Math 230 D **Fall 2015**
Homework 4 **Drew Armstrong**

Problem 1. Rational Numbers. We have used the rational numbers a lot but we never defined them. Now we will. For all integers $a, b \in \mathbb{Z}$ with $b \neq 0$ we define an abstract symbol $[a, b]$. Let $\mathbb{Q}$ be the set of all these symbols:

$$\mathbb{Q} := \{[a, b] : a, b \in \mathbb{Z} \text{ with } b \neq 0\}.$$

We will "multiply" and "add" abstract symbols as follows:

$$[a, b] \cdot [c, d] = [ac, bd] \quad \text{and} \quad [a, b] + [c, d] = [ad + bc, bd].$$

Finally, we declare that $[a, b] = [c, d]$ if and only if $ad = bc$.

(a) Prove that the sum and product of abstract symbols is well-defined. That is, if $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$, prove that we have

$$[a_1, b_1] \cdot [c_1, d_1] = [a_2, b_2] \cdot [c_2, d_2] \quad \text{and} \quad [a_1, b_1] + [c_1, d_1] = [a_2, b_2] + [c_2, d_2].$$

(b) One can check that $\mathbb{Q}$ satisfies all of the axioms of $\mathbb{Z}$ except for the Well-Ordering Axiom (please don't check this), with additive identity $[0, 1] \in \mathbb{Q}$ and multiplicative identity $[1, 1] \in \mathbb{Q}$. But $\mathbb{Q}$ has one crucial advantage over $\mathbb{Z}$: **Prove** that every nonzero element of $\mathbb{Q}$ has a multiplicative inverse.

Proof. For part (a), assume that we have $[a_1, b_1], [a_2, b_2], [c_1, d_1], [c_2, d_2] \in \mathbb{Q}$ such that $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$. In other words, we have integers $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$ with $b_1, b_2, d_1, d_2 \neq 0$, such that $a_1 b_2 = a_2 b_1$ and $c_1 d_2 = c_2 d_1$. In this case we want to prove that

(1) $[a_1, b_1] \cdot [c_1, d_1] = [a_2, b_2] \cdot [c_2, d_2]$, and
(2) $[a_1, b_1] + [c_1, d_1] = [a_2, b_2] + [c_2, d_2]$.

To prove (1), note that we are being asked to show that $[a_1 c_1, b_1 d_1] = [a_2 c_2, b_2 d_2]$; in other words, that $(a_1 c_1)(b_2 d_2) = (a_2 c_2)(b_1 d_1)$. And this is certainly true because

$$\begin{aligned}(a_1 c_1)(b_2 d_2) &= (a_1 b_2)(c_1 d_2) \\ &= (a_2 b_1)(c_2 d_1) \\ &= (a_2 c_2)(b_1 d_1).\end{aligned}$$

To prove (2), note that we are being asked to show that $[a_1 d_1 + b_1 c_1, b_1 d_1] = [a_2 d_2 + b_2 c_2, b_2 d_2]$; in other words, that $(a_1 d_1 + b_1 c_1)(b_2 d_2) = (a_2 d_2 + b_2 c_2)(b_1 d_1)$. And this is certainly true because

$$\begin{aligned}(a_1 d_1 + b_1 c_1)(b_2 d_2) &= (a_1 d_1)(b_2 d_2) + (b_1 c_1)(b_2 d_2) \\ &= (a_1 b_2)(d_1 d_2) + (c_1 d_2)(b_1 b_2) \\ &= (a_2 b_1)(d_1 d_2) + (c_2 d_1)(b_1 b_2) \\ &= (a_2 d_2)(b_1 d_1) + (b_2 c_2)(b_1 d_1) \\ &= (a_2 d_2 + b_2 c_2)(b_1 d_1).\end{aligned}$$

For part (b), consider any $[a, b] \in \mathbb{Q}$ such that $[a, b] \neq [0, 1]$. In other words, consider any two integers $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $a1 \neq b0$, i.e., $a \neq 0$. In this case we want to prove that there exists an element $[c, d] \in \mathbb{Q}$ such that $[a, b] \cdot [c, d] = [1, 1]$, i.e., $[ac, bd] = [1, 1]$. In other words, we want to prove that there exist integers $c, d \in \mathbb{Z}$ with $d \neq 0$ such that

$ac1 = bd1$, i.e., $ac = bd$. Well, when you put it that way it's pretty easy: Since $a \neq 0$ we can just choose $c = b$ and $d = a$. Then we have $ac = ab = ba = ba$. The end. $\square$

[Remark: That looked like a lot of abstract nonsense, but actually we are verifying that fractions work the way you always thought they did. Part (a) shows that show that if you reduce two fractions and then add/multiply them, then you get the same thing as when you add/multiply them and then reduce the result. You use this all the time, of course, but maybe you never realized that it needs to be proved. Part (b) says that to divide by a fraction you should multiply by the reciprocal fraction. Both parts are easy to prove once you know what's being asked. The hard part is to figure out what is being asked.]

Problem 2. Generalizations of Euclid's Lemma.

(a) Let $a, b, d \in \mathbb{Z}$. Prove that if $d|ab$ and $\gcd(a, d) = 1$ then we have $d|b$. [Hint: Since $\gcd(a, d) = 1$ there exist $x, y \in \mathbb{Z}$ such that $ax + dy = 1$.]

(b) Consider $a_1, a_2, \ldots, a_n, p \in \mathbb{Z}$ with p prime. Prove that if $p|(a_1 a_2 \cdots a_n)$ then there exists $1 \leq i \leq n$ such that $p|a_i$. [Hint: Use induction or well-ordering. You can assume that the result is true when $n = 2$ (it follows from part (a)).]

Proof. For part (a), consider $a, b, d \in \mathbb{Z}$ with $d|ab$, say $ab = dk$, and $\gcd(a, d) = 1$. Since $\gcd(a, d) = 1$, Bézout's Identity says that there exist $x, y \in \mathbb{Z}$ such that $ax + dy = 1$. Then multiplying both sides of this equation by b gives

$$\begin{aligned} ax + dy &= 1 \\ (ax + dy)b &= b \\ abx + dby &= b \\ dkx + dby &= b \\ d(kx + by) &= b, \end{aligned}$$

and hence $d|b$ as desired.

For part (b), let $p \in \mathbb{Z}$ be prime. For all $n \in \mathbb{N}$ we define the statement $P(n)$ = "If $p|a_1 a_2 \cdots a_n$ for some integers $a_1, a_2, \ldots, a_n$ then there exists $i \in \{1, 2, \ldots, n\}$ such that $p|a_i$." We want to prove that $P(n) = T$ for **all** $n \in \mathbb{N}$. First note that $P(1)$ = "If $p|a_1$ then $p|a_1$" is trivially true, and that $P(2)$ = "If $p|a_1 a_2$ then $p|a_1$ or $p|a_2$" is Euclid's Lemma, which we proved in class.

Now assume for contradiction that there exists some $n \in \mathbb{N}$ such that $P(n) = F$. Then by Well-Ordering there exists a **smallest** such number, which we will call m. Since $P(1) = P(2) = T$ we have $m \geq 3$. We also know that $P(m-1) = T$ by the minimality of m. To finish the proof we will show that $P(m-1) = T$ implies $P(m) = T$, which will contradict the fact that $P(m) = F$.

So consider any m integers $a_1, a_2, \ldots, a_m \in \mathbb{Z}$ and suppose that $p|a_1 a_2 \cdots a_m$. Using parentheses creatively gives $p|(a_1 \cdots a_{m-1})a_m$, and since $P(2) = T$ this implies that $p|a_1 \cdots a_{m-1}$ or $p|a_m$. If $p|a_m$ then we are done, so suppose that $p \nmid a_m$. Then we have $p|a_1 \cdots a_{m-1}$ and since $P(m-1) = T$ this implies that there exists $i \in \{1, 2, \ldots, m-1\}$ such that $p|a_i$. We conclude that $P(m) = T$. Contradiction.

Since our original assumption (that there exists $n \in \mathbb{N}$ with $P(n) = F$) is false, we conclude that $P(n) = T$ for all $n \in \mathbb{N}$. $\square$

[Remark: We will have much more practice with induction and well-ordering after Exam2.]

Problem 3. Linear Diophantine Equations I. Consider $a, b \in \mathbb{Z}$, not both zero.

(a) Suppose that $d = \gcd(a, b)$ with $a = da'$ and $b = db'$. Prove that $\gcd(a', b') = 1$

(b) Use part (a) and Problem 2(a) to find **all integer solutions** $x, y \in \mathbb{Z}$ to the equation $ax + by = 0$.

Proof. For part (a), let $d = \gcd(a, b)$ with $a = da'$ and $b = db'$. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$, and then canceling d from both sides gives

$$\begin{aligned} ax + by &= d \\ da'x + db'y &= d \\ d(a'x + db'y) &= d \\ a'x + b'y &= 1. \end{aligned}$$

I claim that this last equation implies $\gcd(a', b') = 1$. Indeed, suppose that e is **any** common divisor of a' and b', with $a' = ea''$ and $b' = eb''$. Then we have

$$\begin{aligned} a'x + b'y &= 1 \\ ea''x + eb''y &= 1 \\ e(a''x + b''y) &= 1, \end{aligned}$$

hence $e|1$. Since $1 \neq 0$ this implies that $e \leq |e| \leq |1| = 1$. Since every common divisor e of a' and b' satisfies $e \leq 1$ we conclude that 1 is the **greatest** common divisor.

For part (b), consider $a, b, d \in \mathbb{Z}$ as in part (a). We are looking for all integers $x, y \in \mathbb{Z}$ such that $ax + by = 0$. By canceling d from both sides of this equation note that we have

$$ax + by = 0 \quad \iff \quad a'x + b'y = 0.$$

Now let $x, y \in \mathbb{Z}$ be a solution to the equation on the right. Then

$$\begin{aligned} a'x + b'y &= 0 \\ a'x &= -b'y \end{aligned}$$

implies that $a'|b'y$ and $b'|a'x$. Since we have $\gcd(a', b') = 1$ [from part (a)], Problem 2(a) implies that $a'|y$ and $b'|x$, say $y = a'k$ and $x = b'\ell$ for some $k, \ell \in \mathbb{Z}$. Plugging these back into the equation gives

$$\begin{aligned} a'x &= -b'y \\ a'(b'\ell) &= -b'(a'k) \\ \ell &= -k. \end{aligned}$$

We conclude that every solution to $a'x + b'y = 0$ has the form $(x, y) = (-b'k, a'k)$ for some $k \in \mathbb{Z}$. Since every (x, y) of this form **is** a solution, we conclude that this is the complete solution. □

Problem 4. Linear Diophantine Equations II. Let $a, b, c \in \mathbb{Z}$ be integers, where a and b are not both zero. We are interested in finding all integer solutions $x, y \in \mathbb{Z}$ to the equation $ax + by = c$. Consider the **set** of solutions

$$V_c := \{(x, y) : ax + by = c\}.$$

(a) If $\gcd(a, b)$ does not divide c, prove that $V_c = \emptyset$.

(b) If $ax' + by' = c$ is **one particular solution**, prove that

$$V_c = ((x', y') + V_0) := \{(x' + x, y' + y) : ax + by = 0\}.$$

[Hint: You have to show $V_c \subseteq ((x', y') + V_0)$ and $((x', y') + V_0) \subseteq V_c$ separately.]

(c) Let $d = \gcd(a, b)$. Suppose that $c = dc'$ and suppose that $ax' + by' = c$. Use everything you have learned to find **all integer solutions** $x, y \in \mathbb{Z}$ to the equation $ax + by = c$. [Hint: You know what V_0 is from Problem 3. Now use part (b).]

Proof. For part (a), consider $a, b, c, d \in \mathbb{Z}$ with $d = \gcd(a, b)$, say $a = da'$ and $b = db'$. We will prove the (equivalent) contrapositive statement: $V_c \neq \emptyset \implies d|c$. So assume that $V_c \neq \emptyset$ so there exist some $x, y \in \mathbb{Z}$ with $ax + by = c$. Then we have

$$c = ax + by = da'x + db'y = d(a'x + b'y),$$

hence $d|c$.

For part (b) consider $x', y' \in \mathbb{Z}$ such that $ax' + by' = c$. First we will show that $V_c \subseteq ((x', y') + V_0)$. So suppose that we have $(u, v) \in V_c$; that is, suppose that $au + bv = c$. If we define $x = u - x'$ and $y = v - y'$ then we have

$$\begin{aligned} ax + by &= a(u - x') + b(v - y') \\ &= (au + bv) - (ax' + by') \\ &= c - c \\ &= 0. \end{aligned}$$

We conclude that $(x, y) \in V_0$ and hence $(u, v) = (x' + x, y' + y)$ is in $((x', y') + V_0)$ as desired. Next we will show that $((x', y') + V_0) \subseteq V_c$. So consider any $(u, v) \in ((x', y') + V_0)$. This means that $u = x' + x$ and $v = y' + y$ for some x, y such that $ax + by = 0$. Then we have

$$\begin{aligned} au + bv &= a(x' + x) + b(y' + y) \\ &= (ax' + by') + (ax + by) \\ &= c + 0 \\ &= c, \end{aligned}$$

and hence $(u, v) \in V_c$ as desired.

For part (c), let $d = \gcd(a, b)$ with $a = da'$ and $b = db'$. We want to find all elements of the set V_c. Suppose that $(x', y') \in V_c$ is one particular element. Then from part (b) we have $V_c = ((x', y') + V_0)$ so it suffices to find all elements (x, y) of the set V_0. By Problem 3(b) we know that

$$V_0 = \{(-b'k, a'k) : k \in \mathbb{Z}\},$$

and it follows that

$$V_c = \{(x' - b'k, y' + a'k) : k \in \mathbb{Z}\}.$$

□

[Remark: In practice you will use the Extended Euclidean Algorithm to find one particular solution $(x', y') \in V_c$. Then the complete solution follows easily.]