# MATH 356-01
# Solutions to Homework Assignment 6

4.5 We seek a solution to

$$x \equiv 3 \pmod{17}$$
$$x \equiv 10 \pmod{16}$$
$$x \equiv 0 \pmod{15}$$

Note that $15, 16$, and $17$ are pairwise relatively prime. Let $N = 15 \cdot 16 \cdot 17 = 4080$, $m_1 = \frac{N}{17} = 240$, $m_2 = \frac{N}{16} = 255$, and $m_3 = \frac{N}{15} = 272$. We need inverses for $240 \equiv 2 \pmod{17}$, $255 \equiv 15 \pmod{16}$, and $272 \equiv 2 \pmod{15}$, which are $9, 15$, and $8$, respectively. We construct our solution $x = 3 \cdot 9 \cdot 240 + 10 \cdot 15 \cdot 255 + 0 \cdot 8 \cdot 272 = 44730 \equiv 3930 \pmod{4080}$. You can check that this is indeed a solution.

4.6 (a) $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2-1)(3-1)(5-1) = 8$.

(b) $\varphi(144) = \varphi(2^4 \cdot 3^2) = (2^4 - 2^3)(3^2 - 3) = 24$.

(c) $\varphi(143) = \varphi(11 \cdot 13) = (11-1)(13-1) = 120$.

(d) $\varphi(108) = \varphi(2^2 \cdot 3^3) = (2^2 - 2)(3^3 - 3^2) = 36$.

4.22 I think I meant 4.22 since 4.21 is actually in the text. If $a \equiv b \pmod{n}$, then $a - b = nq$ fr some $q \in \mathbb{Z}$. Thus $ka - kb = (kn)q$, so $ka \equiv kb \pmod{kn}$. Conversely, we can work backwards and cancel the $k$s since $k \neq 0$.