CS 135 Spring 2018: Problem Set 7.

Problem 1. (10 points) Let p be a prime number. In class we proved that every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse. Since $1 \cdot 1 \equiv 1\ (mod\ p)$ it is obvious that $1^{-1} \equiv 1\ (mod\ p)$. In other words, 1 is its own inverse, and we say that 1 is a self-inverse mod p.

a. For each non-zero number in $\mathbb{Z}_5$ compute its inverse mod 5. Which numbers are self-inverses mod 5?

b. For each non-zero number in $\mathbb{Z}_{11}$ compute its inverse mod 11. Which numbers are self-inverses mod 11?

c. Prove that the only self-inverses mod p in $\mathbb{Z}_p$ are 1 and $p-1$.
To get started, note that if k is a self-inverse then $k^2 \equiv 1\ (mod\ p)$.
Starting with this congruence, use the fact that $k^2 - 1 = (k-1)\cdot(k+1)$ to complete your proof.

$$k^2 \equiv 1\ (mod\ p)$$
$$\Leftrightarrow k^2 - 1 \equiv 0\ (mod\ p)$$
$$\Leftrightarrow (k-1)(k+1) \equiv 0\ (mod\ p)$$

Now, since p is prime, $\gcd(p, k-1) = 1$ for $1 < k < p$.
But then $(k-1)(k+1) \equiv 0\ (mod\ p)$ is true if and only if $(k+1) \equiv 0\ (mod\ p)$

Similarly, $\gcd(p, k+1) = 1$ for $0 < k < p-1$, so that
$(k-1)(k+1) \equiv 0\ (mod\ p)$ is true if and only if $(k-1) \equiv 0\ (mod\ p)$

Thus,
$$k^2 \equiv 1\ (mod\ p) \Leftrightarrow (k-1) \equiv 0\ (mod\ p)\ \ or\ (k+1) \equiv 0\ (mod\ p)$$
$$\Leftrightarrow k = 1\ or\ k = p-1$$

d. (Extra Credit) For any natural number n, the factorial function $n!$ is defined as

$$n! \stackrel{\text{def}}{=} n(n-1)(n-2)\cdots 1$$

Prove that for every prime number p, $(p-1)! \equiv -1\ (mod\ p)$
Hint: Consider every number in the product and use the result of part (c).
Consider $(p-1)! = (p-1)(p-2)\cdots 3\cdot 2\cdot 1$
Since p is prime, we know that $\forall a \in \{1,2,\dots,p-1\}\ \exists a^{-1} : a\cdot a^{-1} \equiv 1\ (mod\ p)$ such that a^{-1} is unique.
From part (a), the only numbers that are self-inverses are 1 and p-1.
If $p = 2$, then $1 \equiv p-1 \equiv -1$, and the claim is true.
Otherwise, the remaining numbers 2,3,… ,(p-2) can be paired up into (p-3)/2 pairs so that each number is paired up with its inverse. The product of each pair is 1 (mod p). Thus,

$$(p-1)! \equiv 1\cdot 1^{\frac{p-3}{2}}\cdot(p-1)$$
$$\equiv (p-1)$$
$$\equiv -1\ (mod\ p)$$

Problem 2. (10 points) Consider the following system of congruences:

$$x \equiv 5 \ (mod\ 7)$$
$$x \equiv 3 \ (mod\ 11)$$
$$x \equiv 8 \ (mod\ 13)$$

a. Find the unique solution modulo $7 \times 11 \times 13 = 1001$. Show all steps of your work.
b. Write an expression that represents all solutions to the system of congruences.

Step 1. Calculate $m = m_1 m_2 m_3 = 7 \times 11 \times 13 = 1001$

Step 2. Calculate $M_1 = m_2 m_3 = 143; M_2 = m_1 m_3 = 91; M_3 = m_1 m_2 = 77$

Step 3. Calculate $y_1 \equiv M_1^{-1} (mod\ m_1)$

$$143 = 7 \cdot 20 + 3$$
$$7 = 3 \cdot 2 + 1$$
$$\Rightarrow 1 = 7 - 3 \cdot 2$$
$$= 7 - (143 - 7 \cdot 20) \cdot 2$$
$$= 42 \cdot 7 - 2 \cdot 143$$
$$So, 143^{-1} \equiv -2 \equiv 5 \ (mod\ 7)$$

Calculate $y_2 \equiv M_2^{-1} \ (mod\ m_2)$

$$91 = 11 \cdot 8 + 3$$
$$11 = 3 \cdot 3 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$\Rightarrow 1 = 3 - 2$$
$$= 3 - (11 - 3 \cdot 3)$$
$$= 3 \cdot 4 - 11$$
$$= 4(91 - 11 \cdot 8) - 11$$
$$= 4 \cdot 91 - 33 \cdot 11$$
$$So, 91^{-1} \equiv 4 \ (mod\ 11)$$

Calculate $y_3 \equiv M_3^{-1} (mod\ m_3)$

$$77 = 13 \cdot 5 + 12$$
$$13 = 12 \cdot 1 + 1$$
$$\Rightarrow 1 = 13 - 12$$
$$= 13 - (77 - 13 \cdot 5)$$
$$= 13 \cdot 6 - 77$$
$$So, 77^{-1} \equiv -1 \equiv 12 \ (mod\ 13)$$

Step 4. Calculate $X \equiv a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 \ (mod\ m)$

$$\equiv 5 \cdot 5 \cdot 143 + 3 \cdot 4 \cdot 91 + 8 \cdot 12 \cdot 77 \ (mod\ 1001)$$
$$\equiv 3575 + 1092 + 7392 \ (mod\ 1001)$$
$$\equiv 572 + 91 + 385$$
$$\equiv 1048$$
$$\equiv 47 \ (mod\ 1001)$$