MATH36206 Quiz7 Learning With Errors and Regev

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**INSTRUCTIONS:** Show all details in your solutions. Marks are given for the level of understanding shown. Good luck!

1. **(5 marks)** Solve the LWE problem with q = 41, e = (−2, 1), and samples:

((13,15),11), ((1,22),35)

1. For the Regev cryptosystem with q = 13, private key s = (4, 3, 2), and public key:

((12,3,4),1), ((9,5,2),4), ((7,3,5),9)

1. **(2 marks)** Encrypt “1” using S = {2, 3}.
2. **(3 marks)** Decrypt “(6,6,9),10”.

