Sui numeri binari quadrati

Troncana F.

Introduzione

Qualche tempo fa, Matilde mi ha presentato un'interessante congettura:

Proposizione 0.1: Calabri I

Gli unici numeri della forma $a_0 + 10a_1 + 100a_2 + ...$ con $a_i \in \{0, 1\}$ che sono quadrati perfetti sono della forma 10^{2k} per qualche $k \in \mathbb{N}$.

Dopo un infruttuoso attacco a forza di congurenze modulari, ho deciso di utilizzare tecniche a me più familiari, ovvero provare a ragionare in termini di polinomi.
Stabiliamo un pochino di linguaggio:

Definizione 0.1: Numeri e polinomi binari

Un numero ***binario in base*** β, o numero β***-binario***, è un numero della forma

$$\sum_{i=0}^{n} a_i \beta^i \qquad \text{con } a_i \in \{0, 1\}$$

Analogamente, un ***polinomio binario*** è un polinomio della forma

$$\sum_{i=0}^{n} a_i x^i \qquad \text{con } a_i \in \{0, 1\}$$

Definiremo $\mathbf{2}[x]$ l'insieme dei polinomi binari nella variabile x.

Possiamo vedere che quindi la congettura di Matilde riguarda i numeri 10-binari; procediamo a dimostrare il

Teorema 0.1: Teorema del treno per polinomi

Sia $p \in \mathbb{N}[x]$ di grado d tale che $p^2 \in \mathbf{2}[x]$.
Allora $p = x^d$ se $d \geq 0$, altrimenti $p = 0$.

Dimostrazione

I casi $d \in \{-\infty, 0\}$ sono banali, assumiamo $d \geq 1$ e scriviamo per esteso p e p^2:

$$p = \sum_{i=0}^{d} a_i x^i, \qquad p^2 = \sum_{k=0}^{2d} b_k x^k \quad \text{dove} \quad b_k = \sum_{i=0}^{k} a_i a_{k-i} \quad \text{e} \quad \forall j > d, a_j = 0$$

Dimostriamo prima che $p \in \mathbf{2}[x]$ (lemma della locomotiva) e successivamente che $p = x^d$ (lemma della ferrovia):

- Dato che abbiamo assunto la binarietà di p^2, per ogni k bisogna avere $b_k \in \{0, 1\}$, dunque deve esistere al più un i tale che $a_i a_{k-i} > 0$, poichè altrimenti b_k sarebbe maggiore di 1; inoltre, dato che l'unico caso in cui il prodotto di due numeri naturali è uguale a 1 è quello in cui questi sono entrambi uno, deve valere $a_i = a_{k-i} = 1$, dunque per ogni j deve valere $a_j \in \{0, 1\}$ e dunque $p \in \mathbf{2}[x]$.
- Per l'unicità di i vista nel punto precedente, deve valere anche $i = k - i$, ovvero $k = 2i$ e quindi b_k può essere uguale a 1 soltanto per k pari. Scriviamo quindi

$$p^2 = \sum_{k=0}^{d} b_{2k} x^{2k} \quad \text{con} \quad b_{2k} = \sum_{i=0}^{2k} a_i a_{2k-i}$$

Notiamo che abbiamo "gratis" $b_{2d} = 1$ e $b_0 = a_0^2$ e supponiamo per assurdo che per un qualche $0 < h < d$ si abbia $b_{2h} = 1$; questo significherebbe che $a_h = 1$ e che quindi $b_{d+h} \neq 0$, e in particolare

$$b_{d+h} = \sum_{i=0}^{d+h} a_i a_{d+h-i} = \underbrace{\sum_{i=0}^{h-1} a_i a_{d+h-i}}_{=0} + \underbrace{a_h a_d}_{=1} + \underbrace{\sum_{i=h+1}^{d-1} a_i a_{d+h-i}}_{\geq 0} + \underbrace{a_d a_h}_{=1} + \underbrace{\sum_{i=d+1}^{d+h+1} a_i a_{d+h-i}}_{\geq 0} \geq 2$$

assurdo per ipotesi di binarietà di p^2, dunque dobbiamo concludere che $b_{2h} = 0$ per ogni $0 < h < d$ e perciò $p^2 = x^{2d} + a_0$, ma dato che $x^{2d} + 1$ è irriducibile in $\mathbb{R}[x]$ chiaramente lo è anche in $\mathbb{N}[x]$ e ovviamente in $\mathbf{2}[x]$ e quindi $a_0 = 0$.

□

Prima di essere certi di averlo dimostrato per i numeri, ci serve il seguente lemma:

Lemma 0.1: Corrispondenza biunivoca tra polinomi binari e numeri β-binari

Sia $\beta \in \mathbb{N}_{\geq 2}$, sia $V_\beta : \mathbb{N}[x] \to \mathbb{N}$ l'omomorfismo di semianelli che manda p in $p(\beta)$. Allora:

1. La restrizione $V_\beta : \mathbf{2}[x] \to B_\beta$ è una mappa biettiva di insiemi.
2. Un $n \in B_\beta$ è un quadrato in $\mathbb{N}$ se e solo se $p = V_\beta^{-1}(n)$ è un quadrato in $\mathbb{N}[x]$

Dimostrazione

1. Il seguente diagramma commuta in **Set**:

$$\begin{tikzcd}
\mathbb{N}[x] \arrow[rr, "V_\beta"] & & \mathbb{N} \arrow[dd, leftrightarrow] \\
\mathbf{2}[x] \arrow[u, hook] \arrow[r, "V_\beta"] \arrow[dr, leftrightarrow] & B_\beta \arrow[ur, hook] \arrow[d, leftrightarrow] & \\
& \{0,1\}^\infty \arrow[r, hook] & \{0, ..., \beta - 1\}^\infty
\end{tikzcd}$$

   Dato che la restrizione di V_β è uguale alla composizione di due biezioni (la scrittura in base β e la sostituzione del simbolo β col simbolo x), è una biezione.

2. Assumiamo che $p = q^2$, allora banalmente $n = p(\beta) = q^2(\beta) = (q(\beta))^2$.
   Ora assumiamo che $n = p(\beta) = m^2$. Scriviamo p

$$p = \sum_{i=0}^{d} a_i x^i$$

Corollario 0.1: Teorema del treno per numeri β-binari

Sia p un quadrato perfetto β-binario.
Allora p è della forma β^{2n} per qualche $n \in \mathbb{N}$ oppure $p = 0$.

Dimostrazione

Scriviamo p in base β, vediamo le sue cifre come coefficienti di un polinomio $p(x) \in \mathbf{2}[x]$ e applichiamo il teorema del treno per polinomi, ottenendo che $p(x) = x^{2n}$ per qualche $n \in \mathbb{N}$ oppure $p(x) \equiv 0$.
Valutiamo $p(\beta)$ per ottenere $p = \beta^{2n}$ oppure $p = 0$.

□

Corollario 0.2: Calabri I

Gli unici numeri della forma $a_0 + 10a_1 + 100a_2 + ...$ con $a_i \in \{0, 1\}$ che sono quadrati perfetti sono della forma 10^{2k} per qualche $k \in \mathbb{N}$.

Dimostrazione

Applichiamo il teorema del treno per numeri β-binari nel caso $\beta = 10$.