Homework 2: Due Tuesday, September 8

Exercises

Exercise 1: Let $a, b, c \in \mathbb{Z}$. Using only the material through Section 2.4 (so without using the Fundamental Theorem of Arithmetic), show that the following are equivalent, i.e. prove that (1) implies (2) and also that (2) implies (1):

1. $\gcd(ab, c) = 1$.
2. $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

Exercise 2: Given $a \in \mathbb{Z}$, let $Mult(a) = \{n \in \mathbb{Z} : a \mid n\}$ be the set of multiples of a.
a. Show that for all $a, b \in \mathbb{Z}$, there exists a unique $m \in \mathbb{N}$ such that $Mult(a) \cap Mult(b) = Mult(m)$.
b. Let $a, b \in \mathbb{Z}$, and let m be the unique element of $\mathbb{N}$ given by part (a). Show that $a \mid m$, that $b \mid m$, and that if $n \in \mathbb{Z}$ is such that both $a \mid n$ and $b \mid n$, then $m \mid n$.
Note: For a given $a, b \in \mathbb{Z}$, the unique such m is called the *least common multiple* of a and b.

Exercise 3: Let A, B, C be sets and let $f \colon A \to B$ and $g \colon B \to C$ be functions.
a. Show that if $g \circ f$ is injective, then f is injective.
b. Show that if $g \circ f$ is surjective and g is injective, then f is surjective.

Problems

Problem 1: Let $a, b, c \in \mathbb{Z}$ with $a \geq 0$. Show that $\gcd(ab, ac) = a \cdot \gcd(b, c)$.
Aside: Think about why we have the assumption that $a \geq 0$ here. What would happen if $a < 0$?
Hint: Let $m = \gcd(b, c)$. Show directly that am satisfies the defining properties of $\gcd(ab, ac)$.

Problem 2: In this problem, we show how to use the existence of the gcd of two integers to prove the existence of the gcd of three integers (which can, of course, be further generalized). Let $a, b, c \in \mathbb{Z}$, and let $m = \gcd(a, \gcd(b, c))$.
a. Show that m divides each of a, b, and c.
b. Show that if d divides each of a, b, and c, then $d \mid m$.
c. Show that there exist $x, y, z \in \mathbb{Z}$ with $ax + by + cz = m$.

Problem 3: Let $S = \{2n : n \in \mathbb{Z}\}$ be the set of even integers. Notice that the sum and product of two elements of S is still an element of S. Call an element $a \in S$ *irreducible* if $a > 0$ and there is no way to write $a = bc$ with $b, c \in S$. Notice that 6 is irreducible in S (because there is no way to write 6 as a product of two even numbers) even though it is not prime in $\mathbb{Z}$.
a. Give a characterization (with proof) of the irreducible elements of S.
b. Show that the analogue of Fundamental Theorem of Arithmetic fails in S by finding a positive element of S which does *not* factor uniquely (up to order) into irreducibles.

Problem 4: Let $A = \mathbb{N}^+$ and define $a \sim b$ to mean that there exists $n \in \mathbb{Z}$ with $a = 2^n b$.
a. Show that $\sim$ is an equivalence relation on A.
b. Characterize (with proof) which elements of A are the smallest elements of their equivalence class. In other words, find a simple characterization of the set $\{a \in A : a \leq b \text{ for all } b \in A \text{ with } a \sim b\}$.

Problem 5: Let Q and P be defined as in Section 3.5 of the notes. Thus, Q is the set of equivalence classes of the set $\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$ under the equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$, and P is the set of equivalence classes of the set $\mathbb{R}^2 \backslash \{(0, 0)\}$ under the equivalence relation $(x_1, y_1) \sim (x_2, y_2)$ if there exists a real number $\lambda \neq 0$ with $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Determine which of the following functions on equivalence classes are well-defined. In each case, <u>either</u> give a proof or a specific counterexample.

a. $f : Q \to \mathbb{Z}$ defined by $f(\overline{(a, b)}) = a - b$.

b. $f : Q \to Q$ defined by $f(\overline{(a, b)}) = \overline{(a^2 + 3ab + b^2, 5b^2)}$.

c. $f : P \to \mathbb{R}$ defined by

$$f(\overline{(x, y)}) = \frac{2xy^3 + 5xy}{x^4 + y^4}$$

d. $f : P \to P$ defined by $f(\overline{(x, y)}) = \overline{(x^3 + 5xy^2, y^3)}$.