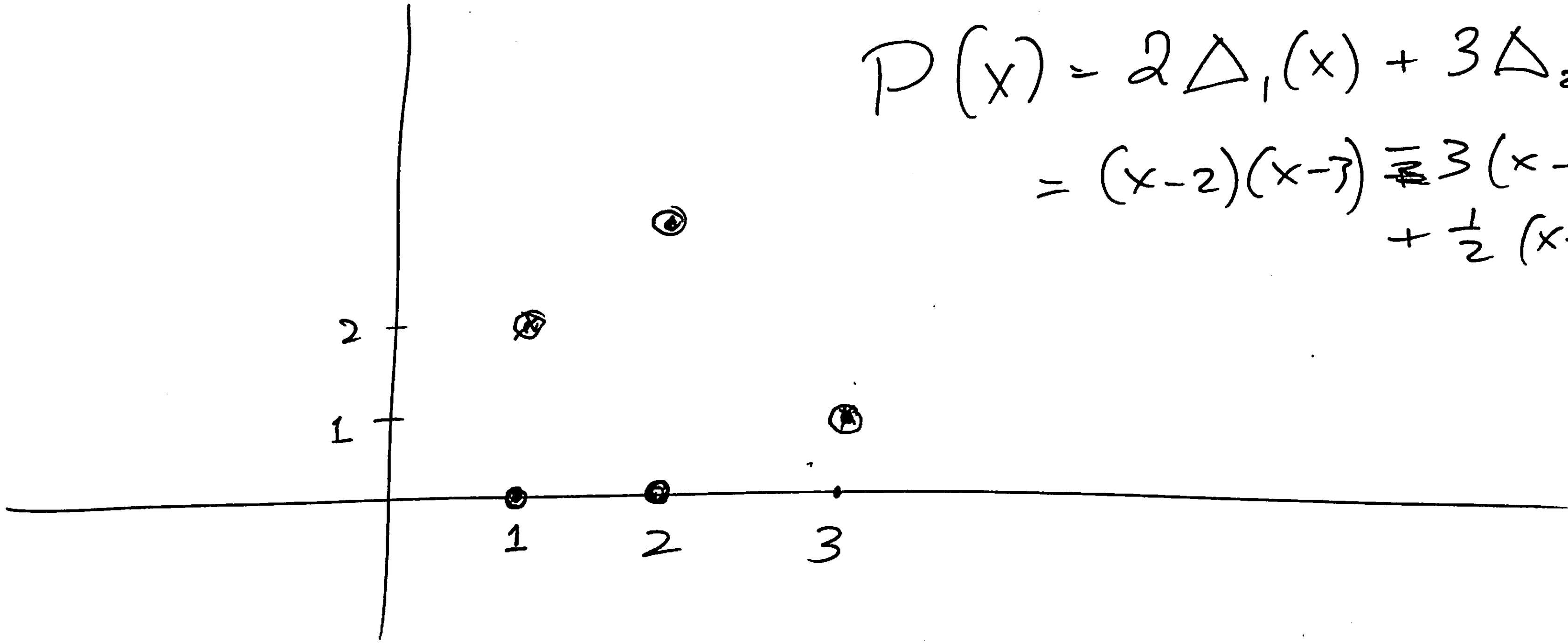
Polynomial of degree d has $\le d$ roots.



$$P(x) = 2\Delta_1(x) + 3\Delta_2(x) + \Delta_3(x).$$
$$= (x-2)(x-3) - 3(x-1)(x-3) + \tfrac{1}{2}(x-1)(x-2).$$

$P(1) = 2$ $\quad$ $P(2) = 3$ $\quad$ $P(3) = 1$.

$d+1$ values.
Unique degree d polynomial.

$\frac{1}{2}(x-1)(x-2)$

$x=1$	0
$x=2$	0
$x=3$	$\cancel{2}\ 1$

$\Delta_3(x) = \frac{1}{2}(x-1)(x-2).$

$-(x-1)(x-3)$

$x=1$	0
$x=2$	$+1$
$x=3$	0

$\Delta_2(x) = -(x-1)(x-3).$

$\frac{1}{2}(x-2)(x-3)$

$x=1$	$\cancel{2}\ 1$

$\Delta_1(x) = \frac{1}{2}(x-2)(x-3).$

Values at $d+1$ points.

$P(x_1) = y_1 \quad P(x_2) = y_2 \quad \cdots \quad P(x_{d+1}) = y_{d+1}$

Unique polynomial of degree d.

Suppose not.

$P(x)$ & $Q(x)$.

$P(x) - Q(x)$ has degree $\leq d$.

& has $d+1$ roots.

$P(x_i) - Q(x_i) = y_i - y_i = 0$.

Contradiction. i.e. P unique.

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

$a_i \in \mathbb{R}$.

$+, -, \times, \div$ except division by 0.

---

m prime

arithmetic (mod m)

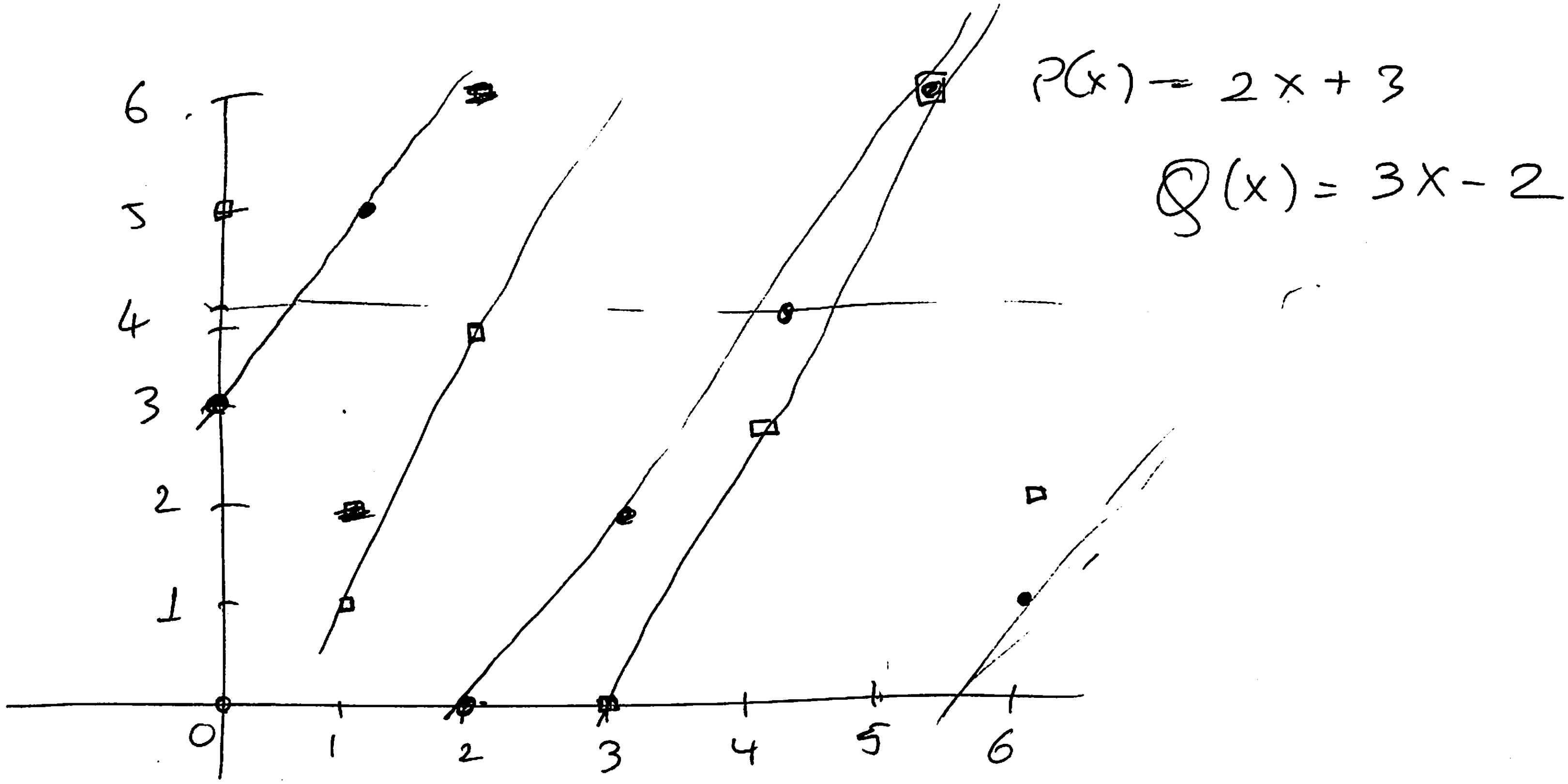
$m = 7$

$2x + 3 \pmod 7$

$$2x + 3 = 0 \pmod 7$$

$$2x = 4 \pmod 7$$

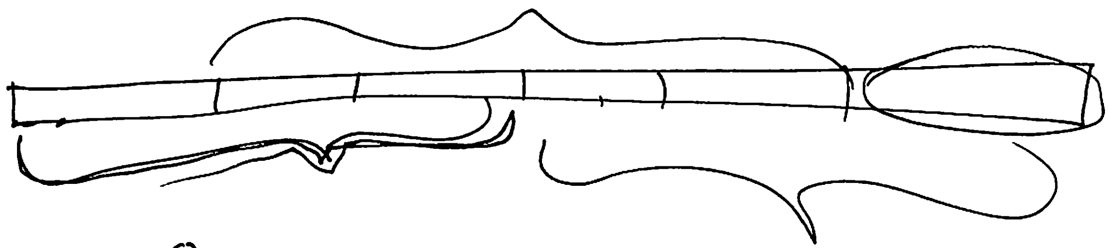
$$x = 2$$

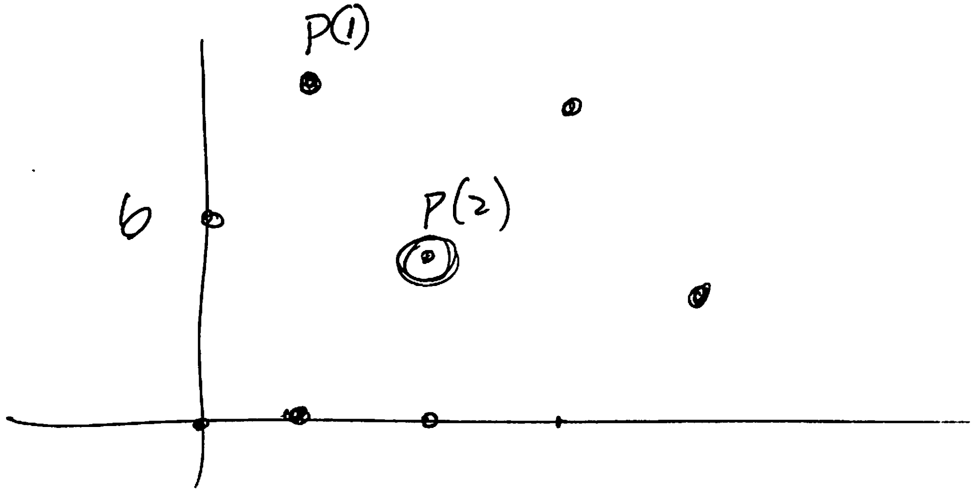


* A polynomial of degree d has at most d roots.

* Given value at $d+1$ pts $p(x_i) = y_i$ then there is a unique polynomial P of degree d.

Secret Sharing





10 officials.

≥ 2.

$P(x) = ax + b$

mod m

launch code $= b$.

≥ 5

$P(1)$
$P(2)$
$\vdots$
$P(10)$.

$\boxed{\text{polynomial of degree 4}}$

$P(0)$ $P(1)$ $P(2)$ $P(3)$ $P(4)$.

$\parallel$

b.

reconstruct $P(x)$.

$P(5)$, $P(6)$ --- $P(10)$.