Homework 2

Problem 0. Shaunak's conjecture: Let $n \geq 1$. Prove that $5^n | F_{5^n}$. Hint: Use Binet's formula. Let $\gamma = \frac{1+\sqrt{5}}{2}$ and $\bar{\gamma} = \frac{1-\sqrt{5}}{2}$. Then $F_r = \frac{1}{\sqrt{5}}(\gamma^r - \bar{\gamma}^r)$. So you'll want to use the binomial expansion. Note that it follows from Proposition 3.2 (which you will use repeatedly in the homework below) that $5^n | F_{k5^n}$ for any positive integer k.

Remark. In the homework below, we will find three new ways of creating Fibonacci pseudoprimes that require primality testing but do not require factoring. These have the advantage of not requiring factoring, but have the disadvantage that these examples are much less dense than the examples from the method you've been working on.

Method 1 (not a homework problem): The smallest Fibonacci pseudoprime is $323 = 17 \cdot 19$. If p and $p+2$ are both primes then they are called *twin primes*. Let's generalize this example. If p and $p+2$ are both primes and $p \equiv 2 \bmod 5)$ then $p(p+2)$ is a Fibonacci pseudoprime. Fun fact: It is conjectured that there are infinitely many twin primes, but no one has proven it.

Problem 1.1. Prove the result in Method 1.

Problem 1.2. Write a program that searches through positive integers k that are $7 \pmod{10}$, tests whether k and $k+2$ are each prime (or each passes a probabilistic primality test), and then whether $k(k+2)$ is a base-2 pseudoprime.

Method 2: The second smallest Fibonacci pseudoprime is $377 = F_{14}$. Let's generalize this example. Let $p > 5$ be prime. Then F_{2p} is a Fibonacci pseudoprime. We will prove this result using several homework problems below.

Problem 2.1. Prove the following: Let $p > 5$ be prime. Then $F_{2p} \equiv (\frac{5}{p}) (\bmod p)$. Hints: Look at the proofs of Theorems 1.4 and 1.9 for the value of γ^{p-1} when $p \equiv \pm 1 (\text{mod } 5)$ and of γ^p and $\bar{\gamma}^p$ when $p \equiv \pm 2 (\bmod 5)$.

Problem 2.2. No need to write up a proof for this one. Just observe that it's true. If $n \equiv \pm 1, \pm 2 (\bmod 10)$ then $F_n \equiv \pm 1 (\bmod 5)$. If $n \equiv \pm 3, \pm 4 (\bmod 10)$ then $F_n \equiv \pm 2 (\bmod 5)$. Hint: If $a \equiv b (\bmod 40)$ then $F_a \equiv F_b (\bmod 5)$. So it suffices to check the statement for Fibonacci numbers with indices between 1 and 40.

Problem 2.3. Prove the following statements (yes - this is now easy): Let $p > 5$ be prime. If $p \equiv \pm 1 (\bmod 5)$, then $F_{2p} \equiv \pm 1 (\bmod 5)$. If $p \equiv \pm 2 (\bmod 5)$, then $F_{2p} \equiv \pm 2 (\bmod 5)$.

Problem 2.4. Prove the following statement. Let $p > 5$ be prime. Then $(\frac{5}{F_{2p}}) = (\frac{5}{p})$. Hints: Note that F_r is even if and only if $3|r$ (you need not prove this statement). Also Proposition 1.15.

Problem 2.5. Prove the following statement. Let $p > 5$ be prime. Then F_{2p} is a Fibonacci pseudoprime. Hint: Prove that $F_{2p} \equiv (\frac{5}{F_{2p}}) (\bmod 2p)$.

Problem 2.6. Write a program that searches through odd positive integers k and tests if k is prime (or passes a probabilistic primality test). If so, compute F_{2k}. Then test is F_{2k} is a base-2 pseudoprime.

Method 3: The fifth smallest Fibonacci pseudoprime is F_{19}. We can generalize this example. Let $p > 5$ be prime and F_p be composite. Then F_p is a Fibonacci pseudoprime. We will prove this result using the homework problems below.

Problem 3.1. Prove the following statement. Let $p > 5$ be prime. Then $F_p \equiv (\frac{5}{p}) (\bmod\, p)$. Hint: Use Binet's formula and the hints for Problem 2.1.

Problem 3.2. Prove the following statement. Let $p > 5$ be prime. Let $n = F_p$. Then $n | F_{n-(5/n)}$. Hint: Use Problem 2.2.

Problem 3.3. Write a program that searches through odd positive integers k and tests if k is prime (or passes a probabilistic primality test). If so, compute F_k and test if F_k is prime (or passes a probabilistic primality test). If not, then test if F_k is a base-2 pseudoprime.