

**Numeri Perfetti:
gioco, estetica e pragmatica**

Andrea Previtali

Menaggio, 16 Maggio 2003

Protagonisti

Già Euclide (325-265 a.c.) aveva definito il concetto di "essere divisibile", numero primo e divisori di un numero intero. Formalizziamo questi concetti.

Dati due interi a, b dico che b **divide** a se $a = bc$, per qualche intero c , e scrivo $b|a$. b viene anche detto un **divisore** di a .

Un numero p si dice **primo** se ammette solo 1 e p come divisori.

Un numero che non è primo si dice **composto**.

Esempio: 2, 3, 5, 7, 11, 13 sono primi, mentre 4, 6, 8, 9, 12 sono composti.

Teorema Fondamentale dell'Aritmetica

Sempre Euclide aveva capito che i numeri primi sono i **mattoni** necessari alla costruzione di tutti gli interi. Infatti vale il **Teorema Fondamentale dell'Aritmetica**

Teorema 1 (Euclide). *Ogni intero si scrive in un ed un SOLO modo come prodotto di primi.*

Allora è importante sapere affrontare il seguente

Problema: quanti sono i numeri primi?

Avete provato a indovinare?

Tentiamo qualche esperimento. 2 è primo.

$3 = 2 + 1$ è primo. ATTENZIONE $4 = 3 + 1$ non è primo. Ma $7 = 2 \cdot 3 + 1$ lo è.

Quanti Primi?

Cosa accade a $2 \cdot 3 \cdot 5 + 1$? Anche lui è primo. Quindi questi esperimenti potrebbero condurci a pensare che se ho un po' di primi, ne faccio il prodotto e sommo 1 ottengo un NUOVO primo.

Ma $3 \cdot 5 + 1 = 16$ è composto. Forse devo prendere TUTTI i numeri primi minori di un certo intero.

Ora è più delicato capire cosa accade, ma ancora otteniamo numeri composti, ad esempio

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$, ove 59 e 509 sono primi.

L'**algoritmo**, ossia la procedura di calcolo, qui delineata ci conduce a infiniti primi.

Teorema 2 (Euclide). *I numeri primi sono infiniti.*

Se fossero in numero finito, sia n l'intero che ottengo sommando 1 al loro prodotto. Sia p un divisore primo di n , allora p è un primo diverso dai precedenti, quindi i numeri primi sono infiniti.

Numeri Perfetti

Dato un intero n sia $\sigma(n)$ la **somma dei suoi divisori**. In particolare $\sigma(2) = 3 < 2 \cdot 2$,
 $\sigma(6) = 2 \cdot 6$ e $\sigma(12) > 2 \cdot 12$.

Definiamo un numero n **perfetto** se $\sigma(n) = 2n$.
Quindi 6 è un numero perfetto, anzi è il minimo numero perfetto.

Ce ne sono altri?

Potremmo cominciare una ricerca esaustiva, ossia provare tutti i numeri uno dopo l'altro. L'uso di linguaggi di calcolo come Maple ci mostrano in circa 70 secondi che gli unici numeri perfetti minori di 10000 sono 6, 28, 498, 8128.

Vedi una regola?

Sembrano pochi, solo 4 su 10000.

Sono tutti pari.

Visto che essere perfetto dipende dai divisori del numero consideriamo la loro fattorizzazione in primi:

$$2 \cdot 3, 2^2 \cdot 7, 2^4 \cdot 31, 2^6 \cdot 127.$$

Quindi non solo i pochi esempi sono pari ma risultano essere divisibili per elevate potenze di 2.

Possiamo dire qualcosa degli esponenti? Questi sono 1, 2, 4, 6. Se sommo 1 ottengo 2, 3, 5, 7
ESATTAMENTE i primi 4 numeri primi!!

Vedi una regola?

E il secondo fattore? Questi sono 3, 7, 31, 127. Se sommo 1 ottengo $2^2, 2^3, 2^5, 2^7$.

Ossia i primi 4 numeri perfetti sono della forma

$$2^{p-1} \cdot (2^p - 1)$$

con p primo.

Forse ci siamo. Proviamo con $p = 11$, purtroppo $2^{10} \cdot (2^{11} - 1)$ non è perfetto. Ora 3, 7, 31, 127 sono primi, mentre $2^{11} - 1 = 23 \cdot 89$. Forse il motivo del nostro fallimento si trova qui.

Dato l'intero n , definiamo $M(n) = 2^n - 1$

l'ennesimo **numero di Mersenne** in onore del frate Mersenne (1588-1648) che per primo li studiò.

I primi di Mersenne

Mostriamo che $M(n)$ è primo solo se n è primo.

Infatti se $n = ab$, con $a, b > 1$, allora

$M(n) = (u - 1)(u^{b-1} + u^{b-2} + \dots + u + 1)$, ove $u = 2^a$. In particolare $M(n)$ ammette due fattori propri.

Attenzione $M(11) = 23 \cdot 89$ NON è primo, quindi n primo NON implica $M(n)$ primo.

I numeri perfetti pari

Ora mostriamo che l'interesse per i primi di Mersenne è giustificato. Infatti Eulero (1707-1783), il più prolifico matematico di tutti i tempi (la sua Opera Omnia consiste di 22 volumi), ha provato **Teorema 3 (Eulero)**. *Sia n un numero perfetto pari, allora*

$$n = 2^{p-1} \cdot (2^p - 1),$$

dove $2^p - 1$ è un primo di Mersenne. In particolare p è primo.

Infatti se $n = 2^{p-1}q$, ove $q = 2^p - 1$ è primo, allora i divisori di n sono 2^i e $2^i q$, ove $i = 0, \dots, p - 1$.

Sia $S = 1 + 2 + \dots + 2^{p-2} + 2^{p-1}$, allora

$S = 2S - S = 2^p - 1 = q$. Quindi la somma dei divisori di n vale $q + q^2 = q(q + 1) = 2n$.

Viceversa sia $n = 2^{p-1}q$ perfetto con q dispari.

Allora $2n = 2^p q = (2^p - 1)\sigma(q)$. Per cui

$\sigma(q) = \frac{2^p q}{2^p - 1} = q + \frac{q}{2^p - 1}$. Entrambe gli addendi

sono divisori di q . Quindi q ammette solo due

divisori. Allora q è primo e $q = 2^p - 1$. In

particolare p è primo.

E quelli dispari?

Ripetuti sforzi non hanno tuttora prodotto un numero perfetto dispari, anzi i risultati che ora elencherò supportano la congettura enunciata da Sylvester (1814-1897) che

Non esistono numeri perfetti dispari.

Sia n un numero perfetto dispari.

1. n ammette almeno 29 fattori primi;
2. uno di questi supera 10^{20} ;
3. $n > 10^{300}$.