

## [选做题一] 数论小练习

---

Let  $p, N$  be integers such that  $p$  divides  $N$ . Prove that for any integer  $X$ ,  $[(X \bmod N) \bmod p] = [X \bmod p]$ . Show that, in contrast,  $[[X \bmod p] \bmod N]$  need not equal  $[X \bmod N]$ .

Proof:

- let  $X = aN + r, r = bp + t$ , so  $X = aN + bp + t$
- therefore  $[(X \bmod N) \bmod p] = t = [X \bmod p]$
- however  $[[X \bmod p] \bmod N] = t$  and  $[X \bmod N] = r = bp + t$
- So it may not be equal