Math 230 D **Fall 2012**
Homework 4 **Drew Armstrong**

Problem 1. Let $a, b, c \in \mathbb{Z}$ be integers. Prove the following.

(a) If $a|b$ and $b|c$, then $a|c$.
(b) If $a|b$ and $a|c$, then $a|(bx + cy)$ for any $x, y \in \mathbb{Z}$.
(c) If $a|b$ and $b|a$, then $a = \pm b$.

Proof. To prove (a), suppose that $a|b$ and $b|c$, i.e., there exist $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = b\ell$. Then we have $c = b\ell = (ak)\ell = a(k\ell)$, hence $a|c$. To prove (b), suppose that $a|b$ and $a|c$, i.e., there exist $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = a\ell$. Then for any $x, y \in \mathbb{Z}$ we have $bx + cy = (ak)x + (a\ell)y = a(kx + y\ell)$, hence $a|(bx + cy)$. Finally, we prove (c). We assume that a and b are nonzero, otherwise the whole thing is pretty silly. Now suppose that $a|b$ and $b|a$, i.e., there exist $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $a = b\ell$. Then we have $a = b\ell = (ak)\ell = a(k\ell)$, hence $a(1 - k\ell) = 0$. Since $a \neq 0$, this implies $1 - k\ell = 0$ or $k\ell = 1$. We conclude that $k = \ell = \pm 1$ and hence $a = \pm b$. □

Problem 2. Given $a, b \in \mathbb{Z}$ not both zero, define the set of linear combinations

$$a\mathbb{Z} + b\mathbb{Z} := \{ax + by : x, y \in \mathbb{Z}\}.$$

What does this set look like? If $d = \gcd(a, b)$, **prove that**

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} := \{dk : k \in \mathbb{Z}\}.$$

This shows that "gcd(a, b) is the smallest positive linear combination of a and b." [Hint: You must show that $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ and $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ **separately**. One direction requires Bézout's Identity.]

Proof. Consider $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. First we will show that $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$. So consider an arbitrary element $ax + by \in a\mathbb{Z} + b\mathbb{Z}$. Since d is a common divisor of a and b there exist $k, \ell \in \mathbb{Z}$ such that $a = dk$ and $b = d\ell$. Then we have

$$ax + by = (dk)x + (d\ell)y = d(kx + \ell y) \in d\mathbb{Z}.$$

Conversely, we will show that $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. So consider an arbitrary element $dk \in d\mathbb{Z}$. By Bézout's Identity (proved by the Extended Euclidean Algorithm), there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. Then we have

$$dk = (ax + by)k = a(xk) + b(yk) \in a\mathbb{Z} + b\mathbb{Z}.$$

□

Problem 3. Let $a, b, r \in \mathbb{Z}$ be integers and define the set

$$V_r := \{(x, y) : ax + by = r\}.$$

Thus V_0 is the set of solutions (x, y) to the homogeneous equation $ax + by = 0$. If $ax_r + by_r = r$ (i.e., if (x_r, y_r) is any particular solution to the equation $ax + by = r$), **prove** that the general solution to the equation $ax + by = r$ is given by

$$\begin{aligned} V_r = (x_r, y_r) + V_0 &:= \{(x_r, y_r) + (x_0, y_0) : (x_0, y_0) \in V_0\} \\ &= \{(x_r + x_0, y_r + y_0) : ax_0 + by_0 = 0\}. \end{aligned}$$

That is, "the general solution equals the homogeneous solution shifted by any particular solution." [Hint: You must show that $V_r \subseteq ((x_r, y_r) + V_0)$ and $((x_r, y_r) + V_0) \subseteq V_r$ **separately**.]

Proof. Suppose that $ax_r + by_r = r$. We consider (x_r, y_r) as **fixed** for the rest of the problem. First we will show that $V_r \subseteq ((x_r, y_r) + V_0)$. So **consider an arbitrary element** $(x, y) \in V_r$, i.e., such that $ax + by = r$. Then we have

$$a(x - x_r) + b(y - y_r) = (ax + by) - (ax_r + by_r) = r - r = 0,$$

hence $(x - x_r, y - y_r) \in V_0$. It follows that $(x, y) = (x_r, y_r) + (x - x_r, y - y_r)$ **is an element of the set** $(x_r, y_r) + V_0$.

Conversely, we will show that $((x_r, y_r) + V_0) \subseteq V_r$. So **consider an arbitrary element** $(x, y) \in (x_r, y_r) + V_0$. This means we can write $(x, y) = (x_r, y_r) + (x_0, y_0) = (x_r + x_0, y_r + y_0)$ for some $(x_0, y_0) \in V_0$, i.e., such that $ax_0 + by_0 = 0$. Then we have

$$a(x_r + kx_0) + b(y_r + ky_0) = (ax_r + by_r) + k(ax_0 + by_0) = r + k0 = r,$$

hence (x, y) **is an element of** V_r. □

The next problems use the notation "$a \equiv b \bmod n$," which means exactly that "n divides $a - b$."

Problem 4 (Generalization of Euclid's Lemma).

(a) Suppose that $d|ab$. If $\gcd(a, d) = 1$, prove that $d|b$.
(b) Let $\gcd(c, n) = 1$. If $ac \equiv bc \bmod n$, prove that $a \equiv b \bmod n$.

Proof. To prove (a), suppose that $d|ab$, say $ab = dk$, and $\gcd(a, d) = 1$. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $ax + dy = 1$. Multiply both sides of this equation by b to obtain

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

We conclude that $d|b$. To prove (b), let $\gcd(c, n) = 1$ and suppose that $ac \equiv bc \bmod n$, i.e., $n|(ac - bc) = c(a - b)$. Then since $n|c(a - b)$ and $\gcd(c, n) = 1$, we conclude from part (a) that $a \equiv b \bmod n$ as desired. □

[Question: Given integers $a, b, c \in \mathbb{Z}$ with $c \neq 0$, why does $ac = bc$ imply $a = b$? We certainly can't "divide" by c! Answer: Subtract to get $ac - bc = 0$, or $(a - b)c = 0$. Then since $c \neq 0$ this implies $a - b = 0$, or $a = b$. (This itself can be proved from the axioms of order, e.g. if $\alpha > 0$ and $\beta > 0$, then $\alpha\beta > 0$.) So what did we just do in Problem 4(b)? We showed that $ac \equiv bc$ and "c is not 'zero' " implies $a \equiv b$ in some other kind of "number system."]

Problem 5 (Generalization of Euclid's Proof of Infinite Primes).

(a) Consider an integer $n > 1$. **Prove** that if $n \equiv 3 \bmod 4$ then n has a prime factor of the form $p \equiv 3 \bmod 4$. [Hint: You may assume Prop 2.51 from the text. There are three kinds of primes: the number 2, primes $p \equiv 1 \bmod 4$ and primes $p \equiv 3 \bmod 4$.]
(b) Prove that there are infinitely many prime numbers of the form $p \equiv 3 \bmod 4$. [Hint: Suppose there are only **finitely** many and call them $3 < p_1 < p_2 < \cdots < p_k$. Then consider the number $N = 4p_1p_2 \cdots p_k + 3$. Apply part (a).]

Proof. To prove (a), let $n > 1$ be an integer such that $n \equiv 3 \bmod 4$. Consider its prime factorization

$$n = q_1 q_2 \cdots q_m.$$

Since n is odd (why?), the prime 2 does not appear in this factorization, so each prime factor is either $q_i \equiv 1$ mod 4 or $q_i \equiv 3$ mod 4. We claim that **at least one prime factor** is $\equiv 3$ mod 4. Suppose not, i.e., suppose that **every** prime factor is $\equiv 1 \bmod 4$. Then n is a product of numbers $\equiv 1$ mod 4, hence n itself is $\equiv 1$ mod 4 (why?), contradiction.

To prove (b), suppose for contradiction that there are only **finitely many** primes of the form 3 mod 4, and call them $3 < p_1 < p_2 < \cdots < p_k$. (The fact that I didn't call $3 = p_1$ is a small trick. We will need it later on.) Now consider the number

$$N := 4p_1 p_2 \cdots p_k + 3.$$

We have $N \equiv 3$ mod 4, hence by part (a) there exists a prime $p \equiv 3$ mod 4 such that $p|N$. If we can show that this prime p is not in the set $\{3, p_1, \ldots, p_k\}$, we will obtain a contradiction. (We really needed part (a) because if $p \equiv 1$ mod 4, then $p \notin \{3, p_1, \ldots, p_k\}$ is **not** a contradiction.) But notice that none of $p_1, p_2, \ldots, p_k$ divides N, because if $p_i|N$ then we would have $p_i|(N - 4p_1 \cdots p_k)$ by Problem 1(b), hence $p_i|3$. But this contradicts the fact that $3 < p_i$. Finally, we note that $p \neq 3$ because 3 doesn't divide N. (If $3|N$ then we would also have $3|4p_1 \cdots p_k$, and then Euclid's Lemma implies that 3 divides some prime other than 3; contradiction.) We conclude that

$$p \notin \{3, p_1, p_2, \ldots, p_k\},$$

so p is a **new** prime of the form $3 \bmod 4$, contradicting the assumption that we had all of them. □

[We have just proved tiny piece of a famous theorem called "Dirichlet's Theorem on arithmetic progressions," (1837). It says that for any positive integers $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, there are **infinitely many** primes in the set

$$\{a, a + b, a + 2b, a + 3b, \ldots\}.$$

We proved the case of $a = 3$ and $b = 4$. If you want a bigger challenge, try to prove the case of $a = 1$ and $b = 4$, or look it up online.]