Math 230 D | **Fall 2012**
Exam 2 — Wed Oct 24 | **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 Extended Euclidean Algorithm to compute $\gcd(12, 7)$. Consider the collection of triples $(x, y, r) \in \mathbb{Z}^3$ such that $12x + 7y = r$. We perform the Extended Euclidean Algorithm on these triples.

x	y	r
1	0	12
0	1	7
1	−1	5
−1	2	2
3	−5	1
−7	12	0

We conclude that $\gcd(12, 7) = 1$.

(b) Tell me the complete solution to the equation $12x + 7y = 2$. That is, tell me all pairs of integers $(x, y) \in \mathbb{Z}^2$ that satisfy the equation. [Hint: You did most of the work in part (a).]

The second last row tells us that $12(3)+7(-5) = 1$. Doubling this solution gives $12(6)+7(-10) = 2$. This is **one particular solution** to the equation $12x+7y = 2$. The general solution to the **homogeneous equation** $12x + 7y = 0$ is given by the last row above: we have $12(-7k) + 7(12k) = 0$ for all $k \in \mathbb{Z}$. Combining these gives the complete solution to the **non-homogeneous** equation $12x + 7y = 2$:

$$(x, y) = (6 - 7k, -10 + 12k) \quad \text{for all } k \in \mathbb{Z}.$$

Problem 2. Let $a, b, c \in \mathbb{Z}$ with $d := \gcd(b, c)$.

(a) If $a|b$ and $a|c$, prove that a divides $bx + cy$ for all $x, y \in \mathbb{Z}$.

Proof. Suppose that $a|b$ and $a|c$, say $b = ak$ and $c = a\ell$ for some $k, \ell \in \mathbb{Z}$. Then for any $x, y \in \mathbb{Z}$ we have

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

hence $a|(bx + cy)$. □

(b) Accurately state "Bézout's Identity."

"**For all** $a, b \in \mathbb{Z}$, **there exist** $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$."

(c) If $a|b$ and $a|c$, prove that a divides $d = \gcd(b, c)$.

Proof. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $d = bx + cy$. Then by part (a) we know that a divides d. □

Problem 3.

(a) Accurately state (some equivalent version of) the "Well-Ordering Principle."

> "Every non-empty set of positive integers has a least element."
>
> More formally:
>
> $$\forall \emptyset \neq S \subseteq \mathbb{N}, \exists\, a \in S, \forall\, b \in S, a \leq b.$$

[Note: The formal statement is just for your information. The informal statement is completely acceptable, and probably preferable.]

(b) Explicitly use the Well-Ordering Principle to **prove** that every integer $n > 1$ has a prime factor (that is, there exists a prime $p \in \mathbb{Z}$ such that $p|n$). [Hint: Consider the set S of integers $n > 1$ that **do not** have a prime factor. Suppose for contradiction that this set is **not** empty.]

Proof. Let S be the set of integers $n > 1$ that **do not** have a prime factor (that is, for all $n \in S$ there does not exist a prime p such that $p|n$). Suppose for contradiction that this set is not empty. Then by the Well-Ordering Principle, S has a least element. Call it $m \in S$.

Since m has no prime factor, m itself is not prime. Thus it can be written as a product $m = ab$ with $1 < a, b < m$. Since $1 < a < m$ and m is smallest in S we know that a **does** have a prime factor. That is, there exists a prime p and an integer k such that $a = pk$. But then $m = ab = (pk)b = p(kb)$. Contradiction. □

Problem 4. Let X and Y be any two sets.

(a) Explain in general how to prove that $X \subseteq Y$.

> **Let** x be an arbitrary element of X. **Show** that x is an element of Y.

Now let $a, b \in \mathbb{Z}$ with $d = \gcd(a, b)$ and define the sets

$$X = \{ax + by : x, y \in \mathbb{Z}\},$$
$$Y = \{dz : z \in \mathbb{Z}\}.$$

(b) Prove that $X \subseteq Y$.

Proof. Let $ax + by$ be an arbitrary element of X. Since $d|a$ and $d|b$ there exist $k, \ell \in \mathbb{Z}$ such that $a = dk$ and $b = d\ell$. But then

$$ax + by = (dk)x + (d\ell)y = d(kx) + d(\ell y) = d(kx + \ell y)$$

is an element of Y. □

(c) Prove that $Y \subseteq X$.

Proof. Let dz be an arbitrary element of Y. By Bézout's Identity, there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. But then

$$dz = (ax + by)z = (ax)k + (by)z = a(xz) + b(yz)$$

is an element of X. □