Quick Review

- Polynomials can be represented two ways
  - ↳ Coefficients: e.g. $x^2 + 2x + 1$
  - ↳ Pointwise: P has degree 2, $P(0) = 1$, $P(1) = 4$, $P(-1) = 0$.
- Coefficients → Pointwise: Plug in numbers.
- Pointwise → Coefficients: Interpolation
  - ↳ Write P as a linear combination of basis polynomials
- Polynomials over Finite Fields (i.e. $GF(p)$)
  - ↳ All coefficients are integers between 0 and $p-1$.
  - ↳ Interpolation still works (use inverses instead of division though)
  - ↳ Degree of a polynomial is bounded by $p-1$ (consequence of FLT).
- Can take advantage of coefficient / pointwise representation to do secret-sharing
  - ↳ Make P a secret.
  - ↳ Give each person $\deg(P)$ and $P(i)$
  - ↳ Only have the polynomial when $\deg(P)$ people come together.