Math 230 E **Fall 2013**
Exam 2 — Fri Nov 8 **Drew Armstrong**

There are 4 problems, worth 5 points each. This is a closed book test. Anyone caught cheating will receive a score of **zero**.

Problem 1.

(a) Use the Euclidean Algorithm to show that $\gcd(41, 12) = 1$.

$$\begin{aligned} & & &\gcd(41,12)\\ 41 &= 3\cdot 12+5 & &=\gcd(12,5)\\ 12 &= 2\cdot 5+2 & &=\gcd(5,2)\\ 5 &= 2\cdot 2+1 & &=\gcd(2,1)\\ 2 &= 2\cdot 1+0 & &=\gcd(1,0)\\ & & &=1 \end{aligned}$$

(b) Use the Extended Euclidean Algorithm to find **one specific solution** $x, y \in \mathbb{Z}$ to the equation $41x + 12y = 1$.

We consider the triples $x, y, r \in \mathbb{Z}$ such that $41x + 12y = r$:

x	y	r
1	0	41
0	1	12
1	-3	5
-2	7	2
5	-17	1
-12	41	0

The second last row says $41(\mathbf{5}) + 12(-\mathbf{17}) = 1$.

(c) Tell me **infinitely many solutions** $x, y \in \mathbb{Z}$ to the equation $41x + 12y = 1$. [You don't need to find all of them.]

Combining the last two rows from (b) gives

$$41(\mathbf{5} - \mathbf{12k}) + 12(-\mathbf{17} + \mathbf{41k}) = 1 \qquad \text{for all } k \in \mathbb{Z}.$$

Problem 2. Fix a nonzero integer $0 \neq n \in \mathbb{Z}$ and define a relation $\equiv_n$ on $\mathbb{Z}$ as follows:

$$a \equiv_n b \qquad \Longleftrightarrow \qquad n|(a-b)$$

(a) For all $a \in \mathbb{Z}$ prove that $a \equiv_n a$.

Proof. Consider $a \in \mathbb{Z}$. Then we have $a - a = 0$ and $n|0$ because $0 = n0$. We conclude that $a \equiv_n a$. □

(b) For all $a, b \in \mathbb{Z}$ prove that $(a \equiv_n b) \Rightarrow (b \equiv_n a)$.

Proof. Assume that $a \equiv_n b$. This means that $n|(a - b)$, i.e. $(a - b) = nk$ for some $k \in \mathbb{Z}$. But then we have $(b - a) = n(-k)$, hence $n|(b - a)$. We conclude that $b \equiv_n a$. □

(c) For all $a, b, c \in \mathbb{Z}$ prove that $(a \equiv_n b \text{ AND } b \equiv_n c) \Rightarrow (a \equiv_n c)$.

Proof. Assume that $a \equiv_n b$ and $b \equiv_n c$. In other words, there exist $k, \ell \in \mathbb{Z}$ such that $(a-b) = nk$ and $(b-c) = n\ell$. Then we have

$$a - c = (a-b) + (b-c) = nk + n\ell = n(k+\ell).$$

We conclude that $n|(a-c)$ and hence $a \equiv_n c$. $\square$

Problem 3. Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$.

(a) Accurately state Bézout's Identity.

There exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.

(b) If $a = da'$ and $b = db'$, prove that there exist $x, y \in \mathbb{Z}$ such that $1 = a'x + b'y$.

Proof. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. Then

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

Cancelling d (which is nonzero) from both sides gives $a'x + b'y = 1$. $\square$

(c) Use part (b) to prove that $\gcd(a', b') = 1$.

Proof. Let e be **any** common divisor of a' and b', i.e., suppose we have $a' = ea''$ and $b' = eb''$ for some $a'', b'' \in \mathbb{Z}$. Then from part (b) we have

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

We conclude that $e|1$, which implies that $e = \pm 1$. Thus the **greatest** common divisor of a' and b' is 1. $\square$

Problem 4. Consider a sequence of integers $n_1, n_2, n_3, \ldots \in \mathbb{Z}$ such that

$$n_1 > n_2 > n_3 > \cdots \geq 0.$$

You will prove that there exists some k such that $n_k = 0$.

(a) Accurately state the Well-Ordering Axiom.

Every nonempty set of positive integers has a smallest element.

(b) Assume for contradiction that no such k exists and consider the set $S = \{n_1, n_2, \ldots\}$. What does the Well-Ordering Axiom say about this set?

Assume that $n_k > 0$ for all k. Since S is a nonempty set of positive integers, it has a smallest element. This element has the form n_m for some m.

(c) Use part (b) to derive a contradiction.

Since $n_m \neq 0$ we have $n_m > n_{m+1}$ for some other element $n_{m+1} \in S$. This contradicts the fact that n_m was smallest.

[Note: This result is false over the rational numbers $\mathbb{Q}$ because, for example,

$$1 > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} > \cdots \geq 0.]$$