Exercise set 6 page 161 #117:

Let p be a prime and r a positive integer, $\gcd(r, p-1) = 1$.
Let $f: \mathbb{Z}_p \to \mathbb{Z}_p$, $f([x]) = [x]^r$.
Then f is a bijection.

Proof: The Diophantine Equation

$$rx + (p-1)y = 1$$

has a solution, since $\gcd(r, p-1) = 1$. Hence, the congruence class of r in $\mathbb{Z}_{p-1}$ is invertible, $[r][s] = [1]$ in $\mathbb{Z}_{p-1}$, for some integer s (which we can choose to be positive). Now $(p-1) \mid (rs - 1)$, so $rs = (p-1)q + 1$, $q \geq 0$, $q \in \mathbb{Z}$.

Let $g: \mathbb{Z}_p \to \mathbb{Z}_p$ be given by

$$g([x]) = [x]^s.$$

Then $f(g([x])) = g(f([x])) = [x]^{rs} = [x]^{(p-1)q+1} =$

$$= [x] \cdot \left([x]^{(p-1)}\right)^q = [x] \quad (\text{in } \mathbb{Z}_p).$$

The last equality clearly holds for $[x] = [0]$. If $[x] \neq [0]$, then $[x]^{p-1} = [1]$, by Fermat's Little Theorem, and so the equality holds again.

Q.E.D