Solutions to Daily Due Oct 12 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

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

Conventions as in lecture. To add P and Q: (1) take the line L through P and Q (the tangent line if $P = Q$), and find its third intersection point R with E; (2) $P + Q = -R$, the second intersection of the vertical line through R with E. Writing L as $y = \lambda x + \nu$ and substituting into $y^2 = x^3 + ax + b$ gives the cubic $x^3 - \lambda^2 x^2 + \cdots = 0$, whose three roots are x_P, x_Q, x_R. Since the sum of the roots is λ^2 (the trace trick from lecture),

$$x_R = \lambda^2 - x_P - x_Q, \qquad y_R = \lambda x_R + \nu = \lambda(x_R - x_P) + y_P, \qquad P + Q = (x_R, -y_R).$$

Every division is a modular inverse.

Problem 1: $P + Q$ on $E : y^2 = x^3 + x + 1 \pmod 7$

$P = (0, 1)$ and $Q = (2, 2)$ are on E: $1 = 0 + 0 + 1$ and $4 \equiv 8 + 2 + 1 = 11$.

Line through P and Q:

$$\lambda = \frac{2 - 1}{2 - 0} = \frac{1}{2} \equiv 1 \cdot 4 = 4 \pmod 7 \quad (\text{since } 2 \cdot 4 = 8 \equiv 1),$$

and the y-intercept is $\nu = 1$ (the line passes through $(0, 1)$), so $L : y \equiv 4x + 1$.

Third intersection: substituting, $(4x + 1)^2 \equiv x^3 + x + 1$, i.e. $x^3 - 16x^2 - 7x \equiv x^3 - 2x^2 \equiv 0 \pmod 7$. The sum of the roots is $2 = \lambda^2$, and two roots are 0 and 2, so $x_R = 2 - 0 - 2 = 0$ and $y_R = 4 \cdot 0 + 1 = 1$: $R = (0, 1)$. (Check: $x^3 - 2x^2 = x^2(x - 2)$ has roots $0, 0, 2$; the line is tangent to E at P.)

Reflect:

$$P + Q = -R = (0, -1) = (0, 6).$$

Check: $6^2 = 36 \equiv 1 = 0^3 + 0 + 1$. ✓

Problem 2: $P + \infty$

∞ is the identity of the group, so $P + \infty = P = (0, 1)$. Geometrically, the "line through P and ∞" is the vertical line $x = 0$, whose third intersection is $R = (0, 6) = -P$, and reflecting gives back P.

Problem 3: $-P$

The inverse is the reflection in the x-axis: $-P = (0,-1) = (0,6)$. Indeed the vertical line $x = 0$ meets E at $(0,1)$, $(0,6)$ and ∞, so $(0,1) + (0,6) + \infty = \infty$.

Notice that problem 1 gave $P + Q = -P$.

Problem 4: $Q + Q$ by the tangent line

Differentiating $y^2 = x^3 + x + 1$ implicitly gives $2y\,y' = 3x^2 + 1$, so at $Q = (2,2)$ the tangent slope is

$$\lambda = \frac{3 \cdot 2^2 + 1}{2 \cdot 2} = \frac{13}{4} \equiv \frac{6}{4} \equiv 6 \cdot 2 = 12 \equiv 5 \pmod 7 \quad (\text{since } 4 \cdot 2 = 8 \equiv 1).$$

The tangent line is $y \equiv 5x + \nu$ with $2 \equiv 5 \cdot 2 + \nu$, so $\nu \equiv 2 - 10 \equiv 6$: $L : y \equiv 5x + 6$.

The roots of the cubic are $2, 2, x_R$ (the point of tangency counts twice) with sum $\lambda^2 = 25 \equiv 4$, so

$$x_R = 4 - 2 - 2 = 0, \qquad y_R = 5 \cdot 0 + 6 = 6, \qquad R = (0,6).$$

Therefore

$$2Q = Q + Q = -R = (0,1) = P.$$

Check: $(0,1)$ is on E. ✓(In fact the points of this curve are $\infty, (0,1), (0,6), (2,2), (2,5)$, five in all, and $P, 2P = (2,5), 3P = (2,2) = Q, 4P = (0,6), 5P = \infty$: a cyclic group of order 5 generated by P. That is why $2Q = 6P = P$ and $P + Q = 4P = -P$.)

Problem 5: if $P = (x,0)$ then $2P = \infty$

The tangent slope at P is $\lambda = (3x^2 + a)/(2y)$, and $y = 0$ makes the denominator zero: the tangent line at P is *vertical*, $X = x$. A vertical line meets E at (x,y), $(x,-y)$ and ∞; here $(x,0)$ is its own reflection, so the three intersections are P, P (tangency) and ∞. The third intersection point is $R = \infty$ and $2P = -R = \infty$.

Equivalently: $-P = (x,-0) = (x,0) = P$, so $P + P = P + (-P) = \infty$. Points with $y = 0$ are exactly the points of order 2.

Problem 6: $(3,3) + (1,2)$ on $y^2 = x^3 + 2x + 1 \pmod 5$

Both points are on the curve: $9 \equiv 4 \equiv 27 + 6 + 1 = 34$ and $4 = 1 + 2 + 1$.

$$\lambda = \frac{2-3}{1-3} = \frac{-1}{-2} = \frac{1}{2} \equiv 3 \pmod 5 \quad (2 \cdot 3 = 6 \equiv 1).$$

Line: $y \equiv 3x + \nu$ with $3 \equiv 9 + \nu$, so $\nu \equiv -6 \equiv 4$: $L : y \equiv 3x + 4$. Then

$$x_R = \lambda^2 - 3 - 1 = 9 - 4 = 5 \equiv 0, \qquad y_R = 3 \cdot 0 + 4 = 4, \qquad R = (0,4),$$

and

$$(3,3) + (1,2) = -R = (0,-4) = (0,1).$$

Check: $1^2 = 1 = 0 + 0 + 1$. ✓

Problem 7: $(0,6)+(0,1)$ on $y^2 = x^3 + 2x + 1 \pmod 7$

The slope would be

$$\lambda = \frac{1-6}{0-0} = \frac{-5}{0},$$

and 0 has no inverse modulo 7: the computation fails at the very first step. That is the signal. The two points have the same x-coordinate (and $6 \equiv -1$, so they are reflections of each other), so the line through them is the vertical line $x = 0$, whose third intersection with E is ∞. Hence

$$(0,6) + (0,1) = \infty,$$

i.e. $(0,1) = -(0,6)$. In general, "denominator is 0 modulo p" when adding $P \neq Q$ means $x_P = x_Q$, hence $Q = -P$ and the sum is ∞.

Problem 8: $(28,13)+(21,22)$ on $y^2 = x^3 + 2x + 1 \pmod{35}$

Both points are on the curve modulo 35: $13^2 = 169 \equiv 29$ and $28^3 + 56 + 1 = 22009 \equiv 29$; $22^2 = 484 \equiv 29$ and $21^3 + 42 + 1 = 9304 \equiv 29$.

The slope would be

$$\lambda = \frac{22-13}{21-28} = \frac{9}{-7} = \frac{9}{28} \pmod{35},$$

and 28 (equivalently 7) has **no inverse modulo** 35, because $\gcd(28, 35) = 7 \neq 1$. The computation fails, but the failure is informative: the gcd that blocks the inverse is a proper factor,

$$\gcd(28, 35) = 7, \qquad 35 = 5 \cdot 7.$$

Relationship to problems 6 and 7. By the Chinese Remainder Theorem, working modulo 35 is the same as working modulo 5 and modulo 7 at once, and the two given points reduce to exactly the earlier problems:

$$(28,13) \equiv (3,3), \quad (21,22) \equiv (1,2) \pmod 5; \qquad (28,13) \equiv (0,6), \quad (21,22) \equiv (0,1) \pmod 7.$$

Modulo 5 the addition goes through fine (problem 6: the sum is $(0,1)$). Modulo 7 the two points are inverses of each other, the line through them is vertical, and the sum is ∞ (problem 7). So modulo 35 the "sum" would have to be a finite point modulo 5 and ∞ modulo 7 at the same time, which is not a point at all; what we see instead is a denominator $x_Q - x_P = -7$ that is zero modulo 7 but nonzero modulo 5, so its gcd with 35 picks out the prime 7. Doing elliptic curve arithmetic modulo a composite n and waiting for a denominator that shares a factor with n is the idea behind Lenstra's elliptic curve factoring method.