All'origine della funzione toziente di Eulero

Questa funzione è stata introdotta dal matematico svizzero Leonhard Euler (1707-1783). Essa è al centro di una memoria apparsa nel 1784, in cui viene trattato il problema di determinare il numero delle frazioni ridotte ai minimi termini che siano strettamente comprese fra 0 ed 1 ed abbiano un denominatore (positivo) assegnato. Detto D questo denominatore, il numero cercato, denotato πD, conta, in effetti, i numeri interi tra 1 e $D-1$ che sono coprimi con D.
L'autore presenta dunque l'esempio del denominatore 24, per il quale elenca i possibili numeratori, che sono complessivamente 8. Dopo di ciò osserva che, se D è primo, allora $\pi D = D-1$.

SPECVLATIONES
CIRCA QVASDAM INSIGNES PROPRIETATES NVMERORVM.

Auctore

L. EVLERO.

§. 1.

Nullum eſt dubium, quin multitudo omnium fractionum diuerſarum, quae inter terminos 0 et 1 conſtitui poſſunt, ſit infinita; vnde cum multitudo omnium numerorum integrorum etiam ſit infinita, manifeſtum eſt, multitudinem omnium plane fractionum adhuc infinities eſſe maiorem; quandoquidem inter binos numeros, vnitate differentes, innumerabiles fractiones diuerſae admitti debent. Hic autem aſſumitur, denominatores fractionum in infinitum augeri poſſe: at ſi terminus praeſcribatur, quem numeratores ſuperare non debeant, tum vtique numerus fractionum, quas inter terminos 0 et 1 conſtituere licet, erit determinatus. Quantus autem iſte numerus ſit futurus, pro quouis limite, qui denominatoribus praeſcribitur, quaeſtio quidem primo intuitu non ita difficilis videtur; verum ſi rem attentius conſideremus, tantae difficultates occurrunt, vt perfecta iſtius quaeſtionis ſolutio vix adhuc ſperari poſſe videatur.

§. 2. Quoniam enim fractiones, de quibus hic quaeritur, omnes inter ſe diuerſae eſſe debent, ex quolibet denominatore aliae fractiones formari nequeunt, niſi quarum numeratores non ſolum ſint denominatore minores, ſed etiam ad eundem primi, quia alioquin ad formam ſimpliciorem, ideoque ad denominatores minores reduci poſſent. Ita cum factio $\frac{15}{24}$ reducatur ad $\frac{5}{8}$, iſta fractio pro denominatore $= 24$ non amplius numerari poterit, quoniam pro denominatore 8 iam eſt numerata. Totum igitur negotium huc redit, vt pro quolibet denominatore, qui ſit $= D$, multitudo numerorum ipſo minorum, et qui cum eo nullum habeant diuiſorem communem, aſſignetur, quippe qui ſoli pro numeratoribus accipi poſſunt. Ita pro denominatore 24 alii numeratores admitti nequeunt, praeter 1, 5, 7, 11, 13, 17, 19, 23, quorum multitudo eſt tantum 8, cuius ratio in compoſitione numeri 24 eſt ſita. Si enim denominator D eſſet numerus primus, tum vtique omnes numeri ipſo minores, quorum multitudo eſt $D-1$, idoneos praeberent numeratores. Quo plures autem denominator D habuerit diuiſores, eo magis multitudo numeratorum reſtringitur.

§. 3. Hinc igitur iſta quaeſtio naſcitur: vt, propoſito quocunque numero D, multitudo numerorum ipſo minorum, ad eumque ſimul primorum, aſſignetur. Quod quo facilius praeſtari poſſit, denotet character π D multitudinem iſtam numerorum ipſo D minorum, et qui cum eo nullum habeant diuiſorem communem. Ac primo quidem manifeſtum eſt, ſi fuerit D numerus primus, fore π D $=$ D $-$ 1. Ante autem quam numeros compoſitos e-

Viene quindi fornita la lista dei valori di πD per i numeri D da 1 a 100:

$\pi\ 1 = 0$	$\pi 21 = 12$	$\pi 41 = 40$	$\pi 61 = 60$	$\pi\ 81 = 54$
$\pi\ 2 = 1$	$\pi 22 = 10$	$\pi 42 = 12$	$\pi 62 = 30$	$\pi\ 82 = 40$
$\pi\ 3 = 2$	$\pi 23 = 22$	$\pi 43 = 42$	$\pi 63 = 36$	$\pi\ 83 = 82$
$\pi\ 4 = 2$	$\pi 24 = 8$	$\pi 44 = 20$	$\pi 64 = 32$	$\pi\ 84 = 24$
$\pi\ 5 = 4$	$\pi 25 = 20$	$\pi 45 = 24$	$\pi 65 = 48$	$\pi\ 85 = 64$
$\pi\ 6 = 2$	$\pi 26 = 12$	$\pi 46 = 22$	$\pi 66 = 20$	$\pi\ 86 = 42$
$\pi\ 7 = 6$	$\pi 27 = 18$	$\pi 47 = 46$	$\pi 67 = 66$	$\pi\ 87 = 56$
$\pi\ 8 = 4$	$\pi 28 = 12$	$\pi 48 = 16$	$\pi 68 = 32$	$\pi\ 88 = 40$
$\pi\ 9 = 6$	$\pi 29 = 28$	$\pi 49 = 42$	$\pi 69 = 44$	$\pi\ 89 = 88$
$\pi 10 = 4$	$\pi 30 = 8$	$\pi 50 = 20$	$\pi 70 = 24$	$\pi\ 90 = 24$
$\pi 11 = 10$	$\pi 31 = 30$	$\pi 51 = 32$	$\pi 71 = 70$	$\pi\ 91 = 72$
$\pi 12 = 4$	$\pi 32 = 16$	$\pi 52 = 24$	$\pi 72 = 24$	$\pi\ 92 = 44$
$\pi 13 = 12$	$\pi 33 = 20$	$\pi 53 = 52$	$\pi 73 = 72$	$\pi\ 93 = 60$
$\pi 14 = 6$	$\pi 34 = 16$	$\pi 54 = 18$	$\pi 74 = 36$	$\pi\ 94 = 46$
$\pi 15 = 8$	$\pi 35 = 24$	$\pi 55 = 40$	$\pi 75 = 40$	$\pi\ 95 = 72$
$\pi 16 = 8$	$\pi 36 = 12$	$\pi 56 = 24$	$\pi 76 = 36$	$\pi\ 96 = 32$
$\pi 17 = 16$	$\pi 37 = 36$	$\pi 57 = 36$	$\pi 77 = 60$	$\pi\ 97 = 96$
$\pi 18 = 6$	$\pi 38 = 18$	$\pi 58 = 28$	$\pi 78 = 24$	$\pi\ 98 = 42$
$\pi 19 = 18$	$\pi 39 = 24$	$\pi 59 = 58$	$\pi 79 = 78$	$\pi\ 99 = 60$
$\pi 20 = 8$	$\pi 40 = 16$	$\pi 60 = 16$	$\pi 80 = 32$	$\pi 100 = 40$

Più avanti, Eulero enuncia e dimostra la formula per il calcolo di πN a partire dalla fattorizzazione di *N*. Dopo aver formulato il relativo quesito ed averne proposto la soluzione, Eulero aggiunge un esempio di applicazione:

Problema.

Propoſito numero quocunque N inuenire multitudinem omnium numerorum ipſo minorum ad eumque primorum.

Solutio.

§. 16. Quicunque fuerit numerus N, ſemper tali forma repraeſentari poteſt, vt ſit $N = p^\alpha q^\beta r^\gamma s^\delta$ etc. exiſtentibus p, q, r, s numeris primis. Inuenimus autem tum fore

$$\pi N = p^{\alpha-1} q^{\beta-1} r^{\gamma-1} s^{\delta-1} (p-1)(q-1)(r-1)(s-1).$$

Hinc igitur erit

$$\frac{\pi N}{N} = \frac{(p-1)(q-1)(r-1)(s-1)}{pqrs},$$

vnde ſequitur fore

$$\pi N = \frac{N(p-1)(q-1)(r-1)(s-1)}{pqrs};$$

ita vt iam non amplius opus ſit exponentes $\alpha\ \beta\ \gamma$ noſſe, ſed ſufficit omnes numeros primos p, q, r, s diuerſos indagaſſe, per quos numerus propoſitus N eſt diuiſibilis; quibus cognitis multitudo numerorum, minorum quam N et qui ſimul ad eum ſunt primi, erit

$$\pi N = \frac{N(p-1)(q-1)(r-1)(s-1)}{pqrs}.$$

§. 17. Ita ſi v. gr. propoſitus fuerit iſte numerus: $N = 9450$, numeri primi, per quos hunc numerum diuidere licet, ſunt 2, 3, 5, 7, quandoquidem per nullos alios diuiſionem admittit; hinc igitur erit

$$\pi\, 9450 = \frac{9450.1.2.4.6}{2.3.5.7} = 2160.$$

L'argomento sarà ripreso da Gauss nelle *Disquisitiones Arithmeticae*, a cui risale l'attuale notazione con la lettera greca ϕ.

Theoremata varia.

38.

PROBLEMA. ***Invenire, quot numeri positivi dentur numero positivo dato A minores simulque ad ipsum primi.***

Designemus brevitatis gratia multitudinem numerorum positivorum ad numerum datum primorum ipsoque minorum per praefixum characterem ϕ. Quaeritur itaque ϕA.

I. Quando A est primus, manifestum est omnes numeros ab 1 usque ad $A-1$ ad A primos esse; quare in hoc casu erit

$$\phi A = A - 1$$

II. Quando A est numeri primi potestas puta $= p^m$, omnes numeri per p divisibiles ad A non erunt primi, reliqui erunt. Quamobrem de $p^m - 1$ numeris hi sunt reiiciendi: $p, 2p, 3p \ldots (p^{m-1}-1)p$; remanent igitur $p^m - 1 - (p^{m-1}-1)$ sive $p^{m-1}(p-1)$. Hinc

$$\phi p^m = p^{m-1}(p-1)$$

III. Reliqui casus facile ad hos reducuntur ope sequentis propositionis: *Si A in factores M, N, P etc. inter se primos est resolutus, erit*

$$\phi A = \phi M . \phi N . \phi P \text{ etc.}$$

Interessante è, al successivo paragrafo – che si apre con una giustificazione della scelta di porre, diversamente da Eulero, $\phi(1)=1$ - la dimostrazione dell'identità tra un numero intero positivo A e la somma delle funzioni di Eulero dei suoi divisori positivi.

39.

Si characteris ϕ significatio ita determinatur, ut ϕA exprimat multitudinem numerorum ad A primorum ipsoque A non maiorum, perspicuum est $\phi 1$ fore non amplius $=0$, sed $=1$, in omnibus reliquis casibus nihil hinc immutari. Hancce definitionem adoptantes sequens habebimus theorema.

Si a, a', a'' etc. sunt omnes divisores ipsius A (unitate et ipso A non exclusis), erit

$$\phi a+\phi a'+\phi a''+\text{etc.}=A$$

Ex. sit $A=30$, tum erit $\phi 1+\phi 2+\phi 3+\phi 5+\phi 6+\phi 10+\phi 15+\phi 30 = 1+1+2+4+2+4+8+8=30$.

Demonstr. Multiplicentur omnes numeri ad a primi ipsoque a non maiores per $\frac{A}{a}$, similiter omnes ad a' primi per $\frac{A}{a'}$ etc., habebunturque $\phi a+\phi a'+\phi a''+$ etc. numeri, omnes ipso A non maiores. At

1) omnes hi numeri erunt inaequales. Omnes enim eos qui ex *eodem* ipsius A divisore sint generati, inaequales fore, per se clarum. Si vero e divisoribus diversis M, N numerisque μ, ν ad istos respective primis aequales prodiissent, i. e. si esset $\frac{A}{M}\mu=\frac{A}{N}\nu$, sequeretur $\mu N=\nu M$. Ponatur $M>N$ (id quod licet). Quoniam M ad μ est primus, atque numerum μN metitur, etiam ipsum N metietur, maior minorem. *Q. E. A.*

2) inter hos numeros, omnes hi $1, 2, 3 \ldots A$ invenientur. Sit numerus quicunque ipsum A non superans t, maxima numerorum A, t communis mensura δ eritque $\frac{A}{\delta}$ divisor ipsius A ad quem $\frac{t}{\delta}$ primus. Manifesto hinc numerus t inter eos invenietur qui ex divisore $\frac{A}{\delta}$ prodierunt.

3) Hinc colligitur horum numerorum multitudinem esse A, quare

$$\phi a+\phi a'+\phi a''+\text{etc.}=A. \quad \textit{Q. E. D.}$$

Il ragionamento è il seguente. Dato un divisore positivo a di A, si moltiplicano tutti gli ($\phi(a)$) interi positivi coprimi con a e non maggiori di a per $\frac{A}{a}$. In questo modo si ottengono numeri (interi positivi) a due a due distinti, e non maggiori di A. Sono infatti naturalmente tra loro distinti i prodotti ottenuti a partire dallo stesso valore di a (poiché cambia uno dei fattori, rimanendo invariato l'altro, che è sempre uguale ad $\frac{A}{a}$). Consideriamo allora due divisori distinti M ed N di A, e supponiamo per assurdo che, in corrispondenza di due numeri μ,ν, coprimi e non maggiori rispetto a M ed N rispettivamente, si verifichi l'uguaglianza $\frac{A}{M}\mu=\frac{A}{N}\nu$. Allora si avrà $\mu N=\nu M$. Senza ledere la generalità, si può supporre che sia $M>N$. Poiché M divide il numero μN, ma è coprimo con μ, necessariamente deve dividere N, il che però è impossibile, essendo M maggiore di N.

Inoltre, ogni numero intero compreso fra 1 ed A compare tra i prodotti indicati. Infatti, detto t un numero siffatto, e posto $\delta = \mathrm{MCD}(A,t)$, t si otterrà come prodotto fra $\frac{t}{\delta}$, numero non maggiore del divisore $(a =)\frac{A}{\delta}$ di A, e con esso coprimo, e il quoziente $(\frac{A}{a} =)\delta$. In conclusione, i prodotti ottenuti nel modo suindicato sono, senza ripetizioni, tutti i numeri interi compresi fra 1 ed A. Ma questi sono evidentemente tanti quanto il valore della somma dei numeri $\phi(a)$.

Il nome *totient* è stato introdotto alla fine dell'Ottocento dal matematico britannico James Joseph Sylvester, probabilmente per assonanza con il termine *quotient*: se, in latino, *quotiens* significa "quante volte", *totiens* si traduce come "tante volte", e questa espressione ben si addice al risultato di un conteggio aritmetico.