Math 105, Fall 2010, HW4

1. Suppose $n = 2^j k + 1$, where $j \geq 2$, $2^j > k$, and $3 \nmid k$. Show that n is prime if and only if $3^{(n-1)/2} \equiv -1 \pmod{n}$.

2. Prove the following generalization of the theorem of the Brillhart, Lehmer, Selfridge "$n-1$" theorem: Let $n > 1$ be an integer, suppose that $F \mid n-1$ with $F > \sqrt{n}$, and suppose that for each prime $q \mid F$ there is an integer a_q such that

$$a_q^{n-1} \equiv 1 \pmod{n}, \quad \gcd(a_q^{(n-1)/q} - 1, n) = 1.$$

   Then n is prime.

3. Let $m > 1$ be an integer and let $n = 2^{2^m} - 2^{2^{m-1}} + 1$. Prove that n is prime if and only if $7^{(n-1)/2} \equiv -1 \pmod{n}$.

4. Let f_n be the nth Fibonacci number. We've learned that if p is prime, then $f_{p-(p/5)} \equiv 0 \pmod{p}$. Say a composite integer n is a "Fibonacci pseudoprime" if $f_{n-(n/5)} \equiv 0 \pmod{n}$. Using standard properties of the Fibonacci sequence, show that 323 is a Fibonacci pseudoprime.

5. For a positive integer n let $F(n)$ be the number of integers $a \in [1, n]$ with $a^{n-1} \equiv 1 \pmod{n}$. Prove that

$$F(n) = \prod_{p \mid n} \gcd(p-1, n-1),$$

   where the product is over primes p that divide n. (A *Jeopardy* answer: What is the CRT?)

6. We know from algebra that if p is a prime number then $(\mathbb{Z}/p\mathbb{Z})[x]$ is a principal ideal ring. Show the converse. That is, if $n > 1$ is an integer and $(\mathbb{Z}/n\mathbb{Z})[x]$ is a principal ideal ring, then n is prime.