

Math 400 Fall 2018  
Cryptology HW 7  
Due Thursday, October 18

Problems 2 and 3 will be worth 20 points each.

1. The group  $S_3$  is the set  $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ , where  $e$  is the identity and multiplication obeys the following rules:  $\sigma^3 = e = \tau^2, \tau\sigma = \sigma^2\tau$ .
  - (a) What are  $\sigma^{-1}$  and  $\tau^{-1}$ ? That is, tell me which of the six elements in the set I gave you is  $\sigma^{-1}$  and which is  $\tau^{-1}$ .
  - (b) Compute  $\tau\sigma^2, \tau(\sigma\tau), (\sigma\tau)(\sigma\tau)$ , and  $(\sigma\tau)(\sigma^2\tau)$ . (Again, your answer for each part should be one of the six elements I gave you.)
  
2. Let  $E : y^2 = x^3 - 2x + 4$ , and let  $P = (0, 2)$  and  $Q = (3, -5)$ .
  - (a) Check that  $P, Q \in E(\mathbb{Q})$ .
  - (b) Compute  $\Delta$  to confirm that this is an elliptic curve.
  - (c) Compute  $P \oplus Q$ .
  - (d) Compute  $P \oplus P$  and  $Q \oplus Q$ .
  - (e) Compute  $3P = P \oplus P \oplus P$  and  $3Q = Q \oplus Q \oplus Q$ .
  
3. Let  $E : y^2 = x^3 + 17$ . Let  $P = (-1, 4)$  and let  $Q = (2, 5)$ .
  - (a) Confirm that  $P, Q \in E(\mathbb{Q})$ .
  - (b) Compute  $\Delta$  to confirm that this is an elliptic curve.
  - (c) Compute  $P \oplus Q$  and  $P - Q$ .
  - (d) Compute  $2P = P \oplus P$  and  $2Q = Q \oplus Q$ .
  
4. Consider the following curves:
  - (i)  $y^2 = x^3 - 7x + 3$
  - (ii)  $y^2 = x^3 - 7x + 9$
  - (iii)  $y^2 = x^3 - 7x - 12$
  - (iv)  $y^2 = x^3 - 3x + 2$
  - (v)  $y^2 = x^3$ .

- (a) Compute the discriminant of each curve. Which of these are elliptic curves?
- (b) Sketch a graph of each curve (you may use a computer for this step). How can you visually tell which of these curves was an elliptic curve?