# Week 9 Thursday

## 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? Do you have a plan for how you'll go about practicing that topic more?

# Elliptic Curves Mod a Prime

1. 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!

2. 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) $(5, 5)$