

Quiz 6

Student ID Number:

Name _____

Math 140B, 1PM

Please justify all your answers

February 21, 2019

Please also write your full name on the back

1. List the points on the elliptic curve $Y^2 = X^3 + 2X + 3$ over \mathbb{F}_7 .
2. Let P be a point on an elliptic curve. How many point operations (additions and doublings) does it take to compute $255P$ when using the double-and-add algorithm? What if the ternary expansion is used?
3. How many points of order two are on the elliptic curve $Y^2 = X^3 + X$ over any field with characteristic not equal to 2 or 3?