1.34

a)

* Lets assume x is a square root mod p. If x 2 = b (mod p) is true then we can assume that there is another solution, -x. So -x2 = b (mod p) ≡ x 2 = b (mod p)

To prove there are only two solutions lets assume that there is some number y that

y ≠ x (mod p) and y ≠ -x (mod p) but y2 = b (mod p). So x2 = b = y2 which is

x2 – y2 = b - b ≡ ( x – y ) (x + y). Possible integers are p / (x – y )(a + y).

Using p / (x – y ) , where y = a(mod p) this contradicts the assumption that y≠ x (mod p). Therefore, b must have exactly 2 solutions if it has one solution.

b)

i) (p,b) = (7,2) x2 = 2 (mod 7)

0 1 2 **3 4** 5 6 7 8 9 **10 11** 12 13 14 15 16 **17 18** (squared and modulo 7)

0 1 4 2 2 4 1 0 1 4 2 2 4 1 0 1 4 2 2

There seems to be a pattern. Any integer mod 7 that equals 3 or 4 is a solution

And taking the negative of that number and doing modulo 7 they will result in either a 3 or 4 those are solutions as well.

Examples: -3 mod 7 = 4 -11 mod 7 = 3

ii) (p,b) = (11,5) x2 = 5 (mod 11)

0 1 2 3 **4** 5 6 **7**  8 9 10 11 12 13 14 **15** 16 17 **18** (squared and modulo 11)

0 1 4 9 5 3 3 5 9 4 1 0 1 4 9 5 3 3 5

Solutions can be found when, x mod 11 = 4 or x mod 11 =7

iii) (p,b) = (11,7) x2 = 7 (mod 11)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 (squared and modulo 11)

No solutions

iv) (p,b) = (7,2) x2 = 3 (mod 37)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 **15** 16 17 18 (squared and modulo 37)

0 1 3 9 16 25 1 12 27 7 26 10 33 21 11 3 34 30 28

Solutions are 15 and – 15

c) how many square roots does 29 have modulo 35? Why doesn’t this contradict the assertion (a) ?

0 1 2 3 4 5 6 7 **8** 9 10 11 12 13 14 15 16 17 18 x2 = 29 (mod 35)

0 1 4 9 16 25 1 14 29 11 30 16 4 29 21 15 11 9 9 11 15 21 29

8 and -8 are square roots. It doesn’t contradict because it is either 2 solutions or no solutions.

d) Let p be an odd prime and let g be a primitive root modulo p. Then any number a is equal to some power of g modulo p, say a ≡ gk (mod p). Prove that a has a square root modulo p if and only if k is even.

Let’s assume k is even. Then k = 2n ( k being divisible by 2), so a a ≡ g2n (mod p).