

Introduction to mathematical cryptography  
Homework problems  
Week 11

21. Let  $E$  be the real elliptic curve given by the equation  $Y^2Z = X^3 - XZ^2$ . Solve the equation  $P + P = \mathcal{O}$  (where  $\mathcal{O}$  is the unit element in  $(E, +)$ ).
22. Let  $p > 3$  be a prime number. Prove that an elliptic curve over  $\mathbf{F}_p$  has at most  $2p + 1$  points. (The proof must be elementary, e.g. you cannot refer to Hasse's theorem.)

**Note:** Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.