Solutions to Daily Due Oct 14 (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. $\mathbb{P}^k_F$ *is the set of nonzero vectors in* F^{k+1} *modulo length:* $\vec{v}_1 \sim \vec{v}_2$ *iff* $\vec{v}_1 = \lambda \vec{v}_2$ *for some* $\lambda \in F^* = F \setminus \{0\}$. *The equivalence class of* $(a_0, \ldots, a_k)$ *is written* $[a_0, \ldots, a_k]$. *Problem 1 (compare with the previous solutions) and problem 4 (the video) have no written solution.*

Problem 2: four vectors in $\mathbb{R}^2$ with the same image in $\mathbb{P}^1_{\mathbb{R}}$

Any nonzero multiples of one vector will do. For example

$$(1,2), \qquad (2,4), \qquad (-1,-2), \qquad (\tfrac{1}{2},1)$$

are four different vectors in $\mathbb{R}^2$, and each is a nonzero scalar multiple of $(1,2)$ (by 1, 2, -1 and $\frac{1}{2}$), so

$$[1,2] = [2,4] = [-1,-2] = [\tfrac{1}{2},1] \quad \text{in } \mathbb{P}^1_{\mathbb{R}}.$$

Geometrically, all four lie on the line through the origin of slope 2, and that line is the single point of $\mathbb{P}^1_{\mathbb{R}}$ they represent. (Over $\mathbb{R}$ there are infinitely many vectors in each class, one for every $\lambda \in \mathbb{R}^*$.)

Problem 3: one colour class of $\mathbb{P}^2_{\mathbb{F}_3}$, and the total count

In $\mathbb{F}_3$ the nonzero scalars are $\mathbb{F}_3^* = \{1,2\}$, so each class consists of a vector $\vec{v}$ and $2\vec{v}$. Take, for instance, the class of $(1,1,2)$:

$$2 \cdot (1,1,2) = (2,2,4) \equiv (2,2,1) \pmod 3, \qquad \text{so} \qquad [1,1,2] = [2,2,1],$$

exactly the example from lecture. Check: $(2,2,1) = 2 \cdot (1,1,2)$ and $(1,1,2) = 2 \cdot (2,2,1)$ (since $2 \cdot 2 = 4 \equiv 1$), so the two vectors are equivalent and the class contains nothing else. Any other colour works the same way; e.g. $[1,0,0] = [2,0,0]$, $[0,1,2] = [0,2,1]$, $[1,2,0] = [2,1,0]$.

Total. $\mathbb{F}_3^3$ has $3^3 = 27$ vectors, of which 26 are nonzero. Every class has exactly 2 elements, so there are

$$|\mathbb{P}^2_{\mathbb{F}_3}| = \frac{26}{2} = 13$$

points in the projective plane over $\mathbb{F}_3$. (Listing them by the first nonzero coordinate: four of the form $[0,0,1]$, $[0,1,0]$, $[0,1,1]$, $[0,1,2]$ with first coordinate 0, and nine of the form $[1,y,z]$ with $y, z \in \mathbb{F}_3$; $4 + 9 = 13$.)

Problem 5: all the elements of $\mathbb{P}^1_{\mathbb{F}_5}$

Now $\mathbb{F}_5^* = \{1,2,3,4\}$, so each class has four vectors: $\vec{v}, 2\vec{v}, 3\vec{v}, 4\vec{v}$. There are $5^2 - 1 = 24$ nonzero vectors in $\mathbb{F}_5^2$, giving $24/4 = 6$ classes:

$$\begin{aligned}
[0,1] &= \{(0,1),\ (0,2),\ (0,3),\ (0,4)\} \quad \text{(the vertical line, "slope } \infty\text{")} \\
[1,0] &= \{(1,0),\ (2,0),\ (3,0),\ (4,0)\} \quad \text{(slope 0)} \\
[1,1] &= \{(1,1),\ (2,2),\ (3,3),\ (4,4)\} \quad \text{(slope 1)} \\
[1,2] &= \{(1,2),\ (2,4),\ (3,1),\ (4,3)\} \quad \text{(slope 2)} \\
[1,3] &= \{(1,3),\ (2,1),\ (3,4),\ (4,2)\} \quad \text{(slope 3)} \\
[1,4] &= \{(1,4),\ (2,3),\ (3,2),\ (4,1)\} \quad \text{(slope 4)}
\end{aligned}$$

For example $3 \cdot (1,2) = (3,6) \equiv (3,1)$ and $4 \cdot (1,2) = (4,8) \equiv (4,3)$. As with $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$, the six points are the five slopes $0,1,2,3,4 \in \mathbb{F}_5$ together with ∞: $\mathbb{P}^1_{\mathbb{F}_5} = \mathbb{F}_5 \cup \{\infty\}$.

Problem 6: class sizes and $|\mathbb{P}^k_{\mathbb{F}_p}|$ in general

Each class is $\{\lambda\vec{v} : \lambda \in \mathbb{F}_p^*\}$, and the $p-1$ vectors $\lambda\vec{v}$ are all different (if $\lambda\vec{v} = \mu\vec{v}$ then $(\lambda-\mu)\vec{v} = \vec{0}$, so $\lambda = \mu$ since $\vec{v} \neq \vec{0}$). So **every class has exactly $p-1$ vectors**: 2 for $p=3$, 4 for $p=5$, as above.

There are $p^{k+1} - 1$ nonzero vectors in $\mathbb{F}_p^{k+1}$, so

$$|\mathbb{P}^k_{\mathbb{F}_p}| = \frac{p^{k+1}-1}{p-1} = p^k + p^{k-1} + \cdots + p + 1.$$

Checks: $\mathbb{P}^1_{\mathbb{F}_3}$ has $(9-1)/2 = 4$ points, $\mathbb{P}^1_{\mathbb{F}_5}$ has $(25-1)/4 = 6$, and $\mathbb{P}^2_{\mathbb{F}_3}$ has $(27-1)/2 = 13$, matching problems 3 and 5 and the lecture. (The sum form says the same thing as the chart picture: $\mathbb{P}^k_{\mathbb{F}_p}$ is an affine piece $\mathbb{F}_p^k$, with p^k points, plus a copy of $\mathbb{P}^{k-1}_{\mathbb{F}_p}$ at infinity. For the projective line, $p+1$ points: p slopes and ∞.)

Problem 7: the points of $y^2 = xy - 1$ at infinity

Homogenize. Substituting $x = X/Z$, $y = Y/Z$ and clearing denominators (every term must have the same degree, here 2):

$$Y^2 = XY - Z^2.$$

Its points are the $[X,Y,Z] \in \mathbb{P}^2$ satisfying this equation; the substitution makes sense on classes because scaling (X,Y,Z) by λ scales both sides by λ^2.

The affine part $Z \neq 0$. Scaling so that $Z = 1$ gives back $y^2 = xy - 1$: these are the points of the original curve.

The line at infinity $Z = 0$. The equation becomes $Y^2 = XY$, i.e. $Y(Y - X) = 0$, so $Y = 0$ or $Y = X$.

- $Y = 0$: the points $[X,0,0]$ with $X \neq 0$, which are all the single point $[1,0,0]$.
- $Y = X$: the points $[X,X,0]$ with $X \neq 0$, which are all the single point $[1,1,0]$.

So the curve has exactly **two points on the line at infinity**, $[1,0,0]$ and $[1,1,0]$. They correspond to the slopes 0 and 1 of the two asymptotic directions: writing $y^2-xy+1=0$ as $y=\left(x\pm\sqrt{x^2-4}\right)/2$, for large x the two branches look like $y\approx 0$ and $y\approx x$. (Compare the elliptic curve from lecture, $Y^2Z=X^3+aXZ^2+bZ^3$, where $Z=0$ forces $X^3=0$ and leaves only the one point $[0,1,0]$.)

Problem 8: vertical lines pass through $[0,1,0]$

The affine vertical line $x=c$ homogenizes to $X=cZ$ (degree 1 on both sides). The point $[0,1,0]$ satisfies it: $X=0$ and $cZ=c\cdot 0=0$. So every vertical line, whatever c is, passes through the same point at infinity $[0,1,0]=\infty$ of the elliptic curve. (A non-vertical line $y=\lambda x+\nu$ homogenizes to $Y=\lambda X+\nu Z$, and at $[0,1,0]$ this reads $1=0$: those lines miss ∞.)

This is what the group law from last week was using. The three intersection points of the vertical line $X=cZ$ with E are the two affine points $(c,\pm d)$, which are the pair P and $-P$, and the point $\infty=[0,1,0]$. The rule "$P+Q+R=\infty$ when P,Q,R are the three intersections with a line" therefore gives $P+(-P)+\infty=\infty$, i.e. $P+(-P)=\infty$, and ∞ really is a point of the curve, not just a symbol.