Math 230 **Fall 2018**
Homework 5 **Drew Armstrong**

Problem 1. In this problem you will give another proof that $\sqrt{d} \notin \mathbb{Z} \Rightarrow \sqrt{d} \notin \mathbb{Q}$ for all $d \in \mathbb{Z}$. The key is to use unique prime factorization. For all $n, p \in \mathbb{Z}$ with p prime we will write $p^k \| n$ to mean that $p^k | n$ and $p^{k+1} \nmid n$.

(a) If $d \in \mathbb{Z}$ and $\sqrt{d} \notin \mathbb{Z}$, prove that we have $p^k \| d$ for some prime p and **odd** integer k.
(b) Assume that we have $\sqrt{d} = a/b$, and hence $a^2 = db^2$, for some $a, b \in \mathbb{Z}$. Derive a contradiction by considering the multiplicity of p on both sides.

Problem 2. In this problem you will use induction to generalize Euclid's lemma. Let $p \in \mathbb{Z}$ be prime and for all integers $n \geq 1$ consider the following statement:

$$P(n) = \text{“for all integers } a_1, \ldots, a_n \in \mathbb{Z} \text{ we have } p|(a_1 a_2 \cdots a_n) \Rightarrow (p|a_i \text{ for some } i).\text{”}$$

(a) Explain why $P(2)$ is a true statement.
(b) Assume for induction that $P(n)$ is a true statement. In this case, prove that $P(n+1)$ is also a true statement.

Problem 3. In this problem you will give Euclid's proof that there exist infinitely many prime numbers. Assume for contradiction that there exist only **finitely** many prime numbers, and call them

$$1 < p_1 < p_2 < p_3 < \cdots < p_k.$$

Now consider the number $N := p_1 p_2 \cdots p_k + 1$. You know from HW4 Problem 4 that there exists a prime number $p \in \mathbb{Z}$ such that $p|N$. On the other hand, prove that $p \neq p_i$ for all i. This is a contradiction.

Problem 4. Let $\sim$ be an equivalence relation on a set S and for each element $x \in S$ let $[x] := \{y \in S : x \sim y\} \subseteq S$ be its equivalence class. For all $x, y \in S$ prove that the following three statements are equivalent:

(1) $x \sim y$,
(2) $[x] = [y]$,
(3) $[x] \cap [y] \neq \emptyset$.

[Hint: You need to prove some cycle. I recommend (1)⇒(2)⇒(3)⇒(1).]

Problem 5. Fix a nonzero integer $n \in \mathbb{Z}$ and recall that $[a]_n = [b]_n$ means $n|(a-b)$. Now assume for some $a, b, a', b' \in \mathbb{Z}$ that $[a]_n = [a']_n$ and $[b]_n = [b']_n$. In this case prove that

$$[a+b]_n = [a'+b']_n \qquad \text{and} \qquad [ab]_n = [a'b']_n.$$

In other words: The addition and multiplication of integers mod n is “well-defined.”