Math 255 - Spring 2022
Solving multiple linear congruences
15 points
This homework invites you to solve several systems of linear congruences. Students taking this class for graduate credit are only required to answer problems 4 and 5 (though they are welcome to answer all problems of course).

1. (6 points) Solve each of the following systems of congruences. For each system of equations, be sure to list all distinct solutions, and the ring they belong to.
(a) $x \equiv 5(\bmod 6), \quad x \equiv 4(\bmod 11), \quad x \equiv 3(\bmod 17)$
(b) $x \equiv 2(\bmod 5), \quad 2 x \equiv 3(\bmod 7), \quad 3 x \equiv 4(\bmod 11)$
(c) $4 x \equiv 4(\bmod 8), \quad 5 x \equiv 6(\bmod 25), \quad 3 x \equiv 6(\bmod 27)$
2. (2 points) Find a multiple of 7 that leaves a remainder of 1 when divided by $2,3,4,5$ and 6.
3. ( 2 points) Solve the linear congruence $17 x \equiv 3(\bmod 210)$ by noticing that $210=$ $2 \cdot 3 \cdot 5 \cdot 7$ and solving the system

$$
\begin{array}{cccc}
17 x \equiv 3 & (\bmod 2), & 17 x \equiv 3 & (\bmod 3) \\
17 x \equiv 3 & (\bmod 5), & 17 x \equiv 3 & (\bmod 7)
\end{array}
$$

4. (2 points) Consider the system of congruences

$$
\begin{aligned}
6 x & \equiv 3 \\
10 x & (\bmod 9) \\
\equiv 8 & (\bmod 16) .
\end{aligned}
$$

(a) Solve each of the following congruences:
i. $6 x \equiv 3(\bmod 9)$
ii. $10 x \equiv 8(\bmod 16)$
(b) The system of congruences above is equivalent to 6 distinct systems of congruences of the form $x \equiv a_{1}(\bmod 9), \quad x \equiv a_{2}(\bmod 16)$. Write down these 6 systems and solve each of them using the Chinese Remainder Theorem.
(c) The system of congruences above is equivalent to a single system of congruences of the form $a_{1} x \equiv b_{1}(\bmod 3), \quad a_{2} x \equiv b_{2}(\bmod 8)$. Write down this system, solve it using the Chinese Remainder Theorem, and lift your solutions to $\mathbb{Z} / 144 \mathbb{Z}$.
5. (3 points) Let $x, r, s$ and $m$ be integers, with $m>1$. Show that if $x \equiv r(\bmod m)$ and $x \equiv s(\bmod m+1)$, then

$$
x \equiv r(m+1)-s m \quad(\bmod m(m+1)) .
$$

