Question 5

Part A

CODE:

```
1  // http://rise4fun.com/Dafny/Is4L
2  // return the index of an integer -- key in an integer array -- a
3  // if the key is not found then return -1
4
5  method FindWithLoops(a: array<int>, key: int) returns (i: int)
6  requires a != null;
7  ensures i >= 0 <==> 0 <= i <= a.Length - 1 && a[i] == key;
8  {
9    i := a.Length - 1;
10   while i >= 0
11     invariant forall j :: a.Length  - 1 > j > i >= 0 ==> a[j] != key;
12   {
13     if a[i] == key { return; }
14     i := i - 1;
15   }
16 }
```

PROOF:

$$I = \forall j, a.\text{Length} - 1 > j > i \geq 0 \implies a[j]! = \text{key} \tag{1}$$

At the beginning of the loop there is no possible j so the invariant holds.

During the loop if there exists $j > i$ such that \$a[j] = key \$ then there must have been an $i^(\text{th})$ iteration of the loop where $a[i] = \text{key}$ and therefore the fucntion would have returned at line 18 which is a contradiction.

At the termination of the loop there are two cases

$$\exists i, a.\text{Length} - 1 > i \geq 0 \wedge a[i] = \text{key}$$

where the key was found or,

$$i = -1 \implies \nexists i, a.\text{Length} - 1 > i \geq 0 \wedge a[i] = \text{key}$$

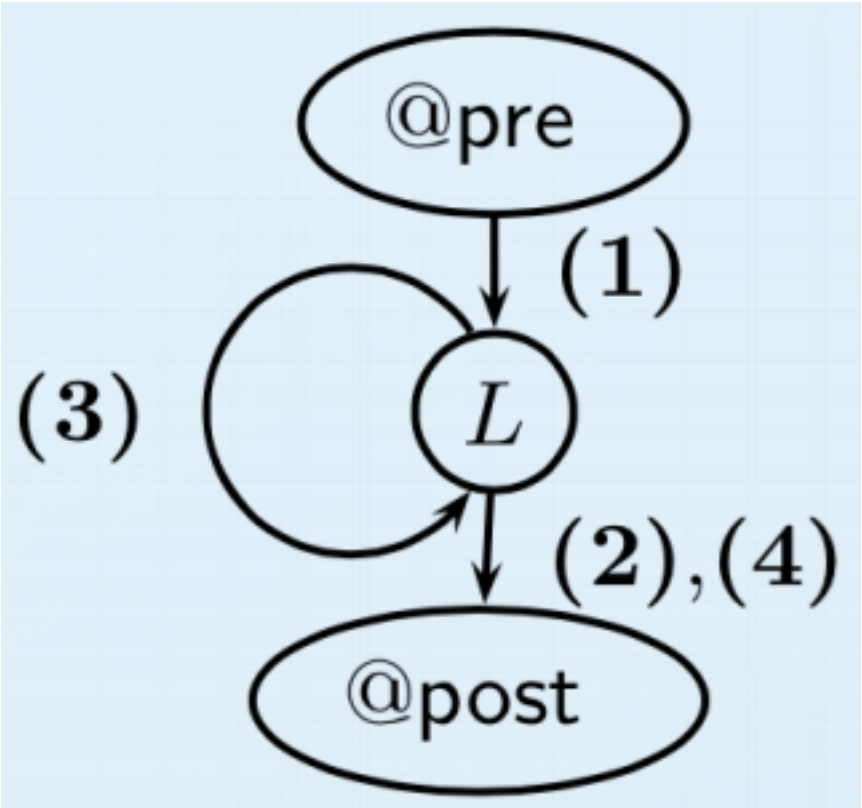
in which cases the invariant also holds since it implies

$$\forall j, a.\text{Length} - 1 > j > i = -1, \nexists a[j] = \text{key}$$

which is equivalent to the invariant.

Therefore the invariant holds before during and after the loop.

Part B



Path (1) goes from the precondition to the loop invariant

$$@pre\ a! = \text{null};$$

$$i := a.\text{Length} - 1;$$

$$@L\ \forall j :: a.\text{Length} - 1 > j > i \geq 0 \implies a[j] \neq \text{key};$$

Path (2) goes from the loop invariant to the postcondition

$$@L\ \forall j :: a.\text{Length} - 1 > j > i \geq 0 \implies a[j] \neq \text{key};$$

$$\text{assume } a[i] = \text{key}$$

$$@post\ i \geq 0 \iff 0 \leq i \leq a.\text{Length} - 1 \wedge a[i] == \text{key};$$

Path (3) goes once through the loop

$$@L\ \forall j :: a.\text{Length} - 1 > j > i \geq 0 \implies a[j] \neq \text{key};$$

$$\text{assume} a[i] \neq \text{key};$$

$$i := i - 1;$$

$$@L\ \forall j :: a.\text{Length} - 1 > j > i \geq 0 \implies a[j] \neq \text{key};$$

Path (4) goes from the loop invatiant to the postcondition

$$@L\ \forall j :: a.\text{Length} - 1 > j > i \geq 0 \implies a[j] \neq \text{key};$$

$$\text{assume } i < 0;$$

$$@\mathit{post}\ i \geq 0 \iff 0 \leq i \leq a.\text{Length} - 1 \wedge a[i] = \text{key};$$