Week 10 Monday

Make sure you're sitting next to someone!

Moar Practice

Make sure you know your neighbors' names, and then discuss:

What's a topic (besides elliptic curves) that we've discussed this quarter that you think you could use more practice with?

Elliptic Curves

1. Which of the following Weierstrass equations over the reals cannot be singular, no matter what b is chosen to be?

(A) $y^2 = x^3 + b$

(B) $y^2 = x^3 - x + b$

(C) $y^2 = x^3 + x + b$

(D) None of the above OR more than one of the above

2. Which of the following Weierstrass equations mod $p = 5$ cannot be singular, no matter what b is chosen to be?

(A) $y^2 = x^3 + b$

(B) $y^2 = x^3 - x + b$

(C) $y^2 = x^3 + x + b$

(D) None of the above OR more than one of the above

3. Consider the elliptic curve E over the reals defined by $y^2 = x^3 + 8$. Verify that $P = (1, 3)$ is a point on this curve, and then compute $2P$.

Do this in stages, and compare intermediate calculations with your neighbors as you go! Here are some *examples* of intermediate steps you could compare:

- What is the equation of the tangent line through P?
- What is the "third" point of intersection of that line with E?

Make sure you're on the same page as your neighbors as you do this calculation!

4. Consider the elliptic curve E mod $p = 5$ defined by $y^2 = x^3 + 8$. Verify that $P = (1, 2)$ and $Q = (1, 3)$ are point on this curve, and then compute $P + Q$.

Again, do this in stages and compare intermediate calculations with your neighbors as you go!

5. The following points are all on the elliptic curve mod $p = 7$ defined by $y^2 = x^3 + x$. Which of them has order 2?

(A) $(1, 3)$

(B) $(1, 4)$

(C) $(0, 0)$

(D) $(5, 5)$