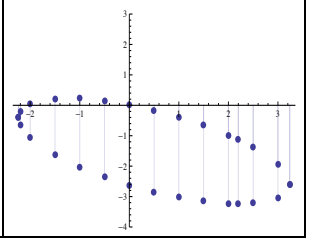
MatematicaMente

ISSN: 2037-6367



Pubblicazione mensile della sezione veronese della MATHESIS – Società Italiana di Scienze Matematiche e Fisiche – Fondata nel 1895 – Autorizzazione del Tribunale di Verona n. 1360 del 15 – 03 – 1999 – I diritti d'autore sono riservati. Direttore: Luciano Corso - Redazione: Alberto Burato, Elisabetta Capotosto, Carlo Marchiori, Giovanna Tessari – Via IV Novembre, 11/b – 37126 Verona – tel e fax (045) 8344785 – 338 6416432 – e-mail: lcorso@iol.it – Stampa in proprio - Numero 180 – Pubblicato il 05 – 7 – 2013

Una dimostrazione di tipo combinatorio del Piccolo Teorema di Fermat

di Alessio Russo [*]

1 Introduzione

Un procedimento tipico della matematica combinatoria consiste nel contare in due modi diversi gli elementi di un insieme finito allo scopo di ottenere, uguagliando i risultati, relazioni numeriche che prescindono dall'insieme di partenza e dai suoi elementi.

In questa nota, nell'ottica precedente, faremo vedere come, contando opportunamente il numero delle funzioni esistenti fra due insiemi finiti, sia possibile ottenere una facile dimostrazione di un ben noto risultato di teoria dei numeri: il *Piccolo Teorema di Fermat*. Quest'ultimo assicura che *se n è un numero primo, allora per ogni numero naturale m si ha che n è un divisore della differenza* $m^n - m$.

Il Piccolo Teorema di Fermat fu enunciato per la prima volta da Pierre de Fermat, che lo comunicò, senza darne esplicita dimostrazione, a Frènicle de Bessy il 18 ottobre del 1640.

Il risultato fu poi provato da Eulero nel 1736 utilizzando il Principio di Induzione e la Formula del Binomio di Newton (in realtà già nel 1683 Leibniz ne aveva fornito una dimostrazione, che però non fu mai pubblicata). Successivamente, sono state date anche altre dimostrazioni, alcune molto rapide, basate sull'*aritmetica modulare*, un settore della teoria dei numeri introdotto nel 1801 da Gauss, appena ventiquattrenne, nell'opera *Disquisitiones Arithmeticae* (cfr. ad esempio, [2]). Invece, la prima dimostrazione di tipo combinatorio è stata data da Golomb nel 1956 (cfr. [5]). Una versione simile a quella che qui riportiamo, ottenuta mediante gli anagrammi delle parole, si può trovare al seguente indirizzo internet:
www.unife.it/geometria/Mat2000/picfermat.htm.

Il Piccolo Teorema di Fermat, la cui scoperta è forse legata alla teoria dei cosiddetti *numeri perfetti* (cioè quei numeri naturali che hanno la proprietà di essere uguali alla somma dei loro divisori propri), negli ultimi decenni ha avuto delle sorprendenti applicazioni, sia per quanto riguarda la messa a punto di sofisticati test di primalità, sia nella realizzazione di quello che oggi è forse il sistema crittografico a chiave pubblica più utilizzato: il *crittosistema RSA* (cfr. [1], [3] , [6] e [7]).

2. Come possiamo contare le funzioni fra due insiemi finiti?

Cominciamo introducendo un po' di terminologia e di notazioni. Siano S e T insiemi finiti di ordini rispettivamente n ed m, ed indichiamo con T^S l'insieme di tutte le funzioni di S in T. Un primo modo di contare gli elementi dell'insieme T^S si ottiene mediante una semplice applicazione del Principio di Induzione.

Proposizione 2.1 *L'insieme* T^S *è finito e ha ordine* m^n.

DIMOSTRAZIONE – Ragioniamo per induzione su n. Se $n = 1$ esistono ovviamente m funzioni di S in T, e quindi T^S è un insieme finito di ordine $m^1 = m$. Sia $n > 1$, e sia x un elemento di S. Assumiamo per induzione che $T^{S\setminus\{x\}}$ sia un insieme finito di ordine m^{n-1}. D'altra parte, se f è un elemento di $T^{S\setminus\{x\}}$, allora esistono m prolungamenti di f su S. Ne segue che T^S è un insieme finito di ordine $m \cdot m^{n-1} = m^n$.

Poiché per la Proposizione 2.1 l'ordine di T^S non cambia se si sostituisce S con un altro insieme finito avente n elementi, allora è lecito porre $S=\{1, 2, \ldots, n\}$.

Ciò premesso, sia $f : S \to T$ una funzione di S in T. Se si pone $y_j = f(j)$, per ogni $j \in S$, allora f determina la n-pla ordinata $(y_1, y_2, \ldots, y_n)$. Chiameremo quest'ultima *la n-pla ordinata associata ad f*. È ovvio che le funzioni di S in T sono in corrispondenza biunivoca con le n-ple ordinate di elementi di T. Se Y è il *codominio* di f, cioè l'insieme delle immagini degli elementi di S tramite f, allora, considerato un $y \in Y$, diciamo *frequenza* di y la cardinalità r_y dell'insieme $\{j \in S \mid f(j) = y\}$. Pertanto, r_y è il numero degli elementi della n-pla ordinata $(y_1, y_2, \ldots, y_n)$ uguali ad y. Chiaramente la somma delle frequenze degli elementi di Y è n. Cerchiamo ora di scrivere il numero m^n delle funzioni di S in T in modo diverso. Osserviamo innanzitutto che se f è una funzione di S in T avente per codominio un sottoinsieme T_k di T di ordine k, allora è facile rendersi conto che $k \le n$ e che $r_y \le n - k + 1$, per ogni $y \in T_k$. Ciò premesso, denotiamo con μ il più piccolo fra m e n. Siano poi i un intero positivo tale che $i \le \mu$ e T_i un *arbitrario* sottoinsieme di ordine i di T. Definiamo *funzione di frequenze* relativa all'insieme T_i, ogni applicazione $v : T_i \to \{1, \ldots, n - i + 1\}$ tale che

$$\sum_{y\in T_i} v(y) = n .$$

Quante funzioni suriettive esistono di S in T_i tali che per ogni $y \in T_i$ la frequenza $r_y = v(y)$? Per rispondere a tale domanda, sia $(y_1, y_2, \ldots, y_n)$ la n-pla ordinata associata ad una funzione f di questo tipo. Occorre capire come possiamo collocare gli elementi di T_i negli n spazi in modo da ottenere le frequenze definite dalla funzione v. Permutiamo gli elementi di tale n-pla in tutti i modi possibili. Se partiamo da y_1 abbiamo n possibilità di collocarlo negli n spazi di cui disponiamo. Sistemato y_1 è chiaro che per y_2 avremo $n - 1$ possibilità, mentre per y_3 ne restano $n–2$, e così via per gli altri elementi. Ciò significa che vi sono in tutto $n!$ modi di permutare gli elementi della nostra n-pla. Poiché nella n-pla $(y_1, y_2, \ldots, y_n)$ associata ad f vi possono essere degli elementi che si ripetono (e ciò è legato alla funzione v), è chiaro che il numero delle n-ple distinte ottenute mediante tutte le permutazioni è in generale minore di $n!$. Questo accade perché tutte quelle permutazioni che scambiano di posto elementi uguali della n-pla $(x_1, x_2, \ldots, x_n)$ non danno luogo a nuove funzioni. Le considerazioni precedenti mostrano che il numero di funzioni suriettive di S in T_i tali che la frequenza $r_y = v(y)$ per ogni $y \in T_i$ è data da

$$\frac{n!}{\prod_{y\in T_i} v(y)!} .$$

In particolare, per $i = 1$ il precedente numero vale 1, poiché $v(y) = n$. Sia $N(T_i)$ l'insieme delle funzioni di frequenze relative a T_i. Allora il numero delle funzioni suriettive di S in T_i è il seguente:

$$\sum_{v\in N(T_i)} \frac{n!}{\prod_{y\in T_i} v(y)!} .$$

A questo punto, per procedere occorre determinare il numero dei sottoinsiemi di ordine i ($\le \mu$) di T. A tale scopo ricordiamo alcune definizioni. Si chiama *coefficiente binomiale* di μ rispetto ad i, e si denota col simbolo

$$\binom{\mu}{i},$$

la frazione

$$\frac{\mu!}{i!(\mu-i)!}.$$

Si pone inoltre

$$\binom{\mu}{0}=1.$$

È facile provare che risulta:

$$\binom{\mu}{i}+\binom{\mu}{i-1}=\binom{\mu+1}{i}.$$

Ciò premesso si ha:

Lemma 2.2 *Siano μ ed i numeri interi positivi tali che $i \le \mu$, e sia V un insieme finito di ordine μ. Allora il numero dei sottoinsiemi di V di ordine i è il coefficiente binomiale*

$$\binom{\mu}{i}.$$

DIMOSTRAZIONE – Ragioniamo per induzione su μ. Se $\mu = i$, allora chiaramente V ha un unico sottoinsieme di ordine i, e

$$\binom{\mu}{i}=\binom{i}{i}=1.$$

In particolare l'asserto è vero se $\mu = 1$.
Inoltre, se $i = 1$ il numero di parti di ordine i di V è ovviamente

$$\mu=\binom{\mu}{1}.$$

Pertanto possiamo assumere che $1 < i < \mu$. Fissiamo ora un elemento v di V. Per l'ipotesi d'induzione, il numero delle parti di ordine i di $V\setminus\{v\}$ è

$$\binom{\mu-1}{i}.$$

D'altra parte, ancora per l'induzione, l'insieme $V\setminus\{v\}$ ha

$$\binom{\mu-1}{i-1}$$

sottoinsiemi di ordine $i-1$, sicché v sta in

$$\binom{\mu-1}{i-1}$$

sottoinsiemi di V di ordine i. Pertanto il numero di parti di V d'ordine i è

$$\binom{\mu-1}{i}+\binom{\mu-1}{i-1}=\binom{\mu}{i},$$

e ciò prova l'asserto.
Con le notazioni prima introdotte, il Lemma 2.2 ci assicura che il numero delle applicazioni di S in T che hanno per codominio un sottoinsieme di ordine $i \le \mu$ di T è

$$\binom{\mu}{i}\sum_{v\in N(T_i)}\frac{n!}{\prod_{y\in T_i}v(y)!}$$

dove ora T_i è il *generico* sottoinsieme di ordine $i \le \mu$ di T.
Possiamo dunque enunciare il seguente risultato:

Proposizione 2.3 *Siano S e T insiemi finiti non vuoti di ordini rispettivamente n ed m, e sia $\mu = \min\{m, n\}$. Se per ogni $i \in \{1, \ldots, \mu\}$ denotiamo rispettivamente con T_i il generico sottoinsieme di ordine i di T e con $v : T_i \to \{1, \ldots, n - i + 1\}$ una funzione di frequenze relativa a T_i, allora il numero delle applicazioni di S in T è dato dalla formula*

$$\sum_{i=1}^{\mu}\left[\binom{\mu}{i}\sum_{v\in N(T_i)}\frac{n!}{\prod_{y\in T_i}v(y)!}\right].$$

Osserviamo che il risultato precedente si poteva anche ottenere direttamente utilizzando la *formula di Leibnitz* che fornisce lo sviluppo della potenza di una somma (cfr. [4], pp. 64-67).

3. Un'applicazione: Il Piccolo Teorema di Fermat

La Proposizione 2.1 e la Proposizione 2.3 ci hanno fornito due modi diversi per scrivere il numero delle applicazioni fra due insiemi finiti S e T di ordini n ed m rispettivamente. Poiché per $i = 1$ si ottengono le m applicazioni costanti di S in T, allora è chiaro che sussiste la seguente formula:

$$m^n - m = \sum_{i=2}^{\mu}\left[\binom{\mu}{i}\sum_{v\in N(T_i)}\frac{n!}{\prod_{y\in T_i}v(y)!}\right].$$

Cosa diventa la formula precedente nel caso in cui n è un numero primo? Poiché gli unici divisori positivi di n sono 1 ed n ed inoltre ogni $v(y) < n$, allora è chiaro che ogni

$$\frac{n!}{\prod_{y\in T_i}v(y)!}$$

è un *multiplo* di n, sicché tale è anche la differenza $m^n - m$. Abbiamo così dimostrato il seguente risultato.

3.1 (Piccolo Teorema di Fermat)

Sia n un numero primo. Allora, per ogni numero naturale m, si ha che n è un divisore di $m^n - m$.

Si osservi che utilizzando il risultato precedente, si ha subito che n è un divisore di $m^n - m$ per ogni numero *intero* m. Inoltre, il Piccolo Teorema di Fermat si può enunciare equivalentemente dicendo che *n è un numero primo, allora n è divisore di $m^{n-1} - 1$ per ogni intero m non divisibile per n.*

(Pierre de Fermat 1601-1665)

Bibliografia: [1] L. Berardi – A. Beutelspacher: *Come rendere sicura la posta elettronica*, Archimede, **3**(1999), 137-143. [2] T. P. Dence - J.B. Dence: *Elements of the Theory of Numbers*, Academic Press, San Diego (1998). [3] K. Devlin: *Dove va la matematica*, 2ª ed., Bollati Boringhieri, Torino (1998). [4] A. Franchetta: *Algebra lineare e geometria analitica*, Liguori, Napoli (1984). [5] S.W. Golomb: *Combinatorial Proof of Fermat's 'Little' Theorem*", Amer. Math. Monthly, **63**(1956), 718. [6] A. Russo, *Il Piccolo Teorema di Fermat e la Crittografia*, Periodico di Matematiche, **2/3** (2007), 109-121. [7] S. Singh: *Codici & Segreti*, 1ª ed., Rizzoli, Milano (1999).

[*] Dipartimento di Matematica e Fisica - Seconda Università di Napoli, Viale Lincoln 5, 81100 Caserta - e-mail: alessio.russo@unina2.it