Preliminaries.

Read the following article on introduction to modular arithmetic:

> https://nrich.maths.org/4350

In the above article, the existence of a multiplicative inverse is proved using Euclid's GCD algorithm, which is explained in these two links:

> https://nrich.maths.org/1357
> https://nrich.maths.org/1728

In fact, Euclid's GCD algorithm is a fast way to compute the multiplicative inverse of a number modulo a prime p. (Much faster than trying all (p-1) possibilities one by one.)

Another well-known (non-algorithmic) proof of the existence of multiplicative inverse is here:

> Let x be a non-zero number in {1, 2, …, p-1}. Then, no two among the following (p-1) numbers are congruent to each other modulo p:
>
> > x, 2.x, …., (p-1).x
>
> Further, note that none of these numbers is congruent to zero modulo p (i.e., is divisible by p).
>
> Therefore, there exists *exactly* one y in {1, 2, …, p-1} such that x.y is congruent to 1 modulo p.

Q3 Solution Outline.

(I am using ~ for the congruent symbol below.)

Suppose we use quadratic probing and let:

> g(x,i) = h(x) + c1*i + (c2*i^2) (mod p)

Suppose, for some 0 <= i < j <= p-1 :

> h(x)+ c1*i + (c2*i^2) ~ h(x) + c1*j + (c2*j^2) (mod p)

This is equivalent to (apply rules for operating on congruences):

$$c1*i - c1*j + (c2*i^2) - (c2*j^2) \sim 0 \pmod p$$
$$c1*(i-j) + c2*(i^2-j^2) \sim 0 \pmod p$$
$$(i-j) * (c1 + c2*(i+j)) \sim 0 \pmod p$$

Now, $-(p-1) <= (i-j) <= -1$. Therefore, $(i-j)$ is not divisible by p.

This implies that

$$(c1 + c2*(i+j)) \sim 0 \pmod p \quad \text{-------------------------} \ (*)$$

We assume c2 is not equal to 0 modulo p. (Otherwise it is just a form of linear probing.) Further, this also implies that c2 has a (unique) multiplicative inverse d such that $d.(c2) \sim 1 \pmod p$.

Then, equation (*) reduces to:

$$c2*(i+j) \sim (-c1) \pmod p$$

Multiply both sides by d to get:

$$(i+j) \sim [(-c1)*d] \pmod p$$

Putting $v = (-c1)*d \pmod p$, we get that:

$$(i+j) \sim v \pmod p \quad \text{----------------------} \ (**)$$

Thus, we get that, for every $0<=i<=p-1$:

$$g(x,i) = g(x,v-i)$$

This divides {0, 1, 2, …, p-1} into at most [floor((p-1)/2)+1] disjoint pairs. Both indices (i1, i2) in the same pair have the same values for corresponding probe locations g(x,i1) and g(x,i2).

Thus, the number of distinct probe locations is at most [floor((p-1)/2)+1].

(We saw a base case of above in class, where we picked c1=c2=1 and p=17. Then, d=1, v = -1, and g(x,i) = g(x,-1-i) for every 0<=i<=16.)