Solutions to Daily Due Oct 16 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

Throughout, $E : y^2 = x^3 + x + 1 \pmod{11}$ *and* $P = (1, 5)$*. The key idea for the whole sheet: the table says every point of* E *is* kP *for some* k*, and* $kP + \ell P = (k + \ell)P$*. So adding points is just adding the labels* k *modulo* 14*.*

k	kP	k	kP
1	$(1, 5)$	8	$(0, 1)$
2	$(3, 3)$	9	$(4, 5)$
3	$(8, 2)$	10	$(6, 6)$
4	$(6, 5)$	11	$(8, 9)$
5	$(4, 6)$	12	$(3, 8)$
6	$(0, 10)$	13	$(1, 6)$
7	$(2, 0)$	14	∞

Problem 1: the number of points and Hasse's bound

The table lists 13 affine points plus ∞, so

$$\#E = 14.$$

(Checked by brute force: exactly 13 pairs (x, y) modulo 11 satisfy the equation.) Hasse's bound says $|\#E - (p+1)| \le 2\sqrt{p}$. Here $p+1 = 12$ and $2\sqrt{11} \approx 6.63$, so the allowed range is $5.37 \le \#E \le 18.63$, i.e. $6 \le \#E \le 18$. And $|14 - 12| = 2 \le 6.63$. ✓

Problem 2: curves modulo 13

For $p = 13$: $p + 1 = 14$ and $2\sqrt{13} \approx 7.21$, so

$$14 - 7.21 \le \#E \le 14 + 7.21, \qquad \text{i.e.} \qquad 7 \le \#E \le 21$$

(the number of points is an integer, so round inward). The minimum is 7 and the maximum is 21.

Problem 3: addition by table lookup

$(3, 3) + (8, 9)$**.** From the table, $(3, 3) = 2P$ and $(8, 9) = 11P$, so

$$(3, 3) + (8, 9) = 2P + 11P = 13P = (1, 6).$$

$(6,5) + (6,5)$**.** $(6,5) = 4P$, so

$$(6,5) + (6,5) = 4P + 4P = 8P = (0,1).$$

(These agree with the chord and tangent formulas, checked by computer.)

Problem 4: $-(4,6)$

$(4,6) = 5P$, and $5P + 9P = 14P = \infty$, so

$$-(4,6) = 9P = (4,5).$$

Geometrically, $-Q$ is the reflection of Q in the x-axis: $-(4,6) = (4,-6) = (4,5)$ modulo 11. The two answers agree. In general $-(kP) = (14-k)P$, which is why the table's right column reflects its left column: $13P = (1,6) = -(1,5)$, $12P = (3,8) = -(3,3)$, and so on.

Problem 5: orders

The order of $7P = (2,0)$ is 2: $7P + 7P = 14P = \infty$, and $7P \neq \infty$. This is problem 5 from the daily due October 12th. A point with $y = 0$ has a vertical tangent line, so $2Q = \infty$; equivalently $-Q = (x,-0) = Q$. So $(2,0)$ is the only point of order 2, since it is the only point with $y = 0$.

In general, kP has order $14/\gcd(k,14)$, since $m(kP) = \infty$ exactly when $14 \mid mk$.

- **Order 7:** $\gcd(k,14) = 2$, so $k = 2,4,6,8,10,12$: the points

$$(3,3),\ (6,5),\ (0,10),\ (0,1),\ (6,6),\ (3,8).$$

- **Order** 14**:** $\gcd(k,14) = 1$, so $k = 1,3,5,9,11,13$: the points

$$(1,5),\ (8,2),\ (4,6),\ (4,5),\ (8,9),\ (1,6).$$

Together with ∞ (order 1) and $(2,0)$ (order 2), that accounts for all 14 points. This is exactly like a cyclic group $\mathbb{Z}/14\mathbb{Z}$, or like $(\mathbb{Z}/p\mathbb{Z})^*$ with a primitive root: the generators are the $\varphi(14) = 6$ values of k coprime to 14.

Problem 6: the ECDLP

Lookup: $(6,6)$ is in the row $k = 10$, so

$$k = 10 \qquad (10P = (6,6)),$$

and k is unique modulo 14.

Why this doesn't scale. For a curve modulo a 256-bit prime, Hasse says $\#E \approx p \approx 2^{256} \approx 10^{77}$. The table would need about 10^{77} rows, roughly the number of atoms in the universe, so it can't be computed or stored.

Why fast multiplication doesn't help. Double-and-add computes any *single* kP from k in about $2\log_2 k \approx 512$ group operations. That is the easy direction. The DLP asks for the reverse:

given the *output* Q, find k. Being able to compute kP quickly for a k you choose only lets you guess and check, and a random guess is right with probability about $1/\#E$. The multiples kP jump around the curve with no visible pattern relating k to the coordinates of kP, just as $g^k \bmod p$ did, so there is nothing to steer a search. The best general attacks (baby-step giant-step, Pollard ρ) take about $\sqrt{\#E} \approx 2^{128}$ steps. Unlike $(\mathbb{Z}/p\mathbb{Z})^*$, a general elliptic curve has no "factor base" (no notion of a small point), so index calculus is not available.

Problem 7: Elliptic Curve Diffie-Hellman

Copy Diffie-Hellman, replacing "g^a" with "aP":

1. **Public:** Alice and Bob agree on a curve E modulo a prime p and a point P on E (ideally of large prime order).
2. **Private choices:** Alice picks a secret integer a, and Bob picks a secret integer b.
3. **Exchange:** Alice sends $A = aP$, and Bob sends $B = bP$ (both by double-and-add).
4. **Shared secret:** Alice computes $aB = abP$, and Bob computes $bA = baP$. These are the same point.

An eavesdropper sees E, P, A, B, and recovering abP from these is the elliptic curve Diffie-Hellman problem. It would follow from solving the ECDLP (problem 6). In practice the shared secret is usually the x-coordinate of abP.

Example with the table: Alice picks $a = 4$ and sends $A = 4P = (6, 5)$. Bob picks $b = 9$ and sends $B = 9P = (4, 5)$. Both get $36P = 8P = (0, 1)$, since $36 \equiv 8 \pmod{14}$.