- CONTROLLO PARI

$m \to n$ ad L m

- grado n pari $m = 2cm$
- grado n dispari $m = \frac{2c}{n}$

traffico m nodi grado $m \le \frac{2m}{n}$ $n \ge 2$
(nodo m ap. ADJ nodi)

$h_{kl} = ((ak + b) \bmod p) \bmod m$

$\mathcal{H}_{pm} = \{ h_{kl} : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p \}$

TEO $\mathcal{H}_{pm}$ è UNIVERSALE

$\forall k, l$ dove $k, l \in \mathbb{Z}_p$: $k \neq l$

$r = (ak + b) \bmod p$

$s = (al + b) \bmod p$

$r \neq s$:

$r - s = a(k - l) \bmod p$

$a \neq 0$ $\{ a \in \mathbb{Z}_p^* \}$

$(k - l) \bmod p$

r a l coll. primo m p

s $(k-l)$ è coll. primo m p

$\Leftrightarrow a \cdot (k - l)$ " " "

$k \neq l \implies r \neq s$

per collisione tra k e l

$= \Pr_h(r = s \bmod m)$

$\Pr_h = \frac{1}{m}$ $\lceil \frac{p}{m} \rceil - 1$ dato s: $r = s \bmod m$

prof

$n = 2$ $n = 4$ $n = 2$

$s = 6, r = 16$ $s = 5, r = 11$ $s = 6, r = 16$

prob

$\lceil \frac{p}{m} \rceil \le \frac{p + m - 1}{m}$

$\lceil \frac{p}{m} \rceil - 1 \le \frac{(p + m - 1)}{m} - 1 = \frac{p - 1}{m}$

$\Pr_h(\text{collisione}) = \Pr(r = s \bmod m) = \frac{\frac{p-1}{m}}{p-1} = \frac{1}{m}$

aspettiamo

$m = \Theta(n)$

ristrutturiamo

$m \to m'$ $m' > m$

fatto

$\Theta(m + n) \Rightarrow \Theta(n)$

esercizi: 1. RISPONDI

1. $m = 1$

$\Theta(1 + 2 + 3 + 4 + \dots n) = \Theta(n^2)$

2. $2 \cdot m$

$\Theta(1 + 2 + 4 + 8 \dots n)$

$\sum_{i=0}^{k} 2^i = \frac{1 - 2^{k+1}}{1 - 2} = 2^{k+1} - 1$

$= 2n - 1$

$= \Theta(n)$

QUALCOSA. PROBLEM PARTE

Dato un insieme n, esistono n elementi primi. n nodi hanno per cardinalità sono assegnati diff numeri $\Rightarrow \Theta(1)$