Second Homework Assignment

Write the solution to each question on a single page.
The deadline for handing in solutions is 22 February 2010.

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 fac-
tors.

(a) Let $1 \leq a \leq p - 1$. Use the above recol-
lection to show that as $b$ runs through the
integers from 0 to $p - 1$, the products $a \cdot p \cdot b$
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 2.2-22 in our textbook).
Either find an equation of the form $a \cdot_n x = b$ in
$\mathbb{Z}_n$ that has a unique solution even though $a$ and
$n$ are not relatively prime, or prove that no such
equation exists. In other words, either prove the
statement that if $a \cdot_n x = b$ has a unique solution
in $\mathbb{Z}_n$, then $a$ and $n$ are relatively prime, or find
a counterexample.

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 $x^{n-1} \mod n \neq 1$.