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. 1 $\square$

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

   Solution. 4 $\square$

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

   Solution. No solution. $\square$

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. $\square$

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, $ax \equiv b \pmod{n}$. $\square$

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 1.40, 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 1.40, 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. Because $(24, 213) = 3$ and $123 = 3 \times 41$, we know by theorem 3.20 that a solution to $24x \equiv 123 \pmod{213}$ exists. □

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. We will find all integers x in the canonical complete residue system modulo 213 such that $24x \equiv 123 \pmod{213}$ using the extended euclidean algorithm. Here we find the integers x and y such that $ax + ny = b$.

$$\begin{aligned} 21 &= 24 \cdot -8 + 213 \cdot 1 \\ 3 &= 21 \cdot -1 + 24 \cdot 1 \\ 3 &= (24 \cdot -8 + 213 \cdot 1) \cdot -1 + 24 \cdot 1 \\ 3 &= 24 \cdot 9 + 213 \cdot -1 \end{aligned}$$

Also $3 \cdot 41 = 123$.

$$\begin{gathered} 24(9) + 213(-1) = 3 \\ 41(24(9) + 213(-1)) = 41(3) \\ 24(369) + 213(-41) = 123 \\ 24(369) - 123 = 213(41) \end{gathered}$$

Therefore $24(369) \equiv 123 \pmod{213}$. Also, since $369 = 213 \cdot 1 + 156$, we have that $369 \equiv 156 \pmod{213}$. So our solution is $24(156) \equiv 123 \pmod{213}$, or $x = 156$. $\square$