Algebraic and Geometric Methods in Engineering and Physics

Homework 3

Due on October 2

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 $p > 2$ is prime then any element $[a] \in \mathbb{Z}_p \setminus \{0\}$ has either two or zero square roots. Is this true if p is not prime?