

1991

## **Fibonacci Sequences**

By Sally Clark and Nicole Matt  
8/17/91

## Fibonacci Sequences

### Introduction

We first give some definitions and notation, and then we shall describe the objectives of our project.

We define a function  $G: \mathbf{Z}_p \rightarrow \mathbf{Z}_p$  given by  $G(n) = [\text{Fib}(n) \bmod p]$  where  $p$  is a prime in  $\mathbf{Z}$ ,  $\mathbf{Z}_p$  is the field of least residues of  $p$  (integers from zero to  $p-1$ ),  $n$  is an element of  $\mathbf{Z}_p$ , and  $\text{Fib}(n)$  denotes the  $n^{\text{th}}$  Fibonacci number.

Recall that the Fibonacci numbers are given by the recurrence relation

$\text{Fib}(n) = \text{Fib}(n-1) + \text{Fib}(n-2)$ , where  $\text{Fib}(0) = 0$  and  $\text{Fib}(1) = 1$ ; or

equivalently by the Binet formula  $\text{Fib}(n) = (\alpha^n - \underline{\alpha}^n) / (\alpha - \underline{\alpha})$  where  $\alpha$  represents the golden mean  $1/2 (1 + \sqrt{5})$  and  $\underline{\alpha}$  is its conjugate  $1/2(1 - \sqrt{5})$ .

A sequence derived from our function  $G$  can be found in the following way. Suppose the prime is 29 and we want to find the sequence beginning with 17. Referring to the values found in appendix A, we find  $\text{Fib}(17) = 1597$ , which is  $2 \pmod{29}$ .  $\text{Fib}(2) = 1 \equiv 1 \pmod{29}$ . Since  $\text{Fib}(1) = 1 \equiv 1$

(mod 29), we have a fixed point of the function  $G$ , and the sequence continues as a series of ones. This sequence is written  $\{17,2,1\}$  and is among the series listed in appendix B.

The following definitions are borrowed from Fractals Everywhere by Michael Barnsley.

- a) Def.- A dynamical system is a transformation  $F:X \rightarrow X$  on a metric space  $(X,d)$ . It is denoted  $\{X;f\}$ . The orbit of a point  $x$  in  $X$  is the sequence  $\{F^n(x)\}_{n=0}^{\infty}$ . [pg 134]
- b) Def. - Let  $\{X;f\}$  be a dynamical system. A periodic point of  $f$  is a point  $x$  in  $X$  such that  $F^n(x) = x$  for some positive integer  $n$ . Any positive integer  $n$  for which  $F^n(x) = x$  is called a period of  $x$ , and the least such  $n$  is called the minimal period of  $x$ . The orbit of a periodic point of  $f$  is called a cycle of  $f$  and the period of a cycle is the number of distinct points it contains. [pg 136]
- c) Def. - Let  $\{X;f\}$  be a dynamical system. A point  $x$  in  $X$  is eventually periodic if  $F^m(x)$  is a periodic point of  $f$  for some positive integer  $m$ . [pg 137]
- d) Def. - We call  $x$  a fixed point of a function  $f$  if  $f(x) = x$ .

Our original goal was to study the dynamical system  $\{Z_p; G\}$ , to examine the orbits of points from  $Z_p$  to look for cycles and fixed points, to formulate a description of these cycles and fixed points, and, finally, to predict when they might occur. Two early questions we had were:

1) Does there exist any prime  $p$  such that a cycle of period  $n \geq 2$  occurs in the dynamical system  $\{Z_p; G\}$ ? (i.e. are there any instances of cycles which are not merely fixed points?)

2) It is clear that 0,1, and 5 are always fixed points of  $G$ , since they are fixed points of the Fibonacci function; does any prime  $p$  yield other fixed points?

The answer to both questions, we found simply through data collection, was "yes." There exist primes for which  $\{Z_p; G\}$  has 1 or more cycles, one or more new fixed points, both, or neither. So far, we haven't been able to determine any way to predict the occurrence of cycles, nor can we predict most of the fixed points, but we were able to explain one fixed point which is part of a larger pattern shown in the table below. Notice that we distinguish between two types of primes: those congruent to  $\pm 1 \pmod{5}$  we will call  $p$ -primes or simply denote by  $p$ , and those

congruent to  $\pm 2 \pmod{5}$  are  $q$ -primes, denoted by  $q$ . The reason for this distinction will be explained later.

Table 1

Fib(n)	$G(p - k), k \text{ in } \{1,2,3,\dots\}$	$G(q - k)$
Fib(0) = 0	$G(p - 1) \equiv 0$	$G(q - 1) \equiv 1$
Fib(1) = 1	$G(p - 2) \equiv 1$	$G(q - 2) \equiv q-2^*$
Fib(2) = 1	$G(p - 3) \equiv p-1 \equiv -1$	$G(q - 3) \equiv 3$
Fib(3) = 2	$G(p - 4) \equiv 2$	$G(q - 4) \equiv q-5$
Fib(4) = 3	$G(p - 5) \equiv p-1 \equiv -3$	$G(q - 5) \equiv 8$
Fib(5) = 5	$G(p - 6) \equiv 5$	$G(q - 6) \equiv q-13$

\*this is the fixed point that we were able to show would always occur.

For example,  $G(p-1) \equiv 0$  tells us that, for the prime  $p = 41$ ,  $G(40) \equiv 0$ ; we see this is true since  $\text{Fib}[p - 1] = \text{Fib}[40] = 10,2334,155 \equiv 0 \pmod{41}$ .

The behavior of  $G$  shown in the above table is easily explained using three theorems from Number Theory in the Quadratic Field with Golden Section Unit by Fred Wayne Dodd, but before we present the theorems and make use of them, a little background information is necessary to understand their content.

Let  $\mathbf{Q}(\sqrt{5})$  be the quadratic number field whose elements are of the form  $a + b\sqrt{5}$ , where  $a$  and  $b$  are elements of  $\mathbf{Q}$ , and let  $\mathbf{Z}(\alpha)$  be the set of all  $c + d\alpha$  where  $c$  and  $d$  are in  $\mathbf{Z}$ .  $\mathbf{Z}(\alpha)$  is called the set of quadratic integers of  $\mathbf{Q}(\sqrt{5})$ , since every element of  $\mathbf{Z}(\alpha)$  can be written  $1/2(2c + d) + 1/2(d)\sqrt{5}$  in  $\mathbf{Q}(\sqrt{5})$ . The elements of  $\mathbf{Z}(\alpha)$  found in the intersection of  $\mathbf{Q}(\sqrt{5})$  and  $\mathbf{Q}$  are none other than the set of rational elements of  $\mathbf{Z}$ . [Dodd, pg 2].

An element  $\beta$  in  $\mathbf{Z}(\alpha)$  has the form  $c + d\alpha$  where  $c$  and  $d$  are in  $\mathbf{Z}$ . Equivalently,  $\beta$  can have the form  $\beta = a + b\sqrt{5}$  where  $a$  and  $b$  are elements of  $\mathbf{Z}$  and  $a \equiv b \pmod{2}$ . The conjugate of  $\beta$ , written  $\bar{\beta}$ , is  $c + d\alpha$  or  $a - b\sqrt{5}$ . The norm of  $\beta$ , written  $N(\beta)$ , is  $N(\beta) = \beta\bar{\beta}$ . A unit in  $\mathbf{Z}(\alpha)$  is a divisor of 1;  $\gamma$  is a unit iff  $\gamma\delta = 1$  for some  $\delta$  in  $\mathbf{Z}(\alpha)$ . [Dodd pg2]

$\beta$  is an associate of  $\beta_1$  if  $\beta = \gamma\beta_1$ , for some unit  $\gamma$ . [Dodd, pg 16].  $\beta$  is a prime in  $\mathbf{Z}(\alpha)$  if  $\beta$  is not a unit  $\gamma$  and every time  $\beta = \gamma\delta$  with  $\gamma$  and  $\delta$  in  $\mathbf{Z}(\alpha)$  then one of  $\gamma$  or  $\delta$  is a unit.

### Important facts

1) The units in  $\mathbf{Z}(\alpha)$  are  $\pm\alpha^n$  where  $n$  is an element of  $\mathbf{Z}$ . [pg 21]

2) For positive  $n$ ,  $\alpha^n = \text{Fib}(n-1) + \alpha \text{Fib}(n)$ ;  $\underline{\alpha}^n = \text{Fib}(n+1) - \alpha \text{Fib}(n)$ ; and

$$\alpha^{-n} = (-1)^n [\text{Fib}(n+1) - \alpha \text{Fib}(n)]. \quad [\text{pg } 22]$$

3) The primes in  $\mathbf{Z}(\alpha)$  are of three types.

a)  $2 + \alpha$  and its associates

b)  $q$ -primes and their associates

c) every  $p$ -prime =  $|N(\mu)| = |\mu\underline{\mu}|$  where  $\mu$  and  $\underline{\mu}$  are nonassociates in

$\mathbf{Z}(\alpha)$ .  $\mu$ ,  $\underline{\mu}$  and their associates are primes in  $\mathbf{Z}(\alpha)$ . [pg 25]

Here we see the reason for making a distinction between  $q$ -primes and  $p$ -primes of  $\mathbf{Z}$ 's. In  $\mathbf{Z}(\alpha)$ ,  $q$ -primes are still prime, while  $p$ -primes are not. Hence, they behave differently.

4)  $\alpha^2 = \alpha + 1$ ;  $\alpha + \underline{\alpha} = 1$ ;  $N(\alpha) = \alpha\underline{\alpha} = -1$ ;  $\alpha^2 = \underline{\alpha} + 1$ ;  $N(\beta)$  and  $(\beta + \underline{\beta})$

are elements of  $\mathbf{Z}$  for all  $\beta$  in  $\mathbf{Z}(\alpha)$ .  $N(\beta) = 0$  iff  $\beta = 0$ .  $N(\beta\gamma) =$

$N(\beta) \cdot N(\gamma)$ , and  $N(\beta/\gamma) = N(\beta)/N(\gamma)$  if  $\gamma \neq 0$ .  $\underline{\beta\gamma} = \underline{\beta} \cdot \underline{\gamma}$  and  $\underline{\beta/\gamma} = \underline{\beta}/\underline{\gamma}$  where

$\gamma \neq 0$ . [pg 8,9]

5)  $\beta \equiv \gamma \pmod{\partial}$  in  $\mathbf{Z}(\alpha)$  if  $(\beta - \gamma) = \mu\partial$  for some  $\mu$  in  $\mathbf{Z}(\alpha)$ . [pg 41]

Notice that we use "mod" when working in  $\mathbf{Z}(\alpha)$  and "mod" in  $\mathbf{Z}$ .

The following is an example of arithmetic in  $\mathbf{Z}(\alpha)$ :

$$(6-\alpha) \equiv 2 + 2\alpha \pmod{3 - 2\alpha} \text{ since } 6 - \alpha - (2 + 2\alpha) = \mu(3 - 2\alpha) \text{ for some } \mu$$

in  $\mathbf{Z}(\alpha)$ . We find  $\mu$  like so:

$$\begin{aligned} \mu &= (6 - \alpha - (2 + 2\alpha))/(3 - 2\alpha) = (4 - 3\alpha)/(3 - 2\alpha) = ((4 - 3\alpha)(3 - 2\alpha))/((3 - 2\alpha)(3 - 2\alpha)) \\ &= (12 - 8\alpha - 9\alpha + 6\alpha^2)/(9 - 6\alpha - 6\alpha + 4\alpha^2) = (12 - 8(1 - \alpha) - 9\alpha + 6(-1))/(9 - 6(+1) + 4(-1)) \\ &= (12 - 8 - \alpha - 6)/(-1) = -1(-2 - \alpha) = 2 + \alpha \end{aligned}$$

Now, armed with these definitions and facts about number theory in  $\mathbf{Z}(\alpha)$ , we return to the problem of explaining the behavior of our function  $G$  as shown in Table 1. We use the following three theorems.

Theorem 1 If  $p$  and  $q$  are primes in  $\mathbf{Z}$  such that  $p \equiv \pm 1 \pmod{5}$ , and  $q \equiv \pm 2 \pmod{5}$ , and  $\beta$  is any element of  $\mathbf{Z}(\alpha)$ , then  $\beta^p \equiv \beta \pmod{p}$  and  $\beta^q \equiv \beta \pmod{q}$ . The proof involves more theory on  $\mathbf{Z}(\alpha)$  than we will give; see Dodd pg 64.

Theorem 2 If  $m$  is an element of  $\mathbf{Z}$ ,  $m \mid \text{Fib}(n)$  iff  $\alpha^n \equiv k \pmod{m}$  for some  $k$  in  $\mathbf{Z}$ . Also if  $m \mid F(n)$  then  $\alpha^n \equiv \text{Fib}(n - 1) \pmod{m}$ .

Proof  $(\Rightarrow)$  If  $m \mid F(n)$  then  $\alpha^n \equiv \text{Fib}(n - 1) + \text{Fib}(n) \equiv \text{Fib}(n - 1) \pmod{m}$ .  $(\Leftarrow)$  Suppose  $\alpha^n \equiv k \pmod{m}$  for some  $k$  in  $\mathbf{Z}$ . Since  $\alpha^n$  is in  $\mathbf{Z}(\alpha)$ , it can be written in the form  $c + d\alpha$  for  $c$  and  $d$  in  $\mathbf{Z}$ ; in particular, here  $\alpha^n = (k + rm) + (sm)\alpha \equiv k \pmod{m}$  for some  $r$  and  $s$  in  $\mathbf{Z}$ . Similarly,  $\alpha^n = (\alpha^n) = (k +$



$rm) - (sm)\alpha \equiv k \pmod{m}$ . So  $\alpha^n - \underline{\alpha}^n \equiv 0 \pmod{m}$ . But we know  $\alpha^n - \underline{\alpha}^n = \sqrt{5} \text{Fib}(n)$  from the Binet formula, so  $0 \equiv \sqrt{5} \text{Fib}(n) = (-1 + 2\alpha) \text{Fib}(n) = \alpha^{-1}(2 + \alpha) \text{Fib}(n) \pmod{m}$ . Since  $\alpha^{-1}$  is a unit in  $\mathbf{Z}(\alpha)$  and  $(2 + \alpha)$  is a prime in  $\mathbf{Z}(\alpha)$ ,  $m$  cannot divide either of them. So it follows that  $m \mid \text{Fib}(n)$ . [pg 121]

Theorem 3 If  $p$  and  $q$  are primes in  $\mathbf{Z}$  with  $p \equiv \pm 1 \pmod{5}$ ,  $q \equiv \pm 2 \pmod{5}$ , then the following are true:

- 1)  $p \mid \text{Fib}(p - 1)$
- 2)  $q \mid \text{Fib}(q + 1)$
- 3)  $5 \mid \text{Fib}(5)$ .

Proof Case 3) is trivial;  $\text{Fib}(5) = 5$ , so of course  $5 \mid \text{Fib}(5)$ . For case 1), we see that  $\alpha^{p-1} \equiv 1 \pmod{p}$ , by Theorem 1. Then using Theorem 2,  $p \mid \text{Fib}(p - 1)$ . For case 2),  $\alpha^{q+1} \equiv \alpha\alpha = N(\alpha) = -1 \pmod{q}$  and so  $q \mid \text{Fib}(q + 1)$ .

Using these theorems, we explain Table 1. Theorem 3 tells us that  $\text{Fib}(p - 1) \equiv 0 \pmod{p}$  and  $\text{Fib}(q + 1) \equiv 0 \pmod{q}$ . Theorem 2 says that if  $p \mid \text{Fib}(p - 1)$  then  $\alpha^{p-1} \equiv \text{Fib}(p - 2) \pmod{p}$ , but we know  $\alpha^{p-1} \equiv 1$  so  $\text{Fib}(p - 2) \equiv 1 \pmod{m}$ , and since  $\text{Fib}(p - 2)$ , 1 and  $m$  are all in  $\mathbf{Z}$ , this is true with the ordinary mod, too. That is,  $\text{Fib}(p - 2) \equiv 1 \pmod{m}$ .

Similarly,  $\alpha^{(q+1)-1} \equiv \text{Fib}((q + 1) - 1) \equiv -1 \pmod{q}$ , so  $\text{Fib}(q) \equiv -1 \pmod{q}$ . Working backwards with the definition of the Fibonacci, one can generate the observations in our table. In fact, we can extend the result we have just proved to show that if  $p \equiv 1 \pmod{4}$  then  $\text{Fib}((p-2)/2) \equiv 0 \pmod{p}$ , and similarly, if  $q \equiv 1 \pmod{4}$  then  $\text{Fib}((q+1)/2) \equiv 0 \pmod{q}$ . We have arranged our data in Table 2 below, to make the proof clearer.

Table 2

$\text{Fib}(p - 1) \equiv 0 \equiv -\text{Fib}(0)$	$\text{Fib}(p - 1) \equiv 0 \equiv \text{Fib}(0)$
$\text{Fib}(p - 2) \equiv 1 \equiv +\text{Fib}(1)$	$\text{Fib}(p - 1) \equiv -1 \equiv -\text{Fib}(1)$
$\text{Fib}(p - 3) \equiv -1 \equiv -\text{Fib}(2)$	$\text{Fib}(p - 1) \equiv 1 \equiv +\text{Fib}(2)$
:	:
$\text{Fib}(p - (p + 1)/2) \equiv k \equiv \text{Fib}((p - 1)/2)$	$\text{Fib}(q - (q - 1)/2) \equiv m \equiv \text{Fib}((q + 1)/2)$
for some $k$ such that $ k  \in \mathbb{Z}_p$	for some $m$ such that $ m  \in \mathbb{Z}_q$

First notice that  $(p - 1)/2$  is an even integer, so the negative sign preceding " $\text{Fib}((p-1)/2)$ " is correct; also  $(q+1)/2$  is odd, so the negative sign in front of " $\text{Fib}((q+1)/2)$ " is correct as well. Next note that  $(p - (p - 1)/2) \equiv (p-1)/2 \pmod{p}$ , and  $(q - (q-1)/2) \equiv (q+1)/2 \pmod{q}$ . This means

that in fact  $k \equiv -k \pmod{p}$  and  $m \equiv -m \pmod{q}$ . The only  $k$  and  $m$  that satisfy these congruences are  $k = m = 0$ .

We conclude by noting several questions we would still like to look into, or would like to suggest to anyone interested in continuing our work.

1) Our original problem of predicting cycles and fixed points is still open.

We include at the end of this paper a copy of our Mathematica functions  $\text{Fib}[n\_]$  and  $G[p,r]$ , and a table of data that we have already collected, which we hope will be a timesaver.

2) A specific question on points which go directly to zero - Table 2 and proof show that there is a zero-point approximately "halfway" between 0 and  $p$ , or 0 and  $q$ , for certain  $p$  and  $q$  primes. We have noticed that sometimes other zero points occur at regular intervals, but we don't know why, or when to expect them to show up.

For example, for the prime  $p=61$ , zero points occur every fourth of the way from 0 to  $p-1$ ; that is,  $\text{Fib}(15) = 0$ ,  $\text{Fib}(30) = 0$ ;  $\text{Fib}(45) = 0$ ; (and  $\text{Fib}(60) = 0$ , of course). For  $p= 89$ , zero points appear every eighth of the way from 0 to  $p-1$ .  $\text{Fib}(11) = \text{Fib}(22) = \text{Fib}(33) = \text{Fib}(44) = \dots = 0$ . For  $q=47$ , zero points happen every third of the way, from 0 to  $q +1$ .  $\text{Fib}(16) = \text{Fib}(32) = 0 \pmod{q}$

However,  $q = 23$  has no zero points,  $p = 41$  only has the "halfway zero

point  $\text{Fib}(30) = 0$ , and most others are disappointing as well.


3) To what extent do fixed points and cycles of  $G$  act like magnets, drawing in the orbits of other points? Some seem to be very attractive while others are not at all. An example of this is seen in the behavior of the prime  $q = 53$ . The fixed point 34 appears in the orbits of 5 other points besides its own; the fixed point 51 appears only in its own orbit.

## Appendix A

### *Fibonacci Numbers $F_1$ – $F_{40}$*

$F_1 = 1$	$F_{21} = 10946$
$F_2 = 1$	$F_{22} = 17711$
$F_3 = 2$	$F_{23} = 28657$
$F_4 = 3$	$F_{24} = 46368$
$F_5 = 5$	$F_{25} = 75025$
$F_6 = 8$	$F_{26} = 121393$
$F_7 = 13$	$F_{27} = 196418$
$F_8 = 21$	$F_{28} = 317811$
$F_9 = 34$	$F_{29} = 514229$
$F_{10} = 55$	$F_{30} = 832040$
$F_{11} = 89$	$F_{31} = 1346269$
$F_{12} = 144$	$F_{32} = 2178309$
$F_{13} = 233$	$F_{33} = 3524578$
$F_{14} = 377$	$F_{34} = 5702887$
$F_{15} = 610$	$F_{35} = 9227465$
$F_{16} = 987$	$F_{36} = 14930352$
$F_{17} = 1597$	$F_{37} = 24157817$
$F_{18} = 2584$	$F_{38} = 39088169$
$F_{19} = 4181$	$F_{39} = 63245986$
$F_{20} = 6765$	$F_{40} = 102334155$

## Appendix B

The data presented on the next few pages is the result of running function  $G$  on primes and their residues. The number on the left is the prime used as a modulus in the function, and the strings of numbers on the right are the orbits of the residues. Notice for larger primes we omit all but the first few numbers of the orbit of a point, to save space. Arrows represent cycles. On the left margin, the symbol  means a cycle occurs, and \* means a new fixed point occurs.

Dynamics of Residues

- 7 {0}, {1}, {2,1}, {3,2,1}, {4,3,2,1}, {5}, {6,1}
- 11 {0}, {1}, {2,1}, {3,2,1}, {4,3,2,1}, {5}, {6,8,10,0}, {7,2,1}, {8,10,0}, {9,1}, {10,0}
- \* 13 {6,8}, {7,0}, {8}, {9,8}, {10,3,2,1}, {11}, {12,1}
- 17 {6,8,4,2,1}, {7,13,12,2,4,2,1}, {8,4,2,1}, {9,0}, {10,4,3,2}, {11,4,3,2,1}, {12,8,4,2,1}, {13,12,3,4,2,1}, {14,3,2,1}, {15}, {16,1}
- 19 {6,8,2,1}, {7,13,5}, {8,2,1}, {9,15,2,1}, {10,17,1}, {11,13,2}, {12,11,13,5}, {13,2}, {14,14,18,0}, {15,2,1}, {16,2,0}, {17,1}, {18,0}
- 23 {6,6,2,1}, {7,13,3,2,1}, {8,2,1}, {9,11,20,2,1}, {10,9,11,20,2,1}, {11,20,3,2,1}, {12,6,2,2,1}, {13,3,2,1}, {14,9,11,20,2,1}, {15,10,11,20,3,2,1}, {16,2,1}, {17,10,9,11,20,3,2,1}, {18,8,2,1}, {19,18,2,2,1}, {20,3,2,1}, {21}, {22,1}
- 29 {6,7,2,1,13,1}, {7,13,1}, {8,2,1,13,1}, {9,5}, {10,26,22,0}, {11,2,1}, {12,2,0}, {13,1}, {14,0}, {15,1}, {16,1}, {17,2,1}, {18,3,2,1}, {19,5}, {20,2,2,1}, {21,1,1,1}, {22,2,1,1,1}, {23,1}, {24,26,22,0}, {25,2,1}, {26,22,0}, {27,1}, {28,0}
- 31 {6,8,2,1,2,2,1}, {7,13,16,26,22,0}, {8,2,1,3,2,1}, {9,3,2,1}, {10,24,23,13,16,26,22,0}, {11,27,2,1}, {12,20,7,13,16,26,22,0}, {13,16,26,22,0}, {14,5}, {15,2,1,2,1}, {16,26,22,0,0}, {17,16,26,22,0,0}, {18,11,27,2,1}, {19,27,2,1}, {20,7,13,16,26,22,0}, {21,2,1}, {22,10,24,23,13,16,26,22,0}, {23,1}, {24,1}, {25,1}, {26,1}, {27,1}, {28,1}, {29,0}
- \* 37 {6,8,2,1,3,1,24,7,13,11,15,18}, {7,13,11,15,18,3,24}, {8,2,1,3,1,18}, {9,3,1,1,1,1}, {10,14,15}, {11,13}, {12,23,22,2,2,1,3,1,18}, {13,7}, {14,7,24}, {15,11}, {16,25,26,23,32,2,2,1,3,1,18}, {17,6}, {18,1}, {19,0}, {20,3,1,2,2}, {21,3,1,2,2}, {22,25,1,1}, {23,14,0}, {24,3,1}, {25,1}, {26,1}, {27,22,1}, {28,18,15}, {29,3,2,1}, {30,2,1,1,1,1}, {31,18}, {32,8,2,1,3,1,18}, {33,32,1}, {34,5,2,1}, {35,36}
- 41 {6,8,2,1,4,0,0}, {7,13,20,20,0}, {8,1}, {9,34,22,13,3}, {10,14,8,3}, {11,7,3}, {12,2,1,2,0}, {13,1}, {14,1}, {15,36,33,40,0}, {16,2,2,1}, {17,29,13}, {18,1}, {19,40,0}, {20,0}, {21,40,0}, {22,40,0}, {23,34,1}, {24,38,40,0}, {25,20,20,3}, {26,33,13,3}, {27,20,20,0}, {28,1}, {29,7,30,40,0}, {30,27,3}, {31,34,33,3}, {32,20,0}, {33,3}, {34,1}, {35,0}, {36,38,40,0}, {37,2,1}, {38,0}, {39,0}
- 43 {6,8,2,1,4,0,0}, {7,13,2,4,2,2,1}, {8,1}, {9,34,13,5,2,3}, {10,12,10,2,1}, {11,11,10,2,1}, {12,11,10,2,1}, {13,11,10,2,1}, {14,11,10,2,1}, {15,11,10,2,1}, {16,11,10,2,1}, {17,11,10,2,1}, {18,11,10,2,1}, {19,11,10,2,1}, {20,11,10,2,1}, {21,11,10,2,1}, {22,11,10,2,1}, {23,11,10,2,1}, {24,11,10,2,1}, {25,11,10,2,1}, {26,11,10,2,1}, {27,11,10,2,1}, {28,11,10,2,1}, {29,11,10,2,1}, {30,11,10,2,1}, {31,11,10,2,1}, {32,11,10,2,1}, {33,11,10,2,1}, {34,11,10,2,1}, {35,11,10,2,1}, {36,11,10,2,1}, {37,11,10,2,1}, {38,11,10,2,1}, {39,11,10,2,1}, {40,11,10,2,1}, {41,11,10,2,1}, {42,11,10,2,1}, {43,11,10,2,1}

P

Arithmetic

46 cont'd

£12, 15, 8--3, £13, 18, 4--3, £14, 33, 40, 3, 2, 1, £15, 5, 8--3, £16, 4, 13, £17, 6--3, £18, 4--3  
£19, 10--3, £20, 14--3, £21, 24, 14--3, £22, 38, 5--3, £23, 19--3, £24, 14--3, £25, 25, 10, 3, 2  
£26, 4--3, £27, 37, 30, 23, 40--3, £28, 4, 13, £29, 5, 9--3, £30, 33--3, £31, 25--3, £32, 18--3  
£33, 40, 2, 2, 1, £34, 12--3, £35, 9--3, £36, 21--3, £37, 30--3, £38, 8--3, £39, 38--3, £40, 3, 2, 1  
£41, £42, 13

47

£6, 7, 2--3, £7, 13, 45, £8, 21, 42, £9, 34, 10, 10, £10, 2, 10, £11, 42, 8, 2, 13, £12, 3, 2, 13,  
£13, 45, £14, 13, £15, 46, 13, £16, 0, £17, 46, 13, £18, 46, 13, £19, 45, £20, 44, 3, 2, 3, £21, 42,  
£22, 30, £23, 45, £24, 34, 13, £25, 26, 39, 13, 45, £26, 15, 45, £27, 5, £28, 5, £29, 11,  
£30, 46, 13, £31, 13, £32, 0, £33, 13, £34, 13, £35, 2, 13, £36, 2, 2, 13,  
£37, 5, £38, 2, 13, £39, 13, 45, £40, 21, 42, £41, 34, 13, £42, 2, 2, £43, 2, 2, 13,  
£44, 2, 2, £45, £46, 13

53

£6, 2, 21, 26, 23, 37, 46, £7, 13, 21, 46, £8, 21, 46, £9, 34, £10, 2, 13, £11, 36, 40, 6, 2, 2,  
£12, 38, 33, 25, 30, 46, 37, £13, 21, 46, £14, 6, £15, 27, 0, £16, 33, 35, 30, 46, 37,  
£17, 7, £18, 40, 6, £19, 47, 40, £20, 30, £21, 46, £22, 9, 30,  
£23, 28, £24, 46, 37, £25, 30, 46, 37, £26, 23, 28, £27, 0, £28, 21, £29, 22, 28,  
£30, 46, 37, £31, 46, £32, 9, 34, £33, 35, £34, £35, 6, £36, 40, 6, £37,  
£37, 23, £38, 33, £39, 26, £40, 6, £41, 22, 9, 34, £42, 28, £43,  
£43, 17, £44, 2, £45, 19, £46, 37, £47, 40, £48, £49, 48, £50, 3, 2, 1,  
£51, £52, 13

59

£6, 2, 11, 31, 7, 13, 56, 52, 0, £7, 13, 52, 58, 0, £8, £9, 24, 6, £10, 55, 2, 13, £11, 30, 22,  
£12, 26, 5, 32, 11, £13, 56, 52, 0, £14, 26, 42, 16, 48, 20, 59, 51, 13, £15, 20, 39, 51, 13,  
£16, 42, 20, 39, £17, 4, £18, 47, £19, 51, 13, £20, 39, 51, £21, 11, 7,  
£22, 11, 30, £23, 42, 16, £24, 53, 5, £25, 36, 48, 10, £26, 30, 11, £27, 7, £28, 37, 31,  
£29, 44, 22, 48, 4, £30, 11, £31, 7, £32, 22, £33, 36, 48, 10, £34, 6, £35, 42, 16, £36,  
£37, 48, 4, £38, 51, 13, £39, 5, 13, £40, 12, £41, 4, £42, 16, £43, 21,  
£44, 36, £45, 56, 58, 0, £46, 33, £47, 30, 11, £48, 4, £49, 34, £50, 32, £51, 3,  
£52, 7, £53, 5, £54, 56, 58, 0, £55, 2, 13, £56, 52, 0, £57, 13, £58, 0

61

£6, 8, 21, 27, 59, 13, £7, 12, 50, 6, £8, £9, 34, 58, 60, 0, £10, 55, 5, £11, 28, 13, £12, 22, 21,  
£13, 50, £14, 11, 28, 13, £15, 0, £16, 11, £17, 11, £18, 22, 21, £19, 33, 59, 13, £20, 55, 5,  
£21, 27, £22, 21, £23, 48, 29, 27, 59, 13, £24, 8, £25, 56, 58, 60, 0, £26, 3, 2, 13, £27, 51, 13,  
£28, 13, £29, 40, 0, £30, 0, £31, 60, 0, £32, 60, 0, £33, 59, 13, £34, 58, 60, 0, £35, 56, 58, 60, 0,  
£36, 53, 13, £37, 42, 39, 27, £38, 40, 6, £39, 27, £40, 6, £41, 27, £42, 29, £43, 11,  
£44, 50, 6, £45, 0, £46, 50, 6, £47, 50, 6, £48, 39, £49, 59, 13, £50, 6, £51, 24











## Appendix C

To program our Fibonacci function, type the following into Mathematica:

```
Fib[n_] := Block[ {q=n, r, V = {{0}, {1}}, M = {{0,1}}, {1,1}} ], While [ q! = 0, r  
= Mod[q,2]; q= Quotient[q,2]; If [r == 1, V = M.V]; M = M.M]; Return [v[[1,1]] ] ]
```

Our G function is a 2-variable function; p stands for "prime" and r stands for "residue", but of course any positive integers would work. For instance, we tried squared of primes and their residues. G does rely on the program "Fib," so type it in first.

```
G[p_,r_] := Block [{j = r, k = 0}, While [ k < 20, Print [j]; j = Mod[ fib[j], p]; k  
++] ]
```

## Bibliography

1. Barnsley, Michael. Fractals Everywhere. Academic Press: New York, 1988.
2. Dodd, Fred Wayne. Number Theory in the Quadratic Field with Golden Section Unit. Polygonal Publishing House: Passaic, NJ, 1983.
3. McCoy, Neal. Modern Algebra. Allyn and Bacon, Inc: Boston, 1975.