Second Homework Assignment

Write the solution to each problem on a single page. The deadline for handing in solutions is February 6.

Question 1. ($20 = 10 + 10$ points). (Problem 2.1-12 in our textbook). We recall that a prime number, p, that divides a product of integers divides one of the two factors.

(a) Let $1 \leq a \leq p-1$. Use the above recollection to show that as b runs through the integers from 0 to $p-1$, the products $a \cdot_p b$ are all different.

(b) Explain why every positive integer less than p has a unique multiplicative inverse in $\mathbb{Z}_p$.

Question 2. (20 points). (Problem 2.2-19 in our textbook). The *least common multiple* of two positive integers i and j, denoted as $\mathrm{lcm}(i, j)$, is the smallest positive integer m such that m/i and m/j are both integer. Give a formula for $\mathrm{lcm}(i, j)$ that involves $\gcd(i, j)$.

Question 3. ($20 = 10 + 10$ points). (Problem 2.2-17 in our textbook). Recall the Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for all $i \geq 2$.

(a) Run the extended gcd algorithm for $j = F_{10}$ and $k = F_{11}$, showing the values of all parameters at all levels of the recursion.

(b) Running the extended gcd algorithm for $j = F_i$ and $k = F_{i+1}$, how many recursive calls does it take to get the result?

Question 4. (20 points). Let $n \geq 1$ be a nonprime and $x \in \mathbb{Z}_n$ such that $\gcd(x, n) \neq 1$. Prove that $x^{n-1} \bmod n \neq 1$.