The Number of Residues in the Fibonacci Sequence Modulo P

Heather M. Johnston

June 4, 1990

1 Introduction

The sequence of Fibonacci numbers F(n) is defined by the recurrence relation

$$F(n+1) = F(n) + F(n-1)$$

with the initial conditions $F(0) = 0$ and $F(1) = 1$. When this sequence is considered modulo p, i.e. in the field with p elements, it will clearly repeat itself as there are only p^2 possible pairs of numbers. We shall call the number of terms before the sequence repeats itself its period.

Roberts showed that for $p \equiv \pm 1 \bmod 5$ and $\pm 2 \bmod 5$, the periods of repetition for the Fibonacci sequences modulo p divide $p - 1$ and $2p + 2$ respectively, [5]. He also gave an elementary proof of the following lemma.

Lemma 1 *The period of the Fibonacci sequence mod p is equal to the order of* α *in the ring* $\mathcal{Z}[\alpha]/(p)$ *where* $\alpha = \frac{1+\sqrt{5}}{2}$.

For simplicity in this paper we will restrict our attention to the case of maximal period. In his paper, Roberts also made the following conjectures about the number R of different residues that appear in the Fibonacci numbers mod p with maximal period k.

Conjecture 2 *If* $p \equiv \pm 2 \bmod 5, k = 2p + 2$, *then* $R \approx\ 0.75p$.

Conjecture 3 *If* $p \equiv \pm 1 \bmod 5, p \equiv 3 \bmod 4, k = p - 1$, *then* $R \approx\ 0.625p$.

Conjecture 4 *If* $p \equiv \pm 1 \bmod 5, p \equiv 1 \bmod 4, k = p - 1$, *then* $R \approx\ 0.43p$.

The following table of conjectures reflects data collected through computer experimentation by Wedekind and Greco, [7].

p (mod 20)	k	R/k
3, 7	$2p + 2$	.3750
13, 17	$2p + 2$	.37
11, 19	$p - 1$	.6250
9	$p - 1$	.6250
3, 7, 13, 17	$(2p + 2)/3$	.45
3, 7, 13	$(2p + 2)/9$	.48
11, 19	$(p - 1)/3$	.70
11	$(p - 1)/9$	.72

Note that the first three lines of the table agree with the conjectures of Roberts, while the fourth line contradicts his results and was probably an error in their report. My results show that in Conjecture 2, the residue ratio which appears is 5/8. Also, my results confirm Roberts' Conjecture 3, putting the value of the ratio at 7/16. The main results of this paper are presented in the following three theorems.

Theorem 5 *For* $p \equiv \pm 2 \bmod 5$ *such that the Fibonacci sequence modulo* p *has period* $2p + 2$, *the number of residues appearing in the sequence is* $\frac{3}{4}p + \mathcal{O}(\sqrt{p})$.

Theorem 6 *For* $p \equiv \pm 1 \bmod 5$ *and* $p \equiv 3 \bmod 4$ *such that the Fibonacci sequence modulo* p *has period* $p - 1$, *the number of residues appearing in the sequence is* $\frac{5}{8}p + \mathcal{O}(\sqrt{p})$.

Theorem 7 *For* $p \equiv \pm 1 \bmod 5$ *and* $p \equiv 1 \bmod 4$ *such that the Fibonacci sequence modulo* p *has period* $p - 1$, *the number of residues appearing in the sequence is* $\frac{7}{16}p + \mathcal{O}(\sqrt{p})$.

The method of proof is similar for all three. The numbers $F(n)$ can be

written as

$$F(n) = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \text{ where } \alpha = \frac{1+\sqrt{5}}{2} \text{ and } \overline{\alpha} = \frac{1-\sqrt{5}}{2}. \qquad (1)$$

When considering $\alpha^n - \overline{\alpha}^n \bmod p$, we must work in the ring of integers in $\mathcal{Q}(\sqrt{5})$. The meaning of mod$p$ varies depending on whether or not the ideal (p) splits in this ring. That is whether $p \equiv \pm 2 \bmod 5$ or $p \equiv \pm 1 \bmod 5$. We must also consider whether or not -1 is a quadratic residue in the ring, i.e., whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. The following variation of Weil's theorem, [2], will become useful in our proofs:

Theorem 8 (Weil) *If C is an absolutely irreducible affine curve of degree d over $\mathcal{F}_q$, then the number N_q of affine $\mathcal{F}_q$-rational points on C satisfies* $-(d-1)(d-2)\sqrt{q} - d \leq N_q - (q+1) \leq (d-1)(d-2)\sqrt{q}$.

This theorem can be applied to the equation $5m^2 + 4 = s^2$ for example. For the number N of solutions to this equation, we see that $p-1 \leq N \leq p+1$.

A proof of Theorem 5 can be found in §2, preceded by the proof of a powerful lemma due to Roberts. A proof of Theorem 6 and a similar proof of Theorem 7 are in §3. The paper concludes with some generalizations which can be made from these theorems.

2 The Case $p \equiv \pm 2 \bmod 5$

Greco and Wedekind did not prove any of the ideas generated from their data, but Roberts came close to a proof of his first conjecture with the following lemma.

Lemma 9 *For $p \equiv \pm 2 \bmod 5$ such that the Fibonacci sequence mod p has period $2p+2$, the number of residues appearing in the sequence is the same as the number of values of m such that at least one of $5m^2+4$ and $5m^2-4$ is a quadratic residue in $\mathcal{F}_p$.*

Proof: We would like to know when m appears in the Fibonacci sequence mod p, i.e. when does

$$\frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} \equiv m \bmod p \tag{2}$$

for some n. As pointed out above, for any manipulation of this equation to make sense we must consider it in the ring $\mathcal{Z}[\alpha]/(p)$. Let (m/n) denote the Legendre symbol. For $p \equiv \pm 2 \bmod 5$, $(5/p) = (p/5) = -1$, by quadratic reciprocity. Thus the ideal (p) remains prime in $\mathcal{Z}[\alpha]$ and we have:

$$\mathcal{Z}[\alpha]/(p) \approx \mathcal{F}_p[\alpha] \approx \mathcal{F}_{p^2}$$

By rearranging equation 1 in this field, we get the following equation for x where x is a power of α and c is the norm of x.

$$x^2 - \sqrt{5}mx - c = 0.$$

Whether or not a value of m appears in the sequence depends on whether or not there exists such an x. Some simple computation shows that the two possible solutions to the above equation $x = \frac{\sqrt{5}m \pm \sqrt{5m^2+4c}}{2}$ both have norm c as desired if and only if $\sqrt{5m^2+4c}$ is an element of $\mathcal{F}_p$. In this case $\overline{x} = \frac{-\sqrt{5}m \pm \sqrt{5m^2+4c}}{2}$ and it is easy to see that the norm of x is c.

Recalling Lemma 1, we see that the order of α is $2p+2$. Because α has norm -1, all of its powers have norm 1 or -1. Note that in $\mathcal{F}_{p^2}$, the size of the kernel of the norm map is $p+1$. Therefore, because the norm is surjective, the number of elements with norm 1 or -1 is $2p+2$. Thus these elements must be exactly the set of elements generated by α, and the condition for m to appear in the sequence is that at least one of $5m^2 \pm 4$ be a quadratic residue.

The following proof of Roberts' first conjecture uses his lemma.

Theorem 10 *For $p \equiv \pm 2 \bmod 5$ such that the Fibonacci sequence modulo p has period $2p+2$, the number of residues appearing in the sequence is*

$\frac{3}{4}p + \mathcal{O}(\sqrt{p})$.

Proof: Given the above Lemma 9 all that remains to be shown is that the number M of m in $\mathcal{F}_p$ such that at least one of $5m^2+4$ and $5m^2-4$ is a quadratic residue in $\mathcal{F}_p$, is approximately $3p/4 + \mathcal{O}(\sqrt{p})$. Consider N_+, the number of solutions to the equation $5m^2+4 = s^2$ in $\mathcal{F}_p \times \mathcal{F}_p$. From Theorem 8 theorem we see that that $p-1 \leq N_+ \leq p+1$. We are actually interested in the number of values for m such that there exists an s solving the equation. It is easily seen that each value of m corresponds to two values for s, $\pm s$, so we must divide the above inequality through by two. Note that I have simplified by ignoring the case $s = 0$, since the affect this has on the value of M is negligible. After a similar analysis is performed for $5m^2-4$, all that remains is to determine the number of values of m for which there exists a simultaneous solution to the equations $5m^2 + 4 = s^2$ and $5m^2 - 4 = t^2$. With some knowledge of algebraic geometry one can see that the algebraic set defined by these two quadratic equations is a absolutely irreducible affine curve of degree four. Both an inuitive glance at the equations and numerical data support this statement. However, I have left it without proof here, because the proof would involve a whole new set of ideas. The proof will be found in [3], but

for now it will suffice to say that a proof exists. The number $N_\pm$ of points on this curve is given by Weil's theorem, $p - 3 - 6\sqrt{p} \leq N_\pm \leq p + 1 + 6\sqrt{p}$. Here the number of points corresponding to each value of m for which a solution exists is 4, corresponding to $\pm s$ and $\pm t$. Direct computation from these inequalities produces the desired result:

$$\frac{3p - 5 - 6\sqrt{p}}{4} \leq M \leq \frac{3p + 7 + 6\sqrt{p}}{4}. \tag{3}$$

3 The Case $p \equiv \pm 1 \bmod 5$

Theorem 11 *For $p \equiv \pm 1 \bmod 5$ and $p \equiv 3 \bmod 4$ such that the Fibonacci sequence modulo p has period $p - 1$, the number of residues appearing in the sequence is $\frac{5}{8}p + \mathcal{O}(\sqrt{p})$.*

Proof: With $p \equiv \pm 1 \bmod 5$, $(p/5) = (5/p) = 1$. Therefore p splits in $\mathcal{Z}[\alpha]$ and

$$\mathcal{Z}[\alpha]/(p) \approx \mathcal{F}_p \times \mathcal{F}_p$$

The same argument as above produces the quadratic equation $x^2 - \sqrt{5}mx - c = 0$. Again m appears in the Fibonacci sequence exactly when there exists a solution to this equation such that c is the norm of x and x is a member of the multiplicative group generated by α. In this case the solutions are

expressed as ordered pairs:

$$x = (\frac{\sqrt{5}m \pm \sqrt{5m^2 + 4c}}{2}, \frac{-\sqrt{5}m \pm \sqrt{5m^2 + 4c}}{2})$$

Here the condition that c is the norm of x is satisfied when the $\pm$ signs agree. Taken together the two conditions, that x belong to the multiplicative group generated by α and that c be the norm of x, produce the requirement that $c = \pm 1$. Clearly such a solution exists if a least one of $5m^2 \pm 4$ is a quadratic residue in $\mathcal{F}_p$.

The number of elements in $\mathcal{F}_p \times \mathcal{F}_p$ whose norm is 1 or -1 is $2p - 2$. However, here the period and thus the order of α, by Lemma 1, is only $p - 1$. Hence, α only generates half of the elements whose norm is ± 1, so the above argument can not be used.

Note that in this case α is represented by the ordered pair, $(a, \overline{a})$ where the norm of α is $a\overline{a} = -1$. For $p = 3 \bmod 4$, -1 is not a quadratic residue in $\mathcal{F}_p$. Thus exactly one of a, $\overline{a}$ is a quadratic residue. Without loss of generality, we assume here that a is the quadratic residue. If x has norm 1 or -1 it is generated by α exactly when its first coordinate is a quadratic residue in $\mathcal{F}_p$. So m appears in the sequence when one of $\frac{\sqrt{5}m \pm \sqrt{5m^2 \pm 4}}{2}$ exists and is a quadratic residue in $\mathcal{F}_p$.

First consider the two solutions to a particular equation $x^2 - \sqrt{5}mx + 4 = 0$. Note that their product,

$$(\frac{\sqrt{5}m + \sqrt{5m^2+4}}{2})(\frac{\sqrt{5}m - \sqrt{5m^2+4}}{2}) = -1$$

Note that -1 is not a quadratic residue in $\mathcal{F}_p$. Thus if they exist, exactly one of $\frac{\sqrt{5}m \pm \sqrt{5m^2+4}}{2}$ is a quadratic residue. We see that m appears in the sequence whenever they exist, i.e whenever $5m^2 + 4 = s^2$ has a solution. Recall from above that this happens M_+ times where

$\frac{p-1}{2} \leq M_+ \leq \frac{p+1}{2}$.

On the other hand when considering the two solutions to $x^2 - \sqrt{5}mx - 4 = 0$ we see that their product $(\frac{\sqrt{5}m+\sqrt{5m^2-4}}{2})(\frac{\sqrt{5}m-\sqrt{5m^2-4}}{2}) = 1$ is a quadratic residue. Thus if they exist, either both or neither of $\frac{\sqrt{5}m \pm \sqrt{5m^2+4}}{2}$ are quadratic residues and we must check first if the two numbers exist and second if they are quadratic residues.

These two conditions produce the following pair of equations:

$$\begin{aligned} 5m^2 - 4 &= s^2 \\ \sqrt{5}m + s &= 2r^2 \end{aligned} \tag{4}$$

If there exists a solution to these equations, then m appears in the sequence. Note that the number of solutions corresponding to each m for which there

exists a solution is 4, corresponding to $\pm s$ and $\pm r$. By reasoning similar to that used for the above quadratic equations, the algebraic set defined by these two equations is an absolutely irreducible affine curve of degree 4. Thus for M_-, the number of values for m such that there exists a solution,

$$\frac{p-3-6\sqrt{p}}{4} \leq M_- \leq \frac{p+1+6\sqrt{p}}{4}$$

The question remaining is how many values of m satisfy both of these conditions, i.e. for how many values of m do the following equations have a solution:

$$\begin{aligned} 5m^2+4 &= s^2 \\ 5m^2-4 &= t^2 \\ \sqrt{5}m+t &= 2r^2 \end{aligned} \tag{5}$$

If there exists a solution for a given m, then there exist exactly eight solutions, corresponding to $\pm s, \pm t, \pm r$. By reasoning similar to that used for the above quadratic equations, the algebraic set defined by these equations is an absolutely irreducible affine curve of degree eight. Thus from Weil's theorem, we have the following inequality for $M_\pm$, the number of values of

m satifying the above conditions:

$$\frac{p-7-42\sqrt{p}}{8} \leq M_{\pm} \leq \frac{p+1+42\sqrt{p}}{8}$$

The total number of residues which appear in the sequence, M is then determined by simple arithmetic $M = M_+ + M_- - M_{\pm}$.

$$\frac{5p-17-54\sqrt{p}}{8} \leq M \leq \frac{5p+6+54\sqrt{p}}{8}$$

Theorem 12 *For $p \equiv \pm 1 \bmod 5$ and $p \equiv 1 \bmod 4$ such that the Fibonacci sequence modulo p has period $p-1$, the number of residues appearing in the sequence is $\frac{7}{16}p + \mathcal{O}(\sqrt{p})$.*

Proof: This argument is very similar to that for $p \equiv 3 \bmod 4$, with the exception that here -1 is a quadratic residue mod p. Again $\alpha = (a, \overline{a})$ and $a\overline{a} = -1$, which in this case implies that either both or neither of a and $\overline{a}$ are quadratic residues. If both of them were quadratic residues, then the order of α could not be $p-1$, which it is. Therefore neither is a quadratic residue. If x has norm 1 or -1, x is generated by α exactly when either both of its coordinates are quadratic residues or neither of its coordinates is a quadratic residue.

We must also consider the product of the first coordinates of the two solutions to a particular equation $x^2 - \sqrt{5}mx \pm 1$.

$$(\frac{\sqrt{5}m + \sqrt{5m^2 \pm 4}}{2})(\frac{\sqrt{5}m - \sqrt{5m^2 \pm 4}}{2}) = \pm 1$$

Both 1 and -1 are quadratic residues in $\mathcal{F}_p$. Thus either both of the solutions to $x^2 - \sqrt{5}mx + c = 0$ are quadratic residues for a given value of c or neither solution is.

A residue m appears in the sequence when at least one of the following sets of equations or corresponding sets for $5m^2 - 4$ has a solution.

$$\begin{aligned} 5m^2 + 4 &= s^2 \\ \sqrt{5}m + s &= 2t^2 \\ \sqrt{5}m - s &= 2r^2 \end{aligned} \tag{6}$$

or

$$\begin{aligned} 5m^2 + 4 &= s^2 \\ \sqrt{5}m + s &= 2qt^2 \\ \sqrt{5}m - s &= 2qr^2 \end{aligned} \tag{7}$$

Here q is a given quadratic nonresidue in $\mathcal{F}_p$. M_1, the number of values of m such that there exists a solution to a set of equations is the same

for all four such triples. By reasoning similar to that used for the above quadratic equations, the algebraic set defined by these three equations is an absolutely irreducible affine curve of degree eight. If there exists a solution for a given m, then there exists eight such solutions, corresponding to the different combinations of $\pm s$, $\pm t$, $\pm r$. From this information and Weil's theorem, we have the following condition on M_1.

$$\frac{p-7-42\sqrt{p}}{8} \leq M_1 \leq \frac{p+1+42\sqrt{p}}{8}$$

There are four different ways in which a value of m can satisfy more than one set of equations, (for each c either both solutions must be quadratic residues or neither solution must be a quadratic residue.) For example, consider M_2, the number of values of m such that there exists a simultaneous solution to the following set of equations.

$$\begin{aligned} 5m^2+4 &= s^2 \\ 5m^2-4 &= t^2 \\ \sqrt{5}m+s &= 2u^2 \\ \sqrt{5}m-s &= 2v^2 \\ \sqrt{5}m+t &= 2w^2 \end{aligned} \tag{8}$$

$$\sqrt{5}m - t \;=\; 2r^2$$

By reasoning similar to that used for the above equations, the algebraic set defined by these equations is an absoutely irreducible affine curve of degree 64. For each value of m for which there exists a solution, there are exactly 64 such solutions, (coresponding to the different values for $\pm s$, $\pm t$, $\pm u$, $\pm v$, $\pm w$, $\pm r$). From this fact and Weil's theorem we have the following inequality for M_2.

$$\frac{p - 63 - 3096\sqrt{p}}{64} \leq M_2 \leq \frac{p + 1 + 3906\sqrt{p}}{64}$$

The total number of residues m which appear as residues in the Fibonacci sequence, M is then $4M_1 - 4M_2$.

$$\frac{7p - 119 - 4242\sqrt{p}}{16} \leq M \leq \frac{7p + 9 + 4242\sqrt{p}}{16}$$

4 Generalizations

These results can easily be generalized to determine the number of residues which appear in a Fibonacci sequence mod p^k with period $1/n$ times the maximal period in the following theorems:

Theorem 13 *The number of residues which appear in the Fibonacci sequence modulo p of period $1/n$ times the maximal period is as follows with error of order $\sqrt{p}$:*

$\frac{4n-1}{4n^2}p$ for $p \equiv \pm 2 \bmod 5$ and $n|(p+1)$

$\frac{2n-1}{n^2}p$ for $p \equiv \pm 2 \bmod 5$ and not $n|(p+1)$

$\frac{8n-1}{16n^2}p$ for $p \equiv \pm 1 \bmod 5$ and $4n|(p-1)$

$\frac{6n-1}{8n^2}p$ for $p \equiv \pm 1 \bmod 5$ and not $4n|(p-1)$

The analysis which produces the equation $x^2 - \sqrt{5}mx + c = 0$ remains intact. For $p \equiv \pm 2 \bmod 5$ the condition that $x = \alpha^n$ is converted into a requirement that $x = y^n$ and for $p \equiv \pm 1 \bmod 5$ a requirement that the first coordinate of x be equal to y^{2n}. Whether or not one solution generated by α insures the same for the other solution depends for $p \equiv \pm 2 \bmod 5$ on whether or not the equation $x^n = -1$ has a solution in $\mathcal{F}_{p^2}$ and for $p \equiv \pm 1 \bmod 5$ on whether or not $x^{2n} = -1$ has a solution in $\mathcal{F}_p$. Then depending on whether or not one solution generated by α implies the same for the other solution, an analysis similar to that for $p \equiv \pm 1 \bmod 5$ and either $p \equiv 3 \bmod 4$ or $p \equiv 1 \bmod 4$ will produce an inequality bounding the number of residues

which appear in the sequence. This type of analysis may easily be extended to sequences generated by other recurrence relations as well.

References

[1] Artin, M. *Rings and Fields, 18.702 course notes.* MIT, 1989, unpublished.

[2] Fried, Michael D. and Jarden, Moshe. *Field Arithmetic.* Springer-Verlag, Berlin, 1986.

[3] Johnston, Heather M., Roberts, Boyd and Robson, Robert O. *The Number of Residues in Two-Term Recurrence Relations Modulo p* In Progress.

[4] Marcus, Daniel A. *Number Fields.* Springer-Verlag, New York, 1977.

[5] Roberts, Boyd. "Report on Fibonacci Numbers Mod P." *Undergraduate Summer Research Program in Mathematics,* Oregon State University, 1987, unpublished.

[6] Wall, D.D. "Fibonacci Series Modulo M." *American Mathematical Monthly,* Vol. 67, 1960, pp. 525-532.

[7] Wedekind, Bonnie and Greco, Colleen S. "Discourse on Fibonacci Numbers Modulo P." *Undergraduate Summer Research in Mathematics,* Oregon State University, 1988, unpublished.