$x \neq y$

$1 \quad 2$

$\underline{2.2.3}$

$$s = (a_1 x + b) \bmod p$$

$$s = (a_2 x + b) \bmod p$$

$$(a_1 x - a_2 x) \bmod p = 0$$

$$\underbrace{(a_1 - a_2)}_{<p} \cdot \underbrace{x}_{<p} \bmod p = 0$$

$$(a_1 - a_2) \cdot x = i \cdot p$$

$$\cancel{x = 0} \quad X$$

$$\underline{a_1 = a_2}$$

for any valid pair of $(s,t)$

there is exactly one pair

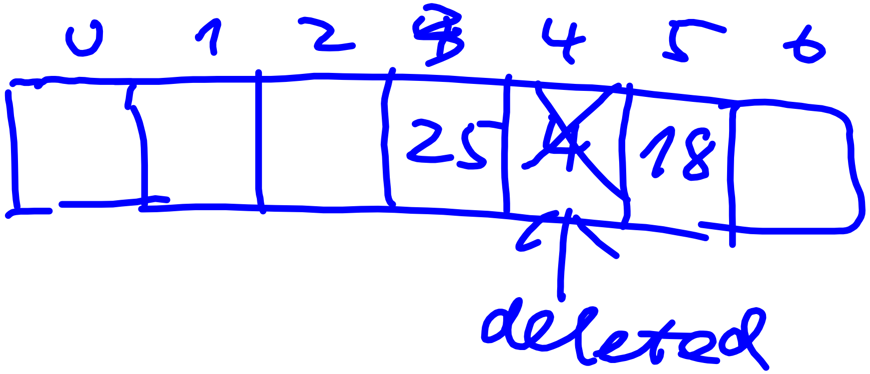
$(a,b)$, s.t.

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

$$t = (ay+b) \bmod p$$

the number of pairs $(a,b)$, s.t $\underline{h_{a,b}(x) = h_{a,b}(y)}$

is less than $\underline{p(p-1)/m}$




$$\left(h(x) - s(j_1, x)\right) \bmod m$$

$$\left(h(x) - s(j_2, x)\right) \bmod m$$

$$s(j_1, x) - s(j_2, x) \equiv 0 \pmod m$$

$$(-1)^{j_1} * \lceil \tfrac{}{2}$$

$$(-1)^{j_1} * \left\lceil \frac{j_1}{2} \right\rceil^2 - (-1)^{j_2} * \left\lceil \frac{j_2}{2} \right\rceil^2$$

$$= 0 \quad (\bmod m)$$

1) $j_1, j_2$ are even.

$$\left\lceil \frac{j_1}{2} \right\rceil^2 - \left\lceil \frac{j_2}{2} \right\rceil^2 = 0 \quad (\bmod m)$$

$$\left(\frac{j_1}{2} + \frac{j_2}{2}\right) \cdot \underline{\left(\frac{j_1}{2} - \frac{j_2}{2}\right)} = 0 \quad (\bmod m)$$