

NS

$$|m^k - n!| \leq m$$

massimo di $\frac{m}{m}$

$$m=2, m=1, k=1 \quad \text{va bene} \quad \frac{m}{m} = 2$$

CLAIM: 2 è davvero il max!

x assumo l'ho (k, m, n) con $n > 2m$

$$h = |m^k - n!|, \quad h \leq m \Rightarrow h | m!$$

$$m^k = n! \pm h = h \left(\frac{n!}{h} \pm 1 \right)$$

$$m = 2m \left(\frac{n!}{h} \pm 1 \right) \quad \frac{m^2}{n!}$$

$$\frac{n!}{h} = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (h-1)(h+1) \cdot \dots \cdot m$$

$$m \mid \frac{n!}{h}$$

$$\left(m, \frac{n!}{h} \pm 1 \right) = 1$$

\Downarrow

$$\frac{n!}{h} \pm 1 = 1, -1$$

$$\frac{m!}{h} = 1, 2$$

Bisogna fare
i casi $m = 1, 2, 3$



N8

$$p(x) = x^3 + x$$

vogliamo sapere quando $p(x) \equiv p(y) \pmod{q}$

$$x^3 + x \equiv y^3 + y$$

$$(x-y)(x^2 + y^2 + xy + 1) \equiv 0 \pmod{q}$$

$$x^2 + xy + y^2 + 1 \equiv 0 \pmod{q} \quad (*)$$

se fissiamo y , le "soluzioni"

$$x_{1,2} \equiv \frac{-y \pm \sqrt{\Delta}}{2}$$

se $\exists a$ t.c. $\Delta \equiv a^2 \pmod{q}$ $\sqrt{\Delta} \equiv a \pmod{q}$

se Δ non è r.q. l'equazione non ha sol.

$$\left(\frac{m}{q}\right) = \begin{cases} 0 & \text{se } q|m \\ 1 & \text{se } m \text{ è r.q.} \\ -1 & \text{se } m \text{ non è r.q.} \end{cases}$$

le soluzioni di una quadratica mod q
sono $1 + \left(\frac{\Delta}{q}\right)$

$$\Delta \equiv y^2 - 4(y^2 + 1) \equiv -3y^2 - 4$$

Fatto noto 1 (criterio di Eulero)

$$\left(\frac{m}{q}\right) \equiv m^{\frac{q-1}{2}} \pmod{q}$$

"dim." $m^{q-1} \equiv 1 \pmod{q}$ $(m^{\frac{q-1}{2}} + 1)(m^{\frac{q-1}{2}} - 1) \equiv 0 \pmod{q}$
 $q^{q-1} - 1 \equiv 0$

Fatto noto 2

$$f(x) = a_{k-2} x^{k-2} + \dots + a_0 \quad (\text{dove } a_i \text{ può essere tutto mod } q)$$

$$\sum_{i=0}^{q-1} f(i) \equiv 0 \pmod{q}$$

$$\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right) \left(\frac{3}{q}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{q}{3}\right) (-1)^{\frac{q-1}{2} \cdot \frac{q-1}{2}}$$

Reciprocità quadratica

$$\left(\frac{q}{h}\right) = \left(\frac{h}{q}\right) (-1)^{\frac{h-1}{2} \frac{q-1}{2}}$$

$$\rightarrow \left(\frac{q}{3}\right) (-1)^{q-1} = \left(\frac{q}{3}\right) = 1$$

$$\Downarrow$$

$$q \equiv 1 \pmod{3}$$

Scegliendo $q \equiv 1 \pmod{3}$

$$\sum_{y=0}^{q-1} \left(\frac{\Delta}{q}\right) = -1$$

$$-3y^2 - 4 \equiv 0 \pmod{q} \quad -3 \equiv a^2 \pmod{q}$$

$$y^2 \equiv \frac{4}{a^2} \pmod{q} \quad y \equiv \pm \frac{2}{a} \pmod{q}$$

$\left(\frac{\Delta}{q}\right) = 0$ per esattamente 2 valori di y

$$a \cdot 1 + b \cdot (-1) = -1$$

$$a + b = q - 2$$

$$\Rightarrow b = \frac{q-1}{2} \quad a = \frac{q-3}{2}$$

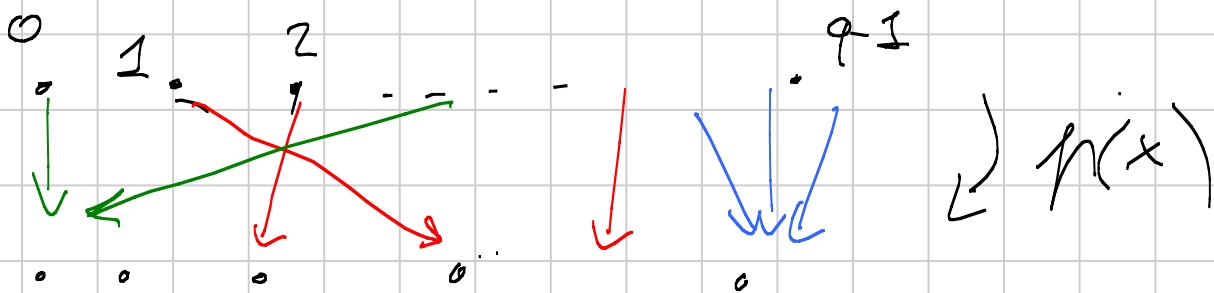
↑

per tutti gli y t.c. $\left(\frac{\Delta(y)}{q}\right) = -1$ $f(x) \equiv f(y) (q)$
 \updownarrow
 $x \equiv y (q)$

quindi f prende già $\frac{q-1}{2}$ valori DISTINTI

$y_0, q-y_0$ per cui $\left(\frac{\Delta(y_0)}{q}\right) = 0$

\downarrow ho altri 2 valori nell'immagine di f



— gli y t.c. $\left(\frac{\Delta(y)}{q}\right) = -1$

— $= 0$ (cioè ho 2
 precece in arrivo)

almeno

$\frac{q-1}{2} + 2$ valori DISTINTI raggiunti da f

Evitiamo la Rec. Quadratica

$q \equiv 1 \pmod{3} \Leftrightarrow x^3 - 1 \equiv 0 \pmod{q}$ ha 3 soluzioni.

$\Leftrightarrow x^2 + x + 1 \equiv 0 \pmod{q}$ ha 2 soluz. mod q

$\Leftrightarrow \Delta = -3$ è un quadrato modulo q

Contare le soluzioni di $x^2 + xy + y^2 \equiv -1 \pmod{q}$

Sia $q \equiv 1 \pmod{3}$. Allora $\exists \omega : \omega^2 + \omega + 1 \equiv 0 \pmod{q}$

$$x^2 + xy + y^2 \equiv (x - \omega y)(x - \omega^2 y) \equiv -1 \pmod{q}$$

$\nwarrow \quad \nearrow$
 $AB \equiv -1 \pmod{q}$

$$x = \frac{\omega A - B}{\omega - 1}$$

$$\left\{ \text{soluz. di } x^2 + xy + y^2 \equiv -1 \pmod{q} \right\} \xleftrightarrow{\sim} \left\{ \text{soluz. di } AB \equiv -1 \right\}$$

$q-1$

N 6 | SIA $C(n)$ LA SOMMA DELLE CIFRE
 DI n . SIA $a_1 = 1$, $a_{n+1} =$
 $= a_n + C(a_n)$. SI MOSTRI CHE ESISTONO
 INFINITI PRIMI p CHE DIVIDONO QUALCUNO
 a_n .

a_n CRESCE "LENTAMENTE"

I NUMERI CON DEI DIVISORI PRIMI FISSATI
 SONO "POCHI".

PER ASSURDO: I PRIMI CHE COMPAIONO
 TRA I DIVISORI DI a_1, a_2, \dots SONO
 $p_1, p_2, p_3, \dots, p_h$

COME DIRE CHE GLI a_n SONO
 TANTI.

QUANTI SONO GLI $a_n \leq 10^k$?

$$a_{n+1} - a_n = C(a_n)$$

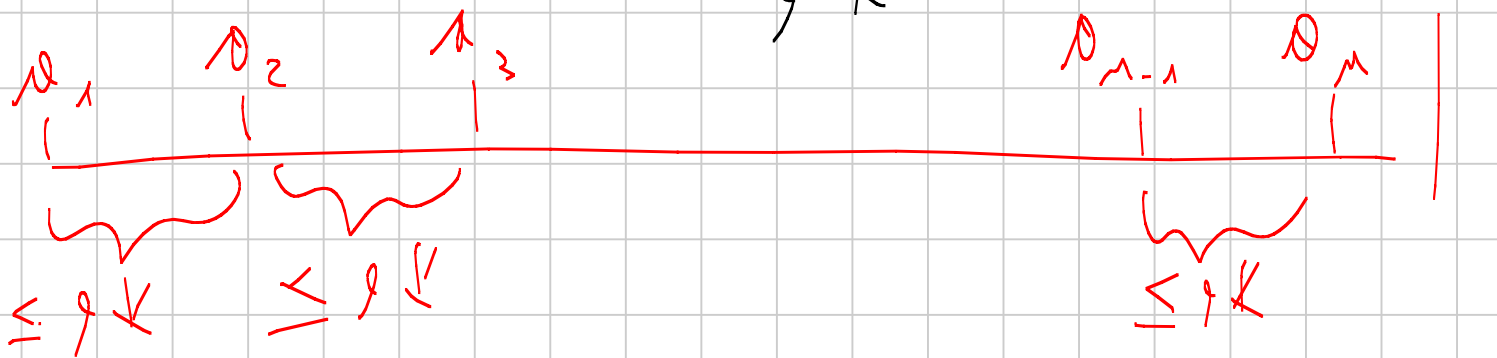
SE $a_n \leq 10^k \xrightarrow{?} C(a_n) = ?$

$$C(a_n) \leq 9 \cdot k$$

Il MAX di $c(x)$ con $x < 10^k$ è gk .

Visto CHE SE $a_n < 10^k$ ALLORA
 $0 < a_{n+1} - a_n < gk$

IL NUMERO DI a_n MINORI DI 10^k
SARÀ ALMENO $\frac{10^k}{gk}$



II STIMA (SUI p_1, \dots, p_h)

CI CHIEDIAMO QUANTI SIANO I NUMERI
DELLA FORMA $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_h^{\alpha_h} < 10^k$

STIMA PARZIALE
 $h=1$

QUANTI SONO I NUMERI DELLA FORMA
 $p_1^{\alpha_1}$ CON p_1 FISSATI MINORI,

$$10^k \mid p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \mid p_1^{\beta-1}$$

$$p_1^{\beta} < 10^k$$

$$\downarrow$$

$$2^{\beta} < 10^k$$

$$\updownarrow$$

$$16^{\beta/4} < 10^k$$

$$\downarrow$$

$$10^{\beta/4} < 10^k$$

$$\updownarrow$$

$$\beta < 4k$$

Sono AL PIÙ
 $4k$
 (oss.: c'è ANCHE
 LO ZERO MA
 $\beta < 4k$)
 DIRETTO

Quindi, numeri della forma $p_i^{\alpha_i}$
 con p_i fissato sono $\leq 4k$

I numeri della forma

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n} \quad \text{sono AL PIÙ}$$

$$(4k)^h$$

PERCHÉ OGNI NUMERO

DI QUESTA FORMA È PRODOTTO DI
 $p_i^{\alpha_i} < 10^k$

RIEPILOGANDO:

$$\# \{ a_n < 10^k \} \geq \frac{10^k}{g^k}$$

$$\# \{ p_1^{\alpha_1} \dots p_n^{\alpha_n} < 10^k \} \leq (4k)^h$$

SE GLI a_n FOSSERO TUTTI, DELLA FORMA
 $p_1^{\alpha_1} \dots p_n^{\alpha_n}$

$$\{ a_n < 10^k \} \subseteq \{ p_1^{\alpha_1} \dots p_n^{\alpha_n} < 10^k \}$$

$$(4k)^h \geq \frac{10^k}{g^k}$$



$$4^h \cdot g \cdot k^{h+1} \geq 10^k \quad \text{con } h \text{ FISSATO.}$$

PER k GRANDE LHS $\ll \ll$ RHS
molto

GLI ESPONENZIALI CRESCONO PIÙ VELOCEMENTE
DEI POLINOMI.

7.] SIA n UN INTERO POSITIVO E SIA
 $m > n^{n-1}$.

DIMOSTRARE CHE ESISTONO PRIMI DISTINTI
 p_1, p_2, \dots, p_h TALI CHE $p_k \mid m+k$
 $\forall 1 \leq k \leq h$.

FISSIAMO UN k :

$$m+k = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_h^{\alpha_h}$$

HOPE: UN QUALCUNO $p_i^{\alpha_i}$ È $\geq n$.

SUPPONIAMO IL CONTRARIO:

$$n < m+k = \prod_{i=1}^h p_i^{\alpha_i} \leq n^h$$

A NOI PIACEREBBE $h \leq n-1$

QUANTE POSSONO ESSERE LE POTENZE
DI PRIMO $\leq n-1$?

SICURAMENTE, AL PIÙ $n-1$.

QUINDI $h \leq n-1$ PERCHÉ

$p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_n^{\alpha_n}$ SONO PER

IPOTESI ASSURSA POTENZE DI PRIMO DISTINTE

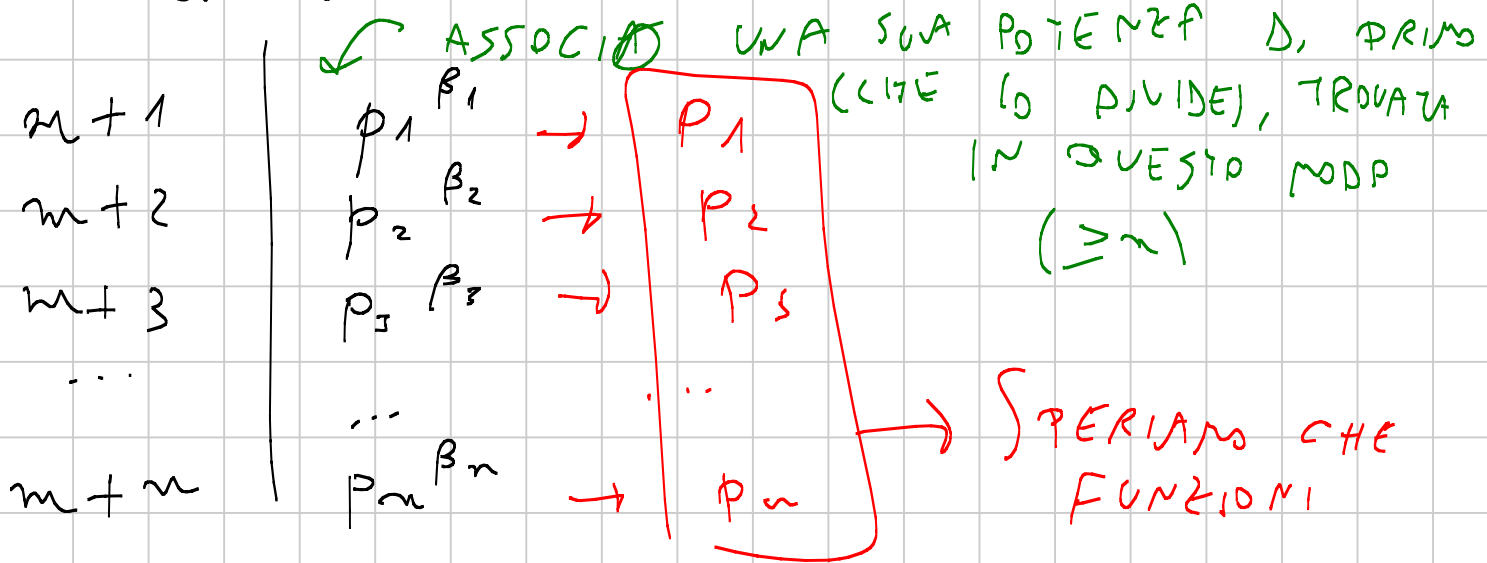
$$\leq n^{-1}$$

$$m^{n-1} < m + K \leq n^h \leq n^{n-1}$$

ASSURSO!

HOPE: ✓

ESISTE UNA POTENZA DI PRIMO $\geq n$ CHE
 DIVIDE $m + K$.



SICURAMENTE $p_k \mid m + k$.

MAFARI NON SONO DISTINTI.

SUPPONIAMO $p_i = p_j = p$ PER $1 \leq i \neq j \leq n$

$$p^{\beta_i} \mid m + i$$

$$p^{\beta_i} \geq n$$

$$p^{\beta_j} \mid m + j$$

$$p^{\beta_j} \geq n$$

SIA $\beta = \min \{ \beta_i, \beta_j \}$

$$\rightarrow p^\beta \mid m+i \quad p^\beta \mid m+j$$

$$p^\beta \geq n$$

$$\rightarrow p^\beta \mid j-i$$

$$\exists \epsilon \quad j \neq i, \quad |j-i| \leq n-1$$

MA ALLORA $p^\beta \mid j-i \rightarrow$

$$p^\beta \leq n-1 \quad \text{ASSURDO.}$$

66

DIAMO UNA STIMA ESPlicita DI

D_n .

$$D_n \leq \cancel{1000} + 50 \cdot n \cdot \log_{10} n$$

COME DIMOSTRARLO?

INDUZIONE

— D_1 ✓

— INDUTTIVO $D_n \leq \cancel{1000} + 50 n \log_{10} n$

Lo miriamo con n

QUANTITÀ DA AGGIUNGERE $\leq 50 \log_{10}(n)$

VORREMO $a_{n+1} \leq \cancel{1000} + 50 (n+1) \log_{10} (n+1)$

SU $C(n)$ SAPPIAMO: $\log_{10} (10 \cdot n) \geq$
CIFRE DI n

$$C(n) \leq 9 \cdot \log_{10} (10 \cdot n)$$

$$a_{n+1} = a_n + C(a_n) \leq a_n + 9 \cdot \log_{10} (10 \cdot a_n) \leq$$

$$\leq \cancel{1000} + 50 n \log_{10} n + 9$$

$$\log_{10} \left(\cancel{10000} + 500 n \log_{10} n \right)$$

\sim

$$50 \cdot \log_{10} n$$

$$\left(\cancel{10000} + 500 n \log_{10} n \right)^9 \leq n^{50}$$

TATE A CASA LE
5 TIME

COMUNQUE:

$$a_n \leq c + d \cdot n \cdot \log_{10} n$$

FATTO POTENTE:

SE HO UN INSIEME $0 < a_1 < a_2 < a_3 < \dots$

DI INTERI POSITIVI TALE CHE

$$\sum_{i=1}^{+\infty} \frac{1}{a_i} \rightarrow +\infty \quad \text{ALLORA I DIVISORI}$$

PRIMI AL VARIARE DEGLI a_n SONO
INFINITI.

SUPPONIAMO CHE I PRIMI p_1, \dots, p_h
SIANO FINITI.

FORMA: $p_1^{a_1} \cdot \dots \cdot p_h^{a_h}$

$$\sum_{a_1, a_2, \dots, a_h=0}^{+\infty} \left(p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_h^{a_h} \right) =$$

$(\text{OGNI } a_i \text{ TRA } 0 \text{ E } +\infty)$

$$= \left(\sum_{i=0}^{+\infty} \frac{1}{p_1^i} \right) \cdot \left(\sum_{i=0}^{+\infty} \frac{1}{p_2^i} \right) \cdot \dots \cdot \left(\sum_{i=0}^{+\infty} \frac{1}{p_h^i} \right)$$

OGNI $p_1^{A_1} \dots p_n^{A_n}$ può essere scritto in un E CM solo modo

$$1 + x + x^2 + \dots = \frac{1}{1-x} \quad \text{PER } 0 < x < 1$$

$$= \left(\frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdot \dots \cdot \frac{1}{1 - \frac{1}{p_n}} \right) < +\infty$$

È un numero finito

Ci basta $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$

$$\sum_{n=1}^{+\infty} \frac{1}{p_n} \geq \sum_{n=1}^{+\infty} \frac{1}{(d \cdot n \log_{10} n)} \geq$$

$$\frac{1}{d} \sum_{n=1}^{+\infty} \frac{1}{n \log_{10} n}$$

CONDENSAZIONE DI CAUCHY

VERSIONE AD HOC:

$$\sum_{n=1}^{+\infty} a_n = +\infty \iff \sum_{n=1}^{+\infty} 10^n \cdot a_{(10^n)} = +\infty$$

a_n DEVE ESSERE DECRESCENTE E POSITIVA

$$\frac{1}{d} \cdot \sum_{n=1}^{+\infty} \frac{10^n}{10^n \cdot \log_{10}(10^n)} \stackrel{?}{=} +\infty$$

$$\frac{1}{d} \sum_{n=1}^{+\infty} \frac{1}{n} = +\infty$$

↓ (CAUCHY DIVISOR)

$$\frac{1}{d} \sum_{n=1}^{+\infty} \frac{10^n}{10^n} (1) = +\infty$$