Arithmetics *mod n*

1. Prove

a) $(\forall n,k)\ (n \bmod k) \bmod k = n \bmod k$

b) $(\forall n,k,p)\ (n+p) \bmod k = (n \bmod k + p \bmod k) \bmod k$

c) $(\forall n,k,p)\ (np) \bmod k = ((n \bmod k)(p \bmod k)) \bmod k$

2. Prove

a) multiplication mod *n* is associative, i.e. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

b) addition mod *n* is associative.

c) multiplication mod *n* is distributive with respect to addition mod n.

3. Calculate

a) 17mod4

b) 4mod17

c) (-2)mod5

4. Solve equations in indicated sets

a) $2x =$ in $\mathbf{Z}_7$

b) $3x=1$ in $\mathbf{Z}_6$

c) $5x = 1$ in $\mathbf{Z}_7$

d) $x^2=3$ in $\mathbf{Z}_{11}$

e) $(2x + 3 = 0)$ in $\mathbf{Z}_5$

f) $x+k=0$ in $\mathbf{Z}_n$

5. Show that $(Z_n-\{0\}, \otimes)$ is a group iff n is a prime.