Geoffrey Parker - grp352
HW 17: 3.180-3.22
M328K
March 27th, 2012

3.18 Exercise. *Find all solutions in the appropriate canonical complete residue system modulo n that satisfy the following linear congruences:*

1. $26x \equiv 14 \pmod 3$.

   Solution. All integers x such that $x \equiv 1 \pmod 3$. □

2. $2x \equiv 3 \pmod 5$.

   Solution. All integers x such that $x \equiv 4 \pmod 5$. □

3. $4x \equiv 7 \pmod 8$.

   Solution. No solution. □

4. $24x \equiv 123 \pmod{213}$. *(This congruence is tedious to do by trial and error, so perhaps we should defer work on it for now and instead try to develop some techniques that might help.)*

   Solution. See 3.22. □

3.19 Theorem. *Let a, b, and n be integers with $n > 0$. Show that $ax \equiv b \pmod n$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.*

Proof. Let a, b, and n be integers with $n > 0$. We will show that $ax \equiv b \pmod n$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.
First, assume that $ax \equiv b \pmod n$ has a solution x. Then $n \mid ax - b$. Using the definition of divides, let $-y$ be the integer such that $n(-y) = ax - b$. So $ax + ny = b$.
Now assume that there exist integers x and y such that $ax + ny = b$. Then $ax - b = -ny$, so by the definition of divides $n \mid ax - b$. Therefore by the definition of congruence mod n, $ax \equiv b \pmod n$. □

3.20 Theorem. *Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n)|b$.*

Proof. Let a, b, and n be integers with $n > 0$. We will show that the equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.

First, assume that $ax \equiv b \pmod{n}$ has a solution x. By theorem ??, there exist integers j and k such that $aj + nk = (a, n)$. So $n(-k) = aj - (a, n)$ and $n \mid aj - (a, n)$ Also, by the definition of congruence modulo n, $n \mid ax - b$. So by theorem 1.1, $n \mid ax - b + aj - (a, n)$, and by the definition of divides $nm = a(x + j) - b - (a, n)$ for some integer m. Then for some integers c and d,

$$c(a, n)m = d(a, n)(x + j) - b - (a, n).$$

Rearranging this gives us :

$$-cm(a, n) + d(x + j)(a, n) - (a, n) = b$$

or:

$$(a, n)(d(x + j) - cm - 1) = b.$$

Since $d(x + j) - cm - 1$ is an integer, $(a, n) \mid b$.

Now assume that $(a, n) \mid b$. By the definition of divides there exists some integer m such that $(a, n)m = b$. And by theorem ??, there exist integers j and k such that $aj + nk = (a, n)$. Multiplying both sides by m gives us $m(aj + nk) = b$, or $ajm - b = nm(-k)$. So by the definition of divides $n \mid ajm - b$, and if we let $x = jm$, then by the definition of congruence modulo n, we have $ax \equiv b \pmod{n}$. □

3.21 Question. *What does the preceding theorem tell us about the congruence* (4) *in Exercise* 3.18 *above?*

Solution. Type your solution here! □

3.22 Exercise. *Use the Euclidean Algorithm to find a member x of the canonical complete residue system modulo* 213 *that satisfies* $24x \equiv 123 \pmod{213}$. *Find all members x of the canonical complete residue system modulo* 213 *that satisfy* $24x \equiv 123 \pmod{213}$.

Solution. Type your solution here! □