Zackery Field
ID: 23031734
CS 70, Summer 2013
Homework 2
Problem 6 [15 Points]

1. [15 Points] Solving linear equations.

   (a) [9 Points] Consider the equation $ax \equiv b(modm)$, where x is the unknown and a, b, m are given. Prove that the equation has either no solutions or exactly $d$solutions modm where $d = GCD(a, m)$, and describe when these two cases hold.

$$(ax - km = b) \equiv (ax \equiv b(modm))$$

$$px - qk = b/d \begin{cases} p = a/d \\ q = m/d \end{cases}$$

If does not $d|b$, then there is no integer linear combination that will satisfy $px - qk = b/d$. Therefore, if $d|b$ a solution exists otherwise there is no solution. Let $c = d|b$, $r \in \mathbb{Z}$, and x^* be the solution.

$$\begin{aligned} px &\equiv x(modq) \\ x^* &= cp^{-1} \\ 0 < x^* &\leq q \\ \\ ax^* - km &= b \\ ax^* &\equiv b(modm) \\ \\ 0 < x^* &< q(d-r) \\ 0 < x^* + rq &< qd \\ 0 < x^* + rq &< m = qd \\ 0 < x^* + (d-1)q &< m \end{aligned}$$

$0 < x^* + rq < m = qd$ This equation follows from the fact that x* is a solution to $px \equiv x(modq)$ and adding a multiple of q to it will convert it to a solution to $ax^* \equiv b(modm)$. The last line shows that there are d solutions, $0 < x^* + (d-1)q < m$.

   (b) [6 Points] Solve the following linear congruence equations:

      i. $4x + 28 = 2(mod63)$

$$
\begin{aligned}
4x + 28 &\equiv 2(mod 63) \\
4x &\equiv -26 \\
4x &\equiv 37 \\
&Eulers \\
63 &= 15 * 4 + 3 \\
4 &= 1 * 3 + 1 \\
&Back \\
1 &= 4 - 3 \\
&= 4 - (63 - 15 * 4) \\
&= 4 - 63 + 15 * 4 \\
&= -1 * 63 + 16 * 4 \\
\\
4(592) &\equiv 37(mod 63) \\
x &= 592(mod 63) \\
x &= 25
\end{aligned}
$$

ii. $7x + 50 = 35(mod 63)$

$$
\begin{aligned}
7x + 50 &\equiv 35(mod 63) \\
7x &\equiv -15 \\
7x &\equiv 48 \\
&Eulers \\
63 &= 9 * 7 + 0
\end{aligned}
$$

Not solveable, because $GCD(7, 63) = 0$

iii. $7x + 50 = 36(mod 63)$

$$
\begin{aligned}
7x + 50 &\equiv 36(mod 63) \\
7x &\equiv -14 \\
7x &\equiv 49 \\
&Eulers \\
63 &= 9 * 7 + 0
\end{aligned}
$$

Not solveable, because $GCD(7, 63) = 0$