1. Introduction.

The Fibonacci sequence has been studied ever since its discovery in the 12^{th} century. Only in the last thirty years, however, have there been any attempts made to answer questions about the Fibonacci sequence mod m. For example, it was only in the mid 70's that the question "When is the Fibonacci sequence uniformly distributed mod m?" was answered. In this paper I will ask the question "How many different residue classes actually appear mod p, where p is an odd prime?". I will then make a series of conjectures, based on numerical evidence, answering this question. Finally, I will give a heuristic argument for one conjecture and discuss the remaining cases.

2. Notation and Conventions.

The n^{th} Fibonacci number will be denoted by F(n). We let $\alpha=(1+\sqrt{5})/2$, $\mathfrak{o}$ be the ring of integers in $\mathbb{Q}(\sqrt{5})$, and σ the Fobenius automorphism of $\mathbb{F}_p2$, the Galois field with p^2 elements. Further, $(\ /p)$ will denote the Legendre symbol mod p and $\bar{\alpha}$ will denote the conjugate of α, i.e. $\bar{\alpha}=(1-\sqrt{5})/2$. N will denote the norm mapping from $\mathbb{Q}(\sqrt{5})\to\mathbb{Q}$ or from $\mathbb{F}_p{}^2\to\mathbb{F}_p$, depending on the context.

3. A new proof of some results of D.D. Wall [1].

In [1] Wall proved that if $p\equiv 3$ or 7 mod 10, then the period of the Fibonacci sequence considered mod p divides 2p+2, and if $p\equiv 1$ or 9 mod 10, then the period of the Fibonacci sequence considered mod p divides p-1. I will give new proofs of slightly different theorems, namely:

Theorem: If $p\equiv 2,3$ (mod 5) then the period of the Fibonacci sequence mod p divides 2p+2. If $p\equiv 1,4$ (mod 5), then the period divides p-1.

Proof: Since the sequence will repeat when 0 and 1 appear as

consecutive terms, it suffices to show that $F(2p+2)=0$ and $F(2p+3)=1$.

Since $p\equiv 2,3 \pmod 5$ implies that $(5/p)=1$ and that p does not divide the discriminant of $\mathbb{Q}(\sqrt{5})$, it follows that the ideal (p) remains prime in θ. Hence $\theta/p\theta \cong \mathbb{F}_p{}^2 \cong \mathbb{F}_p(\sqrt{5})$. Now, since conjugation is a non-trivial automorphism of $\mathbb{F}_p(\sqrt{5})$ which fixes $\mathbb{F}_p$, and the order of the Galois group of $\mathbb{F}_p(\sqrt{5})/\mathbb{F}_p$ is 2, it follows that σ is equal to conjugation. Hence $\alpha^p=\bar{\alpha}$ and $\bar{\alpha}^p=\alpha$. Calculating:

$F(2p+2) = (\alpha^{2p+2} - \bar{\alpha}^{2p+2})/(\alpha - \bar{\alpha}) = (\alpha^p\alpha^p\alpha^2 - \bar{\alpha}^p\bar{\alpha}^p\bar{\alpha}^2)/(\alpha - \bar{\alpha}) =$
$(\bar{\alpha}^2\alpha^2 - \alpha^2\bar{\alpha}^2)/(\alpha - \bar{\alpha}) = 0.$
$F(2p+3) = (\alpha^{2p+3} - \bar{\alpha}^{2p+3})/(\alpha - \bar{\alpha}) = (\alpha^p\alpha^p\alpha^3 - \bar{\alpha}^p\bar{\alpha}^p\bar{\alpha}^3)/(\alpha - \bar{\alpha}) =$
$(\alpha - \bar{\alpha})/(\alpha - \bar{\alpha}) = 1.$

If $p\equiv 1,4 \pmod 5$, it follows that $(5/p)=-1$ and so (p) splits. Hence $\theta/p\theta \cong \mathbb{F}_p \oplus \mathbb{F}_p$ and so $\alpha^p=\alpha$ and $\bar{\alpha}^p=\bar{\alpha}$. We calculate:

$F(p-1) = (\alpha^{p-1} - \bar{\alpha}^{p-1})/(\alpha - \bar{\alpha}) = 0.$ $F(p) = (\alpha^p - \bar{\alpha}^p)/(\alpha - \bar{\alpha}) = 1.$ ■

4. Some conjectures on the number of residues actually appearing when p is an odd prime.

Conjecture A. If $p\equiv 2,3 \bmod 5$ and the period of the sequence mod p is 2p+2, then the number of residues that appear is approximately pC, where $C\approx .75$.

Conjecture B. If $p\equiv 1,4 \bmod 5$, $p\equiv 3 \bmod 4$, and the period of the sequence mod p is p-1, then the number of residues that appear is approximately pK, where $K\approx .625$.

Conjecture C. If $p\equiv 1,4 \bmod 5$, $p\equiv 1 \bmod 4$, and the period of the sequence mod p is p-1, then the number of residues that appear is approximately pL, where $L\approx .43$.

These conjectures are based on numerical evidence; calculations were made for all primes less than 5000. Now in the case of Conjectures B and C, the analysis seems to be harder than the

analysis of Conjecture A, for which I will now provide a heuristic argument.

5. The case $p \equiv 2,3 \pmod 5$.

The residue m appears mod p iff $F(n) \equiv m \pmod p$ for some n, i.e. iff $\alpha^n - \bar{\alpha}^n \equiv m(\alpha - \bar{\alpha}) \pmod p$ for some n. Multiplying through by α^n and simplifying we obtain: $(\alpha^n)^2 - m\sqrt{5}\alpha^n - N(\alpha^n) \equiv 0 \pmod p$. Now, consider the polynomial $f(x) = x^2 - m\sqrt{5}x + c$, where $c = 1$ or -1. Suppose this polynomial has a root in $\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{5})$. An easy calculation shows that the (local) norm of any such root is c.

We claim that α generates $N^{-1}(\{-1,1\})$ if and only if the period of the sequence is $2p+2$. We note that $|\mathrm{Ker}\ N| = p+1$ since N is surjective (this because 5 is a nonresidue mod p and hence $\{a^2 - 5b^2 \mid a,b \in \mathbb{Z}\}$ runs through all residues mod p) and hence $|N^{-1}(\{-1,1\})| = 2p+2$. If $\alpha^n = 1$ in $\mathbb{F}_p$, then $F(n) = 0$ and $F(n+1) = 1$ by direct calculation. Hence if the period of the sequence is $2p+2$, α has order at least $2p+2$ and since it has norm 1, it must generate Ker N. If the period of the sequence mod p is n, $F(n) = 0$ implies $\alpha^n = \bar{\alpha}^n$. We have $1 = F(n+1) = \alpha^n$. Hence, if α has order $2p+2$ the sequence has period $2p+2$.

Hence, in our case we know that if the polynomial f has a root in $\mathbb{F}_p(\sqrt{5})$, it has a root of the form α^n, so a residue shows up in the sequence iff the polynomial f has a root in $\mathbb{F}_p(\sqrt{5})$.

The question has become "How many such polynomials f have roots in $\mathbb{F}_p(\sqrt{5})$?" Clearly such a polynomial has a root iff $5m^2 + 4c$ is a quadratic residue mod p. If we could prove the following lemma, we would then have a proof of Conjecture A, since it would imply that about 75 per cent of the polynomials have roots in $\mathbb{F}_p(\sqrt{5})$, and hence approximately 75 per cent of the residues will appear:

Lemma Let NR be the set of quadratic nonresidues mod p. Then the set $T(A) = \{k \pm A \mid k \in NR\}$ contains either $(p-1)/4$ or $(p-3)/4$ quadratic nonresidues, where $A \in \mathbb{Z}$.

6. The case $p \equiv 1,4 \pmod 5$

Since in this case $\vartheta/p\vartheta \cong \mathbb{F}_p \oplus \mathbb{F}_p$, we have no nice results on the way in which the polynomial $x^2 - m\sqrt{5}x \pm 1$ behaves and hence cannot carry out the above analysis.

[1] D.D. Wall, Fibonacci Series Modulo m, American Mathematical Monthly, 67, (1960), pp. 525-532.