Chapter 3: Congruence

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 3.12. *Let*

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

be a binomial coefficient, and suppose that p is a prime. If $1 \leq k \leq p-1$, show that p divides $\binom{p}{k}$. Deduce $(a+1)^p \equiv a^p + 1 \pmod{p}$.

Proof.

(1) If $1 \leq k \leq p-1$, then $p \nmid k!$ and $p \nmid (p-k)!$ since p is a prime number.

(2) Write $a = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$.

$$\begin{aligned} a = \frac{p!}{k!(p-k)!} &\Longleftrightarrow p! = ak!(p-k)! \\ &\Longrightarrow p \mid p! \text{ or } p \mid ak!(p-k)! \\ &\Longrightarrow p \mid a \qquad ((1)) \end{aligned}$$

Hence p divides $\binom{p}{k}$ if $1 \leq k \leq p-1$.

(3)

$$\begin{aligned} (a+1)^p &\equiv \sum_{k=0}^{p} \binom{p}{k} a^k \\ &\equiv 1 + \left(\sum_{k=1}^{p-1} \binom{p}{k} a^k \right) + a^p \\ &\equiv 1 + a^p \\ &\equiv a^p + 1 \pmod{p}. \end{aligned}$$

□