**Geoffrey Parker - grp352**
**HW 18: 3.23-3.25**
**M328K**
**March 29th, 2012**

**3.23 Question.** *Let $a$, $b$, and $n$ be integers with $n > 0$. How many solutions are there to the linear congruence $ax \equiv b \pmod{n}$ in the canonical complete residue system modulo $n$? Can you describe a technique to find them?*

*Solution.* Find the two integers $q$ and $r$ such that $b = (a, n)q + r$. If $r$ is not 0, theorem 3.20 says there are no solutions. If $r$ is 0, then $b = (a, n)q$.

Use the Euclidean Algorithm to find two integers $x$ and $y$ such that $ax + ny = (a, n)$. Then $ax - (a, n) = n(-y)$ and $axq - (a, n)q = n(-yq)$. Equivalently, $a(xq) - b = n(-yq)$ so $n \mid a(xq) - b$. Therefore $a(xq) \equiv b \pmod{n}$. Now use the division algorithm find $z$ such that $xq \equiv z \pmod{n}$. Now $z$ is one solution in the canonical complete residue system modulo $n$. To find the others, repeatedly add multiples of $\frac{n}{(a,n)}$ until you have all $(a, n)$ solutions. □

**3.24 Theorem.** *Let $a$, $b$, and $n$ be integers with $n > 0$. Then,*

1. *The congruence $ax \equiv b \pmod{n}$ is solvable in integers if and only if $(a, n)|b$.*
2. *If $x_0$ is a solution to the congruence $ax \equiv b \pmod{n}$, then all solutions are given by*
$$x_0 + \left(\frac{n}{(a, n)} \cdot m\right) \pmod{n}$$
*for $m = 0,\ 1,\ 2,\ \ldots,\ (a, n) - 1$.*
3. *If $ax \equiv b \pmod{n}$ has a solution, then there are exactly $(a, n)$ solutions in the canonical complete residue system modulo $n$.*

*Proof.* Let $a$, $b$, and $n$ be integers with $n > 0$. By theorem 3.20, we know that the congruence $ax \equiv b \pmod{n}$ is solvable in integers if and only if $(a, n)|b$.

Let $x_0$ be a solution to the congruence $ax \equiv b \pmod{n}$. Let $T$ be the canonical complete residue system modulo $(a, n)$. Let $S$ be the set of integers $z$ such that $z$ is in the canonical complete residue system modulo $n$ and $x_0 + \left(\frac{n}{(a,n)} \cdot m\right) \equiv z \pmod{n}$ for any integer $m$ which is an element of $T$. We will show both that every element of $S$ is a solution to $ax \equiv b \pmod{n}$ and that all solutions to $ax \equiv b \pmod{n}$ are elements of $S$. Let $s$ be an arbitrary element of $S$. So $n \mid \left(\frac{n}{(a,n)} \cdot t\right) - s$, or $x_0 + \left(\frac{n}{(a,n)} \cdot t\right) = cn + s$ for some $t \in T$ and some integer $c$. And $s = x_0 + n\left(\frac{t}{(a,n)} - c\right)$. Since $n \mid ax_0 - b$ and $n \mid n\left(\frac{t}{(a,n)} - c\right)$, by theorems 1.6 and 1.1 $n \mid ax_0 + an\left(\frac{t}{(a,n)} - c\right) - b$. Rewriting gives us $n \mid a\left(x_0 + n\left(\frac{t}{(a,n)} - c\right)\right) - b$. Substiuting in $s$ gives us $n \mid as - b$, so $as \equiv b \pmod{n}$. Therefore every element of $S$ is a solution to $ax \equiv b \pmod{n}$.

Now consider an arbitrary integer $p$ such that $ap \equiv b \pmod{n}$. Let $q$ be the integer such that $p = x_0 + \frac{qn}{(a,n)}$. Since $T$ is a complete residue system modulo $(a, n)$, there exists some $q' \in T$ such that $q \equiv q' \pmod{(a, n)}$. Let $p' = x_0 + \frac{q'n}{(a,n)}$. So $p - p' = x_0 + \frac{qn}{(a,n)} - \left(x_0 + \frac{q'n}{(a,n)}\right) = n \cdot \frac{q-q'}{(a,n)}$. Therefore $n \mid p - p'$ and $p \equiv p' \pmod{n}$. Now let $r$ be the element of the canonical complete residue system modulo $n$ such that $p' \equiv r \pmod{n}$. By the definitions of $p'$ and the set $S$, $r$ must be an element of $S$. However, since $p \equiv p' \pmod{n}$, then by theorem 1.11 $p \equiv r \pmod{n}$. So we have taken an arbitrary solution to the congruence $ax \equiv b \pmod{n}$ and shown that it is equivalent to an element of $S$. Therefore all solutions are given by $S$.

Since all solutions in the canonical complete residue system mod $n$ are given by $S$, the number of solutions is the cardinality of $S$. And since $S$ is defined to have exactly one elemnent for every element of the canoninical complete residue system modulo $(a, n)$, then if there is 1 solution, there are exactly $(a, n)$ solutions. □

**3.25 Exercise.** *A band of* 17 *pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions,* 3 *coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The coins were redistributed, but this time an equal division left* 10 *coins. Again they fought about who should get the remaining coins and another pirate was killed. Now, fortunately, the coins could be divided evenly among the surviving* 15 *pirates. What was the fewest number of coins that could have been in the sack?*

*Solution.* Let $n$ be the number of coins in the sack. Our pirate story gives us these three equations:
$n \equiv 3 \pmod{17}$
$n \equiv 10 \pmod{16}$
$n \equiv 0 \pmod{15}$

The answer is 3930.

□