Theorem 6.11 (Fermat's Little Theorem)**.** *For an integer m and a prime p,*

$$m^p \equiv m \bmod p \ .$$

Proof. Fix a prime p. If $p = 2$, then Fermat's Little Theorem just says that m^2 is even if and only if m is even, which was the content of Proposition 6.7. For the remainder of the proof, $p > 2$, i.e., p is an odd prime.

We will use induction to first prove $m^p \equiv m \bmod p$ for integers $m \geq 0$. The base case $m = 0$ follows immediately, as $0^p \equiv 0 \bmod p$ just says that $p|0$.

For the induction step, assume that we know $m^p \equiv m \bmod p$. Then

$$(m+1)^p = \sum_{k=0}^{p} \binom{p}{k} m^k 1^{p-k} = \sum_{k=0}^{p} \binom{p}{k} m^k.$$

However, Proposition 5.16 says that $\binom{p}{k} \equiv 0 \bmod p$ for $0 < k < p$. Hence

$$(m+1)^p = \sum_{k=0}^{p} \binom{p}{k} m^k \equiv \binom{p}{0} m^0 + \binom{p}{p} m^p = 1 + m^p \equiv 1 + m \bmod p \ ,$$

where we have used the induction hypothesis in the last step. We have proved that $(m+1)^p \equiv m + 1 \bmod p$, which completes the induction step.

This proves $m^p \equiv m \bmod p$ for integers $m \geq 0$. If $m < 0$, let $n = -m$, so $n > 0$, and we know from the first part that $n^p \equiv n \bmod p$. Since p is odd, $m^p = -n^p$, and so $m^p \equiv m \bmod p$ follows from $n^p \equiv n \bmod p$. $\square$