Bollettino
Unione Matematica Italiana

Giuseppe Palamà

Su di una regola di Fermat per la fattorizzazione dei numeri e su di una sua questione relativa alle parti aliquote.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **8** (1953), n.4, p. 414–422.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1953_3_8_4_414_0>

Su di una regola di Fermat per la fattorizzazione dei numeri e su di una sua questione relativa alle parti aliquote.

Nota di GIUSEPPE PALAMA (a Lecce)

Sunto. *Si fanno osservazioni su di una regola di* FERMAT *per fattorizzare grandi numeri, e sulla questione, di cui pure* FERMAT *si occupò, della ricerca di numeri che sono sottomultipli secondo numeri semplici della somma delle loro parti aliquote.*

1. FERMAT in un frammento di una sua lettera (1), forse diretta a MERSENNE ed a FRENICLE, dice:

« ... Un nombre me soit donné, par exemple 2 027 651 281, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit.

« J'extrais la racine, pour connaître le moindre des dits nombres, et trouve 45 029 avec 40 440 de reste, lequel j'ôte du double plus 1 de la racine trouvée, savoir de 90 059: reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19, et partant je lui ajoute 90 061, savoir 2 plus que 90 059 qui est le double plus 1 de la racine 45 029. Et parce que la somme 139 680 ne est pas encore quarrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de 2, savoir 90 063, et je continue ainsi d'ajouter tant que la somme soit un quarré, comme on peut voir ici (FERMAT, dice il compilatore delle sue Opere, deve aver effettuato al margine i calcoli indicati, che non sono stati riprodotti sulla copia). Ce qui n'arrive qu'à 1 040 400 qui est quarré de 1020, et partant le nombre donné est composé; ...

« Pour savoir maintenant les nombres qui composent 2 027 651 281 j'ôte le nombre que j'ai premièrement ajouté, savoir 90 061, du dernier ajouté 90 081. Il reste 20, à la moitié duquel plus 2, savoir à 12, j'ajoute la racine premièrement trouvée 45 029. La somme est 45 041, au quel nombre ajoutant et ôtant 1020, racine de la dernière somme 1 040 400, on aura 46 061 et 44 021, qui sont les deux nombres plus prochains qui composent 2 027 651 281. Ce sont aussi les seuls, parce que l'un et l'autre sont premiers ».

Ecco in breve in che consiste il procedimento di FERMAT.

Sia N il numero che si voglia fattorizzare e siano rispettivamente r e d la sua radice quadrata a meno di una unità per difetto ed il relativo resto, sia cioè

$$N = r^2 + d, \qquad d \leq 2r. \tag{1}$$

(1) *Oeuvres*, Gauthier-Villars, Paris, (1894), t. II, pp. 256-258.

Si aggiunga successivamente all'espressione

$$2r + 1 - d$$

ciascuno dei numeri

$$2r + 3,\ 2r + 5,\ 2r + 7, \ldots,\ 2r + 2n - 1, \ldots \tag{2}$$

sino a quando la somma non diventi un quadrato q^2; allora, se ciò succede quando si aggiunge $2r + 2n - 1$, si ha, dice FERMAT, per N la seguente fattorizzazione

$$N = (n + r + q)(n + r - q) \tag{3}$$

Questa regola di FERMAT si giustifica immediatamente.

Difatti se è

$$2r + 1 - d + (2r + 3) + (2r + 5) + \ldots + (2r + 2n - 1) = q^2,$$

si ha anche

$$2rn + n^2 - d = q^2$$

che, eliminando d con la (1), può scriversi

$$(n + r)^2 - q^2 = N, \tag{4}$$

dalla quale segue la (3)

Nell'esempio dato da FERMAT, si ha

$$N = 2\,027\,651\,281,\ r = 45\,029,\ d = 40\,440$$

e quindi

$$2r + 1 - d = 49\,619$$

che non è un quadrato; aggiungendo allora a 49 619 successivamente ciascuno dei numeri

$$90\,061,\ 90\,063,\ 90\,065, \ldots$$

non si perviene ad un quadrato che dopo aver aggiunto 90 081 e si ha per valore della corrispondente somma $1\,040\,400 = 1020^2$, pertanto è

$$n = 12,\ q = 1020$$

e quindi per la (3)

$$2\,027\,651\,281 = 46\,061 \times 44\,021,$$

in cui i due fattori sono primi.

A prima vista si rimane quasi abbagliati dalla semplicità del procedimento, ma ci vuol poco per convincersi che la regola esposta in generale è di assai modesto interesse pratico, perchè il numero dei termini della serie (2), che successivamente si devono aggiungere a $2r + 1 - d$ per ottenere un quadrato, se tale espressione

già non lo è, risulta enorme allorchè il numero dato non si può scomporre nel prodotto di due fattori poco differenti tra loro, anche se, come avverte il FERMAT, si possano fare ovviamente delle abbreviazioni nei calcoli che è facile stabilire caso per caso. Difatti dalla (3) si desume che q è la semidifferenza dei due fattori di N e quindi, a parità, all'incirca, di N, tanto maggiore è la differenza dei due fattori, tanto maggiore è q e perciò anche tanto maggiore è il numero dei tentativi che si devono fare per ottenere q^2.

Se per esempio si volesse fattorizzare con questa regola il numero

$$N = 710\,478\,611$$

(che è uguale a $71 \times 10\,006\,741$ in cui quest'ultimo fattore è primo), occorrerebbe un numero di tentativi

$$n = 4\,976\,756 \text{ (!)}.$$

Naturalmente il procedimento di FERMAT può teoricamente applicarsi per riconoscere se N è primo. Difatti perchè N sia primo è necesssario che si abbia

$$n + r - q = 1$$

che dà

$$q = n + r - 1.$$

Portando tale valore di q nella (4) si trae per il valore del numero n dei tentativi occorrenti

$$n = \frac{N - 2r + 1}{2}. \tag{5}$$

In generale se un dato numero ammette la decomposizione

$$N = f_1 \cdot f_2,$$

per pervenirvi con la regola di FERMAT, è necessario un numero di tentativi dato da

$$n = s - r,$$

ove $s = \frac{f_1 + f_2}{2}$, che per $f_1 = 1$, $f_2 = N$, cosa che succede quando N è primo, dà luogo appunto alla (5).

Ora se N è primo ed è grande, risulta anche naturalmente grande il valore di n dato dalla (5) ed il procedimento è allora assolutamente di nessuna pratica applicazione, tanto quanto non lo è quello elementare che consiste nel dividere N per i successivi numeri primi della serie naturale $< \sqrt{N}$.

Ad es. se si volesse riconoscere la primalità di

$$N = 100\,000\,007$$

che è effettivamente primo) con la regola di FERMAT, essendo $r = 10000$ occorrerebbe un numero n di tentativi dato da

$$n = (100\,000\,007 - 20\,001)\,1/2 = 49\,999\,003 \text{ (!)};$$

invece la detta regola elementare richiederebbe soltanto 1 227 divisioni, perchè altrettantti sono i numeri primi $< 10\,000$.

Le abbreviazioni di calcolo derivanti dalla semplice ispezione delle cifre finali delle successive somme ottenute con la regola di FERMAT, e da altri accorgimenti, ridurrebbero in maniera quasi irrilevante la grande fatica occorrente.

2. Osserviamo però che si può talvolta molto utilmente applicare la regola di FERMAT anzichè al numero dato N ad un suo multiplo conveniente come si vede nei seguenti esempi.

Es. I°. Si voglia fattorizzare

$$N = 1\,308\,859.$$

Moltiplichiamo tale numero per

$$m = 3 \times 5 \times 7 \times 11 = 1\,155.$$

Si ha allora che la radice quadrata r di mN ed il resto d hanno i valori

$$r = 38\,880, \qquad d = 77\,745$$

e quindi si ha

$$2r + 1 - d = 16$$

che è già un quadrato, pertanto applicando la (3), essendo ora $n = 1$, $q = 4$, risulta

$$mN = 38\,885 \times 38\,877,$$

e questa divisa per m dà

$$N = 101 \times 12\,959$$

in cui i due fattori sono primi.

La fattorizzzazione invece di N con la stessa regola avrebbe richiesto un numero di tentativi

$$n = 5\,386.$$

Es. 2°. Sia da fattorizzare

$$N = 23\,015\,122\,847.$$

Si moltiplichi N per

$$m = 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 = 4\,849\,845.$$

I valori di r e d relativi ad mN sono

$$r = 334\,095\,463, \qquad d = 66\,724\,346,$$

e quindi si ha

$$2r + 1 - d + 2r + 3 + 2r + 5 = 1\,937\,848\,441 = 44\,021^2$$

e pertanto

$$mN = 334\,139\,487 \times 334\,051\,445$$

che dà

$$N = 2\,273 \times 10\,125\,439$$

in cui i due fattori sono primi.

La fattorizzazione diretta di N avrebbe richiesto invece dei soli tre nostri tentativi ben

4 912 149 tentativi!

Naturalmente possono usarsi fattori m di diverso tipo da quello da noi usati.

L'impiego di fattori m più grandi, composti da molti fattori, aumenta la probabilità della loro efficacia, ma d'altra parte se N è grande diminuisce anche molto tale probabilità e rende altresì malagevole il lavoro, perchè esso si deve svolgere su numeri assai alti.

3. FERMAT nelle decomposizioni di numeri N non piccoli, per i quali non era agevole il metodo elementare consistente nel dividere N per tutti i primi $< \sqrt{N}$, si servì altresì di *molte vie e metodi* per ridurre il numero di tali divisioni e certamente delle forme lineari che si addicevano ai divisori dei numeri di data forma, cui furono dati ulteriori notevoli contributi da EULERO e GAUSS.

Ecco ad esempio cosa scrive FERMAT a CARCAVI in una lettera dell'agosto del 1659 (2): « J'avoue que mon invention pour découvrir si un nombre donné est premier ou non n'est pas parfaite, mais j'ai *beaucoup de voies et de méthodes* pour réduire le nombre des divisions et pour les diminuer beaucoup en abrégeant le travail ordinaire. Si M. FRENICLE baille ce qu'il a médité là dessus, j'estime que ce sera un secours très considérable pour les savans ».

Nelle risoluzioni di molte questioni FERMAT si trovò nella necessità di dover riconoscere la primalità di numeri alquanto grandi; una di tali questioni, con la quale i suoi corrispondenti speravano di metterlo in difficoltà, e la cui risoluzione richiedeva il rapido riconoscimento della primalità e la fattorizzazione di numeri non piccoli, è ad esempio contenuta nella lettera di FERMAT

(2) Cfr. l. c in (1), p. 435.

a MERSENNE del martedì 7 aprile 1643 ove il FERMAT scrive testualmente (3): « Vous me demandiez donc quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes :

(6) 214 748 364 800 000, 11, 19, 43, 61, 83, 169, 223, 331, 379, 601, 757, 961, 1 201, 7 019, 823 543, 616 318 177, 6 561, 100 895 598 169.

« Vous me demandiez ensuite si ce dernier nombre est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.

« À la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties.

« À la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux:

898 493 et 112 303

qui sont premiers ».

Ricordiamo che le parti aliquote di un numero N sono i divisori di N minori di N. Ora se indichiamo con N il prodotto dei numeri (6), si ha intanto che

$$N = 2^{36} \times 3^8 \times 5^5 \times 7^7 \times 11 \times 13^2 \times 19 \times 31^2 \times 43 \times 61 \times 83 \times \times 223 \times 331 \times 379 \times 601 \times 757 \times 1\,201 \times 7\,019 \times 616\,318\,177 \times \times 100\,895\,598\,169.$$

FERMAT, per poter procedere nella ricerca della somma delle parti aliquote di N, dovette fattorizzare innanzi tutto $2^{37} - 1$ e riconoscere poi che il numero 616 318 177, certamente non piccolo, è primo (4); dopo di che, indicata con s la somma dei divisori di 100 895 598 169, si trova che il numero N e la somma S dei suoi divisori sono dati rispettivamente da

$$N = M \times 2^6 \times 7\,019 \times 100\,895\,598\,169,$$
$$S = M \times 3 \times 898\,423 \times s,$$

ove M è un prodotto di fattori comuni tra N ed S.

Allora sorge spontaneo di provare, come del resto è stato già

(3) Cfr. l. c. in (1), pp. 255-256.

(4) Nella risoluzione di FERMAT della questione del testo è implicita infatti la notevole fattorizzazione del numero di MERSENNE

$$2^{37} - 1 = 223 \times 616\,318\,177,$$

ove $2^{37} - 1$ dà la somma di tutti i divisori di 2^{36}.

notato [5], se 100 895 598 169 è divisibile per 898 423 e si trova difatti che

$$100\,895\,598\,169 = 898\,423 \times 112\,303$$

e *quindi che, riconosciuta da* FERMAT *la primalità di questi due* ultimi fattori

$$S = 6N,$$

cioè che la somma delle parti aliquote di N è

$$S - N = 5N$$

e così FERMAT potè rispondere alle due questioni, ma egli dovette fattorizzare $2^{37} - 1 = 137\,438\,953\,471$ e riconoscere speditamente (tutto in un sol giorno (!) se rispettò i limiti di tempo fissati nella questione), a prescindere da numeri più piccoli, che

$$112\,303,\ 898\,423,\ 616\,318\,177$$

sono primi.

4. FERMAT alle questioni relative alle parti aliquote connetteva un'importanza forse, eccessiva [6].

Egli ad esempio in una lettera a CARCAVI del 1643 (non si è potuto però precisare completamente la data [7], dopo aver dato un numero *sous-triple* delle somma delle sue parti aliquote, due *sous-quadruple*, due *sous-quintuple* e uno *sous-double* che moltiplicato per 3 diventa un *sous-triple*, aggiunge testualmente: « C'est *parmi quantité d'autres que j'ai trouvés, que j'ai choisi par avance* ceux-ci pour vous en faire part, afin que vous en puissiez juger par cet échantillon. J'ai trouvé la méthode générale pour trouver

(5) Cfr. l. c. in (1), p. 256, nota (1).

(6) Famosa è una sfida (la prima) che FERMAT lanciò a tutti i matematici d'Europa il 3 gennaio 1657 proponendo le due seguenti questioni relative appunto alle parti aliquote:

1ª - Trovare un cubo che, aggiunto alla somma delle sue parti aliquote, faccia un cubo;

2ª - Si domanda anche un numero quadrato che, aggiunto alla somma delle sue parti aliquote, faccia un cubo.

Ne nacque una disputa cui presero parte FERMAT, FRENICLE, WALLIS, VAN SCOOTEN, HUDDE, HUYGENS, BROUNCKER (ed alcuni di quest'ultimi malvolentieri perchè venivano così distratti da ricerche di più alto interesse scientifico) che assunse accenti vivaci, non sempre corretti, con spunti polemici che se destano sorpresa nel lettore interessano però questi vivamente: Cfr. l. c. in (1), t. III, *Traduction du Commercium epistolicum de Wallis.*

(7) Cfr. l. c. in (1), p. 248.

tous les possibles, de quoi je suis assuré que M. DE ROBERVAL sera étonné et le bon PERE MERSENNE aussi; car il n'y a certainement quoi que ce soit dans *toutes les Mathématiques plus difficile que ceci*, et hors M. DE FRENICLE et peut-être M. DESCARTES, je doute que *personne en connoisse le secret*, qui pourtant ne le sera pas pour vous, non plus que mille autres inventions, dont je pourrai vous entretenir un'autre fois ».

Ora su questa questione, che involge quella di riconoscere la primalità e la fattorizzazione di numeri talora non piccoli, noi vogliamo fare un'osservazione che permette di trovare, talvolta a mezzo di qualche tentativo, in maniera però agevole e spesso rapida, moltissimi numeri che sono sottomultipli secondo numeri semplici della somma delle loro parti aliquote. Utilizzando il procedimento che subito esporremo, noi abbiamo ritrovato, quasi sempre con lieve fatica, tutti gli esempi dati da FERMAT.

Si parta da un numero N che sia il prodotto di potenze aventi per basi alcuni dei più piccoli numeri primi ad es. 2, 3, 5 per un numero N_1 da stabilirsi. Si ponga ad es.

$$N = 2^{14} \times N_1$$

e indicata con S ed S_1 la somma dei divisori di N ed N_1 rispettivamente si ha

$$S = 7 \times 31 \times 151 \times S_1 ; \tag{7}$$

assumiamo

$$N_1 = 7 \times 31 \times 151 \times N_2$$

in cui 7, 31, 151 sono i fattori numerici che compaiono nella (7), allora si ha

$$N = 2^{14} \times 7 \times 31 \times 151 \times N_2 ,$$

$$S = 2^{11} \times 7 \times 19 \times 31 \times 151 \times S_2 , \tag{8}$$

si faccia $N_2 = 19N_3$, ove 19 è il nuovo fattore che figura nella (8), cioè si ponga

$$N = 2^{14} \times 7 \times 19 \times 31 \times 151 \times N_3$$

e si ha allora

$$S = 2^{13} \times 5 \times 7 \times 19 \times 31 \times 151 \times S_3 ;$$

infine assumendo $N_3 = 5$, si ha che

$$N = 2^{14} \times 5 \times 7 \times 19 \times 31 \times 151 = 51\,001\,180\,160$$

ha la somma S dei suoi divisori uguale a $3N$ e quindi N è la metà della somma delle sue parti aliquote, conforme all'ultima affermazione dell'ultima lettera citata di FERMAT, ed inoltre si ha che il

numero $3N$ è un terzo della somma delle sue parti aliquote, come lo stesso FERMAT aveva osservato.

Se invece si applica il procedimento al numero

$$N = 2^{36} \cdot N_1$$

si ritrova, mediante la fattorizzazione di $2^{37} - 1$ e il riconoscimento della primalità dei numeri 112 303, 898 423, 616 318 177, la questione, e la risoluzione che FERMAT ne diede, di cui ci siamo occupati al precedente N. 3.

Si tenga presente però che in quest'ultimo esempio, e talvolta anche in altri, conviene attribuire ad uno od a più dei fattori numerici di qualche N_i un esponente maggiore di quello che hanno nel corrispondente S_i.

Infine se si considera il numero

$$N = 2^{p-1} N_1 ,$$

si ha

$$S = (2^p - 1) S_1 ; \tag{9}$$

ora se $2^p - 1$ è primo, ciò che importa che lo sia anche p, e si assume

$$N_1 = 2^p - 1,$$

ove $2^p - 1$ è il fattore che compare nella (9), si ha

$$N = 2^{p-1}(2^p - 1) \tag{10}$$

ed

$$S = (2^p - 1) \cdot 2^p$$

e si ritrova quindi il noto risultato, dovuto ad EUCLIDE, secondo cui i numeri (10), con p e $2^p - 1$ primi, sono perfetti.