Julia Nelson

CS 135 Spring 2018: Problem Set 7.

"I pledge my honor that I have abided by the Stevens Honor System." JNelson

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.

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).

a) $Z_5 = \{0,1,2,3,4\}$

$1^{-1} = 1$

$2^{-1} = 3$ as $2\cdot 3 \equiv 1 \bmod 5$

so, $3^{-1} = 2$

$4^{-1} = 4$ as $4\cdot 4 = 16 \equiv 1 \bmod 5$

1 and 4 are self-inverse mod 5

b) $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$

$1^{-1} = 1$

$2^{-1} = 6$ as $2\cdot 6 = 12 \equiv 1 \bmod(11)$ $\Rightarrow 6^{-1} = 2$

$3^{-1} = 4$ as $3\cdot 4 = 12 \equiv 1 \bmod(11)$

so, $4^{-1} = 3$

$5^{-1} = 9$ as $5\cdot 9 = 45 \equiv 1 \bmod(11)$

so, $9^{-1} = 5$

$7^{-1} = 8$ as $7\cdot 8 = 56 \equiv 1 \bmod(11)$

so, $8^{-1} = 7$

$10^{-1} = 10$ as $10\cdot 10 = 100 \equiv 1 \bmod(11)$

Only 1 and 10 are self inverses for mod(11)

c) $K \in Z_p$ is a self-inverse if...

$K^2 \equiv 1 \bmod p$

$K^2 - 1 \equiv 0 \bmod p$

$(K+1)(K-1) \equiv 0 \bmod p$

Since Z_p is an integral domain...

$K+1 \equiv 0 \bmod p$ as $K-1 \equiv 0 \bmod p$

$K \equiv -1 \bmod p$ as $K \equiv 1 \bmod p$

$K = p-1 \bmod p$ as $K = 1 \bmod p$

so 1 and $p-1$ are the only self inverses.

d) in order to prove $(p-1)! \equiv -1 \bmod p$ we must consider

$(p-1)! \equiv (p-1)(p-2)\cdots 3\cdot 2\cdot 1$

each # in product belongs to Z_p and has an inverse other the #. except $(p-1)$ because it's its own inverse.
(we shouldn't consider 1 as $(p-1)! \equiv (p-1)(p-2)\cdots(3)(2)$)
Pairing each "a" number in the product with its inverse to get 1.
So,

$(p-1)! = (p-1)\cdots(3)(2) = (p-1)(a\cdot a^{-1})(b\, b^{-1})\cdots =$

$= (p-1)(1)(1)\cdots(1) = p-1 \equiv -1 \bmod p$

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

$$x \equiv 5 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$
$$x \equiv 8 \pmod{13}$$

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.

a) $M = 7 \times 11 \times 13 = 1001$

M_i: $M_1 = 11 \times 13 = 143$ (all except 7)

$M_2 = 7 \times 13 = 91$ (all except 11)

$M_3 = 7 \times 11 = 77$ (all except 13)

$M_i \times Y_i \equiv 1 \bmod D_i$

D_i is respective divisor

$M_1 = 143 \Rightarrow 143 \times Y_1 \equiv 1 \bmod 7$

$\Rightarrow Y_1 = 5$

as $143 \times 5 = 715$

$\Rightarrow 715 \bmod 7 = 1$

$M_2 = 91 \Rightarrow 91 \times Y_2 \equiv 1 \bmod 11$

$\Rightarrow Y_2 = 4$

as $91 \times 4 = 364$

$\Rightarrow 364 \bmod 11 = 1$

$M_3 = 77 \Rightarrow 77 \times Y_3 \equiv 1 \bmod 13$

$\Rightarrow Y_3 = 12$

as $77 \times 12 = 924$

$\Rightarrow 924 \bmod 13 = 1$

$x = \sum R_i \times M_i \times Y_i$

R_i is corresponding remainder

M_i is corresponding value above

Y_i are velues above found

$x = (R_1 \times M_1 \times Y_1) + (R_2 \times M_2 \times Y_2) + (R_3 \times M_3 \times Y_3)$

$x = (5 \times 143 \times 5) + (3 \times 91 \times 4) + (8 \times 77 \times 12)$

$x = 3575 + 1092 + 7392$

$x = 12059$

Now, $x = 12059 \bmod 1001 = 47$

b) $M \times t + x$

$\Rightarrow 1001 \times t + 47$

if $t = 0$

$x = 47$