

## Lemma

If  $x, y \in \mathbb{Z}$ , and  $p$  prime, then

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

## Proof.

From Binomial Theorem,

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

By Lemma 1, all of the interior coefficients are multiples of  $p$ , so modulo  $p$  this is

$$x^p + y^p.$$

