Mathematics 243 – Algebraic Structures
Selected Solutions – Problem Set 7
October 30, 2006

2.5/35. We let $d = \gcd(a, n)$, where $n > 1$. If there is a solution $x \in \mathbf{Z}$ of the congruence $ax \equiv b \bmod n$, then by the definition of the congruence mod $n$ relation, $n|(ax - b)$, or

$$\begin{aligned} ax - b &= nq \\ \Rightarrow b &= -nq + ax \end{aligned}$$

for some integer $q$. Because $d = \gcd(a, n)$, we have $d|a$ and $d|n$, so $a = sd$ and $n = td$ for some integers $s, t$. If we substitute these into the equation for $b$ in the last centered equation above, we get

$$b = -(td)q + (sd)x = d(-tq + sx),$$

which shows that $d|b$. This is what we wanted to show.

2.5/36. Consider a congruence $ax \equiv b \bmod n$ where $\gcd(a, n) = d > 1$. Also assume $d|b$ so the necessary condition for solutions from problem 35 is satisfied. Write

$$a = da_0 \quad n = dn_0 \quad \text{and} \quad b = db_0. \tag{1}$$

a) We want to show that if $x$ is an integer then

$$ax \equiv b \bmod n \Leftrightarrow a_0x \equiv b_0 \bmod n_0.$$

To show this, we will show the two implications separately.

$\Rightarrow$: Assume $ax \equiv b \bmod n$. Then $ax - b = nq$ for some integer $q$. Substitute for $a, b, n$ from (1) above: $da_0x - db_0 = dn_0q$. Since both terms on the left have a factor of $d$, we can factor it out and cancel to get $a_0x - b_0 = n_0q$, which shows $n_0|(a_0x - b_0)$, so $a_0x \equiv b_0 \bmod n_0$.

$\Leftarrow$: Now assume $a_0x \equiv b_0 \bmod n_0$, so $n_0|(a_0x - b_0)$. This says $a_0x - b_0 = n_0q$ for some integer $q$. If we multiply both sides of this equation by $d$, we get $da_0x - db_0 = dn_0q$. But $da_0 = a$, $db_0 = b$ and $dn_0 = n$ by (1). So $ax - b = nq$, which says $n|(ax - b)$ so $ax \equiv b \bmod n$.

b) The key observation necessary for this part is that since $d = \gcd(a, n)$, when we factor out $d$, $\gcd(a_0, n_0) = 1$. This implies that if $a_0x_1 \equiv b_0 \bmod n_0$ and $a_0x_2 \equiv b_0 \bmod n_0$, then $a_0(x_1 - x_2) \equiv 0 \bmod n_0$ (substitution rule). This implies $n_0|a_0(x_1 - x_2)$. But $\gcd(a_0, n_0) = 1$ so no factor $> 1$ of $n_0$ can divide $a_0$. It follows that $n_0$ divides $x_1 - x_2$, and hence $x_1 \equiv x_2 \bmod n_0$.

*Comment:* It's good to be aware that textbook authors often write problems like this so that you can *use previous parts to deduce later parts* in fairly simple ways. Part c here is a perfect example.

c) We are given that $a_0x_1 \equiv b_0 \bmod n_0$. Since $in_0 \equiv 0 \bmod n_0$ for all $i = 0, 1, \ldots, d-1$, we have by the substitution rule

$$a_0(x_1 + in_0) = a_0x_1 + ain_0 \equiv b_0 + 0 \equiv b_0 \bmod n_0.$$

So all the $x = x_1 + in_0$ for $i = 0, 1, \ldots, d-1$ are solutions of $a_0x \equiv b_0 \bmod n_0$. But then part a of the problem implies that $ax \equiv b \bmod n$ also(!)

d) Aiming for a contradiction, suppose $x_1 + in_0$ and $x_1 + jn_0$ are different (that is, $i \neq j$), but that they are congruent mod $n$, We can take $i$ to be the larger of the two coefficients of $n_0$ just by the way we name things, so we will assume $0 \leq j < i \leq d-1$. Then

$$(x_1 + in_0) - (x_1 + jn_0) = (i-j)n_0.$$

Since $i, j \leq d-1$, $0 < i - j < d-1$. Hence $0 < (i-j)n_0 < (d-1)n_0$. But recall that $n = n_0d$. The integer $(d-1)n_0$ is positive, but strictly smaller than $n = dn_0$. So there is no way that $n$ can divide it. This contradicts the assumption that $x_1 + in_0 \equiv x_1 + jn_0 \bmod n$.

e) Finally, we want to show that every solution $x$ of $ax \equiv b \bmod n$ is congruent mod $n$ to one of the solutions from part c. This is another place where we can use parts a and b to get a very quick and slick proof. Let $x_1$ be as in part c, and let $x$ be any other solution. Then from part a, $a_0x \equiv b_0 \bmod n_0$, and $a_0x_1 \equiv b_0 \bmod n_0$. Part b then implies that $x \equiv x_1 \bmod n_0$, since mod $n_0$ there is just one solution of the congruence $a_0x \equiv b_0 \bmod n_0$. Hence $x = x_1 + in_0$ for some integer $i$. The integer $i$ can be taken to lie in the range $0 \leq i \leq d-1$ since $dn_0 = n$. If $i \equiv i' \bmod d$, then $x_1 + in_0 \equiv x_1 + i'n_0 \bmod n$.

2.5/42. To illustrate the procedure for solving congruences $ax \equiv b \bmod n$ when $\gcd(a, n) > 1$, consider

$$21x \equiv 18 \bmod 30 \tag{2}$$

here $a = 21, n = 30$ so $d = \gcd(21, 30) = 3$. Note that $b = 18$ is also divisible by $d = 3$. Hence

$$a_0 = 7, \quad b_0 = 6, \quad n_0 = 10.$$

By part c of problem 36, we start by solving the congruence $7x \equiv 6 \bmod 10$. There is just one solution mod 10, namely $x_1 = 8$. Then 3 solutions of (2) that are not congruent mod 30 are the elements of

$$\{x_1, x_1 + n_0, x_1 + 2n_0\} = \{8, 18, 28\}.$$

It is easy to check that each is a solution of (2).