Week 10 Wednesday

Make sure you're sitting next to someone!

Quadratic Residues, ECC

1. Which of the following is *not* a quadratic residue mod 13?

(A) 3

(B) 4

(C) 5

(D) 9

2. What is $\left(\frac{2}{7}\right)$?

(A) 1

(B) -1

(C) 0

3. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice must pick a secret integer a. From which range should this secret integer be chosen?

(A) $0 \leqslant a < 5$

(B) $0 \leqslant a < 11$

(C) $0 \leqslant a < 18$

(D) None of the above

4. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice picks the secret integer $a = 11$. What does she send Bob?

(Just write down an outline of *how* she'll do this calculation; you don't need to do this calculation out in full by hand...)

5. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice picks the secret integer $a = 11$. She receives $Q_b = (10, 10)$ from Bob. What is her shared secret with Bob?

(Again, just write down an outline of *how* she'll do this calculation; you don't need to do this calculation out in full by hand...)