Il Problema delle monete

La formula di Bezout implica che se a, b sono interi coprimi allora ogni intero (in particolare ogni intero positivo) n si scrive come

$$n = ua + vb$$

dove u, v sono numeri interi. Ovviamente, in una tale rappresentazione di n non è detto che u, v siano (o anche possano) essere non-negativi. Il problema di Frobenius (anche detto 'Problema delle monete') riguarda proprio rappresentazioni come somme a coefficienti non-negativi.

Tale questione ha un risvolto pratico abbastanza tangibile. Ad esempio: *quali cifre è possibile pagare avendo a disposizione tre tagli di monete* (diciamo, del valore di 6, 10 e 15 unità)? e simili cose...

Se avete provato a fare qualche tentativo con queste monete (dai tagli un po' improbabili) avrete forse trovato che ogni cifra $n > 29$ si può pagare, mentre 29 non è possibile. Cioè, per ogni $n > 29$ esistono interi non negativi x, y, z tali che $n = 6x + 10y + 15z$, mentre 29 non ammette una tale rappresentazione.

Questo fatto (l'esistenza cioè di una 'soglia' sopra la quale ogni intero si rappresenta con coefficienti non negativi) non è fortuito, come vedremo tra poco (Teorema 1). Prima, concordiamo la seguente semplificazione espositiva: fissati interi positivi $a_1, a_2, \ldots, a_k$, diciamo semplicemente che un intero $n \geq 0$ è *rappresentabile* se è rappresentabile come combinazione a coefficienti interi non negativi dei numeri $a_1, a_2, \ldots, a_k$.
Osserviamo il fatto, ovvio, che se S, R sono numeri rappresentabili, allora è rappresentabile anche ogni intero del tipo $nR + mS$, con n, m interi non negativi.

Teorema 1. *Siano $a_1, a_2, \ldots, a_k$ interi positivi con $MCD(a_1, a_2, \ldots, a_k) = 1$. Allora esiste un massimo intero positivo $g(a_1, \ldots, a_k)$ che non è rappresentabile.*

(Ad esempio, come notato sopra, $g(6, 10, 15) = 29$.)

Proof. Sia $a_1 \leq a_2 \leq \ldots \leq a_k$, e sia $n \in \mathbb{N}$. Poiché $MCD(a_1, a_2, \ldots, a_k) = 1$, esistono interi $z_1, z_2, \ldots, z_k$ tali che

$$1 = z_1 a_1 + z_2 a_2 + \ldots + z_k a_k.$$

Sia P la somma dei termini $z_i a_i$ che sono positivi (quindi z_i positivo), e $-Q$ la somma dei termini negativi (cioè tali che $z_i < 0$). Quindi $1 = P - Q$; e, chiaramente, P e Q sono rappresentabili.
Sia n intero con $n \geq a_1 Q$, e lo si divida per a_1: $n = h a_1 + r$ con $h \geq Q$ e $0 \leq r < a_1$. Allora

$$n = (h - Q)a_1 + Q a_1 + r(P - Q) = (h - Q)a_1 + rP + (a_1 - r)Q;$$

poiché $h - Q, r, a_1 - r$ sono interi non negativi e a_1, P, Q rappresentabile, n è rappresentabile. Dunque

$$g(a_1, \ldots, a_k) \leq a_1 Q - 1.$$

□

La dimostrazione mostra che $g(a_1, \ldots, a_k) \leq a_1 Q$, ma si tratta di stime più che abbondanti: ad esempio, nel caso $(6, 10, 15)$ dell'esempio di prima, il valore minimo

per Q si ricava dalla scrittura $1 = 1 \cdot 6 + 1 \cdot 10 - 1 \cdot 15$ ed $Q = 15$, per cui $a_1 Q = 6 \cdot 15 = 90$, che è ben più grande del valore preciso 29 trovato prima.

Il *Problema di Frobenius* consiste proprio nel determinare i valori esatti $g(a_1, \ldots, a_k)$. Formulato alla fine del diciannovesimo secolo è ancora in larga parte aperto[1]. Mentre per il caso $k = 2$ è piuttosto semplice trovare il valore $g(a_1, a_2)$ (la prima dimostrazione è di solito attribuita a Sylvester e apparve nel 1882), solo molto recentemente (2017) sono state trovate, da A. Tripathi, formule esplicite per i valori $g(a_1, a_2, a_3)$ (formule che sono troppo elaborate per essere riportate qui), anche se programmi efficienti per calcolarli erano noti da qualche decina d'anni. Per $k \geq 4$ molto poco è noto in generale, ad esclusione di casi piuttosto particolari. Esistono diverse limiti sia superiori che inferiori che funzionano più o meno bene a seconda dei casi; cito solo un risultato ormai classico di I. Schur, secondo il quale, se $1 < a_1 \leq a_2 \leq \cdots \leq a_k$ sono interi coprimi, allora $g(a_1, \ldots, a_k) \leq (a_1 - 1)(a_k - 1) - 1$.

Teorema 2 (Sylvester)**.** *Siano p, q interi non negativi e coprimi. Allora*

$$g(p, q) = pq - p - q.$$

Proof. Sia n un intero. Poiché p, q sono coprimi, esistono $x, y \in \mathbb{Z}$ tali che

$$n = xp + yq. \tag{1}$$

Se (x_1, y_1) è un'altra coppia di numeri interi tali che $x_1 p + y_1 q = n$, allora

$$(x - x_1)p = (y_1 - y)q$$

e, dunque, poiché p, q sono coprimi, $q \mid x - x_1$ (Lemma di Euclide). Viceversa, si vede subito che per ogni $z \in \mathbb{Z}$ la coppia $x_1 = x + qz$, $y_1 = y - pz$ è una soluzione di (1). Questo ci dice che tra le soluzioni (x, y) di (1) ce n'è una e una sola tale che $0 \leq x < q$. Sia (x, y) tale soluzione; ne segue che n è rappresentabile (ovvero (1) ammette soluzioni non-negative) se $y \geq 0$, e non è rappresentabile se $y < 0$. Il più grande caso non-rappresentabile si ottiene per $x = q - 1$ e $y = -1$, ovvero

$$(q - 1)p - q = qp - p - q.$$

Dunque, $g(p, q) = pq - p - q$. □

I problemi che seguono trattano due casi semplici per 3 interi.

Problema 1 (classico: Chicken McNuggets)**.** *Un certo prodotto alimentare viene venduto in confezioni che contengono $6, 9$ o 20 pezzi. Dire qual è il massimo numeri di pezzi che non è possibile acquistare.*

Soluzione. Si tratta di determinare $g(6, 9, 20)$. Cominciamo osservando che, poiché

$$g(3, 10) = 30 - 3 - 10 = 17,$$

ogni numero *pari* strettamente maggiore di 34 è rappresentabile come combinazione a coefficienti non negativi di 6 e 20. Sia $n > 43$ un numero dispari, allora $n - 9 > 34$ è un numero pari, quindi $n = (n - 9) + 9$ è rappresentabile in $6, 9, 20$. D'altra parte, poichè 43 è dispari, se fosse rappresentabile come $43 = 6x + 9y + 20z$, il coefficiente y deve essere un numero dispari; ma né $43 - 9 = 34$, nè $43 - 27 = 16$ sono rappresentabili in $6, 20$. Quindi, 43 non è rappresentabile in $6, 9, 20$. Dunque

$$g(6, 9, 20) = 43$$

[1] Si veda, ad esempio, J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem. Oxford University Press, 2005.

che è la risposta al problema. ∎

Problema 2. *Sia n un intero positivo pari; si provi che*

$$g(n, n+1, n+2) = \frac{n^2}{2} - 1.$$

SOLUZIONE. Sia n un intero positivo pari, e sia $k \geq \frac{n^2}{2}$. Allora, $k = qn + r$ con $q \geq \frac{n}{2}$ e $0 \leq r < n$. Poniamo $(b, c) = (0, \frac{r}{2})$ se r è pari, $(b, c) = (1, \frac{r-1}{2})$ se r è dispari; in ogni caso $b + 2c = r$ e $b + c \leq \frac{n}{2} \leq q$; poniamo infine $a = q - (b + c)$. Allora

$$an + b(n+1) + c(n+2) = (a+b+c)n + (b+2c) = qn + r = n,$$

dunque n è rappresentabile. Proviamo ora che $k = \frac{n^2}{2} - 1$ non è rappresentabile. Infatti, supponiamo per assurdo

$$\frac{n^2}{2} - 1 = an + b(n+1) + c(n+2) = (a+b+c)n + (b+2c)$$

cone $a, b, c \in \mathbb{N}$; allora $b + 2c \equiv -1 \pmod{n}$, e dunque $b + 2c \geq n - 1$. Ma allora

$$n - 1 \leq b + 2c \leq 2(a+b+c) \leq 2(n/2 - 1) = n - 2,$$

che è assurdo. Abbiamo quindi provato $g(n, n+1, n+2) = \frac{n^2}{2} - 1$. ∎