Bonnie Wedekind
Oregon State University

Colleen S. Greco
University of Portland

DISCOURSE ON FIBONACCIS MODULO P

The Fibonacci Numbers have become of great interest over recent years. There are a number of ways one can generate the Fibonacci sequence. The two methods implemented in this project were simple recursion, $f_{n+2} = f_{n+1} + f_n$, and matrix multiplication. The matrix which characterizes the Fibonacci sequence is $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$

The characteristic polynomial of this matrix is $x^2 - x - 1$ with roots $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$ contained in the field $\mathbb{Q}(\sqrt{5})$.

Definitions:

1) $f_n \pmod p$: denotes the Fibonacci sequence modulo p, where p is a prime.

2) residues: the remainders generated when applying mod p to the Fibonacci sequence.

3) cycle length: the total number of residues in the sequence $f_n \pmod p$ counted until the starting values repeat, denoted by k(p).

Two algorithms used to compute cycle lengths were implemented in this project. The first method was straight forward. The Fibonaccis were generated mod p by using the relation $f_{n+2} = f_{n+1} + f_n$ for $n>0$, $f_0 = 0$, and $f_1 = 1$. This process continued until a 0 and 1 reappeared in succession, and the cycle length was computed.

The second algorithm used depended on the following facts as shown by D. D. Wall.

If $p = 2,3 \bmod 5$, then the cycle length of the Fibonacci sequence mod p divides $2p + 2$.

If $p = 1,4 \bmod 5$, then the cycle length of the Fibonacci sequence mod p divides $p-1$.

This second algorithm factored the maximal cyclengths, (2p+2) or (p-1), as described above. All prime factors and their combinations of factors were computed as the power "n" in the following equation.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

Each possibility was attempted until f_n and f_{n+1} equal 0 and 1 respectively. This prime factor or combination thereof was the divisor of (2p+2) or (p-1) which yielded the cycle length.

A conjecture after exploration of cycle lengths:

1) if p = 3,7,11,13,17,19 mod 20 then the divisors of (2p + 2) or (p-1), where applicable, are 1 or 3 mod 4.

Residues:

Some facts used in calculating residues from an article published by Brother U. Alfred:
Let "d" be the distance between zeros for any given Fibonacci sequence mod p.

A) if d is of the form 2(2x+1), then k = d.
B) if d is of the form 2x + 1, then 4d = k.
C) if d is of the form $2^n(2x+1)$, then 2d = k.

One method used to count distinct residues implemented a matrix initialized with negative ones and as f_n(mod p) was calculated, the residues were stored in increasing numerical order. If a residue repeated, it was superimposed in the appropriate slot.

A second method found residues by looking at mirror images. This was done by generating the sequence up to the first zero. Depending on Brother U. Alfred's findings, the length "d" is one-fourth, one-half, or equal to the cycle length.

The residues beyond the first 0 were calculated by taking (-1) times the residues up to the first 0 and calculated that number mod p. This brought us to another interesting question. That is, how often do residues repeat for any f_n(mod p) given the cycle length?

Ratios:

Here, the ratio of distinct residues:cycle length was of great importance. The ratio of distinct residues to cycle length was computed for six digit primes and above. The following conjectures were verified:

(Note: Working with positive integers mod 20, the possible equivalence classes were {1,3,7,9,11,13,17,19}.)

Conjecture 1: If $p = 3,7 \bmod 20$ with maximal cycle length $(2p+2)$, then the ratio of residues:cycle length converges to 0.3750.

Conjecture 2: If $p = 11,19 \bmod 20$ with maximal cycle length $(p-1)$, the the ratio converges to 0.6250.

Conjecture 3: If $p = 13, 17 \bmod 20$ with maximal cycle length $(2p+2)$, then the ratio converges to 0.37.

Conjecture 4: If $p = 9 \bmod 20$ with maximal cycle length $(p-1)$, then the ratio converges to 0.6250.

Conjecture 5: If $p = 3,7,13,17 \bmod 20$ with cycle length $(2p+2)/3$, then the ratio converges to 0.45.

Conjecture 6: If $p = 3,7,13 \bmod 20$ with cycle length $(2p+2)/9$, then the ratio converges to 0.48.

Conjecture 7: If $p = 11,19 \bmod 20$ with cycle length $(p-1)/3$, then the ratio converges to 0.70.

Conjecture 8: If $p = 11 \bmod 20$ with cycle length $(p-1)/9$, then the ratio converges to 0.72.

(Note: Patterns were unclear for equivalence classes 1 and 9; more exploration and data is necessary to check convergence.)

Another method of computing ratios is to sample random six-digit plus primes, store 1000 successive residues, compute distince residues in this block, and compute the ratio. This may or may not verify the above conjectures.