

Algebraic and Geometric Methods in Engineering and Physics

Homework 3

Due on October 1

1. (a) Compute the order of \mathbb{Z}_{187}^* .
(b) Find the multiplicative inverse of $[18] \in \mathbb{Z}_{187}$.
(c) Find a decryption exponent d corresponding to the encryption exponent $e = 7$ in \mathbb{Z}_{187} .

2. Show that if $p \in \mathbb{N}$ is a prime number then the set

$$GL_2(\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_p \text{ with } ad - bc \neq 0 \right\}$$

is a finite non-abelian group.