HASHING

$\mathcal{H}$ = universal hash family

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

random choice

$a \in \mathbb{Z}_p^+ = \{1, 2, \dots, p-1\}$

$b \in \mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$

tR
%p
mod 5
Sha-128
..
} good but these are not enough or p prime is difficult to choose often

1) We can draw, uniformly at random, a choice of $h_{ab} \in \mathcal{H}$ with $pr = \frac{1}{|\mathcal{H}|} = \frac{1}{(p-1)p}$

1) m is provided by the user

1) p is a prime in $[m+1 \dots 2m]$ (it exists !)

We say $\mathcal{H}$ is **universal** $\quad h \in \mathcal{H} : U \to [m]$

U: universe of keys; $[m]$: range of values: $0..m-1$

For any choice $k_1, k_2 \in U$, $k_1 \neq k_2$, (user decides them so k_1, k_2 are **not** random but are given: no control on them)

$$\#\{h \in \mathcal{H} \text{ s.t. } \underbrace{h(k_1) = h(k_2)}_{\text{collision}}\} \text{ is } \frac{|\mathcal{H}|}{m}$$

$$\Pr_{h \in \mathcal{H}}(\text{collision}) = \frac{\#\text{BAD choices}}{\#\text{ choices}} = \frac{|\mathcal{H}|/m}{|\mathcal{H}|} = \frac{1}{m}$$

$h_{a,b}(x) = ax+b \,\%\, p \,\%\, m$ is UNIVERSAL $U \subseteq \mathbb{Z}_p$

$|U| = (p-1)p \Rightarrow$ #a_s, b_s BAD choices is $\frac{|U|}{m} = \frac{(p-1)p}{m}$

$k_1 \neq k_2$

$$\left.\begin{array}{l} ak_1+b \,\%\, p \\ \text{or } ak_2+b \,\%\, p \end{array}\right\}$$

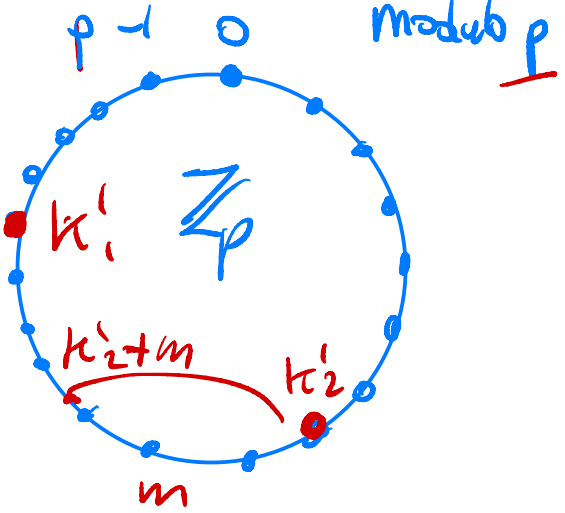
Q. how many a_s, b_s satisfy this system ?

For each choice of $a \in \mathbb{Z}_p^+$ there is a single $b \in \mathbb{Z}_p$ satisfying

$p-1$ choices for $a \to k_1'$

$\sim \frac{p}{m}$ choices for b (modulo m) $\hookrightarrow k_2' \,\%\, m$

$$\frac{ak_1+b \,\%\, p \,\%\, m}{ak_2+b \,\%\, p \,\%\, m}$$



$k_1' = a k_1 + b \pmod p$

$k_2' = a k_2 + b \pmod p$

$k_1' \neq k_2' \iff k_1 \neq k_2$ $\quad U \subseteq \mathbb{Z}_p$

$k_1' \bmod m = k_2' \bmod m$

$\frac{p}{m}$ choices for k_2' gives

↳ b

BAD choices $(p-1)\frac{p}{m} = \frac{|\mathcal{H}|}{m}$

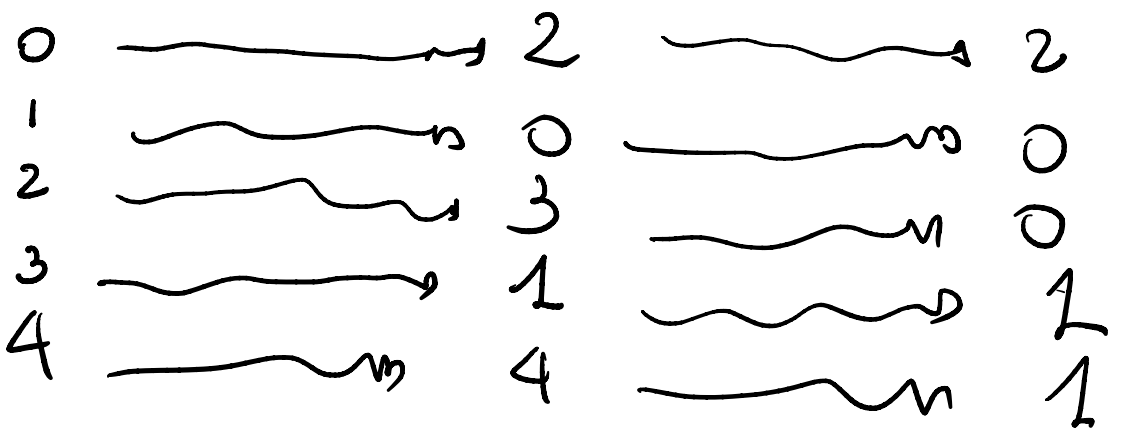
$a, b, x \in \mathbb{Z}_p$

$a \neq 0$

$p = 5$ $\quad a = 3, b = 2$

$\mathbb{Z}_p$ $\quad 3x + 2 \ \%5$

$m = 3$

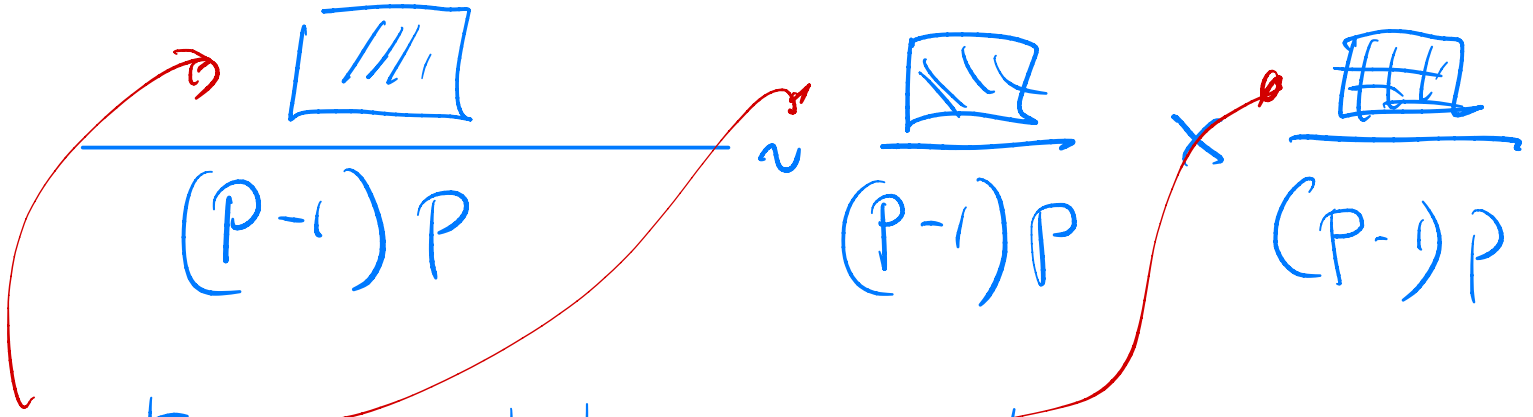


x

$$\left\lceil \frac{p}{m} \right\rceil = 2$$

$h_{ab}(x) = ax+b \;\%p\;\%m$ is 2-independent

$$\Pr_{h\in H}\left(h(x_1)=y_1 \wedge h(x_2)=y_2\right) = \Pr_{h\in H}\left(h(x_1)=y_1\right) \times \Pr_{h\in H}\left(h(x_2)=y_2\right)$$



numerators: count how many choices of a_s, b_s are BAD