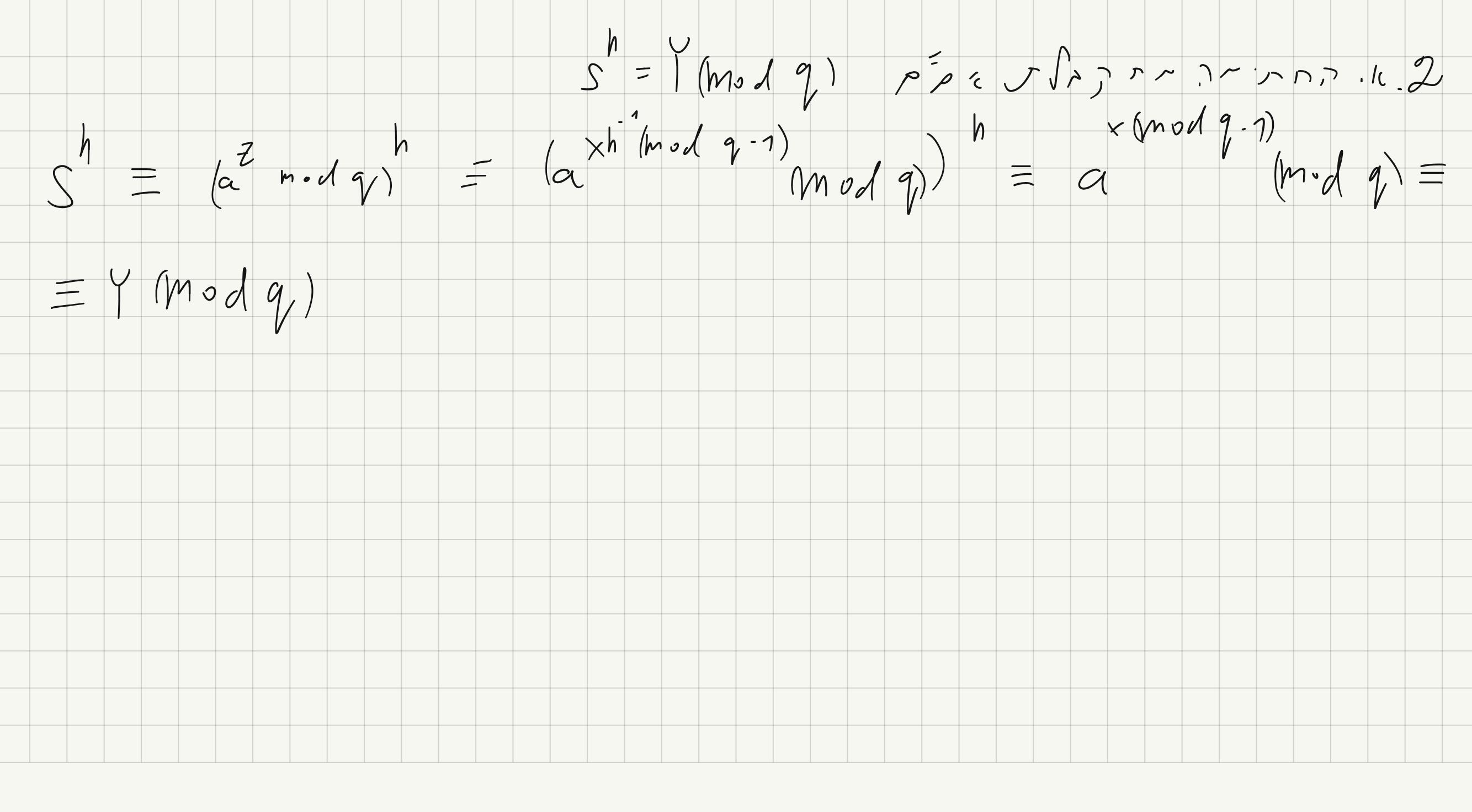
$= 2 \left( \frac{1}{2} \left( h(M) + \frac{1}{2} + r \right) \left( mod h \right)^{2} + 3 \left( \frac{1}{2} k(h(M) + \frac{1}{2} + r) \left( mod h \right)^{2} \right) + 3 \left( \frac{1}{2} k(h(M) + \frac{1}{2} + r) \left( mod h \right)^{2} \right)$ => 2 - 2 (hm) + 1+1) (modn) + 9 2 × (hm) + - +) (modn) ~ 1 5 5 - 5 5 5 = ) 2 - 2 (hm) r - r) + 9 k (hm) r - r) (mod h) 2 1 Cmp 2 H \_ x x 3 1.  $=) 2^{-2} (h(m)r^{-1}+r)^{2}+k^{2} \cdot (-(k^{-1})^{2}) (h(m)r^{-2}-r)^{2}) (mod h)$ K, K 100 118 m  $= \frac{1}{2} \left( \frac{1}{h(M)} + \frac{1}{1} + \frac{1}{h(M)} + \frac{1}{1} + \frac{1}{h(M)} + \frac{1}{h(M)$  $= \frac{1}{2} \frac{1}{(1hm)^{2}} \frac{1}{1} + \frac{1}{2} \frac{1}{hm} + \frac{1}{1} \frac{1}{1} \frac{1}{1} + \frac{1}{2} \frac{1}{hm} \frac{1}{hm} + \frac{1}{1} \frac{1}{1}$ 7311~100



 $S' = (S(h(M))^{-1})h(M)$   $S' = (S(h(M))^{-1})h(M)$   $S' = (S(h(M))^{-1})h(M)$  $= \sum_{i=1}^{n} h(m') \left( h(m') h(m') \right) h(m')$   $= \sum_{i=1}^{n} h(m') h(m$ ver (M, S) = ver (M, S) = true