Fermat e Tartaglia:
alcune condizioni necessarie e sufficienti affinché un intero positivo n sia primo

di
Antonio Rita

Premessa

E' bello immaginare che nell'Aldilà ci sia un'anima responsabile per ogni branca del sapere umano la quale indirizza ed aiuta lo sviluppo delle conoscenze che meglio possano contribuire al benessere dell'umanità. Se così fosse, Niccolò Tartaglia (1499-1557) avrebbe il compito di fornire al genere umano le indicazioni per individuare ad uno ad uno tutti i numeri primi contenuti in N, insieme dei numeri naturali positivi. Per adempiere al delicato incarico, Tartaglia potrebbe avvalersi della collaborazione di Pierre de Fermat (1601-1665).

Tale scelta non vuole significare poca riconoscenza nei confronti di Carl Friedrich Gauss[1] (1777-1855) e del suo allievo Bernhard Riemann (1826-1866) che hanno fornito contributi insostituibili sia allo studio dei numeri primi che allo sviluppo di tutte le branche della matematica e delle altre materie scientifiche. Ad esempio, Albert Einstein (1879-1955) non avrebbe avuto gli strumenti di base per formulare la *Teoria della Relatività Generale* senza gli studi e le applicazioni di Gauss e di Riemann.

Il contenuto di questo articolo ha un obiettivo importante: *mettere in evidenza come lo studio e la distribuzione dei numeri primi nell'insieme N può ancora avere bisogno di tecniche di calcolo elementari.* Questo può valere anche per la scomposizione in fattori primi di un numero composto e di altri importanti enigmi dell'insieme N ancora da dimostrare (la congettura dei numeri primi gemelli, quella di Goldbach, ecc).

In generale, partendo da teoremi con una soluzione facile, si cerca di far emergere che lo studio della matematica è una bellissima avventura intellettuale ed una magnifica sfida a cui molti, in particolare giovani, possono partecipare e verificare che certi argomenti non sono solo per studiosi e ricercatori.

I grandi problemi della matematica, in genere, nascondono soluzioni semplici, eleganti ed accessibili a molti; dopo che sono stati formulati hanno bisogno solo di essere diffusi con un impegno adeguato. Si può citare ad esempio

---

[1] " Il teorema dei numeri primi" di Gauss che riguarda la distribuzione asintotica dei numeri primi, da una distribuzione approssimata degli stessi e presenta, inoltre, un legame profondo con la funzione Z di Riemann che sarebbe legata alla distribuzione effettiva dei numeri primi di N dai suoi zeri nel campo complesso C (congettura nota come "Ipotesi di Riemann: tutti gli zeri complessi della funzione Z hanno parte reale ½").

la brillante soluzione elaborata da Euclide (III secolo d.c.) per la dimostrazione che i numeri primi sono infiniti; nonostante sia comprensibile a molti è quasi sconosciuta sia ai giovani che ai meno giovani.

Queste poche righe sono necessarie per rammentare che il rapido evolversi delle numerose conoscenze matematiche degli ultimi quattro secoli ha radici profonde anche nella scuola di matematica italiana del tardo Rinascimento. Questo progresso, infatti, è stato determinato in gran parte dall'impegno profuso da tutti i matematici per risolvere i geniali enigmi formulati da Fermat, grazie agli studi di Galilei e di Tartaglia.

Ad un altro francese (Mersenne) vanno riconosciuti grandi meriti perché ha raccolto e diffuso gli studi e le ricerche delle migliori menti del mondo scientifico francese, italiano ed europeo, vissute nella prima metà del XVII secolo.

Il circolo culturale di Marin Mersenne (1588-1648)

Il monaco Marin Mersenne (teologo, filosofo e matematico), persona cordiale ed ortodossa sia in campo scientifico che religioso, è noto soprattutto per aver compilato una *"lista"* di undici numeri primi ricavati dalla espressione $M_p = 2^p - 1$ (numero di Mersenne di indice p, con $2 \leq p \leq 257$ numero primo). Detta "lista" comprendeva anche M_{67} e M_{257} che non sono primi ma non includeva M_{61} , M_{89} e M_{107} che in effetti sono primi.

I numeri primi di Mersenne finora conosciuti sono quarantasette di cui il più piccolo è $M_2=2^2-1= 3$, poi abbiamo $M_3=7$, $M_5 =31$, $M_7 =127$, $M_{13}=8191$, M_{17} , M_{19}, M_{31} , M_{61} , M_{89} , M_{107} , M_{127} (dodicesimo numero primo di Mersenne), e così via; il più grande numero primo di Mersenne conosciuto è $M_{43.112.609} = 2^{43112609} - 1$ che risulta proprio il quarantasettesimo. Come si può facilmente verificare, essi hanno un numero rilevanti di cifre per cui possono essere scritti e letti solo nella notazione esponenziale.

E' opportuno ricordare che Marin Mersenne ha svolto un ruolo notevole nella diffusione delle nuove teorie scientifiche in quanto si faceva promotore di periodiche riunioni a cui partecipavano gran parte degli scienziati francesi della prima metà del '600 come Cartesio (1596-1650), Fermat (1601-1665), Pascal (1623-1662), Desargues (1591-1661), ecc. Era inoltre in corrispondenza con gli italiani Galileo Galilei (1564-1642), Bonaventura Cavalieri (1598-1647), Evangelista Torricelli (1608-1647),ecc.

Il circolo culturale gestito da Mersenne ha funzionato come una vera e propria officina dove venivano confrontate e diffuse le idee non solo dei geni francesi ma anche degli italiani e di altri scienziati europei. Il monaco francese ha espresso più volte la solidarietà a Galilei per le sue note disavventure giudiziarie ed alcuni ipotizzano che dopo l'abiura lo abbia consigliato di pubblicare i suoi scritti in Olanda (*Il discorso intorno a due nuove scienze*). Tanto cortesia costringeva il nostro Galilei, che non aveva un buon carattere e alcuna attitudine alle relazioni umane, ad essere più aperto e quindi fornire ai soci del circolo contributi scientifici

rilevanti; si può ipotizzare che abbia descritto dettagliatamente non solo le sue convinzione riguardante i *principi della relatività* ma ha parlato anche della "*numerabilità dei quadrati dei numeri interi*" e delle numerose altre proprietà ricavate dagli studi di Tartaglia.

In effetti, Mersenne ha svolto il ruolo di traduttore e divulgatore delle opere di Galileo Galilei e di tanti altri. In particolare, ha ripreso e diffuso, in modo abile e coinvolgente, i teoremi senza dimostrazione di Pierre de Fermat allo scopo, non solo di suscitare interesse, ma di accendere vere e proprie sfide tra i matematici europei dell'epoca.

Questo è, pertanto, un forte indizio di come gli studi di Tartaglia e di Galilei siano stati utilizzati da Fermat per formulare i suoi tre più famosi enigmi. Le congetture relative al "piccolo" ed "ultimo" teorema di Fermat" sono state incluse nell'articolo dal titolo "I quadrati di Galileo Galilei" (bookshelf di Rudi Mathematici) e quindi viene riproposta solo quella conosciuta come "i numeri primi di Fermat", che si è dimostrata errata. La terza congettura risulta così sintetizzabile:

I numeri interi $F_n = 2^p+1$ *sono primi quando l'intero p assume valori di potenza di 2, cioè* $p=2^n$ *con n intero qualsiasi.*

Abbiamo che i primi cinque numeri di Fermat sono effettivamente primi e cioè: $F_0=2^0+1=2$, $F_1=2^2+1=5$, $F_2=2^4+1=17$, $F_3=2^8+1=257$, $F_4= 2^{16}+1=65537$, mentre gli altri probabilmente sono tutti composti con una peculiarità che li classificherebbe, comunque, come "*falsi primi*"(concetto che vedremo più avanti). Eulero, infatti, ha scoperto i divisori di $F_5=2^{32}+1$, la cui struttura offre indicazione utili ad individuare i divisori di $F_6 =2^{64}+1$ e così via (i dettagli saranno oggetto di un altro articolo, dedicato a Fermat, Tartaglia ed Eulero).

La terza congettura di Fermat possiamo, ormai, considerarla un supporto alla "lista" che Mersenne elaborò proprio con la speranza di mettere in condizione qualche matematico di trovare una relazione per esprimere con notazioni esponenziali qualche famiglia di numeri primi.

Brevi note storiche sul triangolo di Tartaglia

Prima di passare ad esaminare alcune importanti proprietà (in gran parte note ma poco utilizzate) dei singoli coefficienti contenuti nel triangolo di Tartaglia è opportuno presentare al lettore alcune brevi note storiche sulla più famosa *tabella* della matematica.

Il metodo di calcolo dei coefficienti binomiali è stato descritto da Niccolò Tartaglia in un ampio volume dal titolo "**Generale Trattato di Numeri e Misure"**: *grande opera di matematica elementare, scritto nel 1560 e contenente numerosi problemi risolvibili con semplici equazioni di primo grado ed applicati, in gran parte, al calcolo della probabilità con cui si verifica un evento casuale*.

In effetti, il metodo descritto dal matematico veneziano era noto in Cina già da molti anni ed il matematico Zhu Shijie lo rappresentò, nell'anno1303, nella

"*Tavola del Vecchio Metodo dei Sette Quadrati Moltiplicatori*", lasciando intendere che la sua opera fosse una riedizione di conoscenze elaborate in vari paesi dell' Asia (Cina, Persia, India), in epoche molte antiche . Anche Blaise Pascal ha scritto nel 1564, quasi un secolo dopo Tartaglia, un testo dedicato all'argomento dal titolo "*Le* T*riangle Aritmétique*" utilizzato, in particolare, per lo studio del calcolo combinatorio.

Oggi il *triangolo dei coefficienti binomiali* è noto, soprattutto nei paesi anglosassoni e francofoni, con il nome di "Triangolo di Pascal". In Germania la elaborazione di detta tavola è attribuita a Stiefel che l'ha descritta in un elaborato del 1544.

Isaac Newton, nella seconda metà del XVII, elaborò un metodo nuovo per ricavare i coefficienti binomiali, particolarmente apprezzato da quei matematici che si occupavano degli studi sulle teorie analitiche; ha messo, infatti, tutti d'accordo sul fatto che il calcolo dello sviluppo della potenza ennesima di un binomio risultasse molto più facile eseguirlo con la bella e semplice formula del *teorema del binomiale:* $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Il presente articolo non vuole ripristinare l'uso della tabella per calcolare la potenza ennesima di un binomio, ma semplicemente far osservare al lettore che con gli elementi del triangolo di Tartaglia si possono costruire altri tipi di polinomi omogenei (di cui parleremo nel prossimo articolo). Sono polinomi importanti perché da questi polinomi Fermat ha ricavato gli elementi necessari alla formulazione del suo più famoso ed avvincente enigma della storia della matematica, noto come "Ultimo Teorema di Fermat".

Si propone, invece, l'obiettivo di stimolare il lettore ad approfondire l'argomento per comprendere quali proprietà possiedono gli elementi di una qualunque riga orizzontale o quelli allineati su una linea obliqua, e le modalità con cui le stesse si ripetono nel triangolo di Tartaglia, ecc.

I numeri primi e il "Triangolo Universale" di Tartaglia

Il triangolo di Tartaglia, può essere costruito per ogni nϵN. E' una tabella sintetica, a forma di triangolo, ed è costituita da righe parallele da cui si ricavano i coefficienti necessari a scrivere lo sviluppo di una qualsiasi potenza di un binomio. La generica riga ennesima è implementata a partire dagli elementi della riga (n-1) e serve a sviluppare il binomio $(x+y)^n$.

L'i-esimo elemento sulla riga n lo abbiamo indicato con $\Gamma_{i,n}$ (*gamma maiuscolo con i ed n)*, solo per tener conto che Fermat non conosceva i simboli della formula di Newton; in effetti, abbiamo che $\Gamma_{i,n}=\binom{n}{i}=n!/i!(n-i)!$.

La tabella può essere costruita come un triangolo isoscele rovesciato (vertice verso il basso) i cui lati obliqui sono le linee esterne formate da tutti 1 e l'altezza quella linea immaginaria che intercetta i coefficienti centrali dei numeri pari . Le

basi dei vari triangoli sono ovviamente le linee orizzontali costituite dagli (n+1) coefficienti binomiali della generica riga n.

La suddetta tabella, costruita per ogni nϵN fino all'infinito che potremmo chiamare "triangolo universale di Tartaglia", offre la possibilità di ricavare molte informazioni solo osservando sia la disposizione ordinata dei coefficienti lungo le sue linee orizzontali ed oblique che la loro composizione fattoriale. In sintesi si possono ricavare importanti proprietà, come:

1) tutti i numeri primi n>2 delimitano, all'interno del triangolo universale costruito con vertice verso il basso (rovesciato), un altro triangolo , disposto con vertice verso l'alto, che ha come base la linea orizzontale (n-1), quella del numero pari immediatamente prima di n e come lati le linee oblique che hanno origine ai vertici della base nei coefficienti 1 e si sviluppano ognuna parallelamente ai lati del triangolo principale. I due lati obliqui si incontrano, formando il terzo vertice, nel coefficiente binomiale centrale ($\binom{2(n-1)}{n-1}$) del numero pari 2(n-1);

2) tutti i coefficienti contenuti in questo triangolo secondario, generato dal numero primo n e denominato T_n, hanno come fattore n ad eccezione di quelli della base (riga n-1) . Ogni singolo triangolo T_n è interconnesso almeno con il triangolo generato dal numero primo immediatamente più piccolo e con quello del numero primo immediatamente più grande di n (postulato di Bertrand dimostrato da Chebychev nel 1850) . La famiglia dei triangoli T_n forma una grande catena all'interno del triangolo di Tartaglia;

3) la base di T_n, per un qualsiasi numero primo n>2, coincide con la linea del numero pari (n-1) i cui coefficienti, ad eccezione del primo e dell'ultimo, possono essere trasformati in multipli di n semplicemente aggiungendo alternativamente +1 e -1 . I coefficienti che si ottengono con questo artificio sono pertanto legati sia alla linea n che alla linea (n-1); sono, infatti, quelli del polinomio omogeneo di grado (n-1) che si ottengono dividendo il "Cuore di Tartaglia" di $(x+y)^n$ per la somma delle basi ovvero sono ricavati dalla divisione $C_{(x+y)}{}^n/(x+y)$. Con il simbolo $C_{(x+y)}{}^n$, denominato "Cuore di Tartaglia", indichiamo lo sviluppo ordinato di $(x+y)^n$ privato del primo (x^n) ed ultimo termine (y^n) ;

4) il generico numero primo n caratterizza certamente la linea orizzontale di cui fa parte con il fatto che i coefficienti, escluso i due estremi, sono multipli di n , ma anche quella obliqua che ha come secondo elemento n (origine sempre in 1) e si sviluppa fino all'infinito parallelamente alla linea principale degli 1. Su tale linea obliqua, infatti, i coefficienti binomiali sono tutti caratterizzati dalla circostanza di avere n come fattore ad esclusione di quelli che si posizionano nell'incrocio con le linee orizzontali multiple di (n-1). Sulla ennesima linea obliqua dopo 1 abbiamo consecutivamente (n-1) coefficienti che presentano n come fattore e tale circostanza si esaurisce nell'incrocio con la linea orizzontale 2(n-1) per poi riprendere a 2n e fermarsi all'incrocio con la linea 3(n-1) e così via fino all'infinito;

5) in sintesi sulle linee oblique dei numeri primi n, genericamente indicate con L_n, troviamo fino all'infinito lo stesso numero primo n come fattore nei relativi coefficienti ad eccezione proprio quando la linea obliqua incrocia le linee orizzontali multiple di (n-1);

6) le linee oblique L_n del numero primo n quando tagliano un triangolo T_i del numero primo i, presentano nei coefficienti comuni a T_i , oltre a i anche il fattore primo n.

7) Ogni elemento *(coefficient*e) $\Gamma_{n,k} = \binom{n}{k}$ della riga ennesima può essere ricavato, in modo pratico dagli elementi della riga (n-1) ovvero da quelli della linea obliqua L_{k-1} . Ad esempio, il kappa-esimo elemento della riga ennesima $\binom{n}{k} = \Gamma_{n,k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ si ottiene di norma come somma di due coefficienti adiacenti della riga (n-1) ma anche come somma dei primi (n-1) coefficienti situati sulla linea obliqua L_{k-1} a partire da 1 e fino all'elemento che essa intercetta sulla riga orizzontale (n-1).

Il lettore che vuole approfondire le proprietà del triangolo di Tartaglia può utilizzare il computer evidenziando con colori diversi alcune caratteristiche tra quelle innanzi descritte di un numero primo scelto a caso. Ad esempio, per un qualsiasi n primo, può verificare come il triangolo T_n si espande all'interno della tabella di Tartaglia, moltiplicandosi sia verticalmente che orizzontalmente, fino all'infinito, fornendo esplicite indicazioni sui multipli di n.

Un' altra proprietà che si rileverà decisiva per la elaborazione di una soluzione elementare dell'Ultimo Teorema di Fermat è ricavabile proprio da uno studio approfondito del triangolo di Tartaglia. E' quella riportata nel lemma seguente, che giustamente prende il nome del nostro grande matematico veneziano in quanto ha lo scopo di legare Fermat a Tartaglia (è tratto dal testo scritto da Antonio Rita ed edito dalla casa editrice di Roberta Fiore di Potenza, in corso di pubblicazione).

E' opportuno ricordare che gli stessi risultati si possono ricavare dal binomio di Newton che però era sconosciuto a Fermat.

Il Primo Teorema di Tartaglia

Se n è un qualsiasi numero intero di $N_0=N+\{0\}$, i coefficienti della ennesima riga di Tartaglia hanno come somma 2^n; per i soli coefficienti del Cuore di Tartaglia la somma è pari a $2^n - 2 = 2\left(2^{n-1} - 1\right)$. In sintesi, gli addendi dello sviluppo di un binomio elevato alla potenza ennesima $(x+y)^n$ sono 2^n, mentre quelli del polinomio omogeneo, denominato "Cuore di Tartaglia" ed indicato con il simbolo $C_{(x+y)}{}^n$ sono (2^n-2).

Se $(x,y)\epsilon N^2$ è una qualunque coppia di interi positivi possiamo scrivere:

$$(x+y)^n = (x+y)(x+y)^{n-1} = (x+y)(x+y)(x+y)^{n-2} = \left(x^n\right) + \left(x^{n-1}y\right) + \ldots\ldots + \left(xy^{n-1}\right) + \left(y^n\right)$$

Lo sviluppo del binomio alla ennesima potenza è costituito da un numero di addendi con coefficiente unitario pari alle combinazioni con ripetizioni dei due

elementi x,y su n posti che risulta pari proprio a 2^n. E' immediatamente verificabile anche che è vera per:

a) n=0

$2^0 = 1$ e tale risulta $(x+y)^0 = 1$;

b) n=1

$2^1 = 2$ che uguaglia la somma dei coefficienti unitari di $(x+y)^1 = x+y$;

c) n=2

$2^2 = 4$ rappresenta anche la somma dei quattro coefficienti unitari del binomio $(x+y)^2 = x^2 + xy + xy + y^2$.

Per n=3 si hanno otto addendi e così via. La dimostrazione risulta vera per ogni n proprio in base al principio di induzione.

Infatti, essendo vera per n=1 e se la supponiamo vera per (n-1) ovvero se abbiamo che $\sum_{i=o}^{n-1}\binom{n-1}{i} = 2^{n-1}$ (una sommatoria di 2^{n-1} coefficienti unitari) si ottiene di conseguenza che $\sum_{i=0}^{n}\binom{n}{i} = 2*2^{n-1} = 2^n$ in quanto gli addendi di coefficienti unitari di $(x+y)^n$ sono il doppio di quelli di $(x+y)^{n-1}$

Dal triangolo di Tartaglia e dallo sviluppo di un binomio all' ennesima potenza possiamo facilmente ricavare quanto segue:

1) la somma dei coefficienti di un qualsiasi binomio elevato alla potenza ennesima è pari 2^n, quella dei coefficienti della riga (n-1) risulta 2^{n-1} e quindi risulta la metà della riga successiva. In generale, la somma dei coefficienti della riga i è pari 2^i da cui si può ottenere quella della riga n>i moltiplicandola per 2^{n-i}.

2) tutte le potenze ennesime di un binomio hanno ovviamente in comune i fattori primi della somma delle basi; la somma dei coefficienti delle varie righe hanno in comune, invece, solo e sempre il fattore 2.

Quanto sopra detto è valido, oltre che per i binomi, per i trinomi, per i quadrinomi ovvero per i polinomi in genere. Ripetendo gli stessi ragionamenti, avremo pertanto:

La somma dei coefficienti di un qualsiasi polinomio elevato alla ennesima potenza è pari a x^n dove x è il numero intero che indica il numero di addendi del polinomio di base cioè x=1,2,3 quando parliamo rispettivamente di monomi, di binomio, di trinomio e così via.

In sintesi, il numero delle disposizioni con ripetizioni di 2 oggetti su n posti, pari a 2^n, eguaglia la somma dei coefficienti binomiali di una potenza ennesima;il numero di disposizioni con ripetizioni di 3 oggetti su n posti risulta pari a 3^n, che rappresenta il numero complessivo degli addendi che si ricavano dallo sviluppo

della potenza ennesima di un trinomio. Ciò può essere ripetuto per la potenza di un polinomio qualsiasi.

Il teorema della funzione dei numeri primi

Se n>2 è un qualsiasi numero primo di N, si ha che $(2^n-2)=2*3*n*q$ *con q un intero positivo dispari non multiplo di n;in generale, per ogni numero primo di N, il rapporto* $(a^n-a)/n=a*3*q$ *è intero con* $a\epsilon N$ *intero maggiore di 1.*

Anche senza far riferimento al "piccolo teorema di Fermat" ed alla dimostrazione di Eulero, se n è un numero primo, risulta evidente che il rapporto $(2^n-2)/n$ è un numero intero in quanto il numeratore della divisione (2^n-2) altro non è che la somma dei soli coefficienti del "Cuore di Tartaglia $C_{(x+y)}{}^n$" del generico binomio elevato alla potenza ennesima. Ognuno di questi coefficienti (addendi), infatti, contiene n come fattore primo e quindi esso è necessariamente presente nel risultato della loro somma.

Non comporta eccessive difficoltà verificare che il risultato di (2^n-2), quando n>2 è primo, risulta divisibile per 3 una o più volte ma sempre una sola volta sia per 2 che per n.

Possiamo ricavare da quanto sopra la funzione reale $y=2(2^{x-1}-1)/x$, definita per $\forall\, x\epsilon R-\{0\}$, che in R^- assume sempre valori non interi mentre in R^+ si ottengono valori interi ogni qualvolta x è un numero primo oppure un "falso primo"(concetto che verrà ripreso più avanti). L'espressione $y=2(2^{x-1}-1)/x$ fornisce ordinatamente a partire da 2 la lista di tutti i numeri primi a cui si aggiungono in modo casuale alcuni interi positivi composti, detti pseudo primi di (2^n-2) o semplicemente *falsi primi*. I cinesi, già 2500 anni fa, utilizzavano tale relazione per verificare se n fosse primo o meno , quando nella Magna Grecia, Pitagora disquisiva del più famoso teorema della matematica e della perfezione dei numeri interi. Il metodo è caduto in disuso con la scoperta dei falsi primi.

Si ritiene di denominarla "funzione dei numeri primi" proprio perché da essa è possibile evidenziare non solo i numeri primi ma anche le condizioni essenziali dell'esistenza di infiniti "falsi primi" allo scopo di comprendere meglio le loro proprietà. E' da tener presente che potrebbe essere molto utile anche nella scomposizione in fattori dei numeri composti. La denominazione deriva anche dal fatto che tale relazione, quando n è primo, ha un legame inscindibile con la relazione x^n+y^n dell'Ultimo Teorema di Fermat.

Quando x è un numero intero positivo, il fattore $(2^{x-1}-1)$ può essere espresso con una sommatoria di addendi, ovvero $y_s= 2^{x-1}-1=2^{x-2}+2^{x-3}+\ldots\ldots+2^3+2^2+2+1$ che prende il nome di "funzione dei numeri primi semplificata". Nella suddetta ipotesi di $x\epsilon N$, possiamo porre n=x e, quindi, abbiamo che tale sommatoria o "serie speciale" è costituita dalla somma di (n-1) potenze di 2 decrescenti a partire da (n-2) ed ha la particolarità che ogni singolo addendo è pari alla somma meno 1 degli addendi che lo precedono. Tale sviluppo in "serie speciale" non è l'unico; per avere informazioni più dettagliate è opportuno uguagliarla alla sommatoria degli

(n-1) addendi rappresentati dai coefficienti binomiali $\Gamma_{n-1,k}=\binom{n-1}{k}$ della riga (n-1), escludendo il primo: $y_s=(n-1)+\Gamma_{(n-1),2}+\ldots..+(n-1)+1=(2^{n-1}-1)$.

La funzione dei numeri primi evidenzia, pertanto, una particolare famiglia di numeri interi composti che si comportano, pur essendo composti come veri e propri primi per la relazione $y=(2^n-2)$. I "falsi primi n=ab" , infatti, sono quelli che presentano un risultato intero del rapporto $(2^n-2)/n$; tali falsi primi hanno un inscindibile legame con i numeri pari.

A tale scopo, l'insieme dei numeri pari (N_p) può essere considerato suddiviso in due sottoinsiemi disgiunti con un numero di elementi perfettamente uguale. Abbiamo, pertanto: 1) il sottoinsieme dei numeri pari divisibile una sola volta per 2 indicato con il simbolo $N_{ps}=\{2, 6, 10, 14,\ldots..,n=2d,\ldots\}$, con d numero dispari (*da leggere sottoinsieme delle parità semplice*); 2) il sottoinsieme dei numeri pari divisibile almeno per 4, indicato con $N_{pm}=\{4, 8, 12, 16,\ldots., n=4p,\ldots.\}$, con p numero intero che può risultare pari o dispari (*da leggere sottoinsieme delle parità multiple*).

Ad esempio, è semplice verificare che se n è un falso primo dispari, (n-1) ha sempre *parità multipla*, mentre i falsi primi pari sono sempre di *parità semplice* . I falsi primi o pseudo primi di (2^n-2) sono infiniti e sono sia pari che dispari. Il più piccolo falso primo è 341=11*31 e seguono: 561, 1.105, 1.729, ecc; il più piccolo falso primo pari è 161.038.

In sintesi, la funzione dei numeri primi, espressa dalla relazione canonica $y=2(2^{n-1}-1)$ o dalla "serie speciale"ricavata dalla somma dei coefficienti binomiali della riga ennesima, fornisce indicazioni sufficienti a separare i numeri primi dai falsi primi. Le uniche vere difficoltà sono contenute nei numeri di Fermat perché, quando non sono primi, risultano "falsi primi speciali"nel senso che hanno una proprietà che gli altri non hanno (l'argomento è interessante ma vasto e sarà ripreso in un altro articolo dedicato proprio ai numeri di Mersenne e di Fermat)).

Il paragrafo seguente è una breve sintesi di alcuni teoremi contenuti nel testo sopra menzionato intitolato "La funzione dei numeri primi".

La funzione dei numeri primi "ridotta o della linea centrale"

In questo paragrafo tratteremo, in due lemmi diversi, la condizione necessaria e sufficiente affinché un numero intero n dispari possa essere primo. Nel primo lemma parleremo delle proprietà degli *n* coefficienti della riga *(n-1)* del triangolo di Tartaglia.

Il generico coefficiente di base *a=0, 1, 2,....,(n-1)* ed, in particolare essendo *n* dispari, quello centrale della riga *(n-1)* del triangolo di Tartaglia , con la formula binomiale di Newton, sono così scritti:

5.3.1) $\binom{n-1}{a}=\Gamma_{a,n-1}=[(n-1)(n-2)(n-3)\ldots..(n-a)]/2*3*4*\ldots\ldots.*a$, con a>0

5.3.2) $\binom{n-1}{(n-1)/2}=\Gamma_{(n-1)/2,n-1}=[(n-1)(n-2)(n-3)\ldots.(n+1)/2]/[2*3*4*\ldots..(n-1)/2]$.

Quando *n* è primo, con semplici esercizi si può constatare che se ai singoli coefficienti binomiali della riga *(n-1),* escludendo il primo e l'ultimo che sono unitari, viene aggiunto alternativamente +1 e -1, si ottengono *(n-1)* espressioni ($\Gamma_{a,n-1}\pm1$) tutte con il numeratore divisibile per n. Tali espressioni sono i coefficienti del polinomio omogeneo ${}_{+}C_{1,n}$ ottenuto dal rapporto $C_{(x+y)}{}^{n}/(x+y)$ che denominiamo i coefficienti "*ridotti*" di Tartaglia. Viene aggiunto +1 quando i fattori del numeratore del coefficiente binomiale sono pari, -1 quando sono dispari. In sintesi, quando *n* è primo, può essere costruita una nuova tabella di coefficienti tutti multipli di *n* per calcolare la potenza (*n-1)* di un binomio.

Avere alternativamente resto +1 e -1 nella divisione per n dei coefficienti binomiali della riga (n-1) è una peculiarità solo dei numeri primi n anzi possiamo assumerla come condizione primaria o meglio necessaria e sufficiente affinché n sia primo.

Un' elegante e semplice dimostrazione di quanto sopra evidenziato in corsivo si ottiene mettendo a confronto le formule di Newton con cui si ricavano i singoli coefficienti binomiali della riga ennesima con quelle che implementano il triangolo di Tartaglia fino a detta riga.

Se *n* è primo e se escludiamo il primo e l'ultimo coefficiente dell' ennesima riga, le formule di Newton ci assicurano che tutti gli altri *(n-2)* coefficienti della stessa riga sono divisibili per *n* in quanto esso è un fattore del numeratore che non può esistere al denominatore. Se invece *n* è composto, il denominatore elimina almeno uno dei suoi fattori (quello maggiore di $\sqrt{n}$) o, se è presente, ha esponente più piccolo di quello posseduto come sottomultiplo di *n*.

Le formule di Tartaglia ricavano i medesimi coefficienti dalla somma di due elementi adiacenti della riga (n-1); sommano, infatti, due elementi che nella divisione per n hanno resto rispettivamente +1 e -1. Partendo dal primo addendo della riga (n-1) che è +1 e finendo all'ultimo addendo che è sempre +1, si dimostra l'asserto. Quando n è primo si crea sulla riga (n-1) un *effetto catena,* nel senso che il primo elemento condiziona il secondo e così via: il primo elemento, avendo resto +1 nella divisione per n, impone al secondo di avere resto -1 in quanto la loro somma deve risultare multipla di n. Il secondo per le stesse ragioni impone al terzo resto +1 e così via.

Messe a confronto, le due formule ci rilevano, quindi, che solo quando n è primo, la divisione per n dei coefficienti della riga (n-1) ha resto alternativamente ±1. Quando n è composto, infatti, la catena si interrompe proprio in corrispondenza del coefficiente che ha come indice di base il più piccolo fattore primo di n.

Con due esempi è possibile fare una breve sentesi di quanto detto sopra. Il primo esempio è costituito, nell'ordine, dai coefficienti binomiali della riga del numero primo n=11, da quelli della riga (n-1)=10 e sotto di questa il resto della divisione dei singoli coefficienti della riga 10 per 11; il secondo, invece, riporta i coefficienti e i resti riferiti al numero composto n=15 ed ad (n-1)=14:

1) coefficienti delle righe 11 e 10 e resto della divisione $\binom{10}{i}/11$, con $0 \leq i \geq 10$

1	11	55	165	330	462	462	330	165	55	11	1
	1	10	45	120	210	252	210	120	45	10	1
	+1	-1	+1	-1	+1	-1	+1	-1	+1	-1	+1

2) coefficienti delle righe 15 e 14 e resti della divisione $\binom{14}{i}/15$, con $0 \leq i \geq 14$

1	15	115	475	1375	3003	5005	6435	6435	5005	3003	1375	475	115	1
	1	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1
	+1	-1	+1	+4	-4	+7	+3	-3	+3	+7	-4	+4	+1	-1	1

I resti della divisione $\binom{n-1}{i}/n$ sono distribuiti secondo una precisa relazione che tiene conto, quando n è composto, dei sottomultipli di n (l'argomento sarà ripreso in un prossimo articolo).

Il secondo lemma, di cui riportiamo solo l'enunciato (dimostrazione lunga ma semplice), riguarda le proprietà dei coefficienti binomiali della linea centrale del triangolo universale ed è denominato *la funzione dei numeri primi "ridotta":*

Condizione necessaria e sufficiente affinché un intero positivo dispari n>1 sia primo è che risulti divisibile per n il coefficiente centrale del triangolo di Tartaglia relativo alla riga (n-1) a cui è stato aggiunto +1 se (n-1) è un intero semplicemente pari oppure -1 se (n-1) risulta di parità multipla. Abbiamo, quindi, che il risultato della seguente funzione non risulta mai multipla di n se e solo se n è un numero dispari composto:

5.3.3) $y_r = \Gamma_{(n-1)/2,(n-1)} \pm 1$

Il test di verifica se l'intero dispari n è primo o meno si può fare utilizzando la formula sopra scritta riferita ad un qualsiasi indice di base $a > \sqrt{n}$, con +1 se a e dispari e -1 se a è pari ($y_{ra} = \Gamma_{a,(n-1)} \pm 1$).

In allegato è riportato un altro importante test sui numeri primi.

Conclusioni

Una breve sintesi del presente articolo è rappresentata dal fatto che Tartaglia ricava le indicazione per stabilire se un intero dispari **n** è primo o composto da tutti o alcuni coefficienti della riga *(n-1)* del suo "triangolo universale". Nel prossimo articolo vedremo come Fermat fornisce la conferma a Tartaglia utilizzando la relazione (anche detta di Diofanto) della sua famosa congettura x^n+y^n ripetendo i passaggi principali della "meravigliosa dimostrazione".

In effetti, questo articolo insieme a quello già presente nel bookshelf di "**Rudi Mathematici**" dal titolo "i quadrati di Galileo Galilei" contengono elementi indispensabili per dimostrare con metodi elementari *l'Ultimo Teorema di Fermat*. Si può dimostrare il caso n=4 e di $\left(2^{2^n}\right)$ con gli elementi contenuti nei "quadrati di Galilei". Con la funzione dei numeri primi si dimostra il caso generale, sfruttando la sua proprietà principale: *quando n è primo, i fattori 2, 3, n di* $y=2^n-2$ *sono presenti anche in* $C_{(x+y)}{}^n$*, denominato "Cuore di Tartaglia" che è il polinomio*

omogeneo ottenuto dallo sviluppo ordinato di $(x+y)^n$ escludendo i due termini della relazione di Fermat(x^n e y^n).

Allegato

Nell'allegato è riportato il teorema della "funzione dei numeri primi del fattoriale (f.n.p.f.)" che è da intendere come un semplice test che individua e seleziona i numeri primi ad uno ad uno. Può essere utile a qualche lettore per approfondire quanto riportato nell'articolo ma anche per ricercare nuovi elementi sulla distribuzione dei numeri primi e particolari proprietà dei numeri composti.

4.8) Una proprietà fondamentale della (f.n.p.)

La funzione dei numeri primi (f.n.p.) $y=2^n-2=2(2^{n-1}-1)$ è divisibile per n, ogniqualvolta n è primo. E' semplice verificare, applicando i noti metodi algebrici sulla differenza di due potenze che hanno lo stesso grado k, che l'espressione $y=2^{k(n-1)+1}-2=2(2^{k(n-1)}-1)$, quando n è primo e k un intero positivo qualsiasi, è anch'essa divisibile per n.

Gli elementi $I=\{n, 2(n-1)+1, 3(n-1)+1,\ldots, (n+1)(n-1),\ldots., k(n-1)+1,\ldots\ldots\}$ costituiscono, al variare di k in N, un insieme infinito di esponenti della (f.n.p.) che generano il fattore n nella scomposizione in fattori primi della stessa funzione.

L'insieme I gode di alcune proprietà fondamentali di N:

a) è crescente ed ordinato, nel senso che n è il primo elemento, 2(n-1)+1 è il secondo , e quindi, k(n-1)+1 è l'elemento di ordine k, mentre (k+1)(n-1)+1 è l'elemento di ordine (k+1). Se k(n-1)+1 è un elemento di I, il successivo risulta k(n-1)+1+(n-1)=(k+1)(n-1)+1 a cui segue (k+1)(n-1)+1+(n-1)=(k+2)(n-1)+1;

b) se λ è un intero positivo, gli elementi n, (n+1)(n-1)+1,……,(λn+1)(n-1)+1 costituiscono un sottoinsieme "speciale" di I. Questi esponenti sono multipli di n e generano n nella scomposizione in fattori primi della (f.n.p.);

c) la relazione d'ordine dell'insieme I è la stessa di N, nel senso che valgono per I le stesse condizioni, simboli e denominazione di N. Abbiamo, quindi, che n elementi consecutivi di I hanno un solo multiplo di n.

Tali proprietà trovano applicazioni nel seguente teorema, la cui dimostrazione più semplice è ricavata proprio tramite la funzione dei numeri primi (f.n.p.). Questo teorema è un'altra procedura che permette di selezionare i numeri primi di N, ordinatamente e senza che vengano prodotti falsi o pseudo primi.

4.9) La funzione dei numeri primi del fattoriale (f.n.p.f.)

Se n>1 è un intero positivo dispari qualsiasi, le due espressioni $y_{(n-1)}=(n-1)!+1$ e $y_{(n-2)}=(n-2)!-1$ sono entrambe divisibili per n, solo e solo se n è primo.

E' ovvio che il test può essere limitato all'utilizzo di una sola espressione.

Se n=p*q è composto, e quindi ottenuto come prodotto di numeri interi positivi maggiori di 1, non può risultare, per noti teoremi di algebra, divisore della prima e

tanto meno della seconda espressione. In tale ipotesi, infatti, le scomposizioni in fattori primi di $y_{(n-1)}$ e di $y_{(n-2)}$ non possono contenere fattori primi $p_i \leq (n-1)$.

Se n divide $y_{(n-1)}$ risulta primo ed è semplice verificare che divide anche $y_{(n-2)}$. Si ha infatti, che la divisione $y_{(n-1)}/n=[(n-1)!+1]/[(n-1)+1]$ presenta come primo resto parziale l'intero $-(n-2)!+1$ che deve risultare necessariamente divisibile per n perché tale risulta il dividendo.

Al contrario, se n è primo, costruiamo due sottoinsiemi di N "con proprietà speciali" allo scopo di individuare i multipli di n tra gli elementi del primo e del secondo. Il primo, formato da n elementi consecutivi di N denominati i "consecutivi del fattoriale", è costruito tramite la relazione $y_{(n-1)+h}=(n-1)!+1+h$ e con $0 \leq h \leq (n-1)$.

Abbiamo, quindi: $I_s=\{(n-1)!+1, (n-1)!+2,\ldots\ldots, (n-1)!+n\}$. Le proprietà più importanti, evidenti o facili da verificare, degli elementi di I_s si ricavano direttamente da quelle di N e riguardano:

a) (n-1)!+n non può risultare multiplo di n,

b) escludendo l'ultimo, un altro tra gli elementi di I_s deve necessariamente risultare multiplo di n.

c) con n primo, per le proprietà fondamentali della (f.n.p.) descritte nel paragrafo precedente, la relazione $y=(2^{(n-1)!+1}-2)$ risulta divisibile per n.

d) Il sottoinsieme Is ha in comune con I solo l'elemento (n-1)!+1.

Costruiamo, a partire da (n-1)!+1, il secondo sottoinsieme I_f , costituito da n elementi consecutivi di I che chiameremo gli "*esponenti del fattoriale*":

1) (n-1)!+1,

2) (n-1)!+1+(n-1) =[(n-2)!+1](n-1)+1,

3) (n-1)!+1+2(n-1)= =[(n-2)!+2](n-1)+1,

……..,

β-1) (n-1)!+1+β(n-1)=[(n-2)!+β](n-1)+1, con $0 \leq \beta < n$

……..,

n) (n-1)!+1+(n-1)(n-1) =[(n-2)!+(n-1)](n-1)+1.

Gli "*esponenti del fattoriale*" costituiscono un sottoinsieme I_f di I, ordinato e crescente , nel senso che , a partire da (n-1)!+1, raccoglie n esponenti di (f.n.p.) che si susseguono uno dopo l'altro nell'insieme I, le cui proprietà fondamentali, descritte dettagliatamente nel paragrafo precedente, sono le stesse che godono n elementi consecutivi di N.

Anche il sottoinsieme I_f è finito ed è costituito da n elementi, la cui proprietà più importante riguarda la seguente condizione: *tra gli elementi I_f, uno ed uno solo deve risultare multiplo di n.*

Con l'espressione $y_{(n-1)+\beta}=(n-1)!+1+\beta(n-1)$, con i valori di $0\leq\beta\leq(n-1)$, si possono ricavare tutti gli elementi di I_f ed uno solo tra questi deve risultare multiplo di n.

Siamo in presenza di due sottoinsiemi finiti che hanno il primo elemento in comune che è (n-1)!+1, l'ultimo elemento di I_s [(n-1)+n] eguaglia il secondo di I_f (β=1) (per ipotesi essendo n primo, questo elemento comune non può risultare multipli di n) mentre tutti gli altri elementi di I_s sono più piccoli di quelli di I_f.

Premettiamo una proprietà elementare dei numeri interi sia positivi che negativi: se un numero intero a qualsiasi è multiplo di n lo è anche (a +αn), con α intero positivo o negativo. La quantità αn viene denominata "*parametro di aggancio di multipli di n*" , nel senso che, fissando un multiplo di n qualsiasi, tutti gli altri multipli di n appartenenti all'insieme dei numeri relativi Z possono essere determinati tramite il suddetto parametro facendo variare α a piacimento proprio nell'insieme degli interi relativi Z.

Abbiamo, quindi, che se un determinato elemento di I_s è multiplo di n attraverso, *"il parametro di aggancio αn"* possiamo individuare l'elemento di I_f che, a sua volta, risulta multiplo di n. E' vero anche il contrario, nel senso che da un elemento di I_f, multiplo di n, si può individuare un unico corrispondente in I_s che, a sua volta, risulti multiplo di n.

In sintesi, la somma di ogni elemento di I_s con la quantità αn viene eguagliata ad un elemento di I_f:

4.9.1) $y_{(n-1)+h}+\alpha n= y_{(n-1)+\beta}=(n-1)!+1+h+\alpha n= (n-1)!+1+\beta(n-1)$.

Per ogni elemento di I_s è necessario discutere n semplici equazioni di primo grado $\alpha n=\beta(n-1)-h=\beta n-\beta-h$, dove α è l'incognita e la coppia $0\leq(h,\beta)\leq(n-1)$ sono gli interi positivi con cui vengono ricavati, a partire dal primo, con h gli elementi di I_s e con β quelli di I_f .

Scrivendo tutte le possibili eguaglianze in base al valore di $0\leq\beta\leq n$ e scegliendo $h=(n-\beta)$ otteniamo come risultato $\alpha=(\beta-1)$. E' banale la verifica che con α=0, β=0 e h=0 il primo elemento di I_s coincide con il primo elemento di I_f ; per β=1, otteniamo l'ultimo elemento di I_s (n-1)!+1+(n-β)=(n-1)!+n, mentre per β=2 il corrispondente elemento di I_s presenta h=(n-2) e così via.

In sintesi, rispettando i limiti imposti alla coppia (h,β), quando ipotizziamo che un elemento (*esponente del fattoriale*) di I_f è multiplo di n, siamo in grado, pertanto, di individuare, "*il consecutivo del fattoriale"* appartenente a I_s che risulta multiplo dello stesso n.

Tenendo conto della relazione $y_{(n-1)+h}=(n-1)!+1+h$, con $0\leq h\leq(n-1)$, per scegliere l'elemento di I_s multiplo di n, utilizziamo la "condizione del resto": *un elemento di I_s che risulta multiplo di n, nella divisione [(n-1)!]/n, ha necessariamente il resto r=-(h+1).*

Facciamo considerazioni analoghe utilizzando l'espressione che genera gli elementi di I_f $y_{(n-1)+\beta}=(n-1)!+1+\beta(n-1)=(n-1)!+1+n\beta-\beta$, con $0\leq\beta\leq(n-1)$: *un elemento*

di I_f che risulta multiplo di n, nella divisione [(n-1)!]/n, ha necessariamente il resto r=(β-1).

E' immediata la constatazione che questi due resti, nella 4.9.1), debbano coincidere e quindi si ottiene -(h+1)=(β-1) da cui ricaviamo β=-h; per rispettare i limiti di esistenza (entrambi variabili da 0 a n-1) di h e β, l'uguaglianza è certamente possibile solo per h=0 e β=0.

Abbiamo pertanto, che solo il primo elemento di I_s, coincidente con il primo di I_f, risulta multiplo di n, ovvero (n-1)!+1 è divisibile per n , quando n è primo.

Quando n è primo pertanto, risulta dimostrato anche la condizione sufficiente affinché la relazione $y_{(n-1)}$ =(n-1)!+1 risulti multipla di n. E' evidente che ciò vale anche per $y_{(n-2)}$=(n-2)!-1.

La "funzione dei numeri primi del fattoriale (f.n.p.f.)" genera solo primi e può essere così sintetizzata:

Se a è un numero intero pari qualsiasi, l'espressione a!+1 può essere un numero primo oppure divisibile per (a+1) che a sua volta deve risultare primo; viceversa, quando (a+1) risulta primo, l'espressione y_a=[a!+1]/(a+1) ha resto nullo. Ragionamento analogo si può ripetere per $y_{(a-1)}$=[(a-1)!-1]/n .

Con N_p={2, 3, 5,..., p,...} indichiamo il sottoinsieme dei numeri primi e con N_c={1, 4, 6, 8, 9,..., c,..} quello dei numeri composti a cui è stato aggiunto {1} che si possono costruire ordinatamente attraverso le relazioni y_a, oppure con $y_{(a-1)}$.

Con la (f.n.p.f.) è semplice costruire l'insieme dei numeri primi N_p con la stessa relazione utilizzata da Fermat:4n±1. E' anche semplice verificare che la espressione 6h±1 serve allo stesso scopo riducendo di molto i numeri composti da scartare (multipli di 3).

Un'altra importante applicazione della (f.n.p.) riguarda i numeri di Mersenne.

Antonio Rita