Assignment 21: Congruence 4

Declan Murphy Zink

11/9/2020

6 The number $(p-1)!$ (mod p) came up in our proof of Fermat's Little Theorem, although we didn't need to find it. Calculate $(p-1)!$ (mod p) for some small prime numbers p. Find a pattern and make a conjecture. Prove your conjecture!

$p = 2 \Rightarrow (p-1)! \equiv 1 \equiv -1 \text{ mod } 2$
$p = 3 \Rightarrow (p-1)! \equiv 2 \equiv -1 \text{ mod } 3$
$p = 5 \Rightarrow (p-1)! \equiv 24 \equiv -1 \text{ mod } 5$
$p = 7 \Rightarrow (p-1)! \equiv 720 \equiv -1 \text{ mod } 7$

Conjecture: For a prime number p, $(p-1)! \equiv -1$ mod p

Proof:
$(p-1)! = (1)(2)(3)...(p-3)(p-2)(p-1)$
Let $a_1 = 1, ..., a_{p-1} = p-1$
Since p is prime we know that any a_i must be coprime to p.
This means $\forall$ a_i $\exists$ $x \in \mathbb{Z}_p$ such that $a_i x \equiv 1$ mod p. This x is unique in $\mathbb{Z}_p$.