

Homework #8 - Elementary Modern Algebra I (Fall 07)

10/22/07

Please, write down your solutions neatly and explain your reasoning clearly.

1. (4 points) Find the distinct cosets and the index of $\langle 10 \rangle$ in \mathbb{Z}_{24} .
2. (4 points) In order to receive secret messages by using the RSA system, Alice has published her public key $(n, k) = (5251, 3403)$.
 - (a) Find Alice' secret key l using the fact that $5251 = 59 \cdot 89$ where 59 and 89 are prime numbers.
 - (b) Alice has received the encrypted message 950. What is the plain text of the message (i.e. find $950^l \pmod n$)?
3. (4 points) Consider the maps $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$, $a \mapsto 5a$, and $\psi : \mathbb{Z}_9 \rightarrow \mathbb{Z}_2$, $a \mapsto a \pmod 2$. Decide whether φ and ψ are group homomorphisms.

Due date: October 29, 2007