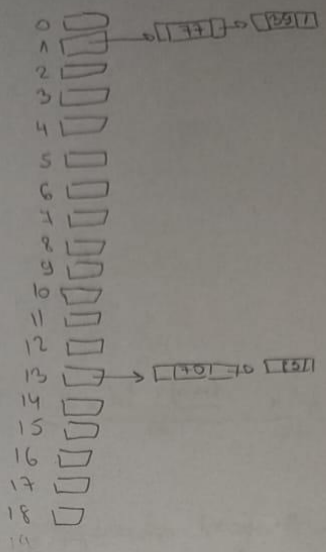
①

1.a) $h(k) = k \bmod m$

h(k)	key
77 mod 19	1
69 mod 19	12
39 mod 19	1
70 mod 19	13
6 mod 19	6
8 mod 19	8
40 mod 19	2
89 mod 19	13
49 mod 19	11
15 mod 19	15



b) $h_1(k) = k \bmod m$ $h_2(k) = 1 + k \bmod m$

⇒ key: 77

$h_1(77) = 77 \bmod 19 = 1$

$h_2(77) = 1 + (77 \bmod 18) = 6$ ⇒ $h(77,0) = (1 + 0 \cdot 6) \bmod 19 = 1$

⇒ key: 69

$h_1(69) = 69 \bmod 19 = 12$

$h_2(69) = 1 + (69 \bmod 18) = 16$ ⇒ $h(69,0) = (12 + 0 \cdot 16) \bmod 19 = 12$

⇒ key: 39

$h_1(39) = 39 \bmod 19 = 1$

$h_2(39) = 1 + (39 \bmod 18) = 4$ ⇒ $h(39,0) = (1 + 0 \cdot 1) \bmod 19 = 1$

⇒ $h(39,1) = (1 + 1 \cdot 4) \bmod 19 = 5$

⇒ key: 70

$h_1(70) = 70 \bmod 19 = 13$

$h_2(70) = 1 + (70 \bmod 18) = 17$ ⇒ $h(70,0) = (13 + 0 \cdot 17) \bmod 19 = 13$

⇒ key 8

$h_1(8) = 8 \bmod 19 = 8$
$h_2(8) = 1 + (8 \bmod 18) = 9$
$\Rightarrow h(8,0) = (8 + 0 \cdot 9) \bmod 19 = 8$

⇒ key: 40

$h_1(40) = 40 \bmod 19 = 2$
$h_2(40) = 1 + (40 \bmod 18) = 5$
$h(40,0) = (2 + 0 \cdot 5) \bmod 19 = 2$

⇒ key: 89

$h_1(89) = 89 \bmod 19 = 13$
$h_2(89) = 1 + (89 \bmod 18) = 18$
$h(89,0) = (13 + 0 \cdot 18) \bmod 19 = 13$
$\Rightarrow h(89,1) = (13 + 1 \cdot 18) \bmod 19 = 12$
$h(89,2) = (13 + 2 \cdot 18) \bmod 19 = 11$

⇒ key 49

$h_1(49) = 49 \bmod 19 = 11$
$h_2(49) = 1 + (49 \bmod 18) = 14$
$h(49,0) = (11 + 0 \cdot 14) \bmod 19 = 11$
$\Rightarrow h(49,1) = (11 + 1 \cdot 14) \bmod 19 = 16$
$h(49,2) = (11 + 2 \cdot 14) \bmod 19 = 14$
$h(49,3) = (11 + 3 \cdot 14) \bmod 19 = 15$

⇒ key 15

$h_1(15) = 15 \bmod 19 = 15$
$h_2(15) = 1 + (15 \bmod 19) = 16$
$h(15,0) = (15 + 0 \cdot 16) \bmod 19 = 15$
$\Rightarrow h(15,1) = (15 + 1 \cdot 16) \bmod 19 = 12$
$h(15,2) = (15 + 2 \cdot 16) \bmod 19 = 9$

0 ☐
1 ~~49~~
2 ~~40~~
3 ☐
4 ☐
5 ~~49~~ i = 1
6 16
7 ☐
8 8
9 15 i = 2
10 ☐
11 89
12 ~~89~~
13 ~~89~~
14 ☐
15 ~~49~~ i = 3
16 ☐
17 ☐
18 ☐

2. Je li hash funkcija $f(x) = \sum_{i=1}^{n} a_i x \pmod{8}$ univerzalna?

Funkcije može biti univerzalna samo ako je n prost broj, što u ovom slučaju ne vrijedi, $n=8$.

npr $a_i = 2$, $i = 1 \dots n$

$\Rightarrow f(x) = 0$, $\forall x$

②

$X \sim \begin{pmatrix} \text{broj koraka} & 1 & 2 & 3 & \dots & n-1 \\ \text{vjerojatnost} & \frac{1}{m} & \frac{2}{m} & \frac{3}{m} & \dots & \frac{n-1}{m} \end{pmatrix}$

sl. var. X modelira vrij. složenosti

$\Rightarrow EX = \sum_{i=1}^{n-1} \frac{n \cdot i}{m} = \frac{n^2 - \frac{n(n+1)}{2}}{m} = \frac{n^2 - n}{2m} \approx \frac{1}{2}$

Očekivani broj koraka je proporcionalan broju ključeva kvadratno