**Homework #6**

**Due Wed Nov 5th**

**1)** Let A be the 2 by 2 matrix A = 1 1

1 0.

Let 0, 1, 1, 2, 3, 5, 8, 13, … be the Fibonacci numbers.

Then fn = 1 1 fn-1 = A fn-1

fn-1 1 0 fn-2 fn-2

Hence fn = An-1 f1

fn-1 f0

but f0 = 0, f1 = 1.

Hence fn = An-1 1

fn-1 0

**Theorem 1**

Let n be an odd prime. Let ϵ(n) = 1 if n ≡ ±1 (mod 5), and ϵ(n) = -1 if n ≡ ±2 (mod 5). Let ϵ(n) = 0 if n ≡ 0 (mod 5). Then fn-ϵ(n) ≡ 0 (mod n).

**(a)** Use the powers of the matrix A to verify theorem 1 for the primes 7919, 106 – 17, and 109 – 63. Use the recursive algorithm to compute Ak (mod n) at the end of Crypto notes #1.

**Definition**

A probable Fibonacci prime is an n that satisfies

fn-α(n) ≡ 0 (mod n),

where α(n) = J(5, n), where J(a, b) is the Jacobi symbol. Lecture notes B2 contains pseudocode for J(a, b).

**(b)** Find the smallest k such that 108 – k is a probable Fibonacci prime.

**Definition**

The Lucas sequences are {Uj} and {Vj} such that Uj = PUj-1 – QUj-2 and (U0, U1) = (0, 1), whereas Vj = PVj-1 – QVj-2 and (V0, V1) = (2, P).

**Theorem 2**

If n is an odd prime, and gcd(n, QΔ) = 1, then Un-δ(n) ≡ 0 (mod n), where δ(n) = J(Δ, n), where Δ is the discriminant Δ = P2 – 4Q which is assumed not to be a perfect square.

Let A be the 2 by 2 matrix B = P -Q

1 0.

We can express the Us using powers of B in a manner analogous to how the Fibonacci numbers can be calculated using powers of the matrix A.

Um = PUm-1 – QUm-2

Um = P -Q Um-1

Um-1 1 0 Um-2

Um = Bm-1 U1

Um-1  U0

Recall: (U0 , U1)= (0, 1).

**Definition**

We say that n is a probable Lucas prime if it satisfies theorem 2.

**2)** Find the smallest k such that 107 – k is a probable Lucas prime.

Again, use the pseudocode at the end of lecture note Crypto #1 to find the powers of the matrix B. Use P = 7 and Q =3. Then Δ = P2 – 4Q = 49 – 12 = 37, which is not a perfect square.