2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

## **Problem 4**

The elliptic curve  $Y^2 = X^3 + 2$  has six mod 5 points including  $\infty$ . Five of them are  $\infty$ , (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  $\leq$  S, T  $\leq$  4) satisfying  $T^2 \equiv S^3+2 \pmod{5}$ .

♦ 
$$S^3+2 \pmod{5}$$
  
 $0^3+2\equiv 2$   $1^3+2\equiv 3$   $2^3+2\equiv 0$   
 $3^3+2\equiv 4$   $4^3+2\equiv 1$ 

T<sup>2</sup> (mod 5) 0<sup>2</sup>≡0 1<sup>2</sup>≡1 2<sup>2</sup>≡4 3<sup>2</sup>≡4 4<sup>2</sup>≡1

## **Problem 4**

• 0 ≡ T² ≡ S³+2 ⇒ S ≡ 2, T ≡ 0  
• 1 ≡ T² ≡ S³+2 ⇒ S ≡ 4, T ≡ 1 or 4  
• 4 ≡ T² ≡ S³+2 ⇒ S ≡ 3, T ≡ 2 or 3  
The mod 5 points are  

$$\infty$$
, (2,0), (4,1), (4,4), (3,2), (3,3)  
The sixth point is (3,2).

**Answer** 
$$S = 3$$
,  $T = 2$