choosing $m = 2^p - 1$ when

k is a character string interpreted in radix 2^p.

$c_1 \; c_2 \; c_3$

C A T ① $\rightarrow \left(c_1 * (2^p)^2 + c_2 * 2^p + c_3 \right) \bmod (2^p - 1)$.

T A C

⋮

② $\rightarrow \left(c_2 * (2^p)^2 + c_3 * 2^p + c_1 \right) \bmod (2^p - 1)$

① $= \left(c_1 * \left((2^p - 1)^2 + 2 \cdot (2^p - 1) + 1 \right) + c_2 * (2^p - 1 + 1) + c_3 \right) \bmod (2^p - 1)$

$= (c_1 + c_2 + c_3) \bmod (2^p - 1)$

② $= (c_2 + c_1 + c_3) \bmod (2^p - 1)$

thus ① = ②

$$\left|\{h \in H \mid h(x) = h(y)\}\right| = w$$

$$\underline{w \leq \frac{|H|}{m}}$$

x, y

$h \in H$

$$\frac{w}{|H|}$$

$m = 3$

$|U| = 5$

$\frac{5 * 4}{3} = 6$

$ax+b$

$x=1$

b \ a	1	2	3	4
0	1	2	3	4
1	2	3	4	5
2	3	4	5	6
3	4	5	6	7
4	5	6	7	8

$ax+b$

$x=4$

b \ a	1	2	3	4
0	4	8	12	16
1	5	9	13	17
2	6	10	14	18
3	7	11	15	19
4	8	12	16	20

$(ax+b) \bmod 5$

b \ a	1	2	3	4
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

b \ a	1	2	3	4
0	4	3	2	1
1	0	4	3	2
2	1	0	4	3
3	2	1	0	4
4	3	2	1	0

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

Given x, y, $x \neq y$

Let

$$s = (ax+b) \bmod p$$

$$t = (a\cancel{x}y+b) \bmod p$$

$$s = t \,?$$

$$\underline{s - t} = (a(x-y)) \bmod p$$

Assume $s - t = 0$, $a \neq 0$ $a < p$

$$s - t = ((p-w)\cdot(p-v)) \bmod p$$

where $1 \leq w, v \leq p-1$

$$s - t = (p^2 - pv - pw + vw) \bmod p$$

$\Rightarrow x = y \Rightarrow$ contradiction.

thus we have $s \neq t$.

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

$s = (ax+b) \bmod p$

$t = (a\cancel{x}y+b) \bmod p$

$s \neq t.$

(s,t) is valid, if

$s \bmod m = t \bmod m$

$\left| \{(s,t) \mid (s,t) \text{ is valid}\} \right|$

$s: p \quad t: \lceil p/m \rceil - 1$

$p * (\lceil p/m \rceil - 1)$

$$\lceil p/m \rceil = \begin{cases} p/m & \text{if } p \bmod m = 0 \\ p/m + 1, & \text{if } p \bmod m \geq 1 \end{cases}$$

$$\lceil p/m \rceil \leq \frac{p+m-1}{m} = \frac{p-1}{m} + 1$$

$$\Longrightarrow p * \frac{p-1}{m}$$

For a given pair (s,t)

$s = (ax+b) \bmod p$

$t = (a\cancel{x}y+b) \bmod p$

how many pairs (a,b)