# Quiz 4

Student ID Number: Name _____

Math 173B, 1PM

Please justify all your answers February 20, 2020

Please also write your full name on the back

1. True or false?

   (a) Let $E$ be an elliptic curve over the finite field $\mathbb{F}_{p^k}$. Then for any integer $m$, the $m$-torsion subgroup $E(\mathbb{F}_{p^k})[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

   (b) The Weil pairing, $e_m : E(\mathbb{F}_q)[m] \to \mathbb{F}_q^\times$ satisfies $e_m(P, P) = 1$ for all $P \in E(\mathbb{F}_q)[m]$.

2. Let $E$ be an elliptic curve over $\mathbb{F}_q$ and let $P \in E(\mathbb{F}_q)[\ell]$ be a point of prime order such that there is an $\ell$-distortion map for $P$. Let $\hat{e}_\ell$ be the associated modified Weil pairing. Show that you can use $\hat{e}_\ell$ to solve the decision Diffie-Hellman problem. That is, given $aP$, $bP$, and $cP$, show that we can decide whether $abP = cP$.