1. Define* a sequence of numbers $F_n$ as follows:

$$F_0 = 1, \quad F_1 = 1$$

For any $n \geq 1$, $F_{n+1} = F_n + F_{n-1}$

So this sequence starts $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. This sequence is called the Fibonacci sequence, and the number $F_n$ is called the $n$th Fibonacci number. Prove that for all $n \in \mathbb{N}$, the number of steps required for the Euclidean Algorithm to compute $\gcd(F_n, F_{n+1})$ is exactly $n$. (*Hint: Induction*)

2. Let $a$ and $b$ be integers, not both 0, and let $g = \gcd(a, b)$. We know from Chapter 8 that the smallest positive element of $\mathcal{I}(a, b)$ is $g$. Prove that $\mathcal{I}(a, b)$ is the same as the set of all multiples of $g$. That is, prove that

$$\mathcal{I}(a, b) = \{kg \mid k \in \mathbb{Z}\}.$$

(*Hint: Recall from class that to prove two sets are equal, you usually need to do two smaller proofs: first show that $\mathcal{I}(a, b) \subseteq \{kg \mid k \in \mathbb{Z}\}$, then show that $\mathcal{I}(a, b) \supseteq \{kg \mid k \in \mathbb{Z}\}$.)

3. Let $a$ and $b$ be integers, not both zero, and let $k$ be a natural number. Prove that

$$\gcd(ka, kb) = k \cdot \gcd(a, b).$$

For any natural numbers $a$ and $b$, we define the least common multiple of $a$ and $b$, denoted $\text{lcm}(a, b)$, to be the smallest natural number that is a multiple of both $a$ and $b$. That is, saying that $m = \text{lcm}(a, b)$ means the following:

(i) $a \mid m$ and $b \mid m$.

(ii) For any $n \in \mathbb{N}$, if $a \mid n$ and $b \mid n$ then $m \leq n$.

The next three problems ask you to prove some basic facts about least common multiples. You should do these without using the Fundamental Theorem of Arithmetic.

4. Let $a$ and $b$ be natural numbers. Prove that if $a$ and $b$ are relatively prime, then $\text{lcm}(a, b) = ab$.

5. Prove that for any natural numbers $a$, $b$, and $k$,

$$\text{lcm}(ka, kb) = k \cdot \text{lcm}(a, b).$$

*The fact that this definition uses the previously defined $F_n$ and $F_{n-1}$ to define the next value, $F_{n+1}$, makes this an example of a recursive definition (also sometimes called an inductive definition, due to its relationship to proof by mathematical induction).*
6. Let $a$ and $b$ be natural numbers. Prove that

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$  

(Hint: There are a few ways to do this. Most of them start by using problem 3 from Homework 3. Perhaps the easiest proof is to combine that problem with the results of the previous two problems.)

7. The previous problem provides an easy way to compute the LCM of any two natural numbers, as long as you can compute their GCD... which we can do very efficiently. Use this to compute the least common multiple of each of the following pairs of numbers:

(a) 24 and 40
(b) 5754 and 7392
(c) 3134376 and 1759968

8. Let $a$ and $b$ be natural numbers. Recall from class that one way of writing their prime factorizations is

$$a = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot 7^{e_7} \cdots = \prod_{p \text{ prime}} p^{e_p}$$

$$b = 2^{f_2} \cdot 3^{f_3} \cdot 5^{f_5} \cdot 7^{f_7} \cdots = \prod_{p \text{ prime}} p^{f_p}$$

where the numbers $e_p$ and $f_p$ are nonnegative integers, only finitely many of which are not zero.

(a) Prove that $a \mid b$ if and only if $e_p \leq f_p$ for all prime numbers $p$.
(b) Find an expression for $\gcd(a, b)$ in terms of the prime factorizations of $a$ and $b$. Prove that your answer is correct.
(c) Find an expression for $\operatorname{lcm}(a, b)$ in terms of the prime factorizations of $a$ and $b$. Prove that your answer is correct.

9. Use the results of the previous exercise to compute the following:

(a) $\gcd(2^4 \cdot 3^8 \cdot 5^3 \cdot 19^1, 2^2 \cdot 3^3 \cdot 7^1 \cdot 11^2 \cdot 13^3)$
(b) $\operatorname{lcm}(2^3 \cdot 3^2 \cdot 5^9 \cdot 13^3, 2^5 \cdot 5^6 \cdot 7^4 \cdot 12^2 \cdot 17^1)$

10. Let $a$ and $b$ be natural numbers. Prove that if $a^2 \mid b^2$, then $a \mid b$.

11. Reduce each of the following. That is, compute the remainder when the expression is divided by the given modulus. (Remember, for a modulus $n$, this remainder should be between 0 and $n - 1$.)
12. Reduce each of the following. Again, for a modulus $n$, your answer should be between 0 and $n – 1$.
   (a) $1294 \cdot 29352 + 96273 \cdot 4751 \pmod{9}$
   (b) $84526 \cdot 862967^3 - 448184 \cdot 591183^2 \pmod{15}$

13. Compute each of the following inverses modulo $n$, or state that it doesn’t exist. Again, each answer should be between 0 and $n – 1$.
   (a) $3^{-1} \pmod{8}$
   (b) $16^{-1} \pmod{29}$
   (c) $14^{-1} \pmod{63}$
   (d) $1723^{-1} \pmod{4914}$

14. Solve each of the following for $x$. Note that your answer should not be a single number $x$, but rather a congruence relation: $x \equiv \_ \pmod{\_}$.
   (a) $3x \equiv 7 \pmod{8}$
   (b) $16x \equiv 6 \pmod{29}$
   (c) $1723x \equiv 3574 \pmod{4914}$