

# I numeri idonei di Eulero

Umberto Cerruti  
Università di Torino

## 1 Introduzione

Nel 1621 Bachet de Méziriac osservò, con una certa cautela, che *quasi tutti* i numeri primi della forma  $4k + 1$  si possono scrivere come somma di due quadrati. Qualche anno dopo, nel 1625, Albert Girard, nel suo commentario ai lavori matematici di Simon Stevin, azzardò l'ipotesi che *tutti* i primi congrui a 1 modulo 4 siano somma di due quadrati.

Nel 1641 Fermat enunciò, in una lettera a Frenicle de Bessy, il medesimo teorema aggiungendo che la somma si ottiene in modo unico. Per esempio  $7933 = 43^2 + 78^2$ , e questa espressione è unica. Fermat sosteneva di avere una dimostrazione, e illustrò anche il metodo (della *descente infinie*) che aveva in mente. Non scese però nei dettagli.

Frenicle nella sua lettera di risposta propose un problema: posto che  $m$  si scriva in modi diversi come somma di quadrati, determinare una fattorizzazione di  $m$ .

Pe esempio dal fatto che  $221 = 10^2 + 11^2 = 5^2 + 14^2$ , dedurre che  $221 = 13 \times 17$ .

Fu Eulero che, tra il 1750 e il 1758 dimostrò sia il teorema di Girard - Fermat che il suo inverso.

Denotiamo con  $\mathbb{N}$  l'insieme dei numeri naturali,  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$  e con  $\mathbb{N}^+$  l'insieme dei numeri naturali positivi,  $\mathbb{N}^+ = \{1, 2, 3, \dots\}$ .

### **Teorema 1.** (1750)

*Un numero primo dispari  $p$  è la somma di due quadrati  $x^2 + y^2$ , con  $x, y \in \mathbb{N}^+$  se e solo se  $p \equiv 1 \pmod{4}$ .*

*Inoltre questa rappresentazione è unica, e  $\text{MCD}(x, y) = 1$ .*

### **Teorema 2.** (1758)

*Se un intero dispari  $m > 1$  è rappresentabile come somma di due quadrati*

$$m = x^2 + y^2 \quad \text{con } x, y \in \mathbb{N}$$

*esattamente in un sol modo, e se, inoltre, i due interi  $x, y$  sono coprimi, allora  $m$  è primo.*

Si noti l'importanza di una formulazione esatta dell'enunciato del Teorema (2). Se a  $\mathbb{N}$  si sostituisse  $\mathbb{N}^+$ , allora 25 dovrebbe essere primo, perché si scrive in modo unico come  $3^2 + 4^2$  e  $\text{MCD}(3, 4) = 1$ . Invece 25 ha due rappresentazioni con  $x, y \in \mathbb{N}$ , che sono  $0^2 + 5^2$  e  $3^2 + 4^2$ .

Se poi si dicesse:

*Se un intero dispari  $m > 1$  è rappresentabile come somma di due quadrati*

$$m = x^2 + y^2 \quad \text{con } x, y \in \mathbb{N}$$

esattamente in un sol modo con  $x, y$  coprimi, allora  $m$  è primo.

si cadrebbe ancora in errore. Infatti 125 si scrive in un modo solo con  $x, y$  coprimi,  $125 = 2^2 + 11^2$ . Ha però un'altra scrittura,  $125 = 5^2 + 10^2$ .

Infine non sarebbe sufficiente dire *esattamente in un sol modo*, omettendo la coprimalità.

Infatti 45 si scrive in modo unico come somma di quadrati:  $45 = 3^2 + 6^2$ .

In realtà la storia della espressione dei numeri interi mediante forme quadratiche ha avuto diversi problemi di *comunicazione*. Dovuti in parte allo stesso Eulero, il quale, pur avendo chiarissime le idee, sovente ne scriveva senza la necessaria precisione.

Si veda, a questo proposito, l'articolo di Steinig ([9]).

## 2 Eulero a caccia di primi

Il 16 Marzo 1778, Eulero inviò all'Accademia di San Pietroburgo l'articolo *Utrum hic numerus: 1000009 sit primus, nec ne, inquiritur* ([2]). Eulero dimostra che  $m = 1000009$  non è primo utilizzando il Teorema (1). Si vede a occhio che  $m = 1000^2 + 3^2$ . Se si riesce a scrivere  $m$  come somma di altri due quadrati,  $m$  non può essere primo.

Con un procedimento assai ingegnoso Eulero trova che  $m = 235^2 + 972^2$ . Dalla doppia espressione di  $m$  come somma di due quadrati, Eulero scopre anche la sua fattorizzazione:  $m = 293 \times 3413$ .

Eulero conosceva bene il Piccolo Teorema di Fermat

### Teorema 3.

Se  $m$  è primo e  $m$  non divide  $a$  allora

$$a^{m-1} \equiv 1 \pmod{m}$$

Egli stesso aveva dimostrato un risultato assai più generale, noto come *Teorema di Eulero*, (per una discussione elementare del Teorema di Eulero e di una sua applicazione alla Crittografia si veda ([1])).

Quindi avrebbe potuto effettuare quello che oggi chiamiamo un *test* calcolando

$$a^{1000008} \pmod{1000009}$$

Infatti se il risultato è diverso da 1 allora il numero è certamente composto, proprio per il Teorema (3).

Il calcolo si esegue facilmente a mano, con molta pazienza, utilizzando il metodo delle *quadrature successive*. Prediamo  $a = 2$ .

Scriviamo  $m - 1 = 1000008$  in binario, ottenendo  $m = 11110100001001001000$ . Questo significa che

$$1000008 = 2^3 + 2^6 + 2^9 + 2^{14} + 2^{16} + 2^{17} + 2^{18} + 2^{19}$$

ovvero

$$2^{1000008} = 2^{2^3} \times 2^{2^6} \times 2^{2^9} \times 2^{2^{14}} \times 2^{2^{16}} \times 2^{2^{17}} \times 2^{2^{18}} \times 2^{2^{19}} \quad (1)$$

Naturalmente non dobbiamo calcolare questi numeri così grandi, ma soltanto i resti delle divisioni per  $m$ .

Partiamo da 2 e iniziamo a calcolare la successione dei quadrati:

4, 16, 256, 65536, 4294967296

L'ultimo numero calcolato è  $2^{2^6} = 2^{32}$  ed è il primo quadrato che supera  $m$ . Allora dividiamo per 1000009 e troviamo 928650. Il quadrato di questo, modulo  $m$ , è 61053. Per fare il calcolo dobbiamo quindi moltiplicare, mediamente, numeri di 6 cifre e dividere interi di 12 cifre per  $m$ . Dobbiamo fare 19 quadrati, con le relative riduzioni. Otteniamo

4, 16, 256, 65536, 928650, 61053, 435266, 785670, 793461, 692355

131866, 485464, 174239, 955899, 674595, 318359, 540722, 649891, 510695

Nella prima riga si trovano, in ordine, le potenze che vanno da  $2^2$  a  $2^{2^{10}}$ , modulo  $m$ . Nella seconda ci sono i resti relativi alle potenze  $2^{2^{11}}$  fino a  $2^{2^{19}}$ .

Ora, tenendo presente la (1) dobbiamo moltiplicare, in sequenza, i seguenti otto numeri, riducendo ogni volta modulo  $m$ :

256, 61053, 793461, 955899, 318359, 540722, 649891, 510695

Il risultato  $M$  della moltiplicazione è, come sappiamo,  $2^{1000008} \bmod 1000009$ . Risulta  $M = 706398$ . Quindi  $m$  non è primo.

Non bisogna pensare che questi calcoli costituissero un ostacolo. Eulero era abituato a ben altro, visto che non c'erano i computer.

Calcolare le potenze è un metodo efficace ma, potremmo dire, di *forza bruta*. Inoltre si applica, sempre uguale, ad ogni test, non cambia mai, e non insegna niente di nuovo.

Invece il metodo delle somme di quadrati è elegante, richiede ingegno per poter essere utilizzato, permette alla fine la fattorizzazione del numero composto, e, soprattutto, genera nuove idee, è creativo.

Dopo averlo messo in opera molte volte, Eulero si chiese perché non utilizzare altre forme quadratiche, oltre a  $x^2 + y^2$ . Questo lo condusse alla scoperta dei *numeri idonei*, presentati con vera gioia nell'articolo *De formulis speciei  $mxx + nyy$  ad numeros primos explorandum idoneis, earumque mirabilibus proprietatibus* ([3]). Questi numeri gli permettevano di trovare numeri primi grandi (relativamente all'epoca, naturalmente) con una certa facilità. L'entusiasmo di Eulero traspare fin dal titolo di uno dei suoi successivi articoli: *Facillima methodus plurimos numeros primos praemagnos inveniendi* ([4]). In questo lavoro Eulero prova che per ogni intero  $a$  nella lista sottostante

1, 2, 3, 5, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 20, 22, 24, 26, 27, 28, 31, 35, 36, 37, 38, 44, 45, 46, 48, 49, 50, 52, 53, 62, 67, 71, 72, 73, 74, 76, 79, 81, 82, 86, 87, 94, 95, 99, 100, 104, 106, 107, 112, 113, 115, 118, 119, 121, 124, 126, 127, 136, 138, 142, 144, 149, 150, 151, 152, 153, 155, 157, 158, 159, 167, 170, 172, 173, 175, 176, 177, 180, 182, 188, 189, 197, 200, 201, 204, 205, 210, 213, 219, 226, 227, 228, 229, 230, 238, 248, 249, 250, 251, 254, 255, 258, 259, 261, 262, 264, 267, 269, 270, 275, 277, 280, 281, 283, 285, 288, 289, 291, 294, 299

il numero  $232 \times a^2 + 1$  è primo!

Conseguentemente quelli che seguono sono 124 primi

233, 929, 2089, 5801, 8353, 11369, 18793, 23201, 33409, 39209, 52201, 59393, 67049, 75169, 92801, 112289, 133633, 156833, 169129, 181889, 222953, 284201, 300673, 317609, 335009, 449153, 469801, 490913, 534529, 557033, 580001, 627329, 651689, 891809, 1041449, 1169513, 1202689, 1236329, 1270433, 1340033, 1447913, 1522153, 1559969, 1715873, 1756009, 2049953, 2093801, 2273833, 2320001, 2509313, 2606753, 2656169, 2910209, 2962409, 3068201, 3230369, 3285353, 3396713, 3567233, 3683233, 3741929, 4291073, 4418209, 4678049, 4810753, 5150633, 5220001, 5289833, 5360129, 5430889, 5573801, 5718569, 5791649, 5865193, 6470249, 6704801, 6863489, 6943529, 7105001, 7186433, 7268329, 7516801, 7684769, 8199809, 8287273, 9003689, 9280001, 9373033, 9654913, 9749801, 10231201, 10525609, 11126953, 11849633, 11954729, 12060289, 12166313, 12272801, 13141409, 14268929, 14384233, 14500001, 14616233, 14967713, 15085801, 15442849, 15562793, 15804073, 15925409, 16169473, 16539049, 16787753, 16912801, 17545001, 17801129, 18188801, 18318953, 18580649, 18844201, 19243009, 19376873, 19645993, 20053153, 20741033

Che cosa ha di speciale 232? E' un numero idoneo!

### 3 I numeri idonei

I numeri idonei (o convenienti) sono quegli interi  $n$  per i quali vale il seguente Teorema

#### Teorema 4.

*Sia  $m > 1$  un intero dispari. Supponiamo che  $m$  si rappresenti in un solo modo nella forma  $x^2 + ny^2$ , con  $x, y \in \mathbb{N}$ . Supponiamo inoltre che  $MCD(x, ny) = 1$ . Allora  $m$  è primo.*

Pertanto il Teorema (2) dimostra che 1 è un numero idoneo.

Eulero scoprì 65 numeri idonei:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848

Per provare che un intero  $n$  non è idoneo è dunque sufficiente trovare un  $m$  che verifichi le ipotesi di (4) e non sia primo.

Per esempio  $n = 11$  non è idoneo, in quanto 15 si scrive in modo unico come  $x^2 + 11y^2$ , con  $x = 2, y = 1$  e inoltre  $MCD(2, 11) = 1$ .

Eulero trovò il seguente Criterio di Idoneità (vedi ([6]))

#### Teorema 5.

*Un numero intero  $n > 0$  è idoneo se e solo se ogni numero  $m$  della forma*

$$m = n + x^2 < 4n \quad \text{con } x, n \text{ coprimi e } x > 0$$

*appartiene a una di queste quattro categorie:*

$$m = p, \quad m = 2p, \quad m = p^2, \quad m = 2^s$$

*dove  $p$  è un numero primo dispari e  $s$  è un intero positivo.*

Vediamo che  $n = 12$  verifica il criterio.

$$12 + 1^2 = 13 = p$$

$$12 + 5^2 = 37 = p$$

Segue che 12 è idoneo. Si badi bene che la somma  $n + x^2$  va calcolata soltanto se  $x$  è coprimo con  $n$  e  $n + x^2 < 4n$ .

Viceversa si vede subito che 17 non è idoneo, in quanto  $17 + 1^2 = 18 = 2p^2$ , e  $2p^2$  non appartiene a una delle quattro categorie previste dal Teorema (5).

Vi sono molte altre caratterizzazioni dei numeri idonei. Il lettore interessato può trovarle nei Riferimenti Bibliografici.

Servendosi del suo stesso criterio Eulero produsse la sua lista di 65 numeri idonei, compresi tra 1 e 1848. In questo elenco troviamo 232, il numero utilizzato da Eulero per generare i 124 primi del paragrafo precedente. Ora possiamo capire come fece. Seguiamo il ragionamento di Eulero, esposto in ([4]).

Lo scopo è quello di eliminare gli  $a$  per i quali  $m = 232a^2 + 1$  è composto.

Se  $m = 232a^2 + 1$  è composto, allora, poichè  $m$  è della forma  $m = 232u^2 + v^2$  e 232 è idoneo, questa rappresentazione non può essere unica e si avrà anche  $m = 232x^2 + y^2$ . Pertanto

$$232a^2 + 1 = 232x^2 + y^2$$

e quindi

$$232(a^2 - x^2) = y^2 - 1.$$

Poniamo  $y = 1 \pm 58z$ . Sostituendo e semplificando otteniamo

$$a^2 - x^2 = \frac{1}{2}z(29z \pm 1)$$

Poichè  $(a^2 - x^2) = (a + x)(a - x)$  possiamo porre  $\frac{1}{2}z(29z \pm 1) = r \times s$ , con  $r = (a + x)$ ,  $s = (a - x)$  e conseguentemente  $a = \frac{r+s}{2}$ . Si noti che  $r, s$  hanno la stessa parità.

Ora facciamo variare  $z = 1, 2, 3, \dots$  e eliminiamo via via i valori di  $a$  che vengono generati. Poniamo  $z = 1$ . Allora  $\frac{1}{2}z(29 \pm 1) = r \times s$  e  $r \times s$  può valere 15 o 14. Escludiamo 14 perché in questo caso  $r, s$  avrebbero parità diversa. Quindi  $r \times s = 15$  e  $r = 5, s = 3, a = 4$ . Il valore  $a = 4$  deve essere escluso. Procedendo a ritroso vediamo infatti che  $z = 1, x = 1, y = 59$  e

$$3713 = 232 \times 4^2 + 1^2 = 232 \times 1^2 + 59^2$$

Ovviamente 3713 non può essere primo:  $3713 = 47 \times 79$ .

Eulero continua poi con  $z = 2, 3, \dots$ , fino a escludere i valori di  $a \leq 300$  che generano composti della forma  $232a^2 + 1$ .

Certamente Eulero ogni volta che trovava un nuovo numero idoneo doveva sentire un sottile brivido di piacere: era una nuova arma formidabile da utilizzare nella sua appassionata caccia ai numeri primi! E grandissimo sarà stato il suo disappunto quando, superato il numero 1848, si trovò davanti a un deserto! Tanto che già il 20 Aprile 1778, poco più di un

mezzo mese dall'annuncio della scoperta dei numeri idonei, inviò all'Accademia l'articolo ([5]) dal titolo *Illustratio paradoxæ circa progressionem numerorum idoneorum sive congruorum*.

Ecco l'inizio dell'articolo:

*Insigne istud paradoxon in hoc consistebat, quod, etiamsi numeri idonei secundum certam legem formentur et progrediantur, multitudo tamen eorum non sit infinita sed tantum usque ad 65 terminos porrigatur, cuiusmodi paradoxon circa nullam adhuc aliam seriem observatum esse memini; neque vero etiam istum finitum terminorum numerum aliter stabilire mihi licuit, nisi quod post terminum 65, qui est 1848, nullus præterea se obtulerit, etiamsi examen usque ad 10000 et ultra continuaverim.*

Proprio per l'ampiezza delle ricerche che aveva condotto, Eulero si convinse che non vi fossero altri numeri idonei oltre ai 65 interi che aveva listato. Chiamiamo questa supposizione **Congettura di Eulero**.

Si legge spesso nella letteratura sull'argomento che un solo altro numero idoneo può esistere. Questo non è esatto, e la formulazione corretta si trova in ([8]). Ricordiamo che un intero  $n$  si dice *privo di quadrati* se è prodotto di primi distinti (equivalentemente  $n$  non è divisibile per alcun quadrato). Ecco lo stato attuale della Congettura di Eulero:

*Esattamente uno di questi fatti è vero:*

1. Non esistono numeri idonei  $> 1848$ .
2. Esiste un numero idoneo  $n > 1848$ . L'intero  $n$  è privo di quadrati e  $n \equiv 1 \pmod{4}$ .
3. Ci sono due numeri idonei  $n_1 > n_2 > 1848$ . Il più piccolo,  $n_2$ , è privo di quadrati e  $n_2 \equiv 2 \pmod{4}$ . Inoltre  $n_1 = 4n_2$ .

Si sanno anche altre due cose:

- Se esiste un altro numero idoneo, esso è  $> 2 \times 10^{11}$ .
- Se è vera la GRH (una generalizzazione della Congettura di Riemann) allora non esistono altri numeri idonei.

Trovare un 66-esimo numero idoneo disproverebbe la GRH, e sarebbe un risultato epocale, giudicato assai improbabile.

A questo si aggiunga che l'esistenza da qualche parte uno o due altri numeri idonei, isolati da tutto, sembra strana.

Personalmente io scommetto sulla verità della congettura di Eulero!

## 4 Numeri idonei, somme di tre quadrati e lo spettro del cubo

Inaspettatamente, nel 1973, i fisici Hilf e Baltés, nel loro articolo *130 and the Cube Spectrum* ([7]), scoprirono una connessione strettissima tra le soluzioni di un problema che è studiato

nell'ambito della più pura e incontaminata teoria dei numeri, e le soluzioni di un problema eminentemente fisico, riguardante l'equazione delle onde in un dominio di forma cubica con le condizioni di Dirichlet al contorno.

Il problema fisico li condusse - direi in maniera obbligata - a studiare l'insieme, che chiamarono  $\mathcal{H}$ , così definito:

$$\mathcal{H} = \{h > 0 : h \neq r^2 + s^2 + t^2 \text{ con } r, s, t \in \mathbb{N}^+ \quad e \quad h \neq 4^a(8b + 7) \text{ con } a, b \in \mathbb{N}\}$$

Un ben noto teorema di Gauss dice che un intero  $n$  può essere scritto come somma  $x^2 + y^2 + z^2$  con  $x, y, z \in \mathbb{N}$  se e solo se  $n$  non è della forma  $4^a(8b + 7)$  con  $a, b \in \mathbb{N}$ . Pertanto  $\mathcal{H}$  è formato dagli  $n$  che non sono somma di tre quadrati positivi, ma sono somma di tre quadrati non-negativi. Ne consegue che  $\mathcal{H}$  si può anche scrivere così :

$$\mathcal{H} = \{h > 0 : h \neq r^2 + s^2 + t^2 \text{ con } r, s, t \in \mathbb{N}^+ \quad e \quad h = a^2 + b^2 \text{ con } a, b \in \mathbb{N}\}$$

Denotiamo con  $\mathcal{B}$  l'insieme degli elementi di  $\mathcal{H}$  non divisibili per 4.  $\mathcal{B}$  contiene l'insieme  $\mathcal{D}$  formato da questi dieci numeri:

$$\mathcal{D} = \{1, 2, 5, 10, 13, 25, 37, 58, 85, 130\}$$

Si congettura che  $\mathcal{B} = \mathcal{D}$ .

Si congettura cioè che 130 sia il più grande intero  $n$  tale che

- $n$  non è somma di tre quadrati positivi
- $n$  non è della forma  $4^a(8b + 7)$
- $n$  non è divisibile per 4

E' stato dimostrato che l'insieme  $\mathcal{B}$  è contenuto nell'insieme dei numeri idonei!

Quindi, con la medesima fiducia di prima, mi dichiaro disposto a scommettere sul fatto che  $\mathcal{B}$  è formato esattamente da quei dieci interi!

## Riferimenti bibliografici

- [1] Umberto Cerruti - Collane colorate, Fermat, Eulero e la crittografia - *Divertiamoci con la Matematica*, 2008.
- [2] Leonhardo Eulero - Utrum hic numerus: 1000009 sit primus, nec ne, inquiritur - *Nova Acta Academiae Scientiarum Imperialis Petropolitanae* **10** (1797), 63-73, inviato il 16 Marzo 1778 all'Accademia di San Pietroburgo.

- [3] Leonhardo Eulero - De formulis speciei  $mxx + nyy$  ad numeros primos explorandum idoneis, earumque mirabilius proprietatibus -  
*Nova Acta Academiae Scientiarum Imperialis Petropolitanae* **12** (1801), 22-48, inviato il 16 Marzo 1778 all'Accademia di San Pietroburgo.
- [4] Leonhardo Eulero - Facillima methodus plurimos numeros primos praemagnos inveniendi -  
*Nova Acta Academiae Scientiarum Imperialis Petropolitanae* **14** (1805), 310, inviato il 16 Marzo 1778 all'Accademia di San Pietroburgo.
- [5] Leonhardo Eulero - Illustratio paradoxii circa progressionem numerorum idoneorum sive congruorum -  
*Nova Acta Academiae Scientiarum Imperialis Petropolitanae* **15** (1806), 2932, inviato il 20 Aprile 1778 all'Accademia di San Pietroburgo.
- [6] Günter Frei - Leonhard Euler's Convenient Numbers -  
*The Mathematical Intelligencer*, **7**, 1985, pp. 55–58, 64.
- [7] E. R. Hilf, H. P. Baltes - 130 and the Cube Spectrum -  
<http://smallsystems.isn-oldenburg.de/publications/preprint>, 1973.
- [8] Ernst Kani - Idoneal Numbers and some Generalizations -  
*preprint*, 2010.
- [9] T. J. Steinig - On Euler's Idoneal Numbers -  
*Elemente Math.*, **21**, 1966, pp. 73–88.