MATEMATICA
DISCRETA

Argomenti di "Teoria dei Numeri" per le delle classi IV e V del Liceo Scientifico.

Sommario

$$\frac{\pi}{2} = \frac{2\times2\times4\times4\times6\times6\times\ldots}{3\times3\times5\times5\times7\times7\times\ldots}$$

Illustration 1: Identità di Wallis

	
Leonhard Euler (1707-1783)	Pierre de Fermat(1601-1665)
	
Leonardo Pisano(1170-1250)	Evariste Galois(1811-1831)
	

	
Marin Mersenne (1588-1648)	Hermann Minkowski (1864-1909)
	
K Friedrich Gauss (1777-1855)	Snirivasa Ramanujan (1887-1920)

Sui numeri primi

Importanza dei numeri primi

I numeri primi sono importanti perche' sono i "costituenti ultimi" i "mattoni" di tutti gli altri interi, cosi' come gli atomi sono i mattoni che formano la materia, etc. Indagare le proprieta' dei numeri primi equivale, quindi, a conoscere meglio i numeri interi stessi. Ecco i primi 50 numeri primi:

```
Table[Prime[i], {i, 1, 50}]
```

```
{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83,
 89, 97, 101, 103, 107, 109, 113, 127, 131,
 137, 139, 149, 151, 157, 163, 167, 173, 179,
 181, 191, 193, 197, 199, 211, 223, 227, 229}
```

Rappresentazione in fattori

Il teorema che e' alla base di tutto e' il Teorema Fondamentale dell'Aritmetica: *a parte l'ordine dei fattori,la scomposizione in fattori primi e' unica:*

$$n := 2^a \times 3^b \times 5^c \times 7^d \times 9^e \times 11^f \ldots = \prod_{i=1}^{\infty} p_i^{a_i}$$

I vari esponenti rivelano quante volte un dato numero primo "entra" nella scomposizione. In particolare, se un esponente e' nullo, il numero primo corrispondente non e'

presente tra i fattori:

```
FactorInteger[2^3 * 3^5 * 7^1]
```

```
{{2, 3}, {3, 5}, {7, 1}}
```

Quindi, conoscere la scomposizione equivale a conoscere la serie degli esponenti {a,b,c,d, ...} e questa rivela parecchie proprieta' del numero. Ad esempio: se n e' un quadrato perfetto, tutti gli esponenti devono essere pari. Come mai?

Numeri primi sempre piu' grandi. Perche'?

I numeri primi sono in numero illimitato (risultato dovuto ad Euclide). Questo significa che non esiste un primo che possa essere definito "l'ultimo dei numeri primi". Se fosse cosi', potremmo moltiplicare tutti questi primi e sommarci 1. Il risultato non sarebbe fattorizzabile in termine dei primi noti, eppure sarebbe piu' grande dell'ipotetico "ultimo".

La ricerca di numeri primi sempre piu' grandi ha varie motivazioni. Da sempre l'uomo ama collezionare cose rare e preziose. Cercare questi numeri e' come setacciare "pepite" nel greto di un fiume. Ma questi numeri, oggidi', sono anche diventati "utili" ....

Un processo asimmetrico: la criptografia digitale

Moltiplicare tra loro due numeri primi p e q (e trovare n=pq) non e' difficile. Molto piu' difficile e', dato n grande, trovare i suoi fattori q e p. Il metodo della forza bruta, cioe'

la divisione per tutti i primi piu' piccoli conosciuti, porta a tempi di elaborazione impossibili. Questo fatto puo' essere sfruttato nei protocolli criptografici: moltiplicando *si cifra*; fattorizzando *si decifra*.

Esempio steganografico

Come nascondere le tree cifre {a,b,c} di un codice personale all'interno di un singolo numero intero n, in modo che siano recuperabili in un secondo momento? Basta formare il numero $n = 2^a \times 3^b \times 5^c$:

$$\{3,\ 4,\ 7\} \to 2^3 \times 3^4 \times 5^7 = 50\,625\,000$$

E' chiaro che per ritrovare la tripletta {a,b,c} e' sufficiente decomporre il numero in fattori primi, cosa che si puo' fare in maniera univoca.
E' anche naturale che, se voglio raggiungere un buon grado di sicurezza, dovrei usare numeri primi MOLTO piu' gradi di 2,3 e 5. Inoltre, devo conservarli in un luogo sicuro, dato che mi servono nuovamente per la decodifica.

E' possibile inventare una formula per produrre primi in quantita' industriale?

L'esempio che segue mostra come il ragionamento "poiche' vale per questi primi casi, allora vale sempre" puo' condurre a false ipotesi. La seguente formula polinomiale:

$$p(\mathrm{n\_}) := n^2 + n + 41$$

produce infallibilmente solo numeri primi, per n=0, n=1, n=2 fino ad n=39. Ma per 40 fallisce miseramente:

```
Table[{n, p(n), PrimeQ[p(n)]}, {n, 0, 40}]
```

```
{{0, 41, True}, {1, 43, True}, {2, 47, True},
 {3, 53, True}, {4, 61, True}, {5, 71, True},
 {6, 83, True}, {7, 97, True}, {8, 113, True},
 {9, 131, True}, {10, 151, True}, {11, 173, True},
 {12, 197, True}, {13, 223, True}, {14, 251, True},
 {15, 281, True}, {16, 313, True}, {17, 347, True},
 {18, 383, True}, {19, 421, True}, {20, 461, True},
 {21, 503, True}, {22, 547, True}, {23, 593, True},
 {24, 641, True}, {25, 691, True}, {26, 743, True},
 {27, 797, True}, {28, 853, True}, {29, 911, True},
 {30, 971, True}, {31, 1033, True}, {32, 1097, True},
 {33, 1163, True}, {34, 1231, True}, {35, 1301, True},
 {36, 1373, True}, {37, 1447, True}, {38, 1523, True},
 {39, 1601, True}, {40, 1681, False}}
```

In realta' si puo' dimostrare che nessun polinomio come questo puo' produrre SOLTANTO numeri primi.
Compito per casa :-) : come mai e' invece evidente che deve fallire per n=41?

Come sono distribuiti i numeri primi?

Ci sono piu' numeri primi nell'intervallo tra 1 e un milione, oppure tra un milione e due milioni? C'e' una funzione di *Mathematica* PrimePi[n] in grado di dare il numero di primi inferiori ad n. Effettuando sottrazioni, si puo' determinare

che:

```
{PrimePi[10^6], PrimePi[2*10^6] - PrimePi[10^6]}
```

{78 498, 70 435}

Nel secondo intervallo vi sono circa 8000 primi in meno. Brutta notizia: *i numeri primi diventano sempre piu' rari andando avanti.*
Gauss fu il primo a trovare una formula approssimata per la funzione PrimePi[n]. Egli scopri' che il suo andamento e' del tipo n/ln(n). Questo vuol dire che presi i primi n numeri interi, soltanto una frazione 1/ln(n) di essi e' fatta di numeri primi, in media. Ma se questa frazione diminuisce, necessariamente la densita' dei primi deve dimuire col crescere di n.

Generazione di numeri primi

Preliminari: Una formula di scomposizione

L'equazione $z^n - 1 = 0$ ammette lo zero z=1. Effettuando la divisione tra $z^n - 1$ e (z-1) si trova il seguente risultato generale:

```
z^n - 1 = (z - 1) (1 + z + z^2 + z^3 + .... z^(n-1))
```

(NB: Se n non e' primo, il secondo fattore in genere si scompone ulteriormente) Esempi:

```
{z^7 - 1, z^4 - 1} // Factor
```

$$\{(-1+z)\left(1+z+z^2+z^3+z^4+z^5+z^6\right),\ (-1+z)(1+z)\left(1+z^2\right)\}$$

Esiste una scomposizione analoga anche per $z^n + 1$. Se n e' dispari, infatti, abbiamo comunque la soluzione z=-1. Effettuando la divisione con Ruffini, troveremmo:

```
z^d + 1 = (z + 1) (1 - z + z^2 - z^3 + .... z^(d-1))
```

Esempi:

```
{z^4 + 1, z^7 + 1} // Factor
```

$$\{1+z^4,\ (1+z)\left(1-z+z^2-z^3+z^4-z^5+z^6\right)\}$$

Qualche applicazione ...

Il numero $8^5 - 1$ dev'essere divisibile per 8-1=7. I numeri della forma $n^3 + 1$ devono essere tutti composti (sono

divisibili per n+1, o no?)

Primi di Mersenne

(padre Marin Mersenne, 1588-1648, francese, fisico. Ebbe contatti epistolari con Cartesio, Fermat, Hobbes, Galilei, etc)

Con in numeri primi in mente, consideriamo i numeri della forma:

$$M(\mathrm{n\_}) := 2^n - 1$$

La formula per $z^n - 1$ predice il solo fattore banale 2-1=1 e puo' dunque alimentare la speranza che i numeri di questa forma possano generare parecchi numeri primi.
Se n e' composto, pero', certamente M(n) non e' primo.
Infatti: se n=pq, possiamo scrivere:

$$2^n - 1 = (2^q)^p - 1 = (2^q - 1)\,(\ldots \text{ altro fattore } \ldots)$$

Esempio: $2^6 - 1 = 8^2 - 1 = (8-1)(8+1) = 7*9 = 63$

E' naturale quindi "far girare" l'esponente n solo tra i numeri primi. Ma anche cosi', putroppo, non tutti i numeri di Mersenne sono anche, ohibo', *primi di Mersenne*. Ecco alcuni M(p) (con p=primo) col relativo test di primalita':

```
Map[{#, M[#], PrimeQ[M[#]]} &, Prime[Range[8]]]
```

```
{{2, 3, True}, {3, 7, True}, {5, 31, True},
 {7, 127, True}, {11, 2047, False}, {13, 8191, True},
 {17, 131 071, True}, {19, 524 287, True
```

n=11213) le poste americane mel 1968 emisero un apposito francobollo commemorativo. Il piu' grande primo di Mersenne conosciuto oggi e' quello per n=86243. Usando il logaritmo decimale per valutarne la grandezza ....

```
Log[10, 2^86 243 - 1] // N
```

```
25 961.7
```

si trova che ha *solo* poco piu' di 25000 cifre. Ci aspettavamo di piu' :-).

Primi di Fermat

(Pierre de Fermat 1601-65, francese, magistrato e matematico a tempo perso. Detto anche "il principe dei dilettanti". Famoso per due teoremi: il "piccolo" e "l'ultimo")

Per analogia al caso di Mersenne, viene spontaneo esplorare la primalita' dei numeri della forma $2^n + 1$. Se n e' dispari, per la formula di scomposizione vista prima, questi numeri hanno 2+1=3 come fattore e non possono essere primi. n deve quindi essere per forza pari. Ma cio' non basta, purtroppo ....

```
Table[{n, 2^n + 1, PrimeQ[2^n + 1]}, {n, 1, 16}]
```

```
{{1, 3, True}, {2, 5, True}, {3, 9, False}, {4, 17, True},
 {5, 33, False}, {6, 65, False}, {7, 129, False},
 {8, 257, True}, {9, 513, False}, {10, 1025, False},
 {11, 2049, False}, {12, 4097, False},
 {13, 8193, False}, {14, 16 385, False},
 {15, 32 769, False}, {16, 65 537, True}}
```

Da una piccola ispezione, notiamo che effettivamente gli unici primi si hanno per gli n pari: 2,4,8,16 . Mmm ... questa successione dovrebbe dirci qualcosa. E' la successione delle potenze del 2. E' proprio cosi': solo per i casi $n = 2^m$ si producono primi. I primi di questa forma sono detti "*primi di Fermat*":

$$\mathbf{Fermat(m\_) := 2^{2^m} + 1}$$

```
Table[{n, Fermat[n], PrimeQ[Fermat[n]]}, {n, 0, 4}]
```

```
{{0, 3, True}, {1, 5, True}, {2, 17, True},
 {3, 257, True}, {4, 65 537, True}}
```

Tutti gli altri n pari si devono per forza scrivere nella forma $n = 2^m k$, dove k raccoglie tutta la scomposizione con primi dispari di n. Ne consegue che *k e' dispari*. Ma allora il numero e' composto. Infatti:

$$\mathbf{2^n + 1 = 2^{k2^m} + 1 = \left(2^{2^m}\right)^k + 1 = \left(2^{2^m} + 1\right)(\ldots \text{altro fattore} \ \ldots)}$$

e questo dimostra che solo le pure potenze del due "sono buone" come esponente.

Ci verrebbe quindi voglia di congetturare che tutti i numeri di Fermat sono primi. Ehm. Purtroppo gia' F(5) non e' primo. Non solo: questi quattro sono anche gli unici primi di Fermat conosciuti (!). Notare che F(5) si scompone nel prodotto 641*6700417 e, a tutt'oggi, non si sa se vi siano altri primi di Fermat oltre questi.

Aritmetica modulare ed Equazioni diofantee

Notazioni

Per dire che p e' un divisore di q ("p divide q") si scrive p|q. Il *massimo comun divisore* di p e q si indica con MCD(q,p) o con (q,p). Il *minimo comune multiplo* si indica con mcm(a,b). Due numeri di dicono "relativamente primi" se (q,p)=1.

Gli occhiali di Harry Potter

E' ben noto che dividendo N=17 per M=7 si ottiene come quoziente q=2 e come resto r=3 ed e' anche noto che queste informazioni possono essere utili per decomporre 17 in termini di 7: (17)=2*(7)+3. In generale, la decomposizione e' N=q*M+r, con r<M.

Immaginiamo ora di avere sotto gli occhi tutti i numeri interi {1,2,3,4, ...} e di inforcare gli occhiali modulari di Harry Potter (non ancora in vendita). Sono occhiali magici dotati di una rotellina numerata M, con la seguente proprieta': se regolo la rotellina su M, gli occhiali cancellano tutti i multipli di M che vedono. Con gli occhiali regolati su M=7, ad esempio, il 17 mi apparirebbe come un 3, il 14 come 0, il 3 come 3, l'8 come un 1, etc. In sostanza, come hai capito benissimo, *gli occhiali rimpiazzano ogni numero col resto*

della divisione per M. Ma i possibili resti modulo M sono solo 0,1,2,... M-1. Ne consegue che con gli occhiali M=7, la mia lista di numeri mi apparira' come una infinita ripetizione della serie {0,1,2,3,4,5,6}. Nei punti dove mi appare uno "0", ci sono in realta' i multipli di 7.

Congruenze modulari

Diremo che *due numeri, p e q, sono congruenti modulo M, se appaiono uguali attraverso l'occhiale modulare M ,* in simboli p=q (mod M). Questo e' come dire che i loro resti nella divisione per M sono uguali, o anche che essi differiscono per un multiplo di M. [NB, qualche volta, dove sottinteso, togliero' la dicitura (mod M)]

Inforchiamo gli occhiali M=6 e diamo un'occhiata a qualche quaderno di aritmetica dell'elementari. Vedremmo subito un sacco di relazioni piuttosto strampalate, ma che la maestra non ha corretto! Dov'e' scritto 5+1=6 noi vedremmo 5+1=0; qualche volta anche 5=-1; o anche anche 3+3=0. Ma vedremmo anche cose un po' piu' raccapricianti, tipo: 2*3=0 o 2*4=2.

Moduli primi. Perche' le ultime due turbano maggiormente? La prima perche' nell'aritmetica "normale" un prodotto si annulla solo se si annulla uno dei fattori. E la seconda? Beh, se semplificassimo ingenuamente per 2, troveremmo 4=1, che e' falso *anche* nel mondo di Harry Potter, oltre che nel nostro. Queste anomalie hanno una

causa e la causa e' che *M=6 non e' primo*. Con M=7 non succedebbero (varrebbe la legge dell'annullamento del prodotto e della semplificazione).

Criteri di divisibilita' e "Prova del Nove"

Un numero come 623 si puo' anche scrivere nella forma $6*10^2+2*10^1+3$. Se inforcassimo gli occhiali M=9 (ma sarebbe lo stesso per M=3) tutti i 10 diventerebbero degli 1 e noi vedremmo semplicemente 6+2+3=11=3 (mod 9). *Un numero e' divisibile per 3 o per 9 se la somma delle cifre lo e'.*

Immaginiamo di voler controllare la correttezza dell'operazione 352x12=4224. Mettiamo gli occhiali M=9. Ogni numero verrebbe rimpiazzato dalla somma delle sue cifre modulo 9, e noi vedremmo semplicemente 1x 4= 4, che e' esatto! Questo classico metodo di controllo va sotto il nome di "prova del nove". Ma non e' certo infallibile. Che succede se scambiamo due cifre? Eh-eh.

Equazioni diofantee lineari

Per equazione diofantea (Diofanto, III d.C) si intende un'equazione polinomiale nelle variabili intere {x,y,z , ...}, con tutti coefficienti interi. Il problema interessante e' la ricerca delle *soluzioni intere* (se esistono) e nel loro conteggio (se sono in numero finito).

Problema: la mamma compra un certo numero di bottiglie di vino ad 8 euro l'uno ed un certo numero di pizzette a 5 euro

l'una. Si sa che ha speso in tutto 81 euro e che le bottiglie di vino sono in numero pari. Trovare quante bottiglie e quante pizzette ha comprato.

Il problema e' matematicamente descritto dall'equazione 8x+5y=81, ma c'e' una difficolta': le incognite sono due (x,y) e l'equazione e' una sola. Se si volessero le soluzioni *reali,* il tutto risulterebbe piuttosto banale: sono tutte le infinite coppie (x,y) disposte lungo la retta di data equazione. Si, ma quante di queste sono coppie intere positive? E se la retta non incontrasse *nessuno* dei punti del reticolato del mio foglio?

Risoluzione mediante congruenze

Proviamo a guardare l'equazione con gli occhiali M=5. Cancellando tutti i multipi di 5 (8=5+3, 81=5*16+1) vedremmo 3x=1 (mod 5). Per risolvere per x dobbiamo eliminare il 3; basterebbe moltiplicare i due membri per quel q per il quale si ha 3q=1 (ma anche -1 va bene). Un buon q e' q=3. Infatti 3*3=9=10-1=-1 (sempre modulo 5). Moltiplicando per 3 e spostando il segno meno, troverei x=-3, che e' lo stesso che dire x=2 (mod 5) (posso sempre sommare o sottrarre i 5 che voglio, no?). Sapendo che x=2 nel mondo di Harry Potter, per avere x nel mondo reale basta aggiungere i multipli di 5 che l'occhiale ha cancellato, quindi x=2+5u, con u intero qualsiasi (anche negativo). Se si sostituisce questa espressione per x nell'equazione originaria, si trova che y=13-8u. La soluzione generale e'

dunque:

{x=2+5u, y=13-8u}.

Dovendo essere x>0 e y>0, sono permessi solo i valori u=0 (x=2,y=13) e u=1 (x=7, y=5) Nel caso in esame, dato che x doveva essere anche pari, l'unica soluzione e' proprio (x=2, y=13). Provare per credere!

Quand'e' che non esistono affatto soluzioni? Considera la seguente equazione diofantea: 6x+9y=40. I coefficienti 6 e 9 hanno un divisore comune: 3. Ora, mentre il primo membro e' divisibile per 3 (e viene infatti 2x+3y), il secondo non lo e'. Come potrebbe esistere una soluzione?! Ne consegue che l'equazione ax+by=k ha soluzioni solo se l'MCD di a e b divide anche k: in simboli (a,b)|k. Se e' cosi', e' meglio effettuare fin da principio la divisione, riducendosi al caso in cui (a,b)=1 (coeff. relativamente primi).

Un problema da Scientific American

In tutti i punti di un reticolo piano sono stati sistemati dei birilli. Un cacciatore (posizionato sul birillo {0,0}) spara in direzione del birillo {a,b}. Quanti birilli colpisce il proiettile, oltre al birillo {a,b}, tra tutti quelli che sono tra il cacciatore e il bersaglio? [libero adattamento]

In termini diofantei avremmo y/x=b/a e quindi ay-bx=0. La soluzione generale, in forma parametrica, e' {x = (u*mcm[a, b])/b, y = (u*mcm[a, b])/a}. Dovendo essere x

compreso tra 0 e "a", ne consegue che il massimo u possibile e' $\frac{ab}{\text{mcm}(a.b)}$ che (si puo' dimostare) fa sempre MCD(a,b).

Se spara verso {8,12}, colpira' in tutto MCD(8,12)=4 birilli.

```
Table[ {u * 24 / 12, u * 24 / 8}, {u, 1, 4}]
```

```
{{2, 3}, {4, 6}, {6, 9}, {8, 12}}
```

Applicazioni piacevoli dei criteri di divisibilità (e altri giochi)

Divisibilità per 99

Prendiamo un numero di 8 cifre decimali e raggruppiamo le cifre in coppie, a partire da destra: x=XX.XX.XX.XX. Detti a,b,c,d i numeri (minori di 99), rappresentanti i tre gruppi di cifre, avremmo $a + b10^2 + c\left(10^2\right)^2 + d\left(10^2\right)^3$. Il che è come dire che, in base 100, il numero è rappresentato da "dcba".

Essendo 100=99+1, il numero si puo' scrivere come:

$$x = a + b(99 + 1) + c(99 + 1)^2 + d\,(99 + 1)^4 .$$

Inforchiamo ora gli occhiali modulo 99. Tutti i 99 scompaiono, e il numero diventa x=a+b+c+d. Quand'e' che un numero x è multiplo di 99? Quando, visto modulo 99, risulta x=0. Siamo arrivati alla conclusione: *un numero x è divisibile per 99 se, suddiviso in gruppi di due crifre, a partire da destra come visto nell'esempio, si ha a+b+c+d+ ... =0 (modulo 99)*

Correzione degli errori degli hard-disk

Prendiamo il numero 1164933=01.16.49.33. Calcolando la somma a+b+c+d (modulo 99) si ha 33+49+16+1=99=0. La somma fa 0, dunque il numero e' divisibile per 99. Supponiamo che per qualche motivo (ad esempio: durante la trasmissione informatica del numero) si sia cancellata la

terza cifra: 11*4933, ma si sappia che il numero era multiplo di 99. *Problema: e' possibile (e come) ricostruire la cifra mancante?* Facile: si contano le cifre e si assegna all'asterisco l'unica cifra per la quale il totale faccia 99 o un multiplo di 99.

Un giochino col 99

Si dice ad una persona di pensare un numero *dispari di cifre* (27513), di rovesciare la cifre (31572), e di farne la differenza (31572-27513=4059). Tutte le volte che si fa questa procedura, si ottiene un numero multiplo di 99 (infatti 4059=41*99). A questo punto si chiede alla persona di moltiplicare il risultato (4059) per un altro numero a piacere (es 387: 4059x387=1570833). Ora fatevi dire il numero trovato, ma facendo nascondere una cifra, ad ed esempio: 1570*33. *Come ricostruire l'8 perduto?*

Suddividendo in gruppi di due cifre e sommando si ha 33+57+1+x=0, cioe' x=-91. Ma il risultato e' sempre modulo 99, per cui si possono aggiungere i multipli di 99 necessari a renderlo positivo. In questo caso x=-91+99=8.

Divisibilità per 101

Prendiamo un numero di 8 cifre decimali (il caso generale è una ovvia estensione) e raggruppiamo le cifre in coppie, a partire da destra: x=XX.XX.XX.XX. Detti a,b,c,d i numeri

(minori di 99), rappresentanti i tre gruppi di cifre, avremmo $a + b10^2 + c\left(10^2\right)^2 + d\left(10^2\right)^3$. Il che è come dire che, in base 100, il numero è rappresentato da "dcba".

Essendo 100=101-1, il numero si puo' scrivere come:

$$x = a + b(101 - 1) + c(101 - 1)^2 + d\,(101 - 1)^4 .$$

Inforchiamo ora gli occhiali modulo 101. Tutti i 101 scompaiono, e il numero diventa x=a-b+c-d. Quand'e' che un numero x è multiplo di 101? Quando, visto modulo 101, risulta x=0. Siamo arrivati alla conclusione: *un numero x è divisibile per 101 se, suddiviso in gruppi di due crifre, a partire da destra, si ha a - b+c - d + ... =0 (notare i segni alternati!)*

Un giochino col 101

Numeri come 3737, 1515, 2323, ... sono tutti multipli di 101. Infatti, per questi numeri c=0, d=0, etc mentre a=b e, quindi a-b=0.

Se chiedete all'uditorio di pensare un numero (37), raddoppiarne le cifre (3737), moltiplicarlo per qualsiasi altro numero, otterranno tutti un multiplo di 101 come risultato. Questo fatto puo' essere sfruttato, esattamente, come nel giochino precedente, per indovinare cifre perdute, o cancellate.

Decimali Periodici, Ciclotomia, Costruibilita'

Preliminare: la serie armonica

Per il seguito e' utile sapere che, se |x|<1, allora:

$$\sum_{n=0}^{\infty} z^n = 1 + z + z^2 + z^3 + \ldots = \frac{1}{1-z}$$

Sviluppi decimali e serie armonica

Tutti sanno che alcune frazioni portano ad uno *sviluppo finito* dopo la virgola (es: 1/2 =0.5, 1/5=0.2) mentre altre conducono ad uno *sviluppo infinito,* benche' periodico (1/3=0,3333.... ; 1/11=0,090909 ...). Sappiamo che tutti i numeri razionali p/q portano invariabilmente ad uno sviluppo di tipo finito o del tipo periodico. Possiamo travare la frazione generatrice usando la serie armonica per sommare tutte le sue cifre. Esempio per 1/11:

$$x = 0.09090909\ldots = 09 * \left(10^{-2} + 10^{-4} + 10^{-8} + \ldots\right)$$

Posto $q = 10^{-2}$ l'espressione tra parentesi vale $\frac{1}{1-q} - 1 = \frac{q}{1-q} = \frac{1}{99}$. Ne consegue che $x = \frac{9}{99} = \frac{1}{11}$.

Decimali periodici

Dagli esempi verrebbe voglia di dire che 1/p con p=primo

dia sempre uno sviluppo periodico. Ma, allora, perche' con 1/5 l'idea non funziona, benche' 5 sia primo?

Si potrebbe dimostrare che le frazioni del tipo 1/N hanno sviluppo finito solo se N ha come fattori solo il 2 o il 5: $N = 2^a 5^b$. Le frazioni 1/2, 1/5, 1/10, ... entrano tutte in questa classe. Le frazioni cosiffatte, moltiplicando "sopra e sotto" per appositi numeri, si possono sempre riscrivere con denominatore a potenza del 10. Esempio (moltipilcando sopra e sotto per 2):

$$\frac{1}{50} = \frac{1}{2 * 5^2} = \frac{2}{100} = 0,02$$

Invece 1/15=1/(3*5) e' illimitato periodico, a causa dell'extra fattore 3 al denominatore.

Lunghezza del periodo

Come mai alcuni sviluppi hanno un periodo corto (1/3=0,3333...) ed altri,come 1/7=0,142857...,hanno un periodo cosi' lungo? Si puo' dimostrare che la lunghezza del periodo di 1/p con p=primo e' il piu' piccolo intero k tale che $10^k = 1 \pmod p$. Inoltre, il periodo non puo' superare p-1.

L'impossibile heptagono

Costruzioni con riga e compasso

Tre problemi (duplicazione del cubo, trisezione dell'angolo e quadratura del cerchio) hanno destato interesse per intere generazioni di matematici, fin dall'antichita'. Il problema non e' di natura algebrica, ma di natura costruttiva: bisogna risolverli usando *punti del piano costruibili* con la sola riga (non graduata) e il compasso.

Com'e' noto, con riga e compasso si possono risolvere facilmente problemi quali: tracciare assi, bisettrici, mediane, proiettare punti, trasportare segmenti, etc, ma anche operazioni piu' complesse, quali estrarre la radice quadrata, e quindi la radice quarta, sedicesima, etc.

Quest'ultimo fatto non dovrebbe stupire: in fondo, e' noto che intersecando cerchi e rette si ottengono equazioni di 2° e 4° grado. La cosa puo' essere generalizzata fino a dimostrare che tutti i problemi risolubili con riga e compasso devono essere descritti in termini di eq. diofantee di grado 2^n (2,4,8,16, ...) . Sia la duplicazione del cubo (risolvente: $x^3 = 2$), sia la trisezione dell'angolo (risolvente $8\,x^3 - 6\,x - 1 = 0$) che la quadratura del cerchio $\left(x^2 = \pi\right)$ cadono fuori di questo ambito.

Ciclotomia e poligoni regolari

Con la sola riga e il compasso e' facile costruire il triangolo equilatero e il quadrato inscritto nella circonferenza E dato che e' facile tracciare l'asse di un segmento (e quindi le bisettrici), dal triangolo possiamo passare facilmente

all'esagono, e dal quadrato all'ottagono, etc, bisecando gli angoli. Anche il pentagono (p=5) e' costruibile, come ogni studente sa . Ma, fatto davvero rimarchevole, l'eptagono, il poligono di 7 lati, non e' costruibile. Perche' mai p=5 si e p=7 no? Mistero.

Ricordate le radici n-esime complesse dell'unita'? Le p soluzioni dell'equazione $z^p - 1 = 0$ si disponevano, con regolarita' sul cerchio di raggio 1 a formare p-agoni regolari. Ora, essendo $(z^p - 1) = (z - 1)\left(1 + z + ... + z^5\right)$, a parte z=1 che c'e' sempre, il problema e' del 5° ordine. Ma 5 non e' una potenza del due, e quindi *non e' costruibile*.

Generalizzando, gli p-agoni con p=primo, sono costruibili se p-1 e' una potenza del due: $p - 1 = 2^n$, e cioe' $p = 2^n + 1$. Ma, per quanto visto allorche' parlammo dei primi di Fermat, i numeri della forma $2^n + 1$ possono essere primi solo se n stesso e' una potenza del due. In conclusione, dev'essere $p=2^{2^m} + 1$:

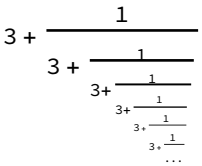
```
{3, 5, 17, 257, 65 537}
```

Sono percio' costuibili p=3, p=5, p=17 (p=17 lo costruì Gauss) ... ma anche i prodotti di primi di Fermat (p=3*5=15) e tutti i raddoppiamenti di questi (p=6, p=10, p=30, ...). In sintesi: l'n-agono e' costruibile quando, scomposto in fattori primi n, gli unici fattori primi sono il 2 o uno dei primi di Fermat (presi un qualunque numero di volte).

Frazioni continue, calendari (avanzato)

Frazioni continue

Quanto mai varra' una una mostruosa frazione come la seguente?



Le frazioni di questo tipo (naturalmente, ponendo altri interi dove ora ci vedi il solo 3) si chiamano *frazioni continue.*

Beh, osservandola per un po', appare chiaro che le varie parti si ripetono. In un certo senso, qui "la parte" e' uguale "al tutto". Se chiamiamo con x il suo valore, e' evidente che dev'essere $x = 3 + \frac{1}{x}$ e cioe' $x^2 - 3x - 1 = 0$. Risolvendo l'equazione di 2° grado, troveremmo x=3,302775... *En passant*, si tratta di un numero irrazionale. Le frazioni continue permettono di studiare gli irrazionali e di indagare la presenza di qualche forma di periodicita' in essi, cosi' come si conosce tutto sulla periodicita' dei numeri razionali.

Scrivere un decimale in frazione continua

Prendiamo un numero decimale come x=4.4624 (che e' 415/93). Come prima approssimazione, il risultato è 4 piu'

qualcosa. Scriviamo il *qualcosa* nella forma 1/r, con r intero: 4+1/r. E' chiaro che la migliore risposta e' 4+1/2=9/2. Ma il 2 del denominatore non è corretto, è un po' più di 2, circa 2 e 1/6. Scriviamo quindi: 4 + 1 /(2 + 1/6)=58/13. Ma ancora, il 6 nel denominatore dell'ultima frazione non è corretto; il denominatore corretto è un po' più di sei, per la precisione 6 + 1/7. Scriviamo percio': 4 + 1 /(2 + 1 /(6 + 1/7)). Questo valore è esattamente uguale a 415/93, e può essere scritto con la notazione abbreviata [4; 2, 6, 7].

Questo modo di costruire approssimazioni razionali (cioe' 4, 9/2, 58/13, etc) di un numero decimale (ma anche reale) produce frazioni p/q di tipo *minimale*, cioe' che usino numeri p e q piu' piccoli possibili.

Frazioni continue e calendari

Com'e' noto, il periodo di rivoluzione della terra T, espresso in giorni, non e' un numero intero ma, mediamente, T=`365.2419`. Cercando di scrivere T come una frazione minimale, cominceremmo con 365 +1/4. Ma il 4 di 1/4 non e' proprio 4 ma 4+1/7, cosi' via:

$$T = 365.2419 = 365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{\text{"..."}}}}$$

Chiaramente, il fatto che T non sia un numero intero e' un problema e, se non effettuassimo qualche correzione, ben presto avremmo la neve a ferragosto. Nei calendari mod-

erni si introducono dei cicli di parecchi anni *q,* aggiungendo alcuni bisestili *p* per ogni ciclo, in maniera che l'*anno medio* sia quanto piu' vicino possibile al valore misurato di T:

$$\frac{p + 365\,q}{q} = 365 + \frac{p}{q} = 365.2419\ldots$$

Dei vari approssimanti razionali di p/q={1/4,7/29,8/33,...}, soltanto il primo (1/4, cioe' un bisestile ogni 4: p=1, q=4) e' pratico: i periodi come 29, 33, etc porterebbero piu' confusione che benefici (anche se q=33 avrebbe un certo fascino ...). Il calendario col ciclo q=4 e' detto *calendario Giuliano.* E' un calendario cosi' poco preciso che, nel corso del suo impiego, si dovette ad un certo punto cancellare parecchi giorni di calendario per far tornare la Pasqua nel periodo giusto.

E' per questo motivo che si sono cercarti cicli di correzione piu' lunghi di q=4. Il *calendario gregoriano*, ad esempio, usa q=400 anni.

Calendario Gregoriano

Posto q=100q', si avrebbe $\frac{p}{q} = \frac{p}{100\,q'}$ = 0.24 .... quindi:

$$\frac{p}{q'} = 24.19\ldots = 24 + \cfrac{1}{4 + \cfrac{1}{\text{"...."}}}$$

con approssimanti p/q'=97/4,121/5, etc. Il primo di questi (97/4), condurrebbe a 97 bisestili ogni 400 anni. Come

inserire questi bisestili nell'arco dei 400 anni? Basta fare un' inserzione ogni 4 anni. Le annate multiple di 4, dunque. Ma sono 100, non 97. Dobbiamo cancellare 3 bisestili e la scelta e' cancellare la bisestilita' di 100,200 e 300.

Si potrebbe continuanare scrivendo q=400q', e apportare ulteriori correzioni ogni q di cicli di 400 anni. Si troverebbe come terzo approssimante la frazione 775/8: cioe' 775 bisestili ogni 8*400=3200 anni. Il gregoriano puro prevederebbe 8*97=776 bisestili, invece che 775. Si potrebbe quindi correggere il gregoriano cancellando un addizionale bisestile ogni 3200 anni.

Basta solo aspettare :-)

Numeri di Fibonacci e Sezione Aurea

La Successione di Fibonacci

(Leonardo Pisano, Fili Bonacci, Pisa 1170-1250. Introdusse in europa le cifre arabe]

Consideriamo la successione di interi $F_n = \{1, 1, 2, 3, 5, 8, 13, 21, \ldots\}$. Come si vede, a partire dalla coppia (1,1), tutti gli altri sono formati sommando i due numeri che li precedono. In forma ricorsiva: $F_n = F_{n-1} + F_{n-2}$, con la condizione che $F_1 = F_0 = 1$.

False scomposizioni e numeri di Fibonacci

I numeri di Fibonacci 5,8,13 (ma sarebbe lo stesso per qualsiasi altra tripletta contigua della stessa serie. Provare per credere!) godono della seguente proprieta': 13x5-8x8=1.

Un vecchio trucchetto di falsa scomposizione, consiste nel prendere il quadrato 8x8, tagliarlo in triangoli e trapezi per poi rimontarlo a formare un rettangolo 13x5. Apparentemente, la scomposizione e' possibile e le varie parti combaciano molto bene. Peccato pero' che il rettangolo abbia l'area piu' grande, anche se di poco: un quadretto in piu'. Evidentemente, le varie parti *non combaciavano tanto bene* come si voleva far credere ....

Sezione Aurea

Immaginiamo di avere un segmento lungo AB=1+ϕ e di volerlo dividere in una parte "corta" AC=1 e una parte "lunga" CB=ϕ,ma con la condizione che le varie parti siano in proporzione: tutto:lungo=lungo:corto. In simboli: $\frac{\phi+1}{\phi} = \frac{\phi}{1}$, e cioe' $\phi^2 = \phi + 1$, oppure, $\phi = 1 + \frac{1}{\phi}$. Risolvendo quest'equazione con i medoti ordinari delle equazioni quadratiche e scartando la soluzione negativa, troviamo il numero irrazionale $\phi = \frac{1}{2}\left(1 + \sqrt{5}\right) = 1.6180\ldots$

Utilizzando le due forme $\phi = \sqrt{1+\phi}$ e $\phi = 1 + \frac{1}{\phi}$ in maniera ricorsiva, possiamo ricavare due interessanti quanto misteriori sviluppi per il famoso numero ϕ:

$$\left\{\phi == \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}}\ ,\right.$$

$$\left.\phi == 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ldots}}}}}}\right\}$$

Legame tra ϕ e la successione di Fibonacci

Se si prova a calcolare i vari rapporti $\frac{F_{n+1}}{F_n}$ nella serie di Fibonacci, a formare cioe' le frazioni 8/5,13/8,21/13, si nota

subito che dopo un po' essi tendono a stabilizzarsi su un valore prossimo a 1.6180 ....

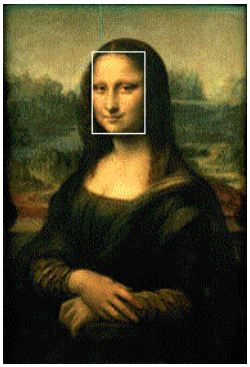
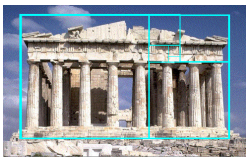
```
Table[Fibonacci[n + 1] / Fibonacci[n], {n, 2, 15}] // N
```

```
{2., 1.5, 1.66667, 1.6, 1.625, 1.61538,
 1.61905, 1.61765, 1.61818, 1.61798,
 1.61806, 1.61803, 1.61804, 1.61803}
```

Ma questo e' proprio il valore di ϕ ¡la sezione aurea! Spiegare come mai questo accade non e' facile, pero' prova a prendere la relazione che definisce ϕ (cioe' $\phi^2 = \phi + 1$) e moltiplica i due membri varie volte per ϕ stesso.Troverai una serie di relazioni quali: $\phi^3 = \phi^2 + \phi$, $\phi^4 = \phi^3 + \phi^2$,... $\phi^n = \phi^{n-2} + \phi^{n-1}$, che brillano per la loro somiglianza con la relazione fondante degli F_n: $F_n = F_{n-1} + F_{n-2}$.

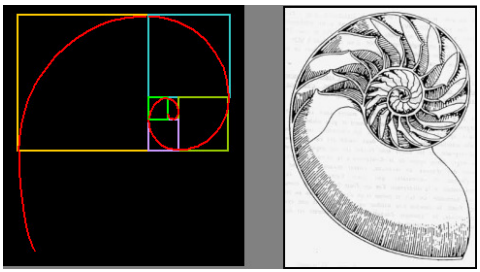
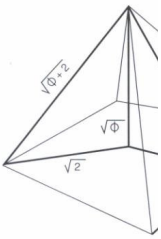
Ora,per motivi che galleggiano tra l'estetico, il magico e ... la pura suggestione, dal medioevo in poi i rettangoli i cui lati abbiamo circa questi rapporti 8x5,13x8,21x13, etc sono sempre stati considerati di aspetto piu' gradevole degli altri e per tale motivo sono stati usati in vario modo nelle arti figurative (la cosiddetta *divina proportione*).

Nell'arte


Rettangoli aurei: Il volto della Gioconda, Il Partenone. Rettangoli e pentagoni: Salvador Dali', *Il sacramento dell'Ultima Cena*, 1955. La successione di Fibonacci, in forma di numeri luminosi, e' stata recentemente messa sulla Mole Antonelliana (Torino) e in chissa' quanti altri posti ancora ....

In Natura

Il Nautilus. La piramide di Cheope.

In Musica e Letteratura

In molti ritmi e armonie musicali si incontrano i rapporti 3/2 o 5/3. *Le serpent qui danse* di Baudelaire e' composta con versi di 8 e 5 sillabe, come *Nostalgia* di Saba, etc. etc.

I polinomi: fatti principali. Teoremi di Fermat.

Fattorizzazione

Se un polinomio P(x) ammette lo zero x_1, P(x) dev'essere divisibile per $(x - x_1)$. Questo significa che, detto Q(x) il quoziente, si deve poter scrivere $P(x) = (x - x_1) * Q(x)$. Se x_2 e' uno zero di Q(x), possiamo applicare la stessa procedura piu' volte , fino a decomporre totalmente il polinomio (sotto certe condizoni):

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n =$$
$$a_n (x - x_1)(x - x_2) \ldots (x - x_n)$$

L'equazione $2x^2 + x - 6 = 0$, ad esempio, ha per zeri x=-2 e $x = \frac{3}{2}$ e si puo' quindi scrivere nella forma:

$$2\left(x - \frac{3}{2}\right)(x + 2) = (2x - 3)(x + 2) = 0.$$

Il fatto (puramente algebrico) che P(x) debba decomporsi nel prodotto (2x-3)(x+2) non e' senza conseguenze di tipo aritmetico, anzi! Riguardando la scomposizione dal punto di vista dei numeri interi, siamo in grado di affermare parecchie proprieta' di P(x) che non avremmo sospettato: dal fatto che (x+2) divide P(x), consegue che P(0) e' un numero pari, che P(5) e' un multiplo di 7. Dal fatto che (2x-3) divide P(x), sappiamo che P(4) dev'essere divisibile per 2*4-3=5 etc, etc e, *dulcis in fundo*, siamo proprio certi

che con un tale P(x) non siamo in grado di produrre neanche un numero primo :-)

Concludendo: Se x =n e' uno zero (x-n)|P(x); se $x = \frac{p}{q}$ e' uno zero, (q-px) | P(x) .

Zeri interi e razionali

Teorema: Se x e' uno zero intero, deve dividere il termine noto (in simboli $x \mid a_0$.) Se *x e' uno zero razionale* $x = \frac{p}{q}$, *p deve dividere il termine noto e q deve divide il coeff. direttore* (in simboli: $p \mid a_0$ e $q \mid a_n$)

Questi due teoremi si possono dimostrare anche facendo uso degli occhiali modulari di Harry Potter. Supponiamo sia $x = \frac{p}{q}$ con p e q privi di fattori comuni (eventuali fattori si possono sempre semplificare); sostituiamo x=p/q in P(x)=0 e moltiplichiamo tutto per q^n. Troveremmo un'espressione senza frazioni del tipo

$$a_0\, q^n + a_1\, q^{n-1}\, p + \ldots a_n\, p^n = 0.$$

Se inforcassimo gli occhiali modulo=p, l'equazione ci apparirebbe nella forma $a_0\, q^n$=0 (conseguenza: a_0 dev'essere multiplo di p). Se invece inforcassimo gli occhiali modulo=q, l'equazione ci apparirebbe nella forma $a_n\, p^n$=0 (conseguenza: a_n dev'essere multiplo di q. Il caso intero si ricava da questo ponendo q=1. CVD.

Il Teorema dei due quadrati di Fermat

I numeri primi della forma 4k+1 si possono sempre esprimere come somma di due quadrati perfetti $p = x^2 + y^2$. *(esempio* $17 = 4^2 + 1^2$*)*

Analisi numeri primi. Per risolvere questo problema, useremo gli occhiali modulari M=4. Con questi occhiali, gli unici numeri che vediamo sono 0,1,2,3. Tra questi, gli unici *candidati primi* sono solo quelli che corrispondo a 1 e 3, sono cioe' della specie 4k+1 o 4k+3 (i 4k e i 4k+2 sono pari!) Basta dunque dimostrare che solo la specie 4k+1 puo' essere decomposta in somma di due quadrati. Il primi 7=1*4+3 e' , ad esempio, del tipo "sbagliato" e non e' decomponibile.

Analisi dei quadrati. Ogni intero n si puo' scrivere in una delle due forme: n=2k (se e' parti), n=2k+1 (se e' dispari). Nel seguito, dove vedi "k" leggi "multiplo". Cosi', 2k significa "multiplo di 2". Effettuando il quadrato n^2, per i numeri pari troveremmo $n^2 = 4\,k$ (ho ribattezzado k^2 nuovamente k, per significare "multiplo" di 4) e per i dispari troveremmo $n^2 = 4\,k + 1$ (ho ribattezzato ancora). Ne consegue che i quadrati perfetti *sono solo di due specie*: la specie 4k e la specie 4k+1, a seconda se sono pari o dispari (16=4*4, 25=4*6+1). Per ottenere un primo p dobbiamo necessariamente sommare due quadrati di specie diversa, altrimenti avremmo un risultato pari! Ma sommando "modello" 4k con un "modello" 4k+1, troviamo solo numeri

della specie 4k+1. CVD.

Ancora sui quadrati

1) Il quadrato in un numero di una cifra non puo' mai terminare per 2,3,7 o 8 (verificare a mano).
2) Un quadrato di piu' cifre deve terminare come termina il quadrato dell'ultima cifra. Infatti, con gli occhiali M=10, $(10\,a + b)^2$ coincide con b^2 .
3) un quadrato non puo' terminare per 26. Posto infatti $n^2 = 100\,a + 26$, con gli occhiali M=4 apparirebbe come $n^2 = 4\,k + 2$, e non e' possibile .
4) in un quadrato, la somma delle cifre non puo' fare 48. Infatti: sarebbe divisibile per 3, ma non per 9. Ma la scomposizione in fattori di n^2 deve contenere i primi alla potenza pari.

Ancora sui cubi

1) La somma delle cifre di n^3, presa modulo 9, puo' fare solo 0,1 o 8.
2) $n^3 - n$ e' sempre divisibile per 6. Infatti:
$n^3 - n = (n - 1)\,(n)\,(n + 1)$. Essendo il prodotto di tre interi consecutivi, uno deve essere multiplo di 2 (c'e' un pari ogni due) e uno deve essere multipo di 3 (c'e' un multipo di 3 ogni tre).

Il "piccolo" teorema di Fermat

$$x^p = x \pmod p \text{ se } p \text{ è primo}$$

E' chiamato "piccolo" teorema di Fermat o anche "Primo" teorema di Fermat, per distinguerlo dall'altro, e piu' celebre, l'Ultimo Teorema di Fermat (LFT, Last Fermat Theorem), il teorema che ha sfidato per parecchi secoli le piu' celebri menti matematiche e che e' stato dimostrato solo negl'anni 90 (A.Wiles; vedi in seguito).

Esempio di applicazione: con x=2, il teorema afferma che per ogni p primo, $2^p - 2$ e' sempre multimo di p. Con p=17 si ha $2^{17} - 2 = 131070$ e $\frac{131070}{17} = 7710$.

I cinesi credevano anche all'inverso del teorema: $x^p = x \pmod p$ *allora* p e' primo. Se fosse vero, avremmo a disposizione un metodo per stabilire la primalita' di p. Putroppo pero', vale anche per numeri composti come p=341=11*31. Dato che non e' cosi' facile calcolare a mano 2^{341}, si puo' perdonare loro l'errore :-)

Un applicazione: consideriamo l'insieme di tutti i possibili risultati (le possibili colonne) di una schedina del totocalcio (13 partite, 3 risultati per ogni partita). Da questo insieme togliamo i casi in cui la colonna e' fatta di risultati uguali: tutti 1, tutti 2 o tutti X. Le colonne che rimangono sono in multiplo di 13. *Dimostrazione*: 3^{13} sono tutte le colonne; 3 sono quelle a risultato identico. Restano $3^{13} - 3$. Essendo p=13 un numero primo, il teorema di Fermat garantisce che

questo valore e' multiplo di 13 (infatti: 1594320=122640*13)

Traccia per una dimostrazione: mettiamo gli occhiali modulo M=p. Con questi occhiali, sviluppando un binomio come $(a+b)^p$ troveremmo soltanto $a^p + b^p$, cioe' il primo e l'ultimo termine della formula di Newton. Il motivo e' che, nei termini intermedi, compaiono dei coefficienti tutti divisibili per p, dato che contengon o p!

Lo stesso capita per il trinomio: $(a+b+c)^p = a^p + b^p + c^p$, etc. Se scrivessimo x=1+1+1+1...+1 (con x addendi), troveremmo che $x^p = 1^p + 1^p + \ldots \times .1^p = x$.

L' "ultimo" teorema di Fermat (LFT)

Sul margine del libro che stava leggendo (era una copia dell'Aritmetica di Diofanto) Fermat scrisse:

"l'equazione $x^n + y^n = z^n$ non ammette soluzioni intere (x,y,z) non nulle, nel caso che sia n>2. Ho trovato una bellissima dimostrazione, ma non c'e' spazio per riportarla su questo margine".

Per n=2, come ben sai, le soluzioni intere ci sono eccome. Esempio (3,4,5).

Per piu' di 300 anni questo teorema ha rappresentato una sfida per le migliori menti matematiche, ma e' stato dimostrato soltanto negli anni 90, da un matematico americano (A. Wiles). Pare che la dimostrazione non sia

cosi' breve ne' cosi' semplice e che occupa centinaia di pagine piene di alta matematica, appositamente costruita allo scopo.

Certo, non e' la soluzione che Fermat aveva in mente!

Sulle Terne pitagoriche

Rileggere il paragrafo relativo alle proprieta' dei quadrati. In particolare, ci servono questi risultati: 1) i quadrati pari sono di classe 4k e quelli dispari di classe 4k+1 2) non esistono quadrati di classe 4k+2 o 4k+3.

Terne primitive: definizione

Una *terna pitagorica* è una tripletta di numeri interi (a,b,c) soddisfacenti l'equazione $a^2 + b^2 = c^2$. Una terna è detta *primitiva* se i numeri (a,b,c) non hanno fattori comuni. Questo significa, ad esempio, che *non possono essere tutte e tre pari,* altrimenti avrebbero 2 come fattore comune. Ricordiamo che il triangolo (ka,kb,kc) non è altro che il triangolo (a,b,c) *ingrandito* di un fattore moltiplicativo k, per cui desideriamo escluderli dall'analisi.

L'ipotenusa c può essere pari?

Se l'ipotenusa è pari, allora a e b devono essere entrambi pari o entrambi dispari. Entrambi pari lo escludiamo, perchè la vogliamo primitiva. Resta il caso di *entrambi dispari*. Ma due quadrati dispari sono di classe 4k+1: la loro somma sarebbe di classe 4k+2 e non potrebbe essere un quadrato perfetto. Dunque: *l'ipotenusa c dev'essere dispari*. I due cateti devono essere uno pari e l'altro dispari. (Notare che [4,5,6] soddisfa).

Una formula per generare terne

Sfruttando semplici proprietà dei prodotti notevoli (in special modo la formula $a^2 - b^2 = (a - b)(a + b)$) è facile accorgersi che:

$$(r^2 + s^2)^2 - (2\,rs)^2 = (r^2 - s^2)^2$$

Possiamo quindi generare terne pitagoriche ponendo, ad esempio, $a = r^2 - s^2$, $b = 2\,rs$, $c = r^2 + s^2$, e scegliendo (r,s) a piacere tra i numeri interi.

Nella simulazione che segue pongo r=8 e faccio variare s tra 1 e 7: notare che b e è sempre pari e che a e c sono sempre dispari.

```
Table[{r^2 - s^2, 2 r * s, r^2 + s^2},
  {r, 8, 8}, {s, 1, 7}] // MatrixForm
```

$$\left(\begin{pmatrix}63\\16\\65\end{pmatrix}\ \begin{pmatrix}60\\32\\68\end{pmatrix}\ \begin{pmatrix}55\\48\\73\end{pmatrix}\ \begin{pmatrix}48\\64\\80\end{pmatrix}\ \begin{pmatrix}39\\80\\89\end{pmatrix}\ \begin{pmatrix}28\\96\\100\end{pmatrix}\ \begin{pmatrix}15\\112\\113\end{pmatrix}\right)$$

Ma r ed s sono veramente "a piacere"?

Ricordiamoci delle condizioni sui lati: *c* dev'essere dispari, *b* dev'essere pari e *a* dev'essere dispari. Ma $a = r^2 - s^2$ non sarebbe dispari se r ed s hanno la stessa parità. Dunque, *r ed s devono avere partità diversa* : uno pari, l'altro dispari. Vuol dire che, nell'esempio precedente, dato che r=8, i casi r=2, r=4 ed r=6 devono aver prodotto *terne non primitive,* anche se sono comunque terne. **Controlla!**

ab e' sempre multiplo di 4 (+ facile)

Considera il prodotto dei cateti: $ab = \left(r^2 - s^2\right) 2\,rs$. Essendoci il fattore 2, ab è un numero pari. Abbiamo detto pero' che r ed s devono avere diversa parita': dunque, uno di essi è pari. Questo porta ad un secondo fattore 2. Due fattori pari fanno sì che ab sia del tipo 4k. cvd

ab e' sempre multiplo di 3 (+ difficile)

Considera il prodotto dei cateti: $ab = \left(r^2 - s^2\right) 2\,rs$. Dobbiamo dimostrare che, in questa espressione, c'è almeno un fattore 3, nascosto da qualche parte. Se c'è in r o in s, la dimostrazione è finita. Se non c'e' nè in r nè in s, dobbiamo dimostrare che dev'essere per forza nascosto in $r^2 - s^2$.
Dimostrazione: per ipotesi, r ed s sono di classe 3k+1 o di classe 3k+2. Elevando al quadrato, la classe 3k+1 resta 3k+1; la classe 3k+2, al quadrato, diventa 3k+4, ma 4=1. Quindi, r^2 e s^2 sarebbero entrambi di classe 3k+1. Sottraendoli, avremmo un numero di classe 3k. cvd

L'area della terna e' sempre multipla di 6

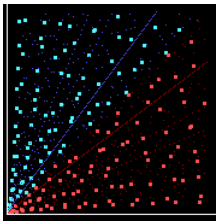
Essendo ab multiplo contemporaneo di 3 e di 4, sarà multiplo di 12. Ne consegue che ab/2 è multiplo di 6. Nella famosa terna (3,4,5) è proprio esattamente 6.

Almeno uno dei tre lati e' multiplo di 5

In sostanza, uno dei tre numeri (a,b,c) deve per forza finire con 0 o 5. Interessante. Per la terna (3,4,5) vale, ma come dimostrarlo in generale?
Considera il prodotto
abc = $\left(r^2 - s^2\right) 2\,\mathrm{rs}\left(r^2 + s^2\right) = 2\,\mathrm{rs}\left(r^4 - s^4\right)$. Dobbiamo far vedere che, da qualche parte, in uno dei tre pezzi, deve nascondersi il fattore 5. Se uno almeno tra r o s è multiplo di 5, lo sarà anche abc, e avremmo finito. E se nessuno tra r ed s lo è? Allora, dobbiamo far vedere che $\left(r^4 - s^4\right)$ è multiplo di 5 se r ed s *non lo sono.*
Dimostrazione: se prendi r ed s di classe 5k+{1,2,3,4} ed elevi al quadrato, ottiene sempre numeri di classe 5k+{1,4}. Se elevi di nuovo al quadrato, ottieni solo numeri di classe 5k+1. Esempio: `27^4`=106288*5+1. Ne consegue, che sottraendo due quarte potenze di questo genere, otteniamo un numero di classe 5k. cvd.

Visualizzasione grafica delle terne

Nell'immagine che segue sono stati esplorati i triangoli con (a,b) nel range 1-500. Ogni volta che è stata trovata una terna primitiva, il computer ha messo un quadratino. Le terne non-primitive (terne derivate) sono rappresentate con dei punti:



Dimostrazioni senza parole

Uno "strana" tecnica dimostrativa, basata solo sulle immagini. Alcune di queste dimostrazioni sono molto ingegnose. Le dimostrazioni relative alle arcotangenti sono un classico: gli sviluppi in arcotangente, infatti, sono usati per calcolare le cifre di π a milionate.

```
g = Import["/home/michele/math/numbt/media.jpg"];
Show[g];
```

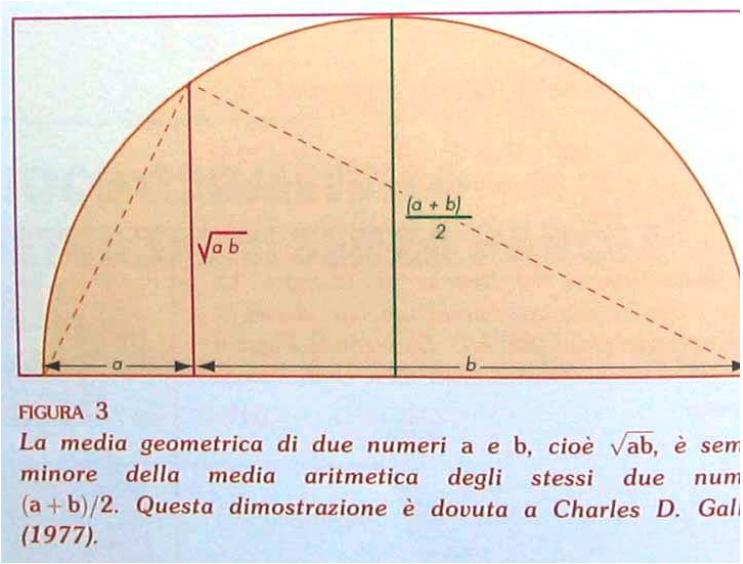
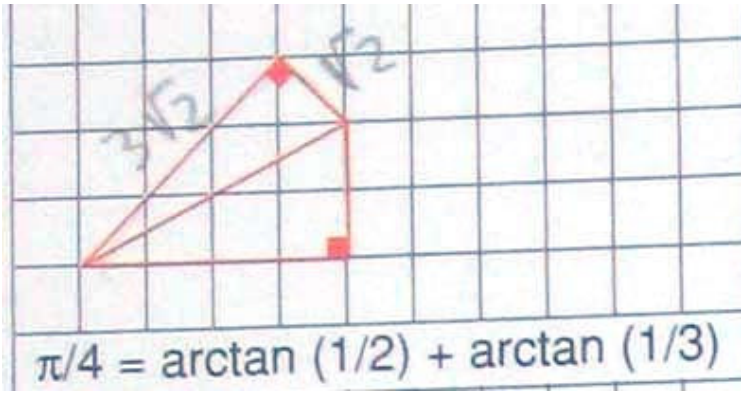
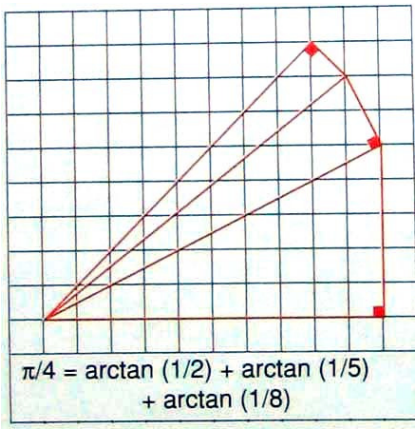


FIGURA 3
La media geometrica di due numeri a *e* b, *cioè* $\sqrt{ab}$, *è sem*
minore della media aritmetica degli stessi due num
$(a+b)/2$. *Questa dimostrazione è dovuta a Charles D. Gal*
(1977).

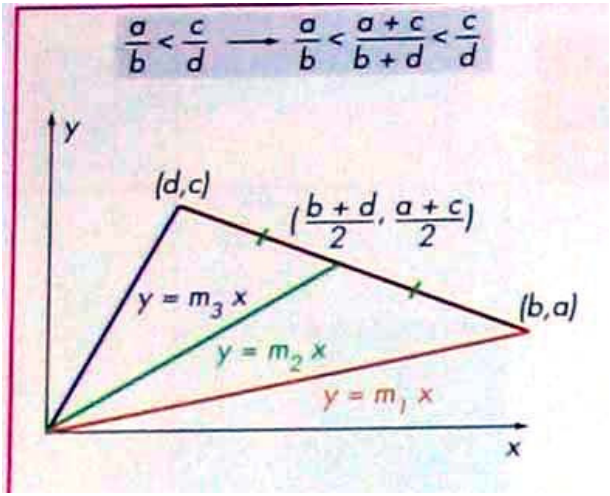
```
g = Import["/home/michele/math/numbt/arctan1.jpg"];
Show[g];
```



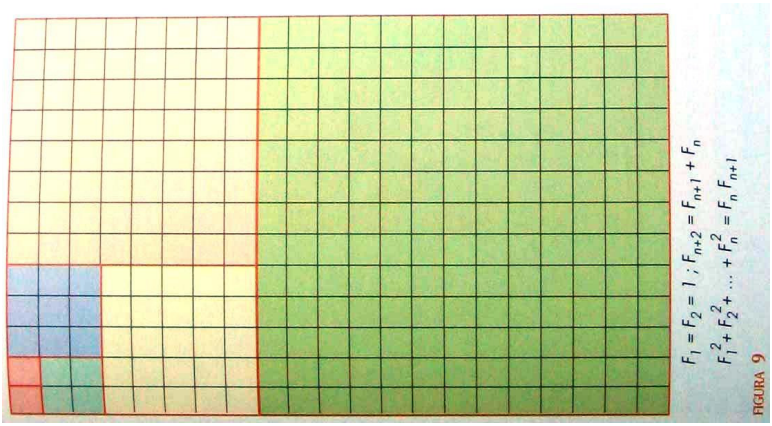

```
g = Import["/home/michele/math/numbt/arctan2.jpg"];
Show[g];
```



```
g = Import[
   "/home/michele/math/numbt/coeff-angolari.jpg"];
Show[g];
```



```
g = Import[
   "/home/michele/math/numbt/quadrati-fibo2.jpg"];
Show[g];
```



La somma dei quadrati dei numeri di Fibonacci da 1 fino ad n e' uguale al prodotto dell' ultimo per il successivo : $F_n F_{n+1}$

Decomposizioni folli: somme e prodotti infiniti

Somme e prodotti di infiniti termini

Quello delle somme (serie, simbolo: $\sum_{k=0}^{\infty} A_k$) di infiniti termini e dei prodotti di infiniti fattori (produttorie, simbolo: $\prod_{k=0}^{\infty} B_k$) e' un argomento molto affascinante e ha storicamente rappresentato i primi tentativi di approccio all'"infinito" in Matematica. Nel seguito, te ne presento qualche esempio, condotto in maniera *naive*, cioe' senza riguardi alle questioni relative alla convergenza.

Una classica serie per π (sviluppo dell'arctan)

Ponendo $z = -x^2$ nella onnipresente serie geometrica $\frac{1}{1-z} = 1 + z + z^2 + z^3 + \ldots$, si ottiene il seguente sviluppo a segni alterni.

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

Dall' Analisi, si sa che l'integrale di $\frac{1}{1+x^2}$ e' proprio arctan(x), per cui, integrando i due membri, avremmo:

$$\arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots = \sum_{k=0} (-1)^k \frac{x^{2k+1}}{2k+1}$$

Ponendo x=1 e ricordando che arctan(1) = $\frac{\pi}{4}$, si ha che sommando gli inversi di tutti i numeri dispari, ma a segno alterno, si ottiene $\pi/4$:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots.$$

La formula di Wallis per π

E se provassimo ad applicare il teorema della decomposizione polinomiale (*uno zero, un fattore*) a funzioni che non siano polinomi? La funzione sin(x), ad esempio, ha, oltre x=0, anche gli zeri positivi nπ e gli zeri negativi -nπ, con n=1,2,3 ... Uhm.

Ma se ad ogni zero devo associare un fattore, qui abbiamo a che fare con infiniti fattori, quali x, $\left(1 - \frac{x}{\pi}\right)$, $\left(1 + \frac{x}{\pi}\right)$, $\left(1 - \frac{x}{2\pi}\right)$, $\left(1 + \frac{x}{2\pi}\right)$, etc.

Associandoli a coppie (il positivo col negativo) e lasciando fuori il solo x=0, arriveremmo ad una decomposizione del tipo:

$$\sin x = x\left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\left(1 - \frac{x^2}{16\pi^2}\right)\ldots$$

Qualunque cosa essa significhi, deve valere per ogni x; ad esempio, deve valere per $x = \frac{\pi}{2}$. Sostituendo questo valore nella relazione precedente e riarrangiando un po' i termini,

troviamo la celebre Identita' di Wallis:

$$\frac{\pi}{2} = \frac{2^2 \times 4^2 \times 6^2 \ldots.}{3^2 \times 5^2 \times 7^2 \ldots.}$$

Sviluppi per e^x,sin(x) e cos(x)

Com'e' noto dall'Analisi, il numero "e" (o meglio: tutte le sue potenze e^x) si possono ottenere come limite della successione $\left(1 + \frac{x}{n}\right)^n$, quando n tende all'infinito. Proviamo a sviluppare la potenza n-esima usando la formula binomiale di Newton:

$$\left(1 + \frac{x}{n}\right)^n = \sum_{k=0\ldots n} C_{n,k} \left(\frac{x}{n}\right)^k =$$

$$1 + (n)\left(\frac{x}{n}\right) + \frac{n(n-1)}{2!}\left(\frac{x}{n}\right)^2 + \frac{n(n-1)(n-2)}{3!}\left(\frac{x}{n}\right)^3 + \ldots.$$

Ma se n e' davvero grande, un espressione come n(n-1) puo' essere sostituita approssimativamente con n^2; n(n-1)(n+2) con n^3, etc. E' facile vedere che queste potenze di n vanno a semplificarsi con le potenze $\frac{1}{n^2}$, $\frac{1}{n^3}$ etc provenienti dal termine (x/n), ottenendo:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Come casi particolari, si ha che "e" non e' altro che la somma degli inversi di tutti i fattoriali (compreso 1/0!), mentre "1/e" contiene gli stessi addendi, ma a segni alterni.

Se invece si applica lo stesso sviluppo alla celebre formula di Eulero ($e^{ix} = \cos(x) + i * \sin(x)$), eguagliando parte reale e parte immaginaria, troveremmo le formule di sviluppo per il seno e il coseno. Essendo cos(x) una funzione pari, "si prenderebbe" le potenze pari, mentre sin(x) quelle dispari, ma a segno alterno.

Le decomposizioni piu' folli: la funzione Zeta di Riemann

Quelle che seguono sono certamente le decomposizioni piu' curiose, piu' straordinarie, piu' folli che si possono incontrare (se si eccettuano quelle del matematico indiano Ramanujan) per il semplice fatto che mettono insieme la serie dei numeri primi e quantita' che, come π,apparentemente non c'entrano nulla, ne' con i primi, ne' con gli interi.

Immagina di calcolare tutte le frazioni del tipo $\frac{p^2}{p^2-1}$, dove p e' un numero primo: p=2,p=3,p=5,p=7, etc e poi di moltiplicarle tutte tra loro:

$$\prod_{p=\text{primo}}^{\infty} \frac{p^2}{p^2-1} = \frac{2^2}{2^2-1}\,\frac{3^2}{3^2-1}\,\frac{5^2}{5^2-1}\,\frac{7^2}{7^2-1}\ldots.$$

Beh, non ci crederai, ma il risultato fa $\frac{\pi^2}{6}$, e che questo stesso risultato e' pari alla somma degli inversi di tutti i quadrati perfetti: $\sum_{k=1}^{\infty} \frac{1}{k^2}$. Ora magari ti starai chiedento cosa succede se invece di p^2 usassimo p^3 nella nostra folle

produttoria. Esatto: viene la somma degli inversi di tutti i cubi perfetti! Con un ultimo salto, se usassimo le potenze p^z, otterremo la famosa funzione zeta di Riemann:

$$\zeta(z) = \prod_{p=\text{primo}}^{\infty} \frac{p^z}{p^z - 1} = \sum_{k=1}^{\infty} \frac{1}{k^z}$$

una delle funzioni piu' celebrate della Matematica. Ogni cosa in piu' che si scopre sulla funzione $\zeta(z)$,e' una cosa in piu' che si scopre sulla distribuzione dei numeri primi nell'ambito della serie dei naturali. Grazie a questa funzione, e' possibile applicare alla Teoria dei Numeri, i tipici metodi dell'Analisi funzionale (derivate, integrali, etc).

Dimostrare che l'equazione $41 = 3^m - 2^n$ non ammette soluzioni con n ed m interi positivi (Olimpiadi 94)

Un classico metodo per risolvere questo tipo di questioni e' provare ad inforcare qualche occhiale di Harry Potter, con un modulo M opportuno. Con M=3, la relazione apparirebbe nella forma $2 = -2^n$. Ma se n e' pari (n=2k), $2^n = 4^k = (1+3)^k$; dunque apparirebbe come $1^k = 1$, modulo 3. Col segno meno, avremmo -1=2 (mod 3). Se n e' dispari (n=2k+1), $2^n = 2\,4^k$; e apparirebbe come 2. Col segno meno: -2=-2+3=1 (mod 3). Quindi, l'unica e' che n dev'essere pari: $41 = 3^m - 2^{2k} = 3^m - 4^k$. Passando ad M=4, vedremmo $1 = 3^m$. Ma $3^m = (4-1)^m = (-1)^m$: avremmo 1 solo se m e' pari (m=2h). In conclusione, dev'essere $41 = 3^{2h} - 2^{2k} = \left(3^h - 2^k\right)\left(3^h + 2^h\right)$. Ma 41, essendo primo, deve contenere solo il fattore 1 o se stesso. Dev'essere per forza $3^h - 2^k = 1$. Sostituendo, avremmo che $41 = 2^{k+1} + 1$, e cioe' $40 = 2^{k+1}$; il che e' impossibile, perche' 40 non e' una potenza del due!

Data la successione

$\{a_n = n\, a_{n-1} + 1,\ a_0 = 1994\}$, quale resto si ottiene dividendo a_{100} per 9? (Cortona 90)

Osserviamo che $a_{100} = 100\, a_{99} + 1 = 100\,(99\, a_{98}+1)+1$. Con gli occhiali M=9, il 99 scomparirebbe e il 100 diventerebbe 1, ottenendo $a_{100} = 2 \pmod 9 = 2 + 9\,k$. *La risposta e' quindi 2.*

Qual'e' la cifra dell'unita' di 1999^{1999}? (Olimpiadi 99)

Tutte le volte che si parla dell'ultima cifra a destra di un numero intero conviene ragionare in modulo 10. Infatti, con M=10, le decine, le centinaia etc si cancellerebbero: *ogni intero e' equivalente alla cifra dell'unita', modulo 10*. Se inforcassimo gli occhiale M=10, potremmo subito scrivere la seguente catena:
$1999^{1999} = 9^{1999} = (10-1)^{1999} = (-1)^{1999}) = -1 = 9$. *L'ultima cifra e' 9.*

Dati 5 interi consecutivi, cosa si puo' sulla cifra dell'unita' del loro prodotto? (Olimpiadi 96)

Immagina di avere davanti a te l'intera serie dei naturali: 1,2,3,4 ... Un intero ogni due e' multiplo di 2 (1/2), uno ogni

tre e' multiplo di 3 (1/3) ... uno ogni 5 e' multiplo di 5. Nei nostri 5 interi consecutivi, dev'esserci almeno un multiplo di 5 e almeno un multiplo di 2. Il loro prodotto dev'essere per forza multiplo di 10. *Risposta: e' sempre 0.*

Qual' e' la cifra dell' unita' di $1^2 + 2^2 + 3^2 + \ldots 1996^2$? 1, 2, 4, 6 oppure 8 ? (Olimpiadi 96)

Raggruppiamo innanzitutto gli addenti in gruppi di 10: da 1^2 a 10^2, da 11^2 a 20^2, etc, piu' gli ultimi 1991^2 ... 1996^2. La somma dei primi 10 quadrati fa 385: apparirebbe quindi come "5" attraverso gli occhiali M=10. La stessa cosa succede per tutti i 199 gruppi di 10 addendi, che danno quindi in totale una somma parziale 5, modulo 10. Gli ultimi 6 appaiono come 1^2+... + 6^2=91=1 (mod 10). In totale abbiamo 6 (modulo 10). *Il numero deve terminare con 6.*

La somma delle cifre del quadrato di 999,999,999,999,999,995 e' 150,160,170,180 oppure 190? (Olimpiadi 2002)

Chiamamo n il numero, e inforchiamo le lenti modulari M=9. Con M=9, ogni numero viene rimpiazzato dalla somma delle sue cifre modulo 9 Avremo quindi n=15*9+5=5 e $n^2 = 25 = 7 \pmod 9$. Dei quattro risultati dati solo il 160 ha la

somma delle cifre uguale a 7. *Il risultato e' 160.*

Con quanti zeri finali termina il fattoriale di 10000? (difficile; da Internet)

Posto n=10000, si ha n!=1*2*3...10000. Un numero che termina con k zeri dev'essere divisibile per $10^k = 2^k \times 5^k$. In teoria, basterebbe contare quante coppie (2,5) compaiono nel prodotto. Si puo' dimostrare che se n multiplo di 100 allora gli zeri finali sono $\frac{n}{4} - 1$. Nel nostro caso, sono 2499 zeri.

Un professore scrive alla lavagna $x^2 + 10\,x + 20$. Tutti gli alunni della classe, a turno, vanno alla lavagna e diminuiscono o aumentano di 1 il termine noto o il coefficiente della x, ma non entrambi. Alla fine ottengono $x^2 + 20\,x + 10$. E' vero che ad un certo punto, durante le operazioni, alla lavagna e' stata scritta un'equazione con le radici intere? (Olimpiade Russe, 1984).

Sia $x^2 + bx + c$ l'equazione. La quantita' b – c puo' solo aumentare o diminuire di 1, durante ogni operazione. All'inizio vale b – c = –10 e alla fine vale b – c = 10. Per continuita',

ci sara' stato un momento in cui b − c = 1, cioe' b = c + 1. Con questo valore il trinomio si scompone in fattori : $x^2 + (c + 1)\, x + c = (x + 1)\,(x + c)$ e le soluzioni intere erano x = −1 e x = −c.

La somma di 3 cubi consecutivi e' sempre multiplo di 9

Com'e' noto, tutti i numeri interi si possono scrivere in una sola delle tre forme: n=3q+r, con r=0,1,2. Se si calcola n^3 si trova $n^3 = 9 * k + r^3$. Questo significa che, con gli occhiali M=9, i cubi sono solo tre: 0,1 e 8 (questa e' anche la somma delle loro cifre, modulo 9). Se sommiamo tre cubi consecutivi, prenderemo certamente tutti e tre i tipi, ottenendo 0+1+8=9=0. CVD.

Esercizi proposti

(1) Dimostra che $3^{15} - 1$ e' composto e trova tutti i fattori che ti riesce.

Osserva che 15=3*5 e che questo permette alcune differenti decomposizioni.

(2) Dimostra che $2^{24} + 1$ e' composto e trova tutti i fattori che ti riesce.

Osserva che 15=3*5 e che questo permette alcune differenti decomposizioni.

(3) Per quali valori di n il numero $P = n^3 - 8n^2 + 2n$ e' divisibile per $Q = n^2 + 1$?

Eseguita la divisione tra P e Q, si potra' scrivere P=q*Q+r. Ne consegue che Q deve dividere anche il resto r. Questo controllo si puo' effettuare manualmente e si trova n=2.

(4) Dimostra che $5^{5k+1} + 4^{5k+2} +$

3^{5k} e' sempre divisibile per 11, per qualsiasi k.

Passa al modulo M=11. Per avere il modulo 11 di un numero, basta sommare le cifre a segni alterni (-1 per quelle di posto dispari, +1 per quelle di posto pari). Ad esempio: 1024=-1+0-2+4=1. Ricorda inoltre che $x^{5k+1} = x*\left(x^5\right)^k$.

(5) Ogni numero positivo n si puo' scrivere nella forma a_1 1!+ a_2 2!+ ... a_k k!, con a_i nell' intervallo [0, i] (S.ANNA)

E' una specie di decomposizione di n nella base (1!,2!,3! ...) invece che in (1,10,100,1000,...). Gli a_i sarebbero "le cifre" della decomposizione, e a_k non e' altro che l'ultima cifra. La dimostrazione si puo' fare in maniera "costruttiva". Parti da un certo n, e cerca il massimo fattoriale k! tale che k!<n<(k+1)!. A questo punto fai la divisione n/k!, cioe' scrivi nella forma $n = (k!)\, a_k + r$. E' chiaro che a_k dev'essere minore di k. Procedi in maniera identica con r, finquando r=1.

Sequenze

Argomento avanzato

La formula di Newton

Un classico problema dell'enigmistica matematica e' il seguente: dati i primi pochi numeri di una sequenza infinita, dedurre la formula che li ha generati. Il metodo di Newton risolve il problema nel caso di formule polinomiali. Detta f(n) la sequenza, la "formula di interpolazione" di Newton e' la seguente:

$$f(n) = \sum_k \binom{n}{k} d_k = d_0 + \mathrm{nd}_1 + \frac{n(n-1)}{2} d_2 \ldots.$$

Come si vede, sono proprio i coefficienti binomiali a produrre le potenze in n del polinomio risultante. Ma cosa sono i numeri d_k? Ecco come ottenerli: scrivere una prima riga con la sequenza originale. Produrre una seconda riga ottenuta dalla precedente sottraendo i termini contingui. Procedere fino a quando non si ottenga una riga nulla e incolonnare le righe in forma di matrice. Bene: la successione d_k non e' altro che la prima colonna di questa matrice.

Esempio

Prendiamo la successione {1,3,17,55,129,251, ...}. La seconda riga e' {2,14,38,74,122,...}. La terza e' { 12, 24,36,48,...}. La quarta e' {12,12,12, ...} e la quinta {0,0,0,0 ...}. La successione e' $d_k = \{1,\ 2,\ 12,\ 12\}$, dato che tutti gli altri termini

saranno senz'altro nulli. Ne consegue che la formula generatrice e':

$$1\binom{n}{0}+2\binom{n}{1}+12\binom{n}{2}+12\binom{n}{3}=1+2n^3$$

Esercizi: Provare con {3,4,7,12,19,28,...} , con {1,5,23,91,269,641,...} , e con {41,43,47,53,61,71, ...}

Sequenze ricorrenti

Per sequenza definita "per ricorrenza" si intende una successione F_n definita dando alcuni termini iniziali e gli altri attraverso un meccanismo induttivo, tale che, grazie ad una formula, si possa calcolare il termine n+1 dai termini precedentemente calcolati. Come procedere se volessimo una "soluzione" esplicita per F_n, cioe' una formula diretta, non ricorsiva?

Una tipica tecnica e' quella di "provare" dei modelli di soluzione del tipo $F_n = x^n$. Inserendo questo modello nell'equazione ricorrente, si ottiene un polinomio (il *polinomio caratteristico)* di cui si ottengono le soluzioni x_1, x_2 etc. Fatto questo, si cerca di combinare linearmente i vari modelli trovati, nella forma $F_n = A(x_1)^n + B(x_2)^n + \ldots$, determinando gli A,B,... a partire dalle condizioni iniziali (i primi valori noti della sequenza).

Esempio

Supponiamo di voler risolvere l'equazione ricorrente $F_{n+1} = \frac{1}{2} F_n$ (caso *omogeneo*). Posto $F_n = x^n$, si ha $x^{n+1} = \frac{1}{2} x^n$.

Dividendo per x^n, otteniamo $x = \frac{1}{2}$. La soluzione e' quindi $F_n = A\left(\frac{1}{2}\right)^n$ (una progressione geometrica). E se invece dovessimo risolvere $F_{n+1} = \frac{1}{2} F_n + 1$(caso *non-omogeneo*) ? In questo caso non possiamo piu' dividere per x^n. Possiamo pero' trovare una soluzione particolare: una sequenza a valori costanti che soddisfa. Posto $F_n = x$=cost, dev'essere $x = \frac{1}{2} x + 1$, che e' soddisfatto con x=2. La teoria generale prevede che si possa sommare la soluzione speciale $x = \frac{1}{2}$ a quella gia' trovata , ottenendo $F_n = A\left(\frac{1}{2}\right)^n + 2$. Questa F_n soddisfa l'equazione data per ogni A. Per determinare A basta il valore di partenza $F_0 = A + 2$, per cui $A = F_0 - 2$.

Applicazione: Catene di Markov

Un viaggiatore ha la seguente abitudine: se oggi va a lavoro con la macchina (M), domani va sicuramente col treno (T); se invece oggi va a lavoro col treno, domani va decidera' se usare la macchina o il treno con una moneta. Determinare al giorno n con che probabilita' lo troviamo sul treno (T_n) e con quale alla guida della sua macchina (M_n).

Un tale processo probabilistico e' detto "catena markoviana" e conduce, in questo caso, a due equazioni ricorrenti (un sistema ricorrente in T ed M). Per impostare le equazioni, invece di pensare ad un singolo viaggiatore, pensa ad un certo numero di viaggiatori (ad esempio 100). Al giorno n-esimo, avremo T_n viaggiatori sul treno e M_n

viaggiatori con la macchina. Il giorno successivo (n+1), quelli che sono sul treno sono meta' di quelli che sono sul treno oggi + tutti quelli che oggi hanno preso la macchina: $T_{n+1} = \frac{1}{2} T_n + M_n$. L'altra meta' di quelli che sono sul treno, domani prenderanno tutti la macchina: $M_{n+1} = \frac{1}{2} T_n$. Ecco le due equazioni ricorrenti, a cui dobbiamo aggiungere il fatto che $M_n + T_n = 1$ (per ogni n), naturalmente.

Usando un po' di algebra, non e' difficile separare le due equazioni, trovando:

$$M_{n+1} = \frac{1 - M_n}{2} = -\frac{1}{2} M_n + \frac{1}{2}$$

che e' proprio del tipo dell'esempio considerato prima. La soluzione speciale e' M=1/3 e quella omogenea e' $A\left(-\frac{1}{2}\right)^n$. Complessivamente si ha $M_n = A\left(-\frac{1}{2}\right)^n + \frac{1}{3}$. Se assumiamo che il giorno 0 il tizio abbia usato la macchina ($M_0 = 1$) troviamo $A = \frac{2}{3}$ e quindi

$$M_n = \frac{2}{3}\left(-\frac{1}{2}\right)^n + \frac{1}{3}$$

Si tratta di una funzione che inizialmente oscilla un po':

```
Table[{n, 2 / 3 * (-1 / 2)^n + 1 / 3}, {n, 0, 10}] // N
```

```
{{0., 1.}, {1., 0.}, {2., 0.5}, {3., 0.25}, {4., 0.375},
 {5., 0.3125}, {6., 0.34375}, {7., 0.328125},
 {8., 0.335938}, {9., 0.332031}, {10., 0.333984}}
```

ma che tende inesorabilmente verso la sequenza stabile 1/3,1/3,1/3 ...

Esercizi

Prova a risolvere queste equazioni per ricorrenza:

```
RSolve[{F[n] == 3 F[n - 1] + 1, F[0] == 1}, F[n], n]
```

$$\left\{\left\{F[n] \to \frac{1}{2}\left(-1+3^{1+n}\right)\right\}\right\}$$

```
RSolve[
  {F[n] == F[n - 1] + F[n - 2], F[1] == 1, F[0] == 0}, F[n], n]
```

$$\left\{\left\{F[n] \to -\frac{\left(\frac{1}{2}-\frac{\sqrt{5}}{2}\right)^{n}-\left(\frac{1}{2}+\frac{\sqrt{5}}{2}\right)^{n}}{\sqrt{5}}\right\}\right\}$$

```
RSolve[{F[n] == 1 / 2 * F[n - 1] + 1, F[0] == 2}, F[n], n]
```

{{F[n] → 2}}