

XXXVII Olimpiade Italiana di Matematica

Sedi distrettuali, 6 maggio 2021

1. Un intero positivo m si dice *portatore di zeri* se esiste un intero positivo k tale che
 - k è un quadrato perfetto,
 - k è multiplo di m ,
 - l'espressione decimale di k contiene almeno 2021 cifre 0, ma l'ultima cifra (quella più a destra) è diversa da 0.

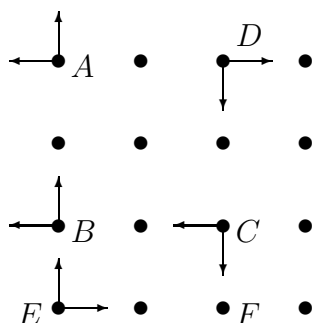
Determinare tutti gli interi portatori di zeri.

2. Sia ABC un triangolo e sia I il centro della sua circonferenza inscritta. Sia D il simmetrico di I rispetto al lato AB , e sia E il simmetrico di I rispetto al lato AC .

Dimostrare che le circonferenze circoscritte ai triangoli BID e CIE sono tra di loro tangenti.

3. Una griglia è costituita da $n \times n$ punti, con n intero positivo. In alcuni di questi punti è disposta una sentinella. Ogni sentinella sceglie due direzioni tra di loro perpendicolari (tra quelle delle righe e delle colonne della griglia) e sorveglia tutti i punti che si trovano nelle direzioni prescelte. Ogni sentinella sorveglia anche la casella che occupa, e le sentinelle che si trovano al bordo possono anche ritrovarsi a guardare verso il vuoto, a seconda delle direzioni scelte.

Ad esempio, nella figura sottostante, relativa ad una disposizione di 5 sentinelle in una griglia 4×4 , le sentinelle in A, B, C, D, E sorvegliano, rispettivamente, 1, 3, 4, 5, 7 punti; i punti D ed E sono sorvegliati da una sola sentinella, il punto C è sorvegliato da 2 sentinelle, i punti A, B ed F sono sorvegliati da 3 sentinelle.



- (a) Dimostrare che possiamo posizionare 12 sentinelle in una griglia 4×4 in modo che ogni punto della griglia sia sorvegliato da al più 2 sentinelle.
- (b) Sia $S(n)$ il massimo numero di sentinelle che possiamo disporre in una griglia $n \times n$ in modo tale che ogni punto della griglia sia sorvegliato da al più 2 sentinelle. Dimostrare che $3n \leq S(n) \leq 4n$ per ogni $n \geq 3$.

4. Date due frazioni a/b e c/d , definiamo la loro *somma pirata* come

$$\frac{a}{b} \diamond \frac{c}{d} = \frac{a+c}{b+d},$$

dove si intende che le due frazioni iniziali sono ridotte ai minimi termini (cioè semplificate il più possibile), ed anche il risultato viene poi ridotto ai minimi termini. Così, per esempio, la somma pirata di $2/7$ e $4/5$ è uguale a $1/2$.

Dato un intero $n \geq 3$, inizialmente sulla lavagna sono scritte le frazioni

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}.$$

Ad ogni mossa scegliamo due frazioni scritte sulla lavagna, le cancelliamo, e scriviamo al loro posto la loro somma pirata. Continuiamo allo stesso modo fino a quando sulla lavagna resta una sola frazione.

Determinare, in funzione di n , il massimo ed il minimo valore possibile per quest'ultima frazione.

5. Sia ABC un triangolo acutangolo, sia M il punto medio di BC , e sia H il piede dell'altezza uscente da B . Indichiamo con Q il centro della circonferenza circoscritta al triangolo ABM , e con X l'intersezione tra l'altezza BH e l'asse di BC .

Dimostrare che i seguenti due fatti sono equivalenti:

- (i) la circonferenza circoscritta al triangolo ACM , la circonferenza circoscritta al triangolo AXH , e la retta CQ passano per uno stesso punto;
- (ii) le rette BQ e CQ sono perpendicolari.

6. Una successione $x_1, x_2, \dots, x_n, \dots$ è costituita da un blocco iniziale di p interi positivi *distinti*, che poi si ripetono periodicamente. Questo vuol dire che $\{x_1, x_2, \dots, x_p\}$ sono p interi positivi distinti, e $x_{n+p} = x_n$ per ogni intero positivo n .

I termini della successione non sono noti, e l'obiettivo è individuare il periodo p . Per far questo, ad ogni passaggio è possibile rivelare il valore di un termine della successione a propria scelta (e la scelta può dipendere dall'esito dei passaggi precedenti).

- (a) Sapendo a priori che $1 \leq p \leq 10$, determinare il minimo n per cui esiste una strategia che permette di individuare con certezza p rivelando al più n termini.
- (b) Sapendo a priori che p è uno dei primi k numeri primi, determinare per quali valori di k esiste una strategia che permette di individuare con certezza p rivelando al più 5 termini.

Problema 1 – Soluzione. Un intero positivo m è portatore di zeri se e solo se m non è divisibile per 10.

Condizione necessaria Se m è multiplo di 10, allora m non può essere portatore di zeri, in quanto ogni multiplo di m^2 terminerà necessariamente con almeno due cifre 0.

Condizione sufficiente Dimostriamo che, se m non è multiplo di 10, allora è portatore di zeri. A tal fine consideriamo, per ogni intero positivo a , il numero

$$k = (10^a + 1)^2 m^2 = 10^{2a} m^2 + 2 \cdot 10^a m^2 + m^2 = 10^a \cdot m^2 (10^a + 2) + m^2.$$

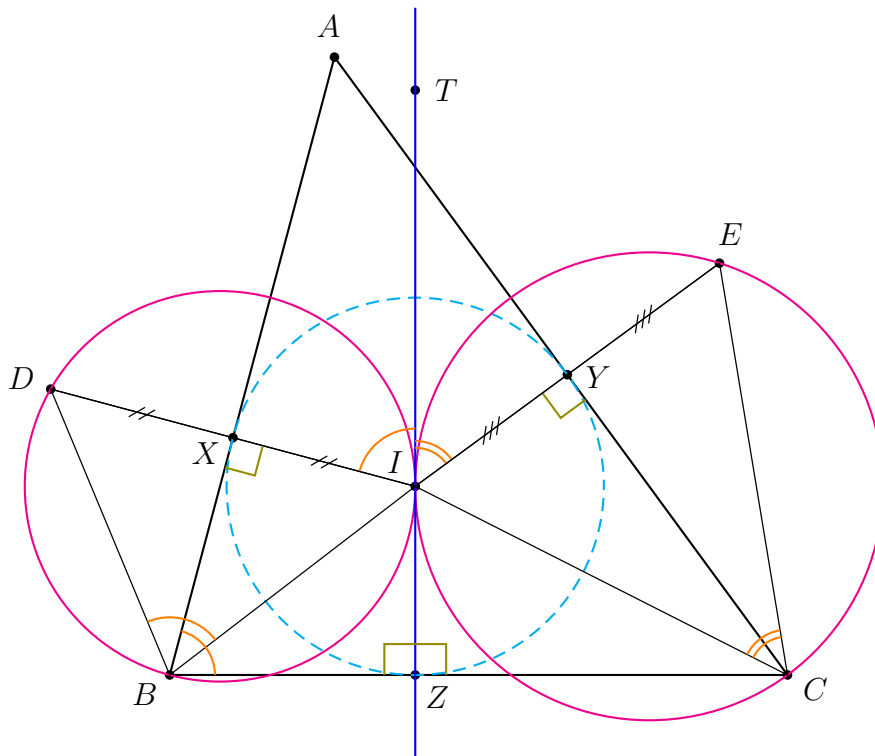
Scritto in questo modo, il primo addendo è multiplo di 10^a , dunque la sua espressione decimale termina con a cifre 0. Se indichiamo con M il numero di cifre di m^2 , e poniamo $a = 2021 + M$, allora siamo sicuri che l'espressione decimale di k terminerà con le M cifre di m^2 , precedute da 2021 cifre 0. Inoltre la cifra delle unità di k sarà diversa da 0, come richiesto.

Problema 2 – Soluzione. Siano X, Y, Z i punti di tangenza della circonferenza inscritta con i lati AB, AC, BC , rispettivamente. Dimostriamo che la retta IZ è tangente ad entrambe le circonferenze.

Indichiamo con α, β, γ le ampiezze degli angoli in A, B, C , rispettivamente. Indichiamo con T un punto sulla retta ZI , dalla parte opposta di Z rispetto ad I . Dimostrare che la retta ZI è tangente alla circonferenza circoscritta al triangolo BID è equivalente a dimostrare che $\angle DBI = \angle DIT$. Mostriamo che entrambi gli angoli sono uguali a β .

Infatti, il quadrilatero $IXBZ$ è ciclico, in quanto ha gli angoli in X e Z retti. Ne segue che $\angle TIX = \angle ZBX = \beta$, in quanto entrambi supplementari di $\angle XIZ$. D'altra parte $\angle DBI = 2\angle XBI$ (in quanto BX è altezza rispetto alla base, dunque anche bisettrice, nel triangolo isoscele DBI) e $\angle XBI = \beta/2$ in quanto BI è bisettrice del triangolo ABC .

In maniera del tutto analoga si dimostra che $\angle ECI = \angle EIT = \gamma$.



Soluzione alternativa Se le circonferenze circoscritte ai triangoli BID e CIE sono tangenti, allora il punto di tangenza è necessariamente I . Indicati con O_1 e O_2 i circocentri di BID e CIE , la tesi vale se e soltanto se i punti O_1, I e O_2 sono allineati.

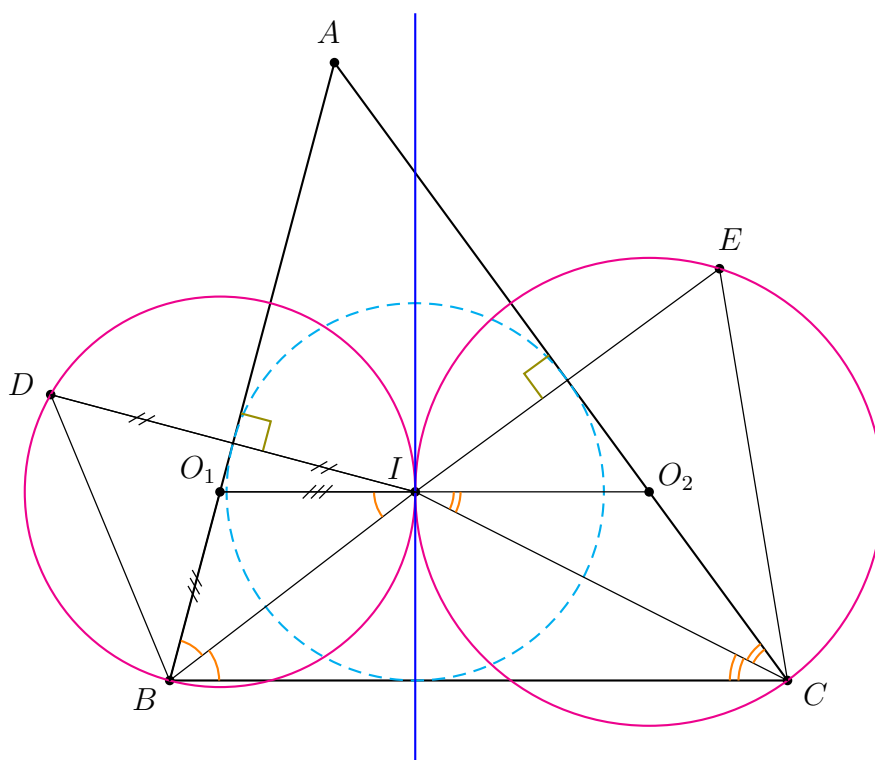
Indichiamo con α, β, γ le ampiezze degli angoli in A, B, C , rispettivamente. Il triangolo BID è isoscele, quindi O_1 appartiene all'asse di DI , cioè alla retta AB . I segmenti O_1I e O_1B sono uguali in quanto raggi, dunque il triangolo O_1IB è isoscele. Inoltre la retta BI è bisettrice dell'angolo in B . Ne segue che

$$\angle O_1IB = \angle IBO_1 = \angle IBC = \frac{\beta}{2},$$

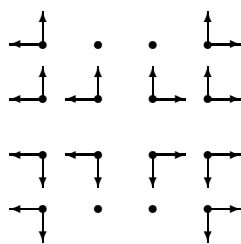
e pertanto le rette BC e O_1I sono parallele in quanto formano angoli alterni interni uguali con la trasversale IB .

In maniera analoga si dimostra che la retta O_2I è parallela a BC .

Ma allora O_1I e O_2I sono rette parallele passanti per I , dunque coincidono, ovvero i punti O_1, I, O_2 sono allineati, da cui segue la tesi.



Problema 3 – Soluzione. Punto (a). Una possibile disposizione nel caso 4×4 è la seguente.



Punto (b). Dimostriamo intanto che $S(n) \leq 4n$. Supponiamo per assurdo che $S(n) > 4n$ per un qualche valore di n . Allora esiste almeno una riga in cui ci sono almeno 5 sentinelle. Di queste 5 sentinelle, almeno 3 guardano in orizzontale nella stessa direzione. Ma allora l'ultimo punto della riga in quella direzione sarà sorvegliato da almeno 3 sentinelle, il che è contro l'ipotesi.

Dimostriamo ora che $S(n) \geq 3n$. Per questo generalizziamo la costruzione del caso 4×4 distinguendo due casi.

- *Caso n pari.* Mostriamo che, per un generico n pari della forma $n = 2k$, è possibile posizionare $4n - 4$ sentinelle (e questo numero è maggiore di $3n$ non appena $n \geq 4$).

Dividiamo la griglia in 4 quadranti $k \times k$. Nel quadrante in alto a sinistra disponiamo tutte le sentinelle sui punti della diagonale (quella contenente il vertice della griglia iniziale) e sui punti appena sotto la diagonale. Tutte queste sentinelle hanno lo sguardo rivolto verso l'alto e verso sinistra. Disponiamo le sentinelle sugli altri 3 quadranti riflettendo opportunamente la configurazione appena descritta.

Osserviamo che in ogni quadrante abbiamo disposto esattamente $k + (k - 1) = n - 1$ sentinelle, quindi in totale ci sono $4n - 4$ sentinelle.

Osserviamo che ogni punto è sorvegliato soltanto da sentinelle che si trovano nel suo quadrante, perché le altre sentinelle guardano altrove. All'interno del quadrante in alto a sinistra, un punto è sorvegliato solo da sentinelle che si trovano sulla stessa colonna e sotto tale punto, o sulla stessa riga e alla destra di tale punto. Se su un punto non ci sono sentinelle, queste stanno o solo sotto (e sono al più 2) o solo a destra (e sono al più 2). I punti in cui stanno le sentinelle sono sorvegliati solo dalla sentinella lì presente e, al più, dalla sentinella appena sotto o appena a destra, e dunque in ogni caso le sentinelle che lo sorvegliano sono al più 2.

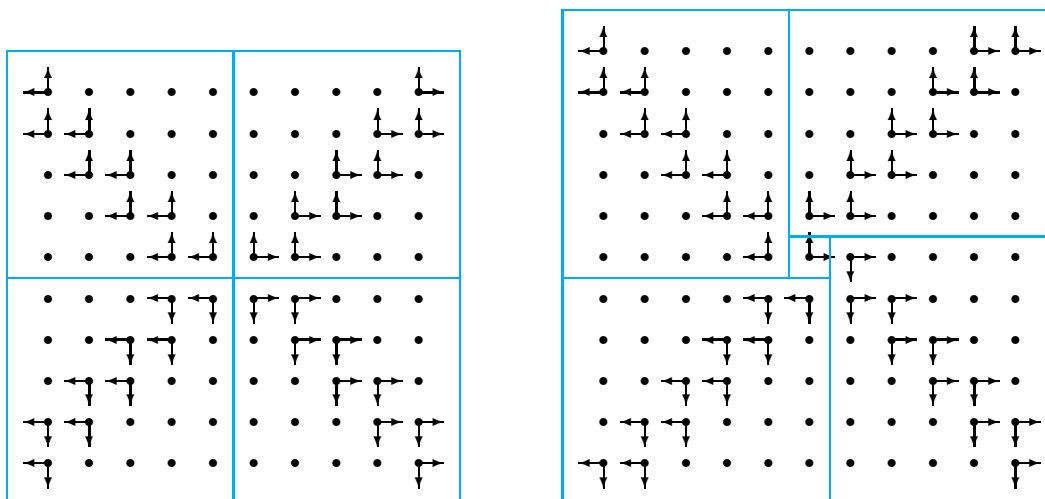
- *Caso n dispari.* Mostriamo che per un generico n dispari della forma $n = 2k - 1$, con $k \geq 2$, è possibile posizionare $4n - 3$ sentinelle (e questo numero è maggiore di $3n$ non appena $n \geq 3$).

In questo caso pensiamo la griglia come unione di quattro rettangoli $k \cdot (k - 1)$, più un quadratino centrale. In ciascun rettangolo ripetiamo sostanzialmente la disposizione delle sentinelle descritta per i blocchi $k \times k$ del caso pari. La condizione per cui ogni punto è sorvegliato da al più due sentinelle è soddisfatta per lo stesso motivo del caso pari.

In questo modo abbiamo sistemato $2(k - 1)$ sentinelle in ogni rettangolo, per un totale di $8k - 8 = 4n - 4$ sentinelle. Osserviamo ora che nella riga e nella colonna centrale abbiamo

disposto solo due sentinelle, quindi possiamo ancora sistemare una ulteriore sentinella nel quadratino centrale, con lo sguardo rivolto in due direzioni a piacere, senza violare le condizioni del problema.

La figura sottostante illustra le costruzioni descritte sopra nei casi particolari $n = 10$ e $n = 11$. Nel caso 11×11 possiamo orientare a piacere la sentinella nella casella centrale.



Problema 4 – Soluzione. Poniamo $M_n = 1/2$ e $m_n = 1/(n-1)$. Dimostriamo che M_n è il massimo valore possibile per l'ultima frazione, mentre m_n è il minimo valore possibile per l'ultima frazione. La dimostrazione consiste di due parti: una costruzione che mostra che tali valori sono effettivamente realizzabili, e una verifica dell'ottimalità di tali valori, cioè che non si può ottenere di più o di meno.

Costruzione. Per ottenere m_n accoppiamo ad ogni passaggio i due numeri più grandi scritti sulla lavagna. Al primo passaggio accoppiamo $1/1$ e $1/2$, ottenendo $2/3$. Al secondo passaggio accoppiamo $2/3$ e $1/3$, ottenendo $1/2$. Pertanto, dopo due passaggi sulla lavagna risultano scritti i numeri

$$\frac{1}{2}, \quad \frac{1}{4}, \quad \frac{1}{5}, \quad \dots, \quad \frac{1}{n}.$$

A questo punto per induzione si dimostra facilmente che al k -esimo passaggio avremo sulla lavagna i numeri

$$\frac{1}{k}, \quad \frac{1}{k+2}, \quad \frac{1}{k+3}, \quad \dots, \quad \frac{1}{n},$$

e quindi dopo $n-2$ passaggi resteranno solo $1/(n-2)$ e $1/n$, componendo i quali si ottiene esattamente m_n .

La costruzione per M_n è analoga, semplicemente accoppiando ad ogni passaggio i due numeri più piccoli. Al primo passaggio accoppiamo $1/n$ e $1/(n-1)$, ottenendo $2/(2n-1)$. Al secondo passaggio accoppiamo $2/(2n-1)$ e $1/(n-2)$, ottenendo $1/(n-1)$. Pertanto, dopo due passaggi avremo sulla lavagna i numeri

$$\frac{1}{1}, \quad \frac{1}{2}, \quad \dots, \quad \frac{1}{n-4}, \quad \frac{1}{n-3}, \quad \frac{1}{n-1}.$$

A questo punto per induzione si dimostra facilmente che al k -esimo passaggio avremo sulla lavagna i numeri

$$\frac{1}{1}, \quad \frac{1}{2}, \quad \dots, \quad \frac{1}{n-k-2}, \quad \frac{1}{n-k-1}, \quad \frac{1}{n-k+1}.$$

Ne segue che dopo $n-2$ passaggi resteranno solo $1/1$ e $1/3$, componendo i quali si ottiene esattamente $1/2$.

Ottimalità. Per dimostrare che non si può ottenere più di M_n o meno di m_n utilizzeremo il seguente risultato preliminare.

Lemma. Per ogni coppia di razionali positivi a/b e c/d (ridotti ai minimi termini) vale la disuguaglianza

$$\min \left\{ \frac{a}{b}, \frac{c}{d} \right\} \leq \frac{a}{b} \diamond \frac{c}{d} \leq \max \left\{ \frac{a}{b}, \frac{c}{d} \right\}.$$

Inoltre, vale una qualunque delle due uguaglianze se e solo se $a/b = c/d$.

Per dimostrare il lemma, indichiamo con m il minimo tra i due numeri razionali, e con M il massimo. Questo vuol dire che $mb \leq a \leq Mb$ e $md \leq c \leq Md$, da cui segue che

$$m = \frac{mb + md}{b + d} \leq \frac{a + c}{b + d} \leq \frac{Mb + Md}{b + d} = M,$$

che è proprio la disuguaglianza della tesi. Lo stesso argomento mostra che, se $a/b \neq c/d$, allora entrambe le disuguaglianze sono strette. \square

Dimostriamo ora che non si può ottenere più di M_n . Consideriamo il primo numero x/y che interagisce con $1/1$. Il numero x/y è il risultato di operazioni svolte a partire dalle frazioni $\{1/2, 1/3, \dots, 1/n\}$, e dunque per il lemma sarà necessariamente minore o uguale a $1/2$. Inoltre, se $x/y = 1/2$, allora necessariamente il numero $1/2$ non è mai stato coinvolto in somme pirata fino a questo momento (se fosse stato coinvolto, per il lemma tali somme avrebbero prodotto numeri strettamente minori di $1/2$). Distinguiamo ora due casi.

- Se $x/y < 1/2$, allora $y > 2x$ e dunque $y \geq 2x + 1$. Ne segue che

$$\frac{1}{1} \diamond \frac{x}{y} = \frac{x+1}{y+1} \leq \frac{x+1}{2x+2} = \frac{1}{2}.$$

- Se $x/y = 1/2$, allora ovviamente la somma pirata con $1/1$ produce come risultato $2/3$. Consideriamo ora il numero e/f che ad un certo punto interagisce con $2/3$. Per quanto osservato precedentemente sappiamo che e/f è il risultato di operazioni svolte a partire dalle frazioni $\{1/3, \dots, 1/n\}$, e dunque per il lemma sarà necessariamente minore o uguale a $1/3$. Ma allora $f \geq 3e \geq 2e + 1$ e dunque

$$\frac{2}{3} \diamond \frac{e}{f} = \frac{2+e}{3+f} \leq \frac{e+2}{2e+4} = \frac{1}{2}.$$

In entrambi i casi ci siamo ridotti ad avere solo frazioni minori o uguali a $1/2$, e dunque per il lemma tutti i numeri successivi, e in particolare l'ultimo rimasto, saranno minori o uguali di $1/2$.

Dimostriamo in maniera analoga che non si può ottenere meno di m_n . Sia z/w il primo numero che interagisce con $1/n$. Per il lemma sappiamo che $z/w \geq 1/(n-1)$, e che vale il segno di uguale se e solo se il numero $1/(n-1)$ non è mai stato utilizzato fino a questo momento. Distinguiamo ora due casi.

- Se $z/w > 1/(n-1)$, allora $w < (n-1)z$ e dunque $w \leq (n-1)z - 1$. Ne segue che

$$\frac{1}{n} \diamond \frac{z}{w} = \frac{z+1}{n+w} \geq \frac{z+1}{nz - z + n - 1} = \frac{1}{n-1}.$$

- Se $z/w = 1/(n-1)$, allora ovviamente la somma pirata con $1/n$ produce come risultato $2/(2n-1)$. Consideriamo ora il numero h/k che ad un certo punto interagisce con $2/(2n-1)$. Per quanto osservato precedentemente sappiamo che h/k è il risultato di operazioni svolte a partire dalle frazioni $\{1/1, 1/2, \dots, 1/(n-2)\}$, e dunque per il lemma sarà necessariamente maggiore o uguale di $1/(n-2)$. Ma allora $k \leq h(n-2) \leq h(n-1) - 1$ e dunque

$$\frac{2}{2n-1} \diamond \frac{h}{k} = \frac{2+h}{2n-1+k} \geq \frac{2+h}{2n-1+h(n-1)-1} = \frac{1}{n-1}.$$

In entrambi i casi ci siamo ridotti ad avere solo frazioni maggiori o uguali di $1/(n-1)$, e dunque per il lemma da quel momento in poi, ed in particolare alla fine, ci saranno solo numeri maggiori o uguali di $1/(n-1)$.

Osservazione geometrica Quella che nel testo del problema è stata chiamata *somma pirata* è nota in letteratura come *mediant* o *freshman sum*, e può essere interpretata nel piano cartesiano in termini di somma di vettori. Infatti, le frazioni a/b e c/d sono i coefficienti angolari delle rette passanti per l'origine e per i punti (a, b) e (c, d) , rispettivamente, mentre la loro somma pirata è il coefficiente angolare della retta che passa per l'origine e per il punto $(a + c, b + d)$, ottenuto sommando i vettori precedenti con la classica regola del parallelogramma. Il lemma e i passaggi successivi della dimostrazione presentata precedentemente posso essere tutti interpretati in termini di coefficienti angolari.

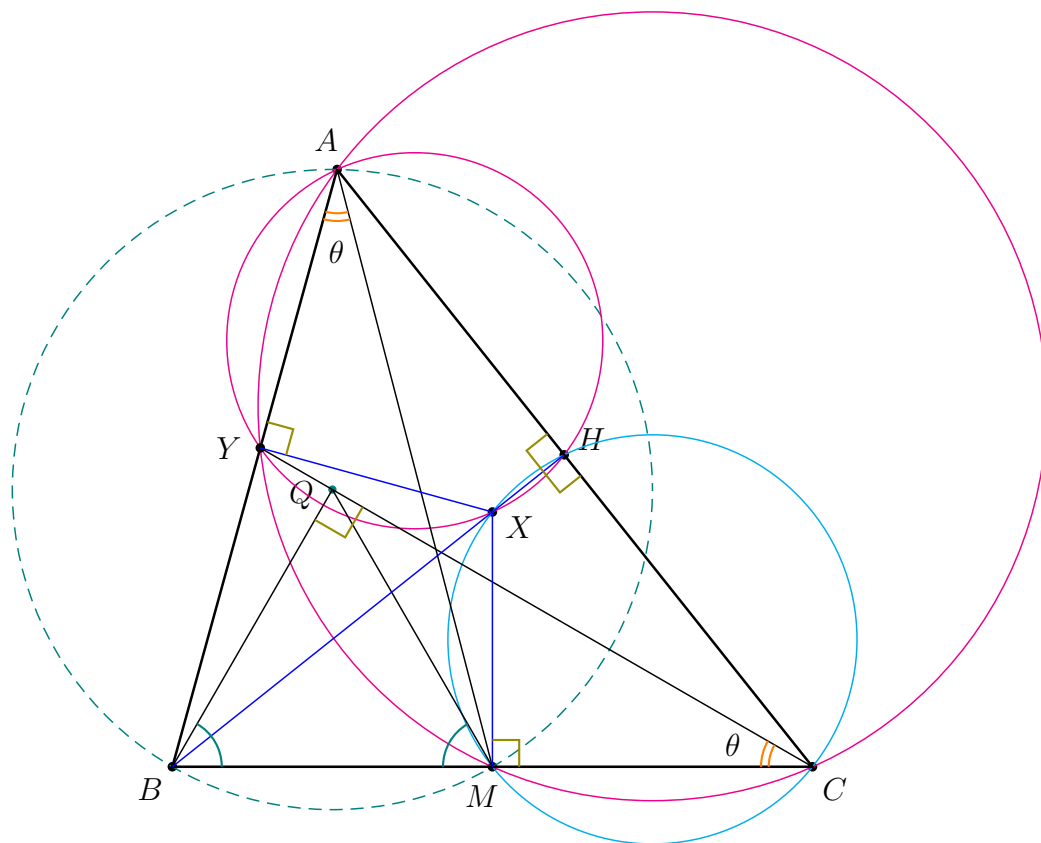
Simmetrie del problema Concludiamo osservando alcune simmetrie intrinseche in questo problema, che avrebbero potuto semplificare la trattazione. La prima è che il problema non cambia se ovunque sostituiamo x con $1/x$. Ne segue che la tesi è equivalente a dimostrare che, partendo dalle "frazioni" $\{1, 2, \dots, n\}$, possiamo ottenere al massimo $n - 1$ e come minimo 2.

Analogamente, possiamo osservare che non cambia nulla se ovunque sostituiamo x con $(n + 1) - x$, dunque basta dimostrare il risultato per il massimo o per il minimo, e l'altro seguirà di conseguenza. In effetti le argomentazioni presentate precedentemente per il massimo e per il minimo sono del tutto analoghe.

Problema 5 – Soluzione. Sia Y la proiezione di X su AB . Dimostriamo che le circonferenze circoscritte ai triangoli AMC e AXH passano entrambe per Y . Questo è equivalente a dimostrare che $BY \cdot BA = BM \cdot BC$, e questo a sua volta è vero in quanto entrambi i prodotti sono uguali a $BX \cdot BH$, dal momento che i quadrilateri $AYXH$ e $HXMC$ sono ciclici, avendo entrambi per costruzione una coppia di angoli opposti retti.

A questo punto la tesi è diventata che i punti Y, Q, C sono allineati se e solo se BQ e CQ sono perpendicolari.

Indichiamo ora con θ l'ampiezza dell'angolo BAM . Dalla ciclicità di $AYMC$ sappiamo che $\angle YCB = \theta$. Inoltre $\angle QBC = 90^\circ - \theta$, in quanto nel triangolo isoscele BQM l'angolo al vertice in Q ha ampiezza 2θ (qui stiamo usando che Q è il circocentro di ABM e gli angoli al centro sono il doppio degli angoli alla circonferenza). Ne segue che Y, Q, C sono allineati se e solo se $\angle BCQ = \angle BCY = \theta$, cioè se e solo se $\angle BCQ + \angle QBC = 90^\circ$, cioè se e solo se BQ e CQ sono perpendicolari.



Osservazione A posteriori, nella configurazione in cui BQ e CQ sono perpendicolari, il triangolo BQM risulta equilatero. Ne segue che $\angle BQM = 60^\circ$, e quindi $\theta = 30^\circ$.

Problema 6 – Soluzione. Dividiamo la dimostrazione in 3 parti: prima esibiamo una strategia in quattro passi per il punto (a), poi esibiamo una strategia in cinque passi per il punto (b) con $k \leq 52$, ed infine mostriamo l'ottimalità del numero dei passi di tali strategie.

Strategia per il punto (a) Una possibile strategia consiste nel rivelare i seguenti quattro termini della successione: $x_{1000}, x_{1004}, x_{1010}, x_{1045}$ (o in generale $x_a, x_{a+4}, x_{a+10}, x_{a+45}$).

Per dimostrarlo, chiamiamo p il periodo, e osserviamo che $x_i = x_j$ se e solo se p divide $j - i$ (in questo punto è fondamentale sapere che i p termini che si ripetono periodicamente sono tutti tra di loro distinti). Di conseguenza, a seconda del valore di p tra 1 e 10, avremo tutte e sole le identità fra i numeri rivelati indicate nella seguente tabella.

Periodo	Identità	Periodo	Identità
1	$x_{1000} = x_{1004} = x_{1010} = x_{1045}$	6	$x_{1004} = x_{1010}$
2	$x_{1000} = x_{1004} = x_{1010}$	7	$x_{1010} = x_{1045}$
3	$x_{1000} = x_{1045}, x_{1004} = x_{1010}$	8	nessuna identità
4	$x_{1000} = x_{1004}$	9	$x_{1000} = x_{1045}$
5	$x_{1000} = x_{1010} = x_{1045}$	10	$x_{1000} = x_{1010}$

Dalla tabella segue che è possibile determinare univocamente il periodo a seconda di quali identità si osservano.

Strategia per il punto (b) Basta esibire una strategia che permetta di distinguere fra i primi 52 periodi primi: la medesima strategia distinguerà, a maggior ragione, fra i primi $k \leq 52$ primi.

Per descrivere una possibile strategia, siano p_1, \dots, p_{52} i primi 52 numeri primi, e sia P il loro prodotto. Considerando ora l'insieme $S = \{1, 2, 3, 4, 5\}$, e definiamo *partizione* di S un qualunque modo di suddividere questo insieme in sottoinsiemi non vuoti. Per esempio, $\{\{1, 2\}, \{4\}, \{3, 5\}\}$ è una partizione di S (si intende che l'ordine in cui vengono presentati i sottoinsiemi $\{1, 2\}, \{4\}, \{3, 5\}$ è irrilevante in questa scrittura).

Mostriamo in seguito che l'insieme S ammette esattamente 52 partizioni. Numeriamo in qualche modo queste partizioni da 1 a 52, facendo in modo che la prima sia quella costituita dal solo sottoinsieme S , e la seconda sia $\{\{1\}, \{2, 3, 4, 5\}\}$. Per ogni intero i tra 1 e 52 consideriamo la funzione $f_i: S \rightarrow S$ che associa ad ogni elemento $x \in S$ il più piccolo $y \in S$ che appartiene alla stesso sottoinsieme di x nella i -esima partizione. Per esempio, se la 42-esima partizione fosse $\{\{1, 2\}, \{4\}, \{3, 5\}\}$, allora avremmo $f_{42}(1) = 1, f_{42}(2) = 1, f_{42}(3) = 3, f_{42}(4) = 4, f_{42}(5) = 3$. Osserviamo che $1 \leq f_i(x) \leq p_i$ per ogni scelta ammissibile di i e x (gli unici primi che potrebbero creare problemi sono $p_1 = 2$ e $p_2 = 3$, ma per come abbiamo scelto le prime due partizioni dell'elenco il problema non si pone).

La strategia consiste nel rivelare i cinque elementi della successione i cui indici a_1, a_2, a_3, a_4, a_5 sono definiti da

$$a_n = \sum_{i=1}^{52} \left(f_i(n) \cdot \frac{P}{p_i} \right) \quad \forall n \in \{1, 2, 3, 4, 5\}.$$

Per dimostrare che questa strategia funziona, procediamo come nel punto (a), studiando le uguaglianze che si possono avere fra questi cinque elementi della successione.

Sia p_i il periodo della successione, con $1 \leq i \leq 52$. Dal momento che i p_i termini della successione che si ripetono periodicamente sono tutti distinti, come nel punto (a) deduciamo che $x_{a_m} = x_{a_n}$ se e solo se p_i divide $a_m - a_n$. Inoltre, dal momento che nella sommatoria che definisce a_n tutti gli addendi sono divisibili per p_i tranne al più l' i -esimo, deduciamo che p_i divide $a_m - a_n$ se e solo se p_i divide $f_i(m) - f_i(n)$. Infine, essendo $f_i(m)$ e $f_i(n)$ entrambi compresi tra 1 e p_i , la divisibilità avviene se e solo se $f_i(m) = f_i(n)$, ossia se e solo se m ed n appartengono allo stesso sottoinsieme della i -esima partizione.

Ne segue che, verificando per quali coppie di indici m ed n vale l'uguaglianza $x_{a_m} = x_{a_n}$, è possibile ricostruire in modo univoco una partizione di S : l'indice i di tale partizione nell'elenco delle 52 partizioni di S determina il periodo p_i .

Resta da dimostrare che le partizioni di S sono 52. A tal fine, indichiamo più in generale con B_b^a il numero delle partizioni di b elementi in a sottoinsiemi, cioè il numero di modi di rappresentare un insieme di b elementi come unione disgiunta di a sottoinsiemi. Chiaramente c'è una sola partizione di b elementi in b o in 1 sottoinsiemi, dunque $B_b^b = B_b^1 = 1$. Una partizione di $b + 1$ elementi in $a + 1$ sottoinsiemi si può ottenere in due modi: o aggiungendo il $(b + 1)$ -esimo elemento ad una delle $a + 1$ parti di una partizione dei primi b elementi in $a + 1$ sottoinsiemi, o aggiungendo il $(b + 1)$ -esimo elemento, come sottoinsieme a sé, ad una partizione di b elementi in a sottoinsiemi. Valgono quindi le relazioni

$$B_b^b = B_b^1 = 1, \quad B_{b+1}^{a+1} = (a + 1)B_b^{a+1} + B_b^a,$$

da cui è possibile completare iterativamente la tabella qui sotto. Il numero di partizioni di un insieme di 5 elementi è la somma dei numeri dell'ultima riga, e cioè 52.

	$a = 1$	2	3	4	5
$b = 1$	$B_b^a = 1$				
2	1	1			
3	1	3	1		
4	1	7	6	1	
5	1	15	25	10	1

Continuando la tabella, e sommando i numeri della riga k -esima, si ottiene il numero di partizioni di un insieme di k elementi¹.

Ottimalità delle strategie L'idea di fondo, per dimostrare che non si può fare di meglio delle strategie illustrate sopra, è di argomentare che l'unica informazione disponibile alla strategia deve essere contenuta nelle uguaglianze che si osservano fra i numeri rivelati. Un'assegnazione di uguaglianze fra k variabili, che immaginiamo rappresentare i k numeri rivelati nei k passi di una qualunque strategia, determina una partizione dell'insieme di queste k variabili. Per cui, in k passi, una strategia può distinguere al più tanti periodi quanti sono le partizioni di un insieme di k elementi, cioè la somma dei numeri della k -esima riga della tabella precedente.

Nel valutare le soluzioni proposte dai concorrenti per questo problema, la precedente argomentazione è stata ritenuta sufficiente.

¹Questi sono noti in letteratura come *numeri di Bell*.

Tuttavia, la traduzione formale dell'idea intuitiva non è ovvia, in quanto il testo del problema ammette esplicitamente strategie “dinamiche” in cui ogni mossa può dipendere dall'esito delle mosse precedenti tenendo conto di svariati fattori, ad esempio la parità dei numeri rivelati, il loro essere o non essere primi, la loro grandezza, e così via.

Nel seguito, dato un qualunque sottoinsieme \mathbb{P} degli interi positivi, indichiamo con $\text{Succ}(\mathbb{P})$ l'insieme di tutte le successioni di interi positivi che hanno periodo $p \in \mathbb{P}$ e hanno i primi p termini distinti (p non è necessariamente un numero primo). Per brevità indichiamo con una singola lettera gli elementi di $\text{Succ}(\mathbb{P})$, cioè scriveremo brevemente x per indicare la successione $x_1, x_2, \dots, x_n, \dots$. L'obiettivo è di dimostrare il seguente enunciato².

Lemma. *Sia k un intero positivo, e sia \mathbb{P} un sottoinsieme degli interi positivi. Supponiamo che esista una strategia che permette di determinare il periodo di ogni successione in $\text{Succ}(\mathbb{P})$ in al più k mosse.*

Allora il numero di elementi di \mathbb{P} è minore o uguale del numero di partizioni dell'insieme $\{1, \dots, k\}$.

Per la dimostrazione del lemma, occorre introdurre un po' di notazioni. Chiamiamo *m-esito* una sequenza E di m coppie $[(a_1, v_1), \dots, (a_m, v_m)]$ di interi positivi, dove a_1, \dots, a_m sono gli indici dei termini rivelati dalla strategia alle mosse $1, \dots, m$, e v_1, \dots, v_m sono i corrispondenti valori rivelati.

Definiamo *peso* di E il numero $\text{Peso}(E) = |\{v_1, \dots, v_m\}|$, cioè il numero di elementi distinti tra v_1, \dots, v_m .

Diciamo che un periodo $p \in \mathbb{P}$ è *credibile* per un certo m -esito E se esiste una successione $z \in \text{Succ}(\mathbb{P})$ di periodo p tale che $z_{a_i} = v_i$ per ogni $i \in \{1, \dots, m\}$.

Indichiamo con $\text{Per}(E)$ il sottoinsieme di \mathbb{P} costituito dai periodi credibili per E , e chiamiamo *incertezza* di E il numero $\text{Inc}(E) = |\text{Per}(E)|$, cioè il numero dei periodi tra i quali restiamo incerti se dopo m passaggi la strategia ci ha fornito E come risultato.

Supponiamo ora che esista una strategia che individua il periodo di ogni elemento di $\text{Succ}(\mathbb{P})$ in al più k mosse. Possiamo supporre che la strategia effettui sempre k mosse prima di indicare il periodo (eventualmente aggiungendo mosse irrilevanti).

Definiamo *ottenibili* tutti gli m -esiti che si possono ottenere applicando la strategia ad una qualche successione in $\text{Succ}(\mathbb{P})$, ed indichiamo con $\mathcal{E}(m)$ l'insieme di tutti gli m -esiti ottenibili. Dimostriamo che vale la stima

$$\text{Inc}(E) \leq C_m^{\text{Peso}(E)} \quad \forall m \in \{1, \dots, k\}, \quad \forall E \in \mathcal{E}(m) \quad (1)$$

dove i numeri C_b^a sono definiti ponendo $C_k^a = 1$ per ogni $1 \leq a \leq k$, e poi a ritroso

$$C_m^a = aC_{m+1}^a + C_{m+1}^{a+1} \quad \forall m \in \{1, \dots, k-1\}, \quad \forall a \in \{1, \dots, m\}.$$

Dando per buono questo risultato, per $m = 1$ avremo in particolare che

$$\text{Inc}(E) \leq C_1^1 \quad \forall E \in \mathcal{E}(1).$$

²Risultato di attribuzione incerta, spesso citato nella letteratura olimpica come *Lemma di Passaro*. Osserviamo che può essere visto come duale del meglio consolidato *Lemma di Damiano*, o come corollario del meno noto *Lemma di Pierrat*.

Tale disuguaglianza è equivalente alla tesi, in quanto per ogni 1-esito E l'incertezza $\text{Inc}(E)$, cioè l'incertezza dopo la prima mossa, è proprio il numero di elementi di \mathbb{P} , dal momento che chiaramente dopo la prima mossa ogni periodo è ancora credibile, mentre C_1^1 è il numero di partizioni di $\{1, \dots, k\}$ (per uno specifico valore di k questo si può verificare calcolando esplicitamente C_1^1 mediante la ricorrenza; per il caso generale si può dimostrare, per induzione su m , che la somma

$$\sum_{a=1}^m B_m^a C_m^a$$

è indipendente da $1 \leq m \leq k$, da cui la conclusione confrontando i casi $m = 1$ e $m = k$).

Per dimostrare la disuguaglianza (1), procediamo per induzione inversa su m . Se $E \in \mathcal{E}(k)$, allora $\text{Inc}(E) = 1$, qualunque sia il peso di E , in quanto per ipotesi la strategia funziona, dunque ogni possibile esito dopo k mosse individua il periodo in modo univoco.

Supponiamo ora che valga la (1) per un certo $m + 1$, con $1 \leq m \leq k - 1$, e dimostriamo che vale per m . Consideriamo dunque un m -esito ottenibile E , che pensiamo come sempre della forma $[(a_1, v_1), \dots, (a_m, v_m)]$. Osserviamo che l'insieme $\text{Per}(E)$ dei periodi credibili per E è contenuto nell'unione degli insiemi $\text{Per}(E')$, dove E' varia tra tutti gli $(m + 1)$ -esiti ottenibili che coincidono con E fino al passo m . Osserviamo anche che l'indice a_{m+1} di ogni E' di questo tipo è sempre lo stesso, in quanto dipende unicamente dalla storia fino al passo m . Di conseguenza, tutti gli $(m + 1)$ -esiti che ci interessano si ottengono aggiungendo ad E una coppia della forma (a_{m+1}, v) , dove v varia in un opportuno insieme \mathcal{F} di interi positivi.

Abbiamo dunque ottenuto l'inclusione

$$\text{Per}(E) \subseteq \bigcup_{v \in \mathcal{F}} \text{Per}([(a_1, v_1), \dots, (a_m, v_m), (a_{m+1}, v)]). \quad (2)$$

Ora il valore v può coincidere o meno con uno dei valori v_1, \dots, v_m coinvolti in E . Questo ci porta a pensare l'unione in (2) come unione dell'insieme

$$\bigcup_{v \in \{v_1, \dots, v_m\}} \text{Per}([(a_1, v_1), \dots, (a_m, v_m), (a_{m+1}, v)]) \quad (3)$$

e dell'insieme

$$\bigcup_{w \in \mathcal{F} \setminus \{v_1, \dots, v_m\}} \text{Per}([(a_1, v_1), \dots, (a_m, v_m), (a_{m+1}, w)]). \quad (4)$$

Nella (3) il numero di insiemi che stiamo unendo è $\text{Peso}(E)$ e ciascuno di essi ha, per ipotesi induttiva, un numero di elementi minore o uguale a $C_{m+1}^{\text{Peso}(E)}$. Ne segue che il numero di elementi della prima unione è minore o uguale di

$$\text{Peso}(E) \cdot C_{m+1}^{\text{Peso}(E)}.$$

Nella (4) gli insiemi che stiamo unendo sono (fortunatamente) tutti uguali, in quanto l'insieme dei periodi compatibili con un certo $(m + 1)$ -esito $[(a_1, v_1), \dots, (a_m, v_m), (a_{m+1}, w_1)]$ coincide con l'insieme dei periodi compatibili con l' $(m + 1)$ -esito $[(a_1, v_1), \dots, (a_m, v_m), (a_{m+1}, w_2)]$, qualunque siano gli interi positivi w_1 e w_2 , purché diversi da v_1, \dots, v_m . Infatti, se p è un periodo credibile dato il primo $(m + 1)$ -esito, allora esiste una successione $z \in \text{Succ}(\mathbb{P})$ di periodo p tale che $z_{a_j} = v_j$ per j che va da 1 a m , e $z_{a_{m+1}} = w_1$; ora, sostituendo nella successione z ogni

occorrenza di w_1 con w_2 , e viceversa, si ottiene una nuova successione in $\text{Succ}(\mathbb{P})$ di periodo p e compatibile con il secondo $(m+1)$ -esito, e dunque p è credibile anche dato il secondo esito. Il viceversa è analogo.

Osserviamo infine che tutti gli insiemi (uguali) che compaiono nell'unione (4) sono i periodi credibili per opportuni $(m+1)$ -esiti ammissibili il cui peso è uguale a $\text{Peso}(E)+1$, e dunque per ipotesi induttiva il numero di elementi della seconda unione è minore o uguale di $C_{m+1}^{\text{Peso}(E)+1}$.

Tornando alla (2), abbiamo dimostrato che per ogni $E \in \mathcal{E}(m)$ vale la stima

$$\text{Inc}(E) \leq \text{Peso}(E) \cdot C_{m+1}^{\text{Peso}(E)} + C_{m+1}^{\text{Peso}(E)+1} = C_m^{\text{Peso}(E)},$$

il che completa il passo induttivo, e dunque la dimostrazione del lemma.

Un approccio alternativo al lemma consiste nel ragionare per assurdo, mostrando che, se il numero di elementi di \mathbb{P} è maggiore del numero di partizioni di $\{1, \dots, k\}$, allora per ogni strategia S in k passi esistono due successioni in $\text{Succ}(\mathbb{P})$, di periodo diverso, agendo sulle quali la strategia produce lo stesso k -esito, rendendo quindi impossibile l'individuazione univoca del periodo.

Per mostrare questo risultato, diciamo che un m -esito $[(a_1, v_1), \dots, (a_m, v_m)]$ è *morigerato* se $v_1 = 1$ e $v_i \leq \max\{v_1, \dots, v_{i-1}\} + 1$ per ogni $i \in \{2, \dots, m-1\}$. Diciamo che una successione è *S-morigerata* se la strategia S , applicata alla successione, produce un k -esito morigerato (e dunque anche tutti gli m -esiti ottenuti strada facendo sono morigerati). In altri termini, il valore rivelato (non l'indice) dalla strategia S su una successione *S-morigerata* al passo m è uno dei valori precedenti, oppure il massimo dei valori precedenti aumentato di 1.

L'esistenza delle due successioni di periodo diverso che producono lo stesso k -esito segue ora, grazie al principio del pigeonhole, da tre claim.

1. Se due k -esiti di una stessa strategia S hanno gli stessi valori nello stesso ordine, allora hanno anche gli stessi indici nello stesso ordine.
2. Il numero di possibili k -esiti di una data strategia S applicata a successioni *S-morigerate* è minore o uguale del numero di partizioni di $\{1, \dots, k\}$.
3. Per ogni strategia S e per ogni periodo $p \in \mathbb{P}$, esiste in $\text{Succ}(\mathbb{P})$ almeno una successione *S-morigerata* di periodo p .

Il primo claim si dimostra per induzione, sfruttando che l'indice che sarà rivelato al passo $m+1$ dipende solo dagli indici e dai valori rivelati fino al passo m .

Per dimostrare il secondo claim osserviamo che, grazie al primo claim, un k -esito morigerato ottenuto da una data strategia S è univocamente determinato dalla k -upla (v_1, \dots, v_k) dei suoi valori. A questo punto basta osservare che esiste una corrispondenza biunivoca tra tali k -uple e le partizioni di $\{1, \dots, k\}$ (basta considerare i passi a cui si è ottenuto come valore 1, 2, ...).

Per dimostrare il terzo claim, consideriamo il più grande intero $m \in \{1, \dots, k\}$ per cui esiste una successione in $\text{Succ}(\mathbb{P})$ di periodo p i cui esiti sono *S-morigerati* fino al passo m . Osserviamo preliminarmente che, detto a_1 l'indice del termine rivelato dalla strategia S al primo passo, esiste di sicuro una successione di periodo p con $x_{a_1} = 1$, dunque m è ben definito, nel senso che l'insieme di cui è il massimo non è vuoto.

Ora se $m = k$ non c'è nulla da dimostrare. Se invece $m < k$, consideriamo una qualunque successione $x \in \text{Succ}(\mathbb{P})$ di periodo p che realizza il massimo. Al passo $m + 1$ la strategia S applicata a x produrrà una coppia (a_{m+1}, w) per un certo $w > w' + 1$, dove w' è il massimo dei valori rilevati nei primi m passi. Se però ora consideriamo la successione y ottenuta scambiando in x ogni occorrenza di w con $w' + 1$, e viceversa, si può verificare che y è ancora un elemento di $\text{Succ}(\mathbb{P})$ di periodo p , ed i suoi esiti sono morigerati fino almeno al passo $m + 1$ (e coincidono con quelli di x fino al passo m). Questo contraddice la massimalità di m .

Osservazioni conclusive Il “convitato di pietra” nei problemi di questo tipo è il concetto di strategia. La domanda fondamentale che uno si potrebbe porre è: *cos'è una strategia?* Il problema può cambiare di molto a seconda della risposta a questa domanda.

In questo caso specifico si sarebbe potuto formulare il problema usando solo strategie “statiche”, in cui il “giocatore” deve dichiarare subito all’inizio tutti gli indici dei termini che vuole rivelare. In questa formulazione una strategia in n passi è quindi, dal punto di vista formale, semplicemente una n -upla di interi positivi, cioè appunto gli indici richiesti. Le soluzioni presentate all’inizio per i punti (a) e (b) mostrano in effetti delle strategie statiche che risolvono il problema in un certo numero di mosse. Per quanto riguarda l’ottimalità, la dimostrazione si semplifica di molto se ci si limita alle sole strategie statiche, perché a quel punto basta un argomento di scambio di valori per mostrare rigorosamente che l’unica informazione rilevante sono le uguaglianze tra i valori rilevati.

Una classe più ampia di strategie comprende quelle che potremmo chiamare strategie “dinamiche deterministiche”. Il giocatore ora sceglie il primo indice a_1 da rivelare, e poi ad ogni mossa successiva sceglie l’indice a_{m+1} sulla base dell’ m -esito. La strategia è quindi formalmente costituita da un numero (il primo indice) e da una funzione che ad ogni m -esito associa l’indice successivo. Il determinismo consiste nel fatto che il passo iniziale è sempre lo stesso, e lo stesso m -esito porterà sempre a richiedere lo stesso indice al passo successivo. Le due dimostrazioni del lemma di ottimalità fornite precedentemente, così come sono state scritte, sono pensate nella classe delle strategie dinamiche deterministiche.

Una classe ancora più ampia di strategie comprende quelle che potremmo chiamare strategie “dinamiche probabilistiche”. Dopo aver visto l’ m -esito, ora il giocatore “tira un dado”, e sceglie l’indice successivo da rivelare in base all’ m -esito ed al risultato del dado (e analogamente per la scelta del primo indice). Lo stesso m -esito può dunque condurre ora a indagare indici diversi al passo successivo. Le due dimostrazioni precedenti di ottimalità si possono, con piccole modifiche, adattare in modo da includere anche strategie di questo tipo, pur di assumere che il dado si comporti “in maniera imparziale”. Invece non possiamo concedere come “strategia” l’uso di un dado non imparziale che, ad esempio, alla prima mossa ci fa rivelare il 2021-esimo termine, e alla seconda mossa “per caso” richiede proprio il termine di indice $2021 + p$, dove p è il periodo della successione. Con un dado del genere, se p è primo, ce la caveremmo sempre in due mosse!