2) Argue tha the points incident with the line

$$a = (a_1, -1, a_3) \text{ are } (x, a_1x + a_3, 1) \text{ ad } (1, a_1, 0)$$

where $x \in GF(p)$. Explain why these are, or are not, all the points incident with the line

For a point to lie on a line in $GF(p)$, $x \cdot a$ must equal zero. For the point $(x, a_1x + a_3, 1)$, $x \cdot a$ is

$$\begin{aligned}(x, a_1x + a_3, 1) \cdot (a_1, -1, a_3) &= xa_1 - (a_1x + a_3) + a_3, \\ &= (xa_1 - a_1x) + (a_3 - a_3), \\ &= 0.\end{aligned}$$

$(x, a_1x + a_3, 1)$ is incident with the line $(a_1, -1, a_3)$. For $(1, a_1, 0)$.

$$\begin{aligned}(1, a_1, 0) \cdot (a_1, -1, a_3) &= a_1 - a_1 + 0, \\ &= 0.\end{aligned}$$

$(1, a_1, 0)$ is incident with the line $(a_1, -1, a_3)$. We know the geometry of $PG(2, p)$ mandates that each line be incident with $p + 1$ points. Since $x \in GP(p)$ while a_1 and a_3 remain constant, the point $(x, a_1x + a_3, 1)$ accounts for p points alone the line $(a_1, -1, a_3)$. The last of these $p + 1$ points is accounted for by the point $(1, a_1, 0)$. We have accounted for all $p + 1$ points on the line.

5) Establish that each pair of lines intersects at a unique point.

Lines in $PG(2, p)$ are isomorphic to vectors in $GF(p)^3$ so we can write two unique lines as

$$l_1 = (a_1, a_2, a_3) \text{ and } l_2 = (a_4, a_5, a_6).$$

A point that is incident to both l_1 and l_2 must satisfy

$$\begin{aligned}p \cdot l_1 = 0 &= x_1a_1 + x_2a_2 + x_3a_3, \\ p \cdot l_2 = 0 &= x_1a_4 + x_2a_5 + x_3a_6.\end{aligned}$$

Written in matrix form, these equations become

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

In our geometry, if l_1 and l_2 are unique lines, they must be linearly independent in their coefficients. As a result, the coefficient matrix by necessity has rank two. Given three unknowns and a rank two matrix, the infinite family of solutions to this under-determined system of linear equations must form a one dimensional vector space, or a space of scalar multiples of a single vector. In $PG(2, p)$, points are isomorphic to vectors in $GP(p)^3$, and we equate all points that are scalar multiples of each other. Thus, this system has one unique solution.

6) Show that (0,2,1), (2,4,1), and (5,4,1) unlock secret (1,3,0) in the example at the end of the module

Given the bases of V_d and π, we can map our representation of $PG(2, p)$ to π by

$$\begin{aligned}(\alpha, \beta, \gamma) \mapsto \alpha(4, 1, 0, 6, 2) + \beta(1, 5, 3, 6, 1) + \gamma(0, 1, 5, 5, 2), \\ = (4\alpha + \beta, \alpha + 5\beta + \gamma, 3\beta + 5\gamma, 6\alpha + 6\beta + 5\gamma, 2\alpha + \beta + 2\gamma).\end{aligned}$$

The given codes mapped to π under mod (7) are then:

$$(0,2,1) \mapsto (2,4,4,3,4),$$
$$(2,4,1) \mapsto (5,2,3,6,3),$$
$$(5,4,1) \mapsto (3,5,3,3,2).$$

The secret being in both V_d and π means that

$$\begin{aligned}(s_1,s_2,s_3,s_4,s_5) &= \alpha(2,4,4,3,4)+\beta(5,2,3,6,3)+\gamma(3,5,3,3,2)\\ &= \rho(6,6,2,2,2)+\sigma(4,5,0,4,5)+\nu(2,6,0,2,2)\end{aligned}$$

These equalities yield the following system of five linear equations

$$\begin{bmatrix}2&5&3&-6&-4&-2\\4&2&5&-6&-5&-6\\4&3&3&-2&0&0\\3&6&3&-2&-4&-2\\4&3&2&-2&-5&-2\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\\\rho\\\sigma\\\nu\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}.$$

Row reducing over mod(7) arithmetic yields

$$\begin{bmatrix}1&0&0&0&6&0\\0&1&0&0&3&0\\0&0&1&0&5&0\\0&0&0&1&3&0\\0&0&0&0&0&1\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\\\rho\\\sigma\\\nu\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}.$$

The first three equations give

$$(\alpha,\beta,\gamma)=\sigma(-6,-3,-5)=\sigma(1,4,2).$$

Our secret then is

$$\begin{aligned}(s_1,s_2,s_3,s_4,s_5) &= \sigma((2,4,4,3,4)+4(5,2,3,6,3)+2(3,5,3,3,2)),\\ &= \sigma(0,1,1,5,6).\end{aligned}$$

To get the three digit code for the secret we need to solve

$$(4\alpha+\beta,\alpha+5\beta+\gamma,3\beta+5\gamma,6\alpha+6\beta+5\gamma,2\alpha+\beta+2\gamma)=\sigma(0,1,1,5,6).$$

In matrix form this is

$$\begin{bmatrix}4&1&0\\1&5&1\\0&3&5\\6&6&5\\2&1&2\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\end{pmatrix}=\sigma\begin{pmatrix}0\\1\\1\\5\\6\end{pmatrix}.$$

Row reducing the augmented matrix results in

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\\0&0&0\\0&0&0\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\end{pmatrix}=\sigma\begin{pmatrix}4\\5\\0\\0\\0\end{pmatrix},$$

yielding $(\alpha,\beta,\gamma)=\sigma(4,5,0)$. By letting $\sigma=2$ we can normalize in the first digit giving

$$s=(1,3,0)$$

as expected.

7) Show that (3,2,1) and (5,4,1) fail to unlock the secret (1,3,0) in the example at the end of the module.

Given the bases of V_d and π, we can map our representation of $PG(2,p)$ to π by

$$\begin{aligned}(\alpha,\beta,\gamma) &\mapsto \alpha(4,1,0,6,2)+\beta(1,5,3,6,1)+\gamma(0,1,5,5,2),\\ &= (4\alpha+\beta,\alpha+5\beta+\gamma,3\beta+5\gamma,6\alpha+6\beta+5\gamma,2\alpha+\beta+2\gamma).\end{aligned}$$

The given codes mapped to π under mod (7) are then:

$$\begin{aligned}(3,2,1)&\mapsto(0,0,4,0,3),\\ (5,4,1)&\mapsto(3,5,3,3,2).\end{aligned}$$

The secret being in both V_d and π means that

$$\begin{aligned}(s_1,s_2,s_3,s_4,s_5) &= \alpha(0,0,4,0,3)+\beta(3,5,3,3,2)\\ &= \rho(6,6,2,2,2)+\sigma(4,5,0,4,5)+\nu(2,6,0,2,2)\end{aligned}$$

These equalities yield the following system of five linear equations

$$\begin{bmatrix}0&3&-6&-4&-2\\0&5&-6&-5&-6\\4&3&-2&0&0\\0&3&-2&-4&-2\\3&2&-2&-5&-2\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\rho\\\sigma\\\nu\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}.$$

Row reducing over mod(7) yields

$$\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{pmatrix}\alpha\\\beta\\\rho\\\sigma\\\nu\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}.$$

This tells us that the multipliers must all be zero which would yield a secret comprised of zeros. Not only is this not the secret, it is a point we exclusively excluded from $PG(2,7)$.

8) Show that

Level 1 Codes	**(0,2,1), (10,10,1), (9,7,1), (8,4,1)**
Level 2 Codes	**(1,1,1), (5,3,1), (6,3,1), (0,1,0)**

is a valid secret sharing scheme in $PG(2,11)$. You may assume that lines through pairs of Level 2 points do not contain the secret.

Tabulting our known codes gives

Line				
t	1	2	3	4
point	(0,2,1)	(10,10,1)	(9,7,1)	(8,4,1)
Oval				
i or j	1	2	3	4
point	(1,1,1)	(5,3,1)	(6,3,1)	(0,1,0)

First, we will show that any line through two Level 2 codes on the oval is not incident with the any Level 1 code on the line. The sixteen lines from points j to t are

j	t=1	t=2	t=3	t=4
1	(10,-1,2)	(1,-1,0)	(9,-1,3)	(2,-1,10)
2	(9,-1,2)	(8,-1,7)	(1,-1,9)	(4,-1,5)
3	(2,-1,2)	(10,-1,9)	(5,-1,6)	(6,-1,0)
4	(-1,0,0)	(-1,0,10)	(-1,0,9)	(-1,0,8)

Using the dot product to determine incidence, the matrices A^t, defined by

$$A^t_{i,j} = \begin{cases} 1, & \text{if point } j \text{ is incident to the line defined by points } t \text{ and } i \\ 0, & \text{otherwise} \end{cases}$$

are found to be

$$A^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; A^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; A^3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; A^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

An example calculation for A^1 is as follows:

Let L^t be the matrix of lines where L^t_j is the line from point j to t. Let P be a matrix whose rows are vectors of the level two points. Let D be the matrix of element-wise dot-products between L and P.

$$L \cdot P = D$$

$$\begin{bmatrix} (10,-1,2) & (10,-1,2) & (10,-1,2) & (10,-1,2) \\ (9,-1,2) & (9,-1,2) & (9,-1,2) & (9,-1,2) \\ (2,-1,2) & (2,-1,2) & (2,-1,2) & (2,-1,2) \\ (-1,0,0) & (-1,0,0) & (-1,0,0) & (-1,0,0) \end{bmatrix} \cdot \begin{bmatrix} (1,1,1) & (5,3,1) & (6,3,1) & (0,1,) \\ (1,1,1) & (5,3,1) & (6,3,1) & (0,1,) \\ (1,1,1) & (5,3,1) & (6,3,1) & (0,1,) \\ (1,1,1) & (5,3,1) & (6,3,1) & (0,1,) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 10 & 10 \\ 9 & 0 & 1 & 10 \\ 10 & 6 & 0 & 10 \\ 8 & 4 & 3 & 0 \end{bmatrix}$$

Using the fact that the dot product between a line and an incident point in $PG(2, 11)$ is zero, we can generate A^1 using the definition of $A^t_{i,j}$ above. A^1 is found to be:

$$A^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Simply indexing through t in L^t_j and reevaluating the element-wise dot-product allows one to find A^2, A^3, and A^4.

All A^t being the identity matrix shows that no secant of level 2 points on the oval is incident with a level 1 point on the line.

Next, we must show that Level 1 codes form a line that we will assume contains the secret. The line the Level 1 codes lie on can be found by taking a cross-product of two Level 1 codes. If the dot product of each Level 1 code with this line is zero, then each Level 1 code is incident with the line. First, the line $a = t_1 \times t_2$ is

$$a = (0, 2, 1) \times (10, 10, 1) = (3, 10, 2)$$
$$a = (3, -1, 2)$$

The dot products of t_1, t_2, t_3, and t_4 with a are

	t_1	t_2	t_3	t_4
$t_i \cdot a$	0	0	0	0

All level one points form a line.

Lastly, we must show that all Level 2 points form an oval that we will assume defines the plan containing the secret. In $PG(2, p)$, points on an oval are defined to be

$$\{(y, y^2, 1) : y \in GF(p)\} \cup \{(0, 1, 0)\}.$$

Creating triples of based on the first digit of each given level two code, and then taking each digit mod(11), gives

point	1	2	3	4
$(y, y^2, 1)$	(1,1,1)	(5,25,1)	(6,36,1)	(0,1,0)
mod(11)	(1,1,1)	(5,3,1)	(6,3,1)	(0,1,0)

All of our level 2 codes lie on an oval in $PG(2, 11)$.

With the assumption that no secant through Level 2 points contains the secret, we have fulfilled all of the design goals for a secret sharing scheme. All Level 1 codes form a line, all Level 2 codes form an oval, and no secant line through points on the oval of Level 2 codes is incident with any Level 1 code on the line. The given codes form a valid secret sharing scheme in $PG(2, 11)$.

9) Assume the public knowledge is

$$(9, 5, 0, 10, 9),\ (6, 7, 0, 6, 7),\ \textbf{and}\ (10, 8, 0, 10, 10).$$

What is the code for the secret in the scheme of the previous exercise if the mapping from $PG(2, 11)$ to π is

$$(\alpha, \beta,) \mapsto (\alpha, \beta, \gamma, 0, 0)?$$

Let us use the two level one codes (0,2,1) and (10,10,1). These codes mapped to π via $(\alpha.\beta, \gamma) \mapsto (\alpha, \beta, \gamma, 0, 0)$ are

$$(0, 2, 1) \mapsto (0, 2, 1, 0, 0)$$
$$(10, 10, 1) \mapsto (10, 10, 1, 0, 0)$$

The secret being in both V_d and π means that

$$\begin{aligned}(s_1, s_2, s_3, s_4, s_5) &= \alpha(0, 2, 1, 0, 0) + \beta(10, 10, 1, 0, 0) \\ &= \rho(9, 5, 0, 10, 9) + \sigma(6, 7, 0, 6, 7) + \nu(10, 8, 0, 10, 10)\end{aligned}$$

These equalities yield the following system of five linear equations

$$\begin{bmatrix} 0 & 10 & -9 & -6 & -10 \\ 2 & 10 & -5 & -7 & -8 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -10 & -6 & -10 \\ 0 & 0 & -9 & -7 & -10 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \\ \rho \\ \sigma \\ \nu \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Row reducing over mod(11) yields

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 9 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \\ \rho \\ \sigma \\ \nu \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The first two equations give

$$(\alpha, \beta) = \nu(-9, -2)$$

Our secret is then

$$\begin{aligned}(s_1, s_2, s_3, s_4, s_5) &= \nu(-9(0, 2, 1, 0, 0) - 2(10, 10, 1, 0, 0)) \\ &= \nu(2, 6, 0, 0, 0)\end{aligned}$$

Taking the inverse of our mapping from $PG(2, 11)$ to π yields $s = (2, 6, 0)$. Taking $\nu = 6$ and normalizing in the first digit yields

$$s = (1, 3, 0)$$