Giovanni Vaccaro

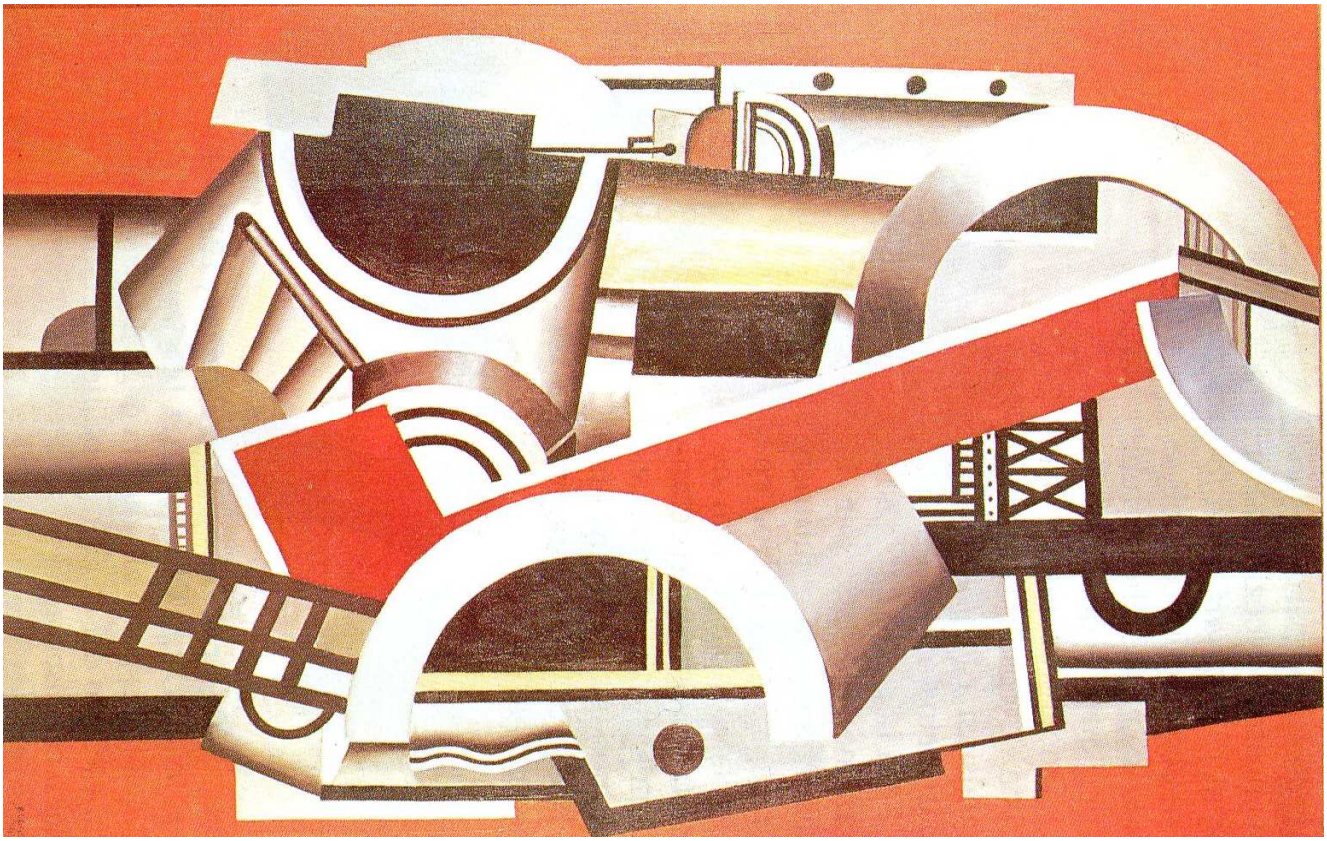
******

SINERGIA

TRA

MATEMATICA E INFORMATICA

PER LA VERIFICA di CONGETTURE e TEOREMI



SU

FUNZIONI ARITMETICHE, GAMMA, ZETA E PRIMALITÀ

FRAZIONI CONTINUE E SUE APPLICAZIONI

Con affetto al mio caro fratello Lillo

Con stima ai Colleghi del
Liceo “ M. Curie” di Tradate

Introduzione

Agli inizi del percorso formativo di ogni studente l'Aritmetica occupa un posto di primordine nello studio della Matematica, anzi costituisce la struttura base degli studi della scuola primaria. Nella pluriennale storia della matematica l'Aritmetica è stata oggetto di studio dei più grandi matematici, in essa ancora permangono proprietà indimostrate (dette congetture), che costituiscono dei veri rompicapo per chi si vuole accingere a dimostrarle. Nello scorrere del tempo con la scoperta di nuove strutture matematiche, nonché di algoritmi operativi si è riusciti a dimostrarne alcune congetture: ultima il Teorema di Fermat: $x^n + y^n = z^n$ con $\forall n \in N: n > 2$.

L'avvento di calcolatori e di software adeguati hanno permesso di verificare congetture su grandezze numeriche dell'ordine di 10^{400} con ore ed ore di lavoro continuato, mettendo anche in sinergia numerosi operatori. La ricerca matematica in questo campo è ancora oggi oggetto di impegno nei diversi centri di studio, sparsi in numerosi università; tale ricerca pur non raggiungendo il traguardo sperato tuttavia ha dato spunto a scoperte di nuove strutture ed algoritmi che arricchiscono il sapere matematico.

Obiettivo di questo scritto vuole essere portare a conoscenza e sensibilizzare gli studenti particolarmente interessati allo studio della matematica su temi non trattati nei normali corsi della scuola secondaria superiore, ma che costituiscono un affascinante campo di conoscenze che possono sprigionare passione e amore e quindi ricerca; nella consapevolezza che l'interesse intellettivo verso un oggetto culturale nasce quando alla mente dello studioso arrivano stimoli conoscitivi sugli argomenti che trattano quell'oggetto. Tali temi trovano fondamento nello studio degli argomenti trattati in un normale corso di studio di un liceo tecnico-scientifico. La Teoria dei Numeri costituisce il fondamento naturale di questo scritto (il prossimo impegno di chi scrive sarà la stesura di " Elementi di teoria dei numeri: dai Naturali ai Complessi "), che permetterà al lettore di avere un quadro di riferimento sulla costruzione ed assiomatizzazione delle strutture numeriche.

L'Aritmetica, trattando i numeri naturali che risultano nella loro totalità un insieme discreto, si presta facilmente a trattare e verificare le proprietà enunciate in essa con l'ausilio di algoritmi informatici, pertanto in questo scritto sono esposti una serie di programmi completi in linguaggio Turbo Pascal che implementano proprietà aritmetiche, teoremi e congetture. Lo studio delle strutture informatiche presenti in tali programmi permetterà di crearne di nuovi e aiuterà a sviluppare capacità operative nello studente e quindi sensibilità ed amore alla ricerca. Chissà se qualche studente possa riuscire a trovare quelle strategie risolutive atte a dimostrare congetture ancora in essere ? Lo scrivente è convinto dallo studio della Storia della Matematica che solo nelle menti giovani la creatività matematica trova terreno adatto e fruttifero: infatti i grandi matematici hanno fatto le loro scoperte in età giovanile e successivamente le hanno sviluppato, perfezionato e razionalizzato in età adulta.

Questo scritto si sviluppa in quattro capitoli, che trattano: le funzioni aritmetiche , la funzione Gamma di Eulero e la funzione Zeta di Riemann, i numeri primi e la primalità, le frazioni continue e sue applicazioni

L’esposizione, essendo rivolta a studenti del triennio di un liceo, è volutamente informativa ed indicativa al fine di portare a conoscenza gli argomenti trattati: le dimostrazioni sono ridotte all’essenziale.

CAPITOLO I

FUNZIONI ARITMETICHE

Generalità

In generale si chiama funzione aritmetica ogni funzione a valori reali (o in generale complessi) definita nell'insieme dei numeri naturali: cioè ogni legge che a qualunque elemento x preso nell'insieme dei numeri naturali fa corrispondere un elemento f(x) del campo dei numeri reali (o in generale dei numeri complessi).
Tuttavia si è soliti riservare al nome di funzione aritmetica ad una funzione del tipo anzidetto che si riferisce a qualche proprietà più spiccatamente aritmetica. Le più notevoli e tipiche funzioni aritmetiche consacrate dalla tradizione sono quelle indicate comunemente coi simboli:

$y = \varphi\,(\,n\,)\;;\quad y = \tau\,(\,n\,)\;;\; y = \mu\,(n)\;;\; y = \sigma\,(n)\;;\quad y = r\,(\,n\,)\,;\, f(n) = 1\,;\; I(n) = n$

NB. La simbologia d|n , che incontreremo spesso in questo capitolo, afferma che d è un divisore di n.

1) La funzione $y = \varphi\,(\,n\,)$, detta *indicatore di Eulero o Totiene*, rappresenta il numero dei numeri naturali primi con *n* e minori di *n.*
2) La funzione $y = d\,(\,n\,)$ rappresenta il numero dei numeri naturali che dividono *n.*
3) La funzione $y = \sigma\,(n)$ rappresenta la somma dei divisori di *n*.
4) La funzione $y = \mu\,(n)$ è la *funzione di Möbius*
5) La funzione $y = r\,(\,n\,)$ rappresenta il numero delle soluzioni, in interi x e y , dell'equazione $x^2 + y^2 = n$
6) La funzione $f(n) = 1$, detta *funzione unitaria, è* una funzione costante che associa ad ogni $n \in N$ l'unità dell'insieme *N*: 1.
7) La funzione $I(n) = n$, detta *funzione identità*,è una funzione che fa corrispondere ad ogni $n \in N$ il valore *n.*

Analizziamo singolarmente le diverse funzioni

A) Indicatore di Eulero o totiene : funzione $y = \varphi\,(\,n\,)$

Def. Si chiama *indicatore di Eulero o Totiene* la funzione aritmetica $y = \varphi\,(\,n\,)$ il cui valore è il numero dei numeri naturali primi con *n* e minori di *n.*

Es.

- Sia *n* = 24. Tutti i numeri primi con 24 e minori di 24 sono: 1, 5, 7, 11, 13, 17, 19, 23; per un totale di 8 elementi. Pertanto $\varphi\,(\,24\,) = 8$
- Sia *n* = 13. Essendo 13 un numero primo, tutti i numeri primi con 13 e minori di 13 sono tutti i numeri naturali che vanno da 1 a 12, per un totale di 12 elementi. Pertanto

$$\varphi\,(\,13\,) = 12.$$

Cerchiamo ora una formula che ci permette di individuare il valore di $\varphi\,(\,n\,)$

Se *n* = p numero primo, tutti i numeri naturali minori di p sono primi con p, per un totale di (p – 1); pertanto

$$\varphi\,(\,p\,) = p - 1$$

Se $n = p^m$: cioè ad una potenza di un numero primo, consideriamo tutti i multipli q di p con $p \le q \le p^m$: del tipo q = k·p con $1 \le k \le p^{m-1}$, per un totale di p^{m-1} ; pertanto la totalità dei numeri naturali minori di $n = p^m$ e primi con $n = p^m$ sono

$$\varphi\,(\,p\,) = p^m - p^{m-1} = p^{m-1}(p-1) = p^m\left(1 - \frac{1}{p}\right)$$

Se *n* è un numero composto, sappiamo dal Teorema fondamentale dell'Aritmetica che tale numero è decomponibile in fattori primi e tale decomposizione è unica a meno dell'ordine dei fattori. Sia $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ la decomposizione canonica di *n* in fattori primi, il valore di $\varphi\,(\,n\,)$ è dato da:

$$(1) \qquad \varphi\,(\,n\,) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

scritta in forma sintetica con l'introduzione del *produttorio*, si ha

$$\varphi\,(\,n\,) = n \cdot \prod_{p|n}\left(1 - \frac{1}{p}\right) = \prod_{p_i{}^{\alpha_i}|n}(p_i{}^{\alpha_i} - p_i{}^{\alpha_i - 1})$$

in quanto, come avremo modo di vedere, la funzione $\varphi\,(\,n\,)$ è moltiplicativa: cioè se *n* = $p_1 \cdot p_2$,

$$\varphi\,(\,n\,) = \varphi(p_1 \cdot p_2) = \varphi\,(\,p_1\,) \cdot \varphi(p_2) = (p_1 - 1)(p_2 - 1) = p_1 \cdot p_2 \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) =$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

L'espressione formale (1) costituisce la formula per individuare il valore di $\varphi\,(\,n\,)$, dopo aver scomposto in fattori primi il numero *n.*

Es. Sia $n = 28 = 2^2 \cdot 7^1$, $\varphi\,(\,28\,) = 28 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{7}\right) = 2 \cdot 1 \cdot 6 = 12$: infatti i numeri naturali minori di 28 e primi con 28 sono: 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27; per un totale di 12.

Stesura del programma in Turbo Pascal relativo alla funzione $\varphi\,(\,n\,)$

```
program Gauss_Eulero_Funzione_Fi;
uses crt;
var a,i,r,k,mcd,fi,n,s,q:word;
begin
  clrscr;
  textcolor(15);
  writeln('Il programma ti permette di determinare il valore della funzione Fi');
  writeln;
  Writeln('cioè dato un numero naturale N determinare la quantità dei numeri ');
  writeln('inferiori ad  N  e primi con N ');
  writeln;
  textcolor(11);
  repeat
```

```
write('immetti il numero intero : ');readln(a);
until a>1;
textcolor(14);
writeln;
writeln('Questi sono i numeri inferiori a ',a,' e primi con ',a);
writeln;
write('  ');
fi:=0;
for i:=2 to a do
begin
n:=a;
k:=i;
s:=a mod i;
if s<>0 then q:=i;
r:=n mod k;
while r<>0 do
        begin
          r:=n mod k;
          n:=k;
          k:=r;
        end;
 mcd:=n;
 if mcd=1 then begin fi:=fi+1;write(q,'  ');end;
 end;
  textcolor(12);
 writeln;writeln;writeln('Pertanto');
writeln;
 writeln('La quantità dei numeri minori di ',a,' e primi con ',a,' e" ',fi);
 writeln;
 writeln('Quindi   ---->         Fi = ',fi);
readln;
end.
```

La funzione $\varphi\ (\ n\ )$ gode delle seguenti proprietà:

a) $n = \sum_{d|n} \varphi(d)$

b) $n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$

c) $n = 2 \cdot \varphi(n)$ *se e solo se* $n = 2^k$ *con* $k \geq 1$

d) Se $n\ (\geq 2)$ ha r fattori primi distinti, allora $\varphi(n) \geq \frac{n}{2^r}$

Se $n\ (\geq 2)$ ha s fattori primi dispari distinti, allora 2^s *divide* $\varphi(n)$

Se $n\ (\geq 2)$ è un numero composto, allora $\varphi(n) \leq n - \sqrt{n}$

e) Per $n > 2$ la $\varphi(n)$ è pari

f) Se n è dispari allora $\varphi(2n) = \varphi(n)$

Se n è pari allora $\varphi(2n) = 2 \cdot \varphi(n)$

g) $\varphi(3n) = \begin{cases} 3 \cdot \varphi(n) & \text{se 3 è un divisore di } n \\ 2 \cdot \varphi(n) & \text{in ogni altro caso} \end{cases}$

h) $\varphi(n^2) = n \cdot \varphi(n) \quad \forall\, n \in N$

Applicazioni della funzione $\varphi\,(n)$.

- Teorema di Eulero: Se MCD (a , n) = 1 , allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.
  Questo teorema ci permette di calcolare l'ultima cifra di una potenza una volta scritta in forma estensiva.
  Es. Si voglia calcolare il numero delle unità della potenza 13^5. Usando una normale calcolatrice la sua forma estensiva è $13^5 = 371293$, pertanto la cifra delle unità è 3. Usiamo ora il teorema di Eulero. La cifra delle unità di un numero è il resto della divisione del numero per 10. Calcoliamo prima $13 \equiv 3 \pmod{10}$ e $\varphi(10) = 4$ con l'esponente $5 = 4\cdot 1 + 1$
  Sostituendo in $13^5 \equiv 3^{4\cdot 1+1} = (3^4)^1 \cdot 3^1$, ma $3^4 \equiv 1 \pmod{10}$, quindi sostituendo si ha $13^5 \equiv 3^{4\cdot 1+1} = (3^4)^1 \cdot 3^1 \equiv 1^1 \cdot 3^1 = 3$, pertanto il resto della divisione di 13^5 per 10 è 3, che costituisce la cifra delle unità del numero in forma estensiva della potenza di 13^5.
  Questo esempio è alquanto banale in quanto una calcolatrice o il calcolo manuale ci permette di trovare in tempi brevi la cifra delle unità.
  Calcoliamo ora la cifra delle unità della potenza 237^{135}. In questo caso le normali calcolatrici non ti permettono di scrivere in forma estensiva tale potenza. Applichiamo il procedimento fatto prima:
  $237 \equiv 7 \pmod{10}$; $\varphi(10) = 4$, $135 = 33\cdot 4 + 3$; sostituendo
  $237^{135} \equiv 7^{33\cdot 4+3} = (7^4)^{33} \cdot 7^3$, ma $7^4 \equiv 1 \pmod{10}$, quindi sostituendo si ha:
  $237^{135} \equiv 7^{33\cdot 4+3} = (7^4)^{33} \cdot 7^3 = 1^{33} \cdot 7^3 = 343 \equiv 3 \pmod{10}$
  In definitiva la cifra delle unità della potenza 237^{135} è 3.

- Il numero delle frazioni proprie ridotte ai minimi termini con denominatore n è $\varphi\,(n)$.
  Es. Sia n = 12. Tutte le frazioni proprie con denominatore 12 sono:
  $\frac{1}{12}$; $\frac{2}{12}=\frac{1}{6}$; $\frac{3}{12}=\frac{1}{4}$; $\frac{4}{12}=\frac{1}{3}$; $\frac{5}{12}$; $\frac{6}{12}=\frac{1}{2}$; $\frac{7}{12}$; $\frac{8}{12}=\frac{2}{3}$; $\frac{9}{12}=\frac{3}{4}$; $\frac{10}{12}=\frac{5}{6}$; $\frac{11}{12}$;
  le frazioni ridotte con denominatore uguale a 12 sono:
  $$\frac{1}{12} \;;\; \frac{5}{12} \;;\; \frac{7}{12} \;;\; \frac{11}{12}$$
  Per un totale di 4; ora $\varphi\,(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$; il numero delle frazioni proprie ridotte ai minimi termini con denominatore 12 sono precisamente $\varphi\,(12)$.

- La cardinalità dell'insieme degli elementi invertibili nell'anello Z_n della classe resto modulo n
  è $\varphi\,(n)$

  Es. - Consideriamo la classe resto modulo 4 : $Z_4 = \{[0], [1], [2], [3]\}$. Introduciamo due operazioni l'addizione + e la moltiplicazione *. Siano

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

le tabelle operative. Si dimostra che la struttura algebrica $(Z_4, +, *)$ costituisce un anello: un anello non di integrità in quanto presenta un divisore dello zero il 2 : infatti 2 * 2 = 0. Gli elementi invertibili sono l' 1 e il 3 : infatti essi ammettono se stessi come elementi inversi: cioè 1 * 1 = 1 e 3 * 3 = 1. Pertanto il numero degli elementi invertibili sono 2 che risulta uguale $\varphi(4) = 2$. Se $\mathcal{U}(Z_4) = \{[1], [3]\}$, allora $\# \mathcal{U}(Z_4) = 2 = \varphi(4)$

- Consideriamo la classe resto modulo 5 : $Z_5 = \{[0], [1], [2], [3], [4]\}$. Introduciamo due operazioni l'addizione + e la moltiplicazione *. Siano

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

le tabelle operative. Si dimostra che la struttura algebrica $(Z_5, +, *)$ costituisce un anello, anzi un anello di integrità privo di divisori dello zero (0).

Gli elementi invertibili sono 1, 2, 3, 4 : infatti essi ammettono come elementi inversi rispettivamente 1, 3, 2, 4: cioè 1 * 1 = 1, 2 * 3 = 1 , 3 * 2 = 1, 4 * 4 = 1 . Pertanto il numero degli elementi invertibili sono 4 che risulta uguale $\varphi(5) = 4$.

Se $\mathcal{U}(Z_5) = \{[1], [2], [3], [4]\}$, allora $\# \mathcal{U}(Z_5) = 4 = \varphi(5)$

B) La funzione $y = d\,(\,n\,)$

Def. La funzione $y = d\,(\,n\,)$ è la funzione aritmetica il cui valore è il numero dei divisori del numero *n.*

Es: - Calcolare il numero dei divisori del numero 12.
I divisori del numero 12 sono: 1, 2, 3, 4, 6, 12; per un totale di 6 elementi. Pertanto $d\,(\,12\,) = 6$

- Calcolare il numero dei divisori del numero 13.
I divisori del numero 13 sono: 1 e 13: in fatti il numero 13 è un numero primo; per un totale di 2 elementi. Pertanto $d\,(\,13\,) = 2$.

Cerchiamo ora una formula che ci permette di individuare il valore di $d\,(\,n\,)$

Se *n* = p: cioè un numero primo i divisori sono 1 e p per un totale di 2: quindi $d\,(\,n\,) = 2$
Se *n* = p^m: cioè ad una potenza di un numero primo p, i divisori di *n* sono tutte le potenze di p del tipo p^k con $0 \leq k \leq m$; per un totale di m+1; pertanto $d\,(\,n\,) = m + 1$
Se *n* è un numero composto, sappiamo dal Teorema fondamentale dell'Aritmetica che tale numero è decomponibile in fattori primi e tale decomposizione è unica a meno dell'ordine dei fattori. Sia $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ la decomposizione canonica di *n* in fattori primi, il valore di $d\,(\,n\,)$ è dato da:

$$(2) \qquad d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1) = \prod_{p^{\alpha}|n}(\alpha + 1)$$

in quanto, come avremo modo di vedere, la funzione $d\,(\,n\,)$ è moltiplicativa: cioè se $n = p_1^m \cdot p_2^r$,

$$d\,(\,n\,) = d\,(p_1^m \cdot p_2^r) = d\,(\,p_1^m) \cdot d(\,p_2^r\,) = (m + 1)(r + 1)$$

L'espressione formale (2) costituisce la formula per individuare il valore di $d\,(\,n\,)$, dopo aver scomposto in fattori primi il numero *n.*

Es. Sia *n* = 18 , scomposto in fattori primi risulta $18 = 2^1 \cdot 3^2$; pertanto

$$d\,(\,18) = (1 + 1)(2 + 1) = 6.$$

Infatti i divisori di 18 sono 1, 2, 3, 6, 9, 18 ; per un totale di 6 elementi.

La funzione $d(n)$ gode della seguente proprietà:

a) $\forall n \in N \;:\; \prod_{m|n} m = n^{\frac{d(n)}{2}}$
b) $d(n)$ è dispari se e solo se *n* è un quadrato perfetto
c) $d(n) = 2$ se e solo se *n* un numero primo

C) La funzione $y = \sigma(n)$

Def. La funzione $y = \sigma(n)$ è una funzione aritmetica il cui valore è la somma dei divisori di *n*.

Es.: a) Calcolare la somma dei divisori di 24.
I divisori di 24 sono 1, 2, 3, 4, 6, 8, 12, 24, la cui somma è :
1 + 2 + 3 + 4 + 6 + 8 + 12 + 24 = 60
Pertanto $\sigma(24) = 60$

b) Calcolare la somma dei divisori di 17.
Il numero 17 è primo, pertanto i suoi divisori sono 1 , 17, la cui somma è 1 + 17 = 18
Pertanto $\sigma(17) = 18$

Cerchiamo ora una formula che ci permette di individuare il valore di $\sigma(n)$

Se *n* = p numero primo, i divisori di un numero primo sono 1 e p, pertanto $\sigma(n) = p + 1$.
Se *n* = p^k : cioè *n* è uguale ad una potenza di un numero primo, i divisori di *n* sono tutte le potenze di p del tipo p^m con $0 \leq m \leq k$ per un totale di k + 1 elementi . Tali divisori costituiscono una progressione geometrica di ragione p, pertanto la somma di tali divisori, ricordando la formula della somma degli elementi di una progressione geometrica, è

$$\sigma(n) = p^0 \ \frac{p^{k+1}-1}{p-1} = \frac{p^{k+1}-1}{p-1}$$

Se *n* è un numero composto, sappiamo dal Teorema fondamentale dell'Aritmetica che tale numero è decomponibile in fattori primi e tale decomposizione è unica a meno dell'ordine dei fattori. Sia $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ la decomposizione canonica di *n* in fattori primi, il valore di $\sigma(n)$ è dato da:

(3) $$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1} = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

L'espressione formale (3) costituisce la formula per individuare il valore di $\sigma(n)$, dopo aver scomposto in fattori primi il numero *n.*

Es. Sia *n* = 48 , scomposto in fattori primi risulta $48 = 2^4 \cdot 3^1$; pertanto

$$\sigma(48) = \frac{2^5-1}{2-1} \cdot \frac{3^2-1}{3-1} = \frac{31}{1} \cdot \frac{8}{2} = 124.$$

Infatti i divisori di 48 sono 1, 2, 3, 4, 6, 8, 12, 16, 24, 48 , la cui somma è
1 + 2 + 3 + 4 + 6 + 8 + 12 + 16 + 24 + 48 = 124

Tale funzione gode della seguente proprietà:

a) $\forall n \in N \ : \ \frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$
b) $\sigma(n)$ è dispari se e solo se *n* è un quadrato perfetto o *n* è il doppio di un quadrato perfetto.

Stesura del programma in Turbo Pascal relativo alle funzione $d\ (\ n\ )$ e $\sigma\ (n)$

```
program funzione_divori_di_n;
uses crt;
var i,j,k,a,s:longint;
   m:array[1..1000] of longint;
   risp:char;
procedure numero(v:integer);
var n,r:integer;
begin
  k:=0 ;
  for n:=v downto 1 do
       begin
         r:= v mod n;
         if r = 0 then
           begin k:=k+1; m[k]:= v div n;end;
       end;
end;
begin
 repeat
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma determina i divisori di un numero naturale assegnato');
 writeln('determina il numero di tali divisori: cioè la funzione d(n), la somma:');
 writeln('cioè la funzione σ(n) ; inoltre il prodotto di tali divisori.');
 writeln;
 textcolor(12);
 write('Inserisci un numero intero positivo a = ');readln(a);
 textcolor(10);
 numero(a);
 writeln('I divisori di ',a,' sono: ');
 s:=0;
 for j:=1 to k do
  begin
  write(m[j]:5);
  s:=s+m[j];
  end;
 writeln;
 writeln('Per un totale di : d(',a,') = ',k);
writeln;
 writeln('La somma dei divisori di ',a,': cioè σ(',a,') = ',s);
 writeln;
 textcolor(14);
 write('Vuoi continuare con altro valore di n ? (S/N): ');
 readln(risp);
```

```
until (risp='n') or (risp='N');
end.
```

D) La funzione $y = r(n)$

Def. La funzione $y = r(n)$ rappresenta il numero delle soluzioni, in interi x e y, dell'equazione $x^2 + y^2 = n$.

Se indichiamo con $d_1(n)$ il numero dei divisori di n della forma $4 \cdot k + 1$ e con $d_3(n)$ il numero dei divisori di n della forma $4 \cdot k + 3$, allora il valore di $r(n)$ è dato da:

$$r(n) = 4 \cdot [d_1(n) - d_3(n)]$$

Es. 1) Determinare il numero delle coppie (x ; y) soluzioni intere, se esistono, dell'equazione $x^2 + y^2 = 28$

Risoluzione:

I divisori di 28 sono 1, 2, 4, 7, 14 , 28 di cui

1 è della forma 4k+1

7 è della forma 4k+3

$r(28) = 4 \cdot (1 - 1) = 0$, pertanto l'equazione non ammette alcuna coppia di numeri interi che risolve l'equazione data

2) Determinare il numero delle coppie (x ; y) soluzioni intere, se esistono, dell'equazione $x^2 + y^2 = 32$

Risoluzione:

I divisori di 32 sono 1, 2, 4, 8, 16, 32 di cui

1 è della forma 4k+1

Non sono presenti tra i divisori numeri della forma 4k+3

$r(32) = 4 \cdot (1 - 0) = 4$, pertanto l'equazione data ammette quattro coppie di soluzioni intere e precisamente: (4 ; 4) , (-4 ; 4) , (-4 ; -4) , (4 ; -4)

3) Determinare il numero delle coppie (x ; y) soluzioni intere, se esistono, dell'equazione $x^2 + y^2 = 37$

Risoluzione:

I divisori di 37 sono 1, 37 di cui

1 e 37 sono della forma 4k+1

Non sono presenti tra i divisori numeri della forma 4k+3

$r(37) = 4 \cdot (2 - 0) = 8$, pertanto l'equazione data ammette otto coppie di soluzioni intere e precisamente: (6 ; 1) , (-6 ; 1) , (-6 ; -1) , (6 ; -1) , (1 ; 6) , (-1 ; 6) , (-1 ; -6) , (1 ; -6)

NB

1) Se consideriamo la coppia (x ; y), con $|x| \neq |y|$, come le coordinate di un punto riferito ad un sistema di coordinate cartesiane ortogonali, gli elementi delle coppie soluzioni dell'equazione $x^2 + y^2 = n$ risultano invertibili e simmetriche rispetto agli assi cartesiani e rispetto all'origine del sistema cartesiano. Pertanto

trovata una coppia, le altre coppie si trovano per simmetria ed invertibilità, nel caso che | x | = | y | le altre coppie si trovano solo per simmetria.

2) Se $n = z^2$: cioè risulta un quadrato perfetto la risoluzione va ricercata nelle terne pitagoriche che verificano l'equazione: quindi se z è della forma m^2+1, allora x è della forma $m^2 - 1$ e y della forma 2m. Pertanto per ogni coppia che verifica bisogna moltiplicare per 8 e sommare le quattro coppie banali (z ; 0) , (-z ; 0) , (0 ; -z) , (0 ; 0).

Es. Determinare il numero delle coppie (x ; y) soluzioni intere, se esistono, dell' quazione $x^2 + y^2 = 25$

Risoluzione:

$z = 5 = 4 + 1 = 2^2 + 1$, pertanto $x = 2^2 - 1 = 3$ e $y = 2 \cdot 2 = 4$

Col metodo delle terne pitagoriche, l'esistenza di una coppia permette di individuare tutte le altre coppie per simmetria ed invertibilità per un totale di 8 coppie; inoltre bisogna aggiungere (5 ; 0) , (-5 ; 0) , (0 ; 5) , (0 ; - 5); per un totale complessivo di 12 coppie

Col metodo dei divisori operando si ha:

i divisori di 25 sono 1, 5, 25 sono della forma 4k+1

Non sono presenti tra i divisori numeri della forma 4k+3

$r(32) = 4 \cdot (3 - 0) = 12$, pertanto l'equazione data ammette 12 coppie

Pertanto i due metodi si equivalgono.

Stesura del programma in Turbo Pascal relativo alla funzione $r\ (n)$

```
program funzione_r(n);
uses crt;
var n,k,j,x,y:integer;
   risp:char;
procedure divisori;
 var i:integer;
 begin
    write('I divisori propri ed impropri di ',n,' sono:');
    for i:=1 to n do
       if n mod i = 0 then write('  ',i);
    writeln;
  end;
procedure divisori1;
 var i:integer;
 begin
   k:=0;  j:=0;
   write('I divisori del tipo 4k+1 di ',n,' sono:');
   for i:=0 to n div 4 do
       if n mod (4*i+1) = 0 then
         begin
```

```
            k:=k+1;
            write('  ',4*i+1);
           end;
     writeln;
     write('I divisori del tipo 4k+3 di ',n,' sono:');
    for i:=0 to n div 4 do
        if n mod (4*i+3) = 0 then
           begin
            j:=j+1;
            write('  ',4*i+3);
           end;
     writeln;
  end;
begin
  repeat
   clrscr;
   writeln('Questo programma ti permette calcolare la funzione r(n),che');
   writeln('rappresenta il numero delle soluzioni in interi relativi (x,y)');
   writeln('dell''equazione    x^2 + y^2 = n ');
   writeln;
   writeln('Se indichiamo con d1(n) il numero dei divisori di n del tipo 4k+1');
   writeln('          e  con d3(n) il numero dei divisori di n del tipo 4k+3');
   writeln('          allora    r(n) = 4*( d1(n) - d3(n) ).');
   textcolor(10);
   write('Immetti il valore del termine noto  n = ');readln(n);
   textcolor(11);
   divisori;
   divisori1;
   writeln('Pertanto il numero dei divisori del tipo 4k+1 è d1(',n,') = ',k);
   writeln('  mentre il numero dei divisori del tipo 4k+3 è d3(',n,') = ',j);
   if k-j<>0 then
   begin
   writeln('Quindi la funzione r(',n,') = ',4*(k-j));
   writeln('Infatti: ');
   for x:=-100 to 100 do
    for y:=-100 to 100 do
      if x*x+y*y=n then writeln('        (',x,')^2 + (',y,')^2 = ',n);
   end
   else
   writeln('Non esistono coppie di numeri interi tale che x^2 + y^2 = ',n);
   readln;
   write('Vuoi ripetere con altri numeri ? (S/N) ');
   readln(risp);
   risp:=upcase(risp);
```

```
    until risp='N';
  end.
```

E) La funzione $y = \mu(n)$, detta *funzione di Möebius*

Def. La funzione $y = \mu(n)$, detta *funzione di Möebius*, è la funzione aritmetica così caratterizzata:

$$\begin{cases} \mu(1) = 1 \\ \mu(n) = 0 \quad se\ nella\ decomposizione\ canonica\ di\ n, qualche\ esponente\ a_i > 1 \\ \mu(n) = (-1)^r \ \ se\ nella\ decomposizione\ canonica\ di\ n, ogni\ esponente\ \alpha_i = 1 \end{cases}$$

Dove r indica il numero dei fattori primi ad esponente 1 della decomposizione canonica.

Esempi:

1) Determinare $\mu(54)$.
   Risoluzione: $54 = 2 \cdot 3^3$. La decomposizione canonica di 54 presenta un fattore primo ad esponente $3 > 1$, pertanto $\mu(54) = 0$.
2) Determinare $\mu(210)$.
   Risoluzione: $210 = 2 \cdot 3 \cdot 5 \cdot 7$. La decomposizione canonica di 30 presenta tutti e quattro i fattori primi ad esponente 1 , pertanto $\mu(30) = (-1)^4 = 1$.
3) Determinare $\mu(23)$.
   Risoluzione: $23 = 23$. La decomposizione canonica di 23 presenta un fattore primo ad esponente 1 , pertanto $\mu(23) = (-1)^1 = -1$.

Stesura del programma in Turbo Pascal relativo alla funzione $\mu(n)$

```
program Mobius;
uses crt;
var n,k,b,i,y,r,p,t1,n1,s,j,mu:longint;
   a,b1,m,q:array[1..1000] of longint;
   t:boolean;
   risp:char;
function pot(x,y:integer):integer;
begin
  if y=0 then pot:=1
        else pot:=x*pot(x,y-1);
end;
procedure divisori(y:integer);
var i:integer;
begin
   for i:=1 to y do
        if (y/i)=int(y/i) then write('  ',i);
end;
begin
```

```
repeat
  clrscr;
  textcolor(14);
  writeln('Questo programma ti permette di determinare la funzione di MÖEBIUS');
  writeln('così definita:    mu(1)=1');
  writeln('                  mu(n)=0 se scomposto in fattori primi n, questi');
  writeln('                        presentano almeno un esponente >1');
  writeln('                  mu(n)=(-1)^r,dove r è il numero dei fattori primi');
  writeln('                        di n con esponenti tutti uguali ad 1');
  writeln;
  textcolor(10);
  write('Immetti un numero positivo : ');
  readln(n); n1:=n;
  writeln;
  if n<>1 then
     begin
       write('Scomposto in fattori primi risulta: ');
       b:=n;
       y:=0;
       for k:=2 to n do
          begin
           t:=false;
           for i:=2 to k-1 do
              if k/i=int(k/i) then t:=true;
           if t=false then
                    begin
                      y:=y+1;
                      a[y]:=k;
                    end;
          end;
     write(b,' = ');
     i:=0;
    for k:=1 to y do
       begin
         r:=0;
         repeat
           if (n mod a[k] = 0) then
             begin
               r:=r+1;
               n:=n div a[k];
             end;
         until (n mod a[k] <>0) or (r=0);
         if r<>0 then
            begin
              i:=i+1;
              write(a[k],'^',r,' ú ');
              q[i]:=a[k];
```

```
                    b1[i]:= r;
                  end;
               s:=i;
             end;
          writeln;
          k:=0;
          for i:=1 to s do
              if (b1[i]=1) then k:=k+1;
          if k = s then mu:=pot(-1,k)
                else mu:=0;
       end
       else
         if n1=1 then mu:=1;
       writeln;
    writeln('La funzione di Möebius  m(',n1,') = ',mu);
      readln;
      textcolor(11);
      write('Vuoi ripetere con altro valore di n ? (S/N): ');
      readln(risp);
    until (risp='n') or (risp='N');
end.
```

- **Trasformata e formula di inversione di Möebius**

Def. Sia f (n) una funzione aritmetica, si chiama *trasformata di Möebius* di f(n) la funzione aritmetica F così definita:

$$F(n) = \sum_{d|n} f(d) \qquad \forall\, n \in N_0$$

Def. (Formula di inversione di Möbius). Siano *f* una funzione aritmetica ed *F(n)* la sua trasformata di Möebius, la relazione

$$f(n) = \sum_{e|n} \mu(e) \cdot F\left(\frac{n}{e}\right) \qquad con \;\; e = \frac{n}{d}$$

è detta *formula di inversione di Möebius* .

Enunciamo ora il Teorema di inversione di Möbius :

Teorema Siano f(n) e g(n) due funzioni aritmetiche, se $f(n) = \sum_{d|n} g(d)$ allora $g(n) = \sum_{d|n} f\left(\frac{n}{d}\right)\mu(d)$ e viceversa.

Da questo teorema di inversione possiamo dedurre che $n = \sum_{d|n} \varphi(d)$, sapendo che

$$\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d)$$

Esempio: Sia n = 12, scomposto in fattori primi è $12 = 2^2 \cdot 3$.

$$d(12) = 12 \cdot \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3}\right) = 3 \cdot 2 = 6 \;\; ; \;\; \varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

I divisori di 12 sono: 1 ; 2 ; 3 ; 4 ; 6 ; 12

$\mu(1) = 1$; $\mu(2) = -1$; $\mu(3) = -1$; $\mu(4) = 0$; $\mu(6) = 1$; $\mu(12) = 0$

$$\varphi(12) = \frac{12}{1}\cdot(1) + \frac{12}{2}(-1) + \frac{12}{3}(-1) + \frac{12}{4}(0) + \frac{12}{6}(1) + \frac{12}{12}(0) = 4 =$$

$$= \sum_{d|12} \frac{12}{d}\mu(d)$$

$\varphi(1) = 1$; $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(6) = 2$; $\varphi(12) = 4$

$$n = 1 + 1 + 2 + 2 + 2 + 4 = 12 = \sum_{d|12} \varphi(d)$$

Teorema di Gauss: Se $\Phi(n) = \sum_{d|n} \varphi(d)$ è la trasformata di Möebius della funzione $\varphi(n)$ di Eulero, allora $\Phi(n) = I(n) = n$.

Es. Vogliamo verificare che $\Phi(12) = 12$

I divisori di 12 sono: 1 ; 2 ; 3 ; 4 ; 6 ; 12

$\varphi(1) = 1$; $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(6) = 2$; $\varphi(12) = 4$

$$n = 1 + 1 + 2 + 2 + 2 + 4 = 12 = \sum_{d|12} \varphi(d)$$

Applicando il Teorema di Gauss si ha : $\Phi(12) = \sum_{d|12} \varphi(d) = 12$

Stesura del programma relativo al Teorema di Gauss

```
program Teorema_di_Gauss;
uses crt;
var n,k,j,h,s:integer;
   m,fi:array[1..100] of integer;
   risp:char;
function mcd(x,t:longint):longint;
begin
 if t=0 then mcd:=x
       else mcd:=mcd(t,x mod t);
end;
procedure divisori(v:integer);
var i,r:integer;
begin
 k:=0 ;
 for i:=v downto 1 do
      begin
        r:= v mod i;
        if r = 0 then
          begin k:=k+1; m[k]:= v div i;end;
      end;
end;
function f(a:integer):integer;
```

```
var i:integer;
begin
  h:=0;
  for i:=1 to a do
    if mcd(a,i)=1 then h:=h+1;
  f:= h;
end;
begin
   textbackground(1);
   clrscr;
    repeat
      textcolor(15);
      writeln('Questo programma ti permette di verificare il Teorema di Gauss, che dice:');
      writeln(' "La trasformata di Moebius della funzione Totiene di Eulero è uguale');
      writeln('  alla funzione identita" I(n)=n "  ');
      writeln;
      textcolor(12);
      write('Immetti un numero naturale  n = ');readln(n);
      divisori(n);
      writeln;
      writeln('Le seguenti coppie sono costituite da un divisore di n e dal suo totiene:');
      s:=0;
      for j:=1 to k do
                 begin
                    fi[j]:=f(m[j]);
                    write('( ',m[j],';',fi[j],') - ');
                    s:=fi[j]+s;
                 end;
      writeln;writeln;textcolor(10);
      write('La trasformata di Moebius del totiene di ',n,' vale ',s);
      if n=s then writeln(', pertanto vale il teorema di Gaus ')
            else writeln(', pertanto non vale il teorema di Gaus ');
      writeln;writeln; textcolor(14);
      write('Vuoi continuare con altro valore di n ? (S/N) ');
      readln(risp);
    until (risp='n') or (risp='N');
end.
```

La funzione inversa della funzione aritmetica d è la funzione unitaria:

$$v(n) = \sum_{m|n} \mu(m) \cdot d\left(\frac{n}{m}\right) = 1$$

La funzione inversa della funzione aritmetica σ è la funzione identità:

$$I(n) = \sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n$$

Relazioni fra le funzioni aritmetiche:

Si dimostra che

a) $\varphi(n) = \sum_{k|n} \frac{n}{k}\mu(k)$

a) $\sum_{m|n} \sigma(m) = n \cdot \sum_{m|n} \frac{d(m)}{m}$

b) $\sum_{m|n} d(m) = n \cdot \sum_{k|n} \frac{\sigma(m)}{m}$

c) $\forall n \in N:$ $\varphi(n) + \sigma(n) = 2 \cdot n$ se e solo se n è primo

Funzioni aritmetiche moltiplicative

In analisi nello studio delle funzioni si dimostra che la funzione derivata e la funzione integrale sono funzioni additive: infatti siano $y_1 = f(x)$ e $y_2 = g(x)$ due funzioni continue, derivabili nello stesso insieme di definizione, siano $y_1' = f'(x)$ e $y_2' = g'(x)$ le loro derivate. Si consideri la funzione $h(x) = f(x) + g(x)$, la derivata $h'(x) = f'(x) + g'(x)$; se $y_1 = f(x)$ e $y_2 = g(x)$ due funzioni integrabili nello stesso intervallo , allora

$$\int h(x)dx = \int \big(f(x) + g(x)\big)dx = \int f(x)dx + \int g(x)dx$$

Mentre la funzione limite oltre che essere additiva e anche moltiplicativa infatti

$$\lim_{x\to x_0}[f(x) + g(x)] = \lim_{x\to x_0} f(x) + \lim_{x\to x_0} g(x)$$

$$\lim_{x\to x_0}[f(x) \cdot g(x)] = \lim_{x\to x_0} f(x) \cdot \lim_{x\to x_0} g(x)$$

Consideriamo ora le funzioni aritmetiche

Si può verificare con un contro esempio che esse non sono additive.

Vogliamo enunciare una definizione che impone delle condizioni perché le funzioni aritmetiche siano moltiplicative

Def. Siano $m, n \in N,\ con\ MCD(m,n) = 1$, e f una funzione aritmetica, si dice che la funzione *f è semplicemente moltiplicativa* se è verificata la relazione

$$f(n \cdot m) = f(n) \cdot f(m)$$

nel caso che $\forall\, m, n \in N$ si verifica che $f(n \cdot m) = f(n) \cdot f(m)$, la funzione *f* si dice *totalmente moltiplicativa.*

Tutte le funzioni aritmetiche trattate precedentemente, fatta eccezione di $y = r(n)$, sono semplicemente e non totalmente moltiplicative.

20

a) Consideriamo la funzione aritmetica $\varphi\ (\ n\ )$ e dimostriamo che essa è moltiplicativa se $\forall\ m,n\ \in N\ \ con\ \ MCD(m,n) = 1$ allora $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Dimostrazione

Per il teorema dell'unicità della decomponibilità in fattori primi di un numero naturale siano

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \quad \text{e} \quad m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$$

Poiché per ipotesi MCD(m ; n) = 1, allora $\forall\ p_i^{\alpha_i}\ e\ q_j^{\beta_j}$ elementi delle decomposizioni essi sono diseguali; moltiplicando m per n la decomposizione del prodotto presenta come fattori primi tutti i fattori primi delle singole decomposizioni di n e di m

$$n \cdot m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$$

Applicando la definizione di φ , scriviamo

$$\varphi(n \cdot m) = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) \cdot \left(1 - \frac{1}{q_1}\right) \cdot \left(1 - \frac{1}{q_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{q_s}\right)$$

Per la proprietà associativa del prodotto, scriviamo:

$$\varphi(n \cdot m) = \left[\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)\right] \cdot \left[\left(1 - \frac{1}{q_1}\right) \cdot \left(1 - \frac{1}{q_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{q_s}\right)\right]$$

Sapendo che

$$\varphi\ (\ n\ ) = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) \ \text{ e } \ \varphi\ (\ m\ ) = \left(1 - \frac{1}{q_1}\right) \cdot \left(1 - \frac{1}{q_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{q_s}\right)$$

e sostituendo, otteniamo

$$\varphi(n \cdot m) = \varphi(\ n\ ) \cdot \varphi(\ m\ )$$

cvd.

Abbiamo dimostrato che la funzione $\varphi\ (\ n\ )$ è moltiplicativa quando presi due numeri naturali m , n, il loro MCD(m;n)=1 ; nel caso che tale MCD(m;n) $\neq$ 1 allora

$$\varphi\ (\ n\ \cdot m) = \varphi\ (\ n\ ) \cdot \varphi\ (\ m\ ) \cdot \frac{d}{\varphi\ (\ d)}\ ,$$

dove d = MCD (n ; m), non è moltiplicativa.

Esempio:

- Siano m = 15 e n = 12 , calcolare il numero dei numeri minori di 15 x 12 ma primi con 15 x 12, noti il numero dei numeri minori di 15 e 12 e primi con questi.
  Risoluzione: $\varphi\ (\ 15\ ) = 8\ ;\ \varphi\ (\ 12\ ) = 4\ \ ;\ \ \text{MCD}(\ 15\ ;\ 12\ ) = 3\ ;\ \varphi\ (\ 3\ ) = 2$

  $$\varphi\ (\ 15 \cdot 12\ ) = \ \varphi\ (\ 15\ ) \cdot \varphi\ (\ 12\ ) \cdot \frac{3}{\varphi\ (\ 3\ )}$$

  $$\varphi\ (\ 15 \cdot 12\ ) = 8\ \cdot 4 \cdot \frac{3}{2} = 48$$

  Calcolando il numero dei numeri minori di 180 ma primi con 180, esso risulta 48.
- Siano n = 14 e m = 9 , calcolare il numero dei numeri minori di 14 x 9 ma primi con 14 x 19, noti il numero dei numeri minori di 14 e 9 e primi con questi.
  Risoluzione: $\varphi\ (\ 14\ ) = 4\ \ ;\ \varphi\ (\ 9\ ) = 3\ \ ;$ MCD (14 ; 9) = 1 ;

  $$\varphi\ (\ 14 \cdot 9\ ) = \ \varphi\ (\ 14\ ) \cdot \varphi\ (\ 9\ )$$

  $$\varphi\ (\ 14 \cdot 9\ ) = 4\ \cdot 3 = 12$$

  Calcolando il numero dei numeri minori di 126 ma primi con 126, esso risulta 12

Per $\varphi\ (\ n\ )$ non moltiplicativa , si dimostra le seguenti relazioni:

a) Se *n* divide *m*, allora $\varphi(n)$ divide $\varphi(m)$

b) $\varphi(n)\cdot\varphi(m)=\frac{\varphi(n\cdot m)\cdot\varphi(d)}{d}$ con d = MCD (n ; m)

c) $\varphi(n)\cdot\varphi(m)=\varphi(d)\cdot\varphi(t)$ con d = MCD(n ; m) e t = mcm(n ; m)

Stesura programma in Turbo Pascal relativa alla funzione $\varphi(n\cdot m)$

```
Program fi_moltiplicativa;
uses crt;
var  a,b,m,n,p,p1,d,d1:longint;
function mcd(x,t:longint):longint;
begin
  if t=0 then mcd:=x
        else mcd:=mcd(t,x mod t);
end;
function fi(a:longint):longint;
var i,k:longint;
begin
  k:=0;
  for i:=1 to a do
    if mcd(a,i)=1 then k:=k+1;
  fi:=k;
end;
begin
  clrscr;
  textcolor(14);
  writeln('Questo programma ti permette di verificare che la funzione di Eulero');
  writeln('                    fi(n*m)= fi(n)*fi(m) ');
  writeln('cioŠ essa Š moltiplicativa nel caso che MCD(m,n)= 1 ');
  writeln;
  writeln('Nel caso che MCD(m,n)=d <> 1 allora fi(n*m)= fi(n)*fi(m)*d/fi(d) ');
  writeln;
  textcolor(12);
  write('Immetti il primo fattore:   a = ');readln(a);
  writeln('          fi(',a,') = ',fi(a));
  write('Immetti il secondo fattore: b = ');readln(b);
  writeln('          fi(',b,') = ',fi(b));
  m:=fi(a);
  n:=fi(b);
  p:=a*b; p1:=fi(p);
  d:=mcd(a,b); d1:=fi(d);
  textcolor(10);
  writeln;write('d = MCD(',a,';',b,') = ',d);
```

```
        writeln('    -       fi(',d,') = ',fi(d));
        writeln;
        textcolor(15);
        if d=1 then
            begin
            writeln('fi(',a,'*',b,') = fi(',a,')*fi(',b,'): ', p1,' = ',m,'*',n);
            writeln('Infatti fi(',a*b,') = ',fi(a*b));
            end
            else
            begin
            writeln('fi(',a,'*',b,') = fi(',a,')*fi(',b,')*d/fi(d) : ', p1,' = ',m,'*',n,'*',d,'/',d1);
            writeln('Infatti fi(',a*b,') = ',fi(a*b));
            end;
        readln;
      end.
```

b) Consideriamo la funzione aritmetica $d(\,n\,)$ e dimostriamo che essa è moltiplicativa se $\forall\ m,n\ \in N\ \ con\ \ MCD(m,n) = 1$ allora $d(n\cdot m) = d(n)\cdot d(m)$

Dimostrazione

Per il teorema dell'unicità della decomponibilità in fattori primi di un numero naturale siano

$$n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot \ldots \cdot p_r^{\alpha_r} \quad \text{e} \quad m = q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot \ldots \cdot q_s^{\beta_s}$$

Poiché per ipotesi MCD(m ; n) = 1, allora $\forall\ p_i^{\alpha_i}\ e\ q_j^{\beta_j}$ elementi delle decomposizioni essi sono diseguali; moltiplicando m per n la decomposizione del prodotto presenta come fattori primi tutti i fattori primi delle singole decomposizioni di n e di m

$$n\cdot m = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot \ldots \cdot p_r^{\alpha_r}\cdot q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot \ldots \cdot q_s^{\beta_s}$$

Applicando la definizione di d , scriviamo

$$d(n\cdot m) = mn\left(1-\frac{1}{p_1^{\alpha_1}}\right)\cdot\left(1-\frac{1}{p_2^{\alpha_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{p_r^{\alpha_r}}\right)\cdot\left(1-\frac{1}{q_1^{\beta_1}}\right)\cdot\left(1-\frac{1}{q_2^{\beta_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{q_s^{\beta_s}}\right)$$

Per la proprietà associativa e commutativa del prodotto, scriviamo:

$$d(n\cdot m) = \left[n\cdot\left(1-\frac{1}{p_1^{\alpha_1}}\right)\cdot\left(1-\frac{1}{p_2^{\alpha_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{p_r^{\alpha r}}\right)\right]\cdot\left[m\cdot\left(1-\frac{1}{q_1^{\beta_1}}\right)\cdot\left(1-\frac{1}{q_2^{\beta_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{q_s^{\beta_s}}\right)\right]$$

Sapendo che

$$d(\,n\,) = n\cdot\left(1-\frac{1}{p_1^{\alpha_1}}\right)\cdot\left(1-\frac{1}{p_2^{\alpha_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{p_r^{\alpha r}}\right) \text{ e } \tau\,(\,m\,) = \left(1-\frac{1}{q_1^{\beta_1}}\right)\cdot\left(1-\frac{1}{q_2^{\beta_2}}\right)\cdot \ldots \cdot\left(1-\frac{1}{q_s^{\beta_s}}\right)$$

e sostituendo, otteniamo

$$d(n\cdot m) = d(\,n\,)\cdot d(\,m\,)$$

cvd

Per la funzione $y = d\,(\,n\,)$ vale il seguente lemma:

Lemma: Siano a e b due numeri naturali coprimi, il numero dei divisori del loro prodotto è uguale al prodotto dei numeri dei divisori di a e di b; inoltre d è un divisore del prodotto $a\cdot b$ se e solo se è della forma $m\cdot n$, con MCD (m ; n) = 1 , m|a ed n|b.

```
program divisori_del_prodotto;
uses crt;
var i,j,k,p,a,s,k1,k2,c,b,k0:longint;
    m:array[1..1000] of longint;
    risp:char;
function mcd(x,y:longint):longint;
begin
  if y = 0 then mcd:=x
           else mcd:=mcd(y,x mod y);
end;
procedure numero(v:integer);
var n,r:integer;
begin
  k:=0 ;
  for n:=v downto 1 do
        begin
          r:= v mod n;
          if r = 0 then
             begin k:=k+1; m[k]:= v div n;end;
        end;
end;
begin
 repeat
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma determina i divisori di due numeri naturali assegnati');
 writeln('determina il numero di tali divisori, quindi determina il numero dei ');
 writeln('divisori del loro prodotto, verificando che, se MCD ( a ; b) = 1 il ');
 writeln(' prodotto dei numeri dei divisori dei due numeri assegnati coincide col ');
 writeln(' numero dei divisori del loro prodotto ');writeln;
 textcolor(12);
 write('Inserisci il primo numero intero positivo a = ');readln(a);
 write('Inserisci il secondo numero intero positivo b = ');readln(b);
 textcolor(10);
 numero(a);
 k0:=k;
 writeln('I divisori di ',a,' sono: ');
 s:=0; p:=1;
 for j:=1 to k do
  begin
  write(m[j]:5);
  s:=s+m[j];
```

```
 p:=p*m[j];
 end;
writeln;
writeln('Per un totale di : d(',a,') = ',k0);
numero(b);
writeln('I divisori di ',b,' sono: ');
k1:=k;
s:=0; p:=1;
for j:=1 to k1 do
     begin
       write(m[j]:5);
       s:=s+m[j];
       p:=p*m[j];
    end;
writeln;
writeln('Per un totale di : d(',b,') = ',k1);
c:=a*b;
numero(c);
writeln('I divisori di ',c,' sono: ');
k2:=k;
s:=0; p:=1;
for j:=1 to k2 do
 begin
 write(m[j]:5);
 s:=s+m[j];
 p:=p*m[j];
 end;
writeln;
writeln('Per un totale di : d(',c,') = ',k2);
if mcd(a,b)=1 then
writeln('Poiché il MCD(',a,';',b,') = ',MCD(a,b),', allora ',k2,' = ',k0,'*',k1)
            else
writeln('Poiché il MCD(',a,';',b,') = ',MCD(a,b),', allora ',k2,' ≠ ',k0,'*',k1) ;
textcolor(14);
write('Vuoi continuare con altro valore di n ? (S/N): ');
readln(risp);
until (risp='n') or (risp='N');
end.
```

c) Consideriamo la funzione aritmetica $\sigma(n)$ e dimostriamo che $\sigma(n)$ è moltiplicativa se $\forall\ m,n \in N\ con\ MCD(m,n) = 1$ allora $\sigma(n \cdot m) = \sigma(n) \cdot \sigma(m)$

Dimostrazione

Per il teorema dell'unicità della decomponibilità in fattori primi di un numero naturale siano

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \quad \text{e} \quad m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$$

Poiché per ipotesi MCD(m ; n) = 1, allora $\forall\ p_i^{\alpha_i}\ e\ q_j^{\beta_j}$ elementi delle decomposizioni essi sono diseguali; moltiplicando m per n la decomposizione del prodotto presenta come fattori primi tutti i fattori primi delle singole decomposizioni di n e di m

$$n \cdot m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$$

Applicando la definizione di σ, scriviamo

$$\sigma(n \cdot m) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1} \cdot \frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} \cdot \ldots \cdot \frac{q_s^{\beta_s+1}-1}{q_s-1}$$

Per la proprietà associativa della moltiplicazione, scriviamo

$$\sigma(n \cdot m) = \left[\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}\right] \cdot \left[\frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} \cdot \ldots \cdot \frac{q_s^{\beta_s+1}-1}{q_s-1}\right]$$

Sapendo che

$$\sigma(n) = \left[\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}\right] \quad \text{e} \quad \sigma(m) = \left[\frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \frac{q_2^{\beta_2+1}-1}{q_2-1} \cdot \ldots \cdot \frac{q_s^{\beta_s+1}-1}{q_s-1}\right]$$

E sostituendo, otteniamo:

$$\sigma(n \cdot m) = \sigma(n) \cdot \sigma(m)$$

cvd.

Teorema: Se *f* è una funzione aritmetica moltiplicativa, la funzione F(n) , trasformata di Möebius di *f*, è moltiplicativa

Dimostrazione

Siano $p, q \in N$ tali che MCD(p ; q) = 1. I divisori di $p \cdot q$ sono tutti del tipo $d_p \cdot d_q$, con d_p divisori di p e d_q divisori di q. Sia $F(p \cdot q) = \sum_{d!pq} f(d)$ con $d = d_p \cdot d_q$.

Ora

$$\sum_{d!pq} f(d) = \sum_{d_p!p} \sum_{d_q!q} f(d_p \cdot d_q) = \sum_{d_p|p} \sum_{d_q|q} f(d_p) \cdot f(d_q) =$$

$$= \sum_{d_p|p} f(d_p) \cdot \sum_{d_q|q} f(d_q) = \text{F(p)} \cdot \text{F (q)}$$

Quindi la funzione F è moltiplicativa.

Così la trasformata della funzione $\mu(n)$ di Möebius: $M(n) = \sum_{d|n} \mu(d)$ è moltiplicativa. Essa è uguale ad 1 nel caso che n=1, è uguale a 0 nel caso che n > 1.

Es. Dopo aver determinato la trasformata della funzione $\mu(24)$, verificare che essa è uguale a 0.

Risoluzione

Per definizione la trasformata di $\mu(24)$ è $M(24) = \sum_{d|24} \mu(d)$.

I divisori di 24 sono: 1, 2, 3, 4, 6, 8, 12, 24; i valori di $\mu(d_i)$ di tali divisori sono $\mu(1) = 1$; $\mu(2) = -1$; $\mu(3) = -1$; $\mu(4) = 0$; $\mu(6) = 1$; $\mu(8) = 0$; $\mu(12) = 0$; $\mu(24) = 0$

Pertanto $M(24) = \sum_{d|24} \mu(d) = 1 - 1 - 1 + 1 = 0$

Teoremi di Euclide e di Eulero sui numeri perfetti

Vogliamo ora dimostrare due teoremi uno di Euclide ed uno di Eulero, le dimostrazione dei quali richiedono la funzione aritmetica $\sigma(n)$.

Prerequisiti:

- Scomposizione in fattori primi di un numero naturale
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r}$$
- Conoscenza della definizione e della formula relativa alla funzione $\sigma(n)$.
$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \frac{p_3^{\alpha_3+1}-1}{p_3-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$
- Se p e $q \in N$ tali che MCD (p ; q) = 1, allora $\sigma(p \cdot q) = \sigma(p) \cdot \sigma(q)$: cioè la funzione $\sigma(n)$ è moltiplicativa
- Def. Un numero si dice perfetto se è uguale alla somma dei suoi divisori (1 compreso e sé stesso escluso).
- Teorema: C.N.S. perché un numero $n \in N$ sia perfetto è che $\sigma(n) = 2n$.

Teorema di Euclide:

Sia $n \in N$. Se $p = 2^{n+1} - 1$ è un numero primo, allora $m = 2^n \cdot (2^{n+1} - 1)$ è un numero perfetto.

Dimostrazione:

Sia $p = 2^{n+1} - 1$ un numero primo. Si considerino il numero $m = 2^n \cdot p$ e la funzione $\sigma(m)$ relativa ad m:

$$\sigma(m) = \sigma(2^n \cdot p)$$

Poiché MCD $(2^n;\ p) = 1$, la funzione $\sigma(2^n \cdot p)$ è moltiplicativa, quindi

$$\sigma(2^n \cdot p) = \sigma(2^n) \cdot \sigma(p)$$

Ora $\sigma(2^n) = \frac{2^{n+1}-1}{2-1} = 2^{n+1} - 1$ e $\sigma(p)$, essendo p un numero primo, è dato dalla somma di p e 1 unici divisori di p: cioè $\sigma(p) = (2^{n+1} - 1) + 1 = 2^{n+1}$

Andando a sostituire in

$\sigma(2^n \cdot p) = \sigma(2^n) \cdot \sigma(p) = (2^{n+1} - 1) \cdot (2^{n+1}) =$

$= (2^{n+1}) \cdot (2^{n+1} - 1) = 2 \cdot 2^n \cdot (2^{n+1} - 1) = 2m$

Si ha $\sigma(m) = 2m$. Per il teorema sulla C.N.S perché un numero sia perfetto, si può affermare che m è un numero perfetto e quindi è possibile esprimerlo

$$m = 2^n \cdot (2^{n+1} - 1)$$

cvd

Teorema di Eulero:

Se $m \in N$ è un numero perfetto pari, allora esiste un $n \in N$ tale che $p = 2^{n+1} - 1$ è un numero primo e $m = 2^n \cdot (2^{n+1} - 1)$.

Dimostrazione

Siano p e $n \in N$, con p dispari, tali che $m = 2^n \cdot p$. Si consideri la funzione $\sigma(m)$ relativa ad m:

$$\sigma(m) = \sigma(2^n \cdot p)$$

Poiché MCD $(2^n; p) = 1$, la funzione $\sigma(2^n \cdot p)$ è moltiplicativa, quindi

$$1) \qquad \sigma(m) = \sigma(2^n \cdot p) = \sigma(2^n) \cdot \sigma(p)$$

Ora m è un numero perfetto per ipotesi quindi $\sigma(m) = 2m$, ma $m = 2^n \cdot p$ perciò

$\sigma(m) = 2^{n+1} \cdot p$; $\sigma(2^n) = \frac{2^{n+1}-1}{2-1} = 2^{n+1} - 1$, sostituendo 1) si ha :

$$2^{n+1} \cdot p = (2^{n+1} - 1) \cdot \sigma(p)$$

Dividendo ambo i termini dell'uguaglianza per $2^{n+1} \cdot \sigma(p)$ e semplificando, otteniamo la seguente uguaglianza fra frazioni:

$$\frac{p}{\sigma(p)} = \frac{(2^{n+1} - 1)}{2^{n+1}}$$

Per la proprietà invariantiva delle frazioni esiste una costante $c \in N$ tale che

$$p = (2^{n+1} - 1) \cdot c \quad \text{e} \quad \sigma(p) = 2^{n+1} \cdot c$$

Se *c* fosse diverso da 1, il numero *p* oltre che 1 e sé stesso *p* avrebbe come divisore anche *c*; e, pertanto $\sigma(p) = 1 + p + c = 1 + (2^{n+1} - 1) \cdot c + c = 2^{n+1} \cdot c + 1 > \sigma(p)$: cioè $\sigma(p) > \sigma(p)$

manifestamente falso, pertanto $c = 1$ e $p=(2^{n+1} - 1)$ è un numero primo ed $m = 2^n \cdot (2^{n+1} - 1)$.

Cvd

Congetture

Generalità

Nella ricerca matematica spesso lo studioso si imbatte in situazioni comportamentali da parte degli oggetti che tratta in quanto sembra che essi manifestano proprietà comuni che si ripetono, costringendo il suo pensiero a formulare regole generali; tuttavia, essendo il numero degli oggetti trattati infinito e illimitato, lo studioso non sa se tale proprietà è vera o falsa.

La formulazione della regola generale costituisce per lo studioso una *congettura* finché egli non è in grado di dimostrare la verità o la falsità di tale proprietà. Per la falsificazione basta costruire o trovare un controesempio in cui non vale la proprietà all'interno degli oggetti di studio; per la dimostrazione è necessario costruire un ragionamento deduttivo mediante le regole di inferenza logica di cui la proprietà diventa la tesi: infatti secondo Popper non bastano mille e più prove contingenti a rendere vera una proprietà.

Oggi l'utilizzo dei calcolatori permette di ampliare a dismisura, entro i limiti della memoria del calcolatore, il numero delle prove in cui si verifica la proprietà nella speranza di trovare delle prove che contraddicono la proprietà. Il lavoro del calcolatore si limita sempre ha corroborare la congettura ma non costituisce una vera dimostrazione.

Le congetture, che andremo ad esporre , costituiscono un buon allenamento a pensare ai problemi matematici ancora aperti e di cui si cerca la soluzione razionale-dimostrativa.

Vediamo di illustrare quanto detto con due esempi (dal testo E. Gallo LA MATEMATICA Editore S.E.I)

" Supponiamo di aver calcolato, in una ricerca sui numeri naturali, i seguenti prodotti:

$$1 \cdot 3 = 3 \ ; \ \ 2 \cdot 4 = 8 \ ; \ \ 3 \cdot 5 = 15 \ ; \ \ 4 \cdot 6 = 24$$

Osservandoli, si trova che a primo membro sono indicati i prodotti di due naturali ottenuti aggiungendo e sottraendo 1 rispettivamente a 2, 3, 4, 5 e che i numeri scritti a secondo membro sono tutti quadrati diminuiti di 1, poiché :

$$3 = 4 - 1 = 2^2 - 1 = (2-1)(2+1) \quad ; \quad 8 = 9 - 1 = 3^2 - 1 = \ (3-1)(3+1) \ ;$$

$$15 = 16 - 1 = 4^2 - 1 = (4-1)(4+1) \quad ; \quad 24 = 25 - 1 = 5^2 - 1 = (5-1)(5+1)$$

Possiamo quindi formulare la seguente proprietà: *moltiplicando tra loro il precedente ed il successivo di un numero naturale qualunque, si ottiene il quadrato di tale numero diminuito di 1* cioè in formula:

$$(n-1)(n+1) = n^2 - 1$$

Questa è una congettura "

Tale congettura è possibile dimostrarla applicando il V postulato di Peano

La proprietà è vera per $n_0 = 2$; supponiamo che sia vera per n , se la proposizione è vera per n+1 allora è vera per qualunque valore di n $\in N - \{0 , 1\}$.

Verifichiamo che è vera per n+1; $[(n + 1) – 1] [(n + 1) + 1] = (n + 1)^2 - 1]$

Operando all'interno delle parentesi quadre si ha: $[n + 1 – 1][n + 1 + 1] = n^2 + 2n + 1 – 1$

Poiché $1 – 1 = 0$ e $1+1 = 2$, sostituendo si ha: $n(n+2) = n^2 + 2n$; applicando la proprietà distributiva del prodotto rispetto alla somma nel primo membro otteniamo un'identità:

$$n^2 + 2n = n^2 + 2n$$

verificata per qualunque valore di n.

Pertanto la congettura essendo stata dimostrata sempre vera costituisce un teorema dell'aritmetica; anzi costituisce un caso particolare di un teorema più generale nei numeri razionali assoluti che afferma:

moltiplicando tra loro due numeri razionali assoluti qualunque, si ottiene la differenza tra il quadrato della semisomma diminuito del quadrato della semidifferenza dei due numeri

Siano p_1 , $p_2 \in Q_0$. Il Teorema formalmente afferma:

a) $p_1 \cdot p_2 = [(p_1 + p_2) : 2]^2 - [(p_2 - p_1) : 2]^2$ (con $p_2 > p_1$)

NB. Se p_1 , $p_2 \in N_0$ e p_2 è il successivo di p_1 , si ha la proprietà iniziale relativa alla congettura, dimostrata vera con argomentazioni interne alla struttura dei numeri naturali.

Vogliamo ora stendere un programma in Turbo Pascal col quale possiamo effettuare numerosi esempi numerici che verificano il teorema generale nel caso di due numeri naturali qualsiasi:

```
program congettura1;
uses crt;
var a,b,d,m,n:integer;
    risp:char;
begin
  clrscr;
  writeln('         Congettura ( Teorema )');
  writeln('Il prodotto di due numeri naturali entrambi pari o entrambi dispari è uguale');
  writeln('alla differenza dei quadrati della loro semisomma e della loro semidifferenza ');
  writeln('              a*b = [(a+b):2]2-[(b-a):2]2 ( con b>a) ');
  writeln;
  repeat
     write('Immetti il primo numero naturale: a = '); readln(a);
      if a mod 2 = 0 then
           repeat
             write('Immetti un numero pari b > ',a,': b = ');
```

```
                readln(b)
              until b mod 2 = 0
               else
                    repeat
                      write('Immetti un numero dispari b > ',a,' b = ');
                      readln(b)
                    until b mod 2 <>0;
      m:=(b+a) div 2;
      d:=(b-a) div 2;
      writeln;
      writeln( a,' * ',b,' = ',sqr(m) - sqr(d),' = ',sqr(m),' - ',sqr(d),' = ',m,'2 - ',d,'2 = ‘)
      writeln(‘ = [(',a,'+',b,'):2]2 - [(',b,'-',a,'):2]2 ‘);
      readln;
      write('Vuoi continuare con un altra coppia di numeri naturali ? (S/N) ');
      readln(risp);
  until (risp='n') or ( risp = 'N');
end.
```

“ Supponiamo ora di aver osservato in un’altra situazione di ricerca che

$$6 \cdot 1 - 1 = 5 \quad ; \quad 6 \cdot 2 - 1 = 11 \quad ; \quad 6 \cdot 3 - 1 = 17 \quad ; \quad 6 \cdot 4 - 1 = 23$$

Siamo indotti a *formulare la congettura* che

Sottraendo 1 ad un multiplo di 6, si ottiene un numero primo

Infatti 5, 11, 17, 23 sono tutti numeri primi.

Ma se seguiamo a proseguire otteniamo:

$$6 \cdot 5 - 1 = 29 \quad ; \quad 6 \cdot 6 - 1 = 35$$

Come appare manifesto 29 è ancora un numero primo, ma 35 non è un numero primo. L’ultima relazione rende falsa la congettura, pertanto essa è da rifiutare. Questa relazione fornisce un controesempio che fa cadere la congettura fatta.”

Congetture classiche

La matematica è stata ed è luogo, di molte celebri congetture che hanno resistito spesso molti anni prima di essere contraddette oppure dimostrate : quali per esempio *il problema dei quattro colori* proposto nel 1852 da Francis Guthrie e dimostrato nel 1976; così pure il *Teorema di Fermat* $x^n + y^n = z^n$ formulato nel XVII secolo e dimostrato negli ultimi anni del XX secolo.

Congettura di Leibnitz :

Sul secondo esempio riportato Leibnitz formulò una congettura non ancora dimostrata:*Tutti i numeri primi maggiori od uguale a 5 sono o della forma* $6k - 1$ *o della forma* $6k + 1$

La proposizione possiamo formularla in forma implicativa:

Se un numero maggiore od uguale a 5 è primo, allora esso è o della forma $6k - 1$ o della forma $6k + 1$ con k ∈ N_0

Di questa congettura vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche.

```
program Congettura_di_Leibnitz;
uses crt;
var j,a,b,y,h,k,m,xmin,xmax:longint;
   risp:char;
procedure numeroprimo(x:longint);
  var i:longint;
  begin
      i:=1;
     repeat
        i:=i+1
     until x mod i = 0;
     if (i=x) and (x>=xmin) and (x<=xmax) then
              begin
                 write(x:10);
                  y:=1
              end
               else y:=0;
  end;
begin
  repeat
   textbackground(1);
   clrscr;
   textcolor(15);
   writeln;
   writeln('                          CONGETTURA DI LEIBNIZ ');
   writeln('"Tutti i numeri primi ( >=6 ) sono della forma 6*k+1 o della forma 6*k-1" ');
   writeln;
   writeln('Questo programma determina i numeri primi in un intervallo dato e la loro');
   writeln('quantit…, inoltre distingue quelli dalla forma 6*k+1 da quelli della forma');
   writeln('6*k-1 ');
   writeln;
   textcolor(12);
   write('Immetti l" estremo inferiore (>=6) dell"intervallo: inf = ');readln(xmin);
   write('Immetti l"estremo superiore dell"intervallo : sup = ');readln(xmax);
   textcolor(10);
   writeln;
   k:=0;h:=0;
   for j:=xmin div 6 to xmax div 6  do
```

```
    begin
      a:= 6*j-1;
      b:=6*j+1;
      numeroprimo(a); k:=k+y;
      numeroprimo(b); h:=h+y;
    end;
    writeln;
    m:=k+h;
    writeln('Il numero dei numeri primi nell''intervallo [',xmin,' ; ',xmax,'] dell''insieme N Š ',m);
    writeln;
    textcolor(13);
    writeln('Quelli della forma 6*k-1 sono ',k,' elementi e precisamente : ');
    writeln;
    for j:=xmin div 6 to xmax div 6  do
       begin
         a:= 6*j-1;
         numeroprimo(a);
       end;
    writeln;  writeln;
    writeln('Quelli della forma 6*k+1 sono ',h,' elementi e precisamente : ');
    writeln;
    for j:=xmin div 6 to xmax div 6  do
       begin
         b:=6*j+1;
         numeroprimo(b);
       end;
    textcolor(14);
    writeln;writeln;
    write('Vuoi continuare con altro intervallo ? (S/N) : ');
    readln(risp);
  until (risp='n') or ( risp='N');
end.
```

Congettura di Nicomaco

Premessa:

Def. Si chiama numero triangolare quel numero naturale esprimibile nella forma

$$n = \frac{m(m+1)}{2}$$

dove m è un qualsiasi numero naturale diverso da 0.

Nella rappresentazione figurata di Pitagora sono numeri triangolari:

1 · ; 3 · · ; 6 · · · ; 10 · · · · ; ecc.
. . . .
. . .
. .
.

Dalla definizione per

m = 1 → n = 1
m = 2 → n = 3
m = 3 → n = 6
m = 4 → n = 10
m = 5 → n = 15
……

Sia n un numero naturale e sia t l'n-simo numero triangolare, sia $\mathcal{U}$(t) la successione naturale dei numeri dispari costituita da t termini.
Il cubo di n è dato dalla somma degli ultimi n termini della successione $\mathcal{U}$(t) *dei numeri dispari.*

Es. Sia n = 8 , l'ottavo numero triangolare è $t = \frac{8\cdot(8+1)}{2} = 36$. La successione $\mathcal{U}$(36) è costituita da:

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71.

Il cubo di 8 ($8^3 = 512$) è dato dalla somma degli ultimo 8 termini di $\mathcal{U}$(36): cioè

57 + 59 + 61 + 63 + 65 + 67 + 69 + 71 = 512

Tale congettura proposta da Nicomaco di Gerasa, matematico e filosofo neopitagorico, tra il I e il II secolo d.C è ancora oggi oggetto di studio : fino ad oggi non sono emersi controesempi capaci di negare tale congettura.

Di questa congettura vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche.

```
program nicomaco;
uses crt;
var k,n,nt,cubo,som:word;
    disp:longint;
    risp:char;
begin
 repeat
 clrscr;
 textcolor(2);
 gotoxy(20,2);writeln('CONGETTURA DI NICOMACO' );
 textcolor(15);
```

```
 gotoxy(4,3); writeln('Sia n un numero naturale e sia t l''n-simo numero triangolare ');
 gotoxy(4,4);writeln('Sia data D(t) la successione naturale dei numeri dispari costituita');
 gotoxy(4,5);writeln('da t termini')
textcolor(2);
gotoxy(3,6);
writeln('Il cubo di n è dato dalla somma degli ultimi n termini della successione ');
 gotoxy(3,7);writeln('D(t) dei numeri dispari'); writeln;textcolor(15);
 write(' Introduci n (con n<=20 per vedere l''esposizione a monitor )  ');
 readln(n);
 writeln;
 nt:=n*(n+1) div 2; (* triangolare di n *)
 writeln('il ',n,'° numero triangolare e'' = ',nt);writeln;
 (* calcolo i primi nt numeri dispari *)
 writeln('i primi ',nt,' numeri dispari sono:');
 for k:=0 to nt-1 do
  begin
    disp:=(k)*2+1;
    write(disp:4)
  end;
 writeln; writeln;
 writeln('Il cubo di ',n,' e''la somma degli ultimi ',n,' numeri dispari:');
 cubo:=0;
 for k:=nt-n to nt-2 do
  begin
    disp:=k*2+1;
    write(disp,' + ');
    cubo:=cubo+disp
  end;
  write(disp+2,' = ',cubo+disp+2);
 writeln;
 writeln;
 writeln(n,'^3 = ',cubo+disp+2);
 readln;
 write('Vuoi continuare con altro numero n ? (S/N) ');
 readln(risp);
 until (risp='n') or (risp='N');
end.
```

Congettura di Gauss

Gauss nel suo Disquisitiones Aritmeticae aveva proposto la seguente congettura , ben presto dimostrata col Principio di induzione matematica,

La somma dei cubi dei primi n numeri naturali è uguale al quadrato della somma degli stessi n numeri naturali.

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = (1 + 2 + 3 + 4 + \cdots + n)^2$$

Es. Per n = 5 si ha: $1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 225$

$(1 + 2 + 3 + 4 + 5)^2 = 15^2 = 225$

Pertanto $1^3 + 2^3 + 3^3 + 4^3 + 5^3 = (1 + 2 + 3 + 4 + 5)^2$

La dimostrazione viene effettuata applicando il Principio di induzione matematica: V postulato di Peano e la somma di n termini di una progressione aritmetica:
La proprietà o congettura è vera per n = 1: infatti $1^3 = 1 = 1^2$
Supponiamo la proprietà o congettura vera per n :

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = (1 + 2 + 3 + 4 + \cdots + n)^2$$

Se la proprietà o congettura è vera per n+1 allora la congettura è vera per qualunque n $\in N_0$:
Verifichiamo che è vera per n+1:

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 + (n+1)^3 = [(1 + 2 + 3 + 4 + \cdots + n) + (n + 1)]^2$$

$(1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^3 =$

$$= (1 + 2 + 3 + 4 + \cdots + n)^2 + 2(n + 1)(1 + 2 + 3 + 4 + \cdots + n) + (n + 1)^2 =$$

$$= (1 + 2 + 3 + 4 + \cdots + n)^2 + 2(n + 1)\frac{(1+n)n}{2} + (n + 1)^2$$

$(1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^3 = (1 + 2 + 3 + 4 + \cdots + n)^2 + n(n + 1)^2 + (n + 1)^2$

$(1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^3 = (1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^2 (n + 1)$

$(1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^3 = (1 + 2 + 3 + 4 + \cdots + n)^2 + (n + 1)^3$

Operando , abbiamo ottenuto un'identità; pertanto la proprietà vale $\forall n \in N_0$
Di questa proprietà o teorema vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche entro la memoria del calcolatore.

```
program somma_di_cubi;
uses crt;
var n,s1,s2,i:longint;
begin
  clrscr;
  writeln('Questo programma ti permette di verificare che la somma dei cubi');
  writeln('dei primi n numeri interi è uguale al quadrato della somma degli ');
  writeln('stessi n numeri interi :');
  write('Immetti il valore N = ');readln(n);
  s1:=0; s2:=0;
  for i:=1 to n do
        begin
         s1:=s1+i*i*i;
         write(i*i*i);
         if i<n then write(' + ');
        end;
        write(' = ',s1);
        writeln;
```

```
  for i:=1 to n do
        begin
          s2:=s2+i;
          write(i);
          if i<n then write(' + ');
        end;
        write(' = ',s2);
  writeln;
  writeln;
  write(s1,'  =  ',s2,'^2');
  readln;
end.
```

Congetture di Goldbach

Nel 1742 il matematico tedesco C. Goldbach propose queste due congetture di cui la seconda è stata dimostrata recentemente:

- *Ogni numero pari* ≥ 6 *è la somma di due numeri primi dispari*
- *Ogni numero dispari* ≥ 9 *è la somma di tre numeri primi dispari.*

Es. Consideriamo il numero naturale pari n = 12. Esso è possibile scriverlo come somma di due numeri primi: 5 e 7 : 12 = 5 + 7; così pure n = 54 : infatti 54 = 7 + 47 oppure 54 = 23+31; ecc..
Consideriamo il numero naturale dispari n = 27. Esso non è possibile scriverlo come somma di due numeri primi (provare !!!), ma è possibile scriverlo come somma di tre numeri primi: 27 = 3 + 11 + 13 ; così pure n = 65: infatti 65 = 5 + 13 + 47 oppure 65 = 13 + 23 + 29; ecc.
NB. La scrittura non è unica: cioè le somme possono essere costituite da addenti diversi purché primi

Di queste proprietà vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche entro la memoria del calcolatore.

```
program Prima_congettura_di_Golbach;
uses crt;
var n:integer;
    risp:char;
procedure immetti;
begin
  repeat
   write('Immetti n: ');
   readln(n);
  until n mod 2 = 0;
end;
```

```
function primo(a:integer):boolean;
var i,n:integer;
begin
  n:=0;
  for i:=2 to a-1 do if a mod i = 0 then inc(n);
  if n>0 then primo:=false else primo:=true;
end;
procedure trovanp(n:integer);
var i1,i2:integer;
begin
  for i1:=3 to n do
  for i2:=i1+1 to n do
   if (primo(i1) and primo(i2))  and (i1+i2=n) then
       writeln(n,' = ',i1,' + ',i2);
end;
begin
  repeat
  clrscr;
  writeln('*** Prima Congettura di Golbach *** ');
  writeln;
  repeat
  writeln('Ogni numero intero pari >= 6 può essere scritto come somma di due numeri’);
writeln(‘ primi dispari');
  immetti;
  until n>4;
  writeln;
  trovanp(n);
  readln;
  write('Vuoi ripetere con altro valore di n ? (S/N): ');
  readln(risp);
  until (risp='n') or (risp='N');
end.
```

```
program Seconda_Congettura_di_Golbach;
uses crt;
var n:integer;
    risp:char;
procedure immetti;
begin
   repeat
    write('Immetti n: ');
    readln(n);
   until n mod 2 <> 0;
```

```
end;
function primo(a:integer):boolean;
var i,n:integer;
begin
  n:=0;
  for i:=2 to a-1 do if a mod i = 0 then inc(n);
  if n>0 then primo:=false else primo:=true;
end;
procedure trovanp(n:integer);
var i1,i2,i3:integer;
begin
  for i1:=3 to n do
  for i2:=i1+1 to n do
  for i3:=i2+1 to n do if (primo(i1) and primo(i2)) and (primo(i3)) and (i1+i2+i3=n) then
      writeln(n,' = ',i1,' + ',i2,' + ',i3);
end;
begin
  repeat
  clrscr;
  writeln('*** Seconda Congettura di Golbach *** ');
  writeln;
  repeat
  write('Ogni numero intero dispari ≥ 9 può essere scritto come somma di tre numeri primi ‘);
  writeln(‘ ( 1 compreso )’);
  immetti;
  until n>7;
  writeln;
  trovanp(n);
  readln;
  write('Vuoi ripetere con altro valore di n ? (S/N): ');
  readln(risp);
  until (risp='n') or (risp='N');
end.
```

Congettura di Lagrange

Sulla scia di Goldbach si colloca Lagrange che formula la sua congettura:

Ogni numero naturale è possibile scriverlo come somma di quattro quadrati di numeri naturali di cui due diversi da zero

Di queste proprietà vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche entro la memoria del calcolatore.

```
program lagrange;
uses crt;
var n:word;
procedure immetti;
begin
 write('Immetti n: ');
 readln(n);
end;
procedure calcola(n:longint);
var i1,i2,i3,i4,max,nn:longint;
begin
  max:=round(sqrt(n));
  for i1:= 0 to max do
  for i2:=i1 to max do
  for i3:=i2 to max do
  for i4:=i3 to max do
                    if n=sqr(i1)+sqr(i2)+sqr(i3)+sqr(i4) then
                    begin
                      nn:=0;
                      if i1=0 then inc(nn);
                      if i2=0 then inc(nn);
                      if i3=0 then inc(nn);
                      if i4=0 then inc(nn);
                      if nn<=2 then
                      begin
                       writeln;
                       write(n,' = ',i1,'^2 + ',i2,'^2 + ',i3,'^2 + ',i4,'^2');
                      end;
                    end;

end;
begin
  clrscr;
  writeln('*** Teorema di Lagrange *** ');
  writeln;
  writeln('Ogni numero intero si può scrivere come');
  writeln('somma di 4 quadrati di cui almeno due diversi da zero');
  writeln;
  immetti;
  calcola(n);
  readln;
end.
```

Congettura di Girard

Tale congettura è stata proposta da A.Girard nel 1580 e dimostrata da Fermat ; essa afferma

Se n è un numero primo allora esso è possibile scriverlo come differenza dei quadrati di due numeri naturali; se inoltre è della forma 4k+1 allora è possibile scriverlo come somma dei quadrati di due numeri naturali.

Es. Sia dato il numero primo n = 29 , esso è possibile scriverlo come differenza dei quadrati di 15 e 14: $29 = 225 – 196 = 15^2 – 14^2$. Inoltre essendo della forma 4k+1: cioè 4*7 + 1, esso è possibile scriverlo come somma dei quadrati di 5 e 2 : $29 = 25 + 4 = 5^2 + 2^2$.
Sia dato il numero primo n = 43, esso è possibile scriverlo come differenza dei quadrati di 22 e 21 : $43 = 484 – 441 = 22^2 – 21^2$; non essendo della forma 4k+1 non è possibile scriverlo come somma di due quadrati

Di queste proprietà vogliamo qui proporre un programma in Turbo Pascal che permette di effettuare numerose verifiche entro la memoria del calcolatore.

```
program congettura_di_Girard;
uses crt;
var n,a,b,c,k,j,i,h,jj,ii:integer;
    risp:char;
function primo(x:integer):integer;
var i,k: integer;
begin
  k:=0;
  for i:=1 to x div 2 do
    if x mod i = 0 then k:=i;
    if k=1 then primo:=x;
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('          CONGETTURA DI GIRARD ( dimostrata da Fermat )  ');
  writeln(' Questo programma ti permette di determinare se un numero immesso da tastiera');
  writeln(' è un numero primo; nel caso che il numero fosse primo , esso te lo esprime');
  writeln(' come differenza di due  quadrati; se poi il numero fosse sempre primo ma  ');
  writeln(' della forma 4*k + 1, allora esso è possibile scriverlo come somma di due ');
  writeln(' quadrati.');writeln;
  textcolor(12);
```

```
write('Immetti un numero intero positivo n = ');readln(n);
writeln;
textcolor(10);
if n=primo(n) then
   begin
     write(n,' è primo:   ');
     a:= n div 2;
     b:= a+1;
     write( n,' = ',b,'^2 - ',a,'^2  = ',b*b,' - ',a*a);
   end
   else write(n,' non è un numero primo ');
c:=(n-1) div 4 ;
h:=0;
writeln;
writeln;
if n=primo(n) then
  for k:=1 to c do
    if (n mod (4*k+1)) = 0 then
      for j:=1 to n div 2 do
        for i:=1 to j do
          if n = j*j+i*i then
              begin
                h:=h+1;
                jj:=j;
                ii:=i;
              end;
if h<>0 then
   begin
    writeln('Inoltre ',n,' è un numero primo della forma 4*k + 1, quindi è possibile ');
    writeln('scriverlo come somma di due quadrati: ');
    writeln;
    write('      ',n,' = ',jj,'^2 + ',ii,'^2 = ',jj*jj,' + ',ii*ii);
    writeln;
   end
   else
    if n=primo(n) then
      begin
        writeln(n,' è un numero della forma 4*k - 1, quindi non è possibile scriverlo');
        writeln('come somma di due quadrati ');
      end;
writeln;
textcolor(14);
write('Vuoi continuare con altri numeri ? ( S/N ) : ');
readln(risp);
```

```
 until (risp='N') or ( risp = 'n');
end.
```

Relazione Sezione aurea

Tale relazione, pur esulando dall'ambito artmetico, è strettamente connessa ai numeri naturali; essa stabilisce che
Il valore della sezione aurea *di un segmento, preso come unità di misura, è determinato dalla parte decimale dell'n-sima frazione della successione determinata ricorsivamente dalla seguente legge:*

$$\begin{cases} F(n) = \frac{b}{a} \\ F(n+1) = \frac{b+a}{a} \end{cases} \qquad \text{con } a \text{ e } b \in N_0$$

Per n tendente all'infinito.
NB. Per *n* finito si ha una approssimazione del valore della Sezione aurea.

Vogliamo qui proporre un programma in Turbo Pascal che permette di calcolare il valore della sezione aurea di un segmento unitario , fornendo lo scostamento dal valore dato dalla formula, già presente negli *Elementi* di Euclide, entro la memoria del calcolatore.

```
{$N+}
program congettura_Sezione_aurea;
uses crt;
var num,den,x,a,c,d,x1,err,errpercent:double;
    i,n:integer;
    risp:char;
begin
  repeat
  clrscr;
  writeln('Questo programma ti permette di verificare la congettura che la');
  writeln('Sezione aurea di un segmento preso come unità di misura è deter-');
  writeln('minata dalla parte decimale delle frazioni della successione ');
  writeln('costruita dalla F(n)=b/a ed F(n+1)=(b+a)/b con a,b due numeri ');
  writeln('naturali, quando n tende all"infinito');
  readln;
  clrscr;
  write('Immetti un numero intero per numeratore : ');readln(num);
  write('Immetti un numero intero per denominatore : ');readln(den);
  write('Immetti la posizione della frazione della successione n = ');
  readln(n);
  writeln;writeln;
```

```
  textcolor(2);
  for i:=1 to n do
    begin
      a:=den;
      x:=num/a;
      write(trunc(num),'/',trunc(den),'    ');
      c:=num; d:=den;
      den:=num;
      num:=num+a;
     end;
  writeln;writeln;
  textcolor(12);
  writeln('Il valor determinato dalla frazione della successione è: ');
  writeln(trunc(c),'/',trunc(d),' - 1 = ',frac(x):5:15);
  writeln;
  textcolor(14);
  writeln('Il valore determinato dal calcolo (sqrt(5)-1)/2 = ',(sqrt(5)-1)/2:5:15);
  err:= frac(x)-(sqrt(5)-1)/2 ;
  writeln('Lo scostamento dal valor standard è : ',err:1:15 );
  errpercent:=err/((sqrt(5)-1)/2 )*100;
  writeln('L"errore percentuale è : ',errpercent:5:15);
  readln;
  write('Vuoi ripetere con altre frazioni ? (S/N) ');
  readln(risp);
  until (risp='n') or (risp='N');
end.
```

Congettura sui numeri amicabili:

Def. Due numeri si dicono amici se ognuno è la somma dei divisori dell'altro escluso l'altro ed incluso 1 .

Es. a) I numeri 220 e 284 sono amici: infatti
I divisori di 284 sono: 1, 2, 4, 71, 142 , la cui somma è 220
I divisori di 220 sono: 1, 2, 4, 5, 10,11, 20, 22, 44, 55, 110, la cui somma è 284

b) I numeri 1184 e 1210 sono amici: infatti
I divisori di 1184 sono: 1, 2, 4, 8, 32, 37, 74, 148, 296, 592, la cui somma è 1210
I divisori di 1210 sono: 1, 2, 5, 10,11, 22, 55, 110, 121, 242, 605 la cui somma è 1184.

Congettura. *Due numeri naturali a e b sono amici se* $\sigma(a) = \sigma(b) = a + b$.

Verifichiamo :

$\sigma(220) = 504$, $\sigma(284) = 504$; 220 + 284 = 504

Quindi $\sigma(220) = \sigma(284) = 220 + 284$

$\sigma(1184) = 2394$, $\sigma(1210) = 2394$; 1184 + 1210 = 2394

Quindi $\sigma(1184) = \sigma(1210) = 1184 + 1210$

Vogliamo proporre un programma che calcola i numeri amicabili in Turbo Pascal.

```
program numeri_amicabili;
uses crt;
var a,b,k,k1,k2,j,s,s1,t,w,a1,b1:integer;
   m,m1,m2:array[1..100] of integer;
   risp:char;
procedure numero(v:integer);
var n,r:integer;
begin
 k:=0 ;
 for n:=v downto 1 do
      begin
        r:= v mod n;
        if r = 0 then
          begin k:=k+1; m[k]:= v div n; end;
      end;
end;
begin
 repeat
 clrscr;
 writeln('Questo programma ti permette di trovare in un intervallo di valori');
 writeln('eventuali coppie di numeri amicabili: cioè numeri la cui somma dei');
 writeln('loro divisori escluso se stessi ed incluso 1 sia uguale all''altro');
 writeln('numero: sono coppie di numeri amici (220 ; 284), (1184 ; 1210),');
 writeln('(2620 ; 2924) , (5020 ; 5564), (6232 ; 6368) ');
 textcolor(12);
 writeln('Introduci l''intervallo nel quale vuoi trovale due numeri amici:');
 readln(t,w);
 for a:=t to w do
 for b:=t to a do
 begin
 numero(a);
 s:=0;
 for j:=1 to k-1 do
   begin
    m1[j]:= m[j];
    s:=s+m1[j];
   end;
 s1:=0;
```

```
numero(b);
k2:=k;
 for j:=1 to k-1 do
   begin
     m2[j]:= m[j];
     s1:=s1+m2[j];
   end;
if (s=b) and (s1=a) and (s<>s1) then
      begin
      textcolor(10);
      writeln(a,' e ',b,' sono due numeri amicabili ');
      readln;textcolor(11);
      writeln('Verifichiamo che la somma dei divisori di ',a,' sia uguale a ',b,' e viceversa');
      writeln;
      writeln('la somma dei divisori di ',a,' è : ');
      numero(a);
      for j:=1 to k-1 do write(m1[j],'+'); writeln(' = ',b);
      writeln;
       writeln('la somma dei divisori di ',b,' è : ');
      numero(b);
      for j:=1 to k-1 do write(m2[j],'+'); writeln(' = ',a);
      end;
end;
writeln;textcolor(14);
writeln('Vuoi ripetere con altro intervallo ? (S/N) ');
readln(risp);
until (risp='n') or (risp='N');
end.
```

Congettura sui numeri primi di Sophie Germain

Def. Un numero primo p si dice di S.Germain se il numero 2p + 1 è un numero primo.

Es. I numeri primi 2 , 3 , 5 … sono numeri primi di S. Germain: infatti i numeri 5, 7, 11, … derivati da essi mediante la formula 2p + 1 sono numeri primi.

Nella ricerca di questo tipo di numeri primi ci si imbatte in un problema che tali valori per intervalli ad esempio di 1000 in 1000 al crescere dei valori inziali e finali di tali intervalli la quantità di tali numeri primi va significativamente diminuendo, questo potrebbe indurci ad affermare che la totalità di tali numeri è costituita da un numero , per quanto grande possa essere, è finto.
La *congettura*, espressa da S. Germain, afferma il contrario: cioè la totalità di tali numeri è infinita. Tale congettura a tutt'oggi non è stata dimostrata e costituisce un problema aperto.

46

Il seguente programma permette di individuare, entro intervalli determinati, quali e quanti sono tali numeri primi.

```
Program numero_primo_di_S_Germain;
uses crt;
var k,i,j,t,n,inf,sup,w:longint;
    perc:real;
    m,s:array[1..3000] of longint;
    risp:char;
procedure primo(x:longint);
var i:integer;
begin
  k:=0;
  for i:=2 to x div 2 do
      if x mod i = 0 then k:=k+1;
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('  Questo programma individua in un intervallo di estremi [2 ; sup ]  ');
  writeln('  quali e quanti sono i numeri primi di Sophie Germain: cioŠ quei  ');
  writeln('  numeri primi p tale che 2p+1 sono a loro volta numeri primi');
  writeln('  Inoltre trova la percentuale di tali numeri rispetto alla totalit…');
  writeln('  dei numeri primi presenti in tale intervallo ');
  writeln;
  textcolor(11);
  write('  Immetti l''estremo superiore dell''intervallo: sup = ');
  readln(sup);
  writeln;
  textcolor(18);
  writeln('                  Attendere il calcolo ... !!');
  writeln;
  w:=0;
  for n:=2 to sup do
   begin
     primo(n);
     if k=0 then w:=w+1;
   end;
  j:=0;
  for n:=2 to sup do
   begin
```

```
    primo(n);
    if k=0 then
       begin
         j:=j+1;
         m[j]:=2*n+1;
         s[j]:=n;
       end;
  end;
 t:=0;
 textcolor(12);
 write('  ');
 for i:=1 to j-1 do
   begin
    primo(m[i]);
    if k=0 then
       begin
         t:=t+1;
         write(s[i],'  ;  ');
       end;
   end;
 writeln(s[j]);
 writeln;
 textcolor(18);
 writeln('                  FINE calcolo.');
 writeln;
 writeln;
 textcolor(14);
 writeln('  La totalità dei numeri di S.Germain nell''intervallo [',inf,' ; ',sup,']');
 writeln('  sono ',t);
 writeln('  La totalità dei numeri primi nell''intervallo [',inf,' ; ',sup,']');
 writeln('  sono ',w);
 perc:=t/w*100;
 writeln('  La percentuale di tali numeri rispetto alla totalità dei numeri primi');
 writeln('  presenti nell''intervallo è : ',perc:2:2,' % ');
 writeln;
 writeln;
 write('  Vuoi aumentare l''estremo superiore dell''intervallo ? (S/N) ');
 readln(risp);
until (risp='N') or (risp='n');
end.
```

CAPITOLO II
Funzione Gamma – Funzione Zeta

Funzione gaussiana y = e^{-x^2}

Prima di accingerci a definire e studiare la funzione Γ(x) di Eulero, vogliamo studiare, sviluppare in serie ed integrare la funzione gaussiana:

$$y = e^{-x^2}$$

strettamente connessa alla funzione Gamma.

Studio della funzione :

a) Tipo: funzione trascendente esponenziale in base $e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 2{,}718\ldots$
b) C.E ≡ R ; C.V. ≡ R^+
c) Intersezione assi:
   - Asse delle ascisse : $\begin{cases} y = 0 \\ y = e^{-x^2} \end{cases}$ impossibile
   - Asse delle ordinate: $\begin{cases} x = 0 \\ y = e^{-x^2} \end{cases} \rightarrow \begin{cases} x = 0 \\ y = 1 \end{cases}$

   La funzione $y = e^{-x^2}$ non presenta intersezione cpon l'asse delle ascisse, mentre interseca l'asse delle ordinate nel punto A (0 ; 1)

d) Simmetrie fondamentali: Poiché la funzione presenta la variabile indipendente x a grado pari, essa risulta una funzione pari: cioè simmetrica rispetto all'asse delle ordinate.
e) Segno:
   La funzione essendo una funzione esponenziale risulta sempre positiva: $\forall x \in C.E: \ y > 0$
f) Asintoti:
   - Verticali: la funzione non presentando punti di discontinuità non ha asintoti verticali
   - Orizzontali: $\lim_{x\to\pm\infty} e^{-x^2} = 0$, pertanto la retta y = 0 : cioè l'asse delle ascisse costituisce l'asintoto orizzontale della funzione.
g) Derivate:
   $y' = -2xe^{-x^2}$; $y'' = 2(2x^2-1)e^{-x^2}$
   - Crescenza e decrescenza: $y' \gtrless 0$
     y' > 0 per x < 0 : pertanto nell'intervallo aperto ($-\infty$; 0) la funzione è sempre crescente
     y' < 0 per x > 0 : pertanto nell'intervallo aperto (0 ; $+\infty$) la funzione è sempre decrescente
   - Massimi e minimi: $y' = 0$ per x = 0. Poiché la funzione presenta a sinistra del punto A (0 ; 1) un andamento crescente e a destra dello stesso punto decrescente, tale punto costituisce un punto di massimo per la funzione.

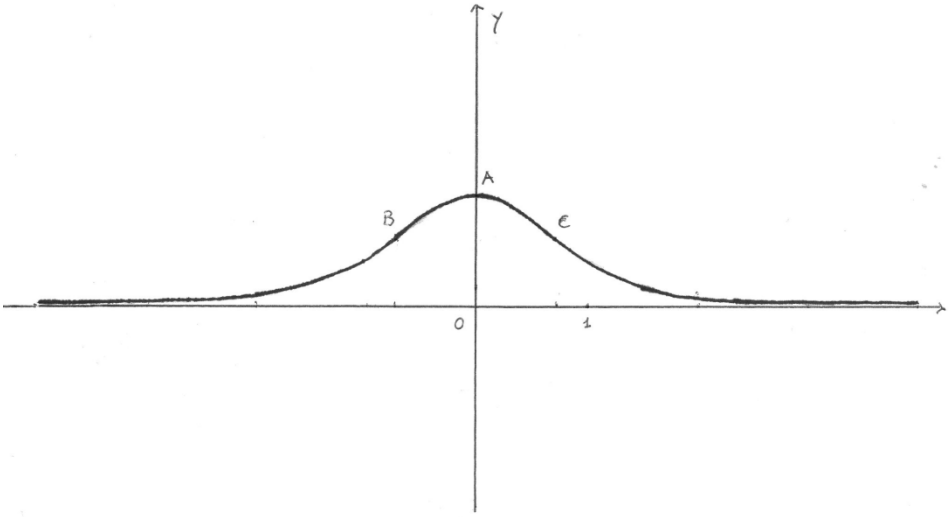
- Concavità: $y'' \gtrless 0$

  y'' > 0 per $x < -\frac{\sqrt{2}}{2}$ o $x > \frac{\sqrt{2}}{2}$: pertanto negli intervalli aperti $(-\infty\,;\,-\sqrt{2})$ e $(\sqrt{2}\,;\,+\infty)$ la funzione volge la concavità verso il semipiano delle ordinate positive.

  y'' > 0 per $-\frac{\sqrt{2}}{2} < x < \frac{\sqrt{2}}{2}$: pertanto nell'intervallo aperto $(-\sqrt{2}\,;\,\sqrt{2})$ la funzione volge la concavità verso il semipiano delle ordinate negative.

- Flessi : y'' = 0 per $x = \pm\frac{\sqrt{2}}{2}$. Poiché la funzione presenta a sinistra e a destra dei punti: B$\left(-\frac{\sqrt{2}}{2}\,;\,e^{-\frac{1}{2}}\right)$ e C $\left(\frac{\sqrt{2}}{2}\,;\,e^{-\frac{1}{2}}\right)$ diversa concavità, tali punti costituiscono i punti di flesso per la funzione

h) Grafico



Sviluppo in serie della funzione

Sviluppo in serie di Mac Laurin nel punto iniziale $x_o = 0$.

- Determiniamo i coefficienti dello sviluppo in serie:

  $y' = -2xe^{-x^2}$: $y'(0) = 0$

  $y'' = 2(2x^2 - 1)e^{-x^2}$: $y'' = -2$

  $y''' = 4x(3 - 2x^2)e^{-x^2}$: $y''' = 0$

  $y^{IV} = 4(4x^4 - 12x^2 + 3)e^{-x^2}$: $y^{IV} = 12$

  $y^{V} = 8x(-4x^5 + 20x^2 - 15)e^{-x^2}$: $y^{V} = 0$

  $y^{VI} = 8(8x^7 - 24x^5 - 40x^4 + 90x^2 - 15)e^{-x^2}$: $y^{VI} = -120$

  ……

- Sviluppo:

  $e^{-x^2} = 1 + \frac{x^2}{2!}(-2) + \frac{x^4}{4!}(12) + \frac{x^6}{6!}(-120) + \ldots$

  $e^{-x^2} = 1 - x^2 + \frac{x^4}{2} - \frac{x^6}{6} + \ldots$

Iterando il procedimento si ha lo sviluppo in serie della funzione:

$$e^{-x^2} = 1 - \frac{x^2}{1!} + \frac{x^4}{2!} - \frac{x^6}{3!} + \cdots + (-1)^n \frac{x^{2n}}{n!} + \ \ldots$$

Allo stesso risultato si poteva giungere considerando la funzione esponenziale y = e^t. Le cui derivate di qualunque ordine sono $y^{(n)} = e^t$, pertanto dovendo calcolare tali derivate nel punto $t_o = 0$ si ha che $\forall\, n \in N:\ y^{(n)} = 1$; per cui lo sviluppo in serie di

$$e^t = 1 + \frac{t}{1!}(1) + \frac{t^2}{2!}(1) + \frac{t^3}{3!}(1) + \cdots + \frac{t^{(n)}}{n!}(1) + \ \ldots.$$

Sostituendo ala variabile t la variabile $-x^2$, si ha:

$$e^{-x^2} = 1 - \frac{x^2}{1!} + \frac{x^4}{2!} - \frac{x^6}{3!} + \cdots + (-1)^n \frac{x^{2n}}{n!} + \ldots$$

Strategia molto meno laboriosa della precedente.

Integrale della funzione

Calcolo dell'integrale della funzione $y = e^{-x^2}$ in tutto il Campo di Esistenza $(-\infty\ ;\ +\infty)$: cioè

$$\mathcal{J} = \int_{-\infty}^{+\infty} e^{-x^2}\, dx$$

Dallo studio di funzioni sappiamo che la funzione suddetta è una funzione pari, pertanto

$$\mathcal{J} = 2\int_{0}^{+\infty} e^{-x^2}\, dx$$

Ci limitiamo al calcolo di **I = $\mathcal{J}/2$:**

$$I = \int_{0}^{+\infty} e^{-x^2}\, dx$$

Applicando i due teoremi sugli integrali:

Teorema: Funzioni limitate e monotone nell'intervallo (a ; b) sono integrabili

Def. Data una funzione $g(x)$ continua e limitata nell'intervallo (a ; $+\infty$) , si dice *integrabile in senso generalizzato* se esiste ed è finito il

$$\lim_{b\to+\infty} \int_{a}^{b} g(x)dx$$

Teorema. Sia $g(x)$ una funzione non negativa in (a ; +∞) ed ivi continua, limitata e integrabile in senso generalizzato, se per ogni x > a si verifica che $|f(x)| \leq g(x)$ (con f(x) funzione continua e limitata) , allora la funzione f(x) è integrabile in senso generalizzato in (a ; +∞).

Intanto la funzione $f(x) = e^{-x^2}$ nell'intervallo [0 ; +∞) è continua e limitata: infatti in tale intervallo non presenta punti di discontinuità di alcun tipo, il suo campo di variazione è tutto compreso tra 0 e 1. Se ora consideriamo la funzione $g(x) = \frac{1}{1+x^2}$, tale funzione nell'intervallo [0 ; +∞) risulta non negativa, continua e limitata; inoltre essa è la reciproca della funzione polinomiale $r(x) = 1 + x^2$, come $f(x) = e^{-x^2}$ è la reciproca di una funzione esponenziale
$h(x) = e^{x^2}$. Poiché $\forall x \in [0 ; +\infty)$ $h(x) \geq r(x)$, discende che $f(x) \leq g(x)$. Inoltre la funzione $g(x)$ è integrabile in senso generalizzato:

$$\lim_{b\to+\infty} \int_0^b \frac{1}{1+x^2}\, dx = \lim_{b\to+\infty} |\arctan(x)\,|_0^b = \frac{\pi}{2}$$

Quindi per il teorema precedente possiamo affermare che $f(x) = e^{-x^2}$ è integrabile in senso generalizzato nello stesso intervallo [0 ; +∞) : cioè esiste ed e finito

$$I = \int_0^{+\infty} e^{-x^2}\, dx$$

Tuttavia il calcolo di tale integrale non è elementarmente eseguibile: infatti tale integrazione sfrutta il metodo degli integrali multipli, in particolare quelli doppi.
Consideriamo l'integrale doppio:

$$\iint_D f(x;y)dxdy$$

dove $D \subseteq R^2$ è il dominio di integrazione. Vogliamo ora passare da un sistema cartesiano xOy ad un sistema sempre cartesiano uO'v dello stesso piano π , dove le variabili x e y sono legate a *u* e *v* dalle seguenti relazioni:

$$\begin{cases} x = \varphi(u\,;v) \\ y = \psi(u\,;v) \end{cases}$$

dove le funzioni $\varphi(u)$ e $\psi(v)$ le supponiamo continue assieme alle loro derivate parziali prime in un certo dominio **T**. Supponiamo pure che le relazioni scritte sopra stabiliscono una corrispondenza biunivoca tra i due domini **T e D** e che il determinante Jacobiano:

$$J = \begin{vmatrix} \frac{\partial\varphi}{\partial u} & \frac{\partial\varphi}{\partial v} \\ \frac{\partial\psi}{\partial u} & \frac{\partial\psi}{\partial v} \end{vmatrix}$$

sia sempre diverso da zero.
Sotto tali ipotesi vale la seguente formula di trasformazione dell'integrale doppio:

$$\iint_D f(x;y)dxdy = \iint_T f(\varphi(u\,;v);\psi(u\,;v))\,|J\,|dudv$$

cioè: *il cambiamento di variabili in un integrale doppio si esegue sostituendo nella funzione integranda alle variabili x , y le loro espressioni nelle nuove variabili u e v , moltiplicando quindi per il valore assoluto dello Jacobiano della sostituzione, ed estendendo il nuovo integrale al dominio T, corrispondente del dominio D, nel piano riferito al sistema uO'v.*

Nel caso particolare del passaggio dalle coordinate cartesiane x, y alle coordinate polari ρ , ϑ , avendosi:

$$\begin{cases} x = \rho cos\vartheta \\ y = \rho sen\vartheta \end{cases} ;$$

$$J = \begin{vmatrix} \frac{\partial\varphi}{\partial u} & \frac{\partial\varphi}{\partial v} \\ \frac{\partial\psi}{\partial u} & \frac{\partial\psi}{\partial v} \end{vmatrix} = \begin{vmatrix} cos\vartheta & -\rho sen\vartheta \\ sen\vartheta & \rho cos\vartheta \end{vmatrix} = \rho cos^2\vartheta + \rho sen^2\vartheta = \rho$$

La formula di trasformazione diviene

$$\iint_D f(x;y)dxdy = \iint_T f(\rho cos\vartheta;\ \rho sen\vartheta)\ \rho d\rho d\vartheta$$

Tornando al calcolo di

$$I = \int_0^{+\infty} e^{-x^2}\,dx$$

Dalla teoria dell'integrazione finita, noi sappiamo che la varabile di integrazione è una variabile muta: cioè qualunque sia la lettera che figura come variabile di integrazione, il valore dell'integrale non varia; pertanto possiamo identificare i due integrali:

$$\int_0^{+\infty} e^{-x^2}\,dx = \int_0^{+\infty} e^{-y^2}\,dy$$

sostituendo alla lettera x del primo integrale, la lettera y del secondo integrale. Se ora andiamo a moltiplicare i due integrali, otteniamo il quadrato del valore iniziale: I^2

$$I^2 = \int_0^{+\infty} e^{-x^2}\,dx \cdot \int_0^{+\infty} e^{-y^2}\,dy$$

Ora la funzione f(x ; y) = f(x) · f(y) nell'intervallo (0 ; +∞) , soddisfacendo le ipotesi del Teorema di Fubini, possiamo scrivere:

$$\int_0^{+\infty} e^{-x^2}\,dx \cdot \int_0^{+\infty} e^{-y^2}\,dy = \int_0^{+\infty}\int_0^{+\infty} e^{-x^2-y^2}dxdy$$

da cui

$$I^2 = \int_0^{+\infty}\int_0^{+\infty} e^{-x^2-y^2}dxdy$$

Ora siamo in presenza di un radicale doppio nelle variabili x, y con $D_x = [0 ; +\infty)$ e $D_y = [0 , +\infty)$

Vogliamo ora passare a coordinate polari ρ , ϑ con $T_\rho = [0 ; +\infty)$ e $T_\vartheta = [0 ; \frac{\pi}{2})$; applicando il cambio di variabili si ha:

$I^2 = \int_0^{+\infty}\int_0^{\frac{\pi}{2}} e^{-(\rho cos\vartheta)^2-(\rho sen\vartheta)^2}\rho d\vartheta d\rho = \int_0^{+\infty}\int_0^{\frac{\pi}{2}} e^{-\rho^2}\rho d\vartheta d\rho = \int_0^{+\infty}(\int_0^{\frac{\pi}{2}} d\vartheta)e^{-\rho^2}\rho d\rho =$

$\frac{\pi}{4}\int_0^{+\infty}(2\rho e^{-\rho^2})d\rho = \frac{\pi}{4}\left|e^{-\rho^2}\right|_0^{+\infty} = \frac{\pi}{4}$

$$I^2 = \frac{\pi}{4} \quad \rightarrow \quad I = \frac{\sqrt{\pi}}{2}$$

Quindi

$$\mathcal{I} = \int_{-\infty}^{+\infty} e^{-x^2}\,dx = \sqrt{\pi}$$

Se volessimo calcolare il valore approssimato di I in un intervallo limitato [a ; b], occorre applicare il metodo di integrazione per serie: infatti per questa funzione non negativa, ovunque definita e monotona la serie ad essa associata è convergente (per il criterio di convergenza delle serie a segno alterno di Leibniz) e quindi è possibile integrarla per serie.

Sia dato lo sviluppo in serie di Mac Laurin della funzione $f(x) = e^{-x^2}$:

$$e^{-x^2} = 1 - \frac{x^2}{1!} + \frac{x^4}{2!} - \frac{x^6}{3!} + \cdots + (-1)^n\frac{x^{2n}}{n!} + \ldots$$

Calcoliamo l'integrale nell'intervallo [0 ; b]

$$\int_0^b e^{-x^2}\,dx = \int_0^b \left(1 - \frac{x^2}{1!} + \frac{x^4}{2!} - \frac{x^6}{3!} + \cdots + (-1)^n\frac{x^{2n}}{n!} + \ldots\right)dx$$

$$= \left|x - \frac{x^3}{1!3} + \frac{x^5}{2!5} - \frac{x^7}{3!7} + \cdots + (-1)^n\frac{x^{2n+1}}{n!(2n+1)} + \ldots\right|_0^b =$$

$$= b - \frac{b^3}{1!3} + \frac{b^5}{2!5} - \frac{b^7}{3!7} + \cdots + (-1)^n\frac{b^{2n+1}}{n!(2n+1)} + \ldots$$

Bloccando la serie ad una opportuna (dipendente dalla approssimazione richiesta) potenza si ottiene il valore approssimato cercato dell'integrale.

NB Per b = 2 il valore dell'integrale a meno di 10^{-1} è necessario che l'ultimo addendo della serie sia

$$\frac{2^{19}}{9! \cdot 19}$$

man mano che cresce il valore della potenza di b dell'ultimo addendo della serie, la funzione gaussiana cresce, di qui la necessità della tabulazione della gaussiana: tale tabulazione è presente nei testi di statistica, dove la gaussiana ha un ruolo fondamentale nella funzione di ripartizione di una variabile statistica normalizzata.

Dopo questa ampia premessa, torniamo alla funzione Gamma di Eulero.

Funzione Gamma di Eulero

La funzione Γ (x) è una generalizzazione della funzione fattoriale : non a caso essa è chiamata come la funzione interpolatrice del funzione aritmetica f(n) = n!, detta semplicemente fattoriale di n $\in N$. Essa è definita per x > 0 nel modo seguente:

$$\Gamma(x) = \int_0^{+\infty} t^{x-1}\, e^{-t} dt$$

L'analogia con il fattoriale discende da queste relazioni, che costituiscono le regole di ricorsività sia della funzione gamma che del fattoriale:

$$\Gamma(1) = \int_0^{+\infty} e^{-t}\, dt = \lim_{b\to+\infty} \int_0^b e^{-t}\, dt = \lim_{b\to\infty} |-e^{-t}|_0^b = \lim_{b\to+\infty}(-e^{-b} + 1) = 1$$

$$\Gamma(x+1) = \int_0^{+\infty} t^x\, e^{-t} dt = \left[|t^x(-e^{-t})|_0^{+\infty} + x \cdot \int_0^{+\infty} t^{x-1}\, e^{-t} dt\right]_{\textit{integrando per parti}} =$$

$$= x \cdot \int_0^{+\infty} t^{x-1}\, e^{-t} dt = x \cdot \Gamma(x)$$

Di qui la formula ricorsiva:

$$\begin{cases} \Gamma(1) = 1 \\ \Gamma(x+1) = x \cdot \Gamma(x) \end{cases}$$

Analoga alla formula ricorsiva del fattoriale:

$$\begin{cases} 1! = 1 \\ (n+1)! = (n+1) \cdot n! \end{cases}$$

Se nella formula ricorsiva della funzione Gamma x coincide con il numero naturale, si hanno le seguenti uguaglianze:

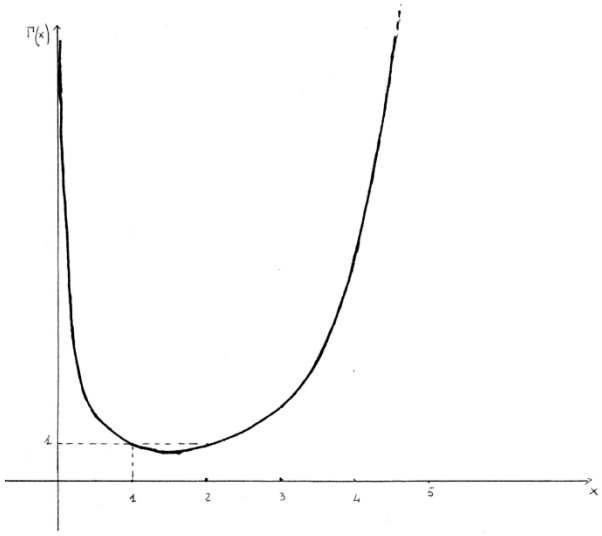
$$\Gamma(n+1) = n \cdot \Gamma(n) = n \cdot (n-1) \cdot \Gamma(n-1) = n \cdot (n-1) \cdot (n-2) \cdot \Gamma(n-2) =$$

$$= n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = n!$$

Di qui la relazione che lega il fattoriale alla funzione Gamma:

$$n! = \Gamma(n+1) = \int_0^{+\infty} t^n\, e^{-t} dt$$

Andando a tracciare la funzione aritmetica f(n) = n! che è costituita da punti del primo quadrante di un sistema di assi cartesiani ortogonali con ascissa ed ordinata dei punti numeri interi positivi e tracciando la parte di grafico di Γ(x) del primo quadrante , si osserva che i punti di f(n) giacciono sull'arco di curva di Γ(x).



$0! = \Gamma(1) = 1$; $1! = \Gamma(2) = 1$;

$2! = \Gamma(3) = 2$; $3! = \Gamma(4) = 6$; ……

La funzione fattoriale è una funzione divergente all'infinito in modo veloce più di ogni altra funzione algebrica o trascendente, quest'ultima è ancor più veloce se ad esponente figura la funzione fattoriale. Si dice che il fattoriale è di ordine infinito superiore ad ogni altra funzione, per cui il calcolo per n = 30 , $n! > 10^{32}$, per cui i normali calcolatori non forniscono che una approssimazione di tale valore. Tuttavia anche prima dell'avvento dei computer ci si poneva il problema di come approssimare il fattoriale per valori di n grandi.

La formula di Stirling è una formula che descrive il comportamento asintotico della funzione $\Gamma(x)$ cioè per $x \to +\infty$ succede che

$$\lim_{x\to+\infty} \frac{\Gamma(x+1)}{\left(\frac{x}{e}\right)^x \sqrt{2\pi x}} = 1$$

Che è lo stesso scrivere: $\Gamma(x+1) = \left(\frac{x}{e}\right)^x \sqrt{2\pi x} + \omega(x)$

Pertanto Γ(x + 1) per x molto grandi viene approssimata da $\left(\frac{x}{e}\right)^x \sqrt{2\pi x}$; ora nel caso che x sia intero positivo: cioè x = n con n∈ N , si ha $n! = \Gamma(x+1)$. Quindi possiamo affermare che n! viene approssimato dalla formula di Stirling:

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

Questa formula è frequentemente usata in statistica e calcolo combinatorio, perché permette , quando n sufficientemente grande, di sostituire ad $n!$ l'espressione a secondo membro, semplificando notevolmente il calcolo: infatti il valore del secondo membro lo possiamo trovare mediante l'uso dei logaritmi.

Esempio: Si vuole calcolare 500! Applicando la formula di Stirling $k = \left(\frac{500}{e}\right)^{500} \sqrt{1000\pi}$, passando ai logaritmi si ha: $\ln k = 500 \cdot (\ln 500 - 1) + \frac{1}{2}(\ln 1000 + \ln \pi) = 2611{,}33029$ da cui k = $e^{2611,33029}$, che risulta dell'ordine di 10^{1120}cioè un numero intero positivo con circa 1120 cifre.

Vogliamo ricavare tale formula di Stirling sfruttando la funzione Gamma.
Partiamo dalla relazione: $n! = \Gamma(n+1)$ e dalla definizione: $\Gamma(x+1) = \int_0^{+\infty} t^n e^{-t} dt$.
Calcoliamo l'integrale :

$$\int_0^{+\infty} t^n e^{-t} dt.$$

Posto t = ny, calcoliamo il differenziale $dt = n\, dy \;\; se\; t = 0\,, allora\; y = 0$. Andiamo a sostituire tali valori nell'integrale indefinito:

$$\int_0^{+\infty} t^n e^{-t} dt = \int_0^{+\infty} (ny)^n e^{-ny} n dy = n^{n+1} \int_0^{+\infty} (y \cdot e^{-y})^n dy \ .$$

Sia $f(y) = (y \cdot e^{-y})^n$. Calcoliamo il logaritmo di tale funzione f(y):

$$\ln f(y) = n \cdot \ln(y \cdot e^{-y}) = n \cdot (\ln y - y) \quad \text{con f(y) } > 0 \quad \text{et} \quad y > 0$$

Posto y = x+1 con x > -1 e sostituendo nell'ultima, relazione si ha

$$\ln f(x+1) = n \cdot [\ln(x+1) - x - 1]$$

Sviluppando in serie di MacLaurin nel punto iniziale $x_0 = 0$, si ha:

$$\ln(x+1) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots - \frac{x^{2n}}{2n} + \frac{x^{2n+1}}{2n+1} - \cdots$$

Fermando lo sviluppo al secondo ordine si ha

$$\ln(x+1) = x - \frac{x^2}{2} + \omega(x)$$

Possiamo approssimare, tralasciando il termine $\omega(x)$, il $\ln(x+1)$:

$$\ln(x+1) \approx x - \frac{x^2}{2} +$$

Andando a sostituire tale approssimazione in

$$\ln f(x+1) = n \cdot [\ln(x+1) - x - 1]$$

Otteniamo:

$$\ln f(x+1) \approx n \cdot \left[x - \frac{x^2}{2} - x - 1\right] = -\frac{nx^2}{2} - n$$

Da cui passando all'antilogaritmo, si ha

$$f(x+1) \approx e^{-\frac{nx^2}{2} - n} = \frac{e^{-\frac{nx^2}{2}}}{e^n}$$

Pertanto

$$F(y) = F(f(x+1) \approx n^{n+1} \int_{-1}^{+\infty} \frac{e^{-\frac{nx^2}{2}}}{e^n} dx = \left(\frac{n}{e}\right)^n \cdot n \cdot \int_{-1}^{+\infty} e^{-\frac{nx^2}{2}} dx$$

Posto w = $\sqrt{\frac{n}{2}} \cdot$x , passando al differenziale $dw = \sqrt{\frac{n}{2}} \cdot dx$ e ricavando $dx = \sqrt{\frac{2}{n}} \cdot dw$, inoltre in

x = -1 w = - $\sqrt{\frac{n}{2}}$ sostituiamo nell'ultimo integrale :

$$\text{F(t)} \approx F(y) = F(f(x+1) \approx F(w) = \left(\frac{n}{e}\right)^n \cdot n \cdot \sqrt{\frac{2}{n}} \int_{-\sqrt{\frac{n}{2}}}^{+\infty} e^{-w^2} dw$$

Un estremo di integrazione dipende da n che tende all'infinito, pertanto l'ultimo integrale diviene:

$$\int_{-\infty}^{+\infty} e^{-w^2}\, dw = \sqrt{\pi}$$

Quindi sostituendo

$$\text{n!} = \Gamma(n+1) = \text{F(t)} \approx F(y) \approx \left(\frac{n}{e}\right)^n \cdot n \cdot \sqrt{\frac{2}{n}} \cdot \sqrt{\pi} = \left(\frac{n}{e}\right)^n \cdot \sqrt{2n\pi}$$

Cioè

$$\text{n!} \approx \left(\frac{n}{e}\right)^n \cdot \sqrt{2n\pi}$$

ottenendo così la formula di Stirling.

Andiamo ora a determinare il valore della funzione Gamma nel punto x = $\frac{1}{2}$

$$\Gamma\left(\frac{1}{2}\right) = \int_0^{+\infty} t^{\frac{1}{2}-1}\, e^{-t} dt = \int_0^{+\infty} t^{-\frac{1}{2}}\, e^{-t} dt$$

Calcoliamo l'ultimo integrale col metodo della sostituzione:

posto t = z^2 , *d* t = *2z d* z e sostituendo si ha $\Gamma\left(\frac{1}{2}\right) = \int_0^{+\infty} z^{-1}\, e^{-z^2} 2z dz = 2\int_0^{+\infty} e^{-z^2}\, dz$

tale integrale risulta l'integrale gaussiano calcolato precedentemente:

$$\Gamma\left(\frac{1}{2}\right) = 2\int_0^{+\infty} e^{-z^2}\, dz = 2 \cdot \frac{\sqrt{\pi}}{2} = \sqrt{\pi}$$

Quindi

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$

Applicando la formula ricorsiva possiamo determinare il valore di $\Gamma(x+1)$ = x $\Gamma(x)$

Se x = $\frac{1}{2}$, allora $\Gamma\left(\frac{1}{2}+1\right) = \Gamma\left(\frac{3}{2}\right) = \frac{1}{2} \cdot \Gamma\left(\frac{1}{2}\right) = \frac{\sqrt{\pi}}{2} = \frac{1 \cdot \sqrt{\pi}}{2^1}$

Se x = $\frac{3}{2}$, allora $\Gamma\left(\frac{3}{2}+1\right) = \Gamma\left(\frac{5}{2}\right) = \frac{3}{2} \cdot \Gamma\left(\frac{3}{2}\right) = \frac{3\sqrt{\pi}}{4} = \frac{1 \cdot 3 \cdot \sqrt{\pi}}{2^2}$

Se x = $\frac{5}{2}$, allora $\Gamma\left(\frac{5}{2}+1\right) = \Gamma\left(\frac{7}{2}\right) = \frac{5}{2} \cdot \Gamma\left(\frac{5}{2}\right) = \frac{15\sqrt{\pi}}{8} = \frac{1 \cdot 3 \cdot 5 \cdot \sqrt{\pi}}{2^3}$

Se x = $\frac{7}{2}$, allora $\Gamma\left(\frac{7}{2}+1\right) = \Gamma\left(\frac{9}{2}\right) = \frac{7}{2}\cdot\Gamma\left(\frac{7}{2}\right) = \frac{105\sqrt{\pi}}{16} = \frac{1\cdot3\cdot5\cdot7\cdot\sqrt{\pi}}{2^4}$

……..

Se x= $\frac{2n+1}{2}$, allora $\Gamma\left(\frac{2n+1}{2}+1\right) = \Gamma\left(\frac{2n+3}{2}\right) = \frac{2n+1}{2}\cdot\Gamma\left(\frac{2n+1}{2}\right) = \frac{(2n+1)!!}{2^{n+1}}\cdot\sqrt{\pi}$ con n≥ 0

dove il doppio punto esclamativo sta ad indicare il doppio fattoriale del numero naturale che lo precede:

es. per n = 0 → 1!! = 1

per n = 1 → $3!! = 1\cdot3$

per n = 2 → $5!! = 1\cdot3\cdot5$

…….

Per n = n → $(2n+1)!! = 1\cdot3\cdot5\cdot7\cdot\ldots\cdot(2n+1)$

In generale il valore del doppio fattoriale n!! è dato:

- Se n è dispari dal prodotto del numero n per tutti i numeri naturali dispari che lo precedono
- Se n è pari dal prodotto del numero n per tutti i numeri naturali pari che lo precedono.

Si assume per definizione che (-1)!! = 0!! = 1!! = 1

Considerato che

$$n! = \Gamma(n+1)$$

Possiamo dedurre che

$\left(\frac{1}{2}\right)! = \Gamma\left(\frac{1}{2}+1\right) = \Gamma\left(\frac{3}{2}\right) = \frac{1}{2}\cdot\Gamma\left(\frac{1}{2}\right) = \frac{\sqrt{\pi}}{2} = \frac{1\cdot\sqrt{\pi}}{2^1}$

$\left(\frac{3}{2}\right)! = \Gamma\left(\frac{3}{2}+1\right) = \Gamma\left(\frac{5}{2}\right) = \frac{3}{2}\cdot\Gamma\left(\frac{3}{2}\right) = \frac{3\sqrt{\pi}}{4} = \frac{1\cdot3\cdot\sqrt{\pi}}{2^2}$

$\left(\frac{5}{2}\right)! = \Gamma\left(\frac{5}{2}+1\right) = \Gamma\left(\frac{7}{2}\right) = \frac{5}{2}\cdot\Gamma\left(\frac{5}{2}\right) = \frac{15\sqrt{\pi}}{8} = \frac{1\cdot3\cdot5\cdot\sqrt{\pi}}{2^3}$

……

$\left(\frac{2n-1}{2}\right)! = \Gamma\left(\frac{2n-1}{2}+1\right) = \Gamma\left(\frac{2n+1}{2}\right) = \frac{2n-1}{2}\cdot\Gamma\left(\frac{2n-1}{2}\right) = \frac{(2n-1)!!}{2^n}\cdot\sqrt{\pi}$

Questo ci permette di estendere la definizione di *fattoriale* dall'insieme dei numeri naturali all'insieme A = $\left\{\forall x \in Q : x = n+\frac{1}{2} \ con\ n \in N\right\}$:

$$\left(n+\tfrac{1}{2}\right)! = \Gamma\left(\left(n+\tfrac{1}{2}\right)+1\right) = \tfrac{(2n+1)!!}{2^{n+1}}\sqrt{\pi}$$

Vogliamo ora determinare la funzione Γ(x) , quando x = $\left(\frac{1}{2}-n\right)$ con n > 0; sempre con l'uso della formula ricorsiva e conoscendo ormai il valore di $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$, possiamo scrivere:

$\sqrt{\pi} = \Gamma\left(\frac{1}{2}\right) = \Gamma\left(-\frac{1}{2}+1\right) = -\frac{1}{2}\cdot\Gamma\left(-\frac{1}{2}\right)$ da cui $\Gamma\left(-\frac{1}{2}\right) = -2\cdot\sqrt{\pi} = -\frac{2^1}{1!!}\sqrt{\pi}$

$-2\cdot\sqrt{\pi} = \Gamma\left(-\frac{1}{2}\right) = \Gamma\left(-\frac{3}{2}+1\right) = -\frac{3}{2}\cdot\Gamma\left(-\frac{3}{2}\right)$ da cui $\Gamma\left(-\frac{3}{2}\right) = -\frac{4}{3}\cdot\sqrt{\pi} = \frac{2^2}{3!!}\sqrt{\pi}$

$\frac{2^2}{3!!}\sqrt{\pi} = \Gamma\left(-\frac{3}{2}\right) = \Gamma\left(-\frac{5}{2}+1\right) = -\frac{5}{2}\cdot\Gamma\left(-\frac{5}{2}\right)$ da cui $\Gamma\left(-\frac{5}{2}\right) = -\frac{8}{15}\cdot\sqrt{\pi} = -\frac{2^3}{5!!}\sqrt{\pi}$

……

$$\Gamma\left(\tfrac{1}{2}-n\right) = (-1)^n\cdot\tfrac{2^n}{(2n-1)!!}\cdot\sqrt{\pi} \quad \text{con } n\in N \text{ e } n\neq 0$$

Da cui

$$\left(\tfrac{1}{2}-n\right)! = \Gamma\left(\left(\tfrac{1}{2}-n\right)+1\right) = \Gamma\left(\tfrac{1}{2}-(n-1)\right) = (-1)^{n-1}\cdot\tfrac{2^{n-1}}{(2n-3)!!}\cdot\sqrt{\pi}$$

Questo ci permette di estendere la definizione del *fattoriale* anche a numeri negativi appartenenti all'insieme B = $\left\{\forall x\in Q: x=\frac{1}{2}-n \ \ con\ n\in N\ e\ n>0\right\}$:

$$\left(\frac{1}{2}-n\right)! = (-1)^{n-1}\cdot\frac{2^{n-1}}{(2n-3)!!}\cdot\sqrt{\pi}$$

In generale per valori negativi della x, poiché l'integrale di definizione diverge, la funzione gamma (come si è visto per il caso di x = $\frac{1}{2}-n$) viene definita a partire dalla formula di ricorsività.

Il fattoriale trova applicazione nel Calcolo Combinatorio in particolare nel calcolo dei coefficienti del binomio di Newton e precisamente

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$$

Dove $\binom{n}{k}$, detto *coefficiente binomiale*, per la legge dei tre fattoriali è

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

Nel contesto del calcolo delle potenze del binomio di Newton l'esponente n è un intero positivo. Vediamo ora come è possibile determinare il valore del *coefficiente binomiale* nel caso che n sia un numero reale:

$$\binom{x}{k} = \frac{x!}{k!\,(x-k)!}$$

Usando la funzione Gamma per $x \in R$, sappiamo che per la formula ricorsiva

$$x! = \Gamma(x+1) = x \cdot \Gamma(x) = \text{x} \cdot h$$

dove abbiamo posto per comodità operativa h = Γ(x) = $\frac{x!}{x}$.

$\Gamma(x) = (x-1)\Gamma(x-1) \quad \rightarrow \quad \Gamma(x-1) = \frac{\Gamma(x)}{(x-1)} = \frac{h}{(x-1)}$

$\Gamma(x-1) = (x-2)\Gamma(x-2) \quad \rightarrow \quad \Gamma(x-2) = \frac{\Gamma(x-1)}{(x-2)} = \frac{h}{(x-1)(x-1)}$

$\Gamma(x-2) = (x-3)\Gamma(x-3) \quad \rightarrow \quad \Gamma(x-3) = \frac{\Gamma(x-2)}{(x-3)} = \frac{h}{(x-1)(x-2)(x-3)}$

……..

$\Gamma(x-k) = [x-(k-1)]\Gamma[x-(k-1)] \quad \rightarrow$

$$\Gamma[x-(k-1)] = \frac{\Gamma[x-(k-2)]}{[x-(k-1)]} = \frac{h}{(x-1)(x-2)(x-3)\cdot \ldots \cdot (x-k+1)}$$

Di qui il fattoriale:

$(x-k)! = \frac{h}{(x-1)(x-2)(x-3)\cdot\ldots\cdot(x-k+1)}$ con k ∈ $N - \{0\}$

$$\binom{x}{k} = \frac{x!}{k!(x-k)!} = \frac{x\cdot h}{k!} \cdot \frac{(x-1)(x-2)(x-3)\cdot\ldots\cdot(x-k+1)}{h} = \frac{x(x-1)(x-2)(x-3)\cdot\ldots\cdot(x-k+1)}{k!}$$

Formula analoga nel Calcolo Combinatorio relativa alla Combinazione a k a k di n oggetti , solo che in questo contesto n = x numero reale.

Questa formula ci permette di calcolare potenze di binomi ad esponente numeri frazionari, che spesso si incontrano in vari contesti.

Esempio:

a) Applicando la formula

$$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = \sum_{k=0}^{+\infty} \binom{\frac{1}{2}}{k} x^k = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \cdots$$

b) Applicando la funzione gamma:

$$\binom{\frac{1}{2}}{k} = \frac{\left(\frac{1}{2}\right)!}{k!\left(\frac{1}{2}-k\right)!}$$

Per k = 1 → $\binom{\frac{1}{2}}{1} = \frac{\left(\frac{1}{2}\right)!}{1!\left(-\frac{1}{2}\right)!} = \frac{\frac{1}{2}\sqrt{\pi}}{1\cdot\sqrt{\pi}} = \frac{1}{2}$

Per k = 2 → $\binom{\frac{1}{2}}{2} = \frac{\left(\frac{1}{2}\right)!}{2!\left(-\frac{3}{2}\right)!} = \frac{\frac{1}{2}\sqrt{\pi}}{2\cdot(-2\sqrt{\pi})} = -\frac{1}{8}$

Per k = 3 → $\binom{\frac{1}{2}}{3} = \frac{\left(\frac{1}{2}\right)!}{3!\left(-\frac{5}{2}\right)!} = \frac{\frac{1}{2}\sqrt{\pi}}{6\cdot(\frac{4}{3}\sqrt{\pi})} = \frac{1}{16}$

Per k = 4 → $\binom{\frac{1}{2}}{4} = \frac{\left(\frac{1}{2}\right)!}{4!\left(-\frac{7}{2}\right)!} = \frac{\frac{1}{2}\sqrt{\pi}}{24\cdot(-\frac{8}{15}\sqrt{\pi})} = -\frac{5}{128}$

……..

$$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = \sum_{k=0}^{+\infty}\binom{\frac{1}{2}}{k}x^k = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \cdots$$

Come è possibile constatare i due metodi coincidono.

NB. Questa formula permette di sviluppare in serie di potenze la funzione y = $\sqrt{1+x}$ senza ricorrere all' Analisi matematica con l'applicazione dello sviluppo in serie di MacLaurin.

Così se volessi sviluppare in serie la funzione y =$\frac{1}{\sqrt[3]{(1-x)^2}}$ posso usare la formula sopra scritta

Senza andare a calcolare le derivate di detta funzione richieste dal metodo di MacLaurin

Un'altra applicazione della funzione Gamma consiste nel calcolo della funzione Beta, detta *funzione euleriana di prima specie*. Venne studiata da Eulero e poi da Legendre ; essa è così definita:

per p e q reali e positivi

$$\beta(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx = \frac{\Gamma(p)\cdot\Gamma(q)}{\Gamma(p+q)}$$

Esempio: $\beta(2;3) = \int_0^1 x(1-x)^2dx = \left|\frac{1}{2}x^2 - \frac{2}{3}x^3 + \frac{1}{4}x^4\right|_0^1 = \frac{1}{12}$

$$\beta(2;3) = \frac{\Gamma(2)\cdot\Gamma(3)}{\Gamma(5)} = \frac{1\cdot 2}{24} = \frac{1}{12}$$

$$\beta(2,3) = \int_0^1 x(1-x)^2dx = \frac{\Gamma(2)\cdot\Gamma(3)}{\Gamma(5)} = \frac{1}{12}$$

Per completezza di informazione la funzione Gamma, come funzione complessa di variabile complessa viene definita da Eulero in modi diversi una prima volta nel seguente modo come prodotto infinito:

$$\Gamma(z) = \prod_{k=1}^{+\infty} \frac{\left(1+\frac{1}{k}\right)^{z-1}}{1+\frac{z-1}{k}}$$

Successivamente con l'introduzione della costante di Eulero-Mascheroni:

$$\gamma = \lim_{n\to+\infty}\left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\ln(n+1)\right] \approx 0{,}57721566\ 4901532861\ldots,$$

la definisce sempre come prodotto infinito con questa formulazione:

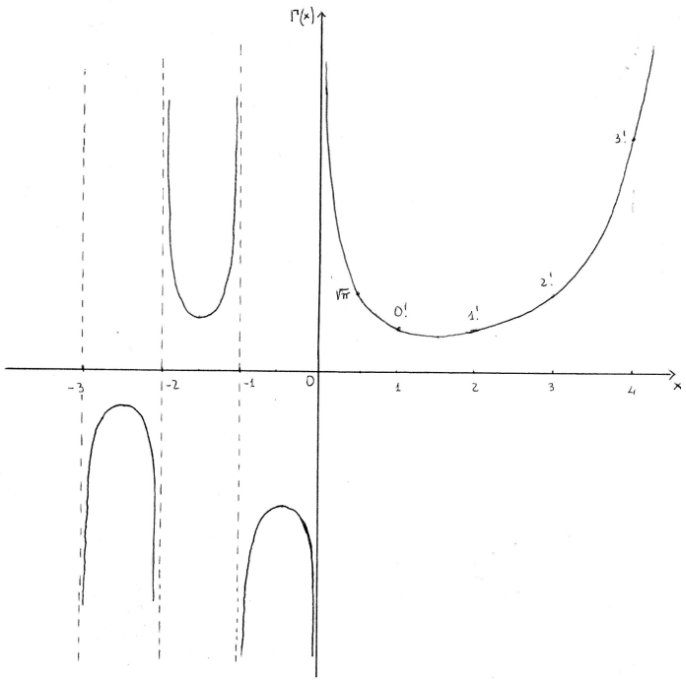
$$\Gamma(z) = \left\{ze^{\gamma z}\prod_{n=1}^{+\infty}\left[\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right]\right\}^{-1}$$

Tale funzione è chiamata anche *funzione euleriana di seconda specie*

Per x $\in R$ e $x > 0$, vale la seguente formula :

$$\Gamma(x) = \int_0^{+\infty} t^{x-1}\, e^{-t} dt$$

Formula di cui abbiamo trattato precedentemente come funzione interpolatrice della funzione fattoriale, la cui rappresentazione cartesiana completa è nella figura



```
program funzione_Gamma;
{$N+}
uses crt;
var  k,n,i,t,w:longint;
       b,h,c,c1,q,s,m,inf,sup,passo,passo1,passo2,diff,area1,area2:extended;
       a:real;
       risp:char;
function pot(x:real; y:longint):extended;
   begin
     if y=0 then pot:=1
            else pot:=x*pot(x,(y-1));
   end;
function f(x:real):extended;
   begin
     f:=pot(x,n-1)*exp(-x);
   end;
 begin
  repeat
    textbackground(1);
    clrscr;
    textcolor(15);
    writeln('Questo programma ti permette di calcolare la Funzione Γ (z) col');
    writeln('metodo del produttorio, con quello del limite e con quello del-');
    writeln('l''integrale, quando l''argomento è un numero intero positivo.');
    writeln('Si dimostra che per tali valori Γ (n)=(n-1)!.');  writeln;
    textcolor(12);
    write('Immetti il valore massimo della variabile k : k = ');  readln(k);
    write('Immetti il valore dell''argomento di Γ(n)   : n = '); readln(n);
    inf:=0.001;
    sup:=k;
    h:=10*k;
    c1:=1;
    textcolor(29);
    for i:=1 to k do
   begin
     if i<k then
       begin
         gotoxy(3,8);write('Attendere prego sto elaborando ');
       end;
     if i=k then
       begin
          gotoxy(3,8);write('                              ');
       end;
     a:=1+1/i;
     t:=n-1;
     b:=pot(a,t);
     c1:=c1*(b/(1+t/i));
```

```
end;
a:=pot(k,n);
s:=1; b:=1;
for i:=1 to n-1 do b:=b*i;
for i:=1 to n do s:=s*(k+i);
q:=a*b/s;
c:=1;
for i:=1 to n-1 do c:=c*i;
gotoxy(3,8);write('Attendere prego sto elaborando');
passo1:=h;
passo:=(sup-inf)/passo1;passo2:=(sup-inf)/(passo1-1);
w:=1;
repeat
  passo1:=passo1*w;
  passo:=(sup-inf)/passo1;passo2:=(sup-inf)/(passo1-1);
 a:=inf;
 area1:=0;
 repeat
   b:=a+2*passo;
   m:=a+passo/2;
   area1:=area1+(b-a)*f(m);
   a:=b;
 until a>=sup-passo;
 a:=inf;
 area2:=0;
 repeat
   b:=a+2*passo2;
   m:=a+passo2/2;
   area2:=area2+(b-a)*f(m);
   a:=b;
 until a>=sup-passo;
 diff:=abs(area1-area2);
 w:=w+1;
 until diff<1e-4;
 gotoxy(3,8);write('                          ');
  textcolor(10);
 writeln;
 writeln('La funzione Γ (',n,'), con il metodo del produttorio vale : ');
 writeln('         ',c1:6:12,' quando k = ',k);
 writeln;
 writeln('La funzione Γ (',n,'), col metodo del limite, vale: ');
 writeln('        ',q:6:12,' quando k = ',k);
 writeln;
 writeln("La funzione Γ (',n,'),  col metodo degli integrali, vale :',abs(area1):5:8);
 writeln;
 writeln('Operando con il fattoriale si ha il valore limite del produttorio, ');
 writeln('quando k tende all''infinito, che risulta : (',n,'-1)! = ',c:2:0);
 writeln;
```

```
    textcolor(14);
    write('Vuoi continuare con altro valore di K o di n ? (S/N) : ');
    readln(risp);
  until (risp='n') or (risp='N');
end.
```

2) seconda versione

program Funzione_Gamma_per_multipli_di_$\pm\frac{1}{2}$;

```
{$N+}
uses crt;
var a,b,i,d,c:longint;
    c1:char;
function pot(x,y:longint):longint;
begin
  if y=0 then pot:=1
        else pot:=x*pot(x,y-1);
end;
function dopfat(x:longint):longint;
begin
  if (x=-1) or (x=0) or (x=1) then dopfat:=1
                          else dopfat:=x*dopfat(x-2);
end;
begin
  clrscr;
  writeln('Questo programma ti permette di calcolare la funzione Gamma');
  writeln('per i primi 8 multipli dispari di ±1/2  ');
  writeln;
  i:=1;
  repeat
    a:=dopfat(i-2);
    c:=round((i-1)/2);
    b:=pot(2,c);
    writeln('Γ(',i,'/2) = ',a,'/',b,'*√π= ',a/b*sqrt(pi):3:18);
    i:=i+2;
  until i>=16;
  writeln;writeln;
   i:=1;
  repeat
    b:=dopfat(2*i-1);
    if i mod 2 <>0 then begin c1:='-';d:=-1 end
                   else begin c1:='+';d:=1 end;
    a:=pot(2,i);
    writeln('Γ(',1-2*i,'/2) = ',c1,'',a,'/',b,'*√π = ',d*a/b*sqrt(pi):3:18);
    i:=i+1;
  until i>=9;
readln;
end.
```

FUNZIONE ZETA di RIEMANN

La funzione ζ(z) è una funzione analitica: cioè una funzione complessa di variabile complessa, studiata da Riemann. Essa viene definita per Re(z) > 1 come somma della serie armonica generalizzata:

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} = \sum_{n=1}^{\infty} e^{-z \ln n}$$

Fra le sue numerose applicazioni nell'ambito della teoria dei numeri, essa esprime un'importante relazione con la successione dei numeri primi: infatti essa può essere espressa in questo modo:

$$\zeta(z) = \prod_p \frac{1}{1-\frac{1}{p^z}}$$

dove il prodotto infinito o produttorio deve essere esteso a tutti i numeri primi positivi.
Note le serie di Dirichlet possiamo trovare delle relazioni della funzione Zeta con le funzioni aritmetiche:

1) $\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$
2) $\zeta^2(s) = \sum_{n=1}^{+\infty} \frac{d(n)}{n^s}$
3) $\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s}$
4) $\zeta(s) \cdot \zeta(s-1) = \sum_{n=1}^{+\infty} \frac{\sigma(n)}{n^s}$

Il primo a notare la connessione e l'importanza della funzione Zeta nello studio dei numeri primi fu Eulero che nel 1737 dimostrò l'identità nel campo dei numeri reali:

$$\prod_{p_i} \frac{1}{1-p_i^{-x}} = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

dove x è un numero intero maggiore di 1, p_i sono gli infiniti numeri primi ed *n* i numeri naturali.

Proviamo a verificare tale identità:

Consideriamo la serie geometrica di ragione $0 < p_i^{-x} < 1$ con p_i numero primo ed x intero >1:

$$\sum_{m=0}^{\infty} (p_i^{-x})^m$$

Per la proprietà delle serie geometriche di ragione $q \in (-1\,;\,1)$, essa è convergente e precisamente alla somma infinita della progressione geometrica ad essa associata:

$$\sum_{m=0}^{\infty} (p_i^{-x})^m = \lim_{m\to\infty} \frac{1-(p_i^{-x})^m}{1-p_i^{-x}} = \frac{1}{1-p_i^{-x}}$$

Consideriamo la successione delle serie attribuendo a p_i valori numerici :

Per $p_1 = 2 \quad \rightarrow \quad \sum_{m=0}^{\infty}(2^{-x})^m = (2^{-x})^0 + (2^{-x})^1 + (2^{-x})^2 + \cdots = \frac{1}{1-2^{-x}}$

Per $p_2 = 3 \quad \rightarrow \quad \sum_{m=0}^{\infty}(3^{-x})^m = (3^{-x})^0 + (3^{-x})^1 + (3^{-x})^2 + \cdots = \frac{1}{1-3^{-x}}$

Per $p_3 = 5 \quad \rightarrow \quad \sum_{m=0}^{\infty}(5^{-x})^m = (5^{-x})^0 + (5^{-x})^1 + (5^{-x})^2 + \cdots = \frac{1}{1-5^{-x}}$

……

$\forall p_i \quad \rightarrow \quad \sum_{m=0}^{\infty}({p_i}^{-x})^m = ({p_i}^{-x})^0 + ({p_i}^{-x})^1 + ({p_i}^{-x})^2 + \cdots = \frac{1}{1-{p_i}^{-x}}$

……

Moltiplichiamo i vari membri delle uguaglianza tra di loro si ha:

$$\prod_{p_i}\left[\sum_{m=0}^{\infty}\left({p_i}^{-x}\right)^m\right] = [(2^{-x})^0 + (2^{-x})^1 + (2^{-x})^2 + \cdots][(3^{-x})^0 + (3^{-x})^1 + (3^{-x})^2 + \cdots] \cdot$$

$$\cdot [(5^{-x})^0 + (5^{-x})^1 + (5^{-x})^2 + \cdots] \cdot \ldots \cdot [({p_i}^{-x})^0 + ({p_i}^{-x})^1 + ({p_i}^{-x})^2 + \cdots] \cdot \ldots =$$

$$= \frac{1}{1-2^{-x}} \cdot \frac{1}{1-3^{-x}} \cdot \frac{1}{1-5^{-x}} \cdot \ldots \cdot \frac{1}{1-{p_i}^{-x}} \cdot \ldots = \prod_{p_i} \frac{1}{1-{p_i}^{-x}}$$

Eseguendo il prodotto dei termini presenti nelle parentesi quadre, raccogliendo in unica parentesi i fattori che individuano la decomposizione in fattori primi dei numeri naturali e applicando la proprietà distributiva inversa delle potenze , otteniamo la somma dei numeri naturali, aventi per esponente (–x): cioè

$$\sum_{n=1}^{\infty} n^{-x} = \sum_{n=1}^{\infty} \frac{1}{n^x} = \zeta(x)$$

ma $\sum_{n=1}^{\infty} n^{-x} = \prod_{p_i} \frac{1}{1-{p_i}^{-x}}$; per la proprietà transitiva dell'uguaglianza possiamo scrivere

$$\sum_{n=1}^{\infty} \frac{1}{n^x} = \zeta(x) = \prod_{p_i} \frac{1}{1-{p_i}^{-x}}$$

Come aveva osservato Eulero. Da questa relazione Eulero dedusse che i numeri primi sono infinti senza rifarsi alla dimostrazione di Euclide. Infatti egli constata che la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^x}$$

Per x = 1 , si ha la serie armonica che risulta divergente, così pure risulta divergente la sotto serie

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

Per x =2 , la serie $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converge a $\frac{\pi^2}{6}$.

Eulero confrontando la successione dei numeri primi con quella dei quadrati dei numeri naturali afferma che i numeri primi sono più numerosi dei quadrati perfetti in qualunque intervallo [1 ; n] della successione dei numeri naturali.

Sfruttando la serie di Dirichlet, possiamo determinare il valore della funzione zeta per x reale:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6} = 1{,}645 \ldots$$

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \cdots = \frac{\pi^4}{90} = 1{,}0823 \ldots$$

$$\zeta(6) = \frac{1}{1^6} + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + \cdots = \frac{\pi^6}{945} = 1{,}0173 \ldots$$

……..

$$\zeta(2k) = \frac{1}{1^{2k}} + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \cdots = \frac{\pi^{2k}}{m} = \frac{2^{2k-1}\pi^{2k}|B_{2k}|}{(2k)!}$$

Dove B_{2k} è il 2k-simo numero di Bernoulli.

(NB. Sono detti numeri di Bernoulli i coefficienti dello sviluppo in serie di MacLaurin della funzione

$$y = \frac{x}{e^x - 1}$$

Cioè:

$$\frac{x}{e^x - 1} = 1 - \frac{1}{2}x + \frac{1}{6} \cdot \frac{x^2}{2!} - \frac{1}{30} \cdot \frac{x^4}{4!} + \frac{1}{42} \cdot \frac{x^6}{6!} - \frac{1}{30} \cdot \frac{x^8}{8!} + \frac{5}{66} \cdot \frac{x^{10}}{10!} - \frac{691}{2730} \cdot \frac{x^{12}}{12!} + \frac{7}{6} \cdot \frac{x^{14}}{14!} + \cdots$$

Pertanto i numeri di Bernoulli sono:

$B_2 = \frac{1}{6}$; $B_2 = -\frac{1}{30}$; $B_2 = \frac{1}{42}$; $B_2 = -\frac{1}{30}$; $B_2 = \frac{5}{66}$; $B_2 = -\frac{691}{2730}$; $B_2 = \frac{7}{6}$;

…

(Per il calcolo vedi Appendice)

Per i numeri dispari non esiste alcuna formula pertanto si accettano quei valori che fino ad oggi sono stati trovati, ne esponiamo i valori relativi a:

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots = 1{,}202 \ldots$$

$$\zeta(5) = \frac{1}{1^5} + \frac{1}{2^5} + \frac{1}{3^5} + \frac{1}{4^5} + \cdots = 1{,}0369 \ldots$$

$$\zeta(7) = \frac{1}{1^7} + \frac{1}{2^7} + \frac{1}{3^7} + \frac{1}{4^7} + \cdots = 1{,}0083 \ldots$$

La funzione zeta come funzione analitica

Fu poi Riemann a considerare e a studiare la funzione Zeta ($\zeta(s)$) come funzione analitica a variabile complessa sotto la condizione che la parte reale *Re(s)* fosse > 1. Questa condizione risultava necessaria perché la serie:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

fosse convergente.

Ipotesi di Riemann

Una delle proprietà più importanti della funzione Zeta è che soddisfa la seguente equazione funzionale:

$$\zeta(s) = 2^s \pi^{s-1} sen\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

Questa equazione per $sen\left(\frac{\pi s}{2}\right) = 0$: cioè per Re(s) = - 2k con k = 1 ; 2 ; 3 ; … ha zeri semplici o banali: abbiamo presi Re(s)<1, in quanto il produttorio di Eulero per Re(s) > 1 non ammette zeri.
Pertanto eventuali zeri della funzione Zeta devono essere ricercati per 0 < Re(s) < 1.
Vari sono i risultati ottenuti da Riemann nell'utilizzo di tale funzione tra cui una formula che mostra la dipendenza della funzione enumerativa $\pi(n)$ dei numeri primi dagli zeri della funzione Zeta.
Per pura curiosità la formuliamo:

$$\pi(x) = \sum_{m=1}^{\infty} \mu(m) \frac{\int_2^{x^{\frac{1}{m}}} \frac{1}{\ln(t)} dt - \sum_\rho \int_2^{x^{\frac{\rho}{m}}} \frac{1}{\ln(t)} dt + \int_{x^{\frac{1}{m}}}^{\infty} \frac{1}{t(t^2-1)lnt}\, dt}{m}$$

La correlazione con la funzione zeta sta nel fatto che i valori della variabile ρ , che figura nella sommatoria, sono i moduli degli zeri complessi non banali della funzione Zeta.
Tuttavia egli non riuscì a calcolare tali zeri, asserendo però che
" è molto probabile che tutti gli zeri non banali della funzione Zeta abbiano parte reale $\frac{1}{2}$: cioè giacciono nel piano complesso sulla retta *Re(s)*=$\frac{1}{2}$ "
Questa asserzione è detta " Ipotesi di Riemann " ed è oggi una congettura. Tale Ipotesi costituisce uno dei problemi aperti della matematica grazie anche alle conseguenze che implicherebbe, qualora fosse dimostrata, sulla distribuzione dei numeri primi.

L'ipotesi di Riemann e la funzione Zeta son connesse alle funzioni aritmetiche: infatti l'ipotesi di Riemann vale se la serie

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

converge per $Re(s) > \frac{1}{2}$. Inoltre se $Re(s) > 1$ vale l'identità:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

L'ipotesi di Riemann è equivalente al seguente limite, dimostrato da Landau nel 1899:

$$\lim_{n\to\infty} \frac{\lambda(1)+\lambda(2)+\lambda(3)+\cdots+\lambda(n)}{n^{\frac{1}{2}+\varepsilon}} = 0 \qquad \forall \varepsilon > 0$$

Dove $\lambda(n)$ è la funzione di Lionville: così definita

$$\begin{cases} \lambda(1) = 1 \\ \lambda(n) = (-1)^{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_r} \end{cases}$$

dove gli α_i sono gli esponenti della scomposizione in fattori primi di n:

$$n = p_1^{\alpha_1} \cdot p_1^{\alpha_1} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_1^{\alpha_1}.$$

L'Ipotesi di Riemann costituisce l'ottavo problema dei 23, proposti da Hilbert al Congresso Ufficiale di Matematica tenuto a Parigi nel 1900. Hilbert era convinto che una dimostrazione di questa Ipotesi potesse portare a risolvere l'annosa questione sulla distribuzione dei numeri primi, in particolare che i numeri primi accoppiati o gemelli sono infiniti.

Il valore $\pi(n)$

Def: $\pi(n)$ è il numero dei numeri primi minori od uguale ad un numero intero positivo *n* assegnato

Teorema dei numeri primi (Gauss 1792 – de la Vallée Poussin-Hadamard 1890)

" Il numero $\pi(n)$ dei numeri primi minori od uguale di un dato numero intero n si avvicina asintoticamente al quoziente $\frac{n}{ln(n)}$, quando n cresce all'infinito. "

Questo teorema, contenuto in una formula scritta da Gauss in un suo appunto, fu espressamente enunciato da Čebyšev nella forma

" Se $\pi(n)$ è la funzione che esprime il numero dei numeri primi minori od uguali ad n, allora

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{ln(n)}} = 1 \qquad "$$

Ma questi non fu in grado di dimostrare l'esistenza di tale limite. Soltanto due anni dopo la sua morte nel 1896 due matematici: uno belga C.J.de la Vallée_Poussin ed uno francese J. Hadamard indipendentemente l'uno dall'altro e in forma diversa diedero la dimostrazione di tale limite.

Tale teorema è equivalente a:

a) $\lim_{n\to\infty} \frac{\lambda(1)+\lambda(2)+\lambda(3)+\cdots+\lambda(n)}{n} = 0$

b) Posto $Li = \int_2^x \frac{1}{\ln(t)} dt$, $\pi(n) \approx Li$

```
program funzione_zeta;
{$N+}
uses crt;
var  k,n,i,y:longint;
     b,a:extended;
     c:integer;
     risp:char;
procedure numeroprimo(x:longint);
var i:longint;
begin
  i:=1;
  repeat i:=i+1 until x mod i = 0;
  if (i=x) and (x<=k)
            then begin (*write(x:10);*) y:=1 end
            else y:=0;
end;
function pot(x:longint; y:longint):extended;
begin
   if y=0 then pot:=1
         else pot:=x*pot(x,(y-1));
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('    Questo programma ti permette di determinare il valore della ');
  writeln('                    Funzione ζ(n) di Riemann');
  writeln('Con due metodi: quella del Produttorio e quello della Serie Armonica');
  writeln;
  textcolor(12);
  write('Immetti l''estremo superiore k della successione dei numeri naturali : ');
  readln(k);
  write('Immetti il valore dell''esponente della funzione  ζ(n) : n = ');
  readln(n);
  b:=1; c:=0;
  for i:=2 to k do
    begin
      if i=k then c:=1;
```

```
      numeroprimo(i);
      textcolor(30);gotoxy(3,20);write('Attendere prego sto elaborando ');
      if c=1 then begin gotoxy(3,20);write('                              ');end;
      if y<>0 then
        begin
          a:=pot(i,n);
          b:=b*(a/(a-1));
        end;
   end;
  gotoxy(3,8);
  textcolor(10);
  writeln;
  writeln('        Valore della funzione ζ (n) col metodo del  ');
  writeln('         Produttorio delle potenze dei numeri primi ');
  writeln('             ζ ( ',n,' )= ',b:2:18);
  writeln;
  writeln('Valore della funzione ζ(n) col metodo della Serie Armonica Generalizzata');
  b:=1;
  for i:=2 to k do
    begin
      a:=pot(i,n);
      b:=b+1/a;
    end;
  writeln('               ζ ( ',n,' )= ',b:2:18);
  writeln;
   if n=2 then
       begin
         writeln('Il valore della funzione  ζ(',n,') col metodo del Limite, dovuto ad Eulero, è :');
         writeln('               ζ ( ',n,' )= ',sqr(pi)/6:2:18);
       end;
   writeln;writeln;
   write('Vuoi continuare con altri valori di k e di n ? (S/N) : ');
   readln(risp);
 until (risp='n') or (risp='N');
end.
```

a) Prima versione

```
program Lionville;
uses crt;
var  n,n1,i,k,j,s,r,somma,y:longint;
      a,m,q,b:array[1..1000] of longint;
      risp:char;
procedure numeroprimo(x:longint);
var i:longint;
```

```
  begin
     i:=1;
     repeat
        i:=i+1
     until x mod i = 0;
     if (i=x) and (x<=n)  then y:=1
                          else y:=0;
  end;
begin
     textbackground(1);
   repeat
     clrscr;
    textcolor(15);
    gotoxy(1,2);
    writeln('Questo programma ti permette di calcolare il valore della funzione');
    writeln('di Lionville relativa ad un numero n intero positivo: ');
    writeln('                f(n)=(-1)^(a+b+c+...)');
    writeln('dove a,b,c,... sono gli esponenti della scomposizione di n in fattori');
    writeln('primi.');
    textcolor(12);
    writeln;
    write('Immetti il valore del numero: n = ');readln(n);
    n1:=n;
    textcolor(26);
    if n>700 then
            begin
              gotoxy(2,10);write('Attendere prego, sto elaborando !! ');
            end;
    writeln;
    textcolor(10);
    k:=0;
 for i:=2 to n  do
   begin
     numeroprimo(i);
     if y=1 then
             begin
               k:=k+1;
               m[k]:=i;

             end;
   end;
 writeln;
 write('      ',n,' = ');
 s:=0;
```

```
  for i:=1 to k do
    begin
      r:=0;
      repeat
       if (n mod m[i] = 0) then
                                  begin
                                     r:=r+1;
                                     n:=n div m[i];
                                  end;
     until (n mod m[i] <>0) or (r=0);
     if r<>0 then
               begin
                 s:=s+1;
                 write(m[i],'^',r,' ú ');
                 q[s]:=m[i];
                 b[s]:= r;
               end;
    end;
    textcolor(11);
    if n1>700 then
           begin
             gotoxy(2,10);write(' Fine elaborazione                ');
           end;
  textcolor(14);
  gotoxy(2,14);
  somma:=0;
  for j :=1 to k do somma:=somma+b[j];
  if somma mod 2 = 0 then write('La funzione di Lionville: f(',n1,') = (-1)^',somma,' = 1')
                          else write('La funzione di Lionville: f(',n1,') = (-1)^',somma,' = -1');
  writeln;writeln;
  textcolor(13);
  Write('Vuoi continuare con altro valore di n ? (S/N): ');
  readln(risp);
 until (risp='n') or (risp='N');
end.
```

b) Seconda versione.

```
program Lionville2;
uses crt;
var  n,n1,i,k,j,s,r,somma,y,xmax,xmin:longint;
     a,m,q,b:array[1..1000] of longint;
```

```
      risp:char;
procedure lion(w:longint);
  procedure numeroprimo(x:longint);
    var i:longint;
    begin
       i:=1;
       repeat
          i:=i+1
       until x mod i = 0;
      if (i=x) and (x<=n)  then y:=1
                           else y:=0;
  end;
begin
  n1:=w;
  textcolor(10);
  k:=0;
 for i:=2 to w  do
           begin
             numeroprimo(i);
             if y=1 then
                      begin
                         k:=k+1;
                         m[k]:=i;
                      end;
           end;
 writeln;
 write('      ',w,' = ');
 s:=0;
 for i:=1 to k do
           begin
              r:=0;
              repeat
                if (w mod m[i] = 0) then
                                      begin
                                          r:=r+1;
                                         w:=w div m[i];
                                      end;
              until (w mod m[i] <>0) or (r=0);
              if r<>0 then
                       begin
                          s:=s+1;
                         write(m[i],'^',r,' ú ');
                         q[s]:=m[i];
                         b[s]:= r;
                       end;
           end;
 textcolor(14);
 somma:=0;
```

```
    for j :=1 to s do somma:=somma+b[j];
    if somma mod 2 = 0 then write('--->  f(',n1,') = 1')
                           else write('---> f(',n1,') = -1');
    end;
    begin
        textbackground(1);
        repeat
       clrscr;
        textcolor(15);
        gotoxy(1,2);
        writeln('Questo programma ti permette di calcolare il valore della funzione');
        writeln('di Lionville relativa agli n interi positivi: ');
        writeln('                f(n)=(-1)^(a+b+c+...)');
        writeln('dove a,b,c,... sono gli esponenti della scomposizione degli n in fattori');
        writeln('primi, presi in un intervallo scelto a piacere.');
        textcolor(12);
        writeln;
        write('Immetti il valore dell''estremo inferiore dell''intervallo: ');readln(xmin);
        write('Immetti il valore dell''estremo superiore dell''intervallo: ');readln(xmax);
        for n:=xmin to xmax do
                begin
                   if n mod 16 = 0 then
                        begin
                           readln;
                           textbackground(1);
                           clrscr;
                           textcolor(15);
                           gotoxy(1,2);
                           writeln('Questo programma ti permette di calcolare il valore della funzione');
                           writeln('di Lionville relativa agli n interi positivi: ');
                           writeln('                f(n)=(-1)^(a+b+c+...)');
                           writeln('dove a,b,c,... sono gli esponenti della scomposizione degli n in fattori');
                           writeln('primi, presi in un intervallo scelto a piacere.');
                          textcolor(12);
                         end;
         lion(n);
         end;
        writeln;writeln;
        textcolor(11);
        write('Vuoi continuare in un altro intervallo ? (S/N) : ');
        readln(risp);
 until (risp='n') or (risp='N');
end.
```

La distribuzione dei numeri primi è un argomento che ha sempre affascinato i matematici da Euclide ai nostri giorni. Quello che può essere considerato come un difficile corollario del

Teorema di Euclide sull'infinità dei numeri primi venne dimostrato dal matematico P.G.Lejeune Dirichlet. Il suo Teorema afferma non solo che i numeri primi sono infiniti, ma che anche se considerassimo l'insieme degli interi che compaiono nella progressione aritmetica:

$$a\ ;\ a + b\ ;\ a + 2\cdot b\ ;\ a + 3\cdot b\ ;\ \ldots\ ;\ a + n\cdot b\ ;\ \ldots.$$

con a e b primi fra loro: cioè M.C.D (a ; b) = 1, persino in questa successione relativamente più rada di numeri interi rispetto alla sequenza dei numeri interi esiste una infinità di numeri primi.

Teorema: Se $b \in N$ ed $a \in Z$ tale che MCD (a ; b) = 1 , allora esistono infiniti numeri primi p tale che

$$p \equiv a \bmod b$$

NB. Tale relazione è equivalente alla progressione aritmetica precedentemente scritta: infatti dire che $p \equiv a \bmod b$ significa che $p - a = kb$ con $k \in N$ e di conseguenza sostituendo a k i valori 0, 1, 2, 3, …, otteniamo la progressione.

Lasciamo la dimostrazione ad un testo specialistico, qui stendiamo un programma in Turbo Pascal che ci permette di determinare quali e quanti sono i numeri primi in un intervallo semiaperto a destra e chiuso a sinistra : [2 ; sup) che soddisfano il teorema di Dirichlet; inoltre permette di determinare la loro percentuale rispetto a tutti i numeri primi presenti in tale intervallo. Ripetendo il programma con l'estremo superiore sempre più grande, ci accorgiamo che tale percentuale si va diminuendo .

```
program Teorema_di_Dirichlet;
uses crt;
var k,i,j,h,p,w,sup,b,a,xmax,w:longint;
      r:real;
      m,n:array[1..100] of longint;
      risp:char;
function mcd(x,y:longint):longint;
var resto:longint;
begin
  resto :=x mod y;
  while resto<>0 do
     begin
       x:=y; y:=resto;
       resto:=x mod y
     end;
  mcd:=y;
end;
procedure primo(x:integer);
var i:integer;
begin
 k:=0;
 for i:=2 to x div 2 do
    if x mod i = 0 then k:=k+1;
end;
```

```
begin
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('  Questo programma verifica operativamente con la ricerca dei numeri ');
  writeln('  primi il Teorema di Dirichlet, che afferma:');
  writeln;
  writeln('  " Dati un numero q intero positivo, diverso da zero, e un numero ');
  writeln('    intero a tale che MCD(b;a)=1, esistono infiniti numeri primi p ');
 writeln('    tali che   p ≡ a mod b.  " ');
  writeln;
  repeat
  textcolor(10);
  write('  Immetti un numero intero positivo b = ');readln(b);
  repeat
  write('  Immetti un numero intero a primo con b ');readln(a);
  until mcd ( b , a ) = 1;
  writeln;
  textcolor(12);
  writeln('  Poichè l''aritmetica del calcolatore è finita, come strategia di ');
  writeln('  verifica del teorema adoperiamo intervalli di ricerca predefinita.');
  writeln;
  repeat
  textcolor(11);
  write('  Immetti l''estremo superiore dell''intervallo sup = ');readln(sup);
  writeln;
  textcolor(14);
  j:=0;
  for i:=2 to sup do
          begin
            primo(i);
            if (k=0) and ((i-a) mod b = 0) then
                        begin
                          j:=j+1;
                          m[j]:=i;
                        end;
          end;
  for i:=1 to j-1 do
        write(m[i],' ; ');
   writeln(m[j]);
  w:=0;
  for i:=2 to sup do
       begin
          primo(i);
          if k = 0 then w=w+1;
       end
   r:= j/w*100;
```

```
    writeln;
   textcolor(15);
   writeln(' Il numero dei numeri primi nell"intervallo [2;',sup,'] tale che');
   writeln('           p ≡ ',a,' mod ',b);
    writeln(' sono:           ',j);
   writeln;
   writeln(' Il numero dei numeri primi nell"intervallo [2;',sup,']  è  ', w );
   writeln;
   writeln('La percentuale dei numeri primi relativi al Teorema di Dirichlet rispetto ');
   writeln(' a tutti i numeri primi in [ 2 ; ', sup,'] è  ', r:2:2);
   writeln;
   writeln;
   textcolor(13);
   write('Vuoi provare con un altro intervallo ? (S/N) ');
   readln(risp);
   until (risp='N') or (risp='n');
   write('Vuoi provare con un"altra coppia di numeri q ed a ? (S/N) ');
  readln(risp);
 clrscr;
 until (risp='N') or (risp='n');
end.
```

Appendice

Calcolo dei numeri di Bernoulli

Si chiamano numeri di Bernoulli il valore delle derivate d'ordine pari dello sviluppo in serie di Taylor, nel punto iniziale $x_o = 0$, della funzione

$$f(x) = \frac{x}{e^x - 1}$$

In tale sviluppo, fatta eccezione del derivata prima, tutte le derivate d'ordine dispari sono uguali a zero

Consideriamo $(e^x - 1)f(x) = x$; da cui $e^x f(x) = f(x) + x$

Derivando successivamente ambo i termini dell'equazione rispetto alla x, si ha:

1) $e^x f(x) + e^x f'(x) = f'(x) + 1$
$e^x[f(x) + f'(x)] = f'(x) + 1$

2) $e^x[f(x) + f'(x)] + e^x[f'(x) + f''(x)] = f''(x)$
$e^x[f(x) + 2 \cdot f'(x) + f''(x)] = f''(x)$

3) $e^x[f(x) + 2 \cdot f'(x) + f''(x)] + e^x\left[f'^{(x)} + 2 \cdot f''(x) + f'''(x)\right] = f'''(x)$
$e^x[f(x) + 3 \cdot f'(x) + 3 \cdot f''(x) + f'''(x)] = f'''(x)$

4) $e^x[f(x) + 3 \cdot f'(x) + 3 \cdot f''(x) + f'''(x)] + e^x\left[f'^{(x)} + 3 \cdot f''(x) + 3 \cdot f'''(x) + \right.$
$\left. + f^{IV}(x)\right] = f^{IV}(x)$
$e^x[f(x) + 4 \cdot f'(x) + 6 \cdot f''(x) + 4 \cdot f'''(x) + f^{IV}(x)] = f^{IV}(x)$

5) $e^x[f(x) + 5 \cdot f'(x) + 10 \cdot f''(x) + 10 \cdot f'''(x) + 5 \cdot f^{IV}(x) + f^{V}(x)] = f^{V}(x)$

……

Iterando il procedimento ed osservato che i coefficienti delle derivate sono i coefficienti dello sviluppo del binomio di Newton, possiamo determinare un qualunque sviluppo.

Ponendo $x = 0$ in queste equazioni si ha:

2) $f(0) = 1$
3) $2 \cdot f'(0) + f(0) = 0 \quad \rightarrow \quad f'(0) = -\frac{1}{2}$
4) $3 \cdot f''(0) + 3 \cdot f'(0) + f(0) = 0 \quad \rightarrow \quad f''(0) = \frac{1}{6}$
5) $4 \cdot f'''(0) + 6 \cdot f''(0) + 4 \cdot f'(0) + f(0) = 0 \quad \rightarrow \quad f'''(0) = 0$

6) $5 \cdot f^{IV}(0) + 10 \cdot f'''(0) + 10 \cdot f''(0) + 5 \cdot f'^{(0)} + f(0) = 0 \quad \rightarrow \quad f^{IV}(0) = -\frac{1}{30}$

…….

Otteniamo successivamente, calcolando a parte ,

$f'(0) = -\frac{1}{2}$; $f''(0) = \frac{1}{6}$; $f'''(0) = 0$; $f^{IV}(0) = -\frac{1}{30}$; $f^{V}(0) = 0$; $f^{VI}(0) = \frac{1}{42}$

$f^{VII}(0) = 0$; $f^{VIII}(0) = -\frac{1}{30}$; $f^{IX}(0) = 0$; $f^{X}(0) = \frac{5}{66}$; $f^{XI}(0) = 0$; $f^{XII}(0) = -\frac{691}{2730}$

$f^{XIII}(0) = 0$; $f^{XIV}(0) = \frac{7}{6}$; $f^{XV}(0) = 0$; $f^{XVI}(0) = -\frac{3617}{510}$; $f^{XVII}(0) = 0$

$f^{XVIII}(0) = \frac{43867}{42}$; $f^{XIX}(0) = 0$; $f^{XX}(0) = -\frac{145983377}{2310}$; …..

Se ora indichiamo con

$B_2 = f''(0) = \frac{1}{6}$; $B_4 = f^{IV}(0) = -\frac{1}{30}$; $B_6 = f^{VI}(0) = \frac{1}{42}$; $B_8 = f^{VIII}(0) = -\frac{1}{30}$

$B_{10} = f^{X}(0) = \frac{5}{66}$; $B_{12} = f^{XII}(0) = -\frac{691}{2730}$; $B_{14} = f^{XIV}(0) = \frac{7}{6}$

$B_{16} = f^{XVI}(0) = -\frac{3617}{510}$; $B_{18} = f^{XVIII}(0) = \frac{43867}{42}$; $B_{20} = f^{XX}(0) = -\frac{145983377}{2310}$

……

Lo sviluppo in serie di MacLaurin della funzione $f(x) = \frac{x}{e^x - 1}$ risulta:

$$\frac{x}{e^x - 1} = 1 + \frac{x}{1!}\left(-\frac{1}{2}\right) + \frac{x^2}{2!}B_2 + \frac{x^4}{4!}B_4 + \frac{x^6}{6!}B_6 + \frac{x^8}{8!}B_8 + \frac{x^{10}}{10!}B_{10} + \ ...$$

I coefficienti B_2 , B_4 , B_6 , B_8 , B_{10} , … si chiamano *numeri di Bernoulli*, essendo stati la prima volta studiati da Giacomo Bernoulli.

La funzione $f(x) = \frac{x}{e^x - 1}$

Vista l'importanza della funzione $f(x) = \frac{x}{e^x - 1}$
Vogliamo proporre qui il suo studio ed il suo grafico rispetto ad un sistema di assi cartesiani monometrico ortogonale xOy.

Studio della funzione:

a) Funzione trascendente esponenziale fratta di base e = 2,71828…
b) C.E. = $\mathbb{R}$ - {0}
c) Simmetrie fondamentali.

La funzione non presenta simmetrie rispetto all' asse y, né rispetto all'origine del sistema di riferimento.

d) Segno:

$$\frac{x}{e^x-1} > 0 \quad \text{se} \quad \begin{cases} x > 0 \\ e^x - 1 > 0 \end{cases} \quad \text{oppure} \quad \begin{cases} x < 0 \\ e^x - 1 < 0 \end{cases}$$

Il primo sistema è verificato per x > 0 , il secondo è verificato per x < 0, unendo i due intervalli possiamo affermare la funzione è sempre positiva nel suo campo di esistenza.

e) Ricerca di eventuali asintoti:

a) Asintoto verticale : $\lim_{x\to 0} \frac{x}{e^x-1} = 1$, applicando la regola di De L'Hopital pertanto il punto di ascissa 0 è un punto di discontinuità eliminabile il suo valore è 1. La funzione non ammette asintoti verticali e passa per il punto A (0 ; 1)

b) Asintoto orizzontale: $\lim_{x\to+\infty} \frac{x}{e^x-1} = 0$: la retta y = 0 è un asintoto orizzontale per x che tende a +∞; $\lim_{x\to-\infty} \frac{x}{e^x-1} = +\infty$: per x che tende a $-\infty$ non presenta asintoto orizzontale

c) Asintoto obliquo: $m = \lim_{x\to-\infty} \left(\frac{x}{e^x-1}.\frac{1}{x}\right) = -1$; $q = \lim_{x\to-\infty} \left(\frac{x}{e^x-1} + x\right) = 0$

La retta di equazione y = - x costituisce un asintoto obliquo per x che tende a $-\infty$

f) Derivata prima

$$y' = \frac{e^x(1-x)-1}{(e^x-1)^2}$$

Derivata seconda

$$y' = \frac{e^x[e^x(x-2)+x+2]}{(e^x-1)^3}$$

a) Crescenza e decrescenza: studio del segno di y'

per $\forall x$ il numeratore è negativo, mentre il denominatore è positivo, pertanto la derivata prima è negativa , la funzione è *decrescente*

b) Massimi e minimi

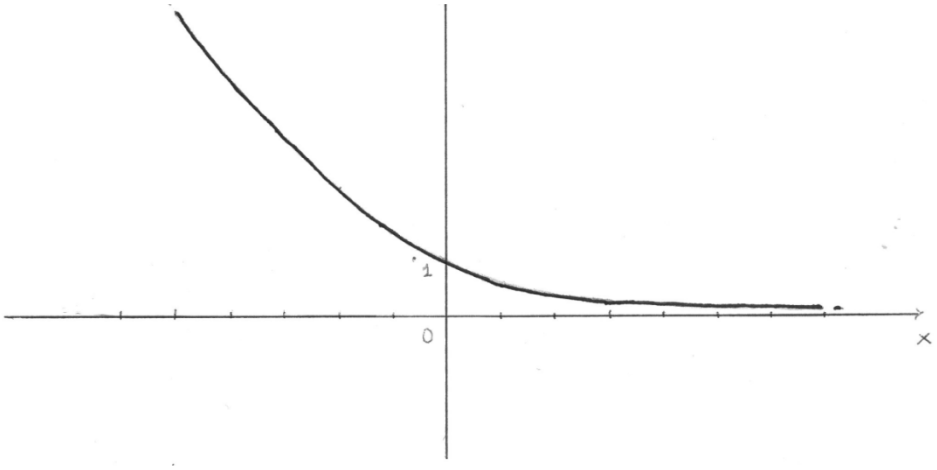
y' ≠ 0 $\forall x$ pertanto la funzione non ammette massimi o minimi.

c) Concavità e convessità: studio del segno di y''

y'' > 0 $\forall x$ pertanto la funzione volge la concavità verso il semiasse positivo delle ordinate

d) Flessi: La funzione non presenta flessi

Grafico:



CAPITOLO III

Numeri primi e Primalita'

A) Divisibilità tra numeri naturali, MCD e mcm

Teorema di divisibilità: Siano a e b $\in N$ con a $\neq 0$, esistono due numeri q ed r $\in$ N tale che

$$b = a \cdot q + r$$

con $0 \leq r \leq a$.

Al numero q si dà nome di quoziente tra b e a e ad r si dà nome di resto: quest'ultimo può essere definito come il risultato dell'operatore *mod* tra numeri naturali r = b *mod* a

Def. Se il resto r = 0 , allora si dice che a è un divisore di b o che b è divisibile per a.

Proprietà dei divisori: Se a è un divisore di b, indichiamo tale asserzione con a | b, allora valgono le seguenti proprietà

- $\forall\, a \in N \;\rightarrow\; a \mid a$
- $\forall\, a,b,c \in N \rightarrow se\ a \mid b\ \ e\ \ b \mid c\ \ allora\ \ a \mid c$
- $\forall\, a,b,c \in N \rightarrow se\ c \mid a\ \ e\ \ c \mid b\ allora\ c \mid (a+b)\ e\ \ c \mid (a-b)\ \ \ con\ a > b$
- $\forall\, a,b,c,x,y \in N \rightarrow se\ c \mid a\ \ \ e\ \ c \mid b\ \ allora\ \ c \mid (x \cdot a + y \cdot b)$
- $\forall a,b \in N \rightarrow se\ \ a \mid b\ e\ b \mid a\ \ allora\ \ a = b$

Def. di Massimo Comun Divisore (MCD): Siano a e b $\in N_0$, si chiama Massimo Comun Divisore tra a e b: MCD(a ; b) , quel numero $m \in N$ tale che

- $\forall\, c \in N \rightarrow se\ \ c \mid a\ \ e\ \ c \mid b\ allora\ \ c \mid m$
- $\exists\exists\, x\ e\ y \in Z\ \ tale\ che\ \ \ m = a \cdot x + b \cdot y$

La prima relazione della definizione ci garantisce che il Massimo Comun Divisore tra a e b è il più grande dei divisori comuni ad a e b. La seconda ci afferma che il Massimo Comun Divisore tra a e b è una combinazione lineare di a e b.

NB. Per convenzione si stabilisce che se uno dei valori a o b è zero il MCD (a; b) è il valore tra a e b diverso da zero.

Inoltre se a e b non sono entrambi nulli si dimostra che

$$1 \leq MCD(a;b) \leq \inf(a\,;b)$$

Proprietà del MCD:

- $\forall a,b \in N \;\rightarrow\; MCD(a\,;b) = MCD\,(\,b\,;a)$
- $\forall\, a\,,k \in N \;\rightarrow MCD\,(a\,;\ k \cdot a) = a$
- $\forall\, a,b,k \in N \;\rightarrow MCD(k \cdot a\,;k \cdot b) = k \cdot MCD(a\,;b)$
- $\forall\, a\,,b,c \in N \rightarrow\ \ MCD(a;c) = 1\ \ e\ \ MCD(b;c) = 1 \leftrightarrow MCD(a \cdot b;\ c) = 1$
- $\forall\, a,b,c \in N \;\rightarrow MCD\,(a\,;\ b\,;\ c) = MCD\,(\,MCD(a\,;b\,);\ c\,) = MCD(a;MCD(b\,;c\,))$

Teorema : Presi comunque due elementi a , b di N_0 (con a > b), il
MCD (a ; b) = MCD (b ; a mod b) oppure MCD (a ; b) = MCD (b ; r)
Dove r è il resto della divisione tra b e a.

Def. di minimo comune multiplo (mcm): Siano a, b $\in N$, si chiama minimo comune multiplo tra a e b : mcm (a ; b), quel numero k $\in N$ tale che

- a | k e b | k
- $\forall c \in N \rightarrow se\ a \mid c\ e\ b \mid c\ allora\ k \mid c$

La prima relazione della definizione ci garantisce che il minimo comune multiplo è un multiplo sia di a che di b: cioè che a e b sono divisori del loro minimo comune multiplo; la seconda che esso è il più piccolo tra i multipli, dovendo dividere tutti i multipli comuni di a e b.

Proprietà del mcm:

- $\forall a, b \in N \rightarrow mcm(a\,;b) = mcm(a\,;b)$
- $\forall a, b, k \in N \rightarrow mcm(k \cdot a\,; k \cdot b) = k \cdot mcm(a\,;b)$
- $\forall a, b, c \in N \rightarrow mcm\,(a\,;\ b\,;\ c) = mcm\,(mcm(a\,;b)\,;\ c) = mcm(a; mcm(b\,;c))$
- $\forall a\,, b \in N \rightarrow mcm\,(a\,;\ b) = \frac{a \cdot b}{MCD(a;\ b)}$

```
program Bezout;
uses crt;
    var  a,b,m,n,c,mcd,r:integer;
         a1,a2,a3,b1,b2,b3,c1,c2,c3,q:integer;
        risp:char;
    begin
     repeat
      clrscr;
      textcolor(15);
      writeln('Questo programma ti permette di verificare il Teorema di Bezout: ');  writeln;
      writeln('Siano A e B due numeri naturali e sia MCD il loro massimo comun');
      writeln('divisore, esistono almeno due numeri relativi x, y tale che :');
      textcolor(12);
      writeln('                MCD(A,B) = x*A + y*B ');
      textcolor(15);
      writeln('cioe" il MCD e" una combinazione lineare di A e B .'); writeln;
      textcolor(14);
      write('Immetti due numeri naturali : ');
      readln(a,b);
      if a<b then
            begin
              c:=a; a:=b; b:=c;
            end;
```

```
 m:=a;  n:=b;  r:=a mod b;
 while r<>0 do
    begin
      a:=b; b:=r; r:=a mod b;
    end;
 mcd:=b;
 writeln('MCD (',m,';',n,') = ',mcd);
 if m mod n <> 0 then
                 begin
                   a1:=m; a2:=1; a3:=0;
                   b1:=n; b2:=0; b3:=1;
                   q:=a1 div b1;
                   repeat
                     c1:=b1;c2:=b2;c3:=b3;
                     b1:=a1-q*b1; b2:=a2-q*b2; b3:=a3-q*b3;
                     a1:=c1;a2:=c2;a3:=c3;
                     q:=a1 div b1;
                   until b1=mcd;
                 end
                else
                 begin
                   b2:=1; b3:=-(m div n - 1);
                 end;
 writeln;writeln;
 textcolor(12);
 writeln(mcd,' = (',b2,')*',m,'+(',b3,')*',n); writeln;
 textcolor(11);
 writeln('x = ',b2,'  e  y = ',b3);
 readln;
 write('Vuoi ripetere con altra coppia di valori ? (S/N) : ') ;
 readl(risp);
until ( risp='n') or ( risp= 'N');
end.
```

B) Numeri primi e scomposizione in fattori primi

Numeri primi:

Def. Un numero naturale p si dice primo se p è maggiore di 1 e se gli unici divisori di p sono 1 e p.

Nella storia della matematica il primo metodo per la ricerca dei numeri primi consiste nell'eliminare dalla sequanza dei numeri naturali tutti i multipli dei numeri 2, successivamente tutti i multipli di 3, poi tutti i multipli di 5 (visto che il 4 è stato eliminato perché multiplo di 2), poi tutti i multipli di 7 (visto che il 6 è stato eliminato perché multiplo del 2) , e così di seguito. Tale metodo è detto del " Crivello di Eratostene ", di cui qui diamo il programma in Pascal.

```
program crivello_di_Eratostene;
uses crt;
const dim=maxint;
type vett=array[1..dim] of boolean;
var  num:vett;
    n,max_ind,nmax,s,q:longint;
    w,z:real;
procedure immetti;
var  i:integer;
begin
 repeat
    write(' Introduci n = ');readln(nmax);
 until (nmax >1) and (nmax<=dim);
 max_ind:=trunc(sqrt(nmax))+1;
 for i:=1 to dim do num[i]:= true;
end;
procedure elimina_multipli(k:integer);
var indice:integer;
begin
 indice:=k;   s:=0;
 while indice<=(nmax-k) do
      begin
        indice:=indice+k;
        num[indice]:=false;
        s:=s+1
      end;
end;
procedure scrivi;
var j:integer;
begin
 q:=0;
 for j:=2 to nmax do
 if num[j] then begin write(j:8);q:=q+1 end;
 writeln;writeln('Il numero dei numeri primi < ',nmax,' Š ',q);
 readln;
end;
begin
 textbackground(1);
 clrscr;
 textcolor(15);
 gotoxy(20,5);write('NUMERI PRIMI: col metodo del CRIVELLO DI ERATOSTENE');
 GOTOXY(3,7);WRITE('Questo programma determina i numeri primi inferiori ad un numero
asseganto');
 gotoxy(3,8);write('col metodo dell''eliminazione successiva di numeri divisibili da 1 fino ad N');
 gotoxy(3,9);write('Inoltre ti determina in approssimazione il numero di questi numeri primi, ');
 gotoxy(3,10);write('dapprima con la formula di Gauss e successivamente con una sua variante.');
```

```
  gotoxy(3,12);
  immetti;
  n:=2;
  repeat
    elimina_multipli(n);
    n:=n+1;
  until n>max_ind;
scrivi;
writeln;
z:=int(nmax/ln(nmax));
write('Il numero dei numeri primi <= ',nmax,' con la formula di Gauss è uguale a ',z:6:0);
writeln;
if (nmax>1) and (nmax<=10) then
w:=int((nmax + (nmax+1)/9)/ln(nmax));
if (nmax>10) and (nmax<=100) then
w:=int((nmax + (nmax+10)/9)/ln(nmax));
if (nmax>100) and (nmax<=1000) then
w:=int((nmax + (nmax+100)/9)/ln(nmax));
if (nmax>1000) and (nmax<=maxint) then
w:=int((nmax + (nmax+1000)/9)/ln(nmax));
writeln('                          mentre con la sua variante è uguale a ',w:3:0);
readln;
end.
```

Un numero naturale $n > 1$ che non sia primo si dice composto. Si denotano con $\mathbb{P}$ i numeri primi e con $\mathbb{N} \setminus \mathbb{P}$ i numeri composti .

Teorema: Due numeri naturali a e b sono primi tra loro o coprimi se e solo se MCD (a ; b) = 1.

Lemma: Se $n \in N$ ed $n > 1$, allora $\exists\, p \in \mathbb{P}$ tale che $p \mid n$

Teorema: Siano $p \in \mathbb{P}$ e a e $b \in N$. Se $p \mid (a \cdot b)$, allora $p \mid a$ e $p \mid b$.

Def. Dato $n \in N_0$, si chiama *fattorizzazione canonica* (o scomposizione in fattori primi) di n il prodotto dei divisori primi presi con il loro grado: cioè

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

con $p_i < p_j$ se i < j, $p_i \in \mathbb{P}$ e $\alpha_i \in N \; per \; i = 1, 2, \ldots, r$.

Teorema fondamentale dell'aritmetica: Per ogni numero naturale $n > 1$ esiste ed è unica la sua fattorizzazione canonica.

Il teorema fondamentale dell'aritmetica afferma che ogni numero naturale si può scomporre, in modo unico (a meno dell'ordine dei fattori)nel prodotto di numeri primi ma non fornisce un metodo per ottenere tale fattorizzazione.

Un metodo per fattorizzare un numero naturale *n* è quello di dividerlo per la sequenza dei numeri primi inferiori a $\frac{n}{2}$. Tale procedimento è però laborioso, anche per i più sofisticati sistemi di calcolo computerizzato, quando il numero è di una certa grandezza.
Molti famosi matematici: quali Fermat, Eulero, Legendre, Gauss, hanno inventato dei metodi per ridurre la quantità di tentativi necessari per scomporre un numero in fattori primi, alcuni dei quali sono oggi alla base di algoritmi per la fattorizzazione di un numero.

```
program scomposizione_in_fattori_primi;
uses crt;
var   n,n1,b,y,y1,k,i,r,w,s:integer;
      t:boolean;
      risp:char;
      m,a,q,b1,p:array[1..1000] of integer;
procedure numeroprimo(x:longint);
var i:longint;
begin
 i:=1;
 repeat i:=i+1 until x mod i = 0;
 if (i=x)
           then y1:=1
           else y1:=0;
end;
begin
 repeat
 textbackground(1);
 clrscr;
 textcolor(15);
 gotoxy(1,2);
 writeln('Questo programma ti permette di scomporre in fattori primi un numero');
 writeln('naturale n ');
 writeln;
 textcolor(12);
 write('Immetti un numero naturale n : ');
  readln(n); n1:=n;
  numeroprimo(n);
  if (y1=1) then
    begin
      writeln; writeln; textcolor(10);
      write('Scomposto in fattori primi risulta: ');
      write(n,' = ',n,'^1');
    end
```

```
   else
    begin
     if (y1=0) then n1:=n div 2;
     w:=0;
     gotoxy(3,7);
     textcolor(30);
     write('Attendere prego, sto elaborando !!');
     for i:=2 to n1   do
       begin
        numeroprimo(i);
        if y1=1 then
            begin
              w:=w+1;
              p[w]:=i;
            end;
       end;
    textcolor(10);
    writeln;writeln;
    write('Scomposto in fattori primi risulta: ');
    b:=n;
    s:=0;
    for k:=1 to w do
      begin
        t:=false;
        for i:=1 to k-1 do
           if p[k]/p[i]=int(p[k]/p[i]) then t:=true;
           if t=false then
                      begin
                        s:=s+1;
                        a[s]:=p[k];
                      end;
      end;
write(b,' = ');
 i:=0;
    for k:=1 to s do
      begin
        r:=0;
         repeat
           if (n mod a[k] = 0) then begin
           r:=r+1;
           n:=n div a[k]; end;
             until (n mod a[k] <>0) or (r=0);
             if r<>0 then
```

```
            begin
              i:=i+1;
              write(a[k],'^',r,' ú ');
              q[i]:=a[k];
              b1[i]:= r;
            end;
     end;
   gotoxy(3,7); writeln('                              ');
  end;
  textcolor(11);
  gotoxy(3,18);
  write('Vuoi proseguire con altro numero n ? (S/N) ');
  readln(risp);
  until (risp='n') or (risp='N');
 end.
```

Siano a e $b \in N$, con a > 1 e b > 1; siano $\prod_{i=1}^{r} p_i^{\alpha_i}$ e $\prod_{i=1}^{s} p_i^{\beta_i}$ le fattorizzazioni canoniche rispettivamente di a e di b , con $r \geq s$:

- MCD (a ; b) = $\prod(p_a \cap p_b)^{\min(\alpha_i;\, \beta_i)}$
- mcm(a ; b) = $\prod(p_a \cup p_b)^{\sup(\alpha_i;\, \beta_i)}$

La prima relazione stabilisce che per determinare il MCD tra a e b si esegue la scomposizione in fattori primi dei due numeri a e b e quindi si opera il prodotto dei fattori primi comuni con il minimo esponente; la seconda stabilisce che per determinare il mcm tra a e b si esegue la scomposizione in fattori primi dei due numeri a e b e quindi si determina il prodotto dei fattori primi comuni e non comuni con il massimo esponente.

1)

```
program numeri_primi; (* in un dato intervallo distinti nelle forme  4k+1 e 4k-1 *)
uses crt;
var j,a,b,y,h,k,m,xmin,xmax:longint;
    risp:char;
procedure numeroprimo(x:longint);
var i:longint;
begin
 i:=1;
 repeat
   i:=i+1
until x mod i = 0;
if (i=x) and (x>=xmin) and (x<=xmax)  then
       begin
          write(x:20);
          y:=1
         end
```

```
          else y:=0;
end;
begin
  repeat
    textbackground(1);
    clrscr;
    textcolor(15);
    writeln(' Questo programma ti permette di determinare i numeri primi in un dato');
    writeln(' intervallo e di distinguerli in due categorie :quelli della forma ');
    writeln(' 4*k-1 e quelli della forma 4*k+1 ');
    writeln;
    textcolor(12);
    write('Immetti l''estremo inferiore ( >= 4 ) dell''intervallo: inf =  ');readln(xmin);
    write('Immetti l''estremo superiore dell''intervallo: sup =  ');readln(xmax);
    writeln;
    textcolor(10);
    k:=0;    h:=0;
   for j:=xmin div 4 to xmax div 4  do
         begin
           a:= 4*j-1;
           b:=4*j+1;
           numeroprimo(a);   k:=k+y;
           numeroprimo(b);   h:=h+y;
        end;
   writeln;
   m:=k+h;
   writeln('Il numero dei numeri primi da ',xmin,' a ',xmax,' è ',m);
   writeln;
   textcolor(14);
   writeln('Sono della forma 4*k-1: ');
   for j:=xmin div 4 to xmax div 4  do
      begin
        a:= 4*j-1;
       numeroprimo(a);
      end;
   writeln;writeln;
   writeln('Sono della forma 4*k+1: ');
    for j:=xmin div 4 to xmax div 4  do
     begin
       b:= 4*j+1;
       numeroprimo(b);
     end;
   writeln;writeln;
   textcolor(13);
   writeln('NB. Tutti i numeri primi è possibile decomporli in differenza di quadrati');
   writeln('ma solo quelli della forma 4*k+1 è possibile decomporli in somma di due');
   writeln('quadrati. Per la verifica vedi il programma Congettura di Girard ');
```

```
   writeln;
   write('Vuoi continuare con altro intervallo ? (S/N) ');
   readln(risp);
  until (risp='n') or (risp='N');
end.
```

Alla fine di quest'ultimo programma è presente la proposizione " tutti i numeri primi è possibile decomporli in differenza dei quadrati di due numeri interi, ma solo quelli della forma 4k+1 è possibile decomporli in somma di due quadrati " . Questa affermazione è un corollario del Teorema di Fermat, che a sua volta si fonda su

Teorema: Siano n , a due interi positivi tale che n è un divisore di (a + 1), esistono due interi x , y primi tra loro tale che $x^2 + y^2 = n$.
Corollario: Siano n, a, b tre interi positivi con a e b primi tra di loro ed n divisore di ($a^2 + b^2$), esistono due interi x ed y primi tra di loro tale che $x^2 + y^2 = n$

Teorema di Fermat: Se p è un numero primo con $p \equiv 1$ *mod* 4 : cioè della forma 4k+1 , allora esistono due interi x , y tale che $x^2 + y^2 = 1$.

I seguenti due programmi verificano rispettivamente il primo il Teorema e d il corollario enunciati sopra, mentre il secondo il Teorema di Fermat.

```
program Teorema_e_corollario;
uses crt;
var i,j,k,k1,p,a,q,x,y:longint;
   m:array[1..1000] of longint;
   risp:char;
function mcd(p,q:longint):longint;
var resto:longint;
begin
  resto :=p mod q;
  while resto<>0 do
     begin
       p:=q; q:=resto;
       resto:=p mod q
     end;
  mcd:=q;
end;
procedure numero(v:longint);
var n,r:longint;
begin
 k:=0 ;
 for n:=v downto 1 do
      begin
```

```
     r:= v mod n;
         if r = 0 then
           begin k:=k+1; m[k]:= v div n;end;
       end;
end;
begin
repeat
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma determina i divisori ( d<>1 ) della somma dei quadrati di due');
 writeln('numeri naturali assegnati, tali che siano primi tra loro, e verifica che ');
 writeln('esistono almeno due numeri interi ( a , b ) tali che  d = aý+ bý ');
 writeln;
 textcolor(12);
 repeat
 write('Inserisci il primo numero intero positivo x = ');readln(x);
 write('Inserisci il secondo numero intero positivo y = ');readln(y);
 writeln;
 until mcd(x,y)=1;
 a:=x*x+y*y;
 textcolor(10);
 numero(a);
 writeln('I divisori di ',a,' sono: ');
 for j:=1 to k do
  write('   ',m[j]:8); writeln;
 writeln;writeln('Infatti ');writeln;
 k1:=1;
 repeat
   for i:=1 to round(sqrt(m[k1])) do
    for j:=1 to i do
     if (mcd(i,j)=1) and (i*i+j*j=m[k1]) then
       begin
         writeln('La coppia (',i,';',j,') verifica che il divisore ',m[k1],' = ',i*i,' + ',j*j);
       end;
     k1:=k1+1;
     if k mod 20 = 0 then readln;
 until (k1=k+1);
 writeln;writeln;
 textcolor(29);
 write('Vuoi continuare con altra scelta ? (S/N) ');
 readln(risp);
until (risp='N') or (risp='n');
end.
```

```
program teorema_di_Fermat_sulla_decomponibilta_in_somma_di_quadrati;
uses crt;
var k,i,j,h,p,w,sup,inf:longint;
    m,n:array[1..100] of longint;
    risp:char;
function mcd(p,q:longint):longint;
var resto:longint;
begin
   resto :=p mod q;
   while resto<>0 do
      begin
        p:=q; q:=resto;
        resto:=p mod q
      end;
   mcd:=q;
end;
procedure primo(x:integer);
var i:integer;
begin
  k:=0;
  for i:=2 to x div 2 do
      if x mod i = 0 then k:=k+1;
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln;
  writeln('  Questo programma ti permette di individuare dapprima i numeri di un');
  writeln('  determinato intervallo che sono somma dei quadrati di due numeri ');
  writeln('  interi positivi, che sono primi tra loro; successivamente individua ');
  writeln('  tra questi i numeri primi, dichiarando la proprietà che li individua.');
  writeln;
  textcolor(10);
  write('  Immetti l''estremo inferiore dell''intervallo : inf = ');
  readln(inf);
  write('  Immetti l''estremo superiore dell''intervallo : sup = ');
  readln(sup);
  writeln;
  h:=1;
   for p:=inf to sup do
     begin
      primo(p);
```

```
   if k=0 then
        begin m[h]:=p;
              h:=h+1 ;
        end;
   end;
textcolor(15);
writeln;
writeln('  Ecco tutti i numeri compresi nell''intervallo [',inf,' ; ',sup,']');
writeln('  che sono somma dei quadrati di due numeri primi tra loro :');
textcolor(12);
k:=0;
for p:=inf to sup do
 for i:=1 to round(sqrt(sup)) do
  for j:=1 to i do
   if (i*i+j*j=p) and (mcd(i,j)=1) then
           begin
             k:=k+1;
             n[k]:=p;
           end;
write('  ');
for i:=1 to k-1 do
       write(n[i],'  ;  ');
write(n[k]);
writeln;writeln;
textcolor(15);
writeln('  Ecco tra questi i numeri primi che sono somma di due quadrati');
textcolor(12);
k:=0;
for w:=1 to h-1 do
 for i:=1 to round(sqrt(m[h-1])) do
  for j:=1 to i do
   if (i*i+j*j=m[w]) and (mcd(i,j)=1) then
           begin
             k:=k+1;
             n[k]:=m[w];
           end;
write('  ');
for i:=1 to k-1 do
      write(n[i],'  ;  ');
writeln(n[k]);
writeln;
textcolor(15);
writeln('  Questi numeri primi sono caratterizzati dalla propriet…: ');
writeln('                 p ≡ 1 mod 4                          ');
```

```
writeln('  cioè: questi numeri divisi per 4 danno resto 1 ');
 writeln;
 writeln('  Da qui la proposizione dimostrata da Fermat, che dice:');
 writeln('  Se p è un numero primo tale p ≡1 mod 4, allora esistono due');
 writeln('  numeri interi ( s ; t ) tali che  s^2+ t^2 = p ');
 writeln;
 writeln(' INVIA per continuare e attendere la fine del calcolo!!');
 readln;
 writeln(' Ecco le coppie relative ai numeri primi indicati a fianco ');
 textcolor(12);
 for w:=1 to h-1 do
    begin
     if (m[w]-1) mod 4 = 0 then
       for i:=1 to m[w] do
        for j:=1 to i do
         if (mcd(i,j)=1) and (i*i+j*j=m[w]) then
            writeln('  la coppia (',i,';',j,') -----> ',m[w],' = ',i*i,' + ',j*j);
    end;
 writeln;
 textcolor(14);
 write('     Vuoi modificare l''intervallo di ricerca ? (S/N) ');
 readln(risp);
until (risp='N') or (risp='n');
end.
```

Il seguente programma calcola i numeri primi in un certo intervello e li distingue nelle forme 6k + 1 e 6k - 1

```
program numeri_primi_di_Leibniz;  (* in un dato intervallo distinti nelle forme  6k+1 e 6k-1 *)
uses crt;
var j,a,b,y,h,k,m,xmin,xmax:longint;
   risp:char;
procedure numeroprimo(x:longint);
var i:longint;
begin
 i:=1;
 repeat
    i:=i+1
 until x mod i = 0;
 if (i=x) and (x>=xmin) and (x<=xmax)  then
      begin
        write(x:20);
        y:=1
      end
      else y:=0;
```

```
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln(' Questo programma ti permette di determinare i numeri primi in un dato');
  writeln(' intervallo e di distinguerli in due categorie :quelli della forma ');
  writeln(' 6*k-1 e quelli della forma 6*k+1 ');
  writeln;
  textcolor(12);
  write('Immetti l''estremo inferiore ( >= 6 ) dell''intervallo: inf =  ');readln(xmin);
  write('Immetti l''estremo superiore dell''intervallo: sup =  ');readln(xmax);
  writeln;
 textcolor(10);
  k:=0; h:=0;
  for j:=xmin div 6 to xmax div 6  do
    begin
      a:= 6*j-1;
      b:=6*j+1;
      numeroprimo(a); k:=k+y;
      numeroprimo(b); h:=h+y;
    end;
    writeln;
    m:=k+h;
    writeln('Il numero dei numeri primi da ',xmin,' a ',xmax,' Š ',m);
    writeln;
    textcolor(14);
    writeln('Sono della forma 6*k-1: ');
   for j:=xmin div 6 to xmax div 6  do
           begin
               a:= 6*j-1;
               numeroprimo(a);
           end;
    writeln;writeln;
    writeln('Sono della forma 6*k+1: ');
     for j:=xmin div 6 to xmax div 6  do
           begin
              b:= 6*j+1;
             numeroprimo(b);
           end;
    writeln;writeln;
    textcolor(12);
    write('Vuoi continuare con altro intervallo ? (S/N) ');
    readln(risp);
  until (risp='n') or (risp='N');
end.
```

2)

```
program densita_numeri_primi_e_quadrati;
uses crt;
var  n,k,y,i,h:longint;
       risp:char;
procedure qua(x:longint);
begin
    if sqr(round(sqrt(x)))=x then
                                    begin
                                       write(x:10);
                                       k:=1
                                    end
                                   else k:=0;
end;
procedure numeroprimo(x:longint);
var i:longint;
begin
     i:=1;
     repeat
         i:=i+1
     until x mod i = 0;
     if (i=x) and (x<=n)   then
                                  begin
                                     write(x:10);
                                     y:=1
                                  end
                                 else y:=0;
end;
begin
    textbackground(1);
    clrscr;
    textcolor(15);
    writeln('Questo programma ti permette di verificare che nella successione');
    writeln('dei numeri naturali, qualunque sia l''estremo superiore di tale');
    writeln('successione, i numeri primi sono più numerosi rispetto ai quadrati');
    writeln('perfetti presenti in tale successione.');
    writeln;
   repeat
      textcolor(12);
      write('Immetti l''estremo dell''intervallo dove vuoi verificare  n= ');
      readln(n);
      textcolor(10);
      h:=0;
      for i:=2 to n do
                          begin
                             numeroprimo(i);
                             if y=1 then h:=h+1;
                           end;
```

```
 writeln;
    writeln('I Numeri primi nell''intervallo [1 ; ',n,'] sono ',h);
    h:=0;
    writeln;
    for i:=1 to n do
                        begin
                            qua(i);
                            if k=1 then h:=h+1;
                        end;
    writeln;
    writeln('I Numeri quadrati nell''intervallo [1 ; ',n,'] sono ',h);
    writeln;writeln;
    write('Vuoi continuare inserendo un nuovo estremo ? (S/N) ');
    readln(risp);
  until (risp='n') or (risp='N');
end.
```

4)

```
program di_sintesi_sui_divisori_col_metodo_della_scomposizione_in_fattori_primi;
uses crt;
var n,k,b,i,y,r,p,t1,n1,s,j:longint;
   a,b1,m,q:array[1..1000] of longint;
   t:boolean;
function pot(x,y:integer):integer;
begin
  if y=0 then pot:=1
        else pot:=x*pot(x,y-1);
end;
procedure divisori(y:integer);
var i:integer;
begin
   for i:=1 to y do
        if (y/i)=int(y/i) then write('   ',i);
end;
begin
 clrscr;
 textcolor(14);
 writeln('Questo programma ti permette di determinare i divisori di un numero ');
 writeln('naturale, la sua scomposizione in fattori primi; esso calcola il  ');
 writeln('il numero dei divisori e la somma di questi divisori col metodo delle');
 writeln('esponenti della scomposizione. Es.: 540 = 2^2·3^3*5^1  il numero dei ');
 writeln('suoi divisori è: (2+1)(3+1)(1+1)=24, dove 2,3,1 sono gli esponenti');
 writeln('della scomposizione; mentre la somma dei divisori è: (1+2^1+2^2)(1+3^1+');
 writeln('3^2+3^3)(1+5^1)=1680, dove tra parentesi figurano tutte le potenze dei ');
 writeln('fattori fino all''ordine indicato dall''esponente della scomposizione.');
 writeln;
 textcolor(2);
```

```
write('Immetti un numero positivo : ');
readln(n); n1:=n;
textcolor(12);
writeln;
write('I divisori di ',n1,' sono:');
divisori(n1);
writeln; writeln;
write('Scomposto in fattori primi risulta: ');
b:=n;
y:=0;
for k:=2 to n do
    begin
      t:=false;
      for i:=2 to k-1 do
          if k/i=int(k/i) then t:=true;
          if t=false then
                    begin
                      y:=y+1;
                      a[y]:=k;
                    end;
     end;
 write(b,' = ');
 i:=0;
 for k:=1 to y do
   begin
     r:=0;
      repeat
        if (n mod a[k] = 0) then begin
        r:=r+1;
        n:=n div a[k]; end;
          until (n mod a[k] <>0) or (r=0);
          if r<>0 then begin
          i:=i+1;
     write(a[k],'^',r,' ú ');
     q[i]:=a[k];
    b1[i]:= r;
    end;
  end;
  writeln;
  t1:=i;
  p:=1;
 for k:=1 to i do
       p:=p*(b1[k]+1);
   writeln;
   writeln('Il numero dei divisori propri ed impropri di ',n1,' sono ',p);
 for k:=1 to t1 do
 begin
  s:=0;
```

```
for i:=0 to b1[k] do
    s:=s+pot(q[k],i);
  m[k]:=s;
end;
p:=1;
for k:=1 to t1 do
    p:=p*m[k];
    writeln;
writeln('La somma di tutti i divisori del numero ',n1,' è ',p);
readln;
end.
```

C) Aritmetica modulare ed equazione modulare.

Aritmetica modulare

A due anni dalla pubblicazione (1799) della tesi di dottorato, Gauss pubblicò la sua opera più famosa, un trattato scritto in latino sulla teoria dei numeri dal titolo *Disquisitiones arithimeticae*. A quest'opera si deve principalmente la terminologia e le notazioni di quella branchia della teoria dei numeri: detta Algebra delle Congruenze o Aritmetica modulare. La trattazione si apre con la definizione:
" Se un numero a è divisore della differenza tra due numeri b e c, allora b e c si dicono numeri congrui altrimenti non congrui, e lo stesso numero a viene chiamato modulo. Ciascuno dei due numeri viene detto residuo dell'altro nel primo caso e non residuo nel secondo caso "
La notazione adottata da Gauss era quella che è ancora oggi in uso, pertanto possiamo dare la seguente definizione:
Def. Siano $a, b, m \in N$, si dice che a è *congruente* a b *modulo* m se m è un divisore di $(a - b)$: in simboli scriviamo:

$$a \equiv b \ (\mathrm{mod}\ m) \ \Leftrightarrow \ m \mid (a - b)$$

Egli costruì un'algebra basata sulla relazione di *congruenza* denotata con " ≡ ", analoga alla comune algebra fondata sulla relazione di *uguaglianza* denotata con " = ".
Alcune, anche se non tutte, delle regole dell'algebra ordinaria possono essere estese alla nuova algebra:

- Non vale la legge di semplificazione: in algebra ordinaria se a x = a y con a≠ 0, allora x = y, nell'algebra delle congruenze non è detto che se a x ≡ a y (mod m) con a≠ 0 , allora x≡ y (mod *m*) : esempio
  $3 \cdot 4 \equiv 3 \cdot 7 \ (\mathrm{mod}\ 9)$ semplificando per 3 si ha $4 \equiv 7 \ (\mathrm{mod}\ 9)$ che risulta falso
  La legge vale nei casi in cui a ed m sono coprimi:cioè MCD(a ; m) = 1
  Esempio
  $34 \equiv 16 \ (\mathrm{mod}\ 9) \ \rightarrow \ 2 \cdot 17 \equiv 2 \cdot 8 \ (\mathrm{mod}\ 9)$ semplificando per 2 si ha $17 \equiv 8 \ (\mathrm{mod}\ 9)$ che risulta vero

- Non vale la legge di annullamento in generale: in algebra ordinaria se x· $y = 0$, allora o x=0
  o y=0 , nell'algebra delle congruenze non è detto che se x· $y \equiv 0 \pmod{m}$, allora o x≡ $0 \pmod{m}$ o $y \equiv 0 \pmod{m}$: esempio
  $30 \equiv 0 \pmod{15} \rightarrow 6 \cdot 5 \equiv 0 \pmod{15}$ ora $6 \equiv 0 \pmod{15}$ e $5 \equiv 0 \pmod{15}$ sono false.
- Nell'algebra ordinaria l'equazione lineare a x + b = 0 ammette una ed una sola soluzione;
  nell'algebra delle congruenze l'equazione $ax + b \equiv 0 \pmod{m}$ può avere più soluzioni
  Es.
  $3 \cdot x + 12 \equiv 0 \pmod{8} \rightarrow x = 4, x = 8, x = 12, \ldots$
  $4 \cdot x + 3 \equiv 0 \pmod{5} \rightarrow x = 8, x = 13, x = 18, \ldots$

Proprietà relative alla congruenza modulare

Siano $m, a, b, c, d \in N$, si verificano le seguenti relazioni:

- $a \equiv a \pmod{m}$ → proprietà riflessiva
- $se\ a \equiv b \pmod{m}$, allora $b \equiv a \pmod{m}$ → proprietà simmetrica
- $se\ a \equiv b \pmod{m}\ e\ b \equiv c \pmod{m},\ allora\ a \equiv c \pmod{m}$ → proprietà transitiva
- $se\ a \equiv b \pmod{m}\ e\ c \equiv d \pmod{m}$, allora $(a + c) \equiv (b + d) \pmod{m}$
- $se\ a \equiv b \pmod{m}\ e\ c \equiv d \pmod{m}$, allora $(a \cdot c) \equiv (b \cdot d) \pmod{m}$

Da un'analisi della definizione e delle proprietà della *congruenza* si nota che essa è una relazione binaria ed inoltre è una relazione di equivalenza su N o su un suo sottoinsieme A. Pertanto introduce in N o in A una partizione e di conseguenza suddivide gli insiemi in classi di equivalenza: se $a \in A$ è un generico elemento della classe, la classe viene indicata con $[a]_m$

Def. $[a]_m = \{x \in A \mid x \equiv a \pmod{m}\}$

Operazioni fra classi:

- $[a]_m + [b]_m = [a + b]_m$
- $[a]_m \cdot [b]_m = [a \cdot b]_m$

Equazione modulare

Def. Un'equazione del tipo $ax \equiv b \pmod{m}$ è detta equazione modulare.

Teorema: L'equazione $ax \equiv b \pmod{m}$ ha soluzioni se e solo se MCD(a; m) è un divisore di b .

Teorema: Se $ax \equiv b \pmod{m}$ ammette soluzione ed x_o è una soluzione, allora $ax \equiv b \pmod{m}$ ha k soluzioni distinte (mod m) con k = MCD (a ; m), date da

$$x_i = x_o + i \cdot \frac{m}{MCD(a\,;m)} \qquad per\ i = 0, 1, 2, \dots, k-1$$

Corollario: L'equazione $ax \equiv 1 \pmod m$ ammette una soluzione se MCD (a ; m) = 1.

Riduzione di potenze nell'aritmetica modulare:

L'aritmetica modulare permette di determinare il resto della divisione di una potenza di base n ed esponente il cui valore è molto grande relativo al divisore *m*: cioè si vuol risolvere l'equazione

$$n^q \equiv x \pmod m$$

col metodo del dimezzamento dell'esponente o applicando il Teorema di Eulero

a) Metodo del dimezzamento dell'esponente

Se n>m, allora ad n assegno r il resto della divisione di n per m; tale da rendere la base della congruenza modulare minore del modulo m. Quindi possiamo senz'altro partire dalla relazione

$$n^q \equiv x \pmod m$$

con n < m.

- Se q è dispari, pongo $q = 2 \cdot q_1 + 1$. Sostituisco nella congruenza, applicando le regole delle potenze :

  $$n^q = n^{2 \cdot q_1 + 1} = n \cdot (n^2)^{q_1} \equiv x \pmod m$$

  se n^2 > m , sostituisco ad n^2 il resto n_1 della divisione di n^2 per m.

- Se q è pari, pongo $q = 2q_1$. Sostituisco nella congruenza, applicando le regole delle potenze :

  $$n^q = n^{2 \cdot q_1} = (n^2)^{q_1} \equiv x \pmod m$$

  se n^2 > m , sostituisco ad n^2 il resto n_1 della divisione di n^2 per m.

ottenendo due alternative , escludendosi a vicenda:

$$n \cdot n_1^{q_1} \equiv x \pmod m \qquad \text{oppure} \qquad n_1^{q_1} \equiv x \pmod m$$

Il ragionamento effettuato su n^q viene riformulato su $n_1^{q_1}$ e così di seguito, finché l'esponente

$q_r = 1$. Si considera infine il prodotto dei vari n_i posti a fattore nel caso che gli esponenti erano dispari con l'ultima base ad esponente 1, se tale prodotto supera il modulo m si assume come valore della x il resto della divisione di tale prodotto per m. Così si risolve l'equazione modulare.

Esempio.

1) Facciamo un esempio che è possibile verificare con la divisione normale fra numeri naturali: risolvere :

   $$3^7 \equiv x \pmod{17}$$

Risoluzione

$3^7 = 3 \cdot 3^6 = 3 \cdot 9^3 = 3 \cdot 9 \cdot 9^2 = 3 \cdot 9 \cdot 81 = 3 \cdot 9 \cdot 13 = 27 \cdot 13 = 10 \cdot 13 = 130$

Sostituendo nell'equazione modulare il prodotto finale, si ha:

$$130 \equiv x \pmod{17} \quad \rightarrow \quad x = 11$$

Verifichiamo col metodo della divisione:

$3^7 = 2187 \rightarrow \quad 2187 = 128 \cdot 17 + 11 \quad \rightarrow$ il resto della divisione è uguale a quello calcolato col dimezzamento della potenza: seguendo poi le regole delle operazioni sulle classi di congruenza modulare.

2) Risolvere : $2^{48} \equiv x \pmod{13}$

Risoluzione:

$$2^{48} = 4^{24} = 16^{12} = 3^{12} = 9^6 = 81^3 = 3^3 = 3 \cdot 3^2 = 3 \cdot 9^1$$

Sostituendo nell'equazione modulare il prodotto finale, si ha:

$$27 \equiv x \pmod{13} \quad \rightarrow \quad x = 1$$

pertanto $2^{48} \equiv 1 \pmod{13}$.

Mentre nel primo esercizio avevamo la possibilità di operare direttamente con la divisione fra numeri naturali, in questo caso la potenza supera di gran lunga il valore di una normale calcolatrice con undici cifre: in questo contesto l'aritmetica modulare ci permette di determinare il resto.

b) Metodo relativo al Teorema di Eulero:

Il Teorema di Eulero afferma:

"Se n ed m sono due numeri coprimi, allora $n^{\varphi(m)} \equiv 1 \pmod{m}$ "

Si vuole ridurre la potenza n^q , il cui valore di q è molto elevato, nell'equazione modulare

$$n^q \equiv x \pmod{m}$$

Si calcoli la funzione euleriana $\varphi(m)$, si divida q per $\varphi(m)$: $q = k \cdot \varphi(m) + r$; si sostituisca tale espressione nell'equazione modulare

$$n^{k \cdot \varphi(m) + r} \equiv x \pmod{m}$$

Applicando le regole delle potenze come nella comune algebra, si ha

$$\left(n^{\varphi(m)}\right)^k \cdot n^r \equiv x \pmod{m}$$

ma $n^{\varphi(m)} \equiv 1 \pmod{m}$ per il teorema di Eulero, sostituendo, si ha:

$$(1)^k \cdot n^r \equiv x \pmod{m}$$

Che è uguale a $n^r \equiv x \pmod{m}$, riducendo così l'esponente.

Esempio: Si voglia ridurre la potenza modulare $2^{340} \equiv$ x (mod 13) e calcolare il valore di x.

Risoluzione: Intanto MCD (2 ; 13) = 1 ; $\varphi(13) = 12$; 340 = 28· 12 + 4, sostituendo si ha

$$2^{340} = 2^{28 \cdot 12 + 4} \quad = (2^{12})^{28} \cdot 2^4 = 1^{28} \cdot 2^4 = 2^4$$

Sostituendo nell'equazione modulare, si ha

$$2^4 \equiv x \ (mod\ 13)$$

da cui x = 3.

```
Program Teorema_di_Eulero;
uses crt;
var prod,a,b,q,a1,m,n,m1,z,p1,k,i:integer;
   m2:array[1..100] of integer;
function pot(x,y:integer):integer;
begin
 if y = 0 then pot:=1
         else pot:=x*pot(x,y-1);
end;
function mcd(x,y:longint):longint;
begin
 if y=0 then mcd:=x
       else mcd:=mcd(y,x mod y);
end;
Function fi(x:integer):integer;
var k,i:integer;
begin
 k:=0;
 for i:=1 to x do
    if mcd(i,x)=1 then k:=k+1;
 fi:=k;
end;
begin
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma ti permette di ridurre una potenza modulare mediante');
 writeln('il Teorema di Eulero che dice:');
 writeln(' Se a ed n sono due numeri naturali coprimi tra loro, allora a^φ(n) ≡1 (mod n)');
 writeln(' dove  φ(n) è la funzione di Eulero.');
 writeln;textcolor(12);
 repeat
 write('Immetti la il valore della base dell''equazione modulare  a = ');
 readln(a);
 write('Immetti la il valore del modulo dell''equazione modulare  n = ');
 readln(n);
 until mcd(a,n)=1;
 write('Immetti la il valore dell''esponente dell''equazione modulare  m = ');
 readln(m);
 m1:=fi(n);
```

```
 writeln;textcolor(10);
 writeln('La funzione fi(',n,') = ',m1,' quindi per il teorema di Eulero ');
 writeln('Š verificata la seguente relazione: ',a,'^',m1,' ð 1 ( mod ',n,')');
 b:=m div m1;
 q:=m mod m1;
  writeln(a,'^',m,' = ',a,'^(',m1,'*',b,'+',q,') = (',a,'^',m1,')^',b,'*',a,'^',q,'= (1)^',b,'*',a,'^',q,' =
',a,'^',q);
  write('riducendo cos    la potenza, ma  ');
 a1:=a;
   p1:=q;
  K:=0;
  repeat
    if p1 mod 2 = 0 then
                  begin
                    a1:=sqr(a1);
                    p1:=p1 div 2;
                    if a1>n then a1:=a1 mod n;
                  end
                else
                  begin
                    k:=k+1;
                    m2[k]:=a1;
              p1:=p1-1;
                  end;
  until p1<=0;
  prod:=1;
  for i:=1 to k do begin prod:=prod*m2[i];prod:=prod mod n; end;
  a1:=prod mod n;
 z:=a1 mod n;
 write(a,'^',q,' ≡ ',z,'(mod ',n,'), pertanto si ha');
 writeln;
 writeln(a,'^',m,' ≡ ',z,'( mod ',n,')');
 readln;
 end.
```

Simbolo di Legendre e di Jacobi

Def. Se *p* è un numero primo ed *a* è un intero, allora $\left(\frac{a}{p}\right)$, detto simbolo di Legendre, è uguale

- 0 se *a* è un multiplo di *p*
- 1 se $\exists\, k \in Z$ tale che $k^2 \equiv a \pmod{p}$: cioè *a* è un residuo quadratico (mod *p*)
- -1 se $\nexists\, k \in Z$ tale che $k^2 \equiv a \pmod{p}$: cioè *a* non è un residuo quadratico (mod *p*)

Nel caso che cade la condizione che *p* si un numero primo, ma che in ogni caso sia dispari, il simbolo di Legendre si chiama simbolo di Jacobi. Per non creare confusione:

- Il simbolo $\left(\frac{a}{p}\right)$ con $p \in N \;\; e\; primo$ viene detto di Legendre
- Il simbolo $\left(\frac{a}{n}\right)$ con $n \in N \;\; e\; dispari$ viene detto di Jacobi

Proprietà del simbolo di Legendre: sono proprietà che consentono di velocizzare i calcoli.

1. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
2. Se $a \equiv b \pmod p$, allora $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. Se $p \equiv 1 \pmod 4$, allora $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$

   Se $p \equiv 3 \pmod 4$, allora $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$
5. Se $p \equiv 1\ o\ 7 \pmod 8$, allora $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$

   Se $p \equiv 3\ o\ 5 \pmod 8$, allora $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$
6. Se a è dispari , allora $\left(\frac{a}{2}\right) = 1$

   Se a è pari, allora $\left(\frac{a}{p}\right) = 0$
7. Se q è un numero primo > 2, allora $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

Il simbolo di Jacobi è una generalizzazione del simbolo di Legendre, che utilizza la scomposizione in fattori primi dell'argomento inferiore, visto che perde la condizione che *p* sia primo, ma che rimane la condizione che *p* sia dispari.
Sia n > 2 un numero naturale dispari: sia $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r}$ la sua scomposizione in fattori primi. Per ogni numero intero *a*, il simbolo di Jacobi è:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \left(\frac{a}{p_3}\right)^{\alpha_3} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}$$

Dove $\left(\frac{a}{p_i}\right)^{\alpha_i}$ con p_i primo è il simbolo di Legendre. Si conviene che $\left(\frac{n}{1}\right) = 1$

Proprietà del simbolo di Jacobi.

1) Se *n* è un numero primo, il simbolo di Jacobi è evidentemente uguale al simbolo di Legendre.
2) $\left(\frac{a}{n}\right) \in \{-1\ ;\ 0\ ;\ 1\}$
3) $\left(\frac{a}{n}\right) = 0\ se\ (\ a\ ;\ n\ ) \neq 1$

4) $\left(\frac{a\cdot b}{n}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right)$
5) $\left(\frac{a}{n\cdot m}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{a}{m}\right)$
6) Se $a \equiv b \pmod{n}$, allora $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
7) $\left(\frac{1}{n}\right) = 1$
8) $\left(\frac{a^2\cdot b}{n}\right) = \left(\frac{b}{n}\right) \quad se \ (a;n) = 1$
9) Se $n \equiv 1 \pmod 4$, allora $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = 1$
   Se $n \equiv 3 \pmod 4$, allora $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = -1$
10) Se $n \equiv 1 \ o \ 7 \pmod 8$, allora $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = 1$
   Se $n \equiv 3 \ o \ 5 \pmod 8$, allora $\left(\frac{2}{2}\right) = (-1)^{\frac{n^2-1}{8}} = -1$
11) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)\cdot(-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)}$

NB.

Se $\left(\frac{a}{n}\right) = -1$ allora *a* non è un residuo quadratico di *n*
Se $\left(\frac{a}{n}\right) = 0$ allora (a ; n) > 1
Se $\left(\frac{a}{n}\right) = 1$ allora non si può dedurre che *a* sia un residuo quadratico di *n.*

Pseudoprimo di Eulero e di Eulero-Jacobi

Un numero *n* è detto pseudoprimo di Eulero in base *a*, con MCD (a ; n) = 1 se *n* è dispari non primo e verifica la relazione:

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$$

Questi numeri *n* sono detti pseudoprimi perché tutti i numeri primi verificano tale relazione, in base al teorema di Fermat: infatti, elevando al quadrato ambo i termini della congruenza si ha

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv (\pm 1)^2 \pmod p \quad \rightarrow \quad a^{p-1} \equiv 1 \pmod p$$

Una forma più forte della relazione precedente è

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$$

Dove $\left(\frac{a}{n}\right)$ è il simbolo di Jacobi. Se *n* verifica questa relazione si dice che *n* è pseudoprimo di Eulero-Jacobi.

NB Ogni pseudoprimo di Eulero-Jacobi è anche pseudoprimo di Eulero , ma non vale il viceversa.

Esempio:

1) 9 è pseudo primo di Eulero in base 17 : $17^{4} \equiv 1 \pmod 9$, ma non è pseudoprimo di Eulero- Jacobi: $\left(\frac{17}{9}\right) = -1 \neq 1$.
2) 9 è pseudoprimo di Eulero-Jacobi in base 19: $19^4 \equiv 1 \pmod 9$; $\left(\frac{19}{9}\right) = 1 \rightarrow$

$$19^4 \equiv \left(\frac{19}{9}\right) \pmod 9$$

9 è pseudo primo di Eulero in base 19: $19^4 \equiv 1 \pmod 9$

NB. Ogni pseudoprimo di Eulero è pseudoprimo di Fermat ma non vale il viceversa. Esistono numeri pseudoprimi di Eulero in ogni base: tali numeri sono detti pseudoprimi assoluti di Eulero, questi costituiscono un sottoinsieme dei pseudoprimi assoluti di Fermat. Il più piccolo pseudo-primo di assoluto di Eulero è 1729, mentre quello di Fermat è 561.

CRIPTOGRAFIA E SISTEMI CRIPTOGRAFICI

La criptografia dal greco χρίπτος (nascosto) e γραφός (scrittura) si intende quella tecnica di " criptare " un messaggio, rendendolo incomprensibile a tutti fuorché al suo destinatario: cioè è un modo di comunicazione scritta segreta che può essere letta solo da chi conosce l'artificio usato, detto *chiave*. Si distinguono in

- Scrittura convenzionale, che consiste in frasi di senso compiuto, usate convenzionalmente con significato del tutto diverso;
- Scrittura cifrata, con impiego di simboli alfanumerici di nessun significato apparente e pertanto comprensibile esclusivamente da coloro che possono decifrarle con l'apposita chiave.

Quest'ultima forma è tuttora la più usata, anzi l'avvento dei computer ha ampliato l'uso di tale scrittura dai rapporti diplomatici e militari si è esteso nel campo commerciale: interscambi aziendali, transazioni bancarie e utilizzo di codici che coinvolgono ormai tutti coloro che usano carte di credito, la rete Internet , firma elettronica, ecc.
Sistemi criptografici e analisi criptografica: l'una studia algoritmi sempre più complessi e veloci atti a codificare e decodificare messaggi e a creare " chiavi " sempre più sofisticate, l'altra studia metodi e algoritmi sofisticati atti a decodificare messaggi criptati senza la conoscenza della " chiave " interpretativa, oggi costituiscono dei campi di ricerca sempre più attivi nelle università: in quanto la sicurezza delle informazioni sensibili costituisce uno degli aspetti più importanti delle interrelazioni fra strutture pubbliche e private, così pure l'utilizzo della firma digitale nei documenti di interscambio. Oggi i sistemi più potenti si fondano sull'utilizzo di numeri primi con un numero di cifre elevatissimo, di qui la ricerca di algoritmi potenti e veloci capaci di stabilire se un numero dispari è primo.

PRIMALITA'

La matematica si è sempre interessata allo studio dei numeri primi, cercando di evidenziarne le proprietà e accentuarne le differenze con gli altri numeri naturali detti composti. Oggi molte di queste caratteristiche sono ancora da formalizzare e rimangono delle congetture.
Recentemente sono stati escogitati algoritmo "efficienti" per testare se un intero positivo sia primo. In realtà, l'interesse sull'efficienza computazionale si è diffuso solo negli anni sessanta con l'avvento dei calcolatori elettronici, ma da parecchi secoli, i matematici si sono cimentati nella produzione di algoritmi di primalità, più o meno veloci.
Il più antico algoritmo capace di individuare i numeri primi risale al 240 a.C. ed è il Crivello di Eratostene. Questo algoritmo produce una lista di numeri primi minori od uguali ad un numero intero positivo assegnato, ma con complessità esponenziale rispetto alle dimensioni dell'imput.
Il XVII secolo segna un passo avanti nella ricerca grazie al piccolo Teorema di Fermat. Il Teorema dimostrò una proprietà per tutti i numeri primi, valida anche per alcuni numeri composti (detti di Carmichael), fornendo lo strumento teorico per costruire il primo algoritmo probabilistico della storia: il test di pseudoprimalità di Fermat.
Nel 1975 Diffie ed Hellman presentarono una nuova crittografia, basata su crittosistemi a chiave pubblica, che anziché usare una stessa chiave (mantenuta segreta) da due interlocutori per codificare e decodificare le informazioni, prevedeva due chiavi distinte, una per la codifica (chiave pubblica) ed una per la decodifica (chiave privata e segreta). La chiave privata non poteva essere calcolata " facilmente" a partire dalla chiave pubblica, pertanto solo il possessore della chiave privata era in grado di decodificare le informazioni.
Nel 1978 questo sistema trova la sua applicazione reale. Infatti R.Rivest, A.Shamir e L Helmann, tre ricercatori americani del MIT, hanno saputo implementare tale logica utilizzando particolari proprietà formali dei numeri primi con alcune centinaia di cifre. L'algoritmo da loro inventato, denominato RSA dalle iniziali dei loro cognomi, non è sicuro da un punto di vista matematico teorico, in quanto esiste la possibilità che tramite la conoscenza della chiave pubblica si possa decriptare un messaggio, ma l'enorme mole di calcoli e l'enorme dispendio di tempo necessario per trovare la soluzione, fa di questo algoritmo un sistema affidabile. Tale algoritmo si fonda sul prodotto di due numeri primi con un numero di cifre elevatissimo: tale prodotto costituisce la chiave pubblica. Con tale chiave pubblica vengono trasmessi i messaggi, chi conosce i due numeri primi ,che costituiscono la chiave privata, può decriptare e quindi accedere al messaggio .
L'applicazione pratica di questa teoria incentivò l'uso dei numeri primi: basti pensare che la robustezza della codice crittografico RSA trae origine dalla difficoltà nel fattorizzare un numero, di cui si sa essere il prodotto di due numeri primi.
Quindi stabilire se un numero è primo o composto è utile per la crittografia, quanto per la crittoanalisi. Più la risposa di un algoritmo di primalità è veloce, più l'RSA e altri crittosistemi diventano vulnerabili. Così nello stesso periodo, nascono algoritmi probabilistici polinomiali come l'algoritmo Di Solovay-Strassen (1975) e l'algoritmo di Miller-Rabin (1976)
Gli ultimi decenni vedono il proliferarsi di algoritmi sempre più veloci, tanto da far avanzare l'ipotesi che si possa costruire un algoritmo deterministico e contemporaneamente polinomiale.

Nel 2002 Agrawal-Kayal_Saxena codificano un algoritmo deterministico polinomiale e lo diffondono con un articolo “PRIMES in P” che costituirà la base da cui inizia una successione di miglioramenti che ad oggi ha fornito i più potenti “ Test di Primalità”.

Portiamo qui un esempio di come eseguire una simulazione di codifica e decodifica di un messaggio mediante RSA tra due interlocutori, detti destinatario e mittente. Intanto questi due interlocutori si mettono d’accordo (pubblicamente! o mediante pubblicazione su un giornale oppure su un sito internet accessibile, ecc.) su come trasformare i messaggi in sequenze di numeri ciascun di lunghezza prefissata: sia *m* uno di questi numeri.
Destinatario: Questi prepara la chiave di decifrazione, che consiste nella scelta di due numeri primi che andrà a moltiplicare: siano $p_1 = 1237$ e $p_2 = 13$ i due numeri primi, il loro prodotto è il numero $n = 16081$. Tale numero *n* sarà poi reso pubblico dallo stesso destinatario.
Successivamente sempre il destinatario calcola la funzione $\varphi(n)$ di Eulero :

$$\varphi(16081) = (1237 - 1)(13 - 1) = 14832.$$

E sceglie un numero h tale che MCD (h, $\varphi(16081)) = 1$: sia h = 7; inoltre calcola un valore

numerico d tale che $d \cdot h \equiv 1\ (mod\ \varphi(16081))$: d = 2119. Tale numero h costituisce il secondo numero pubblico reso dal destinatario. Costituiscono numeri strettamente segreti i numeri p_1 , p_2 , d e $\varphi(16081)$: d costituisce la chiave di decodifica.

Il destinatario in definitiva ha preparato la sua chiave d di decodifica, comunicando pubblicamente a tutti coloro che vogliono scrivergli in modo riservato i due numeri n e h.

Mittente: Questi vuole mandare al destinatario il messaggio m = 12 = “ Sto male non vengo, contraffai la mia firma digitale usando il mio codice “ . Questi cripta tale messaggio calcolando

$$m^h = 12^7 \equiv 3340\ (\ mod\ 16081\ )$$

Il mittente comunica pubblicamente al destinatario il messaggio 3340 , che nessuno è in grado di decodificare, tranne il destinatario che è in possesso della chiave d = 2119.

Quando il destinatario riceve il messaggio 3340, questi calcola il valore x dell’equazione modulare $3340^{2119} \equiv x\ (\mathrm{mod}\ 16081)$, ottenendo come valore proprio il numero 12 a cui corrisponde l’espressione concordata precedentemente.

La riduzione dell’ultima potenza viene effettuata con la regola del dimezzamento dell’esponente e la fattorizzazione come esposto precedentemente nel primo capitolo

```
Program RSA;
uses crt;
var  x,x1,y,y1,z,z1,d,h,p1,p2,mo,c,el:longint;
    d1:real;
    m:array[1..10] of char;
    risp:char;
procedure parola;
```

```
 var j:integer;
     x:char;
 begin
   write('Componi con tre lettere dell''alfabeto un messaggio: ');
   for j:=1 to 3 do
           begin
             read(x);
             m[j]:=x;
           end;
   write('Il messaggio letterale Š : ');
   for j:=1 to 3 do begin textcolor(11);write('  ',m[j],' ');end;
   delay(1000);
   writeln;
   writeln('Il calcolatore trasforma tale messaggio in sequenza numerica : ');
   writeln(' ( ',ORD(m[1]),' ; ',ORD(m[2]),' ; ',ORD(m[3]),' ) ');
 end;

Function mcd(e,f:longint):longint;
 begin
    if f=0 then mcd:=e
           else mcd:=mcd(f,e mod f);
 end;

Function fi(e:longint):longint;
 var k,w:longint;
 begin
     k:=0;
     for w:=1 to e do
     if mcd(e,w) = 1 then k:=k+1;
     fi:=k;
 end;

Function TeoEule(a,n,m:longint):longint;
 var a1,prod,i,r,t,q,b,m1:longint;
     m2:array[1..100] of longint;
 begin
     m1:=fi(n);
     b:=m div m1;
     q:=m mod m1;
     a1:=a;
     r:=q;
     t:=0;
     repeat
       if r mod 2 = 0 then
                    begin
                      a1:=sqr(a1);
                      r:=r div 2;
                      if a1>n then a1:=a1 mod n
                    end
                  else
                    begin
```

```
                    t:=t+1;
                    m2[t]:=a1;
                     r:=r-1;
                   end;
    until r <=0;
    prod:=1;
    for i:=1 to t do
          begin
            prod:=prod*m2[i];
            prod:=prod mod n;
          end;
    a1:=prod mod n;
    TeoEule:=a1 mod n;
  end;
begin
 clrscr;
 writeln('  Questo programma ti simula il codice criptografico RSA ');
 writeln;
 textcolor(10);
 write('  Immetti due numeri primi : ');readln(p1,p2);
 mo:=p1*p2;
 writeln(' Primo numero pubblico n = ',mo);
 el:=fi(mo);
 Write('Scegli il fattore h (<p1 e <p2) e rendilo pubblico ');readln(h);
 c:=0;
 repeat
  d1:=(1+c*el)/h;
  c:=c+1;
 until d1=int(d1);
 d:=round(d1);
 textcolor(14);
 parola;
 writeln;
 textcolor(12);
 writeln ('Successivamente lo Cripta e lo spedisce ');
 x:=TeoEule(ord(m[1]),mo,d);
 y:= TeoEule(ord(m[2]),mo,d);
 z:= TeoEule(ord(m[3]),mo,d);
 textcolor(6); writeln;
 writeln('Messaggio criptato Š la sequenza (',x,';',y,';',z,')');writeln;
 textcolor(15);
 Writeln('Tale maessaggio criptato, sotto forma di sequenza numerica, viaggia ');
 writeln('pubblicamente e viene ricevuto dal destinatario che lo decripta con');
 writeln('la chiave segreta d (=',d,') ed il modulo pubblico (', mo,' ):');
 writeln('NB. Sono pure segreti i due numeri primi (',p1,';',p2,') che determinano ');
 writeln('il modulo pubblico  assieme alla funzione euleriana fi(n) = ',fi(mo),'. ');
 x1:= TeoEule(x,mo,h);
y1:= TeoEule(y,mo,h);
 z1:= TeoEule(z,mo,h);
```

```
 textcolor(11);
 writeln;
 writeln('Messaggio ricevuto decriptato Š (',x1,';',y1,';',z1,')');
 write('A cui corriponde il messaggio letterale : ');
 textcolor(14);
 write(m[1],' ',m[2],' ',m[3]);
 writeln;writeln;
 textcolor(15);
 repeat until keypressed;
end.
```

NB. Per l'esecuzione del programma in tempi brevi si consigliano i seguenti valori:

$p_1 = 29$, $p_2 = 17$, h = 13 e d = 69
$p_1 = 37$, $p_2 = 29$, h = 11 e d = 275
$p_1 = 53$, $p_2 = 47$, h = 29 e d = 165
$p_1 = 67$, $p_2 = 59$, h = 19 e d = 403
$p_1 = 97$, $p_2 = 61$, h = 7 e d = 823

TEST DI PRIMALITA'

Un test di primalità è un algoritmo che permette di verificare se un numero dispari è primo o composto. Il primo di questi è il crivello di Eratostene valido per numeri naturali dell'ordine di 10^5. Esso consiste nell'eliminare dalla sequenza dei numeri naturali quei numeri che ammettono divisori propri: cioè il MCD fra il numero *n* e tutti i numeri inferiori a int($\sqrt{n}$) è diverso da 1. Se il numero *n* è dell'ordine di 10^6 o superiore l'algoritmo del crivello diventa alquanto laborioso. Un altro è il piccolo Teorema di Fermat, che afferma " qualunque si la base *a* la relazione $a^{m-1} \equiv 1 \pmod{m}$ è verificata da tutti i numeri primi ". Il difetto di questo teorema sta nel fatto che non vale il suo teorema inverso: infatti esistono numeri non primi che verificano la relazione per qualunque valore della base *a*: tali numeri sono i numeri di Carmichael. Anche il teorema di Fermat è laborioso dovendo svolgere potenze d'ordine elevato.

Teorema di Fermat: Se $p \in \mathcal{P}$, allora $a^p \equiv a \pmod{p}$. Se *p* è coprimo con *a*, allora

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

NB. Nel teorema di Fermat la condizione che *p* sia primo è una condizione necessaria ma non è sufficiente: cioè se è vera $a^{p-1} \equiv 1 \pmod{p}$ non è detto che *p* sia un numero primo. Fu Gauss ha dare significatività al teorema di Fermat: infatti nelle " disquisitiones" egli afferma che, dopo aver dimostrato la costruibilità del poligono regolare con riga e compasso di 17 lati, un poligono regolare di n lati poteva essere costruito con gli strumenti euclidei se e soltanto se il numero n era della forma:

$$n = 2^m \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

dove m è un numero intero positivo qualsiasi e p_i sono numeri primi di Fermat diversi tra loro.

Il Piccolo Teorema di Fermat afferma , come abbiamo detto:

‘ Se p è un numero primo ed a è un numero non divisibile da p ,allora $a^{p-1} - 1$ è divisibile per p’ ‘

Questo teorema per quanti tentativi siano stati fatti non è stato mai falsificato, tuttavia sono stati fatte delle generalizzazioni, tra queste quella che si attestò all’attenzione dei matematici è:
‘ Se p ed a sono numeri interi positivi, esistono degli p, che dividono $a^p – a$, qualunque sia a.
Questa generalizzazione fa cadere le ipotesi del T.di Fermat.
Se p è primo e a soddisfa l’’ipotesi del teorema di Fermat, l’enunciato di questo teorema è verificato da p.
Se p non è primo ed a qualunque e p divide $a^p – a$, allora a p si dà nome di numero pseudoprimo o numero di Carmichael. Nell’insieme dei numeri naturali tali numeri pseudoprimo sono “rari”, tuttavia è stato dimostrato recentemente (1992) da tre matematici americani che l’insieme di tali numeri hanno la potenza del numerabile: cioè sono infiniti. I primi tre numeri pseudoprimo sono 561 , 1105 , 1729 , …

Questo algoritmo ci permette di verificare il piccolo Teorema di Fermat :

- Sia a la base della potenza e p un numero primo con
- $1 \leq a < p$
- $MCD(a\,;p) = 1$: cioè a coprimo con p

Sotto queste condizioni vale la seguente relazione : $a^{p-1} \equiv 1 \pmod{p}$.

a) Prima versione:

```
program Piccolo_teorema_di_Fermat;
{$N+}
uses crt;
var a,p,p1,q,t:longint;
   s:extended;
   risp:char;
function mcd(x,y:longint):longint;
begin
 if y=0 then mcd:=x
       else mcd:=mcd(y,x mod y);
end;
function primo(x:longint):longint;
var i,k: integer;
begin
 k:=0;
 for i:=1 to x div 2 do
   if x mod i = 0 then k:=i;
   if k=1 then primo:=x;
end;
function pot1(x,y:longint):real;
begin
 pot1:=exp(y*ln(x));
end;
function pot(x,y:longint):longint;
begin
```

```
 if y=0 then pot:=1
       else pot:=x*pot(x,y-1);
end;
procedure immissione;
begin
 textcolor(12+blink);
  gotoxy(5,22);write('Attento a non mettere valori di p tali che a^(p-1) sia > 2^32-1');
 gotoxy(1,8);
 textcolor(15);
 write('Immetti il valore della base a = ');readln(a);
 repeat
 write('Immetti il valore dell"esponente p = ');readln(p);
 until (p>1) and (pot1(a,p-1)<2147483647);
 if p=primo(p) then writeln(p,' è un numero primo');
 if mcd(a,p)=1 then writeln(a,' non è divisibile per ',p);
end;
begin
 repeat
 textbackground(1);
 clrscr;
 textcolor(10);
 gotoxy(10,2);writeln('Piccolo TEOREMA DI FERMAT');
 GOTOXY(5,4);writeln('Se p è un numero primo ed a è un numero non divisibile da p');
 gotoxy(5,5);writeln(' allora      a^(p-1) - 1    è divisibile per  p  ');
 writeln;
 immissione;
 p1:=p;
 if (p=primo(p)) and (mcd(a,p)=1) then
      if ((pot(a,p-1)-1)-p*int((pot(a,p-1)-1)/p)) <> 0 then  writeln('Il teoremma di Fermat non è verificato')
                                 else  writeln('Il teoremma di Fermat è verificato')
                               else
                               begin
                              if p<>primo(p) then writeln(p,' non è un numero primo ') else
                                 if (mcd(a,p)<>1) then writeln(a,' non è primo con ',p);
                                 writeln('... e quindi il teorema di Fermat non vale ');
                               end;
                               writeln;
 s:= pot(a,p-1);
 writeln('Infatti ',a,'^',p1-1,' - 1 = ',round(s)-1,' valore che diviso per ',p1,' d… resto  ',(round(s)-1) mod
p1);
 q:=(round(s)-1) div p ; t:= (round(s)-1) mod p;
 writeln(' cioè :  ',round(s)-1,' = ',q,' x ',p,' + ',t );
readln;
write('Vuoi ripetere con altri numeri ? (S/N): ');
readln(risp);
until (risp='n') or (risp='N');
end.
```

b) Seconda versione:

```
program potenza_modulare;
uses crt;
var a,a1,p,p1,b,prod,k,i,d,y:longint;
   m:array[1..1000] of longint;
function mcd(x,y:longint):longint;
begin
  if y=0 then mcd:=x
        else mcd:=mcd(y,x mod y);
end;
procedure numeroprimo(x:longint);
var i:longint;
begin
 i:=1;
 repeat i:=i+1 until x mod i = 0;
 if (i=x)
          then begin y:=1 end
          else y:=0;
end;
30
begin
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma ti permette di verificare il piccolo teorema di Fermat');
 writeln('ed inoltre ti fa notare che esistono dei numeri che pur verificando il ');
 writeln('teorema non sono primi ');
 writeln;
 textcolor(12);
 write('Immetti la base  a = ');readln(a);
 a1:=a;
 write('Immetti il fattore modulare (>a) : p = ');readln(p);
 d:=mcd(p,a);
 numeroprimo(p);
 if y=1 then
       begin
 writeln(p,' è un numero primo e MCD = (',a1,';',p,') = ',d);
 writeln('Verifica il piccolo teorema di Fermat: ');
  end
       else
       begin
     writeln(p,'non è un numero primo e MCD = (',a1,';',p,') = ',d);
 writeln('Non verifica il piccolo teorema di Fermat a meno che MCD=1 ed il ');
 writeln('numero p è un numero pseudoprimo forte o debole che sia')
   end;
 p1:=p-1;
```

```
K:=0;
 repeat
  if p1 mod 2 = 0 then
                begin
                  a:=sqr(a);
                  p1:=p1 div 2;
                  if a>p then a:=a mod p;
                end
               else
                begin
                  k:=k+1;
                  m[k]:=a;
                  p1:=p1-1;
                end;
 until p1<=0;
 prod:=1;
 for i:=1 to k do begin prod:=prod*m[i];prod:=prod mod p; end;
 b:=prod mod p;
 writeln('         ',a1,'^',p-1,' ≡ ',b,'(mod ',p,')');
 if (y<>1) and (d=1) and (b=1) then writeln(p,'  è un numero pseudoprimo nella base ',a1);
 readln;
 end.
```

Non vale il viceversa: cioè se vale la relazione $a^{p-1} \equiv 1 \ (\bmod p)$, con $1 \leq a < p$ e $MCD(\ a\ ;p\ ) = 1$, non è detto che il modulo p sia un numero primo.

L'aritmetica modulare ci permette di ridurre la difficoltà di calcolo per potenze ad esponente elevato

1. Sia 2 la base della potenza e sia 29 il numero primo ($1 \leq 2 < 29$ e $MCD(\ 2\ ;29\ ) = 1$),
   verificare che vale la relazione:
   $$2^{28} \equiv 1 \ (\bmod 29)$$
   Risolviamo l'equazione:
   $$2^{28} \equiv x \ (\bmod 29)$$
   $$2^{28} = 4^{14} = 16^7 = 16 \cdot 16^6 = 16 \cdot 256^3 = 16 \cdot 24^3 = 16 \cdot 24 \cdot 24^2 = 384 \cdot 576 = 7 \cdot 25$$
   Sostituendo nell'equazione modulare il prodotto finale, si ha:
   $$175 \equiv x \ (\bmod 29\ ) \rightarrow \ \ x\ = 1$$
   Quindi è verificato il Teorema di Fermat.

2. Sia 2 la base della potenza e sia 341 ($1 \leq 2 < 341$ e $MCD(\ 2\ ;341\ ) = 1$), controlliamo la relazione del Teorema di Fermat
   $$2^{340} \equiv 1 \ (\bmod 341)$$

Risolviamo l'equazione

$$2^{340} \equiv x \ (\text{mod } 341)$$

$$2^{340} = 4^{170} = 16^{85} = 16 \cdot 16^{84} = 16 \cdot 256^{42} = 16 \cdot 65536^{21} =$$
$$= 16 \cdot 64^{21} = 16 \cdot 64 \cdot 64^{20} = 1024 \cdot 4096^{10} = 1 \cdot 4^{10} = 16^5 =$$
$$16 \cdot 16^4 = 16 \cdot 256^2 = 16 \cdot 65536 = 16 \cdot 64 = 1024$$

Sostituendo nell'equazione modulare il prodotto finale, si ha:

$$1024 \equiv 1 \ (\text{mod } 341) \rightarrow \ x = 1$$

Il numero 341 verifica il Teorema di Fermat. Ma il numero 341 (= 11 · 31) è un numero composto: quindi se vale la relazione $a^{p-1} \equiv 1 \ (\text{mod } p)$, con $1 \leq a < p$ e

$MCD(a\,;p) = 1$, non è detto che il modulo *p* sia un numero primo

Def. Tutti i numeri naturali che verificano il Teorema di Fermat ma non sono primi si dicono *pseudoprimo* nella base *m*

Il numero 341 dell'esempio 2) è uno pseudoprimo nella base 2
Controlliamo la relazione del Teorema di Fermat sempre per il numero 341, questa volta con la base 13:

$$13^{340} \equiv 1 \ (\text{mod } 341)$$

Risolviamo l'equazione

$$13^{340} \equiv x \ (\text{mod } 341)$$

$$13^{340} = 169^{170} = 28561^{85} = 258 \cdot 258^{84} = 258 \cdot 66564^{42} = 258 \cdot 69^{42} =$$

$$= 258 \cdot 4761^{21} = 258 \cdot 328 \cdot 328^{20} = 84624 \cdot 107584^{10} = 56 \cdot 169^{10} = 56 \cdot 28561^5$$
$$=$$
$$56 \cdot 258 \cdot 258^4 = 14448 \cdot 66564^2 = 126 \cdot 69^2 = 126 \cdot 4761 = 126 \cdot 328 = 41328$$

Sostituendo nell'equazione modulare il prodotto finale, si ha:

$$41328 \equiv 67 \ (\text{mod } 341) \rightarrow \ x \neq 1$$

Il numero 341 non verifica il Teorema di Fermat: infatti il numero 341 (= 11 · 31) è un numero composto.
Il numero 341 per alcune basi verifica il Teorema di Fermat senza essere primo, in altre basi non verifica il teorema di Fermat confermando il teorema.
I numeri pseudoprimo si distinguono in pseudo primo deboli e pseudoprimo forti:

Def. Sono numeri pseudoprimo deboli quei numeri naturali che verificano il Teorema di Fermat per alcune basi; mentre sono pseudoprimo forti quelli che verificano il Teorema di Fermat qualunque sia la base della relazione.

I numeri pseudoprimo forti sono detti di Carmichael.

Numeri di Carmichael:

In teoria dei numeri un numero di Carmichael è un numero naturale composto *n* che soddisfa la congruenza:

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n)$$

per tutti i numeri naturali *a* che sono primi con *n* , prendono nome da Robert Carmichael.
Il piccolo teorema di Fermat afferma che tutti i numeri primi hanno quella proprietà. In questo senso i numeri di Carmichael sono simili ai numeri primi. I numeri che per qualche valore di *a* soddisfano tale relazione sono chiamati pseudoprimi di Fermat rispetto alla base *a.* Siccome i numeri di Carmichael soddisfano la relazione qualunque sia la base purché coprimo con *n,* essi si chiamano pseudoprimi assoluti di Fermat.
I numeri di Carmichael rivestono un'importanza notevole perché passano in ogni caso il test di primalità di Fermat pur essendo composti. L'esistenza di tali numeri impedisce di utilizzare il test di Fermat per certificare la primalità di un numero, mentre può essere utilizzato per dimostrare che un numero è composto.

Una definizione alternativa ed equivalente dei numeri di Carmichael è fornita dal seguente teorema di Korselt:

Teorema: Un intero positivo *n* è un numero di Carmichael se e solo se *n* è privo di quadrati, e per ogni divisore primo di *p* di *n*, è vero che *p* – 1 è un divisore di *n* – 1 .

Corollario: Tutti i numeri di Carmichael sono dispari.

Nel 1899 Korselt fu il primo ad osservare questa proprietà, ma non riuscì a trovare un esempio. Nel 1910 Robert Daniel Carmichael trovò il più piccolo numero con questa proprietà, 561, legando così il suo nome a questi numeri.

E' stato dimostrato che i numeri di Carmichael pur essendo rari nella sequenza dei naturali essi sono infiniti.

Prima versione

```
program Numeri_di_Carmichael;
uses crt;
var i,j,k,p,a,s,y,b,q,l,w:longint;
    m,n,r:array[1..1000] of longint;
    risp:char;
procedure numero(v:longint);
 var n,r:longint;
 begin
    k:=0 ;
    for n:=v downto 1 do
                begin
                   r:= v mod n;
                   if r = 0 then
```

```
                                begin
                                   k:=k+1;
                                   m[k]:= v div n;
                                 end;
                    end;
end;
procedure numeroprimo(x:longint);
  var i:longint;
  begin
     i:=1;
       repeat
           i:=i+1
       until x mod i = 0;
    if  (i=x)   then y:=1
                else y:=0;
   end;
begin
    textbackground(1);
    repeat
       clrscr;
       textcolor(15);
       writeln('Questo programma verifica se un numero naturale assegnato');
       writeln('è un Numero di Carmichael');
       writeln;
       textcolor(12);
       write('Inserisci un numero intero positivo a = ');readln(a);
       textcolor(10);
       numero(a);
       writeln('I divisori di ',a,' sono: ');
       for j:=1 to k do write(m[j]:8);
       writeln;
       s:=0;
      writeln('I divisori primi sono: ');
      for j:=2 to k do
              begin
                 b:=m[j];
                 numeroprimo(b);
                if y=1 then
                          begin
                            s:=s+1;
                            n[s]:=b;
                            write(b:5);
                          end;
                end;
    writeln;
    p:=0;  w:=0;
    for i:=2 to k-1 do
```

```
  if (a mod sqr(m[i])) = 0 then w:=w+1;
    for j:=1 to s do
        if (((a-1) mod (n[j]-1)) <> 0)  then p:=p+1;
 if (p = 0) and (w = 0) and ( a <> n[j]) then  write(a,' è un numero di Carmichael;')
                    else  write(a,' non è un numero di Carmichael;');
    gotoxy(3,20);write('Vuoi continuare la verifica inserendo un altro numero ? (S/N) ');
   readln(risp);
 until (risp='n') or (risp='N');
end.
```

Seconda versione

```
program Numeri_di_Carmichael;
uses crt;
var i,j,k,p,a,s,y,b,q,l,w,e,xmin,xmax,z:longint;
      m,n,r:array[1..1000] of longint;
      risp:char;
procedure car(d:longint);
  procedure numero(v:longint);
    var n,r:longint;
    begin
      k:=0 ;
      for n:=v downto 1 do
            begin
              r:= v mod n;
              if r = 0 then
                        begin
                          k:=k+1;
                          m[k]:= v div n;
                        end;
            end;
    end;
 procedure numeroprimo(x:longint);
   var i:longint;
   begin
     i:=1;
     repeat
        i:=i+1
     until x mod i = 0;
     if  (i=x)   then y:=1
                 else y:=0;
   end;
begin
   a:=d;
   numero(a);
   s:=0;
   for j:=2 to k do
            begin
```

```
            b:=m[j];
            numeroprimo(b);
            if y=1 then
                    begin
                       s:=s+1;
                       n[s]:=b;
                    end;
          end;
 end;
begin
   textbackground(1);
   repeat
     clrscr;
     textcolor(15);
     writeln('Questo programma determina i numeri di Carmichael in un intervallo');
     writeln(' di numeri naturali assegnato, se esistono.');
     writeln;
     textcolor(12);
     write('Immetti l" estremo inferiore dell"intervallo: inf = ');readln(xmin);
     write('Immetti l"estremo superiore dell"intervallo : sup = ');readln(xmax);
     writeln;
     textcolor(29);
     gotoxy(3,7);writeln('Attendere prego, sto eleborando !! ');
     textcolor(12);
     writeln;
    for e:=xmin to xmax do
                  begin
                     car(e);
                     p:=0;  w:=0;
                    for i:=2 to k do
                              if (a mod sqr(m[i])) = 0 then w:=w+1;
                    for j:=1 to s do
                              if (((a-1) mod (n[j]-1)) <> 0)  then p:=p+1;
                   if (p = 0) and (w = 0) and ( a <> n[j] )then
                                                  writeln (a,' è un numero di Carmichael;');
                    end;
    gotoxy(3,7);write('    Fine ricerca                  ');
    gotoxy(3,20);write('Vuoi continuare in un altro intervallo ? (S/N) ');
    readln(risp);
   until (risp='n') or (risp='N');
end.
```

NB Tutti i Test di Primalità fondati sul teorema di Fermat vengono fatti fallire dai numeri di Carmichael.

Un test che risolve il problema dei numeri di Carmichael è quello di Solovay-Strassen. Esso consiste:

“ Sia *n* un intero dispari, si scelgano delle basi *a* in maniera casuale, si controlla se vale:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \quad \text{con } \left(\frac{a}{n}\right) \text{ il simbolo di Jacobi}$$

Se troviamo un *a* per cui tale congruenza non è verificata allora *n* non è pseudoprimo di Eulero rispetto ad *a* e quindi non è primo. “

Da questo teorema si può costruire il test di primalità:

1) Assegnare ad *n* un valore dispari
2) Scegliere a caso un valore $a \in [2\,;n-1]$ come base
3) Calcolare $a^{\frac{n-1}{2}}$ e $\left(\frac{a}{n}\right)$
4) Controllare se $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$

Se tale congruenza è falsa allora concludere che *n* è composto, se invece la congruenza vale si torna la punto 2). L’esecuzione dell’algoritmo termina quando si è provato che *n* è composto oppure dopo che sono state fatte k scelte al punto 2) (dove k è il numero di basi da estrarre casualmente). Se l’algoritmo non termina dichiarando che *n* è composto, si ha che *n* o è primo o è pseudoprimo di Eulero nelle k-basi testate e , quindi la probabilità che *n* sia primo è maggiore di $1-\frac{1}{2^k}$.

```
Program SOLOVAY-STRASSEN ;
{$N+}
uses crt;
var n,k,h,i,p,b:longint;
   q,a,c,d:extended;
   risp:char;
function pot(x:extended; y:longint):extended;
begin
  if y=0 then pot:=1
        else pot:=x*pot(x,(y-1));
end;
begin
 repeat
  textbackground(1);
  clrscr;
  textcolor(15);
  randomize;
  writeln('           TEST DI PRIMALITA" DI SOLOVAY-STRASSEN ');
  writeln('Questo programma ti permette di stabilire ( entro i margini del');
  writeln('simulatore matematico installato nel computer ) se un numero è primo');
  writeln('col metodo di Solovay-Strassen, fondato sul calcolo delle probabilita;');
  writeln('con estrazione a caso delle basi della potenza a^[(n-1)/2]. ');
```

```
 writeln;
 textcolor(12);
 write('Immetti un numero intero positivo dispari (<= 43): n = ');readln(n);
 write('Immetti il numero di estrazioni delle basi casuali da 2 al 10: ');
 readln(p);
 writeln;
 textcolor(10);
 k:=0; h:=0;
 for i:=1 to p do
  begin
  a:=random(8)+2.0;
 b:=(n-1) div 2;
 c:=pot(a,b);
 d:=((c/n-int(c/n))*n) ;
 if ((0.99<d) and (d<1.11)) or (((n-1.11)<d) and (d<(n-0.99))) then k:=k+1
                                                  else h:=h+1;
  end;
  writeln;
  q:=1.0 - 1/pot(2,k);
  if h<k then write(n,' probabilmente è un numero primo con probabilità > ',q:5:5)
        else writeln(n,' è un numero composto ');
 writeln; writeln;
 textcolor(14);
 write('Vuoi continuare con altro numero dispari ? (S/N) : ');
 readln(risp);
until (risp='n') or ( risp='N');
end.
```

Un altro test probabilistico che risolve il problema dei numeri diCarmichael è quello escogitato dai due matematici americani Miller e Rabin .

```
Program Miller_Rabin;
{$N+}
uses crt;
var   a,s,x,m,i,j,mo,mo1,vo,q:longint;
      p:array[1..100] of longint;
      k,k1:extended;
      t:boolean;
function pot(x,y:longint):extended;
begin
   if y=0 then pot:=1
          else pot:=x*pot(x,y-1);
end;
Procedure riduzion(a1:longint);
```

```
var k2,i:integer;
begin
  k2:=0;
  for i:=1 to mo1 do
  begin
  repeat
    if mo1 mod 2 = 0 then
                  begin
                    mo1:=mo1 div 2;
                    a1:=sqr(a1);
                    if a1>m then a1:=a1 mod m;
                  end
                  else
                  begin
                   k2:=k2+1;
                   mo1:=mo1-1;
                   p[k2]:=a1;
                  end;
    until mo1<=0;
    end;
    x:=1;
    for i:=1 to k2 do begin x:=x*p[i];x:=x mod m; end;
end;
function Test(n:longint):boolean;
var w:extended;
begin
  test:=true;
  x:=x mod n;
  if x = 1 then begin test:=false; end
               else
               begin
  j:=0;
  repeat
      if x = n-1 then  test:=false
                    else  x:=sqr(x) mod n;
  j:=j+1;
      until j>vo-1;
      end;
end;
begin
  clrscr;
  gotoxy(2,3);
  writeln('Questo programma ti permette di determinare la primalità di un numero');
  writeln('naturale dispari col metodo di Muller-Rabin');
```

```
 writeln;
 randomize;
 repeat
 write('Immetti un numero dispari m = ');readln(m);
 until m mod 2 <> 0;
 for i:=1 to m do
 begin
 k:=pot(2,i);
 for j:=1 to m do
  begin
     k1:=k*j;
     if ((m - 1)=k1) and ( j mod 2 <>0 ) then
               begin
                 mo:=j;
                 vo:=i;
               end;
  end;
 end;
 writeln(m - 1,' = 2^',vo,' * ',mo,' : dove mo = ',mo,' e vo = ',vo,' e x = a^mo mod m  con a
random (< m)');
 s:=0; q:=0;
  for i:=1 to 100 do
     begin
      mo1:=mo;
      a:=random(m-1)+1;
      riduzion(a);
      if test(m)=true then s:=s+1
                    else q:=q+1;
  end;
  if q>s then write(m,' è primo')
         else write(m,' è composto');
  readln;
 end.
```

Numeri di Perrin

Def. Si dice successione $(a_i)_{i\in N} = P(i)$ di *numeri di Perrin* la sequenza di numeri interi positivi definita ricorsivamente dalla seguente leggge di formazione:

$$\begin{cases} P(0) = 3 \\ P(1) = 0 \\ P(2) = 2 \\ P(n) = P(n-2) + P(n-3) \end{cases}$$

Tale successione si congettura sia un interessante *Test di primalità*, come è stato indicato dal matematico Lucas: infatti se *n* è un numero primo esso divide P(n); tuttavia non è stato ancora dimostrato che tale proprietà sia invertibile, anche se fino ad oggi non si è trovato alcun numero divisore dei numeri di Perrin che non sia primo.

```
Program Perrin;
{$N+}
uses crt;
var  i,j,k,sup,r:longint;
       m:array[1..1000] of longint;
       w,w1,w2:real;
       risp:char;
procedure primo(x:longint);
var i:longint;
    s:boolean;
begin
 s:=false; k:=0;
 for i:=1 to x do
   if (x/i)=int(x/i) then begin s:=true; end
    else
     if s=false then k:=k+1;
end;
function su(x:longint):longint;
begin
 if x=0 then su:=3
        else
        if x=1 then su:=0
              else
              if x=2 then su:=2
                    else su:=su(x-2)+su(x-3);
end;
begin
  repeat
     textbackground(1);
     clrscr;
     textcolor(11);
     writeln('Questo programma ti permette di determinare la successione di numeri di Perrin');
     writeln('definti dalla seguente legge di ricorsione:');
     writeln('                    P(0)=3   ');
     writeln('                    P(1)=0 ');
     writeln('                    P(2)=2 ');
     writeln('                    P(n)=P(n-2)-P(n-3) ');
     writeln('Inoltre ti verifica che se n è primo, tale numero divide P(n); così pure verifi-');
     writeln('ca che il rapporto di un termine della successione con il suo precedente tende ');
     writeln('alla soluzione reale dell''equazione cubica: x^3 - x -1 = 0 ');
```

```
   textcolor(12);
    write('Immetti l"estremo superiore n dell"intervallo di naturali: ');readln(sup);
    primo(sup);
  j:= -1;
   for i := 0 to sup do
       begin
         j := j+1;
        m[j] := su(i);
      end;
  for i:=0 to j do write(m[i]:10);
  writeln;
  writeln(j,'-----> ',m[j]);
  writeln;
  write(' Prima verifica: ');
  if k = 0 then begin if (m[j] mod (j)= 0) then write(m[j],'/',j,' = ',m[j] div (j))
           else write(m[j],' non è divisibile per ',j); end;
  writeln;
  writeln('Seconda verifica:   ');
  write(m[j],'/',m[j-1],' = ');
  write(m[j]/m[j-1]:3:18);
  writeln;
  writeln('La soluzione, applicando le formule di Cardano, data dal calcolatore è');
   w1:=exp(1/3*ln(0.5+sqrt(sqr(0.5)-1/3*sqr(1/3))));
   w2:=exp(1/3*ln(0.5-sqrt(sqr(0.5)-1/3*sqr(1/3))));
   w:=w1+w2;
   writeln('       ',w:3:18);
   write('Vuoi continuare con un altro estremo dell"intervallo ? (S/N) ');
   readln(risp);
   until (risp='n') or (risp='N');
end.
```

Qui si espongono alcuni programmi strettamente connessi con la ricerca di numeri primi molto grandi.

Numeri di Cullen

Def. I numeri interi positivi *m* della forma $m = n \cdot 2^n + 1$ sono detti numeri di Cullen.

Tra gli infiniti numeri di Cullen ci sono dei numeri primi, detti numeri primi di Cullen.
I primi valori di n che rendono primi i numeri di Cullen sono:

1, 141, 4713, 5795, 6611, 18496, ...

Tali numeri primi, essendo come grandezza superiori all"ordine di 10^44, eccedono i normali simulatori matematici dei normali computers; pertanto risultano molto difficili da calcolare.
I numeri naturali che generano i primi due numeri primi nella successione n
di Cullen sono 1 e 141: a questo corrisponde

p = 393050634124102232869567034555427371542904833

Nel 2009 il più alto numero n che genera un numero primo è n=6679881; tale numero primo p è costituito da 2010852 cifre. Tale numero è stato scoperto da Magnus Bergman nell''ambito del progetto di calcolo distribuito PrimeGrid.

```
program numeri_di_Cullen;
{$N+}
uses crt;
var b,bb:longint;
    a,inf,sup:integer;
function pot(x:integer;y:integer):longint;
begin
   if y=0 then pot:=1
          else if y > 0 then
                       pot:=x*pot(x,y-1);
end;
begin
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('Questo programma ti permette di determinare i numeri naturali p di ');
  writeln('Cullen: cioè numeri naturali del tipo p = n*2^n + 1 ');
  writeln;
  textcolor(12);
  write(' Immetti l''estremo inferiore ( >= 0 ) dell''intervallo : ');readln(inf);
  write(' Immetti l''estremo superiore ( <= 26) dell''intervallo : ');readln(sup);
  a:=inf;
  textcolor(10);
  repeat
    b:=pot(2,a);
    bb:=a*b+1;
    if (a>=inf) and ( a <= 13 ) then begin gotoxy(10,a+8);write(a,')  ',bb);end;
    if (a>13) and ( a <= sup ) then begin gotoxy(40,a-6);write(a,')  ',bb);end;
    a:=a+1;
  until a>sup;
readln;
  Clrscr;
  writeln('   I numeri di Cullen che sono anche primi vengono chiamati ');
  writeln('                    NUMERI PRIMI DI CULLEN            ');
  writeln(' I primi valori di n che rendono primi i numeri di Cullen sono:');
  writeln('               1,141,4713, 5795, 6611, 18496, ... ');
  writeln(' Tali numeri primi, essendo come grandezza superiori all''ordine di 10^44,');
  writeln(' eccedono i normali simulatori matematici dei normali computers; pertanto');
  writeln(' risultano molto difficili da calcolare.                              ');
  writeln(' I numeri naturali che generano i primi due numeri primi nella successione n');
  writeln(' di Culle sono 1 e 141: a questo corrisponde ');
```

```
writeln('          p = 39305063412410223286956703455542737154290483 3');
 writeln(' Nel 2009 il più alto numero n che genera un numero primo è  n=6679881;');
 writeln(' tale numero primo p è costituito da 2010852 cifre. Tale numero è stato');
 writeln(' scoperto da Magnus Bergman nell"ambito del progetto di calcolo distribuito');
 writeln('                    PrimeGrid');
 readln;
end.
```

Proprietà dei numeri di Cullen.

Un numero di Cullen C_n è divisibile per p = 2n-1 se p è un numero primo della forma p=8k-3. Inoltre grazie al Piccolo Teorema di Fermat sappiamo che p è un numero dispari, pertanto ne segue che p divide anche $C_{m(k)}$ per ogni $m(k)=(2^k - k)(p - 1) - k$ per ogni k positivo.

E' stato dimostrato che p divide il numero $C_{\frac{p+1}{2}}$, quando il simbolo di Jacobi $\left(\frac{p}{2}\right) = -1$

mentre divide $C_{\frac{3p-1}{2}}$, quando il simbolo di Jacobi $\left(\frac{p}{2}\right)$=+1

Numeri di Bell

Def. Si chiamano numeri di Bell i numeri della prima colonna della matrice triangolare inferiore

1	0	0	0	0	0	0	..
1	2	0	0	0	0	0	..
2	3	5	0	0	0	0	..
5	7	10	15	0	0	0	..
15	20	27	37	52	0	0	..
52	67	87	114	151	203	0	..
…….							

Pertanto la successione dei numeri di Bell è costituita da 1, 1, 2, 5, 15, 52, 203 ,…

Tra gli infiniti numeri di Bell ci sono dei numeri primi, detti numeri primi di Bell.

Se con B_n indichiamo i numeri di Bell relativi al valore n. I primi valori di n per cui B_n è un numero primo sono: 2, 3, 7, 13, 42, 55, 2841,… ed i numeri primi di Bell generati sono:

2, 5, 877, 27644437 ,…

Il numero primo B_{55} eccede la memoria di un normale calcolatore , amaggior ragione B_{2841}

```
program numeri_di_Bell;
{$N+}
uses crt;
var i,j:integer;
   m:array[1..100,1..100] of real;
begin
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln('Questo programma ti permette di determinare, col metodo della matrice');
```

```
 writeln('triangolare, la sequenza dei numeri di Bell. Essa è costituita dagli elementi ');
 writeln('prima colonna di tale matrice ');
 writeln;
 m[1,1]:=1 ;
 textcolor(12);
 for i:=2 to 20 do
   for j:=1 to i do
      if j=1 then m[i,j]:=m[i-1,i-1]
             else
                m[i,j]:=m[i-1,j-1]+m[i,j-1];
 for i:=1 to 11 do
  begin
   writeln;
   for j:=1 to i do
       write(m[i,j]:7:0);
  end;
  writeln;writeln;
 for i:=1 to 20 do
   for j:=1 to i do
     if j=1 then
       write(m[i,j]:16:0);
 readln;
end.
```

Applicazione dei numeri di Bell:

- Se un numero naturale m ha n divisori primi distinti, esso si può ottenere come prodotto dei suoi divisori propri in B_n modi diversi:
  Es. - Sia m = 12 . Esso ha come divisori primi 2 e 3 per un totale di 2. Pertanto posso ottenere 12 come prodotto dei suoi divisori propri, che sono 2, 3, 4, 6 , in $B_2 = 2$ modi diversi: cioè $2 \cdot 6$ e $3 \cdot 4$.
  - Sia m = 60. Esso ha come divisori primi 2, 3 e 5 per un totale di 3. Pertanto posso ottenere 60 come prodotto dei suoi divisori propri, che sono 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, in $B_3 = 5$ modi diversi: cioè $2 \cdot 30$, $3 \cdot 20$, $4 \cdot 15$, $5 \cdot 12$, $6 \cdot 10$
- Il numero delle partizioni in sottoinsiemi non vuoti di un insieme di *n* elementi distinti è B_n

Numeri di Woodall

Def. I numeri interi positivi *m* della forma $m = n \cdot 2^n - 1$ sono detti numeri di Woodall.

Tra gli infiniti numeri di Woodall ci sono dei numeri primi, detti numeri primi di Woodall.
I primi valori di n che rendono primi i numeri di Woodall sono:

2,3,6,30,75,81,115,123,249,362,384, ...

La sequenza dei numeri primi relativi a 2,3,6,30 e 75 di Woodall risulta:

7, 23, 383, 32212254719, 283341988972178712821759 9,

mentre la sequenza dei numeri primi generati dagli altri numeri risulta come valore dei suoi elementi superiore all"ordine di 10^44, eccedendo gli ordinari simulatori matematici dei normali computers; pertanto risultano molto difficili da calcolare.
Nel 2007 è stato verificato che il numero n=3752948 genera un numero primo , costituito da 1129757 cifre. Tale numero è stato scoperto da Matthew J.Thompson nell'ambito del progetto di calcolo distribuito PrimeGrid

```
program numeri_di_Woodall;
{$N+}
uses crt;
var b,bb:longint;
    a,inf,sup:integer;
function pot(x:integer;y:integer):longint;
begin
   if y=0 then pot:=1
          else if y > 0 then
                        pot:=x*pot(x,y-1);
end;
begin
  textbackground(1);
  clrscr;
  textcolor(15);
  writeln('Questo programma ti permette di determinare i numeri naturali p di ');
  writeln('Woodall: cioè  numeri naturali del tipo p = n*2^n - 1 ');
  writeln;
  textcolor(12);
  write(' Immetti l"estremo inferiore ( >= 1 ) dell"intervallo : ');readln(inf);
  write(' Immetti l"estremo superiore ( <= 26) dell"intervallo : ');readln(sup);
  a:=inf;
  textcolor(10);
  repeat
    b:=pot(2,a);
    bb:=a*b-1;
    if (a>=inf) and ( a <= 13 ) then begin gotoxy(10,a+8);write(a,')  ',bb);end;
    if (a>13) and ( a <= sup ) then begin gotoxy(40,a-6);write(a,')  ',bb);end;
    a:=a+1;
  until a>sup;
  readln;
  Clrscr;
  writeln('   I numeri di Woodall che sono anche primi vengono chiamati ');
  writeln('                    NUMERI PRIMI DI WOODALL            ');
  writeln(' I primi valori di n che rendono primi i numeri di Woodall sono:');
  writeln('               2,3,6,30,75,81,115,123,249,362,384, ... ');
  writeln(' tolti numeri primi generati da 2,3,6,30 e 75, gli altri essendo come’);
```

```
 writeln(‘ grandezza superiori all''ordine di 10^44 eccedono i normali simu-');
 writeln(' latori matematici dei normali computers; pertanto risultano molto');
 writeln(' difficili da calcolare.                    ');
 writeln(' La sequenza dei numeri primi relativi a  2,3,6,30 e 75 di Woodall risulta:');
 writeln('  7, 23, 383, 32212254719, 2833419889721787128217599, ...');
 writeln(' Nel 2007 il più grande numero n che genera un numero primo è n=3752948;');
 writeln(' tale numero primo p è costituito da 1129757 cifre. Tale numero è stato');
 writeln(' scoperto da Matthew J.Thompson nell''ambito del progetto di calcolo distribuito');
 writeln('                  PrimeGrid');
 readln;
end.
```

PROPRIETA’

I NUMERI DI Woodall hanno diverse proprietà di divisibilità. Ad esempio, se p è un numero primo, allora divide $W_{\frac{p+1}{2}}$ se il simbolo di Jacobi $\left(\frac{p}{2}\right) = +1$; divide invece $W_{\frac{3p-1}{2}}$ se il simbolo di Jacobi $\left(\frac{p}{2}\right) = -1$.
Esiste una congettura che dice che ci sono infiniti numeri primi di Woodall.

Congettura di Bertrand, dimostrata da Cebycef e da Dirichlet

Essa afferma che, dato un numero n (> 3) intero positivo, esiste almeno un numero primo compreso nell''intervallo [n ; 2n].

```
program congettura_di_Bertrand;
uses crt;
var j,a,b,y,h,k,m,xmin,xmax,n:longint;
   risp:char;
procedure numeroprimo(x:longint);
var i:longint;
begin
 i:=1;
 repeat
    i:=i+1
 until x mod i = 0;
 if (i=x) and (x>=xmin) and (x<=xmax)  then
       begin
         write(x:10);
         y:=1
       end
       else y:=0;
end;
begin
 repeat
```

```
 textbackground(1);
 clrscr;
 textcolor(15);
 writeln;
 writeln('  CONGETTURA DI BERTRAND ( dimostrata da Cebycef e da Dirichlet ) ');
 writeln('Dato un numero n ( > 3 ) intero positivo, esiste almeno un numero primo');
 writeln('compreso nell''intervallo [n ; 2n].');
 writeln;
 textcolor(12);
 write('Immetti il valore del numero n = ');readln(xmin);
 xmax:=2*xmin;
 k:=0;h:=0;
 textcolor(10);
   for j:=xmin div 4 to xmax div 4  do
     begin
       a:= 4*j-1;
       b:=4*j+1;
       numeroprimo(a); k:=k+y;
       numeroprimo(b); h:=h+y;
     end;
   writeln;
   m:=k+h;
   if (k<>0) or (h<>0) then
      begin
        writeln('Il numero dei numeri primi nell''intervallo [',xmin,' ; ',xmax,'] è ',m,' ( > 1 ) :');
        writeln('quindi in tale intervallo è verificata la congettura ');
      end;
   writeln;
   textcolor(14);
   write('Vuoi continuare con altro valore di n ? (S/N): ');
   readln(risp);
 until (risp='n') or (risp='N');
end.
```

CAPITOLO IV

FRAZIONI CONTINUE E SUE APPLICCAZIONI

Introduzione:

Le frazioni continue si ritengono tradizionalmente connesse all'algoritmo di divisione euclidea per la ricerca del MCD fra due numeri interi, tuttavia il formalismo algebrico presente nello sviluppo di tale struttura sembra essere sconosciuta ad Euclide e ai matematici ellenici. Si deve giungere intorno al 550 d.C. applicando il metodo euclideo delle divisioni successive, il matematico Aryabhata risolve un'equazione diofantea lineare: metodo oggi riconducibile alle frazioni continue. Tuttavia il primo a trattarne formalmente in modo esplicito senza peraltro chiamarla frazione continua ma è stato Bombelli nella ricerca del valore approssimato delle radici quadrate , un procedimento più esteso è stato successivamente impostato da Cataldi sempre sulla ricerca approssimata del valore della radice quadrata di un numero naturale usando il metodo escogitato da Bombelli. Oggi gli storici della matematica ritengono che il primo a sistematizzare e a dare una formalizzazione organica delle frazioni continue è stato Eulero nella sua opera *Introductio in Analysin Infinitorum.*

Oggi lo studio delle frazioni continue costituisce un argomento di rilevato interesse in quanto trova strette connessioni con lo studio della Funzione Zeta di Riemann, viene largamente usata nella soluzione non solo delle equazioni lineari diofantee ma anche in quelle particolari equazioni quadratiche diofantee: dette di Pell, il suo metodo algoritmico trova larga applicazione nello studio dei Frattali così pure in vari campi della matematica odierna.

Algoritmo di divisione euclidea

Sia dato l'insieme dei numeri naturali N in essa sono definite le quattro operazioni fondamentali con le relative proprietà che strutturano algebricamente tale insieme. L'addizione e la moltiplicazione sono operazioni chiuse in N: cioè il risultato di tali operazioni sono ancora elementi dell'insieme N; mentre la sottrazione e la divisione in generale sotto opportune condizioni il risultato è ancora un numero naturale, pertanto in generale tali operazioni si dicono non chiuse.

Def. Dividere due numeri naturali a per b (con $a > b$ e $b \neq 0$) consiste nel trovare quel numero naturale q, se esiste, che moltiplicato per b dà per prodotto a: cioè

$$a : b = q \quad \leftrightarrow \quad a = b \cdot q$$

dove (**:**) è il simbolo di divisione, a è detto dividendo, b è detto divisore e q è detto quoto.

NB. Come si può notare la divisione è stata condotta alla moltiplicazione: cioè essa è l'operazione inversa della moltiplicazione. Ecco perché la moltiplicazione, così pure l'addizione, sono dette operazioni dirette.

Da tale definizione possiamo affermare che

Proposizione: Dati due numeri naturali a e b con $a > b$ e $b \neq 0$, si dice che a è divisibile per b se e solo se esiste un numero naturale q, detto quoto, tale che $a = b \cdot q$ o anche che a è multiplo di b secondo q; altrimenti se non esiste q , si dice che a non è divisibile per b o anche che a non è multiplo di b.

Si consideri ora il caso in cui, presi due numeri naturali a e b con $a > b$ e $b \neq 0$, il numero a non sia divisibile per b, in questo contesto si dimostra il seguente teorema di Euclide:

Teorema di Euclide: Dati due numeri naturali **a** e **b,** con $a > b$ e $b \neq 0$, esiste ed è unica la coppia di numeri naturali **q** ed **r,** detti rispettivamente quoziente e resto tale che

$$\mathbf{a = b \cdot q + r}$$

con $0 \leq r < b$

Dimostrazione

Nell'insieme dei numeri naturali si consideri l'intervallo discreto [b ; a] in esso vale l'ordinamento naturale, essendo un sottoinsieme finito e limitato di N; sia ora $k_i = 1,2,3,4,..,n,..$, e si considerino i multipli di b secondo k, che siano elementi dell'intervallo [b ; a], essi costituiscono una successio-ne ordinata di interi positivi: $b = 1b < 2b < 3b < \ldots < k_n b < a$ con k_n il massimo valore per cui $k_n b < a < k_{n+1} b$. Nella successione dei numeri naturali tale valore $k_n b$ esiste in quanto la moltiplicazione fra numeri naturali è un'operazione chiusa. Se consideriamo la divisione tra a e b, il valore $q = k_n$ costituisce il quoziente di tale divisione essendo il massimo intero positivo il cui prodotto $q \cdot b$ non supera a. Dall'essere poi $a > q \cdot b$, sottraendo ad ambo i membri della diseguaglianza $q \cdot b$ otteniamo una diseguaglianza equivalente ed equiversa : $a - q \cdot b > 0$; ora la differenza di due quantità intere positive è ancora una quantità intera positiva: posto $r = a - q \cdot b > 0$. Da quest'ultima uguaglianza si ha $a = q \cdot b + r$; pertanto l'esistenza della coppia q ed r viene provata dai risultati operativi della moltiplicazione e della sottrazione di due numeri interi positivi. Proviamo che $r < b$. Supponiamo che $r = b$. Poiché $a = q \cdot b + r$, sostituendo si ha $a = q \cdot b + b = b (q + 1)$: cioè a è multiplo di b o che è la stessa cosa a è divisibile per b contro le ipotesi del teorema, quindi $r \neq b$. Supponiamo che $r > b$ con r e b $\in$ N . Sottraendo ad ambo i termini della diseguaglianza b si ha $r - b > 0$ e per la proprietà della sottrazione che la differenza è minore del minuendo possiamo affermare che $r - b < r$; ora $r - b = a - q \cdot b - b = a - b (q + 1) < 0$, essendo $b (q+1)$ il multiplo di b che supera a , quindi $r - b < 0$,cioè $r < b$ contro l'ipotesi che $r > b$. Pertanto per la proprietà di tricotomia provando che r non può essere $\geq b$, resta dimostrato che $r < b$.

Proviamo l'unicità della coppia q ed r. Supponiamo che esistano due coppie di valori che soddisfano il teorema e siano q_1 , r_1 e q_2 , r_2 tali che

$$a = b \cdot q_1 + r_1$$
$$a = b \cdot q_2 + r_2$$

Sottraendo ambo i termini tra loro, si ha $0 = b (q_1 - q_2) - (r_1 - r_2)$, da cui

$b (q_1 - q_2) = (r_1 - r_2)$

Se $q_1 > q_2$ allora $b \leq b(q_1 - q_2) = (r_1 - r_2) \leq r_1 < b \rightarrow$ per la proprietà transitiva $\rightarrow b < b$ il che è assurdo.
Se $q_1 < q_2$ allora $b \leq b(q_2 - q_1) = (r_2 - r_1) \leq r_2 < b \rightarrow$ per la proprietà transitiva $\rightarrow b < b$ il che è assurdo.
Per la proprietà di Tricotomia segue necessariamente che $q_1 = q_2$ e di conseguenza $r_1 = r_2$; pertanto le due coppie sono uguali cvd.

Massimo Comun divisore.

Questo teorema costituisce il supporto teorico per la ricerca del MCD fra due numeri interi positivi .

Def. Si chiama Massimo Comun Divisore della coppia $(a ; b) \in N \cdot N$ il numero $m \in N$ tale che

1) m è un divisore sia di a che di b
2) Ogni divisore comune di a e di b è un divisore di m

Teorema: Dati comunque a e b ∈ N , non entrambi nulli, il Massimo Comun Divisore m di a e di b esiste ed è univocamente determinato ed esso è il più grande tra i divisori comuni di a e di b.

Consideriamo due numeri naturali a e b , alla luce del teorema cerchiamo di determinare il loro MCD.

Primo caso: se $a = 0$ e $b \neq 0$, allora MCD (0 ; b) = b , in quanto ogni numero è un divisore dello zero; così pure se $a \neq 0$ e $b = 0$, allora MCD (a ; 0) = a.

Secondo caso: Siano a e b diversi da zero e supponiamo che

-) a > b e a sia multiplo di b o che è lo stesso a è divisibile per b : cioè $a = q \cdot b$, allora il MCD (a ; b) = b, in quanto b divide a e se stesso , quindi è il divisore comune.

-) a < b e b sia multiplo di a o che è lo stesso a divide b: cioè $b = k \cdot a$, allora il MCD (a ; b) = a.

-) a > b e a non sia divisibile per b. Applichiamo il Teorema di Euclide: cioè esistono due valori naturali q_1 ed r_1 tali che $a = q_1 \cdot b + r_1$ con $0 \leq r_1 < b$.
Poiché $r_1 \neq 0$ e $b > r_1$,
se r_1 è un divisore di b allora $b = q_2 \cdot r_1$; sostituendo e raccogliendo r_1 in $a = q_1 \cdot b + r_1$, otteniamo $a = r_1 \cdot (q_1 \cdot q_2 + 1)$, cioè r_1 è un divisore anche di a e pertanto MCD (a ; b) = r_1 ;
se r_1 non è divisore di b , allora, applicando il teorema di Euclide, esistono

due valori naturali q_2 ed r_2 tale che $b = q_2 \cdot r_1 + r_2$ con $0 \leq r_2 < r_1 < b$
Poiché $r_2 \neq 0$ e $r_1 > r_2$,
se r_2 è un divisore di r_1 allora $r_1 = q_3 \cdot r_2$; sostituendo e raccogliendo r_2 in

$b = q_2 \cdot r_1 + r_2$, otteniamo $b = r_2 \cdot (q_2 \cdot q_3 + 1)$, cioè r_2 è un divisore anche di b; andando a sostituire e raccogliendo r_2 in $a = q_1 \cdot b + r_1$, otteniamo $a = r_2[q_1(q_2 \cdot q_3 + 1) + q_3]$: cioè r_2 è un divisore oltre che di b anche di a e pertanto MCD (a ; b) = r_2 ;
se r_2 non è divisore di b , allora, applicando il teorema di Euclide, esistono due valori naturali q_3 ed r_3 tale che $r_1 = q_3 \cdot r_2 + r_3$ con $0 \leq r_3 < r_2 < r_1 < b$
… e così via fino a determinare un resto $r_n = 0$, per cui il

MCD(a ; b) = r_{n-1}

dove $r_{n-1} \neq 0$ ed è un divisore di tutti i resti che lo precedono e del valor b ed a, come d'altronde abbiamo provato r_1 , r_2 , r_3 .

Raggruppando tutte le divisioni effettuate si ha quello che è detto Algoritmo di Euclide per la ricerca del MCD (a ; b):

$$a = q_1 \cdot b + r_1$$
$$b = q_2 \cdot r_1 + r_2$$
$$r_1 = q_3 \cdot r_2 + r_3$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n \cdot r_{n-1} + r_n \qquad \text{con } r_n = 0$$

Come si può notare tale algoritmo permette di trovare il MCD (a ; b) senza conoscere né i divisori di a né i divisori di b.

Questo programma ti permette di trovare il MCD tra due numeri naturali con l'algoritmo di Euclide.

```
program MCD_con_algoritmo_di_Euclide;
 uses crt;
 var  a,b,a1,b1,k,q,r,i:integer;
      m, rest,quot,n:array[1..100] of integer;
      risp:char;
 begin
  repeat
   clrscr;
   textcolor(11);
   writeln('Metodo della divisione per la ricerca del MCD tra due numeri');
   writeln('interi positivi di Euclide ');
   writeln;
   textcolor(13);
   write('   Immetti due numeri interi positivi ( a ; b ):  ');
   readln(a,b);
   writeln;
   a1:=a;
```

```
  b1:=b;
  k:=1;
  repeat
     q:=a div b ; r:=a mod b;
     n[k]:=a;
     m[k]:=b; rest[k]:=r ; quot[k]:=q;
     a:=b; b:=r;
     k:=k+1
  until r=0;
  textcolor(14);
  for i :=1 to k-1 do
        begin
          write ('    ',n[i],' = ', quot[i],'*',m[i],'+',rest[i]);
          writeln;
        end;
        writeln;
  if rest[k-2]=0 then rest[k-2]:=b1;
    writeln('      M.C.D.( ',a1,' ; ',b1,' ) = ',rest[k-2]);
  writeln;
  write('Vuoi continuare con altra coppia di valori interi positivi ? (S/N) ');
  readln(risp);
 until (risp='N') or (risp='n');
end.
```

Proprietà lineare del MCD o identità di Bézout

Identità di Bézout: Siano a e b due numeri interi positivi e sia m il loro Massimo Comun Divisore: m = MCD (a , b) , l'identità di Bézout afferma che m è combinazione lineare di a e b : cioè esistono due interi x ed y tale che m = a x + b y

```
program Identita_di_Bezout;
uses crt;
var  a,b,m,n,c,mcd,r:integer;
     a1,a2,a3,b1,b2,b3,c1,c2,c3,q:integer;
begin
  clrscr;
  textcolor(2);
  writeln('Questo programma ti permette di verificare il Teorema di Bezout: ');
  writeln;
  textcolor(15);
  writeln('Siano A e B due numeri naturali e sia MCD il loro massimo comun');
  writeln('divisore, esistono almeno due numeri relativi x, y tale che :');
  textcolor(12);
  writeln('                  MCD(A,B) = x*A + y*B ');
```

```
 textcolor(15);
 writeln('cioe" il MCD e" una combinazione lineare di A e B .');
 writeln;
 textcolor(14);
 write('Immetti due numeri naturali : ');
 readln(a,b);
 if a<b then
        begin
          c:=a; a:=b; b:=c;
        end;
 m:=a;  n:=b;  r:=a mod b;
 while r<>0 do
   begin
     a:=b; b:=r; r:=a mod b;
   end;
 mcd:=b;
 writeln('MCD (',m,';',n,') = ',mcd);
 if m mod n <> 0 then
                begin
                  a1:=m; a2:=1; a3:=0;
                  b1:=n; b2:=0; b3:=1;
                  q:=a1 div b1;
                  repeat
                    c1:=b1;c2:=b2;c3:=b3;
                    b1:=a1-q*b1; b2:=a2-q*b2; b3:=a3-q*b3;
                    a1:=c1;a2:=c2;a3:=c3;
                    q:=a1 div b1;
                  until b1=mcd;
                end
               else
                begin
                  b2:=1; b3:=-(m div n - 1);
                end;
 writeln;writeln;
 textcolor(12);
 writeln(mcd,' = (',b2,')*',m,'+(',b3,')*',n);
 writeln;
 textcolor(11);
 writeln('x = ',b2,'  e  y = ',b3);
 readln;
end.
```

Frazioni continue

Così Eulero nella Introductio In Analysin Infinitorum, Tomo I° cap XVII definisce le frazioni continue:

… chiamo continua una frazione fatta in modo da avere il denominatore costituito da un numero intero sommato ad una frazione il cui denominatore è fatto a sua volta da un intero e da una frazione e che in avanti sia costituita in simile modo sia che questo comportamento si estenda all'infinito o si ferma ad un certo punto. In questo senso pertanto chiamo frazione continua un'espressione del tipo

$$a + \cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d+\cdots}}} \qquad\qquad a + \cfrac{\alpha}{b+\cfrac{\beta}{c+\cfrac{\gamma}{d+\cdots}}}$$

la prima forma è detta frazione continua semplice, mentre la seconda è detta generalizzata

L'algoritmo euclideo permette di scrivere in forma di frazione continua la frazione che ha per numeratore a e per denominatore b , dove a e b è la coppia di cui l'algoritmo va alla ricerca del MCD.

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}}$$

Considerato che la scrittura a strati è alquanto laboriosa, i matematici hanno proposto queste due forme equivalenti:

$$\frac{a}{b} = [q\,;\ q_1\,;\ q_2\,; q_3\,; \ldots] = q + \frac{1}{q_1+}\ \frac{1}{q_2+}\ \frac{1}{q_3+} \ldots.$$

dove la frazione con denominatore seguito dal simbolo + sta ad indicare che la frazione successiva va sommata al denominatore della frazione precedente.

Numeri razionali assoluti Q^+ e loro sviluppo in frazioni continue

Def. Un numero si dice razionale assoluto se è esprimibile in forma frazionaria con numeratore e denominatore numeri interi positivi

Sono numeri razionali assoluti pertanto i numeri naturali, i numeri decimali finiti e i numeri periodici, semplici o misti: infatti tutti si possono esprimere in forma frazionaria.
I numeri decimali finiti e quelli periodici, una volta trasformati in frazione, e le frazioni vediamo come svilupparli in frazioni continue finite col metodo della divisione di Euclide; per i numeri decimali finiti possiamo trasformarli direttamente in frazioni continue:

Esempio: Sia dato il numero decimale finito 3,456, vogliamo svilupparlo in frazione continua:

$$3{,}456 = 3 + 0{,}456 = 3 + \frac{456}{1000} = 3 + \frac{1}{\frac{1000}{456}} = 3 + \frac{1}{2+\frac{88}{456}} = 3 + \frac{1}{2+\frac{1}{\frac{456}{88}}} = 3 + \frac{1}{2+\frac{1}{5+\frac{16}{88}}} =$$

$$= 3 + \frac{1}{2+\frac{1}{5+\frac{1}{\frac{88}{16}}}} = 3 + \frac{1}{2+\frac{1}{5+\frac{1}{\frac{8}{16}}}} = 3 + \frac{1}{2+\frac{1}{5+\frac{1}{5+\frac{1}{2}}}}$$

$$3{,}456 = [3\ ;\ 2\ ,\ 5,\ 5\ ,\ 2] = 3+\frac{1}{2+}\ \frac{1}{5+}\ \frac{1}{5+}\ \frac{1}{2}$$

Esempio:

1) Vogliamo trasformare in frazione continua la frazione $\frac{132}{50}$.

Risoluzione:

Applichiamo l'algoritmo di Euclide alla coppia (132 ; 50)

$132 = 2 \cdot 50 + 32$	dividendo per 50 si ha	$\frac{132}{50} = 2 + \frac{32}{50}$
$50 = 1 \cdot 32 + 18$	dividendo per 32 si ha	$\frac{50}{32} = 1 + \frac{18}{32}$
$32 = 1 \cdot 18 + 14$	dividendo per 18 si ha	$\frac{32}{18} = 1 + \frac{14}{18}$
$18 = 1 \cdot 14 + 4$	dividendo per 14 si ha	$\frac{18}{14} = 1 + \frac{4}{14}$
$14 = 3 \cdot 4 + 2$	dividendo per 4 si ha	$\frac{14}{4} = 3 + \frac{2}{4}$
$4 = 2 \cdot 2$	dividendo per 2 si ha	$\frac{4}{2} = 2$

MCD(132, 50) =2

Da cui possiamo scrivere:

$$\frac{132}{50} = 2 + \frac{32}{50} = 2 + \frac{1}{\frac{50}{32}} = 2 + \frac{1}{1+\frac{18}{32}} = 2 + \frac{1}{1+\frac{1}{\frac{32}{18}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{14}{18}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{\frac{18}{14}}}} =$$

$$= 2 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{4}{14}}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{\frac{14}{4}}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{3+\frac{2}{4}}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{3+\frac{1}{\frac{4}{2}}}}} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{3+\frac{1}{2}}}}$$

Quindi

$$\frac{132}{50} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{2}}}}}$$

Scrivendo formalmente, si ha:

$$\frac{132}{50} = [2\ ;1\ ,1\ ,1\ ,3\ ,2] = 2 + \frac{1}{1+}\ \frac{1}{1+}\ \frac{1}{1+}\ \frac{1}{3+}\ \frac{1}{2}$$

Come si nota la frazione $\frac{132}{50}$ si sviluppa in una frazione continua semplice finita; dentro parentesi quadre sono presenti i quozienti delle diverse divisioni dell'algoritmo di Euclide, così pure nello sviluppo in frazione continua al denominatore sono presenti i quozienti dal secondo in poi seguito dal + che sta ad indicare che la frazione successiva va sommata al denominatore della

frazione precedente. Pertanto, sviluppato l'algoritmo di Euclide, possiamo senz'altro scrivere formalmente la frazione continua relativa alla frazione data.
Facciamo ora un esempio con una frazione propria:

Esempio: Vogliamo trasformare in frazione continua la frazione $\frac{15}{53}$.

Risoluzione:

Applichiamo l'algoritmo di Euclide alla coppia (15 ; 53)

$15 = 0 \cdot 53 + 15$	dividendo per 53 si ha	$\frac{15}{53} = 0 + \frac{15}{53}$
$53 = 3 \cdot 15 + 8$	dividendo per 15 si ha	$\frac{53}{15} = 3 + \frac{8}{15}$
$15 = 1 \cdot 8 + 7$	dividendo per 8 si ha	$\frac{15}{8} = 1 + \frac{7}{8}$
$8 = 1 \cdot 7 + 1$	dividendo per 7 si ha	$\frac{8}{7} = 1 + \frac{1}{7}$
$7 = 7 \cdot 1$	dividendo per 1 si ha	$\frac{7}{1} = 7$

Considerando solo i quozienti, possiamo sviluppare $\frac{15}{53}$ in frazione continua semplice finita

$$\frac{15}{53} = [0\,;3\,,1\,,1\,,7] = 0 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{7}$$

Esempio: Vogliamo trasformare il numero decimale finito 3,7468 in frazione continua:

$$3{,}7468 = 3 + 0{,}7468 = 3 + \frac{1}{\frac{1}{0{,}7468}} = 3 + \frac{1}{1+0.3390} = 3 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{18+\frac{1}{1+\frac{1}{3}}}}}}$$

$$= [3\,;1\,;2;1\,;18\,;1\,;3;\ldots]$$

Def. Si chiama profondità di una frazione continua il numero di livelli di stratificazioni presenti in essa

Essendo finita la frazione continua relativa ad un numero razionale,la profondità di tale frazione è *n*:
questo sta ad indicare che nello sviluppo in frazione continua si incontra una parte frazionaria nulla dopo n passi.

Es. Consideriamo la frazione $\frac{2}{3}$, che sviluppata in frazione continua risulta: $[0;1,2]$. La sua profondità $n = 2$, pertanto nello sviluppo della frazione continua si incontra un addendo frazionario nullo dopo 2 passi: cioè al terzo passo o strato si ha una frazione con numeratore uguale a zero:

$$\frac{2}{3} = 0 + \frac{1}{1 + \frac{1}{2 + \frac{0}{1}}}$$

146

NB. La scrittura formale generale delle frazioni continue è $[a_0;\ a_1, a_2, a_3, \dots, a_n]$, dove il pedice 1,2,3,..,n indicano il numero di stratificazioni presenti nella frazione continua.
138

Es. Se consideriamo la frazione continua $[2;\ 2,\ 1,\ 3,\ 2]$ relativa alla frazione $\frac{59}{25}$ essa ha una profondità di 4 unità : ciò vuol dire che al quinto passo è presente una frazione nulla:

$$\frac{59}{25} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \frac{0}{1}}}}}$$

Si dimostra in generale che

Teorema: Ogni numero razionale si può rappresentare come frazione continua semplice finita (o limitata): cioè costituita da n-livelli che ne esprimono la profondità .

Teorema inverso: Ogni frazione continua finita rappresenta un numero razionale, che ne costituisce il suo valore.

Osservazione:

-) Se il numero razionale è proprio allora il primo quoziente è 0 , se invece è improprio il primo quoziente è diverso da 0.

-) Relativamente alla scrittura formale della frazione continua gli elementi che figurano dentro parentesi quadre sono detti quozienti parziali o esatti; inoltre se sviluppiamo le frazioni come

nel primo esempio

$$\frac{132}{50} = [2\,;1\,,1\,,1\,,3\,,2] = 2 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{3+}\,\frac{1}{2}$$

abbiamo

$$\frac{2}{1} \quad ; \quad 2 + \frac{1}{1} = \frac{3}{1} \quad ; \quad 2 + \frac{1}{1+\frac{1}{1}} = \frac{5}{2} \quad ; \quad 2 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{7}{3}$$

$$2 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{3}}}} = \frac{29}{11} \quad ; \quad 2 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{3+\frac{1}{2}}}}} = \frac{66}{25} = \frac{132}{50}$$

Le frazioni $\frac{2}{1}$; $\frac{3}{1}$; $\frac{5}{2}$; $\frac{7}{3}$; $\frac{29}{11}$; $\frac{66}{25} = \frac{132}{50}$ sono dette i convergenti o le ridotte

della frazione continua. Tali frazioni hanno il ruolo di approssimare il valore della frazione data, in particolare (considerando l'ordine della successione sia dei quozienti quanto quella delle ridotte come quello dei numeri naturali compreso lo 0) possiamo constatare che le ridotte d'ordine pari approssimano la frazione data per difetto , mentre quelli d'ordine dispari la approssimano per eccesso, di qui il termine coniato di ridotte o convergenti o quozienti approssimati dato a tali frazioni.
Nel secondo esempio

$$\frac{15}{53} = [0\,;3\,,1\,,1\,,7] = 0 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{7}$$

le frazioni ridotte sono

$$\frac{0}{1} \;;\; \frac{1}{3} \;;\; \frac{1}{4} \;;\; \frac{2}{7} \;;\; \frac{15}{53}$$

Anche in questo contesto le frazioni ridotte d'ordine pari : $\frac{0}{1}$; $\frac{1}{4}$ approssimano per difetto la frazione $\frac{15}{53}$, mentre quelle d'ordine dispari : $\frac{1}{3}$; $\frac{2}{7}$ approssimano per eccesso la stessa frazione.

Il programma seguente consente di sviluppare in frazione continua un numero razionale:

```
program Dalla_divisione_di_Euclide_alla_frazione_continua;
 uses crt;
 var  a,b,a1,b1,k,q,r,i:integer;
      m, rest,quot,n:array[1..100] of integer;
 begin
  repeat
   clrscr;
   writeln('Dall"algoritmo di Euclide alla scrittura formale della frazione');
   writeln('continua della frazione avente per numeratore a e denominatore b');
   writeln;
  write('   Immetti due numeri interi positivi ( a ; b ):  ');readln(a,b);
   writeln;
   a1:=a;
   b1:=b;
   k:=1;
   repeat
      q:=a div b ; r:=a mod b;
      n[k]:=a;
      m[k]:=b; rest[k]:=r ; quot[k]:=q;
      a:=b; b:=r;
      k:=k+1
   until r=0;
   textcolor(14);
   for i :=1 to k-1 do
```

```
        begin
          write ('    ',n[i],' = ', quot[i],'*',m[i],'+',rest[i]);
          writeln;
        end;
  if rest[k-2]=0 then rest[k-2]:=b1;

    writeln('      M.C.D.( ',a1,' ; ',b1,' ) = ',rest[k-2]);
  writeln;
  for i :=1 to k-2 do
       begin
         write (n[i],'/',m[i],' = ',quot[i],' + ',rest[i],'/',m[i],' = ');
         write( quot[i],' + 1/',m[i],'/',rest[i]);
         writeln;
       end;
       write(n[k-1],'/',m[k-1],' = ',quot[k-1]);
  writeln;
  writeln('Andando a sostituire a ritroso si ha : ');
  if k = 3 then write(n[1],'/',m[1],' = ',quot[1],' + 1/',quot[2]);
  if k = 4 then write(n[1],'/',m[1],' = ',quot[1],' + 1/(',quot[2],'+1/',quot[3],'))');
  if k = 5 then write(n[1],'/',m[1],' = ',quot[1],' + 1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],')))');
  if k = 6 then write(n[1],'/',m[1],' = ',quot[1],' +
1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],'+1/(',quot[5],'))))');
  if k = 7 then begin write(n[1],'/',m[1],' = ',quot[1],' +
1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],'+1/(',quot[5],'+1/(');
  write(quot[6],')))))');end;
  if k = 8 then
     begin
       write(n[1],'/',m[1],' = ',quot[1],' +
1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],'+1/(',quot[5],'+1/(');
       write(quot[6],'+1/(',quot[7],')))))');
     end;
  if k = 9 then
     begin
       write(n[1],'/',m[1],' = ',quot[1],' +
1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],'+1/(',quot[5],'+1/(');
       write(quot[6],'+1/(',quot[7],'+1/(',quot[8],'))))))');
     end;
  if k = 10 then
     begin
       write(n[1],'/',m[1],' = ',quot[1],' +
1/(',quot[2],'+1/(',quot[3],'+1/(',quot[4],'+1/(',quot[5],'+1/(');
       write(quot[6],'+1/(',quot[7],'+1/(',quot[8],'1+/(',quot[9],')))))))');
     end;
```

```
    writeln;
  writeln; writeln('Vogliamo scrivere in modo formale la frazione continua:');
  writeln;
  write(n[1],'/',m[1],' = [ ',quot[1]);
  for i :=2 to k-1 do
     write(' , ',quot[i]);
  write('] = ',quot[1],'+');
  for i:=2 to k-2 do
     write(' 1/(',quot[i],'+)'); write(' 1/',quot[k-1]);
 write('Vuoi continuare con altra coppia di valori ? ( S/N) ');
readln(risp);
until ( risp='N') or ( risp = 'n');
end.
```

Calcolo delle frazioni ridotte o convergenti di una frazione continua

Per la determinazione delle frazioni convergenti di una frazione continua possiamo individuare un algoritmo ricorsivo:

Per n = 0 si ha $[a_0] = a_0 = \frac{a_0}{1}$

Per n = 1 si ha $[a_0;\ a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$

Per n = 2 si ha $[a_0;\ a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}$

Per n = 3 si ha $[a_0;\ a_1, a_2, a_3] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = a_0 + \frac{1}{a_1 + \frac{a_3}{a_2 a_3 + 1}} = a_0 + \frac{a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} =$

$$= \frac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3}$$

Se indichiamo con P(n) il numeratore e Q(n) il denominatore, allora possiamo scrivere

Per n = 0 $P(0) = a_0$
$Q(0) = 1$

Per n = 1 $P(1) = a_0 a_1 + 1$
$Q(1) = a_1$

Per n = 2 $P(2) = a_0 a_1 a_2 + a_0 + a_2 = a_2 \cdot P(1) + P(0)$
$Q(2) = a_1 a_2 + 1 = a_2 \cdot Q(1) + Q(0)$

Per n = 3 $P(3) = a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1 = a_3 \cdot P(2) + P(1)$
$Q(3) = a_1 a_2 a_3 + a_1 + a_3 = a_3 \cdot Q(2) + Q(1)$

…….

Per n = k $P(k) = a_k \cdot P(k-1) + P(k-2)$
$Q(k) = a_k \cdot Q(k-1) + Q(k-2)$

Pertanto la formula generale per la determinazione della convergente $c_n = \frac{p_n}{q_n}$ è:

$$\frac{p_n}{q_n} = \frac{P(n)}{Q(n)} = \frac{a_n \cdot P(n-1)+P(n-2)}{a_n \cdot Q(n-1)+Q(n-2)}$$

Si dimostra che P(n) e Q(n) sono primi tra loro : cioè MCD(P(n) , Q(n)) = 1 o che è lo stesso la frazione $\frac{p_n}{q_n}$ è ridotta ai minimi termini.

Possiamo quindi scrivere le formule di Ricorrenza per determinare p_n e q_n:

$$\begin{cases} P(0) = a_0 \\ P(1) = a_0 a_1 + 1 \\ P(n) = a_n \cdot P(n-1) + P(n-2) \end{cases} \quad \text{et} \quad \begin{cases} Q(0) = 1 \\ Q(1) = a_0 \\ Q(n) = a_n \cdot Q(n-1) + Q(n-2) \end{cases}$$

Tali formule di ricorrenza costituiscono l'enunciato del *Teorema di Ricorrenza di Eulero-Wallis ;*
inoltre per P(n) e Q(n) valgono le *formule di Lagrange*:

$$P(n) \cdot Q(n-1) - P(n-1) \cdot Q(n) = (-1)^{n-1}$$
$$P(n) \cdot Q(n-2) - P(n-2) \cdot Q(n) = (-1)^{n}$$

Da queste formule discendono alcune proprietà dei convergenti:

a) Al crescere di *n* i convergenti d'ordine pari crescono strettamente, mentre quelli dispari decrescono strettamente
b) Ogni convergente d'ordine dispari è maggiore di ogni convergente d'ordine pari
c) Il valore di una frazione continua è maggiore di ogni suo convergente pari e minore di ogni suo convergente dispari (fatta eccezione per l'ultimo convergente)

Rappresentazione dei numeri irrazionali come frazioni continue infinite (od illimitate)

Teorema: ogni numero reale si può rappresentare in frazione continua e la frazione continua è illimitata se e solo se il numero è irrazionale.

La rappresentazione in frazione continua di un numero reale irrazionale è unica.

Numeri irrazionali quadratici e loro sviluppo in frazioni continue:

Def. Si chiamano numeri irrazionali quadratici o numeri reali algebrici del secondo ordine quei numeri irrazionali che sono soluzioni di equazioni della forma

$$1) \qquad ax^2 + bx + c = 0$$

con a,b,c ∈ Z e sotto le condizioni che a ≠ 0 , c ≠ 0 e b^2- 4ac > 0.

Siano α ed α' le due soluzioni dell'equazione 1).

Def. Si chiama coniugato della soluzione α, relativo all'equazione 1), la soluzione α' della stessa equazione e viceversa.

Se $\alpha = \frac{-b+\sqrt{b2-4ac}}{2a}$, allora il suo coniugato è $\alpha' = \frac{-b-\sqrt{b2-4ac}}{2a}$

Tra i due valori, per la fattorizzazione di un polinomio, esiste la seguente relazione:

$$a(x-\alpha)(x-\alpha')= ax^2+bx+c$$

Il primo ad occuparsi dello sviluppo in frazione continua dei radicali quadratici è stato Bombelli , in infatti nella sua Algebra sono trattati problemi relativi al calcolo approssimato della radice quadrata di 13:

Così egli scrive:

Supponiamo di voler calcolare $\sqrt{13}$, per prima cosa dobbiamo trovare quel numero intero positivo che elevato al quadrato si avvicini il più possibile a 13 senza superarlo, in questo caso sarà 3. Allora si avrà:

$$1) \qquad \sqrt{13} = 3 + x$$

Elevando ambo i termini al quadrato otterremo:

$$13 = 9 + 6x + x^2$$

Sottraendo ad ambo i termini 9 si ha

$$2) \qquad 4 = 6x + x^2$$

Trascurando momentaneamente il quadrato x^2, ricaviamo il valore della x = $\frac{4}{6}$; sostituendo in 1) si ha

$$3) \qquad \sqrt{13} = 3 + \frac{4}{6}$$

Ma se vogliamo un valore più preciso dobbiamo calcolare x^2 ; pertanto dall'essere x = $\frac{4}{6}$, moltiplicando ambo i termini per x si ha: $x^2 = \frac{4}{6}x$. Andando a sostituire in 2) si ha:

$$4 = 6x + \frac{4}{6}x = \left(6 + \frac{4}{6}\right)x$$

Ricavando la x si ha

$$x = \frac{4}{6 + \frac{4}{6}}$$

Sostituendo nella 1) si ha

$$\sqrt{13} = 3 + \frac{4}{6 + \frac{4}{6}}$$

Oggi confrontando la 3) con quest'ultima appare chiaro che alla frazione $\frac{4}{6}$ si può sostituire l'espressione

$$\frac{4}{6 + \frac{4}{6}}$$

iterando il procedimento, abbiamo:

$$\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \cdots}}}$$

E così di seguito, ottenendo così una frazione continua illimitata. Fermando lo sviluppo e andando a ritroso si ottiene una ridotta che approssima il valore di $\sqrt{13} \approx \frac{119}{33} = 3,\overline{60}$

Il cui quadrato è 13,0036 . Se ci fossimo fermati al secondo livello avremmo avuto $\sqrt{13} \approx \frac{18}{5} =$ 3,6 , il cui quadrato è 12,96. Tale metodo ha condotto Bombelli ad escogitare le frazioni continue, fermandosi lui però al secondo livello; sarà poi Cataldi ad applicare tale metodo nella ricerca della radice quadrata di 18 e lo svilupperà a livelli di stratificazioni più numerosi.
Da Eulero in poi si ha un fiorire di teoremi relativi allo sviluppo in frazioni continue dei numeri irrazionali ed in generale dei numeri reali: tale sviluppo permetterà di determinare frazioni il cui valore costituirà un approssimazione sempre più vicina al valore effettivo del numero che non le frazioni decimali; vediamo ciò con un esempio e precisamente con la determinazione di $\sqrt{2}$, che tutti i testi di algebra delle scuole superiori portano come l'elemento di separazione di due classi contigue costruite per troncamento; con le frazioni continue si ha una convergenza più veloce.

$1 < \sqrt{2} < 2$
$1,4 < \sqrt{2} < 1,5$
$1,41 < \sqrt{2} < 1,42$
$1,414 < \sqrt{2} < 1,415$
$1,4142 < \sqrt{2} < 1,4143$
$1,41421 < \sqrt{2} < 1,41422$
$1,414213 < \sqrt{2} < 1,414214$
…….

Sviluppiamo $\sqrt{2}$ in frazione continua:

$$\sqrt{2} = 1 + x$$

Eleviamo al quadrato ambo i termini:

$$2 = 1 + 2x + x^2$$

Sottraiamo 1 ad ambo i membri e nel secondo membro raccogliamo la x

$$1 = x\,(\,2 + x\,)$$

Dividiamo ambo i termini per 2 + x

$$x = \frac{1}{2 + x}$$

Sostituiamo nell'uguaglianza iniziale

$$\sqrt{2} = 1 + \frac{1}{2+x}$$

Sostituiamo alla x il suo valore in ogni evenienza, otteniamo una frazione continua semplice infinita

$$\sqrt{2} = 1 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots}}}}$$

Che possiamo scrivere : $\sqrt{2} = [1;\ 2, 2, 2, 2, \ldots]$.
Come possiamo notare il quoziente parziale 2 si ripete costantemente, pertanto possiamo affermare la frazione continua è periodica di periodo 2: quindi possiamo scriverla:
144

$$\sqrt{2} = [1\ ;\ \bar{2}]$$

Andiamo ora alla ricerca delle frazioni ridotte o convergenti:

$$\frac{1}{1}\ ;\ \frac{3}{2}\ ;\ \frac{7}{5}\ ;\ \frac{17}{12}\ ;\ \frac{41}{29}\ ;\ \frac{99}{70}\ ;\ \frac{239}{169}\ ;\ \frac{577}{408}\ ;\ \frac{1393}{985}\ ;\ \frac{3363}{2378}\ ;\ \ldots$$

Come per i razionali le frazioni d'ordine pari approssimano $\sqrt{2}$ per difetto, mentre quelle d'ordine dispari l'approssimano per eccesso

$$\frac{1}{1} < \sqrt{2} < \frac{3}{2}$$
$$\frac{7}{5} < \sqrt{2} < \frac{17}{12}$$
$$\frac{41}{29} < \sqrt{2} < \frac{99}{70}$$
$$\frac{239}{169} < \sqrt{2} < \frac{577}{408} = 1{,}414215686$$
$$1{,}414213198 = \frac{1393}{985} < \sqrt{2} < \frac{3363}{2378} = 1{,}414213625$$

La calcolatrice scientifica dà per valore di $\sqrt{2}$ = 1,414213562 , come si nota dalla frazione convergente $\frac{1393}{985}$ si hanno 6 cifre decimali esatte: tale frazione dà un'approssimazione a meno di 10^{-6} migliore rispetto alle classi contigue di sopra.

Dallo sviluppo dei due radicali si nota una periodicità e questo in linea con quanto dimostrato nel teorema di Lagrange:

Teorema di Lagrange: Lo sviluppo in frazione continua di un numero reale α è periodico se e solo se α è irrazionale quadratico.

Proprietà delle ridotte o dei convergenti

Anche per lo sviluppo dei numeri irrazionali possiamo individuare alcune proprietà delle ridotte:
-) Le ridotte di indice dispari decrescono strettamente, mentre le ridotte d'ordine pari crescono strettamente
-) Ogni ridotta d'indice dispari è maggiore di ogni ridotta di indice pari
-) Il valore α del numero razionale od irrazionale (in generale reale) è maggiore di ogni ridotta di indice pari ed è minore di ogni ridotta di indice dispari; se α è razionale, esso è uguale

all'ultima ridotta *n*-sima; se α è irrazionale la successione infinita delle ridotte converge ad α stesso.
-) ogni numero razionale può essere espresso in due modi come frazione continua, il primo modo è quello di considerare le convergenti d'ordine pari; il secondo modo è quello di considerare le convergenti d'ordine dispari: le due successioni presi indipendentemente. Mentre ogni numero irrazionale può essere epresso in un nuico modo come frazione infinità: esso è l'elemeto di separazione tra le convergenti d'ordine pari e quelle di ordine dispari.
Teorema: La successione infinita delle ridotte è sempre convergente.

Approssimazione dei numeri reali mediante numeri razionali:

I numeri decimali, che possono essere finiti o periodici (semplici o misti) non hanno mai dato alcun problema ai matematici nei calcoli, in quanto è possibile mediante regole operative renderli frazionari. Con l'avvento dei numeri irrazionali, come le radici quadrate dei numeri naturali non quadrati perfetti , i matematici si sono sempre posti il problema di *approssimazione*: infatti la parte decimale è costituita da infinite cifre prive di periodicità. L'avvento poi delle macchine calcolatrici, il cui insieme dei numeri macchina ha un numero finito di elementi, ha reso più urgente la necessità dell'approssimazione dei numeri irrazionali ed in generale dei numeri reali: cioè cercare quel numero decimale finito o frazione che approssimi in modo migliore il valore effettivo o teorico del numero irrazionale e non limitarsi ai metodi macchina di arrotondamento o troncamento del numero aperiodico infinito. Uno dei metodi escogitati è quello delle frazioni continue.

Definiamo migliore approssimazione razionale di un numero reale α un numero che ha la caratteristica di essere più prossimo ad α di qualunque altra approssimazione con un denominatore più piccolo.
Si dimostra che le ridotte o convergenti $c_n = \frac{p_n}{q_n}$ di una frazione continua aritmetica, di ordine maggiore od uguale ad 1, sono le migliori approssimazioni per un numero irrazionale α : cioè se $c_n = \frac{a_n}{b_n}$ (ridotta ai minimi termini), allora non vi è alcuna frazione con denominatore inferiore a b_n, che approssimi α meglio di c_n ; e, di più, ogni convergente $\frac{p}{q}$ è tale che

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} .$$

Teorema di Hurwitz: Per ogni irrazionale α esistono infiniti razionali $\frac{p}{q}$ tali che $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$

Ad esempio abbiamo visto che $\frac{99}{70}$ è una ridotta dello sviluppo in frazione continua di $\sqrt{2}$; ebbene, non vi è alcuna frazione con denominatore minore di 70 che approssimi $\sqrt{2}$ meglio di $\frac{99}{70}$, per esso vale il Teorema di Hurwitz

$$\left|\sqrt{2} - \frac{99}{70}\right| < \frac{1}{\sqrt{5} \cdot 70^2}$$

Facendo i calcoli su una calcolatrice scientifica si ha:

$$0{,}000072151 \; < \; 0{,}000091268$$

Il teorema di Lagrange ci ha permesso di trovare una certa regolarità nello sviluppo in frazione continua dei numeri irrazionali quadratici: cioè essi sono periodici; anzi le radici quadrate dei numeri naturali non quadrati perfetti non solo sono periodici ma tali espansioni sono palindrome: infatti se il periodo è $\overline{a_1, a_2, a_3, \ldots, a_n, 2a_0}$ gli elementi $a_1, a_2, a_3, \ldots, a_n$ presentano simmetria:

$$a_1 = a_n \; ; \; a_2 = a_{n-1} \; ; \; a_3 = a_{n-2} \; ; \ldots$$

Nello studio dello sviluppo in frazioni continue di numeri irrazionali, non esistono molti numeri irrazionali, oltre ai quadratici, di cui si conosca qualche aspetto di regolarità. Eulero nel 1737 nello sviluppare alcuni di questi trovò alcune regolarità in:

a) $e = [2 \, ; 1 \, , 2 \, , 1 \, , 1 \, , 4 \, , 1 \, , 1 \, 6 \, , 1 \, , 1 \, , 8 \, , \ldots]$

b) $e^{\frac{1}{k}} = [1 \, ; k-1 \, , 1 \, , 1 \, , 3\,k-1 \, , 1 \, , 1 \, , 4k-1 \, , 1 \, , 1 \, , 5k-1 \, , \ldots.] \quad k \in N_o$

c) $\frac{e-1}{e+1} = [0 \, , 2 \, , 6 \, , 10 \, , 14 \, , \ldots.]$

d) $\frac{e^{\frac{2}{k}}-1}{e^{\frac{2}{k}}+1} = [0 \, , k \, , 3k \, , 5k \, , \; 7k \, , \ldots]$

e) $\tan(\frac{1}{k}) = [0 \, ; k-1 \, ; 1 \, ; \; 3k-2 \, ; 1 \, ; 1 \, ; 5k-2 \, ; 1 \, ; 7k-2 \, ; 1 \;] \; ;$

f) $\tanh\left(\frac{1}{k}\right) = \frac{e^{\frac{1}{k}} - e^{-\frac{1}{k}}}{e^{\frac{1}{k}} + e^{-\frac{1}{k}}} = [0 \, ; k \, ; 3k \, ; 5k \, ; \ldots.]; \ldots$

Anche lo sviluppo della *sezione aurea* presenta regolarità e che ancor di più, ordinando i numeratori delle sue convergenti , si ottiene la successione di Fibonacci

$$\frac{\sqrt{5}-1}{2} = 0 + x$$

Da cui , razionalizzando il numeratore si ha .

$$x = \frac{5-1}{2(\sqrt{5}+1)} = \frac{4}{2(\sqrt{5}+1)} = \frac{1}{\frac{\sqrt{5}+1}{2}} = \frac{1}{1+\frac{\sqrt{5}-1}{2}}$$

$$\frac{\sqrt{5}-1}{2} = 0 + \frac{1}{1+\frac{\sqrt{5}-1}{2}} = 0 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{\sqrt{5}-1}{2}}}} = 0 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\cdots}}}}$$

Formalizzando si ha

$$\frac{\sqrt{5}-1}{2} = [0 \, ; 1 \, , 1 \, , 1 \, , 1 \, , \ldots] = [0 \, ; \, \overline{1}]$$

Le cui convergenti risultano:

$$\frac{0}{1}\ ;\ \frac{1}{1}\ ;\ \frac{1}{2}\ ;\ \frac{2}{3}\ ;\ \frac{3}{5}\ ;\ \frac{5}{8}\ ;\ \frac{8}{13}\ ;\ldots$$

La successione dei numeratori costituisce la successione di Fibonacci: 0 , 1, 1, 2, 3, 5, 8, 13, ….
Inoltre vale la seguente affermazione:
“ Presi comunque due convergenti successivi: $\frac{p_{n-1}}{q_{n-1}}$ e $\frac{p_n}{q_n}$, vale la seguente relazione:

$$p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^{n-1} \quad \text{“}$$

Esempio. Prendiamo il 4° e il 5° convergente $\frac{3}{5}\ ;\ \frac{5}{8}$ e verifichiamo la relazione:

$$5 \cdot 5 - 3 \cdot 8 = 25 - 24 = 1 = (-1)^{5-1}$$

Così se prendiamo il 5° e il 6° convergente: $\frac{5}{8}\ ;\ \frac{8}{13}$ e verifichiamo la relazione:

$$8 \cdot 8 - 5 \cdot 13 = 64 - 65 = -1 = (-1)^{6-1}$$

In entrambi i casi la relazione e verificata e così in generale.

Questo programma determina la frazione continua di un numero irrazionale quadratico misto: della forma

$$\frac{c + \sqrt{a}}{d}$$

Con $d \neq 0$, $a > 0$ e a non sia un quadrato perfetto.

```
program Sviluppo_di_un_numero_irrazionale_in_frazione_continua;
{$N+}
uses crt;
var num,num1,k,i,c,c1,d,d1:integer;
   rad,q,r,q1,x,y,num2:real;
   a:array[1..100] of real;
   risp:char;
function p(i:integer):real;
begin
 if i=1 then p:=a[1]
       else if i=2 then p:=a[1]*a[2]+1
                else if i=3 then p:=a[1]*a[2]*a[3]+a[1]+a[3]
                         else p:=a[i]*p(i-1)+p(i-2)
end;
function t(i:integer):real;
begin
 if i=1 then t:=1
       else if i=2 then t:=a[2]
                else if i=3 then t:=a[2]*a[3]+1
                         else t:=a[i]*t(i-1)+t(i-2)
end;
```

```
begin
 repeat
  clrscr;
  textcolor(15);
  writeln('Questo programma ti permette di determinare la frazione continua di');
  writeln('una frazione irrazionale nella forma [a0,a1,a2,...,aN], dove a0,a1.. ');
  writeln('sono i quozienti parziali della frazione continua; ed inoltre deter-');
  writeln('mina l frazioni ridotte o convergenti della stessa frazione continua.');
  writeln;
  writeln('Immetti il numeratore : ');
  write('Immetti la parte intera : a = ');readln(c);c1:=c;
  repeat
     write('Immetti il numero sotto radice quadrata: b = ');
     readln(num);
     num2 := int(sqrt(num))
  until (num > 0) and (num<> sqr(num2));
  writeln('Immetti il denominatore : ');
  repeat write('Immetti un numero intero : d = ');readln(d);d1:=d;
  until d<>0;
  num1:=num;
  k:=1;
  rad:=(c+sqrt(num))/d;
  q:=int(rad);
  r:=rad-q;
  q1:=q;
  repeat
    a[k]:=q;
    r:=1/r;
    q:=int(r);
    r:=r-q;
    k:=k+1;
  until (k>6);
  textcolor(12);
  write('( ',c1,'+ û',num1,') / ',d1,' = [');
  for i:=1 to k-1 do
     write(a[i]:2:0,',');
  write(',...]');
  textcolor(15);
  writeln;writeln;
  writeln('Notare la frazione continua è periodica mista.');
  writeln(' Le frazioni ridotte o convergenti sono: ');
  textcolor(12);
  for i:=1 to k-1 do
```

```
 begin
    x:=p(i);
 y:=t(i);
 write(x:3:0,'/',y:3:0,' , ');
 end;
 writeln;writeln;
 textcolor(14);
 write(' Vuoi continuale con altri valori ? (S/N) ');
 readln(risp);
until (risp = 'N') or (risp='n');
 end.
```

Equazioni diofantee lineari

Diofanto, insigne matematico vissuto tra il 250 e il 350 d.C., trattò nella sua opera *Arithmetica* una serie di problemi relativi alla risoluzione di equazioni e sistemi di equazioni a coefficienti interi a una o più incognite, le cui soluzioni fossero a loro volta intere. Storicamente per il rilievo che viene dato alla risoluzione di problemi indeterminati, la disciplina che tratta questo argomento, noto anche come *analisi indeterminata*, ha ricevuto l'appellativo di *Analisi Diofantea*.

Def. Sia f(x,y,z,…) un polinomio nelle variabili x,y,z,… a coefficienti interi o razionali, viene detta equazione diofantea il problema di trovare una soluzione dell'equazione

$$f(x,y,z,\dots) = 0$$

per valori interi delle variabili x,y,z,….

Le equazioni diofantee si classificano , come le equazioni algebriche ordinarie, a seconda del grado del polinomio f(x,y,z,…) e si diranno , in corrispondenza, di primo grado o lineari, di secondo grado o quadratiche, di terzo grado o cubiche , ecc.

Consideriamo un'equazione lineare diofantea di primo grado a due incognite:

1) $a x + by = c$

con a,b,c ∈ **Z** . Essa in generale nel campo dei numeri razionali ammette infinite soluzioni, al variare di una delle incognite possiamo trovare le soluzioni dell'altra : posto y = k allora

$$x = \frac{c-bk}{a} \qquad \text{con } a \neq 0$$

Pertanto le infinite coppie $\left(\frac{c-bk}{a}\ ; k\right)$ costituiscono le soluzioni, ora per determinare quelle intere: cioè (h, k) con h,k ∈ **Z** , possiamo sfruttare il Teorema di Bézout, che afferma:

Teorema: Condizione necessaria e sufficiente perché l'equazione 1) ammetta soluzioni intere e che il termine noto c sia multiplo del massimo comun divisore tra a e b .

Questo teorema è una logica conseguenza dell'identità dello stesso Bézout. Ora molte questioni che coinvolgono il MCD tra due numeri interi positivi si servono dell'algoritmo euclideo delle divisioni successive: nel caso dell'equazione diofantea del tipo 1) l'algoritmo euclideo non solo permette di riconoscere quando l'equazione ammette soluzione , ma offre anche un procedimento costruttivo per determinarle.

Ad esempio vogliamo determinare, nel caso esistono, le soluzioni dell'equazione diofantea

$$46\,x + 12\,y = 48$$

Risoluzione: Applicando il Teorema di Bézout si ha: MCD (46 , 12) = 2 ; $48 = 2 \cdot 24$, pertanto essendo il termine noto 48 multiplo di 2 = MCD (46 ; 12) , l'equazione è risolvibile.

Applichiamo l'algoritmo euclideo:

$46 = 3 \cdot 12 + 10 \quad \rightarrow \quad \frac{46}{12} = 3 + \frac{10}{12} = 3 + \frac{1}{\frac{12}{10}}$

$12 = 1 \cdot 10 + 2 \quad \rightarrow \quad \frac{12}{10} = 1 + \frac{2}{10} = 1 + \frac{1}{\frac{10}{2}} = 1 + \frac{1}{5}$

$10 = 5 \cdot 2 \quad \rightarrow \quad \frac{46}{12} = 3 + \frac{1}{1+\frac{1}{5}}$

Con scrittura sintetica : $\frac{46}{12} = [3; 1, 5]$ costituisce una frazione continua i cui convergenti

Sono $\frac{3}{1}$; $\frac{4}{1}$; $\frac{46}{12}$. Scelto il penultimo convergente prendiamo u = -1 e v = 4 si ha

$$46 \cdot (-1) + 12 \cdot 4 = -46 + 48 = 2$$

Moltiplico ambo i termini per 24 e si hanno le soluzioni:

$$46 \cdot (-24) + 12 \cdot 96 = -1104 + 1152 = 48$$

Pertanto x = - 24 e y = 96 è una coppia di soluzioni dell'equazione data; ulteriori coppie

Sono date da $\begin{cases} x_k = x_0 + k\frac{b}{MCD(a,b)} \\ y_k = y_0 - k\frac{a}{MCD(a,b)} \end{cases}$ con k = 1,2,3 ,…

Per k = 1 $\rightarrow$ $\begin{cases} x_1 = -24 + \frac{12}{2} = -18 \\ y_1 = 96 - \frac{46}{2} = 73 \end{cases}$ pertanto la coppia $(-18\,;\,73)$ è una soluzione:

160

infatti $46 \cdot (-18) + 12 \cdot 73 = -828 + 876 = 48$

e così via con altri valori di k, essendo indeterminata l'equazione ammette infiniti valori come ci si attendeva .

Il seguente programma in Turbo Pascal ti permette di risolvere l'equazione lineare di Diofanto:

151

ax + by = c sotto la condizione che MCD(a ; b) sia un divisore di c col metodo delle frazioni continue relative al numero razionale $\frac{a}{b}$

```
program Equazione_lineare_diofantea;
uses crt;
var num,den,num1,den1,deno,nume,a2,b2,k,i,q,r,h,j,x,y,c,c1:integer;
   a:array[1..100] of integer;
   risp:char;
function mcd(w,s:integer):integer;
var resto:integer;
begin
 resto:=w mod s;
 while resto <> 0 do
      begin
       w:=s; s:=resto;
       resto:=w mod s;
      end;
 mcd:=s;
end;
function p(i:integer):integer;
begin
 if i=1 then p:=a[1]
       else if i=2 then p:=a[1]*a[2]+1
                  else if i=3 then p:=a[1]*a[2]*a[3]+a[1]+a[3]
                             else p:=a[i]*p(i-1)+p(i-2)
end;
function t(i:integer):integer;
begin
 if i=1 then t:=1
       else if i=2 then t:=a[2]
                  else if i=3 then t:=a[2]*a[3]+1
                             else t:=a[i]*t(i-1)+t(i-2)
end;
begin
```

```
repeat
clrscr;
textcolor(10);
writeln('Questo programma ti permette di determinare la frazione continua di');
writeln('una frazione razionale nella forma [a0,a1,a2,...,aN], dove a0,a1.. ');
writeln('sono i quozienti parziali della frazione continua; inoltre determina');
writeln('le frazioni ridotte o convergenti: la penultima frazione ridotta');
writeln('permette di risolvere l''equazione lineare diofantea o il teorema');
writeln('di Bezout ax+by=c, sotto la condizione che MCD(a,b) divide c.');
writeln;
textcolor(12);
write('Immetti il numeratore della frazione: a = ');readln(num);
write('Immetti il denominatore della frazione: b = ');readln(den);
num1:=num;
den1:=den;
k:=0;
repeat
  k:=k+1;
  q:=num div den;
  r:=num mod den;
  a[k]:=q;
  num:=den;
  den:=r;
until r<1;
textcolor(13);
write(num1,'/',den1,' = [',a[1]);
for i:=2 to k do
   write(‘ , ‘,a[i]);
write(']');
writeln;
textcolor(15);
writeln('Le frazioni ridotte o convergenti della frazione continua trovata sono');
for j:=1 to k-1 do begin
x:=p(j);
y:=t(j);
write(x,'/',y,' ; ');
end;
write(p(k),’/’,t(k));
writeln;
writeln('Inoltre risolve l''equazione indeterminata ax + by = c ');
write('Immetti il termine noto dell''equazione c = ');readln(c);
nume:=p(k-1);
deno:=t(k-1);
```

```
c1:=c div mcd(num1,den1);
if c mod mcd(num1,den1) = 0 then
begin
if num1*deno<den1*nume then begin a2:=-deno; b2:=nume end
          else begin a2:=deno; b2:=-nume end;
writeln('x = ',c1*a2,' e y = ',c1*b2);
writeln('dove x = ',c1,'*(',a2,') e  y = ',c1,'*(',b2,')');
writeln(num1*c1*a2,' + ',den1*c1*b2,' = ',c);
end
else
writeln('L''equazione diofantea ',num1,'x + ',den1,' y = ',c,' non Š risolvibile');
readln;
textcolor(26);writeln;writeln;
gotoxy(4,24);
write('Vuoi ripetere con altra frazione ? (S/N) ');
gotoxy(46,24);readln(risp);
until (risp='N') or (risp='n');
end.
```

Equazioni diofantee quadratiche

Tra tutte le equazioni di secondo grado a più incognite consideriamo quelle a due a coefficienti interi. Poiché tali equazioni presentano più incognite esse sono indeterminate: cioè se ammettono soluzioni queste sono infinite. Le equazioni indeterminate di secondo grado a due incognite vanno sotto il nome di coniche e sono della forma:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Tali equazioni se soggette ad opportune trasformazioni lineari affini è possibile ridurle alla forma

$$X^2 - DY^2 = 1$$

Tale forma è detta *Equazione di Pell,* qualora D non è un quadrato perfetto e le soluzioni di essa vanno ricercate in Z. Quindi le equazioni di Pell sono un sottoinsieme delle equazioni quadratiche a coefficienti interi e a soluzioni a loro volta intere: cioè sono equazioni diofantee.

Def. Si chiama equazione di Pell l'equazione diofantea $x^2 - Dy^2 = 1$, dove D è un numero intero positivo che non sia un quadrato perfetto.

Il primo metodo sistematico per risolvere tale equazione fu escogitato da Lord Brouncker nel 1657. Tale metodo consiste nello sviluppare in frazione continua $\sqrt{D}$ e prendere quella frazione ridotta o convergente dello sviluppo tale che il denominatore e il numeratore sostituiti alle incognite risolvono l'equazione. Successivamente sia Wallis che Fermat affermarono di aver

dimostrato che tale equazione è sempre risolvibile per interi; quest'ultimo aggiunse che tali soluzioni intere sono infinite . Tuttavia la prima dimostrazione pubblicata di quest'ultima affermazione si deve a Lagrange nel 1766. Per inciso va detto che l'equazione fu associata al nome di Pell per errore da Eulero, credendo questi che il metodo di soluzione esibito da Wallis fosse dovuto a John Pell , un matematico inglese dello stesso periodo.

Proposizione: Se (x_1 ; y_1) è una soluzione dell'equazione $x^2 - Dy^2 = \pm 1$, allora la frazione $\frac{x_1}{y_1}$ è una ridotta o convergente dello sviluppo in frazione continua di $\sqrt{D}$: cioè $\frac{x_1}{y_1} = \frac{p_n}{q_n}$ per qualche *n.* Tale frazione approssima il valore di $\sqrt{D}$: cioè vale la relazione

$$\left|\frac{x_1}{y_1} - \sqrt{D}\right| < \frac{1}{y_1^2}$$

Consideriamo la frazione continua

$$\sqrt{D} = [a_0\,;\, a_1\,,\ a_2\,, a_3\,, \ldots, a_n\,, 2a_0] = a_0 + \frac{1}{a_1 +}\,\frac{1}{a_2 +}\,\frac{1}{a_3 +}\ldots\frac{1}{a_n +}\,\frac{1}{2a_0 +}\ldots$$

Per mostrare che l'equazione di Pell ha infinite soluzioni e che queste sono ottenute a partire da ridotte o convergenti di $\sqrt{D}$ che corrispondono ai termini alla fine di ogni periodo, si procede in questo modo:

1) Se n è dispari il numeratore ed il denominatore di queste convergenti sono soluzioni dell'equazione di Pell: cioè le coppie $(p_n\,;\, q_n)$, $(p_{2n}\,;\, q_{2n})$, $(p_{3n}\,;\, q_{3n})$ …..
2) Se n è pari tali convergenti forniscono alternativamente soluzioni dell'equazione con termine noto -1 e dell'equazione di Pell.:
   a) Per -1 le coppie sono $(p_n\,;\, q_n)$, $(p_{2n}\,;\, q_{2n})$, $(p_{3n}\,;\, q_{3n})$ …..
   b) Per $+1$ le coppie sono $(p_{2n+1}\,;\, q_{2n+1})$, $(p_{4n+3}\,;\, q_{4n+3})$, $(p_{6n+5}\,;\, q_{6n+5})$ …..

Pertanto l'equazione di Pelle è sempre risolvibile, come affermato da Fermat, mentre l'equazione con -1 non è sempre risolvibile. Il teorema, che andremo ad enunciare, permetterà di trovare altre soluzioni senza ricorrere alle ulteriori convergenti della frazione continua relativa a $\sqrt{D}$.

Se la coppia (x ; y) non è la soluzione banale dell'equazione di Pell, allora essa è una soluzione positiva se e soltanto se $x + y\sqrt{D} > 1$.

Def. Si chiama *soluzione fondamentale dell'equazione di Pell* quella soluzione positiva che rende minimo il valore dell'espressione $x + y\sqrt{D}$

Teorema: Se la coppia (x_1 ; y_1) è la soluzione fondamentale dell'equazione di Pell, allora tutte le altre soluzioni positive (x_k ; y_k) possono essere ottenute dall'identità:

$$x_k + y_k\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^k$$

Per trovare la soluzione minima positiva possiamo applicare un procedimento puramente algebrico: cioè determinare il valore minimo di k relativo all'espressione $1 + D\,k^2$ in modo tale che questa sia un quadrato perfetto e successivamente porre $y = k_{min}$ e calcolare successivamente $x = \sqrt{1 + D\,y^2}$

NB. Le soluzioni dell'equazione di Pell forniscono un metodo di approssimazione dei numeri reali che sono radici quadrate di interi positivi. La ricerca di tali soluzioni offre un metodo rapido di convergenza di valori approssimanti tali radici quadrate.

Esempio: Data l'equazione $x^2 - 3y^2 = 1$ determinare eventuali coppie (x ; y) di interi positivi che risolvono tale equazione.

Risoluzione. Intanto si tratta di una equazione di Pell, pertanto essa è risolvibile per valori interi positivi delle incognite. Applichiamo il metodo dei convergenti di $\sqrt{3}$, dopo aver calcolato i quozienti parziali col metodo escogitato da Bombelli: intanto $1 < \sqrt{3} < 2$, pertanto possiamo scrivere

1) $\sqrt{3} = 1 + x$ con $0 < x < 1$

Eleviamo ambo i termini della 1) al quadrato, otteniamo

$3 = 1 + 2x + x^2$

Sottraiamo ad ambo i membri di quest'ultima 1 e raccogliamo la x a secondo membro , otteniamo

$2 = x\,(2 + x)$, da cui operando si ha

$$x = \frac{2}{2+x} \quad \rightarrow \quad x = \frac{1}{1+\frac{x}{2}} \quad \text{et} \quad \frac{x}{2} = \frac{1}{2+x}$$

Andando a sostituire in 1) e poi a catena le due ultime relazioni, abbiamo

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2+..}}}}$$

Ottenendo così lo sviluppo in frazione continua di $\sqrt{3}$, che possiamo anche scrivere:

$$\sqrt{3} = [1\,;\ 1\,,2\,,1,2\,,\ldots]$$

Poiché $\sqrt{3}$ è un numero irrazionale quadratico la frazione continua risulta periodica; possiamo quindi scrivere

$$\sqrt{3} = [1\,;\ \overline{1\,,2}\ ]$$

Le frazioni ridotte o convergenti risultano : $\frac{1}{1}$, $\frac{2}{1}$, $\frac{5}{3}$; poiché la lunghezza del periodo è 2 = n+1, allora n =1 è dispari la coppia (2 ; 1) relativa alla convergente $\frac{2}{1}$ risolve la nostra equazione, tale coppia risulta minimale positiva; se voglio ottenere le ulteriori soluzioni positive basta estendere il periodo e trovare le convergenti d'ordine dipari:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad , \ldots$$

$$\frac{1}{1} \ , \ \frac{2}{1} \ , \ \frac{5}{3} \ , \ \frac{7}{4} \ , \ \frac{19}{11} \ , \ \frac{26}{15} \ , \ \frac{71}{41} \ , \frac{97}{56} \ , \text{ ecc.}$$

Le coppie che risolvono l'equazione sono:

$$(2 ; 1) \ , \ (7 ; 4) \ , \ (26 ; 15) \ , \ (97 ; 56) \ , \ \ldots.$$

Un altro metodo, fondandosi sul Teorema enunciato sopra, ci permette, nota la coppia fondamentale (2 ; 1), di trovare le ulteriori coppie soluzione:

$$x_k + y_k\sqrt{3} = (2 + 1\cdot \sqrt{3})^{k} \text{ con } k = 1 , 2, 3, \ldots.$$

per $k = 2 \rightarrow x_2 + y_2\sqrt{3} = (2 + 1\cdot \sqrt{3})^{2} = 4 + 3 + 4 \cdot \sqrt{3} = 7 + 4\cdot \sqrt{3} \rightarrow (7 ; 4)$

per $k = 3 \rightarrow x_3 + y_3\sqrt{3} = (2 + 1\cdot \sqrt{3})^{3} = 8 + 12\cdot \sqrt{3} + 18 + 3\cdot \sqrt{3} = 26 + 15\cdot \sqrt{3} \rightarrow (26 ; 15)$

…… così di seguito.

Verifichiamo che la coppia (26 ; 15) approssima il valore $\sqrt{3}$ con una accuratezza superiore all'inverso del quadrato di 15:

$$\left|\frac{26}{15} - \sqrt{3}\right| < \frac{1}{15^2}$$

Infatti , sviluppando i calcoli si ha che $0{,}001282525 < 0{,}00\overline{4}$; se volessimo una maggiore accuratezza, basterebbe scegliere la coppia (97 ; 56):

$$\left|\frac{97}{56} - \sqrt{3}\right| < \frac{1}{56^2}$$

Sviluppando i calcoli, si ha: 0,000092049 < 0,000318877.

Abbiamo detto sopra che ogni equazione di secondo grado a due incognite è possibile mediante opportune trasformazioni affini trasformarle in equazioni del tipo $x^2 + D y^2 = 1$. Se $D < 0$, allora tale equazione è un'equazione di Pell e pertanto di questa possiamo individuare le infinite soluzioni intere positive, se $D \geq 0$,allora l'equazione trasformata ammette solo come soluzione positiva quel-la banale (1 ; 0) . Vediamo con un esempio quanto detto:

Sia data l'equazione $2x^2 + 36xy + 15y^2 - 16x - 18y + 6 = 0$. Dopo averla trasformata nella forma $x^2 - D\,y^2 = 1$, determinare di questa eventuali valori interi positivi di x e y che la verificano.
A tal proposito applichiamo la seguente trasformazione affine equivalente:

$$\begin{cases} x \to \frac{2}{7}x + \frac{3}{7}y + \frac{1}{7} \\ y \to -\frac{1}{7}x + \frac{2}{7}y + \frac{3}{7} \end{cases}$$

all'equazione data, otteniamo

$$\frac{2}{49}(2x + 3y + 1)^2 + \frac{36}{49}(2x + 3y + 1)(-x + 2y + 3) + \frac{15}{49}(-x + 2y + 3)^2 +$$

$$-\frac{16}{7}(2x + 3y + 1) - \frac{18}{7}(-x + 2y + 3) + 6 = 0$$

Operando algebricamente e riducendo i monomi simile si ha

$$x^2 - 6\,y^2 = 1$$

che risulta un'equazione di Pell, essendo $D = 6 > 0$. Cerchiamo la soluzione positiva minimale col metodo delle frazioni continue:

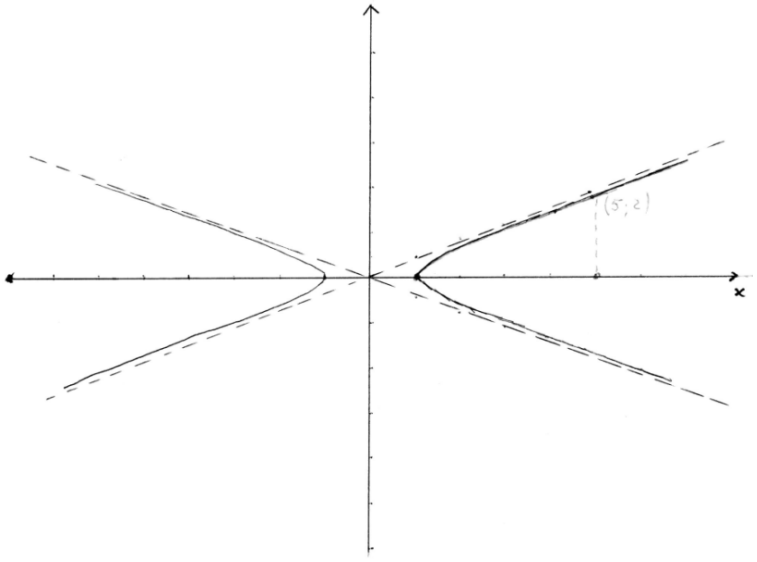
Ora la $\sqrt{6}$ sviluppata in frazione continua risulta:

$$\sqrt{6} = [\,2; \overline{2\,,\,4}\,] = 2 + \cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{4+\cdots}}}} = 2 + \frac{1}{2+}\ \frac{1}{4+}\ \frac{1}{2+}\ \frac{1}{4+}\ \ldots.$$

Le cui ridotte o convergenti sono: $\frac{2}{1}, \frac{5}{2}, \frac{22}{9}, \frac{49}{20}, \frac{218}{89}, \ldots$

Poiché la lunghezza del periodo è 2 = n+1 , n = 1 è dispari ; pertanto la coppia (5 , 2) è la soluzione minimale ; l'ulteriore soluzione è (49 ; 20) , ecc

Diamo qui per inciso che la rappresentazione grafica dell'equazione di Pell è un'iperbole di centro (0 ; 0) con asse trasverso y = 0 vertice di coordinate positive è la soluzione banale (1 ; 0) e asinto-ti le rette $x - \sqrt{6} = 1$ e $x + \sqrt{6}y = 1$



Qualora effettuata la trasformazione il D dovesse risultare negativo, allora l'equazione

$$x^2 - D\,y^2 = 1$$

risulterebbe l'equazione di una ellisse di centro (0 ; 0) , assi x=0 e y=0 e vertici (1,0) , (-1,0) , $\left(0\,;\,\frac{1}{\sqrt{D}}\right)$, $\left(0\,;\,-\frac{1}{\sqrt{D}}\right)$ e pertanto l'unica soluzione a soluzioni intere positive è quella banale (1 ; 0).

Esempio: Sia data l'equazione $46x^2 - 26xy + 9y^2 + 30x - 10y + 4 = 0$. Dopo averla trasformata nella forma $x^2 - D\,y^2 = 1$, determinare di questa eventuali valori interi positivi di x e y che la verificano.

A tal proposito applichiamo la seguente trasformazione affine equivalente:

$$\begin{cases} x \to \frac{1}{7}x + \frac{2}{7}y - \frac{2}{7} \\ y \to \frac{3}{7}x - \frac{1}{7}y + \frac{1}{7} \end{cases}$$

all'equazione data, otteniamo

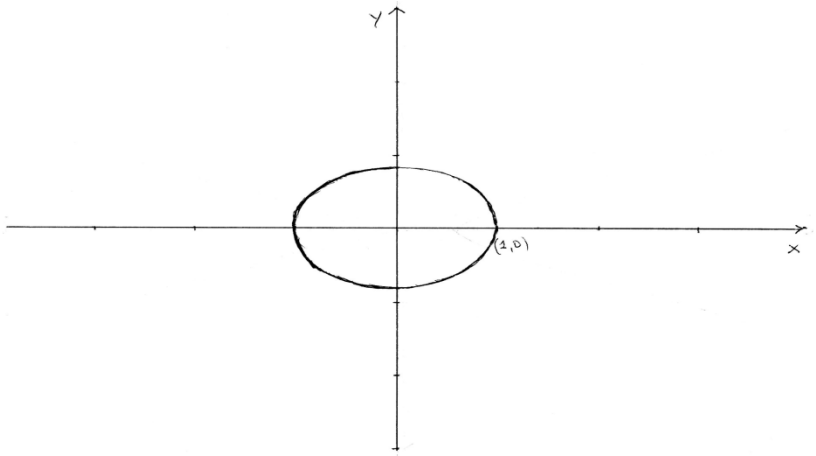
$$\frac{46}{49}(x+2y-2)^2 - \frac{26}{49}(x+2y-2)(3x-y+1) + \frac{9}{49}(3x-y+1)^2 +$$

$$+\frac{30}{7}(x+2y-2) - \frac{10}{7}(3x-y+1) + 4 = 0$$

Operando algebricamente e riducendo i monomi simile si ha

$$x^2 + 5\,y^2 = 1$$

equazione che risulta verificata da coordinate positive esclusivamente da (1 ; 0): infatti rappresentando tale equazione in un sistema di assi cartesiani si ha:



Il seguente programma in Turbo Pascal ti permette di risolvere l'equazione di Pell col metodo delle frazioni continue del numero irrazionale quadratico $\sqrt{D}$

```
program Risoluzione_Equazione_di_Pell_con_le_frazioni_continue;
{$N+}
uses crt;
label 1,2;
var num,num1,k,i:integer;
    rad,q,r,q1,x,y:real;
    a,m:array[1..100] of real;
    risp:char;
function p(i:integer):real;
begin
  if i=1 then p:=a[1]
        else if i=2 then p:=a[1]*a[2]+1
                 else if i=3 then p:=a[1]*a[2]*a[3]+a[1]+a[3]
                          else p:=a[i]*p(i-1)+p(i-2)
end;
function t(i:integer):real;
begin
  if i=1 then t:=1
        else if i=2 then t:=a[2]
                 else if i=3 then t:=a[2]*a[3]+1
                          else t:=a[i]*t(i-1)+t(i-2)
end;
begin
 repeat
  clrscr;
  textcolor(14);
```

```
writeln('Questo programma ti permette di determinare la frazione ridotta o convergente');
 writeln('della frazione continua del numero irrazionale quadratico ûD, relativo ');
 writeln('all''equazione di Pell:   Xý - D Yý= ñ 1');
 writeln('E successivamente determina i valori della coppia ( X ; Y ) che risolvono');
 writeln('l''equazione sopra scritta.');
 writeln;
 textcolor(11);
 write('Immetti il numero intero: D = ( < 100 )');readln(num);
 num1:=num;
 textcolor(14);
 writeln;
 writeln('La frazione continua risulta periodica mista, gli elementi del periodo');
 writeln('sono posti dentro parentesi graffe se k > 2 ; se k=2, il periodo Š ');
 writeln('costituito dall''ultimo elemento: notare la simmetria dentro parentesi rotonda .');
 writeln;
 k:=1;
 rad:=sqrt(num);
 q:=int(rad);
 r:=rad-q;
 q1:=q;
   repeat
   a[k]:=q;
   r:=1/r;
   q:=int(r);
   r:=r-q;
   k:=k+1
 until q=2*q1;
 textcolor(12);
 if k<>2 then
    begin
     write('û',num1,' = [',a[1]:2:0,', {(');
     for i:=2 to k-2 do
             write(a[i]:2:0,' , ');
     write(a[k-1]:2:0, ' ) ,');
     write(' ',2*q1:2:0);
     writeln('}]');
    end
    else
      write('û',num1,' = [',a[1]:2:0,' , ', 2*q1:2:0,']');
 writeln;
 writeln('a[1]=',a[1]:3:0,';  k= ',k);
 x:=p(k-1);
 y:=t(k-1);
```

```
 textcolor(13); writeln;
 writeln('La frazione ridotta o convergente della frazione continua ');
 writeln('Risolvente l''equazione di Pell: Xý - ',num1,'Yý= ñ 1  Š : ',x:3:0,'/',y:3:0);
 writeln;
 writeln('Il valore di x = ',x:3:0,' mentre quello della y = ',y:3:0);
 writeln;
 If k mod 2 = 0
       then
        begin
          writeln('La coppia (x;y) risolve l''equazione Xý- ',num1,'Yý= -1, risultando n=k-2 pari');
          writeln('infatti: ',sqr(x):5:0,' - ',num1*sqr(y):5:0,' = -1');
        end
       else
        begin
          writeln('La coppia (x;y) risolve l''equazione Xý- ',num1,'Yý= 1, risultando n=k-2
dispari');
          writeln('infatti: ',sqr(x):5:0,' - ',num1*sqr(y):5:0,' = 1');
        end;
        writeln;
  textcolor(20);
  write('Vuoi ripetere con altri coefficienti ? (S/N) ');
 readln(risp);
 until (risp='n') or (risp='N');
 end.
```

Conclusione

Lo studio delle frazioni continue è molto importante più di quanto possa sembrare dalle applicazioni esposte precedentemente dall'approssimazione mediante frazioni di radicali quadratici, alla risoluzione di equazioni lineari diofantee e di equazioni di Pell. Oggi diverse teorie fanno uso di tale strumento per la sviluppo di strategie e algoritmi risolutivi nell'ambito della ricerca oggetto di studio : così la Teoria dei Frattali , la Teoria delle Stringhe, la Teoria del Caos o dei Sistemi dinamici Caotici.

La stessa funzione Zeta di Riemann è possibile esprimerla attraverso funzioni continue : infatti scritta attraverso la *trasformata di Mellin*:

$$\zeta\,(\mathrm{s}) = \frac{s}{s-1} - s \cdot \int_0^1 h(x) x^{s-1}\, dx$$

essa presenta la funzione *h(x)*, detta *mappa di Gauss*, come sviluppo in frazione continua di x, .

Se $x = [a_1, a_2, a_3, \ldots] = \frac{1}{a_1+\frac{1}{a_2+\frac{1}{a_3+\cdots}}}$, allora h(x) è il reciproco di x: cioè $h(x)=\frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor$, dove $\left\lfloor \frac{1}{x} \right\rfloor$ è il massimo valore di x minore di $\frac{1}{x}$.

Elenco

dei programmi in Turbo Pascal

CAPITOLO I

CAPITOLO II

CAPITOLO III

CAPITOLO IV

Bibliografia

J.H. Conway – R.K.Guy -- Il Libro dei Numeri -- Ed. Hoepli – Milano

H. Davenport -- Aritmetica Superiore -- Ed. Zanichelli – Bologna

L.E. Dickson -- History of the Theory of Numbers – Rep. Chelsea – AMS

F. Enriques – Questioni riguardanti le matematiche elementari – Ed. Zanichelli

F.Gauss – Disquisitiones Arithmeticae – (trd. Inglese W.C.Waterhouse) - Springer

Maraschini Palma -- Format-SPE -- Ed. Paravia

L.J.Mordel -- Diophantine equations -- Academie Pres

C.D. Olds -- Frazioni Continue – Ed. Zanichelli – Bologna

A. Weil -- Teoria dei Numeri – Ed. Einaudi - Torino

I N D I C E

CAPITOLO II : Funzione Gamma e Funzione Zeta

CAPITOLO III : Numeri primi e Primalità