$$h(k_1i) = (f(k_1) + c_1i + c_2i^2) \text{ mod m} \qquad i = 0, 1, ..., m-1$$

hvih nelolis vrijesmosti:

$$h(2,0) = A(2) + 0$$

$$h(2,1) = A(2) + 1$$

$$h(2,2) = A(2) + 3$$

$$h(2,3) = A(2) + 6$$

Mozemo moerti sla je to verveija:

 $h\left(\mathcal{L}_{i}i\right) = h\left(\mathcal{L}_{i}i-1\right) + i$

 $h(l_i) = l(l) + \sum_{i=0}^{i} = l(l) + \frac{i(i+1)}{2}$ Mje enjems Los:

- All + 2i + 12i

Je rehverje i početne jesmoslobe violino do m [C1 = C2 = 2]

(5) U vlgoritmu imomo m prolinonji. Da hi pretnožio molu poziciji u tellici me pozicije a i b prihion molog prolinonji morgi hit. pozličite.

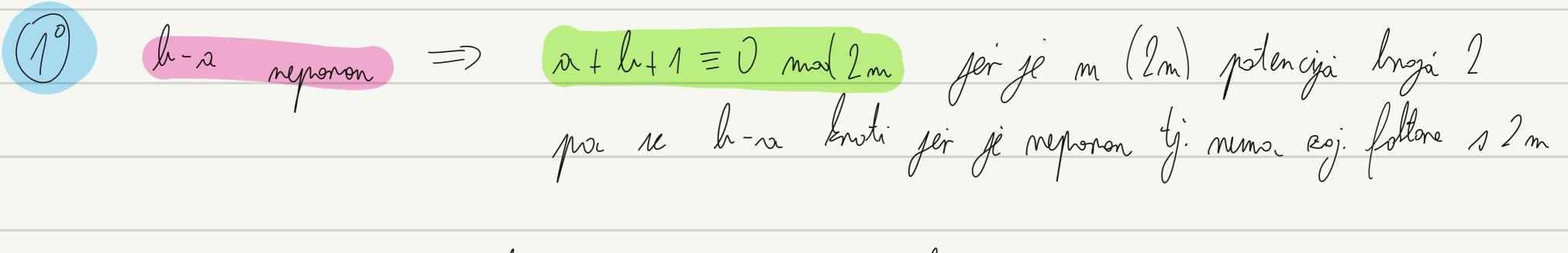
Oretportorino suprotoro, tj. ola 0 za < b zm., Vnýseli:

$$\int \left(\frac{\lambda}{\lambda} \right) + \frac{\lambda \left(\frac{\lambda}{\lambda} \right)}{2} = \int \left(\frac{\lambda}{\lambda} \right) + \frac{\lambda \left(\frac{\lambda}{\lambda} \right)}{2} \mod m$$

$$\frac{\langle -\rangle}{2} = \frac{b(b+1)}{2} mod m / 2$$

 $a^{2} + a \equiv b^{2} + h \mod 2m$ $\left(h - a\right) + \left(h - a\right) \left(h - a\right) + \left(h - a\right) \left(h + a\right)$ $h^{2} - a^{2} = \left(a + b\right) \left(h - a\right) \equiv h - a \mod 2m$ $\left(h - a\right) + \left(h + a\right)$

		,		
()	(h - » (ath +1)	= 0	mool 2m



iz myets 0 < 2 < 1 < m enome 2 < b pa myédi:

sithen 1 = 2h = 2m pa sith = 0

strje I s myëtom 0 / 2 2 < b < m

(2°) h-n peron => a+h+1 mona hit, neporon pa nema ægi, faltore s 2 m

(jer je m potencijā loga 2) te ga knotima i sitoje;

b-a=0 mal 2m

Is rujeta imono:

 $|b-a| \leq b+a \leq 2b \leq 2m$ pa b-a mona liti = 0

stor je apret & s myetom 0 < 2 < b < m

Doble, slysnitom de doiste pretrožiti svolu poziciji u tobba.