Week 09 In-Class Exercises

Guided Exercise

L1. Consider the numbers $S = \{0a, 1a, 2a, \ldots, (p-1)a\}$. We claim that no two of these elements lie in the same equivalence class modulo p.

L2. Indeed, since $p \nmid a$ then $\gcd(p, a) = 1$. Thus if $ma \equiv na \pmod{p}$ then $m \equiv n \mod p$, showing that the elements of S all lie in different equivalence classes.

L3. Since S consists of exactly p elements and so too does $\mathbb{Z}_p$, the elements of S are just a rearrangement of the elements of $\mathbb{Z}_p$.

Multiplying all of the non-zero elements of S together will thus give the same result as multiplying all of the non-zero elements of $\mathbb{Z}_p$ together,

L4. so

$$(a)(2a)\cdots((p-1)a) \equiv (1)(2)\cdots(p-1) \pmod{p}$$
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

L5. Once again, we see that $\gcd(p, (p-1)!) = 1$ (why?)

L6. and so

$$a^{p-1} \equiv 1 \pmod{p},$$

as required.