Math 230 **Fall 2018**
Homework 4 **Drew Armstrong**

Problem 1. Prove the following properties for all integers $a, b, c \in \mathbb{Z}$.

(a) If $a|b$ and $b|c$ then $a|c$.
(b) If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers $x, y \in \mathbb{Z}$.
(c) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$. [Hint: Absolute value is multiplicative.]
(d) If $a|b$ and $b|a$ then $a = \pm b$. [Hint: Use the fact that $uv = 0$ implies $u = 0$ or $v = 0$.]

(a) Let $a|b$ and $b|c$, so that $ak = b$ and $b\ell = c$ for some $k, \ell \in \mathbb{Z}$. Then we have

$$c = b\ell = (ak)\ell = a(k\ell),$$

which implies $a|c$.

(b) Let $a|b$ and $a|c$, so that $ak = b$ and $a\ell = c$ for some $k, \ell \in \mathbb{Z}$. Then for all $x, y \in \mathbb{Z}$ we have

$$bx + cy = (ak)x + (a\ell)y = a(kx + \ell y),$$

which implies that $a|(bx + cy)$.

(c) Let $a|b$, so that $ak = b$ for some $k \in \mathbb{Z}$, and assume that $b \neq 0$. Then we must also have $a \neq 0$ and $k \neq 0$, which implies that

$$\begin{aligned} |k| &\geq 1 \\ |a||k| &\geq |a| \\ |ak| &\geq |a| \\ |b| &\geq |a|. \end{aligned}$$

(d) Let $a|b$ and $b|a$, so that $ak = b$ and $b\ell = a$ for some $k, \ell \in \mathbb{Z}$. If $a = 0$ then this implies that $b = 0k = 0$, and there is nothing to prove. Otherwise, if $a \neq 0$ then we have

$$\begin{aligned} a &= b\ell \\ a &= (ak)\ell \\ a - ak\ell &= 0 \\ a(1 - k\ell) &= 0, \end{aligned}$$

which implies that

$$\begin{aligned} 1 - k\ell &= 0 \\ k\ell &= 1. \end{aligned}$$

From part (c) we have $|k|, |\ell| \leq 1$. So there are exactly two solutions: (1) $k = \ell = 1$, which implies that $a = b$, or (2) $k = \ell = -1$, which implies that $a = -b$.

Problem 2. Euclid's Lemma. For all integers $a, b, c \in \mathbb{Z}$ prove that

$$a|(bc) \text{ and } \gcd(a, b) = 1 \text{ imply that } a|c.$$

[Hint: If $\gcd(a, b) = 1$ then the Extended Euclidean Algorithm tells us that there exist (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$.]

Proof. Suppose that $a|(bc)$, say $ak = bc$, and $\gcd(a,b) = 1$. Then from the Extended Euclidean Algorithm there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$ and it follows that

$$\begin{aligned}1 &= ax + by\\ c &= c(ax + by)\\ c &= acx + (bc)y\\ c &= acx + (ak)y\\ c &= a(cx + ky),\end{aligned}$$

hence $a|c$. □

Problem 3. Let $a, b, c \in \mathbb{Z}$, with a and b not both zero, and consider the sets

$$\begin{aligned}V &= \{(x,y) \in \mathbb{Z}^2 : ax + by = c\},\\ V_0 &= \{(x,y) \in \mathbb{Z}^2 : ax + by = 0\}.\end{aligned}$$

(a) If $(x', y') \in V$ is one particular solution, prove that V is equal to the set

$$(x', y') + V_0 := \{(x' + x, y' + y) : (x,y) \in V_0\}.$$

(b) Let $d = \gcd(a,b)$ with $a = da'$ and $b = db'$ and assume that $c = dc'$ for some $a', b', c' \in \mathbb{Z}$. Prove that V is equal to the set

$$V' := \{(x,y) \in \mathbb{Z}^2 : a'x + b'y = c'\}.$$

(c) Now let $(a, b, c) = (3094, 2513, 21)$. Use the Extended Euclidean Algorithm to find one particular element $(x', y') \in V$. [Hint: From part (b) it is enough to find one particular element of $(x', y') \in V'$.]

(d) Continuing from (c), use Problem 2 to find **all elements** of the set V_0. [Hint: From part (b) we know that $V_0 = V_0' = \{(x,y) \in \mathbb{Z}^2 : a'x + b'y = 0\}$.]

(a) Let (x', y') be any element of the set V, so that $ax' + by' = c$. We are asked to show that the sets V and $(x', y') + V_0$ are equal. There are two things to show.

- To see that $[(x', y') + V_0] \subseteq V$, consider any element (x, y) of the set $(x', y') + V_0$. By definition this means that $(x, y) = (x' + x_0, y' + y_0)$ for some $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 0$. It follows that

$$\begin{aligned}ax + by &= a(x' + x_0) + b(y' + y_0)\\ &= (ax + by) + (ax_0 + by_0)\\ &= c + 0\\ &= c,\end{aligned}$$

  and hence (x, y) is in V.

- To see that $V \subseteq [(x'y') + V_0]$, consider any element $(x, y) \in V$, so that $ax + by = c$. To prove that (x, y) is also in $(x', y') + V_0$ we need to show that $(x, y) = (x' + x_0, y' + y_0)$ for some $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 0$. And there is only one possible choice: let

$$x_0 := x - x' \quad \text{and} \quad y_0 := y - y'.$$

Then we have

$$\begin{aligned} ax_0 + by_0 &= a(x - x') + b(y - y') \\ &= (ax + by) - (ax' + by') \\ &= c - c \\ &= 0, \end{aligned}$$

as desired.

□

(b) Let $d = \gcd(a, b)$ and assume that $a = da', b = db', c = dc'$ for some $a', b', c' \in \mathbb{Z}$. We are asked to show that the sets V and V' are equal. There are two things to show.

- To see that $V' \subseteq V$, consider any element $(x, y) \in V'$ so that $a'x + b'y = c'$. Then

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

  and hence $(x, y) \in V$.

- To see that $V \subseteq V'$, consider any $(x, y) \in V$ so that $ax + by = c$. Then since $d \neq 0$ we have

$$\begin{aligned} ax + by &= c \\ (da')x + (bd')y &= (dc') \\ \not{d}(a'x + b'y) &= \not{d}c' \\ a'x + b'y &= c', \end{aligned}$$

  and hence $(x, y) \in V'$.

(c) Let $(a, b) = (3094, 2513)$ and consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ such that $ax + by = z$. We start with the easy triples $(1, 0, 3094)$ and $(0, 1, 2513)$ and then apply the Extended Euclidean Algorithm to obtain the following table:

x	y	z	row operation	
1	0	3094	(row 1)	
0	1	2513	(row 2)	
1	−1	581	(row 3)	= (row 1) − 1 · (row 2)
−4	5	189	(row 4)	= (row 2) − 4 · (row 3)
13	−16	14	(row 5)	= (row 3) − 3 · (row 4)
−173	213	7	(row 6)	= (row 4) − 13 · (row 5)
359	−442	0	(row 7)	= (row 5) − 2 · (row 6)

Since the last nonzero remainder is 7 we conclude that $\gcd(3094, 2513) = 7$. Since $7|21$ we conclude that the equation $3094x + 2513y = 21$ does have a solution, and we can read off one particular solution from row 6:

$$\begin{aligned} 3094(-173) + 2513(213) &= 7 \\ 3094(-173 \cdot 3) + 2513(213 \cdot 3) &= 7 \cdot 3 \\ 3094(-519) + 2513(639) &= 21. \end{aligned}$$

(d) If $d = \gcd(a, b)$ with $a = da'$ and $b = db'$ then one can show that $\gcd(a', b') = 1$. [Proof omitted.] Now consider any $(x, y) \in V'$ so that $a'x + b'y = 0$, and hence $a'x = -b'y$. Since $\gcd(a', b') = 1$, Problem 2 implies that $x = b'k$ and $y = a'\ell$ for some $k, \ell \in \mathbb{Z}$. But then since $a'b' \neq 0$ we have

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

We conclude that every element of V_0 has the form

$$(x_0, y_0) = (b'k, -a'k) \quad \text{for some } k \in \mathbb{Z}.$$

[Example: In the case $(a, b) = (3094, 2513)$, we have $a' = 3094/7 = 442$ and $b' = 2513/7 = 359$. Thus the complete solution of the equation $3094x + 2513y = 0$ is

$$(x_0, y_0) = (b'k, -a'k) = (359k, -442k) \quad \text{for all } k \in \mathbb{Z}.$$

It is no coincidence that these are the same numbers appearing in row 7 of the table in part (c). Then applying the results of (a),(b),(c) we conclude that the complete solution of the equation $3094x + 2513y = 21$ is

$$(x, y) = (x' + x_0, y' + y_0) = (-519 + 359k, 639 - 442k) \quad \text{for all } k \in \mathbb{Z}.]$$

Problem 4. Consider an integer $n \geq 2$. We say that d is a *proper divisor* of n if $d|n$ and $1 < d < n$. We say that $p \geq 2$ is *prime* if it has no proper divisor. Prove that

every integer $n \geq 2$ has a prime divisor $p|n$.

[Hint: Let S be the set of integers $n \geq 2$ that have no prime divisor. If this set is not empty then it must have a smallest element $m \in S$. You will need 1(c).]

[Remark: The hint is wrong. You don't need 1(c). But you do need 1(a).]

Proof. Consider the set

$$S = \{\text{integers } n \geq 2 : n \text{ has no prime factor}\},$$

and assume for contradiction that this set is not empty. Since S is bounded below (by 2) it follows from the Well-Ordering Axiom that there exists a smallest element $m \in S$. This number satisfies the following properties:

- $m \geq 2$,
- m has no prime factor,
- if $1 < d < m$ then d does have a prime factor.

But I claim that this is nonsense. Indeed, from the second property we know that m is not prime (because m divides itself). But then by definition m must have a proper divisor $d|m$ satisfying $1 < d < m$. Now the third property implies that there exists a prime p dividing d. And from 1(a) the facts $p|d$ and $d|m$ imply $p|m$, which contradicts the second property. $\square$