block = [draw,rectangle,thick,minimum height=2em,minimum width=2em]

(D) $a_0 = b$.

(A) and (D)

3 points determine a parabola.

[domain=0:4,inner sep=2pt] [very thin,color=gray] (-0.1,-1.1) grid (4.9,4.9); [-¿] (-0.2,0) – (4.2,0) node[right] ; [-¿] (0,-1.
[reddot] at (1,.5) ; [reddot] at (2,1) ; [reddot] at (3,2.5) ;
[color=red] plot[id=par3b] function0.5*x*x-x+1 node[right] $P(x) = 0.5x^2 - x + 1$; [bluedot] at (1,1.2) ; [bluedot] at (2,1

Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ points. [3]

2 points not enough.

[domain=0:4,inner sep=2pt]
[very thin,color=gray] (-0.1,-1.1) grid (4.9,4.9); [-¿] (-0.2,0) – (4.2,0) node[right] ; [-¿] (0,-1.2) – (0,4.2) node[above] ;
[bluedot] at (1,1.2) ; [bluedot] at (2,1.3) ; [orangedot] at (0,.5) ; [color=orange] plot[id=par4b] function-0.3*x*x+1*x+.5
[reddot] at (0,1.5) ; [color=red] plot[id=par6] function.2*x*x-.5*x+1.5 node[right] $P(x) = .2x^2 - .5x + 1.5$;
[greendot] at (0,-.1) ; [color=green] plot[id=par7] function-.6*x*x+1.9*x-0.1 node[right] $P(x) = -.6x^2 + 1.9x - .1$;

There is $P(x)$ contains blue points and blue *any* $(0, y)$!

Modular Arithmetic Fact and Secrets

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d+1$ pts.

Shamir's k out of n Scheme:
Secret $s \in \{0, \ldots, p-1\}$

Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1}$.

Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ with $a_0 = s$.

Share i is point $(i, P(i)p)$.

Roubustness: Any k shares gives secret.
blue Knowing k pts only one $P(x)$ evaluate $P(0)$.
Secrecy: Any $k-1$ shares give nothing.
blue Knowing $\leq k-1$ pts any $P(0)$ is possible.

Poll:example.

The polynomial from the scheme: $P(x) = 2x^2 + 1x + 3 \pmod 5$.
What is true for the secret sharing scheme using $P(x)$?

(A) The secret is "2".
(B) The secret is "3".
(C) A share could be $(1, 5)$ cuz $P(1) = 5$
(D) A share could be $(2, 4)$
(E) A share could be $(0, 3)$

From $d+1$ points to degree d polynomial?

For a line, $a_1x + a_0 = mx + b$ contains points $< 1-1 > blue(1,3)$ and $< 1-1 > blue(2,4)$.

¡1¿ Subtract first from second..

Backsolve: $b \equiv 2 \pmod 5$. blue Secret is 2.

And the line is...

Quadratic

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $< 3 > blue(1,2); < 4 > blue(2,4); < 5 > blue(3,0)$.
Plug in points to find equations.