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.

Proof. Suppose that $d \in \mathbb{Z}$ and $\sqrt{d} \notin \mathbb{Z}$.

(a) Consider the prime factorization of d:

$$d = p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots .$$

If every exponent is even, say $d_i = 2k_i \geq 0$ for some $k_i \geq 0$, then we have

$$\sqrt{d} = \left(p_1^{2k_1} p_2^{2k_2} p_3^{2k_3} \cdots\right)^{1/2} = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots \in \mathbb{Z}.$$

But this contradicts the fact that $\sqrt{d} \notin \mathbb{Z}$. Hence there must exist some i such that d_i is odd.

(b) Now assume for contradiction that $\sqrt{d} \in \mathbb{Q}$, say $\sqrt{d} = a/b$ for some $a, b \in \mathbb{Z}$. Consider the prime factorizations:

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots ,$$
$$b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots .$$

Multiplying both sides of $\sqrt{d} = a/b$ by b and then squaring gives

$$\begin{aligned} a^2 &= db^2 \\ (p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots)^2 &= \left(p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots\right)\left(p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots\right)^2 \\ p_1^{2a_1} p_2^{2a_2} p_3^{2a_3} \cdots &= p_1^{d_1+2b_1} p_2^{d_2+2b_2} p_3^{d_3+2b_3} \cdots \end{aligned}$$

By uniqueness of prime factorization this implies that $2a_i = d_i + 2b_i$ for all i, and in particular that $d_i = 2a_i - 2b_i = 2(a_i - b_i)$ is even for all i. This contradicts part (a). □

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.

(a) The statement $P(2)$ says that

“ for all integers $a, b \in \mathbb{Z}$ we have $p|(ab) \Rightarrow (p|a$ or $p|b)$. ”

This is called Euclid's Lemma. We already know that it is true.

(b) Now fix some $n \geq 2$ and assume for induction that $P(n)$ is a true statement. In this case we want to prove that $P(n+1)$ is a true statement. To be specific, we will prove that for any $n+1$ integers $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$ we have

$$p|(a_1 a_2 \cdots a_{n+1}) \quad \Longrightarrow \quad \exists i \in \{1, 2, \ldots, n+1\}, p|a_i.$$

Proof. So consider any integers $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$ and assume that

$$p|(a_1 a_2 \cdots a_{n+1}).$$

Then from $P(2)$ we have

$$p|(a_1 \cdots a_n)a_{n+1} \Longrightarrow p|(a_1 \cdots a_n) \text{ or } p|a_{n+1}.$$

If $p|a_{n+1}$ then we are done, so let us assume that $p|(a_1 \cdots a_n)$. Then since $P(n)$ is true we conclude that $p|a_i$ for some $i \in \{1, 2, \ldots, n\}$. In summary, we have shown that

$$(p|a_1 \text{ or } p|a_2 \text{ or } \cdots \text{ or } p|a_n) \text{ or } p|a_{n+1}.$$

In other words, there exists some $i \in \{1, 2, \ldots, n+1\}$ such that $p|a_i$. □

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.

Proof. Assume for contradiction that there exist only **finitely** many prime numbers, called

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

Now consider the number $N := p_1 p_2 \cdots p_k + 1$. We know from HW4 Problem 4 that there exists some prime p such that $p|N$. By assumption, this prime must be in the set $\{p_1, \ldots, p_k\}$. In other words, we must have $p = p_i$ for some $i \in \{1, 2, \ldots, k\}$. But then we have

- $p|N$ and
- $p|(p_1 \ldots p_k)$,

which implies that p divides 1:

$$p|\left(N - p_1 \cdots p_k\right) = 1.$$

This contradicts the fact that p is prime. (Recall that ± 1 are not prime numbers.) □

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).]

Our proof will use the three axioms of equivalence:

(E1) $\forall x \in S, x \sim x$,
(E2) $\forall x, y \in S, x \sim y \Rightarrow y \sim x$,

(E3) $\forall x, y, z \in S, (x \sim y \wedge y \sim z) \Rightarrow x \sim z$.

Proof. (1)$\Rightarrow$(2): Assume that $x \sim y$. We will prove that $[x] \subseteq [y]$ and $[y] \subseteq [x]$.

- To see that $[x] \subseteq [y]$, consider any $z \in [x]$. By definition this means that $x \sim z$, and hence $z \sim x$ from (E2). Then since $z \sim x$ and $x \sim y$ we have $z \sim y$ from (E3) and then $y \sim z$ from (E2). It follows that $z \in [y]$.
- To see that $[y] \subseteq [x]$, consider any $z \in [y]$. By definition this means that $y \sim z$. Then since $x \sim y$ and $y \sim z$ we have $x \sim z$ from (E3), and hence $z \in [x]$.

(2)$\Rightarrow$(3). Assume that $[x] = [y]$. We will prove that $[x] \cap [y] \neq \emptyset$. But note that

$$[x] \cap [y] = [x] \cap [x] = [x]$$

and this set is not empty because $x \in [x]$ from (E1).

(3)$\Rightarrow$(1). Assume that $[x] \cap [y] \neq \emptyset$, so there exists some $z \in [x] \cap [y]$. We will show that $x \sim y$. Indeed, since $[x] \cap [y] \subseteq [x]$ we have $z \in [x]$ and hence $x \sim z$. Similarly, since $[x] \cap [y] \subseteq [y]$ we have $z \in [y]$, hence $y \sim z$ and (E2) gives $z \sim y$. Finally, since $x \sim z$ and $z \sim y$ we have $x \sim y$ from (E3). $\square$

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."

Proof. Assume that $[a]_n = [a']_n$ and $[b]_n = [b']_n$. By definition this means that

$$a - a' = nk \quad \text{and} \quad b - b' = n\ell$$

for some $k, \ell \in \mathbb{Z}$. Then we have

$$(a + b) - (a' + b') = (a - a') + (b - b') = nk + n\ell = n(k + \ell),$$

which implies that $[a + b]_n = [a' + b']_n$, and we have

$$\begin{aligned} ab - a'b' &= ab - (a - nk)(b - n\ell) \\ &= \cancel{ab} - \cancel{ab} + an\ell + bnk - n^2 k\ell \\ &= n(a\ell + bk - nk\ell), \end{aligned}$$

which implies that $[ab]_n = [a'b']_n$. $\square$