Pomoćni zadaci

4. Prvo proračunajmo nekoliko početnih vrijednosti:

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

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

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

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

Opaženo:

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

Indukcijom možemo dokazat:

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

Ako uzmemo $c_1 = c_2 = \frac{1}{2}$, imamo

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

Za svaki i dobivamo različitu vrijednost.

5. Pretpostavimo suprotno. To znači da postoje dvije različite vrijednosti a i b tako da $0 \leq a < b < m$ za koje je $f(k,a) \equiv f(k,b) \mod m$:

$$h(k) + \frac{a(a+1)}{2} \equiv h(k) \frac{b(b+1)}{2} \mod m$$

$$\frac{a(a+1)}{2} \equiv \frac{b(b+1)}{2} \mod m$$

$$\frac{a(a+1)}{2} - \frac{b(b+1)}{2} \equiv 0 \mod m$$

$$\frac{a^2+a-b^2-b}{2} \equiv 0 \mod m$$

$$\frac{a^2+a+ab-b^2-b-ab}{2} \equiv 0 \mod m$$

$$\frac{(a-b)(a+b+1)}{2} \equiv 0 \mod m$$

Po tom postoji r tako da vrijedi:

$$(a-b)(a+b+1) = 2rm$$

Pošto je m potencija broja 2 i postoji broj p tako da $m = 2^p$ imamo:

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

a i b su brojevi što znači da jedan od brojeva $(a-b)$ i $(a+b+1)$ je paran, a drugi je neparan, tj. jedan od ta 2 broja nije djeljiv s 2. To znači da drugi je djeljiv s 2^{p+1}. To je kontradikcija jer $(a-b)$ ne može biti djeljiv s 2^{p+1} jer vrijedi

$$a-b < m < 2^{p+1}$$

Isto tako ne može biti $(a+b+1)$ jer vrijedi

$$a+b+1 \leq (m-1)+(m-2)+1 = 2m-2 < 2^{p+1}$$

To je kontradikcija i vrijedi $f(k,a) \neq f(k,b)$ za $0 \le a < b < m$, što znači da odg. prelazi različitu poziciju u tablici.