Algoritmi

Problemi e soluzioni con l'aiuto della matematica

Stefano Finzi Vita (Sapienza)

Laboratorio PLS, Scuole GALILEI e DE SANCTIS
Dipartimento di Matematica "G. Castelnuovo", 10 marzo 2017

L'algoritmo dell'amicizia di Sheldon Cooper, *The Big Bang Theory*

Dalla stampa recente...

- *Quando a scrivere è un algoritmo* (EJO, 11.5.2016)
- *Non sempre l'algoritmo di Amazon fa risparmiare* (Internazionale, 27.9.2016)
- *No, gli algoritmi non sono neutrali. Ed è un problema che non possiamo sottovalutare* (L'Espresso, 7.10.2016)
- *Angela Merkel: gli algoritmi di Google e Facebook minacciano il dibattito democratico* (la Stampa, 1.11.2016)
- *Reuters ha creato un algoritmo per verificare le notizie su Twitter* (2.12.2016)
- *Referendum: così gli algoritmi hanno scommesso sul voto* (Il Sole 24 Ore, 5.12.2016)
- *Privacy, no del Garante all'algoritmo della reputazione, viola dignità* (Repubblica, 28.12.2016)

Il metodo matematico

La matematica aiuta a risolvere problemi, spesso costruendo modelli in grado di riprodurre (e quindi eventualmente anche di predire) fenomeni della vita di ogni giorno.

- Per questo è fondamentale analizzare a fondo il problema, da più punti di vista, magari riscrivendolo in un linguaggio formale astratto, per poi trasformarlo in una sequenza di passaggi più semplici in grado di condurre a una soluzione: così nasce in genere un algoritmo.
- A volte di algoritmi possibili se ne trovano diversi, e allora diventa importante riuscire a valutarli e a metterli a confronto.
- Questo tipo di approccio si può esemplificare attraverso semplici problemi di matematica elementare e alcuni algoritmi efficienti per risolverli.
- E visto che in genere sarà un calcolatore a farlo per noi, sarà necessario capire bene con quali numeri lavora e le conseguenze di ciò.

Il codice fiscale (16 caratteri alfanumerici)

Individua univocamente ogni cittadino italiano ai fini fiscali e non solo.

- 3 lettere per il cognome: prime 3 consonanti (se non bastano si riparte dalla prima vocale, ecc., se non bastano ancora si usa una X)
- 3 lettere per il nome: prima, terza e quarta consonante (prima, seconda e terza se solo tre, se meno di tre si usano le vocali e poi X)
- 2 cifre per l'anno di nascita (decine e unità)
- 1 lettera per il mese di nascita:
  GEN=A, FEB=B, MAR=C, APR=D, MAG=E, GIU=H,
  LUG=L, AGO=M, SET=P, OTT=R, NOV=S, DIC=T
- 2 cifre per il giorno di nascita: sommando 40 se si tratta di una donna
- 1 lettera e 3 cifre per ogni comune italiano di nascita (da tabella; es. $Roma = H501$, la lettera è Z se nati all'estero)
- 1 lettera di controllo: si associa ad ogni carattere dei primi 15 un codice numerico in base alla posizione (pari o dispari, da tabelle), si sommano tutti questi codici e si divide per 26, si associa una lettera al resto della divisione (da $A = 0$ a $Z = 25$)

Il codice fiscale: provateci voi

- Scrivete i primi 11 caratteri del CF vostro e delle seguenti persone:
  Alberto ROSSI (21/1/93), Ada BIANCHI (7/12/2001),
  Dario FO (24/3/26), Renato ZERO (30/9/50)

Il codice fiscale: provateci voi

- Scrivete i primi 11 caratteri del CF vostro e delle seguenti persone:
  Alberto ROSSI (21/1/93), Ada BIANCHI (7/12/2001),
  Dario FO (24/3/26), Renato ZERO (30/9/50)
- Risposte:
  RSS LRT 93A21, BNC DAA 01T47
  FOX DRA 26C24, ZRE RNT 50P30

Il codice fiscale: provateci voi

- Scrivete i primi 11 caratteri del CF vostro e delle seguenti persone:
  Alberto ROSSI (21/1/93), Ada BIANCHI (7/12/2001),
  Dario FO (24/3/26), Renato ZERO (30/9/50)
- Risposte:
  RSS LRT 93A21, BNC DAA 01T47
  FOX DRA 26C24, ZRE RNT 50P30
- Più difficile il problema inverso: sapreste riconoscere questi personaggi famosi dall'inizio del loro CF?
  TTT FNC 76P27, BLD LRA 61D68
  MMB CRI 90B20, FRL SRN 64H68

Il codice fiscale: provateci voi

- Scrivete i primi 11 caratteri del CF vostro e delle seguenti persone:
  Alberto ROSSI (21/1/93), Ada BIANCHI (7/12/2001),
  Dario FO (24/3/26), Renato ZERO (30/9/50)
- Risposte:
  RSS LRT 93A21, BNC DAA 01T47
  FOX DRA 26C24, ZRE RNT 50P30
- Più difficile il problema inverso: sapreste riconoscere questi personaggi famosi dall'inizio del loro CF?
  TTT FNC 76P27, BLD LRA 61D68
  MMB CRI 90B20, FRL SRN 64H68
- Risposte:
  Francesco Totti, Laura Boldrini, Ciro Immobile, Sabrina Ferilli

Definizione (dall'Enciclopedia Treccani)

algoritmo (ant. algorismo) s.m. [dal lat. mediev. algorithmus o algorismus, dal nome d'origine, al-Khuwarizmi, del matematico arabo Muhammad ibn Musa del 9 sec., nativo di Kwarizm]

1. Termine che indicò nel medioevo i procedimenti di calcolo numerico fondati sopra l'uso delle cifre arabiche. Nell'uso odierno, anche con riferimento all'uso dei calcolatori, *qualunque schema o procedimento matematico di calcolo*; più precisamente, *un procedimento di calcolo esplicito e descrivibile con un numero finito di regole che conduce al risultato dopo un numero finito di operazioni*, cioè di applicazioni delle regole. In partic., a. euclideo, metodo per determinare il massimo comune divisore di due numeri interi *a* e *b*, basato su divisioni successive.

2. In informatica, insieme di istruzioni che deve essere applicato per eseguire un'elaborazione o risolvere un problema.

Proprietà fondamentali di un algoritmo

1. Numero delle istruzioni finito, così come la lunghezza di ogni istruzione
2. Istruzioni eseguite in sequenza, tramite passi successivi (metodi iterativi)
3. Istruzioni precise e rigorose, non ambigue
4. Finitezza dei dati in ingresso (input) e univocità del risultato (output): a parità di dati in ingresso stesso risultato
5. L'algoritmo presuppone un agente di calcolo che lo esegue (per es. un computer) e uno spazio di memoria a disposizione per gestire le informazioni prodotte durante i calcoli

Valutazione di un algoritmo

- Efficienza: Un algoritmo risolve un problema se per ogni insieme di dati input produce **in tempo finito** la soluzione desiderata (output)
- Complessità: numero di operazioni elementari necessarie, numero di celle di memoria utilizzate
- Stabilità: dipendenza continua dai dati (piccole variazioni in input provocano piccole variazioni in output)

In base a queste proprietà diviene possibile mettere a **confronto** diversi algoritmi che si propongono di risolvere lo stesso problema.
E' spesso opportuno inserire nell'algoritmo un **criterio d'arresto**: i calcoli si fermano se il risultato cercato è ottenuto (almeno con la precisione voluta) oppure se si è raggiunto un numero massimo di iterazioni o un tempo massimo di calcolo.

Se ci aiuta un computer...

Nella maggioranza dei problemi reali la mole di calcoli richiede di servirsi di un computer.

- Servono algoritmi ben strutturati, operazioni semplici ripetute anche milioni di volte (cicli) e diverse strade da percorrere in base alle situazioni (alternative) [*primi elementi di programmazione*] [7 e 1/2]
- Rappresentazione dei numeri: i reali e la loro notazione scientifica (decimale, esponenziale, in virgola mobile, cambi di base), caratterizzazione di razionali e irrazionali.
- Determinazione dell'insieme dei numeri macchina, cioè dei numeri effettivamente rappresentabili su di un computer: un insieme 'colabrodo' in confronto al continuo dei reali.
- L'algebra dei numeri macchina è profondamente diversa da quella dei reali: identità che diventano false, proprietà che non valgono più, operazioni 'pericolose' ed effetti disastrosi.

Un po' di storia

Esempi di algoritmi si trovano sin dall'antichità (papiro di Rhind, papiro di Mosca, matematica babilonese).

Gli stessi Elementi di Euclide sono un libro di costruzioni geometriche, cioè di **algoritmi** e di **dimostrazioni**.

E. Rogora: *La sintesi di dimostrazione e algoritmo, di matematica platonica e tecnologia pratica, porta alla progettazione matematica, alla modellizzazione, alla tecnologia scientifica*, in particolar modo con l'avvento di mezzi di calcolo sempre più potenti.

Ma la matematica resta centrale, perché serve a validare gli algoritmi attraverso la dimostrazione del loro funzionamento e delle loro proprietà .

al-Khwarizmi

La parola 'algoritmo' viene da al-Khwarizmi, nome del matematico arabo che all'inizio dell'800 d.C. scrisse il testo che si può considerare fondativo dell'Algebra:

Kitab al-jabr wa al-muqabala

In esso si propongono metodi pratici (**algoritmi**) per risolvere equazioni che legano radici (x), quadrati (x^2) e numeri, in pratica equazioni di secondo grado. Erano problemi concreti, che nascevano frequentemente da questioni di suddivisione di terreni. La cosa interessante è che tali metodi sono provati con **dimostrazioni geometriche**, basate sulla geometria di Euclide, a quei tempi ben conosciuta dagli arabi che l'avevano ritradotta dal greco.

Un esempio dal libro di al-Khwarizmi

Supponiamo di dover risolvere la seguente relazione

$$4 + x^2 = 2x^2 - 3x$$

La prima fase consiste nel ricondurla ad uno dei casi standard mediante trasformazioni elementari (nel nostro caso a *radici* + *numero* = *quadrati*):

- al-jabr (riparare/aggiustare): somma $3x$ ad ambo i membri:

$$4 + x^2 + 3x = 2x^2 - 3x + 3x = 2x^2$$

- al-mukabala (messa a confronto): sottrai x^2 da ambo i membri

$$4 + x^2 + 3x - x^2 = 2x^2 - x^2 = x^2$$

Siamo così ricondotti al problema *Tre radici e quattro in numero sono uguali a un quadrato*, cioè

$$3x + 4 = x^2$$

L'algoritmo per $3x + 4 = x^2$

$(bx + c = x^2)$

- dividi a metà il numero delle radici $(\frac{b}{2})$
- moltiplicalo per se stesso $(\frac{b^2}{4})$
- aggiungilo a 4 $(\frac{b^2}{4} + c)$
- prendi la sua radice $(\sqrt{\frac{b^2}{4} + c})$
- aggiungila alla metà del numero delle radici
- il numero trovato è il risultato cercato

Provateci ! Quanto viene ?

L'algoritmo per $3x + 4 = x^2$

$(bx + c = x^2)$

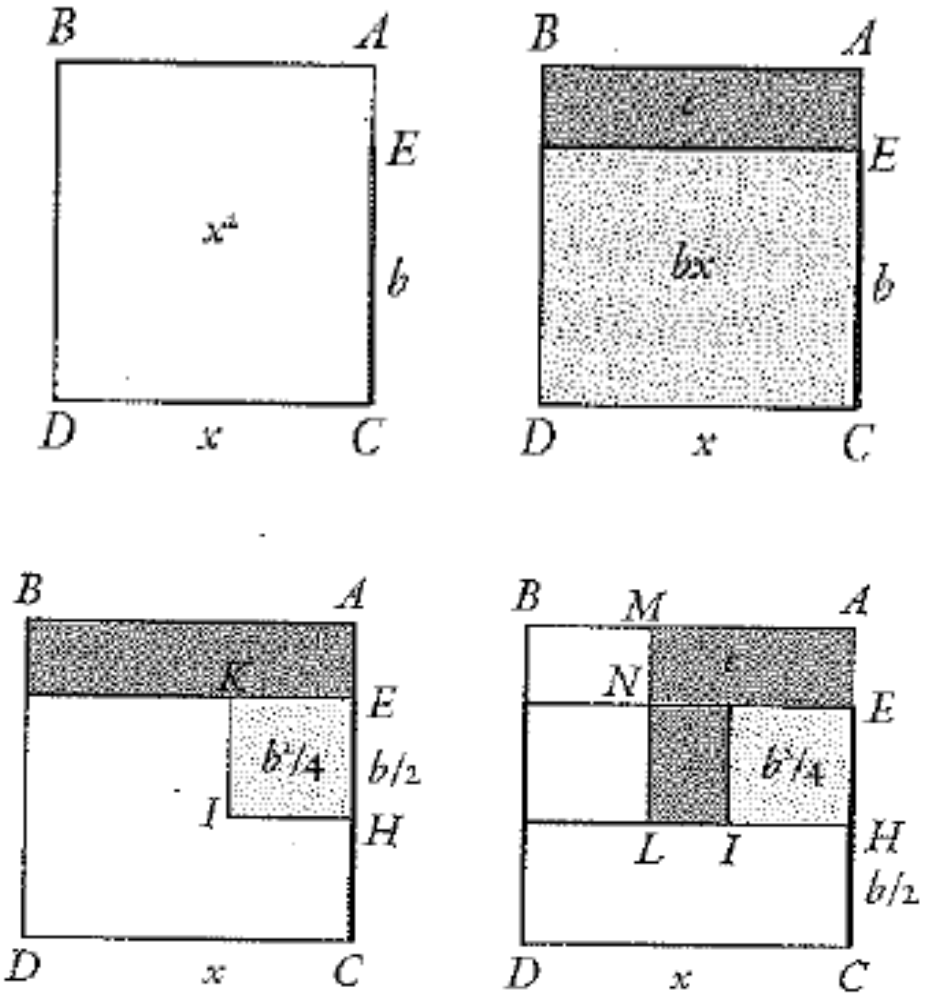
- dividi a metà il numero delle radici $(\frac{b}{2})$: $\frac{3}{2} = 1 + \frac{1}{2}$
- moltiplicalo per se stesso $(\frac{b^2}{4})$: $\frac{3}{2} \times \frac{3}{2} = \frac{9}{4} = 2 + \frac{1}{4}$
- aggiungilo a 4 $(\frac{b^2}{4} + c)$: $6 + \frac{1}{4}$
- prendi la sua radice $(\sqrt{\frac{b^2}{4} + c})$: $\sqrt{6 + \frac{1}{4}} = \frac{5}{2} = 2 + \frac{1}{2}$
- aggiungila alla metà del numero delle radici: $(2 + \frac{1}{2}) + (1 + \frac{1}{2}) = 4$
- il numero trovato è 4

In pratica si è usata la formula:

$$x = \frac{b}{2} + \sqrt{\frac{b^2}{4} + c}$$

che chi ha studiato le equazioni di secondo grado riconoscerà.

Dimostrazione geometrica (si usa Euclide!)



Se è vero che un problema non si capisce a fondo finché non lo si deve insegnare a qualcun altro, a maggior ragione nulla è compreso in modo più approfondito di ciò che si deve insegnare ad una macchina, ovvero di ciò che va espresso tramite un algoritmo.

Donald Knuth (Stanford University, The art of computer programming)

Somme e prodotti

Sono le operazioni più semplici. Proprio perché le più usate, e spesso su grandi quantità di dati, è importante che siano fatte nel modo più efficiente. Se questi dati sono indicizzati, potremmo scrivere:

$$S = \sum_{i=1}^{n} a_i = a_1 + a_2 + .. + a_n \; ; \quad P = \prod_{i=1}^{n} b_i = b_1 * b_2 * .. * b_n \; .$$

In entrambi i casi possiamo pensare a un *ciclo* attraverso il quale accumulare tali quantità in una variabile opportuna (che andrà inizializzata a zero nel primo caso, a uno nel secondo). Ecco gli schemi corrispondenti:

1) $S = 0$; per $i = 1, .., n$ calcola: $S = S + a_i$

2) $P = 1$; per $i = 1, .., n$ calcola: $P = P * b_i$

N.B. Attenzione al significato di '=' in questo caso: $a = b$ equivale a dire che il valore della variabile b viene assegnato alla variabile a ($a <— b$).

Un esempio dove la matematica ci aiuta a risparmiare

Prendiamo il caso in cui $a_i = i$; allora S sarà la somma dei primi n numeri naturali. Il ciclo appena visto ci darebbe il valore cercato mediante n operazioni, quindi ad un costo crescente con n.
In realtà sappiamo che possiamo avere la risposta con sole due operazioni qualunque sia n, visto che possiamo dimostrare che $S = \frac{n(n+1)}{2}$.

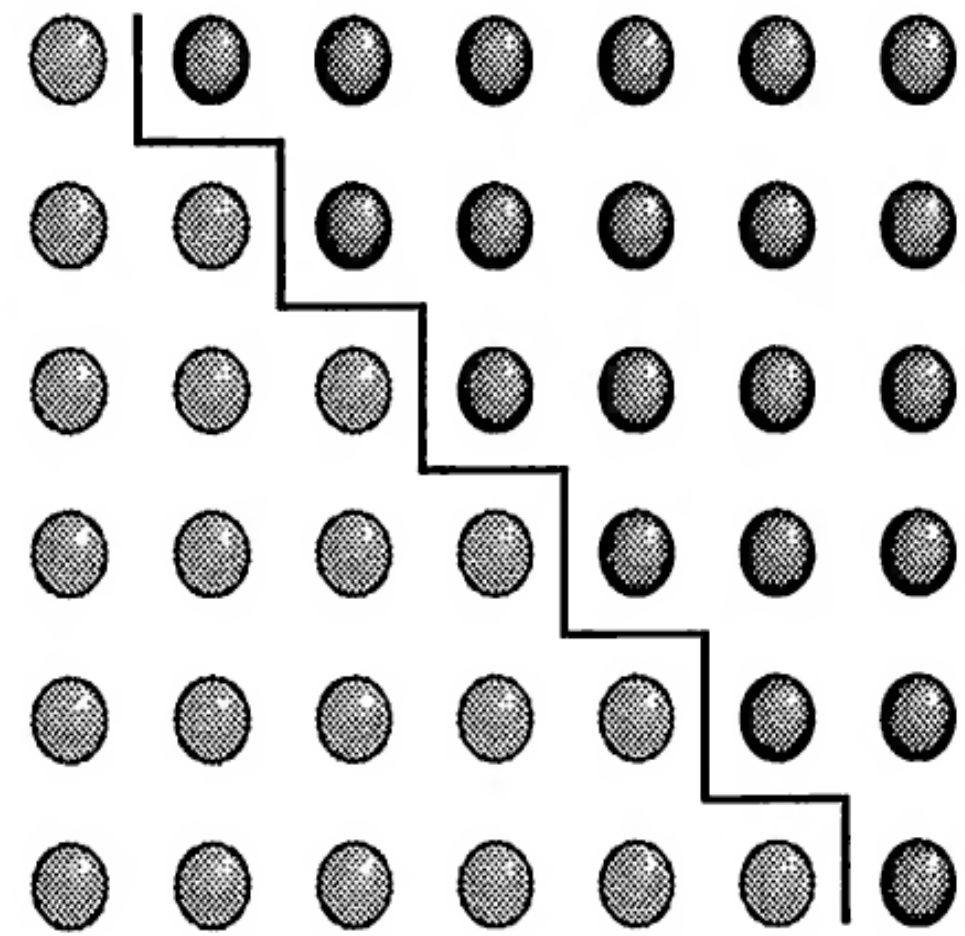
Dim.: Scriviamo i numeri da 1 a n su due righe sovrapposte, una volta da sx a dx, l'altra da dx a sx; per esempio se $n = 10$:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10$$

$$10 \quad 9 \quad 8 \quad 7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2 \quad 1$$

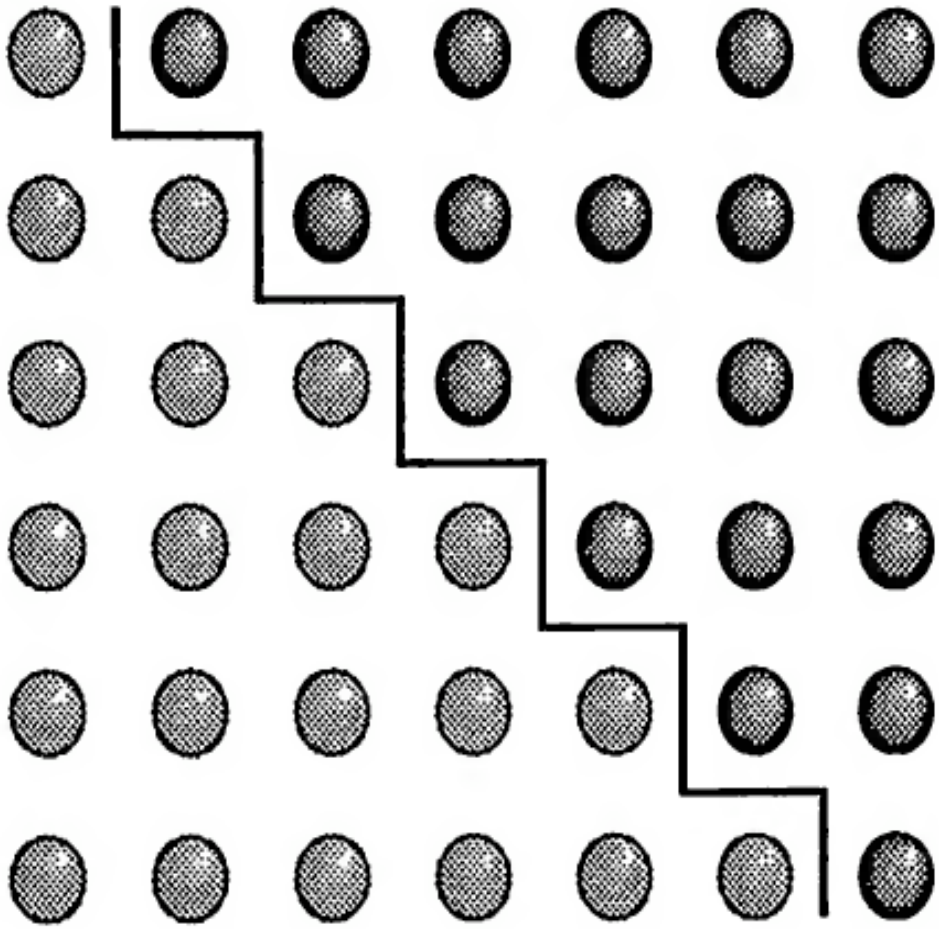
Se ora sommiamo a due a due gli elementi sovrapposti, ci accorgiamo che le n somme valgono sempre 11, cioè $(n+1)$; per avere S basterà quindi prendere la metà del prodotto tra n e $(n+1)$.

Una dimostrazione grafica (per $n = 6$)



Quanto vale la somma dei primi 100 numeri naturali?

Una dimostrazione grafica (per $n = 6$)



Quanto vale la somma dei primi 100 numeri naturali? 5050

Esercizio 1: le potenze

Dall'algoritmo del prodotto ricaviamo subito quello della potenza intera di un numero q. Infatti $q^n = q * q * ... * q$ ($n-1$ prodotti), e quindi:

$$POT = q; \quad \text{per } i = 1, .., n-1 \quad \text{calcola:} \qquad POT = POT * q$$

Stavolta l'indice i serve solo a contare il numero dei fattori in gioco, tutti uguali tra loro. Supponiamo di essere ora interessati a calcolare la quantità:

$$S_n(q) = 1 + q + q^2 + .. + q^n = \sum_{i=0}^{n} q^i,$$

(la somma dei primi n termini della progressione geometrica di ragione q)

1. Quante operazioni servono per calcolare $S_n(q)$ (in funzione di n) eseguendo i calcoli così come sono scritti?
2. Sapreste ottenere lo stesso risultato con soli n prodotti e n somme?
3. Una formula matematica può ridurre ulteriormente il calcolo a n prodotti, un quoziente e due somme.

Soluzione Es. 1

1. $1 + 2 + .. + (n-1) = n(n-1)/2$ prodotti per le potenze, più n somme;

Soluzione Es. 1

1. $1 + 2 + .. + (n-1) = n(n-1)/2$ prodotti per le potenze, più n somme;
2. poiché ogni volta la nuova potenza da sommare è quella del passo precedente moltiplicata per q, basterà una sola moltiplicazione per ogni nuovo addendo se avremo cura di memorizzare quanto già fatto, quindi in totale n prodotti e n somme. Ecco come:

   Dato q; $x = 1$, $s = 1$;
   per $i = 1, .., n$
   ripeti: $x = x * q, \quad s = s + x$;

   Nella variabile x andranno accumulandosi via via le potenze successive di q da aggiungere ad s, che alla fine conterrà la somma richiesta.

Soluzione Es. 1

1. $1 + 2 + .. + (n-1) = n(n-1)/2$ prodotti per le potenze, più n somme;
2. poiché ogni volta la nuova potenza da sommare è quella del passo precedente moltiplicata per q, basterà una sola moltiplicazione per ogni nuovo addendo se avremo cura di memorizzare quanto già fatto, quindi in totale n prodotti e n somme. Ecco come:

   Dato q; $x = 1$, $s = 1$;
   per $i = 1, .., n$
   ripeti: $x = x * q, \quad s = s + x$;

   Nella variabile x andranno accumulandosi via via le potenze successive di q da aggiungere ad s, che alla fine conterrà la somma richiesta.
3. E' facile verificare che per $q \neq 1$ si ha:

$$(1 + q + q^2 + .. + q^n)(1 - q) = 1 - q^{n+1} \Rightarrow S_n(q) = \frac{1 - q^{n+1}}{1 - q},$$

   quindi per calcolare $S_n(q)$ ci servono solo n prodotti (per il calcolo di q^{n+1}), un quoziente e due somme.

Esercizio 2: i polinomi

Supponiamo di dover valutare per $x = \bar{x}$ un polinomio di grado n

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \ .$$

1. Quante operazioni (somme e prodotti) servono per calcolare $p_n(\bar{x})$?

Esercizio 2: i polinomi

Supponiamo di dover valutare per $x = \bar{x}$ un polinomio di grado n

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \ .$$

1. Quante operazioni (somme e prodotti) servono per calcolare $p_n(\bar{x})$?
2. Proviamo ora a riscrivere il polinomio in un altro modo (equivalente):

$$p_n(x) = a_0 + x(a_1 + x(a_2 + x(a_3 + ...(a_{n-1} + a_n x))...)$$

e ad eseguire il calcolo dall'interno all'esterno delle parentesi:

Dato $x = \bar{x}$; $s = a_n$; per $i = 1, .., n$ calcola: $s = s * x + a_{n-i}$.

E' l'algoritmo di Horner, molto noto in Analisi numerica e particolarmente utile quando in un problema occorrono molte valutazioni polinomiali. Quanti sono ora i prodotti effettuati?

Esercizio 2: i polinomi

Supponiamo di dover valutare per $x = \bar{x}$ un polinomio di grado n

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \ .$$

1. Quante operazioni (somme e prodotti) servono per calcolare $p_n(\bar{x})$?
2. Proviamo ora a riscrivere il polinomio in un altro modo (equivalente):

$$p_n(x) = a_0 + x(a_1 + x(a_2 + x(a_3 + ...(a_{n-1} + a_n x))...)$$

e ad eseguire il calcolo dall'interno all'esterno delle parentesi:

Dato $x = \bar{x}$; $\quad s = a_n$; per $i = 1, .., n$ calcola: $s = s * x + a_{n-i}$.

E' l'algoritmo di Horner, molto noto in Analisi numerica e particolarmente utile quando in un problema occorrono molte valutazioni polinomiali. Quanti sono ora i prodotti effettuati?

3. Calcolate il valore di $p_5(2)$ mediante l'algoritmo di Horner per il polinomio $p_5(x) = 3x^5 - 2x^4 + x^2 - 4x + 1$.

Soluzione Es. 2

1. Per ogni valore dato di x saranno necessari $n(n+1)/2$ prodotti e n somme.

Soluzione Es. 2

1. Per ogni valore dato di x saranno necessari $n(n+1)/2$ prodotti e n somme.

2. Le somme sono ancora n, ma ora sono n anche i prodotti. Se n è grande ma soprattutto se dobbiamo valutare il polinomio su tanti valori diversi di x il risparmio sarà notevole.
(Ad esempio per $n = 10$, nel primo caso faremmo 65 operazioni, con Horner solo 20)

Soluzione Es. 2

1. Per ogni valore dato di x saranno necessari $n(n+1)/2$ prodotti e n somme.

2. Le somme sono ancora n, ma ora sono n anche i prodotti. Se n è grande ma soprattutto se dobbiamo valutare il polinomio su tanti valori diversi di x il risparmio sarà notevole.
(Ad esempio per $n = 10$, nel primo caso faremmo 65 operazioni, con Horner solo 20)

3. $$\begin{aligned} p_5(2) &= 1 + 2 * (-4 + 2 * (1 + 2 * (0 + 2 * (-2 + 2 * 3)))) = \\ &= 1 + 2 * (-4 + 2 * (1 + 2 * (0 + 8))) = \\ &= 1 + 2(-4 + 2 * (1 + 16)) = 1 + 60 = 61. \end{aligned}$$

Pari e dispari, divisori, multipli

Sappiamo tutti riconoscere istantaneamente se un numero intero n è pari o dispari. Ma come può farlo un computer?
Possiamo ricorrere al valore del resto della divisione (intera) di n per 2. Se tale resto varrà 0 il numero sarà pari, altrimenti dispari. Con variabili intere, il quoziente di due interi sarà un intero, e quindi:

$$\text{Se} \quad \left(\frac{n}{2}\right) \times 2 = n \quad \Rightarrow \quad n \text{ pari;} \quad \text{altrimenti } n \text{ dispari.}$$

Più in generale un numero intero a sarà un *multiplo* di un altro numero b (o, il che è lo stesso, b sarà un *divisore* di a) se la divisione di a per b dà resto zero.

Congruenza e classi resto

Il resto della divisione tra interi è anche alla base della suddivisione dei numeri interi in *classi resto modulo n* mediante la relazione di equivalenza:

$$a \equiv b \mod n \ (a \text{ congruo } b \text{ modulo } n) \Leftrightarrow (a - b) \text{ è multiplo di } n.$$

Se a e b sono entrambi positivi, la definizione precedente equivale ad affermare che i due numeri divisi per n danno lo stesso resto. Questa relazione suddivide tutto l'insieme dei numeri interi in esattamente n classi di equivalenza, in base al valore del resto della divisione per n:

$$[0], [1], [2], .., [n-1] \ .$$

Ad esempio se $n = 2$ le 2 classi di equivalenza coincideranno con l'insieme dei numeri pari (la classe $[0]$) e quello dei numeri dispari (la classe $[1]$). Oppure se $n = 5$, la classe $[3] \mod 5$ sarà ad esempio l'insieme

$$[3] = \{3, 8, 13, 18, ..., -2, -7, -12, ...\}$$

Esercizio 3

Le classi resto mod n ci possono essere utili ad esempio per stampare una lista di numeri a gruppi di n (cioè n per riga), come nel caso di una tabella.

- Sapreste scrivere uno pseudocodice per stampare i numeri interi da 1 a 25 su 5 righe successive?

Esercizio 3

Le classi resto mod n ci possono essere utili ad esempio per stampare una lista di numeri a gruppi di n (cioè n per riga), come nel caso di una tabella.

- Sapreste scrivere uno pseudocodice per stampare i numeri interi da 1 a 25 su 5 righe successive?
- **Soluzione.**
  per i=1,...,25:
    stampa i ;
    se i-(i/5)*5=0 vai a capo

MCD e mcm

Le formule apprese nella scuola media per il calcolo di **MCD** e **mcm** di due numeri interi a e b si basano sulla preventiva scomposizione di entrambi i numeri in fattori primi. Questo approccio non è in generale conveniente perché costoso. Vediamo come possiamo calcolare il **MCD** senza scomporre i due numeri, e come ricavare di conseguenza anche il **mcm**.

Algoritmo 1 (*delle sottrazioni successive*)
Se due numeri a e b (con $0 < a < b$) sono divisibili per un intero d, lo sarà anche la loro differenza $b - a$. Allora:

$$MCD(b, a) = MCD(b - a, a)$$

e si ripete il ragionamento a partire da numeri più piccoli finché uno dei due numeri diventa zero. Ad esempio:

$$MCD(60, 18) = MCD(42, 18) = MCD(24, 18) = MCD(18, 6) = \\ = MCD(12, 6) = MCD(6, 6) = MCD(6, 0) = 6$$

(si è usata la convenzione $MCD(n, 0) = n$).

L'algoritmo sarà dunque:

dati $0 < a < b$, ripeti:
    $r = b - a$
    se $r = 0 \Rightarrow mcd = a$;
    altrimenti
        se $(r < a)$ poni $b = a$; $a = r$;
        altrimenti poni $b = r$;
finché $(r > 0)$

Questo algoritmo può essere molto lento: se i due numeri fossero ad esempio 900 e 15, servirebbero ben 60 passaggi per concludere che 15 è proprio il loro MCD, come era subito determinabile dal fatto che si tratta di un divisore di 900. Seguiamo quindi un'altra strada.

Algoritmo 2 (*delle divisioni successive*)
Se due numeri a e b (sempre con $0 < a < b$) sono entrambi divisibili per un intero d, lo sarà anche il resto r della divisione di b per a ($b = a \times q + r$, con $0 \leq r < a$). In particolare, se $r = 0$ allora $MCD(b, a) = a$, altrimenti $MCD(b, a) = MCD(a, r)$ e possiamo ripetere il ragionamento a partire da numeri più piccoli finché non si perviene anche anche qui al caso $MCD(s, 0) = s$. Nell'esempio precedente si avrebbe ora:

$$MCD(60, 18) = MCD(18, 6) = MCD(6, 0) = 6.$$

L'algoritmo sarà in questo caso:

dati $0 < a < b$, ripeti:
$r = b - a \times (b/a)$
se $r = 0 \Rightarrow mcd = a$;
altrimenti poni
b=a; a=r;
finché $(r > 0)$

Minimo comune multiplo

E per il **mcm**?

Vale la seguente formula:

$$mcm(a, b) = \frac{ab}{MCD(a, b)} .$$

Proviamo a dimostrarla:

Se $d = MCD(a, b)$, allora dovrà essere $a = q * d$, $b = p * d$,
e necessariamente p e q dovranno essere primi tra loro.

Allora $(a * b)/d = p * q * d$, quindi otteniamo un multiplo di a e b,
necessariamente minimo perché p, q sono primi tra loro.

Esercizio 4

- Calcolare il *MCD* (mediante gli Algoritmi 1 e 2) e il *mcm* dei numeri 6510 e 5880.

Esercizio 4

- Calcolare il *MCD* (mediante gli Algoritmi 1 e 2) e il *mcm* dei numeri 6510 e 5880.
- Soluzione.
  ALG1:
  $(6510, 5880) = (5880, 630) = (5250, 630) = (4620, 630) =$
  $= (3990, 630) = (3360, 630) = (2730, 630) = (2100, 630) =$
  $= (1470, 630) = (840, 630) = (630, 210) = (420, 210) =$
  $= (210, 210) = (\mathbf{210}, 0)$.

  ALG2:
  $(6510, 5880) = (5880, 630) = (630, 210) = (\mathbf{210}, 0)$.

Esercizio 4

- Calcolare il *MCD* (mediante gli Algoritmi 1 e 2) e il *mcm* dei numeri 6510 e 5880.
- Soluzione.
  ALG1:
  $(6510, 5880) = (5880, 630) = (5250, 630) = (4620, 630) =$
  $= (3990, 630) = (3360, 630) = (2730, 630) = (2100, 630) =$
  $= (1470, 630) = (840, 630) = (630, 210) = (420, 210) =$
  $= (210, 210) = (\mathbf{210}, 0)$.

  ALG2:
  $(6510, 5880) = (5880, 630) = (630, 210) = (\mathbf{210}, 0)$.
- $$mcm(6510, 5880) = \frac{38278800}{210} = 182280$$

Un esempio di metodo iterativo per il calcolo di $\sqrt{2}$

L'idea è quella di generare una sequenza di valori che si avvicinino sempre più al valore cercato, che data la sua irrazionalità potrà solo essere approssimato con una certa precisione.

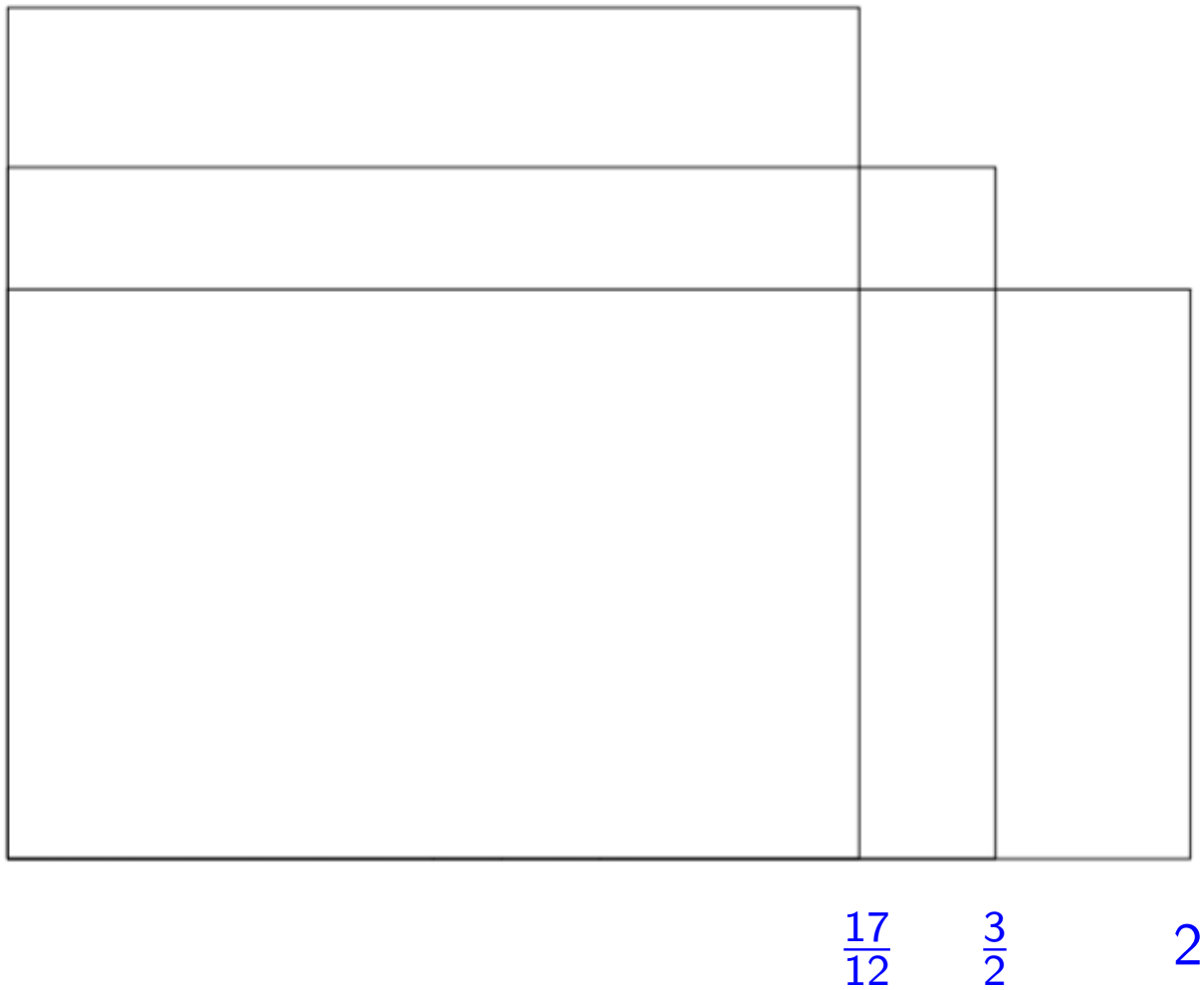
Idea geometrica: $\sqrt{2}$ è la misura del lato del quadrato di area 2. Partiamo allora da un rettangolo di dimensioni x_0 e $2/x_0$ (quindi di area 2) e cerchiamo di generare una sequenza di rettangoli di dimensioni via via più vicine tra loro, che si avvicini quindi sempre più al quadrato cercato. Osserviamo che la media aritmetica tra i valori x_0 e $2/x_0$ sarà compresa tra di essi. Poniamo quindi:

$$x_1 = \frac{1}{2}(x_0 + \frac{2}{x_0})$$

Ad es. se $x_0 = 2$, allora $x_1 = 3/2 = 1.5$, e passeremo quindi da un rettangolo di dimensioni 2×1 a un rettangolo di dimensioni $3/2$ e $4/3$. Ripetendo il procedimento:

$$x_2 = \frac{1}{2}(x_1 + \frac{2}{x_1}) = \frac{1}{2}(\frac{3}{2} + \frac{4}{3}) = \frac{17}{12} = 1.4166666...$$

Idea grafica



Algoritmo di Erone per il calcolo di $\sqrt{2}$

Assegnato $x_0 > \sqrt{2}$, calcola $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$ per $n = 0, 1, 2, ...$

Partendo per esempio da $x_0 = 2$, i primi 5 valori saranno:

1.5
1.416666666666667
1.414215686274510
1.414213562374690
1.414213562373095

Con sole 5 iterazioni otteniamo una precisione di oltre 10^{-10}!

Idea algebrica: partiamo dall'equazione $x^2 = 2$; allora

$$x = \frac{2}{x} \quad \rightarrow \quad 2x = x + \frac{2}{x} \quad \rightarrow \quad x = \frac{1}{2}(x + \frac{2}{x})$$

L'algoritmo di Erone si ottiene trasformando l'ultima equazione (soddisfatta da $\sqrt{2}$) in un metodo iterativo innescato da un valore iniziale.

Funziona sempre? Che succede se prendessimo il metodo : $x_{n+1} = \frac{2}{x_n}$?

La rappresentazione dei numeri: il caso continuo

Ogni numero reale può essere rappresentato come un numero decimale illimitato, periodico o no, in notazione posizionale:

$$x = n.a_1 a_2 \dots a_k \cdots = n + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_k}{10^k} + \dots$$

dove $n \in \mathbb{Z}$ (parte intera), $a_i = 0, 1, \dots, 9$. In particolare:

- periodici $\rightarrow$ razionali ($\mathbb{Q}$) (algoritmo per la frazione generatrice):
  Es.: $2(.00000\dots),\ 3.5(00000\dots),\ 0.\overline{6},\ 7.02\overline{428}$
- non periodici $\rightarrow$ irrazionali ($\mathbb{R}\backslash\mathbb{Q}$):
  Es.: $\sqrt{2},\ \sqrt{3},\ \pi,\ e$

Ogni numero reale x può essere approssimato (con precisione arbitraria) mediante un numero razionale $\overline{x}$ [**densità di $\mathbb{Q}$ in $\mathbb{R}$**] e *la retta reale non ha buchi* [**continuità dei numeri reali**].

Sul cambiamento di base

La scelta di usare la base 10 risponde all'esigenza di facilitare i calcoli, ma ovviamente non è l'unica possibile. Ad esempio si è scoperto che gli Inca usavano per i calcoli un abaco (la Yupana) basato sulla notazione posizionale in base 40 (*N. De Pasquale*, 2001). L'aritmetica dell'orologio è in base 60. E i computer lavorano in base 2. E' quindi utile poter passare da una base all'altra, convertendo la rappresentazione dei numeri.

Attenzione:

- un numero decimale illimitato non periodico lo rimane in ogni base
- un numero decimale finito in una base può restare finito o diventare periodico in un'altra
- un numero decimale periodico in una base può restare periodico o diventare finito in un'altra

Esercizio 5. In quale base il numero periodico $0.\overline{3}_{10}$ diventa un numero con parte frazionaria finita e quale ne sarebbe la rappresentazione?

Sul cambiamento di base

La scelta di usare la base 10 risponde all'esigenza di facilitare i calcoli, ma ovviamente non è l'unica possibile. Ad esempio si è scoperto che gli Inca usavano per i calcoli un abaco (la Yupana) basato sulla notazione posizionale in base 40 (*N. De Pasquale*, 2001). L'aritmetica dell'orologio è in base 60. E i computer lavorano in base 2. E' quindi utile poter passare da una base all'altra, convertendo la rappresentazione dei numeri.

Attenzione:

- un numero decimale illimitato non periodico lo rimane in ogni base
- un numero decimale finito in una base può restare finito o diventare periodico in un'altra
- un numero decimale periodico in una base può restare periodico o diventare finito in un'altra

Esercizio 5. In quale base il numero periodico $0.\overline{3}_{10}$ diventa un numero con parte frazionaria finita e quale ne sarebbe la rappresentazione? 0.1_3

Sul cambiamento di base (segue)

Come si capisce se un numero razionale a in base 10 sia finito o meno in un'altra base b?

- Si calcola la sua frazione generatrice: $a = \left(\frac{n}{m}\right)_{10}$.
- Se m divide una qualche potenza di b (b^k multiplo di m per qualche $k \in \mathbb{N}$), il numero sarà finito in base b, altrimenti no.

Esempi:

$2.5 = \frac{25}{100} = \frac{1}{4} = \frac{1}{2^2} \Rightarrow (2.5)_{10} = (10.1)_2$

$2.7 = \frac{27}{100} = \frac{27}{2^2 5^2} \Rightarrow$ in base due il numero diventa periodico

Ci serve un algoritmo generale per il cambiamento di base, dalla base 10 a un'altra base. Dobbiamo distinguere tra parte intera e parte frazionaria.

Algoritmo per il passaggio da base 10 a base 2

- parte intera: si divide per due finché il risultato non viene zero; i resti delle divisioni in ordine inverso danno la nuova p.i.
- parte frazionaria: si moltiplica per due finché il risultato non ha parte frazionaria nulla o si riottiene una parte frazionaria già incontrata; le parti intere dei prodotti nell'ordine trovato danno la nuova p.f.

Esercizio 6

Algoritmo per il passaggio da base 10 a base 2

- parte intera: si divide per due finché il risultato non viene zero; i resti delle divisioni in ordine inverso danno la nuova p.i.
- parte frazionaria: si moltiplica per due finché il risultato non ha parte frazionaria nulla o si riottiene una parte frazionaria già incontrata; le parti intere dei prodotti nell'ordine trovato danno la nuova p.f.

Esercizio 6

- Trasformate il numero 2.7 in base 2.

Algoritmo per il passaggio da base 10 a base 2

- parte intera: si divide per due finché il risultato non viene zero; i resti delle divisioni in ordine inverso danno la nuova p.i.
- parte frazionaria: si moltiplica per due finché il risultato non ha parte frazionaria nulla o si riottiene una parte frazionaria già incontrata; le parti intere dei prodotti nell'ordine trovato danno la nuova p.f.

Esercizio 6

- Trasformate il numero 2.7 in base 2.
- La parte intera è ovviamente $(10)_2$; per la parte frazionaria avremo:
  $0.7 \times 2 = \mathbf{1}.4$
  $0.4 \times 2 = \mathbf{0}.8$
  $0.8 \times 2 = \mathbf{1}.6$
  $0.6 \times 2 = \mathbf{1}.2$
  $0.2 \times 2 = \mathbf{0}.4$
  $0.4 \times 2 = \mathbf{0}.8$ ecc. ecc
  per cui possiamo dire: $(2.7)_{10} = (10.1\overline{0110})_2$, numero periodico come previsto.