1. 是对的，h(k,i) = (h(k)+i) where h is a hash function, so h(k) = {0,…….,m-1}

因为I = 0,1….,m

h(k)+i里面有超过m个连续的数字，所以当（h(k)+i）mod m的时候可以把m的module（余数）全部沾满 （结果只能是0到m之间，而h(k) = {0,…….,m-1}）

image of h(k, i) is {0,1,…..,m-1}

1. 不可能，可以通过穷举，暴力破解

h(k, i) = (h(k) + i^2 ) mod m

因为h(k) = {0,…….,m-1}, i是随便去的，但I mod m的值只能等于{0,1,….m-1}

= (h(k) mode m + i^2 mod m) mod m

=（h(k)+( i mod m)^2 mode m）

let j = {0,1….6}

=（（h(k)+ j^2 mod m） mode m）

然后来算一下j^2 mod m （m等于7这里）

j^2= 0 1 4 9 16 25 36

j^2 mod m = 0 1 4 2 2 4 1

假设h（k）就是很很不好的hash function，let h(k) = 0 （可以等于任意function）

=（（h(k)+ j^2 mod m） mode m）

=（（0+ j^2 mod m） mode m）

={0,1,2,4} mod m肯定是占不满整个bucket的（1，2，3，4，5，6，7）

所以image of h(k, i)={0,1,2,4}

（c）假设p是一个prime number

size m is a prime number greater then 3

first m/2 probe locations = prime number/2 = (p-1)/2=是个基数

h(k, i) = (h(k) + i^2 ) mod m

=(h(k) mod m + i^2 mod m) mod m

= (h(k) + (I mod m)^2 mod m

若i的取值是positive integer

那I mod m的取值就是{0,1,…..m-1}

let j = I mod m,那m= {0,1,2….m-1}

=（h(k)+ j^2） mod m

=（h(k) mod m+ j^2 mod m） mode m

=占有率超过一半=j^2 mod m的结果超过m/2

现在就要看j^2 mod m的结果是否超过m/2

j^2=0 1 4 9 16 25 36, ……………, ((p-1)/2)^2, ((p+1)/2)^2,………………..,(p-2)^2, (p-1)^2

注意：1和(p-1)^2 , mod m的结果是一样的

2和(p-2)^2, mod m的结果是一样的

所以i^2 == (p-i)^2 mod p

所以要看j里面有多少不同的值，只要看前一部分就好

所以得到j^2 mod p = {0 mod p, 1^2 mod p , ……….. (p-1)/2}^2 mod p , ((p+1)/2)^2 mod p}

= 一共有(p+1)/2个值

= p/2的向上取整

就说明j^2 mod p有超过一半以上的结果了，那就要证明里面那些东西都不一样

use contradiction to prove

let j1,j2属于「0，……., (p-1)/2」，let j1 != j2, and j1^2 mod = j2^2 mod p（整除这个是错的）

等于 j1^2 = j2^2 mod p（assume j1>j2）

根据module的性质，j1^2 = kp + j1^2 where k is a positive integer

j1^2 = j2^2 = kp

so (j1+j2)(j1-j2)=kp

but p is a prime number, 任何数都不可能是p的因数(any number is not a factor of p)

因为j1，j2是属于「0，……., (p-1)/2」，所以j1+j2<p,| j1+j2|<p，所以他们两个的乘积就不可能等于kp。

so, (j1+j2) and (j1-j2) are not factor of p.

so(j1+j2)(j1-j2)! =kp

so by contradiction

所以在「0，……., (p-1)/2」里的每个数字都是不一样的

所以|j^2 mod p | = (p+1)/2

i: 0,1,2….

j = I mod p: 0,…..p-1

j^2 mod p属于{0 mod p, 1 mod p, …., ((p-1)/2)^2 mod p}

k = j^2 mod p

|k| = (p+1)/2 > p/2

AVL tree的rotation：

如果你是单个孩子的，把我的父亲连接到我的孩子，然后把我插入我的孩子上

旋转：

LL的话就right rotation，RR的话就left rotation

如果是左右，就右左转，如果是右左，就左右转