Exercise 2

Proof by Induction

Base case:

$a = 0$
1) $0^p \equiv 0 \pmod p$
True for all p

$a = 1$
1) $1^p \equiv 1 \pmod p$
True for all p

Inductive step:

Assume true for $k \geq 1$, prove $k+1$

1) $(k+1)^p \equiv (k+1) \pmod p$

Using binomial theorem to expand LHS:

$(k+1)^p = k^p + \binom{p}{1} k^{p-1} + \binom{p}{2} k^{p-2} \ldots + \binom{p}{p-1} k + 1$

We know that p divides all of our binomial coefficients except k^p and 1.

$\binom{p}{r}$ for $1 \leq r \leq p-1$

This is because we expand $\binom{p}{i}$ as:

$\binom{p}{i} = \frac{p!}{i!(p-i)!}$ ← has factor p
← no factor p (all $< p$)

We therefore know:

$(k+1)^p \equiv k^p + 1 \pmod p$

By the principle of induction, true for all $k \geq 0$.

For $k < 0$:

$(-a)^p \equiv -(a^p) \pmod p$

Because p is prime (thus odd) there will always be a negative value popped out

Given (1), we now prove (2):

$a^p \equiv a \pmod p$ and $p \nmid a$

We know:

$p \mid a^p - a$ by definition of congruence

$p \mid a(a^{p-1} - 1)$

By the coprime divisibility property, if $p \mid ab$ and $p \nmid a$, then $p \mid b$.

We know $p \nmid a$, so $p \mid a^{p-1} - 1$.
By definition of congruence:

If $p \nmid a$, $a^{p-1} \equiv 1 \pmod p$.
→ We have proven statement (2) contingent on (1) being true.