ZADAĆA 2 MATEJ SPAJIĆ

3. 4.

$f(k,0) = h(k) + 0 = C + 0$

$f(k,1) = f(0) + 1 = h(k) + 1 = C + 1$

$f(k,2) = f(1) + 2 = f(0) + 1 + 2 = h(k) + 3 = C + 3$

$f(k,3) = f(2) + 3 = f(1) + 2 + 3 = f(0) + 1 + 2 + 3 = h(k) + 6 = C + 6$

tj. $f(k,i) = f(k,i-1) + i$

=> REKURZIVNA RELACIJA POMOĆU KOJE DOKAZUJEMO:

$$f(k,i) = h(k) + \sum_{j=0}^{i} j = h(k) + \frac{n(n+1)}{2}$$

$c_1 = c_2 = \frac{1}{2}$ ZBOG TOGA ŠTO:

$$f(k,i) = h(k) + \frac{1}{2}i + \frac{1}{2}i^2$$

5. $0 \leq a < b < m$ ZA KOJE VRIJEDI $f(k,a) = f(k,b) \bmod m$:

$$h(k) + \frac{a(a+1)}{2} = h(k) \frac{b(b+1)}{2} \bmod m$$

$$\Downarrow$$

$$\frac{a(a+1)}{2} = \frac{b(b+1)}{2} \bmod m$$

$$\Downarrow$$

$$\frac{a(a+1)}{2} - \frac{b(b+1)}{2} = 0 \bmod m$$

$$\Downarrow$$

$$\frac{a^2 + a + ab - b^2 - b - ab}{2} = 0 \bmod m$$

$$\Downarrow$$

$$\frac{(a-b)(a+b+1)}{2} = 0 \bmod m$$

$$\Rightarrow \frac{(a-b)(a+b+1)}{2} = rm$$

$$(a-b)(a+b+1) = r \cdot 2^{p+1}$$

JEDAN OD: $(a-b)$ ILI $(a+b+1)$ SU DJELJIVI S 2^{p+1}. ZNAMO DA NIJE $(a-b)$ JER $a-b < m < 2^{p+1}$, TAKOĐER ZNAMO DA NIJE $(a+b+1)$ JER $a+b+1 \leq (m-1)+(m-2)+1 = 2m-2 < 2^{p+1}$. $\lightning$ $f(k,a) \neq f(k,b)$ ZA $0 \leq a < b < m$.