

ASPETTI FONDAMENTALI DELLA MATEMATICA DISCRETA NELL'INSEGNAMENTO SECONDARIO.

F. Eugeni, *Università degli Studi di Teramo, Dipartimento MET*; email: eugenif@tin.it

G. Manuppella, *Scuola Media Sec.Inf. "B.Croce", Pescara*; email: giuseppemanuppella@libero.it

R. Mascella, *Università degli Studi di Teramo, Dipartimento MET*; email: rmascella@tin.it

Abstract. Nell'era delle tecnologie e alla luce dell'inarrestabile crescita di cultura di massa la matematica discreta gioca un ruolo fondamentale nell'insegnamento secondario. Essa da un lato fornisce motivazioni allo studio e chiarisce l'utilità ed il significato concreto della matematica, dall'altro potenzia le capacità di ragionamento e di logica indispensabili in tutte le questioni della vita quotidiana.

1. Introduzione.

Nel corso della Scuola Secondaria molti studenti, soprattutto se provenienti da scuole nelle quali l'interesse verso lo studio della matematica non è eccessivo, maturano definitivamente un profondo rigetto nei confronti della disciplina matematica, mettendo in serio dubbio la sua utilità nella vita pratica. Questo risultato scolastico, di per sé molto preoccupante, è una grossa contraddizione nei termini. Tutti sappiamo che la matematica nasce proprio da problemi concreti che l'uomo vuole risolvere, da questioni legate esclusivamente alla routine della vita quotidiana, senza pesanti problematiche filosofiche, almeno nelle sue tappe iniziali.

E' importante e di notevole interesse chiedersi quali siano le ragioni prevalenti di questi insuccessi in serie. Va intanto osservato che la disciplina presenta difficoltà oggettive, per essere una disciplina ordinata, che non si può studiare senza conoscere molto bene gli innumerevoli prerequisiti insegnati in precedenza, ma vi è anche altro. Uno degli aspetti spesso indicato delle difficoltà si può rilegare all'eccessivo ricorso alla formalizzazione e all'uso pesante di simboli, uso che è presente in molteplici settori dell'insegnamento della matematica. Ma questo problema è ampiamente noto, non solo presso i "didattici". Molti oggi sostengono che la percezione negativa della matematica da parte del grande pubblico derivi da un approccio sbilanciato: troppa forma e poca sostanza. Questo approccio produrrebbe una scarsa motivazione all'apprendimento, quando questo sia fatto quasi esclusivamente di tecniche di calcolo fredde e distanti. Vi sarebbe dunque una difficoltà ad acquisire concetti e modelli senza il necessario apprendistato, senza ripensamenti e rielaborazioni, senza un lavoro lento di costruzione in termini di esempi, verifiche e prove di calcolo.

I tradizionali temi dell'aritmetica, della geometria e dell'algebra sono fondamentali nella costruzione della conoscenza matematica e nello sviluppo delle strutture cognitive logiche. Ma quando in queste tematiche gli studenti trovano seri ostacoli, la reazione più ricorrente è quella di abbandonare il treno dell'apprendimento. Del resto le strategie sono spesso perdenti in questi abbandoni, il metodo della ripetizione dei contenuti è in realtà la ripetizione del metodo rifiutato, cioè si tende a fare di più ma a ripetere nuovamente le stesse argomentazioni, sulla stessa linea, con le medesime manipolazioni dei simboli. Molti studenti, anche se apparentemente meno dotati, rifiutano che le tematiche siano presentate senza interdipendenza, senza intellegibilità, e avvertono quell'atteggiamento che porta a trascurare le possibilità di esplorare opportunamente e significativamente i concetti in contesti diversi o applicarli in situazioni nuove.

La matematica discreta, con la sua ampia varietà di concetti e di tecniche, rappresenta certamente un'ottima soluzione alle problematiche poste nell'insegnamento secondario. Questa branca della matematica, che si occupa di combinare e classificare oggetti distinti, include una larga varietà di argomenti e tecniche che saltano fuori dalla vita quotidiana, come ad esempio *trovare la migliore strada da una città all'altra*, problema nel quale gli oggetti sono le città posizionate su una mappa ma nel quale il senso ... *del trovare la migliore* .. è tutto da precisare. La matematica discreta include anche molteplici attività di conteggio, come ad esempio trovare il *numero di combinazioni diverse di sapori* da mettere su una pizza, scegliere *l'ordine migliore nel quale eseguire una lista di operazioni*, capire come nei computers si possano immagazzinare informazioni e come poi recuperarle senza eccessivi ingombri della memoria. In buona sostanza la matematica discreta è la matematica utilizzata per prendere decisioni giornaliere nella nostra società, fatta di problemi concreti, e quindi di insiemi finiti ai quali spesso, ma non sempre, si associano anche numeri non troppo elevati. Per questo le sue più semplici applicazioni, peraltro molto varie, sono un valido ausilio per lo studente a vedere la rilevanza della matematica nel mondo in cui vivono.

La matematica discreta offre una serie di materiali “freschi” che conducono ad approcci oggi raccomandati: apprendimento per scoperta, problem solving, sperimentazione, apprendimento cooperativo, uso di tecnologie. Con la matematica discreta lo studente è più coinvolto nel “fare” matematica, può lui stesso sentirsi un matematico, invece di un semplice applicatore di procedure risolutive e sequenze di istruzioni standard.

Le seguenti motivazioni a favore dell'insegnamento della matematica discreta sono solo esempi di riflessioni sui loro interessanti contenuti. Circa questo ramo può dirsi che la matematica discreta ...

- è attraente, molti problemi sono delle piccole sfide, possono interessare e possono attirare studenti, e si prestano all'esplorazione e alla scoperta;
- i quesiti che si presentano sono facilmente accessibili, infatti per capire molte problematiche occorrono pochissimi prerequisiti, spesso è sufficiente la sola aritmetica, o la sola algebra elementare;
- offre temi per tutti, poiché le motivazioni che ne derivano sono appropriate sia per studenti già abituati al successo, sia per studenti abituati al fallimento. A nostro avviso sono proprio questi ultimi che forse necessitano di approcci nuovi;
- utilizza tecniche applicabili in moltissime aree della conoscenza, ed oltre a fornire attrezzi preziosi contribuiscono a creare modellizzazioni e descrizioni della realtà molto efficaci.

Nonostante il termine “matematica discreta” potrebbe suonare non familiare, molti dei suoi argomenti sono già presenti nelle classi. Nel momento in cui si contano oggetti, si ordinano, si listano, quando si presentano e si seguono istruzioni, quando si giocano e si analizzano dei giochi, gli insegnanti stanno già introducendo i loro allievi alla matematica discreta. Un esempio molto banale: chiamando tre studenti a lavorare alla lavagna in posizioni diverse l'insegnante potrebbe chiedere: *in quanti modi questi tre studenti possono occupare le varie posizioni?* Questa domanda, pur nella sua semplicità, può essere rapportata con un'altra versione “geometrica” e accostare così problemi apparentemente differenti, laddove, in realtà, è diverso solo il contesto. Così si può far notare come in relazione ad un triangolo fissato, e all'utilizzo delle lettere A, B, e C per i vertici, la domanda: *“in quanti modi è possibile etichettare i vertici del triangolo?”* è una domanda del tutto identica a quella delle posizioni degli studenti.

2. Alcuni problemi di interesse discreto.

Non è nostra intenzione, in questa breve nota, accennare alle varie teorie che nascono o che forniscono problemi, ma piuttosto cercare di capire come la varietà di problemi e quesiti della matematica discreta possa essere vista da un'angolazione orientata esclusivamente all'insegnamento e allo stimolo di particolari capacità degli studenti. Non ci occuperemo perciò dei problemi per appartenenza all'interno delle proprie aree teoriche, siano esse calcolo combinatorio, teoria dei

grafi, teoria dei numeri, geometrie finite, configurazioni e disegni, permutazioni, teorica dei codici, e via dicendo, ma piuttosto cercheremo di distinguerne l'utilità in funzione dell'obiettivo scolastico.

Abbiamo già detto che, con la sua enfasi sul ragionamento logico e sull'analisi e la risoluzione dei problemi, la matematica discreta fornisce un catalizzatore per il pensiero generale e le capacità di problem-solving. A questo proposito si possono diversificare gli ambiti che possono, e in alcuni lo sono già, essere ampiamente approfonditi, curati, esplorati a tutti i possibili livelli scolari.

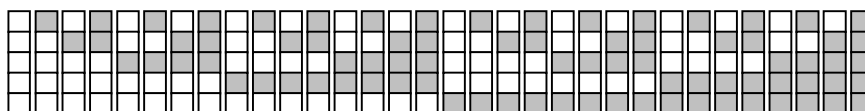
- conteggio ed elencazione metodica di oggetti;
- modellizzazione discreta di situazioni e problemi concrete (usando grafi, alberi e magari anche geometrie finite);
- sviluppo, comprensione e utilizzo di metodi e processi iterativi;
- creazione e applicazione di gruppi di istruzioni e procedure risolutive (algoritmi);
- organizzazione e trattamento dell'informazione (utilizzo delle informazioni criptate).

Nel prosieguo useremo per comodità questa distinzione, ovviamente non unica e della quale si intuiscono numerose e personali varianti. Senza entrare nei misteri dell'arte dell'insegnante la useremo solo per classificare alcuni problemi discreti e alcune capacità logiche che nelle nostre discussioni abbiamo individuato come capacità da allenare e sviluppare.

2.1. Conteggio ed elencazione metodica degli oggetti.

Il tipo di problemi che portano ad elencare i modi, e a contarne il numero, che consentono il completamento di un particolare compito, e quindi le strategie che in essi sono coinvolti vanno evidentemente differenziate fra i vari ordini di scuola. Per descrivere un possibile iter di crescita logico/cognitivo degli studenti, nonché di evoluzione delle difficoltà dei concetti possiamo immaginare per studenti di scuola elementare quesiti in cui si richiede di contare e fare liste di possibili abbinamenti a partire da un certo numero di abiti, (due pantaloni, due magliette ed un maglione), oppure elencazione dei possibili pasti che si possono effettuare scegliendo le pietanze dal menu di un ristorante. In questa prima fase, in buona sostanza, è necessario chiarire il ruolo della moltiplicazione nei problemi di conteggio ovvero di sviluppare l'idea intuitiva del *principio fondamentale del calcolo combinatorio*.

Un esempio, magari successivo, può essere quello di contare tutte le possibili torri di 5 blocchi, formate però solo da blocchi bianchi e neri, come illustrato in figura 1.



- Fig. 1 -

Nella figura le 32 torri sono riportate in modo sistematico utilizzando un criterio ben preciso: le prime 16 torri hanno il primo blocco rosso, le ultime 16 hanno il primo blocco blu, così nelle prime 8 torri anche il secondo blocco è rosso mentre nelle successive 8 il secondo blocco è blu, e così via. Una valida alternativa potrebbe essere anche quella di elencare tutte le torri che hanno solo blocchi rossi, quindi tutte le torri che hanno un solo blocco blu, poi tutte quelle aventi esattamente due blocchi blu, e via dicendo. Questa semplice differenza di elencazione, seppur banale, non è priva di utilità, mettendo a disposizione la possibilità di costruire varie metodologie. Anche il classico *principio del pecoraio* è molto utile a rafforzare questo tipo di comprensione.

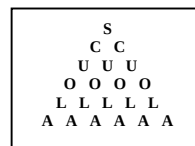
Negli stadi successivi si può passare al conteggio di oggetti che abbiano caratteristiche di ordine insite nella loro costruzione. In altre parole sono utili problemi di *permutazioni* e *disposizioni* eventualmente anche con ripetizione. Esempi tipici sono i numeri e gli anagrammi: quanti sono i numeri formati da quattro cifre, costruibili con le cifre dell'insieme {1,2,3,5,8,9}? Oppure: quante sono le possibili parole, anche non di senso compiuto, che si possono formare con le lettere della parola SCUOLA?

Ultimo aspetto sul quale appuntare l'attenzione è quello dell'ordine che in linea teorica porta alla differenziazione fra *disposizioni* e *combinazioni*. La comprensione di questo aspetto è

generalmente una delle più complesse, al crescere della difficoltà dei problemi. Esempio tipico è il seguente: in quanti modi posso scegliere nella classe quattro studenti? Quanti sono i modi se ai quattro studenti assegno anche compiti particolari e diversi fra loro? Altra possibilità è la seguente: se si hanno a disposizione 10 sapori per preparare una pizza, quante pizze posso preparare in modo che ciascuna abbia 3 gusti differenti?

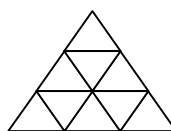
In questo ambito vanno inoltre inclusi tutta una serie di giochi, che diventano vere attività matematiche, nel momento in cui gli studenti riflettono sistematicamente sulle mosse che fanno e usano queste riflessioni per decidere le mosse successive. Esempi di giochi di questo tipo sono il “domino”, “master mind”, “forza quattro”, ecc.

Esempi ricchi di problematiche si desumono dal classico triangolo aritmetico, detto triangolo di Tartaglia, ovvero di sue interpretazioni e varianti. Tipico problema è quello di determinare il numero di possibili cammini per pronunciare la parola SCUOLA nel diagramma a lato (Fig. 2), con le regole di procedere dall’alto in basso, solo a destra o sinistra della lettera che precede e fissando in anticipo in quale lettera A devono terminare i cammini. Questa semplice impostazione permette una diversa formulazione ed un ulteriore approccio alla comprensione del triangolo aritmetico: ora ogni numero del triangolo di Tartaglia dà esattamente il numero dei cammini che giungono nella posizione occupata da quello stesso numero.

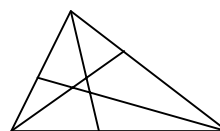


- Fig. 2 -

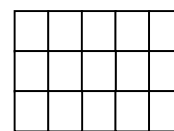
Esistono, tra gli altri, anche tutta una gamma di problemi di conteggio in cui l’approccio e il tipo di enumerazione risulta di fondamentale importanza per la ricerca completa degli oggetti sotto osservazione. Ad esempio il conteggio dei triangoli nelle figure 3 e 4 e dei rettangoli nella figura 5.



- Fig. 3 -



- Fig. 4 -



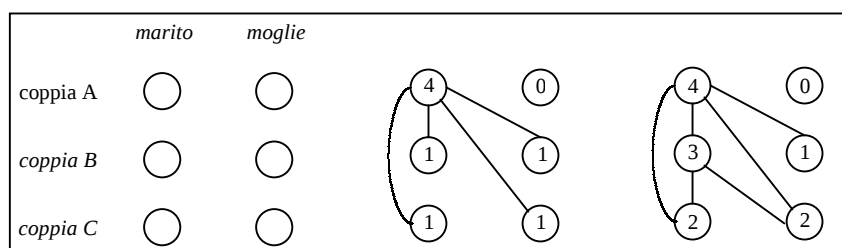
- Fig. 5 -

Questo tipo di problemi è molto utile per catalizzare l’attenzione sulle problematiche di conteggio in ambienti caotici, metodi che non possono essere casuali ma suggeriti da una strategia.

2.2. Modellizzazione discreta dei problemi.

Esempi notevoli di modelli matematici discreti è quello delle reti o *grafi*, che consistono di punti, detti nodi o *vertici*, e linee che li congiungono, generalmente chiamate *archi*. Esempi che conducono a questa modellizzazione sono ovviamente molteplici: si può pensare ad isole (i vertici) congiunte da ponti (gli archi) sulla falsariga del classico problema di Eulero dei ponti di Königsberg, ma anche edifici collegati da strade, abitazioni e collegamenti telefonici, persone e loro relazioni. In altre parole qualunque collezione in cui gli oggetti siano legati da connessioni, il modello matematico può essere un grafo.

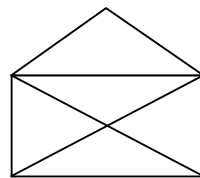
Un primo problema che può chiarire in che modo l’uso dei grafi semplifica l’interpretazione e la soluzione di un problema è il seguente. Ad una festa di amici si ritrovano in una stanza chiusa tre coppie (marito-moglie) fra loro sconosciute. Ogni persona comincia a presentarsi alle altre, tranne che al proprio partner perché evidentemente già lo conosce, con una stretta di mano. Improvvisamente va via la luce e le presentazioni si arrestano. In quel momento il più veloce nel presentarsi ha conosciuto già tutti mentre il più lento non ha conosciuto nessuno. Più in dettaglio le conoscenze fatte da ciascuna persona sono esattamente 4, 3, 2, 1 e 0 (una persona ne ha conosciute 4, una persona ne ha conosciute 3, e via dicendo). La domanda del quesito è: quante conoscenze ha fatto l’unica persona della quale non si hanno



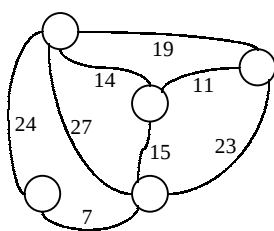
- Fig. 6 -

informazioni? Il problema, apparentemente carente di dati, è modellizzabile come in figura 6 e risulta, a seguito di tale impostazione, assolutamente banale. I grafi riportati nella figura 6 mostrano come procedere verso la soluzione, che nel nostro caso è 2.

Un problema tipico, analogo al problema dei ponti di Königsberg e anche molto diffuso fra gli stessi studenti, è il *problema della busta da lettere*: è possibile tracciare la busta indicata in figura 7 senza staccare mai la penna dal foglio e senza passare più volte su uno stesso arco? Problemi di questo tipo, sono di fatto modellizzazioni con grafo in cui si ricerca un cammino euleriano (cammini in cui ogni arco del grafo occorre in esso esattamente una volta), problemi che possono avere una formulazione applicata molto semplice: è possibile per un viaggiatore percorrere questi tragitti senza passare per più volte su una stessa strada? Per affrontare questo tipo di problemi di piccola ricerca, utilizzando anche altri modelli, in



- Fig. 7 -



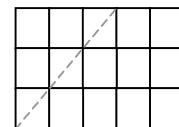
- Fig. 8 -

una prima fase si può procedere per tentativi, ma dal livello di scuola secondaria ci si può astrarre per capire le proprietà che di fatto consentono ad un grafo di avere un tale cammino, cioè analizzare più in generale il problema dell'esistenza.

Altro problema semplice da modellizzare con i grafi è il *problema del commesso viaggiatore*. Un venditore deve compiere un viaggio fra alcune città e vuole calcolare il tragitto complessivamente più breve. Il problema conduce alla costruzione di un modello di *grafo pesato* nel quale i pesi di

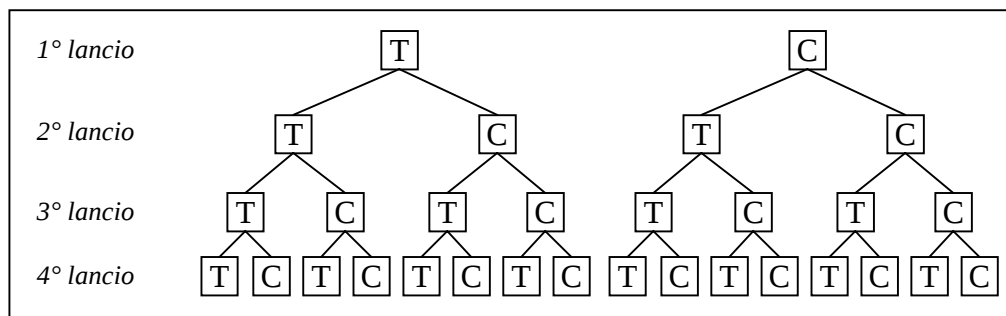
ciascun arco sono le distanze chilometriche. Un esempio è quello riportato in figura 8. La ricerca è in realtà un esercizio di ottimizzazione ed è un primo approccio alle tematiche proprie della ricerca operativa.

Altri problemi di cammini sono quelli in cui la figura a fianco può essere la mappa di una città con edifici e vie di collegamento e nel quale vanno ricercati i percorsi che portano da un estremo all'altro, magari senza attraversare la diagonale tratteggiata (*problema del ballottaggio*).



- Fig. 9 -

Passiamo ad alcuni esempi in cui la modellizzazione porta alla costruzione di un *albero*. L'esempio forse più immediato è quello della *costruzione del proprio albero genealogico*. Problemi tipici sono inoltre tutti quelli legati alle prove ripetute, come il lancio di un dado o di una moneta: quante sono le possibili sequenze di 4 lanci di una moneta in cui compaiano almeno due teste (T) consecutive? Questa elencazione può essere fatta in vari modi, una è quella in figura che mostra come la risposta sia facilmente calcolabile e nel nostro caso è 8.



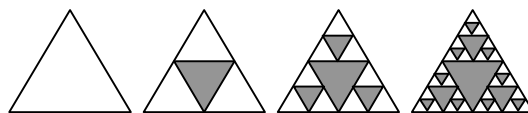
- Fig. 10 -

Questa piccola gamma di esempi crediamo possa delineare il contesto generale delle diverse modellizzazioni. A nostro avviso sono molto utili perché accanto alla percezione e alla comprensione dei modelli planari e spaziali generali, che costituiscono il mondo nel quale ci muoviamo, molte problematiche ricorrenti hanno bisogno di impostazioni diverse e la comprensione di questa fenomenologia è di grosso aiuto.

2.3. Sviluppo, comprensione e uso di processi iterativi e ricorsivi.

In questa sezione intendiamo comprendere tutti quei processi che inducono per più volte la ripetizione di un singolo passo o di una sequenza di passi. A livello elementare il primo esempio di processo iterativo sta nella comprensione della *moltiplicazione*, ovvero l'addizione di un certo numero ripetuta per un numero specificato di volte. A questa età molti altri esempi sono di facile investigazione, ad esempio la decorazione di un pavimento con mattonelle di vari colori o di varie forme ripetuti nella stessa sequenza.

A livello secondario la situazione si fa molto interessante. A livello geometrico le iterazioni più significative sembrano essere quelle che portano alla produzione di *frattali*, così non è privo di interesse



- Fig. 11 -

l'implementazione dei primi passi che portano ad esempio al triangolo Sierpinski (Fig. 11).

Da un punto di vista numerico il primo approccio può avvenire con le progressioni, sia quelle aritmetiche che quelle geometriche. Una vasta gamma di esempi portano alla utilizzazione di questi processi, fra tutti spiccano i problemi di matematica finanziaria per il calcolo di un capitale dopo alcuni anni di deposito, oppure per il pagamento di un'autovettura in un tempo stabilito.

Anche con il calcolatore si possono implementare procedure iterative per il calcolo di soluzioni numeriche di semplici operazioni, ad esempio per il calcolo della radice quadrata. Supponendo di voler calcolare la radice quadrata di 10 prendiamo un'approssimazione iniziale, che può essere 3, e si effettua la divisione $10/3$ del cui risultato si fa la media aritmetica con 3. Quanto ottenuto, cioè 3,1666667, è la nuova approssimazione da cui ripartire per effettuare ulteriori iterazioni.

Particolare attenzione va inoltre dedicata ai procedimenti ricorsivi, per loro natura più complessi in quanto la visione è rovesciata rispetto alle iterazioni: la situazione attuale si riconduce al caso precedente, dunque procediamo a ritroso. Un gioco che ben si presta alla comprensione e all'uso di un processo ricorsivo è quello della *Torre di Hanoi*.

Facciamo un esempio in cui è utile applicare il ragionamento ricorsivo. Calcolare le sequenze di lunghezza 6 delle lettere A, B, C in modo tale che A e B non siano mai vicini. Una possibile procedura potrebbe essere la costruzione di una albero in quanto a partire dalla prima lettera si possono costruire le varie ramificazioni al crescere della lunghezza della

sequenza, tuttavia risulta più agevole ragionare astraendo un po' i concetti. Se indichiamo con T_n il numero delle sequenze di lunghezza n che rispecchiano tale proprietà e, fra queste, con $T_{n,A}$, $T_{n,B}$, $T_{n,C}$ le sequenze che terminano rispettivamente per A, B e C allora la procedura ricorsiva è di banale costruzione e con pochi calcoli è facile trovare la soluzione. Il procedimento è mostrato in figura 12.

L'idea che guida lo sviluppo di queste competenze è certamente quello di lasciare agli studenti l'idea che un tema chiave di tutta la matematica è il metodo che riconduce una situazione "diciamo attuale" ad altra nota sia con l'operare per analogia sia con il "ritorno al caso precedente".

Questa problematica è da capire anche in termini non del tutto codificati, d'altronde è un aspetto sociale abbastanza evidente che una situazione che oggi viviamo in un certo contesto è determinata da quanto è accaduto in precedenza, magari ieri o la settimana precedente.

Dei paragoni interessanti si possono fare anche usando l'aneddoto paradossale del matematico che cuoce l'uovo, riportandosi in modo cretino al caso precedente, ma l'aneddoto è comunque significativo.

$$\begin{aligned} T_{n,A} &= T_{n-1,A} + T_{n-1,C} \\ T_{n,B} &= T_{n-1,B} + T_{n-1,C} \\ T_{n,C} &= T_{n-1} \end{aligned} \quad \text{con dati iniziali } T_0 = 0 \text{ e } T_1 = 3$$

perciò sommando:

$$\begin{aligned} T_n &= T_{n,A} + T_{n,B} + T_{n,C} = \\ &= T_{n-1,A} + T_{n-1,C} + T_{n-1,B} + T_{n-1,C} + T_{n-1} = \\ &= 2T_{n-1} + T_{n-1,C} = 2T_{n-1} + T_{n-2} \end{aligned} \quad \text{da cui}$$
$$T_6 = 2T_5 + T_4 = 2(2T_4 + T_3) + (2T_3 + T_2) = \dots = 210.$$

- Fig. 12 -

2.4. Creazione e applicazione di procedure e algoritmi.

In questo ambito intendiamo raggruppare la ricerca di soluzioni rispetto a problematiche un po' più complesse, ludiche o derivanti da questioni quotidiane. Dunque va tenuta in considerazione

non solo la ricerca di “una” soluzione ma anche l’ottimizzazione della stessa.

Un esempio di livello elementare, per ora di semplice scrittura, è quello di ricapitolare, con una precisa descrizione, la serie di istruzioni che bisogna seguire per effettuare la divisione o la moltiplicazione tra due numeri, possibilmente di due o tre cifre.

Ritornando ad un problema già accennato in precedenza, si possono scrivere e risolvere quesiti che coinvolgono distanze, tempi e costi associati per andare da una città all’altra su una mappa, in modo che a criteri diversi si accordino meglio strade differenti.

Tutta una serie di giochi-problemi possono essere inclusi in questo ambito, se in essi è coinvolta la ricerca di una strategia risolutiva. Un esempio è il seguente.

Siamo bendati davanti ad un tavolo rotondo con sopra quattro bicchieri disposti in modo simmetrico (rispetto al centro) ed in posizione casuale (nella figura 13 le palline sono bianche, scure e con una croce ad indicare rispettivamente la posizione del bicchiere all’insù, capovolta, ignota). Dobbiamo portare tutti i bicchieri nella stessa posizione (capovolti o all’insù) ma potendo toccare soltanto due bicchieri per mossa, con il tavolo che viene fatto girare e fermato in posizione casuale prima di ogni nostra operazione. E’ possibile trovare una strategia sempre vincente? E’ possibile trovare una strategia vincente che porti tutti i bicchieri esclusivamente in posizione capovolta? La soluzione a questo bel quesito si trova nella figura 13.

La ricerca della strategia vincente è indispensabile per rispondere alla prima domanda, nella quale si chiede se tale soluzione esiste. Si può evincere dalla risoluzione che i passi da percorrere sono pochi e l’algoritmo, seppur semplice, è motivato da un ragionamento molto originale. Per capire il tipo di strategia da applicare ci sono due passaggi chiave: 1) la posizione casuale del tavolo esclude la certezza di poter toccare tutti e quattro i bicchieri, ma non la certezza di toccarne almeno tre; 2) la configurazione cui bisogna pervenire per la risoluzione definitiva è quella in cui su ogni diagonale i bicchieri sono disposti nello stesso modo.

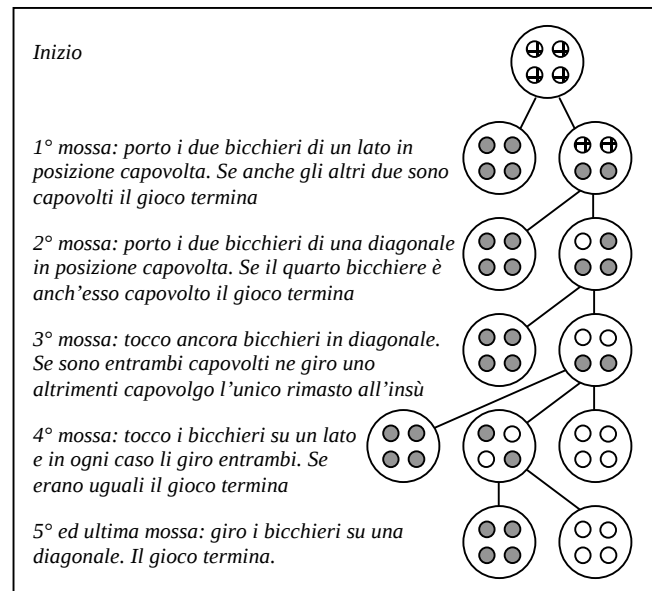
La risposta alla seconda domanda è invece negativa, in quanto non è possibile avere la certezza di portarli tutti in una posizione prefissata: una volta arrivati all’ultima mossa dipende tutto da quale diagonale tocchiamo e nulla può escludere che la dea bendata ci faccia toccare sempre la stessa. Dunque la risposta ai quesiti è differenziata e questa apparentemente piccola variazione va compresa.

Nel paragrafo successivo (§3) approfondiremo la problematica di ricerca degli algoritmi e delle procedure risolutive in ambito propriamente informatico.

2.5. Organizzazione e trattamento dell’informazione.

Questa ultimo ambito di problemi ha motivazioni e connessioni evidenti con le problematiche che la continua evoluzione tecnologica ci propone. Il trattamento delle informazioni nei modi più variegati, utilizzando codici di varia natura, consentono molteplici facilitazioni.

I primi problemi in questa direzione, a livello elementare, possono essere legati all’investigazione dei modi per ordinare degli oggetti utilizzando criteri differenti come colore, forma e dimensione e di classificare dei dati in grafici, tabelle o diagrammi ad albero. In secondo piano vi può essere l’esplorazione conoscitiva dell’uso dei codici per comunicare informazioni, con l’esempio notevole dei codici commerciali, i codici a barre e i codici ISBN. Può essere di interesse



- Fig. 13 -

anche la conoscenza della metodologia che gli scanner appositi usano per leggere le informazioni e per riconoscere eventuali errori di lettura, così come l'investigazione sui metodi per la correzione degli errori usata per la trasmissione di immagini digitalizzate dallo spazio o più in generale attraverso canali rumorosi.

A nostro avviso merita un capitolo a parte la crittografia, la sua storia, i metodi per codificare e le strategie di decrittazione utilizzate anche in contesti importanti, come nelle due guerre mondiali. Nell'ultimo paragrafo (§4) ci occuperemo di alcune tecniche, recenti e non, esclusivamente ludiche e realmente applicate, da utilizzare come buoni esercizi scolastici.

§3. Il ruolo dell'informatica nella risoluzione di alcuni problemi.

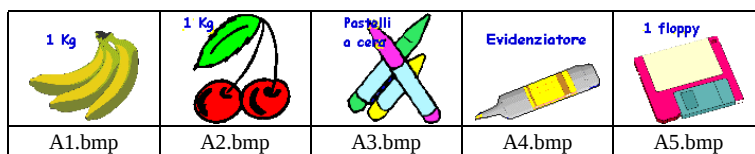
Il ricorso all'informatica per la risoluzione di problemi scolari è di interesse notevole poiché può favorire un approccio non traumatico alla matematica e non solo a questa. Riteniamo che oggi è anche molto opportuno ricorrere a mezzi multimediali per il fascino che tali mezzi esercitano sugli allievi. E' facile constatare come essi si motivino maggiormente in questo contesto ed a volte si lanciano a voler risolvere problemi anche non banali con uno scopo particolare, quello di realizzare un prodotto finito accattivante e di bell'aspetto. Gli scriventi ritengono che sia nostro compito il ricercare queste sinergie e ritengono pure che il mezzo multimediale presenta un interesse nuovo nell'uso e nell'insegnamento dell'informatica. Non è con questo che noi vogliamo criticare la didattica del passato consistente nel far costruire agli studenti qualche semplice programma in Pascal, questo è sempre utile. Casomai va solo rilevato che oggi ci sono prodotti nuovi ed alcune metodiche, sia pur note, hanno tendenza a divenire non solo linguaggi obsoleti ma anche di scarso impatto per l'interesse degli allievi.

Nei primi mesi del 2001 è stato pubblicato, da elementi del nostro gruppo di ricerca, un CD-Rom dal titolo "Pensare in Euro" realizzato da L. De Panfilis e G. Manuppella. Tale prodotto è stato poi allegato ad un testo di matematica per la Scuola Media (Tris) della casa editrice Paravia.

L'obiettivo che gli Autori si erano prefissato era quello, vista l'imminenza del passaggio dalla lira all'euro, di avvicinare gli alunni al momento del cambio della moneta in maniera ludica e semplice, ma didatticamente valida. Il problema era quello, lavorando solo graficamente, di presentare una serie di oggetti di uso comune con il loro costo in euro, di assegnare un budget in euro scelto in maniera casuale all'interno di quattro fasce (fino a 10 euro, da 10 a 100 euro, da 100 a 1000 euro e da 1000 a 10000 euro), di presentare una serie di oggetti scelti in maniera random all'interno di una di queste fasce e di invitare l'alunno a scegliere gli oggetti da acquistare senza superare il budget assegnato.

La difficoltà era quella, senza appesantire troppo il programma, di associare delle immagini ad una sequenza di numeri casuale e di presentarle per permetterne la scelta all'alunno. Non appena questa scelta è stata fatta il programma deve calcolare quanto è stato speso e se il budget è stato superato o meno. Alla complessità del problema da risolvere si aggiunge il fatto che si sta operando non con un linguaggio di programmazione potente ma con un programma autore (Neobook Professional nella versione 3.2f), che non ha grosse capacità in questo senso. Dopo attento studio, si è deciso di scegliere 80 immagini, divise in quattro serie da 20, a ciascuna delle quali è stata associata una variabile.

Nella figura 14 sono state riportate le prime 5 immagini della prima serie (le variabili considerate sono quindi A1, A2, ..., A20. Le altre 3 serie di immagini avranno quindi le



- Fig. 14 -

variabili B1, B2, ..., B20 per la seconda serie; C1, C2, ..., C20 per la terza serie; D1, D2, ..., D20 per la quarta serie. L'algoritmo che è stato studiato e usato è quello riportato nella Appendice 1.

Un secondo CD-Rom prodotto dal nostro gruppo e precisamente da F. Eugeni e R. Mascella, in una collaborazione tra il Dipartimento MET dell'Università di Teramo e l'Associazione ANFE Abruzzo nell'ambito del Corso Polivalente Biennale per Insegnanti di Sostegno, pur non avendo scopi diretti in ambito matematico, si inquadra anche in tematiche di tipo generale e nell'ottica del nostro discorso. Il Cd-Rom, dal titolo "Didattica per l'Handicap: Iper testi", è stato realizzato anch'esso con un programma autore (Macromedia Director versione 8.0) ed è un supporto multimediale contenente iper testi didattici su vari argomenti, finalizzati all'apprendimento di alcuni contenuti da parte di ragazzi portatori di handicap. Ci interessa innanzitutto rimarcare una delle ragioni alla base del progetto: l'ideazione, l'elaborazione, l'organizzazione e la preparazione finale di un iper testo, operazioni che nell'insieme debbono contemplare la conoscenza dell'argomento e la capacità di creare effetti multimediali, possono essere di alto livello, come metodologia di lavoro, per l'apprendimento dei contenuti in oggetto. Questo metodo può sembrare poco efficace, dispendioso di energie e superfluo, ma lo stimolo e l'enfasi per la costruzione del prodotto multimediale rende più leggero lo sforzo di acquisizione dei concetti, facendolo passare attraverso canali molto motivanti e collocandolo sullo sfondo dello scopo apparente, che è quello della creazione dell'iper testo, pur essendo, invece, lo scopo primario. In secondo luogo, inoltre, nella progettazione dell'iper testo vengono affinate capacità logiche e di problem solving, di deduzione e di associazione dei concetti, a causa delle svariate problematiche che in esso compaiono. In altre parole questa attività rappresenta, e non soltanto per lo studente, un esempio concreto di situazione complessa, multiforme, da risolvere con ragionamento tipicamente discreto.

§4. Un ambiente fonte di problemi discreti: la crittografia.

La crittografia, se adeguatamente semplificata e preparata per gli studenti, può avere un enorme potenziale nello sviluppare le capacità matematiche. In primo luogo essa dà alla matematica utilizzata uno sfondo teatrale intriso di mistero e avventura, in quanto nell'utilizzare le tecniche di cifratura è necessario costruire scenari in cui i ragazzi si scambiano i messaggi. In secondo luogo fornisce un modo naturale per portare gli studenti a scoprire da soli alcuni concetti chiave e, soprattutto negli eventuali tentativi di decrittazione dei messaggi, evidenzia la necessità di saper risolvere un problema, sfruttando il fatto che la sicurezza di un crittosistema spesso è legata alla nostra incapacità di risolvere un problema di algebra, di teoria dei numeri o di combinatorica.

Il primo approccio in questo ambito può avvenire utilizzando il *Metodo di Cesare* che effettua la cifratura utilizzando una sostituzione delle lettere dell'alfabeto. Per cifrare il messaggio occorre fissare soltanto un numero intero, più piccolo di 26, ad esempio 10, e rimpiazzare ogni lettera del messaggio in chiaro con la lettera che, nell'ordine usuale, si trova di seguito nella decima posizione. Unica accortezza deriva dal ricominciare a contare le posizioni dalla A una volta che il conteggio della posizione arriva alla Z, cioè in fondo all'alfabeto. Il concetto matematico in questo caso è quello di addizione in un gruppo ciclico.

Può essere interessante per uno studente anche il tentativo di rompere questo sistema di cifratura e, se l'attacco stenta a decollare, si può suggerire l'analisi delle frequenze utilizzando i testi scolastici usati nelle altre discipline.

Un secondo approccio si può fare con il *Metodo di Vigènère*, che sfrutta sempre un criterio di sostituzione delle lettere, ma stavolta per gruppi di caratteri utilizzando una parola chiave. Per il funzionamento del metodo rimandiamo al testo [4]. In questa breve descrizione diciamo solo che il concetto matematico utilizzato è legato alla cosiddetta *tabula recta*, la cui composizione è identica alla struttura additiva di Z_{26} , e che le operazioni di cifratura e decifratura sono semplici estensioni del metodo di Cesare. In questo caso la decrittazione del metodo è più complessa, dunque il tentativo dello studente è quasi sicuramente destinato a fallire, ma è possibile fare qualche passo in questa direzione suggerendo qual è il nodo centrale, ovvero la lunghezza della parola chiave iniziale, per poter utilizzare di nuovo la decrittazione del metodo di Cesare.

Esercizi molto interessanti si possono fare nella direzione dei codici a chiave pubblica. Un modello crittografico certamente intrigante, ma difficile da insegnare, è il *sistema RSA*. Le ragioni di queste difficoltà risiedono nella contemporanea presenza di molti concetti di teoria dei numeri: si spazia tra l'aritmetica modulare, numeri primi molto grandi e la funzione di Eulero. A questo proposito gli autori, ed altri, hanno di recente sviluppato un progetto, che attualmente è in fase di sperimentazione, per insegnare in modo ludico la tecnica RSA, attraverso la costruzione di un gioco RSA "semplificato" per ragazzi del primo ciclo di Scuola Secondaria (ved. [7]). Ci sembrano di interesse, infine, i due esempi che seguono, tratti dal sito riportato in bibliografia.

Il primo esempio è chiamato *Kid-RSA* ed il suo funzionamento è brevemente illustrato in figura 15. Le semplificazioni di questo modello sono notevoli, ma la filosofia di base è molto vicina a quella originale. Da un punto di vista didattico ci sembra che questo approccio possa essere molto utile poiché oltre a non utilizzare numeri primi molto grandi, non utilizza le potenze e non ha bisogno neppure della funzione di Eulero. Ciò che serve, come si evince, sono soltanto le quattro operazioni. Va tuttavia rilevato che questo metodo non si presta ad un vero utilizzo nella pratica quotidiana in quanto la sua decrittazione è banale. Anzi può essere anche un buon esercizio la ricerca, da parte degli studenti, di una tecnica per la sua rottura. A tale scopo, infatti, è sufficiente trovare un intero d tale che $ed = 1 \pmod{n}$.

Il secondo esempio è invece legato all'utilizzo di grafi e viene chiamato *Codice Perfetto a Chiave Pubblica*. La descrizione del suo funzionamento è in figura 16. Come piccola premessa definiamo in un grafo l'*intorno* di un vertice come l'insieme dei punti che sono connessi al vertice

Ogni ragazzo, nel nostro caso Alberto, calcola la sua coppia di chiavi nel seguente modo:

- Alberto sceglie due numeri naturali qualsiasi a e b e calcola $M = ab - 1$.
 - Alberto sceglie due altri naturali a' e b' e calcola
 $e = a'M + b$,
 $d = b'M + b$,
 $n = (ed - 1)/M = a'b'M + a'b + ab' + 1$.
- A questo la sua chiave pubblica è (e, n) mentre la chiave privata è (d, n) .

Siamo pronti per cifrare e decifrare il messaggio:

- ogni carattere dell'alfabeto viene tradotto in numero ($A = 0, B = 1, \dots, Z = 26$)
- il numero m viene **cifrato** nel numero c ottenuto moltiplicando em in modulo n cioè: $c = em \pmod{n}$
- il numero c viene **decifrato** nel numero m calcolando il prodotto dc in modulo n , infatti vale:
 $dc = dem = (Mn+1)m = m \pmod{n}$.

- Fig. 15 -

Dato un insieme di punti disposti su un foglio (15-25 punti), ciascun ragazzo costruisce il proprio grafo fissando il suo *codice perfetto* e tracciando una serie di archi (per far ciò: 1) fissa alcuni punti; 2) traccia un arco tra ciascun punto non scelto ed uno dei punti fissati; 3) traccia tutti gli archi che vuole tra i soli punti non scelti).

La costruzione delle chiavi è ultimata: il codice perfetto è la propria chiave privata, il grafo nel suo complesso è la propria chiave pubblica.

Supponiamo che il messaggio è il numero m e che Alberto vuole trasmetterlo a Barbara. Alberto scrive su ogni vertice un qualsiasi numero intero in modo tale che la somma complessiva dia esattamente m . Quindi sulla chiave pubblica di Barbara scrive, in corrispondenza di ogni vertice, la somma dei numeri che si trovano sui vertici del suo intorno. Questa serie di numeri sul grafo pubblico di Barbara è il messaggio cifrato.

In fase di decifrazione Barbara ottiene il messaggio m , semplicemente sommando i numeri che si trovano sul proprio codice perfetto (chiave privata).

- Fig. 16 -

in questione tramite un arco, incluso lo stesso vertice, e un *codice perfetto* come un sottoinsieme di vertici tali che ogni vertice, sia interno che esterno al sottoinsieme, appartenga all'intorno di un solo vertice. In altre parole ogni vertice è congiunto ad un solo vertice del codice perfetto.

A nostro avviso questo esempio sembra essere un sistema crittografico a chiave pubblica didatticamente molto efficace. Oltre alla costruzione del modello grafico, la strategia, nel suo complesso, non è difficoltosa ed i calcoli da fare sono esclusivamente addizioni. Anche la sua decrittazione può essere sottoposta all'analisi degli studenti, sempre in modo ludico. A prima vista il problema della rottura del codice può sembrare troppo difficile da affrontare in quanto la ricerca dei codici perfetti nei grafi può essere estremamente complessa (in generale non esiste un algoritmo "veloce" per effettuare questo tipo di ricerca),

ma in realtà occorre conoscere soltanto un po' di algebra lineare.

In effetti ogni messaggio inviato può essere rappresentato attraverso una serie di equazioni (per ogni vertice si scrive un'equazione che sintetizzi il fatto che ogni "intorno" produce tale numero, ad esempio se i vertici sono etichettati con $a, b, \dots, t$, le equazioni assumono la forma:

$a + e + f + h + l + s = 21$; $b + f + k + m + n + p + t = 45$; ecc.) ed i numeri iniziali sconosciuti in cui è stato suddiviso il messaggio m si trovano facilmente attraverso una serie di eliminazioni fra le varie equazioni. Dunque la conoscenza della procedura di eliminazione delle incognite fra le equazioni, le cosiddette eliminazioni di Gauss, risolve di fatto il problema della decrittazione.

Bibliografia.

- [1] M. CERASOLI, F. EUGENI, M. PROTASI, *Elementi di Matematica Discreta*, Zanichelli Editore, Bologna, 1988.
- [2] F. EUGENI, *La Matematica Discreta attraverso i problemi*, Atti del Convegno "Mathesis Centenario 1895-1995": Cento anni di matematica, Fratelli Palombi Editori, Roma, 1996.
- [3] F. EUGENI, *Le due rivoluzioni matematiche del secolo: da Bourbaki alla Matematica del discreto*, Periodico di Matematiche, vol. 68, nr. 1 (1992), pp. 3-21.
- [4] A. SGARRO, *Codici Segreti*, Ed. Mondadori Giochi, Milano, 1989.
- [5] L. DE PANFILIS, G. MANUPPELLA, *Pensare in Euro*, Cd allegato a Tris - testo scolastico per la Scuola Media, Ed. Paravia, 2001.
- [6] F. EUGENI, R. MASCELLA, *Didattica per l'Handicap: Ipertesti*, Supporto multimediale didattico nell'ambito del Corso Polivalente Biennale per Insegnanti di Sostegno, a cura dell'ANFE Abruzzo, Teramo, 2001.
- [7] F. EUGENI, R. MASCELLA, *A Note on Generalized Fibonacci Numbers*, Journal of Discrete Math. Sciences & Cryptography, vol. 4, nr. 1 (2001), pp. 33-45, Academic Forum Ed., N. Delhi.
- [8] F. EUGENI, R. MASCELLA, D. TONDINI, *La crittografia a chiave pubblica per giocare e imparare: il gioco del codice RSA*, Periodico di Matematiche, vol. 1, nr. 1 (2001), pp. 77-84.
- [9] <http://www.math.washington.edu/~koblitz/crlogia.html>

Appendice 1: Codice per la selezione delle immagini (dal Cd-rom “Pensare in Euro”).

0) In questa prima fase si inizializzano le variabili.

```
SetVar "[bar_graph]" ""
SetVar "[DIECI]" "0"
SetVar "[TIPO]" "A"
SetVar "[RNN[OGGETTO]]" ""
SetVar "[CONTATORE]" "1"
While "[CONTATORE]" "<" "11"
```

1) Si scelgono gli oggetti.

```
:START
Random "20" "[NUMOGGETTO]"
StrIns "[TIPO]" "[NUMOGGETTO]" "1" "[OGGETTO]"
```

2) Si controlla se l'oggetto è stato già scelto.

```
SetVar "[ARRAY_COUNT]" "1"
While "[ARRAY_COUNT]" "<" "10"
If "[OGGETTO]" "=" "[RNN[ARRAY_COUNT]]"
GotoLine "START"
EndIf
SetVar "[ARRAY_COUNT]" "[ARRAY_COUNT]+1"
EndWhile
```

3) Si mettono in un array gli oggetti selezionati

```
SetVar "[RNN[CONTATORE]]" "[OGGETTO]"
SetVar "[CONTATORE]" "[CONTATORE]+1"
EndWhile
GotoPage "10 Euro 1"
```

4) Si calcola la posizione dell'oggetto sulla pagina e viene mostrato (I riga)

```
SetVar "[ARRAY_COUNT]" "1"
While "[ARRAY_COUNT]" "<" "6"
Math "21+122.5*([ARRAY_COUNT]-1)" "" "[X]"
PopupImage "[X]" "85" "C:\archivio30\RNN[ARRAY_COUNT]].bmp"
"-1" "None" "0"
Math "[PREZZO[RNN[ARRAY_COUNT]]]" "2"
"[POSTO[ARRAY_COUNT]]"
.SetVar "[POSTO[ARRAY_COUNT]]"
"[PREZZO[RNN[ARRAY_COUNT]]]"
SetVar "[ARRAY_COUNT]" "[ARRAY_COUNT]+1"
EndWhile
```

5) Si calcola la posizione dell'oggetto sulla pagina e viene mostrato (II riga)

```
SetVar "[ARRAY_COUNT]" "6"
While "[ARRAY_COUNT]" "<" "11"
Math "21+122.5*([ARRAY_COUNT]-6)" "" "[X]"
PopupImage "[X]" "265"
"C:\archivio30\RNN[ARRAY_COUNT]].bmp" "-1" "None" "0"
Math "[PREZZO[RNN[ARRAY_COUNT]]]" "2"
"[POSTO[ARRAY_COUNT]]"
.SetVar "[POSTO[ARRAY_COUNT]]"
"[PREZZO[RNN[ARRAY_COUNT]]]"
SetVar "[ARRAY_COUNT]" "[ARRAY_COUNT]+1"
EndWhile
SetVar "[bar_graph]" ""
PopupImage "15" "429" "D:\Archivio30\Seleziona.BMP" "-1" "None"
"0"
```

6) Si scelgono gli oggetti.

```
SetVar "[AZZERA]" "1"
While "[AZZERA]" "<" "11"
SetVar "[PRESO[AZZERA]]" "No"
SetVar "[AZZERA]" "[AZZERA]+1"
EndWhile
```

7) Si calcola il costo totale in Euro degli oggetti scelti.

```
SetVar "[TOTALE]" ""
SetVar "[AZZERA]" "1"
While "[AZZERA]" "<" "11"
SetVar "[COSTO[AZZERA]]" "0"
SetVar "[AZZERA]" "[AZZERA]+1"
EndWhile
SetVar "[VAI]" "1"
```

8) Si mostrano gli oggetti scelti con il relativo prezzo.

```
SetVar "[RISULTATO]" ""
SetVar "[ARRAY_COUNT]" "1"
While "[ARRAY_COUNT]" "<" "[SELEZIONE]"
Math "25+122.5*([ARRAY_COUNT]-1)" "" "[X]"
SetVar "[ETICHETTA]" ""
StrIns "E" "[SELEZIONATO[ARRAY_COUNT]]" "1" "[ETICHETTA]"
PopupImage "[X]" "25"
"C:\archivio30\SELEZIONATO[ARRAY_COUNT]].bmp" "-1"
"None" "0"
PopupImage "[X]" "149" "C:\archivio30\ETICHETTA].bmp" "-1"
"None" "0"
SetVar "[ARRAY_COUNT]" "[ARRAY_COUNT]+1"
If "[ARRAY_COUNT]" "=" "6"
GotoLine "FILA2"
EndIf
EndWhile
:FILA2
If "[SELEZIONE]" "<=" "6"
GotoLine ":FINE"
EndIf
While "[ARRAY_COUNT]" "<=" "[SELEZIONE]"
Math "25+122.5*([ARRAY_COUNT]-6)" "" "[X]"
SetVar "[ETICHETTA]" ""
StrIns "E" "[SELEZIONATO[ARRAY_COUNT]]" "1" "[ETICHETTA]"
PopupImage "[X]" "205"
"C:\archivio30\SELEZIONATO[ARRAY_COUNT]].bmp" "-1"
"None" "0"
PopupImage "[X]" "329" "C:\archivio30\ETICHETTA].bmp" "-1"
"None" "0"
SetVar "[ARRAY_COUNT]" "[ARRAY_COUNT]+1"
If "[ARRAY_COUNT]" "=" "[SELEZIONE]"
GotoLine "FINE"
EndIf
EndWhile
:FINE
```

9) Si verifica se il budget è stato superato.

```
If "[TOTALE]" "<=" "[BUDGET]"
SetVar "[RISULTATO]" "Budget non superato!"
SetVar "[RISULTATO1]" "Hai disponibili ancora"
Math "[BUDGET]-[TOTALE]" "2" "[DIFFERENZA]"
SetVar "[EURO]" "euro"
Else
SetVar "[RISULTATO]" "Attenzione!!!"
SetVar "[RISULTATO1]" "Hai un debito di"
Math "[TOTALE]-[BUDGET]" "2" "[DIFFERENZA]"
SetVar "[EURO]" "euro"
EndIf
```