MATH 113 HOMEWORK 2
DUE MONDAY, JULY 6TH

1. Basic Problems

Divisibility.

Problem 1.1. Let a and b be integers and let n be a natural number. Let $d = \gcd(a, n)$. Show that the equation

$$ax \equiv b (\text{mod } n)$$

has a solution if and only if $d|b$.

Problem 1.2. Do Judson, Ch. 2 Additional Exercises 1-4 (you can skip the programming exercise 1(e)). These are the exercises on UPC symbols and ISBN codes.

Groups and Subgroups.

Problem 1.3. Let $(G, \circ)$ and $(H, \star)$ be two groups. Define the *direct product* $(G, \circ) \times (H, \star)$ to be the set $G \times H$ with the operation $(g_1, h_1)(g_2, h_2) = (g_1 \circ g_2, h_1 \star h_2)$. Show that this operation makes $G \times H$ into a group. We often write $G \times H$ for $(G, \circ) \times (H, \star)$ when the operations $\circ$ and $\star$ are understood.

Problem 1.4. Do Judson, Ch. 2 Exercises 10, 16, 17, 32, 39, and 52.

Problem 1.5. Define an equivalence relation $\sim$ on $\mathbb{Q}$ by $a \sim b$ if $a - b \in \mathbb{Z}$. We write $\mathbb{Q}/\mathbb{Z}$ for $\mathbb{Q}/\sim$. Show that:

(1) The relation $\sim$ is in fact an equivalence relation.
(2) If $a, b \in \mathbb{Q}$ and $0 \leq a < b < 1$, then $[a] \neq [b]$. Conclude that $\mathbb{Q}/\mathbb{Z}$ is infinite.
(3) The operation $+$ on $\mathbb{Q}/\mathbb{Z}$ defined by $[a] + [b] = [a + b]$ is well-defined.
(4) $(\mathbb{Q}/\mathbb{Z}, +)$ is an abelian group.
(5) Every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. More specifically, if $a/b \in \mathbb{Q}$ is a proper fraction in lowest terms, calculate the order of $[a/b]$ in $\mathbb{Q}/\mathbb{Z}$.
(6) The operation $\cdot$ on $\mathbb{Q}/\mathbb{Z}$ defined by $[a] \cdot [b] = [a \cdot b]$ is *not* well-defined.

Problem 1.6. Let G be a group with identity e and suppose that $a^2 = e$ for all $a \in G$. Show that G is abelian.

Cyclic Groups and Subgroups.

Problem 1.7. Do Judson, Ch.3 Exercises 4, 5, 6, 9.

Problem 1.8. Let a and b be integers. Show that $H = \{na+mb \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. This is called the *subgroup generated by* a and b. Since $\mathbb{Z}$ is cyclic, H must also be cyclic. Find the generator of H in terms of a and b (with proof!).

Problem 1.9. Prove or disprove: the group $(\mathbb{Q}, +)$ is cyclic.

2. Creative Problems

Problem 2.1. Do Judson Ch.3 Exercise 13.

Problem 2.2. Let $(G, \circ)$ be an abelian group. We say a subgroup H of G is *generated by two elements* if there exist elements $g, h \in H$ such that every element of H can be written in the form $g^n h^m$ for some integers n and m. Investigate the subgroups of $(\mathbb{Q}, +)$ which are generated by two elements. Compute a few examples and make some conjectures. Try to prove your conjectures.

3. Challenge Problem

Problem 3.1. Show that $(\mathbb{Q}/\mathbb{Z}, +)$ has a subgroup H with the following two properties:

(1) H is infinite.
(2) Every proper subgroup of H is finite.