2 ADACA 2 4) par početnih vojednosti f(&,0) = c+0 f(&,1) = f(0)+1=h(&)+1=c+1 f(2,2) = f(1)+2 = f(0)+1+2 = c+3 f(2,2) = f(2,1-1)+i20 c1=c2=2 => f(k,i)=6(2)+2i+2i2 za soli razlicite vijednosti 5) postaje 2 različite mjednoti a, osasbem $f'(2, a) = f(2, 6) \mod i$ $h(2) + a(a+1) - h(2) b(b+1) \mod m$ a(a+1) = b(b+1) mod m $\frac{a(a+1)}{2} - \frac{b(b+1)}{2} = 0 \text{ mod } m$ (a-b)(a+b+1) = 0 med m =) $\exists r + d$. (a-b)(a+b+1) = 2rm=) $\exists p + d$. $m = 2^{p}$ ger je m put. br. 2 $(a-b)(a+b+1) = r \cdot 2^{p+1}$ - jedan od (a+b) ili (a+b+1) je param, drugi neparam, pa je jedan dieljir o 2^{p+1} a to re mjedi jer (a-b) mje geljir jer $a-b < m < 2^{p+1}$ (a+b+1) $-1+\cdots = 2(m-2) < 2^{p+1}$ Dable 20 0 € a < 6 < m med: f (8, a) × f(8, b) =) alp. pretrovziranja pretroži snolen posaje u tablici