
2. Let $p$ be an odd prime number. Let $a \in \mathbb{Z}$ be an integer not divisible by $a$.

   (i) Show that the residue class $[a]$ of $a$ in $\mathbb{Z}_p$ satisfies either
   
   \begin{align*}
   (*) & \quad [a]^{p-1} = [1] \\
   \text{or} & \quad (**) [a]^{p-1} = [-1] = [p-1].
   \end{align*}

   (ii) There are $p-1$ residue classes in $\mathbb{Z}_p$ not equal to $[0]$. How many of them satisfy equation $(*)$? How many satisfy equation $(**)$?

   (Hint: If you don’t know the answer, you can check $p = 3$, $p = 5$, $p = 7$, and formulate a guess for the general case based on what you observe. Then you can try to prove your guess.)