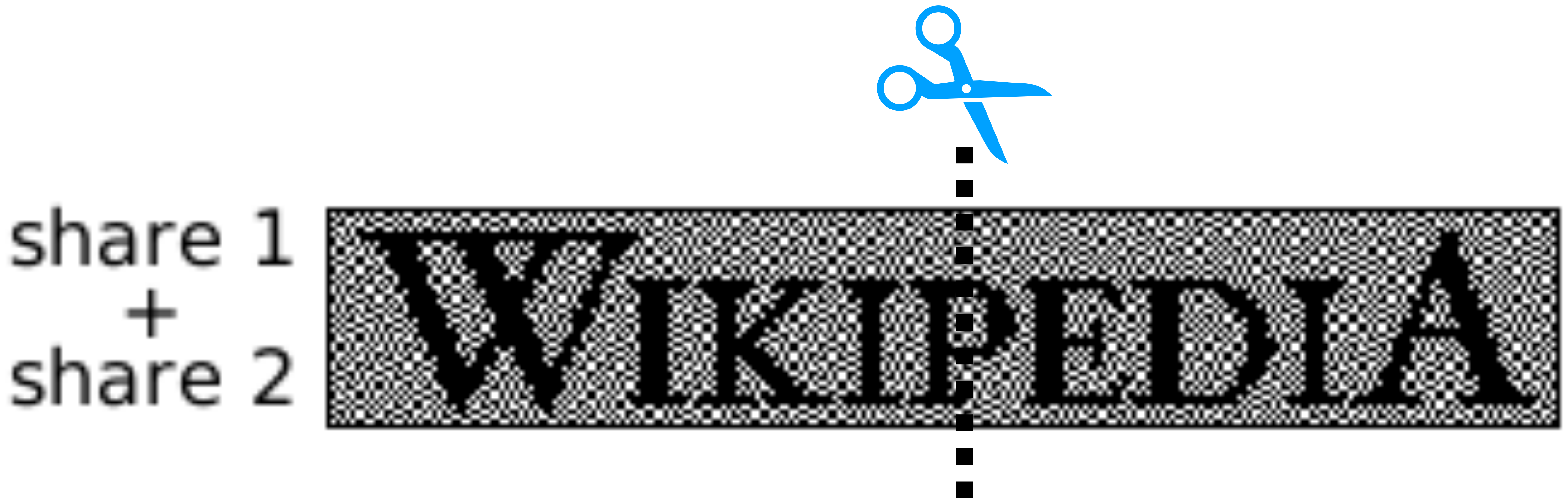
# Mathematically Sharing Secrets

## UMD Girls Talk Math // Spring Event

Noemi Glaeser // May 22, 2021

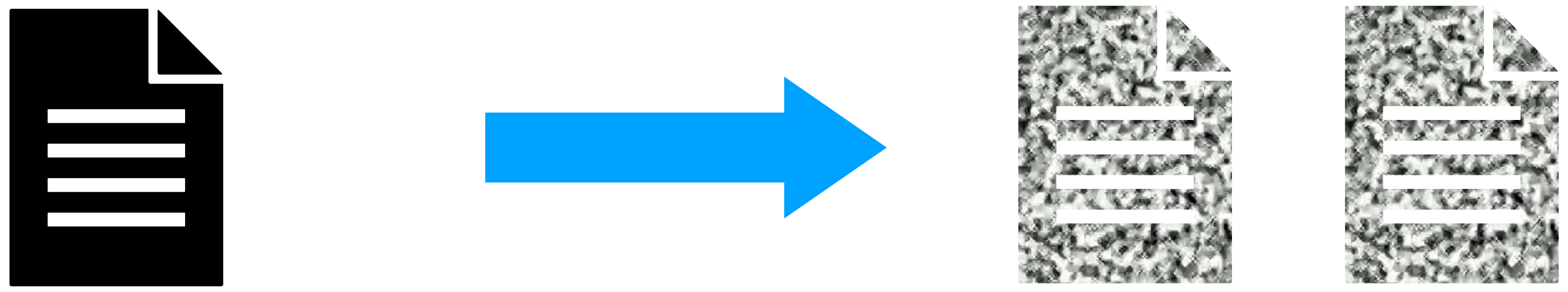
# What is secret sharing?

- Dividing a secret into pieces
  - Each piece by itself tells you nothing about the secret (privacy)
  - Putting the pieces back together gives you back the secret (correctness)



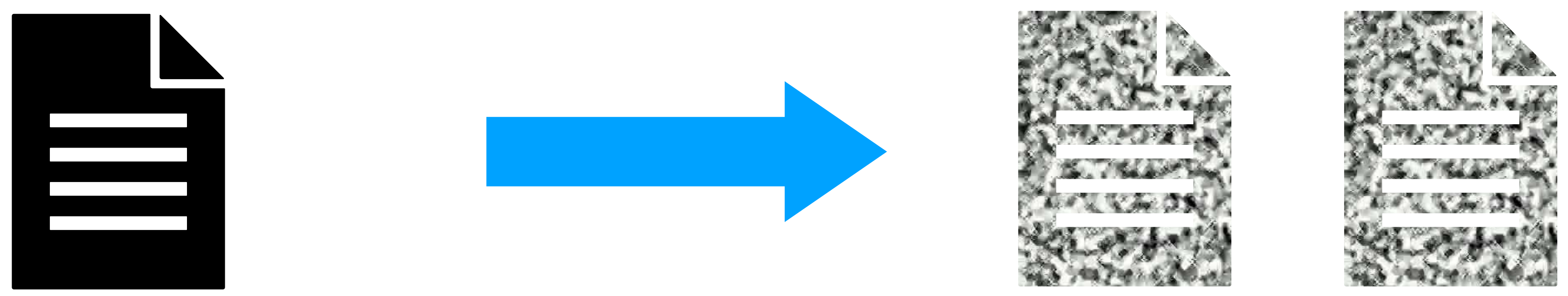
# Why is it useful?

- Share a note

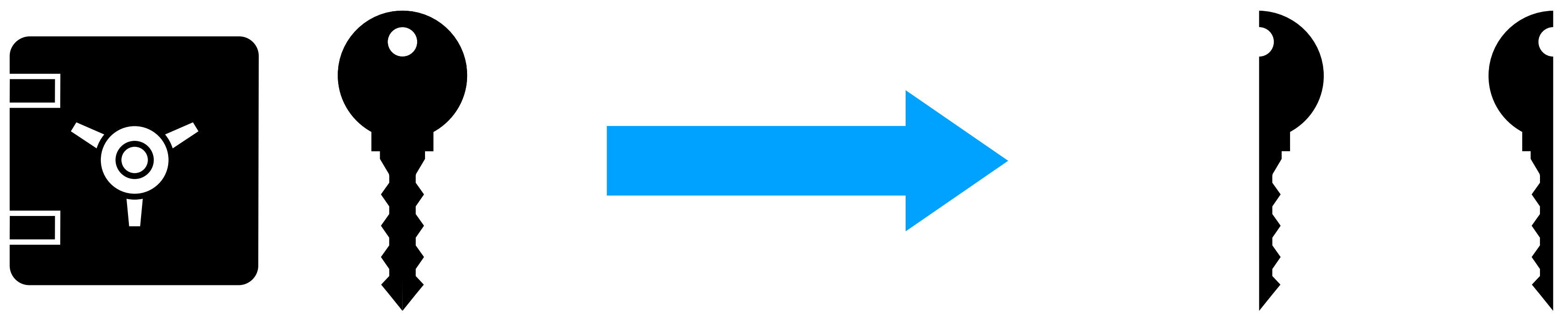


# Why is it useful?

- Share a note



- Share passwords



random: don’t depend on s

# Sharing numbers

- Share a secret (s = 42) between people (n = 3)
  - Pick n-1 random numbers: 12, 27
  - Give 12, 27, and 42-(12+27)=3 to the 3 people

**Share**

  - Can they work together to get back the secret?

12+27+3 = 42

**Reconstruct**

random: don’t depend on s

# Sharing numbers

- Share a secret ($s = 42$) between people ($n = 3$)
  - Pick n-1 random numbers: 12, 27
  - Give 12, 27, and 42-(12+27)=3 to the 3 people

Share

  - Can they work together to get back the secret?

12+27+3 = 42

Reconstruct

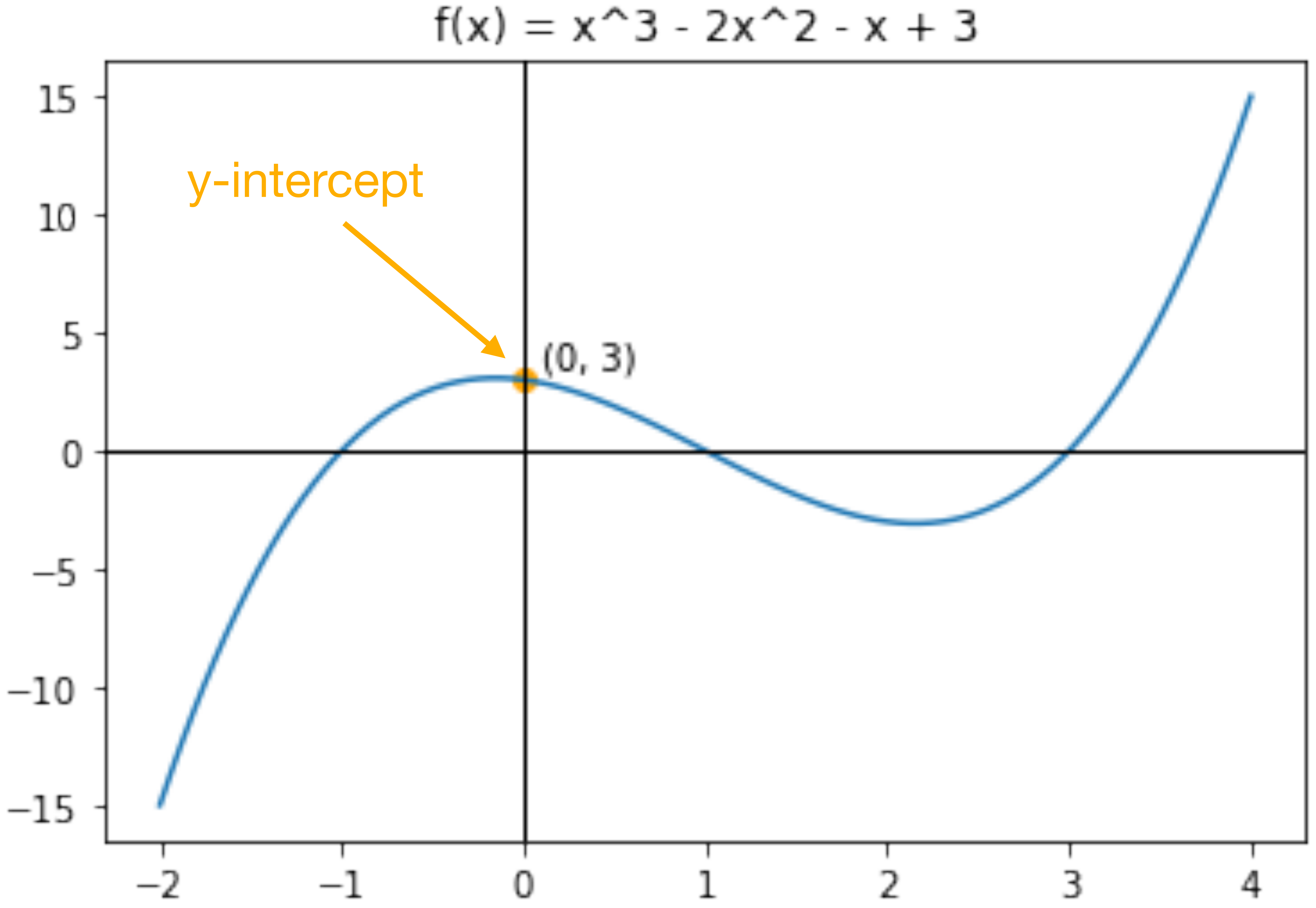
This is an **n-out-of-n** secret sharing (for any number n)

What about reconstructing with less than n (out of n) shares?

# Polynomial Review: Terms

- y-intercept:
  - f(0)
  - the constant term in the equation:

$$f(x) = x^3 - 2x^2 - x + 3$$



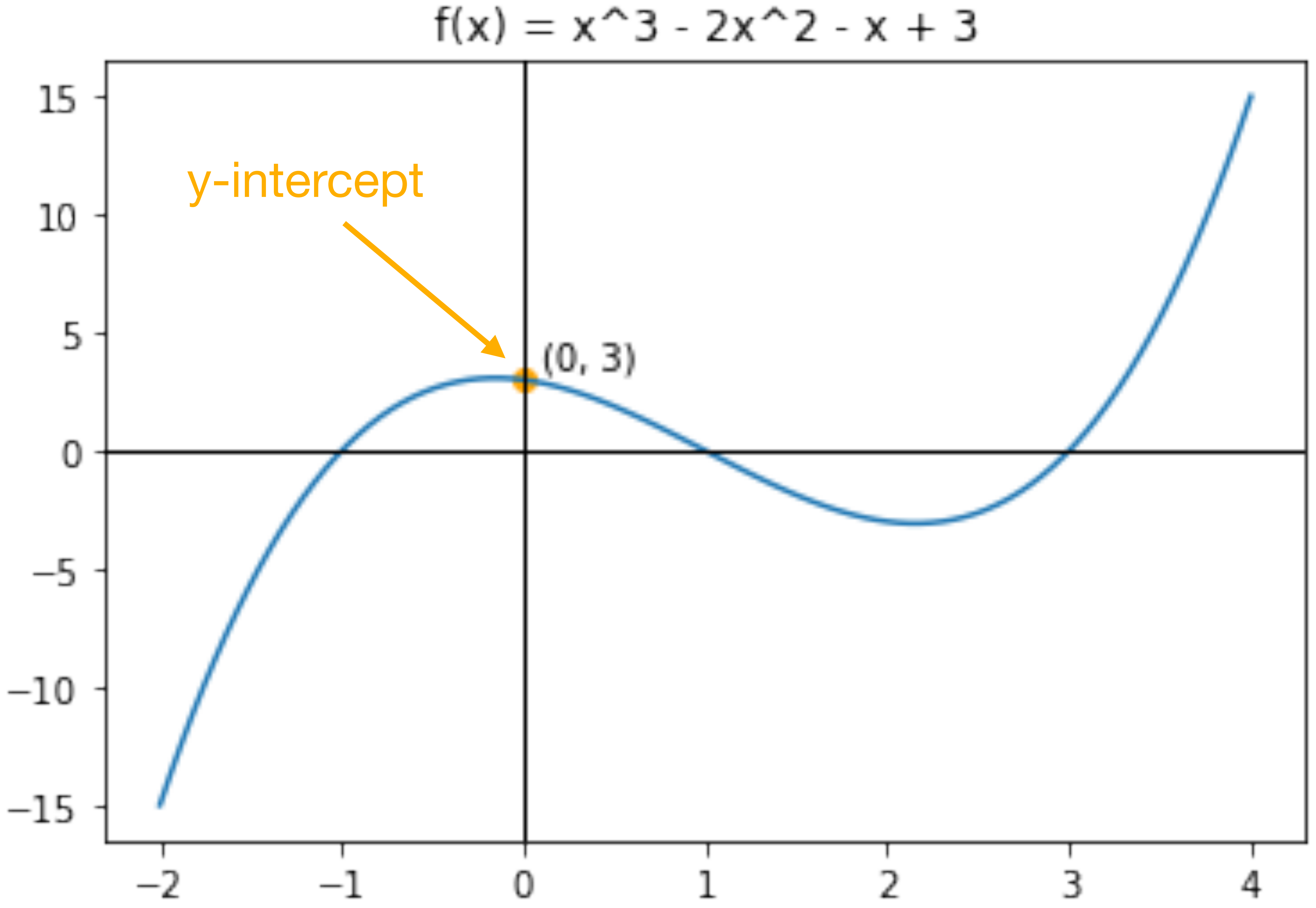
# Polynomial Review: Terms

- y-intercept:
  - f(0)
  - the constant term in the equation:

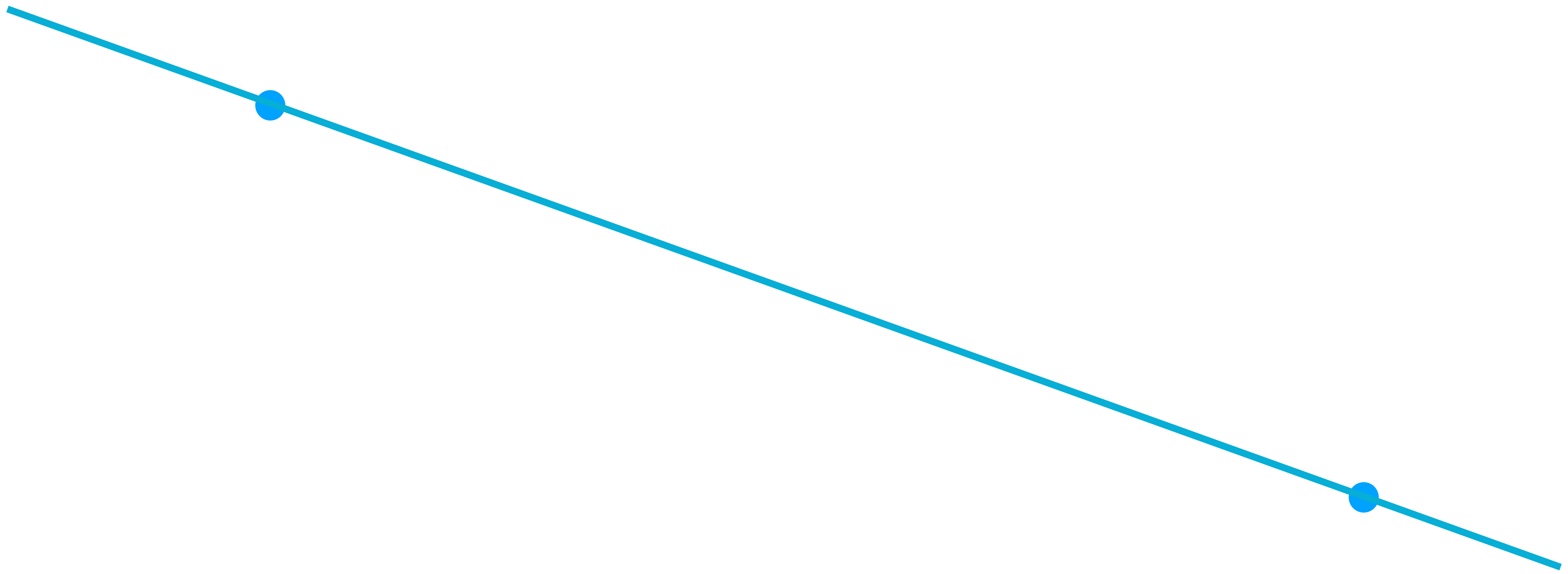
$$f(x) = x^3 - 2x^2 - x + 3$$

- degree:
  - Highest exponent in the equation

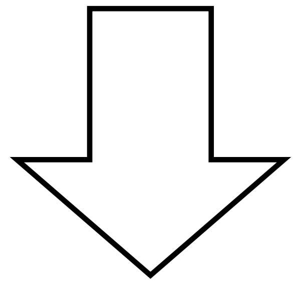
$$f(x) = x^3 - 2x^2 - x + 3$$



# Polynomial Review: Uniqueness



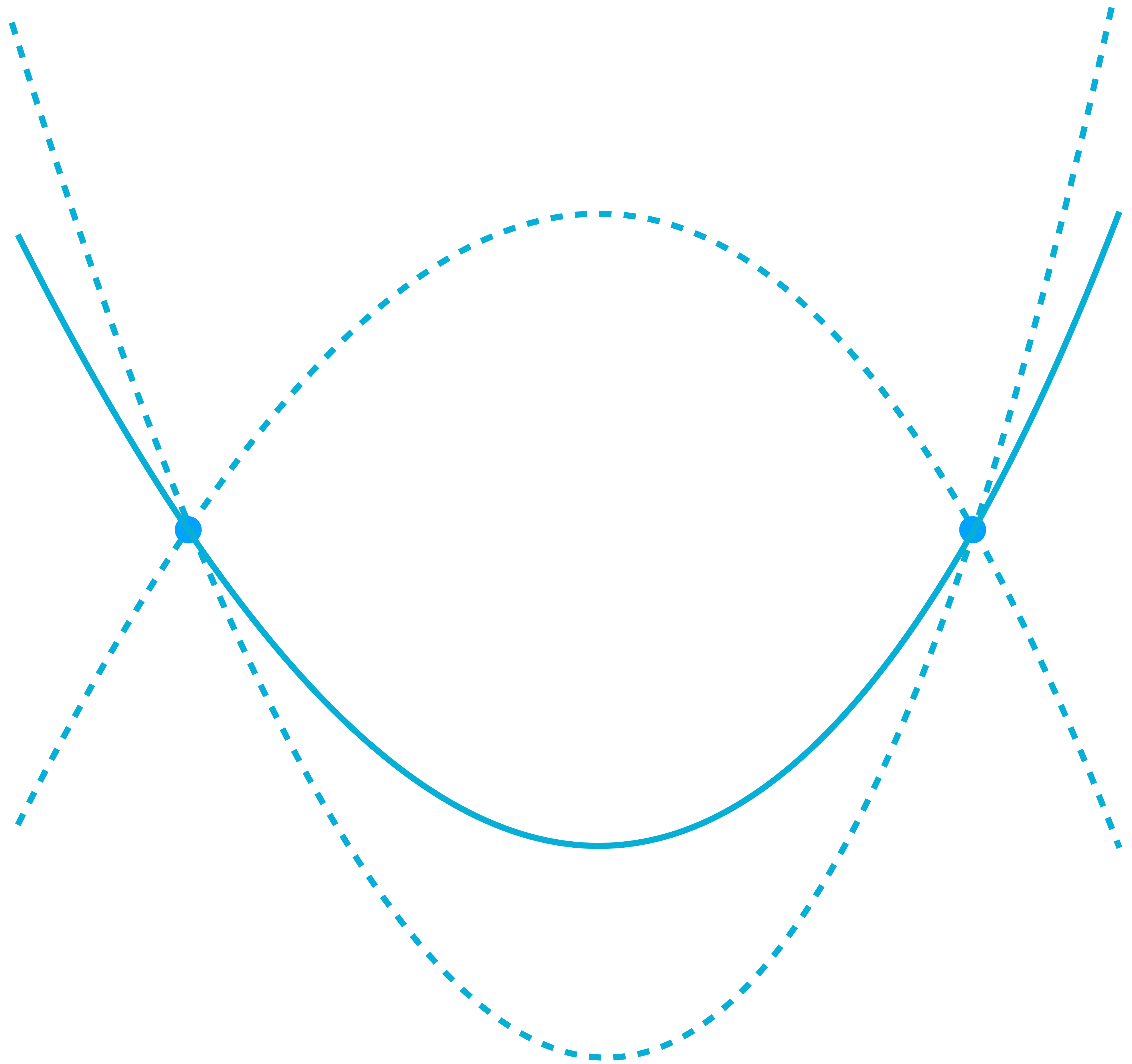
$f(x) = ax + b$



Degree: 1

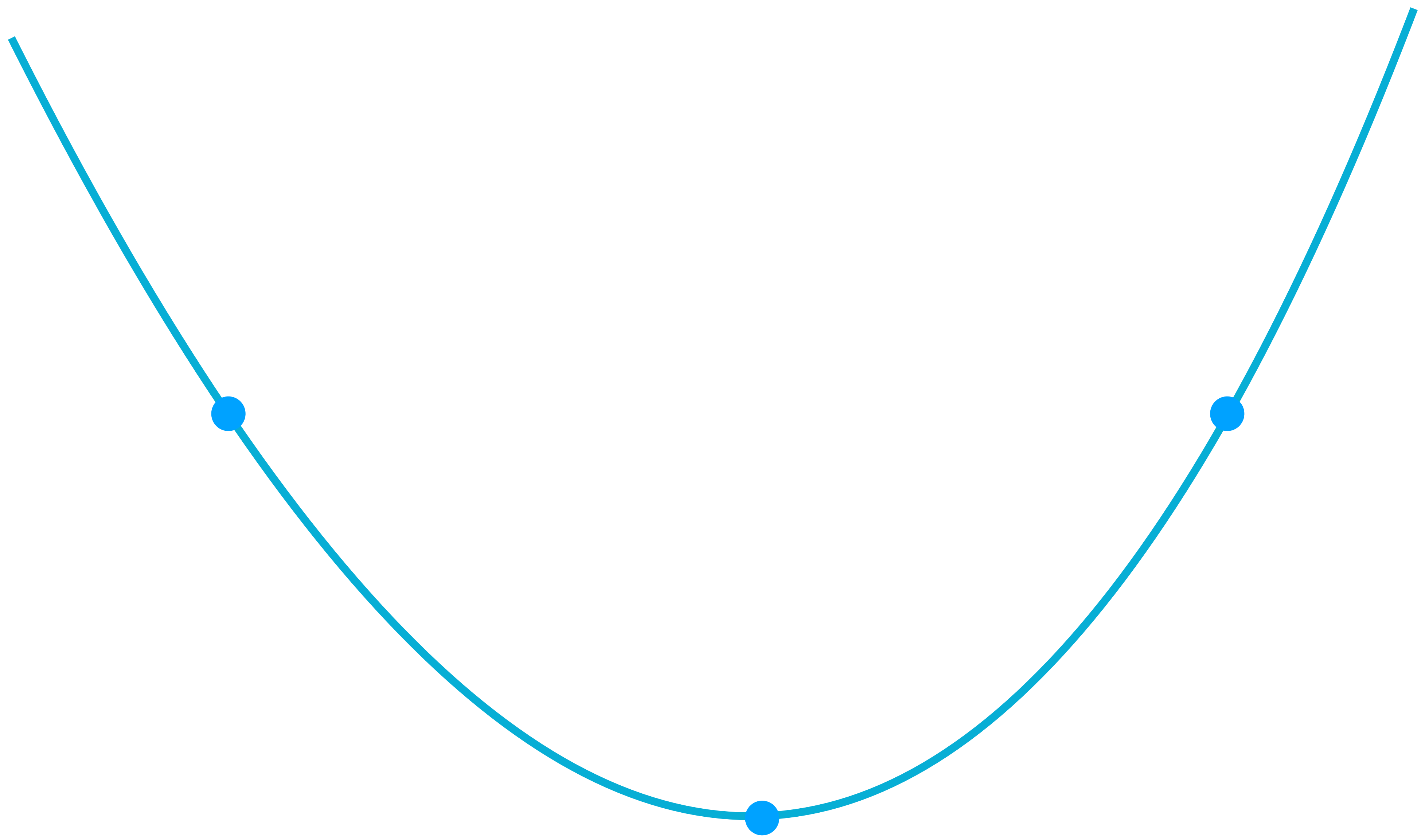
Points: 2

# Polynomial Review: Uniqueness



$f(x) = ax^2 + bx + c$

# Polynomial Review: Uniqueness



$f(x) = ax^2 + bx + c$

↓

Degree: 2

Points: 3

t+1 points uniquely define a degree-t polynomial.

# Shamir Secret Sharing

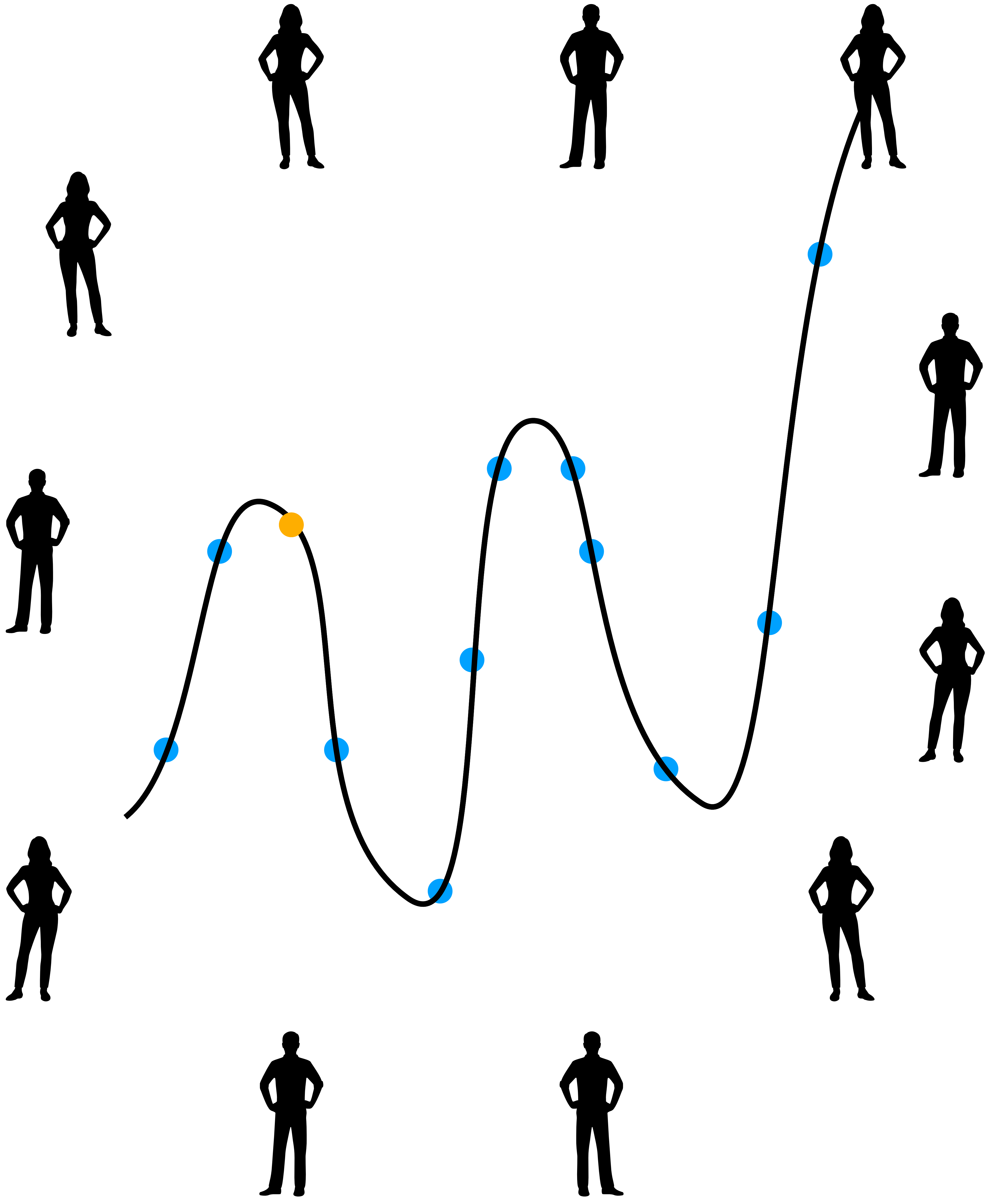
(t+1)-out-of-n secret sharing

Share

- Pick a random degree t polynomial f
  - Pick t random coefficients
  - Set the constant term (y-intercept) to the secret s
- Pick n points on f
  - Distribute them to n parties

Recon.

- Any t+1 points uniquely define f!
- To get s, compute f(0)



# Shamir Secret Sharing

Example: 4-out-of-6 secret sharing with s = 3

**Share**

- Pick a random degree t polynomial f
  - Pick t random coefficients
  - Set the constant term (y-intercept) to the secret s
- Pick n points on f
  - Distribute them to n parties

**Recon.**

- Any t+1 points uniquely define f!
- To get s, compute f(0)

# Shamir Secret Sharing

Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients
  - Set the constant term (y-intercept) to the secret s
- Pick n points on f
  - Distribute them to n parties

Recon.

- Any t+1 points uniquely define f!
- To get s, compute f(0)

# Shamir Secret Sharing

Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients: 1, -2, -1
  - Set the constant term (y-intercept) to the secret s
- Pick n points on f
  - Distribute them to n parties

Recon.

- Any $t+1$ points uniquely define f!
- To get s, compute $f(0)$

# Shamir Secret Sharing

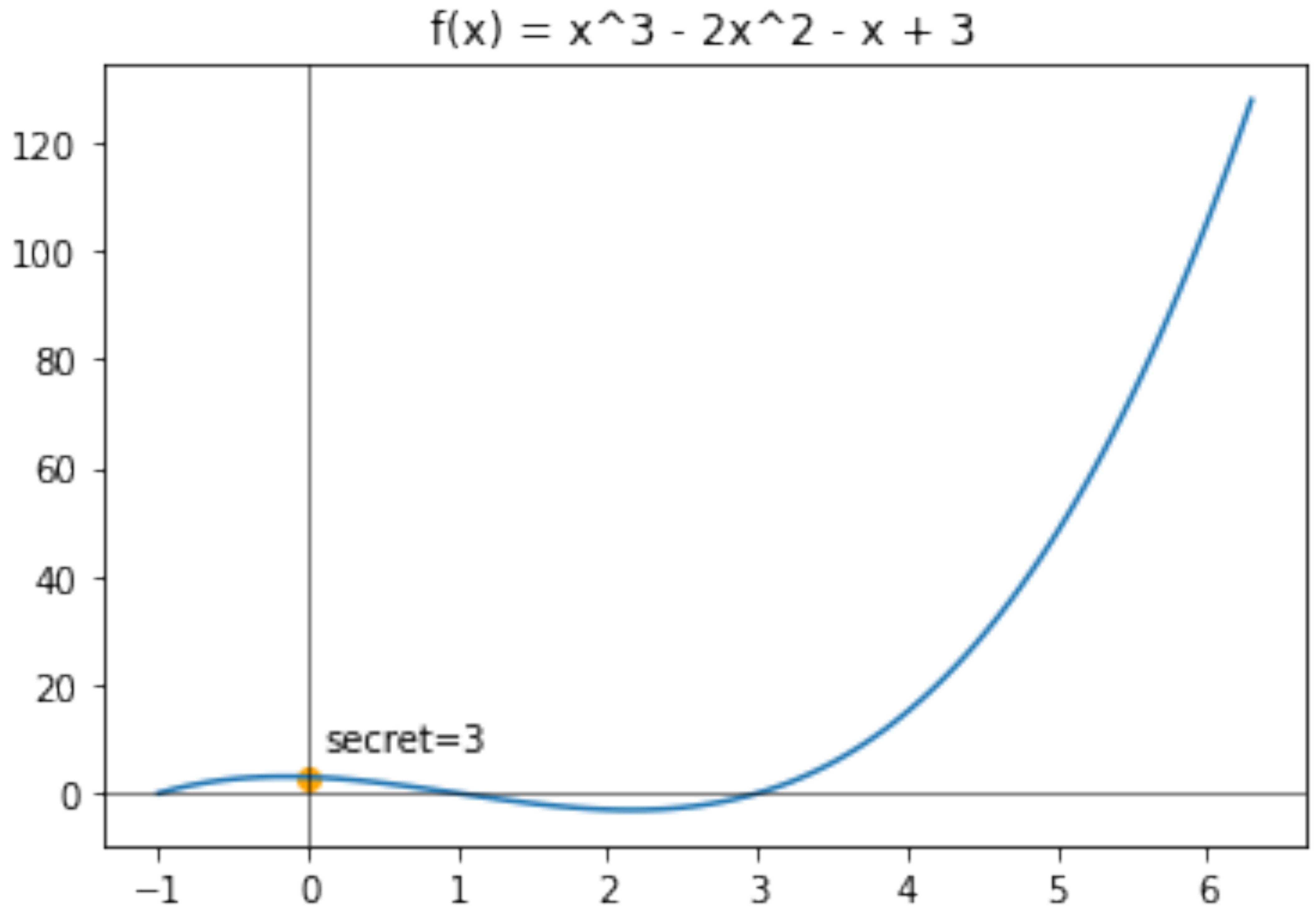
Example: 4-out-of-6 secret sharing with s = 3

Share

- Pick a random degree t = 3 polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = 1x^3 -2x^2 -1x + 3$$

- Pick n points on f
  - Distribute them to n parties



Recon.

- Any t+1 points uniquely define f!
- To get s, compute f(0)

# Shamir Secret Sharing

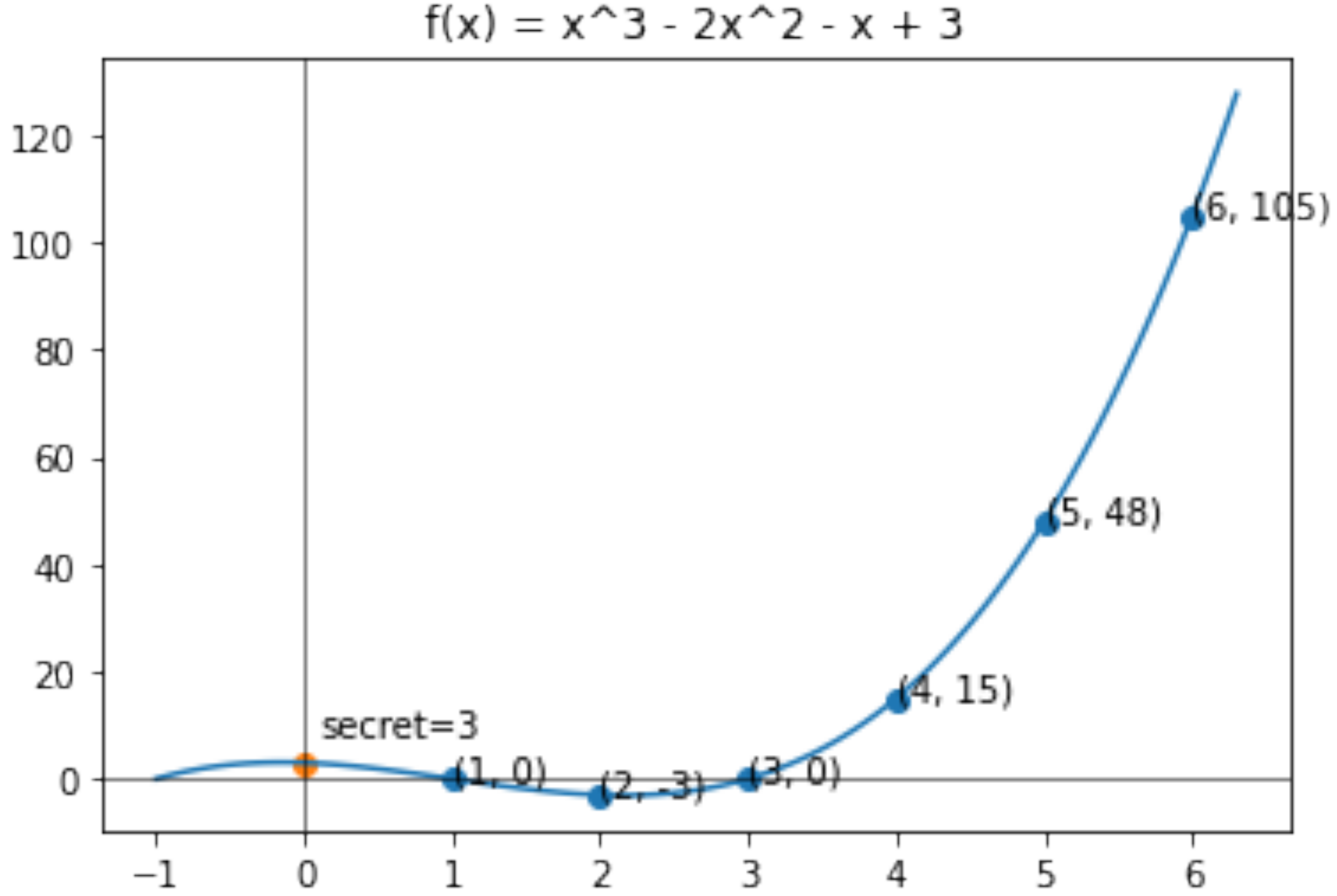
Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = \mathbf{1}x^3 \mathbf{-2}x^2 \mathbf{-1}x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties



Recon.

- Any $t+1$ points uniquely define f!
- To get s, compute $f(0)$

# Shamir Secret Sharing

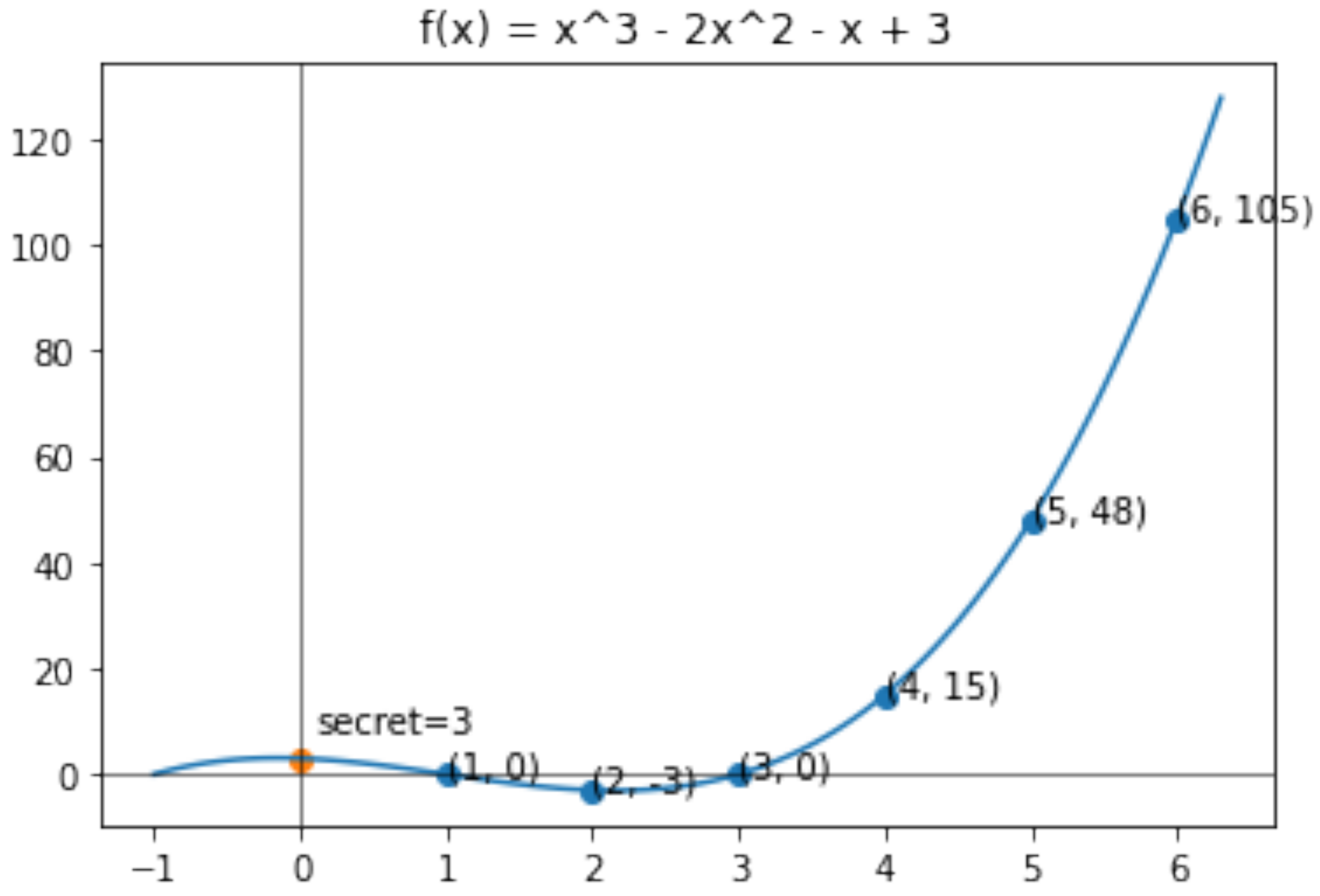
Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = \mathbf{1}x^3\ \mathbf{-2}x^2\ \mathbf{-1}x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties



Recon.

- Any $t+1=4$ points uniquely define f!
- To get s, compute $f(0)$

# Shamir Secret Sharing

Example: 4-out-of-6 secret sharing with s = 3

**Share**

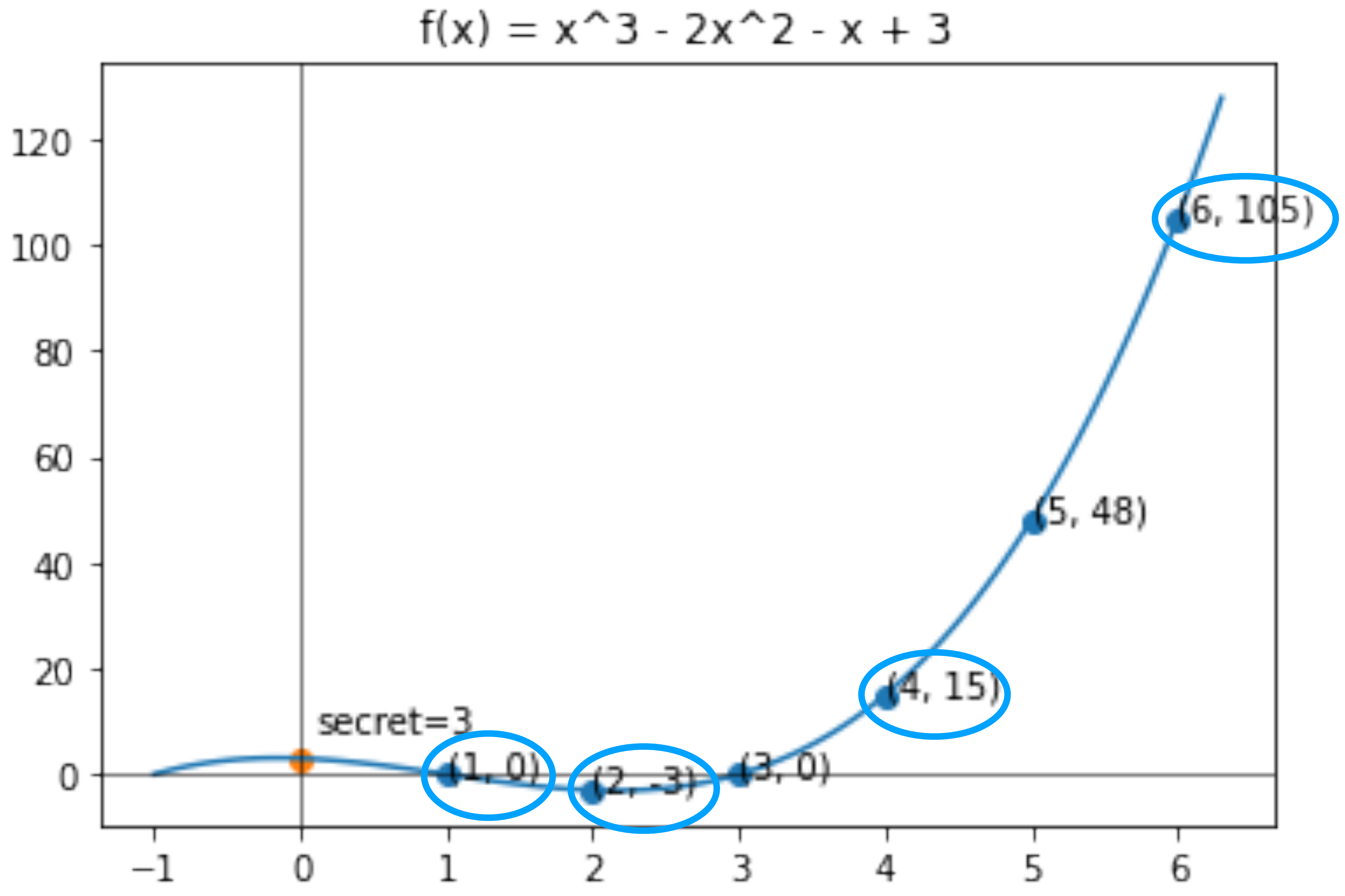
- Pick a random degree t = 3 polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = \mathbf{1}x^3 \mathbf{-2}x^2 \mathbf{-1}x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties

**Recon.**

- Any t+1=4 points uniquely define f!
- To get s, compute f(0)



# Shamir Secret Sharing

Example: 4-out-of-6 secret sharing with s = 3

Share

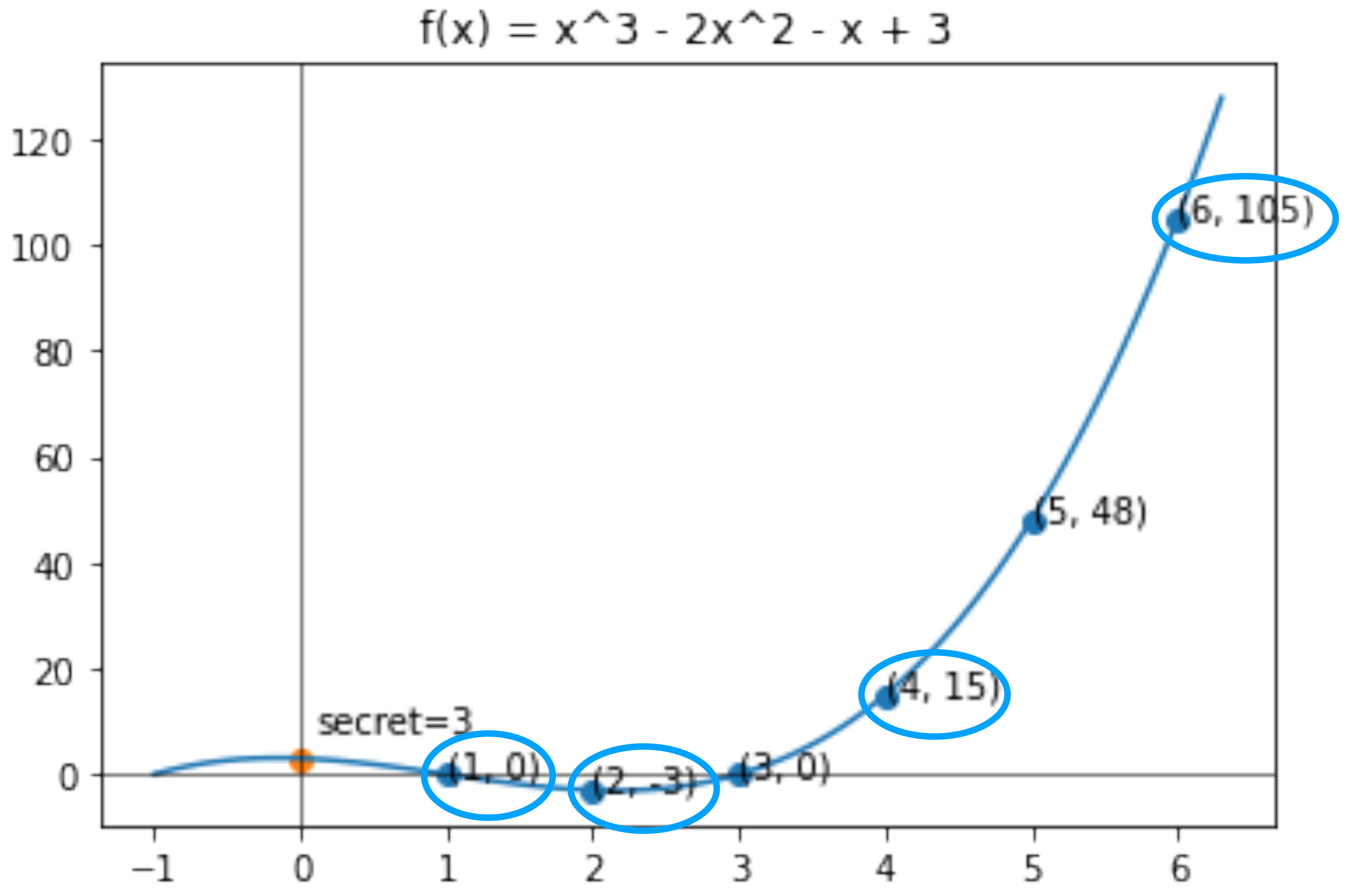
- Pick a random degree t = 3 polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = \mathbf{1}x^3 \mathbf{-2}x^2 \mathbf{-1}x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties

Recon.

- interpolate((1, 0), (2, -3), (4, 15), (6, 105)) → f(x)
- To get s, compute f(0)



# Shamir Secret Sharing

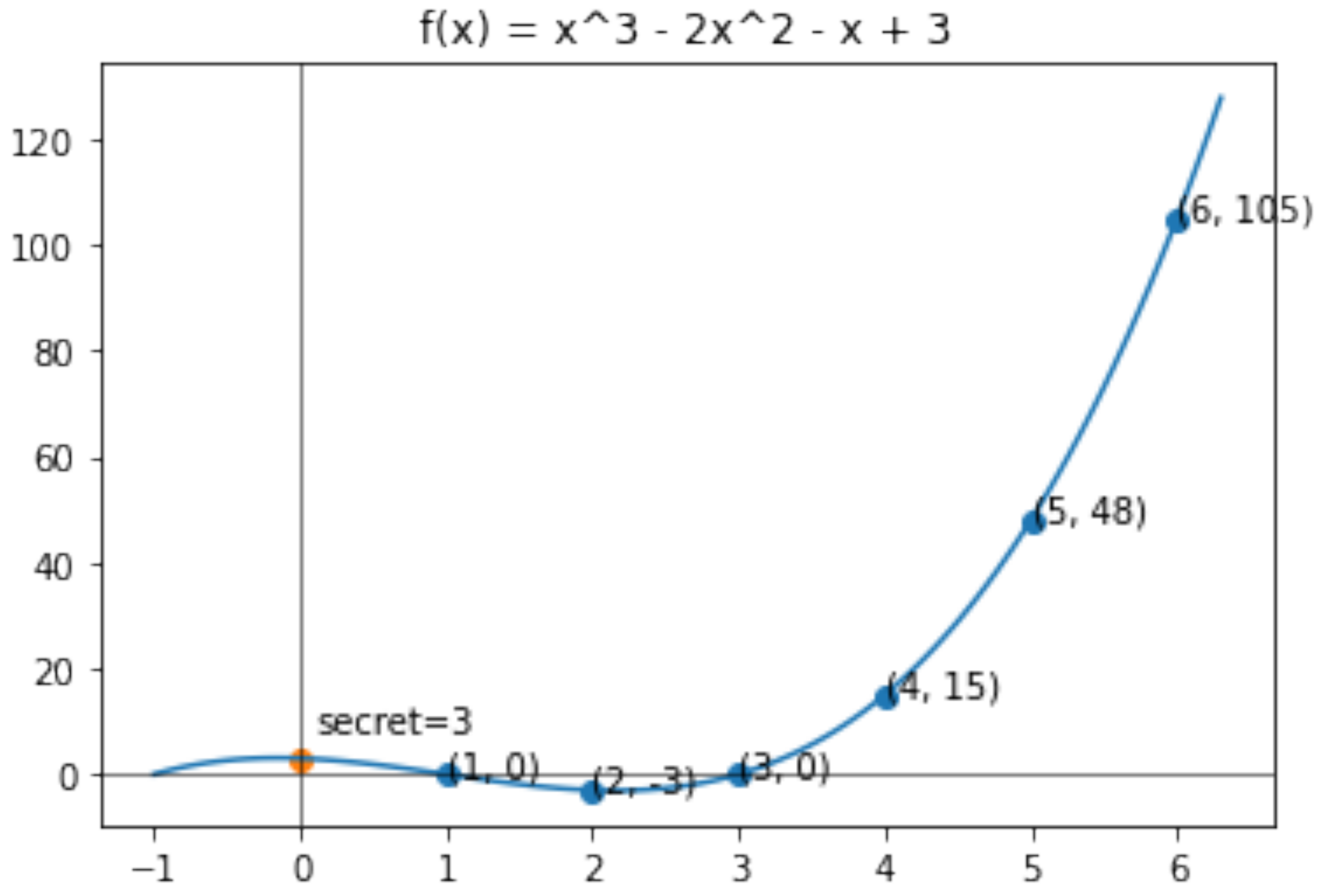
Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = 1x^3 -2x^2 -1x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties



Recon.

- interpolate((1, 0), (2, -3), (4, 15), (6, 105)) → $f(x) = x^3-2x^2-x+3$
- To get s, compute $f(0)$

# Shamir Secret Sharing

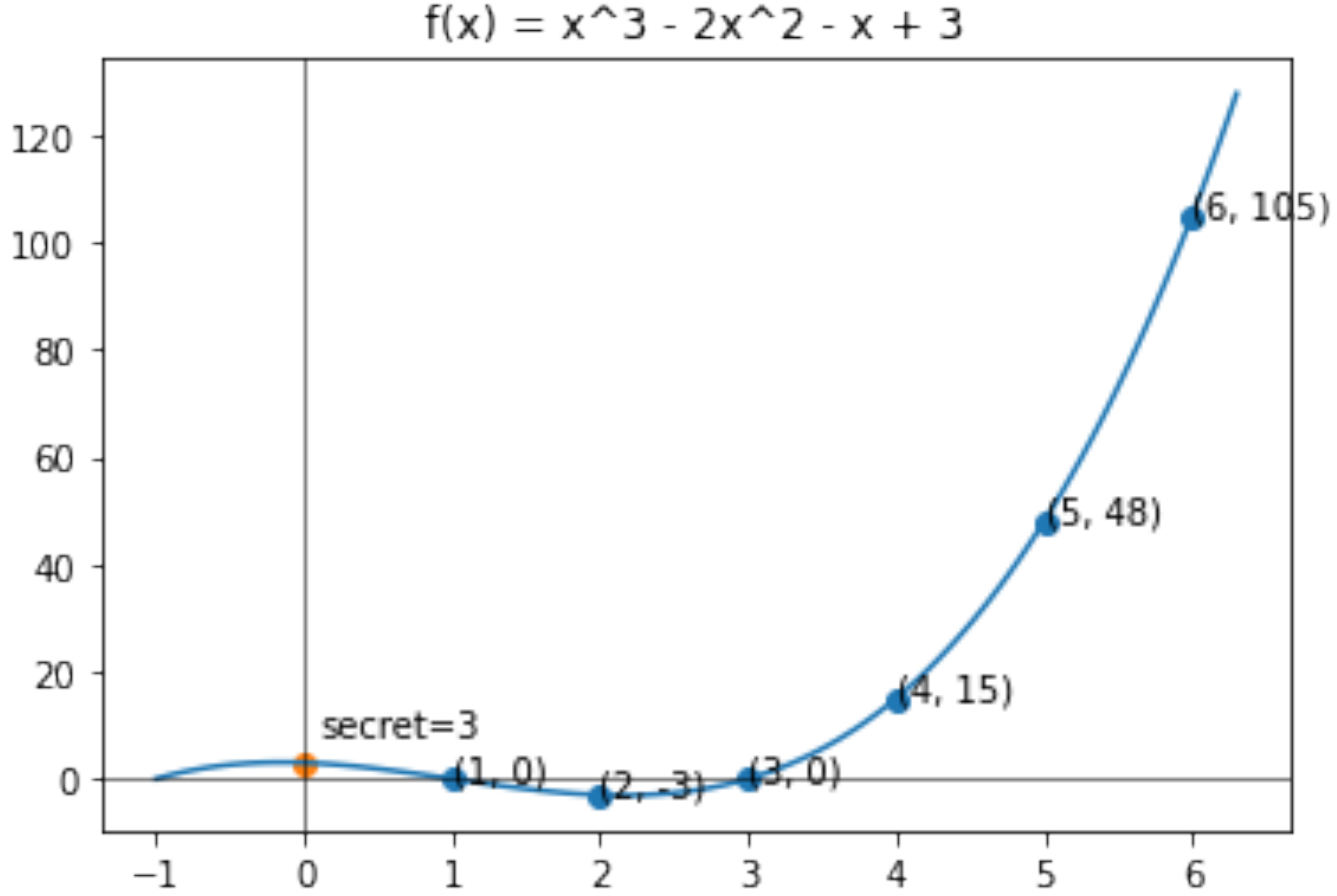
Example: 4-out-of-6 secret sharing with $s = 3$

Share

- Pick a random degree $t = 3$ polynomial f
  - Pick t random coefficients: 1, -2, -1

$$f(x) = \mathbf{1}x^3 \mathbf{-2}x^2 \mathbf{-1}x + 3$$

- (1, 0), (2, -3), (3, 0), (4, 15), (5, 48), (6, 105)
  - Distribute them to n parties



Recon.

- interpolate((1, 0), (2, -3), (4, 15), (6, 105)) → $f(x) = x^3-2x^2-x+3$
- To get s, compute $f(0) = 0 - 2(0) - 0 + 3 = 3$

# Activity!

**http://bit.ly/ShamirSS**