Problem 5.5

1. E: Y2 = X3 + 3X + 2 over F­­7

E(F7) = {0, (0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4)}

03 + 3(0) + 2 = 2 (mod 7)

32 = 2 (mod 7)

42 = 2 (mod 7)

23 + 3(2) + 2 = 2 (mod 7)

32 = 2 (mod 7)

42 = 2 (mod 7)

43 + 3(4) + 2 = 1 (mod 7)

12 = 1 (mod 7)

62 = 1 (mod 7)

53 + 3(5) + 2 = 2(mod 7)

32 = 2 (mod 7)

42 = 2 (mod 7)

1. E: Y2 = X3 + 2X + 7 over F11

E(F11) = {0, (6,2), (6,9), (7,1), (7,10), (10,2), (10,9)}

62 + 2(6) + 7 = 4 (mod 11)

22 = 4 (mod 11)

92 = 4 (mod 11)

72 + 2(7) + 7 = 1 (mod 11)

12 = 1 (mod 11)

102 = 1 (mod 11)

62 + 2(6) + 7 = 4 (mod 11)

22 = 4 (mod 11)

92 = 4 (mod 11)

1. E: Y2 = X3 + 4X + 5 over F11

E(F11) = {0, (0,4), (0,7), (3,0), (6,5), (6,6), (9,0), (10,0)}

03 + 4(0) + 5 = 5 (mod 11)

42 = 5 (mod 11)

72 = 5 (mod 11)

33 + 4(3) + 5 = 0 (mod 11)

02 = 0 (mod 11)

63 + 4(6) + 5 = 3 (mod 11)

52 = 3 (mod 11)

62 = 3 (mod 11)

93 + 4(9) + 5 = 0 (mod 11)

02 = 0 (mod 11)

103 + 4(10) + 5 = 0 (mod 11)

02 = 0 (mod 11)

1. E: Y2 = X3 + 9X + 5 over F11

E(F11) = {0, (0,4), (0,7), (1,2), (1,9), (2,3), (2,8), (3,2), (3,9), (6,0), (7,2), (7,9), (9,1), (9,10)}

03 + 9(0) + 5 = 5 (mod 11)

42 = 5 (mod 11)

72 = 5 (mod 11)

13 + 9(1) + 5 = 4 (mod 11)

22 = 4 (mod 11)

92 = 4 (mod 11)

23 + 9(2) + 5 = 9 (mod 11)

32 = 9 (mod 11)

82 = 9 (mod 11)

33 + 9(3) + 5 = 4 (mod 11)

22 = 4 (mod 11)

92 = 4 (mod 11)

63 + 9(6) + 5 = 0 (mod 11)

02 = 0 (mod 11)

73 + 9(7) + 5 = 4 (mod 11)

22 = 4 (mod 11)

92 = 4 (mod 11)

93 + 9(9) + 5 = 1 (mod 11)

12 = 1 (mod 11)

102 = 1 (mod 11)

1. E: Y2 = X3 + 9X + 5 over F13

E(F13) = {0, (4,1), (4,12), (8,2), (8,11), (9,3), (9,10), (10,4), (10,9)}

43 + 9(4) + 5 = 1 (mod 13)

12 = 1 (mod 13)

122 = 1 (mod 13)

83 + 9(8) + 5 = 4 (mod 13)

22 = 4 (mod 13)

112 = 4 (mod 13)

93 + 9(9) + 5 = 9 (mod 13)

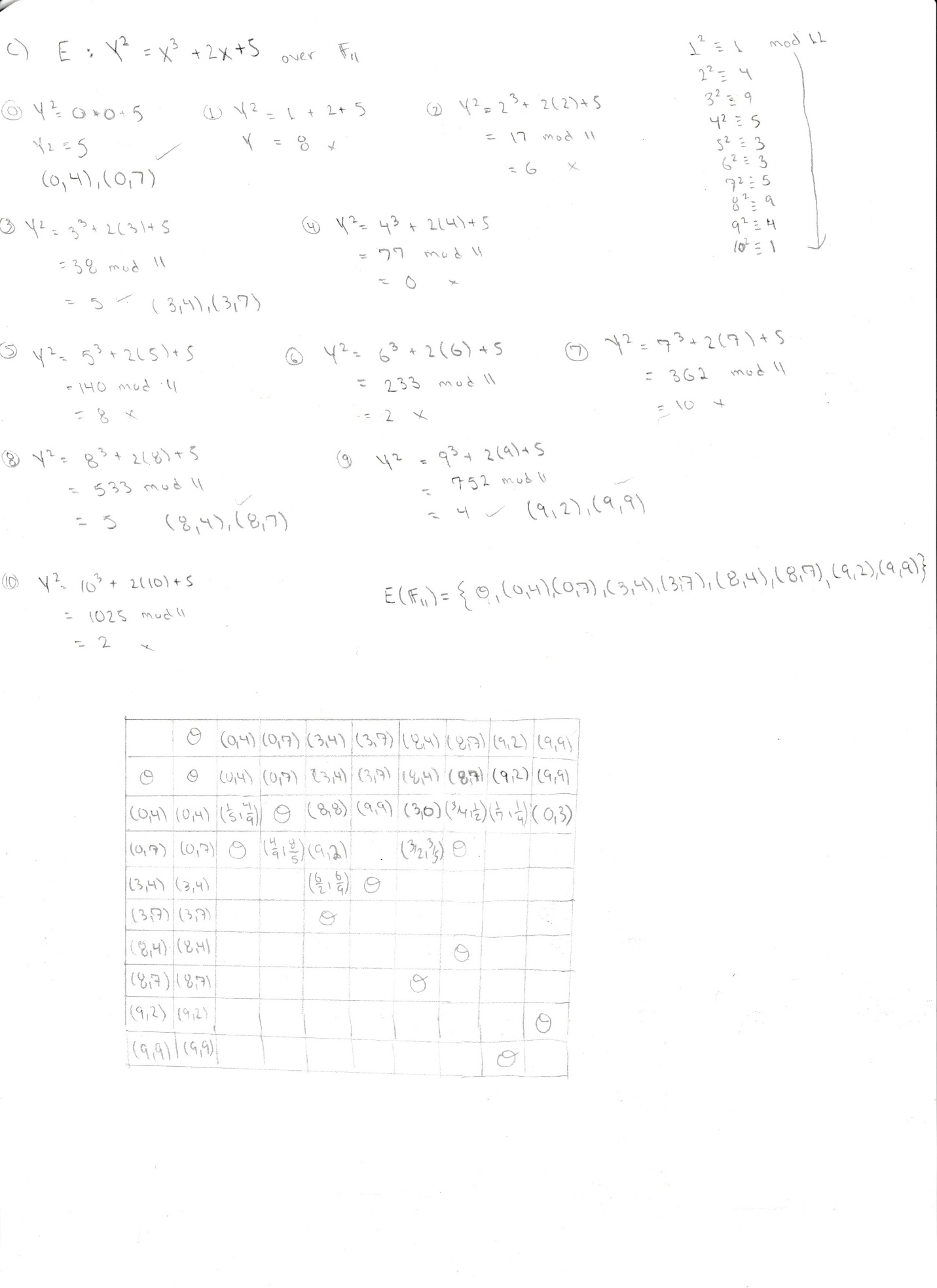
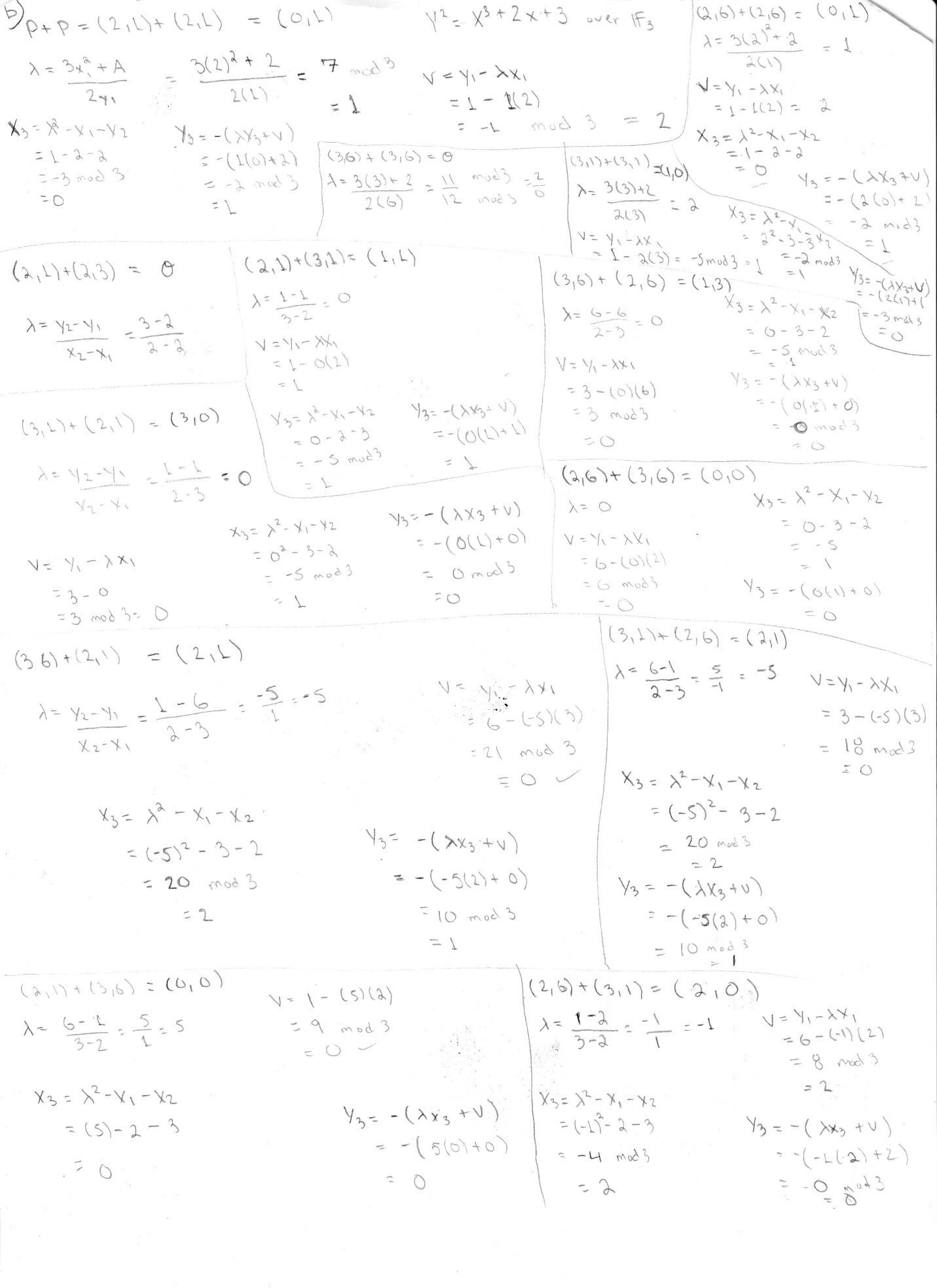
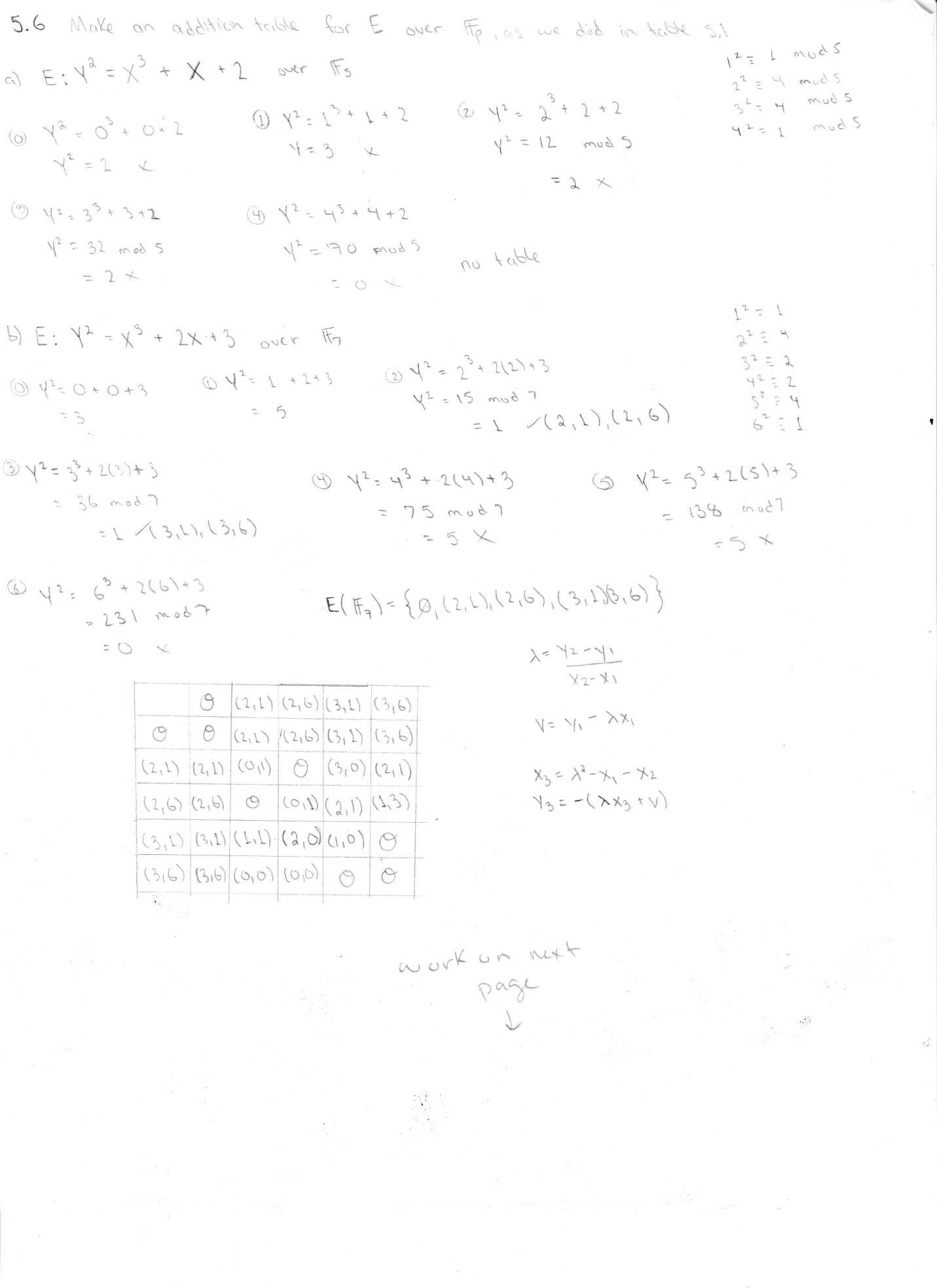
32 = 9 (mod 13)

102 = 9 (mod 13)

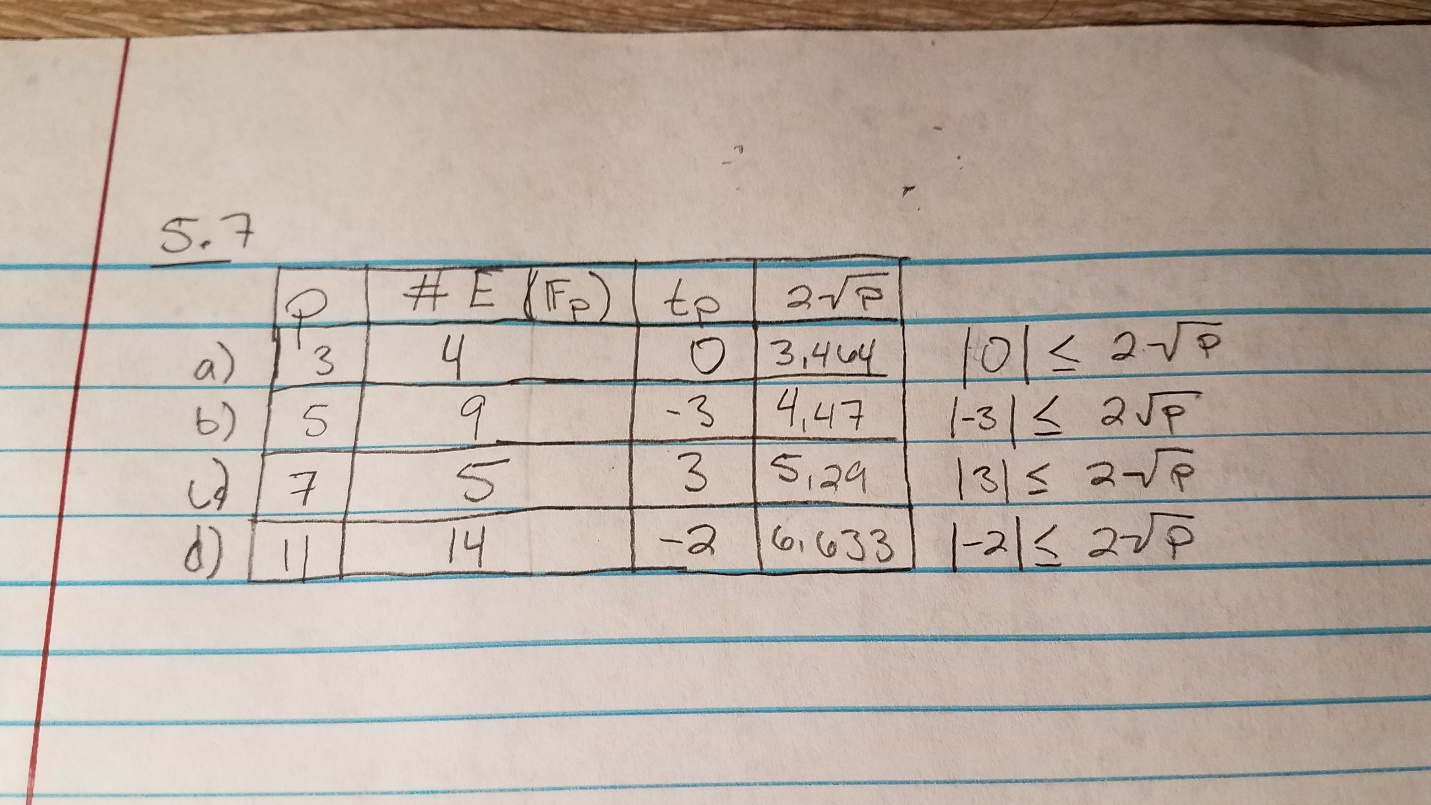
103 + 9(10) + 5 = 3 (mod 13)

42 = 3 (mod 13)

92 = 3 (mod 13)



5.7



5.13

