# Worksheet 9: February 21 (Solutions)

## 1 Modular Inverses

1. For each of the following congruences $a \mod b$, determine whether $a$ is invertible mod $b$, and if so, find its modular inverse.

   (a) $5 \mod 7$
   **Solution:** Inverse is $3 \mod 7$

   (b) $12 \mod 26$
   **Solution:** Not invertible (both 12 and 26 are divisible by 2)

   (c) $3 \mod 10$
   **Solution:** Inverse is $7 \mod 10$

   (d) $59 \mod 11$
   **Solution:** First note that $59 \equiv 4 \mod 11$. Inverse is $3 \mod 11$

   (e) $15 \mod 18$
   **Solution:** Not invertible (both 15 and 18 are divisible by 3)

   (f) $45 \mod 46$
   **Solution:** First note that $45 \equiv -1 \mod 46$. Inverse is $45 \mod 46$

## 2 Chinese Remainder Theorem

2. For each of the following sets of congruences, find some integer $x$ such that every congruence holds.

   (a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 4 \end{cases}$
   **Solution:** $x = 5$

   (b) $\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 0 \mod 5 \\ x \equiv 4 \mod 7 \end{cases}$
   **Solution:** The first two congruences simplify to $x \equiv 5 \mod 20$. The Bezout coefficients for 20 and 7 are $-1$ and 3, because $-1 \cdot 20 + 3 \cdot 7 = 1$. Thus, a solution is $x = 5 \cdot (3 \cdot 7) + 4 \cdot (-1 \cdot 20) = 25$.

(c) $\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 6 \mod 13 \end{cases}$

**Solution:** The first two congruences simplify to $x \equiv 5 \mod 6$. The Bezout coefficients for 6 and 13 are $-2$ and 1, because $-2 \cdot 6 + 1 \cdot 13 = 1$. Thus, a solution is $x = 5 \cdot (1 \cdot 13) + 6 \cdot (-2 \cdot 6) = -7$

(d) $\begin{cases} x \equiv 75 \mod 457 \\ x \equiv 75 \mod 6781 \end{cases}$

**Solution:** Don't need to go through the algorithm; we can see that $x = 75$ works for both.

# 3 Fermat's Little Theorem

3. Evaluate the following congruences:

   (a) $2^{44} \mod 7$
   **Solution:** $2^{44} \equiv 2^{7 \cdot 6+2} \equiv 2^2 \equiv 4 \mod 7$

   (b) $6^{123} \mod 11$
   **Solution:** $6^{123} \equiv 6^{12 \cdot 10+3} \equiv 6^3 \equiv 216 \equiv 7 \mod 11$

   (c) $26^{90941} \mod 13$
   **Solution:** $26^{90491} = 2^{90491} 13^{90491} \equiv 0 \mod 13$

   (d) $43^{43} \mod 11$
   **Solution:** $43^{43} \equiv (-1)^{43} \equiv -1 \equiv 10 \mod 11$

4. State and prove Fermat's Little Theorem.
   **Theorem:** If $p$ is prime and $a$ is an integer not divisible by $p$, then $a^{p-1} \equiv 1 \mod p$.
   **Proof:** $a$ has a multiplicative inverse modulo $p$; call it $b$. Let $S = \{1, 2, 3, \ldots, p-1\}$. Then the function $f : S \to S$ defined by $f(x) = ax \mod p$ is invertible, because its inverse is $f^{-1}(y) = by \mod p$. Thus:

$$\{1 \text{ mod } p, 2 \text{ mod } p, \ldots, (p-1) \text{ mod } p\} = \{1a \text{ mod } p, 2a \text{ mod } p, \ldots, (p-1)a \text{ mod } p\}$$

$$1 \times 2 \times \cdots \times (p-1) \equiv 1a \times 2a \times \cdots \times (p-1)a \mod p$$
$$1 \times 2 \times \cdots \times (p-1) \equiv a^{p-1}(1 \times 2 \times \cdots \times (p-1)) \mod p$$

The number on the left is not divisible by $p$ (because $p$ is prime), so it has a modular inverse. Multiply both sides by this inverse to get $1 \equiv a^{p-1} \mod p$.