Quiz 3

Student ID Number: Name __________________________
Math 173B, 1PM
Please justify all your answers January 30, 2020
Please also write your full name on the back

1. True or False?

   (a) The usual formula for the addition law on an elliptic curve works over $\mathbb{Z}/N\mathbb{Z}$ for any integer $N > 0$.

   (b) If $P = (x, y)$ is a point on the elliptic curve E defined over $\mathbb{F}2^k$ for some $k \geq 1$, then $-P = (x, -y)$.

2. Let E be an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ where N is a composite integer with unknown factorization. You (correctly) program a computer to add points on the curve using the usual point addition formula. You tell your program to compute $2P$ for some point P on E and it gives you an error. Briefly explain how you can use this error to factor N.