Laboratorio di Matematica

Foglio n.2 - 8 marzo 2013

Problema 1. Siano $x_0 < x_1 < \cdots < x_n$ degli interi positivi con $n \geq 1$. Dimostrare che

$$\sum_{k=1}^{n} \frac{1}{\mathrm{lcm}(x_{k-1}, x_k)} \leq 1 - \frac{1}{2^n}.$$

Soluzione. Dimostriamo la disuguaglianza per induzione.
Dato che $1 \leq x_0 < x_1$ allora $x_1 \geq 2$ e $\mathrm{lcm}(x_0, x_1) \geq 2$. Così per $n = 1$,

$$\sum_{k=1}^{n} \frac{1}{\mathrm{lcm}(x_{k-1}, x_k)} = \frac{1}{\mathrm{lcm}(x_0, x_1)} \leq \frac{1}{2} = 1 - \frac{1}{2^n}.$$

Per $n > 1$ distinguiamo due casi.
1) Se $x_{n+1} \geq 2^{n+1}$ allora $\mathrm{lcm}(x_n, x_{n+1}) \geq 2^{n+1}$ e per l'ipotesi induttiva

$$\sum_{k=1}^{n+1} \frac{1}{\mathrm{lcm}(x_{k-1}, x_k)} \leq 1 - \frac{1}{2^n} + \frac{1}{\mathrm{lcm}(x_n, x_{n+1})} \leq 1 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 1 - \frac{1}{2^{n+1}}.$$

2) Se $x_{n+1} < 2^{n+1}$ allora per $0 \leq k \leq n$

$$\frac{1}{\mathrm{lcm}(x_k, x_{k+1})} = \frac{\gcd(x_k, x_{k+1})}{x_k x_{k+1}} = \frac{\gcd(x_k, x_{k+1} - x_k)}{x_k x_{k+1}} \leq \frac{x_{k+1} - x_k}{x_k x_{k+1}} = \frac{1}{x_k} - \frac{1}{x_{k+1}}$$

e quindi

$$\sum_{k=1}^{n+1} \frac{1}{\mathrm{lcm}(x_{k-1}, x_k)} \leq \frac{1}{x_0} - \frac{1}{x_{n+1}} \leq 1 - \frac{1}{2^{n+1}}.$$

□

Problema 2. Per quali valori interi di $n \geq 2$, il numero

$$\left\lfloor \frac{n!}{n+1} \right\rfloor$$

è divisibile per n?

Soluzione. Dimostriamo che n divide $\left\lfloor \frac{n!}{n+1} \right\rfloor$ per ogni $n \neq 3$.
1) Se $n+1$ non è un numero primo e non è il quadrato di un numero primo allora esistono due interi a e b tali che $2 \leq a < b \leq n$ e $n+1 = ab$. Inoltre, dato che $\gcd(n+1, n) = 1$, necessariamente $b < n$. Quindi

$$\left\lfloor \frac{n!}{n+1} \right\rfloor = n \cdot \frac{(n-1)!}{n+1} = n \cdot d$$

con d un numero intero perché $ab = n+1$ divide $(n-1)!$.
2) Se $n = p^2 - 1$ con p numero primo allora, con eccezione del caso $p = 2$ ossia $n = 3$, si ha che $p < 2p \leq p^2 - 2$ Quindi

$$\left\lfloor \frac{n!}{n+1} \right\rfloor = (p^2 - 1) \cdot \frac{(p^2 - 2)!}{p^2} = n \cdot d$$

con d un numero intero perché p^2 divide $(p^2 - 2)!$.
3) Se $n = p - 1$ con p numero primo allora per il teorema di Wilson, $(p-1)! \equiv -1 \pmod{p}$ e

$$\left\lfloor \frac{n!}{n+1} \right\rfloor = \left\lfloor \frac{(p-1)! + 1}{p} - \frac{1}{p} \right\rfloor = \frac{(p-1)! + 1}{p} - 1 = (p-1) \cdot \frac{(p-2)! - 1}{p} = n \cdot d$$

con d un numero intero perché $(p-2)! \equiv 1 \pmod{p}$.

□

Problema 3. Siano A, B delle matrici reali $n \times n$ tali che esiste un vettore non nullo u per cui $Au = 0$ e esiste un vettore v per cui $Av = Bu$. Dimostrare che

$$\sum_{k=1}^{n} \det(A_k) = 0$$

dove A_k è la matrice A dove la k-sima colonna è stata sostituita con la la k-sima colonna di B.

Soluzione. Siano $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ i vettori colonna rispettivamente di A e B. Sia $u = (u_1, \ldots, u_n)$ e sia $v = (v_1, \ldots, v_n)$. Possiamo supporre per simmetria che $u_1 \neq 0$ e da $Au = 0$ otteniamo che $\det(A) = 0$ e $a_1 = -(1/u_1) \sum_{j=2}^{n} u_j a_j$. Così

$$\begin{aligned}
\sum_{k=1}^{n} \det(A_k) &= \det(b_1, a_2, \ldots, a_n) + \sum_{i=2}^{n} \det(a_1, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_n) \\
&= \det(b_1, a_2, \ldots, a_n) - \frac{1}{u_1} \sum_{i=2}^{n} \det(\sum_{j=2}^{n} u_j a_j, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_n) \\
&= \det(b_1, a_2, \ldots, a_n) - \frac{1}{u_1} \sum_{i=2}^{n} \det(u_i a_i, \ldots, a_{i-1}, b_i, a_{i+1}, \ldots, a_n) \\
&= \det(b_1, a_2, \ldots, a_n) + \frac{1}{u_1} \sum_{i=2}^{n} \det(u_i b_i, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \\
&= \det(b_1, a_2, \ldots, a_n) + \frac{1}{u_1} \sum_{i=2}^{n} \det(u_i b_i, a_2, \ldots, a_n) \\
&= \frac{1}{u_1} \sum_{i=1}^{n} \det(u_i b_i, a_2, \ldots, a_n) = \frac{1}{u_1} \det(\sum_{i=1}^{n} u_i b_i, a_2, \ldots, a_n) \\
&= \frac{1}{u_1} \det(\sum_{i=1}^{n} v_i a_i, a_2, \ldots, a_n) = \frac{1}{u_1} \det(v_1 a_1, a_2, \ldots, a_n) = \frac{v_1}{u_1} \det(A) = 0.
\end{aligned}$$

$\square$

Problema 4. È possibile determinare una famiglia di circonferenze $\{C_i\}_{i \in I}$, ciascuna di raggio positivo, tale che per ogni punto $P \in \mathbb{R}^2$ esistono esattamente 4 circonferenze della famiglia che passano per P?

Soluzione. Sì, ad esempio si può prendere la famiglia di circonferenze di centro $(t, n) \in \mathbb{R} \times \mathbb{Z}$ e raggio 1. È facile verficare che per ogni $(x, y) \in \mathbb{R}^2$ esistono esattamente 4 circonferenze della famiglia che passano per P.
1) Se $y \in \mathbb{Z}$ allora le quattro circonferenze hanno centri

$$(x-1, y), \quad (x+1, y), \quad (x, y+1), \quad (x, y-1).$$

2) Se $y \notin \mathbb{Z}$, sia $n = \lfloor y \rfloor$ e $s = y - \lfloor y \rfloor$. Allora le quattro circonferenze hanno centri

$$(x - \sqrt{1-s^2}, n), \quad (x + \sqrt{1-s^2}, n), \quad (x - \sqrt{1-(1-s)^2}, n+1), \quad (x + \sqrt{1-(1-s)^2}, n+1).$$

$\square$

Problema 5. Dato un polinomio a coefficienti interi f si definisca l'insieme

$$I_f := \bigcap_{n\geq 1} f^n(\mathbb{Z})$$

dove f^n indica il polinomio f composto n volte.

i) Per quali polinomi $f \in \mathbb{Z}[x]$, l'insieme I_f è finito?

ii) Dato un insieme finito $S \subset \mathbb{Z}$, è possibile trovare un polinomio $f \in \mathbb{Z}[x]$ tale che $I_f = S$?

Soluzione. i) Intanto è facile verificare che se $f(x) = x + a_0$ oppure $f(x) = -x + a_0$ con $a_0 \in \mathbb{Z}$, allora $f(\mathbb{Z}) = \mathbb{Z}$ e $I_f = \mathbb{Z}$. Dimostriamo che in ogni altro caso I_f è finito. Se $f(x) = a_0$ allora $I_f = \{a_0\}$. Supponiamo ora che $f(x) = a_d x^d + \cdots + a_1 x + a_0$ con $a_d \neq 0$.

1) Se $M := \sum_{i=0}^{d-1} |a_i| + 2 \geq 2$ e $|x| > M$ allora $|f(x)| > |x| + 1$.
Se $d = 1$ allora $M = |a_0| + 2$, $|a_1| \geq 2$ e

$$|f(x)| \geq |a_1||x| - |a_0| = (|a_1| - 1)|x| + |x| - |a_0| > M + |x| - |a_0| > |x| + 1.$$

Se $d \geq 2$ allora $|a_d| \geq 1$ e

$$|f(x)| \geq |a_d||x|^d - \left|\sum_{i=0}^{d-1} a_i x^i\right| > M|x|^{d-1} - \left|\sum_{i=0}^{d-1} a_i x^i\right| \geq \sum_{i=0}^{d-1} |a_i||x|^i + 2|x| - \left|\sum_{i=0}^{d-1} a_i x^i\right| \geq 2|x| > |x| + 1.$$

2) Se $x \in I_f$ allora esiste un intero positivo m tale che $f^m(x) = x$.
Per definizione, per ogni $n \geq 1$ esiste $x_n \in \mathbb{Z}$ tale che $f^n(x_n) = x$. Se $n \geq |x|$ allora $x_n \in \{0, \pm 1, \ldots, \pm M\}$. Infatti se $|x_n| > M$ allora, per 1), $|f^k(x_n)| > M$ per ogni $k \geq 1$ e

$$|x| = |f^n(x_n)| > |f^{n-1}(x_n)| + 1 > \cdots > |x_n| + n > M + |x| > |x|.$$

Quindi esiste $j \in \{0, \pm 1, \ldots, \pm M\}$ tale che per infiniti n, $f^n(j) = x$. Siano $n_1 < n_2$ due di questi n, allora per $m = n_2 - n_1 \geq 1$,

$$f^m(x) = f^{n_2 - n_1}(f^{n_1}(j)) = f^{n_2}(j) = x.$$

3) Se $x \in I_f$ allora $f(f(x)) - x = 0$ oppure $f(f(x)) - 2f(x) + x = 0$ e, dato che f è un polinomio, questo implica che I_f è finito (con al più $2d^2$ elementi).
Infatti se $f(x) = x$ allora x soddisfa entrambe le equazioni. Ora supponiamo che $f^m(x) = x$ per $m \geq 2$ e $f^k(x) \neq x$ per $k = 1, \ldots, m-1$. È facile verificare che se $P \in \mathbb{Z}[x]$ e $a, b \in \mathbb{Z}$ allora $a - b$ divide $P(a) - P(b)$. Dunque $x - f(x)$ divide $f(x) - f^2(x)$, $f(x) - f^2(x)$ divide $f^2(x) - f^3(x)$ e così via fino a $f^{m-1}(x) - f^m(x)$ divide $f^m(x) - f^{m+1}(x) = x - f(x)$. Questo implica necessariamente che

$$|x - f(x)| = |f(x) - f^2(x)| = \cdots = |f^{m-1}(x) - f^m(x)|$$

e in particolare $x - f(x) = \pm(f(x) - f^2(x))$ ossia $f(f(x)) - x = 0$ oppure $f(f(x)) - 2f(x) + x = 0$.

ii) Se $S = \emptyset$ si può prendere $f(x) = (2x+1)^2 + x$. Se invece S è un sottoinsieme finito di $\mathbb{Z}$ si può prendere $f(x) = \prod_{s\in S}(x - s)^2 + x$. □