

Somme di Interi Consecutivi

Numeri di Mersenne e Numeri di Fermat

Umberto Cerruti
Università di Torino

Somme di interi consecutivi e divisori dispari

Le somme dei primi m interi consecutivi sono i numeri triangolari T_m , studiati fin dall'antichità.

Ci domandiamo che cosa accade se consideriamo somme di interi consecutivi che iniziano da un generico h , ovvero somme del tipo

$$n = h + (h + 1) + (h + 2) + \cdots + (h + t) \quad h \geq 1, \quad t \geq 0 \quad (1)$$

Per ogni intero n esiste almeno una espressione di n come somma di interi consecutivi, quella, che diciamo *banale*, data da $h = n$ e $t = 0$

Esistono sempre altre espressioni? Quante sono e come si trovano?

Per rispondere a queste e altre domande, cominciamo col fissare alcune notazioni.

Nel seguito, invece di dire *u è espressione di n come somma di interi consecutivi*, diremo semplicemente *u è una sic di n* .

Una sic è determinata completamente dal *punto di inizio* h , che deve essere un intero strettamente positivo, e dallo *spostamento* t , un intero non negativo. Una sic ν con inizio h e spostamento t darà denotata con

$$\nu = (h, t) \quad (2)$$

La sic ν rappresenta il numero n che è somma dei $t + 1$ interi compresi tra h e $h + t$, estremi inclusi.

Con queste notazioni la sic banale di n è $(n, 0)$. Se n è dispari, n possiede una seconda sic ovvia: $(\frac{n-1}{2}, 1)$. Diciamo *mediana* questa sic.

Denotiamo con \mathcal{S} l'insieme di tutte le sic e con $\mathcal{S}(n)$ l'insieme delle sic di n .

$$\mathcal{S} = \cup_{n=1}^{\infty} \mathcal{S}(n) \quad (3)$$

Da quanto detto segue che $\mathcal{S}(n)$ non è mai vuoto, contiene almeno la sic banale. Inoltre se n è dispari, $\mathcal{S}(n)$ contiene almeno due elementi, la sic banale e quella mediana.

Viene allora da chiedersi se ci sono interi dispari le cui sic sono soltanto quella banale e quella mediana, e se ci sono interi pari che possiedono solamente la sic banale.

Il problema di scrivere un numero come somma di interi consecutivi è evidentemente un problema di tipo additivo. E' sorprendente constatare che esiste un legame strettissimo tra queste somme e la struttura moltiplicativa degli interi.

Vedremo, per esempio, che i numeri primi sono i soli interi dispari che hanno due sole sic, così come sono i soli interi ad avere esattamente due divisori.

Prima di proseguire diamo ancora un paio di definizioni. Denoteremo con \mathcal{D} l'insieme formato dalle coppie di interi (n, d) dove n è un intero maggiore di zero, e d è un *divisore dispari* di n

$$\mathcal{D} = \{(n, d) : n \geq 1, d \text{ è un divisore dispari di } n\} \quad (4)$$

Il simbolo $\mathcal{D}(n)$ denoterà l'insieme delle coppie (n, d) , dove n è fissato e d è un divisore dispari di n . Per esempio

$$\mathcal{D}(45) = \{(45, 1), (45, 3), (45, 5), (45, 9), (45, 15), (45, 45)\} \quad (5)$$

Ovviamente

$$\mathcal{D} = \cup_{n=1}^{\infty} \mathcal{D}(n) \quad (6)$$

Introduciamo anche la funzione γ , che manda la sic $\nu = (h, t)$ nel naturale n che essa rappresenta

$$\begin{cases} \gamma : \mathcal{S} \longrightarrow \mathbb{N} \\ \gamma(\nu) = \gamma(h, t) = \sum_{j=0}^{j=t} (h + j) = n \end{cases} \quad (7)$$

Per esempio se $\nu = (6, 8)$

$$\gamma(\nu) = \gamma(6, 8) = 6 + 7 + \dots + 14 = 90 \quad (8)$$

Ricordiamo infine la formula che ci dà la somma dei primi m interi consecutivi

$$\sum_{j=1}^m j = \frac{m(m+1)}{2} \quad (9)$$

Il seguente Teorema ci permette di costruire una corrispondenza molto interessante tra \mathcal{S} e \mathcal{D} .

Teorema 1 *Sia data la sic $\nu = (h, t) \in \mathcal{S}$, e supponiamo $\gamma(h, t) = n$, ovvero*

$$n = \sum_{j=0}^t (h + j) = h + (h + 1) + (h + 2) + \cdots + (h + t) \quad (10)$$

Allora se t è pari (cioè se n è somma di un numero dispari di interi consecutivi) abbiamo

$$n = (t + 1)\left(h + \frac{t}{2}\right) \quad (11)$$

Altrimenti, se t è dispari (ovvero se n è somma di un numero pari di interi consecutivi)

$$n = (2h + t)\frac{t + 1}{2} \quad (12)$$

Dimostrazione.

La (10) si riscrive immediatamente così

$$n = (t + 1)h + \sum_{j=1}^t j \quad (13)$$

Da questa, utilizzando la 9 si ricava

$$n = (t + 1)h + \frac{t(t + 1)}{2} \quad (14)$$

Se t è pari possiamo raccogliere $(t + 1)$ e otteniamo la (11). In questo caso $t + 1$ è un fattore dispari di n .

Se t è dispari possiamo raccogliere $\frac{t+1}{2}$ e otteniamo la (12). In questo caso $2h + t$ è un fattore dispari di n . ■

Ricapitolando, data la sic $\nu = (h, t)$

- se t è pari allora $t + 1$ è un divisore dispari di $n = \gamma(\nu)$, e pertanto $(\gamma(n), t + 1) \in \mathcal{D}$
- se t è dispari allora $2h + t$ è un divisore dispari di $n = \gamma(\nu)$, e pertanto $(\gamma(n), 2h + t) \in \mathcal{D}$

Questo ci permette di definire la preannunciata funzione tra \mathcal{S} e \mathcal{D} , che chiamiamo ψ .

$$\left\{ \begin{array}{l} \psi : \mathcal{S} \longrightarrow \mathcal{D} \\ \left\{ \begin{array}{l} \psi(h, t) = (\gamma(h, t), t + 1) \quad \text{se } t \text{ è pari} \\ \psi(h, t) = (\gamma(h, t), 2h + t) \quad \text{se } t \text{ è dispari} \end{array} \right. \end{array} \right. \quad (15)$$

Nel Teorema seguente si determina la funzione θ inversa della ψ .

Teorema 2 *Sia data la coppia $(n, d) \in \mathcal{D}$. Si ponga $d = s + 1$ e $k = \frac{n}{d}$.*

Si definisca y così

1. *Se $k > \frac{s}{2} \Rightarrow y = (k - \frac{s}{2}, s)$*

2. *Se $k \leq \frac{s}{2} \Rightarrow y = (\frac{s}{2} - k + 1, 2k - 1)$*

Allora, in entrambi i casi, si ha che y appartiene a $\mathcal{S}(n)$ e $\psi(y) = (n, d)$.

Dimostrazione.

Si noti che poichè d è dispari, s è pari.

Caso 1.

Osserviamo che $y = (h, t) \in \mathcal{S}$ in quanto $h = k - \frac{s}{2} > 0$ e $t = s \geq 0$. La somma $\gamma(k - \frac{s}{2}, s)$ della sic y è

$$\gamma(k - \frac{s}{2}, s) = (k - \frac{s}{2}) + (k - \frac{s}{2} + 1) + \cdots + k + \cdots + (k + \frac{s}{2} - 1) + (k + \frac{s}{2})$$

La somma è formata da $s + 1$ addendi, dei quali $\frac{s}{2}$ alla sinistra e $\frac{s}{2}$ alla destra del k centrale. La somma di due addendi simmetrici rispetto a k è $2k$. Quindi la somma di tutti gli addendi è

$$\gamma(h, t) = \frac{s}{2}(2k) + k = k(s + 1) = kd = n$$

e $y \in \mathcal{S}(n)$. Calcoliamo $\psi(y) = \psi(h, t)$. Poichè t è pari, per definizione (15) si ha $\psi(h, t) = (\gamma(h, t), t + 1) = (n, d)$.

Caso 2.

Anche in questo caso $y = (h, t) \in \mathcal{S}$ in quanto $h = \frac{s}{2} - k + 1 > 0$, e anche $t = 2k - 1$ è positivo.

La somma $\gamma(\frac{s}{2} - k + 1, 2k - 1)$ della sic y è

$$\gamma(\frac{s}{2} - k + 1, 2k - 1) = (\frac{s}{2} - k + 1) + (\frac{s}{2} - k + 2) + \cdots + (\frac{s}{2} + k - 1) + (\frac{s}{2} + k)$$

La somma è formata da $t + 1 = 2k$ addendi. La somma di ogni coppia di addendi simmetrici rispetto al centro vale $s + 1$. Quindi la somma di tutti gli addendi è

$$\gamma(h, t) = k(s + 1) = kd = n$$

e $y \in \mathcal{S}(n)$. Calcoliamo $\psi(y) = \psi(h, t)$. Poichè t è dispari, per definizione (15) si ha

$$\psi(h, t) = (\gamma(h, t), 2h+t) = (n, 2(\frac{s}{2}-k+1)+(2k-1)) = (n, s-2k+2+2k-1) = (n, s+1) = (n, d)$$

■

Il Teorema 2 ci permette di definire la funzione θ tra \mathcal{D} e \mathcal{S}

$$\left\{ \begin{array}{l} \theta : \mathcal{D} \longrightarrow \mathcal{S} \\ \left\{ \begin{array}{l} \theta(n, d) = (\frac{n}{d} - \frac{d-1}{2}, d-1) \quad \text{se } \frac{n}{d} > \frac{d-1}{2} \\ \theta(n, d) = (\frac{d-1}{2} - \frac{n}{d} + 1, \frac{2n}{d} - 1) \quad \text{se } \frac{n}{d} \leq \frac{d-1}{2} \end{array} \right. \end{array} \right. \quad (16)$$

Nel Teorema 2 si è provato che

$$\forall (n, d) \in \mathcal{D} \quad \psi(\theta(n, d)) = (n, d) \quad (17)$$

Dimostriamo ora che la ψ e la θ sono proprio l'una inversa dell'altra. Ci manca soltanto una parte

Teorema 3

$$\forall (h, t) \in \mathcal{S} \quad \theta(\psi(h, t)) = (h, t)$$

Dimostrazione. Vista la definizione (15) di ψ , dobbiamo distinguere due casi.

Caso 1: t pari

In questo caso $\psi(h, t) = (\gamma(h, t), t + 1) = (n, d) \in \mathcal{D}$ (per la definizione di ψ (15)).

Quindi $d = t + 1$ e $n = \gamma(h, t) = (h + \frac{t}{2})d$ (vedi la dimostrazione del Teorema 1). Pertanto, ricordando che $h \geq 1$

$$\frac{n}{d} = h + \frac{t}{2} > \frac{t}{2} = \frac{d-1}{2}$$

e, per definizione (16),

$$\theta(n, d) = (\frac{n}{d} - \frac{d-1}{2}, d-1) = (h + \frac{t}{2} - \frac{t}{2}, t) = (h, t)$$

Caso 2: t dispari

In questo caso $\psi(h, t) = (\gamma(h, t), 2h + t) = (n, d) \in \mathcal{D}$ (per la definizione di ψ (15)).

Quindi $d = 2h + t$ e $n = \gamma(h, t) = (\frac{t+1}{2})d$ (vedi la dimostrazione del Teorema (1)). Pertanto, ricordando che $h \geq 1$

$$\frac{n}{d} = \frac{t+1}{2} \leq \frac{2h+t-1}{2} = \frac{d-1}{2}$$

e, per definizione (16),

$$\theta(n, d) = \left(\frac{d-1}{2} - \frac{n}{d} + 1, \frac{2n}{d} - 1\right) = \left(\frac{2h+t-1}{2} - \frac{t+1}{2} + 1, 2\left(\frac{t+1}{2}\right) - 1\right) = (h, t)$$

■

Prima di trarre le conclusioni, due utili Lemmi, che ci fanno comprendere meglio la funzione θ .

Lemma 4 *Siano dati un intero positivo n ed un suo divisore dispari d . Le seguenti condizioni sono equivalenti*

1. $\theta(n, d) = (h, t)$ con t pari
2. $\frac{n}{d} > \frac{d-1}{2}$
3. $d < \sqrt{2n}$

Dimostrazione. Dimostreremo il Lemma mediante una sequenza di implicazioni.

- 1. \Rightarrow 2.

Sappiamo dal Teorema 3 che se t è pari allora siamo nel Caso 1 e

$$\frac{n}{d} > \frac{d-1}{2}$$

- 2. \Rightarrow 3.

Dalla ipotesi segue che $\frac{2n}{d} > d - 1$. Ora $\frac{2n}{d}$ e $d - 1$ sono entrambi pari, e perciò si deve avere

$$\frac{2n}{d} > d$$

Pertanto $2n > d^2$ e infine $d < \sqrt{2n}$

Le due implicazioni si invertono immediatamente. ■

Naturalmente valgono anche le equivalenze simmetriche

Lemma 5 *Siano dati un intero positivo n ed un suo divisore dispari d . Le seguenti condizioni sono equivalenti*

1. $\theta(n, d) = (h, t)$ con t dispari
2. $\frac{n}{d} \leq \frac{d-1}{2}$
3. $d > \sqrt{2n}$

Si noti che non si può mai avere $d = \sqrt{2n}$, perchè altrimenti d sarebbe pari. ■

Possiamo affermare che i divisori dispari d di un intero n si dividono in due categorie, quelli minori di $\sqrt{2n}$ e quelli maggiori. Diciamo che d è di *prima specie* se $d < \sqrt{2n}$, e diciamo che d è di *seconda specie* nel caso contrario. Pertanto se d è di prima specie avremo che $\frac{n}{d} > \frac{d-1}{2}$ e la sic corrispondente $\nu = \theta(n, d)$ è una somma di un numero *dispari* di interi consecutivi (in quanto t è pari). Viceversa se d è di seconda specie avremo che $\frac{n}{d} \leq \frac{d-1}{2}$ e la sic corrispondente $\nu = \theta(n, d)$ è una somma di un numero *pari* di interi consecutivi.

Possiamo ora rispondere alle domande che siamo posti all'inizio.

Teorema 6 *Le seguenti affermazioni sono conseguenze dirette dei Teoremi precedenti.*

1. *Le sic di un intero positivo n sono tante quante i divisori dispari di n . Esse si trovano tutte applicando la funzione θ alle coppie (n, d) dove d è un divisore dispari di n .*
2. *I numeri che possiedono una sola sic sono quelli con un solo divisore dispari (che ovviamente è 1): essi sono le potenze di 2. Se $n = 2^k$ allora l'unica sic di n è quella banale $(n, 0)$.*
3. *I numeri che possiedono due sole sic sono quelli con esattamente due divisori dispari (che sono 1 e un primo dispari p): essi sono il prodotto di una potenza di 2 per un primo dispari p , $n = 2^k p$. Se n pari (cioè $k > 0$) allora si distinguono due casi*

- $n = 2^k p$ e $2^{k+1} > p$

Ovviamente n ha la sic banale $(n, 0) = \theta(n, 1)$. L'altra sic è $\theta(n, p)$.

L'ipotesi $2^{k+1} > p$ implica che p è un divisore di prima specie. Quindi

$$\theta(n, p) = \left(\frac{n}{p} - \frac{p-1}{2}, p-1 \right) = \left(2^k - \frac{p-1}{2}, p-1 \right)$$

- $n = 2^k p$ e $2^{k+1} < p$

L'ipotesi $2^{k+1} < p$ implica che p è un divisore di seconda specie. Quindi, in questo caso, la sic non banale è

$$\theta(n, p) = \left(\frac{p-1}{2} - \frac{n}{p} + 1, 2\frac{n}{p} - 1 \right) = \left(\frac{p-1}{2} - 2^k + 1, 2^{k+1} - 1 \right)$$

4. Se n ha due sole sic ed è dispari allora n è un primo, $n = p$. Le due sic di p sono quella banale, $(p, 0) = \theta(p, 1)$ e la mediana $(\frac{p-1}{2}, 1) = \theta(p, p)$

■

Esempio 7

- $n = 64$ ha una sola sic: $(64, 0)$
- $n = 6592 = 64 \times 103$ ha due sic: $(6592, 0)$ e $(13, 102)$. Questo significa che

$$6592 = \sum_{j=0}^{j=102} (13 + j)$$

- $n = 3296 = 32 \times 103$ ha due sic: $(3296, 0)$ e $(20, 63)$. Questo significa che

$$3296 = \sum_{j=0}^{j=63} (20 + j)$$

- $n = 103$ ha due sic: $(103, 0)$ e $(51, 1)$.

Nella crittografia moderna sono importanti le cosiddette *one way function*, che sono funzioni facili da calcolare ma estremamente difficili da invertire.

La funzione γ (7) appartiene certamente a questa categoria.

Provi il lettore a rispondere alla domanda seguente.

Dato l'intero N

$N = 3905279202468481885666859638198606408046444679425424993577869896088409414237$

trovare (h, t) non banale tale che

$$\gamma(h, t) = N$$

Equivalentemente: trovare due interi h e t , con $t \geq 0$, $h > 0$, $h \neq N$ e $h \neq \frac{N-1}{2}$ tali che

$$N = \sum_{j=0}^{j=t} (h + j)$$

Numeri primi di Mersenne e numeri primi di Fermat

Premettiamo alcuni Lemmi.

Lemma 8 *Siano q e s due interi positivi. Se $s = a \times b$ con a dispari allora $q^b + 1$ divide $q^s + 1$.*

Dimostrazione. Banalmente $q^b \equiv -1 \pmod{q^b + 1}$. Poichè a è dispari $(q^b)^a \equiv -1 \pmod{q^b + 1}$, ovvero $q^s + 1 \equiv 0 \pmod{q^b + 1}$. Questo significa proprio che $q^b + 1$ divide $q^s + 1$. ■

Lemma 9 *Siano q e s due interi positivi. Se m divide n , allora $q^m - 1$ divide $q^n - 1$.*

Dimostrazione.

Partiamo dalla identità fondamentale

$$(x^t - 1) = (x - 1)(x^{t-1} + x^{t-2} + \dots + x + 1) \quad (18)$$

Per ipotesi esiste u tale che $n = m \times u$. Se poniamo $x = q^m$ e $t = u$ nella (18) otteniamo

$$(q^n - 1) = ((q^m)^u - 1) = (q^m - 1)(q^{m(u-1)} + q^{m(u-2)} + \dots + q^m + 1)$$

e la tesi è provata. ■

Lemma 10 *Se $N = 2^s + 1$ è primo, allora $s = 2^k$.*

Dimostrazione.

Per il Lemma (8) se a dispari divide s , allora $2^{\frac{s}{a}} + 1$ divide N . Pertanto se N è primo l'unico divisore dispari di s è 1, e $s = 2^k$, per un intero $k \geq 0$. ■

Lemma 11 *Se $N = 2^s - 1$ è primo, allora s è primo.*

Dimostrazione.

Infatti se s non è primo si ha $s = m \times u$ con $1 < m < s$ e, per il Lemma (9) $2^m - 1$ è un divisore proprio di N . ■

Definiamo **numero primo di Mersenne** un numero primo q della forma $2^s - 1$. Definiamo inoltre **numero primo di Fermat** un numero primo q della forma $2^s + 1$.

Osserviamo che, per i Lemmi (11) e (10) le definizioni date sono del tutto equivalenti a quelle che seguono.

Definiamo **numero primo di Mersenne** un numero primo q della forma $2^p - 1$, con p primo. Definiamo inoltre **numero primo di Fermat** un numero primo q della forma $2^{2^k} + 1$, con $k \geq 0$.

L'informazione ottenuta, se $2^s + 1$ è primo allora $s = 2^k$, è molto utile. Se vogliamo trovare tutti i primi della forma $q = 2^s + 1$ con una ricerca al computer non dobbiamo prendere $s = 1, 2, 3, 4, 5, \dots$, ma $s = 1, 2, 4, 8, 16, \dots$. Si evita così un grandissimo spreco di tempo. Se proviamo a condurre effettivamente questa ricerca troviamo cinque numeri primi, in corrispondenza dei primi cinque valori possibili di s .

1. $s = 1$ ($k = 0$) $\longrightarrow q = 3$
2. $s = 2$ ($k = 1$) $\longrightarrow q = 5$

3. $s = 4$ ($k = 2$) $\longrightarrow q = 17$
4. $s = 8$ ($k = 3$) $\longrightarrow q = 257$
5. $s = 16$ ($k = 4$) $\longrightarrow q = 65537$

E' ben noto che Fermat riteneva che gli interi di questa forma fossero tutti primi, ma già quello che segue (per $s = 32$ ($k = 5$)) non lo è. Infatti $q = 2^{32} + 1 = 4294967297 = 641 \times 6700417$. Fu Eulero, circa un secolo dopo l'affermazione di Fermat, a scoprire il fattore 641.

Non sono stati trovati altri numeri primi di Fermat. Si tratta di un problema del tutto aperto, ma la congettura più accreditata è che siano in numero finito. Anche se un sesto numero primo di Fermat esiste, può essere che non lo sapremo mai, perchè questi numeri crescono troppo velocemente in funzione di k .

Analogamente a quanto detto per i primi di Fermat, se cerchiamo i primi di Mersenne $q = 2^s - 1$ non dobbiamo prendere $s = 1, 2, 3, 4, 5, \dots$, ma $s = 2, 3, 5, 7, 11, 13, \dots$. Ecco che cosa troviamo.

1. $s = 2 \longrightarrow q = 3$
2. $s = 3 \longrightarrow q = 7$
3. $s = 5 \longrightarrow q = 31$
4. $s = 7 \longrightarrow q = 127$
5. $s = 11 \longrightarrow q = 2047$
6. $s = 13 \longrightarrow q = 8191$

I primi quattro q sono primi, mentre il quinto $2047 = 23 \times 89$ non lo è. Però per $s = 13$ abbiamo di nuovo un numero primo. I numeri primi di Mersenne si presentano con una certa regolarità (si veda per esempio Non smettono di stupire i primi di Mersenne!). Questa constatazione empirica, avvalorata da ragionamenti euristici, insieme al fatto che essi crescono assai meno rapidamente dei numeri primi di Fermat, ha fatto sì che la loro ricerca non venisse abbandonata.

Sono attualmente noti 46 primi di Mersenne. Gli ultimi due sono stati trovati poco tempo fa. Il 23 Agosto 2008 è stato scoperto il 46° (in ordine di grandezza crescente).

$$2^{43112609} - 1$$

un numero primo di ben 12.978.189 cifre.

Il 6 Settembre 2008 si è trovato il 45°.

$$2^{37156667} - 1$$

che possiede 11.185.272 cifre.

Come si vede quello più grande è stato scoperto prima. Questo fenomeno si è verificato altre volte, in passato. Nel 1876 Francois Edouard Anatole Lucas scoperse il 12°. E' un numero di 39 cifre

$$2^{127} - 1 = 170141183460469231731687303715884105727$$

Il 9°, il 10° e l'11° vennero trovati rispettivamente negli anni 1883, 1911, 1914. Fu Lucas a inaugurare l'uso del calcolatore meccanico nella ricerca dei primi di Mersenne, e questi quattro primi, dal 9° al 12° vennero trovati utilizzando questo tipo di macchina.

L'8° e il 13° primo di Mersenne segnano la fine e l'inizio di due epoche. Fu Eulero a trovare l'8°, nel 1750. Da allora si dovette aspettare l'avvento del calcolatore meccanico, non ci furono nuove scoperte per 126 anni. Per vedere un nuovo primo di Mersenne, il 13°, si dovette attendere dal 1914 fino al 1956, quando Raphael M. Robinson lo scoprì utilizzando uno dei primi calcolatori elettronici: lo SWAC.

Nel 1983 David Slowinski trovò il 30°, un numero con 39.751 cifre. Il 29°, con 33.265 cifre fece la sua apparizione soltanto nel 1988.

I record di lunghezza (almeno 10, 100, 1000, ... cifre) dei primi di Mersenne noti riflettono i progressi della tecnica.

- 1750, 10 cifre, 8°, Leonard Euler (carta e penna)
- 1952, 157 cifre, 13°, Raphael M. Robinson (SWAC)
- 1961, 1.281 cifre, 19°, Alexander Hurwitz & John L. Selfridge (IBM 7090)
- 1979, 13.395 cifre, 27°, David Slowinski & Harry L. Nelson (Cray 1)
- 1992, 227.832 cifre, 32°, David Slowinski & Paul Gage (Cray 2)
- 1999, 2.098.960 cifre, 38°, Nayan Hajratwala, Woltman, Kurowski & GIMPS
- 2008, 11.185.272 cifre, 45°, Hans-Michael Elvenich & GIMPS

Da quando si può utilizzare il computer (1952), per passare da un ordine di grandezza all'altro nel numero di cifre, sono trascorsi

- 100-1000 cifre, 9 anni (1952-1961)
- 1000-10000 cifre, 18 anni (1961-1979)
- 10000-100000 cifre, 13 anni (1979-1992)
- 100000-1000000 cifre, 7 anni (1992-1999)
- 1000000-10000000, 9 anni (1999,2008)

Se, ma è un grosso se, si proseguirà a questa velocità un numero primo (di Mersenne) con più di un miliardo di cifre potrebbe essere scoperto prima del 2030.

Nella prossima, e ultima, sezione vedremo quale legame esiste tra le sic e i numeri primi di Mersenne e di Fermat.

Numeri perfetti e imperfetti

La funzione aritmetica σ associa a un intero n la somma dei suoi divisori.

$$\sigma(n) = \sum_{d|n} d \quad (19)$$

Un intero positivo n si dice *perfetto* se

$$\sigma(n) = 2n \quad (20)$$

Diciamo *imperfezione* di n la quantità $imp(n) = \sigma(n) - 2n$. I numeri perfetti sono quelli con imperfezione 0. Se $imp(n) > 0$ diciamo che n è *abbondante*. Nel caso contrario (imperfezione negativa) diciamo che n è *deficiente*.

Se n è primo, ovviamente si ha $\sigma(p) = p + 1$.

L'imperfezione di un numero primo p è $\sigma(p) - 2p = p + 1 - 2p = 1 - p$.

Quindi i primi sono tutti deficienti.

La funzione σ è una funzione *moltiplicativa*. Questo significa che se gli interi a e b sono coprimi allora

$$\sigma(ab) = \sigma(a)\sigma(b) \quad (21)$$

Per calcolare σ è allora sufficiente conoscere $\sigma(p^e)$, con p primo. Questo è facile perchè i divisori di p^e sono le potenze p^k con $k \leq e$.

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1} \quad (22)$$

Nel caso $p = 2$ si ha $\sigma(2^e) = 2^{e+1} - 1$.

L'imperfezione di 2 è -1 . E' interessante il fatto che qualsiasi potenza di 2 ha imperfezione -1 , infatti

$$imp(2^e) = \sigma(2^e) - 2 \times 2^e = 2^{e+1} - 1 + 2^{e+1} = -1$$

Non si sa se esistano altri interi con imperfezione -1 . E' possibile che le potenze di 2 siano gli unici interi con imperfezione -1 , così come sono gli unici interi a non possedere alcuna sic non banale.

Utilizziamo ora le proprietà viste della funzione σ per dimostrare un notevole Teorema, dovuto alla eccezionale coppia Euclide - Eulero.

Teorema 12 *Un intero pari n è perfetto se e solo se $n = 2^{v-1}q$ dove $q = 2^v - 1$ e q è primo.*

Dimostrazione.

Supponiamo $n = 2^{v-1}q$, $q = 2^v - 1$, q primo. Allora

$$\sigma(n) = \sigma(2^{v-1}(2^v - 1)) = \sigma(2^{v-1})\sigma(2^v - 1) = (2^v - 1)2^v = q2^v = 2n \quad (23)$$

Si noti che $\sigma(2^v - 1) = 2^v$ perchè $2^v - 1$ è primo.

Questa implicazione era già nota a Euclide.

Vediamo l'altra parte, provata per la prima volta da Eulero.

Supponiamo che n sia un numero perfetto pari. Avremo allora $n = 2^s T$, con $s > 0$ e T dispari.

Per ipotesi

$$\sigma(n) = \sigma(2^s T) = \sigma(2^s)\sigma(T) = (2^{s+1} - 1)\sigma(T) = 2n = 2^{s+1}T \quad (24)$$

La (24) dice che $2^{s+1} - 1$ divide $2^{s+1}T$. Ma $2^{s+1} - 1$ è dispari, e deve quindi dividere T . Segue

$$\sigma(T) = 2^{s+1} \frac{T}{2^{s+1} - 1} = T + \frac{T}{2^{s+1} - 1} \quad (25)$$

Poichè $\sigma(T)$ è la somma di tutti i divisori di T , segue che T possiede solo due divisori! Essi sono T e $\frac{T}{2^{s+1}-1}$

Pertanto T è un numero primo e $\frac{T}{2^{s+1}-1} = 1$. Quindi $T = 2^{s+1} - 1$.

Infine, abbiamo provato che $n = 2^{v-1}q$ (dove si è posto $v = s + 1$ e $q = T$) e che $q = 2^v - 1$ è primo. ■

Il Teorema (23) mostra l'esistenza di una corrispondenza biunivoca tra l'insieme dei numeri perfetti pari e l'insieme dei numeri primi q della forma $2^v - 1$, che, come sappiamo, sono esattamente i primi di Mersenne. Pertanto possiamo dire che a tutt'oggi sono noti 46 numeri perfetti pari.

Diciamo **pariprimo** un intero n della forma $n = 2^{v-1}q$, con q primo dispari. I numeri perfetti sono i rappresentanti più illustri della classe dei pariprimi.

I pariprimi hanno un solo divisore dispari $\neq 1$ e quindi possiedono *un'unica sic non banale* $\theta(n, q)$.

E' naturale allora chiedersi quale relazione esista tra la imperfezione di un pariprimo $n = 2^{v-1}q$ e l'unica sic che questo numero possiede.

Poniamo

$$\mathcal{T}^{(a)} = \{\gamma(a, k) : k \geq 0\} \quad (26)$$

Quindi $\mathcal{T}^{(a)}$ è l'insieme degli n di questa forma

$$n = \mathcal{T}_k^{(a)} = a + (a + 1) + (a + 2) + \cdots + (a + k) \quad k \geq 0$$

Se $a = 1$ otteniamo l'insieme $\mathcal{T}^{(1)}$ dei numeri (figurati) triangolari. Per a diverso da 1 abbiamo dei numeri che chiamiamo *trapezoidali*. Diciamo $\mathcal{T}^{(a)}$ **classe trapezoidale**.

Esempio 13

- $\mathcal{T}^{(1)} = \{1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, 190, 210, \dots\}$
- $\mathcal{T}^{(2)} = \{2, 5, 9, 14, 20, 27, 35, 44, 54, 65, 77, 90, 104, 119, 135, 152, 170, 189, 209, 230, \dots\}$
- $\mathcal{T}^{(3)} = \{3, 7, 12, 18, 25, 33, 42, 52, 63, 75, 88, 102, 117, 133, 150, 168, 187, 207, 228, 250, \dots\}$

Per definizione $n \in \mathcal{T}^{(a)}$ se e solo se esistono un d e un k tali che $(n, d) = \psi(a, k)$, dove d è un divisore dispari di n . Equivalentemente si deve avere $\theta(n, d) = (a, k)$. Poichè il solo divisore dispari $\neq 1$ di $n = 2^{v-1}q$ è q

$$2^{v-1}q \in \mathcal{T}^{(a)} \iff \theta(2^{v-1}q, q) = (a, k)$$

Diciamo che il pariprimo $n = 2^{v-1}q$ è di **prima specie** se $2^v > q$. Diciamo che è di **seconda specie** se $2^v < q$.

Sappiamo (si veda il Teorema (6)) che

- Se n è un pariprimo di prima specie

$$\theta(n, q) = \left(\frac{n}{q} - \frac{q-1}{2}, q-1 \right) = \left(2^{v-1} - \frac{q-1}{2}, q-1 \right)$$

- Se n è un pariprimo di seconda specie

$$\theta(n, q) = \left(\frac{q-1}{2} - \frac{n}{q} + 1, 2\frac{n}{q} - 1 \right) = \left(\frac{q-1}{2} - 2^{v-1} + 1, 2^v - 1 \right)$$

Pertanto, nel primo caso si deve avere $a = 2^{v-1} - \frac{q-1}{2}$ e nel secondo caso $a = \frac{q-1}{2} - 2^{v-1} + 1$.

Possiamo allora scrivere q in funzione di a , ottenendo $q = 2^v - 2a + 1$ nel primo caso e $q = 2^v + 2a - 1$ nel secondo caso. Concludendo

Teorema 14 *Sia dato il pariprimo $n = 2^{v-1}q$.*

- *Se n è di prima specie*

$$n \in \mathcal{T}^{(a)} \iff q = 2^v - 2a + 1$$

- *Se n è di seconda specie*

$$n \in \mathcal{T}^{(a)} \iff q = 2^v + 2a - 1$$

■

Il Teorema seguente mostra la relazione esistente tra la imperfezione dei numeri pariprimi e la classe trapezoidale alla quale essi appartengono.

Teorema 15 *Sia n il pariprimo $n = 2^{v-1}q$.*

- *Primo caso: n è di prima specie.*

$$n \in \mathcal{T}^{(a)} \iff \text{imp}(n) = 2(a-1)$$

- *Secondo caso: n è di seconda specie.*

$$n \in \mathcal{T}^{(a)} \iff \text{imp}(n) = -2a$$

Dimostrazione.

Si ha sempre $\sigma(n) = \sigma(2^{v-1}q) = \sigma(2^{v-1})\sigma(q) = (2^v - 1)(q + 1)$.

Conseguentemente, in ogni caso

$$\text{imp}(n) = \sigma(n) - 2n = (2^v - 1)(q + 1) - 2^v q = 2^v - q - 1$$

Dimostriamo ora i due casi separatamente.

Primo caso.

Supponiamo $n \in \mathcal{T}^{(a)}$. Dal Teorema (14), segue che $q = 2^v - 2a + 1$.

Quindi

$$\text{imp}(n) = 2^v - q - 1 = 2^v - (2^v - 2a + 1) - 1 = 2(a - 1)$$

Viceversa se $\text{imp}(n) = 2(a - 1)$ allora $2^v - q - 1 = 2a - 2$ e $q = 2^v - 2a + 1$.

Per il Teorema (14) si ha che $n \in \mathcal{T}^{(a)}$.

Secondo caso.

Supponiamo $n \in \mathcal{T}^{(a)}$. Dal Teorema (14), segue che $q = 2^v + 2a - 1$.

Quindi

$$\text{imp}(n) = 2^v - q - 1 = 2^v - (2^v + 2a - 1) - 1 = -2a$$

Viceversa se $\text{imp}(n) = -2a$ allora $2^v - q - 1 = -2a$ e $q = 2^v + 2a - 1$.

Ancora una volta, il Teorema (14) implica che $n \in \mathcal{T}^{(a)}$. ■

Torniamo ora ai numeri primi.

Ogni intero si scrive in modo unico nella forma $2^s T$, dove T è dispari. Diciamo che T è la **parte dispari** di n .

Questa è la successione delle parti dispari dei primi 100 interi:

1, 1, 3, 1, 5, 3, 7, 1, 9, 5, 11, 3, 13, 7, 15, 1, 17, 9, 19, 5, 21, 11, 23, 3, 25, 13, 27, 7, 29, 15, 31, 1, 33, 17, 35, 9, 37, 19, 39, 5, 41, 21, 43, 11, 45, 23, 47, 3, 49, 25, 51, 13, 53, 27, 55, 7, 57, 29, 59, 15, 61, 31, 63, 1, 65, 33, 67, 17, 69, 35, 71, 9, 73, 37, 75, 19, 77, 39, 79, 5, 81, 41, 83, 21, 85, 43, 87, 11, 89, 45, 91, 23, 93, 47, 95, 3, 97, 49, 99, 25

Un numero primo p appare infinite volte in questa sequenza, come parte dispari degli infiniti pariprimi $2^s p$.

Le cose cambiano totalmente se invece di partire dagli interi si parte da una classe trapezoidale.

Se $n \in \mathcal{T}^{(a)}$ allora (14) $n = \mathcal{T}_k^{(a)} = \gamma(a, k) = (k + 1)a + \frac{k(k+1)}{2}$, e sappiamo (1) che $k + 1$ oppure $2a + k$ è un divisore dispari di n . Questo divisore è certamente diverso da 1 e da n se $k \neq 0, 1$. Quindi nella classe $\mathcal{T}^{(a)}$, il numero $n = \mathcal{T}_k^{(a)}$ può essere primo solo se $n = a$ o $n = 2a + 1$.

Chiamiamo $Disp^{(a)}$ la sequenza delle parti dispari dei numeri $\mathcal{T}_k^{(a)}$ in $\mathcal{T}^{(a)}$, con $k \geq 2$. Si osservi che $Disp^{(a)}$ inizia sempre con la parte dispari di $3(a+1)$.

Ecco gli interi $\mathcal{T}_k^{(3)}$, con $2 \leq k \leq 51$:

12, 18, 25, 33, 42, 52, 63, 75, 88, 102, 117, 133, 150, 168, 187, 207, 228, 250, 273, 297, 322, 348, 375, 403, 432, 462, 493, 525, 558, 592, 627, 663, 700, 738, 777, 817, 858, 900, 943, 987, 1032, 1078, 1125, 1173, 1222, 1272, 1323, 1375, 1428, 1482

e le loro parti dispari, ovvero i primi 50 elementi di $Disp^{(3)}$

3, 9, 25, 33, 21, 13, 63, 75, 11, 51, 117, 133, 75, 21, 187, 207, 57, 125, 273, 297, 161, 87, 375, 403, 27, 231, 493, 525, 279, 37, 627, 663, 175, 369, 777, 817, 429, 225, 943, 987, 129, 539, 1125, 1173, 611, 159, 1323, 1375, 357, 741

I numeri dispari in $\mathcal{T}^{(a)}$ passano senza alcun cambiamento in $Disp^{(a)}$ e, per quanto si è appena osservato, sono tutti composti. Pertanto i $Disp_k^{(a)}$ possono essere primi solo se provengono da numeri *pari* di $\mathcal{T}^{(a)}$, cioè se sono la parte dispari q di un pariprimo $n = 2^{v-1}q$.

Quindi in $Disp^{(a)}$ ci possono essere esclusivamente, per il Teorema (14), primi di forma $q = 2^v - 2a + 1$ oppure $q = 2^v + 2a - 1$ (con $v > 1$).

E' interessante notare che, fissato a , un primo q compare al più una volta in $Disp^{(a)}$.

Supponiamo per assurdo che q compaia due volte ed esaminiamo tutti i casi possibili:

- $2^v - 2a + 1 = 2^w - 2a + 1$ con $v > w$

Allora $2^v = 2^w$, assurdo.

- $q = 2^v + 2a - 1 = 2^w + 2a - 1$ con $v > w$

Come prima segue $2^v = 2^w$, assurdo.

- $2^v - 2a + 1 = 2^w + 2a - 1$

Allora $2^v - 2^w = 2(2a - 1)$, e $2^{v-1} - 2^{w-1} = 2a - 1$. Quindi $2^{v-1} - 2^{w-1}$ deve essere dispari. Questo implicherebbe $w = 1$, assurdo.

Vediamo ora tre esempi, relativi ai casi $a = 3$, $a = 2$, $a = 1$.

Esempio 16 $\mathcal{T}^{(3)}$

Se $a = 3$ in $Disp^{(3)}$ si troveranno primi q provenienti da pariprimi n di prima specie con imperfezione $2(a - 1) = 4$, e da pariprimi di seconda specie con imperfezione $-2a = -6$.

Nel primo caso q sarà della forma $2^v - 2a + 1 = 2^v - 5$.

Nel secondo caso avremo $q = 2^v + 2a - 1 = 2^v + 5$.

Se esaminiamo i primi 200.000 elementi di $\mathcal{T}^{(3)}$ troviamo 9 pariprimi:

12, 52, 88, 592, 1888, 32128, 521728, 2102272, 8378368

con rispettive imperfezioni

4, -6, 4, -6, 4, 4, 4, -6, 4

Le parti dispari dei 9 pariprimi sono i primi

3, 13, 11, 37, 59, 251, 1019, 2053, 4091

uguali a

$2^3 - 5, 2^3 + 5, 2^4 - 5, 2^5 + 5, 2^6 - 5, 2^{10} - 5, 2^{11} + 5, 2^{12} - 5$

Esempio 17 $\mathcal{T}^{(2)}$

Se $a = 2$ in $\text{Disp}^{(2)}$ si troveranno primi q provenienti da pariprimi n di prima specie con imperfezione $2(a - 1) = 2$, e da pariprimi di seconda specie con imperfezione $-2a = -4$.

Nel primo caso q sarà della forma $2^v - 2a + 1 = 2^v - 3$.

Nel secondo caso avremo $q = 2^v + 2a - 1 = 2^v + 3$.

Se esaminiamo i primi 200.000 elementi di $\mathcal{T}^{(2)}$ troviamo 16 pariprimi:

14, 20, 44, 104, 152, 464, 1952, 2144, 8384, 130304, 522752, 8382464, 8394752, 134193152, 536920064, 2147581952

con rispettive imperfezioni

-4, 2, -4, 2, -4, 2, 2, -4, -4, 2, 2, 2, -4, 2, -4, -4

Le parti dispari dei 16 pariprimi sono i primi

7, 5, 11, 13, 19, 29, 61, 67, 131, 509, 1021, 4093, 4099, 16381, 32771, 65539

uguali a

$2^2 + 3, 2^3 - 3, 2^3 + 3, 2^4 - 3, 2^4 + 3, 2^5 - 3, 2^6 - 3, 2^6 + 3, 2^7 + 3, 2^9 - 3, 2^{10} - 3, 2^{12} - 3, 2^{12} + 3, 2^{14} - 3, 2^{15} + 3, 2^{16} + 3$

Esempio 18 $\mathcal{T}^{(1)}$ (Numeri Triangolari)

Se $a = 1$ in $\text{Disp}^{(1)}$ si troveranno primi q provenienti da pariprimi n di prima specie con imperfezione $2(a - 1) = 0$ (sono i numeri perfetti!), e da pariprimi di seconda specie con imperfezione $-2a = -2$.

Nel primo caso q sarà della forma $2^v - 2a + 1 = 2^v - 1$ (q è un primo di Mersenne).

Nel secondo caso avremo $q = 2^v + 2a - 1 = 2^v + 1$ (q è un primo di Fermat).

Se esaminiamo i primi 200.000 elementi di $\mathcal{T}^{(1)}$ troviamo 10 pariprimi:

6, 10, 28, 136, 496, 8128, 32896, 33550336, 2147516416, 8589869056

con rispettive imperfezioni

0, -2, 0, -2, 0, 0, -2, 0, -2, 0

Le parti dispari dei 10 pariprimi sono i primi

3, 5, 7, 17, 31, 127, 257, 8191, 65537, 131071

uguali a

$2^2 - 1, 2^2 + 1, 2^3 - 1, 2^4 + 1, 2^5 - 1, 2^7 - 1, 2^8 + 1, 2^{13} - 1, 2^{16} + 1, 2^{17} - 1$

Appaiono qui i primi (e forse gli unici) 5 primi di Fermat e i primi 6 primi di Mersenne. Si noti che 3 in questa lista appare come primo di Mersenne (viene da un pariprimo perfetto, di prima specie) ma è anche il primo primo di Fermat: $3 = 2^{2^0} + 1$.

Concludiamo con una immagine.

Fattorizzare i numeri è difficile: si comportano come una sostanza dura, ardua da spezzare. La *parte pari* si elimina però molto facilmente: basta dividere quanto basta per 2, cosa che fanno tutti. Potremmo pensare agli interi come composti da una parte secca, la parte dispari, e da acqua (la parte pari). In un certo senso l'acqua è necessaria alla perfezione (come alla vita). I numeri perfetti devono (condizione *necessaria* ma non *sufficiente*) possedere una speciale relazione tra parte acquosa e parte secca: la parte asciutta è un briciolino meno di due volte la parte liquida.

Tra i numeri asciutti (i numeri dispari) spiccano i primi, del tutto indecomponibili. Pensiamoli come cristalli.

Prendiamo ora la sequenza dei numeri triangolari: 1, 3, 6, 10, 15, 21 \dots . Strizziamoli ben bene per eliminare l'acqua. Lasciamoli al sole, che si asciugino del tutto. Ora guardiamo l'infinita, arida distesa.

In mezzo a loro brillano di eterna luce i cristalli, 3, 5, 7, 17, 31, 127, \dots : sono loro, e soltanto loro, **i primi di Mersenne e i primi di Fermat!**