Math 230 **Spring 2019**
Exam 2 — Thurs Apr 4 **Drew Armstrong**

Problem 1. Well-Ordering.

(a) Accurately state the Well-Ordering Principle.

Let $S \subseteq \mathbb{Z}$ be a set of integers. If
- S is non-empty ($\exists s \in S$),
- S is bounded below ($\exists b \in \mathbb{Z}, \forall s \in S, b \leq s$)

then S has a least element ($\exists m \in S, \forall s \in S, m \leq s$).

(b) Explicitly use part (a) to prove that there exists a **smallest positive integer** $m > 0$.

Consider the set of positive integers $S = \{n \in \mathbb{Z} : n > 0\}$. Since S is non-empty (it contains 1) and is bounded below (by 0), there exists a least element $m \in S$.

(c) Since $1 > 0$ we know that $m \leq 1$. Prove that in fact $m = 1$. [Hint: Assume for contradiction that $m < 1$. Use the fact that $a < b$ and $0 < c$ imply $ac < bc$.]

Assume for contradiction that $m < 1$ and recall that $m > 0$. Then multiplying the inequality $m < 1$ by m gives $m^2 < m$ and multiplying $0 < m$ by m gives $0 < m^2$, hence

$$0 < m^2 < m.$$

But this contradicts the fact that m is the smallest positive integer.

Problem 2. Euclid's Lemma. Consider $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $ab \neq 0$.

(a) Prove that $a|bc$ implies $a|c$. [Hint: There exist some $x, y \in \mathbb{Z}$ such that $ax + by = 1$.]

Assume that $a|bc$ so that $ak = bc$ for some $k \in \mathbb{Z}$. Since $\gcd(a, b) = 1$ there exist some $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Then multiplying both sides by c gives

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

and hence $a|c$.

(b) Use (a) to prove that $ax + by = 0$ implies $(x, y) = (-bk, ak)$ for some $k \in \mathbb{Z}$. [Hint: These are **not** the same x, y from part (a).]

Assume that $ax + by = 0$ for some $x, y \in \mathbb{Z}$. Then since $a(-x) = by$ we have $a|by$ and hence $a|y$ from part (a). Similarly, since $b(-y) = ax$ we have $b|ax$ and hence $b|x$ from part (a). We have shown that $ak = y$ and $b\ell = x$ for some $k, \ell \in \mathbb{Z}$. Finally, we have

$$\begin{aligned} ax &= -by \\ a(b\ell) &= -b(ak) \\ (ab)\ell &= (ab)(-k) \\ \ell &= -k. \end{aligned}$$

Problem 3. Linear Diophantine Equations.

(a) Use the Euclidean Algorithm to find **one** integer solution of $26x + 16y = 2$.

We consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ such that $26x + 16y = z$. Then we apply the Euclidean Algorithm to the obvious triples $(1, 0, 26)$ and $(0, 1, 16)$ to obtain the following table:

x	y	z
1	0	26
0	1	16
1	−1	10
−1	2	6
2	−3	4
−3	5	2

It follows that $(x, y) = (-3, 5)$ is one solution of $26x + 16y = 2$.

(b) Find the **complete** integer solution of the homogeneous equation $26x + 16y = 0$.

From part (a) we know that $\gcd(26, 16) = 2$. Hence the reduced form of the equation is $13x + 8y = 0$ with $\gcd(13, 8) = 1$. Then from 2(b) the complete solution is $(x, y) = (-8k, 13k)$ for all $k \in \mathbb{Z}$.

(c) Combine (a) and (b) to tell me the complete integer solution of $26x + 16y = 2$.

We add the solutions from (a) and (b) to obtain

$$(x, y) = (-3 - 8k, 5 + 13k) \quad \text{for all } k \in \mathbb{Z}.$$

There are other ways to express the same solution. Yours may look different.

Problem 4. Division With Remainder.

(a) Accurately state the Division Theorem for integers.

For any $a, b \in \mathbb{Z}$ with $b > 0$ there exist **unique** integers $q, r \in \mathbb{Z}$ such that

$$\begin{cases} a = qb + r, \\ 0 \leq r < b. \end{cases}$$

(b) Suppose that $a = r + sb + tb^2$ for some integers $r, s, t, b \in \mathbb{Z}$ with $r, s, t \in \{0, 1, \ldots, b-1\}$. Tell me the quotient and the remainder of a mod b.

Observe that

$$\begin{cases} a = (s + tb)b + r, \\ 0 \le r < b. \end{cases}$$

Hence the remainder is r and the quotient is $q = s + tb$.

(c) Now suppose that $r + sb + tb^2 = r' + s'b + t'b^2$ with $r, s, t, r', s', t' \in \{0, 1, \ldots, b-1\}$. Use parts (a) and (b) to prove that $r = r'$, $s = s'$ and $t = t'$.

Proof. Observe that

$$\begin{cases} a = (s + tb)b + r, \\ 0 \le r < b, \end{cases} \quad \text{and} \quad \begin{cases} a = (s' + t'b)b + r', \\ 0 \le r' < b. \end{cases}$$

Hence $r = r'$ is the unique remainder and $q = s + tb = s' + t'b$ is the unique quotient. Finally, observe that

$$\begin{cases} q = tb + s, \\ 0 \le s < b, \end{cases} \quad \text{and} \quad \begin{cases} q = t'b + s', \\ 0 \le s' < b. \end{cases}$$

Hence the unique remainder of q mod b is $s = s'$ and the unique quotient is $t = t'$. $\square$