Problem 4

The elliptic curve

$$Y^2 = X^3 + 2$$

has six mod 5 points including ∞.
Five of them are **∞, (2,0), (3,3), (4,1), (4,4)**. Find the sixth mod 5 point.

- Finding and counting mod P points on elliptic curves is a very important problem (both theoretically and practically).

Problem 4

- Find integers S,T ($0 \le S, T \le 4$) satisfying

$$\mathbf{T^2 \equiv S^3+2 \pmod 5}.$$

- $S^3+2 \pmod 5$

$0^3+2 \equiv 2$ $1^3+2 \equiv 3$ $2^3+2 \equiv 0$

$3^3+2 \equiv 4$ $4^3+2 \equiv 1$

- $T^2 \pmod 5$

$0^2 \equiv 0$ $1^2 \equiv 1$ $2^2 \equiv 4$ $3^2 \equiv 4$ $4^2 \equiv 1$

Problem 4

- $0 \equiv T^2 \equiv S^3+2 \Rightarrow S \equiv 2,\ T \equiv 0$
- $1 \equiv T^2 \equiv S^3+2 \Rightarrow S \equiv 4,\ T \equiv 1 \text{ or } 4$
- $4 \equiv T^2 \equiv S^3+2 \Rightarrow S \equiv 3,\ T \equiv 2 \text{ or } 3$

The mod 5 points are

$\infty,\ (2,0),\ (4,1),\ (4,4),\ \mathbf{(3,2)},\ (3,3)$

The sixth point is **(3,2)**.

Answer $S = 3,\ T = 2$