Emma Deckers
Math 301 Spring 2022
Homework 5

Page 76 Problem 8 Solve $x \equiv 7(mod 9)$, $x \equiv 13(mod 23)$, and $x \equiv 1(mod 2)$.

Since $(9, 23, 2) = 1$ we can use the Chinese remainder theorem. Observe that $(2 \cdot 23)(7) \equiv 7(mod 9)$, $(2 \cdot 9)(117) \equiv 13(mod 23)$, and $(9 \cdot 23) \equiv 1(mod 2)$. Therefore $x = 46(7) + 18(117) + 207 = 2635$. One can verify that $2635 \equiv 7(mod 9)$, $2635 \equiv 13(mod 23)$, and $2635 \equiv 1(mod 2)$.

Page 76 Problem 12 Solve $2x + 7y \equiv 8(mod 13)$ and $5x + 10y \equiv 7(mod 13)$.

The system of equations gives the following associated system: $-15x \equiv 31(mod 13) = 11x \equiv 5(mod 13)$ and $-15y \equiv 0(mod 13) = 11y \equiv 0(mod 13)$. To solve the first equation for x, we use the Euclidean Algorithm to find that $5 = 13(-25) + 11(30)$. So $x = 30 \equiv 4(mod 13)$. From the second equation we clearly see that $y \equiv 0(mod 13)$, so the least residue solution to y is $y = 0$. Therefore, $(x, y) = (4, 0)$ solves the original system of equations.

Page 82 Problem 4 Prove that 561=3*11*17 is a pseudoprime.

For this proof, I will be using Fermat's definition of pseudoprime to prove the statement. An integer x is said to be pseudoprime (a Carmichael number) if $x^{m-1} \equiv 1(mod m)$ for all $(x, m) = 1$.

Suppose that $(b, 561) = 1$ for some $b \in \mathbb{Z}$. Then it follows that b shall be relatively prime to all of the prime divisors of 561: $(b, 3) = 1$, $(b, 11) = 1$, and $(b, 17) = 1$. Then using Fermat's theorem 3.14, $b^{3-1} \equiv b^2 \equiv 1(mod 3)$, $b^{11-1} \equiv b^{10} \equiv 1(mod 11)$, and $b^{17-1} \equiv b^{16} \equiv 1(mod 17)$. It follows that $b^{560} \equiv b^{2*280} \equiv 1^{280}(mod 3)$, $b^{560} \equiv b^{10*56} \equiv 1^{56}(mod 11)$, and $b^{560} \equiv b^{16*35} \equiv 1^{35}(mod 17)$. By the definition of congruence, $3|b^{560} - 1$, $11|b^{560} - 1$ and $17|b^{560} - 1$. So, $3 * 11 * 17|b^{560} - 1 \rightarrow 561|b^{560} - 1$. Thus, $b^{560} \equiv 1(mod 561)$, hence, 561 is pseudoprime.

Page 82 Problem 7 Find a composite number such that $n|3^n - 3$.

By definition, we have $3^n \equiv 3(mod n)$. We can begin by looking at the composite numbers less than 10:

$$3^4 = 81 \equiv 1(mod 4)$$
$$3^6 = 3^3 * 3^3 \equiv 27 * 27 \equiv 9 \equiv 3(mod 6)$$

Therefore $n = 6$ satisfies $6|3^6 - 3$.