ISSN: 2037-6367

MatematicaMente

Pubblicazione mensile della sezione veronese della MATHESIS – Società Italiana di Scienze Matematiche e Fisiche – Fondata nel 1895 – Autorizzazione del Tribunale di Verona n. 1360 del 15 – 03 – 1999 – I diritti d'autore sono riservati. Direttore: Luciano Corso - Redazione: Alberto Burato, Elisabetta Capotosto, Carlo Marchiori, Giovanna Tessari – Via IV Novembre, 11/b – 37126 Verona – tel e fax (045) 8344785 – 338 6416432 – e-mail: lcorso@iol.it – Stampa in proprio - Numero 174 – Pubblicato il 10 – 12 – 2012

TEOREMA SU UN TEST DI PRIMALITÀ CON FATTORIZZAZIONE

Guido Carolla [*]

[*Segue dal numero* 173]

A chiarimento dei diversi valori interi di n che indichiamo con a e b, dalla prima, $6\cdot a \pm 1 = D$, abbiamo

$$a = \frac{D \mp 1}{6}$$

e dalla seconda $6\cdot(d>1)\cdot b \pm (d>1) = D$ abbiamo

$$b = \frac{D \mp (d>1)}{6\cdot(d>1)},$$

dove $b(D, d)$ può assumere più valori, essendo funzione anche di d che è variabile. Inoltre, il primo caso [1a] si ha se è soddisfatta almeno una delle due congruenze $D \mp 1 \equiv (r = 0)(\mathrm{mod}6)$, cioè se $D \mp 1$ è divisibile per 6, allora per uno stesso D si hanno congiuntamente

$(d=1)\cdot(6\cdot n \pm 1) = \pm 1 + 6\cdot n = D$,

$(d>1)\cdot(6\cdot n \pm 1) = \pm d + 6\cdot d\cdot n = D$,

che denotano D numero dispari composto non multiplo di 3; il secondo e terzo caso si hanno rispettivamente con D divisibile o multiplo di 3 non potenza di 3, e con D potenza di 3, se sono per entrambe soddisfatte le due congruenze $D \mp 1 \equiv (r \neq 0)(\mathrm{mod}6)$, cioè se $D \mp 1$ non è divisibile per 6 con resti $r =$ 2 e 4, allora con una o più coppie di soluzioni $d > 1$, $n \geq 1$, da $(d>1)\cdot(6n \pm 1) = \pm d + 6dn = D$

si denota D non potenza di 3 ma multiplo di 3, per il caso [1b], mentre per il caso [1c] se non si ha alcuna coppia di soluzioni, D è una potenza di 3, infatti per $D = 3^m$, con $m \in \mathbf{N}_0$, si potrà avere solo $(3^m / (6n \pm 1)) \neq d$ dispari, in quanto nessuna potenza di 3 è divisibile per ogni $dnd3$ dispari non divisibile per 3 (che si ottiene dai due binomi $6\cdot n \pm 1$).

Infine, con una sola delle soluzioni di $(d=1)\cdot p = p$, sostituendo di nuovo i valori di $p = 6\cdot n \pm 1$ si avranno i casi banali $(d=1)\cdot(6\cdot n \pm 1) = D$, che denotano D numero primo e ciò prova il punto [2] del teorema. Il teorema è così dimostrato.

Per $D = 1$ si ha il caso [1c] senza soluzioni delle due equazioni, infatti come si può riscontrare dal relativo esempio riportato nell'output del listato del programma, si ha $3^0 = 1$. Si dà per scontato che D sia primo, quando assume valori 2, 3, in quanto, come nel caso di una potenza di 3, non si hanno soluzioni di d e di n, a meno che non si voglia considerare $n = 0$ in disaccordo con i punti [1] e [2] del teorema (si fa osservare che con $n = 0$ le due equazioni darebbero soluzioni di coppie comuni $d = \pm D$, $n = 0$, tanto che D sia un dispari composto che un primo), infatti anche per $D = 2$ e $D = 3$ si potranno avere rispettivamente $(2 / (6n \pm 1)) \neq d$ dispari e $(3 / (6n \pm 1)) \neq d$ dispari, in quanto 2 e 3 non sono divisibili per ogni $dnd3$ dispari non divisibile per 3 (che si ottengono dai due binomi $6n \pm 1$).

Tutti i conosciuti criteri di divisibilità permetterebbero di escludere dal test i valori assegnati a D che risultassero meramente dispari composti e considerati più facilmente individuabili i dispari divisibili per 3 (la somma delle cifre è 3 o un multiplo di 3) e quelli di più cifre con cadenza 5, non perderemmo tempo se non sottoponessimo al test i numeri D con dette caratteristiche, trovandoci chiaramente di fronte a numeri composti, salvo che si voglia avere la fattorizzazione di D.

L'algoritmo $\pm d + 6\cdot d\cdot n$ che genera le due equazioni indeterminate permette anche di ottenere dalle soluzioni delle d la fattorizzazione del termine noto, numero dispari D; infatti, moltiplicando una sola volta i fattori primi comuni e non comuni con il maggiore esponente, abbiamo il minimo comune multiplo che è proprio D.

Essendo un test di primalità un algoritmo che permette di stabilire se un dato numero è primo oppure no, nella teoria della complessità computazionale, questo problema è a volte denotato come PRIMES.

Nel nostro caso le soluzioni d e n, per il test di primalità e la conseguente fattorizzazione, si possono ottenere facilmente con un semplice listato di programma in un qualunque linguaggio, come ad esempio nel QBasic che segue, nel quale abbiamo posto $X=d$ e $Y=n$; si noti che nell'istruzione 30FOR (per D grande si potrà maggiorare il valore del TO) si utilizzano solo gli $X=d$ dispari, non tutti gli $(Y=n)\in \mathbf{N}$, ottenendo un notevole vantaggio nei tempi di esecuzione e quindi ai fini di una migliore classe computazionale (il lettore che vuole risparmiarsi i listati legga solo i quattro esempi).

Equazione indeterminata

```
CLS: PRINT "GUIDO CAROLLA 2012"↵ PRINT "RISOLVE IN N (NATURALI) L'EQUAZIONE INDETERMINATA" ↵ PRINT "A*X+C*X*Y =D. "; " Se nel totale delle due equazioni, digitando" ↵ PRINT "prima A=1, C=6 e dopo A= –1,C=6, con uno stesso D dispari," ↵ PRINT "si hanno solo X=1 e Y>=1, allora D è un numero primo." ↵ PRINT "Negli altri casi D è un numero composto: non multiplo di 3, con almeno" ↵ PRINT "due coppie X >=1 e Y>=1, di cui una X=1 e Y>=1; multiplo di 3," ↵ PRINT "ma non potenza di 3, con almeno una coppia X>1 e Y>=1; potenza di 3," ↵ PRINT "senza alcuna coppia di soluzioni." ↵ PRINT "Dalle soluzioni delle X si può ottenere la fattorizzazione di D." ↵ 20 INPUT "DIGITA A,C,D"; A, C, D ↵ 30 FOR X = 1 TO 200000 STEP 2 ↵ 40 Y = INT((D – A * X) / (C * X)) ↵ 50 E = A * X + C * X * Y 60 IF E <> D THEN 100 ↵ PRINT ↵ 70 IF X = D THEN 100 ↵ 80 PRINT "X="; X; "Y="; Y ↵ 90 PRINT "VERIFICA:D= "; D; "="; A; "*"; X; "+"; C; "*"; X; ↵ PRINT "*"; Y; "="; E ↵ 100 NEXT X ↵ PRINT " SOLO SE SENZA SOLUZIONI DELE DUE EQUAZIONI: (esponente di 3)=(log D)/(log3)="; ↵ PRINT LOG(D) / LOG(3) ↵ END
```

Esempio relativo al punto [1a] del teorema. A*X+B*Y+C*X*Y=D ↵ DIGITA A, C, D ? 1,6,583 ↵ X=1; Y=97 ↵ VERIFICA: D= 583 = 1 * 1 + 6 * 1 * 97 ↵ DIGITA A, C, D ? –1,6,583 ↵ X= 53 ;Y=2 ↵ VERIFICA: D= 583 = –1 * 53 + 6 * 53 *2 = 583 ↵ X=11 ; Y=9 ↵ VERIFICA: D= 583 = –1 * 11 + 6 * 11 * 9 = 583 ↵ Avendosi nell'esempio due accoppiamenti x=d=53, y= n=2 e x=d=11, y=n= 9 (ne bastava uno) e un accoppiamento x=d=1, y=n=97 si deduce che il numero D=583 è composto e non multiplo di 3. Inoltre dalle x si evincono anche i fattori primi, per cui 583 = 53·11.

Esempio relativo al punto [1b] del teorema. DIGITA A, C, D ? 1,6,177 ↵ Nessuna soluzione ↵ DIGITA A, C, D ? -1,6,177 ↵ X= 3; Y=10 ↵ VERIFICA: D= 177 = –1 * 3 + 6 * 3 *10 = 177 ↵ Avendosi una coppia di soluzioni x=d=3, y=n=10 (potevano essere anche più di una) si deduce che il numero *D=177* non potenza di 3 è un multiplo di 3. Inoltre da 177:3=59 si hanno i due fattori primi 3 e 59.

Esempio relativo al punto [1c] del teorema. DIGITA A, C, D ? 1,6,243 ↵ Nessuna soluzione ↵ DIGITA A, C, D ? -1,6,243 ↵ Nessuna soluzione ↵ Esponente di 3=LOG(243) / LOG(3)=5 ↵ Non avendosi alcuna coppia di soluzioni si deduce che il numero D=243 è la potenza 3^5. ↵ Altro particolare esempio relativo al punto 1c) del teorema ↵ DIGITA A, C, D ? 1,6,1 ↵ Nessuna soluzione ↵ DIGITA A, C, D ? -1,6,1 ↵ Nessuna soluzione ↵ Esponente di 3=LOG(1) / LOG(3)=0 ↵ Non avendosi alcuna coppia di soluzioni si deduce che il numero D=1 è la potenza 3^0.

Esempio relativo al punto [2] del teorema. ↵ DIGITA A, C, D ? 1,6,83 ↵ Nes-suna soluzione ↵ DIGITA A, C, D ? –1,6,83 ↵ X=1; Y=14 ↵ VERIFICA: D = 83 = –1 * 1 + 6 * 1 * 14 = 83 ↵ Avendosi solo una coppia di soluzioni x=1 con y=14 si deduce che il numero D=83 è primo! ↵ Il listato che segue, del quale si è realizzato un "exe", è stato integrato e modificato, rispetto al precedente nelle istruzioni 25, 30, 85, secondo quanto detto nella

"Premessa", con la $\sqrt{D}$= F = INT(SQR(D)), allo scopo di ottenere una riduzione dei tempi di esecuzione ovvero un vantaggio computazionale:
CLS: PRINT "GUIDO CAROLLA 2012" ↵ PRINT "RISOLVE IN N (NATURALI) L'EQUAZIONE INDETERMINATA" ↵ PRINT "A*X+C*X*Y =D. "; " Se nel totale delle due equazioni, digitando" ↵ PRINT "prima A=1, C=6 e dopo A=-1,C=6, con uno stesso D dispari," ↵ PRINT "si hanno solo X=1 e Y>=1, allora D è un numero primo." ↵ PRINT "Negli altri casi D è un numero composto: non multiplo di 3, con almeno " ↵ PRINT "due coppie X>=1 e Y>=1, di cui una X=1 e Y>=1; multiplo di 3," ↵ PRINT "ma non potenza di 3, con almeno una coppia X>1 e Y>=1; potenza di 3," ↵ PRINT "senza alcuna coppia di soluzioni." ↵ PRINT "Dalle soluzioni delle X si può ottenere la fattorizzazione di D." ↵ 20 INPUT "DIGITA A,C,D"; A, C, D ↵ 25 F = INT(SQR(D)) ↵ 30 FOR X = 1 TO F STEP 2 ↵ 40 Y = INT((D – A * X) / (C * X)) ↵ 50 E = A * X + C * X * Y ↵ 60 IF E <> D THEN 100 ↵ PRINT ↵ 70 IF X = D THEN 100 ↵ 80 PRINT "X="; X; "Y="; Y ↵ 85 PRINT "Altro fattore D/X="; D / X ↵ 90 PRINT "VERIFICA:D= "; D; "="; A; "*"; X; "+"; C; "*"; X; ↵ PRINT "*"; Y; "="; E ↵ 100 NEXT X ↵ PRINT " SENZA SOLUZIONI DELE DUE EQUAZIONI: (esponente di 3)=(logD)/(log3)="; ↵ PRINT LOG(D) / LOG(3) ↵ END.

Riferimenti bibliografici: [1] Kline M., *Storia del pensiero matematico,* Einaudi, Torino, 1999. [2] Hardy G. H., *Apologia di un matematico,* Garzanti, Milano, 2002. [3] Du Sautoy M., *L'enigma dei numeri primi, l'ipotesi di Riemann: il più grande mistero della matematica*. Rizzoli, Milano, 2005. [4] Derbyshire J., *L'ossessione dei numeri primi. Bernhard Riemann e il principale problema irrisolto della matematica,* Bollati, Boringhieri, Torino, 2006. [5] Pickover C., *Le meraviglie dei numeri*. RBA Italia, Milano, 2008. [6] Carolla Guido, *Aspetti insiemistico-polinomiali dai dispari fino ai primi*, MatematicaMente numero 167, pubblicato il 02-04-2012, MATHESIS Verona. [7] Carolla Guido, *Su alcuni spunti di Digidattica matematica*, pubblicato su CD delle 3^, 4^, 5^ edizioni per gli Atti del 3^ Congresso Nazionale ADT, Associazione Didattica con le Tecnologie, Cattolica, 5/6/7 ottobre 2001. [8] D. P. Bovet e P. Crescenzi, *Teoria della Complessità Computazionale*, Franco Angeli Editore, 1991. [9] Carl B. Boyer, "Storia della matematica", Arnoldo Mondatori Editore, 1997.

[*] Docente di Lecce ordinario di Matematica e Dirigente scolastico in ogni ordine di scuola, ora a riposo. E-mail: guidocarolla@libero.it

NUMERI DI STIRLING DI PRIMA SPECIE

Relazione esistente tra i numeri appartenenti ad una colonna

di Gabriele Pupolin [**]

Abstract: The Stirling Numbers of First Kind without sign, $s(n, k)$, are numbers that satisfy the equation $s(n+1, k) = n \cdot s(n, k) + s(n, k–1)$ for $n \geq 1$ and $1 \leq k < n$. This paper develops the relation that exists for numbers of a column k.

1. Introduzione

I Numeri di Stirling di Prima Specie privati di segno costituiscono un triangolo numerico come rappresentato in Tabella 1.

Tabella 1: Numeri di Stirling di Prima Specie senza segno

(n) \ (k)	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	0	1	1	0	0	0	0
3	0	2	3	1	0	0	0
4	0	6	11	6	1	0	0
5	0	24	50	35	10	1	0
6	0	120	274	225	85	15	1

Tale Triangolo numerico può esser trasformato in una Matrice Triangolare Inferiore imponendo il valore 0 per ogni $s(n, k)$ con $k > n$.

I numeri di Stirling privati di segno soddisfano le seguenti relazioni:
1) $s(0, 0) = 1$; $s(0, k) = 0$ per $k > 0$,
2) $s(n+1, k) = n \cdot s(n, k) + s(n, k–1)$ per $n > 0$, $k > 0$,
2) $s(n+1, 0) = n \cdot s(n, 0)$ per $k = 0$.
I Numeri di Stirling rappresentano i coefficienti, privati di segno, dell'espansione polinomiale del fattoriale di x con n fattori:
$(x)_n = x \cdot (x–1) \cdot (x–2) \cdot \ \ldots \ \cdot (x–n+1)$.
In questo articolo, prefissato un n, saranno esaminate le relazioni esistenti tra i numeri $s(n, k)$ appartenenti alla stessa colonna k verificando la validità dell'equazione

$$s(n,k) = \sum_{i=1}^{n-1} \frac{(n-i-1)! \cdot \begin{pmatrix} n \\ i-1 \end{pmatrix} \cdot s(i,k)}{n-k} \qquad (1)$$

valida per $n \geq 2$; $0 \leq k < n$. In tale equazione $s(i, k)$ rappresenta un generico Numero di Stirling di Prima Specie, privato segno, appartenente alla colonna k sino alla riga $(n–1)$.
Anche il Triangolo di Tartaglia sarà interpretato come Matrice Triangolare Inferiore i cui elementi

$$\begin{pmatrix} n \\ k \end{pmatrix}$$

sono identicamente nulli per $k > n$.

2. La Matrice P

Il prodotto

$$p(n,i) = (n-1-i)! \cdot \begin{pmatrix} n \\ i-1 \end{pmatrix},$$

per $n \geq 2$ e $1 \leq i \leq (n – 1)$, definisce un Triangolo Numerico nelle variabili n e i.
Eseguendo i cambi di variabile $m = (n – 2)$ e $j = (i – 1)$ tale Triangolo può esser trasformato in un nuovo Triangolo Numerico $P(m, j)$ definito per $m \geq 0$, $0 \leq j \leq m$.
Il Triangolo Numerico $P(m, j)$ a sua volta può esser trasformato in una Matrice Triangolare Inferiore $\mathbf{P}[m, j]$, rappresentata in Tabella 2, imponendo valore nullo agli elementi $p(m, j)$ con $j > m$.

Tabella 2: Matrice P

(m) \ (j)	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	3	0	0	0	0	0
2	2	4	6	0	0	0	0
3	6	10	10	10	0	0	0
4	24	36	30	20	15	0	0
5	120	168	126	70	35	21	0
6	720	960	672	336	140	56	28

[*Segue al numero* 175]

Questo lavoro è stato presentato al Congresso nazionale della Mathesis, tenutosi a Rovigo dal 18 al 20 ottobre 2012.

[**] Socio nazionale Mathesis – e-mail: g.pupolin@tin.it

La mela di Alan

Per onorare la memoria del grande matematico Alan Mathison Turing (1912 – 1954), in occasione del centenario della sua nascita, il 7-11-2012 ore 21, presso il teatro Ristori di Verona, si è tenuto lo spettacolo teatrale «La mela di Turing», con la regia di Valeria Patera. Lo spettacolo è stato promosso da numerosi enti culturali, tra cui l'Università degli Studi di Verona e la sezione veronese della Mathesis (Società Italiana di Scienze MM. e FF.), e ha riscosso un buon successo di pubblico.