p^2)$ a root of $X^2 - X - 1$ giving rise to a loop $(1, \beta, \ldots)$ of length $k(p)$. Such a β exists by lemma 2.2. Thus $k(p)$ is the multiplicative order of β. Now part (i) is immediate since then $\beta \in GF(p)^\circ$, the group of units of $GF(p)$. For part (ii), put $\beta_1 = \beta \in GF(p^2) \setminus GF(p)$. Let the other root of $X^2 - X - 1$ in $GF(p^2)$ be β_2. By Galois Theory there in a $GF(p)-$ automorphism of $GF(p^2)$ exchanging β_1 and β_2, so the multiplicative orders of β_1 and β_2 must coincide and be $k(p)$ by Proposition 3.2. Let t be the smallest positive integer such that $\beta_1^t \in GF(p)$. By considering the group $GF(p^2)^\circ / GF(p)^\circ$ we see that t divides $p+1$. It is important to note that if t happens to be odd, then t actually divides $(p+1)/2$. Put $\gamma = \beta_1/\beta_2$. By Galois Theory $\beta_1^u \in GF(p)$ if and only if $\beta_1^u = \beta_2^u$, so then $\gamma^t = 1$. Recall that $\beta_1 \beta_2 = -1$ and so

$$\gamma^t = \beta_1^t / \beta_2^t = (-1)^t \beta_1^{2t} = 1.$$

If t is even $k(p)$ must divide $2t$, and if t is odd, $k(p)$ must divide $4t$. We remarked earlier that t divides $p+1$, and also divides $(p+1)/2$ in the event that t is odd. Either way, we have proved that $k(p)$ must divide $2p+2$.

□

Definition: Suppose G is (temporarily) any Abelian group written additively, and that $\mathrm{g} \in L(G)$. In the event that there exists g_i in the sequence such that $g_i = 0$, we let the rank of apparition of the sequence be r where r is the smallest positive integer such that there exist $m, n \in \mathbf{Z}$ with $g_m = g_n = 0$ and $m - n = r$.

Lemma 2.4. Suppose that x appears immediately before the second 0 in the standard loop $\mathrm{s} \in L(C_p)$, and that $o(x) = t$. We may conclude that $k(p) = rt$ when r is the rank of apparition for p.

Proof.

$f = (0, 1, \ldots 0, x \ldots)$ so multiplication by x rotates f through r. Thus $x^t = 1$ and $x^u \neq 1$ for positive integers u smaller than t, and so $rt = k(p)$.

□

Lemma 2.5. (Vinson) Suppose $p \neq 2$ or 5, then the rank of apparition r of $s \in L(C_p)$ is the multiplicative order of $\gamma = \beta_1/\beta_2$. If r is odd then $k(p) = 4r$. If r is even then either $l = r$ or $l = 2r$.

Proof

Let $\gamma = \beta_1/\beta_2$ and suppose that $o(\gamma) = u$. Notice that

$$s = d(1, \beta_1, \ldots) - d(1, \beta_2, \ldots)$$

where $d = (\beta_1 - \beta_2)^{-1}$. The rank of apparition r is the smallest positive integer such that $\beta_1^r = \beta_2^r$, and so must coincide with the multiplicative order of γ.

Our argument proceeds along the lines of part of the proof of lemma 2.4, though on this occasion we are studying $\gamma = \beta_1/\beta_2$ even when $\beta_1, \beta_2 \in GF(p)$. We may assume that the multiplicative order of β_1 is $k(p)$, else we just interchange the rôles of β_1 and β_2. At any rate, it is still true that $1 = \gamma^r = \beta_1^r/\beta_2^r$ and so $\beta_1^{2r} = (-1)^r$. If r is even this forces $k(p)$ to divide $2r$. Next we are use the fact that p is odd so that $-1 \neq 1$. If r is odd we have $k(p)$ divides $4r$ but not $2r$.

We also know that r divides $k(p)$ irrespective of the parity of r by lemma 2.4. Now we are done.

□

When $p = 2$ the proof of lemma 2.5 goes through almost to the end. It only fails at the point where the distinction is made between -1 and 1. It is true that the rank of apparition is $o(\gamma) = 3$. Thus the Proposition all holds when $p = 2$ save that we must allow $k(2)$ divides $2r$. There is no way round this point, since in fact $k(2) = 3 = r$ so $k(2) \neq 4r$.

Notice that when $p = 5$, we have $\beta_1 = \beta_2 = 3$. In fact the standard loop

$$(0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1)$$

has length 20, and the rank of apparition is 5.

Having tidied the awkward primes, we obtain a clean result.

Corollary.

If p is an odd prime then k is even.

$\square$

We now turn our attention to more general circumstances. In a group of prime order, only the trivial loop $\mathbf{0}$ has the property that two adjacent elements fail to generate the whole group. In general this is not the case. The interesting case is when a pair, and therefore all pairs, of adjacent elements of the loop generate the group – otherwise you simply study a smaller group. We will call a loop (or eloop) a *generating loop* of a finite group G if and only if a pair, and so all pairs, of adjacent elements generate the group. We pursue the theme of p–groups. From this point of view, we may restrict ourselves to p-groups where $G/\phi(G)$, the Frattini quotient, is either cyclic of order p (so G itself is cyclic) or the Cartesian square of the cyclic group of order p. The Abelian case was investigated by Wall. As we observed before, the product of loops is not in general a loop, but we can squeeze out something.

Lemma 2.6. Let G be a finite group with $\mathbf{f} \in L(G)$ a loop. Suppose that $\mathbf{h} \in L(Z(G))$ is a loop of the centre of G, then $\mathbf{f} \cdot \mathbf{h}$, the componentwise product of these loops is a loop of G.

Proof.

For each integer i we have

$$f_i h_i = f_{i-2} f_{i-1} h_{i-2} h_{i-1} = f_{i-2} h_{i-2} f_{i-1} h_{i-1}.$$

□

Theorem A. Suppose G is a p-group for some prime p, and that G has exponent p central length n, then if $\mathbf{f}$ is loop of G then the length of $\mathbf{f}$ must divide $k(p)p^{n-1}$.

Proof.

We induct on the exponent p central length of G, and disposing of the trivial group and the Abelian groups by inspection, we may assume that G has exponent p central length at least 2. We consider the elements f_0, f_1 of G. The group G must have a central subgroup N of exponent p with G/N having exponent p central length $n - 1$. Choose a transversal T for N in G and put $f_i = t_i n_i$ where $t_i \in T$, $n_i \in N$ for $i \in \mathbf{Z}$. The length of the loop $(t_0 N, t_1 N, \ldots)$ in G/N must divide $\lambda = k(p)p^{n-2}$ by the inductive hypothesis. Thus $f_\lambda = t_0 n_\lambda$ and $f_{\lambda+1} = t_1 n_{\lambda+1}$. It is not necessarily true that the bi-infinite sequence (n_i) is a loop of N.

The "ratios" $f_\lambda f_0^{-1}$ and $f_{\lambda+1} f_1^{-1}$ only depend on n_0 and n_1. To see this we tinker with t_0 and t_1 in an arbitrary fashion, and observe that the relevant ratios are left undisturbed. Suppose that $\mathbf{m}$ is any loop of N. Notice that $l(\mathbf{m})$ must divide $k(p)$ by lemma 2.1, and so $l(\mathbf{m})$ must therefore divide λ. Thus

$$\mathbf{m} = (m_\lambda, m_{\lambda+1}, \ldots) = (m_0, m_1, \ldots).$$

Now consider $\mathbf{a} = \mathbf{f} \cdot \mathbf{m}$. By lemma 2.6 this is a loop of G, and by selecting $\mathbf{m}$ appropriately we may force $a_0 = t_0 n$ and $a_1 = t_1 n'$ where n, n' are any chosen pair of elements of N. Now

$$a_\lambda a_0^{-1} = f_\lambda m_\lambda (f_0 m_0)^{-1} = f_\lambda f_0^{-1} = u$$

and

$$a_{\lambda+1}a_1^{-1} = f_{\lambda+1}m_{\lambda+1}(f_1m_1)^{-1} = f_{\lambda+1}f_1^{-1} = v.$$

We have shown that u and v depend only on n_0 and n_1, and do not depend on t_0 or t_1. Thus $f_{j\lambda} = f_{(j-1)\lambda}u$ and $f_{j\lambda+1} = f_{(j-1)\lambda+1}v$ for all positive integers j. We conclude that $f_{p\lambda} = f_0u^p = f_0$ and $f_{p\lambda+1} = f_1v^p = f_1$ and we are done.

$\square$

In Wall [Wa] raises the question as to whether or not it can happen that $k(p) = k(C_p)$ can be equal to $k(C_{p^2})$. He did a computer search and found that $k(p) \neq k(p^2)$ for all primes less than 10^4. It is amusing to note that, with the passage of time, Wall's heroic calculation of 1960 can now be performed in about 1 second on a SUN 4 workstation. We have extended the range of the search, and can announce that equality does not hold for any prime less than 10^8. See Chapter 5 of this document.

Let us focus on the prime 5 for a moment, let G be the Restricted Burnside Group $R(2,5)$ – so $|G| = 5^{34}$ and G is nilpotent of class 12. A computer calculation shows that $k(G) = 20 = k(5)$. In other words, $R(2,5)$ is a homomorphic image of $F(2,20)$. This is the content of Announcement C.

CHAPTER 3

Fourier Sums

We now embark on a large number of calculations concerning *Fourier Sums.* We call them Fourier sums by analogy with the process of integrating a periodic function over its fundamental range, widely studied in other contexts. We will work modulo a prime p, though we could always choose to work modulo an arbitrary natural number by Chinese Remainder Theorem. In the cases where we exclude certain primes, we would have had to impose non-divisibility conditions on the modulus should we have worked modulo a composite number.

We will make the blanket assumption that the prime is at least 5. This simplifies matters considerably. In particular, for odd primes k is even, whereas k is 3 when p is 2. That would lead to all sorts of extra complications. Another prime which causes trouble is the prime 11. This does not start to become awkward until Lemma 3.6, so we will not ban it from the outset. Group theoretically, the cases $p = 2$ or 3 are degenerate in our applications, so we lose little. Some of the congruences hold good when $p = 2$ or 3, a fact which may be verified by direct calculation. Where the range of summation is not stated, it is supposed to be clear. In particular, we begin with sums over the range $0 \le i \le k-1$, exactly over a fundamental period. The key observation to make is that we may translate the range of summation to any other fundamental period without changing the value of the sum. Another useful ruse is to reverse the range of summation.

The philosophy of our (admittedly technical) manipulations is that in order to prove results about finite p-groups, we need to establish that certain sums of monomials manufactured from the Fibonacci sequence modulo p must vanish. These sums can get quite complicated, for example it turns out to be necessary to show that

$$\sum_{r=0}^{k-1}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_r^2 s_j s_i^2 s_{r-j-1} s_{j-i-1}(-1)^{r+1} + \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j\binom{s_j}{2} s_{j-i-1} s_i^2(-1)^{j+1}$$
$$+\sum_{i=0}^{k-1} s_i^2\binom{s_i}{3}(-1)^{i+1} = 0.$$

This is a somewhat daunting sum of sums. We will build an armoury of equations and techniques which will eventually render the above sum tractable. In case the reader might think that any sum (over the fundamental range) of monomials must vanish, we draw his or her attention to $\sum_{i=0}^{k-1} s_i^2(-1)^{i+1}$. We can show that this sum never vanishes for the relevant primes save when the prime is 5.

Another point worth making is that the network of logical dependencies between the equations in the sequel is somewhat complex. We have found a route through to the equations which we need. It is hardly likely that we have found the "shortest path". Some of the equations we study are very friendly, in the sense that almost any sensible attempt to demonstrate their truth will succeed. Others were far more resistant, and required the application of considerable ingenuity before they yielded. There may, of course, be fast tracks to those results, but if so, we have been unable to find them.

Lemma 3.1. The following equations concerning sums of powers of Fibonacci numbers over a fundamental range all hold good.

$$\sum s_i = 0. \tag{1}$$

$$\sum s_i^2 = 0. \tag{2}$$

$$\sum s_i^3 = 0. \tag{3}$$

Proof.

$$\sum s_i = \sum s_{i-1} + \sum s_{i-2} = \sum s_i + \sum s_i.$$

Equation (1) now follows. Note how we have exploited the periodicity of the loop (s_i).

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

so

$$\sum s_i^2 = 2\sum s_i^2 + 2\sum s_i s_{i-1}. \tag{4}$$

Similarly, we express s_{i-2} as $s_i - s_{i-1}$ to obtain

$$\sum s_i^2 = \sum s_{i-2}^2 = 2\sum s_i^2 - 2\sum s_i s_{i-1}. \tag{5}$$

Adding (4) and (5) we obtain

$$2\sum s_i^2 = 4\sum s_i^2$$

from which the equation (2) follows.

$$\sum s_i^3 = \sum s_{i+1}^3 = \sum (s_i + s_{i-1})^3$$

so

$$\sum s_i^3 = 2\sum s_i^3 + 3\sum s_i^2 s_{i-1} + 3\sum s_i s_{i-1}^2. \tag{6}$$

Similarly we may write

$$\sum s_i^3 = \sum s_{i-2}^3 = \sum (s_i - s_{i-1})^3$$

and so

$$\sum s_i^3 = -3\sum s_i^2 s_{i-1} + 3\sum s_i s_{i-1}^2. \tag{7}$$

Add (6) and (7) to obtain

$$2\sum s_i^3 = 2\sum s_i^3 + 6\sum s_i s_{i-1}^2$$

from which it follows that

$$3\sum s_i s_{i-1}^2 = 0. \tag{8}$$

Now we adjust (8) using $s_i = s_{i-1} + s_{i-2}$ to obtain

$$3\sum s_i^3 + 3\sum s_i^2 s_{i-1} = 0. \tag{9}$$

From (6) and (8) we know

$$\sum s_i^3 + 3\sum s_i^2 s_{i-1} = 0. \tag{10}$$

Subtract (10) from (9) to obtain the result.

□

Corollary.

$$\sum s_i s_{i-1} = 0, \tag{11}$$

$$\sum s_i^2 s_{i-1} = \sum s_i s_{i-1}^2 = 0 \tag{12}$$

and

$$\sum s_i^2 s_{i+a} = 0 \ \forall \ a \in \mathbf{Z}. \tag{13}$$

Equation (13) is obtained from equations (3) and (12) using the Fibonacci recurrence and finite induction.

□

Lemma 3.2.

$$s_{k-i} = s_{-i} = s_i(-1)^{i+1} \ \forall i \in \mathbf{Z}, \tag{14}$$

$$\sum s_i(-1)^{i+1} = 0 \tag{15}$$

and

$$\sum s_i^3(-1)^{i+1} = 0. \tag{16}$$

Special Note: Equation (14) is of such crucial importance in the sequel that we will often omit to give future mention to it, else this document would be overwhelmed with such references. The reader is urged to take note of this result. The result is, of course, well-known, as are equations (1) and (15).

Proof.

First notice that $s_i = s_{i-1} + s_{i-2}\ \forall i \in \mathbf{Z}$ forces

$$s_{i-2}(-1)^{i-1} = s_{i-1}(-1)^{i} + s_i(-1)^{i+1}\ \forall i \in \mathbf{Z}.$$

Put $t_{-i} = s_i(-1)^{i+1}$ to obtain $t_i = t_{i-1} + t_{i-2}\ \forall i \in \mathbf{Z}$. Notice also that $t_0 = 0$ and $t_1 = 1$. Thus $(t_i) = (s_i)$, and equation (14) follows. Note that it follows that k is even (for odd primes), because

$$1 = s_1 = s_{k-(k-1)} = s_{k-1}(-1)^k = (-1)^k.$$

(15) : Now

$$\sum s_i(-1)^{i+1} = \sum_{i=0}^{k-1} t_{-i} = \sum_{i=0}^{k-1} t_{k-i}.$$

We now reverse the direction of the range of summation, replacing i by $k-i$. We have

$$\sum s_i(-1)^{i+1} = \sum_{i=1}^{k} s_{-i} = \sum s_{-i} = \sum s_i = 0$$

by (1).

We tackle the proof of equation (16) in the same spirit.

$$\sum s_i^3 = \sum s_{k-i}^3(-1)^{3(i+1)} = \sum s_{k-i}^3(-1)^{k-i+1}$$

since k is even. Now reverse the direction of summation to obtain

$$\sum s_i^3 = \sum_{i=1}^{k} s_i^3(-1)^{i+1} = \sum s_i^3(-1)^{i+1}.$$

Recall that $\sum s_i^3 = 0$ by equation (3) and so we are done.

□

Lemma 3.3. The following equations hold good.

$$\sum s_{i+1}^2 s_i = 0, \tag{17}$$

$$\sum s_{i+1} s_i^2 = 0, \tag{18}$$

$$\sum s_{i+1}^2 s_i (-1)^i = 0 \tag{19}$$

and

$$\sum s_{i+1} s_i^2 (-1)^i = 0. \tag{20}$$

Proof.

We first exploit equation (3),

$$0 = \sum s_{i+2}^3 = \sum (s_{i+1} + s_i)^3 = 2 \sum s_i^3 + 3 \sum s_{i+1}^2 s_i + 3 \sum s_{i+1} s_i^2.$$

Thus

$$3 \sum s_{i+1}^2 s_i + 3 \sum s_{i+1} s_i^2 = 0.$$

Similarly we have

$$0 = \sum s_{i-1}^3 = \sum (s_{i+1} - s_i)^3 = -3 \sum s_{i+1}^2 s_i + 3 \sum s_{i+1} s_i^2.$$

Adding and subtracting these last two equations we obtain (18) and (17). If we repeat this argument, but exploit equation (16) rather than equation (3), we obtain equations (19) and (20).

□

Corollary.

$$\sum s_i^2 s_{i+a} (-1)^i = 0 \ \forall\, a \in \mathbf{Z}. \tag{21}$$

This follows from equations (16) and (20), the Fibonacci recurrence, and finite induction.

$\square$

The next lemma is well-known. We include a proof for completeness.

Lemma 3.4. This is a well-known Fibonacci identity.

$$s_{i+1}s_{i-1} = s_i^2 + (-1)^i \ \forall i \in \mathbf{Z} \tag{22}$$

Proof.

To see this, one may simply observe that

$$\begin{pmatrix} s_{i+1} & s_i \\ s_i & s_{i-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^i$$

in $GL(2, \mathbf{Z})$ by induction on i. Taking determinants yields the result.

$\square$

The next lemma needs a little work. The corresponding non-alternating sum $\sum s_i^4$ is not 0 in general. It is when p is 2 or 3, but a computer search yields no other prime smaller than 900 for which the value of this sum is 0. Happily it is the alternating sum which we need to control.

Lemma 3.5.

$$\sum s_i^4(-1)^i = 0. \tag{23}$$

Proof.

We introduce some temporary shorthand to clarify the proof.

Let

$$\alpha = \sum s_i^4(-1)^i,$$

$$\beta = \sum s_{i+1}^3 s_{i-1}(-1)^i,$$

$$\gamma = \sum s_{i+1} s_{i-1}^3(-1)^i,$$

$$\delta = \sum s_{i+1}^2 s_{i-1}^2(-1)^i,$$

$$\epsilon = \sum s_i^3 s_{i-1}(-1)^i,$$

$$\zeta = \sum s_i s_{i-1}^3(-1)^i$$

and finally

$$\eta = \sum s_i^2 s_{i-1}^2(-1)^i.$$

Our ambition is to demonstrate that $\alpha = 0$. First we show that $\beta = \gamma$.

$$\beta = \sum s_{i+1}^3 s_{i-1}(-1)^i = \sum s_{k-i-1}^3 s_{k-i+1}(-1)^{k-i}.$$

The final equality is obtained using (14) and the fact that k is even – the corollary to lemma 3.2. Now reverse the direction of summation to obtain

$$\beta = \sum_{i=1}^{k} s_{i-1}^3 s_{i+1}(-1)^i = \gamma.$$

The final equality is obtained by translating the range.

Our next ambition is to show that $\alpha = \delta$. We deploy the result of lemma 3.4 (equation (22)) to good effect.

$$\delta = \sum (s_{i+1}s_{i-1})^2(-1)^i = \sum (s_i^2 + (-1)^i)^2(-1)^i$$

so

$$\delta = \sum s_i^4(-1)^i + 2\sum s_i^2 + \sum (-1)^i.$$

Now $\sum s_i^2 = 0$ by (2) and $\sum(-1)^i = 0$ since k is even. Thus $\alpha = \delta$.

Our next target is to show that $\epsilon = \zeta$.

$$\epsilon = \sum s_i^3 s_{i-1}(-1)^i = \sum s_{k-i}^3 s_{k-i+1}(-1)^{k-i+1}.$$

Note that i and $i-1$ have opposite parity. We reverse the range of summation to obtain

$$\epsilon = \sum_{i=1}^{k} s_i^3 s_{i+1}(-1)^{i+1} = \sum s_i s_{i-1}^3 (-1)^i = \zeta.$$

Now for something a little different; we show that $\alpha + \beta = \epsilon$ $(= \zeta)$.

$$\alpha + \beta = \sum s_i^4(-1)^i + \sum s_i^3 s_{i-2}(-1)^{i+1}$$

$$= \sum s_i^3(-1)^i(s_i - s_{i-2}) = \sum s_i^3 s_{i-1}(-1)^i = \epsilon.$$

As a final preliminary, we show that $\eta = 0$. Notice that

$$\eta = \sum s_i^2 s_{i-1}^2(-1)^i = \sum s_{k-i}^2 s_{k-i+1}^2(-1)^{k-i}.$$

Once again we have used (14), and have prepared to reverse the range of summation. Thus

$$\eta = \sum_{i=1}^{k} s_i^2 s_{i+1}^2(-1)^i = \sum s_i^2 s_{i+1}^2(-1)^i.$$

Now translate the range of summation to yield

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

and we are done.

Let us summarize the results of our labour.

$$\beta = \gamma,\ \delta = \alpha,\ \epsilon = \zeta,\ \alpha + \beta = \epsilon,\ \eta = 0.$$

We now embark on calculations to obtain linear relations between α and β, using the binomial theorem as our vehicle.

$$\alpha = \sum (s_{i+1} - s_{i-1})^4(-1)^i = -\alpha - 4\beta + 6\delta - 4\gamma - \alpha$$

so

$$\alpha = -2\alpha - 8\beta + 6\alpha$$

and therefore

$$3\alpha - 8\beta = 0. \tag{$*$}$$

Now we express α in a different way.

$$\alpha = \sum s_{i+1}^4(-1)^{i+1} = \sum (s_i + s_{i-1})^4(-1)^{i+1},$$

so

$$\alpha = -\alpha - 4\epsilon - 6\eta - 4\zeta + \alpha.$$

This simplifies to

$$\alpha = -4(\alpha + \beta) - 0 - 4(\alpha + \beta)$$

and so

$$9\alpha + 8\beta = 0. \tag{$**$}$$

Adding the starred equations we obtain $12\alpha = 0$ from which the result follows.

□

Corollary.

$$\beta = \sum s_{i+1}^3 s_{i-1}(-1)^i = 0, \tag{24}$$

$$\gamma = \sum s_{i+1} s_{i-1}^3(-1)^i = 0, \tag{25}$$

$$\delta = \sum s_{i+1}^2 s_{i-1}^2(-1)^i = 0, \tag{26}$$

$$\epsilon = \sum s_i^3 s_{i-1}(-1)^i = 0, \tag{27}$$

$$\zeta = \sum s_i s_{i-1}^3(-1)^i = 0 \tag{28}$$

and

$$\eta = \sum s_i^2 s_{i-1}^2(-1)^i = 0. \tag{29}$$

$\square$

We now discard the assigned meanings of these Greek letters, since we will wish to use them locally again in the future.

Lemma 3.6. If $p \neq 11$ then

$$\sum s_i^5 = 0 \tag{30}$$

and

$$\sum s_i^5(-1)^i = 0. \tag{31}$$

Proof.

Equation (31) will follow easily from (30), and we address ourselves to (30). Lemma 3.4 (equation (22)) will be our main weapon.

Let $\alpha = \sum s_i^5$ then

$$\alpha = \sum (s_{i+1} - s_{i-1})^5$$

so

$$\alpha = -5\sum s_{i+1}^4 s_{i-1} + 10\sum s_{i+1}^3 s_{i-1}^2 - 10\sum s_{i+1}^2 s_{i-1}^3 + 5\sum s_{i+1} s_{i-1}^4$$

and therefore

$$\alpha = -5\sum s_{i+1}s_{i-1}(s_{i+1}^3 - s_{i-1}^3) + 10\sum s_{i+1}^2 s_{i-1}^2(s_{i+1} - s_{i-1}).$$

We now deploy equation (22) to obtain

$$\alpha = -5\sum (s_i^2 + (-1)^i)(s_{i+1}^3 - s_{i-1}^3) + 10\sum (s_i^2 + (-1)^i)^2 s_i.$$

This expression admits of considerable simplification. In fact one can simply suppress the occurrences of $(-1)^i$ because the following equations hold:

$$\sum s_{i+1}^3(-1)^{i+1} = 0 \text{ from } (16)$$

$$\sum s_{i-1}^3(-1)^{i+1} = 0 \text{ from } (16)$$

$$\sum s_i^3(-1)^{i+1} = 0 \text{ from } (16)$$

and

$$\sum s_i = 0 \text{ from } (1).$$

Thus

$$\alpha = -5\sum s_i^2(s_{i+1}^3 - s_{i-1}^3) + 10\alpha,$$

and so

$$-9\alpha = -5\sum s_i^2(s_{i+1}^3 - (s_{i+1} - s_i)^3).$$

Expanding we obtain

$$-9\alpha = -5\sum s_i^2(3s_{i+1}^2 s_i - 3s_{i+1}s_i^2 + s_i^3)$$

so

$$-9\alpha = -5\sum s_i^2(3s_{i+1}s_i(s_{i+1} - s_i) + s_i^3)$$

and therefore

$$-9\alpha = -5\sum s_i^2(3s_{i+1}s_is_{i-1} + s_i^3).$$

We now close on our quarry using lemma 3.4 again. We have

$$-9\alpha = -5\sum s_i^2(3s_i(s_i^2 + (-1)^i) + s_i^3).$$

Once again we may suppress $(-1)^i$ because of equation (16). Thus

$$-9\alpha = -5\sum 4s_i^5 = -20\alpha.$$

We conclude that $11\alpha = 0$. Since we have excluded the prime 11, we have demonstrated the truth of equation (30).

To prove the second part of the lemma is now an easy task. We have

$$\sum s_i^5(-1)^i = \sum s_{k-i}^5(-1)^{i+1}(-1)^i = -\sum s_{k-i}^5 = -\sum s_i^5 = 0,$$

and by appeal to equation (30), equation (31) is justified.

$\square$

As a matter of interest, the exclusion of the prime 11 in lemma 3.6 is necessary. When $p = 11$ a direct calculation yields $\sum s_i^5 = 1$ and $\sum s_i^5(-1)^i = -1$.

Lemma 3.7. Assuming $p \neq 11$, we have

$$\sum s_i^2 s_{i-1}^3 = 0 \tag{32}$$

and

$$\sum s_i^3 s_{i-1}^2 (-1)^i = 0. \tag{33}$$

Proof.

Put $\alpha = \sum s_i^2 s_{i-1}^3$, so

$$\alpha = \sum (s_{i+1} - s_{i-1})^2 s_{i-1}^3 = \sum (s_{i+1}^2 - 2s_{i+1}s_{i-1} + s_{i-1}^2) s_{i-1}^3.$$

Thus

$$\alpha = \sum s_{i+1}^2 s_{i-1}^3 - 2\sum s_{i+1} s_{i-1}^4 + \sum s_{i-1}^5,$$

but by equation (30) this simplifies to

$$\alpha = \sum s_{i+1}^2 s_{i-1}^3 - 2\sum s_{i+1} s_{i-1}^4. \tag{34}$$

Now deploy equation (22) in conjunction with equation (34) to deduce that

$$\alpha = \sum (s_i^2 + (-1)^i)^2 s_{i-1} - 2\sum (s_i^2 + (-1)^i) s_{i-1}^3,$$

and so

$$\alpha = \sum (s_i^4 + 2s_i^2(-1)^i + 1) s_{i-1} - 2\sum s_i^2 s_{i-1}^3 - 2\sum s_{i-1}^3 (-1)^i.$$

Now equations (19), (1) and (16) come to aid, giving

$$\alpha = \sum s_i^4 s_{i-1} - 2\sum s_i^2 s_{i-1}^3,$$

and so

$$3\alpha = \sum s_i^4 s_{i-1}. \tag{35}$$

We now embark on another tack. This time we exploit equation (30). We have

$$\sum s_{i+1}^5 = \sum (s_i + s_{i-1})^5 = 0$$

so

$$\sum (s_i^5 + 5s_i^4 s_{i-1} + 10 s_i^3 s_{i-1}^2 + 10 s_i^2 s_{i-1}^3 + 5 s_i s_{i-1}^4 + s_{i-1}^5) = 0,$$

which simplifies to

$$5\sum s_i^4 s_{i-1} + 10\sum s_i^3 s_{i-1}^2 + 10\sum s_i^2 s_{i-1}^3 + 5\sum s_i s_{i-1}^4 = 0, \tag{36}$$

thanks to equation (30).

We now repeat this argument, this time observing that equation (30) yields

$$\sum s_{i-2}^5 = \sum (s_i - s_{i-1})^5 = 0.$$

After mimicking our previous calculation, we find

$$-5\sum s_i^4 s_{i-1} + 10\sum s_i^3 s_{i-1}^2 - 10\sum s_i^2 s_{i-1}^3 + 5\sum s_i s_{i-1}^4 = 0. \tag{37}$$

Subtracting (37) from (36) we obtain

$$10\sum s_i^4 s_{i-1} + 20\sum s_i^2 s_{i-1}^3 = 0,$$

or rather

$$20\alpha = -10\sum s_i^4 s_{i-1}. \tag{38}$$

From equations (35) and (38) we deduce $50\alpha = 0$, which really asserts that $25\alpha = 0$. When $p = 5$ the result is true by direct calculation and so equation (32) is established. Now for equation (33).

$$\sum s_i^2 s_{i-1}^3 = \sum s_{k-i}^2 s_{k-i+1}^3 (-1)^i = 0$$

by (32). Now reverse the direct of summation - replacing $k-i$ by i to obtain

$$\sum_{i=1}^{k} s_i^2 s_{i+1}^3 (-1)^i = \sum s_i^3 s_{i-1}^2 (-1)^{i+1} = 0.$$

Thus (33) is also established and we are done.

□

The proviso that $p \neq 11$ is necessary, since a direct calculation yields that, in that instance, the sums described in (32) and (33) are, respectively, 5 and 6.

Corollary.

Unless the prime p is 11, we have

$$\sum s_i^4 s_{i-1} = 0. \tag{39}$$

In the event that $p = 11$, the sum is actually 3.

□

From now on, we will ban the prime 11 from our considerations, since whenever we have recourse to one of the preceding equations (37),(38) or (39), we would have to make an exception for that prime.

Lemma 3.8.

$$\sum s_i^3 s_{i-1}^2 = 0 \tag{40}$$

and

$$\sum s_i^2 s_{i-1}^3 (-1)^i = 0. \tag{41}$$

Proof.

We exploit equation (32). We have

$$\sum s_i^2 s_{i-1}^3 = \sum s_{i-1}^3 (s_{i-1} + s_{i-2})^2 = 0$$

so

$$\sum s_{i-1}^5 + 2\sum s_{i-1}^4 s_{i-2} + \sum s_{i-1}^3 s_{i-2}^2 = 0.$$

The first sum vanishes by equation (30) and the second by equation (39). Thus

$$\sum s_{i-1}^3 s_{i-2}^2 = \sum s_i^3 s_{i-1}^2 = 0$$

and so equation (40) is established. Now we obtain equation (41) by reversing the direction of summation in equation (40). We have

$$\sum s_i^3 s_{i-1}^2 = \sum s_{k-i}^3 s_{k-i+1}^2 (-1)^{i+1} = 0.$$

Replacing $k - i$ by i we obtain

$$\sum_{i=1}^{k} s_i^3 s_{i+1}^2 (-1)^{i+1} = 0.$$

Now replace $i + 1$ by i and then slide the range of summation to yield

$$\sum s_i^2 s_{i-1}^3 (-1)^i = 0$$

as required.

□

Lemma 3.9.

$$\sum s_{i+1} s_i^4 = 0, \tag{42}$$

$$\sum s_i^4 s_{i-1} (-1)^i = 0 \tag{43}$$

and

$$\sum s_{i+1} s_i^4 (-1)^i = 0. \tag{44}$$

Proof.

From equations (39) and (30) we have

$$\sum s_{i+1} s_i^4 = \sum (s_i + s_{i-1}) s_i^4 = \sum s_i^5 + \sum s_i^4 s_{i-1} = 0.$$

Thus equation (42) is established. We have

$$\sum s_{i+1}s_i^4 = \sum s_{k-i-1}s_{k-i}^4(-1)^i = 0.$$

Now reverse the direction of summation in the usual way, replacing $k-i$ by i. This yields

$$\sum_{i=1}^{k} s_{i-1}s_i^4(-1)^i = \sum s_i^4 s_{i-1}(-1)^i = 0$$

and equation (43) is established. Finally we turn to equation (43) as our route to proving equation (44). Thus we see that

$$\sum s_i^4 s_{i-1}(-1)^i = \sum s_i^4(s_{i+1} - s_i)(-1)^i = 0.$$

Now deploy equations (43) and (31) and we are home.

□

Lemma 3.10.

$$\alpha = \sum s_i^2 s_{i-2}^3(-1)^{i+1} = 0. \tag{45}$$

Proof.

$$\alpha = \sum (s_{i-1} + s_{i-2})^2 s_{i-2}^3(-1)^{i+1}$$

so

$$\alpha = \sum s_{i-1}^2 s_{i-2}^3(-1)^{i+1} + 2\sum s_{i-1}s_{i-2}^4(-1)^{i+1} + \sum s_{i-2}^5(-1)^{i+1}$$

so

$$\alpha = \sum s_i^2 s_{i-1}^3(-1)^i - 2\sum s_{i+1}s_i^4(-1)^i - \sum s_i^5(-1)^i.$$

These sums vanish by equations (41), (44) and (31) respectively. Thus $\alpha = 0$ and we are done.

□

Lemma 3.11. This is presumably well-known. For each integer n we have

$$3s_n^2 = s_{n+1}^2 + s_{n-1}^2 + 2(-1)^{n+1}. \tag{46}$$

Proof.

This result actually holds in the ordinary Fibonacci sequence, and not just modulo a prime p.

$$s_n^2 = (s_{n+1} - s_{n-1})^2 = s_{n+1}^2 + s_{n-1}^2 - 2s_{n+1}s_{n-1}$$

but $s_{n+1}s_{n-1} = s_n^2 + (-1)^n$ by equation (22) so

$$s_n^2 = s_{n+1}^2 + s_{n-1}^2 - 2s_n^2 + 2(-1)^{n+1}$$

and the result follows.

□

On the basis of computational experiments, we propose the following conjectures.

Conjecture 1: If q is prime then $\sum s_i^q = 0$ for all but finitely many prime moduli p. The evidence for this conjecture is as follows. We know it holds for primes q less than 11. For primes q larger than 7 we have computed all values of the prime modulus $p < 200$ for which the sum $\sum s_i^q$ fails to vanish. This conjecture looks rather dodgy and we will discard it in published documents unless we find more compelling arguments.

Conjecture 2: The prime moduli causing the sum $\sum s_i^q$ to fail to vanish must be congruent to 1 or -1 mod 5.

q	p
5	11
7	11, 29
11	19, 29
13	19, 29
17	11, 19, 29, 31
19	11, 29, 31
23	29, 31
29	11, 19, 31, 59
31	19, 59
37	11, 29, 59, 71
41	29, 59, 71, 79
43	29, 59, 71, 79
47	11, 19, 29, 31, 59, 71, 79

53	19, 29, 31, 59, 71, 79
59	11, 31, 71, 79
61	71, 79
67	11, 19, 29, 71, 79
71	19, 29, 79

We now embark on the study of Fibonacci double sums, and remind the reader that the primes 2,3 and 11 are barred from our discussions. A typical sum is of the form $\sum_{j=0}^{k-1}\sum_{i=0}^{j-1} f(i,j)$. We abbreviate the notation for this sum to $\sum_{i<j} f(i,j)$. In the event that we wish to consider $\sum_{j=0}^{k-1}\sum_{i=0}^{k-1} f(i,j)$ we will write $\sum_{all} f(i,j)$. As in the case of single sums, we will heavily exploit the periodicity of (s_i), and tinker with ranges of summation. A variety of other tricks is needed too, and we will introduce such ruses on an *ad hoc* basis as the need arises.

Lemma 3.12.

$$\nu = \sum_{i<j} s_j^2 s_{j-i} = 0 \tag{47}$$

and

$$\mu = \sum_{i<j} s_j^2 s_{j-i-1} = 0. \tag{48}$$

Proof.

$$\begin{aligned}
\nu &= \sum_{i<j} s_j^2 s_{j-i+1} - \sum_{i<j} s_j^2 s_{j-i-1} \\
&= \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j^2 s_{j-i+1} - \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j^2 s_{j-i-1} \\
&= \sum_{j=0}^{k-1}\sum_{i=-1}^{j-2} s_j^2 s_{j-i} - \sum_{j=0}^{k-1}\sum_{i=1}^{j} s_j^2 s_{j-i}.
\end{aligned}$$

We can tinker with the ranges of summation providing we only add or subtract terms which vanish, or compensate by inserting new sums. Thus

$$\nu = (\sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j^2 s_{j-i} + \sum_{j=0}^{k-1} s_j^2 s_{j+1} - \sum_{j=0}^{k-1} s_j^2 s_1) - (\sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j^2 s_{j-i} - \sum_{j=0}^{k-1} s_j^3 + \sum_{j=0}^{k-1} s_j^2 s_0).$$

In this expression for ν, the first and fourth terms cancel, the sixth vanishes since $s_0 = 0$, and the remaining terms – the second, third and fifth, vanish by equations (12), (2) and (3) respectively. Thus $\nu = 0$ and (47) is established.

We now address μ,

$$\mu = \sum_{i<j} s_j^2 s_{j-i-1} = \sum_{j=0}^{k-1}\sum_{i=1}^{j} s_j^2 s_{j-i}.$$

We slide down the range for i by 1. The case $i = j$ is harmless since $s_0 = 0$. Thus

$$\mu = \sum_{i<j} s_j^2 s_{j-i} - \sum s_j^3.$$

We deploy equation (3) and equation (47) to deduce $\mu = \nu = 0$, and equation (48) is established.

$\square$

Corollary.

$$\sum_{i<j} s_j^2 s_{j-i+a} = 0 \ \forall a \in \mathbf{Z}. \tag{49}$$

This follows from equations (47),(48), the Fibonacci recurrence and finite induction.

$\square$

Lemma 3.13.

$$\sum_{i<j} s_j^2 s_i^2 s_{j-i-1}(-1)^{j+1} = 0. \tag{50}$$

Proof.

Put

$$\psi = \sum_{i<j} s_j^2 s_i^2 s_{j-i-1}(-1)^{j+1}.$$

Recall equation (46)

$$3s_n^2 = s_{n+1}^2 + s_{n-1}^2 + 2(-1)^{n+1} \quad \forall n \in \mathbf{Z},$$

which will play a central rôle in our manipulations. We introduce some temporary names for various expressions.

$$\alpha = \sum_{i<j} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1},$$

$$\beta = \sum_{i<j} s_{j-1}^2 s_i^2 s_{j-i-1}(-1)^{j+1}$$

and

$$\gamma = \sum_{i<j} s_i^2 s_{j-i-1}.$$

Let $\theta = 3\psi$ then

$$\theta = \alpha + \beta + 2\gamma,$$

by recasting $3s_j^2$ using equation (46). The previous lemma (equation (48)) shows that $\gamma = 0$ so $\theta = \alpha + \beta$. Now

$$\alpha = \sum_{i<j} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} = \sum_{j=1}^{k}\sum_{i=0}^{j-2} s_j^2 s_i^2 s_{j-i-2}(-1)^j.$$

There is no problem in adjusting the range for j since $s_0 = s_k = 0$. Thus

$$\alpha = \sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j^2 s_i^2 s_{j-i-2}(-1)^j.$$

Now we wish to add $j-1$ to the range of i; this too is fine since it involves the creation of the extra term

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

This vanishes by equation (29). Thus

$$\alpha = \sum_{i<j} s_j^2 s_i^2 s_{j-i-2}(-1)^j. \tag{51}$$

We now give β similar treatment.

$$\beta = \sum_{i<j} s_{j-1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} = \sum_{j=-1}^{k-2}\sum_{i=0}^{j} s_j^2 s_i^2 s_{j-i}(-1)^j.$$

We can remove -1 from the range of j since there are no legal values of i less than 0. We wish to introduce $k-1$ into the range of j. This creates an extra term

$$\sum_{i=0}^{k-1} s_{k-1}^2 s_i^2 s_{k-i-1}(-1) = \sum s_i^2 s_{i+1}(-1)^{i+1}.$$

This last sum vanishes by equation (20). The removal of j from the range of i is harmless since $s_0 = 0$. Thus we may write

$$\beta = \sum_{i<j} s_j^2 s_i^2 s_{j-i}(-1)^j. \tag{52}$$

We are roughly half way through this proof. Now, in the spirit of justice, we start again, this time giving i the treatment previously meted out to j.

$$\theta = \delta + \epsilon + 2\zeta$$

where

$$\delta = \sum_{i<j} s_j^2 s_{i+1}^2 s_{j-i-1}(-1)^{j+1},$$

$$\epsilon = \sum_{i<j} s_j^2 s_{i-1}^2 s_{j-i-1}(-1)^{j+1}$$

and

$$\zeta = \sum_{i<j} s_j^2 s_{j-i-1}(-1)^{i+j}.$$

As might be expected, ζ is the easiest term to deal with, and so we tackle it first. We are introducing a new type of ruse here, so the reader may wish to be especially alert. Of course we could prove that $\zeta = 0$ by a direct method, but the following technique illustrates a new weapon at our disposal.

$$\zeta = \sum_{i<j} s_j^2 s_{j-i-1}(-1)^{i+j} = \sum_{i<j} s_j^2 s_{i-j+1}$$

so

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

since $s_k = 0$. Now prepare to reverse direction of summation. We have

$$\zeta = \sum_{j=0}^{k} \sum_{i=0}^{j-1} s_{k-j}^2 s_{(k-j)-(k-i)+1}.$$

We replace $k-j$ by j and $k-i$ by i to yield

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

The clean way to see that this ruse is legitimate is to realize that we were summing over all pairs (i,j) in the range $0 \le i < j \le k$. This is the same as the range $0 \le k-j < k-i \le k$. Thus

$$\zeta = \sum_{j<i} s_j^2 s_{j-i+1} + \sum s_j^2 s_{j-k+1}.$$

The final sum in this last equation is really $\sum s_j^2 s_{j+1}$ which vanishes by equation (12). We can shave of the top of the range of i by equation (18). We conclude that

$$\zeta = \sum_{j<i} s_j^2 s_{j-i+1} = \sum_{all} s_j^2 s_{j-i+1} - \sum_{i<j} s_j^2 s_{j-i+1} - \sum s_j^2 s_1.$$

The second and third terms on the right vanish by equations (49) and (2) respectively. Thus we deduce that

$$\zeta = \sum_{j=0}^{k-1} s_j^2 (\sum_{i=0}^{k-1} s_{j-i+1}).$$

The inner sum is really just $\sum s_i$ which vanishes by equation (1). Thus we have shown that $\zeta = 0$.

We conclude that $\theta = \delta + \epsilon$. Now we work on δ. Notice that

$$\delta = \sum_{i<j} s_j^2 s_{i+1}^2 s_{j-i-1} (-1)^{j+1} = \sum_{j=0}^{k-1} \sum_{i=0}^{j-1} s_j^2 s_{i+1}^2 s_{j-i-1} (-1)^{j+1}.$$

Now change variable i in the sum to obtain

$$\delta = \sum_{j=0}^{k-1} \sum_{i=1}^{j} s_j^2 s_i^2 s_{j-i} (-1)^{j+1}.$$

Now we can slide the range of i down by 1 at both ends since $s_0 = 0$. Thus

$$\delta = \sum_{i<j} s_j^2 s_i^2 s_{j-i} (-1)^{j+1} = -\beta. \tag{53}$$

by equation (52). Thus $\delta = -\beta$. On this bright note, we set off in pursuit of ϵ.

$$\epsilon = \sum_{i<j} s_j^2 s_{i-1}^2 s_{j-i-1} (-1)^{j+1} = \sum_{j=0}^{k-1} \sum_{i=0}^{j-1} s_j^2 s_{i-1}^2 s_{j-i-1} (-1)^{j+1}.$$

Changing variable as before, we obtain

$$\epsilon = \sum_{j=0}^{k-1} \sum_{i=-1}^{j-2} s_j^2 s_i^2 s_{j-i-2} (-1)^{j+1}.$$

Once again we would like to slide the range of i by 1, but this time upwards. When we fix $i = -1$ the contribution to the sum is

$$\sum s_j^2 s_{-1}^2 s_{j-1} (-1)^{j+1}$$

which vanishes by equation (19). When we put $i = j - 1$ the contribution is

$$\sum s_j^2 s_{j-1}^2 s_{-1}(-1)^{j+1}.$$

This vanishes by equation (29). We conclude that

$$\epsilon = \sum_{i<j} s_j^2 s_i^2 s_{j-i-2}(-1)^{j+1} = -\alpha,$$

by equation (51). Pulling things together, we obtain

$$\theta = \alpha + \beta = -(\delta + \epsilon) = -\theta.$$

Thus $\theta = 0$, and so $\psi = 0$ and we are done.

□

Corollary.

$$\zeta = \sum_{i<j} s_j^2 s_{j-i-1}(-1)^{i+j} = 0. \tag{54}$$

Lemma 3.14. Using the notation of the previous lemma

$$\alpha = \sum_{i<j} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} = 0 \tag{55}$$

and

$$\beta = \sum_{i<j} s_{j-1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} = 0. \tag{56}$$

Proof.

In the proof of the previous lemma we obtained $\alpha + \beta = 0$. Also, using equations (52) and (53) we have

$$\beta - \alpha = \sum_{i<j} s_j^2 s_i^2 s_{j-i}(-1)^j - \sum_{i<j} s_j^2 s_i^2 s_{j-i-2}(-1)^j = \sum_{i<j} s_j^2 s_i^2 s_{j-i-1}(-1)^j = -\psi = 0.$$

Thus $\alpha = \beta = 0$.

$\square$

Corollary.

$$\sum_{i<j} s_j^2 s_i^2 s_{j-i+a}(-1)^{j+1} = 0 \quad \forall a \in \mathbf{Z}. \tag{57}$$

This follows from equations (50),(51) and (55), the Fibonacci recurrence and finite induction.

$\square$

Lemma 3.15.

$$\sum_{i<j} s_j s_{j+1} s_i^2 s_{j-i-1}(-1)^{j+1} = 0. \tag{58}$$

Proof.

Temporarily put

$$\lambda = \lambda(i,j) = s_i^2 s_{j-i-1}(-1)^{j+1}.$$

The previous two lemmas tell us (via equations (56),(50) and (54)) that

$$\sum_{i<j} s_{j-1}^2 \lambda = \sum_{i<j} s_j^2 \lambda = \sum_{i<j} s_{j+1}^2 \lambda = 0.$$

Now

$$2\sum_{i<j} s_j s_{j+1} \lambda = -\sum_{i<j} (s_{j+1} - s_j)^2 \lambda = -\sum_{i<j} s_{j-1}^2 \lambda = 0.$$

The final equality is simply equation (56), and we are done.

$\square$

Corollary.

$$\sum_{i<j} s_j s_{j+a} s_i^2 s_{j-i-1}(-1)^{j+1} = 0 \quad \forall a \in \mathbf{Z}. \tag{59}$$

$\square$

Lemma 3.16.

$$\sum_{i<j} s_j s_i^2 s_{j-i+a} = 0 \;\; \forall\, a \in \mathbf{Z}. \tag{60}$$

Proof.

Put

$$\alpha = \sum_{i<j} s_j s_i^2 s_{j-i+a} = \sum_{i<j} s_{j+1} s_i^2 s_{j-i+a} - \sum_{i<j} s_{j-1} s_i^2 s_{j-i+a}.$$

Thus

$$\alpha = \sum_{j=1}^{k}\sum_{i=0}^{j-2} s_j s_i^2 s_{j-i+a-1} - \sum_{j=-1}^{k-2}\sum_{i=0}^{j} s_j s_i^2 s_{j-i+a+1},$$

by adjusting the ranges of i and j. Now we immediately deduce

$$\alpha = \sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j s_i^2 s_{j-i+a-1} - \sum_{j=0}^{k-2}\sum_{i=0}^{j} s_j s_i^2 s_{j-i+a+1}$$

by removing and introducing vanishing terms. Now

$$\sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j s_i^2 s_{j-i+a-1} = \sum_{i<j} s_j s_i^2 s_{j-i+a-1} - \sum_{j=0}^{k-1} s_j s_{j-1}^2 s_a.$$

The last term vanishes by equation (12) so

$$\sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j s_i^2 s_{j-i+a-1} = \sum_{i<j} s_j s_i^2 s_{j-i+a-1}.$$

We now attack the second sum in our expression for α. We see that

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

The final sum being subtracted is tractable. It is simply

$$\sum_{i=0}^{k-1} s_{k-1} s_i^2 s_{i-a} (-1)^{i-a+1},$$

and this vanishes by equation (21). We deduce that

$$\sum_{j=0}^{k-1}\sum_{i=0}^{j} s_j s_i^2 s_{j-i+a+1} = \sum_{i<j} s_j s_i^2 s_{j-i+a+1} + \sum s_j^3 s_{a+1}.$$

The last term vanishes by equation (3), and so we have

$$\alpha = \sum_{i<j} s_j s_i^2 s_{j-i+a-1} - \sum_{i<j} s_j s_i^2 s_{j-i+a+1}.$$

Now $s_{j-i+a-1} - s_{j-i+a+1} = -s_{j-i+a}$ so

$$\alpha = -\sum_{i<j} s_j s_i^2 s_{j-i+a} = -\alpha.$$

Thus $\alpha = 0$ as required.

□

Lemma 3.17.

$$\sum_{i<j} s_j^2 s_{j-i-1} s_i (-1)^{i+j} = 0. \tag{61}$$

Proof.

Let

$$\alpha = \sum_{i<j} s_j^2 s_{j-i-1} s_i (-1)^{i+j},$$

so

$$\alpha = \sum_{i<j} s_j^2 s_i s_{i-j+1}.$$

Now

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

but the inner sum vanishes thanks to equation (21). Thus we have

$$\sum_{all} s_j^2 s_i s_{i-j+1} = 0.$$

Our intention is to use the following trick – the meaning of which should be self evident –

$$\sum_{all} = \sum_{i<j} + \sum_{j<i} + \sum_{i=j}.$$

We must investigate the sum when $i = j$. This is just

$$\sum s_i^2 s_i s_1 = \sum s_i^3 = 0,$$

which vanishes because of equation (3). We conclude that

$$\alpha = -\sum_{j<i} s_j^2 s_i s_{i-j+1} = -\sum_{i<j} s_j s_i^2 s_{j-i+1}.$$

The final equality is obtained by permuting notation. Thus

$$\alpha = -\sum_{i<j} s_j s_i^2 s_{j-i+1}$$

which vanishes by equation (60).

□

Lemma 3.18.

$$\sum_{i<j} s_j^2 s_i s_{i-1} s_{j-i-1} (-1)^{j+1} = 0. \qquad (62)$$

Proof.

Let

$$\alpha = \sum_{i<j} s_j^2 s_i s_{i-1} s_{j-i-1} (-1)^{j+1}.$$

Using $s_{i-1} = s_i - s_{i-2}$ and the equation (50) we obtain

$$\alpha = \sum_{i<j} s_j^2 s_i s_{i-2} s_{j-i-1} (-1)^j.$$

Now use equation (22) so

$$\alpha = \sum_{i<j} s_j^2 s_{i-1}^2 s_{j-i-1} (-1)^j - \sum s_j^2 s_{j-i-1} (-1)^{i+j}.$$

The last term vanishes by equation (54). Now

$$\alpha = \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_j^2 s_{i-1}^2 s_{j-i-1}(-1)^j$$

so

$$\alpha = \sum_{j=1}^{k}\sum_{i=1}^{j-1} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1}.$$

Adjusting the ranges we have

$$\alpha = \sum_{i<j} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} + \sum s_{k+1}^2 s_i^2 s_{k-i-1},$$

so

$$\alpha = \sum_{i<j} s_{j+1}^2 s_i^2 s_{j-i-1}(-1)^{j+1} + \sum s_{i+1} s_i^2 (-1)^i.$$

These last two terms vanish by (55) and (20) so $\alpha = 0$ and we are done.

$\square$

Lemma 3.19.

$$6 s_j s_{j-1}^2 = s_{j+1}^3 + s_{j-2}^3 - 2 s_j^3 \quad \forall j \in \mathbf{Z}. \tag{63}$$

Proof.

For each integer j we have

$$s_{j+1}^3 + s_{j-2}^3 - 2 s_j^3 = (s_j + s_{j-1})^3 + (s_j - s_{j-1})^3 - 2 s_j^3 = 6 s_j s_{j-1}^2.$$

$\square$

Lemma 3.20.

$$6 s_j^2 s_{j-1} = s_{j+1}^3 - s_{j-2}^3 - 2 s_{j-1}^3 \quad \forall j \in \mathbf{Z}. \tag{64}$$

Proof.

For each integer j we have

$$s_{j+1}^3 - s_{j-2}^3 - 2s_{j-1}^3 = (s_j + s_{j-1})^3 - (s_j - s_{j-1})^3 - 2s_{j-1}^3 = 6s_j^2 s_{j-1}.$$

□

Lemma 3.21.

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i s_{i-1}^2 (-1)^{j+1} = 0 \quad \forall a \in \mathbf{Z}. \tag{65}$$

Proof.

Put

$$\alpha = 6\sum_{i<j} s_j^2 s_{j-i+a} s_i s_{i-1}^2 (-1)^{j+1}$$

$$= \sum_{i<j} s_j^2 s_{j-i+a} s_{i+1}^3 (-1)^{j+1} + \sum_{i<j} s_j^2 s_{j-i+a} s_{i-2}^3 (-1)^{j+1} - 2\sum_{i<j} s_j^2 s_{j-i+a} s_i^3 (-1)^{j+1}.$$

Now fiddle with the range of summation for i.

$$\alpha = \sum_{j=0}^{k-1}\sum_{i=1}^{j} s_j^2 s_{j-i+a+1} s_i^3 (-1)^{j+1} + \sum_{j=0}^{k-1}\sum_{i=-2}^{j-3} s_j^2 s_{j-i+a-2} s_i^3 (-1)^{j+1}$$

$$-2\sum_{i<j} s_j^2 s_{j-i+a} s_i^3 (-1)^{j+1}. \tag{66}$$

We deal with these three double sums in equation (66) individually. The first one is

$$\sum_{j=0}^{k-1}\sum_{i=1}^{j} s_j^2 s_{j-i+a+1} s_i^3 (-1)^{j+1} = \sum_{i<j} s_j^2 s_{j-i+a+1} s_i^3 (-1)^{j+1} + \sum_{j=0}^{k-1} s_{a+1} s_j^5 (-1)^{j+1}.$$

The last term vanishes by (31) so

$$\sum_{j=0}^{k-1}\sum_{i=1}^{j} s_j^2 s_{j-i+a+1} s_i^3 (-1)^{j+1} = \sum_{i<j} s_j^2 s_{j-i+a+1} s_i^3 (-1)^{j+1}. \tag{67}$$

Now for the second term in equation (66). We have

$$\sum_{j=0}^{k-1}\sum_{i=-2}^{j-3} s_j^2 s_{j-i+a-2} s_i^3(-1)^{j+1} = \sum_{i<j} s_j^2 s_{j-i+a-2} s_i^3(-1)^{j+1} - \sum s_j^2 s_a s_{j-2}^3(-1)^{j+1}$$

$$- \sum s_j^2 s_{a-1} s_{j-1}^3(-1)^{j+1} + \sum s_j^2 s_{j+a} s_{-2}^3(-1)^{j+1} + \sum s_j^2 s_{j+a+1} s_{-1}^3(-1)^{j+1}.$$

The last four terms vanish by equations (45), (41), (21) and (21) respectively, so

$$\sum_{j=0}^{k-1}\sum_{i=-2}^{j-3} s_j^2 s_{j-i+a-2} s_i^3(-1)^{j+1} = \sum_{i<j} s_j^2 s_{j-i+a-2} s_i^3(-1)^{j+1}. \tag{68}$$

Thus from equations (66), (67) and (68) we have

$$\alpha = \sum_{i<j} s_j^2 s_i^3(-1)^{j+1}(s_{j-i+a+1} + s_{j-i+a-2} - 2s_{j-i+a}).$$

However,

$$s_{j-i+a+1} + s_{j-i+a-2} - 2s_{j-i+a} = (s_{j-i+a+1} - s_{j-i+a}) - (s_{j-i+a} - s_{j-i+a-2})$$

$$= s_{j-i+a-1} - s_{j-i+a-1} = 0.$$

Thus $\alpha = 0$ and we are done.

□

Lemma 3.22.

$$\sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i+a}(-1)^{j+1} = 0 \quad \forall a \in \mathbf{Z}. \tag{69}$$

Proof.

The proof is similar to that of lemma 3.21, but this time we exploit lemma 3.20 rather than lemma 3.19. Put

$$\alpha = 6\sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i+a}(-1)^{j+1},$$

$$\beta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j,$$

$$\gamma = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j$$

and

$$\delta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j.$$

Now we introduce more notation. Put

$$\beta_1 = \sum_{j=1}^{k} \sum_{i=0}^{j-2} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j,$$

$$\gamma_1 = \sum_{j=-2}^{k-3} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j$$

and

$$\delta_1 = \sum_{j=-1}^{k-2} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j.$$

Equation (64) yields that

$$\alpha = \sum_{i<j} s_{j+1}^3 s_i^2 s_{j-i+a}(-1)^{j+1} - \sum_{i<j} s_{j-2}^3 s_i^2 s_{j-i+a}(-1)^{j+1}$$

$$-2\sum_{i<j} s_{j-1}^3 s_i^2 s_{j-i+a}(-1)^{j+1}.$$

Recasting the ranges of summation for j we obtain

$$\alpha = \sum_{j=1}^{k} \sum_{i=0}^{j-2} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j + \sum_{j=-2}^{k-3} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j$$

$$-2 \sum_{j=-1}^{k-2} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j \tag{70}$$

or rather

$$\alpha = \beta_1 + \gamma_1 - 2\delta_1.$$

We must simplify each sum on the right. We take them in sequence. First we have

$$\beta_1 = \beta - \sum s_j^3 s_{j-1}^2 s_a(-1)^j.$$

The last expression vanishes by (33) so $\beta_1 = \beta$. We now approach γ_1. We have

$$\gamma_1 = \sum_{j=0}^{k-3} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j$$

so

$$\gamma_1 = \sum_{j=0}^{k-1} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j - \sum s_{k-2}^3 s_i^2 s_{k-i+a} + \sum_{i=0}^{k} s_{k-1}^3 s_i^2 s_{k-i+a+1}.$$

$$= \sum_{j=0}^{k-1} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j + \sum s_i^2 s_{i-a}(-1)^{i-a+1} + \sum s_i^2 s_{i-a-1}(-1)^{i-a}.$$

The last two sums vanish by (21) so

$$\gamma_1 = \sum_{j=0}^{k-1} \sum_{i=0}^{j+1} s_j^3 s_i^2 s_{j-i+a+2}(-1)^j.$$

We need to attenuate the range of j. We accomplish this task thus –

$$\gamma_1 = \gamma + \sum s_j^5 s_{a+2}(-1)^j + \sum s_j^3 s_{j+1}^2 s_{a+3}(-1)^j.$$

Once again the last two sums vanish, this time because of (31) and (41). We may conclude that $\gamma_1 = \gamma$. Next we tackle δ_1. We have

$$\delta_1 = \sum_{j=-1}^{k-2} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j$$

so

$$\delta_1 = \sum_{j=0}^{k-1} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j - \sum_{i=0}^{k-1} s_{k-1}^3 s_i^2 s_{k-i+a}(-1)^{k-1}$$

$$= \sum_{j=0}^{k-1} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j + \sum s_i^2 s_{i-a}(-1)^{i-a+1}.$$

The last term vanishes by (21) again. Thus we have

$$\delta_1 = \sum_{j=0}^{k-1} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j.$$

We now shrink the range of i and so

$$\delta_1 = \delta - \sum s_j^5 s_{a+1}(-1)^j.$$

The last term vanishes by (31) so $\delta_1 = \delta$. Thus

$$\alpha = \beta_1 + \gamma_1 - 2\delta_1 = \beta + \gamma - 2\delta.$$

Now we can deduce that

$$\alpha = \sum_{i<j} s_j^3 s_i^2 (s_{j-i+a-1} + s_{j-i+a+2} - 2s_{j-i+a+1})(-1)^j.$$

The expression in brackets vanishes by the Fibonacci recurrence because

$$(s_{j-i+a-1} + s_{j-i+a+2} - 2s_{j-i+a+1}) = (s_{j-i+a-1} - s_{j-i+a+1}) + (s_{j-i+a+2} - s_{j-i+a+1})$$

$$= -s_{j-i+a} + s_{j-i+a} = 0.$$

Now we are done.

□

Lemma 3.23. For every integer a we have

$$\sum_{i<j} s_j^3 s_i^2 s_{j-i+a}(-1)^{j+1} = 0. \tag{71}$$

Proof.

Let

$$\alpha = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a}(-1)^{j+1}$$

then

$$\alpha = \sum_{i<j} (s_{j+1} - s_{j-1})^3 s_i^2 s_{j-i+a}(-1)^{j+1}$$

so

$$\alpha = \sum_{i<j} s_{j+1}^3 s_i^2 s_{j-i+a}(-1)^{j+1} - 3\sum_{i<j} s_{j+1}^2 s_{j-1} s_i^2 s_{j-i+a}(-1)^{j+1}$$

$$+3\sum_{i<j} s_{j+1} s_{j-1}^2 s_i^2 s_{j-i+a}(-1)^{j+1} - \sum_{i<j} s_{j-1}^3 s_i^2 s_{j-i+a}(-1)^{j+1}.$$

We now adjust ranges of summation. We have

$$\alpha = \sum_{j=1}^{k}\sum_{i=0}^{j-2} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j - 3\sum_{i<j}(s_j^2 + (-1)^j)s_{j+1}s_i^2 s_{j-i+a}(-1)^{j+1}$$

$$+3\sum_{i<j}(s_j^2 + (-1)^j)s_{j-1}s_i^2 s_{j-i+a}(-1)^{j+1} - \sum_{j=-1}^{k-2}\sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j. \qquad (*)$$

We examine the four sums in (*) separately. We have

$$\alpha = \beta - 3\gamma + 3\delta - \epsilon$$

in the obvious notation. We have

$$\beta = \sum_{j=1}^{k}\sum_{i=0}^{j-2} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j$$

so

$$\beta = \sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j$$

since $s_0 = 0$. Now adjust the range of i, so

$$\beta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j - \sum s_j^3 s_{j-1}^2 s_a(-1)^j.$$

The final term in the last equation vanishes by equation (33) so

$$\beta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j.$$

Next we approach ϵ. We have

$$\epsilon = \sum_{j=-1}^{k-2}\sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j$$

so

$$\epsilon = \sum_{j=0}^{k-1}\sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j - \sum s_{k-1}^3 s_i^2 s_{k-i+a}(-1)^{k-1}.$$

The final term is, up to sign,

$$\sum s_i^2 s_{i-a}(-1)^i$$

which vanishes by equation (21). Thus

$$\epsilon = \sum_{j=0}^{k-1} \sum_{i=0}^{j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j,$$

so adjusting the range of i we obtain

$$\epsilon = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j + \sum s_j^5 s_{a+1}(-1)^j.$$

The last sum vanishes by equation (31). It is now clear that

$$\beta - \epsilon = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a-1}(-1)^j - \sum_{i<j} s_j^3 s_i^2 s_{j-i+a+1}(-1)^j$$

so

$$\beta - \epsilon = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a}(-1)^{j+1} = \alpha.$$

We now approach γ and δ.

$$\gamma = \sum_{i<j} (s_j^2 + (-1)^j) s_{j+1} s_i^2 s_{j-i+a}(-1)^{j+1}$$

so

$$\gamma = \sum_{i<j} s_j^2 s_{j+1} s_i^2 s_{j-i+a}(-1)^{j+1} + \sum_{i<j} s_{j+1} s_i^2 s_{j-i+a}(-1).$$

Similarly

$$\delta = \sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i+a}(-1)^{j+1} + \sum_{i<j} s_{j-1} s_i^2 s_{j-i+a}(-1).$$

Thus

$$\gamma - \delta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a}(-1)^{j+1} - \sum_{i<j} s_j s_i^2 s_{j-i+a}.$$

The final term of the last equation vanishes by equation (60). Thus

$$\gamma - \delta = \sum_{i<j} s_j^3 s_i^2 s_{j-i+a}(-1)^{j+1} = \alpha.$$

From equation (*) we deduce that

$$\alpha = \beta - \epsilon - 3(\gamma - \delta)$$

so

$$\alpha = \alpha - 3\alpha = -2\alpha.$$

It follows that $3\alpha = 0$ and we are done.

$\square$

Lemma 3.24.

$$\sum_{i<j} s_{j+b} s_j s_{j-i+a} s_i^3 (-1)^{j+1}. \tag{72}$$

Proof.

We establish this by showing

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i^3 (-1)^{j+1} = 0 \tag{*}$$

and

$$\sum_{i<j} s_{j+1} s_j s_{j-i+a} s_i^3 (-1)^{j+1} = 0 \tag{**}$$

for all integers a and b. From now on, in the course of this proof we will omit to mention that in all equations involving a and b, the values of a and b are arbitrary integers.

The result follows from (*) and (**), the Fibonacci recurrence and finite induction. Recall equation (65) which asserts that

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i s_{i-1}^2 (-1)^{j+1} = 0.$$

Reverting to detailed notation, this asserts that

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

and changing a variable this means that

$$\sum_{j=0}^{k-1}\sum_{i=-1}^{j-2} s_j^2 s_{j-i+a-1} s_{i+1} s_i^2 (-1)^{j+1} = 0.$$

Now remove the edge effects from this last sum. We have

$$\sum_{j=0}^{k-1}\sum_{i=-1}^{j-2} s_j^2 s_{j-i+a-1} s_{i+1} s_i^2 (-1)^{j+1} = \sum_{i<j} s_j^2 s_{j-i+a-1} s_{i+1} s_i^2 (-1)^{j+1}$$

$$+\sum s_j^2 s_{j+a} s_0 s_{-1}^2 (-1)^{j+1} - \sum s_j^2 s_a s_j s_{j-1}^2 (-1)^{j+1}.$$

The final two sums vanish because $s_0 = 0$, and equation (33) applies (respectively). We may add 1 to a since it is arbitrary, and deduce that

$$\sum_{i<j} s_j^2 s_{j-i+a} s_{i+1} s_i^2 (-1)^{j+1} = 0. \tag{73}$$

Now recall equation (69) which asserts that

$$\sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i+a} (-1)^{j+1} = 0.$$

We use the $\sum_{all} = \sum_{i<j} + \sum_{j<i} + \sum_{i=j}$ trick. Now we have

$$\sum_{all} s_j^2 s_{j-1} s_i^2 s_{j-i+a} (-1)^{j+1} = \sum_{j=0}^{k-1} s_j^2 s_{j-1} (-1)^{j+1} \left(\sum_{i=0}^{k-1} s_i^2 s_{i-j-a} (-1)^{i-j-a+1}\right).$$

The inner sum vanishes by equation (21) so

$$\sum_{all} s_j^2 s_{j-1} s_i^2 s_{j-i+a} (-1)^{j+1} = 0.$$

Now consider the contribution when $i = j$. This is

$$\sum s_i^4 s_{i-1} s_a (-1)^{i+1}$$

which vanishes by equation (43). We may conclude that

$$\sum_{j<i} s_j^2 s_{j-1} s_i^2 s_{j-i+a} (-1)^{j+1} = 0.$$

Now change the rôles of i and j in this equation to obtain

$$\sum_{i<j} s_j^2 s_{i-j+a} s_i^2 s_{i-1} (-1)^{i+1} = 0$$

which equally well asserts that

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i^2 s_{i-1} (-1)^{j+1} = 0. \tag{74}$$

We have spun the term s_{i-j+a} to s_{j-i-a}, replaced a by $-a$, and multiplied by -1 if necessary.

Subtracting equation (74) from equation (73) we obtain equation (*). We now address equation (**) using our new found faith in equation (*). We know from equation (*) that

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i^3 (-1)^{j+1} = 0,$$

so we may change the variable j to deduce that

$$\sum_{j=-1}^{k-2} \sum_{i=0}^{j} s_{j+1}^2 s_{j-i+a+1} s_i^3 (-1)^j = 0.$$

Now the range of summation for j can be slipped up by 1 without damage, so

$$\sum_{j=0}^{k-1} \sum_{i=0}^{j} s_{j+1}^2 s_{j-i+a+1} s_i^3 (-1)^j = 0.$$

Now eliminate the edge effect. Our latest equation can be written

$$\sum_{i<j} s_{j+1}^2 s_{j-i+a+1} s_i^3 (-1)^j - \sum s_{j+1}^2 s_{a+1} s_j^3 (-1)^j = 0.$$

The final term vanishes by equation (41) so

$$\sum_{i<j} s_{j+1}^2 s_{j-i+a+1} s_i^3 (-1)^{j+1} = 0. \tag{75}$$

We have subtracted 1 from a and multiplied by -1.

Now repeat this last enterprise, this time changing the variable j in the opposite direction. We have

$$\sum_{i<j} s_j^2 s_{j-i+a} s_i^3 (-1)^{j+1} = 0,$$

so replacing j by $j-1$ we see that

$$\sum_{j=1}^{k} \sum_{i=0}^{j-2} s_{j-1}^2 s_{j-i+a-1} s_i^3 (-1)^j = 0.$$

Thus

$$\sum_{j=1}^{k} \sum_{i=0}^{j-1} s_{j-1}^2 s_{j-i+a-1} s_i^3 (-1)^j - \sum s_{j-1}^2 s_a s_{j-1}^3 (-1)^j = 0.$$

The final term vanishes by equation (31). Knocking 0 off the range of j is harmless since there are no legal values of i when $j = 0$, so we only have to worry about what happens when $j = k$. Thus

$$\sum_{i<j} s_{j-1}^2 s_{j-i+a-1} s_i^3 (-1)^j + \sum s_{k-1}^2 s_{k-i+a-1} s_i^3 = 0.$$

Now

$$\sum s_{k-1}^2 s_{k-i+a-1} s_i^3 = \sum s_{i-a+1} s_i^3 (-1)^{i+a}$$

which vanishes by equations (23) and (28), and a finite induction. We deduce that

$$\sum_{i<j} s_{j-1}^2 s_{j-i+a} s_i^3 (-1)^{j+1} = 0. \tag{76}$$

We have added 1 to a and multiplied by -1. Now

$$2 s_{j+1} s_j = -(s_{j+1} - s_j)^2 + s_{j+1}^2 + s_j^2 = s_{j+1}^2 + s_j^2 - s_{j-1}^2.$$

Thus adding equations (75) and (*), then subtracting equation (76) we obtain

$$2 \sum_{i<j} s_{j+1} s_j s_{j-i+a} s_i^3 (-1)^{j+1} = 0$$

and we are done.

□

Lemma 3.25.

$$\sum_{i<j<r} s_{r-j-1}s_js_i^2s_{j-i-1} = 0. \tag{77}$$

Proof.

We put

$$\alpha = \sum_{i<j<r} s_{r-j-1}s_js_i^2s_{j-i-1} = \sum_{i<j<r} s_{r-j}s_js_i^2s_{j-i-1} - \sum_{i<j<r} s_{r-j-2}s_js_i^2s_{j-i-1}.$$

Now adjust the ranges of summation, to obtain

$$\alpha = \sum_{r=1}^{k}\sum_{j=0}^{r-2}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1} - \sum_{r=-1}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1}. \tag{*}$$

We study these last two sums separately. Initially we address the first sum.

$$\sum_{r=1}^{k}\sum_{j=0}^{r-2}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1} = \sum_{r=0}^{k}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1}$$

by inserting vanishing terms. Now we must work a little harder.

$$\sum_{r=0}^{k}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1} = \sum_{i<j<r} s_{r-j-1}s_js_i^2s_{j-i-1} - \sum_{i<j} s_{k-j-1}s_js_i^2s_{j-i-1}.$$

The final term here is just

$$\sum_{i<j} s_js_{j+1}s_i^2s_{j-i-1}(-1)^j$$

which vanishes by (58). Thus the first sum in our equation (*) for α can be replaced by

$$\sum_{i<j<r} s_{r-j-1}s_js_i^2s_{j-i-1},$$

which happens to be α. Thus (*) becomes

$$\alpha = \alpha - \sum_{r=-1}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_js_i^2s_{j-i-1}. \tag{**}$$

Now for the remaining unsimplified term in (**). We have

$$\sum_{r=0}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_j s_i^2 s_{j-i-1} = \sum_{r=0}^{k-1}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_j s_i^2 s_{j-i-1} - \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_{k-j-2}s_j s_i^2 s_{j-i-1}.$$

Once again, the second term

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

vanishes, this time because of equation (59). Thus we have

$$\sum_{r=0}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_j s_i^2 s_{j-i-1} = \sum_{r=0}^{k-1}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_j s_i^2 s_{j-i-1}$$

$$= \sum_{i<j<r} s_{r-j-1}s_j s_i^2 s_{j-i-1} + \sum_{r=0}^{k-1}\sum_{i=0}^{r-1} s_{-1}s_r s_i^2 s_{r-i-1}.$$

The final term here is simply another way of writing

$$\sum_{i<j} s_{-1}s_j s_i^2 s_{j-i-1}$$

which vanishes by equation (60). Thus

$$\sum_{r=0}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_{r-j-1}s_j s_i^2 s_{j-i-1} = \sum_{i<j<r} s_{r-j-1}s_j s_i^2 s_{j-i-1} = \alpha.$$

Putting all the pieces together by substituting into (**), we obtain

$$\alpha = \alpha - \alpha = 0.$$

□

Lemma 3.26.

$$\sum_{i<j<r} s_r^2 s_{r-j-1}s_j s_{j-i-1}(-1)^{r+i} = 0. \tag{78}$$

Proof.

Let

$$\alpha = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i} = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i} (-1)^{r+i}$$

$$- \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-2} (-1)^{r+i}.$$

Now adjust the ranges of summation for i to obtain

$$\alpha = \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=-1}^{j-2} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1} - \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=1}^{j} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1}. \tag{$*$}$$

We consider the two sums in (*) separately. First we have

$$\sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=-1}^{j-2} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1} = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1}$$

$$+ \sum_{j<r} s_r^2 s_{r-j-1} s_j^2 (-1)^r - \sum_{j<r} 0.$$

The argument of the the third sum vanishes since $s_0 = 0$. The second expression is simply another way of writing

$$\sum_{i<j} s_j^2 s_i^2 s_{j-i-1} (-1)^j$$

which vanishes by equation (50). Thus (*) becomes

$$\alpha = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1} - \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=1}^{j} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1}. \tag{$**$}$$

We now tackle the second expression in (**). We have

$$\sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=1}^{j} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1} = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1}$$

$$- \sum_{j<r} s_r^2 s_{r-j-1} s_j s_{j-1} (-1)^{r+1} + \sum_{j<r} s_r^2 s_{r-j-1} s_j s_{-1} (-1)^{r+j+1}.$$

The second sum here is really just

$$\sum_{i<j} s_j^2 s_i s_{i-1} s_{j-i-1} (-1)^{j+1}$$

which vanishes by equation (62). The third sum is really

$$\sum_{i<j} s_j^2 s_{j-i-1} s_i (-1)^{i+j+1}$$

which vanishes by equation (61). Thus (**) becomes

$$\alpha = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1} - \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1} (-1)^{r+i+1}$$

$$= -\alpha + \alpha = 0,$$

and we are done.

□

Lemma 3.27.

$$\theta = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-1} (-1)^{r+1} = 0. \tag{79}$$

Proof.

Let

$$\alpha = \sum_{i<j<r} s_{r+1}^2 s_{r-j-1} s_j s_i^2 s_{j-i-1} (-1)^{r+1},$$

$$\beta = \sum_{i<j<r} s_{r-1}^2 s_{r-j-1} s_j s_i^2 s_{j-i-1} (-1)^{r+1},$$

and

$$\lambda = \sum_{i<j<r} s_{r-j-1} s_j s_i^2 s_{j-i-1}.$$

Recall from equation (46) that

$$3s_n^2 = s_{n+1}^2 + s_{n-1}^2 - 2(-1)^n \quad \forall n \in \mathbf{Z}$$

We deploy this, focusing on the variable r, to obtain

$$3\theta = \alpha + \beta + 2\lambda.$$

The equation (73) shows that $\lambda = 0$ so

$$3\theta = \alpha + \beta.$$

We now attempt to find a different linear relation between α and β. We have

$$\alpha = \sum_{r=1}^{k}\sum_{j=0}^{r-2}\sum_{i=0}^{j-1} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i-1}(-1)^r.$$

Sliding the range of r down by 1 is harmless since $s_0 = 0$. We have

$$\alpha = \sum_{i<j<r} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i-1}(-1)^r - \sum_{r=0}^{k-1}\sum_{i=0}^{r-2} s_r^2 s_{-1} s_{r-1} s_i^2 s_{r-i-2}(-1)^r.$$

The second sum is the edge effect, and we need to show it vanishes. We change the dummy variable r to j to render the appearance of the sum more familiar. We have

$$\sum_{j=0}^{k-1}\sum_{i=0}^{j-2} s_j^2 s_{j-1} s_i^2 s_{j-i-2}(-1)^j = \sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i-2}(-1)^j - \sum s_j^2 s_{j-1}^3 s_{-1}(-1)^j.$$

The first sum vanishes by (69) and the second because of equation (41). Thus

$$\alpha = \sum_{i<j<r} s_r^2 s_{r-j-2} s_j s_i^2 s_{r-i-1}(-1)^r. \tag{$*$}$$

We now address β in the same spirit. We have

$$\beta = \sum_{i<j<r} s_{r-1}^2 s_{r-j-1} s_j s_i^2 s_{j-i-1}(-1)^{r+1}$$

$$= \sum_{r=-1}^{k-2}\sum_{j=0}^{r}\sum_{i=0}^{j-1} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-1}(-1)^r.$$

When $j = r$ we get no contribution, so

$$\beta = \sum_{i<j<r} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-1}(-1)^r - \sum_{i<j} s_{k-1}^2 s_{k-1-j} s_j s_i^2 s_{j-i-1}(-1)^{k-1}.$$

The last term, up to sign, is just

$$\sum_{i<j} s_j s_{j+1} s_i^2 s_{j-i-1}(-1)^{j+1}$$

which vanishes by equation (59). Thus

$$\beta = \sum_{i<j<r} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-1}(-1)^r$$

Thus

$$\alpha - \beta = \sum_{i<j<r} s_r^2 (s_{r-j-2} - s_{r-j}) s_j s_i^2 s_{j-i-1}(-1)^r = \theta.$$

Putting this information together, we have

$$3\theta = \alpha + \beta \text{ and } \theta = \alpha - \beta.$$

We are nearly half way home. Put

$$\epsilon = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{i+1}^2 s_{j-i-1}(-1)^{r+1},$$

$$\gamma = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{i-1}^2 s_{j-i-1}(-1)^{r+1}$$

and

$$\zeta = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{j-i-1}(-1)^{r+i}.$$

Equation (46) forces

$$\theta = \epsilon + \gamma + 2\zeta.$$

However, ζ vanishes by equation (78) so $\theta = \epsilon + \gamma$. We address ϵ,

$$\epsilon = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{i+1}^2 s_{j-i-1}(-1)^{r+1} = \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=1}^{j} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i}(-1)^{r+1}$$

so

$$\epsilon = \sum_{i<j<r} s_r^2 s_{r-j-1} s_i s_j^2 s_{j-i}(-1)^{r+1}.$$

We now turn our attention to γ. We have

$$\gamma = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_{i-1}^2 s_{j-i-1} (-1)^{r+1} = \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=-1}^{j-2} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-2} (-1)^{r+1}.$$

This gives us

$$\gamma = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-2} (-1)^{r+1} + \sum_{j<r} s_r^2 s_{r-j-1} s_j s_{j-1} (-1)^{r+1}$$

$$- \sum_{j<r} s_r^2 s_{r-j-1} s_j s_{j-1}^2 (-1)^{r+1},$$

and changing variable names we see that

$$\gamma = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-2} (-1)^{r+1} + \sum_{i<j} s_j^2 s_i s_{i-1} s_{j-i-1} (-1)^{j+1}$$

$$- \sum_{i<j} s_j^2 s_{j-i-1} s_i s_{i-1}^2 (-1)^{j+1}.$$

The final two sums vanish by equations (62) and (65).

$$\gamma = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-2} (-1)^{r+1}. \qquad (**)$$

Notice that the expressions for ϵ and γ yield $\theta = \epsilon - \gamma$.

Summarizing we have

$$\alpha + \beta = 3\theta = \epsilon + \gamma$$

and

$$\alpha - \beta = \theta = \epsilon - \gamma.$$

Thus $\alpha = \epsilon = 2\theta$ and $\beta = \gamma = \theta$.

Now consider

$$\theta = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-1} (-1)^{r+1}.$$

We put

$$\mu = \sum_{i<j<r} s_r^2 s_{r-j-1} s_{j+1} s_i^2 s_{j-i-1} (-1)^{r+1}$$

and

$$\nu = \sum_{i<j<r} s_r^2 s_{r-j-1} s_{j-1} s_i^2 s_{j-i-1} (-1)^{r+1}$$

so

$$\theta = \mu - \nu.$$

Adjusting ranges of summation we see that

$$\mu = \sum_{r=0}^{k-1} \sum_{j=1}^{r} \sum_{i=0}^{j-2} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-2} (-1)^{r+1}$$

and

$$\nu = \sum_{r=0}^{k-1} \sum_{j=-1}^{r-2} \sum_{i=0}^{j} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i} (-1)^{r+1}.$$

Now

$$\mu = \sum_{r=0}^{k-1} \sum_{j=0}^{r-1} \sum_{i=0}^{j-2} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-2} (-1)^{r+1}$$

since we have added and removed vanishing terms. We now extend the range of i so

$$\mu = \sum_{i<j<r} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-2} (-1)^{r+1} + \sum_{j<r} s_r^2 s_{r-j} s_j s_{j-1}^2 s_{-1} (-1)^{r+1}.$$

Changing variable names we see that

$$\mu = \sum_{i<j<r} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-2} (-1)^{r+1} + \sum_{i<j} s_j^2 s_{j-i} s_i s_{i-1}^2 (-1)^{j+1}.$$

The final sum vanishes by (66) and so

$$\mu = \sum_{i<j<r} s_r^2 s_{r-j} s_j s_i^2 s_{j-i-2} (-1)^{r+1}.$$

We now attack ν. We have

$$\nu = \sum_{r=0}^{k-1} \sum_{j=-1}^{r-2} \sum_{i=0}^{j} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i} (-1)^{r+1} = \sum_{r=0}^{k-1} \sum_{j=0}^{r-2} \sum_{i=0}^{j} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i} (-1)^{r+1}$$

since there are no legal values of i less than -1. We increment the top range of j introducing the term

$$\sum_{r=0}^{k-1} \sum_{i=0}^{r-1} s_r^2 s_{-1} s_{r-1} s_i^2 s_{r-i-1} (-1)^{r+1} = \sum_{i<j} s_j^2 s_{j-1} s_i^2 s_{j-i-1} (-1)^{j+1}.$$

which vanishes by (69). We now contract the upper range of i by 1, which is inconsequential since $s_0 = 0$. Thus

$$\nu = \sum_{i<j<r} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i} (-1)^{r+1}.$$

The expressions for μ and ν differ in two places.

Notice that

$$s_{r-j} s_{j-i-2} - s_{r-j-2} s_{j-i} = (s_{r-j-1} + s_{r-j-2}) s_{j-i-2} - s_{r-j-2}(s_{j-i-1} + s_{j-i-2})$$

$$= s_{r-j-1} s_{j-i-2} - s_{r-j-2} s_{j-i-1}$$

so

$$\theta = \mu - \nu = \sum_{i<j<r} s_r^2 s_{r-j-1} s_j s_i^2 s_{j-i-2} (-1)^{r+1} - \sum_{i<j<r} s_r^2 s_{r-j-2} s_j s_i^2 s_{j-i-1} (-1)^{r+1}.$$

Now, examination of the equations in the proof marked (*) and (**) yields that

$$\theta = \gamma + \alpha.$$

However, we know that $\gamma = \theta$ and $\alpha = 2\theta$, so $\theta = 3\theta$. Thus $\theta = 0$ and we are done.

□

Corollary.

In the notation of the lemma, it follows that $\alpha = 0$ and so

$$\sum_{i<j<r} s_{r+1}^2 s_j s_i^2 s_{r-j-1} s_{j-i-1} (-1)^{r+1} = 0. \tag{80}$$

□

Lemma 3.28.

$$\tau = \sum_{i<j<r} s_r s_{r+1} s_{r-j-1} s_j s_i^2 s_{j-i-1} (-1)^{r+1} = 0. \tag{81}$$

Proof.

Put $\kappa = \kappa(i,j) = s_{r-j-1}s_js_i^2s_{j-i-1}(-1)^{r+1}$ so

$$\tau = \sum_{i<j<r} s_r s_{r+1}\kappa.$$

Now exploit the previous corollary (equation (80)) in conjunction with $s_r = s_{r+1} - s_{r-1}$ to obtain

$$\tau = \sum_{i<j<r} s_{r+1}^2\kappa - \sum_{i<j<r} s_{r+1}s_{r-1}\kappa.$$

The first term vanishes by (79), and $s_{r+1}s_{r-1} = s_r^2 + (-1)^r$ for each r by (22). Thus

$$\tau = -\sum_{i<j<r} s_r^2 s_{r-j-1}s_js_i^2s_{j-i-1}(-1)^{r+1} + \sum_{i<j<r} s_{r-j-1}s_js_i^2s_{j-i-1}.$$

The first term vanishes by equation (79) and the second term vanishes by equation (77). Thus $\tau = 0$ and we are done.

□

CHAPTER 4

A Proof of Theorem B

Consider a group $H = H^{\mathbf{Z}}$ with the following presentation:

$$H^{\mathbf{Z}} = < x, y, z, t, u \ : \ (y, x) = z, \ (z, x) = t, \ (t, x) = u \ >$$

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 this group is generated by just 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 $a, b, c, d, e \in \mathbf{Z}$. In fact, we may as well think of this group as being a rather strange group structure on $\mathbf{Z}^5$. 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. We shall use the somewhat sloppy term *integer valued rational polynomials* to describe such polynomials.

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

The relatively free two generator nilpotent groups of class 4 with exponent laws 2 and 3 are, respectively, $C_2 \times C_2$ 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 these primes $p > 3$ on which we shall focus.

We examine the details of the multiplication law of the groups $H^{\mathbf{Z}/p\mathbf{Z}}$. The element u is central, and the group $V =< y, z, t, u >$ 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 α (really x) given by the matrix

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

The group $H^{\mathbf{Z}/p\mathbf{Z}}$ is then realized as the semi-direct product of V with $< \alpha >$.

Notice that the matrix of α^n is

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

so for primes p other than 2 and 3 we have $\alpha^p = 1$. We wish to show that for primes $p > 3$, the group $H^{\mathbf{Z}/p\mathbf{Z}}$ has exponent p.

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

$$(\alpha^n \cdot v)^p = \alpha^{pn} \cdot v(1 + \alpha^n + \ldots + \alpha^{n(p-1)})$$

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

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

Let $m_n \in GF(p)[X]$ denote the minimum polynomial of α^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 $\alpha^n = 1$ so $\beta = 0$. Conversely, if m_n fails to divide $(1 - X)$ then it must divide $1 + X + X^2 + \ldots + X^{p-1}$ so $\beta = 0$.

Thus for primes p greater than 3 the group $H^{\mathbf{Z}/p\mathbf{Z}}$ has exponent p.

We now investigate the group law of $H^{\mathbf{Z}/p\mathbf{Z}}$ in some detail, reverting to the description of $H^{\mathbf{Z}/p\mathbf{Z}}$ as being $(\mathbf{Z}/p\mathbf{Z})^5$ with a peculiar group law. In the obvious notation

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

represents the group law. A straightforward induction argument yields the following:

$$a'' = a + a'$$

$$b'' = b + b'$$

$$c'' = c + c' + a'b$$

$$d'' = d + d' + a'c + \binom{a'}{2}b$$

$$e'' = e + e' + a'd + \binom{a'}{2}c + \binom{a'}{3}b$$

We now use these formulas to calculate the Fibonacci loop $\mathbf{l}(x, y, \ldots)$.

The first few terms are as follows (reduce modulo p of your choice):

$(1, 0, 0, 0, 0)$

$(0, 1, 0, 0, 0)$

$(1, 1, 0, 0, 0)$

$(1, 2, 1, 0, 0)$

$(2, 3, 2, 0, 0)$

$(3, 5, 7, 4, 1)$

$(5, 8, 18, 19, 10)$

$(8, 13, 50, 108, 151)$

$(13, 21, 132, 495, 1265)$

$(21, 34, 351, 2267, 10438)$

$(34, 55, 924, 9944, 77748)$

In particular, choosing the prime 7, we obtain the loop

$(1, 0, 0, 0, 0)$

$(0, 1, 0, 0, 0)$

$(1, 1, 0, 0, 0)$

$(1, 2, 1, 0, 0)$

$(2, 3, 2, 0, 0)$

$(3, 5, 0, 4, 1)$

$(5, 1, 4, 5, 3)$

$(1, 6, 1, 3, 4)$

$(6, 0, 6, 5, 5)$

$(0, 6, 1, 6, 1)$

$(6, 6, 0, 4, 6)$

$(6, 5, 2, 1, 3)$

$(5, 4, 3, 4, 6)$

$(4, 2, 2, 2, 0)$

$(2, 6, 0, 0, 0)$

$(6, 1, 6, 1, 6)$

$(1, 0, 0, 0, 0)$

$(0, 1, 0, 0, 0)$

of length 16.

Let the i^{th} entry of $\mathbf{l}$ be $(s_{i-1}, s_i, z_i, t_i, u_i)$.

From now on we will make the benign assumption that the prime p is not 2,3,5 or 11, so all the results of Chapter 3 may be freely used.

Lemma 4.1.

$$z_k = z_{k+1} = 0.$$

Proof.

Using the formula for multiplication, a simple induction shows that for positive n, we have

$$z_n = \sum_{i=0}^{n-1} s_{n-i-1} s_i^2.$$

Thus

$$z_k = \sum_{i=0}^{k} s_{k-i-1} s_i^2 = \sum s_{k-i-1} s_i^2.$$

By lemma 2.2 (equation (14)) we have

$$z_k = \sum s_{i+1} s_i^2 (-1)^i$$

lemma 3.3 (equation (20)) we have $z_k = 0$.

Similarly

$$z_{k+1} = \sum_{i=0}^{k} s_{k-i} s_i^2 = \sum s_{k-i} s_i^2 = \sum s_i^3 (-1)^{i+1}.$$

This last expression vanishes by lemma 3.2 (equation (16)) so $z_{k+1} = 0$ and we are done.

□

Lemma 4.2.

$$t_k = t_{k+1} = 0.$$

Proof.

We use a similar method as in the proof of lemma 4.1, but the argument is a little more complicated. Once again, we use induction to obtain a formula for t_n for positive n. It is

$$t_n = \sum_{j=0}^{n-1} s_{n-1-j}s_jz_j + \sum_{i=0}^{n-1} \binom{s_i}{2} s_i s_{n-i-1}.$$

In particular,

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

which, after cosmetic treatment, becomes

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

This expression vanishes by appeal to three chapter 3 equations, those numbered (50), (23) and (16) will do the trick.

We address the second problem

$$t_k = \sum_{j=0}^{k-1} s_{k-1-j}s_j \sum_{i=0}^{j-1} s_i^2 s_{j-i-1} + \sum \binom{s_i}{2} s_i s_{i+1}(-1)^i.$$

The second sum vanishes by equations (20) and (28), and so

$$t_k = \sum_{i<j} s_j s_{j+1} s_i^2 s_{j-i-1}(-1)^j.$$

This vanishes by equation (55) and so $t_k = 0$ and we are done.

$\square$

Lemma 4.3.

$$u_k = u_{k+1} = 0.$$

Proof.

The argument is in the same style as the previous two proofs. For positive n, an inductive argument shows that we have

$$u_n = \sum_{r=0}^{n-1} s_{n-r-1}s_r t_r + \sum_{j=0}^{n-1} s_{n-j-1}\binom{s_j}{2} z_j + \sum_{i=0}^{n-1} s_{n-i-1}\binom{s_i}{3} s_i,$$

which expands to

$$u_n = \sum_{r=0}^{n-1}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_{n-r-1}s_r s_{r-j-1}s_j s_{j-i-1}s_i^2 + \sum_{j=0}^{n-1}\sum_{i=0}^{j-1} s_{n-j-1}s_j\binom{s_i}{2} s_i s_{j-i-1}$$
$$+ \sum_{j=0}^{n-1}\sum_{i=0}^{j-1} s_{n-j-1}\binom{s_j}{2} s_{j-1-i}s_i^2 + \sum_{i=0}^{n-1} s_{n-i-1}\binom{s_i}{3} s_i.$$

$$u_{k+1} = \sum_{r=0}^{k}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_r^2 s_j s_i^2 s_{r-j-1}s_{j-i-1}(-1)^{r+1} + \sum_{j=0}^{k}\sum_{i=0}^{j-1} s_{k-j}s_j\binom{s_i}{2} s_i s_{j-i-1}$$
$$+ \sum_{j=0}^{k}\sum_{i=0}^{j-1} s_j\binom{s_j}{2} s_{j-i-1}s_i^2(-1)^{j+1} + \sum_{i=0}^{k} s_i^2\binom{s_i}{3}(-1)^{i+1}.$$

The last of the four sums is quite straightforward; it vanishes because of equations (16), (23) and (31). Thus we have

$$u_{k+1} = \sum_{r=0}^{k}\sum_{j=0}^{r-1}\sum_{i=0}^{j-1} s_r^2 s_j s_i^2 s_{r-j-1}s_{j-i-1}(-1)^{r+1} + \sum_{j=0}^{k}\sum_{i=0}^{j-1} s_j^2\binom{s_i}{2} s_i s_{j-i-1}(-1)^{j+1}$$
$$+ \sum_{j=0}^{k}\sum_{i=0}^{j-1} s_j\binom{s_j}{2} s_{j-i-1}s_i^2(-1)^{j+1}.$$

The first sum vanishes by equation (78), the second by equations (5) and (72), and the last by equations (50) and (70).

$$u_k = \sum_{i<j<r} s_{k-1-r}s_r s_{r-j-1}s_j s_{j-i-1}s_i^2 + \sum_{j=0}^{k-1}\sum_{i=0}^{j-1} s_{k-j-1}s_j\binom{s_i}{2} s_i s_{j-i-1}$$

$$+\sum_{i<j} s_{k-j-1}\binom{s_j}{2}s_{j-i-1}s_i^2+\sum s_{k-i-1}\binom{s_i}{3}s_i.$$

These four sums vanish for the following reasons. The first sum is really

$$\sum_{i<j<r} s_{r+1}s_r s_{r-j-1}s_j s_{j-i-1}s_i^2(-1)^r.$$

This vanishes by (81). The second sum is actually

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

which vanishes by equations (58) and (72).

The next sum is

$$\sum s_{j+1}\binom{s_j}{2}s_{j-i-1}s_i^2(-1)^j.$$

This vanishes by equations (72) and (58). Finally we consider the fourth sum which is

$$\sum s_{i+1}\binom{s_i}{3}s_i(-1)^i.$$

This vanishes by equations (44), (28) and (20).

□

Lemma 4.4. Let

$$H=<x,y,z,t,u\ :\ (y,x)=z,\ (z,x)=t,\ (t,x)=u\ >$$

where those pairs of generators with unspecified commutators are implicitly deemed to commute, and the p-th power of every group element is 1. The Fibonacci loop $(x,y,\ldots)$ in H has length $k=k(p)$.

Proof.

This is simply the upshot of lemmas 4.1,4.2 and 4.3.

□

We use implicit left bracket notation for commutators, so

$$(a,b,c) = ((a,b),c).$$

Recall the identity of Witt,

$$(a,b^{-1},c)^b(b,c^{-1},a)^c(c,a^{-1},b)^a = 1 \qquad (Witt)$$

and Philip Hall's formulas

$$(ab,c) = (a,c)^b(b,c) \text{ and } (a,bc) = (a,c)(a,b)^c \qquad (Hall).$$

These equations hold for all a, b, c elements of an arbitrary group G. See [Ha79].

Lemma 4.5. Suppose that $x, y \in G$, where G has nilpotency class 4. Let $\alpha = (x,y)$, then $(\alpha, x, y) = (\alpha, y, x)$.

Proof.

The Witt identity forces

$$(\alpha,x,y)^{x^{-1}}(x^{-1},y^{-1},\alpha)^y(y,\alpha^{-1},x^{-1})^\alpha = 1.$$

The commutators have weight 4 and so each one is central. Our equation can thus be written

$$(\alpha,x,y)(x^{-1},y^{-1},\alpha)(y,\alpha^{-1},x^{-1}) = 1.$$

Now

$$(x^{-1},y^{-1}) = (x,y)^{x^{-1}y^{-1}} = (x,y)z$$

where $z \in \gamma_3(G)$. Now using $Hall$ we see that

$$(x^{-1},y^{-1},\alpha) = ((x,y)z,\alpha) = ((x,y),\alpha)^z(z,\alpha).$$

Thus we obtain

$$(x^{-1},y^{-1},\alpha) = (\alpha,\alpha)^z(z,\alpha).$$

Now clearly $(\alpha, \alpha) = 1$, and since $z \in \gamma_3(G)$ and $\alpha \in \gamma_2(G)$ then $(z, \alpha) \in \gamma_5(G)$. However, G has class 4 so $\gamma_5(G)$ is trivial. Thus our main equation becomes

$$(\alpha, x, y)(y, \alpha^{-1}, x^{-1}) = 1.$$

Now we work on the final commutator in this expression. We have

$$(y, \alpha^{-1}, x^{-1}) = ((y, (y, x)), x^{-1}) = (((x, y), y)^{\alpha^{-1}}, x^{-1}).$$

Now

$$((x, y), y)^{\alpha^{-1}} = ((x, y), y)t$$

for some $t \in \gamma_4(G)$, and so

$$(((x, y), y)^{\alpha^{-1}}, x^{-1}) = (((x, y), y)t, x^{-1}) = (((x, y), y), x^{-1})^t(t, x^{-1}).$$

Now t is central so we may deduce that

$$(y, \alpha^{-1}, x^{-1}) = (\alpha, y, x^{-1}).$$

Now Hall's formulas force

$$(\alpha, y, x)(\alpha, y, x^{-1})^x = 1.$$

As usual we may omit the final conjugation by x since (α, y, x^{-1}) is central. Thus

$$(\alpha, y, x^{-1}) = (\alpha, y, x)^{-1}.$$

We deduce that

$$(\alpha, x, y) = (\alpha, y, x).$$

□

Theorem B.

If the Fibonacci Group $F(2, n)$ has the two generator relatively free group in the variety of exponent p groups of class 1 as a homomorphic image, then $F(2, n)$ has the two generator relatively free group G in the variety of exponent p groups of class 4 as a homomorphic image.

Proof.

The theorem holds for the primes 2,3,5 and 11 by direct computer aided calculation. In principle a diligent human could perform the task. We may therefore assume that our prime is not 2,3,5 or 11, so all the results of Chapter 3 and 4 may be freely used. Let T be the two generator relatively free class 4 group, and suppose that T is relatively free on x and y. We assume the reader has a passing familiarity with the theory of torsion-free finitely generated nilpotent groups, and refer him or her to $[Ba]$, $[Ha79]$ or $[Se]$ in the event that our presumption is unjustified.

The group T has Hirsch length 8, and a Mal'cev basis may be easily described. It is

$$x, y, (y,x), ((y,x),x), ((y,x),y), (((y,x),x),x),$$

$$(((y,x),y),x) = (((y,x),x),y), (((y,x),y),y).$$

The equality in this list is justified by Lemma 4.5, and we may regard $T = T^{\mathbf{Z}}$ as being the group structure on $\mathbf{Z}^8$ induced by this Mal'cev basis. See [Ha79].

Thanks to [MKS] page 349 exercise 9, and to Eamonn O'Brien for pointing out this reference, we know that $\overline{T} = T/T^p$ has order p^8. It follows that the Mal'cev basis we have described induces a central series in $\overline{T}$ where adjacent terms of the series have quotients which are cyclic of order p. We abusively denote the images of x and y in $\overline{T}$ by the same letters. The group $\overline{T}$ is relatively free, so we have a *Fibonacci automorphism* $\phi : \overline{T} \longrightarrow \overline{T}$ defined by $x\phi = y$ and $y\phi = xy$. Let $M = < (y,x,y) >^{\overline{T}}$, a normal subgroup of order p^3. A routine calculation shows that $M\phi \cap M \cap M\phi^{-1} = 1$.

The details we now explain – using vector notation to express group elements in $\overline{T}$ with respect to the image of the Mal'cev basis of T; we also freely use easy consequences of $(Hall)$ to be found on page 9 of $[Ha79]$. We have

$$M\phi = < (xy, y, xy) >^{\overline{T}} = < (y,x,x)(y,x,y)(y,x,y,x) >^{\overline{T}}$$

so

$$M\phi = \{(0,0,0,a,a,b,a+b+c,c) \mid a,b,c \in \mathbf{Z}/p\mathbf{Z}\}.$$

Also we find that

$$M =< (y,x,y) >^{\overline{T}} = \{(0,0,0,0,a,0,b,c) \mid a,b,c \in \mathbf{Z}/p\mathbf{Z}\}.$$

Finally

$$M\phi^{-1} =< (x, yx^{-1}, x) >^{\overline{T}} =< (y,x,x) >^{\overline{T}}$$

so

$$M\phi^{-1} = \{(0,0,0,a,0,b,c,0) \mid a,b,c \in \mathbf{Z}/p\mathbf{Z}\}.$$

Notice that

$$M \cap M\phi^{-1} =< (y,x,x,y) >^{\overline{T}} =< (y,x,y,x) >^{\overline{T}},$$

a cyclic group of order p. In vector notation this is

$$M \cap M\phi^{-1} = \{(0,0,0,0,0,0,a,0) \mid a \in \mathbf{Z}/p\mathbf{Z}\}.$$

Finally we deduce that

$$M\phi \cap M \cap M\phi^{-1} = 1$$

as required. Note that the appeal to [MKS] is only present to give us a way of showing that the intersection $M\phi \cap M \cap M\phi^{-1}$ is trivial.

We have natural maps $\overline{T} \longrightarrow \overline{T}/M\phi^i$ for each i, and these induce an embedding

$$\theta : \overline{T} \longrightarrow \overline{T}/M\phi \times \overline{T}/M \times \overline{T}/M\phi^{-1}.$$

Now $Im(\overline{T})$ is a subdirect product in $\overline{T}/M\phi \times \overline{T}/M \times \overline{T}/M\phi^{-1}$. Each group $\overline{T}/M\phi^i$ is a copy of the group H studied in this chapter.

When we compute the Fibonacci sequence in $\overline{T}$ the images in $\overline{T}/M\phi \times \overline{T}/M \times \overline{T}/M\phi^{-1}$ of the first four terms are as follows.

$$(x(M\phi), xM, x(M\phi^{-1})) \tag{a}$$

$$(y(M\phi), yM, y(M\phi^{-1})) \tag{b}$$

$$(xy(M\phi), xyM, xy(M\phi^{-1})) \tag{c}$$

$$(yxy(M\phi), yxyM, yxy(M\phi^{-1})) \tag{d}$$

In the second co-ordinate, we are simply calculating the Fibonacci loop which as been the central object of study of this chapter. This is not quite true of the first and third co-ordinates. The groups are the same (up to isomorphism), but the starting values are different. However, in these co-ordinates we are actually dealing with rotations of the series in the second co-ordinate. This is because $(xM)\phi = y(M\phi)$ and $(yM)\phi = xy(M\phi)$ yielding a rotation by 1 place in the loop of the first co-ordinate. Similarly ϕ^{-1} induces a rotation through 1 place in the opposite direction in the third co-ordinate. Thus the loop beginning $(x, y, \ldots)$ in $\overline{T}$ has length $k = k(p)$ as required.

$\square$

Observations:

The final ruse in the proof of Theorem B was used because we did not know that *all* loops in H had length dividing k, we only knew it for the specific loop with which worked throughout Chapter 3 and Chapter 4. Now, however, we are suddenly liberated. From Theorem B it follows that any loop in any class 4 p−group of exponent p has length dividing k, since any such group is a quotient of the relatively free group $\overline{T}$.

CHAPTER 5

On a Conjecture of D D Wall

Let n be a positive integer and suppose (s_i) denotes the standard Fibonacci bi-infinite sequence modulo n. Thus $s_0 = 0$ and $s_1 = 1$. The minimum period of this sequence we call Wall's number $k(n)$, or just k if the modulus is clear. Wall conjectured that for any prime p that $k(p) \neq k(p^2)$. He verified this conjecture for all primes less than 10^4. We have been unable to prove Wall's conjecture, but can announce that we have searched all primes less than 10^8 and Wall's conjecture holds in all cases. In this document, p will always denote an odd prime. Recall Lemma 2.3;

Lemma 5.1. (Wall) For all primes p,

$$\text{if } p \equiv 1 \text{ or } 4 \bmod 5 \text{ then } k(p) \text{ divides } p-1,$$

and

$$\text{if } p \equiv 2 \text{ or } 3 \bmod 5 \text{ then } k(p) \text{ divides } 2p+2.$$

□

For a substantial prime (of order say 10^8) a naive attempt to calculate $k(p)$, let alone $k(p^2)$ is extremely computationally expensive. By naive we mean that one simply calculates the Fibonacci sequence until it repeats. A better way to calculate $k(p)$ is to test divisors of $p-1$ or $2p+2$ (as appropriate). One can calculate a specified term of the Fibonacci sequence (mod p or p^2) relatively cheaply using the Fibonacci matrix equation

$$\begin{pmatrix} s_{i+1} & s_i \\ s_i & s_{i-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^i$$

in $GL(2, R)$ where R is $\mathbf{Z}/p\mathbf{Z}$ or $\mathbf{Z}/p^2\mathbf{Z}$ as appropriate. The method of repeated squaring is, of course, *de rigueur*. Even so, the explicit calculation of $k(p)$ has drawbacks, since multiple calculations are needed to determine the true value of $k(p)$.

The algorithm we used relies on another theorem of Wall, in our terms this is a corollary of Theorem A.

Theorem 5.2. (Wall) If $k(p) \neq k(p^2)$ then $k(p^2) = pk(p)$.

□

We introduce the notation $w(p) = p - 1$ or $w(p) = 2p + 2$ as $p \equiv 1, 4$ or $p \equiv 2, 3 \bmod 5$.

Proposition.

Let p be an odd prime which is not 5, and suppose that (s_i) denotes the Fibonacci sequence modulo p^2. We have $s_{w(p)} = 0$ and $s_{w(p)+1} = 1$ if and only if $k(p) = k(p^2)$.

Proof.

If $k(p^2) = k(p)$ then $k(p^2)$ divides $w(p)$. Conversely if $k(p^2) = pk(p)$ then $pk(p)$ cannot divide either $p - 1$ or $2p + 2$ unless p is 2.

□

This proposition can be readily turned an algorithm for testing Wall's conjecture. We ran this program for several weeks in the background on a variety of SUN 3, SUN 4 and Orion machines. Each machine examined a congruence class or congruence classes of primes modulo 30, depending on the machines relative speed. For almost all of the calculation, the arbitrary precision arithmetic feature of CAYLEY was used to perform the computation, though as an experiment J P ffitch coded the algorithm in LISP and eliminated a small part of the range (circa 5 million).

Note that the repeated squaring of the Fibonacci matrix can be performed more easily than squaring an arbitrary matrix, since all powers of the matrix are symmetric.

The code follows:

```
x = 1;
''Initialize the Fibonacci Matrix''
a11 = 1;
a12 = 1;
a22 = 0;

a = seq(a11,a12,a22);
'' Procedure for multiplying matrices of our special form mod q''
procedure mult(a,b,q;c);
        c11 = (a[1]*b[1] + a[2]*b[2]) mod q;
        c12 = (a[1]*b[2] + a[2]*b[3]) mod q;
        c22 = (a[2]*b[2] + a[3]*b[3]) mod q;
        c = seq(c11,c12,c22);
end;

''Procedure writes the integer q into a reverse binary sequence''
procedure decomp(q;bin);
        bin = empty;
        while q ne 0 do
                r = q mod 2;
                q = (q-r)/2;
                bin = append(bin,r);
        end;
end;

''Main Program''
zz = 50000000 mod 30;
for i = (50000000 - zz + x) to 100000000 by 30 do
        if i mod 1000000 lt 30 then
                print ' done up to ',i;
        end;
        if not prime(i) then
                loop;
```

```
        end;
        y = i^2;
        ''Split into two cases; determine the appropriate multiple
          of Walls Number.''
        if ((i mod 5) eq 1) or ((i mod 5) eq 4) then
                k = i-1;
        else k = 2*i+2;
        end;
        decomp(k;bin);
        u= seq(1,0,1);
        ustore = u;
        m = conseq(u,length(bin));
        m[1] = a;
        b = a;
        ''Compute the appropriate power of the Fibonacci matrix mod y
          using the method of repeated squaring.'';
        for j = 2 to length(m) do
                mult(b,b,y;b);
                m[j] = b;
        end;
        for j = 1 to length(m) do
                if bin[j] eq 1 then
                        mult(u,m[j],y;u);
                end;
        end;
        if u eq ustore then
                print '*****violator*****',i;
        end;
end;
print ' done ';
show time;
```

CHAPTER 6

More Results on Single Fourier Sums

Note that when we mention equation (3.22), we mean that we refer to equation 22 of chapter 3. We will sometimes recap the details of such an equation, in order to save the reader from having to flick backwards and forwards through the thesis.

Lemma 6.1. When p is prime and $p \neq 2$ we have

$$\sum s_i^6 = 0 \tag{1}$$

Proof.

From the Fibonacci relation $s_i = s_{i+1} - s_{i-1}$ for each integer i, and so

$$\sum s_i^6 = \sum (s_{i+1} - s_{i-1})^6.$$

We first exploit the equation,

$$\sum s_i^6 = \sum s_{i+1}^6 - 6\sum s_{i+1}^5 s_{i-1} + 15\sum s_{i+1}^4 s_{i-1}^2 - 20\sum s_{i+1}^3 s_{i-1}^3$$
$$+15\sum s_{i+1}^2 s_{i-1}^4 - 6\sum s_{i+1} s_{i-1}^5 + \sum s_{i-1}^6.$$

We replace $i+1$ by i and $i-1$ by i in the first and last terms on the right hand side, and obtain

$$\sum s_i^6 = 2\sum s_i^6 - 6\sum s_{i+1}s_{i-1}(s_{i+1}^4 + s_{i-1}^4)$$
$$+15\sum s_{i+1}^2 s_{i-1}^2(s_{i+1}^2 + s_{i-1}^2) - 20\sum s_{i+1}^3 s_{i-1}^3.$$

From equation (3.22), $s_{i+1}s_{i-1} = s_i^2 + (-1)^i$,

$$-\sum s_i^6 = -6\sum (s_i^2 + (-1)^i)(s_{i+1}^4 + s_{i-1}^4) + 15\sum (s_i^2 + (-1)^i)^2 (s_{i+1}^2 + s_{i-1}^2)$$
$$-20\sum (s_i^2 + (-1)^i)^3.$$

Some of terms vanish by equations (3.2), (3.23), (3.29) and (3.29) (again), which are $\sum s_i^2 = 0$, $\sum(-1)^i s_i^4 = 0$, $\sum(-1)^i s_i^2 s_{i+1}^2 = 0$, $\sum(-1)^i s_i^2 s_{i-1}^2 = 0$ and since k is even, $\sum(-1)^i = 0$,

$$19\sum s_i^6 = -6\sum s_i^2 s_{i+1}^4 - 6\sum s_i^2 s_{i-1}^4 + 15\sum s_i^4 s_{i+1}^2 + 15\sum s_i^4 s_{i-1}^2.$$

In the first and the second sums on the right side, replace i by $i-1$ and i by $i+1$, respectively, to obtain

$$19\sum s_i^6 = 9\sum s_i^2(s_{i-1}^4 + s_{i+1}^4).$$

By the equation (3.22), we deduce that

$$19\sum s_i^6 = 9\sum(s_{i+1}s_{i-1} + (-1)^{i-1})(s_{i-1}^4 + s_{i+1}^4).$$

Apply equation (3.23) to obtain $\sum s_i^4(-1)^i = 0$, and so

$$19\sum s_i^6 = 9\sum s_{i+1}s_{i-1}^5 + 9\sum s_{i+1}^5 s_{i-1}.$$

By Fibonacci recurrence relations $s_{i+1} = s_i + s_{i-1}$ and $s_{i-1} = s_{i+1} - s_i$,

$$19\sum s_i^6 = 9\sum(s_i + s_{i-1})s_{i-1}^5 + 9\sum s_{i+1}^5(s_{i+1} - s_i).$$

We obtain the equation

$$\sum s_i^6 = 9\sum s_i s_{i-1}^5 - 9\sum s_i s_{i+1}^5.$$

Replacing $i-1$ by i and $i+1$ and i in the first and the second terms on the right side, respectively, we deduce that

$$\sum s_i^6 = 9\sum s_{i+1}s_i^5 - 9\sum s_{i-1}s_i^5.$$

From the Fibonacci recurrence relation $s_{i+1} - s_{i-1} = s_i$, and the assumption that $p \neq 2$, the result follows.

□

Corollary.

$$\sum s_i s_{i-1}^5 = 0, \tag{2}$$

$$\sum s_i^2 s_{i-1}^4 = 0, \tag{3}$$

$$\sum s_i^3 s_{i-1}^3 = 0, \tag{4}$$

$$\sum s_{i+1} s_{i-1}^5 = 0, \tag{5}$$

$$\sum s_{i+1}^2 s_{i-1}^4 = 0 \tag{6}$$

and

$$\sum s_{i+1}^3 s_{i-1}^3 = 0 \tag{7}$$

Proof.

We will prove the equation (2). Proof of the other equations will be similar. From (1) and recurrence relation, $s_i = s_{i+1} - s_{i-1}$,

$$0 = \sum s_i^6 = \sum (s_{i+1} - s_{i-1}) s_i^5 = \sum s_{i+1} s_i^5 - \sum s_{i-1} s_i^5.$$

We change the range of last sum in these equalities

$$\sum s_{i+1} s_i^5 = -\sum s_{k-i-1} s_{k-i}^5 = -\sum s_{i-1} s_i^5.$$

We have

$$-2 \sum s_{i-1} s_i^5 = 0.$$

Replacing $i-1$ by i on the sum and we change the range of sums to obtain

$$-2 \sum s_i s_{i+1}^5 = 2 \sum s_{k-i} s_{k-i-1}^5 = 2 \sum s_i s_{i-1}^5 = 0.$$

So we find

$$\sum s_i s_{i-1}^5 = 0$$

unless $p = 2$.

Lemma 6.2.

$$\sum s_i^7 = 0 \tag{8}$$

and

$$\sum (-1)^{i+1} s_i^7 = 0 \tag{9}$$

unless $p = 11$ or 29.

Proof.

From the Fibonacci recurrence $s_i = s_{i+1} - s_{i-1}$, we may easily obtain that

$$\sum s_i^7 = \sum (s_{i+1} - s_{i-1})^7.$$

We exploit the equation,

$$\sum s_i^7 = \sum s_{i+1}^7 - 7\sum s_{i+1}^6 s_{i-1}$$

$$+21\sum s_{i+1}^5 s_{i-1}^2 - 35\sum s_{i+1}^4 s_{i-1}^3$$

$$+35\sum s_{i+1}^3 s_{i-1}^4 - 21\sum s_{i+1}^2 s_{i-1}^5$$

$$+7\sum s_{i+1} s_{i-1}^6 - \sum s_{i-1}^7.$$

Replacing $i+1$ by i and $i-1$ by i in the first and last term on the right side, respectively, these two terms vanish. So

$$\sum s_i^7 = 7\sum s_{i+1}s_{i-1}(s_{i-1}^5 - s_{i+1}^5)$$

$$+21\sum s_{i+1}^2 s_{i-1}^2 (s_{i+1}^3 - s_{i-1}^3) + 35\sum s_{i+1}^3 s_{i-1}^3 (s_{i-1} - s_{i+1}).$$

Now we deploy equation (3.22), $s_{i+1}s_{i-1} = s_i^2 + (-1)^i$, in the equation

$$\sum s_i^7 = 7\sum (s_i^2 + (-1)^i)(s_{i-1}^5 - s_{i+1}^5)$$

$$+21\sum(s_i^2+(-1)^i)^2(s_{i+1}^3-s_{i-1}^3)-35\sum(s_i^2+(-1)^i)^3 s_i).$$

Expanding we obtain,

$$\sum s_i^7 = 7\sum s_i^2(s_{i-1}^5 - s_{i+1}^5) + 7\sum(-1)^i(s_{i-1}^5 - s_{i+1}^5)$$

$$+21\sum s_i^4(s_{i+1}^3 - s_{i-1}^3) + 42\sum s_i^2(-1)^i(s_{i+1}^3 - s_{i-1}^3)$$

$$+21\sum(s_{i+1}^3 - s_{i-1}^3) - 35\sum s_i^7 - 105\sum s_i^5(-1)^i$$

$$-105\sum s_i^3 - 35\sum(-1)^{3i}s_i.$$

Replacing $i-1$ by i and $i+1$ by i where appropriate, we see that the second and and fifth terms vanish. The fourth and the last three sums vanish by equations (3.32), (3.33) and (3.31), (3.3) and (3.15). So our expression simplifies to

$$\sum s_i^7 = 7\sum s_i^2(s_{i-1}^5 - s_{i+1}^5) + 21\sum s_i^4(s_{i+1}^3 - s_{i-1}^3) - 35\sum s_i^7.$$

From the Fibonacci recurrence relations $s_{i+1} = s_i + s_{i-1}$ and $s_{i-1} = s_{i+1} - s_i$ we deduce that

$$36\sum s_i^7 = 7\sum s_i^2(s_{i-1}^5 - (s_i + s_{i-1})^5)$$

$$+21\sum s_i^4(s_{i+1}^3 - (s_{i+1} - s_i)^3).$$

We expand the equation to obtain

$$36\sum s_i^7 = -7\sum s_i^2(s_i^5 + 5s_i^4 s_{i-1} + 10s_i^2 s_{i-1}^2(s_i + s_{i-1}) + 5s_i s_{i-1}^4)$$

$$+21\sum s_i^4(3s_{i+1}s_i(s_{i+1} - s_i) + s_i^3).$$

$s_{i-1} = s_{i+1} - s_i$ and then equations (3.22), $s_i^2 + (-1)^i = s_{i+1}s_{i-1}$, we find

$$43\sum s_i^7 = -35\sum s_i^6 s_{i-1} - 70\sum s_i^6 s_{i-1} - 70\sum(-1)^i s_i^4 s_{i-1}$$

$$-35\sum s_i^3 s_{i-1}^4 + 84\sum s_i^7 + 63\sum(-1)^i s_i^5.$$

The third and seventh terms on the right side vanish by equations (3.31) and (3.43).

Thus we obtain

$$-41\sum s_i^7 = -105\sum s_i^6 s_{i-1} - 35\sum s_i^3 s_{i-1}^4.$$

Replacing s_{i-1} by $s_i - s_{i-2}$ and s_{i-1}^2 by $s_i s_{i-2} + (-1)^i$, in the equation, we obtain

$$-41\sum s_i^7 = -105\sum s_i^7 + 35\sum 3s_i^6 s_{i-2} - 35\sum s_i^5 s_{i-2}^2$$

$$-70\sum s_i^4 s_{i-2}(-1)^i - 35\sum s_i^3.$$

The last two terms vanish by (3.31), (3.43) and (3.3) in chapter 3.

Our equation simplifies to

$$64\sum s_i^7 = 35\sum s_i^5 s_{i-2}(3s_i - s_{i-2}).$$

Since $3s_i - s_{i-2} = s_{i+1} + s_i$ and $s_{i-2} = s_i - s_{i-1}$, we deduce that

$$64\sum s_i^7 = 35\sum s_i^5(s_i^2 + s_i(s_{i+1} - s_{i-1}) - s_{i+1}s_{i-1}).$$

We find that

$$64\sum s_i^7 = 35\sum s_i^7 - 35\sum(-1)^i s_i^5,$$

and the last term vanishes by (3.31), unless p=11. We are assuming that $p \neq 11$ so this is not a problem. Therefore,

$$29\sum s_i^7 = 0$$

and the result follows.

To prove the second part of the lemma is now easy. We have

$$\sum(-1)^i s_i^7 = \sum(-1)^{i+1}(-1)^i s_{k-i}^7 = -\sum s_i^7 = \sum s_i^7 = 0.$$

Thus

$$\sum s_i^7(-1)^i = 0.$$

□

Corollary.

$$\sum s_i s_{i-1}^6 = 0, \tag{10}$$

$$\sum s_i^2 s_{i-1}^5 = 0, \tag{11}$$

$$\sum s_i^3 s_{i-1}^4 = 0, \tag{12}$$

$$\sum s_{i+1} s_{i-1}^6 = 0, \tag{13}$$

$$\sum s_{i+1}^2 s_{i-1}^5 = 0, \tag{14}$$

$$\sum s_{i+1}^3 s_{i-1}^4 = 0, \tag{15}$$

and the corresponding alternating sums also vanish. This means that

$$\sum (-1)^i s_i s_{i-1}^6 = 0, \tag{10'}$$

$$\sum (-1)^i s_i^2 s_{i-1}^5 = 0, \tag{11'}$$

$$\sum (-1)^i s_i^3 s_{i-1}^4 = 0, \tag{12'}$$

$$\sum (-1)^i s_{i+1} s_{i-1}^6 = 0, \tag{13'}$$

$$\sum (-1)^i s_{i+1}^2 s_{i-1}^5 = 0 \tag{14'}$$

and

$$\sum (-1)^i s_{i+1}^3 s_{i-1}^4 = 0. \tag{15'}$$

The proof of this corollary is similar to those of lemmas 3.7-3.10.

Lemma 6.3.

$$\sum 1 = k, \tag{16}$$

$$\sum s_i^2 (-1)^i = -\frac{2}{5}k \tag{17}$$

and

$$\sum s_i s_{i-1} (-1)^i = \frac{1}{5}k, \tag{18}$$

where k is the Wall number for a prime p.

Proof.

The equation (16) is obvious.

Now we will show that the equations (17) and (18) are valid. From the Fibonacci recurrence relation $s_i = s_{i+1} - s_{i-1}$, we deduce that

$$\sum s_i^2(-1)^i = \sum (s_{i+1} - s_{i-1})^2(-1)^i.$$

We exploit the equation,

$$\sum s_i^2(-1)^i = \sum s_{i+1}^2(-1)^i - 2\sum s_{i+1}s_{i-1}(-1)^i + \sum s_{i-1}^2(-1)^i.$$

On the right side, replacing $i+1$ by i and $i-1$ by i in the first and the last term, respectively, to obtain

$$3\sum s_i^2(-1)^i = -2\sum s_{i+1}s_{i-1}(-1)^i. \tag{19}$$

From the known formula (3.22), $s_{i+1}s_{i-1} = s_i^2 + (-1)^i$, we obtain

$$3\sum s_i^2(-1)^i = -2\sum (s_i^2 + (-1)^i)(-1)^i,$$

so

$$5\sum s_i^2(-1)^i = -2\sum 1.$$

Since we have equation (16), the right side is equal to $-2k$. Thus the result follows.

Secondly we will show that

$$\sum s_i s_{i-1}(-1)^i = \frac{1}{5}k.$$

From (19) and Fibonacci recurrence we have

$$3\sum s_i^2(-1)^i = -2\sum (s_i + s_{i-1})s_{i-1}(-1)^i.$$

We know that

$$\sum s_{i-1}^2(-1)^i = -\sum s_i^2(-1)^i$$

and from (17), we obtain

$$\sum s_i s_{i-1}(-1)^i = \frac{1}{5}k,$$

and we are done.

$\square$

Corollary.

$$\sum s_{i+1}s_{i-1}(-1)^i = \frac{3}{5}k. \tag{20}$$

Lemma 6.4. The following equations are all valid.

$$\sum s_i^4 = \frac{6}{25}k, \tag{21}$$

$$\sum s_i^2 s_{i-1}^2 = -\frac{1}{25}k \tag{22}$$

and

$$\sum s_i s_{i-1}^3 = \frac{3}{25}k. \tag{23}$$

Proof.

Using formula (3.22), $s_i^2 = s_{i+1}s_{i-1} + (-1)^{i+1}$, we deduce that

$$\sum s_i^4 = \sum (s_{i+1}s_{i-1} + (-1)^{i+1})^2.$$

We exploit this equation, which yields

$$\sum s_i^4 = \sum s_{i+1}^2 s_{i-1}^2 + 2\sum s_{i+1}s_{i-1}(-1)^{i+1} + \sum 1.$$

By the Fibonacci recurrence and from (19) and (16), we deduce the equation,

$$\sum s_i^4 = \sum s_i^2 s_{i-1}^2 + 2\sum s_i s_{i-1}^3 + \sum s_{i-1}^4 - \frac{1}{5}k. \tag{24}$$

Replacing s_i by $s_{i+1} - s_{i-1}$ in the second term on the right hand side,

$$\sum s_i^4 = \sum s_i^2 s_{i-1}^2 + 2\sum s_{i+1}s_{i-1}^3 - 2\sum s_{i-1}^4 + \sum s_{i-1}^4 - \frac{1}{5}k.$$

Now we deploy equation (3.22) to obtain

$$\sum s_i^4 = 3\sum s_i^2 s_{i-1}^2 + 2\sum(-1)^i s_{i-1}^2 - \sum s_{i-1}^4 - \frac{1}{5}k.$$

Replacing $i-1$ by i in the second and third sums and then from (17), we obtain

$$2\sum s_i^4 - 3\sum s_i^2 s_{i-1}^2 = \frac{3}{5}k. \tag{25}$$

From the Fibonacci recurrence relation we have

$$\sum s_i^4 = \sum(s_{i-1} + s_{i-2})^4.$$

Expanding we obtain

$$\sum s_i^4 = \sum s_{i-1}^4 + 4\sum s_{i-1}^3 s_{i-2} + 6\sum s_{i-1}^2 s_{i-2}^2$$
$$+4\sum s_{i-1}s_{i-2}^3 + \sum s_{i-2}^4.$$

Replacing $i-1$ by i twice in the second and last sum and once in the rest of the terms on the right hand side, we have

$$\sum s_i^4 + 4\sum s_{i+1}^3 s_i + 6\sum s_i^2 s_{i-1}^2 + 4\sum s_i s_{i-1}^3 = 0.$$

Now

$$\sum s_{i+1}^3 s_i = \sum s_{k-i-1}^3(-1)^{3i} s_{k-i}(-1)^{i+1} = -\sum_{i=k}^{1} s_{i-1}^3 s_i,$$

and reversing the range of summation,

$$\sum s_{i+1}^3 s_i = -\sum s_{i-1}^3 s_i,$$

so we obtain

$$\sum s_i^4 + 6\sum s_i^2 s_{i-1}^2 = 0. \tag{26}$$

Now we have two linear equations (25) and (26). We solve these equations,

$$\sum s_i^2 s_{i-1}^2 = -\frac{1}{25}k$$

and

$$\sum s_i^4 = \frac{6}{25}k.$$

From equations (24), (21) and (22) (in this chapter),

$$\sum s_i s_{i-1}^3 = \frac{3}{25}k.$$

□

Corollary.

$$\sum s_{i+1}^2 s_{i-1}^2 = \frac{11}{25}k \tag{27}$$

and

$$\sum s_{i+1} s_{i-1}^3 = \frac{9}{25}k. \tag{28}$$

Lemma 6.5. The following equations are valid.

$$\sum s_i^6 (-1)^i = -\frac{4}{25}k, \tag{29}$$

$$\sum s_i s_{i-1}^5 (-1)^i = \frac{2}{25}k, \tag{30}$$

$$\sum s_i^2 s_{i-1}^4 (-1)^i = 0 \tag{31}$$

and

$$\sum s_i^3 s_{i-1}^3 (-1)^i = -\frac{1}{25}k. \tag{32}$$

Proof.

We use equation (3.22), $s_i^2 = s_{i+1}s_{i-1} + (-1)^{i+1}$, to deduce that

$$\sum s_i^6 (-1)^i = \sum (s_{i+1}s_{i-1} + (-1)^{i+1})^3 (-1)^i.$$

We exploit the right hand side,

$$\sum s_i^6(-1)^i = \sum s_{i+1}^3 s_{i-1}^3(-1)^i - 3\sum s_{i+1}^2 s_{i-1}^2$$

$$+3\sum s_{i+1}s_{i-1}(-1)^i - \sum 1.$$

Now $\sum s_{i+1}^2 s_{i-1}^2 = \frac{11}{25}k$, $\sum s_{i+1}s_{i-1}(-1)^i = \frac{3}{5}k$ and $\sum 1 = k$ by (27), (20) and (16), respectively. Replacing s_{i+1} by $s_i + s_{i-1}$ in the first term on the right hand side we obtain

$$2\sum s_i^6(-1)^i = \sum s_i^3 s_{i-1}^3(-1)^i + 3\sum s_i^2 s_{i-1}^4(-1)^i$$

$$+3\sum s_i s_{i-1}^5(-1)^i - \frac{13}{25}k. \tag{33}$$

We deploy equation (3.22) in the first sum and $s_i = s_{i+1} - s_{i-1}$ in the second and third terms on the right side, respectively, to deduce that

$$2\sum s_i^6(-1)^i = \sum(-1)^i s_i s_{i+1} s_{i-1}^4 - \sum s_i s_{i-1}^3 + 3\sum s_i^2 s_{i-1}^4(-1)^i$$

$$+3\sum s_{i+1}s_{i-1}^5(-1)^i - 3\sum s_{i-1}^6(-1)^i - \frac{13}{25}k.$$

Now we use (3.22) in the fourth term on the right side and then $\sum s_i s_{i-1}^3 = \frac{3}{25}k$ by (23) and $\sum s_{i-1}^4 = \frac{6}{25}k$ by (21) we obtain

$$\sum s_i^6(-1)^i + \sum s_i s_{i+1} s_{i-1}^4(-1)^i + 6\sum s_i^2 s_{i-1}^4(-1)^i = -\frac{2}{25}k. \tag{34}$$

Firstly, from the Fibonacci recurrence relation $s_i = s_{i+1} - s_{i-1}$ and then equation (3.22) we find the equation

$$\sum s_i^6(-1)^i + \sum s_i^4 s_{i-1}^2(-1)^i + 2\sum s_i^2 s_{i-1}^2 + \sum s_{i-1}^2(-1)^i$$

$$-\sum s_i^2 s_{i-1}^4(-1)^i - \sum s_{i-1}^4 + 6\sum s_i^2 s_{i-1}^4(-1)^i = -\frac{2}{25}k.$$

Replacing $i-1$ by i in fourth and sixth terms, from (22), (17) and (21) we write,

$$\sum s_i^6(-1)^i + \sum s_i^4 s_{i-1}^2(-1)^i - \frac{2}{25}k + \frac{2}{5}k - \frac{6}{25}k$$

$$+5\sum s_i^2 s_{i-1}^4(-1)^i = -\frac{2}{25}k.$$

In the second term, replace i by $i+1$ in the left hand side and then

$$\sum s_{i+1}^4 s_i^2 (-1)^{i+1} = \sum s_{k-i-1}^4 s_{k-i}^2 (-1)^{k-i-1} = -\sum_{i=k}^{1} s_{i-1}^4 s_i^2 (-1)^i.$$

Now reverse the direction of summation to find

$$\sum s_{i+1}^4 s_i^2 (-1)^{i+1} = \sum s_{i-1}^4 s_i^2 (-1)^{i-1}.$$

Thus we may conclude that

$$\sum s_i^6 (-1)^i + 4 \sum s_i^2 s_{i-1}^4 (-1)^i = -\frac{4}{25} k. \tag{35}$$

Secondly, from the Fibonacci recurrence relation $s_i = s_{i+1} - s_{i-1}$,

$$\sum s_i^6 (-1)^i = \sum (s_{i+1} - s_{i-1})^6 (-1)^i.$$

We exploit the equation,

$$\sum s_i^6 (-1)^i = \sum s_{i+1}^6 (-1)^i - 6 \sum s_{i+1}^5 s_{i-1} (-1)^i + 15 \sum s_{i+1}^4 s_{i-1}^2 (-1)^i$$

$$-20 \sum s_{i+1}^3 s_{i-1}^3 (1)^i + 15 \sum s_{i+1}^2 s_{i-1}^4 (-1)^i - 6 \sum s_{i+1} s_{i-1}^5 (-1)^i + \sum s_{i-1}^6 (-1)^i.$$

We replace $i+1$ by i and $i-1$ by i in the first and the last terms, respectively, and then we deploy the equation (3.22) to obtain

$$3 \sum s_i^6 (-1)^i = -6 \sum (s_i^2 + (-1)^i)(s_{i+1}^4 + s_{i-1}^4)(-1)^i$$

$$+15 \sum (s_i^2 + (-1)^i)^2 (s_{i+1}^2 + s_{i-1}^2)(-1)^i - 20 \sum (s_i^2 + (-1)^i)^3 (-1)^i.$$

We expand the equation,

$$3 \sum s_i^6 (-1)^i = -6 \sum s_i^2 s_{i+1}^4 (-1)^i - 6 \sum s_{i+1}^4 - 6 \sum s_i^2 s_{i-1}^4 (-1)^i$$

$$-6 \sum s_{i-1}^4 + 15 \sum s_{i+1}^2 s_i^4 (-1)^i + 30 \sum s_{i+1}^2 s_i^2 + 15 \sum s_{i+1}^2 (-1)^i$$

$$+15 \sum s_i^4 s_{i-1}^2 (-1)^i + 30 \sum s_i^2 s_{i-1}^2 + 15 \sum s_{i-1}^2 (-1)^i - 20 \sum s_i^6 (-1)^i$$

$$-60 \sum s_i^4 - 60 \sum s_i^2 (-1)^i - 20 \sum 1.$$

Now we reverse the direction of the following summations to obtain

$$\sum s_i^2 s_{i+1}^4 (-1)^i = \sum s_{k-i}^2 s_{k-i-1}^4 (-1)^{k-i} = \sum s_i^2 s_{i-1}^4 (-1)^i$$

and

$$\sum s_i^4 s_{i+1}^2 (-1)^i = \sum s_{k-i}^4 s_{k-i-1}^2 (-1)^{k-i} = \sum s_i^4 s_{i-1}^2 (-1)^i$$

and from (21), (17), (22) and (16), which are

$$\sum s_{i+1}^4 = \sum s_{i-1}^4 = \sum s_i^4 = \frac{6}{25} k,$$

$$\sum s_{i+1}^2 (-1)^i = \sum s_{i-1}^2 (-1)^i = -\sum s_i^2 (-1)^i = \frac{2}{5} k,$$

$$\sum s_i^2 s_{i+1}^2 = \sum s_{k-i}^2 s_{k-i-1}^2 = \sum s_i^2 s_{i-1}^2 = -\frac{1}{25} k,$$

$$\sum 1 = k,$$

we obtain the equation

$$23 \sum s_i^6 (-1)^i = -12 \sum s_i^2 s_{i-1}^4 (-1)^i - 72 \frac{6}{25} k + 30 \sum s_i^4 s_{i-1}^2 (-1)^i$$

$$-60 \frac{1}{25} k + 90 \frac{2}{5} k + 30 \sum s_i^4 s_{i-1}^2 (-1)^i - 20k.$$

Replace i by $i+1$ in the third and sixth term and then

$$\sum s_{i+1}^4 s_i^2 (-1)^{i+1} = \sum s_{k-i-1}^4 s_{k-i}^2 (-1)^{k-i-1} = -\sum_{i=k}^{1} s_{i-1}^4 s_i^2 (-1)^i,$$

Reversing the range of summation to obtain

$$\sum s_{i+1}^4 s_i^2 (-1)^{i+1} = \sum_{i=1}^{k} s_{i-1}^4 s_i^2 (-1)^{i-1} = \sum s_{i-1}^4 s_i^2 (-1)^{i-1}.$$

Finally, we obtain

$$23 \sum s_i^6 (-1)^i + 42 \sum s_i^2 s_{i-1}^4 (-1)^i = -\frac{92}{25} k. \tag{36}$$

From linear equations (35) and (36),

$$\sum s_i^6 (-1)^i = -\frac{4}{25} k,$$

$$\sum s_i^2 s_{i-1}^4 (-1)^i = 0$$

and from linear equations (33) and (34),

$$\sum s_i^3 s_{i-1}^3 (-1)^i = -\frac{1}{25}k$$

and

$$\sum s_i s_{i-1}^5 (-1)^i = \frac{2}{25}k$$

and we are done.

□

Corollary.

The following equations are valid.

$$\sum s_{i+1}^3 s_{i-1}^3 (-1)^i = \frac{9}{25}k, \tag{37}$$

$$\sum s_{i+1} s_{i-1}^5 (-1)^i = \frac{6}{25}k \tag{38}$$

and

$$\sum s_{i+1}^2 s_{i-1}^4 (-1)^i = \frac{8}{25}k. \tag{39}$$

Lemma 6.6.

$$\sum s_i^8 = \frac{14}{125}k, \tag{40}$$

$$\sum s_i^4 s_{i-1}^4 = -\frac{1}{125}k \tag{41}$$

and

$$\sum s_i^2 s_{i-1}^6 = \frac{1}{125}k. \tag{42}$$

Proof.

From the Fibonacci recurrence relation $s_i = s_{i+1} - s_{i-1}$,

$$\sum s_i^8 = \sum (s_{i+1} - s_{i-1})^8.$$

We exploit the equation,

$$\sum s_i^8 = \sum s_{i+1}^8 - 8\sum s_{i+1}^7 s_{i-1} + 28\sum s_{i+1}^6 s_{i-1}^2$$

$$-56\sum s_{i+1}^5 s_{i-1}^3 + 70\sum s_{i+1}^4 s_{i-1}^4 - 56\sum s_{i+1}^3 s_{i-1}^5$$

$$+28\sum s_{i+1}^2 s_{i-1}^6 - 8\sum s_{i+1} s_{i-1}^7 + \sum s_{i-1}^8.$$

Replacing i by $i+1$ and i by $i-1$ in the first and the last terms , respectively, on the right side to obtain

$$\sum s_i^8 = 2\sum s_i^8 - 8\sum s_{i+1}s_{i-1}(s_{i+1}^6 + s_{i-1}^6) + 28\sum s_{i+1}^2 s_{i-1}^2(s_{i+1}^4 + s_{i-1}^4)$$

$$-56\sum s_{i+1}^3 s_{i-1}^3(s_{i+1}^2 + s_{i-1}^2) + 70\sum s_{i+1}^4 s_{i-1}^4.$$

By equation (3.22), $s^2 + (-1)^i = s_{i+1}s_{i-1}$, we obtain

$$\sum s_i^8 - 8\sum s_i^2(s_{i+1}^6 + s_{i-1}^6) - 8\sum(-1)^i(s_{i+1}^6 + s_{i-1}^6)$$

$$+28\sum s_i^4(s_{i+1}^4 + s_{i-1}^4) + 56\sum(-1)^i s_i^2(s_{i+1}^4 + s_{i-1}^4) + 28\sum(s_{i+1}^4 + s_{i-1}^4)$$

$$-56\sum s_i^6(s_{i+1}^2 + s_{i-1}^2) - 168\sum s_i^4(-1)^i(s_{i+1}^2 + s_{i-1}^2) - 168\sum s_i^2(s_{i+1}^2 + s_{i-1}^2)$$

$$-56\sum(-1)^i(s_{i+1}^2 + s_{i-1}^2) + 70\sum s_i^8 + 280\sum s_i^6(-1)^i + 420\sum s_i^4$$

$$+280\sum s_i^2(-1)^i + 70\sum 1 = 0.$$

Since

$$\sum s_i^2 s_{i+1}^6 = \sum s_{k-i}^2 s_{k-i-1}^6 = \sum s_i^2 s_{i-1}^6,$$

$$\sum s_i^4 s_{i+1}^4 = \sum s_{k-i}^4 s_{k-i-1}^4 = \sum s_i^4 s_{i-1}^4,$$

$$\sum s_i^6 s_{i+1}^2 = \sum s_{k-i}^6 s_{k-i-1}^2 = \sum s_i^6 s_{i-1}^2,$$

$$\sum s_{i+1}^2 s_i^4(-1)^i = \sum s_{i-1}^2 s_i^4(-1)^i,$$

$$\sum s_i^2 s_{i+1}^4(-1)^i = \sum s_i^2 s_{i-1}^4(-1)^i,$$

and

$$\sum s_i^2 s_{i+1}^2 = \sum s_i^2 s_{i-1}^2,$$

we have

$$71\sum s_i^8 - 16\sum s_i^2 s_{i-1}^6 + 16\sum(-1)^i s_i^6 + 56\sum s_i^4 s_{i-1}^4$$

$$+112\sum(-1)^i s_i^2 s_{i-1}^4 + 56\sum s_i^4 - 112\sum s_i^6 s_{i-1}^2 - 336\sum(-1)^i s_i^4 s_{i-1}^2$$

$$-336\sum s_i^2 s_{i-1}^2 + 112\sum(-1)^i s_i^2 + 280\sum s_i^6(-1)^i + 420\sum s_i^4$$

$$+280\sum s_i^2(-1)^i + 70\sum 1 = 0.$$

Replacing i by $i+1$ in the second and the fifth terms on the left side,

$$\sum s_i^2 s_{i-1}^6 = \sum s_{i+1}^2 s_i^6,$$

$$\sum(-1)^i s_i^2 s_{i-1}^4 = -\sum(-1)^i s_{i+1}^2 s_i^4$$

and then reversing the range of sums,

$$\sum s_{i+1}^2 s_i^6 = \sum s_{i-1}^2 s_i^6,$$

$$\sum(-1)^i s_{i+1}^2 s_i^4 = \sum(-1)^i s_{i-1}^2 s_i^4.$$

The last sum is zero by (31).

We now have

$$71\sum s_i^8 + 56\sum s_i^4 s_{i-1}^4 - 128\sum s_i^6 s_{i-1}^2$$

$$+296\sum(-1)^i s_i^6 + 476\sum s_i^4 - 336\sum s_i^2 s_{i-1}^2$$

$$+392\sum(-1)^i s_i^2 + 70\sum 1 = 0.$$

From the equations (29), (21), (22),(17) and (16), we obtain the equation

$$71\sum s_i^8 + 56\sum s_i^4 s_{i-1}^4 - 128\sum s_i^6 s_{i-1}^2$$

$$-\frac{1184}{25}k + \frac{2826}{25}k + \frac{336}{25}k - \frac{784}{5}k + 70k = 0.$$

We find the linear equation,

$$71\sum s_i^8 + 56\sum s_i^4 s_{i-1}^4 - 128\sum s_i^6 s_{i-1}^2 - \frac{162}{25}k = 0.$$

On the right side, we know

$$\sum s_i^6 s_{i-1}^2 = \sum s_{i+1}^6 s_i^2.$$

Now we can play on the range of last sum,

$$\sum s_{i+1}^6 s_i^2 = \sum s_{k-i-1}^6 s_{k-i}^2 = \sum s_{i-1}^6 s_i^2.$$

So we find the first linear equation,

$$71 \sum s_i^8 + 56 \sum s_i^4 s_{i-1}^4 - 128 \sum s_i^2 s_{i-1}^6 - \frac{162}{25} k = 0. \tag{43}$$

Secondly, from the Fibonacci recurrence relation $s_i = s_{i-1} + s_{i-2}$ we obtain

$$\sum s_i^8 = \sum (s_{i-1} + s_{i-2})^8.$$

We expand the equation,

$$\sum s_i^8 = \sum s_{i-1}^8 + 8 \sum s_{i-1}^7 s_{i-2} + 28 \sum s_{i-1}^6 s_{i-2}^2$$

$$+56 \sum s_{i-1}^5 s_{i-2}^3 + 70 \sum s_{i-1}^4 s_{i-2}^4 + 56 \sum s_{i-1}^3 s_{i-2}^5$$

$$+28 \sum s_{i-1}^2 s_{i-2}^6 + 8 \sum s_{i-1} s_{i-2}^7 + \sum s_{i-2}^8.$$

In this equation, replace $i-1$ by i and $i-2$ by i in the first and the last sums, respectively, in rest of the other terms on the right side replace $i-1$ by i to obtain

$$\sum s_i^8 = 2 \sum s_i^8 + 8 \sum s_i^7 s_{i-1} + 28 \sum s_i^6 s_{i-1}^2$$

$$+56 \sum s_i^5 s_{i-1}^3 + 70 \sum s_i^4 s_{i-1}^4 + 56 \sum s_i^3 s_{i-1}^5$$

$$+28 \sum s_i^2 s_{i-1}^6 + 8 \sum s_i s_{i-1}^7.$$

On the right side, replacing $i-1$ by i in the second, third and fourth terms, we have

$$\sum s_i^8 = 2 \sum s_i^8 + 8 \sum s_{i+1}^7 s_i + 28 \sum s_{i+1}^6 s_i^2$$

$$+56 \sum s_{i+1}^5 s_i^3 + 70 \sum s_i^4 s_{i-1}^4 + 56 \sum s_i^3 s_{i-1}^5$$

$$+28\sum s_i^2 s_{i-1}^6 + 8\sum s_i s_{i-1}^7.$$

Since

$$\sum s_{i+1}^7 s_i = \sum s_{k-i-1}^7 s_{k-i} = -\sum s_{i-1}^7 s_i,$$

and

$$\sum s_{i+1}^5 s_i^3 = \sum s_{k-i-1}^5 s_{k-i}^3 = -\sum s_{i-1}^5 s_i^3.$$

We obtain the second linear equation,

$$\sum s_i^8 + 70\sum s_{i-1}^4 s_i^4 + 56\sum s_i^2 s_{i-1}^6 = 0. \tag{44}$$

By the formula (3.22), $s_i^2 = s_{i-1}s_{i+1} + (-1)^{i+1}$, so

$$\sum s_i^8 = \sum (s_{i+1}s_{i-1} + (-1)^{i+1})^4.$$

We exploit the equation

$$\sum s_i^8 = \sum s_{i+1}^4 s_{i-1}^4 + 4\sum s_{i+1}^3 s_{i-1}^3 (-1)^{i+1}$$

$$+6\sum s_{i+1}^2 s_{i-1}^2 + 4\sum s_{i+1}s_{i-1}(-1)^{i+1} + \sum 1.$$

From the equations (37), (27), (20) and (16), we obtain

$$\sum s_i^8 = \sum s_{i+1}^4 s_{i-1}^4 - \frac{36}{25}k + \frac{66}{25}k - \frac{12}{5}k + k.$$

From the Fibonacci recurrence relation $s_{i+1} = s_i + s_{i-1}$ we obtain

$$\sum s_i^8 = \sum (s_i + s_{i-1})^4 s_{i-1}^4 - \frac{5}{25}k.$$

We expand the equation to get

$$\sum s_i^8 = \sum s_i^4 s_{i-1}^4 + 4\sum s_i^3 s_{i-1}^5$$

$$+6\sum s_i^2 s_{i-1}^6 + 4\sum s_i s_{i-1}^7 + \sum s_{i-1}^8 - \frac{5}{25}k.$$

Replacing s_i^2 by $s_{i+1}s_{i-1}+(-1)^{i+1}$ and s_i by $s_{i+1}-s_{i-1}$ in the second term and replacing s_i by $s_{i+1}-s_{i-1}$ in the fourth term in the equation on the right side, to obtain

$$\sum s_i^8 = \sum s_i^4 s_{i-1}^4 + 4\sum s_{i+1}^2 s_{i-1}^6$$

$$-4\sum s_{i+1}s_{i-1}^7 - 4\sum(-1)^i s_{i+1}s_{i-1}^5 + 4\sum(-1)^i s_{i-1}^6 + 6\sum s_i^2 s_{i-1}^6$$

$$+4\sum s_{i+1}s_{i-1}^7 - 4\sum s_{i-1}^8 + \sum s_{i-1}^8 - \frac{5}{25}k.$$

Since $s_i^2+(-1)^i = s_{i+1}s_{i-1}$ and $\sum s_i^8 = \sum s_{i-1}^8$ we deduce that

$$4\sum s_i^8 = \sum s_i^4 s_{i-1}^4 + 4\sum(s_i^2+(-1)^i)^2 s_{i-1}^4$$

$$-4\sum(s_i^2+(-1)^i)s_{i-1}^6 - 4\sum(-1)^i(s_i^2+(-1)^i)s_{i-1}^4 + 4\sum(-1)^i s_{i-1}^6$$

$$+6\sum s_i^2 s_{i-1}^6 + 4\sum(s_i^2+(-1)^i)s_{i-1}^6 - \frac{5}{25}k.$$

Some of the terms vanish so our equation simplifies to

$$-4\sum s_i^8 + 5\sum s_i^4 s_{i-1}^4 + 6\sum s_i^2 s_{i-1}^6$$

$$+4\sum(-1)^i s_{i-1}^6 + 4\sum(-1)^i s_i^2 s_{i-1}^4 - \frac{5}{25}k = 0.$$

From the equations (31) and (29) we find that

$$-4\sum s_i^8 + 5\sum s_i^4 s_{i-1}^4 + 6\sum(-1)^i s_i^2 s_{i-1}^6$$

$$+\frac{16}{25}k + 0 - \frac{5}{25}k = 0.$$

Finally, we find a third linear equation

$$-4\sum s_i^8 + 5\sum s_i^4 s_{i-1}^4 + 6\sum(-1)^i s_i^2 s_{i-1}^6 + \frac{11}{25}k = 0. \tag{45}$$

From the linear equations (43), (44) and (45),

$$71\sum s_i^8 + 56\sum s_i^4 s_{i-1}^4 - 128\sum s_i^2 s_{i-1}^6 = \frac{162}{25}k,$$

$$\sum s_i^8 + 70\sum s_{i-1}^4 s_i^4 + 56\sum s_i^2 s_{i-1}^6 = 0,$$

$$-4\sum s_i^8 + 5\sum s_i^4 s_{i-1}^4 + 6\sum s_i^2 s_{i-1}^6 = -\frac{11}{25}k.$$

Therefore the results follow. We solved the equations by hand and on the computer.

□

Corollary.

The following equations are all valid.

$$\sum s_{i+1}^4 s_{i-1}^4 = \frac{39}{125}k, \tag{46}$$

$$\sum s_{i+1}^3 s_{i-1}^5 = \frac{36}{125}k, \tag{47}$$

$$\sum s_{i+1}^2 s_{i-1}^6 = \frac{29}{125}k, \tag{48}$$

$$\sum s_{i+1} s_{i-1}^7 = \frac{21}{125}k, \tag{49}$$

$$\sum s_i s_{i-1}^7 = \frac{7}{125}k \tag{50}$$

and

$$\sum s_i^3 s_{i-1}^5 = -\frac{2}{125}k. \tag{51}$$

Proof.

All of these equations can solve by using previous lemmas. Now we will prove equation (48). From (42) and recurrence relation, $s_i = s_{i+1} - s_{i-1}$,

$$\frac{1}{125}k = \sum s_i^2 s_{i-1}^6 = \sum (s_{i+1} - s_{i-1})^2 s_{i-1}^6.$$

We expand the equation

$$\sum s_{i+1}^2 s_{i-1}^6 - 2\sum s_{i+1} s_{i-1} s_{i-1}^6 + \sum s_{i-1}^8 = \frac{1}{125}k.$$

From (3.22), $s_{i+1}s_{i-1} = s_i^2 + (-1)^i$,

$$\sum s_{i+1}^2 s_{i-1}^6 - 2\sum (s_i^2 + (-1)^i) s_{i-1}^6 + \sum s_i^8 = \frac{1}{125}k.$$

By (40),

$$\sum s_{i+1}^2 s_{i-1}^6 - 2\sum s_i^2 s_{i-1}^6 + 2\sum (-1)^i s_i^6 + \frac{14}{125}k = \frac{1}{125}k.$$

From (42)and (29)

$$\sum s_{i+1}^2 s_{i-1}^6 - \frac{2}{125}k - \frac{8}{25}k + \frac{14}{125}k = \frac{1}{125}k.$$

Finally,

$$\sum s_{i+1}^2 s_{i-1}^6 = \frac{29}{125}k.$$

□

On the basis of computational experiments, we conjecture that the following results are true. Note that only powers of 5 occur in the denominators.

$$\sum (-1)^i s_i^{10} = -\frac{252}{3125}k,$$
$$\sum (-1)^i s_i^5 s_{i-1}^5 = \frac{11}{3125}k,$$
$$\sum (-1)^i s_i^4 s_{i-1}^6 = -\frac{18}{3125}k,$$
$$\sum (-1)^i s_i^3 s_{i-1}^7 = -\frac{21}{3125}k,$$
$$\sum (-1)^i s_i^2 s_{i-1}^8 = \frac{28}{3125}k,$$

and

$$\sum (-1)^i s_i s_{i-1}^9 = \frac{126}{3125}k.$$

$$\sum s_i^{12} = \frac{924}{15625}k,$$
$$\sum s_i^6 s_{i-1}^6 = \frac{41}{15625}k,$$

$$\sum s_i^5 s_{i-1}^7 = \frac{7}{15625}k,$$

$$\sum s_i^4 s_{i-1}^8 = -\frac{56}{15625}k,$$

$$\sum s_i^3 s_{i-1}^9 = -\frac{42}{15625}k,$$

$$\sum s_i^2 s_{i-1}^{10} = \frac{126}{15625}k$$

and

$$\sum s_i s_{i-1}^{11} = \frac{462}{15625}k.$$

$\square$

CHAPTER 7

General Recurrence Relations in the Group

Let a G be the free nilpotent group of class 2 and exponent p. We put $z = (y, x)$ as usual. Suppose that we have integers n and m and a recurrence relation in the group:

$$x_{i-2}^{n} * x_{i-1}^{m} = x_i \ \forall i \in Z.$$

We assume that p does not divide n, then we get a definition of two-step general standard Fibonacci sequence which will be $(0, 1, m, n + m^2, ...)$ in Z/pZ. If p were permitted to divide n, then the sequence would be ultimately periodic, but would never return to the consecutive pair $0, 1$. The length of the standard sequence is k which, as usual, we call the Wall number of the sequence.

Each element in the group G can be uniquely represented as $x^a y^b z^c$ where $a, b, c \in \mathbf{Z}/p\mathbf{Z}$. The group laws give us a law of composition of standard forms:

$$x^a y^b z^c \cdot x^{a'} y^{b'} z^{c'} = x^{a''} y^{b''} z^{c''},$$

where a'', b'' and c'' are given by the following explicit formulas.

We have $a'' = a + a'$, $b'' = b + b'$, and $c'' = c + c' + a'b$. We discussed these product laws in the chapter 3. In order to study this recurrence, we need a closed formula to describe how to take the next term of the sequence. Now we will investigate more general elements in the group. Let $(x^a y^b z^c)^n$ and $(x^{a'} y^{b'} z^{c'})^m$ be two elements in the group. The relevant formulas are

$$(x^a y^b z^c)^n (x^{a'} y^{b'} z^{c'})^m = x^{a''} y^{b''} z^{c''},$$

where

$$a'' = na + ma',$$

$$b'' = nb + mb'$$

and

$$c'' = nc + mc' + mna'b + \frac{(n-1)n}{2}ab + \frac{(m-1)m}{2}a'b'.$$

We use vector notation to calculate with the sequence. We put $(1,0,0) = (s_{-1}, r_0, t_0)$ which corresponds to x, and $(0,1,0) = (s_0, r_1, t_1)$ which corresponds to y. We obtain two sequences (r_i) and (t_i) via our recurrence. Notice that we have $s_i = nr_i$ for each integer i. The j th term of the third component of our sequence of vectors is

$$t_j = mn^2 \sum_{i=0}^{j-1} r_{j-i-1} r_i^2 + \binom{n}{2} n \sum_{i=0}^{j-1} r_{j-i-1} r_i r_{i-1} + \binom{m}{2} n \sum_{i=0}^{j-1} r_{j-i-1} r_i r_{i+1}.$$

Now we want to show that $t_k = 0$ and $t_{k+1} = 0$ when $p > 3$.

Theorem 7.1.

$$n^2 m \sum_{i=0}^{k-1} r_{k-i-1} r_i^2 + \binom{n}{2} n \sum_{i=0}^{k-1} r_{k-i-1} r_i r_{i-1} + \binom{m}{2} n \sum_{i=0}^{k-1} r_{k-i-1} r_i r_{i+1} = 0,$$

where $m, n \in \mathbf{Z}/p\mathbf{Z}$ $p > 2$ and $n \neq 0$. There are two other assumptions which will insert

(a) $n^2 - m^3 - n - 3mn \not\equiv 0 \bmod p$,

(b) $3m(m^2 + n) \not\equiv 0 \bmod p$.

Observation: Computational experiments indicate that it is likely that conditions (a) and (b) can be omitted. Work is in hand to attempt to prove that this is indeed the case.

Proof.

Let

$$\theta = n^2 m \sum r_{k-i-1} r_i^2 + \binom{n}{2} n \sum r_{k-i-1} r_i r_{i-1} + \binom{m}{2} n \sum r_{k-i-1} r_i r_{i+1}.$$

Since $r_{i+1} = mr_i + nr_{i-1}$, we can recast the last sum to obtain

$$\theta = \left(n^2 m + \binom{m}{2} nm\right) \sum r_{k-i-1} r_i^2 + \left(\binom{n}{2} n + \binom{m}{2} n^2\right) \sum r_{k-i-1} r_i r_{i-1}.$$

We will prove that $\theta = 0$. We separate this sum to the two parts,

$$\theta_1 = (n^2 m + \binom{m}{2} nm) \sum r_{k-i-1} r_i^2$$

and

$$\theta_2 = ((\binom{n}{2}) n + \binom{m}{2} n^2) \sum r_{k-i-1} r_i r_{i-1}.$$

We can pull out factors without difficulty. We put $l_1 = n^2 m + \binom{m}{2} nm$ and $l_2 = \binom{n}{2} n + \binom{m}{2} n^2$ and then set

$$\phi_1 = \sum r_{k-i-1} r_i^2$$

and

$$\phi_2 = \sum r_{k-i-1} r_i r_{i-1}.$$

Now we have $\theta_1 = l_1 \phi_1$ and $\theta_2 = l_2 \phi_2$. We will show that $\phi_1 = 0$ and $\phi_2 = 0$.

Firstly, we will prove that

$$\phi_2 = \sum r_{k-i-1} r_i r_{i-1} = \sum r_{-(i+1)} r_i r_{i-1} = 0.$$

Now we show that

$$r_{-i} = (-1)^{i+1} (\frac{1}{n})^i r_i.$$

If α and β are the roots of $x^2 - mx - n = 0$, then $\alpha\beta = -n$ and $\alpha + \beta = m$. From the *Binet* formula, $r_i = \frac{\alpha^i - \beta^i}{\alpha - \beta}$ and $r_{-i} = \frac{\alpha^{-i} - \beta^{-i}}{\alpha - \beta}$. When we multiply r_{-i} by $(\alpha\beta)^i$ we see that

$$r_{-i} = (-1)^{i+1} (\frac{1}{n})^i r_i \tag{1}$$

and also we have

$$r_{i+1} r_{i-1} = r_i^2 - (-n)^{i-1}. \tag{2}$$

This formula was known to Somer[So]. Since $r_{-(i+1)} = (-1)^i (\frac{1}{n})^{i+1} r_{i+1}$, and equation (2) holds, we obtain

$$\sum r_{-(i+1)} r_i r_{i-1} = \sum (-1)^i (\frac{1}{n})^{i+1} r_i^3 + \frac{1}{n^2} \sum r_i.$$

We will prove that $\sum r_i = 0$. Since our recurrence relation is $r_i = mr_{i-1} + nr_{i-2}$ we deduce that

$$\sum r_i = m\sum r_{i-1} + n\sum r_{i-2}.$$

Substitute $i-1$ by i in the first sum and $i-2$ by i in the second sum on the right side to yield

$$(m+n-1)\sum r_i = 0. \tag{3}$$

$\sum r_i = 0$ unless $m+n-1$ is congruent to 0 modulo p. If we show

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = 0,$$

then we will be on the half way through the proof. From the recurrence relation,

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = \sum(-1)^i(\frac{1}{n})^{i+1}(mr_{i-1}+nr_{i-2})^3.$$

We expand this equation to obtain

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = m^3\sum(-1)^i(\frac{1}{n})^{i+1}r_{i-1}^3 + 3m^2n\sum(-1)^i(\frac{1}{n})^{i+1}r_{i-1}^2r_{i-2}$$
$$+3mn^2\sum(-1)^i(\frac{1}{n})^{i+1}r_{i-1}r_{i-2}^2 + n^3\sum(-1)^i(\frac{1}{n})^{i+1}r_{i-2}^3.$$

Replacing $i-1$ by i in the first, second and third sums, and $i-2$ by i in the last sum on the right side, we obtain

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = m^3\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_i^3 + 3m^2n\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_i^2r_{i-1}$$
$$+3mn^2\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_ir_{i-1}^2 + n^3\sum(-1)^{i+2}(\frac{1}{n})^{i+3}r_i^3. \tag{4}$$

Now we have

$$(n-\frac{m^3}{n}-1)\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 + 3mn\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_ir_{i-1}(mr_i+nr_{i-1}) = 0.$$

Since $mr_i + nr_i = r_{i+1}$ and

$$r_{i+1}r_{i-1} = r_i^2 - (-n)^{i-1} = r_i^2 + (-1)^i(n)^{i-1},$$

we obtain

$$(n - \frac{m^3}{n} - 1)\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 - 3m\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3$$
$$-3m\sum\frac{1}{n^2}r_i = 0$$

The last sum is zero by (3). Then we have

$$(n - \frac{m^3}{n} - 1 - 3m)\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = 0. \tag{5}$$

When we multiply (5) by n we see that

$$(n^2 - m^3 - n - 3mn)\sum(-1)^{i+1}(\frac{1}{n})^i r_i^3 = 0.$$

Finally, we have

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = 0. \tag{6}$$

unless $n^2 - m^3 - n - 3mn$ is congruent to 0 modulo p.

We deduce that $\phi_2 = 0$. Hence we have done the first part of the proof.

Now we will try to prove that the other part of θ is equal to 0. By (1), we can write

$$\phi_1 = \sum(-1)^i(\frac{1}{n})^{i+1}r_{i+1}r_i^2.$$

By equation (4) we have

$$(n^2 - m^3 - n)\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 + 3m^2n^2\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_i^2 r_{i-1}$$
$$+3mn^3\sum(-1)^{i+1}(\frac{1}{n})^{i+2}r_i r_{i-1}^2 = 0.$$

From (6), we have our first linear equation

$$3m^2n\sum(-1)^i(\frac{1}{n})^{i+1}r_i^2 r_{i-1} + 3mn^2\sum(-1)^i(\frac{1}{n})^{i+1}r_i r_{i-1}^2 = 0. \tag{7}$$

From the recurrence relation, $nr_i = r_{i+2} - mr_{i+1}$ and (6) we get

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^3 = \frac{1}{n^3}\sum(-1)^i(\frac{1}{n})^{i+1}(r_{i+2} - mr_{i+1})^3 = 0.$$

We exploit this equation to obtain

$$\frac{1}{n^3}\sum(-1)^i(\frac{1}{n})^{i+1}r_{i+2}^3 - 3\frac{m}{n^3}\sum(-1)^i(\frac{1}{n})^{i+1}r_{i+2}^2 r_{i+1}$$
$$+3\frac{m^2}{n^3}\sum(-1)^i(\frac{1}{n})^{i+1}r_{i+2}r_{i+1}^2 - \frac{m^3}{n^3}\sum(-1)^i(\frac{1}{n})^{i+1}r_{i+1}^3 = 0.$$

Replacing $i+2$ by i in the first, second and third and $i+1$ by i in the last sum on the left side we see that

$$\frac{1}{n^3}\sum(-1)^{i-2}(\frac{1}{n})^{i-1}r_i^3 - 3\frac{m}{n^3}\sum(-1)^{i-2}(\frac{1}{n})^{i-1}r_i^2 r_{i-1}$$
$$+3\frac{m^2}{n^3}\sum(-1)^{i-2}(\frac{1}{n})^{i-1}r_i r_{i-1}^2 - \frac{m^3}{n^3}\sum(-1)^{i-1}(\frac{1}{n})^{i}r_i^3 = 0$$

The first and last sums vanish by (6). We multiply the equation by n to obtain a second linear equation

$$-3m\sum(-1)^i(\frac{1}{n})^{i+1}r_i^2 r_{i-1} + 3m^2\sum(-1)^i(\frac{1}{n})^{i+1}r_i r_{i-1}^2 = 0. \qquad (8)$$

From the linear equations (7) and (8),

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i^2 r_{i-1} = 0, \qquad (9)$$

$$\sum(-1)^i(\frac{1}{n})^{i+1}r_i r_{i-1}^2 = 0 \qquad (10)$$

unless $3mn(m^2+n)$ is congruent to 0 modulo p. Replacing $i-1$ by i in (10),

$$3m(m^2+n)\sum(-1)^i(\frac{1}{n})^{i+1}r_{i+1}r_i^2 = 0. \qquad (11)$$

So we have finished the second part of the proof.

Therefore we have $\theta = 0$.

□

This result has an obvious interpretation in terms of quotients of groups with presentations similar to those of Fibonacci groups which is:

$$F(2,r,m,n) =< x_1, x_2, \cdots, x_r : x_1^n x_2^m x_3^{-1}, x_2^n x_3^m x_4^{-1}, \cdots, x_{r-1}^n x_r^m x_1^{-1}, x_r x_1^m x_2^{-1} > .$$

Conclusion

In Chapter two, we reproved the theorems of Wall and Vinson concerning the lengths and shapes of Fibonacci sequences modulo primes. We know that there exist Fibonacci sequences in which no entries is 0 when $p \equiv 1$ or 4 mod 5. Thus non-trivial short loops of C_p can only exist when a golden ratio occurs in $GF(p)$. The polynomial $x^2 - x - 1$ has coincident roots in $GF(5)$.

Definition: Let **f** be a loop. If there is no zero in **f**, then the loop is called a golden loop.

For example, the golden ratios are 4 and 8 when $p = 11$. The common ratios of the golden loops are 4 and 8.

Wall proved that if $k(p^2) \neq k(p)$, then $k(p^n) = p^{n-1}k(p)$ for all $n \geq 2$. Wall conjectured that if p is a prime, then $k(p^2) \neq k(p)$. We exhibited theorem A for p-groups. The statement of the theorem A is:

If G is a p-group for some prime p, and that G has exponent p central length n, then if any two elements of G are used to initiate a Fibonacci sequence in G, then that sequence must have minimum period dividing kp^{n-1} where k is the minimum period of the ordinary Fibonacci sequence modulo p.

We gave the computer-proved announcement C which is:

Any Fibonacci sequence constructed by starting off with two elements from the restricted Burnside group R(2,5) must have minimum period dividing 20. This is the least number with this property. Indeed, the number 20 is also the minimum period of the standard sequence in $C_5 \times C_5$.

In chapter 3 we proved that many single, double and triple Fourier sums manufactured from the standard two-step Fibonacci sequence vanish. For example, $\sum(-1)^i s_i = 0$, $\sum s_i = 0$, $\sum s_i^2 = 0$, $\sum s_i^3 = 0$, $\sum(-1)^i s_i^3 = 0$, $\sum(-1)^i s_i^4 = 0$, $\sum s_i^5 = 0$ and $\sum(-1)^i s_i^5 = 0$. The last two sums do not vanish modulo 11. We conjectured that $\sum(-1)^i s_i^q = 0$ and $\sum s_i^q = 0$

except for finitely many primes p (where q is a fixed prime). We also conjecture that these finitely many primes are congruent to 1 or 4 modulo 5. Example of double and triple Fourier sums are $\sum_{i<j}(-1)^{j+1}s_j^2 s_i^2 s_{j-i-1} = 0$ and $\sum_{i<j<r}(-1)^{r+1}s_r^2 s_j s_i^2 s_{r-j-1}s_{j-i-1} = 0$. We proved many formulas concerning the Fibonacci numbers, e.g. $6s_i^2 s_{i-1} = s_{i+1}^3 - s_{i-2}^3 - 2s_{i-1}^3$ for all integers i, but we suspect these formulas are known to the Fibonacci community.

In chapter 4, we proved some commutator results for groups with two generators and nilpotency class 4, and we proved theorem B which is:

If the Fibonacci Group $F(2,n)$ has the two generator relatively free group in the variety of exponent p groups of class 1 as homomorphic image, then $F(2,n)$ has the two generator relatively free group G in the variety of exponent p groups of class 4 as homomorphic image.

Theorem B does not appear to extend to class 5, since computational experiments indicate that the Wall number goes up. Thus $k(p)$ should be replaced by $pk(p)$ for class greater than 5. We have data for primes less than 100.

In chapter 5 is Announcement D. We checked the Wall conjecture which is: If p is an odd prime, then $k(p^2) \neq k(p)$. We report on an algorithm and verified that $k(p^2) = k(p)$ for primes less than 10^8. Wall's conjecture is still open.

In chapter 6, we proved more results on Fourier single sums. Sums and alternating sums of seventh powers of elements of Fibonacci sequences are zero except for finitely many primes (which are 11 and 29). If the power of elements in a sum is even then $\sum s_i^2 = 0$, $\sum(-1)^i s_i^4 = 0$, which are proved in chapter 3; $\sum s_i^6 = 0$, and $\sum(-1)^i s_i^2 = -\frac{2}{5}k$, $\sum s_i^4 = \frac{6}{25}k$, $\sum(-1)^i s_i^6 = -\frac{4}{25}k$, $\sum s_i^8 = \frac{14}{125}k$. We have conjectures which are: if $n = 4l+2$, where $l = 0, 1, \cdots$, then $\sum(-1)^i s_i^n$ depends only on k, and powers of 5 occur in the denominators. If $n = 4l$, where $l = 0, 1, \cdots$, then $\sum s_i^n$ depends only on k, and only powers of 5 occur in the denominators. For example,

$$\sum(-1)^i s_i^{10} = -\frac{252}{3125}k,$$

$$\sum(-1)^i s_i^5 s_{i-1}^5 = \frac{11}{3125}k,$$

$$\sum(-1)^i s_i^4 s_{i-1}^6 = -\frac{18}{3125}k,$$

$$\sum(-1)^i s_i^3 s_{i-1}^7 = -\frac{21}{3125}k,$$

$$\sum(-1)^i s_i^2 s_{i-1}^8 = \frac{28}{3125}k,$$

and

$$\sum(-1)^i s_i s_{i-1}^9 = \frac{126}{3125}k.$$

Moreover,

$$\sum s_i^{12} = \frac{924}{15625}k,$$

$$\sum s_i^6 s_{i-1}^6 = \frac{41}{15625}k,$$

$$\sum s_i^5 s_{i-1}^7 = \frac{7}{15625}k,$$

$$\sum s_i^4 s_{i-1}^8 = -\frac{56}{15625}k,$$

$$\sum s_i^3 s_{i-1}^9 = -\frac{42}{15625}k,$$

$$\sum s_i^2 s_{i-1}^{10} = \frac{126}{15625}k$$

and

$$\sum s_i s_{i-1}^{11} = \frac{462}{15625}k.$$

Otherwise the sum is equal to zero (except, we conjecture, for finitely many primes).

In chapter 7, we proved that Fourier sums associated with more general recurrence relations in a group on 2 generators with nilpotency class are equal to zero.

Experimentally, the technical conditions:

(a) $n^2 - m^3 - n - 3mn \not\equiv 0 \bmod p$,

(b) $3m(m^2 + n) \not\equiv 0 \bmod p$.

(a) and (b) in theorem 7.1 can be omitted. We have conjectured that theorem B applies for more general recurrence relations in such group.

We would like to announce that Dikici and his supervisor, Smith, have been working on similar question about $F(r,n)$ where $r \geq 3$. They claim that more general Fourier sums than those in chapter 3 are zero for $r \geq 3$ by using linear algebra methods. The homogeneous linear equations system obtained from the Fourier sums will be solved by using matrix methods.

They also claim that theorem A and theorem B can be proved for more generalizations of the Fibonacci groups.

APPENDIX

On Similar Distinct Finite 2-Groups

Philip Hall[Ha40] worked on the classification groups of prime power order. In his work, the ideas of an isoclinism, isoclinism families and families of invariants were introduced. Isoclinism is an equivalence relation on the class of groups which is weaker than isomorphism.

R. James, M.F. Newman and E.A. O'Brien[JNO] worked on the groups of order 128. They showed that there are 2328 isomorphism types of group of order 128 and 115 isoclinism families.

The groups may be discriminated with the help of character tables, but we seek to separate them using cruder techniques.

Newman and O'Brien constructed a CAYLEY version 3.6 library for the groups of order dividing 128 by using a p-group generation algorithm. The CAYLEY library includes library twogps. One particular isoclinism family is studied in this work. This comprises 210 groups of order 128. We will try to find natural algebraic invariants which discriminate between non-isomorphic groups in this family. We use the library twogps in the CAYLEY language. This isoclinism family is the largest isoclinism family in groups of order 128. O'Brien suggested[1] that this particular isoclinism class might prove difficult to separate into isomorphism types using simple algebraic invariants. It turns out that he was both right and wrong. One can discriminate between most of the groups in O'Brien's target isoclinism family using fairly crude invariants. There are, however, five pairs of groups which seem resistant to discrimination by elementary methods.

[1] Personal communication.

There is an invariant which will discriminate between these groups; one could use the multiplication tables! A more challenging question is to try to find "simple" invariants which will do the trick. The multiplication table of a group of order 128 contains 2^{14} entries and even then, the order in which the rows and columns are labelled must be taken into account. Another objection to the multiplication table is that it ignores the algebraic structures which algebraists normally use. The subgroup lattice, sizes of generating sets of subgroups, centralizers, normalizers, conjugacy classes etc are notions which enable one to understand a group – but the multiplication table itself is relatively useless; one is swamped with information.

Firstly we will give some background on isoclinism.

Definition: Two groups G_1 and G_2 with centres $Z(G_1)$, $Z(G_2)$ and derived group G_1', G_2' are said to be isoclinic if there exists isomorphisms

$$\theta : G_1/Z(G_1) \longrightarrow G_2/Z(G_2),$$

$$\phi : G_1' \longrightarrow G_2'$$

such that $\phi([\alpha,\beta]) = [\alpha',\beta']$ for all α, $\beta \in G_1$, where $\alpha'\mathrm{Z}(G_2) = \theta(\alpha\mathrm{Z}(G_1))$ and $\beta'\mathrm{Z}(G_2') = \theta(\beta\mathrm{Z}(G_1'))$ (written $G_1 \sim G_2$). In fact it is a equivalence relation and the pair (θ,ϕ) is called an isoclinism. Two groups belong to same family iff they are isoclinic. Equivalence classes are called (isoclinism) families.

There are many properties of isoclinism families. It is clear that $G \sim 1$ iff G is abelian. Any property which is the same for any two groups of the same family will be called a family invariant. If we do not distinguish between isomorphic groups, we may say that the commutator subgroup and central quotient groups are family invariants. The nilpotency class of a prime-power group is a family invariant. For detailed information see Hall[Ha40] and James[Ja].

Every group of order p^n, p is a prime number and n is a natural number, has a power-commutator presentation on n generators. A presentation on n generators defines a group of order p^n if presentation is consistent.

We are studying the groups of order 128 with 4 generators, nilpotency class-2, rank 7 ($= log_2 \mid Z \cap G' \mid + log_2 \mid G/Z \mid$), where Z is centre of G and G' is the derived subgroup of G. These groups all have 38 conjugacy classes.

Library twogps in CAYLEY was constructed by Newman and O'Brien [NO]. This library contains two-groups of order less than 2^8. In this library, there are many sublibraries, but we used just two sublibraries; library gps128d4 (groups of order 128 on 4-generators) and library genrat (which converts from O'Brien's compact description to group presentations).

There are 1153 groups in library gps128d4. We studied 210 groups of these which are in the same isoclinism family. These groups are "similar" groups in positions between 139-348 in the library gps128d4 isoclinism family number 29 in James, Newman, O'Brien[JNO]. Invariants are used to demonstrate non-isomorphism of groups in this isoclinism family.

The first invariants are the numbers of elements of different orders of groups. Every group has 128 elements; an identity element and elements of various 2-power order.

type of grps	numb. of elts. of ord. 2	numb. of elts. of ord. 4	numb. of grps
1	47	80	7
2	63	64	2
3	55	72	3
4	31	96	37
5	39	88	19
6	23	104	56
7	15	112	53
8	7	120	33

The table shows that the 210 groups are separated into eight types.

Second invariants: We investigate the number of subgroups and of Abelian subgroups of our groups. According to these invariants, groups in first three types are non-isomorphic, that is, each group has different number of subgroups and of Abelian subgroups. The rest of types have similar groups which are at most eigth, but a lot of groups in these types are non-isomorphic.

Clearly groups of type 6 and 7 are likely to give us the most difficulty. Non-isomorphic groups are also omitted from the table.

type of groups	4	5	6	7	8
number of	6	2	8	8	8
subgroups and	6	2	6	6	5
of Abelian	3	2	4	6	5
subgroups of	2	2	4	6	3
similar groups	2	2	3	4	3
	2	2	3	3	2
	2		3	2	
	2		2	2	
			2	2	
			2	2	
			2		
			2		
			2		

Third invariants: This invariant is normalizer of subgroups in a group. If normalizer of subgroup in a group is equal to the group, then we investigated number of conjugacy classes of the factor group, the number of subgroups of the factor group and number of elements of order 2 and 4 in the factor group, respectively.

In this step, we obtain that many of our groups are non-isomorphic. There are still similar groups in each type.

type of groups	6	7	8
number of similar	3	2	3
groups	3	2	
	2	2	
	2		

The last invariant is the power map. At the end, five pairs of groups $(2,2,2,2,2)$ are similar. We couldn't separate these groups by using simple invariants; group numbers in the library gps128d4 are 262-267,312-314,331-333, 264-269 and 309-313. All the remaining groups have been demonstrated to be non-isomorphic.

Definition: Let G be a p-group and let C be the set of conjugacy classes of the group G. We define the power map as follows; it is a map

$$f : C \longrightarrow C$$

defined by

$$[x] \longrightarrow [x^p].$$

Here the conjugacy class of the element y is denoted $[y]$. The map f is well-defined (as the reader may verify), and is called power map on the conjugacy classes C.

The use of the power map; we take representative x of conjugacy class number i, we look at x^p and identify its class number, say j, then $i \longrightarrow j$.

For example, let us examine groups 251 and 266 and restrict attention to the conjugacy classes of length 4 and which happen to contain elements of order 4. For each of our groups, we find that the number of such classes is 16. When we look at the power maps of these groups, restricting the domains to the specified conjugacy classes we find the following:

There are 6 conjugacy classes of the specified type in group number 251, whose image under the power map is conjugacy class 23 - a class of size 1. Therefore, there are 24 elements of order 4 in conjugacy class of length 4 with squares conjugate (in fact equal) to the element in cl[23] in gp251. No more than 16 similar elements can be found conjugate to a particular element in gp 266. Thus the power map distinguishes the groups.

We want to take one of these pairs. If we take (262,267),then

Group presetation of gp 262;

$f1^2{=}f7$, $f2^2{=}f5*f6$, $f3^2{=}1$, $f4^2{=}f6$,

$f5^2{=}1$, $f6^2{=}1$, $f7^2{=}1$, $(f2,f1){=}f5$,

$(f3,f1){=}f6$, $(f3,f2){=}f7$, $(f4,f1){=}f5$.

Group presentation of gp 267;

$g1^2{=}g5*g7$, $g2^2{=}g6$, $g3^2{=}1$, $g4^2{=}g5*g6$,

$g5^2{=}1$, $g6^2{=}1$, $g7^2{=}1$, $(g2,g1){=}g5$,

$(g3,g1){=}g6$, $(g3,g2){=}g7$, $(g4,g1){=}g5$.

Groups share these invariants:

number of elements of order 2 and 4 : 23, 104

number of subgroups : 452

number of Abelian subgroups : 310

number of subgroups of order 2, 4, 8, 16, 32, 64.

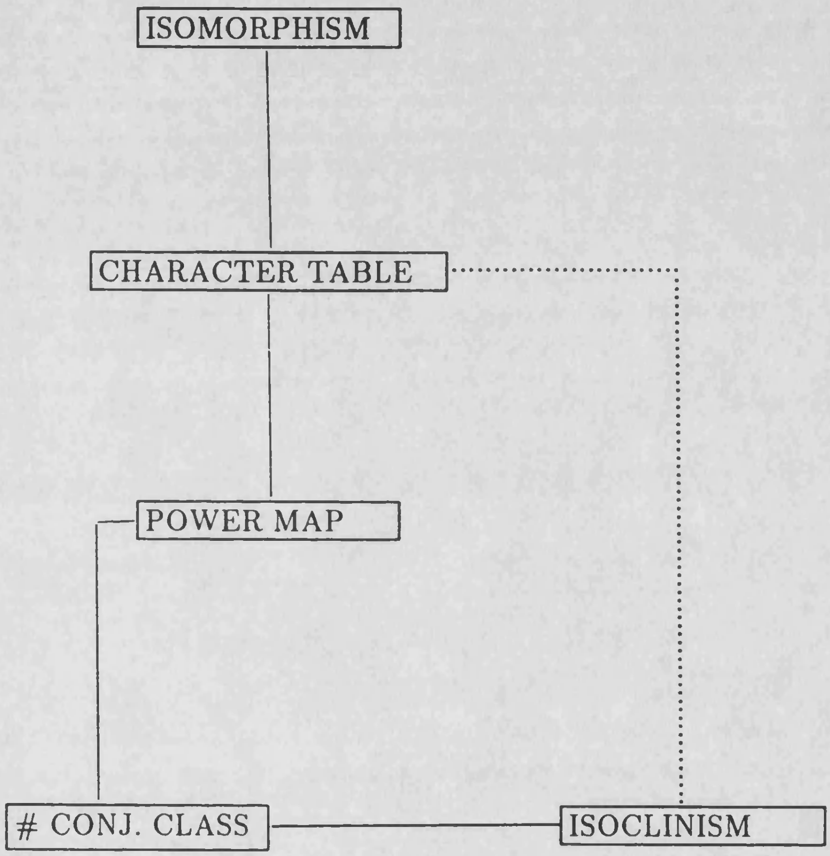
The two groups have identical subgroup lattices, and normal subgroup lattices. The lattices of Abelian subgroups are also identical. They share the same number of conjugacy classes. These statements subsume other co-incidences; for example, the numbers of elements of given order are the same. Lastly, even the power maps are the same.

Challenge

The interested reader is invited to try to distinguish between the 5 pairs of groups using a collection of natural (crude) invariants.

Conclusion

As a result, all of groups except 10 groups between 139-348 in library gps128d4 were demonstrated non-isomorphic using simple invariants. These invariants may be applied to show that isoclinic groups of order 128 are non-isomorphic.


ISOMORPHISM
CHARACTER TABLE
POWER MAP
CONJ. CLASS
ISOCLINISM

References

[Ay] H. Aydin, "On Similar Distinct Finite 2-Groups", Technical Report 90-42, Bath Computer Science, University of Bath, U.K. (1990).

[AS] H. Aydin and G. C. Smith, "Remarks on Fibonacci Sequences in Groups 1", Technical Report 91-50, Bath Mathematics and Computer Science, University of Bath, U.K. (1991).

[Ba] G. Baumslag, "Lecture Notes on Nilpotent Groups", Regional Conference Series in Mathematics, A.M.S. (1969).

[BJK] M. W. Bunder, D.L. Johnson and A. C. Kim, *untitled, in preparation by M.W.B.*, (1991+ϵ)

[Br] A. M. Brunner, "The determination of Fibonacci groups", Bull. Austral. Math. Soc. 11 (1974), 11-14.

[Ca82] J. Cannon, "A Language for Group Theory", Department of Pure Mathematics University of Sydney (1982), Australia.

[Ca87] J. Cannon, "The Cayley Bulletin No 3", Department of Pure Mathematics University of Sydney (1987), Australia.

[CDR] C.M. Campbell, H. Doostie and E.F. Robertson, "Fibonacci Length of Generating Pairs in Groups", Applications of Fibonacci Numbers, ed. G.E. Bergum, A.N. Philippou and A.F. Horada Kluwer vol.3 (1990), 27-35.

[Ch] C.P. Chalk, Ph.D thesis, University of East Anglia (1979 approximately).

[CJ] C.P. Chalk and D.L. Johnson, "The Fibonacci Groups II", Proc. Royal Soc. Edinburgh 77A, (1977), 79-86.

[Co] J.H. Conway "Advanced Problem 5327", Amer. Math. Monthly 72 (1965), 915.

[CR74a] C.M Campbell and E.F. Robertson, "The Orders of Certain Metacyclic Groups", Bull. London Math. soc. 6 (1974) 312-314.

[CR74b] C.M Campbell and E.F. Robertson, "Applications of the Todd-Coxeter algorithm to Generalized Fibonacci groups", Proc. Royal Soc. Edingburgh 73A (1974/75),163-166.

[CT] C.M Campbell and R.M. Thomas, "On Infinite Groups of Fibonacci Type", Proc. Edingburgh Math. Soc. 29 (1986), 225-232.

[Do] H. Doostie, "Fibonacci-type Sequences and Classes of Groups", Ph.D. thesis, St Andrews (1988).

[Ha40] P. Hall, "The Classification of Prime Power Groups", J. Reine Angew Math. 182 (1940), 130-141.

[Ha79] P. Hall, "The Edmonton Notes on Nilpotent Groups", Queen Mary College Mathematics Notes (1979).

[Ha] G. Havas, "Computer Aided Determination of a Fibonacci Group", Bull. Australian Math. Soc. 15 (1976), 297-305.

[Har] B. Hartley, "Topics in the Theory of Nilpotent Groups" , Group Theory ed. K.W. Gruenberg and J.E. Roseblade, London Math. Soc. (1984) 61-120.

[Ja] R. James, "The Groups of Order p^6 (p an odd prime)", Math. Comput. 34(1980), 613-614.

[JNO] R. James, M.F. Newman and E.A. O'Brien, "The Groups of Order 128", Technical Report No 303, Department of Mathematics, Statistic and Computer Science, Marquette University (1989), USA.

[JO] D.L. Johnson and R.W.K. Odoni *in preparation*(1991 + ϵ).

[Jo74] D.L. Johnson, "A Note on the Fibonacci Groups", Israel J. Math. 17 (1974), 277-282.

[JWW] D.L. Johnson, J.W. Wamsley and D. Wright, "The Fibonacci Groups", Proc. Lond. Math. Soc. (3) 29, (1974), 577 - 592.

[Ly] R. Lyndon *unpublished notes*

[MKS] W. Magnus, A. Karrass and D. Solitar, "Combinatorial Group Theory", Dover (1966).

[Ne] M.F. Newman, "Proving a group infinite ", Research Report 26, Department of Mathematics, Australian National University (1988).

[NO] M.F. Newman and E.A. O'Brien, "A Cayley Library for the Groups of Order Dividing 128", Proceeding of the 1987 Singapore Conference (1987), 437-442.

[O'Br] E.A. O'Brien, "The p-group Generation Algorithm", Department of Mathematics, Statistics and Computer Science Marquette University (1989), USA.

[Se] D. Segal, "Polycyclic Groups ", C.U.P. (1983)

[Sea] D.J. Seal, "The Orders of the Fibonacci Groups", Proc. Roy. Soc. Edinburgh 92A (1982), 181-192.

[So] L. Somer, "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes", The Fibonacci Quarterly 18 No 4 (1980), 316-334.

[Th83] R.M. Thomas, "Some Infinite Fibonacci Groups", Bull. London Math. Soc. 15 (1983), 384-386.

[Th89a] R.M. Thomas, "The Fibonacci Groups $F(4k+2,4)$", preprint.

[Th89b] R.M. Thomas, "The Fibonacci Groups - a Survey", Technical Report 23, Department of Computing Studies, University of Leicester (May 1989).

[Th91] R.M. Thomas, "The Fibonacci Groups Revisited", in C.M.Campbell and E.F.Robertson (eds.), Proceedings of Groups St. Andrews 1989 vol. 2 LMS Lecture Note Series 160, CUP, (1991) pp 445 -454.

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

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

[Wi] H. J. Wilcox, "Fibonacci Sequences of Period n in Groups", The Fibonacci Quarterly 24 (1986), 356-361.