# Math 115A Homework 5

1) Find the multiplicative inverse modulo $m$ of each integer $n$ below.

a) $n = 40$, $m = 81$

b) $n = 51$, $m = 99$

2) Let $a'$ be the multiplicative inverse of $a$ modulo $m$ and let $b'$ be the multiplicative inverse of $b$ modulo $m$. Prove that $a'b'$ is the multiplicative inverse of $ab$ modulo $m$.

3) Find the least nonnegative solution to the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

4) Solve the system of linear congruences below by finding all $x$ that satisfy it. *Hint: try rewriting each congruence in the form* $x \equiv a \pmod b$

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 3x &\equiv 2 \pmod 5 \\ 5x &\equiv 4 \pmod 7 \end{aligned}$$

5) a) Prove that the system of linear congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}$$

is solvable if and only if $(m_1, m_2)|(b_1 - b_2)$. In this case, prove that the solution is unique modulo $\operatorname{lcm}(m_1, m_2)$.

b) Formulate a statement for when the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

has a solution. This solution should be unique modulo which value? (no proof necessary but try to explain to yourself or a friend why you think your statement is correct)

6) Solve each system of congruences below.

a)

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

b)

$$\begin{aligned} x &\equiv 2 \pmod 6 \\ x &\equiv 8 \pmod 9 \end{aligned}$$

c)

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 8 \end{aligned}$$

d)

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 5 \pmod{10} \\ x &\equiv 11 \pmod{12} \\ x &\equiv 5 \pmod{15} \end{aligned}$$

7) How difficult was this homework? How long did it take?