

5.2.12) Prove p prime and $1 \leq k \leq p-1 \implies \binom{p-1}{k} \equiv (-1)^k \pmod{p}$.

Proof. Examine

$$\frac{(p-1)!}{k!(p-1-k)!}.$$

Factor out $(p-1-k)!$ from the top and bottom. We are left with

$$\frac{(p-1)(p-2)\cdots(p-k)}{k!}.$$

We know binomial terms are always integers, so we can remove the terms that include p from the congruence. We have

$$\binom{p-1}{k} \equiv \frac{(-1)(-2)\cdots(-k)}{k!} \pmod{p}.$$

This leaves us with

$$\frac{(-1)(-2)\cdots(-k)}{k!} = \frac{(-1)^k k!}{k!} = (-1)^k.$$

Therefore $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$. □