Secondo appello di Laboratorio di Matematica

1 luglio 2011

Problema 1. Dimostrare che

$$F_p^2 \equiv 1 \pmod p \qquad \text{per ogni primo } p \neq 5,$$

dove F_n è l'n-simo numero di Fibonacci definito dalla ricorsione

$$F_0 = 0,\ F_1 = 1 \text{ e } F_n = F_{n-1} + F_{n-2} \text{ per } n \geq 2.$$

Soluzione.
Notiamo che $F_2^2 = 1 \equiv 1 \pmod 2$, $F_3^2 = 4 \equiv 1 \pmod 3$ e $F_5^2 = 25 \equiv 0 \pmod 5$.
Supponiamo ora che p sia un primo maggiore di 5.
Dato che p divide $\binom{p}{k}$ per $k = 1, \ldots, p-1$, per il Teorema di Eulero-Fermat

$$F_p = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^p - \left(\frac{1-\sqrt{5}}{2} \right)^p \right) = \frac{1}{2^{p-1}} \sum_{\substack{0 \leq k \leq p \\ k \equiv 1 \pmod 2}} \binom{p}{k} 5^{(k-1)/2}$$

$$= \frac{1}{2^{p-1}} \sum_{\substack{1 \leq k \leq p-1 \\ k \equiv 1 \pmod 2}} \binom{p}{k} 5^{(k-1)/2} + \frac{5^{(p-1)/2}}{2^{p-1}} \equiv 5^{(p-1)/2} \pmod p.$$

Quindi, ancora per il Teorema di Eulero-Fermat,

$$F_p^2 \equiv \left(5^{(p-1)/2} \right)^2 \equiv 5^{p-1} \equiv 1 \pmod p.$$

□

Problema 2. Sia n un numero intero positivo e siano $z_1, z_2, \ldots, z_n$ dei numeri complessi di modulo unitario (non necessariamente distinti). Dimostrare o confutare che esiste w tale che

$$|w| = 1 \qquad \text{and} \qquad \sum_{k=1}^{n} |w - z_i| > n.$$

Soluzione.
Sia w tale che $|w| = 1$ e $w \neq \pm z_i$ per $i = 1, \ldots, n$. Allora ogni triangolo di vertici z_i, w e $-w$ è non degenere e vale la disuguaglianza

$$|z_i - w| + |z_i - (-w)| > |w - (-w)| = 2.$$

Ora sommando rispetto a $i = 1, \ldots, n$ si ottiene che

$$\sum_{i=1}^{n} |z_i - w| + \sum_{i=1}^{n} |z_i - (-w)| > 2n$$

e quindi almeno una delle due somme è maggiore di n. Pertanto la proprietà richiesta vale per w o per $-w$. □

Problema 3. Determinare per quali interi positivi n, il polinomio

$$P(z) = -1 + \prod_{k=1}^{n} (z - k)$$

è irriducibile su $\mathbb{Z}$.

Soluzione.
Supponiamo che $P(z)$ sia riducibile al prodotto dei polinomi $f, g \in \mathbb{Z}[z]$ di grado minore di n. Allora $f(k)$ e $g(k)$ per $k = 1, \ldots, n$ sono interi e per definizione di P si ha che $f(k)g(k) = -1$. Quindi $f(k) = -g(k) = \pm 1$ e $f + g \in \mathbb{Z}[z]$ è un polinomio di grado minore di n che ha almeno n zeri (i numeri $1, \ldots, n$) da cui segue che $f = -g$. Infine, se $f(z) = az^d + o(z^d)$ allora,

$$z^n + o(z^n) = P(z) = f(z)g(z) = -f(z)^2 = -a^2 z^{2d} + o(z^{2d})$$

che è impossibile perché non esiste un numero intero a tale che $-a^2 = 1$. □

Problema 4. Determinare tutte le funzioni $f \in C^1([0, +\infty))$ tali che

$$|f'(x)| \leq |f(x) - f(0)| \qquad \text{per ogni } x \in [0, +\infty).$$

Soluzione.
Sia $g(x) = f(x) - f(0)$ allora $|g'(x)| \leq |g(x)|$ per $x \geq 0$. Quindi se $M_a = \max_{x \in [0,a]} |g(x)|$, per $x \in [0, a]$ si ha che

$$|g(x)| = \left| \int_0^x g'(t)dt \right| \leq \int_0^x |g'(t)|\, dt \leq \int_0^x |g(t)|\, dt \leq M_a \int_0^x dt = M_a x.$$

In modo simile, per $x \in [0, a]$ si ha che

$$|g(x)| \leq \int_0^x |g(t)|\, dt \leq M_a \int_0^x t dt = \frac{M_a x^2}{2}$$

e continuando a iterare la stima si ottiene che per ogni $n \geq 0$

$$|g(x)| \leq \frac{M_a x^n}{n!}.$$

Calcolando il limite per $n \to +\infty$ si conclude che $|g(x)| = 0$ per ogni $x \in [0, a]$. Data l'arbitrarietà della scelta di a, si ha che $g(x) \equiv 0$ ossia le uniche funzioni f che soddisfano la condizione richiesta sono le funzioni costanti. □
