Practice Questions

1. Suppose Euclid's GCD algorithm is run with inputs F_{n+2} and F_{n+1} where F_i for an integer i is the i^{th} Fibonacci number. Show that the algorithm with these inputs takes at least n recursive calls.

2. Prove that

   (a) if $a \mid b$ and $b \mid c$ then $a \mid c$;

   (b) if $a \mid b$ and $c \mid d$ then $ac \mid bd$;

   (c) if $m \neq 0$, then $a \mid b$ if and only if $ma \mid mb$;

   (d) if $d \mid a$ and $a \neq 0$, then $|d| \leq |a|$.

3. Show that if $p > 1$ and p divides $(p-1)! + 1$, then p is prime.

4. Prove or give counterexample. Suppose $a, b \in \mathbb{N}$ and p is prime. If $gcd(a, p^2) = p$ and $gcd(b, p^2) = p$ then $gcd(ab, p^4) = p^2$.

5. Solve the following congruences.

   (a) $3x \equiv 5 \mod 7$

   (b) $12x \equiv 15 \mod 22$

   (c) $19x \equiv 42 \mod 50$

   (d) $18x \equiv 42 \mod 50$

   (e) $13x \equiv 71 \mod 380$

   (f) $7x \equiv 3 \mod 12$ and $10x \equiv 6 \mod 14$

   (g) $x \equiv 1 \mod 6, x \equiv 5 \mod 14$ and $x \equiv 4 \mod 21$.

6. If G is a group, then prove that $S \subseteq G$ is a subgroup if and only if for all $a, b \in S, ab^{-1} \in S$.

7. Let G be an abelian group. Let $H \subseteq G$ be a subgroup of G. For $a \in G$, define the left coset of H defined by a as $aH = \{ah : h \in H\}$. Define $G/H = \{aH : a \in G\}$. Note that each element in G/H is a set of the form aH.

   (a) Show that $a \in aH$.

   (b) Suppose $a' \in aH$, then $aH = a'H$.

   (c) Show that if $a' \in aH$ and $b' \in bH$, then $a'b'H = abH$.

   (d) Show that G/H with the multiplication defined by the above is an (abelian) group. This group is called the *Quotient Group* of G defined by H.

   (e) Show that the function $f : G \to G/H$ defined by $f(a) = aH$ is a homomorphism from G to G/H.

   (f) Consider $G = \mathbb{Z}$, the set of integers with addition, and $G' = \mathbb{Z}_n$, the mod n system with addition. For a natural number n, let $n\mathbb{Z} = \{in : i \in \mathbb{Z}\}$. Show that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. The quotient map $\mathbb{Z}/n\mathbb{Z}$ is the same as (isomorphic to) G'.

8. Let G, G' be abelian groups. Let $f : G \to G'$ be a homomorphism from G to G' (i.e., the map f satisfies $f(g_1 + g_2) = f(g_1) + f(g_2)$ for all $g_1, g_2 \in G$). Define $\ker(f) = \{g \in G : f(g) = 0\}$ and $\text{img}(f) = \{g' \in G' : g' = f(g) \text{ for some } g \in G\}$.

(a) Show that $\ker(f)$ and $\operatorname{img}(f)$ are subgroups of G and G' respectively.

(b) Show that f is injective if and only if $\ker(f) = \{0\}$ and f is surjective if and only if $\operatorname{img}(f) = G'$.

(c) Let $H = \ker(f)$. Consider the map $f : G/H \to \operatorname{img}(f)$ defined by $f(aH) = f(a)$. Show that the map is well-defined (i.e., show that if $aH = a'H$, then $f(aH) = f(a'H)$).

(d) Show that f is a homomorphism which is both injective and surjective, hence an isomorphism. This result is called the *first homomorphism theorem* for groups.

(e) Define $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(a) = a \mod n$. Show that f is a group homomorphism with respect to addition. What is $\ker(f)$? Apply the homomorphism theorem for this map and draw your conclusion.

9. For what integer values of m can there be a ring homomorphism from $\mathbb{Z}_{10}$ to $\mathbb{Z}_m$? Justify your answer.

10. Consider the map from $\mathbb{Z}_{24}$ to $\mathbb{Z}_4 \times \mathbb{Z}_6$ sending the element x in $\mathbb{Z}_{24}$ to the tuple $(x \mod 4, x \mod 6)$. Show that the map is a ring homomorphism.