Math 230 D **Fall 2015**
Homework 5 **Drew Armstrong**

Problem 1. Multiplicative Cancellation in $\mathbb{Z}$. Many times we've used the fact that the integers have multiplicative cancellation, but we never proved it. Let's prove it now.

(a) Prove that for all integers $a, b \in \mathbb{Z}$ we have

$$(ab = 0) \Rightarrow (a = 0 \text{ or } b = 0).$$

[Hint: You can assume the following two facts: (1) For all $x, y, z \in \mathbb{Z}$, $(x < y \text{ and } 0 < z) \Rightarrow (xz < yz)$. (2) For all $x, y, z, \in \mathbb{Z}$, $(x < y \text{ and } z < 0) \Rightarrow (yz < xz)$. Now there are four cases.]

(b) Use the result of part (a) to prove that for all integers $a, b, c \in \mathbb{Z}$ we have

$$(ab = ac \text{ and } a \neq 0) \Rightarrow (b = c).$$

Proof. For part (a) we will prove the contrapositive statement, that if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$. The proof will use the fact that $0n = 0$ for all $n \in \mathbb{Z}$ so first let me recall the proof of this fact. We have

$$\begin{aligned} (0+0)n &= 0n && \text{(A3)} \\ 0n + 0n &= 0n && \text{(D)} \\ 0n + \cancel{0n} &= 0 + \cancel{0n} && \text{(A3)} \\ 0n &= 0. && \text{(additive cancellation)} \end{aligned}$$

Now consider any $a, b \in \mathbb{Z}$ and assume that $a \neq 0$ and $b \neq 0$. There are four cases.

Case 1: If $a > 0$ and $b > 0$ then we have

$$\begin{aligned} a &> 0, && \text{(assumption)} \\ ab &> 0b, && \text{(1)} \\ ab &> 0, && \text{(above)} \end{aligned}$$

hence $ab \neq 0$.

Case 2: If $a > 0$ and $b < 0$ then we have

$$\begin{aligned} a &> 0, && \text{(assumption)} \\ ab &< 0b, && \text{(2)} \\ ab &< 0, && \text{(above)} \end{aligned}$$

hence $ab \neq 0$.

Case 3: If $a < 0$ and $b > 0$ then we have

$$\begin{aligned} a &< 0, && \text{(assumption)} \\ ab &< 0b, && \text{(1)} \\ ab &< 0, && \text{(above)} \end{aligned}$$

hence $ab \neq 0$.

Case 4: If $a < 0$ and $b < 0$ then we have

$$\begin{aligned} a &< 0, && \text{(assumption)} \\ ab &> 0b, && (2) \\ ab &> 0, && \text{(above)} \end{aligned}$$

hence $ab \neq 0$.

This completes the proof of (a). For part (b) consider integers $a, b, c \in \mathbb{Z}$ such that $ab = ac$ and $a \neq 0$. Then we have

$$\begin{aligned} ab &= ac, \\ ab - ac &= 0, \\ a(b-c) &= 0. \end{aligned}$$

If $b - c \neq 0$ then since $a \neq 0$ part (a) would imply $a(b-c) \neq 0$. Contradiction. We conclude that $b - c = 0$, hence $b = c$ as desired. □

[Remark: Multiplicative cancellation is a fairly subtle property of the integers, involving the interplay of the axioms of addition, multiplication, and order. I guess we could short-circuit this proof by taking multiplicative cancellation as an axiom, but it's typically not done that way. If you study more abstract algebra you will find that a ring with multiplicative cancellation is called an "integral domain".]

Problem 2. Multiplicative Cancellation in $\mathbb{Z}/n$. Fix a nonzero integer $n \in \mathbb{Z}$ and consider the following set of abstract symbols

$$\mathbb{Z}/n := \{[a]_n : a \in \mathbb{Z}\}.$$

We define "equality" of symbols by $([a]_n = [b]_n) \Leftrightarrow (n|(a-b))$ (we proved in class that this is an equivalence relation), "addition" of symbols by $[a]_n + [b]_n := [a+b]_n$ and "multiplication" of symbols by $[a]_n \cdot [b]_n := [ab]_n$.

(a) Prove that addition and multiplication of symbols is well-defined. That is, if $[a]_n = [b]_n$ and $[c]_n = [d]_n$ prove that we must have $[a]_n + [c]_n = [b]_n + [d]_n$ and $[a]_n \cdot [c]_n = [b]_n \cdot [d]_n$.

(b) One can check (but please don't) that $\mathbb{Z}/n$ satisfies the first eight axioms of $\mathbb{Z}$ with additive identity element $[0]_n \in \mathbb{Z}/n$ and multiplicative identity element $[1]_n \in \mathbb{Z}/n$. Prove that the element $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. [Hint: Recall that $(\gcd(a, n) = 1) \Leftrightarrow (\exists x, y \in \mathbb{Z}, ax + ny = 1)$.]

(c) Additive cancellation in $\mathbb{Z}/n$ works exactly as in $\mathbb{Z}$, but multiplicative cancellation is more complicated. Prove that the following statement is true for all $[b]_n, [c]_n \in \mathbb{Z}/n$ **if and only if** $\gcd(a, n) = 1$:

$$([a]_n \cdot [b]_n = [a]_n \cdot [c]_n) \Rightarrow ([b]_n = [c]_n).$$

Proof. For part (a) assume that we have $[a]_n = [b]_n$ and $[c]_n = [d]_n$. In other words, there exist integers $k, \ell \in \mathbb{Z}$ such that $a - b = nk$ and $c - d = n\ell$. In this case we want to prove that $[a]_n + [c]_n = [b]_n + [d]_n$ (that is, $[a+c]_n = [b+d]_n$) and $[a]_n \cdot [c]_n = [b]_n \cdot [d]_n$ (that is, $[ac]_n = [bd]_n$). For the first statement note that

$$\begin{aligned} (a+c) - (b+d) &= (a-b) + (c-d) \\ &= nk + n\ell \\ &= n(k+\ell), \end{aligned}$$

which implies that $[a+c]_n = [b+d]_n$ as desired. For the second statement note that

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + b(c-d) \\ &= nkc + bn\ell \\ &= n(kc + b\ell), \end{aligned}$$

which implies that $[ac]_n = [bd]_n$ as desired.

For part (b), first assume that $\gcd(a,n) = 1$. Then by Bézout's Identity there exist integers $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Reducing this equation mod n gives

$$\begin{aligned} [ax + ny]_n &= [1]_n \\ [a]_n \cdot [x]_n + [n]_n \cdot [y]_n &= [1]_n \\ [a]_n \cdot [x]_n + [0]_n \cdot [y]_n &= [1]_n \\ [a]_n \cdot [x]_n + [0]_n &= [1]_n \\ [a]_n \cdot [x]_n &= [1]_n, \end{aligned}$$

hence $[x]_n$ is a multiplicative inverse of $[a]_n$ as desired. Conversely, assume that there exists $[x]_n \in \mathbb{Z}/n$ such that $[a]_n \cdot [x]_n = [1]_n$. Since $[ax]_n = [1]_n$, there exists $k \in \mathbb{Z}$ such that $ax - 1 = nk$, and hence $ax + n(-k) = 1$. We have proved on multiple occasions that this last equation implies $\gcd(a,n) = 1$.

Now fix an integer a and consider two statements $P =$ "$\gcd(a,n) = 1$" and $Q =$"for all $b, c \in \mathbb{Z}$ we have $([a]_n \cdot [b]_n = [a]_n \cdot [c]_n) \Rightarrow ([b]_n = [c]_n)$". First we will prove that $P \Rightarrow Q$. So assume that $\gcd(a,n) = 1$. By part (b) there exists $x \in \mathbb{Z}$ such that $[a]_n \cdot [x]_n = [1]_n$. Now consider any $b, c \in \mathbb{Z}$ and assume that $[a]_n \cdot [b]_n = [a]_n \cdot [c]_n$. Multiplying both sides by $[x]_n$ gives

$$\begin{aligned} [a]_n \cdot [b]_n &= [a]_n \cdot [c]_n \\ [a]_n \cdot [x]_n \cdot [b]_n &= [a]_n \cdot [x]_n \cdot [c]_n \\ [1]_n \cdot [b]_n &= [1]_n \cdot [c]_n \\ [b]_n &= [c]_n, \end{aligned}$$

as desired. Next we want to show that $Q \Rightarrow P$. This is hard to do so instead we'll prove the contrapositive statement $\neg P \Rightarrow \neg Q$. So assume that $\gcd(a,n) = d \neq 1$. In this case we want to show that **there exist** integers $b, c \in \mathbb{Z}$ such that $[a]_n \cdot [b]_n = [a]_n \cdot [c]_n$ and $[b]_n \neq [c]_n$. (Check that this is indeed the opposite of the statement Q. Aren't you glad we studied logic earlier?) Since d is a common divisor of a and n we have $a = da'$ and $n = dn'$ for some integers $a', n' \in \mathbb{Z}$. Then we have

$$\begin{aligned} [a]_n \cdot [n']_n &= [an']_n \\ &= [(da')n']_n \\ &= [a'(dn')]_n \\ &= [a'n]_n \\ &= [a']_n \cdot [n]_n \\ &= [a']_n \cdot [0]_n \\ &= [0]_n \\ &= [a]_n \cdot [0]_n. \end{aligned}$$

But I claim that $[n']_n \neq [0]_n$. Indeed, if $[n']_n = [0]_n$ then we have $n' = nk$ for some $k \in \mathbb{Z}$ and hence $n = dn' = d(nk') = n(dk')$. Now since $n \neq 0$, Problem 1(b) implies that $1 = dk'$ and hence $d = 1$. Contradiction. Thus we can define $b = n'$ and $c = 0$. □

[Remark: The proof that $Q \Rightarrow P$ was a little (okay, a lot) tricky. The trick was finding a counterexample to cancellation for **each pair** of a and n such that $\gcd(a, n) \neq 1$. The grader will award full points if you provide a counterexample for **one specific pair** of a and n. I gave the example $[2]_6 \cdot [5]_6 = [2]_6 \cdot [2]_6$ in class.]

Problem 3. Induction Practice. Use induction to prove that for all integers $n \geq 1$ the following statement holds:

> "For any n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that $[a_i]_4 = [1]_4$ for all $i \in \{1, 2, \ldots, n\}$, it follows that $[a_1 a_2 \cdots a_n]_4 = [1]_4$."

[Hint: Call the statement $P(n)$. Verify that $P(1)$ is true. Now fix an integer $k \geq 1$ and **assume for induction** that $P(k)$ is true. In this case, prove that $P(k + 1)$ is also true.]

Proof. First note that the statement $P(1)$ is true. Indeed, given an integer $a_1 \in \mathbb{Z}$ such that $[a_1]_4 = [1]_4$, it does follow that $[a_1]_4 = [1]_4$.

Now fix an integer $k \geq 1$ and assume for induction that $P(k)$ is true. That is, assume that for any k integers $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ such that $[a_i]_4 = [1]_4$ for all $i \in \{1, 2, \ldots, k\}$, it follows that $[a_1 a_2 \cdots a_k]_4 = [1]_4$. In this hypothetical case we will show that the statement $P(k + 1)$ is also true. So consider any $k + 1$ integers $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$ such that $[a_i]_4 = [1]_4$ for all $i \in \{1, 2, \ldots, k + 1\}$. We want to show that $[a_1 a_2 \cdots a_{k+1}]_4 = [1]_4$. Indeed, we have

$$\begin{aligned}
[a_1 a_2 \cdots a_{k+1}]_4 &= [(a_1 a_2 \cdots a_k) a_{k+1}]_4 \\
&= [a_1 a_2 \cdots a_k]_4 \cdot [a_{k+1}]_4 \\
&= [a_1 a_2 \cdots a_k]_4 \cdot [1]_4 && \text{(assumption)} \\
&= [1]_4 \cdot [1]_4 && \text{(induction hypothesis)} \\
&= [1]_4,
\end{aligned}$$

and hence $P(k + 1)$ is true.

In summary, we have shown that

- $P(1)$ is true.
- For all $k \geq 1$, $P(k) \Rightarrow P(k + 1)$.

Therefore, the Principle of Induction says that $P(n)$ is true for all $n \geq 1$. □

Problem 4. Generalization of Euclid's Proof of Infinite Primes.

(a) Consider an integer $n \in \mathbb{Z}$ such that $|n| > 1$. Prove that if $[n]_4 = [3]_4$ then n has a prime factor $p|n$ such that $[p]_4 = [3]_4$. [Hint: You can assume (from the FTA) that n is a product of primes. By the Division Theorem, every prime number p must satisfy $p = 2$, $[p]_4 = [1]_4$, or $[p]_4 = [3]_4$. Use Problem 3.]

(b) Prove that there are infinitely many positive prime numbers p such that $[p]_4 = [3]_4$. [Hint: Assume that there are only **finitely many** and call them $3 < p_1 < p_2 < \cdots < p_n$. Now consider the number $N := 4p_1 p_2 \cdots p_n + 3$. Since $[N]_4 = [3]_4$, part (a) says that there exists a prime $p|N$ such that $[p]_4 = [3]_4$. Show that this leads to a contradiction.]

Proof. For part (a), consider $n \in \mathbb{Z}$ such that $|n| > 1$ and $[n]_4 = [3]_4$. The Fundamental Theorem of Arithmetic says that $n = p_1 p_2 \cdots p_k$ for some primes $p_1, p_2, \ldots, p_k$. We want to prove that there exists $i \in \{1, 2, \ldots, k\}$ such that $[p_i]_4 = [3]_4$. Note that $[n]_4 = [3]_4$ implies that n is **odd**, so none of its prime factors is 2. This means that for each $i \in \{1, 2, \ldots, k\}$ we have either $[p_i]_4 = [1]_4$ or $[p_i]_4 = [3]_4$. Assume for contradiction that we have $[p_i]_4 = [1]_4$ for all $i \in \{1, 2, \ldots, k\}$. Then by Problem 3 we conclude that

$$[n]_4 = [p_1 p_2 \cdots p_k]_4 = [1]_4,$$

which contradicts the fact that $[n]_4 = [3]_4$. We conclude that there exists $i \in \{1, 2, \ldots, k\}$ such that $[p_i]_4 = [3]_4$, as desired.

For part (b), assume for contradiction that there exist only finitely many primes p such that $[p]_4 = [3]_4$. Let's name them:

$$3 < p_1 < p_2 < p_3 < \cdots < p_n.$$

[So we have $p_1 = 7$, $p_2 = 11$, $p_3 = 19$, $p_4 = 23$, etc. The key assumption is that this list stops at some point.] Now, following Euclid's famous trick, we will define the integer

$$N := 4p_1 p_2 \cdots p_n + 3.$$

Since $[N]_4 = [3]_4$, part (a) implies that there exists a prime p such that $p|N$ and $[p]_4 = [3]_4$. Since p is a prime of the form $[3]_4$ it must be in our list. That is, we must have $p \in \{3, p_1, p_2, \ldots, p_n\}$. I claim that $p \neq 3$. Indeed, if $p = 3$ then we have $3|N$ and hence

$$3|(N - 3) = 4p_1 p_2 \cdots p_n.$$

By Euclid's Lemma this implies that $3|4$, which is false, or $3|p_i$ for some $i \in \{1, 2, \ldots, n\}$, which is also false because each p_i is a prime number not equal to 3. /// Therefore we must have $p = p_i$ for some $i \in \{1, 2, \ldots, n\}$. Since $p|N$ this implies that $p_i|N$. But we also know that $p_i|4p_1 p_2 \cdots p_n$, and hence

$$p_i|(N - 4p_1 p_2 \cdots p_n) = 3.$$

But this is a contradiction because $3 < p_i$.

We conclude that our original assumption — that there are only finitely many primes p such that $[p]_4 = [3]_4$ — is false. □

[Remark: It is also true that there exist infinitely many primes p such that $[p]_4 = [1]_4$ but this is quite a bit harder to prove. Give it a try if you want a challenge. More generally, if we fix $a, n \in \mathbb{Z}$ such that $\gcd(a, n) = 1$ then there exist infinitely many primes p such that $[p]_n = [a]_n$. This famous theorem was proved by Gustav Lejeune Dirichlet in 1837. His proof uses complex analysis and is way beyond the scope of this course. Number theory is full of problems that are easy to state but hard/impossible to prove.]