TdN 3

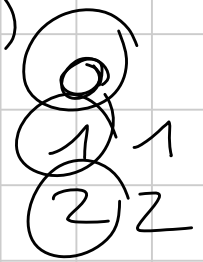
Titolo nota 05/09/2007

n $f(n)$

Tra $f(n)$ interi per forza ce ne sono n la cui somma è divisibile per n

$n=2 \to f(n)=2n-1$ 0 0 $\quad 0+0 \equiv 0 \pmod 2$

$n=3$ 0 0 1 1 $\quad a \equiv b \equiv c \pmod 3$



n $\underbrace{0,\dots 0}_{n-1}$ $\underbrace{1,\dots,1}_{n-1}$ $= 2n-2$

$f(n) \geq 2n-1$

$n=6 \quad f(6)=11>3$ $\quad 2 \mid x_1+x_2=y_1 \quad 2 \mid x_3+x_4=y_2 \quad 2 \mid x_5+x_6=y_3$

$2 \mid x_7+x_8=y_4 \quad 2 \mid x_9+x_{10}=y_5$

$3 \mid y_a+y_b+y_c \qquad 6 \mid y_a+y_b+y_c$

$f(mn) = 2mn - 1$

ce ne sono m tali che $m \mid x_1 + x_2 + \dots + x_m = y_1$

restano $2mn - 1 - m = (2n-1)m - 1 > 2m-1$

$m \mid x_{m+1} + x_{m+2} + \dots + x_{2m} = y_2$

$\vdots$

$m \mid x_{(2n-2)m+1} + \dots + x_{(2n-1)m} = y_{2n-1}$

$m \mid \sum_m y_i \qquad m \mid y_i \quad \text{lcm}(mn) \mid \Sigma y_i$

$m \mid y_i \qquad \frac{y_i}{m} = \text{intero} \qquad \frac{y_1}{m}, \frac{y_2}{m}, \dots \frac{y_{2n-1}}{m}$

$n \mid \sum_n \frac{y_i}{m} \Rightarrow mn \mid \sum_n y_i = \sum_{mn} x_i$

$f(p) \stackrel{?}{=} 2p-1$

Lemma + forte: dati $x_1, x_2, \dots x_{2k-1}$ interi (di cui non ce ne sono $k+1$ congrui mod p) $\Rightarrow$

facendo le somme di k di questi x_i allora queste somme mi coprono almeno k classi di congruenza

Per $k=1$ OVVIO ☺

Per $k=2$ x_1, x_2, x_3 non sono tutti congrui modp

WLOG $x_1 \not\equiv x_2 \Rightarrow x_1 + x_3 \not\equiv x_2 + x_3$

Suppongo vera la tesi per k

Ho $2k+1$ x_i: $x_1, x_2, \dots x_{2k+1}$ non ce ne sono $k+2$ congrui. Ci sono $k+1$ somme?

$x_1, \dots x_{2k-1}$

Al massimo una classe di congruenza che contiene $k+1$ elementi. WLOG ($x_{2k+1} \in$ questa classe, $x_{2k} \in$ un'altra classe)

$x_1, \dots x_{2k-1}$

$S_1, S_2, \dots S_k$

$A = \{S_1 + x_{2k}, S_2 + x_{2k}, S_3 + x_{2k} \dots S_k + x_{2k}\}$

$B = \{S_1 + x_{2k+1}, \dots, S_k + x_{2k+1}\}$

$$\sum S_i + x_{2k} = \sum S_i + k x_{2k}$$

$$\sum S_i + x_{2k+1} = \sum S_i + k\, x_{2k+1}$$

$$\cancel{\sum S_i} + \cancel{k} x_{2k} \equiv \cancel{\sum S_i} + \cancel{k} x_{2k+1} \quad (p)$$

$$x_{2k} \equiv x_{2k+1}$$

$x_1, \dots x_{2p-1}$

$$\left(x_{i_1} + x_{i_2} + x_{i_3} + \dots + x_{i_p}\right)^{p-1} \equiv 1$$

$$\sum \left(x_{i_1} + x_{i_2} + \dots + x_{i_p}\right)^{p-1} \equiv \sum 1 \equiv$$

$i_1, i_2, \dots i_p$ tra $2p-1$ valori? $\{1, 2, \dots 2p-1\}$

$$\equiv \binom{2p-1}{p} \not\equiv 0 \ (p)$$

$$\binom{2p-1}{p} = \frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)!} \not\equiv 0 \ (p)$$

$$\sum \left(x_{i_1} + x_{i_2} + \dots + x_{i_p}\right)^{p-1} \not\equiv 0 \quad (p)$$

$$x_{j_1}^{k_1} \cdot x_{j_2}^{k_2} \cdots x_{j_m}^{k_m} \qquad \sum k_i = p-1 \qquad m < p$$

$$\left(x_{i_1} + x_{i_2} + \dots + x_{i_p}\right)^{p-1} \qquad \{j_1, j_2, \dots j_m\} \subset \{i_1, i_2, \dots i_p\}$$

$$\binom{2p-1-m}{p-m} \cdot C_{j_1, \dots j_m}$$

~~$2p-1-m-p+1$~~

$$p \mid \binom{2p-1-m}{p-m} = \binom{2p-1-m}{p-1} = \frac{(2p-1-m)\cdots(p-m)}{(p-1)!}$$

$2p-1-m > p \qquad p-m < m$

VIETA JUMPING

a,b interi non negativi

$$\frac{a^2+b}{1+ab} = k \Rightarrow k \text{ è un quadrato perfetto.}$$

$(a,b) \Rightarrow (a',b')$ $\quad a+b > a'+b'$

$a \geq b$

$$k = \frac{a^2+b^2}{1+ab}$$

$$k = \frac{x^2+b^2}{1+xb} \Rightarrow x^2 - kbx + (b^2-k) = 0$$

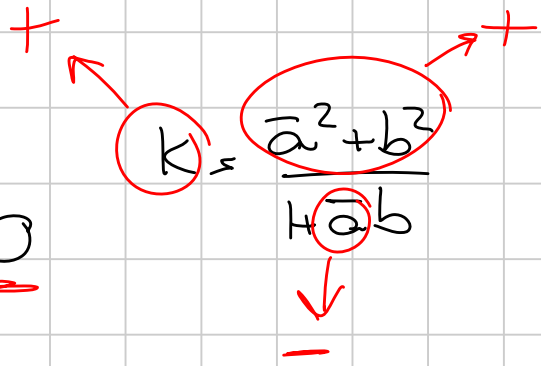
a è una soluzione

$a + \bar{a} = kb \Rightarrow \bar{a}$ è intero

$(\bar{a}, b)$ $\quad \bar{a} < a$

$$x_{1,2} = \frac{kb \pm \sqrt{k^2b^2 - 4b^2 + 4k}}{2}$$

$\bar{a} > 0$



$\bar{a} < a$ $\quad a\bar{a} = b^2 - k < b^2 \leq a^2$

$a\bar{a} < a^2$

k non quadrato perfetto $\qquad k = \frac{a^2+b^2}{1+ab}$

$a+b$ = minimo $\qquad (a,b) \qquad k = \frac{a^2}{1} = a^2$

IMO 2007/5

$k = 4ab-1 \mid (4a^2-1)^2$. Th: non ha soluzioni con $a \neq b$

mod k $\quad 4ab \equiv 1$

$$(4a^2-1)^2 \equiv (4a^2-4ab)^2 \quad (k)$$

$$\equiv (4a)^2[a-b]^2 \quad (k) \qquad (4a, 4ab-1) = 1$$

$$\equiv 0$$

$$(a-b)^2 \equiv 0 \quad (k)$$

1 pt.

$$4ab-1 \mid (a-b)^2$$

$$\frac{a^2-2ab+b^2}{4ab-1} = k \qquad (a,b) = \text{minima}$$

$a > b$

$$x^2 - 2xb - 4kbx + b^2 + k = 0$$

$$x^2 - (2b + 4kb)x + b^2 + k = 0$$

$$x_{1,2} = b + 2kb \pm \sqrt{(b+2kb)^2 - b^2 - k} = \begin{cases} a \\ \bar{a} \end{cases}$$

$\bar{a} > 0$ $\quad$ $\bar{a}$ è intero $\quad$ $\bar{a} < b \leq a$

$\bar{a} < b$ $\quad$ $b + 2kb - \sqrt{(b+2kb)^2 - b^2 - k} < b$

$$4k^2b^2 < b^2 + 4kb^2 + 4k^2b^2 - b^2 - k$$

$$k < 4kb^2$$

Per quali n n si può scrivere nella forma

$$n = \frac{a^2+b^2+c^2+d^2}{1+abcd}$$ (a,b,c,d sono positivi)

$n=1 = \frac{3^2+3^2+3^2+1}{1+3\cdot3\cdot3}$ $\quad n=2 = \frac{1+1+1+1}{1+1}$ $\quad n=3 = \frac{3^2+1+1}{1+3}$

$n = b^2+c^2+d^2 \qquad a = nbcd = (b^2+c^2+d^2)bcd$

$$n = \frac{a^2+n}{1+\frac{a^2}{n}}$$

tutti gli n della forma $b^2+c^2+d^2$ si possono fare. (con b,c,d positivi).

Supp n non sia nella forma $b^2+c^2+d^2$ (non sia scrivibile come somma di 3 quadrati.

$$n = \frac{a^2+b^2+c^2+d^2}{1+abcd}$$

(a,b,c,d) che mi da uguaglianza, con $a \geq b \geq c \geq d$.

$x^2 - \mu abcd\, x + b^2+c^2+d^2-\mu = 0$

Ha soluzioni $a, \bar{a}$

$\bar{a}$ = intero. $\bar{a} \geq 0$

se $\bar{a}=0$ $\quad b^2+c^2+d^2-\mu=0 \Rightarrow \mu = b^2+c^2+d^2$

$\bar{a}$ è positivo

se $a\bar{a} = b^2+c^2+d^2-\mu < b^2+c^2+d^2-1 \leq a^2$

$a\bar{a} < a^2 \Rightarrow \bar{a} < a$

Devo andare sotto $\quad \boxed{b^2+c^2+d^2-1 > a^2}$

$$\mu = \frac{\bar{a}^2+b^2+c^2+d^2}{+\bar{a}bcd} \qquad \mu = \frac{a^2+b^2+c^2+d^2}{+abcd}$$

$+$ sopra, $+$ sopra, $-$ sotto

b, c, d non sono molto più piccoli di a $\quad a \geq b \geq c \geq d$

$$\mu < 4 \qquad \mu = \frac{a^2+b^2+c^2+d^2}{+abcd} \leq \frac{4a^2}{+abcd} <$$

~~$abcd > a^2$~~ $\quad \boxed{bcd > a}$

$K>0$

$b^2+c^2+d^2-1 = a^2+K \Rightarrow b^2+c^2+d^2 = a^2+K \quad K \geq 2$

$bcd > a$ $\quad bcd \geq \sqrt{b^2+c^2+d^2-2} \geq \sqrt{b^2+c^2+d^2-b} \geq a$

$b^2c^2d^2 \geq b^2+c^2+d^2-2$ $\qquad b \geq c \geq d$

$b^2(c^2d^2-1) \geq c^2+d^2-2$

$c^2d^2-1 > 0$ $\quad$ almeno una tra c e d è $> 1 \Rightarrow c^2d^2 \geq 4$

$=0 \iff c=d=1$ la disuguaglianza vale

$c^2d^2-1 \geq 3$

$b^2(c^2d^2-1) \geq 3b^2 > c^2+d^2-2$

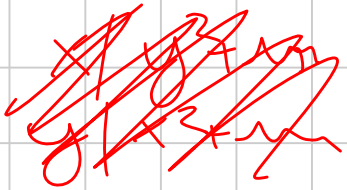
$$M < \frac{4a^2}{1+abcd} < \frac{4a^2}{1+a^2} < 4$$

ESERCIZI

$$\frac{x^2+y^2+z^2}{xyz} = k \Rightarrow \quad k=1 \quad \sqrt{3}$$

$xy \mid x^2+y^2+m$

Fissato m esistono infinite coppie (x,y) che soddisfano



STIME

Es: dimostrare che, fissato un m, esistono m interi consecutivi che non si possono scrivere nella forma

$$a^3+b^5+c^7+d^{11}+e^{13} \qquad (a,b,c,d,e>0)$$

Fissiamo N. Quanti sono i numeri così $\leq N$?

$$a^3+b^5+c^7+\dots \leq N \Rightarrow \begin{cases} a^3 \leq N \Rightarrow \{1,\dots \lfloor N^{\frac{1}{3}} \rfloor\} \\ b^5 \leq N \Rightarrow \{1,\dots \lfloor N^{\frac{1}{5}} \rfloor\} \\ c^7 \leq N \\ d^{11} \leq N \\ e^{13} \leq N \end{cases}$$

$$a^3 + b^5 + c^7 + d^{11} + e^{13}$$

a: $N^{\frac{1}{3}}$ (massimo) possibili valori assunti; b: $N^{\frac{1}{5}}$; c: $N^{\frac{1}{7}}$; d: $N^{\frac{1}{11}}$; e: $N^{\frac{1}{13}}$

$N^{\frac{1}{3}} \cdot N^{\frac{1}{5}} \cdot N^{\frac{1}{7}} \cdot N^{\frac{1}{11}} \cdot N^{\frac{1}{13}} = N^{\Sigma} = N^{K}$ $\qquad \frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13} = K$

$K < 1$

se ci fossero al più $\frac{N}{m}$ tra i primi N

$\{1, \dots m\}$ $\{m+1, \dots 2m\}$ $\dots$ $\{\quad\quad N\}$

1 1 1

$\frac{N}{m}$ $\qquad a^3+b^5+c^7+d^{11}+e^{13}$

$N^K < \frac{N}{m}$ $\qquad m < N^{1-K}$ $\quad 1-K > 0$

$p(n)$ = coefficienti interi

A = l'insieme dei primi p che dividono $p(n)$ per almeno un valore di n intero.

A è infinito

Supponiamo per assurdo che $A = \{p_1, p_2, \dots, p_k\}$

N grande

Quanti sono i valori del polinomio $< N$?

Vorremmo dimostrare che sono più dei numeri della forma $p_1^{\alpha_1} \cdots p_k^{\alpha_k} = Q$ con $Q < N$

Vogliamo fare: ① stima per difetto dei valori assunti dal polinomio e $< N$

② stima per eccesso dei valori assunti da $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e $< N$

② < ①

① $p(m)$ ha grado d

$x^{d-1} < p(x)$ definitivamente $M < x$

$p(x) < x^{d+1} < N$

$0 \dots N^{\frac{1}{d+1}}$ valori di x possibili

$N^{\frac{1}{d+1}}$ è il massimo

$x^{d-1} < p(x) < N \Rightarrow$ il numero massimo di valori possibili per x è $N^{\frac{1}{d-1}}$

$N^{\frac{1}{d-1}}$

$\frac{N^{\frac{1}{d-1}} - M}{d} = (1)$

$N^{\frac{1}{k}}$

(2') valori assunti da $p_1^{\alpha_1} \cdots p_k^{\alpha_k} < N$

$N > p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 2^{\sum \alpha_i}$

$\sum \alpha_i < \log_2 N$

$\alpha_i < \log_2 N$

$(\log_2 N)(\log_2 N) \cdots (\log_2 N) = (\log_2 N)^k$

$(\log_2 N)^k < N^{\frac{1}{k}}$

$\log_2 N < N^{\frac{1}{k^2}}$

(1) i valori assunti dal polinomio V sono più di un certo numero e minori di N

$$p(x) < x^{d+1} < N$$

$$x < N^{\frac{1}{d+1}}$$

$p(x)$ $\quad \frac{N^{\frac{1}{d+1}} = M}{d}$

UBERBEWEIS !!!

DIMOSTRAZIONE DELL'ESISTENZA DI UN GENERATORE

LEMMA: mod p

$\operatorname{ord}(a) = \ell \qquad \operatorname{ord}(b) = k \qquad (\ell, k) = 1 \Rightarrow$

$\operatorname{ord}(ab) = \ell k$

DIM $\operatorname{ord}(ab) \mid \ell k$: $\quad (ab)^{\ell k} \equiv a^{\ell k} \cdot b^{\ell k} \equiv 1 \cdot 1 \equiv 1 \quad (p)$

$\operatorname{ord}(ab) = x = \ell_1 k_1 \qquad \ell_1 \mid \ell, \; k_1 \mid k \qquad \ell_1 \neq \ell$

$$\left[(ab)^{\ell_1 k_1}\right]^{\frac{k}{k_1}} \equiv 1 \equiv (ab)^{\ell_1 k} \equiv a^{\ell_1 k} b^{\ell_1 k} \equiv a^{\ell_1 k}$$

$\operatorname{ord}(a) \mid \ell_1 k \Rightarrow \ell \mid \ell_1 k \Rightarrow \ell \mid \ell_1$ ASSURDO

$\exists g$ tale che $\operatorname{ord}(g) = p-1$?

$p-1 = q_1^{a_1} \cdots q_m^{a_m}$

$\operatorname{ord} x_1 = q_1^{a_1} \qquad \operatorname{ord} x_2 = q_2^{a_2} \cdots \qquad \operatorname{ord} \prod x_i = p-1$

Devo dimostrare che se $q^a \| p-1$ allora esiste un elemento di ordine q^a

$$x^{q^a} \equiv 1 \quad (p) \qquad x^{q^{a-1}} \not\equiv 1 \quad (p)$$

quanti sono gli x che risolvono questa congruenza? q^a

Speriamo che siano q^a

$$x^{q^{a-1}} \equiv 1 \quad (p)$$

q^{a-1}

$$q^a - q^{a-1} > 0$$

Voglio dimostrare che $x^{q^a} - 1 \equiv 0 \ (p)$ ha esattamente q^a soluzioni e che $x^{q^{a-1}} - 1 \equiv 0 \ (p)$ ha esattamente q^{a-1} soluzioni.

In generale $x^d - 1 \equiv 0 \ (p)$ (con $d \mid p-1$) ha esattamente d soluzioni.

$x^{p-1} - 1 \equiv 0 \ (p) \Longrightarrow$ esattamente $p-1$ soluzioni

$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + \dots + 1) = (x^d - 1) \cdot f(x)$

$x^d - 1$ ha al massimo d soluzioni. $f(x)$ ha grado $p-1-d$

$f(x)$ ha al massimo $p-1-d$ soluzioni.

$x^{p-1} - 1 = (x^d - 1)\, f(x)$

ha $p-1$ soluzioni — d max — $p-1-d$

FINE

Abbiamo un bel g = generatore mod p

Th: g è un gen mod p^2 oppure
$g+p$ è un generatore mod p^2.

$g^{p-1} \equiv 1 \ (p) \Longrightarrow \operatorname{ord}_p(g) = p-1$

$g^{\operatorname{ord}_{p^2}(g)} \equiv 1 \ (p^2) \Longrightarrow g^{\operatorname{ord}_{p^2}(g)} \equiv 1 \ (p)$

$p-1 \mid \operatorname{ord}_{p^2}(g) \mid p(p-1)$

$ord_{p^2}(g) = \begin{cases} p-1 \to \\ p(p-1) \to \text{generatore} \end{cases}$

$ord_{p^2}(g) = p-1$

$g+p \qquad (g+p)^{ord_{p^2}(g+p)} \equiv 1 \quad (p^2) \Rightarrow$

$g^{ord_{p^2}(g+p)} \equiv (g+p)^{ord_{p^2}(g+p)} \equiv 1 \quad (p) \Rightarrow p-1 \mid ord_{p^2}(g+p)$;

$ord_{p^2}(g+p) = \begin{cases} \overline{\overline{p-1}} \\ p(p-1) \Rightarrow \text{generatore} \end{cases}$ $\quad | \; p^2-p$

$(g+p)^{p-1} \equiv 1 \quad (p^2)$

$(g+p)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} p g^{p-2} + \binom{p-2}{2} p^2 g^{p-3} + \dots \equiv \quad (p^2)$

$\equiv g^{p-1} + (p-1) p g^{p-2} \equiv g^{p-1} - p g^{p-2} \equiv 1 - p g^{p-2} \not\equiv 1 \; (p^2)$

g è un generatore mod p^α

$g^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$ $\qquad ord_{p^\alpha}(g) = (p-1)p^{\alpha-1}$

Qual è l'ordine di g mod $p^{\alpha+1}$?

$g^{ord_{p^{\alpha+1}}(g)} \equiv 1 \pmod{p^{\alpha+1}} \Rightarrow g^{ord_{p^{\alpha+1}}(g)} \equiv 1 \pmod{p^\alpha}$

$ord_{p^\alpha}(g) \mid ord_{p^{\alpha+1}}(g) = k$

$ord_{p^{\alpha+1}}(g) = \begin{cases} (p-1)p^{\alpha-1} \\ (p-1)p^\alpha = \phi(p^{\alpha+1}) \end{cases}$

$g^k \equiv 1 \pmod{p^\alpha}$

$ord_{p^\alpha}(g) \mid k$

$(p-1)p^{\alpha-1} \mid k$

$k \mid \phi(p^{\alpha+1}) = (p-1)p^\alpha$

$ord_{p^{\alpha+1}}(g) = (p-1)p^{\alpha-1}$

$g^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^{\alpha-1}}$

$g^{p^{\alpha-2}(p-1)} = 1 + kp^{\alpha-1}$; con $(k,p) = 1$ $\quad p \nmid k$

$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$

$g^{(p-1)p^{\alpha-1}} \overset{??}{\not\equiv} 1 \quad (p^{\alpha+1})$

$g^{(p-1)p^{\alpha-1}} \equiv \left[g^{(p-1)p^{\alpha-2}}\right]^p \equiv \left(1+kp^{\alpha-1}\right)^p \equiv 1 + p\cdot k p^{\alpha-1} + \binom{p}{2} p^{2\alpha-2} + \dots$

$\equiv 1 + kp^{\alpha} \not\equiv 1 \quad (p^{\alpha+1})$

$\phi(\phi(p))$

$g^k \qquad (k, \phi p) = 1$

il num di generatori è $\phi(\phi(p^\alpha))$

$p^{\alpha-1}(p-1)$

$\phi(p-1)$ = numero di generatori mod p

$\phi(\phi(p^\alpha)) = \phi(p\cdot(p-1)) = (p-1)\,\phi(p-1)$

$$\varphi(\varphi p^\alpha) = \varphi\left(p^{\alpha-1}(p-1)\right) = p^{\alpha-2}(p-1)\,\varphi(p-1)$$

$$\varphi(\varphi p^{\alpha+1}) = \varphi\left(p^{\alpha}(p-1)\right) = p^{\alpha-1}(p-1)\,\varphi(p-1)$$

$\{1, 2, \dots 3n\}$. Li partizioniamo in 3 insiemi A, B, C tali che $|A| = |B| = |C| = n$

$n = 3$

A	B	C
1	2	5
7	3	6
9	4	8

$\exists\ (a, b, c)$ $a \in A,\ b \in B,\ c \in C$ tale che uno tra a, b, c è somma degli altri 2.

WLOG $1 \in A$ $\quad K \in B$

A: $1, 2, \dots K-1$

B: K

C: ... x ...

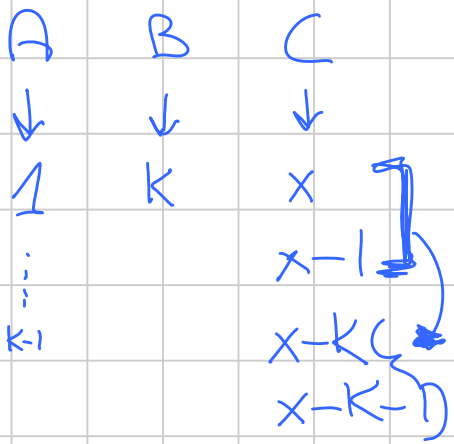
Dove sta $x-1$? $x-1$ non può stare in B $(1, x-1, x)$

Claim: se $x \in C \Rightarrow x-1 \in A$

Supponiamo falso

$x-1 \in C$

$x-K$



① $x-K \in A$. NO $(x-K, K, x)$

② $x-K \in B$ NO $(K-1, x-K, x-1)$

③ $x-K \in C$

$x-K-1$

① $\in A$ NO $(x-K-1, K, x-1)$

② $\in B$ NO $(1, x-K-1, x-K)$

③ $\in C$

$(x, x-1) \in C \Rightarrow (x-k, x-k-1) \in C \Rightarrow (x-k-k, x-k-k-1)$

$\Longrightarrow (x-ik, x-ik-1)$

$x-ik, \; x-ik-1 \in \{1, \dots, k\}$

FINE

$n=1$ 1 3 2

$3 = 2+1$