Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax+b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

x
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax + b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

For all $x = 0, 1, \ldots, 16$ write the values for $h_{1,0}(x)$

x
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax+b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

For all $x = 0, 1, \ldots, 16$ write the values for $h_{1,0}(x)$

x	$h_{1,0}(x)$
0	0
1	1
2	2
3	3
4	4
5	0
6	1
7	2
8	3
9	4
10	0
11	1
12	2
13	3
14	4
15	0
16	1

Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax+b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

For all $x = 0, 1, \ldots, 16$ write the values for $h_{1,0}(x)$ and then $h_{2,2}(x)$.

x	$h_{1,0}(x)$
0	0
1	1
2	2
3	3
4	4
5	0
6	1
7	2
8	3
9	4
10	0
11	1
12	2
13	3
14	4
15	0
16	1

Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax+b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

For all $x = 0, 1, \ldots, 16$ write the values for $h_{1,0}(x)$ and then $h_{2,2}(x)$.

x	$h_{1,0}(x)$	$2x + 2 \bmod 17$	$h_{2,2}(x)$
0	0	2	2
1	1	4	4
2	2	6	1
3	3	8	3
4	4	10	0
5	0	12	2
6	1	14	4
7	2	16	1
8	3	1	1
9	4	3	3
10	0	5	0
11	1	7	2
12	2	9	4
13	3	11	1
14	4	13	3
15	0	15	0
16	1	0	0

Recall the universal hash function family defined by

$$h_{a,b}(x) = \Big((ax+b) \bmod p\Big) \bmod m$$

where $a \in Z_p^*$, $b \in Z_p$ and p is a prime with $p \geq U$.

Let $p = 17$, $m = 5$.

For all $x = 0, 1, \ldots, 16$ write the values for $h_{1,0}(x)$ and then $h_{2,2}(x)$.

Note how "uncorrelated" $h_{2,2}(x)$ looks to the eye.

x	$h_{1,0}(x)$	$2x + 2 \bmod 17$	$h_{2,2}(x)$
0	0	2	2
1	1	4	4
2	2	6	1
3	3	8	3
4	4	10	0
5	0	12	2
6	1	14	4
7	2	16	1
8	3	1	1
9	4	3	3
10	0	5	0
11	1	7	2
12	2	9	4
13	3	11	1
14	4	13	3
15	0	15	0
16	1	0	0