

Soluzione dei problemi di Pasqua

Problema 1 (Nordic Math. Contest, 1992). *Sia $n \geq 1$ e siano $a_1, \dots, a_n$ numeri interi distinti. Si provi che il polinomio*

$$f = (x - a_1)(x - a_2) \dots (x - a_n) - 1$$

è irriducibile in $\mathbb{Q}[x]$.

SOLUZIONE. Poiché f è certamente primitivo, risulta irriducibile in $\mathbb{Q}[x]$ se e solo se è irriducibile in $\mathbb{Z}[x]$. Supponiamo il contrario, allora, poiché f è monico, si ha $f = gh$ con $g, h \in \mathbb{Z}[x]$ polinomi monici di grado minore o uguale a $n - 1$. Allora, per ogni $i = 1, \dots, n$,

$$-1 = f(a_i) = g(a_i)h(a_i);$$

dunque, trattandosi di numeri interi, si ha, per ogni $i = 1, \dots, n$,

$$g(a_i) = -h(a_i) = \pm 1.$$

Sia p il polinomio $p = f + g$. Se $p \neq 0$, allora $\deg p \leq \max\{\deg g, \deg h\} < n$; ma p ha, per quanto osservato sopra, le n radici distinte $a_1, \dots, a_n$, che è assurdo. Dunque $p = 0$, ovvero $h = -g$. Ma allora

$$f = g \cdot h = -g^2$$

che è assurdo perché il coefficiente direttivo di f è 1 mentre quello di $-g^2$ è un numero negativo.

■

Problema 2 (San Pietroburgo 1987). *Rappresentare il numero $n = 989 \cdot 1001 \cdot 1007 + 320$ come prodotto di numeri primi.*

SOLUZIONE. Poniamo $a = 1001$; allora $n = (a - 12) \cdot a \cdot (a + 6) + 320$, da cui

$$n = a^3 - 6a^2 - 72a + 320.$$

Trattiamo il termine di destra come un polinomio a coefficienti interi nell'indeterminata a ; esaminando i divisori del termine noto, si scopre che 4 ne è una radice, e che quindi il polinomio è diviso da $a - 4$. Svolgendo la divisione si trova

$$\begin{aligned} n &= (a - 4)(a^2 - 2a - 80) = (a - 4)((a - 1)^2 - 81) = (a - 4)((a - 1)^2 - 9^2) = \\ &= (a - 10)(a - 4)(a + 8) = 991 \cdot 997 \cdot 1009, \end{aligned}$$

che è la fattorizzazione di n in prodotto di primi. ■

Problema 3 (Baltic Way, 2014). *Dire se il numero $712! + 1$ è un numero primo.*

SOLUZIONE. Cominciamo con l'osservare che un divisore primo di $712! + 1$ non può essere minore o uguale di 712 (l'argomento di Euclide!). Scorrendo la lista dei numeri primi, troviamo che il più piccolo primo maggiore di 712 è 719. Per il teorema di Wilson,

$$712! \cdot 713 \cdot \dots \cdot 717 \cdot 718 = 718! \equiv -1 \pmod{719}.$$

Quindi

$$-1 \equiv (-1)(-2)(-3)(-4)(-5)(-6)(712!) \equiv 720 \cdot (712!) \equiv 712! \pmod{719},$$

e dunque 719 divide $712! + 1$ che pertanto non è un numero primo. ■

Problema 4. Si provi che per ogni $n \geq 1$, il polinomio

$$f = x^n + 5x^{n-1} + 3$$

è irriducibile in $\mathbb{Q}[x]$.

SOLUZIONE. Poiché f è certamente primitivo, risulta irriducibile in $\mathbb{Q}[x]$ se e solo se è irriducibile in $\mathbb{Z}[x]$. Supponiamo il contrario, allora, poiché f è monico, si ha $f = gh$ con $g, h \in \mathbb{Z}[x]$ polinomi monici di grado minore o uguale a $n - 1$. Sia $g = x^t + \dots + a_1x + a_0$ e $h = x^{n-t} + \dots + b_1x + b_0$. Allora $a_0b_0 = 3$, dunque, a meno di scambiare g con h , possiamo supporre $b_0 = \pm 1$ e $a_0 = \pm 3$. Sia $\bar{f}$ la riduzione di f modulo 3. Allora, in $(\mathbb{Z}/3\mathbb{Z})[x]$,

$$x^{n-1}(x-1) = x^n + 2x^{n-1} = \bar{f} = \bar{g} \cdot \bar{h};$$

quindi, per l'unicità della fattorizzazione in irriducibili (e poiché il termine noto di $\bar{g}$ è 0),

$$\bar{g} = x^t \quad \text{e} \quad \bar{h} = x^{n-t-1}(x-1).$$

Siccome $b_0 = \pm 1 \not\equiv 0 \pmod{3}$, il termine noto di $\bar{h}$ non è zero; quindi, necessariamente, $\bar{h} = x - 1$ (e $\bar{g} = x^{n-1}$). Questo forza $h = x + b_0 = x - 1$; per Ruffini si ha allora

$$0 = f(1) = 1 + 5 + 3;$$

che è un assurdo. ■